# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


## Μεταπτυχιακή Διατριβή
## στα Πληροφοριακά Συστήματα

# Μία Επισκόπηση Εργαλείων Ελέγχου Τρωτότητας Δίκτυο-κεντρικών Πληροφοριακών Συστημάτων


**Σπυρίδων Καββαδίας**

**Επιβλέπων Καθηγητής**
**Στέφανος Γκρίτζαλης**



**Ιούνιος 2013**

# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


# Μία Επισκόπηση Εργαλείων Ελέγχου Τρωτότητας Δίκτυο-κεντρικών Πληροφοριακών Συστημάτων


**Σπυρίδων Καββαδίας**

**Επιβλέπων Καθηγητής**
**Στέφανος Γκρίτζαλης**



Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

**Ιούνιος 2013**

# Περίληψη

Η διατριβή, περιλαμβάνει αναλυτική μελέτη και αξιολόγηση ενός μεγάλου αριθμού διαθέσιμων Εργαλείων Ελέγχου Τρωτότητας, δηλαδή μηχανισμών, εργαλείων, εφαρμογών και υπηρεσιών ασφάλειας χρήσιμα στην εύρεση ευπαθειών σε υπό εξέταση συστήματα. Αναπτύχθηκε ένα ολοκληρωμένο πλαίσιο σύγκρισης που περιλαμβάνει τρεις κλάσεις κριτηρίων με επιμέρους κριτήρια για κάθε μία από αυτές. Ως έλεγχο τρωτότητας (penetration testing) ενός δικτυοκεντρικού (net-centric) πληροφοριακού συστήματος περιγράφουμε τη διαδικασία που ακολουθείται προκειμένου να διαπιστωθεί αν ένα πληροφοριακό σύστημα είναι ευπαθές (vulnerable) σε απειλές (threats) που αφορούν την ασφάλειά του (security) και που ενδεχομένως θα μπορούσε να εκμεταλλευτεί ένας κακόβουλος χρήστης για να προκαλέσει ζημιά στο σύστημά μας ή να υποκλέψει ευαίσθητες πληροφορίες.

Το πρώτο μέρος περιλαμβάνει το Θεωρητικό υπόβαθρο των ελέγχων τρωτότητας. Στο **κεφάλαιο 2** περιγράφεται το πρόβλημα που καλούνται να αντιμετωπίσουν αυτά τα προγράμματα, το προφίλ των χρηστών που έχουν απέναντί τους και συγκεκριμένα αριθμητικά στοιχεία που επιβεβαιώνουν την μεγέθυνση του προβλήματος. Περιγράφονται οι διαδικασίες ενός ελέγχου τρωτότητας και στο **Κεφάλαιο 3** τα πιθανά σημεία εκκίνησης και οι στόχοι μίας διαδικασίας εύρεσης ευπαθειών. Στο **Κεφάλαιο 4** παρουσιάζονται συνοπτικά κάποια νομικά ζητήματα και στο **Κεφάλαιο 5** αναλύονται οι πέντε(5) φάσεις μιας δοκιμής διείσδυσης. Το **Κεφάλαιο 6** αφορά τη φάση της αναζήτησης πληροφοριών για το υπό εξέταση σύστημα. Περιγράφονται διαδικασίες, μέθοδοι και εργαλεία για την ολοκλήρωση αυτού του σταδίου. Κατά κανόνα τα προγράμματα που χρησιμοποιούνται εδώ δεν μπορούν να βοηθήσουν σε κάποια άλλη φάση. Επίσης είναι κρίσιμο για μία πετυχημένη δοκιμή διείσδυσης γι' αυτό και έγινε η επιλογή παρουσίασης του σε ξεχωριστό κεφάλαιο. Στο **Κεφάλαιο 7** παραθέτονται τα κριτήρια αξιολόγησης καθώς και το σκεπτικό επιλογής τους. Στο **Κεφάλαιο 8** κατηγοριοποιούνται τα εργαλεία ανάλογα με τον υπό εξέταση στόχο. Περιγράφεται η λειτουργίας τους και βασικά χαρακτηριστικά του καθενός. Σε ορισμένα αντί των πληροφοριών παρατίθεται ένα παράδειγμα ή μία περίπτωση χρήσης. Την παρουσίαση των προγραμμάτων της κάθε κατηγορίας ακολουθεί αξιολόγηση με βάση τα κριτήρια του κεφαλαίου 7, μόνο σε αυτές που κρίνεται χρήσιμο και ουσιώδες. Στο **Κεφάλαιο 9** επαναλαμβάνεται η διαδικασία περιγραφής και σύγκρισης εργαλείων αλλά μόνο για εργαλεία που αφορούν διαδικτυακές εφαρμογές. Το **Κεφάλαιο 10** περιέχει εργαλεία και εφαρμογές για κινητά 3η γενιάς και iPad. Η εργασία ολοκληρώνεται με κάποια συμπεράσματα

# Summary

The thesis includes a detailed study and evaluation of a large number of available vulnerability testing tools, ie instruments, tools, applications and services useful in finding security vulnerabilities in systems under consideration. An integrated framework comparison includes three classes of criteria to individual criteria for each of them. As vulnerability testing a Net Centric information system describes the procedure followed to determine whether a computer system is vulnerable to threats that a malicious user can exploit them and cause damage to our system or to steal sensitive information.

The first part contains the theoretical background of vulnerability checks. Chapter 2 describes the problem that these programs have to face, the user profiles that are specific to them and confirms the growth of the problem with concrete figures. The procedures of a vulnerability audit are described in Chapter 3, possible starting points and objectives of a process of finding vulnerabilities. Chapter 4 summarizes some legal issues and in Chapter 5 we analyze the five (5) phases of a penetration test. Chapter 6 deals with the phase of information gathering on the system under consideration. Describe the procedures, methods and tools to complete this step. Typically the programs used here cannot help in any other phase. It is also crucial for a successful penetration testing. Chapter 7 lists the evaluation criteria and the rationale for their choice. At Chapter 8 we categorized tools depending on the test target. And we describe their function and their basic characteristics. In some of them instead of an example we write down a use case or an example. Presentation of programs in each category followed by an evaluation based on the criteria of Chapter 7 only to those deemed useful and essential. Chapter 9 repeats the process of description and comparison of tools but only for web applications checks. Chapter 10 contains tools and applications for 3rd generation cellphones and iPad. The paper ends with some conclusions

## Περιεχόμενα

# 1. Εισαγωγή

Η παρούσα διπλωματική εργασία φιλοδοξεί να αποτελέσει μία εμπεριστατωμένη μελέτη εργαλείων ελέγχου τρωτότητας ενός υπό εξέταση δίκτυο-κεντρικού συστήματος. Παρουσιάζονται μηχανισμοί, εφαρμογές, και υπηρεσίες που στοχεύουν σε διαφορετικού τύπου συστήματα, με διαφορετικές ανάγκες και απαιτήσεις. Πραγματοποιείται αξιολόγηση των εργαλείων με βάση ένα ολοκληρωμένο πλαίσιο συγκριτικής αξιολόγησης.

Γίνεται αναφορά στα στάδια ενός ελέγχου, στη διαδικασία που είναι θεμιτό να ακολουθείται και στις διαφορετικές διαθέσιμες προσεγγίσεις για την επιτυχημένη επίτευξη αυτού.

## 1.1 Σκοπός της εργασίας.

Σκοπός ήταν η παράθεση όσο το δυνατόν περισσότερων εργαλείων για διαφορετικές περιπτώσεις. Αυτό βοηθάει τον αναγνώστη να αναγνωρίσει κυρίως διαφορετικά υπό εξέταση συστήματα και διαφορετικές περιπτώσεις ανίχνευσης ευπαθειών και να κατανοήσει τις διαφορετικές προσεγγίσεις που χρειάζεται σε κάθε περίπτωση. Κάθε κατηγορία εργαλείων προσφέρεται για περαιτέρω έρευνα ανάλογα με τις ανάγκες του κάθε χρήστη.

Οι περιγραφές των εργαλείων έχουν κοινά στοιχεία μεταξύ τους ως προς τη δομή τους αλλά και σημαντικές διαφορές ως προς την παρουσίαση τους. Δεν υπάρχει αυστηρή δομή σε αυτή. Σε κάποια γίνεται αυστηρή παράθεση των χαρακτηριστικών τους ενώ σε άλλα παρουσιάζεται ο τρόπος λειτουργίας τους μέσω παραδειγμάτων και περιπτώσεων χρήσης. Επιλέχθηκε αυτή η προσέγγιση ώστε ο αναγνώστης της εργασίας να έχει μία σφαιρική άποψη για τη λειτουργία των προγραμμάτων σε θεωρητικό και πρακτικό επίπεδο. Λειτουργεί σαν ένας επιπλέον τρόπος κατανόησης της γενικής συμπεριφοράς εργαλείων που ανήκουν στην ίδια κατηγορία.

# 2. Ασφάλεια Πληροφοριακών Συστημάτων (IT Security) και Δοκιμές Διείσδυσης (Penetration Testing)

Οι έλεγχοι διείσδυσης μπορούν να αποκαλύψουν σε ποιο βαθμό η ασφάλεια των πληροφοριακών συστημάτων (ΠΣ) απειλείται από επιθέσεις hacker, cracker και γενικότερα κακόβουλων χρηστών και αν τα μέτρα και οι πολιτικές ασφάλειας είναι ικανά να εξασφαλίσουν την ασφάλεια των συστημάτων αυτών. Για μια πιο σαφή εικόνα των κινδύνων για την ασφάλεια των ΠΣ το κεφάλαιο αυτό ξεκινά με μια περίληψη των σημερινών απειλών και περιγράφει τα πιο κοινά χαρακτηριστικά των εισβολέων και τις πιο διαδεδομένες τεχνικές επίθεσης σε πληροφοριακά συστήματα. Ακολουθεί μία σύντομη καταγραφή τυπικών μέτρων ασφαλείας ΠΣ,

μερικά από τα οποία μπορούν να ελεγχθούν με δοκιμές διείσδυσης. Τέλος, εξηγείται η διαδικασία της επινόησης της έννοιας δοκιμές διείσδυσης. [9]

## 2.1. Απειλές

Η ετήσια έρευνα της εταιρείας Symantec για την επίδραση του Διαδικτυακού εγκλήματος εμφανίζει αύξηση 6% σε σχέση με το 2011 στο οικονομικό κόστος που προκαλούν αυτές οι επιθέσεις. Οι αναφορές της Norton CyberCrime υπολογίζουν το συνολικό κόστος του κύβερνο-εγκλήματος (cybercrime), για τους 12 μήνες του 2012, στο ποσό των 100 δισεκατομμυρίων δολαρίων.

Η μελέτη υπογραμμίζει την ανάπτυξη νέων μορφών εγκλήματος σε κοινωνικά δίκτυα και σε πλατφόρμες κινητών τηλεφώνων με 21% (1/5) των ενηλίκων να έχει υπάρξει θύμα και στα δύο παραπάνω ενώ για τα κοινωνικά δίκτυα μόνο το ποσοστό φτάνει το 39%. [1]

Η αναφορά του Ponemon Institute που χρηματοδοτείται από την HP δημοσίευσε τα αποτελέσματα της έρευνας της για το 2012.

- 42% αύξηση των κύβερνο-επιθέσεων(cyber attacks) με τους μεγάλους οργανισμούς να αντιμετωπίζουν κατά μέσο όρο 102 επιτυχημένες επιθέσεις τη βδομάδα.
- 72% του κόστους προέρχεται από κακόβουλο κώδικα, D.O.S., κλεμμένες συσκευές και εργαζομένους με κακές προθέσεις
- Ο μέσος χρόνος επαναφοράς μετά από επιθέσεις είναι 24 μέρες

Τα αποτελέσματα επιβεβαιώνουν την ανάγκη για βελτιωμένες πολιτικές ασφάλειας που λαμβάνουν υπ' όψιν την πρόληψη εκτός της ανάκτησης και ανίχνευσης. [2]

Σύμφωνα με την ετήσια αναφορά του OWASP (Open Web Application Security Project ) οι 10 πιο συχνά εμφανιζόμενες απειλές για το 2013 είναι οι παρακάτω. [3]

A1 – Injection
A2 – Cross Site Scripting /XSS
A3 – Broken Authentication / Session Management
A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery
A6 – Security Misconfiguration
A7 – Insecure Cryptographic Storage
A8 – Failure to Restrict URL Access
A9 – Insufficient Transport Layer Protection
A10 – Unvalidated Redirects and Forwards

### 2.1.1. Το προφίλ των Εισβολέων.

Στα μέσα μαζικής ενημέρωσης, ο όρος hacker χρησιμοποιείται για οποιοδήποτε πρόσωπο εισβάλλει σε άλλα πληροφοριακά συστήματα χωρίς εξουσιοδότηση. Ωστόσο, μια λεπτότερη διάκριση γίνεται συχνά μεταξύ hacker, cracker και script kiddies. Ενώ οι hacker θεωρούνται ως πειραματικά μυαλά προγραμματιστών που στοχεύουν σε κενά ασφάλειας στα συστήματα πληροφορικής για τεχνικούς λόγους, οι cracker είναι άτομα που διαπράττουν εγκληματικές ενέργειες που εκμεταλλεύονται τα αδύνατα σημεία των ΠΣ είτε για να αποκτήσουν παράνομο δικαίωμα εισόδου σε ένα σύστημα είτε για την κοινωνική προσοχή και σεβασμό.

Τα script kiddies είναι εισβολείς οι οποίοι συνήθως δεν έχουν βάθος γνώσεων και καθοδηγούνται από την περιέργεια να γνωρίσουν κάποια εργαλεία που «κατεβάζουν» από το διαδίκτυο.

Οι Cracker που έχουν προνομιακή γνώση σχετικά με την οργάνωση που επιτίθενται ονομάζεται Insiders. Συχνά πρόκειται για απογοητευμένους (πρώην) εργαζόμενους ενός οργανισμού, οι οποίοι χρησιμοποιούν τις γνώσεις τους με κακόβουλο τρόπο. Ο κίνδυνος που προέρχεται από τους insiders είναι ιδιαίτερα μεγάλος, επειδή είναι εξοικειωμένοι με την τεχνική και οργανωτική υποδομή και μπορεί ήδη να γνωρίζουν λεπτομέρειες σχετικά με τις υπάρχουσες αδυναμίες.

Εκτός από τις κατηγορίες που περιγράφονται παραπάνω, η βιομηχανική κατασκοπεία αποτελεί επίσης μια σοβαρή απειλή. Ο στόχος της βιομηχανικής κατασκοπείας είναι η απόκτηση γνώσης του επιχειρηματικού απορρήτου, όπως τα καινοτόμα τεχνικά σχέδια, στρατηγικές και ιδέες που βοηθούν στο να αποκτήσουν ανταγωνιστικό πλεονέκτημα και να χρησιμοποιούν αυτές τις πληροφορίες για προσωπικό όφελος.

### 2.1.2. Μέθοδοι.

Υπάρχουν διάφοροι τρόποι διαχείρισης προετοιμασίας ή καταστροφής πληροφοριακών συστημάτων.

- **Επιθέσεις βασισμένες στο διαδίκτυο(Network based)**. Είναι επιθέσεις σε στοιχεία του δικτύου, σε συστήματα ηλεκτρονικών υπολογιστών και σε εφαρμογές που χρησιμοποιούν λειτουργίες του IP/TCP πρωτοκόλλου του δικτύου. Αυτού του είδους οι επιθέσεις εκμεταλλεύονται αδυναμίες ή ελλείψεις σε εξοπλισμό και λογισμικό για την προετοιμασία ή την εκτέλεση επιθέσεων.
  Περιλαμβάνουν ανίχνευση για ανοιχτές πόρτες(port scanning), IP Spoofing, Sniffing, Session hijacking, DoS επιθέσεις, υπερχείλιση μνήμης(buffer overflow), επιθέσεις συμβολοσειράς και εκμετάλλευση αδυναμιών σε Λειτουργικά Συστήματα και στο Πρωτόκολλο του Διαδικτύου.

- **Επιθέσεις Κοινωνικής Μηχανής(Social Engineering).** Είναι προσπάθειες να χειραγωγήσουν τους ανθρώπους με προνομιακή γνώση και να τους οδηγήσουν σε αποκαλύψεις που σχετίζονται με την ασφάλεια πληροφοριών, όπως κωδικούς πρόσβασης. Για παράδειγμα, ένας εισβολέας θα μπορούσε να προσποιηθεί ότι είναι ένας υπάλληλος πληροφορικής ενός οργανισμού ώστε να εξαπατήσει έναν ανυποψίαστο χρήστη στην αποκάλυψη του κωδικού πρόσβασης του δικτύου. Το εύρος των πιθανών σεναρίων επίθεσης, με αυτήν την τεχνική, είναι ιδιαίτερα μεγάλο. Με την ευρύτερη έννοια του όρου, η κοινωνική μηχανική μπορεί να καλύψει, επίσης, τις περιπτώσεις στις οποίες ευαίσθητες πληροφορίες ασφάλειας λαμβάνονται από εκβιασμούς.
- **Καταστρατήγηση των μέτρων φυσικής ασφάλειας.** Δεν μπορεί να υπάρξει ασφάλεια IT χωρίς τη φυσική ασφάλεια της τεχνικής υποδομής. Αν, τα φυσικά μέτρα ασφαλείας ξεπεραστούν και η φυσική πρόσβαση στα συστήματα πληροφορικής έχει αποκτηθεί, είναι μόνο θέμα χρόνου πριν πραγματοποιηθεί επίθεση ή χειραγώγηση των αποθηκευμένων δεδομένων και εφαρμογών. Ένα παράδειγμα είναι η μη εξουσιοδοτημένη είσοδος στο κέντρο πληροφορικής ενός οργανισμού και την απομάκρυνση του σκληρού δίσκου στον οποίο είναι αποθηκευμένα τα εμπιστευτικά δεδομένα. Αυτή η κατηγορία περιλαμβάνει επίσης την αναζήτηση των σκουπιδιών για έγγραφα με κρίσιμες, για την ασφάλεια πληροφορίες (dumpster diving).

## 2.2. Εννοιολογική προέλευση των δοκιμών διείσδυσης (Penetration Tests).

Ο όρος "δοκιμή διείσδυσης» και οι μέθοδοι που χρησιμοποιούνται για τον έλεγχο αυτό εμφανίστηκαν το 1995, όταν ο παρουσιάστηκε ο πρώτος σαρωτής ευπαθειών, βασιζόμενος στα UNIX. Το όνομα του ήταν «SATAN». Εκείνη την εποχή, το πρόγραμμα αυτό ήταν το πρώτο εργαλείο που ήταν σε θέση να ανιχνεύσει αυτόματα τους υπολογιστές για τον εντοπισμό τρωτών σημείων.

Σήμερα, υπάρχουν μια σειρά από δωρεάν και μη σαρωτές ευπάθειας, οι περισσότεροι εκ των οποίων έχουν δυνατότητα ενημέρωσης της βάσης δεδομένων τους με νέες γνωστές αδυναμίες του υλικού και του λογισμικού. Αυτά τα εργαλεία είναι ένας βολικός τρόπος για τον εντοπισμό των τρωτών σημείων στα συστήματα που δοκιμάζονται και ως εκ τούτου τον προσδιορισμό των κινδύνων. Συνήθως, οι πληροφορίες που παρέχονται από αυτά τα εργαλεία περιλαμβάνουν μια τεχνική περιγραφή της ευπάθειας και δίνουν οδηγίες για το πώς να εξαλείψει κάποιος ένα αδύναμο σημείο αλλάζοντας ρυθμίσεις.

Επιπλέον, ένας μεγάλος αριθμός δωρεάν εργαλείων για την εκτέλεση ή την προετοιμασία επιθέσεων σε υπολογιστές στο internet και τα δίκτυα μπορούν να βρεθούν στο διαδίκτυο.

[35]

## 2.3. Διαδικασίες Δοκιμών Διείσδυσης.

Η διαδικασία για τη δοκιμή διείσδυσης περιγράφετε από τα παρακάτω βήματα.

1. **Έρευνα για πληροφορίες σχετικά με το σύστημα-στόχο**

Κάθε Η/Υ με πρόσβαση στο Διαδίκτυο έχει μία επίσημη IP διεύθυνση. Υπάρχουν Βάσεις Δεδομένων ελεύθερα προσβάσιμες που προσφέρουν πληροφορίες για τις IP διευθύνσεις κάθε πάροχο.

2. **Σάρωση στα συστήματα-στόχος για τις υπηρεσίες που προσφέρονται.**

Σάρωση των θυρών του Η/Υ για ανοιχτές πόρτες (port scan) και προσπάθεια να επισημανθούν οι υπηρεσίες που σχετίζονται με αυτές.

3. **Προσδιορισμός των συστημάτων και εφαρμογών**

Τα ονόματα και η έκδοση του λειτουργικού συστήματος και των εφαρμογών στα συστήματα-στόχους μπορούν να ταυτοποιηθούν με τη διαδικασία που ονομάζεται «fingerprinting»

4. **Έρευνα για ευπάθειες**

Πληροφορίες σχετικά με τις ευπάθειες των συγκεκριμένων λειτουργικών συστημάτων και εφαρμογών μπορούν να ερευνηθούν αποτελεσματικά χρησιμοποιώντας τις πληροφορίες που συγκεντρώθηκαν.

5. **Αξιοποίηση των τρωτών σημείων**

Ο εντοπισμός των ευπαθειών μπορεί να χρησιμοποιηθεί για την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο σύστημα ή να προετοιμάσει περαιτέρω επιθέσεις.

Η ποιότητα και η αξία μιας δοκιμής διείσδυσης εξαρτάται κυρίως από το βαθμό στον οποίο η δοκιμή μπορεί να ικανοποιήσει την προσωπική κατάσταση του πελάτη, δηλαδή πόσο μεγάλο μέρος του χρόνου και των πόρων του δοκιμαστή δαπανώνται για τον εντοπισμό των τρωτών σημείων που σχετίζονται με την πληροφοριακή υποδομή και πόσο δημιουργική είναι η προσέγγιση του ελεγκτή. Αυτή η διαδικασία δεν μπορεί να καλυφθεί στην παραπάνω γενική περιγραφή, και αυτή είναι η αιτία για το ότι υπάρχουν τεράστιες διαφορές στην ποιότητα των δοκιμών διείσδυσης ως υπηρεσία.

[12]

## 3. Ταξινόμηση και Στόχοι των Δοκιμών Διείσδυσης.

Αυτό το κεφάλαιο περιγράφει τα πιθανά σημεία εκκίνησης και τα κανάλια πρόσβασης για μια δοκιμή διείσδυσης, τα μέτρα ασφάλειας και προστασίας των Πληροφοριακών Συστημάτων που μπορεί να ελεγχθούν, και πως οι δοκιμές αυτές διαφέρουν από κριτικές ασφάλειας Πληροφοριακών Συστημάτων (IT Security Reviews) και IT ελέγχους(IT Audits).

### 3.1. Εκκίνηση και σημεία πρόσβασης για Δοκιμές Διείσδυσης

Τυπικά σημεία εκκίνησης ή τα σημεία της επίθεσης για μια δοκιμή διείσδυσης είναι firewalls, web servers, RAS σημεία πρόσβασης (π.χ. Modem, απομακρυσμένα σημεία πρόσβασης και συντήρησης) και ασύρματα δίκτυα. Λαμβάνοντας υπόψη τη λειτουργία τους ως πύλη μεταξύ του Διαδικτύου και του δικτύου της εταιρείας, τα firewalls είναι προφανείς στόχοι για απόπειρες επίθεσης και σημεία εκκίνησης για τις δοκιμές διείσδυσης. Οι Web servers έχουν ένα υψηλό δυνητικό κίνδυνο εξαιτίας των πολλαπλών λειτουργιών τους και τα τρωτά σημεία που προκύπτουν. Άλλοι διακομιστές οι οποίοι προσφέρουν υπηρεσίες που είναι προσβάσιμες εξωτερικά, όπως e-mail, FTP και DNS, θα πρέπει να περιλαμβάνονται στη δοκιμή όπως οι κανονικοί σταθμοί εργασίας.

#### 3.1.1 Δοκιμές Διείσδυσης (Penetration Tests), έλεγχος ασφάλειας Πληροφοριακών Συστημάτων(IT audit)

Πρόκειται για δύο έννοιες διαφορετικές. Σε αντίθεση με τις δοκιμές διείσδυσης, ο σκοπός των ελέγχων ασφάλειας Πληροφοριακών Συστημάτων είναι να εξετάσουν γενικά την υποδομή του ΠΣ όσον αφορά τη συμμόρφωση, την αποδοτικότητα, την αποτελεσματικότητα, κλπ. Δεν έχουν κατ 'ανάγκη στόχο την ανίχνευση ευάλωτων σημείων. Για παράδειγμα, μια δοκιμή διείσδυσης δεν περιλαμβάνει την εξακρίβωση του κατά πόσο σε περίπτωση βλάβης των στοιχείων υλικού ορισμένες λειτουργίες και δεδομένα θα μπορούσαν να αποκατασταθούν με ένα κανονικό backup. Ελέγχει μόνο αν τα δεδομένα αυτά θα μπορούσαν να προσεγγιστούν. Αυτό θα μπορούσε επίσης να περιλαμβάνεται σε ένα έλεγχο ασφαλείας, αλλά συνήθως από μια διαφορετική οπτική γωνία και όχι στο τεχνικό χαρακτηριστικό βάθος μιας δοκιμής διείσδυσης.

### 3.2. Στόχοι των Δοκιμών Διείσδυσης

Για την επιτυχή δοκιμή της διείσδυσης που ανταποκρίνεται στις προσδοκίες ενός οργανισμού, ο σαφής καθορισμός των στόχων είναι απολύτως απαραίτητος. Αν οι στόχοι δεν μπορούν να επιτευχθούν ή δεν μπορούν να επιτευχθούν αποτελεσματικά, ο ελεγκτής πρέπει να ενημερώνει τον πελάτη στην φάση της προετοιμασίας και να προτείνει εναλλακτικές διαδικασίες όπως ελέγχου ΠΣ(IT audit) ή συμβουλευτικές υπηρεσίες IT ασφάλειας.

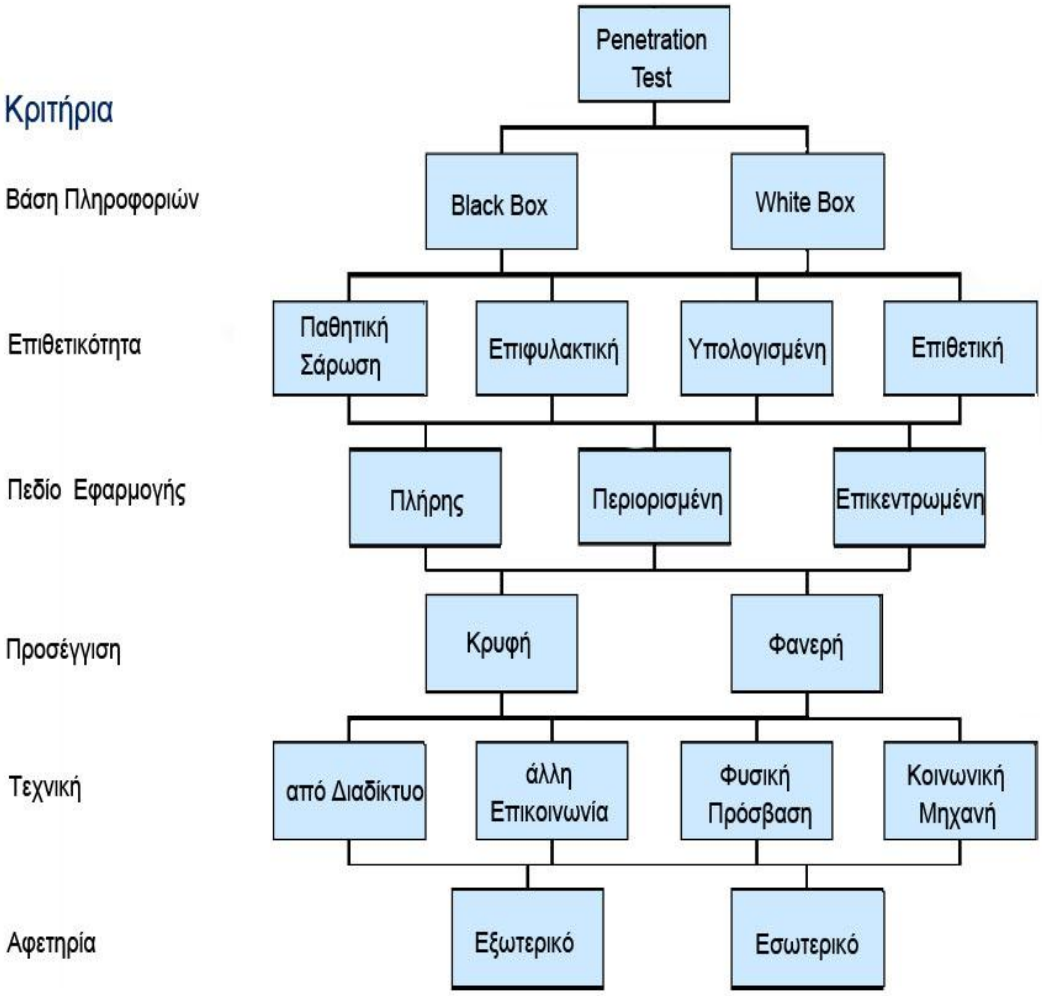
Οι στόχοι του πελάτη που μπορεί να επιτευχθούν με δοκιμή διείσδυσης μπορούν να διαιρεθούν σε τέσσερις κατηγορίες:

1. Βελτίωση της ασφάλειας των τεχνικών συστημάτων
2. Ο εντοπισμός τρωτών σημείων
3. Επικύρωση της Ασφάλειας του ΠΣ από ανεξάρτητο οργανισμό
4. Βελτίωση της ασφάλειας των οργανωτικών υποδομών και του προσωπικού

Το αποτέλεσμα της δοκιμή διείσδυσης θα πρέπει να είναι κάτι περισσότερο από ένας κατάλογος των υφιστάμενων αδυναμιών. θα πρέπει να προτείνει συγκεκριμένες λύσεις για την εξάλειψή τους.

### 3.3. Ταξινόμηση

Ποια κριτήρια είναι αυτά που περιγράφουν μια δοκιμή διείσδυσης, ή αυτά που ξεχωρίζουν τη μία από την άλλη; Χαρακτηριστικά, όπως η έκταση των υπό εξέταση συστημάτων, η επιφυλακτικότητα, η επιθετικότητα των δοκιμών, κλπ., που χαρακτηρίζουν μία συγκεκριμένη δοκιμή διείσδυσης θα πρέπει να προσαρμοστούν ώστε να ταιριάζουν με το στόχο της, προκειμένου να εξασφαλιστεί η πιο αποδοτική και αποτελεσματική δοκιμή με ένα υπολογισμένο κίνδυνο. Το σχήμα 1 δείχνει μία πιθανή ταξινόμηση των δοκιμών διείσδυσης. Στην αριστερή μεριά είναι έξι κριτήρια για τον προσδιορισμό τους, στα δεξιά είναι οι διάφορες τιμές για τα κριτήρια που συνοψίζονται σε ένα συμπαγές διάγραμμα δένδρου.




**Σχήμα 1:** Ταξινόμηση των δοκιμών ελέγχου

Αρχική πηγή: German Federal Office for Information and Security

Μια κατάλληλη δοκιμή της διείσδυσης - για την κάλυψη των στόχων του πελάτη πρέπει να καθορίζεται με βάση τα παραπάνω κριτήρια. Θα πρέπει να σημειωθεί ότι δεν είναι όλοι οι πιθανοί συνδυασμοί χρήσιμοι για δοκιμές, έστω και αν τα κριτήρια της ταξινόμησης έχουν διατηρηθεί όσο το δυνατόν πιο ευδιάκριτα. Μια επιθετική δοκιμή συνήθως εντοπίζεται πολύ γρήγορα και ως εκ τούτου δεν είναι ιδανική για συνδυασμό με την τεχνική της «κρυφής» προσέγγισης. Παρομοίως, ένα φανερό test διείσδυσης δεν είναι κατάλληλο, για παράδειγμα, για την απόκτηση εμπιστευτικών πληροφοριών από υπαλλήλους οι οποίοι είναι υποψιασμένοι λόγω προηγούμενων προσπαθειών εξαπάτησής τους μέσω κοινωνικής μηχανής.

Τα έξι κριτήρια και τις πιθανές τιμές τους συζητούνται παρακάτω:

**1. Βάση Πληροφοριών.** Ποιο είναι το αρχικό επίπεδο γνώσης του ελεγκτή διείσδυσης σχετικά με το δίκτυο-στόχο ή αντικείμενο; Μία θεμελιώδης διαφορά είναι μεταξύ του μαύρου κουτιού(black box) όπου ο δοκιμαστής δεν έχει καμία

γνώση εμπιστευτικών πληροφοριών και άσπρου κουτιού(White Box) όπου ο ελεγκτής έχει γνώση τέτοιων πληροφοριών.

i) Black Box: Προσομοιώνει ρεαλιστικά μια επίθεση από ένα τυπικό hacker στο internet. Ο hacker πρέπει να ερευνήσει τις απαραίτητες πληροφορίες που διατίθενται σε δημόσια προσβάσιμες βάσεις δεδομένων ή να κάνει «ερωτήματα» σαν εξωτερικός χρήστης.

ii) White Box: Δοκιμή μιας επίθεσης από έναν (πρώην) υπάλληλο ή εξωτερικό πάροχο υπηρεσιών με λεπτομερείς γνώσεις σε συγκεκριμένους τομείς. Η έκταση αυτής της γνώσης μπορεί να είναι περιορισμένη, π.χ. από έναν υπάλληλο ο οποίος έχει εργαστεί στην εταιρεία μόνο για ένα μικρό χρονικό διάστημα, είτε βαθιά όπως αυτή που αποκτήθηκε από έναν εξωτερικό πάροχο υπηρεσιών πληροφορικής που έχει εγκαταστήσει συστήματα και προγράμματα σχετικά με την ασφάλεια.

**2. Επιθετικότητα.** Πόσο επιθετικός είναι ο ελεγκτής διείσδυσης κατά τη διάρκεια της δοκιμής;

Για να υπάρχει μία επαρκής διάκριση, τέσσερα επίπεδα επιθετικότητας ορίζονται για τους σκοπούς αυτής της μελέτης:

- **Παθητική Σάρωση.** Τα αντικείμενα υπό δοκιμή διερευνώνται μόνο παθητικά. Τυχόν αδυναμίες που εντοπίζονται δεν αξιοποιούνται.
- **Επιφυλακτική.** Οι αδυναμίες που εντοπίζονται αξιοποιούνται μόνο όταν το σύστημα που θα εξεταστεί δεν «επιβαρυνθεί» από τις δοκιμές. Π.χ. χρησιμοποιώντας γνωστούς, προεπιλεγμένους κωδικούς πρόσβασης ή προσπαθώντας να αποκτήσει πρόσβαση σε καταλόγους σε ένα web server
- **Υπολογισμένη.** Ο ελεγκτής προσπαθεί να εκμεταλλευτεί τρωτά σημεία που θα μπορούσαν να οδηγήσουν σε διαταραχές του συστήματος. Αυτό περιλαμβάνει, για παράδειγμα, την προσπάθεια για αυτόματη ανάκαμψη των κωδικών πρόσβασης και την αξιοποίηση γνωστών ευπαθειών υπερχείλισης μνήμης σε καλά στοχευμένα Πληροφοριακά Συστήματα. Πριν από τη λήψη τέτοιων μέτρων, ο ελεγκτής κρίνει κατά πόσο είναι πιθανό να είναι επιτυχής η δοκιμή και πόσο σοβαρές πρόκειται να είναι οι συνέπειες.
- **Επιθετική.** Το υψηλότερο επίπεδο επιθετικότητας. Ο ελεγκτής προσπαθεί να εκμεταλλευτεί όλα τα πιθανά τρωτά σημεία, π.χ. υπερχειλίσεις μνήμης ακόμα και σε συστήματα-στόχους που δεν είναι σαφώς προσδιορισμένα, ή επιθέσεις DOS (Denial of Service ) όπου τα συστήματα ασφαλείας απενεργοποιούνται από εσκεμμένη υπερφόρτωση. Ο δοκιμαστής πρέπει να έχει υπόψιν του ότι εκτός από τα συστήματα που ελέγχονται μπορεί να προκαλέσει σφάλματα και αποτυχίες και σε γειτονικά συστήματα ή συστατικά του δικτύου.

**3. Πεδίο Εφαρμογής.** Ποια συστήματα πρέπει να δοκιμάζονται;

Όταν μια δοκιμή διείσδυσης διεξάγεται για πρώτη φορά, μια πλήρης δοκιμή πρέπει να λάβει χώρα προκειμένου να εξασφαλιστεί ότι δεν θα υπάρχουν κενά ασφαλείας στο σύστημα που δεν έχουν δοκιμαστεί.

Ο χρόνος που απαιτείται για μία δοκιμή διείσδυσης έχει άμεση σχέση με το πεδίο εφαρμογής των συστημάτων υπό διερεύνηση.

Εάν μόνο ένα συγκεκριμένο υπο-δίκτυο, σύστημα ή υπηρεσία πρόκειται να ελεγχθεί, για τους σκοπούς της διπλωματικής εργασίας, η δοκιμή διείσδυσης ονομάζεται **επικεντρωμένη**. Αυτό το πεδίο δοκιμής είναι σκόπιμο μετά από μια τροποποίηση ή επέκταση του συστήματος, για παράδειγμα. Μία τέτοια δοκιμασία μπορεί να προσφέρει πληροφορίες μόνο για το τμήμα του ΠΣ που εξετάστηκε και όχι γενικές και διευρυμένες γνώσεις περί αυτού του ΠΣ.

Σε μία **περιορισμένη** δοκιμή διείσδυσης, ένας περιορισμένος αριθμός συστημάτων ή υπηρεσιών εξετάζονται. Για παράδειγμα, όλα τα συστήματα στο DMZ, ή τα συστήματα που περιλαμβάνουν μία λειτουργική μονάδα που μπορεί να ελεγχθεί.

