Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή θετικών και εφαρμοσμένων επιστήμων

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Evaluating TLS/SSL proxies for threat visibility

Νταφόπουλος Χρήστος

Επιβλέπων Καθηγητής
Σταύρου Ιλιάνα

10/2022

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή θετικών και εφαρμοσμένων επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Ασφάλεια Υπολογιστών και Δικτύων*

Μεταπτυχιακή Διατριβή

Evaluating TLS/SSL proxies for threat visibility

Νταφόπουλος Χρήστος

Επιβλέπων Καθηγήτρια
Σταύρου Ιλιάνα

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στην ασφάλεια υπολογιστών και δικτύων από τη Σχολή θετικών και εφαρμοσμένων επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

10/2022

Περίληψη

Στην παρούσα διατριβή θα γίνει μια ανασκόπηση στα open source εργαλεία που υπάρχουν για TLS/SSL proxies, ώστε να τα χρησιμοποιήσουμε με σκοπό για να αποκρυπτογραφήσουμε και να κρυπτογραφήσουμε μια επικοινωνία προς το διαδίκτυο στο οποίο επιθυμούμε να επικοινωνήσουμε. Τα πρωτόκολλα επικοινωνίας είναι ζωτικής σημασίας για τα δεδομένα. Η κρυπτογραφία προστατεύει τα δεδομένα μας, ενώ την ίδια στιγμή αποτρέπει τα εργαλεία παρακολούθησης της επικοινωνίας στο διαδίκτυο. Ένας proxy θα μας δώσει την δυνατότητα για να δούμε την επικοινωνία σε πραγματικό χρόνο, ώστε να γνωρίζουμε τι έχει συμβεί. Επίσης από την βιβλιογραφική ανασκόπηση θα χρησιμοποιηθούν πληροφορίες, ώστε να δούμε τα χαρακτηριστικά τους, σε ποιες πλατφόρμες μπορούν να εγκατασταθούν, εάν έχουμε επικοινωνία, επίσης τι λειτουργικό σύστημα υποστηρίζουν τέλος εάν οι εκδόσεις του TLS/SSL proxies έχουν τρωτά σημεία σε κάποιες εκδόσεις. Τα εργαλεία proxy θα αξιολογηθούν περαιτέρω με τη χρήση εικονικών μηχανών.

Summary

In this thesis a review will be made of the open source tools that exist for TLS/SSL proxies, so that we can use them in order to decrypt and encrypt a communication to the internet we wish to communicate. Communication protocols are critical to data. Cryptography protects our data, while at the same time preventing online communication tracking tools. A proxy will allow us to see the communication in real time, so we know what has happened. Also from the literature review information will be used to see their features, on which platforms they can be installed, if we have communication, also what operating system they support and finally if the versions of TLS/SSL proxies have vulnerabilities in some versions. Proxy tools will be further evaluated using virtual machines.

Ευχαριστίες

Μετά από δυο χρόνια έντονης πίεσης ως πατέρας, σύζυγος και εργαζόμενος, έφτασε η ώρα της διπλωματικής. Όπου μέσα από καρδίας θα ήθελα να ευχαριστήσω την οικογένεια μου για την υπομονή και την δύναμη που μου έδωσαν, επίσης την Δρ. Σταύρου Ιλιάνα για την καθοδήγηση της ώστε να συνεχίσω ακούραστος για την εκπλήρωση της διπλωματικής εργασίας.

Περιεχόμενα

1 Εισαγωγή 6
1.1 Στατιστικά στοιχεία επιθέσεων 7
1.2 Πρωτόκολλα TLS/SSL 10
1.2.1 Ο ρόλο και η σημασία κατά την χρήσης των TLS/SSL proxies 11
1.3 Αναφορά στους ερευνητικούς στόχους της διατριβής και συνεισφορά 12
2 Βασική γνώση και βιβλιογραφική ανασκόπηση 13
2.1.1 DDoS 13
2.1.2 Man-in-the-middle (MitM) 14
2.1.3 Επιθέσεις phishing 15
2.1.4 Επίθεση SQL Injection 15
2.1.5 Malware Attack 16
2.2 TLS/SSL proxies – ρόλος και λειτουργία 17
2.2.1 Δομή πρωτοκόλλων 18
2.2.2 Σχεδιασμός πρωτόκολλων 18
2.2.3 Διαχείριση session 19
2.2.4 Εμπιστευτικότητα 20
2.3 Εργαλεία ανοιχτού κώδικα TLS/SSL proxy 20
2.3.1 OpenSSL 21
2.3.2 WolfSSL 21
2.3.3 GnuTLS 22
2.3.4 Mitmproxy 22
2.3.5 SSLsplit 22
2.3.6 Polarproxy 23
2.3.7 Squid proxy 24
2.3.8 Σύγκριση τον proxies 24
Polarproxy 24
2.4 Τρωτά σημεία στο πρωτόκολλο TLS/SSL 26
2.4.1 Τρωτά σημεία από ευπάθεια προδιαγραφών 26
2.4.2 Τρωτών σημείων κατά την υλοποίηση 27
2.5 Proxy και στατιστικά υλοποίησης 29
3 Μεθοδολογία 32
4 Σχεδιασμός υποδομής δικτύου για αξιολόγηση TLS/SSL proxies 34
4.1 Απαιτήσεις σχεδιασμού 35

4.2 Κριτήρια αξιολόγησης 37
4.2.1 Λειτουργιές proxy που υποστηρίζουν 37
4.2.2 Αλγόριθμοι κρυπτογράφησης που υποστηρίζουν 39
4.2.3 Η υποστήριξη του proxy TLS/SSL σε βιβλιοθήκες και πρωτόκολλα 41
4.2.4 Κατά πόσο διαδεδομένο είναι στον χώρο της ασφάλειας 42
4.2.5 Ταχύτητα ανταπόκρισης και επεξεργασίας 43
4.2.6 Πόσο εύκολο είναι η εγκατάσταση και η παραμετροποίηση 44
4.3 Σενάρια υλοποίησης 46
4.3.1 Επιθεώρηση της κίνησης μεταξύ πελάτη και ιστοσελίδας HTTPS 46
4.3.2 Επιθεώρηση της κίνησης μεταξύ πελάτη και ιστοσελίδας HTTP 47
4.3.3 Εργαλεία που επηρεάζουν την εκτέλεση του proxy TLS/SSL και την κίνηση 47
4.3.4 Λειτουργία PCAP αρχείων 47
4.3.5 Λειτουργία Transparent proxy 48
4.3.6 Λειτουργία Reverse proxy 48
5 Υλοποίηση υποδομής δικτύου και αξιολόγηση εργαλείων 50
5.1 Υλοποίηση σεναρίων Mitmproxy σε εικονική μηχανή 51
5.2 Υλοποίηση σεναρίων Polarproxy σε εικονική μηχανή 56
5.3 Υλοποίηση σεναρίων Squid proxy σε εικονική μηχανή 60
6 Επίλογος 65
6.1 Κύρια συμπεράσματα που απορρέουν από την διατριβή 65
6.2 Σύντομη ανάλυση μελλοντικής εργασίας 67
Βιβλιογραφία 68
Config αρχείο του Squid proxy 1
A.1 Config file 1

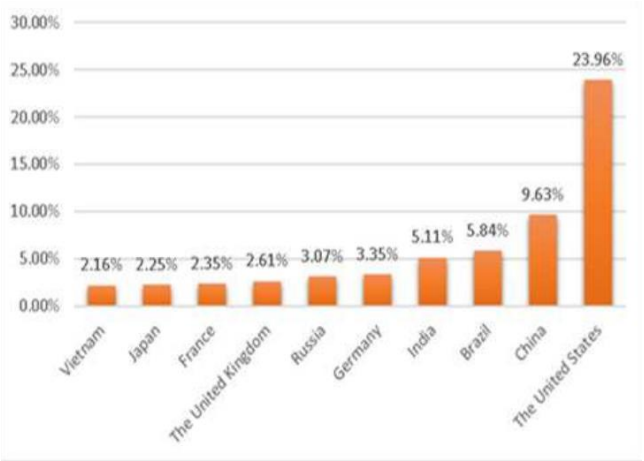
Κεφάλαιο 1
Εισαγωγή

Καθημερινά στον κόσμο πραγματοποιούνται συζητήσεις, για την καινοτομία τον νέων εφαρμογών, υπηρεσιών σε κινητά τηλεφώνα και υπολογιστές που διευκολύνουν τους χρήστες να εκτελέσουν εργασίες ρουτίνας όπως η πληρωμή λογαριασμών κοινής ωφέλειας, αγορά εισιτηρίων μέσω διαδικτύου, παρακολούθηση δελτία καιρού και διαδικτυακή τηλεόραση. Επίσης οι χρήστες μπορούν να κατεβάσουν παιχνίδια και αρχεία μουσικής. Η καινοτομία των εφαρμογών και υπηρεσιών έχει επιταχυνθεί λόγω της μεγάλης επιρροής του διαδικτύου στις τηλεπικοινωνίες τις τελευταίες δύο δεκαετίες. Παράλληλα οι επιθέσεις στον κυβερνοχώρο έχουν γίνει μια αυξανόμενη απειλή τόσο για τους οργανισμούς όσο και για το ευρύτερο δημόσιο κοινό. Αυτό έχει οδηγήσει σε πολύ αρνητικές επιπτώσεις στην οικονομία γενικά και στην καθημερινή ζωή των ανθρώπων. Κάθε επιτυχημένη επίθεση στον κυβερνοχώρο σε στοχευόμενες συσκευές και δίκτυα επισημαίνει τις αδυναμίες στους αμυντικούς μηχανισμούς που είναι υπεύθυνοι για την ασφάλειά τους. Επομένως, η εκ των προτέρων κατανόηση των απειλών στον κυβερνοχώρο είναι απαραίτητη για την αποφυγή πιθανών επιθέσεις στο μέλλον. Έχουν γίνει πολυάριθμες προσπάθειες για την αποφυγή κυβερνοεπιθέσεων, που άφορα την προστασία των πολύτιμων περιουσιακών στοιχείων ενός οργανισμού όσο και προσωπικών στοιχειών. Ωστόσο υπάρχει σαφώς μια άνευ προηγουμένου ανάγκη για μια λύση που να υιοθετεί μια προληπτική προσέγγιση για την κατανόηση πιθανών απειλών στον κυβερνοχώρο σε πραγματικό χρόνο. Η χρήση κατάλληλων πρωτοκόλλων και μεσολαβητών όπου θα δίνουν έμφαση στην κρυπτογράφηση της επικοινωνίας τόσο σε οργανισμούς όσο και στην προσωπική επικοινωνία, ώστε να γίνει

η κατανόηση και πρόβλεψη μελλοντικών επιθέσεων στον κυβερνοχώρο μέσω συλλογής και ανάλυση συμβάντων δικτύου, όπου θα οδηγήσει στον εντοπισμό της δραστηριότητας του εισβολέα. Τέλος θα μπορούσε να χρησιμοποιηθεί για την κατανόηση της φύση μιας επίθεσης.

1.1 Στατιστικά στοιχεία επιθέσεων

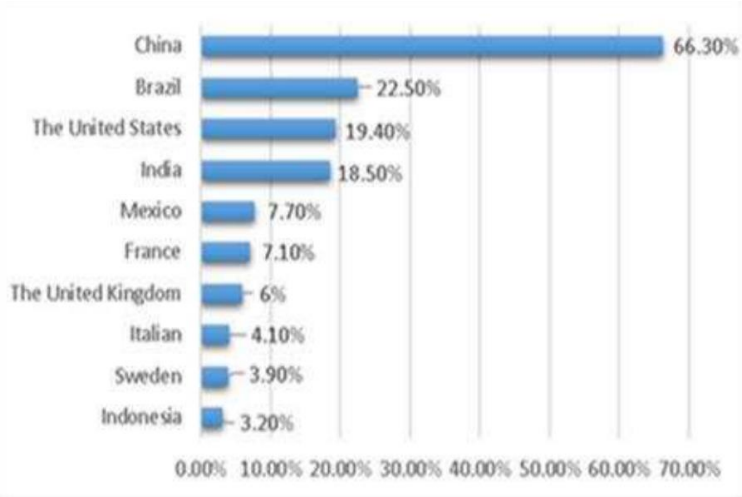
Η ψηφιακή εποχή θεωρείται απαραίτητο εργαλείο για τη μέτρηση της επιτυχίας ή της αποτυχίας σε ατομικό, οργανωτικό και κοινοτικό επίπεδο και αποτελεί ουσιαστικό παράγοντα τις έννοια της ανάπτυξης. Ως εκ τούτου, η ασφάλεια των δεδομένων έχει γίνει ένα σημαντικό ζήτημα και μια αναπτυσσόμενη έννοια, όπου επηρεάζει όλους ανεξαιρέτως τους τομείς. Οι επιτιθέμενοι μπορούν να δουλέψουν να έχουν πρόσβαση σε αυτές τις πληροφορίες και να τις χρησιμοποιούν για δικούς τους σκοπούς. Επομένως οι επιθέσεις χαρακτηρίζονται από στατιστικά στοιχεία που αφορούν την συχνότητα αυτών, όπως και την φύση τους. Σύμφωνα με την αναφορά τον Απρίλιο του 2017 από την Αμερικανή εταιρεία κυβερνοασφάλειας Symantec όπως φαίνεται στο σχήμα 2.1, οι Ηνωμένες Πολιτείες είναι η μεγαλύτερη χώρα που είχε phishing επιθέσεις το 2016. Βρίσκεται στην κορυφή της λίστας της Symantec. Έχοντας πραγματοποιήσει μια αύξηση στο 23,96% [1].



Σχήμα 1.1: 10 χώρες με περισσότερες κυβερνοεπιθέσεις το 2016.

Ο λόγος είναι ότι εμφανίστηκε ένα είδος κακόβουλου λογισμικού και διαδόθηκε σε όλο τον κόσμο, με το όνομα Mirai. Άρχισε να χρησιμοποιεί τον πηγαίο κώδικα Mirai για την αποστολή ευρείας εμβέλειας επιθέσεις DDoS (Distributed Denial Of Service) σε διαφορετικά στόχους. Επίσης το πρώτο εξάμηνο του 2017 γνώρισε μια απεριόριστη μεγάλη επίθεση το διαδίκτυο σε επίπεδο εταιρειών και χρηστών. Οι εκατοντάδες εγκληματικές υποθέσεις στον διαδικτυακό ιστό, όπως επίσης και το επίπεδο της πειρατείας προκάλεσε νέες επιθέσεις όχι μόνο σε αριθμούς αλλά και σε ένταση. Αυτή ήταν μια πολυάσχολη χρονιά για τους βιομηχανία κυβερνοασφάλειας. Συμφωνώντας με δημοσιευμένη της έκθεση από την Symantec Corporation, την κορυφαία εταιρεία στον κόσμο της κυβερνοασφάλειας. Το 2017 σημειώθηκε αύξηση 600 τοις εκατό σε γενικές γραμμές επιθέσεις σε IoT, αυτό σημαίνει ότι οι εγκληματίες του κυβερνοχώρου μπορεί να έχουν εκμεταλλευτεί τη σχετική φύση αυτών των συσκευών [2]. Στο σχήμα 2 δείχνει, τις 10 χώρες που επλήγησαν από το έγκλημα το 2017. Στη Βραζιλία είχαν την

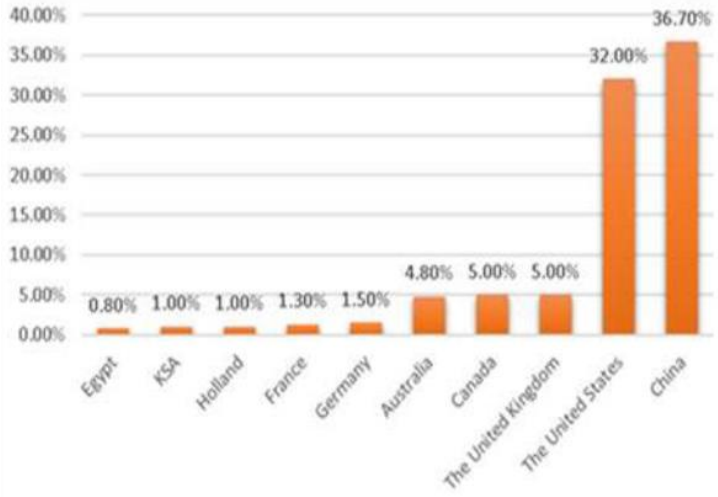
μεγαλύτερη εμπειρία του ηλεκτρονικού εγκλήματος αξίας 22,5 δισεκατομμυρίων δολαρίων ΗΠΑ. Σε γενικές γραμμές, το μέσο θύμα του εγκλήματος στον κυβερνοχώρο έχασε 142 δολάρια Η.Π.Α. Στις Ηνωμένες Πολιτείες το 2017, η εισβολή της Yahoo είχε πρόσφατα καταγραφεί ότι επηρέασε 3 δισεκατομμύρια λογαριασμούς πελατών ήταν από τις μεγαλύτερες επιθέσεις που πραγματοποιηθήκαν.



Σχήμα 1.2: 10 χώρες με περισσότερες κυβερνοεπιθέσεις το 2017.

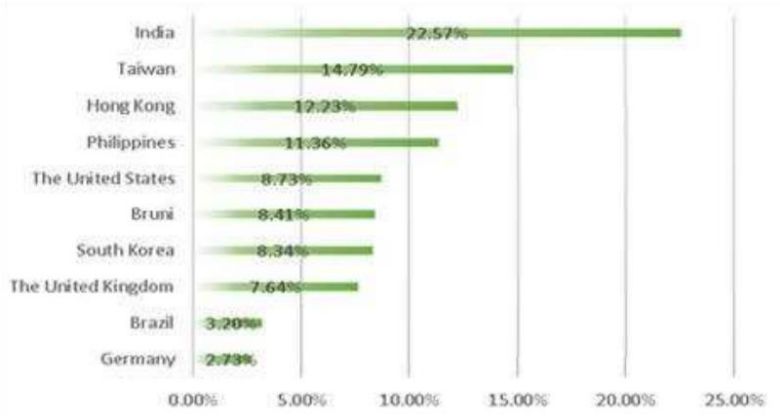
Ακόμα όταν εμφανίστηκε το WannaCry έχει μολύνει περίπου 200.000 υπολογιστές σε 150 χώρες. Πραγματοποίησε επίθεση ασφαλείας σε παλαιότερες εκδόσεις λειτουργικών συστημάτων Windows. Το WannaCry επηρέασε τη μεγαλύτερη ισπανική εταιρεία τηλεπικοινωνιών Telefonica ήταν η πρώτη που αναφέρει μια επίθεση ransomware WannaCry, ακόμα η μεγαλύτερη ρωσική τηλεπικοινωνιακή MegaFon είχε μολυνθεί , επίσης ο Ουγγρικός πάροχος τηλεπικοινωνιών με όνομα Telenor. Το εργοστάσιο παραγωγής της εταιρείας Nissan στο Σάντερλαντ, στην βορειοανατολική Αγγλία επηρεάστηκε και η αυτοκινητοβιομηχανία που ανήκουν στη Renault, όπως και η γερμανική εταιρεία τρένων Deutsche Bahn, μολύνθηκε επίσης το σύστημα IT των Ρωσικών σιδηροδρόμων και η Sberbank η μεγαλύτερη τράπεζα δανεισμού της Ρωσίας, τα εμπορικά κέντρα της Σιγκαπούρης και το Sandvik το Σουηδικό IT, όπως και κέντρα διανομής FedEx. Ορισμένα ιδρύματα κατάφεραν να αποτρέψουν με επιτυχία την επίθεση. Αντίθετα οι κυβερνητικοί φορείς και γραφεία σε πολλές χώρες μολύνθηκαν, όπως επίσης και εκατοντάδες κέντρα υγείας στο Ηνωμένο Βασίλειο που λειτουργούσαν με παλαιότερους υπολογιστές, το ρωσικό Υπουργείο Εσωτερικών είχε περίπου 1.000 υπολογιστές που είχαν επηρεαστεί, η ινδική αστυνομία στην πολιτεία Άντρα Πραντές είχε 18 διαφορετικές αστυνομικές μονάδες έκτος λειτουργιάς, το κινεζικό αστυνομικό τμήμα μετανάστευσης και τα γραφεία δημόσιας ασφάλειας επηρεάστηκαν από την επίθεση ransomware, επίσης το υπουργείο εξωτερικών της Βραζιλίας, όπως και η Κεντρική Τράπεζα της Ρωσιας[3] . Εκτιμήσεις για τη νομισματική ζημιά που προκλήθηκε από το WannaCry εξακολουθούν να αποτελούν σημείο συζήτησης πλησιάζοντας τα 4 δισεκατομμυρίων δολαρίων ΗΠΑ. Επιπλέων η κλοπή ταυτότητας από κεντρικούς πόρων για το 2018, ήταν περισσότερες από 300 στον κόσμο. Σύμφωνα με τον συγγραφέα John Pescatore. Η παραβίαση των δεδομένων επηρέασε ιατρικούς και υγειονομικούς οργανισμούς. Τα μητρώα ιατρικών ασθενών θεωρούνται εύκολοι

στόχοι για μια επίθεση, επειδή στην ασφάλεια συχνά δύνεται λιγότερη σημασία, λόγω της εστίασης στην περίθαλψη των ασθενών. Επίσης, οι ανιχνεύσεις ηλεκτρονικού ψαρέματος αυξήθηκαν παγκοσμίως κατά 250% από Ιανουάριο έως Δεκέμβριο 2018. Οι μέθοδοι έχουν εξελιχθεί, καθώς οι επιτιθέμενοι αναγκάζονται να παρακάμψουν όλο και πιο αποτελεσματικά εργαλεία και τεχνικές κατά του phishing [4]. Παγκοσμίως η Κίνα δέχτηκε τη μεγαλύτερη επίθεση όπως απεικονίζεται στο σχήμα 3 με το 36% του συνόλου περίπου.



Σχήμα 1.3: Παγκόσμια κατανομή των διευθύνσεων IP που έχουν προσβληθεί το 2018.

Επιπροσθέτως το 2019 ήταν το έτος με τη μεγαλύτερη κυβερνοεπίθεση σε ότι άφορα το ransomware στην υγειονομικής περίθαλψης και τον δημόσιου τομέα. Την επίθεση σε επίπεδο δικτύου. Το DDoS κατά το πρώτο και το δεύτερο τρίμηνο του έτους έφτασε 580 εκατομμύρια πακέτα ανά δευτερόλεπτο. Μέσα στο δεύτερο τρίμηνο του έτους τον DDoS επιθέσεων στην Κίνα έφτασε κατά 63,8%. Επίσης στις ΗΠΑ είχαμε επιθέσεις DDoS κατά 17,5 %. Έτσι η Κίνα και οι ΗΠΑ τοποθετήθηκαν ως οι δύο μεγαλύτεροι στόχοι για επιθέσεις DDoS εντός του δεύτερο τρίμηνο του έτους. Το 2019 παρατηρήθηκε ο υψηλός αριθμός επιθέσεων σε επίπεδο δικτύου κατά των επιχειρήσεων στην περιοχή της Ανατολικής Ασίας, κάνοντας την περιοχή εξαιρετικά επικίνδυνο από τον αριθμό των επιθέσεων. Η Ινδία βρίσκεται στην κορυφή της λίστας, όπως φαίνεται στο εικόνα 4 ήταν η χώρα που δέχτηκε τη μεγαλύτερη επίθεση. Η Ανατολική Ασία είχε το ποσοστό 77,7 % σε DDoS επιθέσεις [5].



Σχήμα 1.4: Οι 10 κορυφαίες χώρες που δέχθηκαν επιθέσεις σε επίπεδο δικτύου το 2019.

Τέλος η επίδραση της κοινωνικής μηχανικής ήταν εμφανής από την αρχή του 2020 όταν τα βλέμματα της πανδημίας του κορωνοϊού είχαν αρχίσει να προκαλούν ανησυχία. Οι κυβερνοεγκληματίες χρησιμοποιούν την πανδημία ως μέσω για να πραγματοποιήσουν κλοπή ιδιωτικών δεδομένων από ανυπεράσπιστα θύματα ώστε να χρησιμοποιήσουν. Ο κόσμος έπρεπε να παραμείνει στο σπίτι και να κάνει ηλεκτρονικά συναλλαγές, επομένως το έγκλημα στον κυβερνοχώρο εκμεταλλευτικέ αυτήν την απαίτηση για το διαδίκτυο. Επίσης τον Ιανουάριο του 2020, η ελληνική κυβέρνηση και ιδιαίτερα η ιστοσελίδες των κυβερνητικών υπηρεσιών έκτακτης ανάγκης δέχθηκαν επίθεση. Οι προεδρικές εκλογές των ΗΠΑ δέχθηκαν επίθεση, πιθανών να προκάλεσαν την αλλοίωση του αποτελέσματος. Τον Μάρτιο του 2020, ξεκίνησε η κυβερνοεπίθεση στο υπουργείου υγείας και ανθρωπίνων υπηρεσιών της Αμερικής χωρίς καμία επίπτωση. Στο Παρίσι μια ομάδα θεραπευτικών κέντρων δέχθηκε επίθεση με DDoS προσπάθησαν να απενεργοποιήσουν τις υποδομές ιατρικών ιδρυμάτων. Τέλος στη Γερμανία η εξ αποστάσεως εκπαίδευση δέχθηκε επίθεση όσων άφορα στα πρωτοβάθμια σχολεία.

1.2 Πρωτόκολλα TLS/SSL

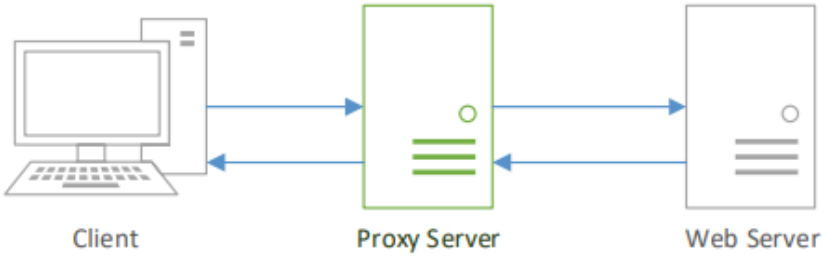
Στον σημερινό δικτυωμένο κόσμο, πολλές εφαρμογές χρειάζονται την ασφάλεια και την κρυπτογραφία για την ασφάλεια στην επικοινωνία, τα βασικά εργαλεία για την παροχή αυτής είναι το πρωτόκολλο SSL/TLS. Ο πρωταρχικοί στόχος του SSL/TLS είναι να χρησιμοποιηθεί για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας των δεδομένων κατά την μεταφορά, επίσης εμφανίστηκε και αναπτύχθηκε από τη Netscape. Τα κρυπτογραφικά πρωτόκολλα χρησιμοποιούνται για τη δημιουργία ασφαλών σηράγγων VPN όπου παρέχουν κρυπτογράφηση και έλεγχο της ταυτότητας, ώστε να χρησιμοποιηθεί για την αποτροπή πολυάριθμων τύποι επιθέσεων που βασίζονται στο δίκτυο, συμπεριλαμβανομένων των υποκλοπών, της πλαστογράφηση IP και παραποίηση. Η χρήση κρυπτογραφικών αλγορίθμων με ασφαλή και αξιόπιστο τρόπο είναι πολύ πιο δύσκολη από ότι πιστεύουν οι περισσότερους άνθρωποι. Οι αλγόριθμοι είναι απλώς δομικά στοιχεία σε κρυπτογραφικά πρωτόκολλα, ως αποτέλεσμα οι κρυπτογράφοι δυσκολεύονται να επινοήσουν πρωτόκολλα που αντιστέκονται σε όλες τις γνωστές επιθέσεις. Για το λογω που αναφέραμε παρουσιάζεται το γνωστό πρωτόκολλο Secure Socket Layer (SSL) που εμφανίστηκε το 1994, εν συνεχεία εξελίχθηκε και μετονομάστηκε σε Transport Layer Security (TLS) στο

επίσημο πρότυπο για την ασφάλεια όσων αφορά την μεταφοράς των δεδομένων. Κύριο χαρακτηριστικό του πρωτόκολλο είναι η ευελιξία του. Οι τρόποι λειτουργίας και οι στόχοι ασφάλειας που μπορούν εύκολα να διαμορφώνονται μέσω διαφορετικών σουιτών κρυπτογράφησης. Ακόμα το πρωτόκολλο είναι ιδιαίτερα χρήσιμο για συσκευές με περιορισμένους πόρους, όπως τα κινητά τηλέφωνα, επίσης χρησιμοποιεί καλύτερα την μπαταρία και άλλους πόρους λόγω του ότι επιλέγει επιλεκτικά τον βαθμό κρυπτογραφικής προστασίας για τη μετάδοση των δεδομένων. Επιπλέον επειδή είναι ένα γενικό πρωτόκολλο που μπορεί να διαπραγματευτεί πολλαπλά κανάλια ασφαλείας, μπορεί να καλύψει ευέλικτα τις απαιτήσεις από διάφορα τερματικά, διακομιστές, εφαρμογές και χρήστες. Τέλος υπάρχουν οι εκδόσεις SSL 2.0, 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2 και 1.3 [6, 7].

1.2.1 Ο ρόλο και η σημασία κατά την χρήσης των TLS/SSL proxies

Καθώς η περιήγηση στο διαδίκτυο γινόταν όλο και πιο δημοφιλής, η κρυπτογράφηση του δικτύου για την μεταφορά δεδομένων έγινε ανάγκη για την ασφαλή επικοινωνία με υπηρεσίες όπως τράπεζες και ιστοσελίδες ηλεκτρονικών αγορών. Επιπλέων βασίζεται κυρίως σε ψηφιακά πιστοποιητικά που υπογράφονται από τις αρχές έκδοσης πιστοποιητικών και των ενδιάμεσων αρχών. Αυτό το σύστημα επικύρωσης είναι αυτή τη στιγμή διακυβεύεται από τη χρήση διακομιστών μεσολάβησης TLS/SSL, που μπορεί να λειτουργήσει ως man-in-the-middle(MitM) για της TLS/SSL συνδέσεις. Ένας διακομιστής μεσολάβησης TLS/SSL μπορεί εκδώσει ένα υπο πιστοποιητικό για οποιονδήποτε ιστότοπο επισκέπτεται ο χρήστης, έτσι ώστε να δημιουργήσει μια κρυπτογραφημένη σύνδεση μέσω διακομιστή μεσολάβηση. Αυτός που εξουσιοδοτείται στη συνέχεια μπορεί να αποκρυπτογραφήσει και να παρακολουθήσει ή να τροποποιήσει όλη την κίνηση των χρηστών, πριν οδηγηθεί μέσω ενός δεύτερου κρυπτογραφημένου καναλιού στον επιθυμητό ιστότοπο. Οι διακομιστής μεσολάβησης TLS/SSL χρησιμοποιούνται για νόμιμους σκοπούς, όπως ο αποκλεισμός κακόβουλου λογισμικού, αλλά μπορεί επίσης να χρησιμοποιηθεί από κακόβουλες οντότητες για να πλήξουν το απόρρητο ή την ασφάλεια των τελικών χρηστών. Η πιο επικίνδυνη πτυχή των proxies TLS/SSL είναι ότι ο χρήστης αγνοεί εντελώς ότι η κρυπτογραφημένη κίνηση παρεμποδίζεται από έναν οργανισμό ή έναν εισβολέα. Η χρήση proxies TLS/SSL είναι αμφιλεγόμενη επειδή το πρόγραμμα περιήγησης στο λογισμικό εξακολουθεί να εμφανίζει ένα εικονίδιο κλειδαριάς κατά τη διάρκεια την περίοδο της σύνδεσης, παραπλανώντας τους χρήστες και διακυβεύοντας την ασφάλεια από άκρο σε άκρο. Για την ανίχνευση του διακομιστή μεσολάβησης, πρέπει να γίνει απόκτηση του πιστοποιητικού ενός πελάτη, όπως ένα πρόγραμμα περιήγησης ιστού, στη συνέχεια συγκρίνετε με το έγκυρο πιστοποιητικό που παρουσιάζεται από τον διακομιστή του πελάτη όπου πραγματοποιείται η επικοινωνία. Μια αναντιστοιχία δείχνει ότι κάποιου είδους εξουσιοδότησης, όπου είτε καλοπροαίρετα είτε κακοπροαίρετα, διακόπτει την κίνηση του πελάτη στον συγκεκριμένο διακομιστή. Για τον προσδιορισμό του επικράτηση στον διακομιστή TLS/SSL, πρέπει να γίνει επανάληψη αυτής της μέτρησης σε όσο το δυνατόν σε περισσότερα συστήματα. Επομένως η χρήση ενός μεσολαβητή έμοιαζε μονόδρομος επομένως δημιουργήθηκαν οι TLS/SSL proxies. Ο πρωταρχικός στόχος των πρωτοκόλλων TLS/SSL είναι να παρέχουν εμπιστευτικότητα,

αυθεντικότητα και ακεραιότητα των δεδομένων μεταξύ δύο εφαρμογών επικοινωνίας [8]. Στην ουσία το πρωτόκολλο TLS/SSL υποτίθεται ότι αποτρέπει την υποκλοπή της πληροφορίας από το δίκτυο, επομένως ένας πελάτης και ένας κεντρικός υπολογιστής να μπορούν να στέλνουν κρυπτογραφημένα μηνύματα ο ένας στον άλλο. Για τη διασφάλιση του πρωταρχικού στόχου της επικοινωνίας μεταξύ δυο σημείων. Επίσης για το HTTPS χρησιμοποιείται η θύρα 443. Έχουμε κρυπτογραφία ιδιωτικού-δημόσιου κλειδιού, τα πιστοποιητικά πρέπει να είναι ψηφιακά υπογεγραμμένα για να είναι έγκυρα, είτε από τον διακομιστή ή από μια αξιόπιστη αρχή[9].



