ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

« Μελέτη και σχεδιασμός ασφάλειας στο επίπεδο ζεύξης δεδομένων σε ένα δίκτυο »

Του φοιτητή
Στεφανίδη Χαράλαμπου
Αρ. Μητρώου: 144227

Επιβλέπων
Αμανατιάδης Δημήτριος
Βαθμίδα: Ε.ΔΙ.Π.

10 Σεπτεμβρίου 2024

Μελέτη και σχεδιασμός ασφάλειας στο επίπεδο ζεύξης δεδομένων σε ένα δίκτυο
23214
Χαράλαμπος Στεφανίδης
Αμανατιάδης Δημήτριος
Ημερομηνία ανάληψης: 31/03/2023
Ημερομηνία περάτωσης: 10/09/2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως πτυχιακή εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

«Σε όλα αυτά τα χρόνια που πέρασα ως φοιτητής και στη φουκαριάρα την μάνα μου...»

Πρόλογος

Η επιλογή του συγκεκριμένου θέματος έγινε με βάση το ενδιαφέρον και την περιέργειά μου πάνω στις τεχνικές δοκιμής διείσδυσης δικτύων. Η ενασχόλησή μου από μικρή ηλικία με τους ηλεκτρονικούς υπολογιστές με έκανε να ψάχνω όλο και περισσότερο νέες πληροφορίες σχετικά με την λειτουργία τους και τον τρόπο που επικοινωνούνε μεταξύ τους. Η μετέπειτα αγάπη μου για τα δίκτυα που προέκυψε μέσα στην σχολή, ήταν το έναυσμα για την επιλογή και την υλοποίηση αυτής της εργασίας η οποία τσέκαρε όλα τα πεδία ενδιαφέροντος. Μέσα από την έρευνα αλλά και το πρακτικό κομμάτι της εργασίας, δημιουργήθηκαν νέες γνώσεις, ήρθαν στην μνήμη παλιές εμπειρίες αλλά ταυτόχρονα αξιοποιήθηκαν και πρόσφατες εμπειρίες από το εργασιακό περιβάλλον.

Περίληψη

Με την διαρκή εξέλιξη της τεχνολογίας, ολοένα και περισσότερες συσκευές συνδέονται σε δίκτυα. Όμως τα δεδομένα που διαμοιράζονται, ελκύουν κακόβουλους χρήστες που προσπαθούν να αποκτήσουν πρόσβαση σε συστήματα και πληροφορίες στα οποία δεν έχουν δικαιοδοσία. Για το λόγο αυτό, είναι απαραίτητο κατά την διαμόρφωση ενός δικτύου να εντοπίζονται οι ευπάθειές του ώστε να αντιμετωπίζονται με αποτελεσματικότητα. Η παρούσα πτυχιακή επικεντρώνεται στη μελέτη ασφάλειας του φυσικού αλλά κυρίως του επιπέδου ζεύξης δεδομένων σε ένα εταιρικό δίκτυο. Μελετήθηκαν οι ευπάθειες, οι απειλές και επιθέσεις σε ένα δίκτυο. Επίσης, σχεδιάστηκαν και υλοποιήθηκαν σε περιβάλλον προσομοίωσης GNS3 οι παρακάτω επιθέσεις: ARP Attacks, MAC Flooding Attack/ CAM Table Overflow Attacks, DHCP Attacks, CDP Attack, Spanning-Tree Attack, VLAN Trunking Protocol Attack, VLAN Hopping Attack, Double-Encapsulated 802.1Q/Nested VLAN Attack, IP/Mac spoofing, Wireless Attacks. Επιπροσθέτως, υλοποίηθηκαν αντίμετρα ασφαλείας που μετριάζουν τις παραπάνω επιθέσεις καθώς επίσης και μηχανισμοί πιστοποίησης ταυτότητας, εξουσιοδότησης και ελέγχου πρόσβασης. Τέλος, προτείνονται τρόποι και τεχνικές που οφείλουν να ακολουθούν οι οργανισμοί, ώστε να αποφύγουν τις καταστροφικές συνέπειες μιας κυβερνοεπίθεσης.