Μια **πλήρης** δοκιμή καλύπτει όλα τα διαθέσιμα συστήματα. Θα πρέπει να σημειωθεί ότι, ακόμη και σε πλήρη δοκιμή ορισμένα συστήματα, π.χ. ανάθεση σε εξωτερικούς συνεργάτες και συστήματα που φιλοξενούνται σε εξωτερικούς εξυπηρέτες(servers) δεν μπορούν να δοκιμαστούν.

**4. Προσέγγιση.** Πόσο ορατή είναι η ομάδα ελέγχου κατά τη διάρκεια των δοκιμών.

Εάν, εκτός από τα πρωτογενή συστήματα ασφαλείας, πρόκειται να δοκιμαστούν και δευτερεύοντα συστήματα-όπως ένα IDS, ή δομές οργανωτικές ή προσωπικές (π.χ. διαδικασίες κλιμάκωσης) η προσέγγιση των δοκιμών θα πρέπει να προσαρμοστεί αναλόγως:

Οι δοκιμές διείσδυσης που πραγματοποιούνται σε δευτερεύοντα συστήματα ασφαλείας και στις υφιστάμενες διαδικασίες κλιμάκωσης(escalation procedures) πρέπει - τουλάχιστον στην αρχή –να είναι συγκεκαλυμμένες(**κρυφές**). Στο αρχικό στάδιο των δοκιμών πρέπει να χρησιμοποιούνται μόνο μέθοδοι επίθεσης που δεν είναι άμεσα αναγνωρίσιμοι από το ΠΣ.

Εάν η κρυφή προσέγγιση αποτύχει να παράγει μια αντίδραση, ή μία δοκιμή white-box πραγματοποιηθεί σε συνεργασία με τους υπεύθυνους για το σύστημα χρησιμοποιείται η **φανερή** μέθοδος δοκιμής, όπως η εκτεταμένη σάρωση ανοιχτών πορτών(port scan) με μια άμεση σύνδεση με το ΠΣ. Το προσωπικό του πελάτη μπορεί να περιληφθεί στην ομάδα διεξάγει την φανερή white-box

δοκιμή. Αυτό είναι ιδιαίτερα καλό με πολύ κρίσιμα συστήματα, διότι συνεπάγεται ότι οι ελεγκτές είναι σε θέση να αντιδρούν ταχύτερα σε απροσδόκητα προβλήματα.

**5. Τεχνική.** Ποιες τεχνικές χρησιμοποιούνται για τη δοκιμή;

Σε ένα συμβατικό τεστ διείσδυσης, τα συστήματα προσβάλλονται μέσω του δικτύου μόνο. Επιπροσθέτως, υπάρχουν και άλλοι τύποι δοκιμών όπως των φυσικών επιθέσεων και τεχνικές κοινωνικής μηχανής που μπορεί να χρησιμοποιηθούν και από κακόβουλους χρήστες για να επιτεθούν σε συστήματα.

- Όταν μία δοκιμή διείσδυσης πραγματοποιείται **από το Διαδίκτυο** προσομοιώνει την κανονική διαδικασία, και μία τυπική επίθεση hacker. Τα περισσότερα δίκτυα χρησιμοποιούν σήμερα το πρωτόκολλο TCP / IP, γι' αυτό και τέτοιες δοκιμές ονομάζονται επίσης IP-based.
- Εκτός από δίκτυα TCP / IP υπάρχουν και **άλλα δίκτυα επικοινωνίας** που μπορούν επίσης να χρησιμοποιηθούν για την υλοποίηση μιας επίθεσης. Αυτά περιλαμβάνουν το τηλέφωνο και δίκτυα φαξ, ασύρματα δίκτυα για την κινητή επικοινωνία, π.χ. βασίζεται σε IEEE 802. και την τεχνολογία bluetooth.
- Σήμερα, η ασφάλεια των συστημάτων όπως τα firewalls κλπ. είναι διαδεδομένη, και η διαμόρφωση των εν λόγω συστημάτων αποδίδει συνήθως ένα υψηλό επίπεδο ασφάλειας, πράγμα που σημαίνει ότι είναι εξαιρετικά δύσκολο, αν όχι αδύνατο, να νικήσει κάποιος τέτοια συστήματα σε μια επίθεση. Είναι συχνά ευκολότερο και ταχύτερο να ληφθούν τα επιθυμητά ή απαραίτητα στοιχεία παρακάμπτοντας αυτά τα συστήματα με μια άμεση φυσική επίθεση. Μια **φυσική πρόσβαση** μπορεί, για παράδειγμα, να περιλαμβάνει άμεση πρόσβαση σε δεδομένα σταθμών εργασίας που δεν προστατεύονται από κωδικό μετά την απόκτηση μη εξουσιοδοτημένης πρόσβασης στο κτίριο και/ ή στο δωμάτιο του διακομιστή.
- Οι άνθρωποι είναι συχνά ο πιο αδύναμος κρίκος στην αλυσίδα της ασφάλειας και ο λόγος για τον οποίο τεχνικές **κοινωνικής μηχανής** που εκμεταλλεύονται ανεπαρκείς δεξιότητες ασφάλειας ή ανεπαρκής ευαισθητοποίηση σε θέματα ασφαλείας είναι συχνά επιτυχής. Οι δοκιμές αυτές είναι κατάλληλες μετά την παρουσίαση μιας γενικής πολιτικής για την ασφάλεια. Λάθος παραδοχές σχετικά με την υποτιθέμενη αποτελεσματικότητα μιας πολιτικής ασφαλείας συχνά οδηγεί σε κινδύνους για την ασφάλεια.

**6. Αφετηρία.** Από πού πραγματοποιείται η δοκιμή διείσδυσης.

Το σημείο όπου ο δοκιμαστής διείσδυσης συνδέει τον υπολογιστή του στο δίκτυο ή το σημείο από όπου ξεκινάει η προσπάθεια επίθεσης μπορεί να είναι είτε εντός είτε εκτός του δικτύου ή του κτιρίου του πελάτη.

- Οι περισσότερες επιθέσεις των κακόβουλων χρηστών πραγματοποιούνται μέσω της σύνδεσης του εσωτερικού δικτύου με το διαδίκτυο. Μια δοκιμή διείσδυσης από το **εξωτερικό** μπορεί να ανιχνεύει και να αξιολογήσει τον δυνητικό κίνδυνο μιας τέτοιας επίθεσης. Αυτές οι δοκιμές ελέγχουν συνήθως, το firewall, τα συστήματα στο DMZ και συνδέσεις RAS.

- Σε μια δοκιμή της διείσδυσης από το εσωτερικό, ο ελεγκτής κανονικά δεν χρειάζεται να ξεπεράσει τα τείχη προστασίας ή ελέγχου εισόδου την πρόσβαση στα εσωτερικά δίκτυα. Κατά συνέπεια, μια δοκιμή από το εσωτερικό μπορεί να αξιολογήσει τι επιδράσεις ενός λάθους στη διαμόρφωση του τείχους προστασίας, μιας επιτυχημένης επίθεσης στο τείχος προστασίας, ή μιας επίθεσης από άτομα με πρόσβαση στο εσωτερικό δίκτυο.

[75]

### 3.4. Πολυεπίπεδη προσέγγιση.

Προκειμένου να ελαχιστοποιηθούν οι κίνδυνοι, προτείνεται ένας συνδυασμός των διαφορετικών δοκιμών διείσδυσης βάση των παραπάνω κριτηρίων ταξινόμησης. Για παράδειγμα, μια επιφυλακτική, κρυφή black box δοκιμή μπορεί να διεξαχθεί από το εξωτερικό σε ένα πρώτο στάδιο, που ακολουθείται από μια επιθετική, φανερή white box δοκιμή από το εσωτερικό. Η προσέγγιση αυτή συνδυάζει τα πλεονεκτήματα μιας black box δοκιμής, είναι ρεαλιστική προσομοίωση μιας πραγματικής επίθεσης και έχει τα οφέλη μίας white box δοκιμής από την άποψη της αποτελεσματικότητας και του περιορισμού των ζημιών.

## 4. Νομικά Ζητήματα

Τα νομικά ζητήματα που πρέπει να λαμβάνονται υπόψη κατά τη διεξαγωγή των δοκιμών διείσδυσης μπορούν να χωριστούν σε δύο κατηγορίες.

- Νομικά ζητήματα που μπορούν να προκαλέσουν ή να παρέχουν κίνητρα σε μια επιχείρηση ή μια δημόσια αρχή να προβεί σε δοκιμές διείσδυσης.

- Νομικές διατάξεις και περιορισμούς όπου ο ελεγκτής πρέπει να τηρεί κατά την διεξαγωγή των δοκιμών οι οποίοι πρέπει να έχουν καθοριστεί με τον πελάτη πριν την εξέταση του ΠΣ.

Οι πιο σημαντικές νομοθετικές ρυθμίσεις που πρέπει να τηρούνται κατά τον καθορισμό και την υλοποίηση ελέγχων διείσδυσης αφορούν οδηγίες και νόμους σχετικές με την ασφάλεια πληροφοριακών συστημάτων επιχειρήσεων και οργανισμών που καλούνται να εφαρμόσουν τα κράτη μέλη της Ευρωπαϊκής Ένωσης για να υπάρχει οικονομική ανάπτυξη. Το 1992 εκδόθηκαν οι οδηγίες αυτές και το 2002 αναθεωρήθηκαν. Στην αναθεώρηση προτείνονται και οι καλές πρακτικές που πρέπει να ακολουθούνται για την αξιολόγηση της ασφάλειας μίας εταιρείας η οργανισμού. Αναφέρεται ότι η αξιολόγηση ασφάλειας είναι απαραίτητη για τη διαπίστωση κενών σε πολιτικές ασφάλειας, καταγράφονται πρακτικές, μέτρα αντιμετώπισης καθώς και διαδικασίες. Στις Η.Π.Α. διαχωρίζεται το νομικό πλαίσιο σε νόμους που αναφέρονται σε παράνομες ενέργειες εντός πληροφοριακών συστημάτων και σε νόμους που καθορίζουν με σαφείς οδηγίες την αξιολόγηση ασφάλειας.

Στην Ελλάδα υπάρχουν αναφορές περί γενικών ζητημάτων ασφάλειας στον ποινικό κώδικα στο Αρ.370 παρ.2

## 5. Οι Πέντε Φάσεις ενός Ελέγχου Διείσδυσης

Παρακάτω αναλύονται οι πέντε(5) φάσεις μιας δοκιμής διείσδυσης :

**Φάση 1: Προετοιμασία:** είναι δύσκολο να επιτευχθούν οι προσδοκίες μιας δοκιμής διείσδυσης χωρίς ενδελεχή προετοιμασία, που περιλαμβάνει μία αρχική συμφωνία σχετικά με τους στόχους του ελέγχου. Είναι αναγκαίο να καθοριστούν ευκρινώς ποια σημεία θα καλύψει η δοκιμή διείσδυσης. Πρέπει να λαμβάνει υπόψη όλες τις σχετικές νομικές διατάξεις από τις οποίες μπορούν να προκύψουν συνέπειες είτε ποινικού είτε αστικού δικαίου. Ο ελεγκτής πρέπει να εξασφαλίσει ότι οι διαδικασίες ελέγχου δεν πρόκειται να παραβιάσουν νομικές διατάξεις ή συμβάσεις.

Μια αποτυχία σωστής συνεννόησης κατά τη φάση της προετοιμασίας θα μπορούσε να οδηγήσει σε διαδικασίες προσφυγών, ως αποτέλεσμα των τεχνικών διείσδυσης που δεν έχουν συμφωνηθεί ή κινδύνων που συνδέονται με τις τεχνικές που χρησιμοποιήθηκαν και δεν είχαν τα αναμενόμενα αποτελέσματα, γι' αυτό είναι απαραίτητο να συζητηθεί και να τεκμηριωθεί η διαδικασία και οι κίνδυνοί της πριν την υλοποίηση των ελέγχων.

Όλες οι λεπτομέρειες που συμφωνήθηκαν θα πρέπει να τεθούν γραπτώς σε ένα συμβόλαιο.

**Φάση 2: Αναγνώριση:** Μετά τον καθορισμό των στόχων, του πεδίου εφαρμογής, των διαδικασιών, των μέτρα έκτακτης ανάγκης κλπ λαμβάνοντας υπόψη τις νομικές και οργανωτικές πτυχές και άλλες συνθήκες, ο ελεγκτής μπορεί να αρχίσει τη συλλογή πληροφοριών σχετικά με το στόχο. Αυτή η φάση είναι η δοκιμασία παθητικής διείσδυσης. Ο στόχος είναι να έχουμε μια πλήρη και λεπτομερή επισκόπηση των συστημάτων που είναι εγκατεστημένα, συμπεριλαμβανομένων των περιοχών που είναι ανοιχτές σε επιθέσεις ή γνωστά κενά ασφαλείας. Ανάλογα με τον αριθμό των υπολογιστών ή με το μέγεθος του δικτύου που πρέπει να εξεταστεί, το στάδιο της αναγνώρισης μπορεί να είναι εξαιρετικά χρονοβόρο. Αν, για παράδειγμα, ένα δίκτυο κλάσης C (256 πιθανές διευθύνσεις IP) πίσω από ένα τείχος προστασίας πρέπει να ελεγχθεί πλήρως, χρειάζεται μια πλήρη σάρωση σε όλες τις πόρτες του(ports) (όλες οι πόρτες είναι 65536) και μπορεί να διαρκέσει αρκετές εβδομάδες, ανάλογα με τη ρύθμιση. Ενώ αυτά τα βήματα δοκιμής συνήθως εκτελούνται αυτόματα, ο χρόνος που απαιτείται για την ολοκλήρωσή τους πρέπει να ληφθεί σοβαρά υπόψη κατά το σχεδιασμό. Έτσι, μια δοκιμή διείσδυσης μπορεί να διαρκέσει 20 ημέρες, για παράδειγμα, ή ακόμη και αρκετές βδομάδες.

**Φάση 3: Ανάλυση πληροφοριών και κινδύνων:** Μια επιτυχημένη, διαφανή και οικονομικά αποδοτική διαδικασία πρέπει να αναλύσει και να αξιολογήσει τις πληροφορίες που συγκεντρώθηκαν πριν από τα στάδια της ενεργής δοκιμής διείσδυση στο σύστημα - τα οποία συχνά είναι εξαιρετικά χρονοβόρα. Η ανάλυση πρέπει να περιλαμβάνει τους καθορισμένους στόχους της δοκιμής διείσδυσης, τους πιθανούς κίνδυνους για το σύστημα και τον εκτιμώμενο χρόνο που απαιτείται για την αξιολόγηση των πιθανών κενών ασφαλείας για στις επόμενες απόπειρες διείσδυσης. Οι στόχοι στην φάση 4 επιλέγονται με βάση την ανάλυση αυτή. Από τη λίστα των καθορισμένων στόχων ο ελεγκτής μπορεί, για παράδειγμα, να επιλέξει για δοκιμή μόνο εκείνες που περιέχουν γνωστά πιθανά τρωτά σημεία λόγω της διαμόρφωσής τους ή λόγω των εφαρμογών / υπηρεσιών που περιέχουν ή εκείνους για τους οποίους ο ελεγκτής είναι ιδιαίτερα πεπειραμένος.

Σε μία δοκιμή διείσδυσης για την οποία ο αριθμός των στόχων είναι σαφώς καθορισμένος στη φάση 2, ο αριθμός των συστημάτων στόχων για τη φάση 4 μειώνεται αυτόματα.

Οι περιορισμοί πρέπει να είναι πλήρως τεκμηριωμένοι και αιτιολογημένοι διότι εκτός από την επιθυμητή βελτίωση σε απόδοση, μπορούν επίσης να οδηγήσουν σε μείωση.

**Φάση 4: Ενεργές απόπειρες εισβολής:** Η φάση αυτή περιέχει τον υψηλότερο κίνδυνο μέσα σε μια δοκιμή διείσδυσης και θα πρέπει να γίνεται με τη δέουσα

προσοχή. Ωστόσο, μόνο αυτή η φάση αποκαλύπτει το βαθμό στον οποίο οι υποτιθέμενες αδυναμίες που εντοπίστηκαν στη φάση της αναγνώρισης αποτελούν πραγματικούς κινδύνους. Η φάση αυτή θα πρέπει να γίνει εάν η επαλήθευση των πιθανών τρωτών σημείων απαιτείται. Για συστήματα με πολύ υψηλές απαιτήσεις διαθεσιμότητας και ακεραιότητας, οι πιθανές επιπτώσεις πρέπει να εξετάζονται προσεκτικά πριν από την εκτέλεση κρίσιμων διαδικασιών δοκιμής, όπως η αξιοποίηση των κατορθωμάτων της υπερχείλισης ενδιάμεσης μνήμης (buffer overflow).

Σε ένα white box τεστ, ένα patch χρειάζεται ενδεχομένως να εγκατασταθεί σε κρίσιμα συστήματα πριν από την εκτέλεση της δοκιμής για την πρόληψη πιθανής βλάβης Η δοκιμή δεν θα είναι σε θέση να εντοπίσει τυχόν αδυναμίες, αλλά θα τεκμηριώσει την ασφάλεια του συστήματος. Σε αντίθεση με μια επίθεση hacking, ωστόσο, η δοκιμή διείσδυσης δεν είναι πλήρης - θα συνεχιστεί.

**Φάση 5: Τελική ανάλυση:** η τελική έκθεση θα πρέπει να περιλαμβάνει την αξιολόγηση των τρωτών σημείων που ανακαλύπτονται υπό τη μορφή πιθανών κινδύνων αλλά και συστάσεις για την εξάλειψη των αδυναμιών και των κινδύνων. Η έκθεση πρέπει να εγγυάται τη διαφάνεια των δοκιμών και τα τρωτά σημεία που παρουσιάζονται. Τα ευρήματα και αντίστοιχοι κίνδυνοι για την ασφάλεια θα πρέπει να συζητηθούν λεπτομερώς μετά την ολοκλήρωση των διαδικασιών δοκιμής.

## 6. Συγκέντρωση Πληροφοριών(Information Gathering)

Η φάση αυτή χωρίζεται στην ενεργητική και παθητική αναζήτηση. Παθητική χαρακτηρίζεται η διαδικασία αναζήτησης πληροφοριών για ένα υπό εξέταση στόχο σε πηγές ξεχωριστές από αυτόν(π.χ. Google). Από την άλλη μέθοδοι που χαρακτηρίζονται ενεργητικοί αφορούν άμεση αλληλεπίδραση με τα αγαθά του συστήματος-στόχου (π.χ. port scanning).

Ανάλογα με τον τύπο του ελέγχου διείσδυσης (ο στόχος μπορεί να είναι γνωστός ή όχι) υπάρχουν διαφορετικές προσεγγίσεις στην εύρεση πληροφοριών. Σε ένα whitebox test όλοι οι στόχοι είναι γνωστοί ενώ σε ένα blackbox test δεν γνωρίζουμε τίποτα για το υπό εξέταση σύστημα και πρέπει πρώτα να βρεθούν πληροφορίες σχετικά με τον στόχο και μετά σχετικά με τα αγαθά του..

Η πληροφόρηση είναι ένα όπλο γι' αυτό και ο υπεύθυνος ασφάλειας πρέπει να ανιχνεύσει όσο το δυνατόν περισσότερες πληροφορίες για το υπό εξέταση σύστημα για μια επιτυχημένη δοκιμή διείσδυσης. Αυτός είναι ο λόγος, που η συλλογή πληροφοριών είναι το πρώτο βήμα της διαδικασίας ελέγχου ευπαθειών.

Μερικές εκ των μη αυτόματων τεχνικών για τη συλλογή πληροφοριών περιλαμβάνουν:

- Αναζήτηση με Dorks

Με εξελιγμένες αναζητήσεις στη Google για:

Filetype: Αναζήτηση μόνο για συγκεκριμένους τύπους αρχείων

Inurl: Αναζήτηση κειμένου σε συγκεκριμένο δοθέν url.

Link: Αναζήτηση συνδέσμων με συγκεκριμένο περιεχόμενο.

Intitle: Αναζήτηση για κάποιον όρο μέσο στον τίτλο ενός εγγράφου.

Facebook Dorks:

Αναζήτηση Group: **site:facebook.com inurl(bofg | "bank of greece")**

Αναζήτηση δημοσιεύσεων τοίχου για ένα group: site:facebook.com **inurl:wall(bofg | "bank of greece")**

Αναζήτηση σελίδων: site:facebook.com inurl:pages (bogr |"bank of Greece")

Αναζήτηση δημόσιων προφίλ: allinurl: people "Καββαδίας Σπύρος" site:facebook.com

LinkedIn Dorks

Για δημόσια προφίλ: **site:linkedin.com inurl:pub(bofg|"bank of Greece")**

Για ενημερώσεις προφίλ: **site: linkedin.com inurl:updates(bofg|"bank of Greece")**

Για προφίλ της εταιρείας:site:**linkedin.com inurl:companies(bofg|"bank of Greece")**

- Επιπλέον σε κοινωνικές μηχανές αναζήτησης(Social Network Search Engines). Υπάρχουν διάφορες μηχανές αναζήτησης που ψάχνουν και δημοσιευμένες πληροφορίες στα κυριότερα κοινωνικά δίκτυα(social networks). Το αρνητικό σχετικά με αυτά της μηχανές είναι ότι βρίσκουν μόνο δημόσιες πληροφορίες.

Twitter: Search.twitter.com

Wink :http://wink.com

Spock: http://spock.com. Διαθέτει και επιλογή για αναζήτηση ιδιωτικών πληροφοριών αλλά όχι σαν δωρεάν υπηρεσία.

Social mention: http://socialmention.com

Whos Talkin: http://www.whostalkin.com

Samepoint: http://www.samepoint.com

OneRiot: http://ww.oneriot.com

Kosmix: http://kosmix.com

YackTrack: http://www.yacktrack.com

Keotag: http://www.keotag.com

Twoogle: http://twoogel.com (Συνδυασμένη αναζήτηση σε Google/Twitter)

KnowEm Username Check: http://knowem.com

Firefox Super Search Add-on: https://addons.mozilla.org/en-US/firefox/addon/13308 (περισσότερες από 160 μηχανές αναζήτησης).

- Αναζήτηση για video και φωτογραφίες σε κοινωνικά δίκτυα και social bookmarking sites.

Pixsy: http://www.pixsy.com

Flickr: http://www.flickr.com/search/?s=rec&w=all&q=”companyname”&m=text

YouTube/Google Video: http://video.google.com/videosearch?q=”companyname”

Junoba Social Bookmark Search: http://www.junoba.com (Digg, Delicious,Reddit κτλ.)

- Υπηρεσίες επί πιστώσει

Filtrbox: http://www.filtrbox.xom

Vocus: http://vocus.com

- Αναζήτηση σε Blogs

Η εξερεύνηση των blogs μπορεί να πραγματοποιηθεί με μία οποιαδήποτε μηχανή αναζήτησης. Ωστόσο αυτό που θα κάνει τη διαφορά σε ένα έλεγχο διείσδυσης και στην αναζήτηση πληροφοριών πιο συγκεκριμένα είναι τα σχόλια στα άρθρα μέσα στα blogs ειδικότερα πρώην και απογοητευμένων υπαλλήλων. Ένα άλλο ενδεχόμενο είναι ότι οι εργαζόμενοι της εταιρείας παραβιάζουν τις πολιτικές

δημοσίευσης πληροφοριών σε άρθρα με αποτέλεσμα να βλάπτουν τη φήμη της εταιρείας και να εκθέτουν ευαίσθητες πληροφορίες που βάπτουν την ασφάλειά της.

Κάποιες από τις ιστοσελίδες που προσφέρουν υπηρεσίες διερεύνησης σε blog και σχόλια είναι :

Social Mention: http://socialmention.com (εξελιγμένη υπηρεσία αναζήτησης σε σχόλια και RSS για παρακολούθηση των αποτελεσμάτων)

Google Blog Search: http://blogsearch.google.com

Blogpulse: http://www/blogpulse.com (διαθέτει και αναζήτηση για σχόλια).

Technorati: http://technorati.com/

IceRocket: http://www.icerocket.com

BackType: http://www.backtype.com

coComment: http://www.cocomment.com

- Αναζήτηση σε αποθετήρια εγγράφων(document repositories)

Αναζήτηση για έγγραφα εταιρειών.

Docstoc: http://www/docstoc.com

Scribd: http://www.scribd.com

SlideShare: http://slideshare.net

PDF Search Engine: http://www/pdf-search-engine.com/

Toodoc: http://www.toodoc.com

- Αναζήτηση meta στοιχείων μέσα σε έγγραφα και εικόνες

Τα metadata είναι δεδομένα μέσα στα δεδομένα. Συνήθως σε αυτά βρίσκομαι πληροφορίες σχετικά με τον συγγραφέα του και το πρόγραμμα που δημιουργήθηκε. Ένας κακόβουλος χρήστης μπορεί να εκμεταλλευτεί γνωστές ευπάθειες προγραμμάτων προσπαθώντας να διεισδύσει σε ένα σύστημα, να ανακαλύψει το Λειτουργικό Σύστημα που έχει, την ταυτότητα ενός χρήστη και ακόμη περισσότερα.

EXIFtool: http://www.sno.phy.queensu.ca/~phil/exiftool

Metagoofil: http://www/edge-security.com/metagoofil.php

Maltego(Διαθέτει λειτουργία για μετασχηματισμού metadata): http://www.paterva.com/web4/index.php/maltego

Meta-Extraxtor: http://meta-extraxtor.sourceforge.net/

FOCA http://www.informatica64.com/foca/

http://touchgraph.com/ --> Ψάχνει σε κοινωνικά δίκτυα

## 6.1. Αναγνώριση στόχου(Footprinting).

Σε αυτό το σημείο έχουμε άμεση και έμμεση αλληλεπίδραση με τον στόχο. Στόχος είναι η συλλογή πληροφοριών που σχετίζονται με τις τεχνολογίες και το περιβάλλον λειτουργίας του υπο εξέταση στόχου. Δεν πρέπει κάποιος ελεγκτής να πηγαίνει αμέσως σε αυτή τη φάση. Είναι απαραίτητο να υπάρχει επαρκής αναζήτηση πληροφοριών για το στόχο προηγουμένως. Είναι σύνηθες, για παράδειγμα, οι οργανισμοί να έχουν τα συστήματα τους εγκατεστημένα σε μεγαλύτερες εγκαταστάσεις με αποτέλεσμα την αναζήτηση σε λάθος και πολύ μεγαλύτερο εύρος IP από τη μεριά του ελεγκτή. Σημειώνεται ότι κάθε ενεργή εμπλοκή με ένα host πρέπει να είναι προεγκεκριμένη από τον οργανισμό που ζητάει τον έλεγχο για την αποφυγή ανεπιθύμητης προσοχής που μπορεί να οδηγήσει σε νομικές κυρώσεις.

Βασίζεται σε διάφορες τεχνικές. Ο κύριος στόχος αυτής της φάση είναι η εύρεση όλων των IP διευθύνσεων, το εύρος όλων των διευθύνσεων ενός Δικτύου καθώς και τα ονόματα των υποδικτύων(subdomains). Ανακαλύπτονται υπηρεσίες όπως mail, web, DNS που παρέχονται από ένα Server.

Πιο συγκεκριμένα οι πληροφορίες που αναζητούνται παρουσιάζονται στον παρακάτω πίνακα:

| **Τεχνολογία** | **Πληροφορίες που μπορούν να συλλεχθούν** |
|---|---|
| Internet | • Domain names<br>• Περιοχή διευθύνσεων δικτύου<br>• Διευθύνσεις IP των συστημάτων που είναι προσπελάσιμα μέσω internet<br>• Υπηρεσίες TCP και UDP που τρέχουν σε κάθε εντοπισμένο σύστημα<br>• Αρχιτεκτονική συστήματος (Sparc vs x86)<br>• Μηχανισμοί ελέγχου προσπέλασης και σχετιζόμενες λίστες ελέγχου<br>• προσπέλασης (Access ControlLists – ACL)<br>• Συστήματα εντοπισμού εισβολών (Intrusion Detection Systems – IDS) |

| | |
|---|---|
| | • Ενεργητική συλλογή πληροφοριών συστήματος (ονόματα χρηστών και ομάδων,<br>• προτροπές και μηνύματα συστήματος – banners, πίνακες δρομολόγησης,<br>• πληροφορίες SNMP)<br>• DNS hostnames |
| Intranet | • Χρησιμοποιούμενα πρωτόκολλα δικτύωσης (π.χ. IP, IPX, DecNET, κλπ)<br>• Εσωτερικά Domain names<br>• Περιοχή διευθύνσεων δικτύου<br>• Διευθύνσεις IP των συστημάτων που είναι προσπελάσιμα μέσω Intranet<br>• Υπηρεσίες TCP και UDP που τρέχουν σε κάθε εντοπισμένο σύστημα<br>• Αρχιτεκτονική συστήματος (Sparc vs x86)<br>• Μηχανισμοί ελέγχου προσπέλασης και σχετιζόμενες λίστες ελέγχου προσπέλασης (Access ControlLists – ACL)<br>• Συστήματα εντοπισμού εισβολών (Intrusion Detection Systems – IDS)<br>• Ενεργητική συλλογή πληροφοριών συστήματος (ονόματα χρηστών και ομάδων, προτροπές και μηνύματα συστήματος – banners, πίνακες δρομολόγησης, πληροφορίες SNMP) |
| Απομακρυσμένη πρόσβαση | • Αριθμοί αναλογικών/ψηφιακών τηλεφωνικών γραμμών<br>• Τύπος απομακρυσμένου συστήματος<br>• Μηχανισμοί πιστοποίησης ταυτότητας<br>• Δίκτυα VPN και σχετιζόμενα πρωτόκολλα (IPSec και PPTP) |
| Extranet | • Domain names<br>• Προέλευση και προορισμός σύνδεσης<br>• Τύπος σύνδεσης<br>• Μηχανισμοί ελέγχου πρόσβασης |

Πηγή: Scambray J.- McClure S. – Kurtz G.,2009

[37],[64]

### 6.1.1 Αναζήτηση στοιχείων.

Τα εργαλεία σε αυτή την φάση μπορούν να διαχωριστούν σε κατηγορίες ανάλογα με το τι ψάχνουν.

- Πληροφορίες για DNS

DnsEnum, Dnsmap, Dnsrecon, DnsTracer, Dns-Walk, Fierce, FindDomains, HostMap, Lynis, OpenMR, RATS, URLcrazy, CookieDigger, AdSuck DNS Server 2.4.1, Dnsgoblin, Active Whois, URLDIGGER,ritx, Dnsmap, dnsdumpster.com, DNSSenum

- Ανιχνευτές Email

Emailtrackerpro, Samspade, GEO Spider, Magic Netrace, 3d Visual Tracer

- Αναλυτές αναφορών(logs)

Logcheck

- Συγκομιδή ηλεκτρονικών διευθύνσεων(email harvesting).

theHarvester, Spahol

- Πληροφορίες από εφαρμογές flash και ActionScript

Deblaze

- Honeypot

Argos, Honeyd, Google Hack Honeypot, Single-honeypot, Fake AP, phoneyc

- Συγκομιδή meta-στοιχείων

FOCA, OOMetaExtractor, Exiftool

- Διαδικτυακές υπηρεσίες

4dnstools.com, DnsStuff.com, DnsTools.com, Mxtoolbox.com, Network-Tools.com, robtex.com, Shodan,Port check, Open Port Finder, Adhoc-IP Tools, who.is,ipcalc.org, domxssscanner.com, www.whoisxy.com, www.robtex.com

- Routing

0trace, Itrace, Lanmap2, Nat Probe, Netenum, Netmask, NMBscan, Protos, Tctrace, TCPtraceroute, IRPAS

- Contacts and domains

Recon-ng

- Μηχανές Αναζήτησης

Bing-ip2hosts,Binging, Creepy, Gggooglescan, GoogleHacker, Goorecon, Gooscan, Maltego, Metagoofil, Scroogle, Search Engine Assessment Toolkit (SEAT), SiteDigger, Subdomainer,Yeti, GoogleDiggity

- Ανιχνευτές Δικτύου(Network Scanners)

vTrace, NetworkMiner,Unicornscan,TripWire,dradis,pbnj,smtprc,Network Spoofer,Trout, SNScan, ScanLine, AutoScan

- Εύρεση ιστοσελίδας σύνδεσης ενός διαχειριστή(Admin Page Finder).

Admin Page Finder Script

- Διαδίκτυο(Web)

goohost

- Για εσωτερικό Δίκτυο

Arping. Βρίσκει τους hosts σε ένα δίκτυο. Είναι πολύ πιο γρήγορο από το nmap(Backtrack -> Information Gathering -> Network Analysis ->Service Fingerprinting -> Arping

Nbtscan. Για να βρούμε τα ονόματα των hosts, τις υπηρεσίες που τρέχουν

Nmap(Zenmap).

### 6.1.2 Εργαλεία για Footprinting.

- http://www.robtex. Παρέχει μία γραφική απεικόνιση πληροφοριών από τον DNS και το WhoIs.
- Dig. Γραμμένο σε Linux με σκοπό την έρευση των IP που συνδέονται με ένα domain name.
- Dnsbf: ένα script για reverse DNS αναζήτηση ένα ένα υποδίκτυο(subnet).
- Dnsdic και το λεξικό του. Ένα script για DNS dictionary bruteforce αναζήτηση για subdomains και ονόματα.
- Dnsmap(Backtrack): Script για το μάζεμα IP διευθύνσεων από ένα domain.
- Dnsrecon(Backtrack): Script για top level domain αναζήτηση. Για παράδειγμα για το OWASP τα αποτελέσματα είναι owasp.org, owasp.net, owsp.gr κτλ.
- DNSWalk(Backtrack)
- Burp Suite
- Dnshistory. DNS old entries

- Metagoofil.
- foxyProxy
- Maltego(backtrack)
- Hostmap.rb
- Fierce(backtrack). Perl script για Linux to conduct DNS search.
- spiderFoot v2.0

## 6.2. Κοινωνική μηχανική(Social Engineering).

Η ικανότητα να μπορεί κάποιος να χειριστεί τους ανθρώπους με τέτοιο τρόπο ώστε να εκτελέσουν συγκεκριμένες πράξεις και να αποκαλύψουν εμπιστευτικές πληροφορίες. Πρόκειται για ένα τέχνασμα με σκοπό τη συλλογή πληροφοριών, την απάτη και την πρόσβαση τελικά σε ένα υπολογιστικό σύστημα.

Θεωρείται ως μία από τις πιο δύσκολες επιθέσεις όσο αναφορά την πρόβλεψή της.

Ονομάζεται διαφορετικά Human Intelligence. Άμεση αλληλεπίδραση με τους υπαλλήλους είτε έχουν στενή είτε μακρινή σχέση με το υπό εξέταση αντικείμενο. Ένας ελεγκτής ασφαλείας μπορεί να παρουσιάσει τον εαυτό του σαν κάποιον τρίτο άνθρωπο εμπιστοσύνης και να προσπαθήσει να αλιεύσει πληροφορίες από τους εργαζομένους(π.χ. τι είδους λογισμικό προστασίας από ιούς χρησιμοποιούν).

Αν και αυτή η τεχνική υπόκειται περισσότερο στην ικανότητα κάποιου ανθρώπου ή στη μελέτη του πάνω σε συγκεκριμένες τεχνικές υπάρχει κάποιο framework που μπορεί να υποστηρίξει την προσπάθεια ανεύρεσης πληροφοριών μέσω της κοινωνικής μηχανικής.

- Social-Engineer Toolkit (SET)

## 6.3. Αυτοματοποιημένα εργαλεία συγκέντρωσης πληροφοριών.

Υπάρχουν εργαλεία ή σουίτες εργαλείων που μπορούν να διευκολύνουν την αναζήτηση πληροφοριών, ακόμη και να την αυτοματοποιήσουν.

### 6.3.1 The Recon-ng – Web Reconnaisance framework

Επίσημη ιστοσελίδα: https://bitbucket.org/LaNMaSteR53/recon-ng

Είναι γραμμένο σε Python. Είναι ένα ολοκληρωμένο εργαλείο με ανεξάρτητες μονάδες, αλληλεπίδραση με Βάση Δεδομένων, ενσωματωμένες λειτουργίες, διαδραστική βοήθεια και ένα σύνολο εντολών. Είναι ένα εργαλείο ανοιχτού κώδικα για τη γρήγορη και αποτελεσματική αναγνώριση διαδικτυακών εφαρμογών.

Μοιάζει πολύ σε όψη με το Metasploit αλλά είναι αρκετά διαφορετικό όσο αναφορά τη λειτουργικότητά του. Χρησιμοποιείται αποκλειστικά στη φάση της αναγνώρισης ενός υπό εξέταση συστήματος.

Διαθέτει τέσσερεις μονάδες λειτουργίας:

- Ανακάλυψη
- Εκμετάλλευση
- Αναγνώριση
- Αναφορά

### 6.3.2 The social-enginner Toolkit(SET)

Επίσημη ιστοσελίδα: https://www.trustedsec.com/downloads/social-engineer-toolkit/

Δημιουργήθηκε από το ιδρυτή της TrustedSec(David Kennedy – ReL1K). Είναι ανοιχτού κώδικα, γραμμένο σε python και χρησιμοποιείται σε ένα έλεγχο τρωτότητας κυρίως για σε μεθόδους κοινωνικής μηχανικής. Το SET έχει περισσότερα από δύο εκατομμύρια μεταφορτώσεις(downloads) και υποστηρίζεται από μία ενεργή και πολυπληθή κοινότητα. Είναι ένα εργαλείο για Linux το οποίο είναι σχεδιασμένο να πραγματοποιεί εξειδικευμένες επιθέσεις ενάντια στον ανθρώπινο παράγοντα. Στο τεχνικό κομμάτι πραγματοποιεί εκτός των άλλων επιθέσεις ηλεκτρονικού ψαρέματος(phising) και προσπάθειες απομακρυσμένου ελέγχου ενός συστήματος.