Σχήμα 1.5: Παρουσιάζεται ένας proxy server TLS/SSL που επιτηρεί μια επικοινωνία μεταξύ Client και Web Server.

1.3 Αναφορά στους ερευνητικούς στόχους της διατριβής και συνεισφορά

Οι στόχοι και η συνεισφορά της είναι να καταδείξει την δικτυακή κίνηση των δεδομένων, ώστε να επιτευχτεί η ασφάλεια σε αυτά, είναι ένα ουσιαστικό βήμα για την παροχή σταθερών υπηρεσιών δικτύου και αποτελεσματικής διαχείρισης πόρων δικτύου, με κύριο στόχο να διασφαλιστεί η ακμαιότητα των δεδομένων, επίσης η εμπιστευτικότητα και η διαθεσιμότητα αυτών με την χρήση κατάλληλων πρωτοκόλλων και εξοπλισμού δικτύου. Τα προβλήματα ασφάλειας, όπως η διαρροή προσωπικών πληροφοριών, η παραβίαση του απορρήτου και η κλοπή λογαριασμού, έγιναν ακόμη πιο σοβαρά στον σύγχρονο κόσμο. Η κρυπτογραφημένη επισκεψιμότητα αυξάνεται με σκοπό την ασφαλή επικοινωνία. Κάτι που απαιτείται για την αποτελεσματική διαχείριση της κυκλοφορίας του δικτύου. Στην διπλωματική, θα πραγματοποιηθούν έλεγχοι ως προς τρόπο λειτουργίας του πρωτοκόλλου SSL/TLS όπου αφορά την κρυπτογραφημένη δικτυακή κίνηση, επίσης θα μελετηθούν οι πιο γνωστοί proxy SSL/TLS ως προς τα χαρακτηριστικά τους, όπου και θα συγκριθούν ως προς αυτά. Ακόμα θα γίνει αναφορά στον τρόπο εγκατάστασης, εάν κάποια εργαλεία λειτουργούν μόνο σε γραμμή εντολών ή έχουν και γραφική αναπαράσταση, την κρυπτογράφηση και αποκρυπτογράφηση τους, καθώς και τι μπορεί να επηρεάσει την ταχύτητα τους κατά την εκτέλεση αυτών.

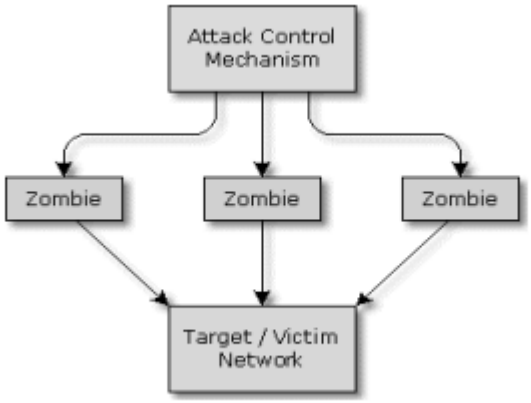
Κεφάλαιο 2
Βασική γνώση και βιβλιογραφική ανασκόπηση

Η κυβερνοασφάλεια είναι ένας κλάδος του οποίου η προέλευση καθορίζεται από την ύπαρξη κυβερνοεπιθέσεων. Οι κύριες απειλές που εμφανίζονται στα δίκτυα υπολογιστών, τα χαρακτηριστικά τους που δικαιολογούν την ανάπτυξη άμυνας όπως TLS/SSL proxies, τον ρόλο και τρόπο λειτουργίας αυτών, όπως επίσης και τα βασικά χαρακτηριστικά εργαλείων ανοιχτού κώδικα.

2.1.1 DDoS

Η επίθεση DDoS (Distributed DoS) στοχεύει σε συμφόρηση ή στην υπερχείλιση της προσωρινή μνήμη της κάρτας διασύνδεσης δικτύου, ώστε ο κεντρικός υπολογιστής να φαίνεται μη διαθέσιμος ή εκτός σύνδεσης σε όλους τους άλλους κεντρικούς υπολογιστές του δικτύου. Είναι γνωστή επίθεση όπου, η πρόσβαση σε πόρους διακυβεύεται από την αύξηση του χρόνου μετ' επιστροφής από την ώρα που πραγματοποιήθηκε η ζήτηση μιας πληροφορίας. Αυτή η αύξηση έχει ως αποτέλεσμα υψηλό ποσοστό πτώσης πακέτων. Σε μια επίθεση τέτοιου τύπου και η προσωρινή μνήμη της κάρτας διασύνδεσης ασύρματου δικτύου υπόκειται σε κορεσμο[10]. Επίσης για την προστασία του συστήματος από επίθεση άρνησης υπηρεσίας, θα πρέπει να περιέχει IDS όπως επίσης και η χρήση του μεσολαβητή proxy server για τον έλεγχο της δικτυακής κίνησης. Τέλος είναι απαραίτητο να διασφαλιστεί ότι υπάρχει πλεόνασμα

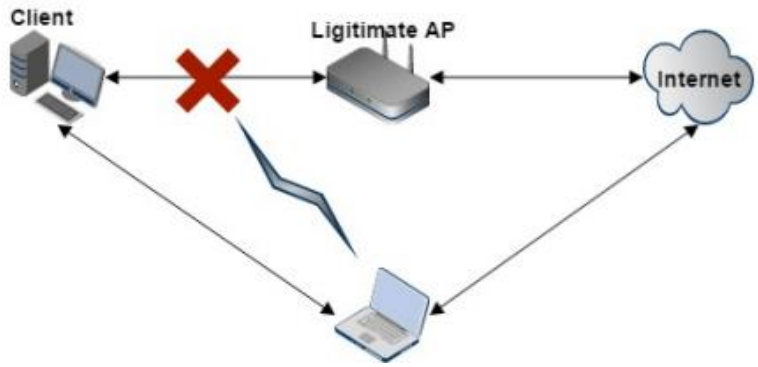
εύρους ζώνης σύνδεσης στο διαδίκτυο σε έναν οργανισμό. Όπως να υπάρχει μεγάλο εύρος ζώνης για αιτήματα κίνησης υπηρεσιών, βοηθά στην προστασία από επιθέσεις DDoS χαμηλής κλίμακας.



Σχήμα 2.1: Απεικονίζεται μια επίθεση DDoS Attack.

2.1.2 Man-in-the-middle (MitM)

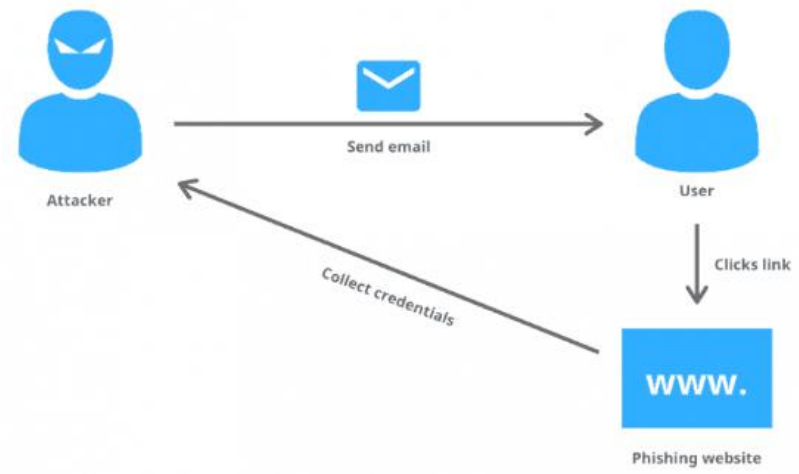
Μια επίθεση MitM λαμβάνει χώρα όταν μπαίνει ένας τρίτος μεταξύ της επικοινωνίας ενός πελάτη και ενός διακομιστή. Ο εισβολέας υποδύεται τόσο τον πελάτη όσο και τον διακομιστή και για να αποκτήσουν πρόσβαση στις πληροφορίες που ανταλλάσουν μεταξύ τους. Αυτού του είδους η επίθεση είναι ένας παράγοντα απειλής με σκοπό να αρπάξει, να στείλει και να λάβει το δεδομένα που προορίζονταν για κάποιον άλλον. Μια επίθεση MITM κάνει κατάχρηση της λειτουργίας των συναλλαγών σε πραγματικό χρόνο, επικοινωνία ή ανταλλαγή άλλων πληροφοριών. Ο διαφορετικοί τύποι επίθεσης man-in-the-middle περιλαμβάνει τα εξής: παραβίαση, πλαστογράφηση IP και απάντηση. Η ανίχνευση εισβολής στο σύστημα μπορεί να ρυθμιστεί, ώστε να αποφευχθεί η επίθεση man-in-middle. Βοηθά επίσης δίνοντας άμεσα ειδοποίηση εάν κάποιος προσπαθήσει να το κλέψει την ροή δικτύου. Μπορεί επίσης να χρησιμοποιηθεί εικονικό ιδιωτικό δίκτυο για την αποτροπή μιας τέτοιας επίθεσης. Αυτό βοηθά στη δημιουργία πρόσθετα ασφαλή επίπεδα κατά την πρόσβαση σε μια εταιρεία και εμπιστευτικό επίπεδο μέσω Wi-Fi[11].



Σχήμα 2.2: Παρουσιάζεται μια επίθεση man-in-the-middle.

2.1.3 Επιθέσεις phishing

Η επίθεση phishing είναι το μέσω αποστολής ψευδών μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχεται από αξιόπιστες πηγές. Ο κύριος στόχος αυτού του είδους της επίθεσης είναι να αποκτήσει πρόσβαση ο επιτιθέμενος σε προσωπικές και ιδιαίτερης σημασίας πληροφορίες. Η επίθεση phishing είναι μια μορφή της κοινωνικής μηχανικής. Είναι με τη μορφή e-mail που αποτελείται από ενσωματωμένους υπερσυνδέσμους που φορτώνουν κακόβουλο λογισμικό στο σύστημά. Μερικές φορές αυτή η σύνδεση οδηγεί επίσης σε παράνομο ιστότοπο που υπάρχει κακόβουλο λογισμικό, που μπορεί να επηρεάσει την λειτουργιά του συστήματος. Προκειμένου να μειωθεί ο κίνδυνος επίθεσης phishing, είναι κρίσιμο να πραγματοποιηθεί ανάλυση των επικεφαλίδων στα ηλεκτρονικά μηνύματα. Επιπλέον, δίνοντας επίγνωση μεταξύ των εργαζομένων του οργανισμού με σκοπό να υπάρξει μετριασμός μια τέτοιας επίθεσης κατά κάποιο βαθμό[12].

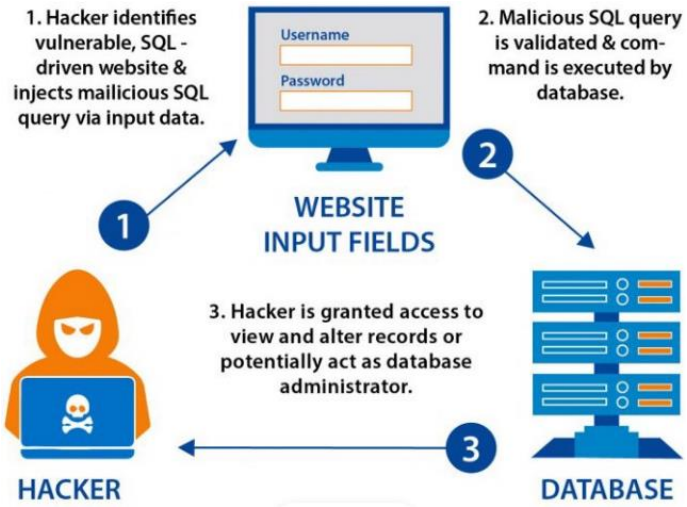


Σχήμα 2.3: Εκτυλίσσεται μια επίθεση phishing attack

2.1.4 Επίθεση SQL Injection

Η SQL (Structured Query Language) είναι μια γλώσσα υπολογιστή που χρησιμοποιείται για την αποθήκευση, το χειρισμό και την ανάκτηση δεδομένων που είναι αποθηκευμένα σε μια βάση δεδομένων. Η γλώσσα SQL χρησιμοποιεί εντολές όπως select, update, delete για να εκτελεστεί μια απαιτούμενη εργασία. Η SQL μπορεί επίσης να εκτελεί ερωτήματα στη βάση δεδομένων, να εισαγάγει εγγραφές σε αυτήν όπως και να δημιουργήσει νέους πίνακες. Η επίθεση SQL Injection κάνει χρήση κακόβουλου κώδικα, για να πραγματοποιηθεί πρόσβαση σε πληροφορίες της βάσης δεδομένων στο backend. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν οποιονδήποτε ευαίσθητο οργανισμό λεπτομέρειες, προσωπικά δεδομένα πελάτη και χρήστη. Αυτό μπορεί να έχει ως αποτέλεσμα την παράνομη προβολή των δεδομένων του χρήστη, η την διαγραφή των δεδομένων του πίνακα και μη εξουσιοδοτημένη επίθεση στη βάση δεδομένων. Ένας εισβολέας που θέλει να εκτελέσει επίθεση SQL Injection θα πραγματοποιήσει ένα τυπικό ερώτημα στην βάση, ώστε να εκμεταλλευτεί τα τρωτά σημεία. Υπάρχουν αρκετές αποτελεσματικούς τρόπους πρόληψης και προστασίας από επιθέσεις SQL Injection. Μπορεί να πραγματοποιηθεί επικύρωση εισόδου για αναγνώριση παράνομης

εισροής χρηστών. Αυτή η μέθοδος δεν είναι πολύ κατάλληλη όσο η χαρτογράφηση όλων των νομικών και παράνομων εισροών δεν είναι εφικτές. Εξαιτίας αυτού, συνήθως ένα τείχος προστασίας κατά την είσοδο στο διαδίκτυο μας προστατεύει από τέτοιες επιθέσεις σημαντικά. Επιπλέων η αναγνώριση υπογραφής, η IP και άλλες μέθοδοι ασφάλειας μπορούν επίσης να χρησιμοποιηθούν για τον εντοπισμό και τον αποκλεισμό της SQL Injection[13].



Σχήμα 2.4: Απεικόνιση μια επίθεση SQL Injection.

2.1.5 Malware Attack

Η επίθεση Malware Attack είναι μια κατηγορία κυβερνοεπιθέσεων στην οποία Το κακόβουλο λογισμικό εγκαθίσταται στον υπολογιστή του χρήστη χωρίς καμία συναίνεση από αυτόν. Επίσης έχει την ονομασία και ως ιό. Τα κακόβουλα προγράμματα έχουν πρόσβαση σε ιδιωτικό δίκτυο, προκαλούν την διακοπή της υπολογιστικής λειτουργίας, πραγματοποιούν κλοπή ευαίσθητων πληροφοριών ή οποιαδήποτε άλλα δεδομένα που αφορούν τους χρήστες. Σήμερα ένα κακόβουλο λογισμικό στοχεύει περισσότερο σε επιχειρηματικές ή οικονομικές πληροφορίες. Ορισμένοι τύποι κακόβουλων λογισμικών είναι οι ακόλουθοι[14]:

- Ιός: Ένα κακόβουλο λογισμικό που συνδέεται με οποιοδήποτε πρόγραμμα υπολογιστή, αντιγραφή και τροποποίηση κωδικούς όταν εκτελείται. Μπορεί να εξαπλωθεί είτε με λήψη από ένα αρχείο ή από εκτέλεση οποιουδήποτε προγράμματος.
- Worms: εξαπλώνονται σε υπολογιστές ή δίκτυα μέσω συνημμένων e-mail. Αυτό μπορεί να οδηγήσει ακόμα και σε άρνηση παροχής υπηρεσιών από τους πόρους του συστήματος.
- Trojans: Ένα από τα πιο επικίνδυνα κακόβουλα προγράμματα που έχει κακόβουλη λειτουργία. Κρύβεται σε ένα χρήσιμο πρόγραμμα ώστε να μην είναι εύκολος ο εντοπισμός του.

- Ransomware: Ένας τύπος κακόβουλου λογισμικού που κλειδώνει τα δεδομένα του χρήστη και απαιτεί την καταβολή χρημάτων, ώστε να μπορέσει χρηστής να τα διαχειριστεί εκ νέου. Είναι πολύ δύσκολο να αποτραπεί παρόλο που ο κώδικας είναι απλός.
- Spyware: Ένα είδος κακόβουλου λογισμικού που με την εγκατάσταση του επιθεωρεί την δραστηριότητα του χρήστη χωρίς την συναίνεση του.

2.2 TLS/SSL proxies – ρόλος και λειτουργία

Το πρωτόκολλο SSL και ο διάδοχό του TLS χρησιμοποιούνται ευρέως για την παροχή ασφαλούς διαύλου επικοινωνίας μεταξύ ενός πελάτη και ενός διακομιστή στο διαδίκτυο, ως αποτέλεσμα έχουν γίνει στάνταρ πρότυπα για ασφάλεια στο επιπέδου μεταφοράς [15]. Ο όρος "SSL" χρησιμοποιείται για να αναφέρεται τόσο στο SSL όσο και στο TLS. Το SSL τρέχει πάνω από κάποιο αξιόπιστο πρωτόκολλο μεταφοράς όπως το TCP, ενώ βρίσκεται κάτω από διάφορα είδη πρωτόκολλων στο επιπέδου εφαρμογής. Πρωτόκολλα επιπέδου εφαρμογής όπως HTTP, TELNET, FTP κ.λπ. μπορούν να εκτελούνται με διαφάνεια με TLS/SSL. Ωστόσο το TLS/SSL χρησιμοποιείται ευρέως για τη διασφάλιση της κυκλοφορίας στο HTTP, συγκεκριμένα στο HTTP Secure(HTTPS). Η διαδικασία εκτέλεσης του TLS/SSL αποτελείται από δύο στάδια. Η δημιουργία σύνδεσης TLS/SSL και την ασφαλή μετάδοση των δεδομένων της εφαρμογής. Αν και τα TLS/SSL είναι τα πιο δημοφιλές πρωτόκολλα που παρέχονται σε ένα κανάλι μετάδοσης μεταξύ πελάτη και διακομιστή στο διαδίκτυο, λογω των κρυπτογραφικών λειτουργιών που έχουν οι λειτουργίες δημόσιου κλειδιού[16]. Το ποσοστό δημοτικότητας μέσω του διαδικτύου είναι μάλλον χαμηλό. Στην πραγματικότητα στην καθημερινή ζωή των ανθρώπων ένα μικρό μέρος αυτών μεταδίδει σε κρυπτογραφημένο κείμενο, εκ των οποίων είναι η κίνηση ευαίσθητων πληροφοριών. Μέχρι στιγμής, ο αριθμός των ιστοσελίδων στο διαδίκτυο έχουν ξεπεράσει τα 850 εκατομμύρια. Ωστόσο λιγότερα από 3 εκατομμύρια από αυτές προσφέρουν TLS/SSL ασφάλεια [17]. Τα αποτελέσματα μιας άλλης έρευνας [18] δείχνουν ότι μόνο μεταξύ της Alexa και με τους κορυφαίους 1.000.000 ιστότοπος περίπου 450.000 προσφέρουν ασφάλεια TLS/SSL. Παρ' όλα αυτά, σήμερα το SSL τείνει να επιτυγχάνει καθολικότητα εντός ολόκληρου του εύρος του διαδικτύου. Όλο και περισσότερο η κίνηση μεταφέρεται ως κρυπτογραφημένο κείμενο. Πολλές έρευνες και έργα αφιερώνονται στη βελτίωση της απόδοσης εκτέλεσης του TLS/SSL, ξεκινώντας από τις οδηγίες επιτάχυνσης για τους κρυπτογραφικούς αλγόριθμους[19] βελτιστοποιώντας τα πρωτόκολλα TLS/SSL κατά την εκφόρτωση και κατά την επανάληψη συνεδρίας . Η επανάληψη συνεδρίας είναι ένας μηχανισμός που παρέχεται από τα πρωτόκολλα, ώστε να επιτρέπει στα δύο μέρη να επανασυνδεθούν χρησιμοποιώντας μια προηγούμενη σύνδεση.

Το SSL/TLS παρέχει πολλαπλούς στόχους ασφαλείας όπως:

- Έλεγχος ταυτότητας – με τη χρήση ψηφιακών πιστοποιητικών
- Εμπιστευτικότητα – με τη χρήση κρυπτογράφησης
- Ακεραιότητα – με τη χρήση κωδικών ελέγχου ταυτότητας μηνυμάτων (MAC).
- Προστασία επανάληψης – με τη χρήση αριθμών ακολουθίας

2.2.1 Δομή πρωτοκόλλων

Τα SSL/TLS είναι και τα δύο πρωτόκολλα πολλαπλών επιπέδων, αλλά όλα βασίζονται στο πρωτόκολλο εγγραφής που αποτελείται από μια αρχιτεκτονική δύο φάσεων:

- Φάση διαπραγμάτευσης και σύνδεση
- Φάση εφαρμογής

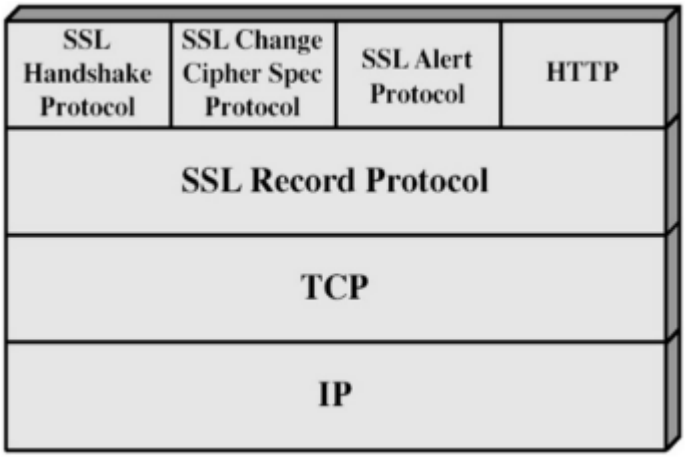
Κατά τη φάση της σύνδεσης, οι παράμετροι ασφαλείας και οι σουίτες κρυπτογράφησης είναι υπό διαπραγμάτευση, καθώς και τη δημιουργία ενός μέσου ανταλλαγής κλειδιών. Επίσης η σύνδεση εξαρτάται από τη σουίτα κρυπτογράφησης. Το υλικό που απαιτείται για μια ασφαλή επικοινωνία προέρχεται από το MasterSecret. Μετά την ολοκλήρωση της φάσης ανταλλαγής μηνυμάτων, ώστε να πραγματοποιηθεί η σύνδεση, τα δύο τελικά σημεία αποτελούν αντικείμενο διαπραγμάτευσης στην ίδια κρυπτογραφική κατάσταση. Το πρωτόκολλο συνεχίζεται με τη φάση της αίτησης όπου βρίσκονται τα πραγματικά δεδομένα, ώστε να ανταλλάσσονται με ασφάλεια μέσω του καθιερωμένου ασφαλούς κανάλι επικοινωνίας.

2.2.2 Σχεδιασμός πρωτόκολλων

Το πρωτόκολλο TLS και ο προκάτοχός του SSL αντιπροσωπεύουν μια εξελιγμένη, εξαιρετικά αρθρωτή αρχιτεκτονική. Ο σχεδιασμός του πρωτοκόλλου είναι πολυεπίπεδο και αποτελείται από διαφορετικά υπο-πρωτόκολλα, καθώς και από διαμορφώσιμη αντικαταστάσιμης αλγοριθμικής κρυπτογράφησης. Ειδικότερα τα πρότυπα ορίζουν τα ακόλουθα υπο-πρωτόκολλα:

- Πρωτόκολλο εγγραφής
- Πρωτόκολλο ώστε να πραγματοποιηθεί η σύνδεση (Handshake)
- Πρωτόκολλο ChangeCipherSpec
- Πρωτόκολλο ειδοποίησης (Alert)
- Πρωτόκολλο Δεδομένων Εφαρμογής (HTTP)

Όλα τα μηνύματα πρέπει τουλάχιστον να ενσωματωθούν στο πρωτόκολλο εγγραφής όπως απεικονίζεται παρακάτω.



Σχήμα 2.5: Απεικόνιση η ενθυλάκωση των πρωτοκόλλων.

Το επίπεδο εγγραφής, είναι ένα επίπεδο πρωτοκόλλου επικοινωνίας που δέχεται μια ροή από byte και χωρίζει αυτά τα byte σε μπλοκ τα οποία υποβάλλονται σε επεξεργασία και έτσι παραδίδονται στο TCP. Κατά το πρώτο στάδιο της επικοινωνίας (Handshake), η επεξεργασία δεν περιλαμβάνει κρυπτογράφηση ή προστασία ακεραιότητας[20].

2.2.3 Διαχείριση session

Η διαχείριση της συνεδρίας είναι ουσιαστικό μέρος του πρωτοκόλλου SSL/TLS. Οι συνεδρίες περιλαμβάνουν μια συγκεκριμένη υπό διαπραγμάτευση για την διαμόρφωση μιας καθιερωμένης σύνδεσης . Επίσης και τους κρυπτογραφικούς αλγόριθμους καθώς και το βασικό MasterSecret. Μια σύνδεση από την άλλη πλευρά, αναφέρεται σε ένα κανάλι επικοινωνίας. Οι συνεδρίες μπορούν να συνεχιστούν και να επαναχρησιμοποιηθούν για διαφορετικές συνδέσεις, με συντόμευση της φάσης διαπραγμάτευσης. Σίγουρα αυτό έρχεται με κίνδυνο σε περίπτωση που παραβιαζόταν το καθιερωμένο MasterSecret αλλά η άλλη πλευρά απλοποιεί τη διαδικασία δημιουργίας καναλιού. Μια επανάληψη συνεδρίας δεν περιορίζεται μόνο σε μεμονωμένα κανάλια, αλλά μπορεί επίσης να χρησιμοποιηθεί για διαχείριση πολλαπλών συνδέσεων παράλληλα, όλες βασισμένες στις ίδιες παραμέτρους. Είναι σημαντικό να σημειωθεί ότι μόνο το MasterSecret επαναχρησιμοποιείται, ενώ το κλειδί εκτελείται για κάθε συνεδρία που συνεχίζεται, για τη δημιουργία νέων βραχυπρόθεσμων κλειδιών. Αυτό σημαίνει ότι κάθε συνεδρία συνεχίζεται ανεξάρτητα από το εάν είναι παράλληλη ή διαδοχική, κρυπτογραφείται ή αποκρυπτογραφείται με διαφορετικό βασικό υλικό. Αυτό το γεγονός σχετίζεται με το κλειδί, είναι μια διαδικασία παραγωγής που εξαρτάται από τις τυχαίες τιμές που παρέχονται από τον πελάτη και τον διακομιστή, οι όποιες αποστέλλονται ως μέρος των δύο πρώτων μηνυμάτων σε μια σύνδεση. Οι περίοδοι σύνδεσης προσδιορίζονται από αναγνωριστικά συνεδρίας που αποτελούν επίσης μέρος των δύο πρώτων μηνυμάτων κατά την επικοινωνία (handshake)[21].

- SSL/TLS συνέδρια (Session): Αναφέρεται σε ένα σύνολο καθιερωμένων κρυπτογραφικών παραμέτρων όπως την σουίτα κρυπτογράφησης και το MasterSecret, που σχετίζονται με ένα αναγνωριστικό μια σύνδεσης. Μια

συνεδρία μπορεί να επαναχρησιμοποιηθεί, αλλά το βασικό υλικό θα διαφέρει κάθε φορά.

- SSL/TLS σύνδεση (connection): Αναφέρεται σε οποιαδήποτε σύνδεση SSL/TLS χωρίς καθορισμό συγκεκριμένων παραμέτρων.
- SSL/TLS κανάλι (channel): Αναφέρεται σε μια συγκεκριμένη σύνδεση SSL/TLS με ένα συγκεκριμένο σύνολο κλειδιών και κρυπτογραφικών παραμέτρων. Γενικά ένα κανάλι SSL/TLS είναι μοναδικό, ακόμα κι αν αυτό δημιουργήθηκε με την επαναχρησιμοποίηση μιας υπάρχουσας περιόδου του SSL/TLS.

2.2.4 Εμπιστευτικότητα

Πολλοί από τους προαναφερθέντες στόχους ασφαλείας βασίζονται σε μια σχέση εμπιστοσύνης μεταξύ των εταίρων μιας επικοινωνίας. Συνήθως αυτή η σχέση εμπιστοσύνης βασίζεται σε ψηφιακά πιστοποιητικά, υπογεγραμμένα από αξιόπιστες αρχή έκδοσης πιστοποιητικών (CA). Η βασική ιδέα είναι ότι κάθε συνεργάτης επικοινωνίας ή τουλάχιστον ένας από αυτούς αποδεικνύει την ταυτότητά του, εκτελώντας εργασίες ως νόμιμος κάτοχος του ψηφιακού πιστοποιητικού, ώστε να ολοκληρώσει με επιτυχία. Η έννοια των ψηφιακά υπογεγραμμένων πιστοποιητικών και η ιεραρχική πιστοποιημένη εμπιστοσύνης είναι γνωστή ως υποδομή δημοσίου κλειδιού (PKI). Στο πιο κοινό σενάριο σε έναν ιστότοπο είναι η σχέση εμπιστοσύνης, όπου σημαίνει ότι ο πελάτης ενδιαφέρεται να αποδείξει την ταυτότητα του διακομιστή του , αλλά ο διακομιστής δεν απαιτεί έλεγχο ταυτότητας του πελάτη. Κατά την περιήγηση στον ιστότοπο, αυτό είναι ένα πολύ κοινό επίπεδο εμπιστοσύνης, όπως ένας χρήστης ενδιαφέρεται για γνήσια περιεχόμενο, αλλά ο διακομιστής web δεν ενδιαφέρεται ποιος ζητά αυτό το περιεχόμενο. Παρόλο που τα σύγχρονα προγράμματα περιήγησης υποστηρίζουν αμοιβαίο έλεγχο ταυτότητας, έλεγχο ταυτότητας πελάτη γίνεται κυρίως σε υψηλότερα επίπεδα στη στοίβα πρωτοκόλλου. Ο λόγος είναι κυρίως η απλότητα, γιατί είναι πιο εύκολο για έναν πελάτη να ορίσει τον δικό του κωδικό πρόσβασης παρά να δημιουργήσει ένα δικό του ψηφιακό πιστοποιητικό και να το πάρει υπογεγραμμένο από αξιόπιστη αρχή πιστοποίησης. Η εμφάνιση της αξιοπιστίας των ιστοσελίδων, όπου τα προγράμματα περιήγησης ιστού είναι μια πρόκληση, περίπλοκη εργασία και υπόκειται σε συνεχή έρευνα [22, 23].

2.3 Εργαλεία ανοιχτού κώδικα TLS/SSL proxy

Στην συνεχεία παρουσιάζονται οι δημοφιλείς υλοποιήσεις σε SSL/TLS proxies, όπου θα γίνει μια λεπτομερή ανάλυση στον τρόπο λειτουργίας των εργαλείων όπου χρησιμοποιούν οι proxy, ακόμα θα υπάρξει μια ταξινόμηση με βάση τα χαρακτηριστικά τους. Λόγω του μεγάλου αριθμού που παρουσιάζουν, η ακόλουθη αναφορά απέχει πολύ από το να είναι πλήρης, ως αποτέλεσμα επισημαίνονται μόνο οι πιο συνηθισμένοι. Δεδομένου ότι σχεδόν όλες οι αναφερόμενες υλοποιήσεις ενημερώνονται συνεχώς, οι λεπτομέρειες που παρέχονται μπορεί να ξεπεραστούν πολύ σύντομα.

2.3.1 OpenSSL

Το OpenSSL είναι ένα πρόγραμμα ανοιχτού κώδικα που αποτελείται από μια κρυπτογραφική βιβλιοθήκη και μια εργαλειοθήκη SSL. Το OpenSSL Project είναι μια συλλογική προσπάθεια για την ανάπτυξη μιας ισχυρής, πλήρους και ανοιχτού κώδικα εργαλειοθήκης που εφαρμόζει τα πρωτόκολλα Secure Sockets Layer (SSL) και Transport Layer Security (TLS) καθώς και πλήρους ισχύος βιβλιοθήκες κρυπτογραφίας γενικού σκοπού. Το OpenSSL είναι ένα de facto πρότυπο το οποίο έχει μακρά ιστορία. Ο κώδικας ξεκίνησε αρχικά τη ζωή του το 1995 με το όνομα SSLeay,1 όταν αναπτύχθηκε από τον Eric A. Young και τον Tim J. Hudson. Το OpenSSL γεννήθηκε τις τελευταίες μέρες του 1998, όταν ο Eric και ο Tim σταμάτησαν τη δουλειά τους στο SSLeay για να δουλέψουν σε μια εμπορική εργαλειοθήκη SSL. Σήμερα, το OpenSSL είναι πανταχού παρόν από την πλευρά του διακομιστή. Είναι ενδιαφέρον ότι τα προγράμματα περιήγησης τείνουν να χρησιμοποιούν άλλες βιβλιοθήκες. Τα εργαλεία γραμμής εντολών που παρέχονται από το OpenSSL χρησιμοποιούνται συνήθως για τη διαχείριση κλειδιών και πιστοποιητικών. Το OpenSSL διαθέτει διπλή άδεια υπό τις άδειες OpenSSL και SSLeay. Και οι δύο είναι τύπου BSD. Η άδεια είναι πηγή διαμάχης για πολύ καιρό, επειδή καμία από τις άδειες δεν θεωρείται συμβατή με την οικογένεια αδειών GPL. Είναι πλήρως υλοποιημένη σε γλώσσα προγραμματισμού C και υποστηρίζει SSL 2.0/3.0, TLS 1.0/1.1/1.2 και Datagram Transport Layer Security (DTLS) 1.0, είναι ουσιαστικά δύο εργαλεία όπου αποτελείται από μια βιβλιοθήκη κρυπτογραφίας και μια εργαλειοθήκη SSL. Οι υλοποιήσεις είναι διαθέσιμες σε Linux και λειτουργικό σύστημα (OS) Windows, επίσης χρησιμοποιείται από πολλές γνωστές εφαρμογές ειδικά στον κόσμο του Unix. Εκτός από τα SSL/TLS, το OpenSSL περιέχει τις δικές του υλοποιήσεις κρυπτογραφικών αλγορίθμων και λειτουργικότητας χρησιμότητας τα πιστοποιητικά X509. Η βιβλιοθήκη κρυπτογραφίας είναι σε θέση να αποκωδικοποιεί, να δημιουργεί και να υπογράφει πιστοποιητικά, όπως επίσης και αίτημα υπογραφής πιστοποιητικού (CSR). Τέλος, διατίθενται διαφορετικές μορφές κωδικοποίησης και δημιουργία κλειδιών. Εξαιτίας αυτής της πρόσθετη λειτουργικότητα, το OpenSSL μπορεί να θεωρηθεί ως ένα πλήρως εξοπλισμένο εργαλείο δημιουργίας και διαχείρισης (Public Key Infrastructure). Για βασικούς σκοπούς δοκιμών και εντοπισμού σφαλμάτων, το OpenSSL κυκλοφορεί με στοιχειώδεις δυνατότητες του πελάτη και του διακομιστή, κάτι που έχει ιδιαίτερη σημασία για τους ελεγκτές διείσδυσης και διαχειριστές συστήματος[24].

2.3.2 WolfSSL

Είναι άλλη μια εφαρμογή ανοιχτού κώδικα, υποστηρίζει τη γλώσσα προγραμματισμού C ως κύρια. Υποστηρίζει επίσης πολλές άλλες γλώσσες, όπως η Java (wolfSSL JNI), η C# (wolfSSL C#) και σε Python. διατίθεται υλοποιήσεις σε Unix και σε λειτουργικά συστήματα Windows, Mac os, επίσης χρησιμοποιείται από πολλές γνωστές εφαρμογές ειδικά στον κόσμο του Unix. Υποστηρίζει έκδοση SSL 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2 και 1.3, ακόμα υποστήριξη DTLS 1.0, 1.2 και 1.3. Υπάρχει συμβατότητα με OpenSSL. Χρησιμοποιεί για κατακερματισμό MD2, MD4, MD5, SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, SHA-3, RIPEMD-160 και Poly1305. Για την επαλήθευση της

κρυπτογράφησης χρησιμοποιεί AES (CBC, CTR, OFB, XTS, GCM, CCM, GMAC, CMAC), Camellia, DES, 3DES, ARC4 και ChaCha20. Επιπλέον για αλγόριθμοι δημόσιου κλειδιού χρησιμοποιεί RSA, DSA, DH, EDH, ECDH-ECDSA, ECDHE-ECDSA, ECDH-RSA, ECDHE-RSA και NTRU. Μπορεί και δημιουργεί υπογεγραμμένα πιστοποιητικών X.509v3 RSA και ECC. Για της βιβλιοθήκες κρυπτογράφησης των πιστοποιητικών υποστηρίζει επεκτάσεις TLS[25].

2.3.3 GnuTLS

Είναι άλλη μια εφαρμογή ανοιχτού κώδικα που υλοποιείται στο C. Υποστηρίζει SSL 3.0, TLS 1.0/1.1/1.2/1.3 και DTLS 1.0. Διαθέσιμη για macOS, Linux και Windows. Υποστήριξη το Online Certificate Status Protocol (OCSP), μεθόδους δημόσιου κλειδιού, συμπεριλαμβανομένου των ελλειπτικών καμπυλών και RSA, επίσης μεθόδους ελέγχου ταυτότητας κωδικού πρόσβασης και κλειδιού, όπως πρωτόκολλα SRP και PSK. Ακόμα παρέχει υποστήριξη για όλους τους ισχυρούς αλγόριθμους κρυπτογράφησης, συμπεριλαμβανομένων των AES και Camellia. Επιπλέων διατίθεται υλοποιήσεις σε Unix και λειτουργικά συστήματα Windows. Χρησιμοποιείται από πολλές γνωστές εφαρμογές ειδικά στον κόσμο του Unix. Τα εργαλεία γραμμής εντολών του GnuTLS αποστέλλονται, όπως και του OpenSSL, με υποτυπώδη εργαλεία πελάτη και διακομιστή, καθώς και βοηθητικά προγράμματα για τη διαχείριση πιστοποιητικών X509. Το GnuTLS δεν αποστέλλεται με δικές του υλοποιήσεις κρυπτογραφικών αλγορίθμων, αλλά βασίζεται στο libgcrypt από προεπιλογή[26].

2.3.4 Mitmproxy

Είναι μια εφαρμογή ανοιχτού κώδικα δωρεάν διαθέσιμη για macOS, Linux και Windows. Υποστηρίζει έκδοση SSL 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2 και 1.3. Είναι ανοιχτού κώδικα, είναι γραμμένη σε γλώσσα προγραμματισμού python. Είναι ένας διακομιστής μεσολάβησης Man-in-the-Middle με δυνατότητα SSL/TLS. Επίσης, εντοπίζει σφάλματα, πραγματοποιεί δοκιμές, μετρήσεις απορρήτου, και δοκιμές διείσδυσης. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση, την επιθεώρηση, την τροποποίηση και την επανάληψη της κυκλοφορίας ιστού όπως HTTP/1, HTTP/2, WebSockets ή άλλα πρωτόκολλα που προστατεύονται από SSL/TLS[27].

2.3.5 SSLsplit

Το εργαλείο SSLsplit είναι ανοιχτού κώδικα, είναι γραμμένο σε γλώσσα προγραμματισμού C, επομένως καθιστά την εκτέλεση του πολύ γρήγορη. Διαθέσιμο για Linux και Windows. Ανάλογα με την έκδοση του OpenSSL, το SSLsplit υποστηρίζει SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 και προαιρετικά SSL 2.0, σε σύγκριση με άλλα εργαλεία, τα οποία παρέχουν μόνο υποστήριξη για HTTPS και HTTP, επίσης χρησιμοποιείται τόσο για IPv4 όσο και για IPv6. Για την σύνδεση SSL και HTTPS, το SSLsplit δημιουργεί μια πλάστη υπογράφει με το πιστοποιητικό X509v3 με βάση τον αρχικό διακομιστή. Η ανακατεύθυνση της κυκλοφορίας γίνεται από το τείχος προστασίας του linux που ονομάζεται iptables και ip6tables για ipv6 στη διεύθυνση και τη θύρα του SSLsplit. Για την επισκεψιμότητα HTTPS μέσω ipv4, είναι η διεύθυνση

0.0.0.0 και η θύρα 10443, για κίνηση μέσω ipv6, στη διεύθυνση ::1 και στη θύρα 10443. Οι ίδιες διευθύνσεις χρησιμοποιούνται για την κυκλοφορία HTTP, ωστόσο, υπάρχει διαφορά στον αριθμό της θύρας που χρησιμοποιείται 10080. Στον NAT χρησιμοποιείται το proxy, λόγω της υποστήριξης ipv4 και ipv6. Είναι το μόνος με ipv6 υποστήριξη σε Linux OS. Για την δημιουργία κλειδιών CA χρησιμοποιεί ένα κλειδί εξουσιοδότησης από το SSL split. Υποστηρίζει πλήρως την Ένδειξη ονόματος διακομιστή (SNI) και μπορεί να λειτουργήσει με κλειδιά RSA, DSA και ECDSA και σειρές κρυπτογράφησης DHE και ECDHE. Το SSLsplit υποστηρίζει πιστοποιητικά CN με πρόθεμα NULL και μπορεί να απορρίψει αιτήματα OCSP με γενικό τρόπο. Για συνδέσεις HTTP και HTTPS, το SSLsplit καταργεί τις κεφαλίδες απόκρισης για το HPKP προκειμένου να αποτρέψει το καρφίτσωμα του δημόσιου κλειδιού, για το HSTS που επιτρέπει στον χρήστη να αποδέχεται μη αξιόπιστα πιστοποιητικά και τα εναλλακτικά πρωτόκολλα για να αποτρέψει τη μετάβαση σε QUIC/SPDY. Ως πειραματικό χαρακτηριστικό, το SSLsplit υποστηρίζει τους μηχανισμούς STARTTLS με γενικό τρόπο[28].

2.3.6 Polarproxy

Το PolarProxy είναι ένας διακομιστής μεσολάβησης TLS που εξάγει την αποκρυπτογραφημένη κίνηση TLS ως αρχεία PCAP. Ο PolarProxy δεν παρεμβαίνει με κανένα τρόπο στα δεδομένα, απλώς παίρνει την εισερχόμενη ροή TLS, την αποκρυπτογραφεί και την κρυπτογραφεί εκ νέου με σκοπό να την προωθήσει στον προορισμό. Εξαιτίας αυτού, το PolarProxy μπορεί να χρησιμοποιηθεί ως γενικός διακομιστής αποκρυπτογράφησης TLS για σχεδόν οποιοδήποτε πρωτόκολλο που χρησιμοποιεί κρυπτογράφηση TLS, συμπεριλαμβανομένων των HTTPS, HTTP/2, DoH, DoT, FTPS, SMTPS, IMAPS, POP3S και SIP-TLS. Έχει σχεδιαστεί κυρίως για την επιθεώρηση κρυπτογραφημένης κίνησης από κακόβουλο λογισμικό, όπως το botnet που χρησιμοποιεί HTTPS για την εντολές του. Άλλες δημοφιλείς περιπτώσεις χρήσης του PolarProxy είναι η επιθεώρηση κρυπτογραφημένης κίνησης από συσκευές IoT και άλλα ενσωματωμένα προϊόντα, ακόμα η ανάλυση κρυπτογραφημένης κίνησης στα κινητά τηλέφωνα και tablet. Το γεγονός ότι το PolarProxy εξάγει την αποκρυπτογραφημένη κίνηση σε αποκρυπτογραφημένη μορφή χωρίς κεφαλίδες TLS, επιτρέπει επίσης στους χρήστες να επιθεωρούν την αποκρυπτογραφημένη κίνηση με προϊόντα που δεν υποστηρίζουν αποκρυπτογράφηση TLS, όπως προϊόντα ανίχνευσης εισβολής και δικτύου όπως Wireshark και NetworkMiner. Το PolarProxy δημιουργεί ένα μοναδικό πιστοποιητικό CA για κάθε εγκατάσταση, το οποίο πρέπει να εμπιστεύονται οι πελάτες που θα αποκρυπτογραφήσουν την κυκλοφορία του TLS [29].

2.3.7 Squid proxy

Ο Squid proxy είναι διακομιστής μεσολάβησης με πλήρεις δυνατότητες, παρέχει υπηρεσίες διακομιστή μεσολάβησης και προσωρινής μνήμης για πρωτόκολλο μεταφοράς υπερκειμένου (HTTP), πρωτόκολλο μεταφοράς αρχείων (FTP) και άλλα δημοφιλή πρωτόκολλα δικτύου. Το Squid μπορεί να εφαρμόσει προσωρινή αποθήκευση και διακομιστή μεσολάβησης αιτημάτων Secure Sockets Layer (SSL), όπως επίσης και προσωρινή αποθήκευση αναζητήσεων διακομιστή ονομάτων τομέα (DNS). Το Squid υποστηρίζει μια μεγάλη ποικιλία πρωτοκόλλων προσωρινής αποθήκευσης, όπως το πρωτόκολλο προσωρινής μνήμης Internet (ICP), το πρωτόκολλο προσωρινής αποθήκευσης υπερκειμένου (HTCP), το πρωτόκολλο δρομολόγησης συστοιχίας προσωρινής μνήμης (CARP) και το πρωτόκολλο συντονισμού προσωρινής μνήμης Web (WCCP). Ακόμα παρέχει εκτεταμένους και λεπτομερείς μηχανισμούς ελέγχου πρόσβασης για την παρακολούθηση κρίσιμων παραμέτρων μέσω του πρωτοκόλλου SNMP. Τέλος υποστηρίζει SSL 2.0, SSL 3.0 ,TLS 1.0, TLS 1.1, και TLS 1.2. [30].

2.3.8 Σύγκριση τον proxies

Από την βιβλιογραφική ανασκόπηση στον ακόλουθο πινάκα, γίνεται μια αναφορά σε ποιες πλατφόρμες μπορούν να υλοποιηθούν οι TLS/SSL proxies, τι είδος κώδικα είναι, ποιες εκδόσεις υποστηρίζουν και σε πια λειτουργικά είναι υλοποιήσιμοι.

OpenSSL	**GnuTLS**	**WolfSSL**	**Mitmproxy**	**SSLsplit**	**Polarproxy**	**Squid proxy**
Open Source	Open Source	Open Source	Open Source	Open Source	NETRESEC	Open Source
Υλοποίηση σε γλώσσα c	Υλοποίηση σε γλώσσα c	Υλοποίηση σε γλώσσα c, Java (wolfSSL JNI), η C# (wolfSSL C#) και σε Python	Υλοποίηση σε γλώσσα python	Υλοποίηση σε γλώσσα c	Υλοποίηση σε γλώσσες Java, Python, PHP, Golang, C, C++, .NET, and Node.js.	Υλοποίηση σε γλώσσα c++
Υποστηρί-ζει SSL 2.0/3.0, TLS 1.0/1.1/1.2 και Datagram Transport	Υποστηρί-ζει SSL 3.0, TLS 1.0/1.1/1.2/1.3 και DTLS 1.0	Υποστηρί-ζει έκδοση SSL 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2 και 1.3, ακόμα	Υποστηρί-ζει έκδοση SSL 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2	Υποστηρί-ζει SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2 και προαιρετι	Υποστηρί-ζει έκδοση SSL 3.0 και TLS εκδόσεις 1.0, 1.1, 1.2 και 1.3, ακόμα	Υποστηρί-ζει SSL 2.0, SSL 3.0 και TLS 1.0, TLS 1.1, TLS 1.2

Layer Security (DTLS) 1.0		υποστήριξη DTLS 1.0, 1.2 και 1.3	και 1.3	κά SSL 2.0	υποστήριξη DTLS 1.0, 1.2 και 1.3	
Υλοποι-ήσεις είναι διαθέσιμες σε Linux και λειτουργικό σύστημα (OS) Windows, επίσης χρησιμοποιεί-ται από πολλές γνωστές εφαρμογές σε Unix.	Υλοποι-ήσεις είναι διαθέ-σιμες σε Unix και λειτουργικά συστήματα Windows	Υλοποι-ήσεις είναι διαθέ-σιμες σε macOS, Linux και Windows.	Υλοποι-ήσεις είναι διαθέσιμες σε macOS, Linux και Windows.	Υλοποι-ήσεις είναι διαθέσιμες σε Linux και Windows.	Υλοποι-ήσεις είναι διαθέσιμες σε Linux, macOS και Windows.	Υλοποι-ήσεις είναι διαθέσιμες σε Linux και Windows.
Operation modes Proxying SSL/TLS, Proxying HTTPS, Proxying TCP και Proxying UDP	Operation modes HTTP και SOCKS proxies	operation modes SSL/TLS Proxy, Reverse Proxy, Load Balancer, Forward Proxy και Transparent Proxy	Operation modes Transparent mode, Reverse proxy, Explicit mode, Upstream proxy και SOCKS proxies	Operation modes Transparent mode, Explicit mode, Split mode και Bridge mode	Operation modes Reverse proxy, Transparent proxy, HAProxy, HTTP CONNECT Proxy, TLS Termination Proxy, Trasparent In-Line Proxy και SOCKS Proxy	Operation modes Transparent proxy, Explicit proxy, Reverse proxy και Intercepting proxy
Αλγόριθ-μοι κρυπτο-γράφησης AES 128, 192 και 256 bits, DES, 3DES	Αλγόριθ-μοι κρυπτο-γράφησης AES, DES, 3DES, RSA, DSA, ECDSA,	Αλγόριθ-μοι κρυπτο-γράφησης AES, DES, 3DES, RSA, ECC, ECDHE,	Αλγόριθ-μοι κρυπτο-γράφησης AES, DES, RC4, 3DES, ECC, SHA-1, SHA-2,	Αλγόριθ-μοι κρυπτο-γράφησης RSA, AES, MD5, SHA-1 και Diffie-	Αλγόριθ-μοι κρυπτο-γράφησης AES, Blowfish	Αλγόριθ-μοι κρυπτο-γράφησης Diffie-Hellman, ECDH, AES, 3DES, SHA,

128 και 192 bits, RC4, RSA 512 bits σε 4096 bits, ECC secp256r1 και secp521r1.	SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), MD5, ECDHE και Diffie-Hellman	DHE, SHA-1, SHA-2, και MD5	και MD5	Hellman	και RSA	MD5 και HMAC
Ειδική λειτουργία Δεν υποστηρί-ζει PCAP files	Ειδική λειτουργία Δεν υποστηρί-ζει PCAP files	Ειδική λειτουργία Δεν υποστηρί-ζει PCAP files	Ειδική λειτουργία Δεν υποστηρί-ζει PCAP files	Ειδική λειτουργία Δεν υποστηρί-ζει PCAP files	Ειδική λειτουργία Υποστηρί-ζει PCAP files	Ειδική λειτουργία Δεν υποστιρί-ζει PCAP files

Πίνακας 2.1: Απεικονίζονται τα χαρακτηριστικά των proxies.

2.4 Τρωτά σημεία στο πρωτόκολλο TLS/SSL

Τα τρωτά σημεία στο πρωτόκολλο TLS/SSL μπορεί να ταξινομηθεί σε δύο τύπους, τον πρώτο ευπάθεια προδιαγραφών και τον δεύτερο υλοποίηση τρωτών σημείων. Τα τρωτά σημεία των προδιαγραφών αφορούν το ίδιο το πρωτόκολλο. Μια ευπάθεια προδιαγραφών μπορεί να διορθωθεί μόνο από μια νέα έκδοση πρωτοκόλλου ή μια επέκταση. Τα τρωτά σημεία υλοποίησης σχετίζονται με τρωτά σημεία σε ορισμένες υλοποιήσεις SSL/TLS, όπως το OpenSSL.

2.4.1 Τρωτά σημεία από ευπάθεια προδιαγραφών

- Το DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) είναι μια από τις πιο πρόσφατες επιθέσεις κατά της ευπάθειας προδιαγραφών [31]. Παρουσιάστηκε τον Αύγουστο του 2016 και πρόκειται για μια πολύπλοκη επίθεση πολλαπλών πρωτοκόλλων στο TLS/SSL. Αν και πολλοί διακομιστές σήμερα παρόλο που δεν επιτρέπεται η υποβάθμιση των συνδέσεων, λόγω ορισμένων εσφαλμένων διαμορφώσεων ή ακατάλληλων προεπιλεγμένων ρυθμίσεων ο διακομιστής μπορεί να υποστηρίζει ακόμα στην έκδοση SSL 2.0. Αυτό δεν θα πρέπει να αποτελεί πρόβλημα, καθώς κανείς δεν χρησιμοποιεί αυτήν την έκδοση SSL/TLS πια, αλλά προκαλεί ένα ελάττωμα ασφαλείας. Η επίθεση σε μια TLS/SSL σύνδεση συνίσταται στην ανάκτηση πληροφοριών σχετικά με τη σύνδεση και τα κοινά μυστικά. Στη συνέχεια ο εισβολέας χρησιμοποιώντας το SSL 2.0 μπορεί να στέλνει τροποποιημένα κρυπτογραφημένα κείμενα στον διακομιστή.
- Μια άλλη πρόσφατη επίθεση κατά μιας ευπάθειας προδιαγραφών είναι το Logjam, το οποίο ανακαλύφθηκε τον Μάιο 2015. Η επίθεση Logjam συνίσταται στην εκμετάλλευση που πραγματοποιείται κατά την ανταλλαγή αδύναμων κλειδιών Diffie-Hellman. Το Logjam είναι μια επίθεση man-in-the-middle που υποβαθμίζει τη σύνδεση σε έναν εξασθενημένο Diffie-Hellman. Η υποστήριξη TLS

Diffie-Hellman με αδύναμους παραμέτρους είναι μια πτυχή που καθιστά επιτυχημένη αυτήν την επίθεση. Η άλλη πτυχή αφορά την εξαγωγική κρυπτογραφίας. Το Logjam θεωρείται αποτέλεσμα ευπάθειας προδιαγραφών πρωτοκόλλου, λόγω του γεγονότος ότι το TLS εξακολουθεί να επιτρέπει τη χρήση του Diffie-Hellman σε αδύναμους παραμέτρους [32].

- Μια άλλη επίθεση που αφορά τις προδιαγραφές του πρωτοκόλλου είναι μια επίθεση padding που ονομάζεται POODLE [33]. Το POODLE (Padding Oracle On Downgraded Legacy Encryption) ανακαλύφθηκε από την Google το 2014. Η προέλευση αυτής της επίθεσης είναι η συμβατότητα προς τα πίσω για το SSL 3.0 από πολλές TLS υλοποιήσεις. Για να είναι επιτυχής ο εισβολέας σε μια επίθεση, θα πρέπει πρώτα να προκαλέσει υποβάθμισης, για να το κάνει μετάβαση από το TLS 1.x στο SSL 3.0. Το POODLE στοχεύει τον τρόπο λειτουργίας CBC που χρησιμοποιείται στο SSL 3.0. Ο εισβολέας μπορεί να τροποποιήσει τις επικοινωνίες μεταξύ του πελάτη και του διακομιστή. Το POODLE είναι μια επίθεση padding, καθώς η επίθεση POODLE μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση των cookies HTTP σε ιστότοπους. Οι υλοποιήσεις που επηρεάζονται είναι εκείνες που δεν ελέγχουν σωστά το padding που χρησιμοποιείται. Η πιο προφανής λύση είναι να αποφύγετε το SSL 3.0 αποκλείοντας τη συμβατότητα προς τα πίσω και καταργώντας το SSL 3.0.

2.4.2 Τρωτών σημείων κατά την υλοποίηση

Παρουσιάζονται ευπάθειες σε κρυπτογραφικούς μηχανισμούς, συγκεκριμένα σε ορισμένους από αυτούς που χρησιμοποιούνται από το πρωτόκολλο TLS/SSL, καθώς μπορεί να χρησιμοποιηθεί σε αρκετούς κρυπτογραφικούς μηχανισμούς που δεν είναι όλοι ασφαλείς. Οι μηχανισμοί που χρησιμοποιείται έχουν τρωτά σημεία που μπορεί να κάνουν την επικοινωνία ανασφαλή εάν γίνει εκμετάλλευση αυτών.

- Κρυπτογραφία δημόσιου κλειδιού: Το RSA είναι ένας κρυπτογραφικός μηχανισμός που χρησιμοποιείται για την κρυπτογράφηση και την υπογραφή μηνυμάτων ή πληροφορίες. Η ασφάλεια του RSA βασίζεται σε δύο προβλήματα, στην παραγοντοποίηση μεγάλων ακεραίων αριθμών και η ισχύς του RSA είναι αντιστρόφως ανάλογη με τη διαθέσιμη υπολογιστική ισχύς. Στο πέρασμα των χρόνων, αναμένεται ότι η παραγοντοποίηση μεγάλων ακεραίων θα γίνεται συχνότερα. Το RSA μπορεί να θεωρηθεί ότι έχει σπάσει όταν αυτά τα προβλήματα θα επιλυθούν σε πρακτικό χρονικό διάστημα. Άλλες επιθέσεις δεν βασίζονται στο σπάσιμο της μαθηματικής πολυπλοκότητας του RSA, αλλά επικεντρώνονται σε άλλες λεπτομέρειες πιο απλές στην επίθεση. Μια επιλεγμένη επίθεση απλού κειμένου είναι μια επίθεση που εκμεταλλεύεται το γεγονός ότι στο RSA από την ίδια είσοδος θα παραχωθεί η ίδια έξοδος.
- Συμμετρική Κρυπτογραφία: Το 3DES είναι ένας μηχανισμός κρυπτογράφησης που βασίζεται στο DES [34]. Όπως λέει και το όνομα, Triple DES αποτελείται από πολλαπλή κρυπτογράφηση με χρήση DES. Το Triple DES μπορεί να υλοποιηθεί χρησιμοποιώντας μια από τα τις ακόλουθες επιλογές κλειδιών.

α. Και τα τρία κλειδιά να είναι ανεξάρτητα.
β. Το κλειδί 1 να είναι ίσο με το κλειδί 3. Το κλειδί 1 και το κλειδί 2 να είναι ανεξάρτητα.

γ. Και τα τρία κλειδιά είναι ίσα.

Κάθε επιλογή κλειδιού σχετίζεται με ένα σύνολο ευπαθειών. Η επιλογή ένα χρησιμοποιεί τρία διαφορετικά κλειδιά 56-bit, δηλαδή ένα κλειδί 168-bit, αλλά λόγω των επιθέσεων Meet-in-the-Middle (MITM) η πραγματική ασφάλεια είναι 112-bit. Ο NIST δηλώνει ότι το Triple DES με την επιλογή κλειδώματος ένα είναι βιώσιμο μέχρι το τέλος του 2030. Από εκεί και μετά, η χρήση του δεν επιτρέπεται. Η επιλογή δύο, χρησιμοποιεί δύο διαφορετικά κλειδιά 56-bit, δηλαδή ένα κλειδί 112-bit. Η επιλογή κλειδώματος δύο, επίσης γνωστή ως τριπλή κρυπτογράφηση δύο κλειδιών, μπορεί να δεχθεί επίθεση χρησιμοποιώντας επιλεγμένες επιθέσεις απλού κειμένου με περίπου 2k βήματα, k = 56. Ο Merkle et al. κατέληξε στο συμπέρασμα ότι είναι προτιμότερο να χρησιμοποιηθεί ένας μόνο αλγόριθμος κρυπτογράφησης με μεγαλύτερο κλειδί από έναν αλγόριθμο πολλαπλής κρυπτογράφησης με μικρότερο κλειδί. Η επιλογή τρία έχει την ίδια ασφάλεια με το DES, γεγονός που το καθιστά ανασφαλή επιλογή. Ο Advanced Encryption Standard (AES), είναι ένας μηχανισμός κρυπτογράφησης όπου δημιουργήθηκε από τους Rijmen και Daemen [35]. Ο AES μπορεί να χρησιμοποιηθεί με διαφορετικά μεγέθη κλειδιών - 128, 192 ή 256. Ο αριθμός των γύρων που αντιστοιχεί σε κάθε μέγεθος κλειδιού είναι, αντίστοιχα, 10, 12 και 14. Το AES έχει γίνει ο τυπικός μηχανισμός κρυπτογράφησης, που χρησιμοποιείται από πολλά πρωτόκολλα όπως το TLS. Η ανάπτυξη του και η δημοτικότητα προσέλκυσε αρκετούς επιτιθέμενους, ώστε να προσπαθήσουν να βρουν ευπάθειες. Η πιο επιτυχημένη κρυπτανάλυση του AES είναι η επίθεση MITM δημοσιεύτηκε το 2011 από τον Bogdanov et al. [36]. Αποδίδει ελαφρώς καλύτερα από τις επιθέσεις brute-force. Ώστε να υπάρξει κατανόηση πόσο δύσκολο είναι η κρυπτανάλυση του AES, η συγκεκριμένη επίθεση πέτυχε γραμμική πολυπλοκότητα 2126:1 για το πλήρες AES με 128-bit (AES-128). Επομένως, το κλειδί μειώνεται σε 126-bit από το αρχικό 128-bit, αλλά θα χρειαζόταν ακόμα πολλά χρόνια για να επιτεθεί με επιτυχία στον AES-128. Δεν υπάρχουν γνωστές πρακτικές επιθέσεις που κατάφεραν να σπάσουν τα κρυπτογραφημένα δεδομένα του AES.

- Λειτουργία Hash: Το MD5 είναι ο διάδοχος του MD4, δημιουργήθηκε από την Rivest το 1991. Το MD5 πραγματοποιεί κρυπτογράφηση και κατακερματισμό, παρόλο που έχει αποδειχθεί ανασφαλές, επίσης εξακολουθεί να χρησιμοποιείται ευρέως στις μέρες μας. Το MD5 παράγει μήνυμα 128-bit και χρησιμοποιείται συνήθως για την επαλήθευση της ακεραιότητας των δεδομένων. Ο Wang et al. απέδειξε το έτος του 2005 ότι το MD5 δεν είναι ανθεκτικό σε σύγκρουση [37]. Η μελέτη που πραγματοποιήθηκε, είχε σχέση με τον τρόπο όπου οι διαφορές στην είσοδο επηρεάζουν την έξοδο. Ο αλγόριθμος κατακερματισμού 1 (SHA-1) είναι μια άλλη κρυπτογραφική συνάρτηση κατακερματισμού που παράγει μηνύματα των 160 bits. Αν και δεν έχουν βρεθεί πραγματικές συγκρούσεις για το SHA-1, θωρείται ανασφαλές και συνιστάται η χρήση SHA-2 ή SHA-3. Έχουν γίνει και άλλες επιτυχημένες επιθέσεις εναντίον του SHA-1. Το 2005, ο Wang et al. παρουσίασε μια επίθεση σύγκρουσης που αφορά το SHA-1 ως αποτέλεσμα να μείωσε τον αριθμό των υπολογισμών με την εύρεση συγκρούσεις από το 280

στο 269 [38]. Οι ερευνητές ισχυρίζονται ότι αυτή ήταν η πρώτη επίθεση με σύγκρουση, όπου στο πλήρες SHA-1 80 με πολυπλοκότητα κατώτερη από το θεωρητικό όριο 280. Στις μέρες μας είναι ακόμα υπολογιστικά ακριβό να εκτελεστούν αυτοί οι αριθμοί υπολογισμοί . Στο εγγύς μέλλον, μέχρι το έτος 2025, μια επίθεση σύγκρουσης αναμένεται να είναι προσιτή σε ερευνητικό πανεπιστημιακό πρόγραμμα.

2.5 Proxy και στατιστικά υλοποίησης

Παρουσιάζονται οι δημοφιλείς στοίβες SSL/TLS, λόγω του πολλαπλού αριθμού, η λίστα απέχει πολύ από το να είναι πλήρης, ως αποτέλεσμα να επισημαίνονται μόνο οι συνηθισμένοι. Δεδομένου ότι σχεδόν όλες οι αναφερόμενες υλοποιήσεις ενημερώνονται συνεχώς οι λεπτομέρειες που παρέχονται μπορεί να ξεπεραστεί πολύ σύντομα.