### 6.3.3 SnmpCheck

Επίσημη ιστοσελίδα: http://www.nothink.org/codes/snmpcheck/index.php

Είναι ένα εργαλείο που συμπεριλαμβάνεται στη διανομή Backtrack 5. Χρησιμοποιείται και αυτό στη φάση συλλογής πληροφοριών ενός ελέγχου ασφάλειας. Η χρήση του για τον έλεγχο ενός Server προϋποθέτει ότι το υπό εξέταση μηχάνημα χρησιμοποιεί την υπηρεσία SNMP. Για να το διαπιστώσει αυτό κάποιος μπορεί να δοκιμάσει με ένα εργαλείο όπως το Nmap για να δει αν η port 161 είναι ανοιχτή. Για να το τρέξει κάποιος το μόνο που χρειάζεται να γνωρίζει είναι η διεύθυνση IP του Server που επιθυμεί να γίνει ο έλεγχος. Όλα τα υπόλοιπα είναι προαιρετικά. Αν υ υπηρεσία SNMP λειτουργεί σε θύρα διαφορετική της 161, μπορεί να καθοριστεί κατά την εκτέλεση του προγράμματος με την παράμετρο –p/

Οι πληροφορίες που επιστρέφουν από το εργαλείο είναι πολύ χρήσιμες.

- Το όνομα του Server
- Το domain στο οποίο ανήκει

- Το λειτουργικό σύστημα
- Τη Λίστα των χρηστών
- Τη MAC διεύθυνση της κάρτας δικτύου
- Λίστα με τις υπόλοιπες ανοιχτές θύρες του Server
- Τους κοινόχρηστους πόρους του δικτύου

### 6.3.4. Maltego

http://www.paterva.com/web6/

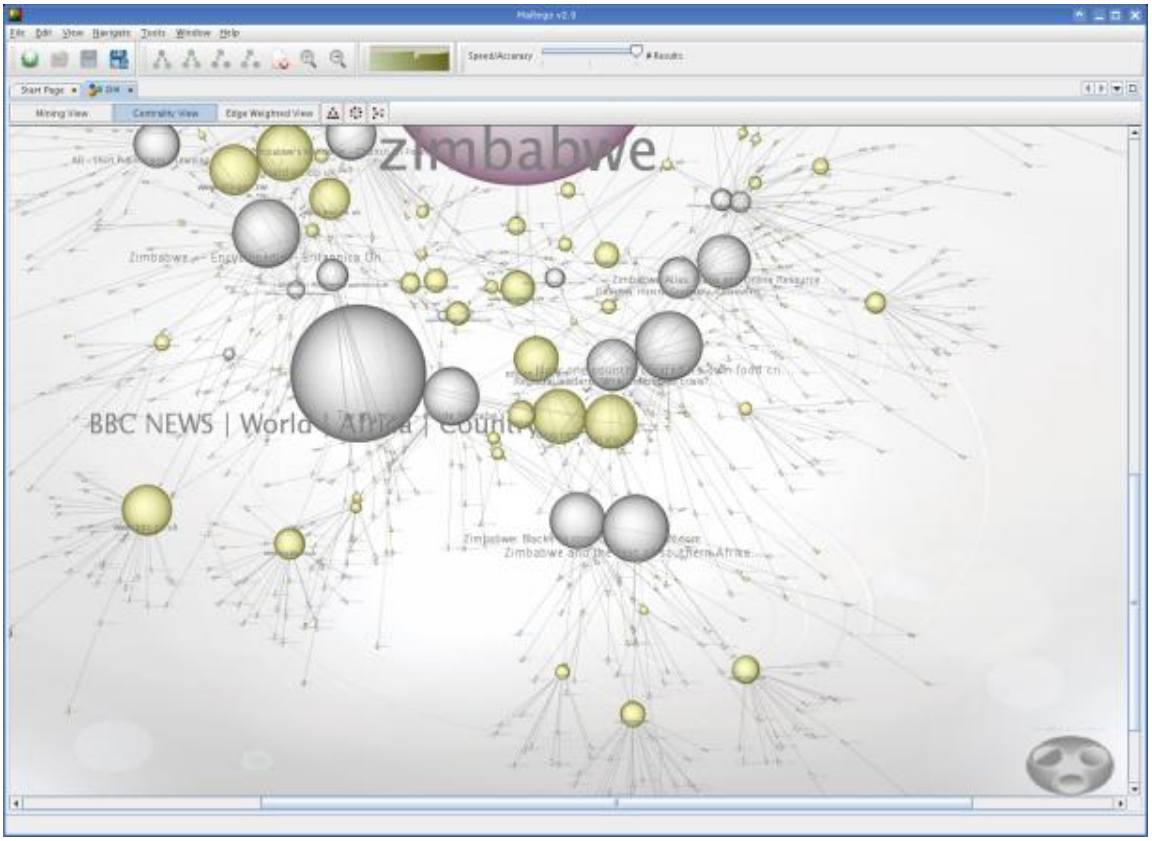
Είναι ίσως το καλύτερο εργαλείο για οπτική απεικόνιση πληροφοριών που βρίσκονται σε κοινωνικά δίκτυα και των σχέσεων μεταξύ τους. Λειτουργεί αρμονικά για δημόσια προφίλ του Twitter, του Facebook, του linked και του MySpace.

Είναι ένα σχετικά νέο εργαλείο ανοιχτού κώδικα με νέα εργαλεία που επιτρέπουν στον μέσο χρήση να πραγματοποιήσει εξόρυξη δεδομένων που στο παρελθόν μόνο εξειδικευμένοι ερευνητές και επαγγελματίες hacker μπορούσαν να πραγματοποιήσουν. Το maltego συλλέγει δημοσίως διαθέσιμα δεδομένα και βοηθάει στη σύνδεση και στις συσχετίσεις μεταξύ αυτών των πληροφοριών.

Αν για παράδειγμα κάποιος ανησυχεί για διαρροές πληροφοριών στην εταιρεία του μπορεί να ελέγχει μέσω γραφικών αναπαραστάσεων κατά πόσο πληροφορίες που βρίσκονται στο διαδίκτυο σχετικά με την εταιρεία προέρχονται από κάποιον από τους εργαζομένους της. Υπάρχει δυνατότητα αναζήτησης με βάση την e-mail διεύθυνση, τον αριθμό τηλεφώνου και προσωπικές ιστοσελίδες.

Συλλέγει πληροφορίες και την αναμιγνύει με ένα ενδιαφέρον τρόπο ώστε να αποδώσουν μία όσο το δυνατόν ξεκάθαρη εικόνα.

Το εργαλείο δεν είναι open source με καμία έννοια. Απλά είναι μία έξυπνη τεχνική marketing για την αποτελεσματικότερη προώθηση του. Ο όρος Open Source αναφέρεται στη διαδικασία εύρεσης στοιχείων που βασίζεται σε open source πηγές. Υπάρχει δωρεάν έκδοση(limited community version) από την επίσημη ιστοσελίδα. Λειτουργεί σε Linux και Windows αλλά όχι σε Mac. Η επαγγελματική έκδοση κοστίζει $430 δολάρια τον πρώτο χρόνο και 320 για κάθε χρόνο μετά από αυτόν.




Εικόνα 6.3.4: το εργαλείο εν δράση. Σύνδεση blogs, συνδέσμων σε αυτά τα blogs, tags σε δευτερεύοντα blogs και ηλεκτρονικές διευθύνσεις.

### 6.3.5. Simple Phising Toolkit v0.6.0

Επίσημη ιστοσελίδα: http://www.sptoolkit.com/?aid=2544&sa=1

Το **SPT** είναι μια απλή εφαρμογή, παρ' όλα αυτά με πολύ ισχυρές δυνατότητες. Το όνομά του προσδιορίζει ακριβώς τις δυνατότητές του: **Simple Phishing Toolkit**.

Η βασική ιδέα της εφαρμογής **SPT** είχε να κάνει με την προσπάθεια ανάπτυξης ενός εργαλείου αποτελεσματικού, εύκολου στη χρήση και δωρεάν το οποίο οι επαγγελματίες της ασφάλειας των πληροφοριών θα μπορούσαν να χρησιμοποιήσουν για να αξιολογήσουν και να εκπαιδεύσουν αυτό που όλοι γνωρίζουμε ότι είναι ο πιο αδύναμος κρίκος σε οποιαδήποτε επιχείρηση: τον άνθρωπο.


Εικόνα 6.3.5 : Αρχική οθόνη SPT

Οι ιδρυτές του **SPT** είναι οι ίδιοι επαγγελματίες της ασφάλειας των πληροφοριών και αντιμετωπίζουν την απογοήτευση των ανθρώπων που ασχολούνται με το εσωτερικό των επιχειρήσεών τους, που ισχυρίζονται ότι «ξέρουν τι κάνουν», αλλά 9 φορές από τις 10 «πέφτουν» στην παγίδα των πιο παράλογων και προφανών μηνυμάτων «**Phishing**» που έχουν δει ποτέ . Ένα malware, ένας κλεμμένος κωδικός πρόσβασης οδηγεί σε απώλεια κρίσιμων δεδομένων και το κόστος που μπορεί να φτάσει σε πολύ υψηλά επίπεδα και νούμερα.

Το **SPT** είναι ένα πλήρως αυτόνομο εργαλείο «**phishing**», που μπορεί να εγκατασταθεί, να ρυθμιστεί και να… «ψαρέψει» σε χρόνο μικρότερο των 15 λεπτών! Βέβαια το ίδιο εργαλείο θα μπορούσε να χρησιμοποιηθεί και από κακόβουλους χρήστες, οπότε καταλαβαίνουμε πλέον πως η προσοχή μας σε άγνωστης προέλευσης ηλεκτρονικά μηνύματα πρέπει να είναι στραμμένη προς αυτή την κατεύθυνση της ασφάλειας των προσωπικών μας δεδομένων και της ευαισθητοποίησής μας σε φαινομενικά "περίεργα" ή ***πολύ καλά για να είναι αληθινά μηνύματα***.

[23],[24],[25],[26],[27],[31],[33],[34],[44],[45],[46],[47],[48],[49],[59]

## 7. Κριτήρια Αξιολόγησης.

Η συγκριτική ανάλυση των εργαλείων θα στηριχθεί σε τρεις διακριτές κλάσεις απαιτήσεων:

- Αντιμετωπιζόμενες απειλές ασφάλειας(confronted security threats).
- Εφαρμοσμένα τεχνολογικά ζητήματα(applied technological issues).
- Ικανοποίηση απαιτήσεων των χρηστών(satisfaction of user demands).

### 7.1 Αντιμετωπιζόμενες απειλές ασφάλειας

Οδηγός για τις διαθέσιμες απειλές που επιλέχθηκαν αποτελεί η έκθεση του μη κερδοσκοπικού οργανισμού OWASP για τις πιο διαδεδομένες απειλές στο έτος 2012.

- Σύμφωνα με την ετήσια αναφορά του OWASP (Open Web Application Security Project ) οι δέκα(10) πιο διαδεδομένες απειλές για το 2012 είναι οι παρακάτω. [3]

- A1. Injection
- A2. Cross Site Scripting/XSS
- A3. Broken Authentication / Session Management
- A4. Insecure Direct Object References
- A5. Cross Site Request Forgery
- A6. Security Misconfiguration
- A7. Insecure Cryptographic Storage
- A8. Failure to Restrict URL Access
- A9. Insufficient Transport Layer Protection
- A10. Unvalidated Redirects and Forwards

Ο πίνακας σύγκρισης αυτής της κλάσης κριτηρίων περιέχει στον οριζόντιο άξονα του τα διαθέσιμα εργαλεία και στον κάθετο τις παραπάνω απειλές ασφάλειας.

Οι διαθέσιμες απαντήσεις είναι ΝΑΙ(+), ΟΧΙ(-) ή ΜΗ ΔΙΑΘΕΣΙΜΟ(x).

- (+) → το πρόγραμμα μπορεί να αντιμετωπίσει την συγκεκριμένη απειλή
- (-) → το πρόγραμμα δεν μπορεί να αντιμετωπίσει μια συγκεκριμένη απειλή
- (x) → Η λειτουργικότητα του προγράμματος δεν περιλαμβάνει την αντιμετώπιση των συγκεκριμένων απειλών.

## 7.2 Εφαρμοσμένα τεχνολογικά ζητήματα

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- B1. Απόδοση
- B2. Πολυπλοκότητα εγκατάστασης
- B3. Τελική αναφορά αποτελεσμάτων
- B4. Φορητότητα
- B5. Χρονική επιβάρυνση

### 7.2.1. Επεξήγηση κριτηρίων.

**Απόδοση**: Κατά πόσο τα αποτελέσματα καταγράφουν ικανοποιητικό ποσοστό των διαθέσιμων ευπαθειών ενός υπό εξέταση συστήματος.

**Πολυπλοκότητα εγκατάστασης**: Λαμβάνονται υπόψιν ο χρόνος ολοκλήρωσης της εγκατάστασης, οι τεχνικές γνώσεις και οι απαιτήσεις που προϋποθέτει καθώς και η δυσκολία απεγκατάστασης του.

**Τελική αναφορά αποτελεσμάτων**: Εξετάζεται αν υπάρχει τελική αναφορά αποτελεσμάτων, αν είναι ευανάγνωστη, λειτουργική και γενικότερα αν βοηθάει τον διαχειριστή να εξοικονομήσει χρόνο.

**Φορητότητα**: Κατά πόσο λειτουργεί σε διαφορετικά Λειτουργικά Συστήματα και σε διαφορετικές εκδόσεις αυτών.

**Χρονική επιβάρυνση**: Ο χρόνος που καταναλώνεται για την ολοκλήρωση μιας αναζήτησης.

Οι διαθέσιμες απαντήσεις είναι Υψηλή(Υ), Χαμηλή(Χ) ή Μέτρια(Μ).

- (Υ) → Το εργαλείο καλύπτει το συγκεκριμένο χαρακτηριστικό στο ακέραιο. Υψηλό μεταφράζεται ως η καλύτερη επιλογή σε κάθε περίπτωση(π.χ. στην πολυπλοκότητα εγκατάστασης το υψηλό σημαίνει ότι είναι πολύ εύκολη και γρήγορη διαδικασία ).
- (Χ) → Το εργαλείο είναι προβληματικό όσο αναφορά το συγκεκριμένο χαρακτηριστικό.
- (Μ) → Το συγκεκριμένο χαρακτηριστικό περιέχεται στο εργαλείο αλλά δεν αποτελεί το δυνατό του σημείο. Ενδεχομένως υπάρχουν προγράμματα με καλύτερη επίδοση στο συγκεκριμένο σημείο.

## 7.3 Ικανοποίηση απαιτήσεων των χρηστών.

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- C1. Ευκολία χρήσης.

- C2. Κοινότητα υποστήριξης
- C3. Κόστος
- C4. Πληρότητα

### 7.3.1 Επεξήγηση κριτηρίων.

**Ευκολία χρήσης:** Εξετάζεται κατά πόσο είναι λειτουργικό για ένα αρχάριο χρήστη, αν απαιτεί εξειδικευμένες τεχνικές γνώσεις, αν διαθέτει γραφικό περιβάλλον, αν οι λειτουργίες του είναι ομαδοποιημένες και αν η σχεδίαση του ικανοποιεί τις απαιτήσεις ενός μέσου χρήστη.

**Κοινότητα υποστήριξης:** Αν υπάρχει κοινότητα που υποστηρίζει το προϊόν(forum,blog,site) και κατά πόσο είναι ενεργή.

**Κόστος:** Αν είναι ανοιχτού κώδικα, αν διατίθεται δωρεάν ή ποιο είναι το κόστος που απαιτείται για την απόκτηση νόμιμης άδειας χρήσης.

**Πληρότητα :** Κατά πόσο ένα εργαλείο ή σουίτα εργαλείων μπορούν να χρησιμοποιηθούν για έλεγχο τρωτότητας σε διαφορετικά συστήματα και για διαφορετικές φάσεις του ελέγχου αυτού.

Οι διαθέσιμες απαντήσεις είναι Υψηλή(Υ), Χαμηλή(Χ) ή Μέτρια(Μ).

- (Υ) → Το εργαλείο καλύπτει το συγκεκριμένο χαρακτηριστικό στο ακέραιο για τον μέσο χρήστη.
- (Χ) → Το εργαλείο είναι προβληματικό όσο αναφορά το συγκεκριμένο χαρακτηριστικό. Δεν ικανοποιεί τις απαιτήσεις του μέσου χρήστη.
- (Μ) → Το συγκεκριμένο χαρακτηριστικό περιέχεται στο εργαλείο αλλά δεν αποτελεί το δυνατό του σημείο. Ενδεχομένως υπάρχουν προγράμματα με καλύτερη επίδοση στο συγκεκριμένο σημείο. Δυσκολεύει και είναι αποτρεπτικό το μέσο χρήστη.

*Σημείωση:* Ο μέσος χρήστης στη συγκεκριμένη περίπτωση ξεπερνάει τις γνώσεις ενός απλού, καθημερινού χρήστη των συστημάτων. Αναφερόμαστε σε ανθρώπους που έχουν προχωρημένη γνώση Η/Υ και δικτύων και βασικές γνώσεις στον τομέα της Ασφάλειας Πληροφοριακών Συστημάτων και του ελέγχου ευπαθειών.

## 8. Εργαλεία ελέγχου τρωτότητας.

Πολλά από τα σύγχρονα εργαλεία ελέγχου τρωτότητας περιλαμβάνουν λειτουργίες που καλύπτουν πάνω από ένα στάδια της μεθοδολογίας ελέγχου. Επιπλέον υπάρχουν πολλά και διαφορετικά προγράμματα ανάλογα με το είδος του υπό εξέταση συστήματος(Server, ασύρματο δίκτυο, Smartphone, VoIP κτλ).

Σε αυτή την ενότητα θα πραγματοποιηθεί παράθεση κάποιων εργαλείων και περιγραφή κάποιων από αυτά. **Η επιλογή τους πραγματοποιήθηκε μα τα παρακάτω κριτήρια:**

- Είναι τελευταίας τεχνολογίας (state-of-the-art) ή αναγνωρισμένο εργαλείο με συνεχή ενημέρωση.
- Μοναδικότητα. Στοχεύει σε πολύ συγκεκριμένους υπό εξέταση στόχους.
- Εξυπηρετεί μία συγκεκριμένη κατηγορία ελέγχων τρωτότητας και η περιγραφή του καλύπτει και τη λειτουργία των υπολοίπων.
- Πολλά εργαλεία μιας συγκεκριμένης κατηγορίας ιδανικά για σύγκριση μεταξύ τους.

Οι περιγραφές των εργαλείων έχουν κοινά στοιχεία μεταξύ τους ως προς τη δομή τους αλλά διαφορετικές προσεγγίσεις ως προς την παρουσίαση τους. Σε άλλα γίνεται αυστηρή παράθεση των χαρακτηριστικών τους ενώ σε άλλα παρουσιάζεται ο τρόπος λειτουργίας τους μέσω παραδειγμάτων και περιπτώσεων χρήσης. Επιλέχθηκε αυτός ο τρόπος ώστε ο αναγνώστης της εργασίας να έχει μία σφαιρική άποψη για τη λειτουργία των προγραμμάτων και θεωρητικά πρακτικά.

### 8.1 Παράθεση εργαλείων

#### 8.1.1 Γενικά

- Owasp web Scarab
- Owasp CAL9000. Είναι μια συλλογή από εργαλεία βασισμένα σε browser που επιτρέπουν τον αποτελεσματικότερο έλεγχο ασφάλειας. Περιλαμβάνει βιβλιοθήκη XSS επιθέσεων, encoder/decoder χαρακτήρων, HTTP request generator και Request Evaluator, λίστες ελέγχου, αυτοματοποιημένο κειμενογράφο επιθέσεων και πολλά άλλα.
- OWASP Pantera web Assessment Studio Project
- SPIKE - http://www.immunitysec.com
- Paros – http://www.parosproxy.org

- Burp Suite – http://port
- Burp Proxy - http://www.portswigger.net
- Achilles Proxy - http://www.mavensecurity.com/achilles
- Odysseus Proxy - http://www.wastelands.gen.nz/odysseus/
- Webstretch Proxy - http://sourceforge.net/projects/webstretch
- Firefox LiveHTTPHeaders, Tamper Data and Developer Tools - http://www.mozdev.org
- Grendel-Scan - http://www.grendel-scan.com
- Netsparker - http://www.mavitunasecurity.com/netsparker/
- Nikto - http://www.cirt.net/nikto2
- Wapikti - http://wapiti.sourceforge.net/
- Firefuzzer - https://code.google.com/p/firefuzzer/
- Arachni - http://www.arachni-scanner.com/
- Zed Attach Proxy - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- OWASP Disbuster - https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- Ratproxy - https://code.google.com/p/ratproxy/
- Davtest - https://code.google.com/p/davtest/
- J-Baah - http://research.sensepost.com/tools/web/j-baah
- Paros Proxy

**Έλεγχος Flash**

- OWASP SWFIntruder http://www.owasp.org/index.php/Category:SWFIntruder, http://www.mindedsecurity.com/swfintruder.html

**Έλεγχος Ajax**

- OWASP Sprajax Project

**Έλεγχος SQL injection**

- OWASP SQLiX
- Multiple DBMS SQL Injection tool - SQL Power Injector
- MySQL Blind Injection Bruteforcing, Reversing.org - [sqlbftools]
- Antonio Parata: Dump Files by SQL inference on Mysql - [SqlDumper]

- Sqlninja: a SQL Server Injection & Takeover Tool - http://sqlninja.sourceforge.net
- Bernardo Damele and Daniele Bellucci: sqlmap, a blind SQL injection tool - http://sqlmap.sourceforge.net
- Absinthe 1.1 (formerly SQLSqueal) - http://www.0x90.org/releases/absinthe/
- SQLInjector - http://www.databasesecurity.com/sql-injector.htm
- bsqlbf-1.2-th - http://www.514.es
- The Mole v0.3
- Fatcat
- Pangolin
- SQLSentinel

**Έλεγχος Oracle**

- TNS Listener tool (Perl) - http://www.jammed.com/%7Ejwa/hacks/security/tnscmd/tnscmd-doc.html
- Toad for Oracle - http://www.quest.com/toad

**Έλεγχος SSL**

- Foundstone SSL Digger - http://www.foundstone.com/resources/proddesc/ssldigger.htm

**Έλεγχος για Brute Force Password**

- THC Hydra - http://www.thc.org/thc-hydra/
- John the Ripper - http://www.openwall.com/john/
- Brutus - http://www.hoobie.net/brutus/
- Medusa - http://www.foofus.net/~jmk/medusa/medusa.html

**Έλεγχος για HTTP methods**

- NetCat - http://www.vulnwatch.org/netcat

**Fuzzer**

- WSFuzzer
- JBrofuzz - https://www.owasp.org/index.php/JBroFuzz

**Έλεγχος για buffer overflow**

- OllyDbg - http://www.ollydbg.de

"A windows based debugger used for analyzing buffer overflow vulnerabilities"

- Spike - http://www.immunitysec.com/downloads/SPIKE2.9.tgz

A fuzzer framework that can be used to explore vulnerabilities and perform length testing

- Brute Force Binary Tester (BFB) - http://bfbtester.sourceforge.net

A proactive binary checker

Metasploit - http://www.metasploit.com/projects/Framework/

A rapid exploit development and Testing frame work

**Googling**

- Foundstone Sitedigger (Google cached fault-finding) - http://www.foundstone.com/resources/proddesc/sitedigger.html

**Εμπορικά εργαλεία ελέγχου Black Box**

- Typhon - http://www.ngssoftware.com/products/internet-security/ngs-typhon.ph
- NGSSQuirreL - http://www.ngssoftware.com/products/database-security/
- Watchfire AppScan - http://www.watchfire.com
- Cenzic Hailstorm – http://www.cenzic.com/products_services/cenzic_hailstorm.php
- SPI Dynamics WebInspect - http://www.spidynamics.com
- Burp Intruder - http://portswigger.net/intruder
- Acunetix Web Vulnerability Scanner - http://www.acunetix.com
- ScanDo - http://www.kavado.com
- WebSleuth - http://www.sandsprite.com
- NT Objectives NTOSpider - http://www.ntobjectives.com/products/ntospider.php
- Fortify Pen Testing Team Tool - http://www.fortifysoftware.com/products/tester
- Sandsprite Web Sleuth - http://sandsprite.com/Sleuth/
- MaxPatrol Security Scanner - http://www.maxpatrol.com
- Ecyware GreenBlue Inspector - http://www.ecyware.com
- Parasoft WebKing (more QA-type tool)
- MatriXay - http://www.dbappsecurity.com
- N-Stalker Web Application Security Scanner - http://www.nstalker.com

**Αναλυτές πηγαίου κώδικα(source code) –Open source/ Freeware**

- OWASP LAPSE
- PMD - http://pmd.sourceforge.net/
- FlawFinder - http://www.dwheeler.com/flawfinder
- Microsoft's FxCop

- Splint - http://splint.org
- Boon - http://www.cs.berkeley.edu/~daw/boon
- Pscan - http://www.striker.ottawa.on.ca/~aland/pscan
- FindBugs - http://findbugs.sourceforge.net

**Αναλυτές πηγαίου κώδικα(source code) –Commercial**

- Fortify - http://www.fortifysoftware.com
- Ounce labs Prexis - http://www.ouncelabs.com
- Veracode - http://www.veracode.com
- GrammaTech - http://www.grammatech.com
- ParaSoft - http://www.parasoft.com
- ITS4 - http://www.cigital.com/its4
- CodeWizard - http://www.parasoft.com/products/wizard
- Armorize CodeSecure - http://www.armorize.com/product
- Checkmarx CxSuite - http://www.checkmarx.com

**Runtime Analysis**

- Rational PurifyPlus
- http://www-306.ibm.com/software/awdtools

**Binary** Analysis

- BugScam - http://sourceforge.net/projects/bugscam
- BugScan - http://www.hbgary.com
- Veracode - http://www.veracode.com

**Site mirroring**

- wget - http://www.gnu.org/software/wget
- http://www.interlog.com/~tcharron/wgetwin.html
- curl - http://curl.haxx.se
- Sam Spade - http://www.samspade.org
- Xenu - http://home.snafu.de/tilman/xenulink.html

**iPhone PenTesting Apps**

*Information Gathering*

- Deep Whois ~ Lookup IPs, Domains, IDNs, ASNs **($1.99 - Pavel Ahafonau)**
- JaNet – Network Tools **($1.99)**

- zTools – Network Utility **($1.99)**

*Network Mapping*

- IP Network Scanner **($9.99 -10base-t interactive; και δωρεάν έκδοση)**
- iNet Pro – Network Scanner **($5.99 - BananaGlue GmbH; και δωρεάν έκδοση)**
- Scany ~ Network and Port Scanner, Traceroute, Ping, Whois, Wake on LAN **($5.99 - Pavel Ahafonau)**
- LANScan **($0.99 - Nutec Network Tools, LLC)**
- Net Master – IT Tools & LAN Scanner **($5.99 -Nutec Apps, LLC)**
- Fing – Network Scanner **(δωρεάν)**
- **SetnetInsight – Scan & Manage Your Wi-Fi Networks ($3.99 - BluesWine, Inc.)**

*Vulnerability Identification*

- zScan Pro **($2.99 - 0×557 Team)**

*Penetration*

- Nada

*Verification*

- iSSH – SSH / VNC Console **($9.99 - Zinger-Soft)**
- SSH Term Pro **($4.99 -Moon Technolabs)**
- zateInet **(δωρεάν)**

*Άλλα*

- ***Wickr – Secure IM & Multimedia Sharing (δωρεάν από Wickr, LLC)***
- ***Silent Phone (Silent Circle)***
- ***Silent Text (Circle)***
- ***Burner – Disposable Phone Numbers (ad Hoc Labs, Inc)***

**wireless sensors networks(WSE)**

- WSN-ETESec – End to End Security Tool for WSN
- Hybrid Automata Stochastic Logic

[14],[22],[32],[50],[51],[52],[61],[69]

## 8.2 Παράθεση εργαλείων.

*Η ενότητα αυτή περιλαμβάνει περιγραφή των εργαλείων που παραθέτονται. Η λειτουργία τους, χαρακτηριστικά τους, υπέρ, κατά και στοιχεία που επαληθεύουν τις επιλογές στους πίνακες σύγκρισης που θα ακολουθήσουν στο επόμενο κεφάλαιο*

### 8.2.1 Περιγραφή εργαλείων

#### 8.2.1.1 Nmap

Επίσημη ιστοσελίδα: http://nmap.org/download.html

Άδεια χρήσης: Ανοιχτού κώδικα(GNU General Public License)

Επιπλέον πληροφορίες: Πρόκειται για ένα από τα πλέον κλασικά εργαλεία. Αν δεν είστε αρχάριος χρήστης το εργαλείο προσφέρει μία δωρεάν και αξιόπιστη λύση για τον έλεγχο ενός δικτύου.

Έκδοση: v1.2. revision:6647

Κυκλοφόρησε τον Σεπτέμβριο του 1997. Ο αρχικός του σκοπός ήταν η ανίχνευση ενός δικτύου, η χαρτογράφηση του(mapping) διευκολύνοντας την ανακάλυψη host και υπηρεσιών που τρέχουν σε αυτά. Οι διαχειριστές δικτύων και οι ειδικοί σε θέματα ασφάλειας Πληροφοριακών συστημάτων το χρησιμοποιούν εκτός της χαρτογράφησης τους δικτύου τους για τους παρακάτω λόγους:

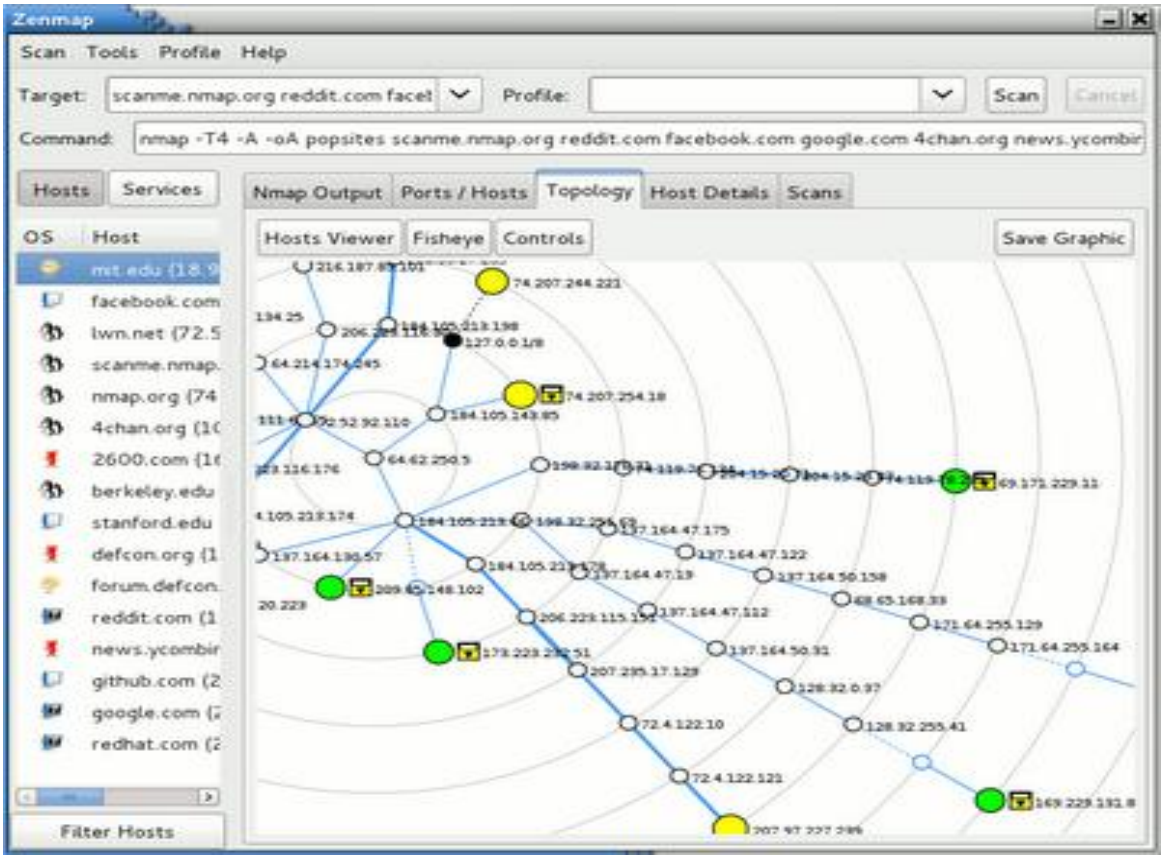
- Για τον αν είναι ή όχι ενεργός ένας host
- Για την ανακάλυψη της ύπαρξης hosts που δεν περίμεναν να υπάρχουν
- Για την εύρεση των διαθέσιμων υπηρεσιών σε ένα host
- Για την εύρεση του τύπου ενός host
- Για την παρουσία firewall ή όχι
- Λειτουργικό σύστημα και έκδοση του πάνω σε ένα host
- Όνομα και έκδοση των υπηρεσιών που τρέχουν σε ένα host

Αρχικά ήταν 100% διαθέσιμο μέσω γραμμής εντολών(command line) απαιτώντας βαθιά εξοικείωση με τις διάφορες επιλογές του για να είναι πλήρως

εκμεταλλεύσιμο. Αναπτύχθηκε όμως ένα γραφικό περιβάλλον με όνομα Zenmap που το έκανε πιο διαισθητικό στη χρήση του.

Το Nmap από μόνο του δεν μπορεί να αναγνωρίσει ευπάθειες σε ένα σύστημα. Άλλες λειτουργίες προστέθηκαν για τα αυξήσουν τις ικανότητές του όπως το Ncat(για την αποστολή και την αποδοχή δεδομένων σύνδεσης) και το Ndiff(δείχνει το delta μεταξύ των αποτελεσμάτων μιας σάρωσης).
Σε μεγάλο βαθμό είναι ένα πολύ χρήσιμο εργαλείο καθώς βοηθάει στην αναγνώριση ενός υπό εξέταση στόχου.

Το Nmap 6 περιλαμβάνει μια πιο ισχυρή μηχανή scripting, 289 νέα scripts, καλύτερο διαδικτυακό έλεγχο, πλήρη υποστήριξη IPv6, το πακέτο ελέγχου Nping και πολλά άλλα. Είναι ένα δωρεάν και ανοιχτού κώδικα βοηθητικό πρόγραμμα για τον έλεγχο ασφάλειας στο διαδίκτυο. Είναι χρήσιμο σε πολλά συστήματα και διαχειριστές σχετικά με την απογραφή και διαχείριση των προσφερομένων υπηρεσιών ενός συστήματος




Εικόνα 8. 2.1.1: Γραφικό περιβάλλον Zenmap

Τα νέα βελτιωμένα χαρακτηριστικά του εργαλείου είναι:

- Ενισχυμένη μηχανή αναζήτησης δικτύου
- Καλύτερος έλεγχος ασφάλειας
- Πλήρης υποστήριξη IPv6
- Νέο εργαλείο Nping
- Καλύτερο Zenmap GUI και η απεικόνιση των αποτελεσμάτων του προγράμματος προβολής μέσω viewers
- Ταχύτερος έλεγχος.

Υπέρ:

Μεγάλη κοινότητα που το υποστηρίζει

Φορητότητα

Διατίθεται δωρεάν

Κατά:

Δεν απευθύνεται σε ένα αρχάριο χρήστη.

Δεν υπάρχει δυνατότητα εξαγωγής αναφορών.

#### 8.2.1.2 Nessus

Επίσημη ιστοσελίδα: http://www.tenable.com/products/nessus

Άδεια χρήσης: εμπορική

Επιπλέον πληροφορίες: έχει πάνω από 17000 πελάτες παγκοσμίως και γύρω στα 54.000 plug-ins.

Το Nessus κυκλοφόρησε το 1998. Αρχικά αναπτύχθηκε σας ένας δωρεάν απομακρυσμένος σαρωτής αλλά αργότερα έγινε κλειστού κώδικα και από το 2008 και έπειτα προσφέρει τις λειτουργίες του έναντι $1200 δολαρίων το έτος. Ο δημιουργός του είναι ο Renaud Deraison συνιδρυτής της εταιρείας Tenable Network Security.

Η κύρια λειτουργία του είναι να προσφέρει επιλογές ελέγχων ασφαλείας μέσω σάρωσης σε ένα χρήστη του. Μπορεί να πραγματοποιήσει ανίχνευση Δικτύου(Network Discocery) και επιπλέον έχει τη δυνατότητα να καθορίζει τις ευπάθειες που βρίσκει. Οι δυνατότητες του Nessus μπορούν να χρησιμοποιηθούν για τους παρακάτω σκοπούς:

- Ελέγχους ασφαλείας
- Ταυτοποίηση των αγαθών του συστήματος
- Ανακάλυψη ευαίσθητων δεδομένων
- Ανάλυση ευπαθειών

Είναι λειτουργίες που μπορεί να πραγματοποιήσει και το Nmap αλλά τις κάνει πιο γρήγορα.

Η Tenable Network Security αναπτύσσει πολλά plugins ελέγχου ασφάλειας. Μεταξύ όλως αυτών των plugins το Nessus μπορεί να ελέγξει περισσότερα από 12,000 CVEs (common vulnerability exposures). Είναι εργαλείο άλλης κλάσης σε σχέση με το Nmap. Χρησιμοποιεί μια διαδικτυακή οθόνη λειτουργίας και επιτρέπει στο διαχειριστή της τη δημιουργία πολλών διαφορετικών χρηστών. Προσφέρει τη δυνατότητα δημιουργίας πολιτικών ασφάλειας που συνδυάζονται με συγκεκριμένα χαρακτηριστικά σχετικά με ένα έλεγχο και υποδεικνύουν ποια plugins ασφάλειας θα χρησιμοποιηθούν, τον τύπο των θυρών που θα σαρωθούν και διάφορες άλλες λεπτομέρειες. Μέσω της πολιτικής που δημιουργήθηκε μπορεί να αρχίσει μία σάρωση στους στόχους που ορίστηκαν(targets).