2.5.1 Δημοφιλές στοίβες υλοποιήσεις

1. Openssl: Όπως αναφέραμε είναι μια εφαρμογή ανοιχτού κώδικα του SSL/TLS. Είναι πλήρως υλοποιήσιμος σε γλώσσα προγραμματισμού C και υποστηρίζει SSL 2.0/3.0, TLS 1.0/1.1/1.2 και Datagram Transport Layer Security (DTLS) 1.0. υλοποιήσεις είναι διαθέσιμα για Unix και λειτουργικό σύστημα Windows χρησιμοποιείται από πολλές γνωστές εφαρμογές, επίσης είναι πολύ δημοφιλές στον κόσμο του Unix. Εκτός από το SSL/TLS, αποστέλλεται με τις δικές του υλοποιήσεις κρυπτογραφημένοι αλγόριθμοι και λειτουργικότητες χρησιμότητας τα πιστοποιητικά X509. Η βιβλιοθήκη είναι σε θέση να αποκωδικοποιεί, να δημιουργεί και να υπογράφει πιστοποιητικά και αίτημα υπογραφής πιστοποιητικού (CSR). Εξαιτίας αυτού το OpenSSL μπορεί να θεωρηθεί ως ένα πλήρως εξοπλισμένο κιτ εργαλείων δημιουργία και διαχείριση (PKI).
2. JSSE: Είναι μέρος της Java Standard Edition πλατφόρμας από την έκδοση 1.4 και περιέχει την προεπιλεγμένη υλοποίηση SSL/TLS της Java. Είναι πλήρως γραμμένη σε Java και υποστηρίζει SSL 3.0 και TLS 1,0/1,1/1,2. Ως μέρος της πλατφόρμας JavaSE, η βιβλιοθήκη είναι διαθέσιμη για όλες τις πλατφόρμες με περιβάλλον JavaSE Runtime Environment Windows και Unix. Οι εφαρμογές που βασίζονται σε Java και σε SSL/TLS είναι πολύ πιθανό να χρησιμοποιήσουν αυτήν την υλοποίηση εκτός εάν ενσωματώνουν τρίτα μέρη. Χρησιμοποιεί την αρχιτεκτονική Java Cryptography Architecture για κρυπτογραφικές λειτουργίες και μπορεί έτσι να χρησιμοποιήσει διαφορετικές κρυπτογραφικές υλοποιήσεις [39].
3. Microsoft SChannel: Από τη Microsoft είναι η προεπιλεγμένη υλοποίηση του SSL/TLS σε λειτουργικά συστήματα Windows. Το SChannel υποστηρίζει το ευρύ φάσμα των SSL 2.0/3.0, TLS 1.0/1.1/1.2 και DTLS 1.0/1.2 και είναι διαθέσιμο αποκλειστικά για τα Windows. Η βιβλιοθήκη είναι ενσωματωμένη ως πάροχος υποστήριξης ασφαλείας. Το SCchannel μπορεί να ρυθμιστεί ώστε να χρησιμοποιεί εφαρμογές κρυπτογράφησης με πιστοποίηση FIPS αλγορίθμων, συμμορφώνοντας έτσι τη ζήτηση για τέτοιες πιστοποιήσεις όταν απαιτούνται σε ευαίσθητα περιβάλλοντα[40].
4. Network Security Services (NSS): Η βιβλιοθήκη NSS9 δημιουργήθηκε από τον αρχικό κώδικα της Netscape Inc. και είναι υλοποιήσιμη σε C και Assembler. Το NSS υποστηρίζει SSL 2.0/3.0 και TLS 1.0/1.1, επίσης σήμερα χρησιμοποιείται κυρίως από προγράμματα περιήγησης και λογισμικό του πελάτη. Τέλος το NSS προσφέρει μια κρυπτογράφηση με πιστοποίηση FIPS[41].

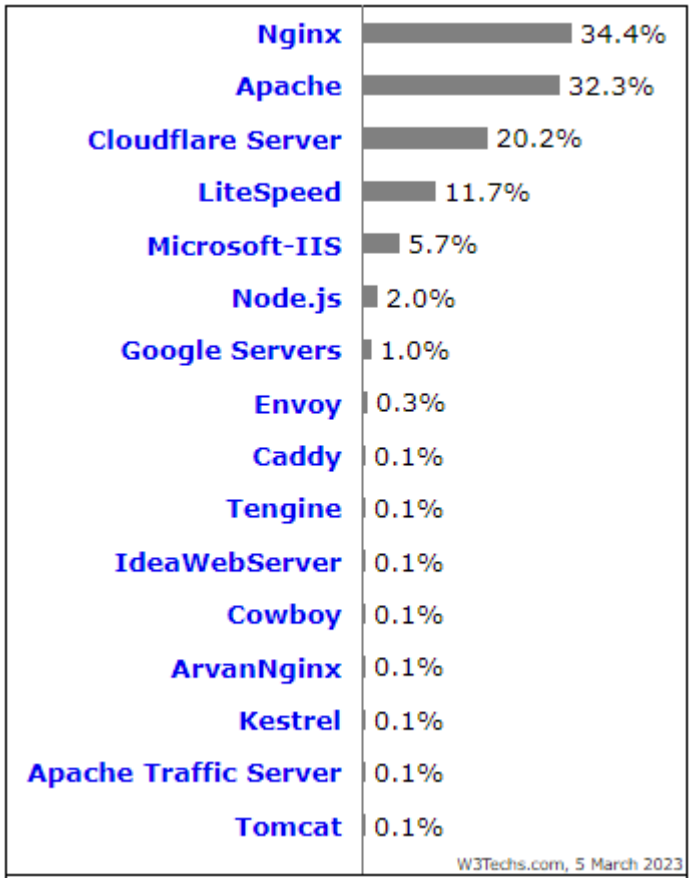
2.5.2 Στατιστικά στοιχεία από την χρήση τους

Δεν υπάρχουν διαθέσιμα ακριβή στατιστικά στοιχεία για την εξάπλωση των υλοποιήσεων, αλλά είναι δυνατή η εκτίμηση με την ανάλυση στατιστικών στοιχείων από την χρήση των προγραμμάτων περιήγησης του ιστού και των διακομιστών, δεδομένου ότι το πρωτόκολλο SSL/TLS στο ποίο βασίζεται κάθε λογισμικό είναι γνωστό στους περισσότερους. Στον ακόλουθο πίνακα παρατίθεται το λογισμικό που χρησιμοποιείται συχνά, όπως και ο αντίστοιχο proxy που το υλοποιεί.

Λογισμικό	Τύπος	Υλοποίηση
Apache	Webserver	OpenSSL
Microsoft IIS	Webserver	SChannel
GlassFish	Webserver	JSSE
Resin	Webserver	JSSE
Nginx	Webserver	OpenSSL
Mozilla Firefox	Browser	NSS
Internet Explorer	Browser	SChannel

Πίνακας 2.2: Απεικονίζονται το αντίστοιχο λογισμικό με πια υλοποίηση στοίβα SSL/TLS συνοδεύεται.

Στο σχήμα 2.6 απεικονίζεται τα ποσοστά των ιστοσελίδων που χρησιμοποιούν διάφορους διακομιστές ιστού, ενώ στο σχήμα 2.7 απεικονίζεται τα ποσοστά από τα προγράμματα περιήγησης.



Σχήμα 2.6: Απεικονίζονται τα ποσοστά των ιστοτόπων που χρησιμοποιούν διάφορους διακομιστές ιστού– Πηγή: W3Schools.com.

2022	Chrome	Edge	Firefox	Safari	Opera
October	79.9 %	8.1 %	5.2 %	4.2 %	1.7 %
September	80.9 %	7.8 %	5.2 %	3.7 %	1.5 %
August	81.1 %	7.6 %	5.2 %	3.4 %	1.7 %
July	81.1 %	7.5 %	5.0 %	3.4 %	2.1 %
June	76.3 %	7.4 %	5.1 %	3.6 %	2.3 %
May	79.9 %	7.3 %	5.3 %	3.8 %	2.4 %
April	80.3 %	7.2 %	5.3 %	3.8 %	2.4 %
March	80.3 %	7.5 %	5.3 %	3.7 %	2.3 %
February	79.9 %	7.5 %	5.4 %	4.0 %	2.3 %
January	80.1 %	7.3 %	5.5 %	3.9 %	2.3 %

Σχήμα 2.7: Απεικονίζεται το μερίδιο αγοράς των προγράμματος περιήγησης – Πηγή: W3Schools.com.

Όπως φαίνεται, οι διακομιστές ιστού Ngnix και Apache είναι μακράν οι πιο χρησιμοποιούμενοι διακομιστές που βασίζονται στο OpenSSL. Αντίθετα, το Google Chrome είναι μακράν το πιο χρησιμοποιούμενο πρόγραμμα περιήγησης, αλλά η στοίβα που χρησιμοποιεί ο Chrome εξαρτάται από το λειτουργικό σύστημα. Τέλος, φαίνεται να είναι έγκυρο να γίνει η υπόθεση ότι το OpenSSL είναι το πιο χρησιμοποιούμενο SSL/TLS στον Ιστότοπο[42,43].

Κεφάλαιο 3
Μεθοδολογία

Για την έρευνα πραγματοποιήθηκε μελέτη στην βιβλιογραφία, ώστε να γίνει μια πιο ολοκληρωμένη ανάδειξη σε ευπάθειες (vulnerabilities) και στον τρόπο λειτουργιάς των TLS/SSL proxies. Συγκεκριμένα για την ανάδειξη στον τρόπο λειτουργίας ώστε να επιτευχτεί η διαθεσιμότητα της πληροφορίας, η εμπιστευτικότητα και η ακμαιότητα, πραγματοποιήθηκε συλλογή δεδομένων από περιοδικά, βιβλιοθήκες και διαδικτυακές βάσεις δεδομένων όπως το Google Scholar, ενοποιημένη αναζήτηση Τεύκρος, openlibrary.org, ResearchGate, ERIC, Scopus και το μέσω του ακαδημαϊκού δικτύου Mendeley. Επίσης έγινε χρήση λέξεων κλειδιών όπως TLS proxy, SSL proxy, TLS/SSL proxy, protect on web, TLS/SSL vulnerabilities, top cyber threat, cyber security, TLS/SSL protocol, TLS/SSL statistics, TLS/SSL tunnel, TLS/SSL open source και session.

Η προσέγγιση της διπλωματικής που άφορα τον σχεδιασμό άφορα τα ακόλουθα στάδια.

- Συλλογή και έλεγχος πληροφοριών από αναγνωρισμένες πήγες, όπως δημοσιεύσεις, βιβλία και επιστημονικές σελίδες με σκοπό να δημιουργηθεί η βιβλιογραφική ανασκόπηση στην οποία θα βασιστεί η έρευνα, ώστε ο χαρακτήρας της διατριβής να είναι ερευνητικός.
- Αναφορά στην ασφάλεια τα τελευταία έτη σε παγκόσμιο επίπεδο, με σκοπό να γίνει μια επισήμανση στα σημαντικά προβλήματα που αντιμετωπίζει η κυβερνοασφάλεια, επίσης να σημειωθεί ότι κάθε χρόνο παρουσιάζεται ζήτημα ευπάθειας και σε διαφορετική χώρα ανά τον κόσμο.
- Τρόπος λειτουργιάς των proxy TLS/SSL αναφορικά με την αρχιτεκτονική τους, όπου θα γίνει εστιάσει στην χρήση τους και την συμπεριφορά τους όσων άφορα την έκδοση τους και τα χαρακτηριστικά τους, πως μια σύνδεση στο διαδίκτυο μπορεί να χαρακτηριστεί ασφαλές με τη χρήση των TLS/SSL proxy, ώστε να γίνει αποφυγή από κακόβουλες επιθέσεις, η πληροφορία να υπόκειται σε κρυπτογράφηση, με σκοπό να περιοριστούν οι επιθέσεις .
- Έλεγχο σημαντικών proxies ως προς τα χαρακτηριστικά τους, σε πιο λογισμικό μπορούν να εγκατασταθούν, ποιες εκδόσεις του πρωτοκόλλου TLS/SSL υποστηρίζουν καθώς και πια πρωτόκολλα κρυπτογράφησης.
- Εύρεση ευπαθειών σε διαφορές εκδόσεις του TLS/SSL, με την εκτέλεση τους θα γίνει έλεγχος για τρωτά σημεία που έχουν, με σκοπό να αναδειχθούν ώστε να περιοριστούν οι επιθέσεις σε αυτές.
- Υλοποίηση σεναρίων με την χρήση proxy TLS/SSL σε εικονικές μηχανές, όπου θα άφορα την χρήση τους και την συμπεριφορά τους σε διάφορες εκδόσεις τους, ακόμα θα δημιουργηθούν εικονικές μηχανές σε open source λογισμικό Ubuntu, για κάθε έναν ξεχωριστά proxy TLS/SSL όπου είναι προς εξέταση, στην συνέχεια θα χρησιμοποιηθούν ιστότοποι από το διαδίκτυο ώστε να εκτελεστεί η πρόσβαση μέσω των proxy με σκοπό να ελεγχθεί η συμπεριφορά τους. Οι εικονικές μηχανές των proxy TLS/SSL θα συνδέονται κάθε φορά και διαφορετική με το διαδίκτυο, ώστε να πραγματοποιηθούν οι διάφοροι έλεγχοι σε αυτούς με σκοπό να προσδιοριστούν κρίσιμα συμπεράσματα.
- Πληροφόρηση και συμπεράσματα, από τους ελέγχους που θα πραγματοποιηθούν σε διαφόρους proxy, θα προκύψουν αποτελέσματα όπου θα πληροφορήσουν για την ευκολία στην εγκατάσταση τους, εάν λειτουργούν μόνο σε γραμμή εντολών ή υποστηριζόταν και γραφικό περιβάλλον, την κρυπτογράφηση και αποκρυπτογράφηση που χρησιμοποιούν, ώστε να μειωθούν οι επιθέσεις σε υποδομές δικτύου, καθώς και πόσο επηρεάζεται η ταχύτητα εκτέλεσης τους από επιμέρους λειτουργίες που εφαρμόζονται.

Αναφορά στα νομικά, δεοντολογικά και επαγγελματικά ζητήματα που προκύπτουν από τη διατριβή.

Η συγγραφή της παρών διατριβής, έγινε με σκοπό να ολοκληρωθεί ο μεταπτυχιακός κύκλος σπουδών όπου αποτελεί και υποχρέωση, Επίσης η διατριβή έχει βασιστεί σε βιβλία συγγραφέων όπως και δημοσιεύσεις επιστημονικών άρθρων τα οποία έχουν καταχωρημένα δικαιώματα. Ο χαρακτήρας της έρευνας είναι να γίνει ενημέρωση αναφορικά με τις κυβερνοεπιθέσεις και όχι να καταχερίσει δικαιώματα.

Κεφάλαιο 4

Σχεδιασμός υποδομής δικτύου για αξιολόγηση TLS/SSL proxies

Στο κεφάλαιο αυτό θα καθοριστούν οι απαιτήσεις για το σχεδιασμό μιας υποδομής δικτύου με χρήση ιδεατών μηχανών, ώστε να αξιολογηθούν εκτενέστερα τα εργαλεία ανοιχτού κώδικα TLS/SSL proxies τα οποία θα επιλεγούν για αξιολόγηση. Επιπρόσθετα θα καθοριστούν τα κριτήρια και τα σενάρια αξιολόγησης τα οποία θα υλοποιηθούν. Οι άξονες αξιολόγησης που θα καθοριστούν, θα βοηθήσουν ώστε να γίνει αναλυτική σύγκριση των δυνατοτήτων των εργαλείων προς εξέταση.

4.1 Απαιτήσεις σχεδιασμού

Για τον σχεδιασμό μιας υποδομής δικτύου, όπου με χρήση ιδεατών μηχανών, θα αξιολογηθούν τα εργαλεία ανοιχτού κώδικα TLS/SSL proxies. Οι απαιτήσεις για τον σχεδιασμό είναι οι ακόλουθες.

- Λογισμικό Windows: Το λογισμικό είναι ένα σύνολο οδηγιών, δεδομένων ή προγραμμάτων που χρησιμοποιούνται για τη λειτουργία υπολογιστών και την εκτέλεση συγκεκριμένων εργασιών. Είναι το αντίθετο του υλικού, το οποίο περιγράφει τις φυσικές πτυχές ενός υπολογιστή. Μπορεί να θεωρηθεί ως το μεταβλητό μέρος ενός υπολογιστή, ενώ το υλικό είναι το αμετάβλητο μέρος. Οι δύο κύριες κατηγορίες λογισμικού είναι το λογισμικό εφαρμογών και το λογισμικό συστήματος. Μια εφαρμογή είναι λογισμικό που ικανοποιεί μια συγκεκριμένη ανάγκη ή εκτελεί εργασίες. Το λογισμικό συστήματος έχει σχεδιαστεί για να εκτελεί το υλικό ενός υπολογιστή και παρέχει μια πλατφόρμα για την εκτέλεση εφαρμογών.
- VirtualBox: Είναι λογισμικό ανοιχτού κώδικα της αρχιτεκτονικής υπολογιστών x86. Λειτουργεί ως hypervisor, δημιουργώντας μια εικονική μηχανή όπου ο χρήστης μπορεί να τρέξει ένα άλλο λειτουργικό σύστημα. Το λειτουργικό σύστημα όπου εκτελείται το VirtualBox ονομάζεται λειτουργικό σύστημα οικοδεσπότη. Το λειτουργικό σύστημα που εκτελείται στο VM ονομάζεται λειτουργικό σύστημα επισκέπτης. Το VirtualBox υποστηρίζει Windows, Linux ή macOS ως κεντρικό λειτουργικό σύστημα. Κατά τη διαμόρφωση μιας εικονικής μηχανής, ο χρήστης μπορεί να καθορίσει πόσους πυρήνες CPU και πόση μνήμη RAM και χώρο στο δίσκο θα πρέπει να αφιερωθεί στο VM. Όταν το VM εκτελείται, μπορεί να γίνει παύση της λειτουργίας του. Η εκτέλεση του συστήματος έχει παγώσει εκείνη τη στιγμή και ο χρήστης μπορεί να συνεχίσει να το χρησιμοποιεί αργότερα[44].

  Απαιτήσεις συστήματος ώστε να πραγματοποιηθεί εγκατάσταση της εικονικής μηχανής σε λειτουργικό Windows.

  1. Έκδοση λειτουργικού συστήματος - Microsoft Windows 10 (32-bit ή 64-bit).
  2. Μνήμη τυχαίας πρόσβασης (RAM) - Συνιστάται τουλάχιστον 4 GB RAM.
  3. Ελεύθερος χώρος στο δίσκο - Συνιστάται τουλάχιστον 25 GB ελεύθερου χώρου.
  4. Καλή σύνδεση στο Internet για λήψη του αρχείου ISO VirtualBox και Ubuntu.
  5. Εάν ο υπολογιστής είναι HP θα πρέπει να ενεργοποιηθεί η Τεχνολογία HP BIOS Virtualization

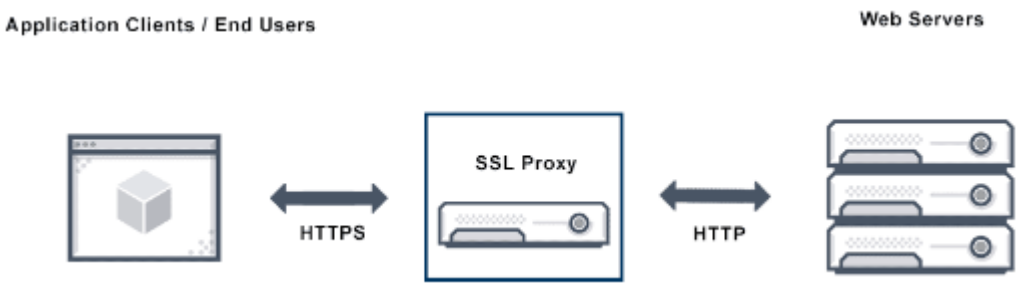
- Ubuntu: Το Ubuntu είναι μια διανομή Linux που βασίζεται στο Debian και αποτελείται κυρίως από δωρεάν λογισμικό ανοιχτού κώδικα. Κυκλοφορεί

επίσημα σε τρεις εκδόσεις Desktop, Server, και Core για συσκευές Internet of things και ρομπότ. Όλες οι εκδόσεις μπορούν να εκτελεστούν μόνο στον υπολογιστή ή σε μια εικονική μηχανή. Επίσης είναι ένα δημοφιλές λειτουργικό σύστημα για το cloud computing. Ακόμα κυκλοφορεί κάθε έξι μήνες, με εκδόσεις μακροπρόθεσμης υποστήριξης (LTS) κάθε δύο χρόνια. Από τον Οκτώβριο του 2022, η πιο πρόσφατη έκδοση είναι 22.10 "Kinetic Kudu" και η τρέχουσα έκδοση μακροπρόθεσμης υποστήριξης είναι 22.04 "Jammy Jellyfish". Τέλος αναπτύσσεται από τη βρετανική εταιρεία Canonical και μια κοινότητα άλλων προγραμματιστών, σύμφωνα με ένα μοντέλο αξιοκρατικής διακυβέρνησης. Η Canonical παρέχει ενημερώσεις ασφαλείας και υποστήριξη για κάθε έκδοση του Ubuntu, ξεκινώντας από την ημερομηνία κυκλοφορίας έως και ότου η κυκλοφορία φτάσει στην καθορισμένη ημερομηνία λήξης ζωής[45].

- Website: Ένας ιστότοπος είναι η τυποποίηση και η αφομοίωση συγκεκριμένης οργάνωσης πόρων του Ιστού, δηλαδή ιστοσελίδων που ανήκουν σε μια συγκεκριμένη καθορισμένη οντότητα. Επίσης ένας ιστότοπος βρίσκεται σε πλατφόρμα φιλοξενείς στο διαδίκτυο.

- Wireshark: Είναι ένα δωρεάν και ανοιχτού κώδικα λογισμικό ανάλυσης πρωτοκόλλου δικτύου που χρησιμοποιείται για την καταγραφή και ανάλυση της κυκλοφορίας δικτύου σε πραγματικό χρόνο. Χρησιμοποιείται ευρέως από διαχειριστές δικτύου, αναλυτές ασφαλείας και προγραμματιστές για την αντιμετώπιση προβλημάτων, την ανάλυση και τον εντοπισμό σφαλμάτων των ζητημάτων δικτύου. Το Wireshark μπορεί να καταγράψει και να αναλύσει την κίνηση από διαφορετικές πηγές, όπως Ethernet, Wi-Fi και Bluetooth. Μπορεί να ανατέμνει ένα ευρύ φάσμα πρωτοκόλλων και να εμφανίζει τα δεδομένα σε μορφή αναγνώσιμη από τον άνθρωπο. Αυτό διευκολύνει την κατανόηση της ροής της κυκλοφορίας και τον εντοπισμό τυχόν ανωμαλιών ή απειλών για την ασφάλεια. Εκτός από τη ζωντανή λήψη και ανάλυση, το Wireshark παρέχει επίσης δυνατότητες όπως φιλτράρισμα, εξαγωγή δεδομένων και αποκωδικοποίηση πρωτοκόλλου. Υποστηρίζει ένα ευρύ φάσμα πλατφορμών συμπεριλαμβανομένων των Windows, macOS και Linux. Συνολικά, το Wireshark είναι ένα ισχυρό εργαλείο για όποιον θέλει να κατανοήσει και να αναλύσει λεπτομερώς την κυκλοφορία του δικτύου. Ωστόσο, θα πρέπει να χρησιμοποιείται δεοντολογικά και με άδεια, καθώς μπορεί επίσης να χρησιμοποιηθεί για τη λήψη ευαίσθητων πληροφοριών όπως κωδικούς πρόσβασης και ονόματα χρήστη[46].

- Τα TLS/SSL proxies Mitmproxy, Polarproxy και Squid proxy, θα αποτελέσουν τα εργαλεία για τα οποία θα προκύψουν συγκρίσεις και συμπεράσματα, μέσα από την εκτέλεση διαφόρων σεναρίων, όπως εάν η έκδοση τους έχει ευπάθεια σε επιθέσεις, το λογισμικό τους πόσο φιλικό είναι στον χρήστη, εάν κάποιος προηγείται έναντι κάποιου άλλου ως προς την ταχύτητα εκτέλεσης.



Σχήμα 4.1: Απεικονίζεται ένα δίκτυο TLS/SSL proxy.

4.2 Κριτήρια αξιολόγησης

Θα πραγματοποιηθεί αξιολόγηση μεταξύ τον proxy TLS/SSL Mitmproxy, Polarproxy και Squid proxy όπου θα αποτελέσουν τα κύρια εργαλεία για την ερευνά στην διατριβή, ώστε να προκύψουν χρήσιμα συμπεράσματα, με σκοπό να αναδεχθεί η σημαντικότητα τους στον σύγχρονο κόσμο.

4.2.1 Λειτουργιές proxy που υποστηρίζουν

- Mitmproxy:

α. Regular είναι ένας τρόπος λειτουργιάς του Mitmproxy, όπου είναι ο απλούστερος και με της ελάχιστες ρύθμιση. Αρχικά διαμορφώνουμε τον πελάτη ώστε να χρησιμοποιεί mitmproxy ορίζοντας έναν διακομιστή μεσολάβησης HTTP. Από προεπιλογή, το mitmproxy ακούει στη θύρα 8080.

β. Transparent είναι μια λειτουργία του mitmproxy, όπου η κίνηση κατευθύνεται σε έναν διακομιστή μεσολάβησης στο επίπεδο δικτύου, χωρίς να απαιτείται η ρύθμιση των παραμέτρων από τον πελάτη. Αυτό καθιστά τον διακομιστή μεσολάβησης ιδανικό, καθώς δεν μπορεί να πραγματοποιηθεί αλλαγή στη συμπεριφορά του πελάτη. Εντολή για την ενεργοποίηση της λειτουργίας transparent mode “mitmdump --mode transparent”.

γ. WireGuard είναι μια λειτουργία του Mitmproxy, όπου λειτουργεί με τον ίδιο τρόπο όπως η Trasparent με τη διαφορά ότι η ρύθμιση και η δρομολόγηση της κυκλοφορίας του πελάτη στο mitmproxy διαφέρουν. Σε αυτήν τη λειτουργία, ο mitmproxy εκτελεί έναν εσωτερικό διακομιστή WireGuard, στον οποίο μπορούν να συνδεθούν συσκευές χρησιμοποιώντας τις τυπικές εφαρμογές του πελάτη. Εντολή για την ενεργοποίηση της λειτουργίας WireGuard mode “mitmweb --mode wireguard”.

δ. Reverse Proxy είναι μια λειτουργία του Mitmproxy, όπου ο διακομιστή μεσολάβησης μπορεί να χρησιμοποιήσει τον mitmproxy για να λειτουργήσει σαν ένας κανονικός διακομιστής HTTP. Εντολή για την ενεργοποίηση της λειτουργίας Reverse Proxy “ mitmdump --mode reverse”

ε. Upstream Proxy είναι μια λειτουργία του Mitmproxy, όπου όλα τα αιτήματα μεταφέρονται άνευ όρων σε έναν διακομιστή μεσολάβησης upstream της επιλογής. Εντολή για την ενεργοποίηση της λειτουργίας Upstream Proxy “ mitmdump --mode upstream”

στ. SOCKS Proxy είναι μια λειτουργία του Mitmproxy, όπου λειτουργεί ως διακομιστής μεσολάβησης SOCKS5. Όπου χρησιμοποιεί SOCKS5 αντί για HTTP για τη δημιουργία σύνδεσης με τον διακομιστή μεσολάβησης. Εντολή για την ενεργοποίηση της λειτουργίας SOCKS Proxy "mitmdump --mode socks5".

ζ. DNS Server είναι μια λειτουργία του Mitmproxy, όπου σε μια εισερχόμενη κίνηση ο DNS θα χρησιμοποιήσει την δυνατότητα του λειτουργικού συστήματος για να επιστρέψει μια απάντηση. Από προεπιλογή χρησιμοποιεί την θύρα 53. Εντολή για την ενεργοποίηση της λειτουργίας DNS Server mitmdump --mode dns.

- Polarproxy:

α. Transparent Forward Proxy όπου ο PolarProxy συνδέεται με εξωτερικούς διακομιστές TLS για λογαριασμό των πελατών σε ένα δίκτυο. Αυτή η λειτουργία χρησιμοποιείται συνήθως για να παρακολουθεί την κρυπτογραφημένη κίνηση των πελατών HTTPS.

β. Reverse Proxy όπου ο PolarProxy συνδέεται σε έναν ή περισσότερους τοπικούς διακομιστές TLS για λογαριασμό εξωτερικών πελατών. Αυτή η λειτουργία χρησιμοποιείται για την παρακολούθηση της εισερχόμενης κίνησης TLS σαν να ήταν μη κρυπτογραφημένη.

γ. TLS Termination Proxy όπου ο PolarProxy τερματίζει την κρυπτογράφηση TLS για τις εισερχόμενες συνδέσεις και προωθεί την κίνηση του επιπέδου εφαρμογής σε αποκρυπτογραφημένη μορφή σε έναν τοπικό διακομιστή με την επιλογή –terminate.

δ. Transparent In-Line Proxy όπου ο PolarProxy αποκρυπτογραφεί, επανακρυπτογραφεί και προωθεί όλες τις συνδέσεις TLS σε συγκεκριμένο διακομιστή μεσολάβησης.

ε. SOCKS Proxy όπου ο PolarProxy εκτελείται ως τοπικός διακομιστής μεσολάβησης SOCKS, τον οποίο οι χρήστες μπορούν να χρησιμοποιήσουν για πρόσβαση στο διαδίκτυο. Όλη η κίνηση TLS που διέρχεται μέσω του διακομιστή SOCKS του PolarProxy θα αποκρυπτογραφηθεί και θα επανακρυπτογραφηθεί ανεξάρτητα από τη θύρα. Με την επιλογή --socks για την ενεργοποίηση του διακομιστή μεσολάβησης SOCKS. Ο διακομιστής μεσολάβησης SOCKS μπορεί να χρησιμοποιηθεί σε συνδυασμό με το --allownontls για να επιτρέψει επίσης την κυκλοφορία εκτός TLS, ώστε να διέρχεται μέσω του διακομιστή μεσολάβησης

στ. HAProxy όπου ο PolarProxy εκτελείται ως τοπικός διακομιστής HAProxy, χρησιμοποιώντας το πρωτόκολλο PROXY v1 (send-proxy), στο οποίο μπορεί να συνδεθεί ένας εξισορροπητής φορτίου HAProxy. Με την επιλογή --haproxy 8081 ώστε να ξεκινήσει μια επικοινωνία HAProxy στη θύρα TCP 8081. Η λειτουργία HAProxy μπορεί να χρησιμοποιηθεί σε συνδυασμό με το --allownontls για να επιτρέψει επίσης την κυκλοφορία εκτός TLS, ώστε να διέρχεται μέσω του διακομιστή μεσολάβησης.

ζ. HTTP CONNECT Proxy όπου ο PolarProxy εκτελείται ως τοπικός διακομιστής μεσολάβησης HTTP. Η κίνηση TLS που διέρχεται μέσω του διακομιστή μεσολάβησης HTTP CONNECT του PolarProxy θα αποκρυπτογραφηθεί και θα επανακρυπτογραφηθεί ανεξάρτητα από τη θύρα. Με την επιλογή --httpconnect ώστε να ενεργοποιηθεί ο διακομιστής μεσολάβησης HTTP CONNECT.

- Squid proxy:

α. Reverse proxy είναι η λειτουργία του squid proxy, όπου είναι μια τεχνική αποθήκευσης των απαντήσεων ή των πόρων από έναν διακομιστή ιστότοπου,

έτσι ώστε τα επόμενα αιτήματα που αφορούν στους ίδιους πόρους να μπορούν να ικανοποιηθούν από τον τοπικό διακομιστή μεσολάβησης, ώστε να μην υπάρχει επικοινωνία με τον διακομιστή web. Η προσωρινή μνήμη ελέγχει εάν το τοπικό αποθηκευμένο αντίγραφο του εγγράφου εξακολουθεί να είναι έγκυρο πριν προβεί στην αποθήκευση του αντιγράφου.

β. Transparent proxy είναι η λειτουργία του squid proxy, όπου ο proxy λειτουργεί ως διαφανής διακομιστής μεσολάβησης, πράγμα που σημαίνει ότι τα αιτήματα των πελατών ανακατευθύνονται στο Squid χωρίς να το γνωρίζει ο πελάτης. Αυτό επιτυγχάνεται συνήθως με τη διαμόρφωση της πύλης δικτύου, όπως έναν δρομολογητή ή ένα τείχος προστασίας, ώστε να προωθούνται όλα τα αιτήματα των πελατών στο Squid. Σε αυτήν τη λειτουργία, το Squid μπορεί να παρέχει μια σειρά από υπηρεσίες στους πελάτες, όπως προσωρινή αποθήκευση, έλεγχος πρόσβασης και φιλτράρισμα περιεχομένου. Επιπλέον, επειδή ο πελάτης δεν γνωρίζει ότι τα αιτήματά του ανακατευθύνονται, δεν χρειάζεται να ρυθμίσει το πρόγραμμα περιήγησής του, για την χρήση διακομιστή μεσολάβησης.

4.2.2 Αλγόριθμοι κρυπτογράφησης που υποστηρίζουν

- Mitmproxy: Υποστηρίζει ένα ευρύ φάσμα αλγορίθμων κρυπτογράφησης, συμπεριλαμβανομένου τόσο συμμετρικούς όσο και ασύμμετρους αλγόριθμους κρυπτογράφησης.

α. SSL/TLS: Αυτό είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο κρυπτογράφησης για ασφαλείς διαδικτυακές επικοινωνίες και υποστηρίζεται από το Mitmproxy.

β. AES (Advanced Encryption Standard): Πρόκειται για έναν ευρέως χρησιμοποιούμενο αλγόριθμο συμμετρικής κρυπτογράφησης που υποστηρίζεται από τον Mitmproxy.

γ. RSA (Rivest-Shamir-Adleman): Πρόκειται για έναν ευρέως χρησιμοποιούμενο αλγόριθμο ασύμμετρης κρυπτογράφησης που υποστηρίζεται από τον Mitmproxy.

δ. DH (Diffie-Hellman): Πρόκειται για έναν ευρέως χρησιμοποιούμενο αλγόριθμο ανταλλαγής κλειδιών που υποστηρίζεται από τον Mitmproxy.

ε. SHA (Secure Hash Algorithm): Πρόκειται για μια ευρέως χρησιμοποιούμενη συνάρτηση κατακερματισμού που υποστηρίζεται από τον Mitmproxy.

στ. MD (Message Digest): Πρόκειται για μια ευρέως χρησιμοποιούμενη συνάρτηση κατακερματισμού που υποστηρίζεται από τον Mitmproxy.

Σημαντικό είναι ότι ο Mitmproxy υποστηρίζει τους αλγόριθμους κρυπτογράφησης με σκοπό την αποκρυπτογράφηση και την επιθεώρηση κρυπτογραφημένης κίνησης του δικτύου. Ωστόσο είναι σημαντικό να χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης που εξακολουθούν να θεωρούνται ασφαλείς και συνιστώνται από ειδικούς σε θέματα ασφάλειας, καθώς η χρήση απαρχαιωμένων ή κατεστραμμένων αλγορίθμων κρυπτογράφησης μπορεί να οδηγήσει σε τρωτά σημεία ασφαλείας.

- Polarproxy: Χρησιμοποιεί διάφορους αλγόριθμους κρυπτογράφησης για την ασφάλεια των δεδομένων που διέρχονται από τον διακομιστή μεσολάβησης. Μερικοί από τους αλγόριθμους κρυπτογράφησης που χρησιμοποιούνται είναι.

α. AES (Advanced Encryption Standard): Ο AES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ευρέως για την κρυπτογράφηση δεδομένων. Το PolarProxy χρησιμοποιεί το AES για την κρυπτογράφηση και την αποκρυπτογράφηση δεδομένων μεταξύ του πελάτη και του διακομιστή.

β. RSA (Rivest–Shamir–Adleman): Ο RSA είναι ένας αλγόριθμος ασύμμετρης κρυπτογράφησης που χρησιμοποιείται για ανταλλαγή κλειδιών και ψηφιακές υπογραφές. Το PolarProxy χρησιμοποιεί RSA για να δημιουργήσει μια ασφαλή σύνδεση μεταξύ του πελάτη και του διακομιστή.

γ. TLS (Transport Layer Security): Το TLS είναι ένα κρυπτογραφικό πρωτόκολλο που χρησιμοποιείται για την ασφάλεια της επικοινωνίας μέσω του Διαδικτύου. Το PolarProxy χρησιμοποιεί TLS για την κρυπτογράφηση δεδομένων μεταξύ του πελάτη και του διακομιστή.

δ. SSL (Secure Sockets Layer): Το SSL είναι ένα καταργημένο κρυπτογραφικό πρωτόκολλο που αντικαταστάθηκε από TLS. Το PolarProxy χρησιμοποιεί SSL για την αποκρυπτογράφηση της κρυπτογραφημένης κίνησης για σκοπούς εντοπισμού σφαλμάτων.

ε. Diffie-Hellman (DH): Ο Diffie-Hellman είναι ένας αλγόριθμος ανταλλαγής κλειδιών που χρησιμοποιείται για τη δημιουργία ενός κοινόχρηστου μυστικού μεταξύ του πελάτη και του διακομιστή. Το PolarProxy χρησιμοποιεί DH για να διαπραγματευτεί μια ασφαλή σύνδεση μεταξύ του πελάτη και του διακομιστή.

Αυτοί οι αλγόριθμοι κρυπτογράφησης βοηθούν να διασφαλιστεί ότι τα δεδομένα που μεταδίδονται μέσω του PolarProxy είναι ασφαλή και προστατευμένα από μη εξουσιοδοτημένη πρόσβαση ή υποκλοπή.

- Squid proxy: Υποστηρίζει αρκετούς αλγόριθμους κρυπτογράφησης για ασφαλή επικοινωνία μεταξύ πελατών και διακομιστών. Αυτοί οι αλγόριθμοι κρυπτογράφησης χρησιμοποιούνται για τη διασφάλιση του απορρήτου και της εμπιστευτικότητας των δεδομένων που μεταδίδονται. Μερικοί από τους αλγόριθμους κρυπτογράφησης που υποστηρίζονται είναι.

α. SSL (Secure Sockets Layer) - Το SSL είναι ένα κρυπτογραφικό πρωτόκολλο που χρησιμοποιείται για την ασφάλεια της επικοινωνίας μέσω του διαδικτύου. Χρησιμοποιεί έναν συνδυασμό συμμετρικής και ασύμμετρης κρυπτογράφησης για να παρέχει εμπιστευτικότητα, ακεραιότητα και αυθεντικότητα.

β. TLS (Transport Layer Security) - Το TLS είναι διάδοχος του SSL και χρησιμοποιείται για την ασφαλή επικοινωνία μέσω διαδικτύου. Παρέχει τα ίδια χαρακτηριστικά ασφαλείας με το SSL και είναι πιο ασφαλές.

γ. AES (Advanced Encryption Standard) - Ο AES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ευρέως για την κρυπτογράφηση δεδομένων. Χρησιμοποιεί ένα κλειδί μεταβλητού μήκους (128, 192 ή 256 bit) και θεωρείται πολύ ασφαλές.

δ. RC4 (Rivest Cipher 4) - Ο RC4 είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ευρέως στο πρωτόκολλο ασφαλείας του Διαδικτύου. Χρησιμοποιεί κλειδί μεταβλητού μήκους (έως 2048 bit) και θεωρείται γρήγορο και αποτελεσματικό.

ε. DES (Data Encryption Standard) - Ο DES είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιήθηκε ευρέως στο παρελθόν. Χρησιμοποιεί κλειδί 56-bit και θεωρείται λιγότερο ασφαλές από το AES.

στ. 3DES (Triple DES) - Το 3DES είναι μια βελτιωμένη έκδοση του DES που χρησιμοποιεί τρία πλήκτρα αντί για ένα. Θεωρείται ότι είναι πιο ασφαλές από το DES αλλά λιγότερο ασφαλές από το AES.

Το Squid Proxy επιτρέπει τη χρήση αυτών των αλγορίθμων κρυπτογράφησης για την ασφαλή επικοινωνία μεταξύ πελατών και διακομιστών. Η επιλογή του αλγορίθμου εξαρτάται από το επίπεδο ασφάλειας που απαιτείται και τις δυνατότητες του πελάτη και του διακομιστή.

4.2.3 Η υποστήριξη του proxy TLS/SSL σε βιβλιοθήκες και πρωτόκολλα

- Mitmproxy: Είναι ένα ισχυρό εργαλείο διακομιστή μεσολάβησης SSL/TLS που μπορεί να υποκλέψει, να επιθεωρήσει και να τροποποιήσει την κυκλοφορία HTTP(S). Παρέχει ένα Python API που επιτρέπει στους προγραμματιστές να δημιουργήσουν προσαρμοσμένα εργαλεία και επεκτάσεις πάνω από τη βασική λειτουργία mitmproxy. Το Python API του mitmproxy περιλαμβάνει υποστήριξη για διακομιστή μεσολάβησης SSL/TLS και παρέχει μια διεπαφή για το χειρισμό της κρυπτογραφημένης κίνησης. Συγκεκριμένα, το mitmproxy παρέχει μια δυνατότητα που ονομάζεται "διαφανής λειτουργία", η οποία του επιτρέπει να παρεμποδίζει την κυκλοφορία SSL/TLS χωρίς να προκαλεί προειδοποιήσεις ασφαλείας στους πελάτες. Εκτός από το HTTP(S), το mitmproxy υποστηρίζει επίσης πολλά άλλα πρωτόκολλα, όπως FTP, TCP, WebSocket και DNS. Τέλος μπορεί να χρησιμοποιηθεί ως αυτόνομο εργαλείο ή μπορεί να ενσωματωθεί σε άλλες εφαρμογές Python για να παρέχει προσαρμοσμένες δυνατότητες διακομιστή μεσολάβησης SSL/TLS.

- Polarproxy: Έχει σχεδιαστεί για να παρακολουθεί και να αναλύει την κυκλοφορία του δικτύου για λόγους ασφάλειας και απόδοσης. Υποστηρίζει μια ποικιλία πρωτοκόλλων, συμπεριλαμβανομένων των HTTP, HTTPS, SMTP, POP3, IMAP, FTP και DNS μέσω TLS. Υποστηρίζει επίσης πολλά πρωτόκολλα κρυπτογράφησης, συμπεριλαμβανομένων των SSLv2, SSLv3, TLSv1.0, TLSv1.1 και TLSv1.2. Για να χρησιμοποιηθεί με βιβλιοθήκες, θα ρυθμιστεί η βιβλιοθήκη ώστε να χρησιμοποιεί το PolarProxy ως διακομιστή μεσολάβησης. Τα συγκεκριμένα βήματα διαμόρφωσης θα εξαρτηθούν από τη βιβλιοθήκη που χρησιμοποιείτε, αλλά γενικά θα πρέπει να καθοριστεί τη διεύθυνση IP και η θύρα του διακομιστή PolarProxy. Όσον αφορά την υποστήριξη πρωτοκόλλου, μπορεί να χειριστεί πολλά πρωτόκολλα ταυτόχρονα. Για παράδειγμα, μπορεί να υποκλέψει και να αναλύσει την κυκλοφορία HTTP, HTTPS και DNS ταυτόχρονα. Αυτή η ευελιξία το καθιστά χρήσιμο εργαλείο για ένα ευρύ φάσμα εργασιών ανάλυσης και παρακολούθησης δικτύου.

- Squid proxy: Υποστηρίζει διακομιστή μεσολάβησης TLS/SSL μέσω της λειτουργίας SSL Bump. Αυτή η δυνατότητα επιτρέπει στο Squid να επιθεωρεί και να τροποποιεί την κυκλοφορία SSL καθώς διέρχεται μέσω του διακομιστή μεσολάβησης, επιτρέποντας στον διακομιστή μεσολάβησης να εκτελεί εργασίες όπως η αποθήκευση στην κρυφή μνήμη και το φιλτράρισμα της κίνησης HTTPS. Όσον αφορά τις βιβλιοθήκες, το Squid χρησιμοποιεί το OpenSSL για την υποστήριξη SSL/TLS. Το OpenSSL είναι μια ευρέως χρησιμοποιούμενη βιβλιοθήκη ανοιχτού κώδικα που παρέχει υποστήριξη για ασφαλή επικοινωνία μέσω δικτύων χρησιμοποιώντας πρωτόκολλα SSL/TLS. Το Squid υποστηρίζει ένα ευρύ φάσμα πρωτοκόλλων, συμπεριλαμβανομένων των HTTP, HTTPS, FTP και πολλών άλλων.

4.2.4 Κατά πόσο διαδεδομένο είναι στον χώρο της ασφάλειας

- Mitmproxy: Είναι ένα ευρέως χρησιμοποιούμενο εργαλείο ανοιχτού κώδικα για την παρακολούθηση, την επιθεώρηση και την τροποποίηση της κυκλοφορίας του δικτύου. Είναι ιδιαίτερα δημοφιλές μεταξύ προγραμματιστών και επαγγελματιών ασφάλειας όπου το χρησιμοποιούν για εντοπισμό σφαλμάτων, δοκιμές και ανάλυση εφαρμογών Ιστού. Η φήμη του Mitmproxy είναι γενικά θετική στις κοινότητες ανάπτυξης και ασφάλειας. Θεωρείται καλό για την ευελιξία, την ευκολία χρήσης και τα ισχυρά χαρακτηριστικά του, τα οποία επιτρέπουν στους χρήστες να καταγράφουν και να αναλύουν την κίνηση HTTP και HTTPS σε πραγματικό χρόνο. Το Mitmproxy έχει επαινεθεί για την ικανότητά του να εντοπίζει και να αντιμετωπίζει γρήγορα προβλήματα δικτύου, καθώς και την αποτελεσματικότητά του στον εντοπισμό τρωτών σημείων ασφαλείας σε εφαρμογές web. Επιπλέον, το mitmproxy έχει μια ενεργή κοινότητα χρηστών που συμβάλλουν στην ανάπτυξή του και παρέχουν υποστήριξη μέσω φόρουμ, τεκμηρίωσης και άλλων πόρων. Αυτό βοήθησε να καθιερωθεί το mitmproxy ως ένα αξιόπιστο και καλά υποστηριζόμενο εργαλείο που το εμπιστεύονται τόσο οι προγραμματιστές όσο και οι επαγγελματίες ασφάλειας. Συνολικά, η ευρεία χρήση και η θετική φήμη του mitmproxy το έχουν καταστήσει πολύτιμο πόρο για όσους εργάζονται στην ανάπτυξη ιστού και την ασφάλεια στον κυβερνοχώρο.

- Polarproxy: Δεν είχε ακόμη αποκτήσει ευρεία δημοτικότητα, αλλά κέρδιζε την έλξη μεταξύ των αναλυτών δεδομένων και των ερευνητών που χρειάζεται να συλλέγουν δεδομένα από ιστότοπους.

- Squid proxy: Είναι ένα ευρέως χρησιμοποιούμενο λογισμικό διακομιστή μεσολάβησης που εκτελείται σε λειτουργικά συστήματα παρόμοια με το Unix. Χρησιμοποιείται συνήθως από οργανισμούς και παρόχους υπηρεσιών διαδικτύου (ISP) για τη βελτίωση της απόδοσης του δικτύου, το φιλτράρισμα του περιεχομένου και την παροχή ασφάλειας και απορρήτου. Το Squid είναι ένα καθιερωμένο και αξιόπιστο λογισμικό διακομιστή μεσολάβησης, με ιστορία που χρονολογείται από τις αρχές της δεκαετίας του 1990. Είναι λογισμικό ανοιχτού κώδικα που αναπτύσσεται και συντηρείται ενεργά από μια κοινότητα

προγραμματιστών. Το Squid έχει αποκτήσει τη φήμη ότι είναι ένα αξιόπιστο και υψηλής απόδοσης λογισμικό διακομιστή μεσολάβησης που μπορεί να χειριστεί μεγάλες ποσότητες επισκεψιμότητας. Έχει υιοθετηθεί ευρέως από οργανισμούς και ISP σε όλο τον κόσμο και χρησιμοποιείται από εκατομμύρια χρήστες καθημερινά. Όσον αφορά το μερίδιο αγοράς, είναι δύσκολο να προσδιοριστεί ο ακριβής αριθμός των οργανισμών και των ISP που χρησιμοποιούν Squid proxy, αλλά υπολογίζεται ότι είναι σε εκατομμύρια. Το Squid χρησιμοποιείται επίσης συχνά σε συνδυασμό με άλλες τεχνολογίες διακομιστή μεσολάβησης και προσωρινής αποθήκευσης, όπως το Nginx και το Varnish, για να παρέχει ακόμα καλύτερη απόδοση και ασφάλεια. Συνολικά, το Squid proxy είναι ένα ευρέως αναγνωρισμένο και σεβαστό λογισμικό διακομιστή μεσολάβησης που είναι γνωστό για την αξιοπιστία, την απόδοση και τα χαρακτηριστικά ασφαλείας του.

4.2.5 Ταχύτητα ανταπόκρισης και επεξεργασίας

- Mitmproxy: Η ταχύτητα απόκρισης και επεξεργασίας στο mitmproxy θα εξαρτηθεί από διάφορους παράγοντες, όπως η επεξεργαστική ισχύς του μηχανήματος που εκτελεί, η ταχύτητα και η καθυστέρηση δικτύου και η πολυπλοκότητα της υποκλοπής κυκλοφορίας. Γενικά, το mitmproxy είναι ένα εργαλείο υψηλής απόδοσης που έχει σχεδιαστεί για να χειρίζεται αποτελεσματικά μεγάλους όγκους κίνησης. Χρησιμοποιεί ασύγχρονη επεξεργασία και μπορεί να χειριστεί πολλές συνδέσεις ταυτόχρονα, γεγονός που συμβάλλει στη μείωση του χρόνου επεξεργασίας και στη βελτίωση της ταχύτητας απόκρισης. Ωστόσο, η ταχύτητα απόκρισης και επεξεργασίας ενδέχεται να εξακολουθεί να επηρεάζεται από παράγοντες όπως το μέγεθος της υποκλοπής κυκλοφορίας, ο αριθμός των φίλτρων και των σεναρίων που χρησιμοποιούνται, καθώς και το επίπεδο αποκρυπτογράφησης και κρυπτογράφησης που εκτελούνται. Για τη βελτιστοποίηση της απόδοσης του mitmproxy, συνιστάται η χρήση ενός μηχανήματος με επαρκή επεξεργαστική ισχύ και μνήμη και για την ελαχιστοποίηση του αριθμού των φίλτρων, καθώς και των σεναρίων που χρησιμοποιούνται. Μπορεί επίσης να είναι χρήσιμο να περιοριστεί ο όγκος της αποκρυπτογράφησης και της κρυπτογράφησης που εκτελείται, λογω ότι μπορεί να επηρεάσει σημαντικά τον χρόνο επεξεργασίας.

- Polarproxy: Θα αναφερθούν οι παράμετροι οι οποίοι επηρεάζουν την ταχύτητα εκτέλεσης και κατά επέκταση την επεξεργασία των δεδομένων.

α. Η ταχύτητα και τοποθεσία του διακομιστή όπου, η ταχύτητα με την οποία ο polarproxy ανταποκρίνεται στα αιτήματα των χρηστών μπορεί να επηρεαστεί από την ταχύτητα και τη θέση των διακομιστών του. Όσο πιο κοντά είναι οι διακομιστές στο χρήστη, τόσο πιο γρήγορος είναι ο χρόνος απόκρισης.

β. Ταχύτητα Διαδικτύου του χρήστη όπου, η σύνδεση του ίδιου του χρήστη στο διαδίκτυο μπορεί επίσης να επηρεάσει την ταχύτητα απόκρισης του polarproxy. Μια αργή ή ασταθής σύνδεση μπορεί να προκαλέσει καθυστερήσεις.

γ. Εάν ο polarproxy έχει μεγάλο όγκο επισκεψιμότητας, αυτό θα μπορούσε να επιβραδύνει τον χρόνο απόκρισης του proxy.

Ολοκληρώνοντας, η ταχύτητα απόκρισης και επεξεργασίας του polarproxy θα εξαρτηθεί από διάφορους παράγοντες και είναι σημαντικό να λαμβάνονται υπόψη αυτούς τους παράγοντες κατά την αξιολόγηση της απόδοσης του proxy.

- Squid proxy: Η ταχύτητα απόκρισης και επεξεργασίας ενός διακομιστή μεσολάβησης squid εξαρτάται από διάφορους παράγοντες όπως οι προδιαγραφές υλικού, την ταχύτητα δικτύου, ο αριθμός των ταυτόχρονων χρηστών, οι ρυθμίσεις προσωρινής αποθήκευσης και τον φόρτο του διακομιστή. Μερικοί από τους τρόπους βελτιστοποίησης του διακομιστή μεσολάβησης squid για καλύτερη ταχύτητα και επεξεργασία είναι οι έξεις.

α. Οι Προδιαγραφές του υλικού, ότι ο διακομιστής που εκτελεί το squid proxy έχει επαρκή μνήμη RAM, CPU και χωρητικότητα αποθήκευσης. Ένας μεγαλύτερος αριθμός πυρήνων CPU μπορεί να βοηθήσει στην ταχύτερη επεξεργασία των αιτημάτων

β. Η ταχύτητα πρόσβασης στο διαδίκτυο, οτι είναι επαρκεί για τη διαχείριση της εισερχόμενης και εξερχόμενης κίνησης. Το υψηλότερο εύρος ζώνης εξασφαλίζει ταχύτερη μεταφορά δεδομένων.

γ. Ρυθμίσεις προσωρινής αποθήκευσης, όπου ο διακομιστής μεσολάβησης Squid μπορεί να διαμορφωθεί ώστε να αποθηκεύει στην κρυφή μνήμη ιστοτόπους και περιεχόμενο με συχνή πρόσβαση. Αυτό μειώνει το φόρτο στον διακομιστή και βελτιώνει τον χρόνο απόκρισης για τα επόμενα αιτήματα.

δ. Συμπίεση όπου, ο διακομιστής μεσολάβησης Squid μπορεί να ρυθμιστεί ώστε να συμπιέζει τα δεδομένα πριν τα στείλει στον πελάτη. Αυτό μειώνει τον όγκο των δεδομένων που πρέπει να μεταφερθούν, ως αποτέλεσμα βελτιώνει την ταχύτητα απόκρισης.

ε. Εξισορρόπηση φορτίου όπου, εάν ο αριθμός των χρηστών που έχουν πρόσβαση στον διακομιστή μεσολάβησης squid είναι υψηλός, μπορεί να εφαρμοστεί εξισορρόπηση φορτίου για τη διανομή του φορτίου σε πολλούς διακομιστές. Αυτό διασφαλίζει ότι κανένας διακομιστής δεν υπερφορτώνεται και βελτιώνει τον χρόνο απόκρισης.

Ως αποτέλεσμα, η βελτιστοποίηση του διακομιστή μεσολάβησης squid για την ταχύτητα και επεξεργασία περιλαμβάνει έναν συνδυασμό διαμορφώσεων υλικού και λογισμικού, βελτιστοποιήσεων δικτύου και τεχνικών εξισορρόπησης φορτίου.

4.2.6 Πόσο εύκολο είναι η εγκατάσταση και η παραμετροποίηση

- Mitmproxy: Η εγκατάσταση και η διαμόρφωση του mitmproxy αποτελείται από τα ακόλουθα πεδία.

α. Εγκατάσταση mitmproxy όπου, μπορεί να εγκατασταθεί σε διάφορα λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows, macOS και Linux. Πραγματοποιείται λήψη του πακέτου εγκατάστασης από τον ιστότοπο του mitmproxy ή με την χρήση ενός διαχειριστή πακέτων όπως το Homebrew (σε

macOS) ή το apt-get (σε Linux). Η διαδικασία εγκατάστασης είναι συνήθως απλή και η επίσημη τεκμηρίωση παρέχει λεπτομερείς οδηγίες για κάθε πλατφόρμα.

β. Διαμόρφωση της συσκευής για την χρήση του mitmproxy, πρέπει να διαμορφωθεί η προσωπική συσκευή ώστε να χρησιμοποιεί διακομιστή μεσολάβησης. Αυτό περιλαμβάνει τη ρύθμιση των ρυθμίσεων διακομιστή μεσολάβησης HTTP/HTTPS στις ρυθμίσεις δικτύου της συσκευής. Θα χρειαστεί να καθοριστεί η διεύθυνση IP και τον αριθμό της θύρας που εκτελείται στον προσωπικό υπολογιστή.

γ. Έναρξη mitmproxy, αφού διαμορφωθεί η προσωπική συσκευή ώστε να χρησιμοποιεί mitmproxy, ξεκινά ο διακομιστής μεσολάβησης εκτελώντας την εντολή mitmproxy στο προσωπικό τερματικό. Από προεπιλογή, το mitmproxy ακούει στη θύρα 8080.

δ. Παρακολούθηση επισκεψιμότητας με mitmproxy όπου, μόλις εκτελεστεί το mitmproxy, ξεκινά την παρακολούθηση της κυκλοφορίας ανοίγοντας τη διεπαφή ιστού mitmproxy στο πρόγραμμα περιήγησής. Από προεπιλογή, η πρόσβαση στη διεπαφή ιστού είναι δυνατή μεταβαίνοντας στη διεύθυνση http://localhost:8081/. Από εδώ, μπορεί να γίνει προβολή και να διαχείριση της κίνησης που διέρχεται από το διακομιστή μεσολάβησης.

Συνολικά, η εγκατάσταση και η διαμόρφωση του mitmproxy είναι μια απλή διαδικασία, εάν υπάρχει μια εξοικείωση με εργαλεία γραμμής εντολών και έννοιες δικτύωσης. Ωστόσο, ένας νέος σε αυτές τις έννοιες, μπορεί να χρειαστεί λίγος χρόνος για να εξοικειωθείτε με το εργαλείο και τις δυνατότητές του.

- Polarproxy: Ο ιστότοπος του PolarProxy παρέχει λεπτομερείς οδηγίες εγκατάστασης για διάφορα λειτουργικά συστήματα, συμπεριλαμβανομένων των Linux, macOS και Windows. Αυτές οι οδηγίες περιλαμβάνουν τη λήψη και την εξαγωγή του λογισμικού, τη ρύθμιση των αρχείων διαμόρφωσης και την εκκίνηση του διακομιστή μεσολάβησης. Αφού πραγματοποιηθεί εγκατάσταση του PolarProxy, η διαμόρφωσή του είναι επίσης σχετικά εύκολη. Ο PolarProxy παρέχει πολλές επιλογές διαμόρφωσης, όπως τον καθορισμό ποιων διευθύνσεων URL να υποκλαπούν, τη ρύθμιση πιστοποιητικών SSL και τη διαμόρφωση της καταγραφής. Αυτές οι επιλογές μπορούν να ρυθμιστούν με επεξεργασία των αρχείων διαμόρφωσης που παρέχονται από το λογισμικό.

  Συνολικά, ενώ μπορεί να απαιτούνται κάποιες τεχνικές γνώσεις για την εγκατάσταση και τη διαμόρφωση του PolarProxy, η διαδικασία δεν είναι υπερβολικά περίπλοκη για κάποιον με κάποια εμπειρία στη δικτύωση και την εγκατάσταση λογισμικού.

- Squid proxy: Η εγκατάσταση και η διαμόρφωση ενός διακομιστή μεσολάβησης Squid είναι σχετικά απλή, ανάλογα με το επίπεδο εμπειρίας και εξοικείωσης με το λειτουργικό σύστημα. Επίσης ακολουθούν τα γενικά βήματα που θα πρέπει να ακολουθούνται για την εγκατάσταση και την ρυθμίσετε του διακομιστή μεσολάβησης Squid.

α. Επιλογή του λειτουργικού σύστημα στο οποίο θα γίνει εγκατάσταση του Squid, επίσης έλεγχο ότι πληροί τις απαιτήσεις συστήματος.
β. Εγκατάσταση του Squid χρησιμοποιώντας τον διαχειριστή πακέτων του λειτουργικού συστήματος ή κατεβάζοντας και μεταγλωττίζοντας τον πηγαίο κώδικα.
γ. Διαμόρφωση του Squid με επεξεργασία του αρχείου διαμόρφωσης (/etc/squid/squid.conf), ώστε να γίνει καθορισμός της θύρας που θα χρησιμοποιηθεί, τα στοιχεία ελέγχου πρόσβασης, τις ρυθμίσεις προσωρινής μνήμης και άλλες επιλογές.
δ. Πραγματοποίηση δοκιμής του διακομιστή μεσολάβησης Squid ρυθμίζοντας έναν πελάτη για να τον χρησιμοποιεί και βεβαιώνοντας ότι λειτουργεί όπως αναμένεται.
ε. Αν και η ίδια η διαδικασία δεν είναι απαραίτητα δύσκολη, υπάρχουν ορισμένες ιδιότητες στη διαμόρφωση του Squid που μπορεί να απαιτούν πρόσθετη έρευνα και πειραματισμό, ειδικά εάν χρειάζεται να γίνει προσαρμογή τις ρυθμίσεις ώστε να ταιριάζει σε ιδιαίτερες ανάγκες. Ωστόσο, υπάρχουν επίσης πολλοί διαθέσιμοι πόροι στο διαδίκτυο, συμπεριλαμβανομένης της επίσημης τεκμηρίωσης, όπου μπορούν να παράσχουν καθοδήγηση στην διαδικασία.

   Συνολικά, εάν υπάρχει εμπειρία με τη διαχείριση συστήματος και τη δικτύωση, η εγκατάσταση και η διαμόρφωση του Squid δεν αποτελεί δύσκολη διαδικασία.

4.3 Σενάρια υλοποίησης

Τα σενάρια υλοποίησης αναφέρονται στους διαφορετικούς τρόπους με τους οποίους το σχέδιο και η στρατηγική μπορεί να τεθεί σε εφαρμογή, ώστε να γίνει η αξιολόγηση τον proxies Mitmproxy, Polarproxy και Squid proxy.

4.3.1 Επιθεώρηση της κίνησης μεταξύ πελάτη και ιστοσελίδας HTTPS

Ο διακομιστής μεσολάβησης θα χρησιμοποιηθεί για την παρακολούθηση και την επιθεώρηση της κυκλοφορίας μεταξύ ενός πελάτη και ενός διακομιστή web. Στην περίπτωση της κίνησης HTTPS, η οποία είναι κρυπτογραφημένη με χρήση SSL/TLS, ο διακομιστής μεσολάβησης μπορεί να λειτουργήσει ως "man-in-the-middle" και να αποκρυπτογραφήσει την κίνηση, να την επιθεωρήσει και, στη συνέχεια, να την κρυπτογραφήσει εκ νέου πριν την στείλει στο ο διακομιστής προορισμού. Για να χρησιμοποιηθεί έναν διακομιστή μεσολάβησης για να επιθεωρεί την κυκλοφορία HTTPS, θα πρέπει να υπάρξει διαμόρφωση στον πελάτη, ώστε να χρησιμοποιεί τον διακομιστή μεσολάβησης για συνδέσεις HTTPS. Ο διακομιστής μεσολάβησης θα δημιουργήσει στη συνέχεια τη δική του σύνδεση SSL/TLS με τον διακομιστή προορισμού και θα λειτουργήσει ως ενδιάμεσος για την κρυπτογραφημένη κίνηση. Αυτή η προσέγγιση είναι χρήσιμη για την παρακολούθηση της κυκλοφορίας του δικτύου και τον εντοπισμό απειλών ασφαλείας ή παραβιάσεων στην πολιτική ασφαλείας. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η υποκλοπή της κυκλοφορίας HTTPS με αυτόν τον τρόπο μπορεί επίσης να δημιουργήσει κινδύνους ασφαλείας, όπως η πιθανότητα έκθεσης ευαίσθητων δεδομένων.

4.3.2 Επιθεώρηση της κίνησης μεταξύ πελάτη και ιστοσελίδας HTTP

Η χρήση διακομιστή μεσολάβησης για πρόσβαση σε ιστοσελίδες HTTP είναι χρήσιμη σε περιπτώσεις όπου χρειάζεται να υπάρχει μεγάλη ταχύτητα στην μεταφορά των δεδομένων. Ο διακομιστής μεσολάβησης ενεργεί ως ενδιάμεσος μεταξύ του πελάτη και του διακομιστή, η κίνηση των δεδομένων δεν είναι κρυπτογραφημένη, επομένως είναι σε μεγάλο βαθμό επιρρεπής σε επιθέσεις. Για να χρησιμοποιηθεί έναν διακομιστή μεσολάβησης ώστε να επιθεωρεί την κυκλοφορία HTTP, θα πρέπει να υπάρξει διαμόρφωση στον πελάτη, ώστε να χρησιμοποιεί τον διακομιστή μεσολάβησης για συνδέσεις HTTP.

4.3.3 Εργαλεία που επηρεάζουν την εκτέλεση του proxy TLS/SSL και την κίνηση

Ακολουθούν ορισμένα εργαλεία που μπορούν να επηρεάσουν την εκτέλεση ενός διακομιστή μεσολάβησης TLS/SSL και την κίνηση που κινείται εκείνη τη στιγμή. Οι διακομιστής μεσολάβησης TLS/SSL μπορούν να χρησιμοποιηθούν σε συνδυασμό με το λογισμικό τείχους προστασίας και συστήματος ανίχνευσης/πρόληψης εισβολής (IDS/IPS) για την παρακολούθηση και τον έλεγχο της κυκλοφορίας του δικτύου. Το τείχος προστασίας και το λογισμικό IDS/IPS μπορούν να χρησιμοποιηθούν για την επιβολή ελέγχων πρόσβασης και τον αποκλεισμό κακόβουλης κυκλοφορίας. Επίσης οι διακομιστής μεσολάβησης TLS/SSL μπορούν να χρησιμοποιηθούν σε συνδυασμό με λογισμικό εξισορρόπησης φορτίου για τη διανομή της κυκλοφορίας δικτύου σε πολλούς διακομιστές ή πόρους. Το λογισμικό εξισορρόπησης φορτίου μπορεί να χρησιμοποιηθεί για να διασφαλιστεί ότι η κυκλοφορία δικτύου κατανέμεται ομοιόμορφα σε πολλούς διακομιστές και για να αποτραπεί η υπερφόρτωση του διακομιστή. Ακόμα οι διακομιστής μεσολάβησης TLS/SSL μπορούν να χρησιμοποιηθούν σε συνδυασμό με λογισμικό παρακολούθησης δικτύου για την παρακολούθηση της κυκλοφορίας του δικτύου και τον εντοπισμό πιθανών απειλών ασφαλείας. Το λογισμικό παρακολούθησης δικτύου μπορεί να χρησιμοποιηθεί για τον εντοπισμό ασυνήθιστης δραστηριότητας δικτύου, όπως αυξήσεις στην κίνηση ή ασυνήθιστες μεταφορές δεδομένων, που μπορεί να υποδηλώνουν παραβίαση ασφάλειας. Τέλος η επιλογή της κρυπτογράφησης που θα επιλεγεί, όπως και η λειτουργία του proxy server επηρεάζουν την ταχύτητα εκτέλεσης του.