Μέσω της web interface μπορεί κάποιος να δει τα αποτελέσματα της σάρωσης ακόμη και όταν αυτή είναι σε εξέλιξη. Οι αναφορές μπορούν να παραχθούν σε διάφορες μορφές.

Windows, Linux, Unix – databases, Web servers

Υπέρ:

Μπορεί να το χρησιμοποιήσει και ένας αρχάριος χρήστης.

Είναι ολοκληρωμένο

Κατά:

Είναι ακριβό

Μερικοί έλεγχοι ασφαλείας σε safe mode μπορούν να «κρασάρουν» ένα σύστημα.

#### 8.2.1.3 METASPLOIT

Επίσημη ιστοσελίδα: http://www.metasploit.com/

Άδεια χρήσης: Δωρεάν

Το framework αυτό έχει γίνει το απαραίτητο για κάθε ειδικό ελέγχων ασφάλειας σε πληροφοριακά συστήματα για ελέγχους τρωτότητας και ανάπτυξη ευπαθειών. Έχει περισσότερα από ένα εκατομμύριο μοναδικά downloads κάθε χρόνο και την μεγαλύτερη βάση δεδομένων σε διαθέσιμα exploits παγκοσμίως.

Το Metasploit Framework είναι ένα πρόγραμμα που αναπτύχθηκε από την Metasploit LLC, αρχικά σε γλώσσα PERL αλλά έπειτα ξαναγράφτηκε σε Ruby. Οι τελευταίες εκδόσεις του εργαλείου έχουν πάει τη διαδικασία εξομοιώσεις και ελέγχου exploits σε άλλο επίπεδο.

Οι μηχανικοί πληροφορικής έχουν τη δυνατότητα να πραγματοποιήσουν ελέγχους ασφαλείας, να εντοπίζουν ευπάθειες και κενά ασφαλείας τα οποία μπορούν να οδηγήσουν σε παραβίαση ώστε στη συνέχεια να προετοιμάσουν τους αμυντικούς μηχανισμούς. Οι ομάδες ασφαλείας αυξάνουν την παραγωγικότητα τους ξοδεύοντας λιγότερο χρόνο για την επιδιόρθωση σημαντικών ευπαθειών και ταυτόχρονα πιστοποιούν ότι η επιδιόρθωση είναι αποτελεσματική.

Το community edition το οποίο βασίζεται στο Metasploit Framework δίνει τη δυνατότητα στους ειδικούς ασφάλειας στην :

- Ευφυή διαχείριση πληροφοριών που αναδεικνύουν τον κίνδυνο.
- Ολοκληρωμένη καταγραφή και γραφική απεικόνιση αδυναμιών ανά χρήστη, τερματικό, εξυπηρέτη ή δικτυακή συσκευή.
- Αυτοματοποίηση της διαδικασίας ελέγχου ασφάλειας.
- Υποστήριξη εισαγωγής αναφορών ανάλυσης ευπαθειών από τρίτες εφαρμογές.

Είναι εύκολο στη χρήση του. Ακολουθεί τα παρακάτω βήματα κατά τη διαδικασία της εκμετάλλευσης ενός υπο εξέταση στόχου:


1. Επιλογή και διαμόρφωση του exploit υπό εξέταση. Αυτός είναι ο κώδικας που στοχοποιεί ένα σύστημα με σκοπό την εκμετάλλευση του για την εύρεση ελαττωμάτων σε ένα σύστημα. Επικυρώνει το αν ένα σύστημα είναι δεκτικό σε κάποιο συγκεκριμένο exploit.
1. Επιλογή και διαμόρφωση του payload(ωφέλιμου φορτίου) που θα χρησιμοποιηθεί και επαλήθευση ότι θα καταφέρει να περάσει από το intrusion Detection System(IDS) με ευκολία.
2. Εκτέλεση του exploit.

Έχει τρία διαθέσιμα περιβάλλοντα εργασίας, το msfconsole, το msfcli και το msfweb. Αυτό που χρησιμοποιείται κατά κόρον είναι το msfcosole. Είναι μία αποτελεσματική εφαρμογή που εκτελείται σε γραμμή εντολών με δικό της set εντολών και περιβάλλον εργασίας.

Κάποιες από τις εντολές του είναι:

1. **search <keyword>**
2. **show exploits**
3. **show payloads**
4. **show options**
5. **info <type> <name>**
6. **use <exploit_name>**
7. **set RHOST <hostname_or_ip>**.
8. **set RPORT <host_port>:**
9. **set PAYLOAD <generic/shell_bind_tcp>**
10. **set LPORT <local_port>**
11. **exploit**
12. **help**

Ακολουθεί μία επίδειξη ελέγχου τρωτότητας :

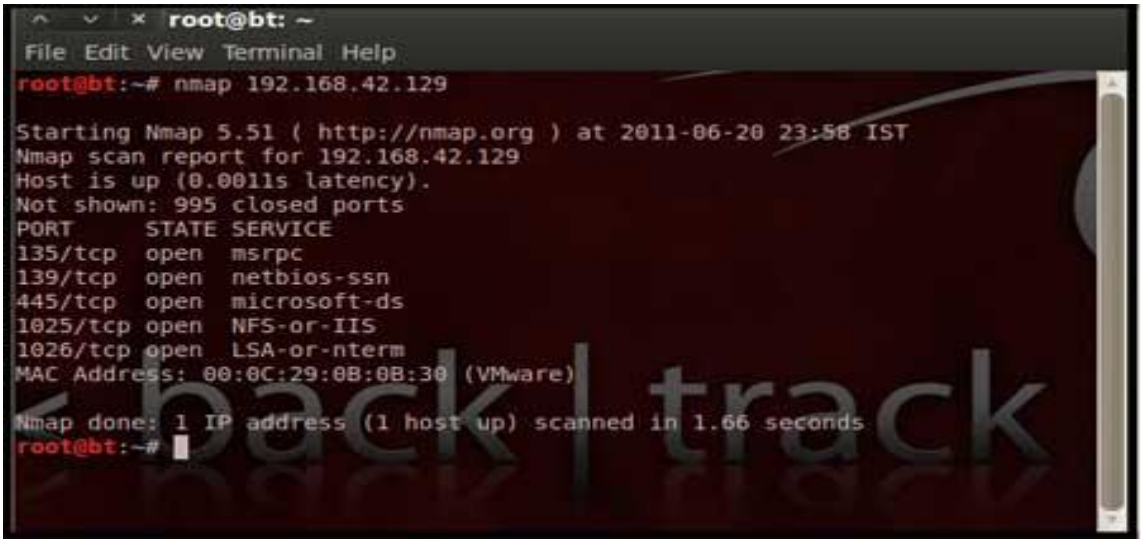
Victim Machine
OS: Microsoft Windows Server 2003
IP: IP: 192.168.42.129

Attacker (Our) Machine
OS: Backtrack 5
Kernel version: Linux bt 2.6.38 #1 SMP Thu Mar 17 20:52:18 EDT 2011 i686 GNU/Linux
Metasploit Version: Built in version of metasploit 3.8.0-dev
IP: 192.168.42.128

Ο σκοπός μας είναι να αποκτήσουμε απομακρυσμένη σύνδεση σε ένα δοθέν στόχο στο οποίο είναι γνωστό ότι τρέχει Windows 2003 server με κάποιες γνωστές ευπάθειες.

Θα πραγματοποιήσουμε μία σάρωση NMap στον απομακρυσμένο Server

Nmap 192.168.42.129




Εικόνα 8.2.1.3.1. Ανίχνευση ανοιχτώ θυρών με Nmap

Παρατηρούμε ότι η πόρτα 135 είναι ανοιχτή. Μπορούμε να ψάξουμε για scripts στο Metasploit και να προσπαθήσουμε να αποκτήσουμε shell Access αν ο server είναι ευπαθής.

- Ανοίγουμε το msfconsole και ψάχνουμε για σχετικά RPC exploits. Χρησιμοποιούμε την εντολή «show exploits»

Στο metasploit Framework 3.8.0 υπάρχουν 696 διαθέσιμα exploits και 224 payloads. Είναι ένας πολύ μεγάλος αριθμός που θα καταναλώνει πολύ χρόνο για την εύρεση του κατάλληλου exploit. Εναλλακτικά μπορεί κάποιος να κάνει αναζήτηση στο

http://metasploit.com/modules η σε κάποια άλλη πηγή.

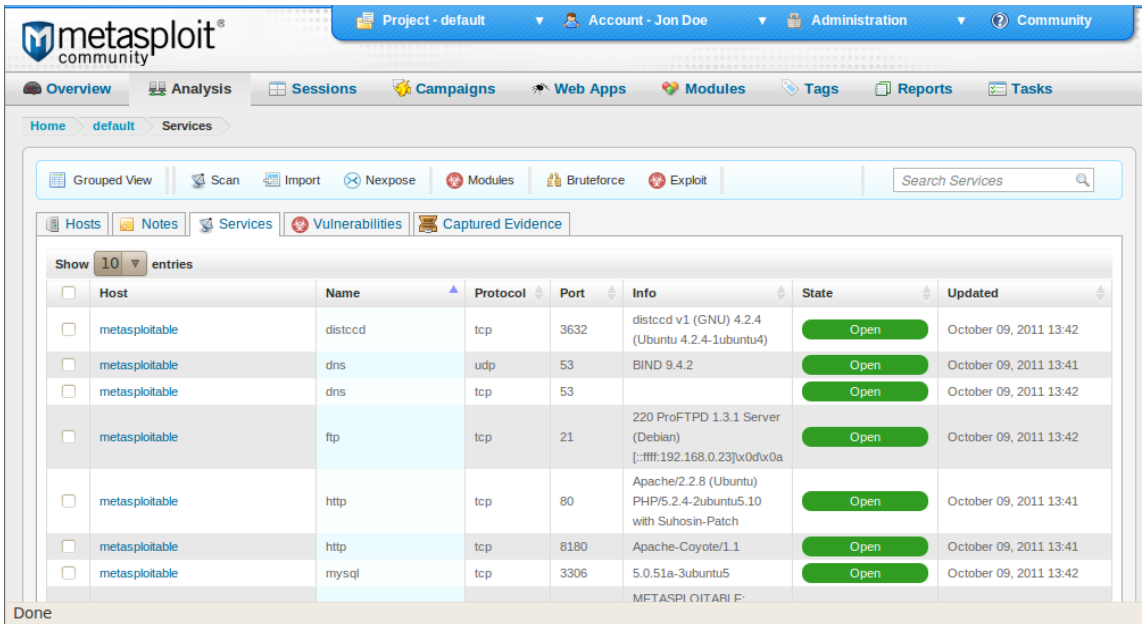
- Μετά την εύρεση του κατάλληλου exploit ακολουθεί η διαμόρφωσή του και στη συνέχεια ο καθορισμός του κατάλληλου payload γι' αυτό το exploit.
- Με την εντολή «check» ελέγχουμε αν το υπό εξέταση σύστημα είναι ευπαθές ή όχι στο exploit μας.

Επιπλέον :

Το metasploit μπορεί να χρησιμοποιηθεί κατά τη διάρκεια ενός ελέγχου τρωτότητας για την επικύρωση αναφορών άλλων εργαλείων τρωτότητας για να επιβεβαίωση ότι δεν έχουν λανθασμένα αποτελέσματα.

Μπορεί να χρησιμοποιηθεί για έλεγχο της αποτελεσματικότητας νέων exploits που δημιουργούνται συνεχώς

Χρησιμοποιείται για τον έλεγχο ενός IDS και το αν αυτός σταματάει αποτελεσματικά επιθέσεις.




Εικόνα 8.2.1.3.2 Το γραφικό περιβάλλον του Metasploit

Υπέρ:

Είναι πολυχρησιμοποιημένο. Μεγάλη πηγή πληροφοριών.

μπορεί να χρησιμοποιηθεί και για ελέγχους ασφάλειας σε VoIP0(SIP πρωτόκολλά)

Κατά:

Χρησιμοποιείται με κλειστό αντι-ικό σε Windows OS.

Βαρύ πρόγραμμα που λειτουργεί σε Windows και Linux.

### 8.2.1.4 OpenVAS

Επίσημη ιστοσελίδα: http://www.openvas.org/news_archive.html#openvas5

Άδεια χρήσης: Δωρεάν

Είναι ένα εργαλείο που εντοπίζει κενά ασφάλειας σε έναν υπολογιστή ή δίκτυο ή ακόμα και σε εφαρμογές. Είναι ανοιχτού κώδικα και προσφέρεται δωρεάν. Λειτουργεί σαν ανεπίσημος αντικαταστάτης του Nessus(αφού έγινε εμπορικό) και αποτελεί μία ολοκληρωμένη πλατφόρμα εργασίας με ένα μεγάλο συνδυασμό εργαλείων που το καθιστούν πολύ δυναμικό και αποτελεσματικό.

Έχει πολλά χαρακτηριστικά από τα οποία το πιο σημαντικό θεωρείται η διασύνδεσή του με το εργαλείο Nikto για των έλεγχο ευπαθειών σε διαδικτυακές εφαρμογές και ιστοσελίδες. Ένα ακόμη σημαντικό χαρακτηριστικό είναι η δυνατότητα να δείχνει τις διαφορές μεταξύ δύο αναφορών από τη σάρωση καθώς και η αντιστοίχηση στην τρέχουσα CPE και CVE μέσα στη Βάση δεδομένων OpenVAS. Το νέο διαχειριστικό περιβάλλον επιτρέπει στο χρήστη να εξετάσει τα αποτελέσματα της σάρωσης, επιλέγοντας οποιαδήποτε IP συσκευής είναι συνδεδεμένη στο δίκτυο.

Βρίσκεται στην 5η έκδοσή του. Ο αριθμός των δωρεάν εργαλείων έχει αυξηθεί σε πάνω από 25.000 και δίνεται ιδιαίτερη έμφαση στην απλούστευση της καθημερινής χρήσης. Θεωρείτε το πιο προηγμένο εργαλείο ανοιχτού κώδικα για τη διαχείριση ευπαθειών. Διατίθεται δωρεάν με άδεια χρήσης GNUGPL.

Υπέρ:

Τρέχει σε εικονικό περιβάλλον.

Ωραίες τελικές αναφορές.

Κατά:

Δυσκολία εγκατάστασης.

#### 8.2.1.5 Nexpose

Επίσημη ιστοσελίδα: http://www.rapid7.com/products/nexpose/editions-and-features.jsp

Άδεια χρήσης: Δωρεάν

Είναι ένα λογισμικό διαχείρισης ευπαθειών. Σαρώνει ένα δίκτυο αναζητώντας misconfigurations, ευπάθειες, λογισμικά κακόβουλης λειτουργίας(malware) και παρέχει οδηγίες για τον περιορισμό αυτών των κινδύνων. Ενσωματώνεται στο Metasploit Framework για τη πλήρη επικύρωση των κινδύνων σε ένα περιβάλλον.

- Παραθέτει αυτόματα όλα αγαθά(assets), τις εφαρμογές και τις υπηρεσίες που είναι ενεργές συμπεριλαμβανομένων IPv6, εικονικών(virtual) και φιλοξενούμενων σε cloud αγαθών.

Σε συγκριτικά test με τα εργαλεία OpenVAS, Nmap και Nessus σε 15 διαφορετικούς τύπους κενών ασφάλειας το Nexpose αναγνώρισε πολύ περισσότερες απειλές, διαμορφωμένες λάθος συσκευές και γνωστά προβλήματα σε Λειτουργικά Συστήματα. Υλοποίησε πετυχημένα και IPv6 ανίχνευση. Μαζί με το Metasploit αποτελούν μία αξιόπιστη λύση για κάθε οργανισμό ή εταιρεία.

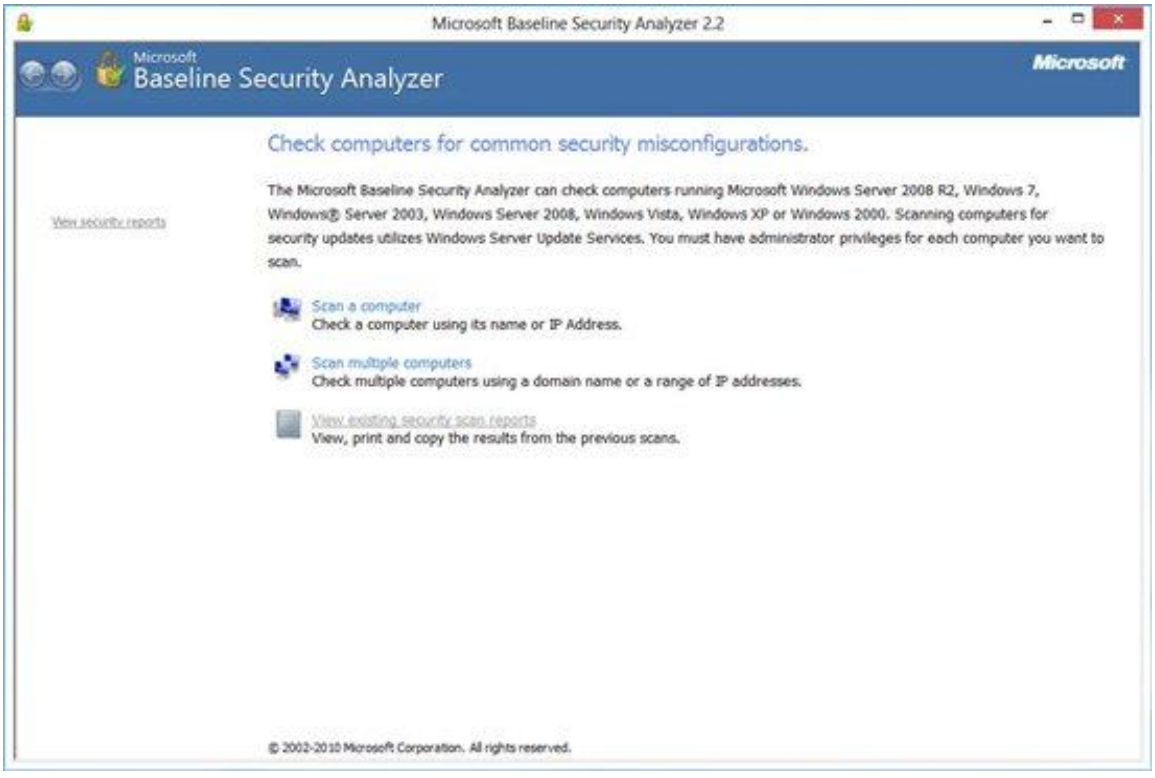
### 8.2.1.6 MBSA – Microsoft Baselive Security Analyzer

Επίσημη ιστοσελίδα: http://www.microsoft.com/en-us/download/details.aspx?id=7558

Άδεια χρήσης: Δωρεάν

Επιπλέον Πληροφορίες: Μόνο για windows

Είναι ένα σχετικά εύκολο εργαλείο να χρησιμοποιηθεί σχεδιασμένο για τεχνικούς ασφάλειας ώστε να ελέγχουν τα επίπεδα ασφάλειας σε υπολογιστές που χρησιμοποιούν Λειτουργικό Σύστημα Windows. Ελέγχει για διαχειριστικές ευπάθειες, για αδύναμους κωδικούς πρόσβασης, για την ύπαρξη ή όχι IIS και SQL ευπαθειών και για ενημερώσεις ασφαλείας που έχουν αμεληθεί.. Οι επιλογές που προσφέρει είναι διαθέσιμες και από τη γραμμή εντολών εκτελώντας το αρχείο MBSACLI.exe




Εικόνα 8.2.1.6 Αρχική οθόνη MBSA

Μπορεί να ελέγχει μία ομάδα μηχανημάτων. Με την ολοκλήρωση του προσφέρει μία λεπτομερή αναφορά σε HTML. Τα ευρήματα είναι ομαδοποιημένα σε κατηγορίες κάτι που διευκολύνει την επίλυση των αδυναμιών. Το εργαλείο αυτό διατίθεται δωρεάν. Είναι μία επαρκής λύση για εύρεση ενημερώσεων ασφαλείας που αμελήθηκαν και συνηθισμένων ευπαθειών.

#### 8.2.1.7 Core impact

Επίσημη Ιστοσελίδα: http://www.coresecurity.com/core-impact-pro

Άδεια χρήσης: εμπορική

Επιπλέον πληροφορίες: Προσφέρει κάθε είδους έλεγχο

Το πιο ακριβό λογισμικό για ελέγχους τρωτότητας. Ξεκινάει από τις 30000 ευρώ και η τιμή του ανεβαίνει ανάλογα με τις επιπλέον λειτουργίες. Προσπαθεί να αντικαταστήσει τελείως τον ανθρώπινο παράγοντα με τις αυτοματοποιημένες λειτουργίες που διαθέτει. Προσπαθεί να εισβάλει σε ένα σύστημα από μόνο του δημιουργώντας ένα secure tunnel για την εισβολή του στον επόμενο δίκτυο ενώ ταυτόχρονα φροντίζει να ασφαλίζει τα exploits που έχει χρησιμοποιήσει και να κλειδώνει backdoors που συναντά. [82]

[13],[15],[16],[17],[54],[56],[57],[67],[71]

#### 8.2.1.8 Σύγκριση Εργαλείων

Ως κριτήρια σύγκρισης θα χρησιμοποιηθούν οι δύο τελευταίες κλάσεις κριτηρίων από το συγκριτικό πλαίσιο αξιολόγησης που περιγράφηκε στο κεφάλαιο 7.

**Εφαρμοσμένα τεχνολογικά ζητήματα**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- B1. Απόδοση
- B2. Πολυπλοκότητα εγκατάστασης
- B3. Τελική αναφορά αποτελεσμάτων
- B4. Φορητότητα
- B5. Χρονική επιβάρυνση

| **Κριτήρια:** <br><br> **Προγράμματα** | **B1** | **B2** | **B3** | **B4** | **B5** |
|---|---|---|---|---|---|
| Nmap | Υ | Υ | M | Y | X |
| Nessus | Y | M | Y | M | Y |
| Metasploit | Υ | M | X | M | M |
| OpenVAS | M | M | M | M | M |
| Nexpose | Y | M | M | M | X |
| MBSA | X | Y | M | X | M |
| Core Impact | Y | M | Y | M | M |

**Ικανοποίηση απαιτήσεων των χρηστών.**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- C1. Ευκολία χρήσης.
- C2. Κοινότητα υποστήριξης
- C3. Κόστος
- C4. Πληρότητα

| **Κριτήρια:** <br><br> **Προγράμματα** | **C1** | **C2** | **C3** | **C4** |
|---|---|---|---|---|
| Nmap | M | Υ | Υ | M |
| Nessus | Υ | X | X | Υ |
| Metasploit | X | Υ | Υ | Υ |
| OpenVAS | Υ | M | Υ | M |
| Nexpose | M | X | Υ | M |
| MBSA | Υ | X | Υ | X |
| Core Impacts | M | X | X | Υ |

*Η διαθέσιμη επιλογή Υψηλή(Υ) σημαίνει σε κάθε περίπτωση την καλύτερη απόδοση. Στο κριτήριο κόστος για παράδειγμα σημαίνει ότι το προϊόν προσφέρεται δωρεάν είτε είναι ανοιχτού κώδικα. Το κριτήριο πληρότητα στη αξιολόγηση εργαλείων που εξετάζουν συγκεκριμένες ευπάθειες αφορά λειτουργίες μέσα στο εύρος δυνατοτήτων των προγραμμάτων αυτής της κατηγορίας.*

## 8.3 Συλλογές εργαλείων

Υπάρχουν διαθέσιμες σουίτες που έχουν συγκεντρώσει πολλά εργαλεία ελέγχου τρωτότητας για τη διευκόλυνση των υπευθύνων ελέγχου ασφάλειας. Δωρεάν διανομές live cd που περιέχουν ένα μεγάλο αριθμό προγραμμάτων ανοιχτού κώδικα ή τις δωρεάν εκδόσεις, πρόσθετα σε περιηγητές διαδικτύου για την εκτέλεση δομικών διείσδυσης ή ακόμη και περιηγητές αφοσιωμένους σε αυτό το ρόλο.

### 8.3.1 Exploit-Me

Είναι ένα πρόσθετο του Firefox για την εκτέλεση ελέγχων τρωτότητας.


Η ασφάλεια των ιστοσελίδων και των διαδικτυακών εφαρμογών έχει γίνει άκρως σημαντική μετά τις πρόσφατες επιθέσεις hacking. Επομένως οι χρήστες θα πρέπει να ευαισθητοποιηθούν σε θέματα ασφάλειας και

να λάβουν τα κατάλληλα μέτρα. Η ασφάλειας γίνεται πιο κρίσιμη για ιστοσελίδες που ανήκουν σε εταιρείες και οργανισμούς., όπου εκεί μπορεί ο αντίκτυπος να είναι ακόμη μεγαλύτερος. Με τη βοήθεια των πρόσθετων του firefox μπορείτε να εκτελέσετε ένα πρώτο έλεγχο στην ιστοσελίδα σας ή στην διαδικτυακή εφαρμογή, για να εντοπίσετε τυχόν κενά ασφαλείας και να τα επιδιορθώσετε έτσι ώστε να μην παραβιάσουν τον ιστότοπο σας. Τα πρόσθετα αφορούν τους ελέγχους που αν αναγνωρίζονται διεθνώς με την ορολογία penetration tests. Ορισμένα από τα οποία παρέχονται στον firefox είναι:

1. Το *Exploit-ME* είναι ένα σύνολο εργαλείων ελέγχου που παρέχεται στον firefox και παρουσιάστηκε πρώτη φορά στο συνέδριο ασφάλειας SecTor στο Τορόντο. Το εργαλείο είναι πολύ εύκολο στη χρήση του και μπορείτε να ελέγξετε οποιαδήποτε ιστοσελίδα για τυχόν ευπάθειες που μπορεί να γίνουν εκμεταλλεύσιμες από ένα επιτιθέμενο,
2. Το *XSS-ME* είναι ένα μέρος του Exploit-ME και εντοπίζει ευπάθειες τύπου Cross-Site-Scripting(XSS) που είναι πολύ γνωστές για την πρόκληση σοβαρών ζημιών σε μια ιστοσελίδα.
3. *SQL inject ME*. Οι ευπάθειες τύπου SQL injection μπορούν να προκαλέσουν σοβαρές ζημιές σε διαδικτυακές εφαρμογές. Ένας κακόβουλος χρήστης μπορεί πιθανότατα να έχει πρόσβαση σε προσωπικές καταγραφές, να τις διαγράψει ή ακόμη και να αποκτήσει πρόσβαση στον εξυπηρέτη σας.
4. *Access ME*. Οι ευπάθειες πρόσβασης μπορούν να επιτρέψουν σε έναν επιτιθέμενο να έχει πρόσβαση σε δεδομένα, χωρίς να είναι εξουσιοδοτημένος. Το Access ME είναι ένα πρόσθετο του firefox για την εκτέλεση ελέγχων που αφορούν την εύρεση ευπαθειών παράνομης πρόσβασης.

### 8.3.2 BackBox Linux 3.0.1 – Pen testing Distro

Επίσημη ιστοσελίδα: http://www.backbox.org/

Το **BackBox** είναι μια έκδοση **Ubuntu** που διαθέτει εργαλεία ελέγχου & τρόπου ηλεκτρονικής διείσδυσης και αξιολόγησης αδυναμιών. Με κύριο γνώμονα την ασφάλεια το Backbox έχει προσανατολισμό την διάθεση ενός ολοκληρωμένου εργαλείο ελέγχου δικτύων πληροφορικής και ανάλυσης συστημάτων.

Η ομάδα **BackBox** κυκλοφόρησε την ενημερωμένη έκδοση του **BackBox Linux, 3.01**. Αυτή η έκδοση περιλαμβάνει χαρακτηριστικά όπως το **Linux Kernel 3.2** και το **Xfce 4.8**.

**Νέα χαρακτηριστικά:**

- Νέα και ενημερωμένα εργαλεία hacking (π.χ. backfuzz, beef, bluediving, cvechecker, htexploit, metasploit, set, sqlmap, websploit, weevely, wpscan, zaproxy κ.α.)
- Βελτίωση του συστήματος
- Upstream components
- Επιδιορθώσεις σφαλμάτων
- Ενισχυμένη απόδοση
- Βελτιωμένο μενού ελέγχου
- Βελτιωμένοι Wi-Fi dirvers (συμβατότητα/υποστήριξη συσκευών - ενημερωμένη έκδοση aircrack)

### 8.3.3 Bugtraq 2 – Μαύρη Χήρα

Επίσημη σελίδα: http://www.bugtraq-team.com/web/


Το **Bugtraq-2 Black Widow** είναι μοναδικό στον τομέα της ασφάλειας, το οποίο επιβεβαιώνει με τον καλύτερο τρόπο πώς πρέπει να είναι μια linux διανομή σχετική με το hacking Ορισμένοι αρχίζουν να το ονομάζουν «Διανομή Όλα-σε-ένα για το hacking».

**Χαρακτηριστικά**

Το σύστημα Bugtraq προσφέρει την πιο ολοκληρωμένη διανομή, με τη βέλτιστη, σταθερή και αυτοματοποιημένη διαχείριση των υπηρεσιών σε πραγματικό χρόνο. Η διανομή έχει ως βάση τους πυρήνες 3.2 και 3.4 PAE, ενώ διαθέτει ένα τεράστιο φάσμα εργαλείων από εργαλεία διείσδυσης, εγκληματολογικής ανάλυσης και λοιπά εργαστηριακά εργαλεία εξομοίωσης. Η ομάδα ανάπτυξης του Bugtraq θεωρεί ότι δεν πρέπει να θέσει όρια στο λειτουργικό και πιστεύει ότι κάθε χρήστης πρέπει να έχει την δυνατότητα να χρησιμοποιεί διαφορετικά εργαλεία καλύπτοντας μια πληθώρα στόχων.

**Εργαλεία**

Μια από τις καινοτομίες του Bugtraq είναι η τεράστια γκάμα εργαλείων σε διαφορετικούς τομείς. Μπορούμε να βρούμε εργαλεία εγκληματολογικής ανάλυσης για κινητά, εξομοίωση και πλατφόρμες ελέγχου κακόβουλων λογισμικών, εργαλεία της Κοινότητας Bugtraq, εργαλεία ελέγχου για το GSM, το ασύρματο δίκτυο, το Bluetooth και το RFID. Επίσης, ολοκληρωμένα εργαλεία για Windows, εργαλεία που επικεντρώνονται σε IPv6 και τυπικά εργαλεία ελέγχου και ηλεκτρονικής εγκληματολογικής ανάλυσης (forensics).

Κάθε εργαλείο εκτελεί όλες τις υπηρεσίες που χρειάζονται για να λειτουργήσουν και έχουν ρυθμιστεί εξαρχής για βέλτιστη απόδοση. Η ομάδα έχει δημιουργήσει σενάρια που επιτρέπουν την καλύτερη διαχείριση και ταχύτητα κατά στην εγκατάσταση ορισμένων εργαλείων. Το Bugtraq-2 είναι ακόμα πιο γρήγορο και δυναμικό σύστημα που με μερικά κλικ μπορείτε να εγκαταστήσετε ή να εκτελέσετε όλες τις διεργασίες που θέλετε, χωρίς να ψάξετε στο διαδίκτυο για tutorials ή τρόπους εγκατάστασης των εργαλείων.

### 8.3.4 Περιηγητής Sandcat

Είναι ένα δωρεάν εργαλείο ειδικά σχεδιασμένο για τεχνικούς ασφάλειας πληροφοριακών συστημάτων με πολλές επιλογές και πρόσθετα, καθώς υποστηρίζεται από την τεχνική ομάδα Szhunt, η οποία έχει δημιουργήσει και τη διαδικτυακή εφαρμογή «Syhunt Web Application Security Scanner». Ο περιηγητής Sandcat έχει σχεδιαστεί με βάση το Chromium, την ίδια πλατφόρμα, δηλαδή, που έχει χρησιμοποιηθεί και για τον περιηγητή Google Chrome και χρησιμοποιεί τη γλώσσα Lua για να παρέχει πρόσθετα και τεχνική υποστήριξη όσο αφορά το scripting.

Χαρακτηριστικά για Pen-Testers:

- Live http Headers
- Κονσόλα Sandcat για την εκτέλεση διαμορφωμένων εντολών και scripts σε μια ιστοσελίδα.
- Επέκταση Request Editor
- Πρόσθετο fuzzer με πολλαπλές μορφές και υποστήριξη για φίλτρα
- Πρόσθετο javascript Executor που επιτρέπει την φόρτωση και εκτέλεση εξωτερικών αρχείων javascript
- Πρόσθετο Lua Executor που επιτρέπει την φόρτωση και εκτέλεση εξωτερικών Lua Scripts
- Syshunt Gelo που απλοποιεί και επιταχύνει τη δημιουργία πρόσθετων για exploit
- Πρόσθετο Pageinfo που επιτρέπει την προβολή page headers, αντικείμενα Javascripts κ.α.
- Πρόσθετο TOR για ανωνυμία κατά τη διάρκεια αποστολής και λήψης εντολών
- HTTP Brute Force, CGI Scanner Scripts, Encoders-Decoders και πολλά άλλα.

### 8.3.5 Arachni Web application Security Scanner Framework

Επίσημη σελίδα: http://www.arachni-scanner.com/

Πρόκειται για ένα «έξυπνο» εργαλείο που μαθαίνει από τις http απαντήσεις που λαμβάνει κατά τη διαδικασία ελέγχου. Είναι ικανό να εκτελέσει meta-ανάλυση χρησιμοποιώντας έναν αριθμό παραγόντων με σκοπό την επιβεβαίωση των αποτελεσμάτων και την ανακάλυψη ενδεχόμενων προβλημάτων τα οποία δεν υπάρχουν.

Προσαρμόζεται εύκολα σε διάφορα περιβάλλονται και περιλαμβάνει από ένα απλό ανιχνευτή γραμμής εντολών μέχρι πλέγμα ανιχνευτών που πραγματοποιούν ανίχνευση σε παγκόσμιο επίπεδο.

Χαρακτηριστικά:

- Cookie-jar/cookie-string υποστήριξη
- Custom header υποστήριξη
- SSL
- User agent spoofing
- Proxy για SOCK4, SOCK5, HTTP/1.1. και HTTP/1.0
- Πιστοποίηση Proxz
- Πιστοποίηση Ιστοσελίδων
- Αυτόματη ανίχνευση καταγραφής
- Ανίχνευση 404 σελίδων
- Δυνατότητα παύσης
- Γραμμή εντολών και γραφικό περιβάλλον
- Υψηλές αποδόσεις ασύγχρονων http requests.

Επιπλέον στην πιο πρόσφατη έκδοση οι χρήστες :

- Γραφικό περιβάλλον για εύκολη εκτέλεση και διαχείριση ελέγχων
- Αρκετά μειωμένη χρήση RAM
- Βελτιωμένα payloads για μηχανήματα με Windows.
- Δυνατότητα αποκλεισμού σελίδων από μία αναζήτηση

[6],[30],[58],[66],[68]

### 8.3.6 Kali Linux Penetration Testing Distribution v1.0.3

Επίσημη σελίδα: http://www.kali.org/

Είναι η νέα γενιά της σουίτας ελέγχων ασφάλειας Backtrack. Έχει υιοθετήσει τα standard του debian και όλα εργαλεία που περιέχει είναι αναθεωρημένα.

Περιέχει :

- Περισσότερα από **300** εργαλεία για ελέγχους τρωτότητας. Κάποια από τα εργαλεία που περιείχε το Backtrack και δεν ήταν λειτουργικά, χρήσιμα ή υπήρχαν κάποια άλλα πιο αποτελεσματικά, αντικαταστάθηκαν.
- Είναι δωρεάν. Δεν πρόκειται για ένα κόλπο marketing. Θα είναι πάντα δωρεάν.
- FHS συμβατότητα. Επιτρέπει στους χρήστες του Linux να εντοπίζουν εύκολα δυαδικά αρχεία, καταλόγους και αρχεία βοήθειας.
- Υποστήριξη ασύρματων συσκευών.
- Υποστήριξη ασφαλών πρωτοκόλλων.
- GPG signed packages και repos.
- Υποστηρίζει πολλές γλώσσες
- Είναι εντελώς παραμετροποιήσιμο.
- Υποστηρίζει ARPMEL και ARMHF

[20],[36],[71],[72],[84]

## 8.4 Έλεγχος Δικτύων

Η υποενότητα αυτή περιλαμβάνει προγράμματα με δυνατότητες καταγραφής και ανάλυσης πακέτων και διαχείρισης της κυκλοφορίας δικτύων ασύρματών ή μη.

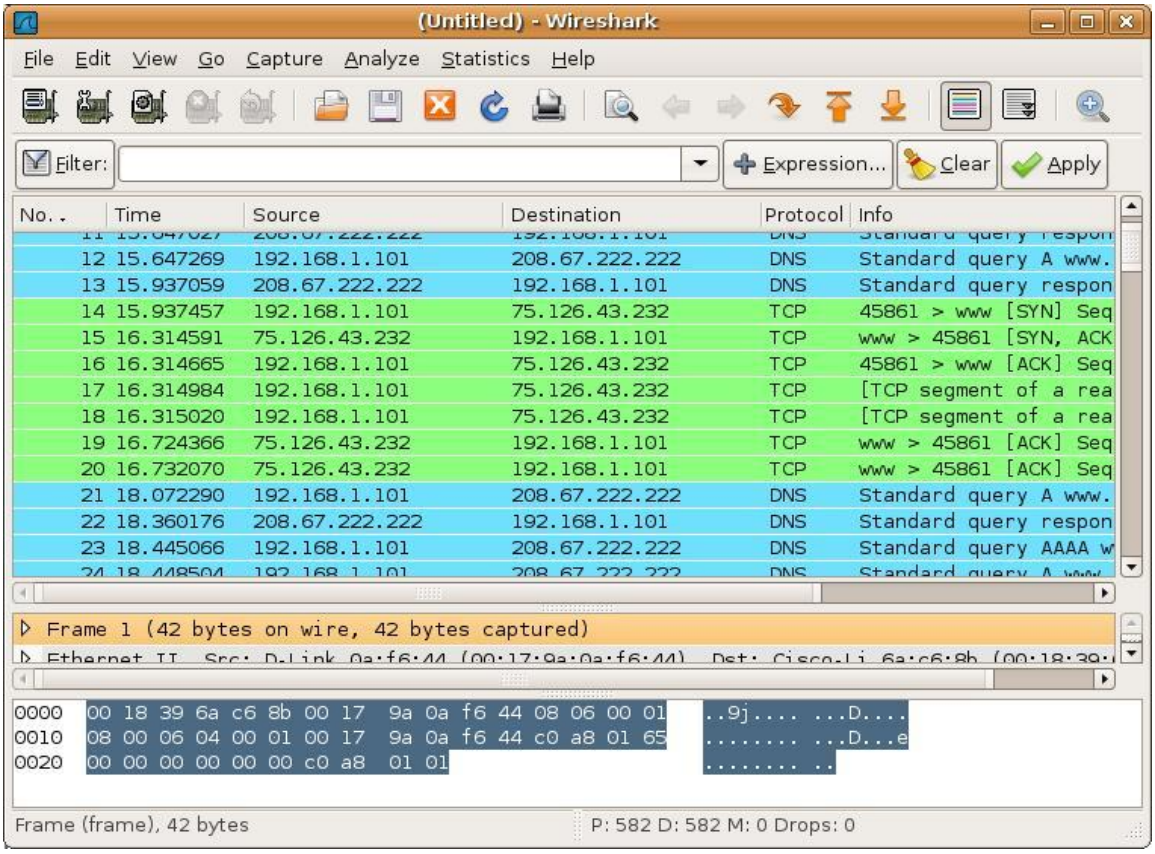
### 8.4.1 Wireshark

Επίσημη ιστοσελίδα: http://www.wireshark.org/

Άδεια χρήσης: Δωρεάν

Επιπλέον πληροφορίες: Είναι ιδανικό για εκπαιδευτικούς σκοπούς

Είναι ένας αναλυτής πακέτων(network sniffer) ανοιχτού κώδικα για Windows, mac και Linux πλατφόρμες.




Εικόνα 8.4.1. Περιβάλλον εργασίας Wireshark.

Το wireshark χρησιμοποιείται για αλίευση (sniffing) και καταγραφή (capturing) πακέτων κυκλοφορίας σε ένα δίκτυο και για την εξέταση πρωτοκόλλων και συνεδριών (sessions) σε βάθος. Αν χρειάζεται κάποιος να καταγράψει την κυκλοφορία σε ένα ασύρματο( ethernet) δίκτυο ή εξετάζει(ακόμη και αποκρυπτογραφεί) συγκεκριμένα πρωτόκολλα είναι ένα εργαλείο που θα του φανεί χρήσιμο. Τρέχει σε διάφορες πλατφόρμες και υποστηρίζει την καταγραφή διαφόρων ειδών αρχείων.

### 8.4.2 AirCRACK-NG

Επίσημη ιστοσελίδα: http://www.aircrack-ng.org/

Άδεια χρήσης: Δωρεάν

Το Aircrack-ng είναι ένα ολοκληρωμένο σύνολο από εργαλεία για την ασφάλεια του δικτύου, που περιλαμβάνει το **aircrack-ng** (που μπορεί να πραγματοποιήσει WEP και WPA επιθέσεις Dictionary), το **airdecap-ng** (το οποίο μπορεί να

αποκρυπτογραφεί WEP ή WPA κρυπτογραφημένα αρχεία καταγραφής), το **airmon-ng** (το οποίο τοποθετεί κάρτες δικτύου σε λειτουργία παρακολούθησης, όπως για παράδειγμα, κατά τη χρήση του σαρωτή ασφαλείας Alfa με rtl8187), το **aireplay-ng** (το οποίο είναι ένας packet-injector), το **airodump-ng** (το οποίο είναι ένας packet sniffer), το **airtun-ng** (που επιτρέπει την σύνδεση μέσω virtual tunnel), το **airolib-ng** (το οποίο αποθηκεύει και διαχειρίζεται ESSID και καταλόγους με κωδικούς πρόσβασης), το **packetforge-ng** (το οποίο μπορεί να δημιουργήσει κρυπτογραφημένα πακέτα για injection), το **airbase-ng** (που ενσωματώνει τεχνικές για να επιθέσεις σε πελάτες) και το **airdecloak-ng** (που αφαιρεί τη WEP απόκρυψη). Περιλαμβάνονται και άλλα εργαλεία όπως **airdriver-ng** (για τη διαχείριση των ασύρματων drivers), το **airolib-ng** (για την αποθήκευση και διαχείριση ESSID καταλόγων με κωδικούς πρόσβασηςr), το **airserv-ng** (το οποία επιτρέπει σε ένα ελεγκτή διείσδυσης την πρόσβαση στις ασύρματες κάρτες απομακρυσμένων υπολογιστών). Το Airolib-ng είναι παρόμοιο με **easside-ng** που επιτρέπει στο χρήστη να τρέχει εργαλεία σε έναν απομακρυσμένο υπολογιστή, το easside-ng (επιτρέπει σε ένα μέσο την επικοινωνία με ένα σημείο πρόσβασης(Access point), χωρίς το κλειδί WEP), το **tkiptun-ng** (για WPA / TKIP επιθέσεις) και το **wesside-ng** (το οποίο αποτελεί ένα αυτοματοποιημένο εργαλείο για την ανάκτηση των κλειδιών WEP).

Περιλαμβάνει ένα γραφικό περιβάλλον(GUI) που ονομάζεται Gerix Wifi Cracker και το οποίο διανέμεται δωρεάν(GNU General Public License). Συμπεριλαμβάνεται σε σουίτες ασφαλείας όπως το Backtrack και το Backbox.

Το Gerix GUI έχει πολλά εργαλεία δοκιμών διείσδυσης που επιτρέπουν την ανάλυση του δικτύου, την ασύρματη σύλληψη πακέτων καθώς και Packet SQL injection.

### 8.4.3 Ettercap.

Επίσημη ιστοσελίδα: http://ettercap.github.io/ettercap/

Άδεια χρήσης: Δωρεάν

Το Ettercap συνοδεύει συνήθως το εργαλείο Cain. Είναι ένα ελεύθερο και ανοικτού κώδικα εργαλείο ασφάλειας για man-the-middle επιθέσεις (MITM) σε ένα τοπικό δίκτυο(LAN). Μπορεί να χρησιμοποιηθεί για την ανάλυση πρωτοκόλλων δικτύων υπολογιστών μέσα σε ένα πλαίσιο ελέγχου ασφαλείας. Το Ettercap έχει τέσσερις μεθόδους λειτουργίας:


Σάρωση ασφαλείας με φιλτράρισμα IP-based πακέτων, Σάρωση με MAC-based φιλτράρισμα όπου τα πακέτα φιλτράρονται με βάση τη διεύθυνση MAC, (αυτό είναι χρήσιμο για sniffing

πακέτων της gateway). Επίσης ARP-based σάρωση χρησιμοποιώντας ARP-poisoning για sniffing σε LAN μεταξύ δύο hosts (γνωστή ως full-duplex). Τέλος PublicARP-based λειτουργικότητα όπου το Ettercap χρησιμοποιεί ARP poisoning για να καταγράψει την κίνηση σε ένα ενεργό LAN από το host του θύματος για όλους τους υπόλοιπους hosts(half-duplex).

### 8.4.4 kismet.

Επίσημη ιστοσελίδα: http://www.kismetwireless.net/

Άδεια χρήσης: δωρεάν

Είναι ένας ανιχνευτής ασύρματων δικτύων, ένας sniffer, ένα σύστημα ανίχνευσης ανεπιθύμητων εισόδων στο σύστημα και ένα εργαλείο ελέγχων τρωτότητας. Μπορεί να καταγράψει και να παρακολουθεί την κυκλοφορία από 802.11b, 802.11g και 802.11n δίκτυα. Αυτό που κάνει το Kismet να διαφέρει από τα υπόλοιπα εργαλεία είναι το γεγονός ότι «εργάζεται» παθητικά κάτι το οποίο σημαίνει ότι δεν στέλνει πακέτα αναφορών κατά τη διάρκεια της καταγραφής ασύρματων Access points και χρηστών που χρησιμοποιούν ασύρματα δίκτυα γενικότερα. Είναι ανοιχτού κώδικα και χρησιμοποιείτε ευρέως.

### 8.4.5 Firesheep

Είναι ένα πρόσθετο του firefox που δίνει τη δυνατότητα σε οποιονδήποτε να υποκλέψει τα cookies άλλων χρηστών που συνδέονται από το ίδιο δημόσιο wifi hotspot. Με ένα απλό κλικ μπορεί κανείς να αποκτήσει πλήρες πρόσβαση στο προφίλ άλλων σε διαδικτυακές υπηρεσίες όπως το facebook, το twitter ,Google, Flicker κτλ.

Τις πρώτες 24 ώρες τις κυκλοφορίας του έγιναν 130.000 λήψεις του firesheep. Δημιουργήθηκε για να δώσει έμφαση στην προβληματική προσέγγιση που ακολουθούν οι ιστοσελίδες σε θέματα ασφάλειας. Η ευκολία με την οποία παραβιάζεται ο λογαριασμός ενός άλλος χρήστη είναι συγκλονιστική

Δεν αφορά WPA passwords

[73],[78]

### 8.4.6 Σύγκριση εργαλείων ελέγχου δικτύων

Ως κριτήρια σύγκρισης θα χρησιμοποιηθούν οι δύο τελευταίες κλάσεις κριτηρίων από το συγκριτικό πλαίσιο αξιολόγησης που περιγράφηκε στο κεφάλαιο 7.

**Εφαρμοσμένα τεχνολογικά ζητήματα**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- B1. Απόδοση
- B2. Πολυπλοκότητα εγκατάστασης
- B3. Τελική αναφορά αποτελεσμάτων
- B4. Φορητότητα
- B5. Χρονική επιβάρυνση

| **Κριτήρια:** <br><br> **Προγράμματα** | **B1** | **B2** | **B3** | **B4** | **B5** |
|---|---|---|---|---|---|
| Wireshark | M | Υ | X | Υ | Υ |
| AirCRACK-NG | Υ | M | M | Υ | M |
| Ettercap | M | M | X | M | M |
| Kismet | M | M | X | M | M |
| Firesheep | Υ | Υ | X | X | Υ |

**Ικανοποίηση απαιτήσεων των χρηστών.**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- C1. Ευκολία χρήσης.
- C2. Κοινότητα υποστήριξης
- C3. Κόστος
- C4. Πληρότητα

| **Κριτήρια:** <br><br> **Προγράμματα** | **C1** | **C2** | **C3** | **C4** |
|---|---|---|---|---|
| Wireshark | M | Υ | Υ | M |
| AirCRACK-NG | M | X | Υ | Υ |
| Ettercap | M | X | Υ | X |
| Kismet | Υ | M | Υ | M |
| Firesheep | Υ | X | Υ | M |

*Η διαθέσιμη επιλογή Υψηλή(Υ) σημαίνει σε κάθε περίπτωση την καλύτερη απόδοση. Στο κριτήριο κόστος για παράδειγμα σημαίνει ότι το προϊόν προσφέρεται δωρεάν είτε είναι ανοιχτού κώδικα. Το κριτήριο πληρότητα στη αξιολόγηση εργαλείων που εξετάζουν συγκεκριμένες ευπάθειες αφορά λειτουργίες μέσα στο εύρος δυνατοτήτων των προγραμμάτων αυτής της κατηγορίας.*

## 8.5 Έλεγχος κωδικών πρόσβασης

### 8.5.1 Pipal

Ανάλυση συνθηματικών χρήσης.

Επίσημη ιστοσελίδα: http://www.digininja.org/projects/pipal.php

Άδεια χρήσης: Δωρεάν

Προσπαθώντας να αποκρυπτογραφήσετε ένα σύνολο κρυπτογραφημένων κωδικών, χρησιμοποιώντας **wordlist** ή **brute force**, τις περισσότερες φορές θα απομένουν κάποιοι κωδικοί που δεν θα μπορείτε να «αποκαλύψετε». Σε αυτές τις περιπτώσεις είναι χρήσιμο ένα εργαλείο ανάλυσης κωδικών ώστε να σας βοηθήσει να «κατευθύνετε» τις επιθέσεις «brute force» σε πιθανούς κωδικούς.

Αυτός ακριβώς είναι ο ρόλος του **Pipal**. Εκτελώντας το, αναλύει τους κωδικούς που έχετε ήδη βρει και σας δίνει στατιστικά στοιχεία ώστε να μπορέσετε να «μαντέψετε» τους υπόλοιπους.

**1. *Πως χρησιμοποιείται/εκτελείται το*** Pipal***:***

Για να το χρησιμοποιήσετε θα πρέπει να υπάρχει εγκατεστημένο περιβάλλον **And 1.9.x**. Αν για παράδειγμα έχετε εγκατεστημένο το τελευταίο backtrack στον υπολογιστή σας, δεν χρειάζεται κάτι παραπάνω. Αφού κατεβάσετε το πρόγραμμα και μπείτε στον φάκελο που το έχετε τοποθετήσει, το μόνο που χρειάζεται να κάνετε είναι να δώσετε δικαιώματα εκτέλεσης στο αρχείο (**chmod +x pipal.rb**) και είστε έτοιμοι. Για να το εκτελέσετε, δίνετε την εντολή «**./pipal.rb FILENAME**», όπου **FILENAME** είναι η λίστα με τους κωδικούς που έχετε ήδη αποκρυπτογραφήσει. Υπάρχει η δυνατότητα εξαγωγής των αποτελεσμάτων σε αρχείο. Για να δείτε όλες τις δυνατότητες του εργαλείου, δώστε την εντολή «**./pipal.rb -?**». Σε ένα μηχάνημα με ισχυρό επεξεργαστή μπορεί να αναλύσει 45.000 κωδικούς σε 1 λεπτό.

**2. *Τα αποτελέσματα του Pipal:***

Το πρώτο πράγμα που μετράει το pipal είναι οι 10 πιο συχνοί κωδικοί. Συγκρατώντας αυτή τη λίστα, μετά την ανάλυση πολλών αρχείων, μπορεί να σας βοηθήσει να δημιουργήσετε μία δική σας wordlist.
(Τα αποτελέσματα που δίνονται ως παράδειγμα παρακάτω προέρχονται από το site του εργαλείου. Το αρχείο που αναλύθηκε είναι οι κωδικοί από το **phpBB**. Πριν την ανάλυση ο χρήστης φρόντισε ο κάθε κωδικός να αναφέρεται μόνο μία φορά και γι' αυτό τα ποσοστά στην αρχή είναι μηδενικά.

*Top 10 passwords*

123456 = 1 (0.0%)
password = 1 (0.0%)

phpbb = 1 (0.0%)

qwerty = 1 (0.0%)

12345 = 1 (0.0%)

12345678 = 1 (0.0%)

letmein = 1 (0.0%)

111111 = 1 (0.0%)

1234 = 1 (0.0%)

123456789 = 1 (0.0%)

Το επόμενο και πολύ χρήσιμο στοιχείο που μετρά το εργαλείο είναι οι βασικές λέξεις. Πρόκειται δηλαδή για λέξεις που περιλαμβάνονται στους κωδικούς και προηγούνται ή έπονται άλλων συμβόλων. Για παράδειγμα οι κωδικοί «!!password123» και «password&*», έχουν ως βασική λέξη το «password». Αυτό το στοιχείο μπορεί να σας βοηθήσει να βρείτε περισσότερους κωδικούς από πριν.

*Top 10 base words*

phpbb = 332 (0.18%)
password = 89 (0.05%)

dragon = 76 (0.04%)

pass = 70 (0.04%)

mike = 69 (0.04%)

blue = 67 (0.04%)

test = 66 (0.04%)

qwerty = 59 (0.03%)

alex = 58 (0.03%)

alpha = 53 (0.03%)

Στη συνέχεια, το pipal μας πληροφορεί για τον πιο συχνό αριθμό χαρακτήρων των κωδικών στη λίστα μας.

*Password length (length ordered)*

1 = 33 (0.02%)
2 = 138 (0.07%)

3 = 777 (0.42%)

4 = 4597 (2.49%)

5 = 8199 (4.45%)

6 = 42069 (22.82%)

7 = 32731 (17.75%)

8 = 55338 (30.01%)

9 = 19187 (10.41%)

10 = 11897 (6.45%)

*Password length (count ordered)*

8 = 55338 (30.01%)
6 = 42069 (22.82%)

7 = 32731 (17.75%)

9 = 19187 (10.41%)

10 = 11897 (6.45%)

5 = 8199 (4.45%)

11 = 4934 (2.68%)

4 = 4597 (2.49%)

12 = 2506 (1.36%)

13 = 1019 (0.55%)

Ακολουθούν μερικά ακόμη στατιστικά στοιχεία που σχετίζονται με το μήκος και το είδος των κωδικών. Όπως για παράδειγμα, πόσοι κωδικοί έχουν 1-6 χαρακτήρες ή πόσοι περιλαμβάνουν μόνο γράμματα και άλλα.

One to six characters = 55807 (30.27%)
One to eight characters = 143874 (78.03%)

More than eight characters = 40507 (21.97%)

Only lowercase alpha = 76041 (41.24%)
Only uppercase alpha = 1706 (0.93%)

Only alpha = 77747 (42.17%)

Only numeric = 20728 (11.24%)

First capital last symbol = 225 (0.12%)
First capital last number = 4749 (2.58%)

Αυτά είναι τα σημαντικότερα χαρακτηριστικά του εργαλείου, όμως το σύνολο των πληροφοριών που μας δίνει το πρόγραμμα είναι τεράστιο. Μετράει, επίσης, πόσες φορές εμφανίζονται ονόματα μηνών ή ημερών στη λίστα μας, ποια τελευταία ψηφία εμφανίζονται συχνότερα, στατιστικά σετ χαρακτήρων (Character sets) καθώς και **Hashcat Masks** (αν χρησιμοποιείτε Hashcat για την αποκρυπτογράφηση των κωδικών, είναι πολύ χρήσιμη πληροφορία).
[7]

### 8.5.2 oclHashcat-plus

Επίσημη ιστοσελίδα: http://hashcat.net/oclhashcat-plus/

Άδεια χρήσης: δωρεάν

Είναι το γρηγορότερο εργαλείο παραβίασης κωδικών πρόσβασης που χρησιμοποιεί GPU και αποκωδικοποιεί md5crypt, phases, smash2 και WPA/WPA2

Χαρακτηριστικά:

- είναι δωρεάν
- multi-gnu(μέχρι 16 gpus)
- multi-hash(μέχρι 24 έκτα. hashes)
- Multi-OS(Windows και Linux native binaries)
- Χαμηλή χρήση ενέργειας, μπορείτε ταυτόχρονα να βλέπετε ταινίες ή να παίζετε ηλεκτρονικά παιχνίδια
- Εστιάζει σε χρήσης αποκρυπτογράφησης hashes με πολλαπλές μεθόδους
- Εστιάζει σε επιθέσεις που βασίζονται σε dictionary
- Υποστηρίζει pause-resume κατά τη διάρκεια του cracking
- Υποστηρίζει την ανάγνωση λέξεων από αρχείο
- Υποστηρίζει την ανάγνωση λέξεων από stdin
- Ενσωματωμένη παρακολούθηση
- Πάνω από 20 υποστηριζόμενοι αλγόριθμοι

### 8.5.3 Hydra v 7.4

Επίσημη ιστοσελίδα: http://www.thc.org/thc-hydra/

Εικόνα 8.5.3. Το σήμα του εργαλείου Hydra

Ένα εργαλείο ελέγχου ασφάλειας που χρησιμοποιείται για την παραβίαση κωδικών πρόσβασης, το **THC-Hydra** διατίθεται πλέον στην ενημερωμένη έκδοση **7.4**.

Το **THC-Hydra** είναι συμβατό με **Linux**, **Windows/Cygwin**, **Solaris 11**, **FreeBSD 8.1** και **OSX**. Υποστηρίζει ένα πολύ μεγάλο αριθμό πρωτοκόλλων όπως AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC και XMPP.

**Νέα χαρακτηριστικά:**

- Νέο module: SSHKEY – για τον έλεγχο προσωπικών κλειδιών ssh
- Πρόσθετη υποστήριξη για win8 και win2012 server στο RDP module
- Καλύτερη κατανομή στόχων εάν χρησιμοποιηθεί η παράμετρος –M
- Προσθήκη χρωματιστών αποτελεσμάτων
- Βελτιωμένος εντοπισμός καταλόγου για Cygwin και OS X

- Επιδιόρθωση της επιλογής –W
- Επιδιόρθωση ευπάθειας στην επιλογή –e, όταν χρησιμοποιούνταν χωρίς τις -u, -l, -L ή –C
- Επιδιόρθωση σφάλματος στο HTTP Form module
- Επιδιόρθωση σφάλματος στο SMB module return code
- Επιδιόρθωση του http-{get|post-form} from xhydra
- Προσθήκη υποστήριξης OS/390 και 64bit
- Προσκη ορίου στην εισαγωγή αρχείων -L, -P, -C και–M
- Προσθήκη επιλογής debug κατά τη χρήση

[8],[18]

## 8.6 Εξειδικευμένες αναζητήσεις

### 8.6.1 Viproy – VoIP Penetration testing Kit

Επίσημη ιστοσελίδα: https://github.com/fozavci/viproy-voipkit

Αναπτύχθηκε για να βελτιώσει την ποιότητα των SIP ελέγχων τρωτότητας. Δίνει τη δυνατότητα δημιουργίας απλών ελέγχων.

Περιλαμβάνει 7 διαφορετικές μονάδες(modules) με υποστήριξη γνησιότητας: επιλογές του ελεγκτή, επιθέσεις τύπου brute force, απογραφέα(enumerator), αναλυτή εμπιστοσύνης, πρόσκληση συνεργάτη ελεγκτή, proxy και ελεγκτή καταχωρήσεων(registration tester). Όλες οι επιθέσεις μπορούν να πραγματοποιηθούν πριν και μετά την πιστοποίηση των fuzz SIP υπηρεσιών.

[80]

### 8.6.2 ERPScan. SAP Pentesting Tool

Είναι ένα εργαλείο για ελέγχους τρωτότητας σε συστήματα SAP. Διατίθεται ελεύθερα και είναι σχεδιασμένο για Black Box μεθοδολογίες ελέγχου. Αυτό σημαίνει ότι δεν χρειάζεται να ξέρει κάποιος καμία πληροφορία για το υπό εξέταση σύστημα ή να έχει ένα νόμιμο λογαριασμό σε αυτό. Όλες οι πληροφορίες μπορούν να μαζευτούν από το εργαλείο.

- Περιέχει 31 modules
- 18 για αναζήτηση πληροφοριών
- 3 για την εκτέλεση εντολών
- 8 Aux
- 4 DoS
- P4 Password decryptor plugin κτλ.

Χαρακτηριστικά :

- Μπορεί να συλλέξει πληροφορίες
- Να εκμεταλλευτεί πιθανές ευπάθειες
- Να συλλέξει κρίσιμα δεδομένα της επιχείρησης.

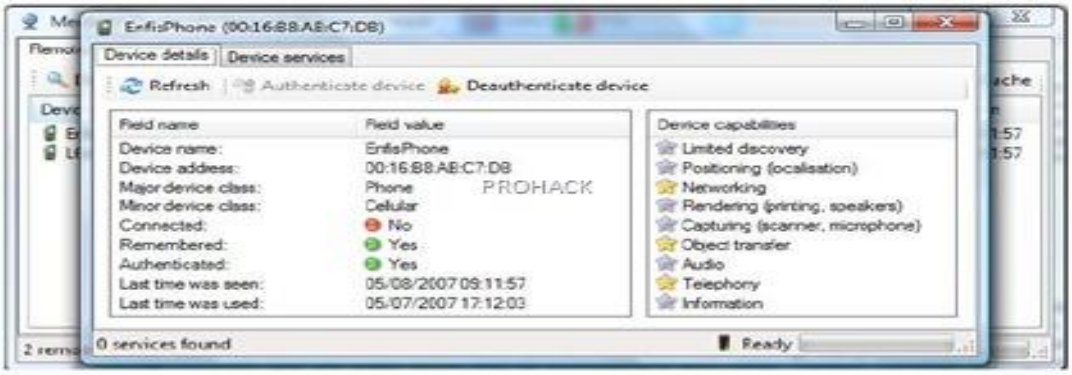
### 8.6.3 PWNTOOTH – Automated Bluetooth Pentesting Tool

Επίσημη ιστοσελίδα: http://sourceforge.net/projects/pwntooth/files/

Σχεδιάστηκε για την αυτοματοποιημένο έλεγχο τρωτότητας σε Bluetooth. Ψάχνει για συσκευές και μετά εκτελεί τα εργαλεία που έχουν καθοριστεί στο αρχείο pwntooth.conf(blueper, bluesnarfer, Bluetooth Stack smasher(BSS) carwhisperer, psm_scan, rfcomm_scan και το vcardblaster). Απευθύνεται σε προχωρημένους χρήστες που επιθυμούν να εκτελέσουν μία σειρά από tests απέναντι σε μία συσκευή. Μπορεί να συνεργαστεί και με άλλα εργαλεία που δεν περιλαμβάνονται στο πακέτο.

### 8.6.4 Mediaval Bluetooth Network Scanner

Επίσημη ιστοσελίδα: http://www.medieval.it/bluescan-pc/menu-id-72.html




Εικόνα 8.6.4. Mediaval- οθόνη κατάστασης συσκευής

Αυτό το πρόγραμμα μπορεί να αναλύσει και να ανιχνεύσει ένα bluetooth δίκτυο δίνοντας λεπτομερής πληροφορίες σχετικά με τοπικές και απομακρυσμένες συσκευές. Είναι απολύτως δωρεάν και αρκετά λειτουργικό. Μπορείτε να ελέγχετε όλες τις υπηρεσίες του Bluetooth με αυτό το λογισμικό.

### 8.6.5 Ghost Phisher

Επίσημη ιστοσελίδα: https://code.google.com/p/ghost-phisher/downloads/list

Επιθέσεις phishing και penetration

Το ghost phisher είναι μια εφαρμογή ελέγχου ασφάλειας για Η/Υ η οποία μπορεί να αναγνωρίσει ένα ψεύτικο διακομιστή DNS, ένα ψεύτικο DHCP Server και ψεύτικο διακομιστή http. Μπορεί να πραγματοποιήσει ολοκληρωμένη λήψη και καταγραφή των διαπιστευτηρίων http μιας Βάσης δεδομένων.

Απαιτήσεις:

Python

Python-qt4

Xterm

Subversion

Για την εγκατάσταση του απλά χρειάζεται η παρακάτω εντολή στο τερματικό μετά την αλλαγή του καταλόγου στο path όπου βρίσκονται τα ληφθέντα δεδομένα.

root@host:~#dpkg -i ghost-phiser_1.3_all.deb

Το Ghost phiser ενεργοποιείται αυτόματα με την επίσκεψη του χρήστη σε ευπαθείς σελίδες μέσω Windows και Linux. Στις σελίδες αυτές μπορεί να πραγματοποιηθεί έλεγχος ασφάλειας. Το ghost αναγνωρίζει αυτόματα το απομακρυσμένο σύστημα λειτουργίας και εμφανίζει ευπαθείς σελίδες σύμφωνα με τις πληροφορίες.

### 8.6.6 HookAnalyser

Επίσημη ιστοσελίδα: http://beenuarora.com/HookAnalyser2.2.zip

**Εργαλείο ανάλυσης κακόβουλων λογισμικών**

Είναι ένα δωρεάν πρόγραμμα που κυκλοφόρησε το 2011 για την ανάλυση εφαρμογών κατά τη λειτουργία τους. Το εργαλείο αυτό μπορεί να φανεί αρκετά χρήσιμο για την ανάλυση των malwares καθώς και για την ανάλυση των αδύναμων σημείων των εφαρμογών.

Χαρακτηριστικά:

1. Ενσωμάτωση στην εφαρμογή – Αυτό το χαρακτηριστικό επιτρέπει στον αναλυτή να παρακολουθεί και να επεμβαίνει στη λειτουργία της εφαρμογής.
2. Σύνδεση σε συγκεκριμένη λειτουργία της εφαρμογής. Επιτρέπει στον αναλυτή να επεμβαίνει κατά τη διάρκεια μιας ενεργής λειτουργίας της εφαρμογής.

3. Εκτέλεση γρήγορης στατικής ανάλυσης malware. Αυτή η ενότητα εκτελεί σάρωση σε εκτελέσιμα αρχεία για τον εντοπισμό πιθανών ιχνών κακόβουλου λογισμικού
4. Ανάλυση δυσλειτουργιών σε εφαρμογές. Ανάλυση του περιεχομένου της μνήμης όταν μια λειτουργία διακόπτεται.

# 9. Αναζήτηση Ευπαθειών στο Διαδίκτυο.

## 9.1 Σουίτες αναζήτησης ευπαθειών στο διαδίκτυο

Εργαλεία που αφορούν αποκλειστικά ελέγχους τρωτότητας στο διαδίκτυο. Η αξιολόγηση τους θα γίνει βάση των 2 τελευταίων κλάσεων σύγκρισης σύμφωνα με το κεφάλαιο 7.

### 9.1.1 OWASP Zed Attack Proxy(ZAP)

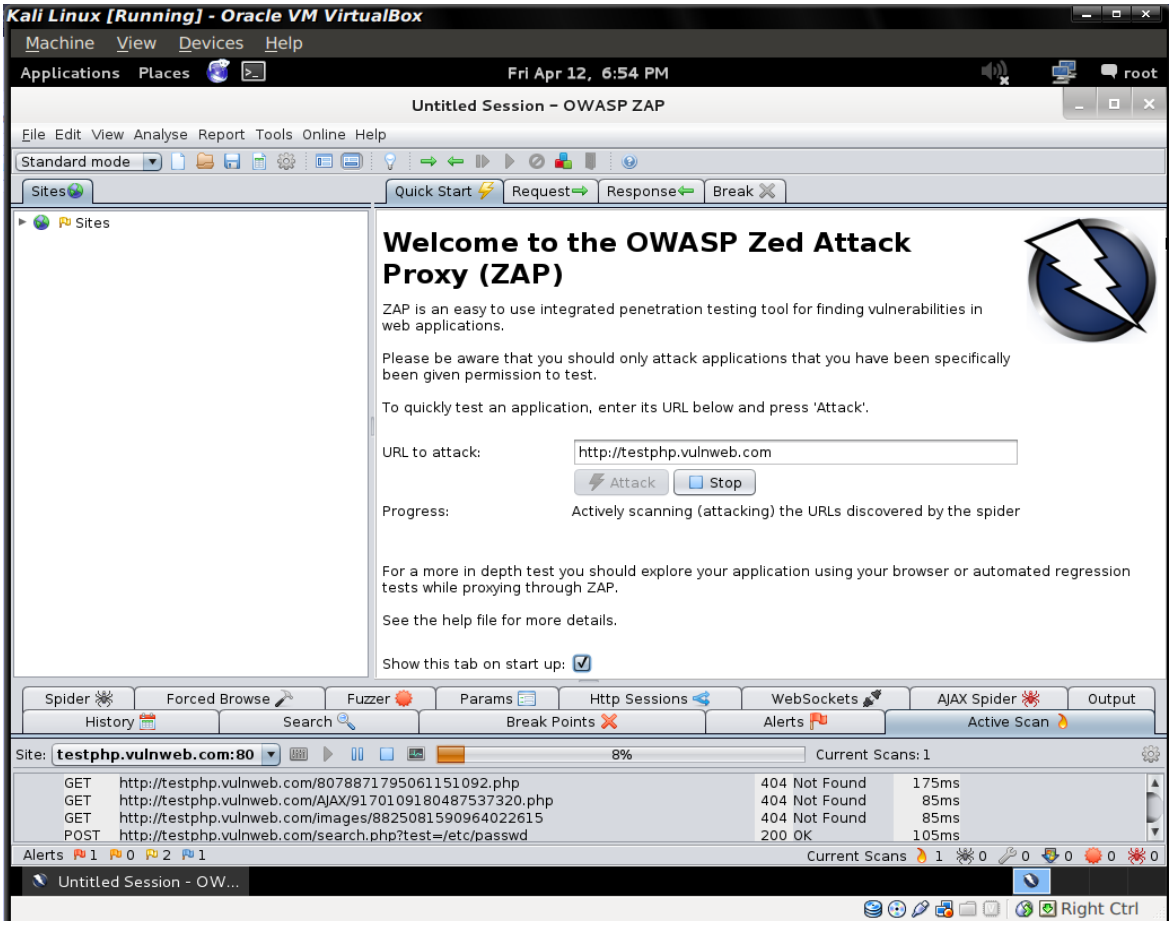
Επίσημη ιστοσελίδα:
https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

Άδεια χρήσης: Open Source

Επιπλέον πληροφορίες: Απευθύνεται σε χρήστες διαφόρων κατηγοριών.
Περιλαμβάνεται στη σουίτα Backtrack.

Πρόκειται για ένα σαρωτή ιστοσελίδων χωρίς πολλές ιδιαιτερότητες αλλά με πολλές επιλογές. Αντί περιγραφής ακολουθεί μία απλή επίδειξη.

Για την παρουσίαση θα κάνουμε μία απλή σάρωση σε μια τρωτή ιστοσελίδα. Ας βάλουμε την ιστοσελίδα του acunetix που είναι ηθελημένα τρωτή για λόγους που είναι αυτονόητοι. Η σελίδα αυτή είναι η http://testphp.vulnweb.com.

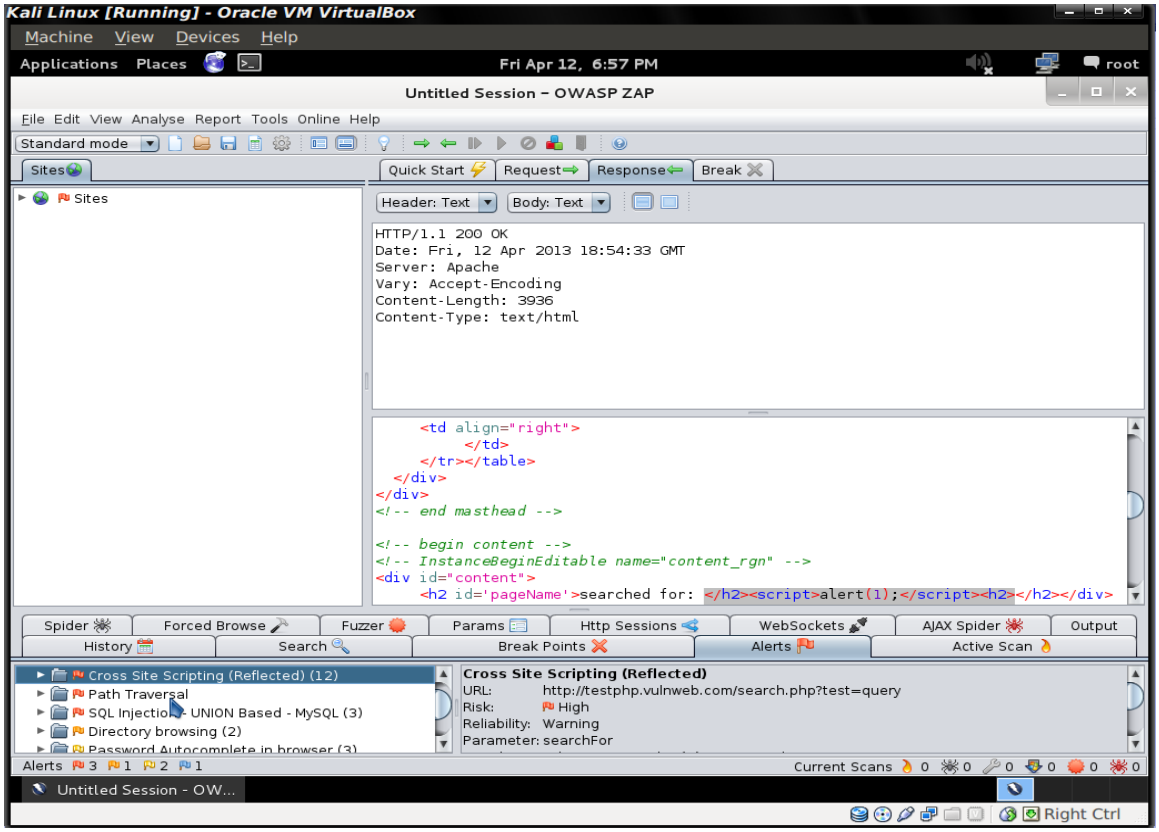



Εικόνα 9.1.1 1 Αρχική οθόνη OWASP Zed Attack Proxy

Ας την σαρώσουμε για να βρούμε τις ευπάθειες που έχει. Οπότε πάμε στο textbox που λέει δίπλα "**URL to attack**" και βάζουμε την παραπάνω διεύθυνση και πατάμε το κουμπί "**Attack**".

Μπορούμε να δούμε σε πιο στάδιο βρίσκεται και για τι είδους ευπάθειες ψάχνει σε πραγματικό χρόνο, όπως και γι' αυτές που έχει ήδη εντοπίσει πατώντας την καρτέλα "**Alerts**".

Μόλις το scan τελειώσει θα μας πάει στην καρτέλα alerts και θα μας δείξει τι βρήκε και που το βρήκε, κατηγοριοποιώντας τα αποτελέσματα ανάλογα με την επικινδυνότητα.




9.1.1 2 Αποτελέσματα ανίχνευσης ευπαθειών

Και σε πραγματικά πολύ σύντομο χρονικό διάστημα έχετε βρει τις περισσότερες αδυναμίες μιας ιστοσελίδας.