4.3.4 Λειτουργία PCAP αρχείων

Θα δημιουργηθούν αρχεία PCAP που περιέχουν δεδομένα κίνησης δικτύου και με την χρήση του αναλυτή δικτύου Wireshark θα πραγματοποιηθεί έλεγχος σε αυτά. Τα αρχεία PCAP μπορούν να χρησιμοποιηθούν για την ανάλυση της κυκλοφορίας δικτύου, συμπεριλαμβανομένης της κίνησης που διέρχεται μέσω του διακομιστή μεσολάβησης. Ωστόσο, για να αναλυθεί η κίνηση που διέρχεται από έναν διακομιστή μεσολάβησης, το αρχείο PCAP πρέπει να καταγράφει την κίνηση σε ένα σημείο του δικτύου όπου χρησιμοποιείται ο διακομιστής μεσολάβησης. Θα χρειαστεί να διαμορφωθεί το Wireshark ώστε να αναγνωρίζει το πρωτόκολλο του διακομιστή μεσολάβησης. Αφού διαμορφωθεί το Wireshark ώστε να αναγνωρίζει το πρωτόκολλο του διακομιστή μεσολάβησης και τυχόν κρυπτογράφηση που μπορεί να χρησιμοποιηθεί,

πραγματοποιείται η χρήση των εργαλεία φιλτραρίσματος και ανάλυσης του Wireshark για να εξεταστεί λεπτομερώς η κίνηση του δικτύου. Αυτό είναι σημαντικό καθώς θα εντοπιστούν ζητήματα απόδοσης, ευπάθειες ασφαλείας και άλλα προβλήματα με τη διαμόρφωση του δικτύου ή του διακομιστή μεσολάβησης.

4.3.5 Λειτουργία Transparent proxy

Ένας διακομιστής μεσολάβησης σε διαφανή λειτουργία (Transparent mode) είναι ένας τύπος διαμόρφωσης διακομιστή μεσολάβησης που επιτρέπει στον διακομιστή να παρακολουθεί και να χειρίζεται τα αιτήματα των πελατών χωρίς οι πελάτες να γνωρίζουν ότι χρησιμοποιείται ο διακομιστής μεσολάβησης. Σε διαφανή λειτουργία, ο διακομιστής μεσολάβησης τοποθετείται μεταξύ του πελάτη και του διακομιστή προορισμού και προωθεί αυτόματα τα αιτήματα και τις απαντήσεις μεταξύ τους. Αυτό σημαίνει ότι τα αιτήματα του πελάτη παρεμποδίζονται με διαφάνεια και ανακατευθύνονται στον διακομιστή μεσολάβησης, ο οποίος στη συνέχεια στέλνει το αίτημα στον διακομιστή προορισμού για λογαριασμό του πελάτη. Αυτός ο τύπος διαμόρφωσης χρησιμοποιείται συνήθως από τους διαχειριστές δικτύου για τη βελτίωση της απόδοσης και της ασφάλειας στα δίκτυά τους. Χρησιμοποιώντας έναν διαφανή διακομιστή μεσολάβησης, οι διαχειριστές δικτύου μπορούν να ελέγχουν και να παρακολουθούν την κυκλοφορία χωρίς να απαιτούν αλλαγές διαμόρφωσης από την πλευρά του πελάτη. Ωστόσο, αξίζει να σημειωθεί ότι οι διαφανείς διακομιστής μεσολάβησης ενδέχεται να μην είναι κατάλληλοι για όλες τις περιπτώσεις χρήσης. Για παράδειγμα, ενδέχεται να μην είναι αποτελεσματικοί στην απόκρυψη της ταυτότητας ή της τοποθεσίας του χρήστη, καθώς ο διακομιστής προορισμού μπορεί να δει την διεύθυνση IP του διακομιστή μεσολάβησης αντί για τη διεύθυνση IP του πελάτη.

4.3.6 Λειτουργία Reverse proxy

Σε μια διαμόρφωση αντίστροφου (Reverse mode) διακομιστή μεσολάβησης, ο διακομιστής μεσολάβησης βρίσκεται μεταξύ του πελάτη και ενός ή περισσότερων διακομιστών. Όταν ένας πελάτης κάνει ένα αίτημα, το αίτημα υποκλέπτεται πρώτα από τον αντίστροφο διακομιστή μεσολάβησης, ο οποίος στη συνέχεια προωθεί το αίτημα στον κατάλληλο διακομιστή. Στη συνέχεια, ο διακομιστής ανταποκρίνεται στον αντίστροφο διακομιστή μεσολάβησης, ο οποίος με τη σειρά του μεταβιβάζει την απάντηση πίσω στον πελάτη. Το κύριο πλεονέκτημα της χρήσης ενός αντίστροφου διακομιστή μεσολάβησης είναι ότι μπορεί να βοηθήσει στη διανομή της κυκλοφορίας σε πολλούς διακομιστές, βελτιώνοντας την απόδοση και την αξιοπιστία. Επιπλέον, ένας αντίστροφος διακομιστής μεσολάβησης μπορεί να παρέχει ένα πρόσθετο επίπεδο ασφάλειας λειτουργώντας ως πύλη μεταξύ του πελάτη και του διακομιστή, επιτρέποντας στον διακομιστή μεσολάβησης να φιλτράρει και να αποκλείει την κακόβουλη κυκλοφορία. Στη λειτουργία αντίστροφου διακομιστή μεσολάβησης, ο διακομιστής μεσολάβησης είναι συνήθως ρυθμισμένος να ακούει σε μια δημόσια διεύθυνση IP ή όνομα κεντρικού υπολογιστή και τα αιτήματα προωθούνται στον κατάλληλο διακομιστή με βάση το όνομα κεντρικού υπολογιστή ή τη διαδρομή διεύθυνσης URL που ζητήθηκε. Αυτό επιτρέπει σε πολλούς διακομιστές να φιλοξενούνται πίσω από μια ενιαία διεύθυνση IP ή όνομα κεντρικού υπολογιστή, απλοποιώντας τη διαμόρφωση και τη διαχείριση. Συνολικά, οι διαμορφώσεις αντίστροφου διακομιστή μεσολάβησης μπορούν να προσφέρουν μια σειρά από οφέλη

για τη διαχείριση και τη βελτιστοποίηση της κυκλοφορίας ιστού, ιδιαίτερα για εφαρμογές ή υπηρεσίες μεγάλης κλίμακας.

Mitmproxy	**PolarProxy**	**Squid Proxy**
Απόδοση και σταθερότητα	Ευέλικτο φιλτράρισμα	Υποστηρίζει μια ποικιλία μηχανισμών ελέγχου ταυτότητας όπως NTLM και Kerberos
Υποστήριξη μεταξύ πλατφορμών	Υποστηρίζει scripting χρησιμοποιώντας JavaScript	Προώθηση αιτήματα πελατών σε άλλους διακομιστές μεσολάβησης
Επεκτασιμότητα	Καταγράφει την κυκλοφορία WebSocket και HTTP/HTTPS	Καταγραφή και αναφορά, όλης της κυκλοφορίας ιστού
Διεπαφή χρήστη που βασίζεται στο Web	Τροποποιήσει την κυκλοφορία του WebSocket	Προσωρινή αποθήκευση περιεχόμενου στη μνήμη, όπου ζητείται συχνά
Τροποποίηση αιτήματος και απόκρισης	Παρακολούθηση και τροποποίηση κυκλοφορίας TCP	Παρέχει ευέλικτους μηχανισμούς ελέγχου πρόσβασης, όπως η διεύθυνση IP, ο έλεγχος ταυτότητας χρήστη, το όνομα τομέα και η ώρα της ημέρας.
Παρακολούθηση της κυκλοφορίας HTTP και HTTPS	Διαχείριση κυκλοφορίας HTTP/HTTPS	Πραγματοποιεί διαχείριση κυκλοφορίας HTTP/HTTPS
Διαχείριση πιστοποιητικών SSL/TLS	Διαχείριση πιστοποιητικών SSL/TLS	Διαχείριση πιστοποιητικών SSL/TLS

Πίνακας 4.1: Απεικονίζονται τα κύρια χαρακτηριστικά των εργαλείων προς εξέταση.

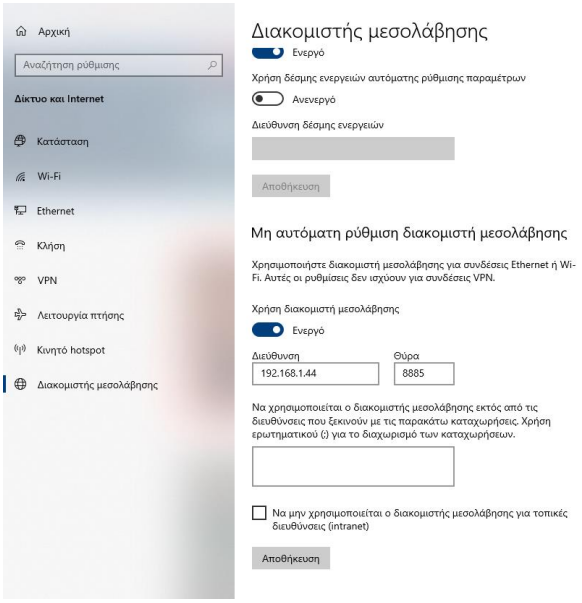
Κεφάλαιο 5

Υλοποίηση υποδομής δικτύου και αξιολόγηση εργαλείων

Σε αυτό το κεφάλαιο θα γίνει καταγραφή της υλοποίησης δικτύου και της αξιολόγησης με βάσει το κεφάλαιο σχεδιασμού. Θα συμπεριληφθούν οι ενέργειες όπου χρειάζονται ώστε να δημιουργηθούν εικονικές μηχανές των proxies TLS/SSL Mitmproxy, Polarproxy και Squid proxy, επίσης θα καταγραφή η δικτυακή τους επικοινωνία μεταξύ αυτών και ιστοσελίδων HTTPS και HTTP, με σκοπό να πραγματοποιηθούν αναλύσεις στα σενάρια που θα αφορούν της ταχύτητα εκτέλεσης τους, τι παράμετροι επηρεάζουν την εκτέλεση τους καθώς και τις λειτουργίες proxy που θα υλοποιηθούν σε Transparent και Reverse.

5.1 Υλοποίηση σεναρίων Mitmproxy σε εικονική μηχανή

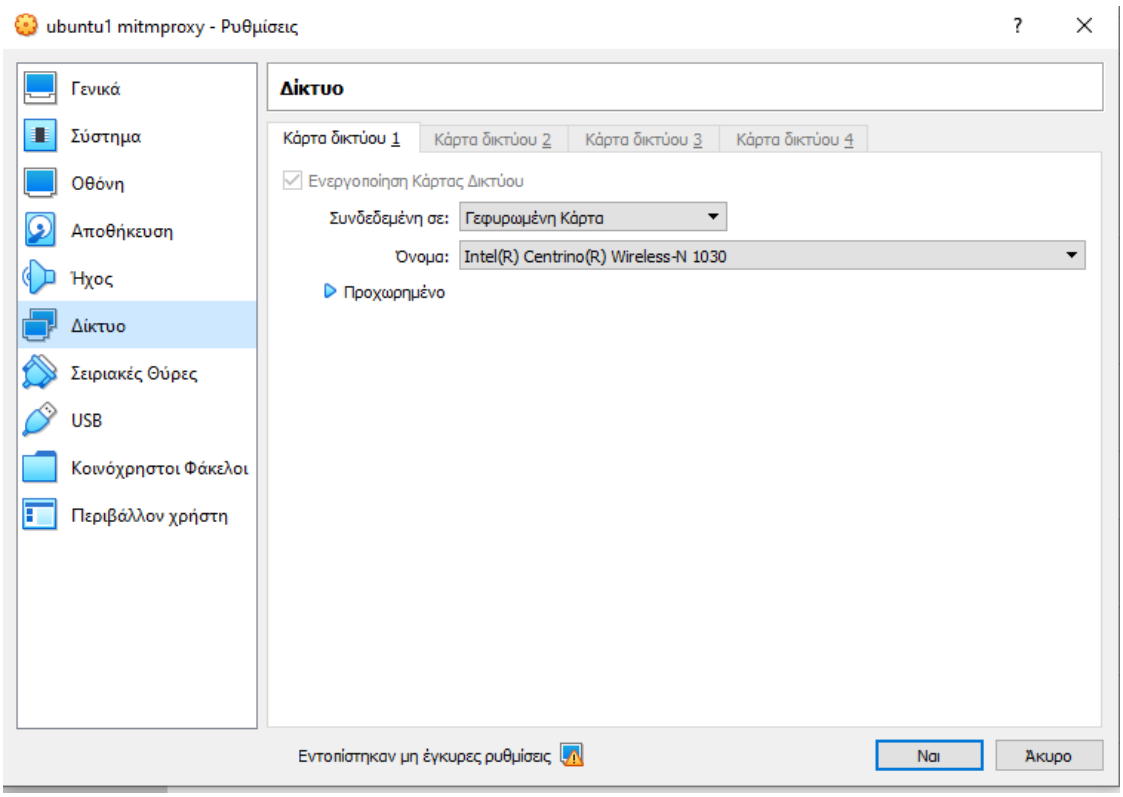
α. Αρχικά για την υλοποίηση των σεναρίων θα πρέπει να ρυθμιστεί κατάλληλα ο υπολογιστής, όπου θα χρησιμοποιείται ως χρήστης ώστε να μεταφέρεται η κίνηση μέσω του proxy. Στο σενάριο ο χρήστης χρησιμοποιεί υπολογιστή με λογισμικό Windows 10.



Σχήμα 5.1: Απεικονίζεται η ρύθμιση στον υπολογιστή του χρήστη, ώστε να μεταφέρει την κίνηση μέσω του διακομιστή μεσολάβησης.

Έχει επιλεγεί η διεύθυνση ip 192.168.1.44, όπου είναι η διεύθυνση του διακομιστή μεσολάβησης και πόρτα εισόδου την 8880 η οποία, επίσης έχει καθοριστεί από τον διακομιστή μεσολάβησης.

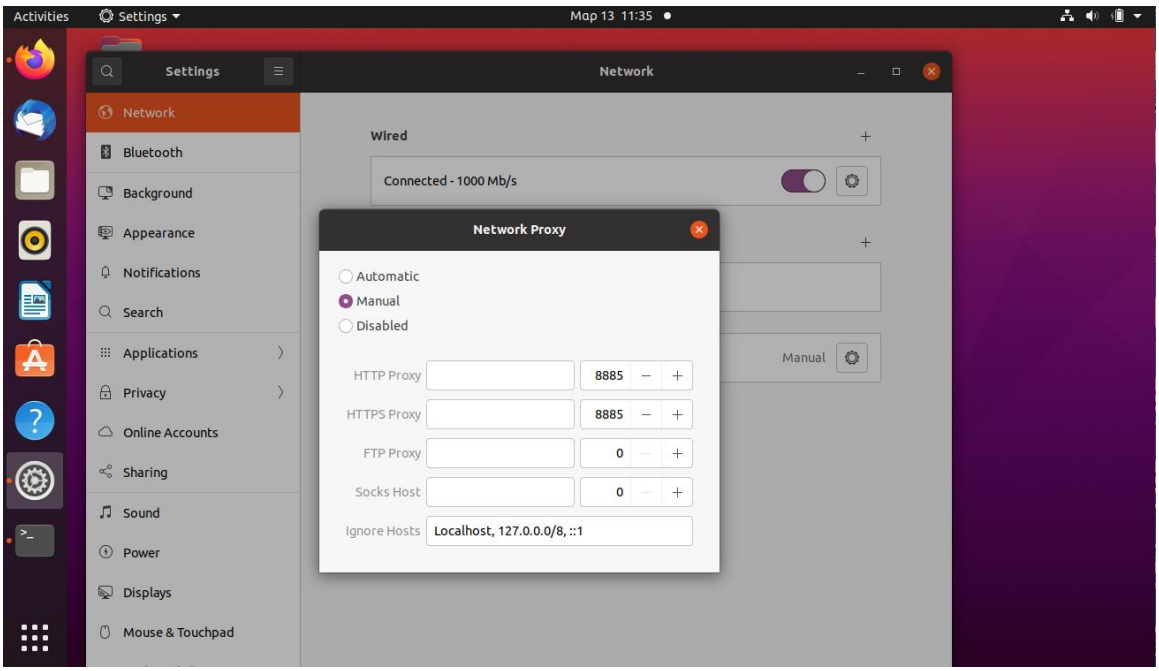
β. Το λειτουργικό Ubuntu είναι το λογισμικό ανοιχτού κώδικα το οποίο έχει επιλεγεί για την εγκατάσταση του mitmproxy μεσολαβητή, η λειτούργει του θα πραγματοποιηθεί με την χρήση της εικονική μηχανή VirtuaBox, επίσης για την ενεργοποίηση του μεσολαβητή θα χρησιμοποιηθούν οι ακόλουθες εντολές, καθώς και η παραμετροποιήσεις της κάρτας δικτύου του VirtuaBox, όπου θα επιτρέπει την δικτυακή κίνηση από τον χρήστη με λογισμικό Windows 10 στο Ubuntu λογισμικό ανοιχτού κώδικα και έπειτα στο διαδίκτυο όπως και αντίστροφα.



Σχήμα 5.2: Απεικονίζεται η ρύθμιση που χρειάζεται να πραγματοποιηθεί ώστε να υπάρξει επικοινωνία μεταξύ διακομιστή μεσολάβησης και χρήστη.

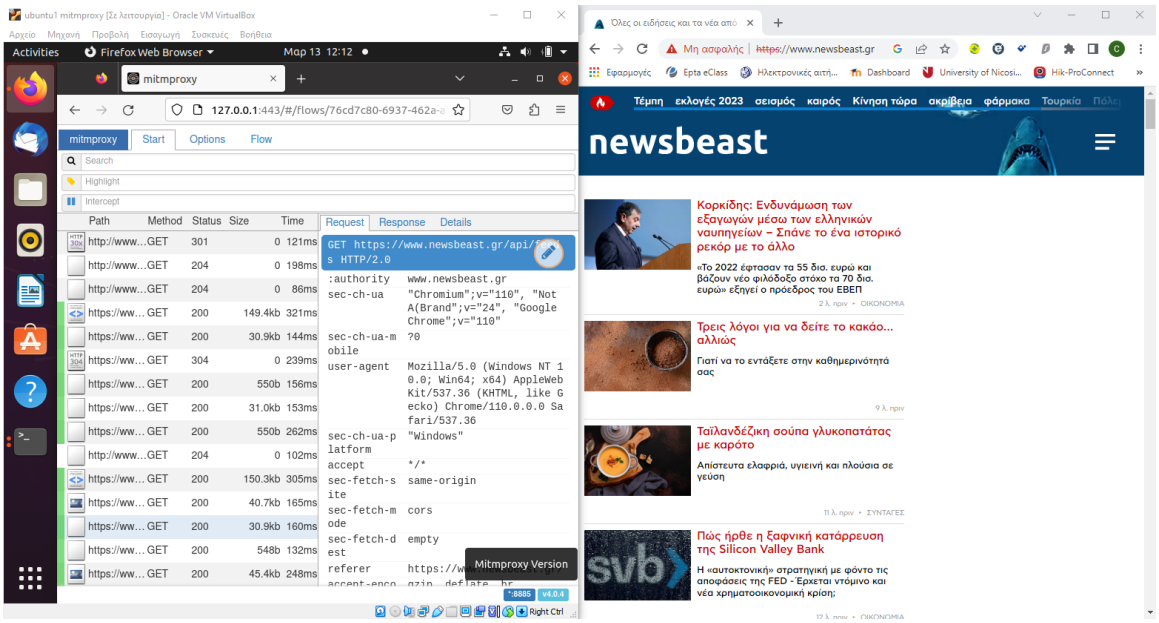
Στην εικόνα 5.2 πραγματοποιείται γεφύρωση της ιδεατής κάρτα δικτύου με την φυσική, καθώς με την ρύθμιση δεν απαιτείται προσθήκη πρόσθετης ιδεατής κάρτας δικτύου.

- sudo apt-get update && sudo apt-get upgrade.
  Πριν πραγματοποιηθεί η εγκατάσταση γίνεται ενημέρωση του λειτουργικού, ώστε να υπάρχει η τελευταία βελτίωση στην ασφάλεια, επιδιορθώσεις σφαλμάτων που υπήρχαν, με σκοπό να βελτιωθεί η απόδοση του λειτουργικού συστήματος.
- sudo apt-get install mitmproxy.
  Εντολή για την εγκατάσταση του διακομιστή μεσολάβησης mitmproxy.
- sudo mitmproxy -p 8880.
  Με την εντολή προσδιορίζουμε την πόρτα η οποία είναι μεταξύ του πελάτη και του διακομιστή μεσολάβησης TLS/SSL, έχει επιλεγεί η πόρτα 8880.
- sudo mitmweb -p 8880 --web-port 443.
  Η εντολή όπου προσδιορίζουμε την κίνηση εκτός από την πόρτα μεταξύ πελάτη και διακομιστή μεσολάβησης, αλλά και μεταξύ του διακομιστή μεσολάβησης με το διαδίκτυο. Έχει επιλεγεί η πόρτα 443 όπου υποστηρίζει την κρυπτογράφηση, οι σελίδες έχουν την ένδειξη https. Επίσης μπορεί να χρησιμοποιηθεί για την 443 η πόρτα 10443, όπου είναι η δευτερεύων πόρτα για την σύνδεση σε διακομιστές μέσω του πρωτοκόλλου SSL/TLS.



Σχήμα 5.3: Απεικονίζεται η ρύθμιση στο Ubuntu, ώστε να καθοριστεί με πια πόρτα θα επικοινωνεί ο διακομιστής μεσολάβησης με τον χρήστη.

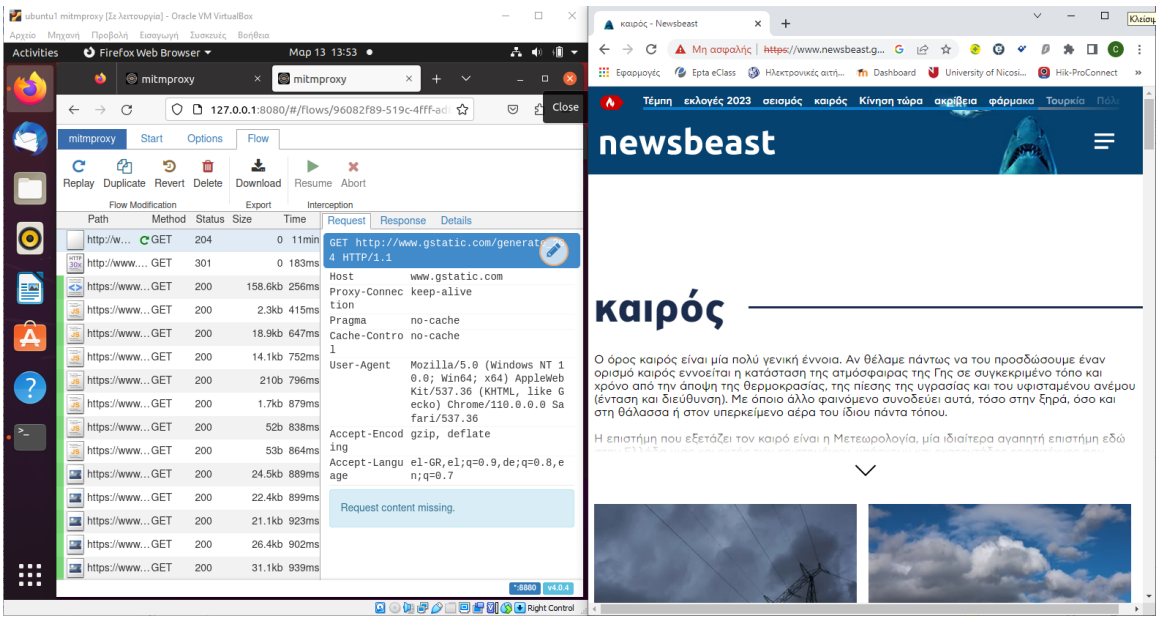
Στην συνέχεια με την βοήθεια της διεύθυνση http://127.0.0.1:443, θα πραγματοποιηθεί έλεγχος στην δικτυακή κίνηση των δεδομένων, μεταξύ του χρήστη και του διαδικτύου από τον διακομιστή μεσολάβησης.



Σχήμα 5.4: Απεικονίζεται η καταγραφή της κίνησης μεταξύ του διακομιστή μεσολάβησης και του ιστότοπου τον οποίο έχει επισκεφτεί ο χρήστης, η κίνηση είναι κρυπτογραφημένη.

- sudo mitmweb –p 8885 –web-port 8080.

Με την εντολή πραγματοποιείται μια σύνδεση με την χρήση της πόρτας 8080, όπου άφορα μια δικτυακή κίνηση η οποία δεν είναι κρυπτογραφημένη μεταξύ του διαδικτύου και του διακομιστή μεσολάβησης.



Σχήμα 5.5: Απεικονίζεται η καταγραφή της κίνησης μεταξύ του διακομιστή μεσολάβησης και του ιστότοπου τον οποίο έχει επισκεφτεί ο χρήστης, η κίνηση δεν είναι κρυπτογραφημένη.

γ. Μεταξύ τον δυο καταγραφών όπου έχουν πραγματοποιηθεί παραπάνω, συμπεραίνουμε ότι, η κρυπτογράφηση της κυκλοφορίας μπορεί να εισαγάγει κάποια επιπλέον επιβάρυνση που μπορεί να επιβραδύνει την απόδοση του δικτύου σε σύγκριση με την μη κρυπτογραφημένη κίνηση. Αυτό συμβαίνει επειδή η διαδικασία κρυπτογράφησης και αποκρυπτογράφησης δεδομένων απαιτεί πρόσθετη επεξεργαστική ισχύ και χρόνο. Όταν τα δεδομένα είναι κρυπτογραφημένα, πρέπει να μετατραπούν σε μη αναγνώσιμη μορφή χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης. Αυτή η διαδικασία μπορεί να είναι υπολογιστικά εντατική, ειδικά για μεγάλους όγκους δεδομένων. Επιπλέον, τα κρυπτογραφημένα δεδομένα πρέπει να μεταδίδονται μέσω του δικτύου, γεγονός που μπορεί να αυξήσει περαιτέρω τον χρόνο επεξεργασίας. Στο άκρο λήψης, τα κρυπτογραφημένα δεδομένα πρέπει να αποκρυπτογραφηθούν χρησιμοποιώντας έναν αλγόριθμο αποκρυπτογράφησης, ο οποίος απαιτεί επίσης επεξεργαστική ισχύ και χρόνο. Αυτό μπορεί να αυξήσει τη συνολική καθυστέρηση στην παράδοση των δεδομένων. Επιπλέον, τα οφέλη της κρυπτογράφησης όσον αφορά την ασφάλεια των δεδομένων και το απόρρητο συχνά υπερτερούν του αντίκτυπου στην απόδοση.

δ. Από του ελέγχους που έχουν πραγματοποιηθεί παραπάνω θα πρέπει να σημειωθεί ότι, ορισμένοι ιστότοποι όπως η theguardia.com, αποτρέπουν την κίνηση μέσω διακομιστή μεσολάβησης χρησιμοποιώντας το πρότυπο HSTS όπου σημαίνει "HTTP Strict Transport Security", διότι θα πρέπει στον περιηγητή να έχει εγκατασταθεί ένα έγκαιρο πιστοποιητικό του διακομιστή μεσολάβησης. Είναι μια πολιτική ασφαλείας που εφαρμόζεται σε διακομιστές ιστού για την

προστασία από επιθέσεις man-in-the-middle (MITM) που θα μπορούσαν να θέσουν σε κίνδυνο την ασφάλεια των ευαίσθητων δεδομένων χρήστη. Όταν ένας ιστότοπος ενεργοποιεί το HSTS, τα προγράμματα περιήγησης ιστού έχουν πρόσβαση στον ιστότοπο μόνο χρησιμοποιώντας μια ασφαλή σύνδεση HTTPS. Αυτό διασφαλίζει ότι τυχόν δεδομένα που αποστέλλονται μεταξύ του προγράμματος περιήγησης του χρήστη και του διακομιστή του ιστότοπου είναι κρυπτογραφημένα και δεν μπορούν να υποκλαπούν από εισβολείς. Το HSTS λειτουργεί προσθέτοντας μια κεφαλίδα απόκρισης σε όλες τις απαντήσεις HTTP που δίνει εντολή στο πρόγραμμα περιήγησης του χρήστη να συνδέεται στον ιστότοπο μόνο μέσω HTTPS για μια καθορισμένη χρονική περίοδο. Αυτό αποτρέπει τους εισβολείς από το να υποκλέψουν ή να χειραγωγήσουν το αρχικό αίτημα HTTP για να ανακατευθύνουν τον χρήστη σε μια έκδοση του ιστότοπου που δεν είναι HTTPS. Η ενεργοποίηση του HSTS είναι μια καλή πρακτική ασφάλειας για κάθε ιστότοπο που χειρίζεται ευαίσθητα δεδομένα, όπως διαπιστευτήρια σύνδεσης ή οικονομικές πληροφορίες. Ωστόσο, είναι σημαντικό να διασφαλιστεί ότι το πιστοποιητικό SSL/TLS του ιστότοπου έχει ρυθμιστεί σωστά, καθώς ένα πιστοποιητικό με εσφαλμένη διαμόρφωση μπορεί να εξακολουθεί να αφήνει τον ιστότοπο ευάλωτο σε επιθέσεις.

ε. Στην Λειτουργιά transparent proxy ο Mitmproxy λειτουργεί ως διαφανής διακομιστής μεσολάβησης, παρεμποδίζοντας την κυκλοφορία καθώς διέρχεται από μια πύλη δικτύου. Η πύλη πρέπει να ρυθμιστεί ώστε να ανακατευθύνει την κυκλοφορία στο MITMProxy, συνήθως χρησιμοποιώντας το iptables για το firewall, ώστε να μην παρεμποδιστεί η δικτυακή κίνηση. Χρήση των ακόλουθων εντολών για την ενεργοποίηση transparent proxy:

- sudo sysctl -w net.ipv4.ip_forward=1.
  Ενεργοποίηση προώθησης της δικτυακής κίνησης ipv4.
- sudo sysctl -w net.ipv6.conf.all.forwarding=1.
  Ενεργοποίηση προώθησης της δικτυακής κίνησης ipv6.
- sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8885
  sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8885
  Ενεργοποίηση εξαιρέσεων για ipv4 στο firewall, ώστε να επιτρέπεται η εισερχόμενη κίνηση από τις θύρες 80 και 443 στη θύρα 8885.
- sudo ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8885
  sudo ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8885
  Ενεργοποίηση εξαιρέσεων για ipv6 στο firewall, ώστε να επιτρέπεται η εισερχόμενη κίνηση από τις θύρες 80 και 443 στη θύρα 8885.
- sudo mitmproxy --mode transparent
  Ενεργοποίηση Mitmproxy σε λειτουργιά transparent.

στ. Στην λειτουργιά reverse proxy ο Mitmproxy λειτουργεί ως ενδιάμεσος μεταξύ ενός πελάτη και ενός διακομιστή. Αντί να παρεμποδίζει την κυκλοφορία από έναν πελάτη σε έναν διακομιστή, το MITProxy παρεμποδίζει την κίνηση από έναν διακομιστή προς έναν πελάτη. Για την ενεργοποίηση της λειτουργίας απαιτούνται οι ακόλουθες εντολές:

- sudo mitmproxy --mode reverse:192.168.1.44
  IP του διακομιστή στον οποίο θα γίνει η επισκεψιμότητα μεσολάβησης.
- sudo mitmproxy --mode reverse:192.168.1.44 -p 8885
  Καθορισμός της θύρας στην οποία θα υπάρχει η επικοινωνία.
  Στον MITProxy για την λειτουργιά reserve proxy θα πρέπει να καθοριστεί η διεύθυνση IP και η θύρας του μηχανήματος που εκτελεί το MITProxy ως διακομιστή μεσολάβησης.