Υπέρ:

Εύκολη εγκατάσταση(χρειάζεται Java 1.6)

Αναλυτικά αρχεία βοήθειας

Είναι σε διαρκή και ενεργή βελτίωση

Είναι δωρεάν

Είναι cross-platform

Κατά:

Είναι σχεδιασμένο κυρίως για μη αυτόματη ανίχνευση κενών ασφάλειας

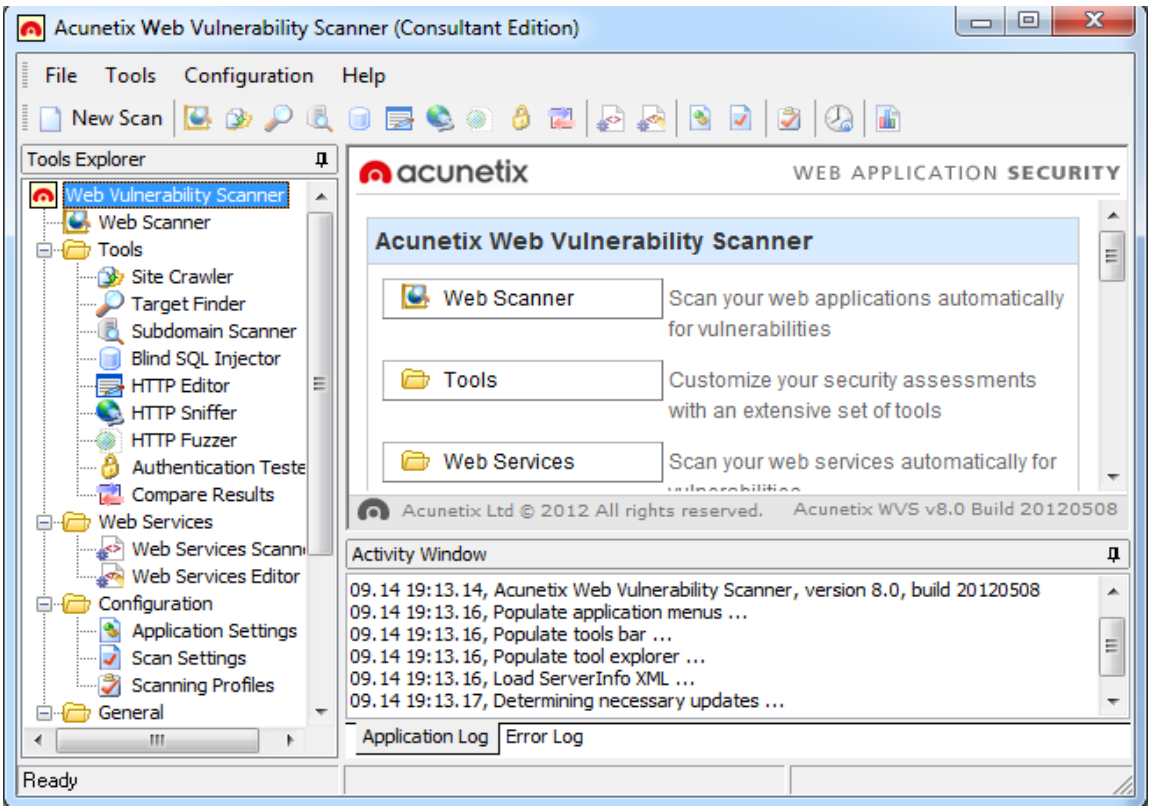
Όταν λειτουργεί αυτοματοποιημένα κάνει αρκεί θορυβώδης αναζητήσεις με αποτέλεσμα να γίνεται αντιληπτό

### 9.1.2 Acunetix Web Vulnerability Scanner

Επίσημη ιστοσελίδα: http://www.acunetix.com/

Άδεια χρήσης: Εμπορική και δωρεάν δοκιμαστική έκδοση.

Θεωρείται ένα από τα καλύτερα εργαλεία στην ασφάλειας διαδικτυακών εφαρμογών. Είναι ικανό για τη λειτουργία πολλών διαφορετικών ευπαθειών όπως SQL injection και XSS Exploits. Έχει πρόσθετους crawlers, http editors και fuzzers και παρέχει ένα μεγάλο αριθμό διαγνωστικών εργαλείων για την επικύρωση – validate and verify flaws.




9.1.2 1 Acunetix Web Vulnerability Scanner – αρχική οθόνη

Η έκδοση του **Acunetix Web Vulnerability Scanner 8** έφερε κάποια νέα χαρακτηριστικά στους ελέγχους ασφάλειας, καθώς επίσης και ενημέρωση για το σύνολο των ευπαθειών.

**Τα νέα χαρακτηριστικά:**

- Δυνατότητα εισαγωγής πολλαπλών καταγραφών HTTP Sniffer στο ίδιο crawl.
- Δυνατότητα συγχώνευσης των καταγραφών HTTP Sniffer στα ήδη υπάρχοντα crawls της ιστοσελίδας.
- Μια νέα επιλογή σας επιτρέπει να καθορίσετε μια διαφορετική διεύθυνση ηλεκτρονικού ταχυδρομείου για κάθε προγραμματισμένη σάρωση.
- Βελτιστοποίηση HTTP Fuzzer
- Μια νέα επιλογή για να καθορίσετε αν θα πρέπει να χρησιμοποιείτε το τελευταίο cookie από την ιστοσελίδα που ελέγξατε ή κάποιο άλλο που ανακαλύφθηκε κατά τη διάρκεια του ελέγχου.

- Νέα επιλογή που δεν επιτρέπει την αντικατάσταση των προεπιλεγμένων cookies με νεότερα που βρέθηκαν μετά την σάρωση της σελίδας.

**Νέοι έλεγχοι ασφάλειας:**

- Προστέθηκε ένας έλεγχος .**Net Cross Site Scripting** (**Request Validation Bypassing**).
- Νέος έλεγχος ασφάλειας για τα ζητήματα ασφάλειας του **MediaWiki**.

Υπέρ:

Πολύ κερδισμένος χρόνος λόγω των αυτοματοποιημένων ελέγχων

Κατά:

Είναι αξιόπιστο αλλά δεν θα γίνει ποτέ απόλυτο στις προβλέψεις του. Οι μελέτες δείχνουν ότι ένας web vulnerability scanner όσο καλός και να είναι δεν μπορεί να εντοπίσει περίπου το 45% των συνολικών κενών ασφαλείας.

Η εμπορική του έκδοση κοστίζει πάνω από 3000 ευρώ. [62]

### 9.1.3 Skipfish

Επίσημη Ιστοσελίδα: https://code.google.com/p/skipfish/

Άδεια χρήσης: Δωρεάν

Επιπλέον πληροφορίες: χρησιμοποιείται και σαν εργαλείο αναγνώρισης ενός συστήματος στην πρώτη φάση ενός ελέγχου τρωτότητας


Οι σαρωτές ευπαθειών έχουν αλλάξει τον κόσμο των ελέγχων διείσδυσης. Με τα κατάλληλα εργαλεία και τεχνικές μπορεί να γίνει έλεγχος οποιουδήποτε δικτύου και διαδικτυακής εφαρμογής. Το skipfist είναι ένα ακόμα εργαλείο αναζήτησης κενών ασφάλειας σε μία ιστοσελίδα. Μπορεί να χρησιμοποιηθεί και ως εργαλείο αναγνώρισης και συγκέντρωσης πληροφοριών.

Δημιουργός του είναι ο Michal Zalewski (icamtuf)

Είναι multi-platform, λειτουργεί σε Linux, BSD, MAC και windows. Είναι ένας πολύ δυναμικός σαρωτής που ψάχνει όλες τις σελίδες μίας σελίδας-στόχου. Συμπεριλαμβάνεται στο Backtrack 5.


Εικόνα 9.1.3 Γραφικό περιβάλλον Skipfish

Το skipfish ταξινομεί τα ευρήματα του ως υψηλού, μέτριου ή χαμηλού κινδύνου. Μερικά από τις υψηλού κινδύνου είναι:

- Server side SQL injection
- Ακριβής σύνταξη στους GET και τους POST παραμέτρους
- Server side shell command injection
- Ευπάθειες στην διαμόρφωση αλφαριθμητικών
- Ευπάθειες υπερχείλισης ακεραίων αριθμών

Χαρακτηριστικά:

- Μεγάλη ταχύτητα. Είναι γραμμένο σε C, βελτιστοποιημένο για τον χειρισμό HTTP αιτήσεων, αφήνει ελάχιστο ίχνος στη CPU και εύκολα πετυχαίνει τις 2000 αιτήσεις(requests) το δευτερόλεπτο.
- Ευκολία χρήσης με ικανότητες αυτόματης μάθησης τεχνολογιών σε ιστοσελίδες, δημιουργίας wordlist on-the-fly και αυτόματης συμπλήρωσης φορμών.
- Λογικές ασφάλειας τελευταίας τεχνολογίας. Υψηλή ποιότητα, χαμηλά ποσοστά false positive, διαφορετικοί μέθοδοι ελέγχων, ικανό να ξεχωρίσει «ρωγμές» συμπεριλαμβάνοντας και blind injection vectors.

Σημ. το nikto και το nessus ίσως έχουν καλύτερη απόδοση και ανάλυση αποτελεσμάτων αλλά αυτό το εργαλείο μπορεί να χρησιμοποιηθεί στο αρχικό στάδιο του ελέγχου.

### 9.1.4 Nikto Vulnerability Scanner

Επίσημη ιστοσελίδα: Nikto Vulnerability Scanner

Άδεια χρήσης: Ανοιχτού κώδικα

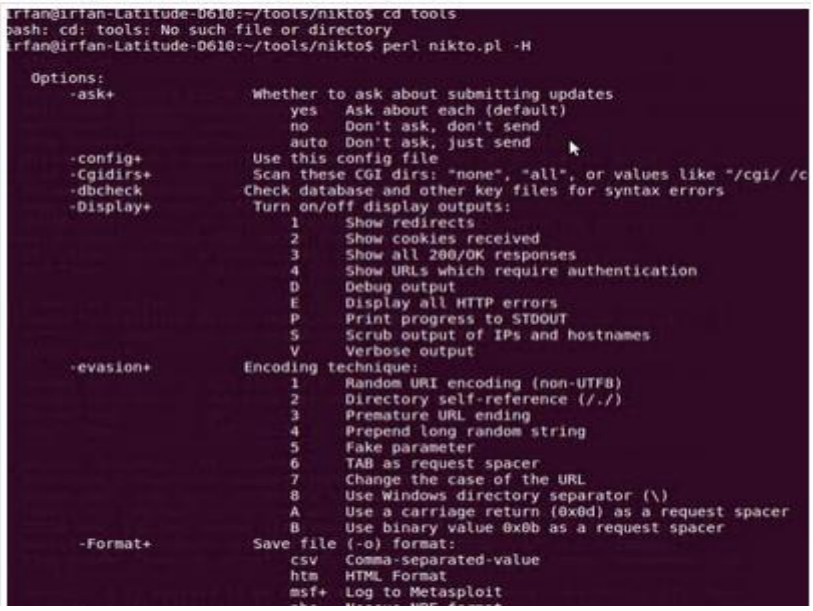
Επιπλέον πληροφορίες: Πραγματοποιεί έλεγχων ευπαθειών σε web server, λειτουργεί σε οποιαδήποτε Λειτουργικό Σύστημα που έχει εγκατεστημένο Perl.

Στον τομέα της ασφάλειας διαδικτυακών εφαρμογών υπάρχουν πολλές επιλογές για να διαλέξει κάποιος υπεύθυνος. Το Nikto είναι ένα εργαλείο που χρησιμοποιείται από μια μεγάλη μερίδα ανθρώπων για την εύρεση ευπαθειών στο διαδίκτυο. Είναι ανοιχτού κώδικα και μερικά από τα χαρακτηριστικά του είναι:

- μπορεί να ελέγξει ένα web server για περισσότερα από 6400 πιθανά επικίνδυνα αρχεία/CGIs.
- Ελέγχει για απαρχαιωμένες εκδόσεις σε περισσότερους από 1000 servers και προβλήματα που σχετίζονται με την έκδοση σε πάνω από 270 servers.
- Ελέγχει τα plugins και λάθος διαμορφωμένα αρχεία
- Είναι γρήγορο
- Είναι αποτελεσματικό
- Ανακαλύπτει τα default αρχεία και προγράμματα
- Ανακαλύπτει μη ασφαλή αρχεία και προγράμματα

Επιπλέον χαρακτηριστικά:

- Ολοκληρωμένη HTTP Proxy υποστήριξη
- Καταμέτρηση(enumeration) ονομάτων χρήστη σε Apache
- Σύνδεση(logging) με το Metasploit
- Υποστήριξη SSL(Secure Socket Layer)
- Subdomain brute forcing(μαντεύει)
- Εύκολες αναβαθμίσεις
- Αποθήκευση των αναφορών σε διάφορες μορφές




Εικόνα 9.1.4: αναβάθμιση του Nikto

Απαιτεί:

- Ένα λειτουργικό σύστημα που έχει εγκατεστημένη τη Perl.
- OpenSSL
- Active State Perl

### 9.1.5 Netsparker

Επίσημη ιστοσελίδα: http://www.mavitunasecurity.com/netsparker/

Άδεια χρήσης: Εμπορική(δοκιμαστική έκδοση 15 ημερών)

Επιπλέον πληροφορίες: Δεν έχει false positive αποτελέσματα

Η λειτουργία του δεν διαφέρει πολύ από αυτή των υπολοίπων ανιχνευτών. Ψάχνει για κάθε link μιας ιστοσελίδας και μετά το ελέγχει για κενά ασφάλειας ανεξάρτητα από το είδος και τη δομή αυτής. Μπορεί να βρει διαφορετικές ευπάθειες όπως SQL-injection, Cross Site Scripting, local file inclusion, εκτέλεση απομακρυσμένου κώδικα και πολλά άλλα.

Ο δημιουργός του προγράμματος υποστηρίζει ότι είναι false positive free που σημαίνει ότι μπορεί να αξιολογεί τις ευπάθειες και να εμφανίζει μόνο αυτές που πραγματικά είναι.


Εικόνα 9.1.5 Netsparker Community Edition

Η community edition παρέχεται δωρεάν και λειτουργεί σε περιβάλλον windows. Το γραφικό του περιβάλλον είναι απλό στη χρήστη και προσφέρεται για αρχάριους χρήστες. Ουσιαστικά αποτελεί ένα SQL-injection Scanner με δυνατότητες εύρεσης XSS αδυναμιών που μπορεί να εκμεταλλευτεί(exploit) τις SQL αδυναμίες που θα βρει. Σύμφωνα με έρευνες ανεξάρτητων οργανισμών το netsparker είχε τις καλύτερες επιδόσεις στην εύρεση SQL-injection αδυναμιών σε ποσοστό 98.53% σε όλα τα SQL-injection test.

Χαρακτηριστικά community edition

- False positive free
- Υποστήριξη Ajax/Javascript
- Hassle Free Licensing
- Δωρεάν αυτοματοποιημένες αναβαθμίσεις
- Error bases sql injection
- Boolean based sql injection
- Refletinve Cross-site Scripting(XSS)
- Permanent/stored XSS

Έλεγχοι ασφαλείας community edition

- Error based sql injection
- Boolean based sql injection
- XSS
- Open Redirect
- Crossdomain.xml ανάλυση

- Εύρεση και ανάλυση πιθανών ζητημάτων στο robots.txt
- Εύρεση και ανάλυση αρχεία google sitemap
- Εντοπισμός TRACE/TRACK μεθόδων
- Εντοπισμός ASP.NET debugging
- Εντοπισμός ιχνών ASP.NET
- Email disclosure
- Internal IP disclosure

### 9.1.6 HconSTF v0.5

Επίσημη ιστοσελίδα: http://www.hcon.in/hconstf-fire-features.html

Άδεια χρήσης: Δωρεάν

Επιπλέον πληροφορίες: Είναι διαθέσιμο σε windows και Linux. Περιέχεται σε όλες τις κύριες σουίτες ελέγχων τρωτότητας.

Είναι ένα εργαλείο ανοιχτού κώδικά για ελέγχους τρωτότητας, που βασίζεται σε διαφορετικές τεχνολογίες προγραμμάτων περιήγησης, γεγονός που βοηθά κάθε τεχνικό ασφάλειας στις δοκιμές διείσδυσης ή στις αξιολογήσεις ευπαθειών, έπειτα από σάρωση.


Το κωδικό όνομα της έκδοσης είναι «Prime». Αξιοσημείωτα χαρακτηριστικά είναι :

Είναι πιο ενισχυμένο για:

- ελέγχους τρωτότητας στο διαδίκτυο(Web penetration testing).
- Ανάπτυξη exploits για το διαδίκτυο
- Ανάλυση διαδικτυακού malware
- Osint, ηλεκτρονική κατασκοπεία και doxing
- Διάφορα άλλα κρυφά χαρακτηριστικά

Εν συντομία το HconSTF v0.5:

- Βασίζεται σε Firefox 17.0.1
- Είναι σχεδιασμένο με χρήση διαδικασιών

- Μικρότερο σε μέγεθος(40MB packed και 80MB extracted) και χρησιμοποιεί λιγότερη μνήμη
- Περισσότερα από 165 + plugins αναζήτησης
- Νέα IDB 0.1
- Καταχώρηση σύνδεσης για κάθε νέα αίτηση
- Περισσότεροι σαρωτές για DomXSS, Reflected XSS
- Νέες δυνατότητες υποβολής εκθέσεων, όπως καταγραφή σημειώσεων και καταγραφή url για εύκολη αναφορά.
- Έξυπνο SearchBox – απλά επιλέξτε τον και θα αλλάξει τη προεπιλεγμένη μηχανή αναζήτησης.
- Ολοκληρωμένη υποστήριξη Tor, AdvoR, I2p και περισσότερα proxies(διακομιστές μεσολάβησης) για απόκρυψη ηλεκτρονικού ίχνους/ταυτότητας
- Νέα Grease monkey scripts (18 scripts)

[21],[53]

### 9.1.7 Burp Suite

Επίσημη ιστοσελίδα: http://portswigger.net/burp/

Άδεια χρήσης: Εμπορική και δωρεάν έκδοση με περιορισμένες δυνατότητες

Περισσότερες πληροφορίες: Η δωρεάν έκδοση προσφέρει μια αξιόπιστη λύση για ελέγχους τρωτότητας στο διαδίκτυο.

Το Burp Suite είναι μία ολοκληρωμένη πλατφόρμα για την εκτέλεση δοκιμών ασφάλειας σε εφαρμογές διαδικτύου. Τα διάφορα εργαλεία του συνεργάζονται αρμονικά για την υποστήριξη της διαδικασίας ελέγχου στο σύνολο της, από την αρχική χαρτογράφηση και ανάλυση της επιφάνειας μιας υπό εξέτασης εφαρμογής ως την εξεύρεση και την εκμετάλλευση των τρωτών σημείων ασφάλειας.

Το Burp δίνει πλήρη έλεγχο επιτρέποντας των συνδυασμό προηγμένων χειροκίνητων τεχνικών με state-of-the-art αυτοματοποιημένες για την γρηγορότερη ολοκλήρωση ενός ελέγχου πιο αποτελεσματικού και πιο διασκεδαστικού.

Περιλαμβάνει τις ακόλουθες συνιστώσες :

- Ένα intercepting Proxy ο οποίος επιτρέπει την επιθεώρηση και την τροποποίηση της κυκλοφορίας μεταξύ του περιηγητή(browser) και της εφαρμογής στόχο.

- Ένα application aware spider για την αυτοματοποιημένη ανίχνευση περιεχομένου και λειτουργικότητας.
- Ένα προχωρημένο ανιχνευτή(Scanner) διαδικτυακών εφαρμογών για την αυτόματη αναγνώριση κάθε πιθανής ευπάθειας.
- Ένα εργαλείο εισβολής(intruder tool) για την εκτέλεση πλήρως παραμετροποιημένων επιθέσεων για την εύρεση και εκμετάλλευση μη συνηθισμένων ευπαθειών.
- Ένα εργαλείο repeater για τη διαχείριση και την αποστολή επιπλέων ατομικών αιτημάτων(requests)
- Ένα εργαλείο Sequencer, για τον έλεγχο της τυχαιότητας των session tokens.
- Δίνεται η δυνατότητα να σώσει κάποιος την εργασία του και να συνεχίσει αργότερα.
- Επεκτασιμότητα. Επιτρέπει την εύκολη ανάπτυξη plugins για την εκτέλεση περίπλοκων και προσαρμοσμένων εργασιών.

- Μπορεί να χρησιμοποιηθεί και από αρχάριους χρήστες.

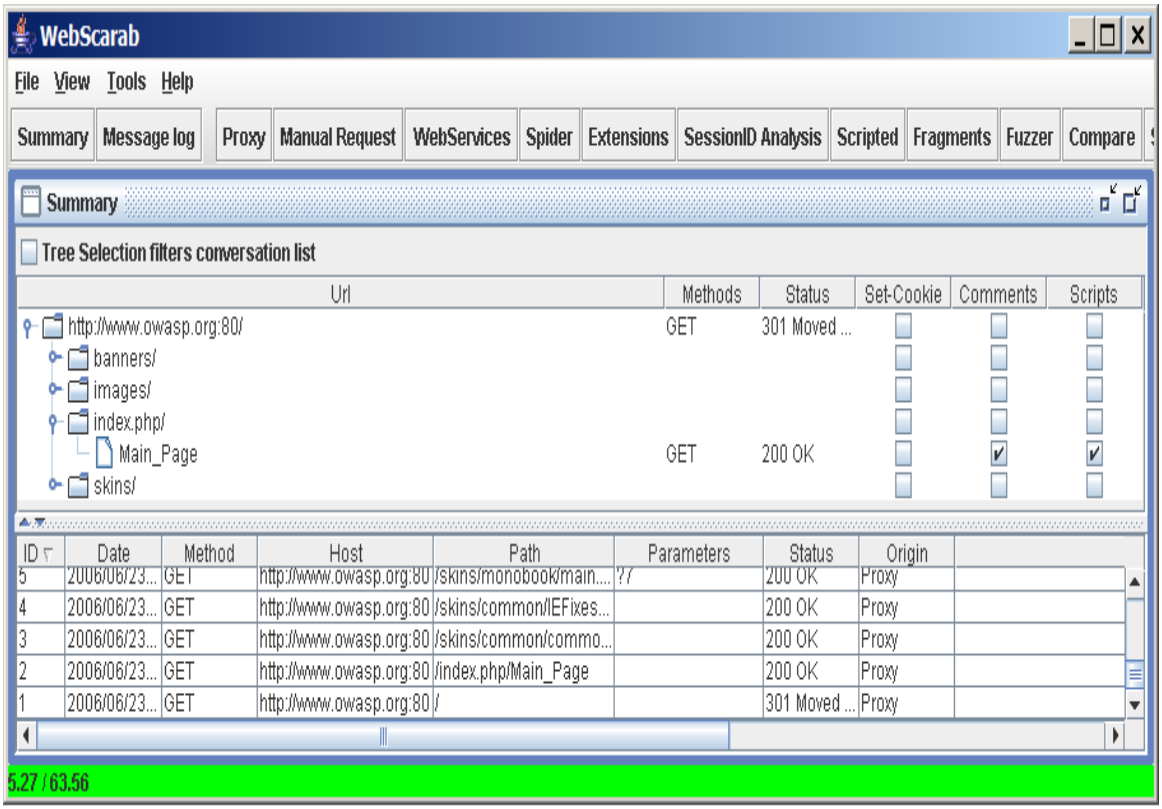
[86]

### 9.1.8 OWASP WebScarab Project

Επίσημη ιστοσελίδα:
https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

Άδεια χρήσης: Ανοιχτού κώδικα

Είναι ένα framework για την ανάλυση εφαρμογών που επικοινωνούν με HTTP και HTTPs πρωτόκολλα. Είναι γραμμένο σε java και χαρακτηρίζεται από φορητότητα σε διάφορες πλατφόρμες. Έχει διάφορες μεθόδους λειτουργίας και εφαρμόζονται πάνω του διάφορα plugins. Η κύρια λειτουργία του είναι να λειτουργεί σαν ένας proxy ανάμεσα σε ένα server και στο browser ώστε να υποκλέπτει requests και να δίνει την δυνατότητα στο διαχειριστή του να τις εξετάσει και να τις τροποποιήσει. Μπορεί να υποκλέψει τόσο HTTP όσο και HTTPs κυκλοφορία.




Εικόνα 9.1.8: Web Scarab μετά από browsing

Πρόκειται για ένα εργαλείο κυρίως σχεδιασμένο να χρησιμοποιείται από ανθρώπους που ξέρουν να γράφουν κώδικα ή έχουν ένα καλό επίπεδο κατανόησης του πρωτοκόλλου HTTP.

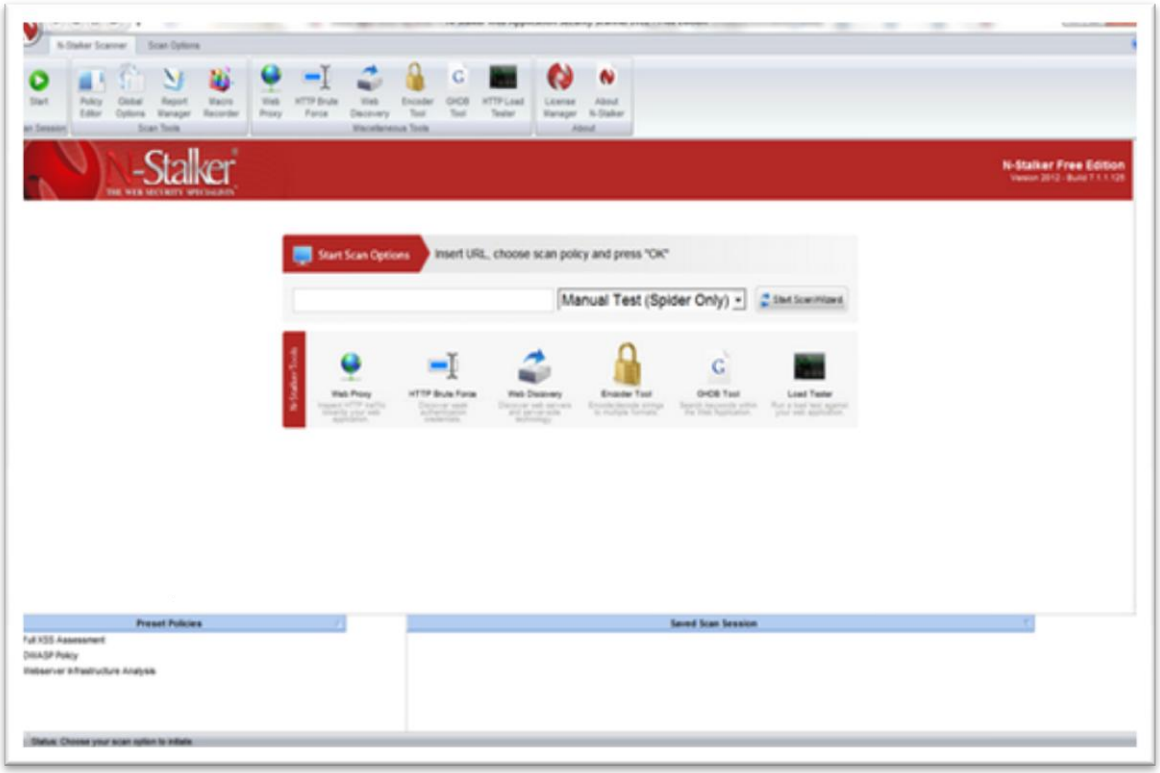
### 9.1.9 N-Stalker

Επίσημη ιστοσελίδα: http://www://nstalker.com

Άδεια χρήσης: Εμπορική και δωρεάν διανομή

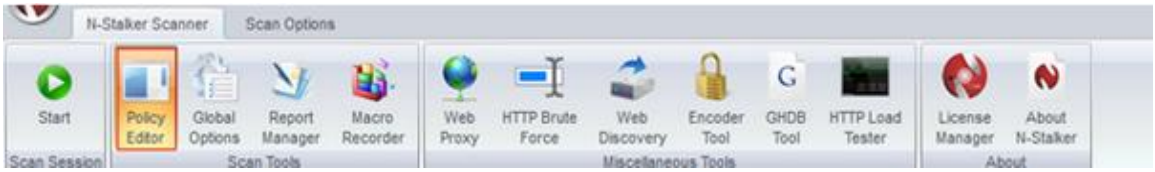
Επιπλέον πληροφορίες: Πάρα πολλά εργαλεία σε ένα.

**Χρήση και δυνατότητες:**




Εικόνα 9.1.9.1: Διεπαφή χρήστη του N-Stalker

Εκ πρώτης όψεως συμπεραίνει κάποιος ότι πρόκειται για ένα επαγγελματικό εργαλείο. Στην κύρια οθόνη όλα είναι άρτια ταξινομημένα και λογικά ομαδοποιημένα κάτι το οποίο διευκολύνει τους αρχάριους χρήστες. Προσφέρονται πάρα πολλές επιλογές ελέγχου μερικές εκ των οποίων είναι η διαδικασία αναζήτησης, ο κειμενογράφος(editor) πολιτικών ασφαλείας και ο διαχειριστής των αναφορών(report manager).

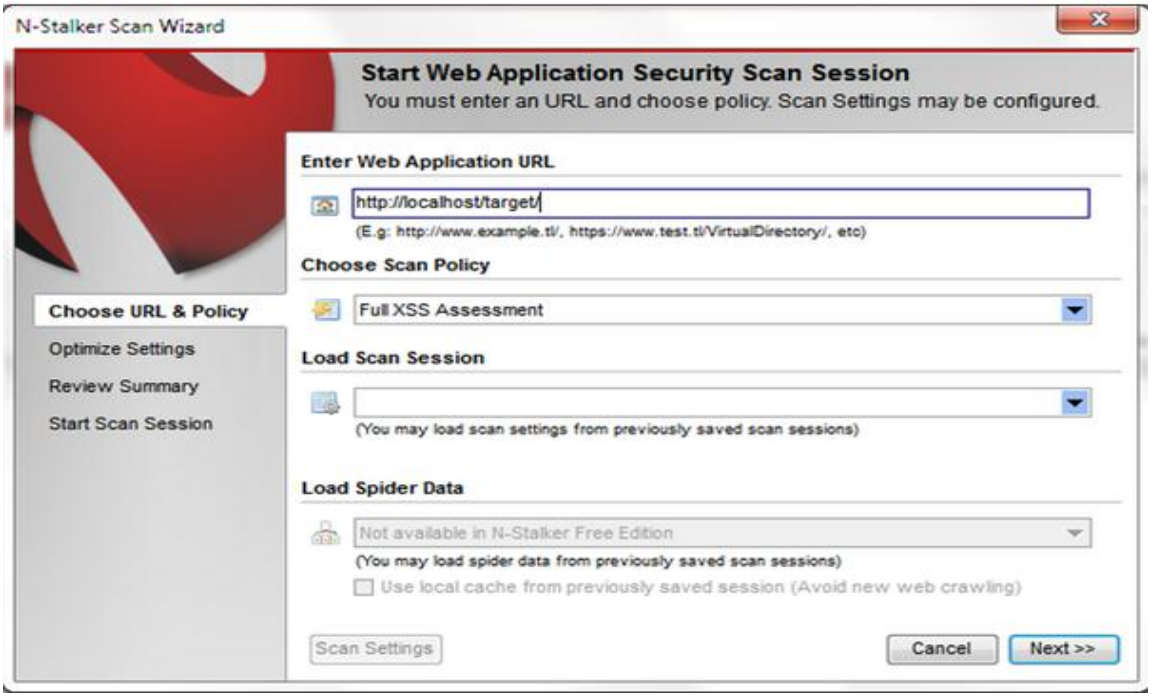



Εικόνα: Επιλογή του Policy Editor από το menu

Πριν την έναρξη ενός ελέγχου τρωτότητας είναι απαραίτητη η δημιουργία μίας πολιτικής με ξεκάθαρα ορισμένους κανόνες. Με την εκκίνηση του editor

εμφανίζεται ένα δέντρο με κανόνες στη αριστερή πλευρά και η περιγραφή τους στη δεξιά.

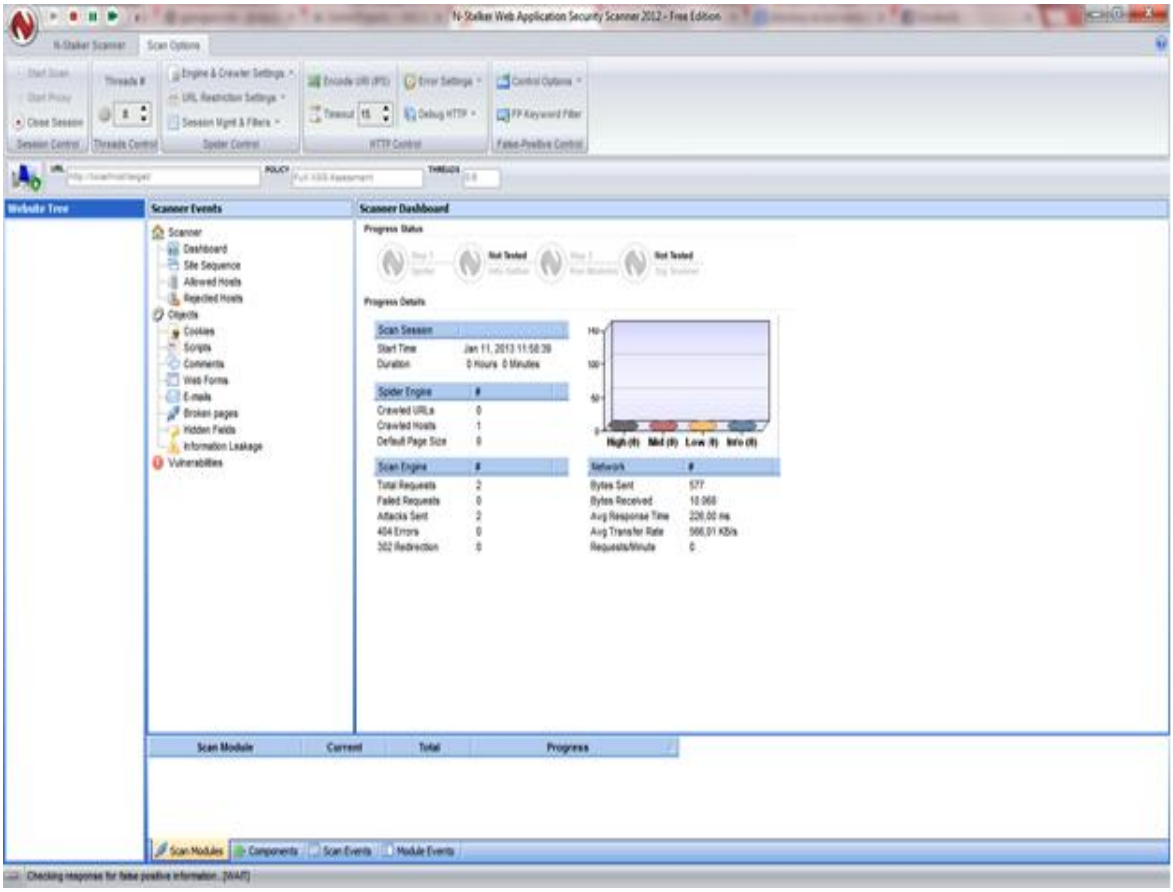
Συμπληρώνουμε όλα τα απαραίτητα πεδία όπως το όνομα της ευπάθειας, τη σοβαρότητά της, τον υπό εξέταση server, μία περιγραφή, τη λύση και αναφορές σε URL. Αφού καθορίσουμε όλους τους κανόνες της πολιτικής μας σώζουμε τις επιλογές και της δίνουμε ένα όνομα.




Εικόνα 9.1.9.2: Δημιουργία και αποθήκευση επιλογών

Για την αναζήτηση ευπαθειών εισάγουμε την επιθυμητή URL, επιλέγουμε την πολιτική που θέλουμε και η οποία θα καθορίσει τι είδους έλεγχο θα εκτελέσουμε. Υπάρχει αυτοματοποιημένος ανιχνευτής συνδέσμων και σελίδων(web spider). Επίσης επιλογές για τη βελτιστοποίηση μιας αναζήτησης όπως η εξαίρεση κάποιων συνδέσμων ή συγκεκριμένων σελίδων.

Το γραφικό περιβάλλον κατά τη διάρκεια της αναζήτησης είναι κάτι το ξεχωριστό. Κάθε ενέργεια που συμβαίνει ομαδοποιείται, δημιουργείται ένα δέντρο με τα περιεχόμενα του site και ένα περιβάλλον για την απόδοση των αποτελεσμάτων της αναζήτησης.




Εικόνα 9.1.9.3: κατά την εκτέλεση της αναζήτησης.

Τέλος δίνεται η δυνατότητα να αποθηκεύσουμε την αναφορά σαν .pdf έγγραφο. Χαρακτηρίζεται και αυτή από πολύ καλή οργάνωση, με πολλές λεπτομέρειες και ομαδοποιημένα αποτελέσματα.

<u>Υπέρ</u>

- Πάρα πολλά εργαλεία.
- Πολύ καλή διαχείριση των πολιτικών ασφάλειας
- Λεπτομερή και επαγγελματική αναφορά αποτελεσμάτων.
- Κοινότητα που το υποστηρίζει

<u>Κατά</u>

- Υπάρχει ένα ενοχλητικό διαφημιστικό παράθυρο που εμφανίζεται συνέχεια.
- Η δωρεάν έκδοση δεν είναι χρηστική
- Η εμπορική έκδοση είναι πολύ ακριβή για απεριόριστο αριθμό ελέγχων(5.000$).

Χαρακτηριστικά:

- Υπάρχει ιστορικό των καταγραφθέντων requests.
- Εξάγει scripts ή html σχόλια από HTML σελίδες
- Μη αυτόματη καταγραφή κυκλοφορίας
- Οτιδήποτε μπορεί να εκφραστεί σε java μπορεί να εκτελεστεί.
- Ανακαλύπτει κρυφα πεδία.
- Bandwidth simulator
- Spider
- SessionId ανάλυση
- Parameter fuzzer
- Σύγκριση
- SOAP
- Αυτόματος έλεγχος για αρχεία που παρέμεινα εσφαλμένα σε ένα server(π.χ .bak, ~ κτλ.)
- XSS/CRLF.

### 9.1.10 Powerfuzzer

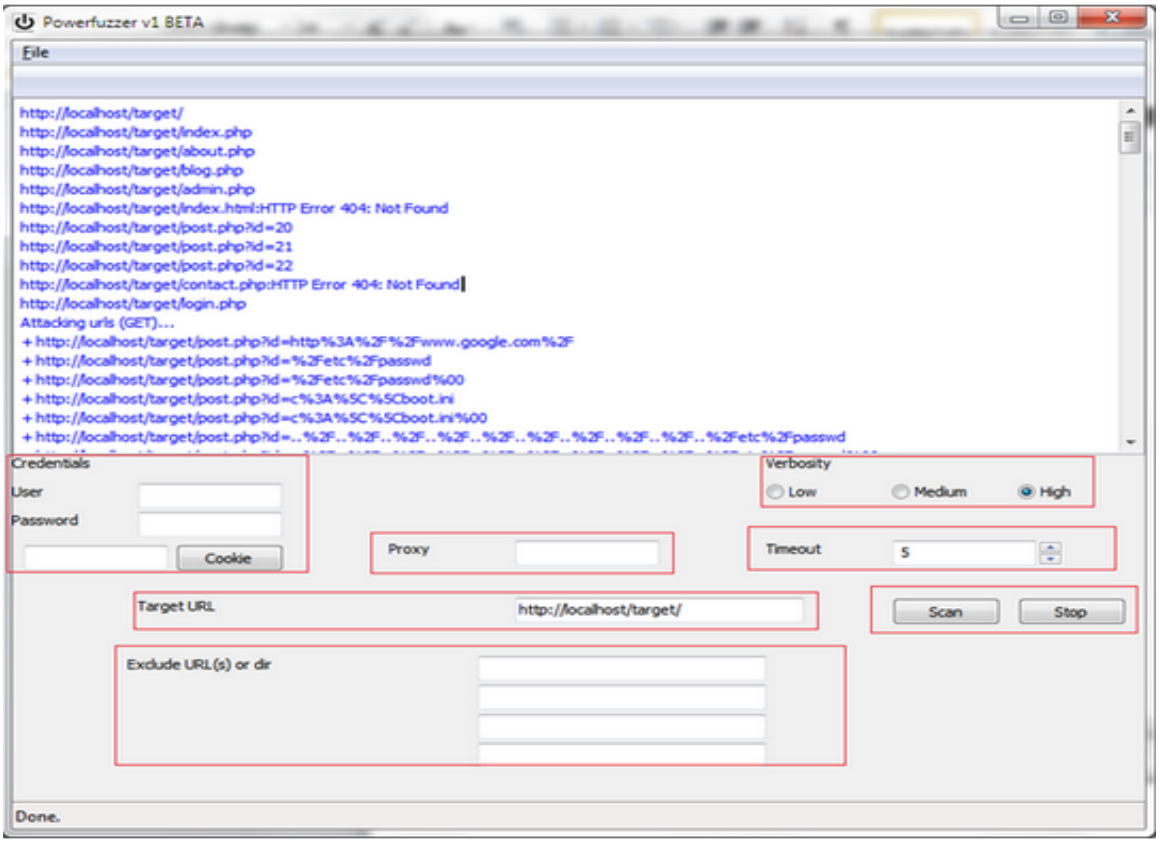
Επίσημη ιστοσελίδα: http://www/powerfuzzer.com

Άδεια χρήσης: Ανοιχτού κώδικα(GNU General Public License)

Επιπλέον πληροφορίες: Δεν έχουν γίνει αλλαγές στο πρόγραμμα από το 2009

**Χρήση και δυνατότητες**

Είναι ένα πολύ εύχρηστο εργαλείο κατάλληλο για αρχάριους χρήστες.




Εικόνα 9.1.10. Powerfuzzer - οθόνη αναζήτησης

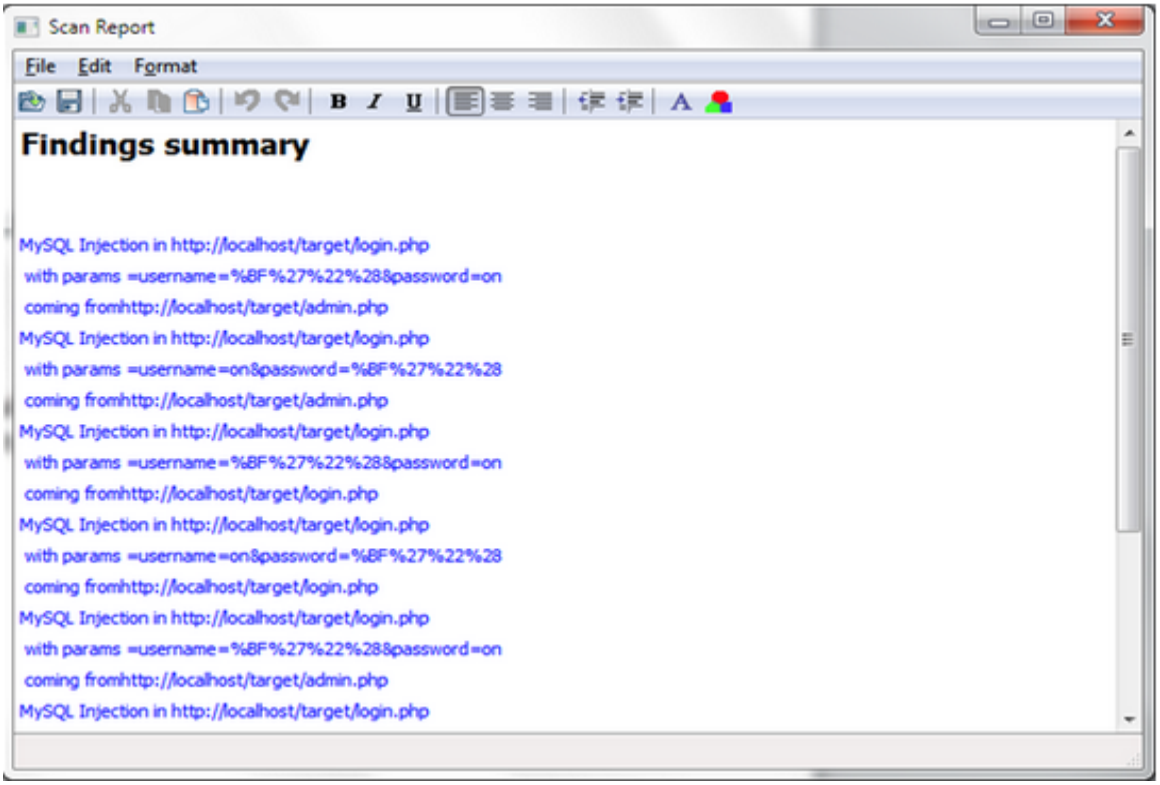
Στο πεδίο target URL βάζουμε την ιστοσελίδα που θέλουμε αν εξετάσουμε και στο πεδίο exclude URL/s or dir τους φακέλους ή τα link που θέλουμε να εξαιρέσουμε από τον έλεγχο(π.χ. scripts για διαγραμμένους χρήστες).

Το πεδίο credentials(διαπιστευτήρια) το συμπληρώνουμε αν υπάρχει κάποιο μέρος της εφαρμογής μας που χρειάζεται όνομα χρήστη(username) ή συνθηματικό (password) ή session. Χρησιμοποιείται ένας proxy για να κάνει τον έλεγχο ανώνυμο. Η επιλογή timeout όπου θέτουμε τον χρόνο μεταξύ των αιτήσεων(requests). Με τον όρο verbosity επιλέγουμε τη «δύναμη» του ελέγχου μας δηλαδή των αριθμό των requests ή των ελέγχων.

Σύμφωνα με την επίσημη βιβλιογραφία το εργαλείο αυτό ανιχνεύει τους παρακάτω τύπους ευπαθειών.

- Injections(SQL, LDAP, κώδικα, εντολών και XPATH)
- CRLF
- HTTP 500 statuses(συχνά δείχνει πιθανές περιπτώσεις αρρυθμιών που μπορούν να οδηγήσουν σε κενά ασφαλείας και σε υπερχείλιση )

Η αναφορά ελέγχου(τα αποτελέσματα) εμφανίζονται σε μια απλή μορφή όπως φαίνεται και στην παρακάτω εικόνα. Αν μία ευπάθεια ανιχνευθεί περιγράφεται με την ακόλουθη μορφή: <Type of vulnerability> in <Link> with parameters <Cause for the vulnerability> coming from <Redirected from link>.




Εικόνα 9.1.10.1 Powerfuzzer - οθόνη αποτελεσμάτων

Υπέρ

- Πολύ απλό στη χρήση του
- Ικανοποιητικό για γρήγορους ελέγχους
- Η χρήση του δεν προϋποθέτει κάποια εμπειρία

Κατά

- Κακή σχεδίαση τους γραφικού περιβάλλοντος. Οι διάφορες επιλογές εμφανίζονται χωρίς λογική σειρά.
- Η αναφορά δεν είναι λεπτομερής και δεν ομαδοποιούνται τα αποτελέσματα
- Το εργαλείο δεν έχει ανανεωθεί από το 2009

### 9.1.11 w3af

w3af
Web Application Attack and Audit Framework

Επίσημη ιστοσελίδα: http://w3af.sourceforger.net

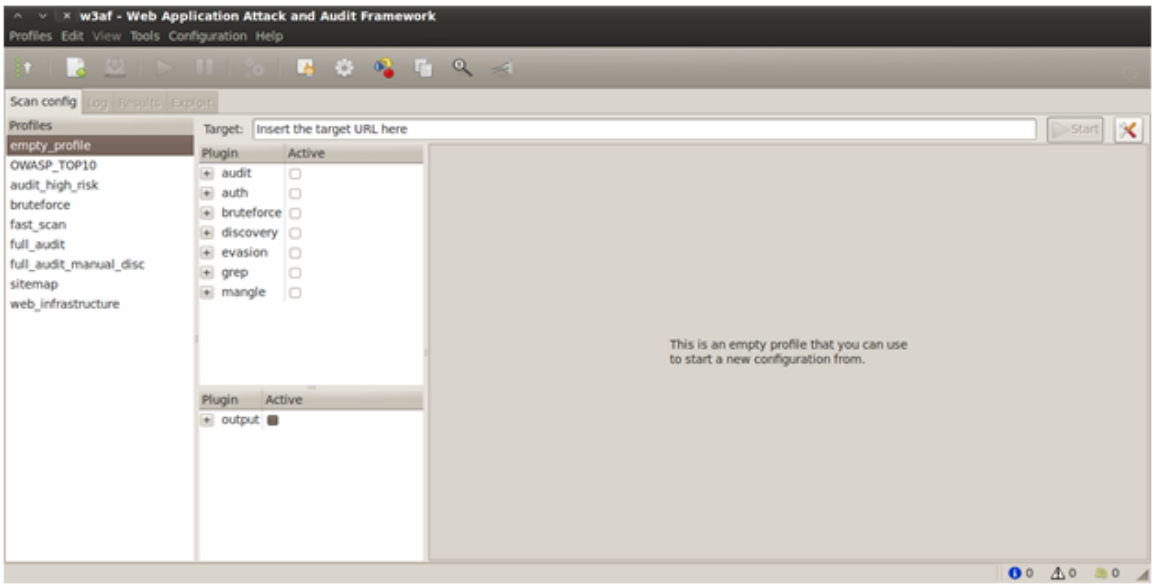
Άδεια χρήσης: Ανοιχτού κώδικα(GNU General Public License)

Επιπλέον πληροφορίες: Στην επίσημη ιστοσελίδα κάθε plugin περιγράφεται λεπτομερώς.

Έκδοση: v1.2. revision:6647

**Χρήση και δυνατότητες:**

Την πρώτη φορά που ανοίγει κάποιος το γραφικό περιβάλλον του w3af ίσως του φανεί λίγο μπερδεμένο και αυτό γιατί υπάρχουν πολλά εικονίδια χωρίς κείμενο που να περιγράφει τη λειτουργία τους εκτός και αν περάσει κάποιος το ποντίκι του από πάνω.

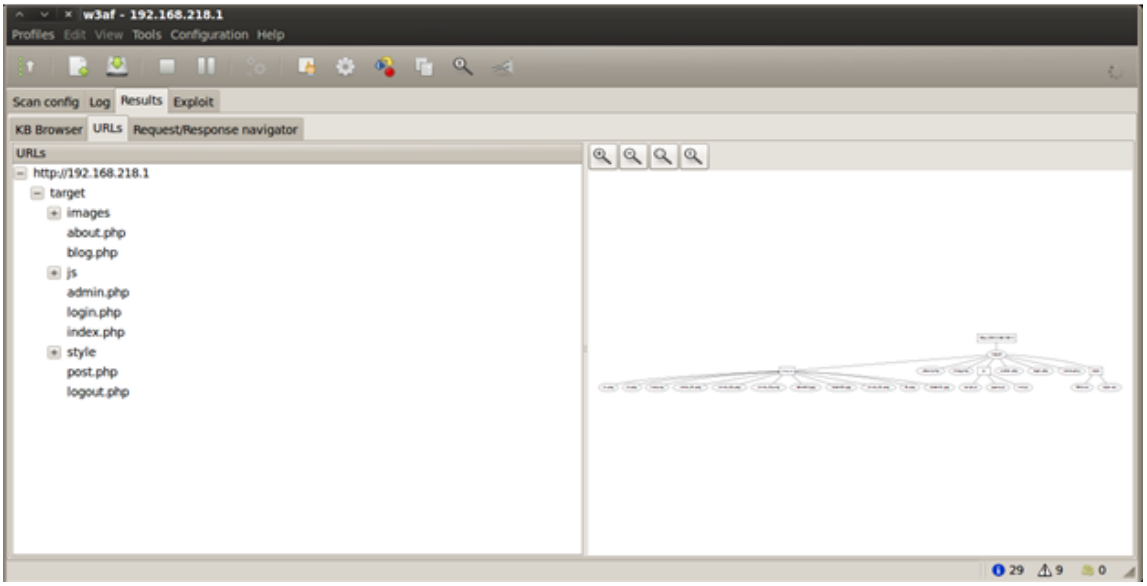



Εικόνα 9.1.11.1: Γραφικό περιβάλλον του w3af

Υπάρχει δυνατότητα δημιουργίας προφίλ που είναι παρόμοιο με τη δημιουργία πολιτικών ασφαλείας. Με τη δημιουργία προφίλ επιλέγονται και τα κατάλληλα εργαλεία για την επικείμενη αναζήτηση.

Καθορίζουμε τον υπό εξέταση στόχο εισάγοντας τη URL του. Μπορούνε να εξερευνήσουμε αυτόματα τη δομή μίας ιστοσελίδας να ανακαλύψουμε συσκευές που ενδεχομένως βρίσκονται μεταξύ του w3af και της web εφαρμογής(firewalls, ips, waf, proxies κτλ.). Μετά τον καθορισμό της δομής του στόχου επιλέγουμε plugins τα οποία θα ενσωματωθούν στη διαδικασία της αναζήτησης και θα μας βοηθήσουν στην ανάλυση ενός web server(το λειτουργικό του σύστημα, την έκδοση, τη γλώσσα προγραμματισμού που χρησιμοποιεί, virtual hosts κτλ.)

Με την αναζήτηση εμφανίζονται αναφορά με πληροφορίες σχετικά με την αναζήτηση.




Εικόνα 9.1.11.2: εμφάνιση των σαρωμένων urls

Το τελικό στάδιο είναι η εκμετάλλευση(exploitation) των αδυναμιών που έχουν βρεθεί.

Υπέρ:

Ξεκάθαρος και ακριβής οδηγός χρήσης

Μεγάλος αριθμός plugins

Η λειτουργία του κάθε plugin περιγράφεται λεπτομερώς στην επίσημη ιστοσελίδα

Ο τρόπος εμφάνισης των urls που έχουν σαρωθεί.

Κατά:

Απαιτεί κάποιο χρόνο από ένα χρήστη για να εξοικειωθεί με το εργαλείο

Υπάρχει μία οθόνη ανακάλυψης Bug(Bug detected screen) που είναι ενοχλητική.

[11], [19],[29],[39],[40],[41],[43],[55],[65],[77],[79]

### 9.1.13 Σύγκριση Εργαλείων

Ως κριτήρια σύγκρισης θα χρησιμοποιηθούν οι τρεις(3) κλάσεις κριτηρίων από το συγκριτικό πλαίσιο αξιολόγησης που περιγράφηκε στο κεφάλαιο 7.

**Αντιμετωπιζόμενες απειλές ασφάλειας**

Οδηγός για τις διαθέσιμες απειλές που επιλέχθηκαν αποτελεί η έκθεση του μη κερδοσκοπικού οργανισμού OWASP για τις πιο διαδεδομένες απειλές στο έτος 2012.

Σύμφωνα με την ετήσια αναφορά του OWASP (Open Web Application Security Project ) οι δέκα(10) πιο διαδεδομένες απειλές για το 2012 είναι οι παρακάτω. [3]

A1. Injection
A2. Cross Site Scripting/XSS
A3. Broken Authentication / Session Management
A4. Insecure Direct Object References
A5. Cross Site Request Forgery
A6. Security Misconfiguration
A7. Insecure Cryptographic Storage
A8. Failure to Restrict URL Access
A9. Insufficient Transport Layer Protection
A10. Unvalidated Redirects and Forwards

Δημιουργήθηκε πίνακας που στον οριζόντιο άξονα του περιέχει τα διαθέσιμα εργαλεία και στον κάθετο τις παραπάνω απειλές ασφάλειας.

Οι διαθέσιμες απαντήσεις είναι ΝΑΙ(+), ΟΧΙ(-) ή ΜΗ ΔΙΑΘΕΣΙΜΟ(x).

(+) → το πρόγραμμα μπορεί να αντιμετωπίσει την συγκεκριμένη απειλή

(-) → το πρόγραμμα δεν μπορεί να αντιμετωπίσει μια συγκεκριμένη απειλή

| **Απειλές:** <br><br> **Προγράμματα** | **A1** | **A2** | **A3** | **A4** | **A5** | **A6** | **A7** | **A8** | **A9** | **A10** |
|---|---|---|---|---|---|---|---|---|---|---|
| ZAP | + | + | - | - | + | - | - | + | - | - |
| Acunetix | + | + | + | + | + | + | + | + | + | + |
| Skipfish | + | + | - | - | - | + | + | - | - | - |
| Nikto | - | - | - | - | - | + | + | + | + | - |
| Netsparker | + | + | - | - | + | - | - | - | - | + |
| HconSTF v0.5 | + | + | + | + | - | + | - | - | - | - |
| Burp Suite | + | + | + | + | + | - | - | + | - | + |
| WebScarab | + | + | - | - | - | + | - | + | - | + |
| N-Stalker | + | + | - | - | + | - | + | - | - | + |
| Powerfuzzer | - | + | - | - | + | - | - | - | - | - |
| w3af | + | + | + | - | + | - | + | - | - | + |

**Εφαρμοσμένα τεχνολογικά ζητήματα**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- B1. Απόδοση
- B2. Πολυπλοκότητα εγκατάστασης
- B3. Τελική αναφορά αποτελεσμάτων
- B4. Φορητότητα
- B5. Χρονική επιβάρυνση

| **Κριτήρια:** **Προγράμματα** | **B1** | **B2** | **B3** | **B4** | **B5** |
|---|---|---|---|---|---|
| ZAP | M | Υ | M | Y | M |
| Acunetix Free | Y | M | Y | X | M |
| Skipfish | M | M | X | Y | X |
| Nikto | Y | M | M | M | M |
| Netsparker | M | Y | M | X | M |
| HconSTF v0.5 | Υ | X | M | M | X |
| Burp Suite | Y | Y | X | X | Y |
| WebScarab | X | M | X | Y | M |
| N-Stalker | M | M | Υ | M | Υ |
| Powerfuzzer | M | Y | X | M | M |
| w3af | Y | M | M | M | M |

**Ικανοποίηση απαιτήσεων των χρηστών.**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

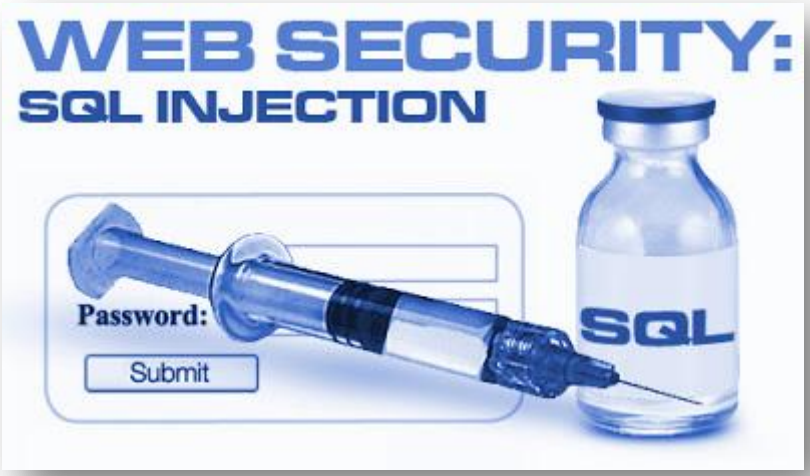
- C1. Ευκολία χρήσης.
- C2. Κοινότητα υποστήριξης
- C3. Κόστος
- C4. Πληρότητα

| **Κριτήρια:** **Προγράμματα** | **C1** | **C2** | **C3** | **C4** |
|---|---|---|---|---|
| Zap | M | X | Y | X |
| Acunetix | M | X | X | Y |
| Skipfish | M | X | Υ | M |
| Nikto | M | M | Y | X |
| Netsparker | X | X | X | X |

| | | | | |
|---|---|---|---|---|
| HconSTF v0.5 | M | X | Υ | M |
| Burp Suite | X | M | X | M |
| WebScarab | M | M | Y | M |
| N-Stalker | M | X | X | M |
| Powerfuzzer | Y | X | Y | X |
| w3af | X | M | Y | Y |

*Η διαθέσιμη επιλογή Υψηλή(Υ) σημαίνει σε κάθε περίπτωση την καλύτερη απόδοση. Στο κριτήριο κόστος για παράδειγμα σημαίνει ότι το προϊόν προσφέρεται δωρεάν είτε είναι ανοιχτού κώδικα. Το κριτήριο πληρότητα στη αξιολόγηση εργαλείων που εξετάζουν συγκεκριμένες ευπάθειες αφορά λειτουργίες μέσα στο εύρος δυνατοτήτων των προγραμμάτων αυτής της κατηγορίας. Στο κριτήριο πολυπλοκότητα εγκατάστασης Υψηλό σημαίνει εύκολη και γρήγορη εγκατάσταση.*

## 9.2 Εργαλεία εκμετάλλευσης SQL Injection




### 9.2.1 SQLMap

Επίσημη ιστοσελίδα: http://sqlmap.org/

Άδεια χρήσης: Open Source

Επιπλέον πληροφορίες: Είναι αρκετά διαδεδομένο εργαλείο. Υποστηρίζει έξι διαφορετικές τεχνικές SQL Injection. Μπορεί να λειτουργήσει και στα windows είτε με το SQL GUI είτε σαν plug in του Burp Suite.

Αν εντοπίσετε μία αδυναμία τύπου Time_Based SQL Injection μπορείτε είτε να προσπαθήσετε να την εκμεταλλευτείτε μόνο σας είτε να χρησιμοποιήσετε κάποιο αυτοματοποιημένο εργαλείο όπως το SQLMap.

Το SQLMap είναι ένα πρόγραμμα γραμμένο σε Python που το τρέχουμε μέσα από το Τερματικό(Terminal). Η χρήση του είναι πολύ απλή και είναι ένα από τα καλύτερα και τα πιο γνωστά στο χώρο. Στο Backtrack θα το βρείτε έτοιμο και εγκατεστημένο, και το μόνο που θα χρειαστεί να κάνετε πριν το τρέξετε είναι να το αναβαθμίσετε(αν δεν είναι ήδη).

*Αντί για περιγραφή παρατίθεται ένα παράδειγμα χρήσης.*

Το πρώτο πράγμα που θα κάνουμε θα είναι να βρούμε τις Βάσεις Δεδομένων της σελίδας.

Αφού είμαστε μέσα στον φάκελο sqlmap πατάμε **./sqlmap.py -u http://target/index.php?rm=1 --dbs**

Αυτόματα θα ξεκινήσει το sqlmap να προσπαθεί να βρει τις Βάσεις της σελίδας. Βάζουμε το τρωτό link και όχι απλά τη σελίδα. Για να δείξουμε πως θέλουμε τις βάσεις της σελίδας βάζουμε στο τέλος "--dbs"(που σημαίνει Databases).

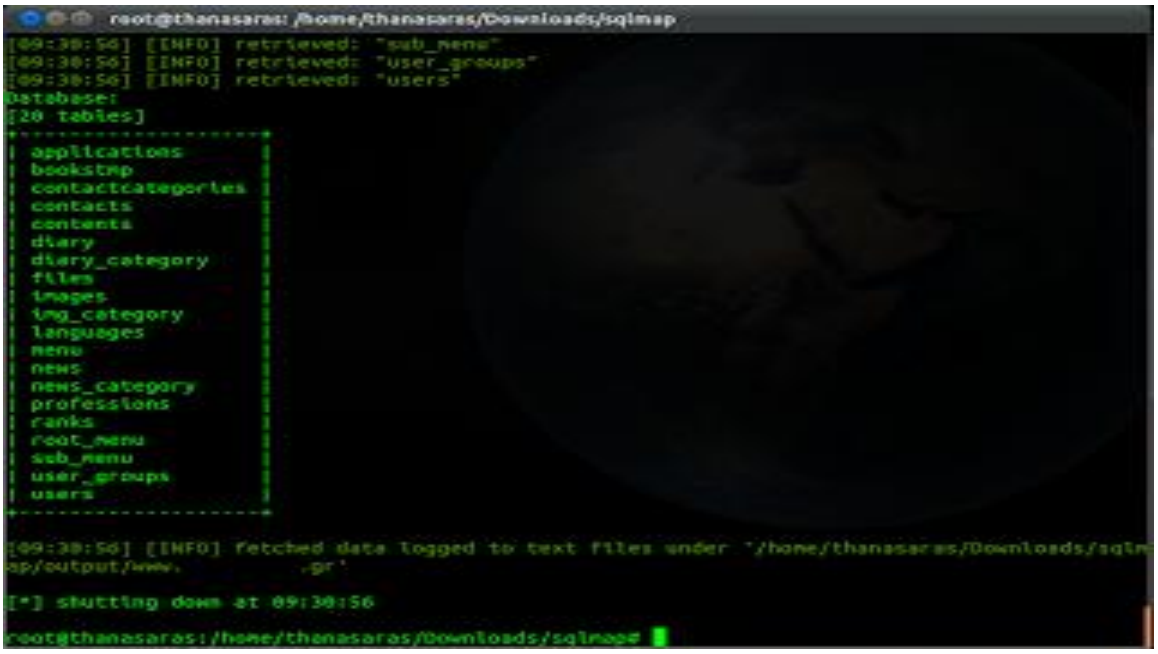
(Μπορούσατε αντί για ./sqlmap.py να γράψουμε και python sqlmap.py, είναι ακριβώς το ίδιο).

Και μετά από λίγο έχουμε πάρει τα αποτελέσματα!


Εικόνα 9.2.1. SQLMap Βάσεις Δεδομένων της υπό εξέταση ιστοσελίδας

**Βρήκε <u>93</u> Databases!** Ακολουθεί η εύρεση των πινάκων(tables) για μία συγκεκριμένη Βάση Δεδομένων.

**./sqlmap.py -u http://www.target/index.php?rm=1 -D nameofDatabase --tables**

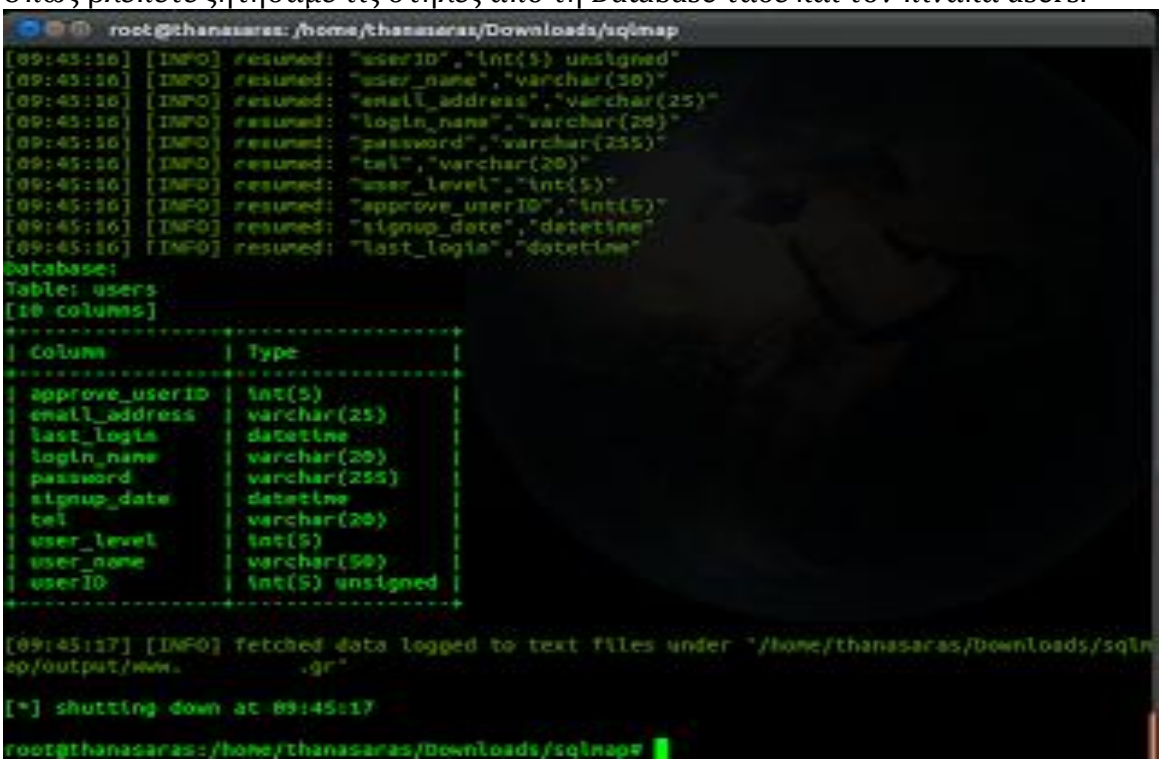



Εικόνα 9.2.1.1. SQLMap Εύρεση πινάκων

Βρήκαμε και τους πίνακες της Βάσης που θέλουμε. Συνεχίζουμε βρίσκοντας τι περιέχει μέσα στον πίνακα "**users**"!

**./sqlmap.py -u http://www.target/index.php?rm=1 -D nameofdatabase -T users --columns**

Όπως βλέπετε ζητήσαμε τις στήλες από τη Database ταδε και τον πίνακα users.

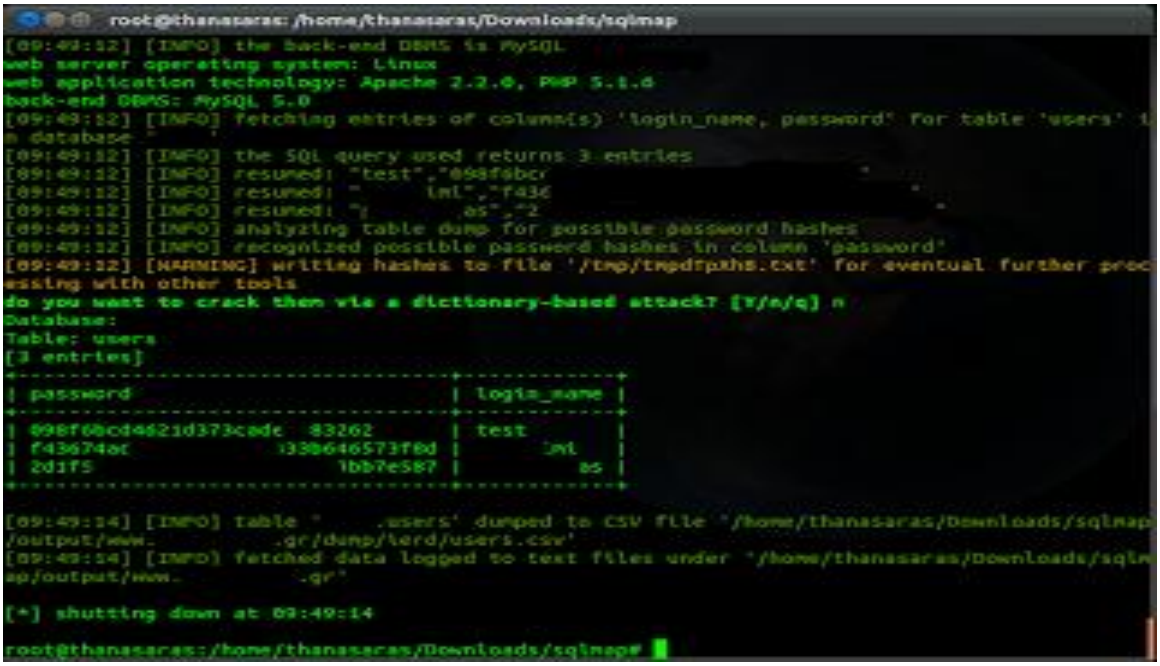



Εικόνα 9.2.1.2. Περιεχόμενα πίνακα users

Τώρα ξέρουμε τι ψάχνουμε(ονόματα columns) και από που(όνομα table) και απομένει να πάρουμε τα δεδομένα

**./sqlmap.py -u http://www.target/index.php?rm=1 -D nameofdatabase-T users -C login_name,password --dump**

**Απλά ζητήσαμε τα δεδομένα από τις στήλες login_name,password που βρίσκονται μέσα στον πίνακα users που βρίσκεται μέσα στην συγκεκριμένη Database.**




Εικόνα 9.2.1.2 SQL Injection

**Μέσα σε λίγα δευτερόλεπτα αποσπάσαμε τα στοιχεία που μας ενδιέφεραν από την Βάση Δεδομένων της τρωτής σελίδας. Η κωδικοποίηση τους σε md5 δεν αποτελεί πρόβλημα.**

Θα μπορούσαμε αν δεν βάζαμε τις παραμέτρους να βρίσκαμε ΟΛΑ τα δεδομένα, ΟΛΩΝ των στηλών ΟΛΩΝ των πινάκων ΟΛΩΝ των βάσεων. Αν δεν υπήρχε το εργαλείο αυτό η διαδικασία θα έπαιρνε ώρες.
Με το πρόγραμμα αυτό μπορείτε να κάνετε πολλά ακόμη πράγματα, όπως να ψάχνετε μέσω ενός Dork που θα εισάγετε σελίδες ενός οργανισμού και όταν βρει μια ευπάθεια σας ενημερώνει και εσείς επιλέγετε τι θέλετε να κάνετε με αυτήν!

Τα αποτελέσματα που έχετε βρει θα αποθηκεύονται στον φάκελο output.

Με σαρωτές όπως το acunetix wvs ή το w3af κτλ, είναι σχεδόν αδύνατο να βρούμε κενά ασφαλείας σε περιπτώσεις εξειδικευμένων αναζητήσεων όπως για παράδειγμα σε CMS's. Ο λόγος είναι πως αυτά τα προγράμματα δεν έχουν σχεδιαστεί για να ψάχνουν αποκλειστικά ευπάθειες στο χ ή ψ CMS, με αποτέλεσμα την αναζήτηση στοιχείων που ξέρουμε πως δεν υπάρχουν, ή αν βρουν κάποιο κενό ασφαλείας η διαδικασία να διαρκέσει ώρες.

Υπέρ:

Μεγάλη κοινότητα που το υποστηρίζει

Πολύ ικανοποιητικά αποτελέσματα

Είναι εύκολο στη χρήση του

Είναι γρήγορο και ακριβές

Εύκολη εγκατάσταση

Κατά:

Δεν έχει δικό του γραφικό περιβάλλον

Απαιτεί εξειδικευμένες γνώσεις

Απαιτεί πρόσθετες ενέργειες για να λειτουργήσει σε Windows

### 9.2.2 The Mole v0.3

Ιστοσελίδα: http://sourceforge.net/projects/themole/files/

Άδεια χρήσης: Δωρεάν

Επιπλέον πληροφορίες: Διαθέσιμο για Windows και Linux.

Το The Mole είναι ένα αυτοματοποιημένο εργαλείο για την εκμετάλλευση αδυναμιών SQL Injection σε διάφορες ιστοσελίδες. Παρέχοντας στο εργαλείο ένα ευπαθές link και ένα έγκυρο string μπορεί κανείς να εντοπίσει τις ευπάθειες και να τις εκμεταλλευτεί χρησιμοποιώντας μια ευρέως διαδεδομένη τεχνική. Είναι διαθέσιμη η έκδοση v0.3.

Χαρακτηριστικά:

- Υποστήριξη για injections που χρησιμοποιούν βάσεις MySQL, SQL Server, Postgres και Oracle.

- Γραμμή εντολών. Διαφορετικές εντολές εκτελούν διαφορετικές ενέργειες

- Αυτόματη ολοκλήρωση εντολών

- Υποστήριξη για φίλτρα και παράκαμψη IPS/IDS

- εκμετάλλευση SQL Injections μέσω παραμέτρων GET/POST/cookie

- Ανάπτυξη σε γλώσσα Python 3

- εκμετάλλευση SQL Injections κατά την διενέργεια ελέγχων ασφαλείας

Υπέρ:

Απλοποιημένη διαδικασία

Κατά:

Μικρή κοινότητα που το υποστηρίζει

### 9.2.3 SQLSentinel

Ιστοσελίδα: http://sourceforge.net/projects/sqlsentinel/files/

Άδεια χρήσης: Ανοιχτού κώδικα.