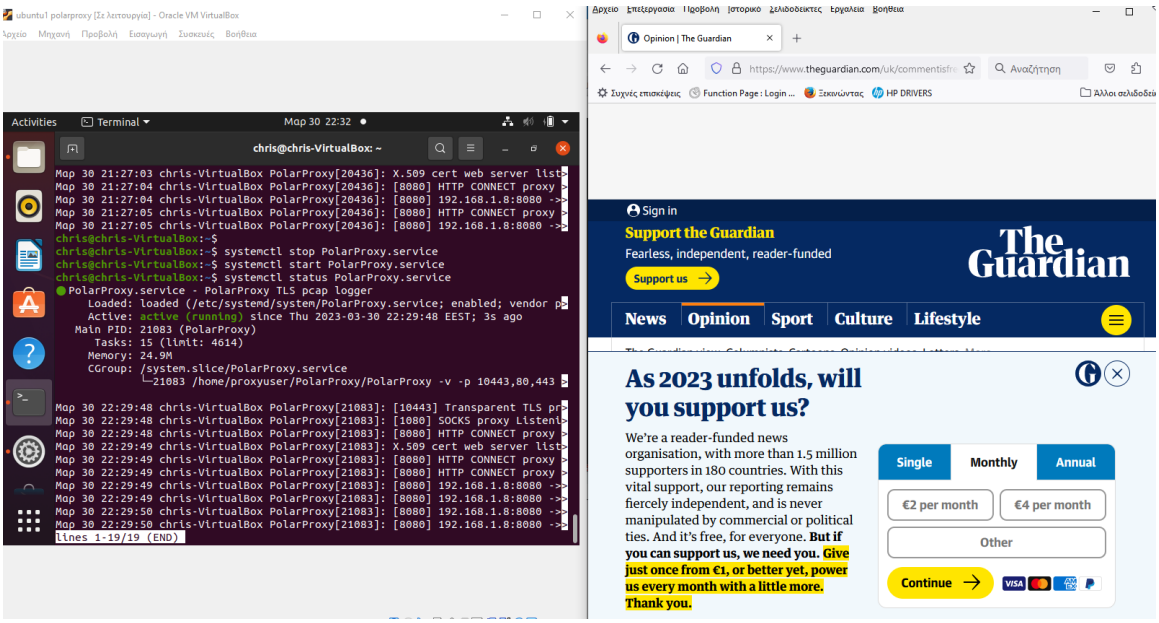
5.2 Υλοποίηση σεναρίων Polarproxy σε εικονική μηχανή

α. Θα πρέπει να γίνει η ανάλογη ρύθμιση με αυτήν που αναφερθεί στον Mitmproxy, ώστε η κίνηση του προσωπικού υπολογιστή του πελάτη να μεταφέρεται μέσω του διακομιστή μεσολάβησης, επίσης ένα έγκυρο ψηφιακό πιστοποιητικό θα πρέπει να εγκατασταθεί στον περιηγητή του χρηστή, καθώς πρόκειται για ένα πιστοποιητικό που εκδίδεται από μια αξιόπιστη αρχή έκδοσης πιστοποιητικών (CA) και χρησιμοποιείται για την επαλήθευση της ταυτότητας ενός ιστότοπου ή ενός διακομιστή. Όταν ένας χρήστης επισκέπτεται έναν ιστότοπο που χρησιμοποιεί HTTPS (HTTP μέσω SSL/TLS), το πρόγραμμα περιήγησης θα ελέγχει το ψηφιακό πιστοποιητικό για να βεβαιωθεί ότι δεν έχει λήξει, ότι έχει εκδοθεί από αξιόπιστη αρχή έκδοσης πιστοποιητικών και ότι ταιριάζει με το όνομα τομέα του ιστότοπου. Όταν ένας χρήστης επισκέπτεται τον ιστότοπο, το πρόγραμμα περιήγησής του θα λάβει το ψηφιακό πιστοποιητικό και θα το χρησιμοποιήσει για να δημιουργήσει μια ασφαλή σύνδεση με τον διακομιστή. Αυτό βοηθά στην προστασία των ευαίσθητων πληροφοριών του χρήστη, όπως κωδικούς πρόσβασης και στοιχεία πιστωτικής κάρτας από υποκλοπή ή πρόσβαση από μη εξουσιοδοτημένα τρίτα μέρη.

β. Για την εγκατάσταση του Polarproxy στο λειτουργικό Ubuntu θα χρησιμοποιηθούν οι ακόλουθες εντολές:

- sudo apt-get update && sudo apt-get upgrade
  Πριν πραγματοποιηθεί η εγκατάσταση γίνεται ενημέρωση του λειτουργικού, ώστε να υπάρχει η τελευταία βελτίωση στην ασφάλεια, επιδιορθώσεις σφαλμάτων που υπήρχαν, με σκοπό να βελτιωθεί η απόδοση του λειτουργικού συστήματος.
- sudo apt-get install polarproxy
  Εντολή για την εγκατάσταση του διακομιστή μεσολάβησης PolarProxy
- sudo adduser --system --shell /bin/bash proxyuser
  Με την εντολή θα δημιουργηθεί χρήστης στο σύστημα του Ubuntu.

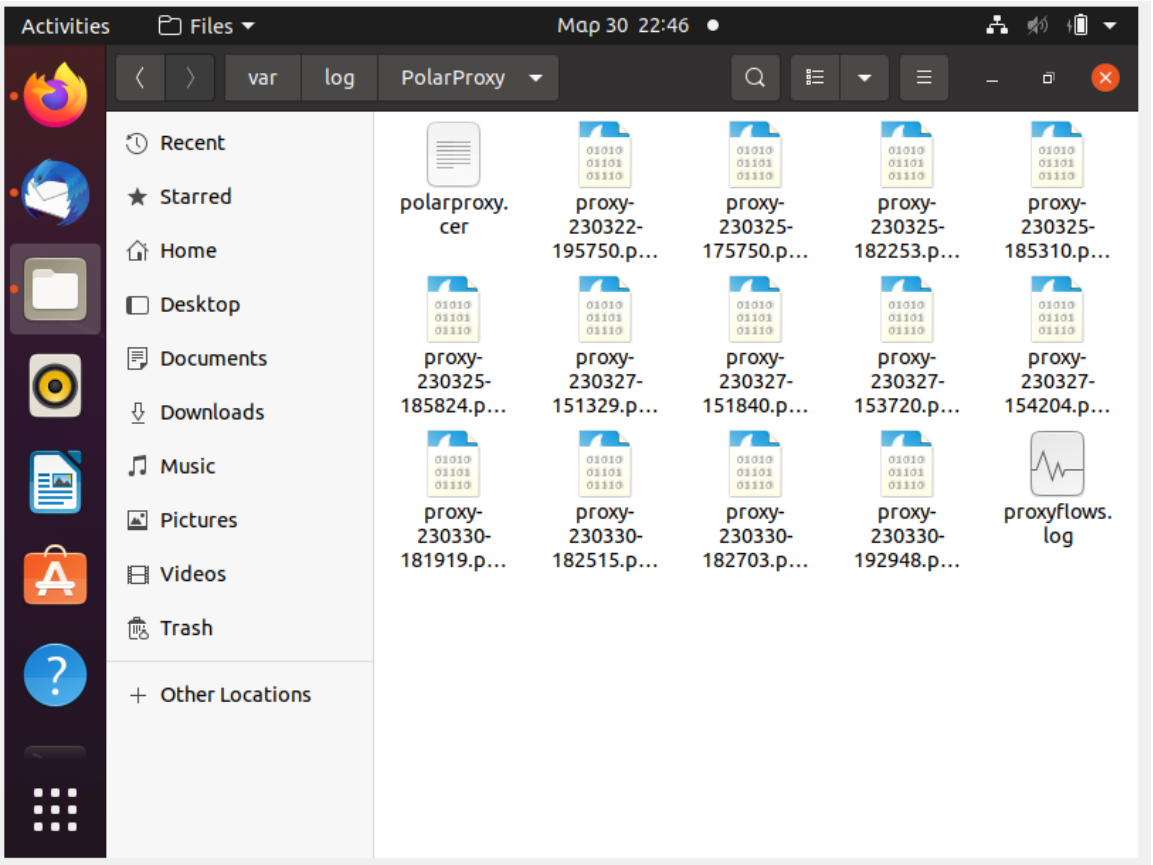
- sudo mkdir /var/log/PolarProxy
  sudo chown proxyuser:root /var/log/PolarProxy/
  sudo chmod 0775 /var/log/PolarProxy/
  Με τις εντολές δημιουργείται κατάλογος για τον proxy χρήστη.
- sudo su - proxyuser
  mkdir ~/PolarProxy
  cd ~/PolarProxy/
  curl https://www.netresec.com/?download=PolarProxy | tar -xzf -
  exit
  Με τις εντολές πραγματοποιείται λήψη και εγκατάσταση.
- sudo cp /home/proxyuser/PolarProxy/PolarProxy.service /etc/systemd/system/PolarProxy.service
  Με την εντολή γίνεται εγκατάσταση του system script για τον PolarProxy.
- sudo systemctl enable PolarProxy.service
  sudo systemctl start PolarProxy.service
  Με τις εντολές πραγματοποιείται ενεργοποίηση και ξεκίνημα του PolarProxy.
- systemctl status PolarProxy.service
  Με την εντολή πραγματοποιείται έλεγχο στην λειτουργία του PolarProxy.
- curl --insecure --connect-to www.netresec.com:443:127.0.0.1:10443 https://www.netresec.com/
  Με την εντολή πραγματοποιείται εξαγωγή αρχείων pcap, ώστε να ελεγχτούν με το wireshark.



Σχήμα 5.6: Απεικονίζεται η καταγραφή της κίνησης μεταξύ του διακομιστή μεσολάβησης και του ιστότοπου τον οποίο έχει επισκεφτεί ο χρήστης, γίνεται χρήση της δευτερεύων πόρτας για το διαδίκτυο 8080.

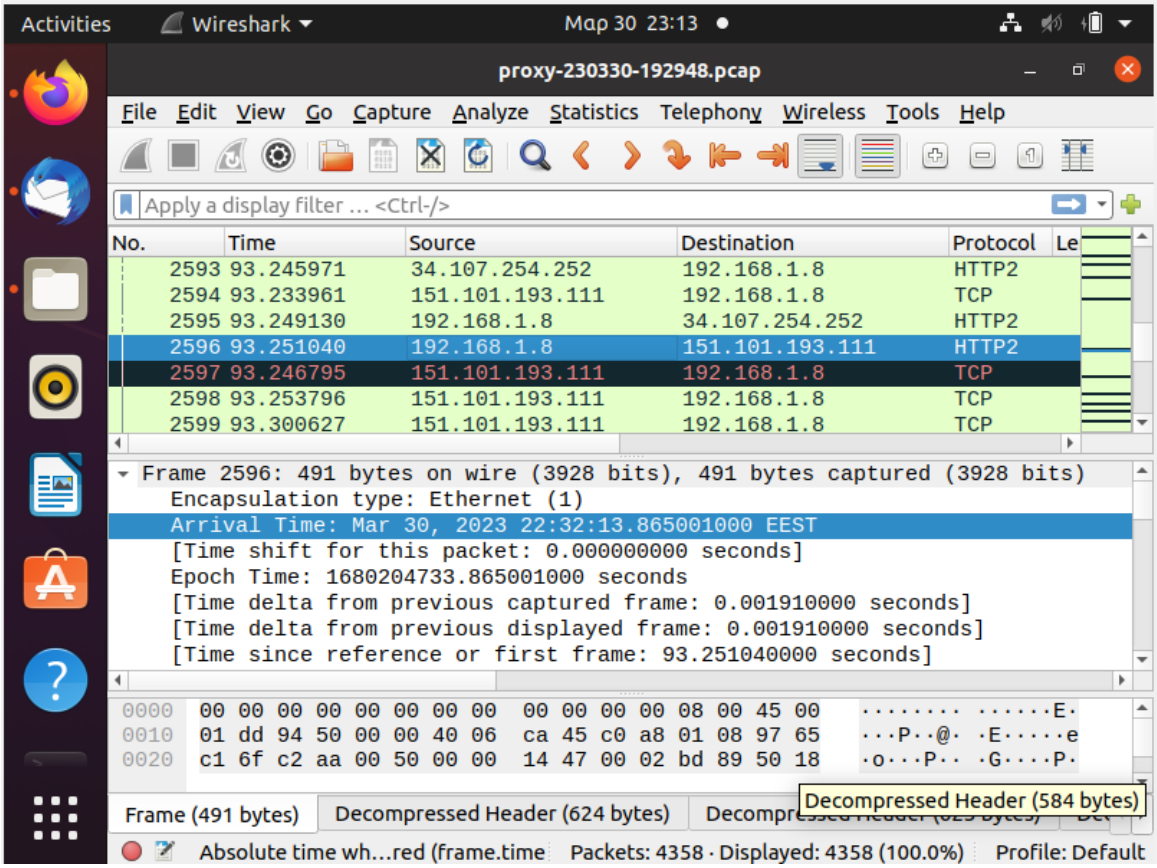
Με την έναρξη της επικοινωνίας ο PolarProxy πραγματοποιεί την καταγράφει αυτής και την αποθήκευση στην διαδρομή var/log/PolarProxy σε μορφή pcap αρχείου. Τα αρχεία pcap είναι μια μορφή αρχείου που χρησιμοποιείται από το λογισμικό λήψης πακέτων δικτύου για την αποθήκευση πακέτων δικτύου που έχουν συλληφθεί. Είναι ένα δυαδικό αρχείο που περιέχει τα ακατέργαστα δεδομένα κίνησης δικτύου, συμπεριλαμβανομένων των κεφαλίδων πακέτων, των ωφέλιμων φορτίων, τη χρονική σήμανση και άλλα μεταδιδόμενα για κάθε

πακέτο. Συνήθως χρησιμοποιούνται για ανάλυση δικτύου, αντιμετώπιση προβλημάτων και έλεγχο ασφαλείας. Μπορούν να αναλυθούν χρησιμοποιώντας λογισμικό ανάλυσης πακέτων όπως το Wireshark, το οποίο επιτρέπει στους χρήστες να εξετάζουν τα περιεχόμενα μεμονωμένων πακέτων, να φιλτράρουν να αναζητούν τα δεδομένα πακέτων, να δημιουργούν αναφορές και στατιστικά στοιχεία σχετικά με την επισκεψιμότητα.



Σχήμα 5.7: Απεικονίζεται η καταγραφή του PolarProxy από την πλοήγηση στον ιστότοπο.

Πραγματοποιείται έλεγχος στα αρχεία pcap τα οποία έχει καταγράψει ο PolarProxy, με το πρόγραμμα wireshark, ώστε να γίνει απεικόνιση της δικτυακής κίνησης.



Σχήμα 5.8: Απεικονίζεται η ανάλυση της δικτυακής κίνησης από το wireshark στα αρχεία pcap.

Με το εργαλείο Wireshark πραγματοποιείται ανάλυση την επισκεψιμότητα που καταγράφηκε, όπως την εξέταση μεμονωμένων πακέτων, το φιλτράρισμα με βάση το πρωτόκολλο ή τη διεύθυνση IP και τη δημιουργία γραφικών στατιστικών στοιχείων δικτύου, επίσης να γίνει εξαγωγή των δεδομένων που αναλύθηκαν σε διάφορες μορφές, όπως CSV ή PDF, για περαιτέρω ανάλυση ή αναφορά.

γ. Στην λειτουργιά transparent proxy ο PolarProxy μπορεί να παρεμποδίσει την κυκλοφορία χωρίς να χρειάζεται να πραγματοποιηθεί ρυθμίσετε τις συσκευής του πελάτες, ώστε να χρησιμοποιηθεί ως διακομιστής μεσολάβησης.

- sudo sysctl -w net.ipv4.ip_forward=1.
  Ενεργοποίηση προώθησης της δικτυακής κίνησης ipv4.
- sudo sysctl -w net.ipv6.conf.all.forwarding=1.
  Ενεργοποίηση προώθησης της δικτυακής κίνησης ipv6.
- sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
  sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080
  Ενεργοποίηση εξαιρέσεων για ipv4 στο firewall, ώστε να επιτρέπεται η εισερχόμενη κίνηση από τις θύρες 80 και 443 στη θύρα 8080.

- sudo ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
  sudo ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080
  Ενεργοποίηση εξαιρέσεων για ipv6 στο firewall, ώστε να επιτρέπεται η εισερχόμενη κίνηση από τις θύρες 80 και 443 στη θύρα 8080.
- sudo systemctl start polarproxy
  Με την εντολή γίνεται επανεκκίνηση του PolarProxy.
- sudo systemctl status polarproxy
  Με την εντολή γίνεται έλεγχος εάν λειτούργει σωστά.

δ. Στην λειτουργιά reverse proxy ο PolarProxy, , ακούει σε μια θύρα του τοπικού υπολογιστή και όταν λαμβάνειi κίνηση σε αυτήν τη θύρα, την προωθεί σε έναν διακομιστή προορισμού.

- sudo nano /etc/polarproxy.conf
  Με την εντολή γίνεται πρόσβαση στο config αρχείο του PolarProxy.
- mode reverse
  forward-address <192.168.1.44 >:<8080>
  Γίνεται εισαγωγή τον εντολών στο config αρχείο, ώστε να γίνει ενεργοποιήσει σε λειτουργία reserve.
- sudo systemctl start polarproxy
  Με την εντολή γίνεται επανεκκίνηση του PolarProxy.
- sudo systemctl status polarproxy
  Με την εντολή γίνεται έλεγχος εάν λειτούργει σωστά.

5.3 Υλοποίηση σεναρίων Squid proxy σε εικονική μηχανή

α. Θα πρέπει να γίνει η ανάλογη ρύθμιση, όπου έχει περιγράφει πιο πάνω, ώστε η κίνηση του προσωπικού υπολογιστή του πελάτη να μεταφέρεται μέσω του διακομιστή μεσολάβησης.

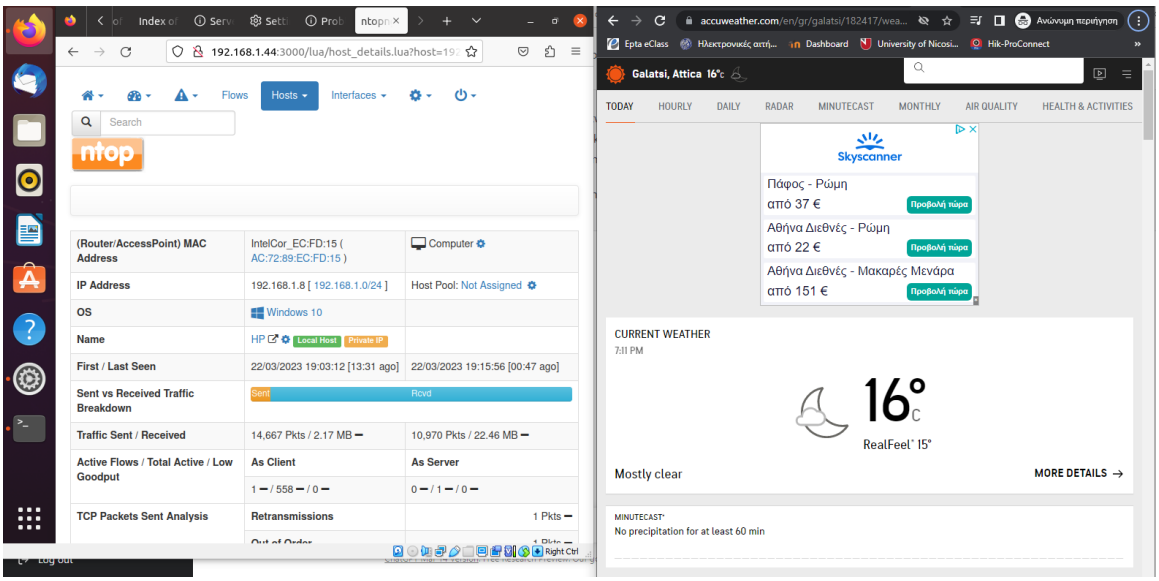
β. Για την εγκατάσταση του Squid proxy σε Ubuntu θα χρησιμοποιηθούν οι ακόλουθες εντολές.

- sudo apt-get update && sudo apt-get upgrade
  Όπου πριν πραγματοποιηθεί η εγκατάσταση γίνεται ενημέρωση του λειτουργικού.
- sudo apt install squid
  Εντολή για την εγκατάσταση του squid proxy.
- sudo nano /etc/squid/squid.conf
  Εντολή ώστε να εισέλθουμε στην παραμετροποίηση του squid proxy. Με σκοπό να γίνει καθορισμός διευθύνσεων, κρυπτογράφηση και διεπαφών όπως:
  acl localnet src 192.168.1.8. Διεύθυνση του υπολογιστή χρήστη.

acl localnet src 192.168.1.0/24. Γίνεται ο καθορισμός του εύρους των διευθύνσεων.
acl Safe_ports port 8885. Επιλογή της διεπαφής του τερματικού του πελάτη, με την οποία θα επικοινωνεί με τον διακομιστή μεσολαβητή.
acl Safe_ports port 443. Επιλογή της διεπαφής του διακομιστή μεσολαβητή, με την οποία θα επικοινωνεί με τον διακομιστή εξυπηρετητή (Web server).
http_access allow all. Επιλογή ώστε να μην υπάρχει περιορισμός στην πρόσβαση, ώστε να πραγματοποιηθούν οι έλεγχοι.
http_port 8885. Η διεπαφή του χρήστη στην οποία θα ανταποκρίνεται ο διακομιστή μεσολαβητή.

- sudo systemctl start squid
  Εντολή για την έναρξη λειτουργίας του squid proxy.
- sudo systemctl status squid
  Εντολή για τον έλεγχο της κατάστασης του squid proxy.
- sudo systemctl stop squid
  Εντολή για να σταματήσει η λειτουργιά του squid proxy.
- sudo systemctl disable squid
  Εντολή για την απενεργοποίηση της υπηρεσία Squid έτσι ώστε να μην ξεκινά αυτόματα κατά την εκκίνηση του συστήματος.

γ. Για τον έλεγχο της κίνησης του squid proxy έχει επιλεγεί το ntopng, όπου είναι λογισμικό ανοιχτού κώδικα που παρέχει πληροφορίες σε πραγματικό χρόνο για την κυκλοφορία δικτύου, συμπεριλαμβανομένων των όγκων κίνησης, των τύπων κίνησης και των πηγών και προορισμών κίνησης. Επίσης μπορεί να αποθηκεύσει ιστορικά δεδομένα κίνησης δικτύου, επιτρέποντας στους χρήστες να αναλύουν τις τάσεις της κυκλοφορίας του δικτύου με την πάροδο του χρόνου. Ακόμα μπορεί να αναλύσει την κυκλοφορία δικτύου σε επίπεδο πρωτοκόλλου, παρέχοντας πληροφορίες για τα πρωτόκολλα που χρησιμοποιούνται στο δίκτυο. Επιπλέον μπορεί να παρέχει πληροφορίες για τις εφαρμογές που δημιουργούν κίνηση δικτύου, επιτρέποντας στους χρήστες να προσδιορίζουν ποιες εφαρμογές χρησιμοποιούν το μεγαλύτερο εύρος ζώνης. Επιπροσθέτως μπορεί να παρέχει πληροφορίες γεωγραφικής τοποθεσίας για την κυκλοφορία δικτύου, επιτρέποντας στους χρήστες να βλέπουν από πού προέρχεται και πού πηγαίνει η κυκλοφορία του δικτύου. Τέλος είναι ένα ισχυρό εργαλείο για την παρακολούθηση και την ανάλυση της κυκλοφορίας του δικτύου, παρέχοντας πληροφορίες σε πραγματικό χρόνο και ιστορικά στοιχεία σχετικά με την κυκλοφορίας του δικτύου, βοηθώντας τους διαχειριστές δικτύου και τους επαγγελματίες ασφαλείας, ώστε να εντοπίσουν και να αντιμετωπίσουν προβλήματα στο δίκτυο.

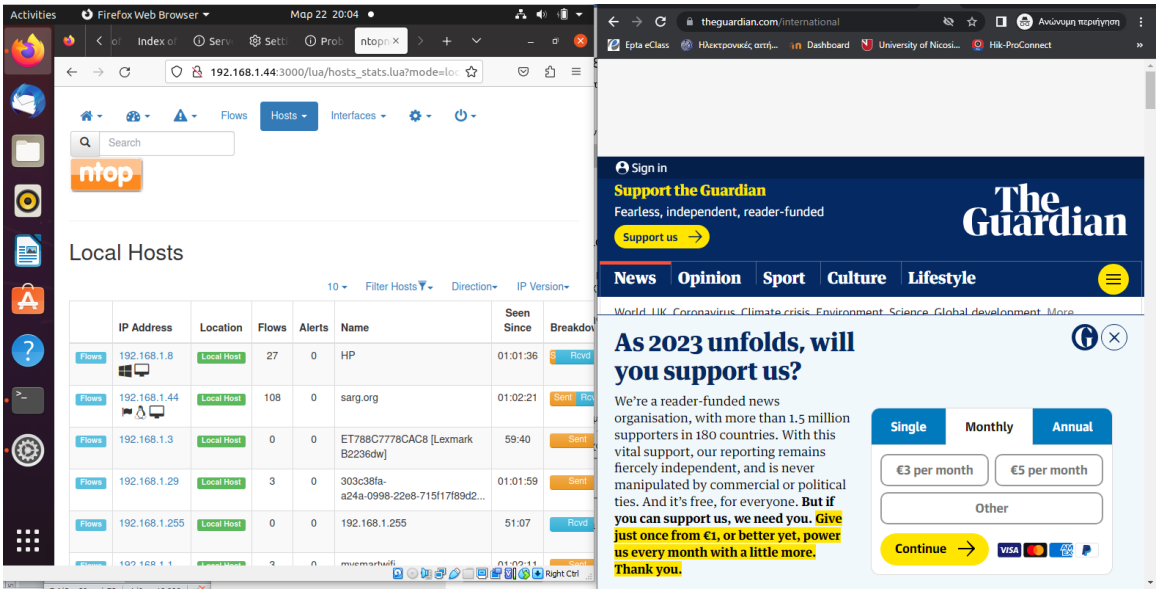


Σχήμα 5.9: Απεικονίζεται η καταγραφή της κίνησης από το ntopng, μεταξύ του διακομιστή μεσολαβητή squid proxy σε λογισμικό Ubuntu και του χρήστη σε λογισμικό Windows 10.

δ. Παραμετροποίηση του ntopng σε Ubuntu:

- sudo apt-get install ntopng
  Εντολή για την εγκατάσταση του λογισμικού ανοιχτού κώδικα για τον έλεγχο της δικτυακής κίνησης.
- vim /etc/ntopng.conf
  Εντολή για την παραμετροποίηση του ntopng.
- systemctl restart ntopng
  Εντολή για την επανεκκίνηση του ntopng.

Στην συνεχεία γίνεται επιλογή του προγράμματος περιήγησης, όπου γίνεται πληκτρολόγηση της διεύθυνσης του μεσολαβητή διακομιστή και την διεπαφή που έχει επιλεγεί από τις ρυθμίσεις, ώστε να υπάρχει πρόσβασης στο πρόγραμμα ntopg, όπως 192.168.1.44:3000.



Σχήμα 5.10: Απεικονίζεται η καταγραφή της κινήσεις στον ιστότοπο theguardian.com χωρίς να υπάρχει ο περιορισμός από το πρότυπο HSTS.

ε. Στην λειτουργιά transparent proxy ο Squid proxy λειτουργεί ως ενδιάμεσος μεταξύ του πελάτη και του διαδικτύου, παρεμποδίζοντας όλη την κίνηση HTTP και HTTPS χωρίς να απαιτεί αλλαγές διαμόρφωσης από την πλευρά του πελάτη.

- sudo nano /etc/squid/squid.conf
  Με την εντολή πραγματοποιείται πρόσβαση ώστε να γίνει παραμετροποίηση για την λειτουργία transparent proxy.
- http_port 8885 transparent
  Με την εντολή επιλέγεται η λειτουργία transparent proxy.
- sudo service squid restart
  Με την εντολή πραγματοποιείται επανεκκίνηση της υπηρεσίας Squid proxy, ώστε να αρχίσει η λειτουργία transparent proxy.
- sudo nano /etc/ufw/before.rules
  Με την εντολή πραγματοποιείται πρόσβαση στο firewall, ώστε να πραγματοποιηθεί καθορισμός των παραμέτρων.
- *nat
  :PREROUTING ACCEPT [0:0]
  -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8885
  COMMIT
  Ενεργοποίηση παραμέτρων ώστε να επιτρέπεται η πρόσβαση στην πόρτα 8885.
- sudo ufw reload
  Εντολή για την επανεκκίνηση του firewall, ώστε να τεθούν σε εφαρμογή οι νέες παραμετροποιήσεις.

στ. Στην λειτουργιά reverse proxy ο Squid proxy λειτουργεί ως διακομιστής μεσολάβησης που προωθεί αιτήματα από πελάτες σε διακομιστές στο διαδίκτυο, αποθηκεύοντας στην κρυφή μνήμη περιεχόμενα με συχνή πρόσβαση για βελτίωση της απόδοσης.

- sudo nano /etc/squid/squid.conf
  Με την εντολή πραγματοποιείται είσοδο στον config αρχείο του Squid proxy.
- http_port 80 accel defaultsite=example.com
  cache_peer example.com parent 8885 0 no-query originserver name=myAccel
  acl myDst dst 192.168.1.0/24 # Change this to your network's IP range
  http_access allow myDst
  http_access allow localhost
  http_access deny all
  cache_peer_access myAccel allow myDst
  cache_peer_access myAccel allow localhost
  cache_peer_access myAccel deny all
  Με την χρήση των εντολών στο config αρχείο διαμορφώνεται ο Squid proxy σε reserve λειτουργία, πρέπει να σημειωθεί ότι το example.com θα γίνει αλλαγή με το domain name του proxy server.
- sudo systemctl restart squid

Με την εντολή πραγματοποιείται επανεκκίνηση του Squid proxy, ώστε να εφαρμοστούν οι νέες ρυθμίσεις.

Κεφάλαιο 6

Επίλογος

Σε αυτό το κεφάλαιο θα γίνει αναφορά στα συμπεράσματα που αναδειχτήκαν από την διατριβή, όπως οι σημαντικές διαφορές μεταξύ των δρομολογητών μεσολάβησης, επιπλέον θα πραγματοποιηθεί μια αναφορά σε μια μελλοντική διατριβή, όπως επίσης και η σημαντικότητα της.

6.1 Κύρια συμπεράσματα που απορρέουν από την διατριβή

Η χρήση ένας διακομιστής μεσολάβησης μπορεί να βοηθήσει στην προστασία από ορισμένους τύπους εισβολέων ενεργώντας ως ενδιάμεσος μεταξύ του υπολογιστή και του διαδικτύου. Όταν πραγματοποιείται σύνδεση στο διαδίκτυο μέσω διακομιστή μεσολάβησης, τα αιτήματά για δεδομένα αποστέλλονται πρώτα στον διακομιστή μεσολάβησης, ο οποίος στη συνέχεια τα προωθεί στους ιστότοπους ή στους διακομιστές στους οποίους θα αποκτηθεί η πρόσβαση. Παρέχει προστασία από ανεπιθύμητες δικτυακές επιθέσεις, καθώς όταν πραγματοποιείται η σύνδεση στο διαδίκτυο μέσω διακομιστή μεσολάβησης, η διεύθυνση IP είναι κρυμμένη από τους ιστότοπους όπου πραγματοποιείται επίσκεψη, γεγονός που καθιστά πιο δύσκολο για τους εισβολείς να εντοπίσουν τις διαδικτυακές δραστηριότητες. Ακόμα μέσω του διακομιστή μεσολάβησης πραγματοποιείται φιλτράρισμα της δικτυακής κίνησης όπως το εργαλείο Wireshark όπου παρέχει πληροφορίες για την κυκλοφορία του ιστού και την ανάλυση των δεδομένων, ως αποτέλεσμα να παρεμποδίζονται οι

κακόβουλες επισκεψιμότητας, οι ιοί, τα κακόβουλα λογισμικά και οι απόπειρες ηλεκτρονικού ψαρέματος. Επιπλέων ορισμένοι διακομιστές μεσολάβησης μπορούν να ρυθμιστούν ώστε να αποκλείουν την πρόσβαση σε γνωστούς κακόβουλους ιστότοπους, αποτρέποντάς από την κατά λάθος επίσκεψη τους και πιθανή έκθεση του υπολογιστή σε κακόβουλο λογισμικό ή άλλες απειλές. Επίσης μπορούν να κρυπτογραφήσουν την επισκεψιμότητα, καθιστώντας είναι πιο δύσκολο για τους εισβολείς να υποκλέψουν και να διαβάσουν τις επικοινωνίες όπου έχουν πραγματοποιηθεί. Τέλος αξίζει να σημειωθεί ότι ενώ ένας διακομιστής μεσολάβησης μπορεί να παρέχει κάποια προστασία από εισβολείς, δεν είναι μια ολοκληρωμένη λύση. Είναι σημαντικό να χρησιμοποιούνται σε συνδυασμό και με άλλα μέτρα ασφαλείας, όπως λογισμικό προστασίας από ιούς, τείχος προστασίας και ισχυρούς κωδικούς πρόσβασης, ώστε να παρέχεται επιπρόσθετη προστασία από διαδικτυακές απειλές.