Επιπλέον πληροφορίες: Βρίσκει ευπάθειες αλλά δεν μπορεί να τις εκμεταλλευτεί(exploit). Συνδυάζεται με το SQLMap

Το SQL Injection είναι η πιο επικίνδυνη και κοινή επίθεση εναντίον διαδικτυακών εφαρμογών και υπάρχουν πολλά διαθέσιμα εργαλεία για την εκμετάλλευση μιας τέτοιας ευπάθειας. Είναι ένα εργαλείο ανοιχτού κώδικα που αυτοματοποιεί τη διαδικασία εύρεσης ευπαθειών σε ένα δικτυακό τόπο. Περιλαμβάνει ανίχνευσει ιστού και σφαλμάτων SQL. Δίνετε ως στοιχείο τη διεύθυνση ενός ιστοχώρου και το πρόγραμμα ερευνά και προσπαθεί να εκμεταλλευτεί σφάλματα ασφάλειας. Όταν η διεργασία έχει ολοκληρωθεί, δημιουργεί ένα αρχείο report σε μορφή .pdf όπου αναφέρονται το ευπαθές url και το url που ερευνήθηκε.

Δεν πρόκειται για ένα εργαλείο εκμετάλλευσης ευπαθειών αλλά εύρεσης ευπαθών url. Μπορούμε στη συνέχεια να χρησιμοποιήσουμε ένα από τα γνωστά εργαλεία εκμετάλλευσης ευπαθειών.

- υπάρχει στο Backtrack

- λειτουργεί με εντολές στο terminal

- λειτουργεί με Java και θέλει ανάλογες εντολές

### 9.2.4 Havij

Δεν υπάρχει επίσημη ιστοσελίδα

Άδεια χρήσης: Δωρεάν και εμπορική.

Επιπλέον χρήση: Κατάλληλο για χρήση με Windows OS

Είναι ένα εργαλείο αυτοματοποιημένων ελέγχων SQL που βοηθάει τους penetration testers να βρουν και να εκμεταλλευτούν SQL Injection ευπάθειες σε μια ιστοσελίδα. Το πρόγραμμα αυτό δίνει τη δυνατότητα back-end database fingerpritning, την ανάκτηση login ονομάτων και hashes κωδικών, την ανάκτηση δεδομένων, πινάκων και στηλών από Βάσεις, την εκτέλεση SQL συνθηκών έναντι του Server, ακόμη και την πρόσβαση στο δίκτυο αρχείων και την εκτέλεση εντολών κελύφους στο Λειτουργικό Σύστημα.

Διαθέτει Δωρεάν και εμπορική έκδοση με μια πληθώρα δυνατοτήτων σε κάθε μία από τις περιπτώσεις.

Είναι απαραίτητη κάποια γνώση – έστω και αρχάριου –για SQL injection. Στις περισσότερες των περιπτώσεων η διαδικασία είναι συγκεκριμένη. Είσοδος του URL στο κατάλληλο πεδίο, επιλογή της επιθυμητής μεθόδου και πάτημα του κουμπιού «Ανάλυσης».

Υπέρ:

Πολύ εύκολο στη χρήση του.

Αυτοματοποιημένη διαδικασία

Κατά:

Είναι επικίνδυνο στα χέρια ενός κακόβουλου χρήστη ακόμη και χωρίς εξειδικευμένες γνώσεις

### 9.2.5 Σύγκριση SQL Injection Εργαλείων

Ως κριτήρια σύγκρισης θα χρησιμοποιηθούν οι δύο τελευταίες κλάσεις κριτηρίων από το συγκριτικό πλαίσιο αξιολόγησης που περιγράφηκε στο κεφάλαιο 7.

**Εφαρμοσμένα τεχνολογικά ζητήματα**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- B1. Απόδοση
- B2. Πολυπλοκότητα εγκατάστασης
- B3. Τελική αναφορά αποτελεσμάτων
- B4. Φορητότητα

- B5. Χρονική επιβάρυνση

| **Κριτήρια:**<br><br>**Προγράμματα** | **B1** | **B2** | **B3** | **B4** | **B5** |
|---|---|---|---|---|---|
| SQLMap | Υ | Υ | Μ | Μ | Υ |
| The Mole | Μ | Υ | Μ | Μ | Μ |
| SQLSentinel | Μ | Μ | Υ | Χ | Μ |
| Havij | Μ | Μ | Μ | Μ | Μ |

**Ικανοποίηση απαιτήσεων των χρηστών.**

Η κλάση αυτή αποτελείται από μία επιμέρους ομάδα κριτηρίων η οποία περιλαμβάνει τα εξής :

- C1. Ευκολία χρήσης.
- C2. Κοινότητα υποστήριξης
- C3. Κόστος
- C4. Πληρότητα

| **Κριτήρια:**<br><br>**Προγράμματα** | **C1** | **C2** | **C3** | **C4** |
|---|---|---|---|---|
| SQLMap | Μ | Υ | Υ | Υ |
| The Mole | Μ | Χ | Υ | Μ |
| SQLSentinel | Μ | Χ | Υ | Χ |
| Havij | Υ | Χ | Μ | Μ |

*Η διαθέσιμη επιλογή Υψηλή(Υ) σημαίνει σε κάθε περίπτωση την καλύτερη απόδοση. Στο κριτήριο κόστος για παράδειγμα σημαίνει ότι το προϊόν προσφέρεται δωρεάν είτε είναι ανοιχτού κώδικα. Το κριτήριο πληρότητα στη αξιολόγηση εργαλείων που εξετάζουν συγκεκριμένες ευπάθειες αφορά λειτουργίες μέσα στο εύρος δυνατοτήτων των προγραμμάτων αυτής της κατηγορίας.*

[87]

## 9.3. Εξειδικευμένες αναζητήσεις σε CMS

### 9.3.1 DPScan

Έλεγχοι ασφάλειας σε Drupal CMS

https://github.com/cervoise/DPScan

Ο ειδικός ασφάλειας Ali Elouafiq και η ομάδα του, δημιούργησαν ένα νέο εργαλείο ελέγχου ασφάλειας για τον έλεγχο ευπαθειών στο Drupal CMS. Το εργαλείο αυτό απαριθμεί τα modules που χρησιμοποιούνται από την Drupal, έτσι ώστε να προσομοιώσει ένα έλεγχο white Box. Το εργαλείο κυκλοφόρησε δημόσια για να βοηθήσει και άλλους ερευνητές ασφάλειας και προγραμματιστές


Πως πραγματοποιεί έλεγχο;

1. Μετά τη λήψη του εργαλείου, μετακινείστε το ληφθέν αρχείο στο προς εγκατάσταση φάκελο ή στην επιφάνεια εργασίας.
2. Μεταβείτε στον φάκελο dpscan χρησιμοποιώντας την εντολή cd

3. Χρησιμοποιήστε την εντολή(εφόσον έχετε εγκατεστημένη την python) για να πραγματοποιήσετε έλεγχο ευπαθειών στην ιστοσελίδα pythonDPScan.py [Target_Drupal_site]

### 9.3.2 WPSCAN

http://wpscan.org/

Αυτό το πρόγραμμα είναι λίγο διαφορετικό, καθώς ο βασικός σκοπός του είναι μέσω κάποιας αδυναμίας να μας δείξει τους administrators της σελίδας και στη συνέχεια μέσω κάποιας λίστας να σπάσουμε αυτό τον κωδικό παίρνοντας πρόσβαση διαχειριστή!

Το συγκεκριμένο πρόγραμμα είναι γραμμένο σε Ruby και μπορείτε να το βρείτε προεγκατεστημένο στο backtrack 5, όσο και στο νεοανακοινωθέν Kali Linux.

Για παράδειγμα θα πάρουμε τους χρήστες από τη σελίδα σύνδεσης του wordpress(site.gr/wp-admin).

Οπότε πληκτρολογούμε "**./wpscan.rb --url www.site.gr --enumerate u**"

Μετά από λίγα δευτερόλεπτα θα σας δώσε μια λίστα με τους admins που μάζεψε. Στο παράδειγμα βρέθηκαν τέσσερα usernames. Το μόνο που μένει να κάνουμε τώρα είναι να προσπαθήσουμε να μπούμε μέσω dictionary attack. Η εντολή θα είναι η εξής:
"**./wpscan.rb --url www.site.gr --wordlist /directory/of/wordlist.txt --username enausernameapoaytapouvrikame**"

Η εντολή αυτή ζητάει την εύρεση μέσω dictionary attack του κωδικού κάποιου χρήστη με μια λίστα που περιέχει πιθανούς κωδικούς, που έχουμε φτιάξει ή κατεβάσει.

### 9.3.3 JOOMSCAN

Σαρωτής JOOMLA

Είναι ένας σαρωτής ευπαθειών εξειδικευμένος σε Joomla. Το συγκεκριμένο CMS χρησιμοποιείται από πολλά εκατομμύρια διαχειριστών σε όλο τον κόσμο. Υπάρχουν πολλές εκδόσεις Joomla με πιο γνωστή την 1.5. Αυτό που κάνει το Joomscan εξαιρετικά αξιόπιστο, σε θέματα εγκυρότητας και ταχύτητας είναι πως αφού βρει την έκδοση του CMS στη συνέχεια ψάχνει στη Βάση δεδομένων του(Database) exploits ειδικά για τη συγκεκριμένη έκδοση.


Αυτό γλιτώνει πολύ χρόνο, μιας και δεν ξεκινάει να ψάχνει για αδυναμίες που αποδεδειγμένα δεν έχει το Joomla(χαρακτηριστικό παράδειγμα το Acunetix WVS).

Το Joomscan αφού βρει την έκδοση(version), δεν μας εμφανίζει όλα τα exploits για τη συγκεκριμένη version, αλλά επιβεβαιώνει πρώτα πως πρόκειται όντως για ένα κενό ασφαλείας που δεν έχει επιδιορθωθεί.

Είναι διαθέσιμο στο Backtrack. Η αρχική οθόνη μας δείχνει το "OWASP". Είναι σημαντικό το εργαλείο να είναι πάντα ενημερωμένο γι' αυτό και πρέπει να το αναβαθμίζουμε συχνά("**./joomscan.pl update**".). Είναι μία διαδικασία πολύ σύντομη. Για αναζήτηση μιας σελίδας πληκτρολογούμε :

"**perl joomscan.pl -u www.site.gr**".

Κατά τη διάρκεια της σάρωσης παρουσιάζονται διάφορες πληροφορίες(όπως και στο Nikto), και στο τέλος θα κάνει μια μικρή σύνοψη για τις ευπάθειες που βρήκε το πρόγραμμα.

## 10. Αναζήτηση ευπαθειών σε κινητά 3ης γενιάς.

### 10.1 Android

#### 10.1.1 Mercury v2.2.0

**Ένα framework εκτίμησης ευπαθειών για Android.**

Επιτρέπει την αλληλεπίδραση με τελικά σημεία(endpoints) ενδοεπικοινωνίας(Inter-Process Communication) εξαγόμενα από μία εφαρμογή εγκατεστημένη σε κάποια συσκευή.

Τα Android είναι σχεδιασμένα κατά αυτόν τον τρόπο ώστε να περιορίζεται μέσω της διαδικασία απομονωμένης λειτουργίας εφαρμογών(Sandbox) οποιαδήποτε είσοδος μη εξουσιοδοτημένης εφαρμογής σε κάποια άλλη εφαρμογή ή συσκευή χωρίς πρώτα να ζητήσει τα κατάλληλα δικαιώματα. Το mercury ξεπερνάει πολλά από αυτά τα ζητήματα πρόσβασης και επιτρέπει σε ένα ελεγκτή τρωτότητας να εξετάσει τους πιθανούς κινδύνους στους οποίους είναι εκτεθειμένη μία συσκευή.

Το Mercury παρέχει λειτουργικότητα μέσα από μια σειρά εργαλείων στατικής ανάλυσης. Επιτρέπει :

- Την αλληλεπίδραση με 4 IPC endpoints – δραστηριότητες, δέκτες μετάδοσης(broadcast receivers), πάροχους περιεχομένου και υπηρεσίες.
- Χρήση ενός κελύφους(shell) που δίνει τη δυνατότητα εξερεύνησης του Λειτουργικού Συστήματος Linux μέσω μία εφαρμογής που δεν έχει δικαιώματα(είναι εντυπωσιακό το πόσα μπορεί κάποιος να δει παρά την έλλειψη δικαιωμάτων).
- Εύρεση πληροφοριών σε εγκατεστημένα πακέτα με δυνατότητα χρήσης φίλτρων αναζήτησης.

- Εργαλεία για το ανέβασμα(upload) και κατέβασμα(download αρχείων μεταξύ από και προς τη συσκευή Android απευθείας από το Διαδίκτυο(χωρίς να χρειάζεται κάποιο ADB πρόγραμμα).
- Δημιουργία νέων μονάδων(modules) για τη εκμετάλλευση(exploit) των πρόσφατων ευρημάτων (κενών).

http://www.it-securityguard.com/Pentest_09_2012.pdf

Διατίθεται δωρεάν; ΝΑΙ

Υπάρχει κοινότητα που το υποστηρίζει; ΟΧΙ

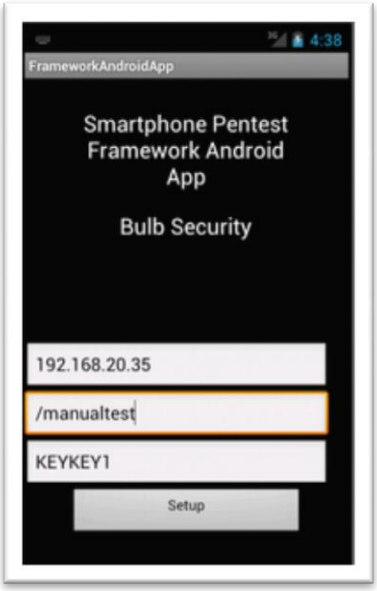
Είναι εύχρηστο; ΟΧΙ – Απαιτεί εξειδικευμένες γνώσεις

Είναι multiplatform: ΟΧΙ

Πλήρες: ΛΙΓΟ

### 10.1.2 SPF – Smartphone Pentest Framework v0.1.7

Επίσημη ιστοσελίδα:http://www.bulbsecurity.com/smartphone-pentest-framework/




Πρόκειται για μία εργαλειοθήκη(toolkit) ανοιχτού κώδικά που αντιμετωπίζει τις πολλές πτυχές της αξιολόγησης ασφάλειας των συσκευών που χαρακτηρίζονται Smartphones. Περιλαμβάνει τις φάσεις της αναζήτησης πληροφοριών(information gathering), της εκμετάλλευσης αδυναμιών(exploitation), της κοινωνικής μηχανικής(social engineering) και της post-exploitation. Ο έλεγχος γίνεται τόσο μέσω ενός παραδοσιακού δικτύου IP όσο και μέσα από ένα modem κινητού. Είναι πολύ χρήσιμο για μια ομάδα ελέγχου τρωτότητας γιατί μπορεί να λειτουργήσει ως μοχλός ελέγχου για την ανακάλυψη της στάσης ενός οργανισμού σε σχέση με την ασφάλεια. Το framework αυτό μπορεί να λειτουργήσει από κονσόλα και γραμμή εντολών, από ένα γραφικό περιβάλλον ή από εφαρμογή σχεδιασμένη να λειτουργεί σε Smartphone

Η πρώτη του έκδοση περιλάμβανε μία κονσόλα διαχείρισης βασισμένη σε κείμενο, ένα web based GUI και μία εφαρμογή διαχείρισης για Android.

- SPF κονσόλα. Είναι ένα πρόγραμμα γραμμένο σε Perl που επιτρέπει στους χρήστες του Framework να εκτελέσουν κάθε είδους λειτουργικότητα του Server του SPF.
- SPF Web based GUI. Έχει ένα web based front-end το οποίο επιτρέπει την εκτέλεση όλων των δυνατών λειτουργιών του Server.
- SPF Android App. Η εφαρμογή αυτή επιτρέπει στους χρήστες να αξιοποίηση του modem του Android Smartphone με το SPF για την αποστολή SMS μηνυμάτων, τη συλλογή πληροφοριών κτλ.
- SPF Android Agent. Προσφέρει post-exploitation δυνατότητες όπως κλιμάκωση προνομίων, συλλογή πληροφοριών και απομακρυσμένη σύνδεση σε κινητά Android που είναι εγκατεστημένος ο agent. Αυτή τη χρονική περίοδο αναπτύσσονται agents για IPhone και Blackberry.


Εικόνα 10.1.2. SPF κεντρικό menu

Διατίθεται δωρεάν; ΝΑΙ (Open Source)

Υπάρχει κοινότητα που το υποστηρίζει; ΟΧΙ

Είναι εύχρηστο; ΛΙΓΟ – Απαιτεί εξειδικευμένες γνώσεις

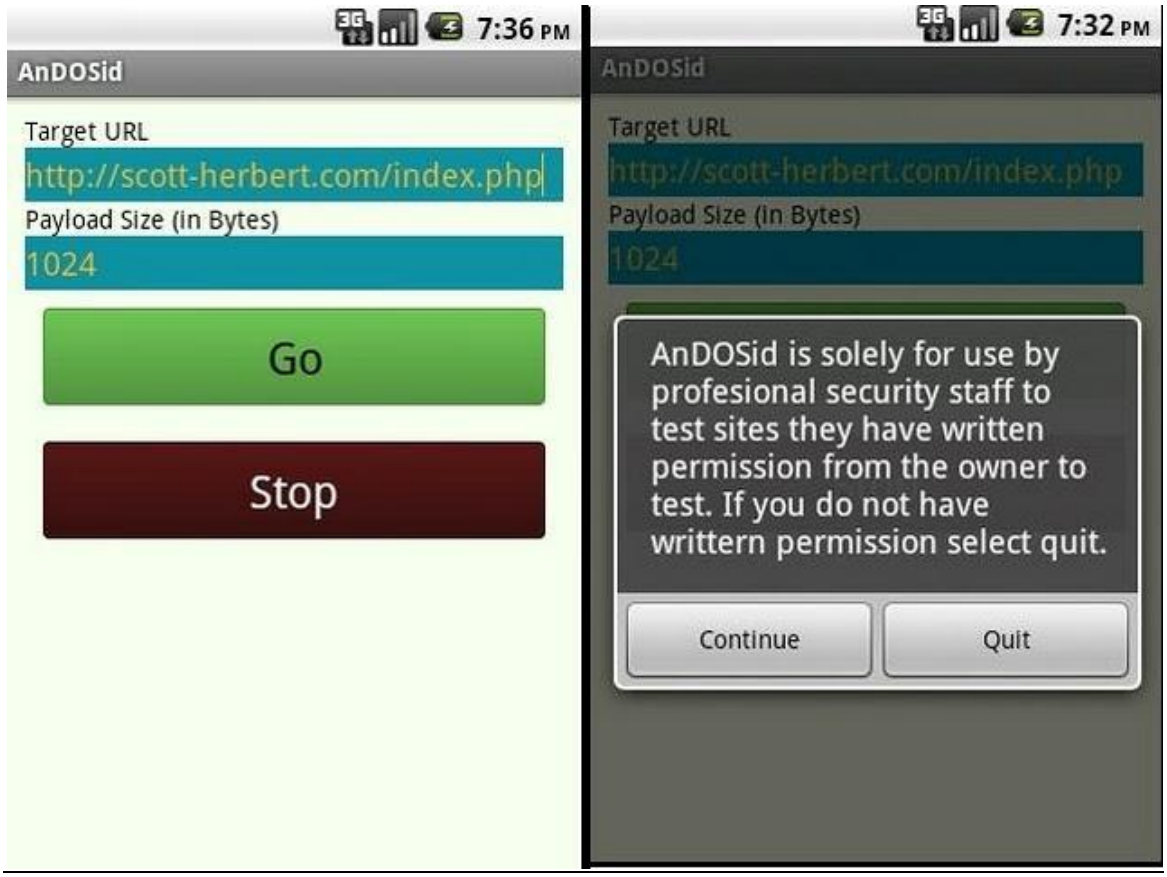
Είναι multiplatform: ΟΧΙ

Πλήρες: ΑΡΚΕΤΑ

### 10.1.3 AnDOSid

Το εργαλείο DoS για Android

Πρόκειται για ένα νέο προϊόν που κυκλοφόρησε από τον SCOTT HERBERT για τα κινητά τηλέφωνα ANDROID. Είναι ένα εργαλείο DoS για τηλέφωνα Android. Η αύξηση των επιθέσεων hacking σε όλο τον κόσμο έχει αναστατώσει πολλούς διαχειριστές στο διαδίκτυο και αναδείξει το ζήτημα της διαδικτυακής ασφάλειας σε άκρως σημαντικό. Υπάρχει ένα κενό ασφάλειας όσο αναφορά συσκευές όπως τα τηλέφωνα τρίτης γενιάς που έχουν πλέον μετατραπεί σε τεράστια πλατφόρμα υπολογιστικών λειτουργιών.




Εικόνας 10.1.3 Γραφικό περιβάλλον anDOSid

Το AnDOSid αποτελεί μια εφαρμογή που έρχεται να καλύψει μέρος του κενού αυτού, επιτρέποντας σε ειδικούς ασφάλειας να προσομοιώνουν επιθέσεις DOS και DDOS εναντίον ενός web server μέσω κινητών τηλεφώνων. Είναι ακόμη σε περίοδο

δημιουργίας και η κοινότητα αναμένει ανατροφοδότηση από τους χρήστες για τη βελτίωσή του,

Μπορείτε να το μεταφορτώσετε από το Android Market place και κοστίζει 1 ευρώ.

### 10.1.4 Android Network Toolkit

Πρόκειται για ένα σύνολο εργαλείων που έχουν αναπτυχθεί για penetration testers και ethical hackers ώστε να ελέγχουν οποιοδήποτε δίκτυο για ευπάθειες από το κινητό του τηλέφωνο. Το toolkit περιλαμβάνει διαφορετικές εφαρμογές που βοηθούν στην εύρεση τρωτών σημείων ενός δικτύου και ενδεχομένων την εκμετάλλευσή τους. Η εταιρεία που το κυκλοφόρησε είναι Ισραηλινή Zimperium.

### 10.1.5 Nmap για Android

Το Nmap είναι ένα από τα καλύτερα network scanner εργαλεία. Αναπτύχθηκε κυρίως για Unix αλλά πλέον είναι διαθέσιμο εκτός από Windows και για το Android. Μόλις τελειώσει η σάρωση της εφαρμογής μπορείτε αν στείλετε με e-mail τα αποτελέσματα.

Σημειώνεται ότι δεν πρόκειται για επίσημη εφαρμογή.

### 10.1.6 FaceNiff-SessionHijacker

Είναι ένα εργαλείο για Session Hijacking των διάσημων ιστοσελίδων κοινωνικής δικτύωσης περιλαμβάνοντας φυσικά το facebook και το twitter. Έχει αναπτυχθεί από τον Bartosz Ponurkiewicz, τον δημιουργό δηλαδή του Firesheep.

### 10.1.7 Santoku Linux Mobile Forensic & Security

Το Santoku είναι μια πλατφόρμα για mobile forensics, ανάλυση malware κινητών και ελέγχους ασφάλειας mobile applications. Η δωρεάν έκδοση του Santokou είναι ένα περιβάλλον εργασίας το οποίο παρέχει εργαλεία drivers και οδηγούς σχετικά με τα εργαλεία. Η έκδοση alpha βασίζεται στη διανομή OWASPMobiSec. Περιέχει :

- Εργαλεία για firmware flashing για διάφορους κατασκευαστές
- Εργαλεία imaging για NAND, media cards και RAM
- Δωρεάν εκδόσεις κάποιων εμπορικών εργαλείων forensics
- Χρήσιμα scripts και εργαλεία ειδικά φτιαγμένα για mobile foernsics.

Εργαλεία ελέγχων:

- Εξομοιωτές κινητών τηλεφώνων
- Εργαλεία για προσομοίωση υπηρεσιών δικτύου για δυναμική ανάλυση
- Εργαλεία decompilation
- Πρόσβαση σε βάσεις δεδομένων malware

Ασφάλειας κινητών. Έλεγχοι mobile application

- εργαλεία decompilation
- scripts για εύρεση κοινών προβλημάτων σε mobile applications

- scripts για αυτοματοποιημένη αποκρυπτογράφηση binaries, εγκατάσταση εφαρμογών, έλεγχοι λεπτομερειών εφαρμογών κ.α


Development tools

- android SDK manager
- BlackBerry JDE
- BlackBerry Table OS SDK
- Lab Server (HTTP και HTTPS)
- BlackBerry Ripple
- BlackBerry Simulators

Penetration Testing

- CeWL
- DirBuster
- Fierce
- Nikto
- Nmap
- Burp Suite
- Mallorz
- W3af Console
- W3af GUI
- ZAP
- BeEF
- Ettercap
- iSniff
- Metasploit Console
- Metasploit GUI
- NetSed
- SQLMap
- SSLStrip

Reverse Enginneering

- APK Tool
- Dexl'jar
- Flawfinder

- Java Decompiler
- Strace

Wireless Analysers

- Aircrack-ng
- Kismet
- Ubertooth Kismet
- Ubertooth Spectrum Analyser
- Wireshark

Device Forensics

- AFLogical Open Source Edition
- Android Encryption Brute Force
- BitPim
- BlackBerry Desktop Manager
- Foremost
- iPhone Back Analyser
- MIAT
- Paraben Device Seizure
- Sift Workstation
- Sleuth Kit
- SQLiteSpy

Mobile Infrastracture

- BES Express
- Google Mobile Management
- iPhone Configuration Tool

[30],[42]

## 10.2. iPhone / iPad

### 10.2.1. LANScan

Αυτή η εφαρμογή διατίθεται για iPhone και iPad και επιτρέπει την γρήγορη και εύκολη πρόσβαση σε διάφορα είδη δικτυακών σαρώσεων όπως TCP, ARP, NetBios, Reverse DNS και Port Scans. Είναι ένα πολύ χρήσιμο εργαλείο για ελέγχους τρωτότητας και ιδιαιτέρως σε ασύρματα τοπικά δίκτυα.


Εικόνα 10.2.1. Γραφικό περιβάλλον LANScan

Τιμή:

iPhone - $3.99

iPad - $6.99

### 10.2.2. Nework “Swiss-Army-Knife”

Διαθέσιμη μόνο για iPhone μέχρι στιγμής με πολλές λειτουργίες να την υποστηρίζουν. Έχει ένα λιτό γραφικό περιβάλλον. Ορισμένες από τις λειτουργίες του περιγράφονται στην παρακάτω εικόνα:


Τιμή:

iPhone: $3.99

### 9.2.3.iNetQCheckPro

Πρόκειται για ένα εργαλείο επαγγελματικό και πολύ λεπτομερές. Παρέχει ένα μεγάλο αριθμό πληροφοριών στο διαχειριστή του.


Εικόνα 10.2.2. Απεικόνιση αποτελεσμάτων

iPhone: $4.99

http://blogs.aerohive.com/blog/the-wireless-lan-architecture-blog-3/top-10-iphone-and-ipad-apps-for-the-network-professional

### 10.2.3 System Scope

Επίσημη ιστοσελίδα: https://itunes.apple.com/us/app/system-scope/id420213874?mt=8

Είναι μία εφαρμογή για iPad για την αντιμετώπιση προβλημάτων σε ένα δίκτυο και επιπλέον χρησιμοποιείται για τη καταγραφή συσκευών και ιστοσελίδων. Επιτρέπει την αποθήκευση και την καταγραφή οποιασδήποτε IP Based δικτυακής συσκευής ή game server χρησιμοποιώντας ICMP v4. Δουλεύει εξίσου καλά τόσο με 3G όσο και με WIFI.

Η εφαρμογή έχει δύο περιοχές λειτουργικότητας. Η αριστερή μεριά επιτρέπει την αποθήκευση των παραπάνω συσκευών ή game servers που θέλουμε να παρακολουθήσουμε . Η κατάσταση(status) και η διαθεσιμότητα τους αποδίδεται με χρωματιστά γραφικά LED. Η δεξιά μεριά επιτρέπει την επίλυση των ζητημάτων μιας συσκευής επιτρέποντας την λεπτομερή διαμόρφωση των ICMP παραμέτρων

από απλά μέχρι πολύπλοκα σενάρια προβλημάτων.


Εικόνα 10.2.3. Γραφικό περιβάλλον system scope

Περιλαμβάνει ένα live γράφο των ICMP χρόνων απάντησης και ακόμη την εκτύπωση και την αποστολή με email των αποτελεσμάτων.

[70]

## 11. Συμπέρασμα.

Η διαδικασία του ελέγχου τρωτότητας ενός δίκτυο-κεντρικού συστήματος μπορεί να είναι μία αποτελεσματική και αποδοτική στρατηγική για την προστασία ενός οργανισμού έναντι επιθέσεων. Αν υλοποιηθεί με το σωστό τρόπο επιτρέπει την αναγνώριση εσωτερικών πρακτικών που αυξάνουν τον κίνδυνο ευπαθειών. Τα αποτελέσματα των αναζητήσεων επιτρέπουν σε ένα οργανισμό να αφαιρέσει αυτές τις ευπάθειες, κατευθύνουν αναλόγως τις προσπάθειες ασφάλειας, πιέζουν τις εταιρείες να βελτιώσουν τα προϊόντα τους, να βελτιώσουν τις πρακτικές ασφάλειας και πείθουν τους πελάτες, τους μετόχους ή τους συνεργάτες τους ότι κάνουν μία σοβαρή προσπάθεια για την προστασία ευαίσθητων δεδομένων της εταιρείας.

Επιπλέον τα οφέλη του περιλαμβάνουν την αποφυγή οικονομικών επιπτώσεων, συμμόρφωση με τις ρυθμιστικές αρχές της οικονομίας και διατήρηση μιας αξιοπρεπούς εικόνας μιας εταιρείας ή οργανισμού.

Ο έλεγχος τρωτότητας αποτελεί μόνο ένα κομμάτι της διαδικασίας ελέγχου επομένως δεν πρέπει να αναμένουμε την εύρεση όλων των πιθανών ευπαθειών κατά την ολοκλήρωση του. Ένας οργανισμός πρέπει να αναπτύξει μία

ολοκληρωμένη στρατηγική ελέγχου ασφάλειας που προσαρμόζεται στις πολιτικές ασφάλειας.

Η διαδικασία εύρεσης ευπαθειών είναι μια συνεχής, επαναλαμβανόμενη διαδικασία που προσαρμόζεται στις αλλαγές της τεχνολογίας, στην στρατηγική μιας επιχείρησης και στα διαθέσιμα εργαλεία από τη μεριά των κακόβουλων χρηστών. Είναι ένας διαρκής κύκλος που σε κάθε ολοκλήρωση του μας προσφέρει μία μέτρηση της κατάστασης της ασφάλειας.

## Πηγές – Βιβλιογραφία

[1]http://www.symantec.com/about/news/release/article.jsp?prid=20120905_02

[2]http://www.hp.com/hpinfo/newsroom/press/2012/121008a.html

[3] https://www.owasp.org/index.php/Main_Page

[4] https://www.owasp.org/index.php/Top_10_2013-Main

[5]http://hackingexperience.blogspot.com/2013/02/bugtraq-2_1613.html#ixzz2RwxPvrZ2

[6] http://www.toolswatch.org/2013/04/arachni-the-web-application-security-scanner-v0-4-2-in-the-wild-boosted-with-new-ui-interface/

[7] http://hackingexperience.blogspot.com/2012/09/pipal-passwords_1492.html#ixzz2RwvzjsBL

[8] http://hackingexperience.blogspot.com/2013/02/hydra-v-74_8218.html#ixzz2Rwxen1z8

[9] http://www.brighthub.com/computing/smb-security/articles/34711.aspx?cid=parsely_rec

[10] http://www.breakthesecurity.com/2012/05/list-of-best-ethical-hacking.html

[11] http://www.securitywizardry.com/index.php/products/scanning-products/network-scanners.html

[12] http://en.wikipedia.org/wiki/Penetration_test

[13] http://sectools.org/

[14] http://www.sharewareconnection.com/software.php?list=Website+Scanner

[15] http://www.symantec.com/connect/articles/penetration-testing-web-applications-part-three

[16] http://www.computerworld.com/s/article/9087439/Five_free_pen_testing_tools

[17] http://www.nightlionsecurity.com/blog/tools/2012/08/nessus-openvas-and-nexpose-comparison-against-metasploitable-2/#.UZG97LV7Ka9

[18] http://www.nightlionsecurity.com/blog/#.UIu1HMUxqSo

[19] http://www.makeuseof.com/tag/give-website-security-check-hackertarget/

[20] http://www.secnews.gr/archives/category/pentest

[21] http://www.secnews.gr/archives/51320

[22] http://www.dummies.com/how-to/content/tools-that-augment-your-firewall-protection.html

[23] http://zitstif.no-ip.org/?cat=6

[24] http://www.securitytube-tools.net/

[25]http://back-track-linux.blogspot.gr/2012/11/information-gathering-using-domain-name.html

[26]http://invisiblespeaks.blogspot.gr/2012/09/hacking-with-backtrack-exploring-your.html

[27]http://hackingexperience.blogspot.com/2012/09/simple-phishing-toolkit-v060_6127.html

[28] http://media.techtarget.com/rms/pdf/BackTrack%205%20tutorial%205.pdf

[29] http://www.security-audit.com/blog/penetration-testing-tools/

[30] http://www.security-audit.com/blog/

[31]http://www.ehacking.net/2011/08/theharvester-backtrack-5-information.html

[32]http://pentestlab.wordpress.com/2013/01/07/windows-tools-for-penetration-testing/?goback=.gde_41186_member_201849662

[33]http://www.spylogic.net/2009/10/enterprise-open-source-intelligence-gathering-part-1-social-networks/

[34] http://n00bpentesting.com/lessons/ptes-101/intelligence-gathering/

[35] http://n00bpentesting.com/lessons/ptes-101/intelligence-gathering/

[36]http://back-track-linux.blogspot.sk/2012/11/backtrack-penetration-testing-tutorial.html

[37] http://www.infond.fr/2010/05/toturial-footprinting.html

[38] http://www.secnews.gr/archives/49389

[39]http://seclist.us/2013/01/owasp-mantra-janus-released-free-and-open-source-browser-based-security-framework.html

[40] http://seclist.us/category/penetration-test

[41] http://sectools.org/tag/web-scanners/

[42] http://www.secnews.gr/archives/60425

[43] http://www.n1tr0g3n.com/?p=3698

[44] http://mateslab.weebly.com/dnmap-the-distributed-nmap.html

[45]http://n00bpentesting.files.wordpress.com/2011/12/intro-to-penetration-testing-lab-guide-0ne1.pdf

[46] http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

[47] http://pentestlab.wordpress.com/category/information-gathering/

[48]http://www.social-engineer.org/framework/Social_Engineers:_Penetration_Testers

[49] https://www.trustedsec.com/downloads/social-engineer-toolkit/

[50] http://thanasaras13.blogspot.sk/2011/11/admin-finder.html

[51] http://hack3rboys.blogspot.sk/2013/01/admin-page-finder-v2.html

[52] http://www.hackforsecurity.net/2012/01/admin-finder-perl-script.html

[53] http://www.hcon.in/hconstf-fire-features.html

[54] http://www.brighthub.com/computing/smb-security/articles/72408.aspx

[55] http://www.acunetix.com/websitesecurity/website-auditing-wp/

[56] http://pauldotcom.com/ZenAndTheArtOfInternalPenTestingPartI.pdf

[57] http://pauldotcom.com/ZenAndTheArtOfInternalPenTestingPartII.pdf

[58] http://rajhackingarticles.blogspot.gr/search/label/Penetration%20Testing

[59] http://www.brighthub.com/computing/smb-security/articles/40171.aspx#

[60]http://www.soldierx.com/tutorials/Pentesting-Tutorial-1-Information-Gathering-Part-1-Nmap

[61] http://hackingexperience.blogspot.com/2012_09_01_archive.html

[62] http://www.acunetix.com/blog/category/docs/

[63] http://digilib.lib.unipi.gr/dspace/bitstream/unipi/3072/1/Koreas.pdf

[64] http://www.vulnerabilityassessment.co.uk/

[65]http://www.michaelboman.org/books/practical-web-application-vulnerability-assessment

[66] http://www.secnews.gr/archives/51519

[67] http://projects.breakthesecurity.com/

[68] http://www.andlabs.org/

[69] http://www.theprohack.com/2008/06/basic-javascript-hacking.html

[70] http://www.security-audit.com/blog/top-5-security-apps-for-iphone/

[71] http://www.toolswatch.org/tag/ethical-hacking-pentesting/

[72] http://www.secnews.gr/archives/category/pentest/page/3

[73]http://www.securitywizardry.com/index.php/products/scanning-products/wireless-tools.html

[74] http://www.pentest-standard.org/index.php/Main_Page

[75]https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/Penetration/penetration_pdf.pdf?__blob=publicationFile

[76] http://dsmc.eap.gr/downloads/PLH40-Kalabounia.pdf

[77] https://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf

[78] https://www.owasp.org/index.php/OWASP_Testing_Project

[79]http://www.packtpub.com/sites/default/files/5580OS-Chapter-6-Attacking-the-Client_0.pdf

[80]http://www.securestate.com/Services/Profiling/Pages/VoIP-Penetration-Test.aspx

[81] http://www.clausewitz.com/readings/Principles/

[82] http://www.coresecurity.com/core-impact-pro

[83] http://www.securitytube.net/

[84] http://www.borntohack.in/search/label/Backtrack

[85] http://www.openvas.org/

[86]http://www.darknet.org.uk/2011/06/burp-suite-free-edition-v1-4-web-application-security-testing-tool/

[87] http://www.secnews.gr/archives/28629

[88] http://www.liatsisfotis.com/search/label/Security%20Tools

[89] http://www.youtube.com/watch?v=OiYLCf7p4AI

[90] http://www-bcf.usc.edu/~halfond/papers/halfond11stvr.pdf