Στο πειραματικό μέρος προέκυψαν τα ακόλουθα συμπεράσματα:
Οι Mitmproxy, PolarProxy και Squid Proxy είναι όλοι δημοφιλείς διακομιστές μεσολάβησης που χρησιμοποιούνται για διάφορους σκοπούς, συμπεριλαμβανομένης της παρακολούθησης και της κυκλοφορίας του δικτύου. Ακολουθούν τα ακόλουθα συμπεράσματα από την σύγκριση αυτών των τριών εργαλείων.
Το Mitmproxy είναι ένα εργαλείο ανοιχτού κώδικα που επιτρέπει στους χρήστες να παρακολουθούν, να επιθεωρούν, να τροποποιούν και να αναπαράγουν την κυκλοφορία HTTP/HTTPS. Το Mitmproxy είναι ένα εργαλείο φιλικό προς το χρήστη, όπου κατά την ενεργοποίηση του και μέσω της διεύθυνσης και της διεπαφής που έχει καθοριστεί πραγματοποιείται έλεγχος της δικτυακής κίνησης. Υποστηρίζει αποκρυπτογράφηση και κρυπτογράφηση SSL/TLS καθώς και φιλτράρισμα της δικτυακής κίνησης. Χρησιμοποιείται ευρέως από προγραμματιστές, ελεγκτές ασφαλείας και ερευνητές για την ανάλυση και τον εντοπισμό σφαλμάτων της κυκλοφορίας του δικτύου. Κατά την ενεργοποίηση του και μέσω της διεύθυνσης και της διεπαφής που έχει καθοριστεί πραγματοποιείται έλεγχος της δικτυακής κίνησης. Η υλοποίηση του είναι αρκετά φιλική

Ο PolarProxy είναι ένας διακομιστής μεσολάβησης υψηλής απόδοσης που μπορεί να χρησιμοποιηθεί για κίνηση HTTP/HTTPS. Επίσης έχει σχεδιαστεί για να ελέγχει την δικτυακή κίνηση μεταξύ του διαδικτύου και του χρηστή, ενώ παράλληλα κάνει καταγραφή αυτής της δραστηριότητας και την εξάγει σε μορφή pcap αρχείου, ώστε να γίνει εισαγωγή στο πρόγραμμα Wireshark όπου θα πραγματοποιηθεί περεταίρω έλεγχος. Επίσης θα πρέπει ο χρήστη να έχει πραγματοποιήσει εγκατάσταση ένα έγκυρο πιστοποιητικό του PolarProxy στο τερματικό, ώστε να του επιτραπεί η επικοινωνία. Ακόμα ο PolarProxy χρησιμοποιεί μια μοναδική προσέγγιση υποκλοπής που του επιτρέπει να αναλύει και να τροποποιεί την κυκλοφορία του δικτύου χωρίς να διακόπτεται η κανονική λειτουργία της εφαρμογής. Τέλος υποστηρίζει αποκρυπτογράφηση και κρυπτογράφηση SSL/TLS

Ο Squid Proxy είναι ένας ευρέως χρησιμοποιούμενος διακομιστής μεσολάβησης που υποστηρίζει πρωτόκολλα HTTP, HTTPS και FTP. Είναι ένας διακομιστής μεσολάβησης προσωρινής αποθήκευσης που μπορεί να επιταχύνει την περιήγηση στον ιστό αποθηκεύοντας στην προσωρινή μνήμη σελίδες με συχνή πρόσβαση και μειώνοντας την κίνηση του δικτύου. Ο Squid Proxy κατά την παραμετροποίηση θα πρέπει να γίνουν

αλλαγές στο config αρχείο του, καθώς υποστηρίζει τον έλεγχο πρόσβασης, έλεγχο ταυτότητας και καταγραφή. Επίσης με την ενεργοποίηση του θα χρειαστεί επιπλέων η εγκατάσταση ενός αρχείου καταγραφής, στην παρούσα διπλωματική έχει επιλεγεί το ntopng, ώστε να υπάρχει απεικόνιση της δικτυακής κίνησης. Συχνά χρησιμοποιείται από οργανισμούς για τον έλεγχο και την παρακολούθηση της πρόσβασης στο διαδίκτυο για τους υπαλλήλους τους.

6.2 Σύντομη ανάλυση μελλοντικής εργασίας

Διαφορές στην δικτυακή κίνηση μεταξύ Proxy Server και VPN, καθώς τόσο οι διακομιστές μεσολάβησης Proxy Server όσο και τα VPN μπορούν να χρησιμοποιηθούν για τη βελτίωση του απορρήτου και της ασφάλειας στο διαδίκτυο, αλλά λειτουργούν διαφορετικά και έχουν διακριτά αποτελέσματα στην κυκλοφορία του δικτύου. Ένας διακομιστής μεσολάβησης λειτουργεί ως ενδιάμεσος μεταξύ της συσκευής ενός χρήστη και του Διαδικτύου. Όταν ένας χρήστης κάνει ένα αίτημα για έναν ιστότοπο ή έναν πόρο, το αίτημα αποστέλλεται πρώτα στον διακομιστή μεσολάβησης, ο οποίος στη συνέχεια προωθεί το αίτημα στον προορισμό που προορίζεται. Η απάντηση από τον προορισμό αποστέλλεται πίσω στον διακομιστή μεσολάβησης, ο οποίος στη συνέχεια την αναμεταδίδει στη συσκευή του χρήστη. Αυτό σημαίνει ότι όλη η κίνηση μεταξύ του χρήστη και του διαδικτύου δρομολογείται πρώτα μέσω του διακομιστή μεσολάβησης. Επίσης ένα VPN, από την άλλη πλευρά, δημιουργεί μια ασφαλή, κρυπτογραφημένη σήραγγα μεταξύ της συσκευής ενός χρήστη και ενός απομακρυσμένου διακομιστή VPN. Όλη η κίνηση που αποστέλλεται και λαμβάνεται από τη συσκευή του χρήστη είναι κρυπτογραφημένη και δρομολογημένη μέσω αυτής της σήραγγας, γεγονός που καθιστά δύσκολο για οποιονδήποτε να παρακολουθεί ή να παρακολουθεί την κυκλοφορία. Όσον αφορά την κίνηση δικτύου, η χρήση ενός διακομιστή μεσολάβησης μπορεί να έχει ως αποτέλεσμα χαμηλότερες ταχύτητες, επειδή όλα τα αιτήματα πρέπει πρώτα να αποστέλλονται στον διακομιστή μεσολάβησης πριν προωθηθούν στον προορισμό τους. Αυτό μπορεί να οδηγήσει σε αυξημένο χρόνο και πιο αργούς χρόνους φόρτωσης σελίδας. Επιπλέον, εφόσον ο διακομιστής μεσολάβησης είναι ενδιάμεσος, ενδέχεται να υπόκειται σε περιορισμούς στους οποίους δεν υπόκειται η συσκευή του χρήστη ή ο διακομιστής προορισμού. Από την άλλη η χρήση ενός VPN, μπορεί να οδηγήσει σε ελαφρώς πιο αργές ταχύτητες λόγω της κρυπτογράφησης και της δρομολόγησης της κυκλοφορίας μέσω του διακομιστή VPN, αλλά η αντιστάθμιση είναι η αυξημένη ασφάλεια και το απόρρητο. Όλη η επισκεψιμότητα είναι κρυπτογραφημένη και παραμένει ιδιωτική, ακόμη και αν υποκλαπεί, και η διεύθυνση IP του χρήστη καλύπτεται, καθιστώντας δύσκολη την παρακολούθηση της διαδικτυακής τους δραστηριότητας. Ολοκληρώνοντας, η επιλογή μεταξύ χρήσης διακομιστή μεσολάβησης Proxy Server ή VPN θα εξαρτηθεί από τις συγκεκριμένες ανάγκες και προτεραιότητες του χρήστη. Εάν το απόρρητο και η ασφάλεια είναι οι κύριες προτεραιότητες, τότε ένα VPN μπορεί να είναι η καλύτερη επιλογή, αλλά εάν ο στόχος είναι η πρόσβαση σε περιορισμένο περιεχόμενο ή το φιλτράρισμα συγκεκριμένων τύπων επισκεψιμότητας, τότε ένας διακομιστής μεσολάβησης Proxy Server είναι πιο κατάλληλη επιλογή.

Βιβλιογραφία

1. The world's 10 biggest cybercrime hotspots in 2016, ranked, available on https://www.globaltechcouncil.org/blockchain/worlds-top-10-cyber-crime-hotspots/, (accessed Oct. 05, 2022).
2. ZEWYA, UAE saw almost 70,000 cyberattacks on smartphones in 2020, available on https://www.intelligentciso.com/2020/06/18/uae-saw-almost-70000-cyberattacks-on-smartphones-in-2020-with-an-increase-during-quarantine, (accessed Oct. 14, 2022).
3. Norton Rose Fulbright, WannaCry Ransomware Attack Summary, available on https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/, (accessed Oct. 14, 2022).
4. Filip Truta, Microsoft: Phishing Attacks Increased 250% from January to December 2018, available on https://securityboulevard.com , (accessed Oct. 18, 2022).
5. Nadav, Global DDoS Threat Landscape Report, available on https://www.imperva.com/blog/2019-global-ddosthreat-landscape-report/, (accessed Oct. 21, 2022).
6. T. Dierks and C. Allen, “The TLS Protocol Version 1.0,” RFC 2246, Jan. 1999
7. P. Velan, "A survey of methods for encrypted traffic classification and analysis", International Journal of Network Management, vol. 25, pp. 355-374, 2015.
8. T. Dierks, E. R. The Transport Layer Security (TLS) Protocol Version 1.2. Proposed standard, Aug. 2008.
9. M. O'Neill et al., "TLS Proxies: Friend or Foe?", Proc. Internet Measurement Conf., pp. 551-557, 2016.
10. K. M. Elleithy, D. Blagovic, W. Cheng, and P. Sideleau, “Denial of Service Attack Techniques: Analysis, Implementation and Comparison,” Journal of Systemics, Cybernetics and Informatics, vol. 3, pp. 66–71, 2006.
11. Anna M. Johnston, Peter S. Gemmell, ”Authenticated Key Exchange Provably Secure against the Man-in-the-Middle Attack”, 2001
12. Ee Hung Chang, Kang Leng Chiew, San Nah Sze, and Wei King Tiong. Phishing detection via identification of website identity. In 2013 International Conference on IT Convergence and Security, pp. 1–4. IEEE, 2013.
13. M. Gandhi and JwalantBaria, “SQL injection attacks in web application,” International Journal of Soft Computing and Engineering (IJSCE), vol. 2, pp. 2231-2307, Jan 2013.

14. BooJoong Kang, Kyoung Soo Han, Byeongho Kang, and Eul Gyu Im. Malware categorization using dynamic mnemonic frequency analysis with redundancy filtering. Digital Investigation, pp. 323–335, Dec. 2014.
15. J. H. Kim, G. S. Choi, and C. R. Das, "An SSL back-end forwarding scheme in cluster-based web servers," IEEE Trans. on Parallel and Distributed Systems, vol. 18, pp. 946-957, June 2007.
16. R. Mraz, "Secure blue: an architecture for a scalable, reliable high volume SSL internet server," in Proc. 17th Annual Computer Security Applications Conference, New Orleans, pp. 391-398, 2001.
17. Netcraft. Half a Million Widely Trusted Websites Vulnerable to Heartbleed Bug. available on: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html, (accessed Oct. 29, 2022).
18. J. Vehent. SSL/TLS analysis of the Internet's top 1,000,000 websites. available on https://jve.linuxwall.info/blog/index.php?post/TLS_Survey, προσπελάστηκε (accessed Nov. 02, 2022).
19. P. Bilski and W. Winiecki, "Multi-core implementation of the symmetric cryptography algorithms in the measurement system," Measurement, vol. 43, pp. 1049-1060, Oct. 2010.
20. T. Dierks and C. Allen, "The TLS Protocol Version 1.0," RFC 2246 (Proposed Standard), Internet Engineering Task Force. available on http://www.ietf.org/rfc/rfc2246.txt, (accessed Nov. 04, 2022).
21. Brice Canvel, Alain P. Hiltgen, Serge Vaudenay, and Martin Vuagnoux. Password interception in a SSL/TLS channel. pp. 583–599, 2003.
22. A. Adelsbach, S. Gajek, and J. Schwenk, "Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures," in Information Secu-rity Practice and Experience, ser. Lecture Notes in Computer Science,R. Deng, F. Bao, H. Pang, and J. Zhou, Eds. Springer Berlin Heidelberg, pp. 204–216, 2005.
23. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: an empirical study of SSL warning effectiveness," in Proceedings of the 18th conference on USENIX security symposium, ser. SSYM'09.USENIX Association, pp. 399–416, 2009.
24. OpenSSL Project. Cryptography and ssl/tls toolkit. available on http://openssl.org/, (accessed Nov. 18, 2022).

25. WolfSSL version 5.5.3. available on https://www.wolfssl.com, (accessed Nov. 19, 2022).
26. Gnussl version 3.7.8. available on https://www.gnutls.org/, (accessed Nov. 21, 2022).
27. Mitm version 9.0 available on https://mitmproxy.org/, (accessed Nov. 21, 2022).
28. Daniel Roethlisberger. Sslsplit - transparent ssl/tls interception. available on https://www.roe.ch/SSLsplit, (accessed Nov. 23, 2022).
29. Polarproxy available on https://www.netresec.com/?page=PolarProxy (accessed Nov. 24, 2022).
30. Squid proxy available on http://www.squid-cache.org/ (accessed Nov. 26, 2022).
31. Στο 25th USENIX Security Symposium available on https://www.usenix.org/conference/usenixsecurity16/technicalsessions/presentation/aviram, (accessed Nov. 30, 2022).
32. D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. Halderman, N. Heninger, D. Springall, E. Thome, L. Valenta, B. Vandersloot, E. Wustrow, and S. Paul, conference Diffie-Hellman fails in practice. Available on https://dl.acm.org/doi/proceedings/10.1145/2810103, (accessed Dec. 01, 2022).
33. B. Moller, T. Duong, and K. Kotowicz, available on https://www.openssl.org/~bodo/ssl-poodle.pdf, (accessed Dec. 04, 2022).
34. D. Boneh and G. Durfee. "Cryptanalysis of RSA with Private Key d Less than n 0.292.", IEEE Trans. Information Theory, vol. 46 pp. 1339–1349, June 2000.
35. V. Rijmen and J. Daemen. Advanced Encryption Standard, available on https://www.nist.gov/publications/advanced-encryption-standard-aes, (accessed Dec. 05, 2022).
36. A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique, "cryptanalysis of the full AES. In Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security", pp. 344–371, 2011.
37. X. Wang and H. Yu., "How to Break MD5 and Other Hash Functions. In Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques", pp. 19–35, 2005.
38. Biham, E., Chen, R., Joux, A., Carribault, P., Jalby, W., Lemuet, C.: Collisions in SHA-0 and Reduced SHA-1, "Annual International Conference on the Theory and Applications of Cryptographic Techniques", pp 36–57. Springer, Heidelberg 2005.
39. JSSE available on https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html (accessed Mar. 2, 2023).

40. Schannel SSP available on https://learn.microsoft.com/en-us/windows-server/security/tls/tls-ssl-schannel-ssp-overview (accessed Mar. 2, 2023).
41. Network Security Services available on https://developer.mozilla.org/en-US/docs/NSS (accessed Mar. 5, 2023).
42. w3techs Usage statistics of web servers available on https://w3techs.com/technologies/overview/web_server (accessed Mar. 5, 2023).
43. w3techs Popular Browsers available on https://www.w3schools.com/browsers/ (accessed Mar. 6, 2023).
44. Virtualbox available on https://www.virtualbox.org/ (accessed Jen. 14, 2023).
45. Ubuntu available on https://ubuntu.com (accessed Jen. 14, 2023).
46. Wireshark available on https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html (accessed Mar. 12, 2023).

Παράρτημα Α

Config αρχείο του Squid proxy

A.1 Config file

***** ACL TYPES AVAILABLE *****

#

acl aclname src ip-address/mask ... # clients IP address [fast]

acl aclname src addr1-addr2/mask ... # range of addresses [fast]

acl aclname dst [-n] ip-address/mask ... # URL host's IP address [slow]

acl aclname localip ip-address/mask ... # IP address the client connected to [fast]

#

#if USE_SQUID_EUI

acl aclname arp mac-address ...

acl aclname eui64 eui64-address ...

[fast]

MAC (EUI-48) and EUI-64 addresses use xx:xx:xx:xx:xx:xx notation.

# #

The 'arp' ACL code is not portable to all operating systems.

It works on Linux, Solaris, Windows, FreeBSD, and some other

BSD variants.
# #
The eui_lookup directive is required to be 'on' (the default)
and Squid built with --enable-eui for MAC/EUI addresses to be
available for this ACL.
# #
Squid can only determine the MAC/EUI address for IPv4
clients that are on the same subnet. If the client is on a
different subnet, then Squid cannot find out its address.
# #
IPv6 protocol does not contain ARP. MAC/EUI is either
encoded directly in the IPv6 address or not available.
#endif
acl aclname clientside_mark mark[/mask] ...
matches CONNMARK of an accepted connection [fast]
# #
mark and mask are unsigned integers (hex, octal, or decimal).
If multiple marks are given, then the ACL matches if at least
one mark matches.
# #
Uses netfilter-conntrack library.
Requires building Squid with --enable-linux-netfilter.
# #
The client, various intermediaries, and Squid itself may set
CONNMARK at various times. The last CONNMARK set wins. This ACL
checks the mark present on an accepted connection or set by
Squid afterwards, depending on the ACL check timing. This ACL
effectively ignores any mark set by other agents after Squid has
accepted the connection.
#
acl aclname srcdomain .foo.com ...
reverse lookup, from client IP [slow]
acl aclname dstdomain [-n] .foo.com ...
Destination server from URL [fast]

acl aclname srcdom_regex [-i] \.foo\.com ...
regex matching client name [slow]
acl aclname dstdom_regex [-n] [-i] \.foo\.com ...
regex matching server [fast]
# #
For dstdomain and dstdom_regex a reverse lookup is tried if a IP
based URL is used and no match is found. The name "none" is used
if the reverse lookup fails.
#
acl aclname src_as number ...
acl aclname dst_as number ...
[fast]
Except for access control, AS numbers can be used for
routing of requests to specific caches. Here's an
example for routing all requests for AS#1241 and only
those to mycache.mydomain.net:

acl asexample dst_as 1241
cache_peer_access mycache.mydomain.net allow asexample
cache_peer_access mycache_mydomain.net deny all
#
acl aclname peername myPeer ...
acl aclname peername_regex [-i] regex-pattern ...
[fast]
match against a named cache_peer entry
set unique name= on cache_peer lines for reliable use.
#
acl aclname time [day-abbrevs] [h1:m1-h2:m2]
[fast]
day-abbrevs:
S - Sunday
M - Monday
T - Tuesday
W - Wednesday

H - Thursday
F - Friday
A - Saturday
h1:m1 must be less than h2:m2
#
acl aclname url_regex [-i] ^http:// ...
regex matching on whole URL [fast]
acl aclname urllogin [-i] [^a-zA-Z0-9] ...
regex matching on URL login field
acl aclname urlpath_regex [-i] \.gif$ ...
regex matching on URL path [fast]
#
acl aclname port 80 70 21 0-1024... # destination TCP port [fast]
ranges are alloed
acl aclname localport 3128 ... # TCP port the client connected to [fast]
NP: for interception mode this is usually '80'
#
acl aclname myportname 3128 ... # *_port name [fast]
#
acl aclname proto HTTP FTP ... # request protocol [fast]
acl aclname method GET POST ... # HTTP request method [fast]
#
acl aclname http_status 200 301 500- 400-403 ...
status code in reply [fast]
#
acl aclname browser [-i] regexp ...
pattern match on User-Agent header (see also req_header below) [fast]
#
acl aclname referer_regex [-i] regexp ...
pattern match on Referer header [fast]
Referer is highly unreliable, so use with care
#
acl aclname ident [-i] username ...
acl aclname ident_regex [-i] pattern ...

string match on ident output [slow]
use REQUIRED to accept any non-null ident.
#
acl aclname proxy_auth [-i] username ...
acl aclname proxy_auth_regex [-i] pattern ...

perform http authentication challenge to the client and match against
supplied credentials [slow]
# #
takes a list of allowed usernames.
use REQUIRED to accept any valid username.
# #
Will use proxy authentication in forward-proxy scenarios, and plain
http authenticaiton in reverse-proxy scenarios
# #
NOTE: when a Proxy-Authentication header is sent but it is not
needed during ACL checking the username is NOT logged
in access.log.
# #
NOTE: proxy_auth requires a EXTERNAL authentication program
to check username/password combinations (see
auth_param directive).
# #
NOTE: proxy_auth can't be used in a transparent/intercepting proxy
as the browser needs to be configured for using a proxy in order
to respond to proxy authentication.
#
acl aclname snmp_community string ...
A community string to limit access to your SNMP Agent [fast]
Example:
# #
acl snmppublic snmp_community public
#
acl aclname maxconn number

This will be matched when the client's IP address has
more than <number> TCP connections established. [fast]
NOTE: This only measures direct TCP links so X-Forwarded-For
indirect clients are not counted.
#
acl aclname max_user_ip [-s] number
This will be matched when the user attempts to log in from more
than <number> different ip addresses. The authenticate_ip_ttl
parameter controls the timeout on the ip entries. [fast]
If -s is specified the limit is strict, denying browsing
from any further IP addresses until the ttl has expired. Without
-s Squid will just annoy the user by "randomly" denying requests.
(the counter is reset each time the limit is reached and a
request is denied)
NOTE: in acceleration mode or where there is mesh of child proxies,
clients may appear to come from multiple addresses if they are
going through proxy farms, so a limit of 1 may cause user problems.
#
acl aclname random probability
Pseudo-randomly match requests. Based on the probability given.
Probability may be written as a decimal (0.333), fraction (1/3)
or ratio of matches:non-matches (3:5).
#
acl aclname req_mime_type [-i] mime-type ...
regex match against the mime type of the request generated
by the client. Can be used to detect file upload or some
types HTTP tunneling requests [fast]
NOTE: This does NOT match the reply. You cannot use this
to match the returned file type.

#
acl aclname req_header header-name [-i] any\.regex\.here
regex match against any of the known request headers. May be
thought of as a superset of "browser", "referer" and "mime-type"

ACL [fast]
#
acl aclname rep_mime_type [-i] mime-type ...
regex match against the mime type of the reply received by
squid. Can be used to detect file download or some
types HTTP tunneling requests. [fast]
NOTE: This has no effect in http_access rules. It only has
effect in rules that affect the reply data stream such as
http_reply_access.
#
acl aclname rep_header header-name [-i] any\.regex\.here
regex match against any of the known reply headers. May be
thought of as a superset of "browser", "referer" and "mime-type"
ACLs [fast]
#
acl aclname external class_name [arguments...]
external ACL lookup via a helper class defined by the
external_acl_type directive [slow]
#
acl aclname user_cert attribute values...
match against attributes in a user SSL certificate
attribute is one of DN/C/O/CN/L/ST or a numerical OID [fast]
#
acl aclname ca_cert attribute values...
match against attributes a users issuing CA SSL certificate
attribute is one of DN/C/O/CN/L/ST or a numerical OID [fast]
#
acl aclname ext_user [-i] username ...
acl aclname ext_user_regex [-i] pattern ...
string match on username returned by external acl helper [slow]
use REQUIRED to accept any non-null user name.
#
acl aclname tag tagvalue ...
string match on tag returned by external acl helper [fast]

DEPRECATED. Only the first tag will match with this ACL.
Use the 'note' ACL instead for handling multiple tag values.
#
acl aclname hier_code codename ...
string match against squid hierarchy code(s); [fast]
e.g., DIRECT, PARENT_HIT, NONE, etc.
# #
NOTE: This has no effect in http_access rules. It only has
effect in rules that affect the reply data stream such as
http_reply_access.
#
acl aclname note [-m[=delimiters]] name [value ...]
match transaction annotation [fast]
Without values, matches any annotation with a given name.
With value(s), matches any annotation with a given name that
also has one of the given values.
If the -m flag is used, then the value of the named
annotation is interpreted as a list of tokens, and the ACL
matches individual name=token pairs rather than whole

name=value pairs. See "ACL Options" above for more info.
Annotation sources include note and adaptation_meta directives
as well as helper and eCAP responses.
#
acl aclname adaptation_service service ...
Matches the name of any icap_service, ecap_service,
adaptation_service_set, or adaptation_service_chain that Squid
has used (or attempted to use) for the master transaction.
This ACL must be defined after the corresponding adaptation
service is named in squid.conf. This ACL is usable with
adaptation_meta because it starts matching immediately after
the service has been selected for adaptation.
#
acl aclname transaction_initiator initiator ...

Matches transaction's initiator [fast]
# #
Supported initiators are:
esi: matches transactions fetching ESI resources
certificate-fetching: matches transactions fetching
a missing intermediate TLS certificate
cache-digest: matches transactions fetching Cache Digests
from a cache_peer
htcp: matches HTCP requests from peers
icp: matches ICP requests to peers
icmp: matches ICMP RTT database (NetDB) requests to peers
asn: matches asns db requests
internal: matches any of the above
client: matches transactions containing an HTTP or FTP
client request received at a Squid *_port
all: matches any transaction, including internal transactions
without a configurable initiator and hopefully rare
transactions without a known-to-Squid initiator
# #
Multiple initiators are ORed.
#
acl aclname has component
matches a transaction "component" [fast]
# #
Supported transaction components are:
request: transaction has a request header (at least)
response: transaction has a response header (at least)
ALE: transaction has an internally-generated Access Log Entry
structure; bugs notwithstanding, all transaction have it
# #
For example, the following configuration helps when dealing with HTTP
clients that close connections without sending a request header:
# #
acl hasRequest has request

acl logMe note important_transaction
avoid "logMe ACL is used in context without an HTTP request" warnings
access_log ... logformat=detailed hasRequest logMe
log request-less transactions, instead of ignoring them
access_log ... logformat=brief !hasRequest
# #
Multiple components are not supported for one "acl" rule, but
can be specified (and are ORed) using multiple same-name rules:
# #

OK, this strange logging daemon needs request or response,
but can work without either a request or a response:
acl hasWhatMyLoggingDaemonNeeds has request
acl hasWhatMyLoggingDaemonNeeds has response
#
acl aclname any-of acl1 acl2 ...
match any one of the acls [fast or slow]
The first matching ACL stops further ACL evaluation.
# #
ACLs from multiple any-of lines with the same name are ORed.
For example, A = (a1 or a2) or (a3 or a4) can be written as
acl A any-of a1 a2
acl A any-of a3 a4
# #
This group ACL is fast if all evaluated ACLs in the group are fast
and slow otherwise.
#
acl aclname all-of acl1 acl2 ...
match all of the acls [fast or slow]
The first mismatching ACL stops further ACL evaluation.
# #
ACLs from multiple all-of lines with the same name are ORed.
For example, B = (b1 and b2) or (b3 and b4) can be written as
acl B all-of b1 b2

```
# # acl B all-of b3 b4
# #
# # This group ACL is fast if all evaluated ACLs in the group are fast
# # and slow otherwise.
#
# Examples:
# acl macaddress arp 09:00:2b:23:45:67
# acl myexample dst_as 1241
# acl password proxy_auth REQUIRED
# acl fileupload req_mime_type -i ^multipart/form-data$
# acl javascript rep_mime_type -i ^application/x-javascript$
#
#Default:
# ACLs all, manager, localhost, and to_localhost are predefined.
#
#
# Recommended minimum configuration:
#
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 0.0.0.1-0.255.255.255 # RFC 1122 "this" network (LAN)
acl localnet src 10.0.0.0/8 # RFC 1918 local private network (LAN)
acl localnet src 100.64.0.0/10 # RFC 6598 shared address space (CGN)
acl localnet src 169.254.0.0/16 # RFC 3927 link-local (directly plugged) machines
acl localnet src 172.16.0.0/12 # RFC 1918 local private network (LAN)
acl localnet src 192.168.0.0/16 # RFC 1918 local private network (LAN)
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines
acl localnet src 192.168.1.44 # test computer
acl localnet src 192.168.1.0/24

acl Safe_ports port 8885 # Customer port
acl SSL_ports port 443
```

```
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
# TAG: proxy_protocol_access
# Determine which client proxies can be trusted to provide correct
# information regarding real client IP address using PROXY protocol.
#
# Requests may pass through a chain of several other proxies
# before reaching us. The original source details may by sent in:
# * HTTP message Forwarded header, or
# * HTTP message X-Forwarded-For header, or
# * PROXY protocol connection header.
#
# This directive is solely for validating new PROXY protocol
# connections received from a port flagged with require-proxy-header.
# It is checked only once after TCP connection setup.
#
# A deny match results in TCP connection closure.
#
# An allow match is required for Squid to permit the corresponding
# TCP connection, before Squid even looks for HTTP request headers.
# If there is an allow match, Squid starts using PROXY header information
# to determine the source address of the connection for all future ACL
# checks, logging, etc.
#
# SECURITY CONSIDERATIONS:
```

#

Any host from which we accept client IP details can place

incorrect information in the relevant header, and Squid

will use the incorrect information as if it were the

source address of the request. This may enable remote

hosts to bypass any access control restrictions that are

based on the client's source addresses.

#

This clause only supports fast acl types.

#Default:

all TCP connections to ports with require-proxy-header will be denied

TAG: follow_x_forwarded_for

Determine which client proxies can be trusted to provide correct

information regarding real client IP address.

#

Requests may pass through a chain of several other proxies

before reaching us. The original source details may by sent in:

* HTTP message Forwarded header, or

* HTTP message X-Forwarded-For header, or

* PROXY protocol connection header.

#

PROXY protocol connections are controlled by the proxy_protocol_access

directive which is checked before this.

#

If a request reaches us from a source that is allowed by this

directive, then we trust the information it provides regarding

the IP of the client it received from (if any).

#

For the purpose of ACLs used in this directive the src ACL type always

matches the address we are testing and srcdomain matches its rDNS.

#

On each HTTP request Squid checks for X-Forwarded-For header fields.

If found the header values are iterated in reverse order and an allow

match is required for Squid to continue on to the next value.
The verification ends when a value receives a deny match, cannot be
tested, or there are no more values to test.
NOTE: Squid does not yet follow the Forwarded HTTP header.
#
The end result of this process is an IP address that we will
refer to as the indirect client address. This address may
be treated as the client address for access control, ICAP, delay
pools and logging, depending on the acl_uses_indirect_client,
icap_uses_indirect_client, delay_pool_uses_indirect_client,
log_uses_indirect_client and tproxy_uses_indirect_client options.
#
This clause only supports fast acl types.
See http://wiki.squid-cache.org/SquidFaq/SquidAcl for details.
#
SECURITY CONSIDERATIONS:
#
Any host from which we accept client IP details can place
incorrect information in the relevant header, and Squid
will use the incorrect information as if it were the
source address of the request. This may enable remote
hosts to bypass any access control restrictions that are
based on the client's source addresses.
#
For example:
#
acl localhost src 127.0.0.1
acl my_other_proxy srcdomain .proxy.example.com
follow_x_forwarded_for allow localhost
follow_x_forwarded_for allow my_other_proxy
#Default:
X-Forwarded-For header will be ignored.
TAG: acl_uses_indirect_client on|off
Controls whether the indirect client address

```
# (see follow_x_forwarded_for) is used instead of the
# direct client address in acl matching.
#
# NOTE: maxconn ACL considers direct TCP links and indirect
# clients will always have zero. So no match.
#Default:
# acl_uses_indirect_client on

# TAG: delay_pool_uses_indirect_client on|off
# Controls whether the indirect client address
# (see follow_x_forwarded_for) is used instead of the
# direct client address in delay pools.
#Default:
# delay_pool_uses_indirect_client on
# TAG: log_uses_indirect_client on|off
# Controls whether the indirect client address
# (see follow_x_forwarded_for) is used instead of the
# direct client address in the access log.
#Default:
# log_uses_indirect_client on
# TAG: tproxy_uses_indirect_client on|off
# Controls whether the indirect client address
# (see follow_x_forwarded_for) is used instead of the
# direct client address when spoofing the outgoing client.
#
# This has no effect on requests arriving in non-tproxy
# mode ports.
#
# SECURITY WARNING: Usage of this option is dangerous
# and should not be used trivially. Correct configuration
# of follow_x_forwarded_for with a limited set of trusted
# sources is required to prevent abuse of your proxy.
#Default:
# tproxy_uses_indirect_client off
```

TAG: spoof_client_ip

Control client IP address spoofing of TPROXY traffic based on

defined access lists.

spoof_client_ip allow|deny [!]aclname ...

If there are no "spoof_client_ip" lines present, the default

is to "allow" spoofing of any suitable request.

#

Note that the cache_peer "no-tproxy" option overrides this ACL.

#

This clause supports fast acl types.

See http://wiki.squid-cache.org/SquidFaq/SquidAcl for details.

#Default:

Allow spoofing on all TPROXY traffic.

TAG: http_access

Allowing or Denying access based on defined access lists.