«Research and implementation of security at the data link layer in an network»

Charalampos Stefanidis

Abstract

With the continuous development of technology, more and more devices are connecting to networks. But the data being shared attracts malicious users who try to gain access to systems and information over which they do not have authorization. For this reason, it is necessary when configuring a network to identify its vulnerabilities so that they can be effectively addressed. This paper focuses on the security study of the physical but mainly of the data link layer in a enterprise network. Vulnerabilities, threats and attacks on a network were studied. Also, the following attacks were designed and implemented in a GNS3 simulation environment: ARP Attacks, MAC Flooding Attack/ CAM Table Overflow Attacks, DHCP Attacks, CDP Attack, Spanning-Tree Attack, VLAN Trunking Protocol Attack, VLAN Hopping Attack, Double-Encapsulated 802.1Q /Nested VLAN Attack, IP/Mac spoofing, Wireless Attacks. In addition, security countermeasures were implemented to mitigate the above attacks as well as authentication, authorization and accounting mechanisms. Finally, methods and techniques are suggested that organizations should follow in order to avoid the devastating consequences of a cyber attack.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την οικογένειά μου για όλη την υποστήριξη που μου παρείχαν.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

2FA	(Two-Factor Authentication)
ACK	(Acknowledge)
ACL	(Access Control List)
AI	(Artificial Intelligence)
ARP	(Address Resolution Protocol)
ASA	(Adaptive Security Appliance)
ASCII	(American Standard Code for Information Interchange)
BGP	(Border Gateway Protocol)
BIOS	(Basic Input/Output System)
BPDU	(Bridge Protocol Data Unit)
CAM	(Content Addressable Memory)
CAM	(Confidentiality Integrity Availability)
CCITT	(International Telegraph and Telephone Consultative Committe)
CDP	(Cisco Discovery Protocol)
CIA	(Confidentiality Integrity Availability)
CRC	(Cyclic Redundancy Check)
CR-CR-LF	(Carriage Return-Carriage Return-Line Feed)
DES	(Data Encryption Standard)
DHCP	(Dynamic Host Configuration Protocol)
DORA	(Discover, Offer, Request, Acknowledge - DHCP process)
DOS	(Denial of Service)
DDOS	(Distributed Denial of Service)
DNS	(Domain Name System)
DTP	(Dynamic Trunking Protocol)
EBCDIC	(Extended Binary Coded Decimal Interchange Code)
FTP	(File Transfer Protocol)
GNS3	(Graphical Network Simulator-3)
HPE VSR	(Hewlett-Packard-Enterprise Virtual Services Router)
HTTP	(Hypertext Transfer Protocol)
HTTPS	(Hypertext Transfer Protocol Secure)
ICMP	(Internet Control Message Protocol)
IDS	(Intrusion Detection System)
IDPS	(Intrusion Detection and Prevention System)
IOT	(Internet Of Things)
IOU	(Internetwork Operating System on Unix)
IP	(Internet Protocol)
IPV6	(Internet Protocol Version 6)
IPS	(Intrusion Prevention System)
IPX	(Internetwork Packet Exchange)
ISO	(International Organization for Standardization)
ITU-TS	(The International Telecommunication Union Telecommunication Standardization Sector)
LAN	(Local Area Network)
LLC	(Logical Link Control)
MAC	(Media Access Control)
MFA	(Multi-Factor Authentication)
MITM	(Man-In-The-Middle)
NIC	(Network Interface Card)
NFS	(Network File System)
OSI	(Open Systems Interconnection)
OSPF	(Open Shortest Path First)
OTP	(One Time Password)
PC	(Personal Computer)
PDF	(Portable Document Format)
PDU	(Protocol Data Unit)
POP3	(Post Office Protocol 3)

PVST	(Per-VLAN Spanning Tree)
RC4	(Rivest Cipher 4)
SDU	(Service Data Unit)
SMTP	(Simple Mail Transfer Protocol)
SPDU	(Session Protocol Data Unit)
SQL	(Structured Query Language)
SPX	(Sequenced Packet Exchange)
SSH	(Secure Shell)
SSL	(Secure Sockets Layer)
STP	(Spanning Tree Protocol)
SYN	(Synchronization)
TCP	(Transmission Control Protocol)
TLS	(Transport Layer Security)
UDP	(User Datagram Protocol)
VLAN	(Virtual Local Area Network)
VTP	(VLAN Trunking Protocol)
WEP	(Wired Equivalent Privacy)
WIFI	(Wireless Fidelity)
WLAN	(Wireless Local Area Network)
WPA	(Wi-Fi Protected Access)
WPA2	(Wi-Fi Protected Access 2)
WPS	(Wi-Fi Protected Setup)
XSS	(Cross-Site Scripting)
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
Π.Ε.	Πτυχιακή Εργασία

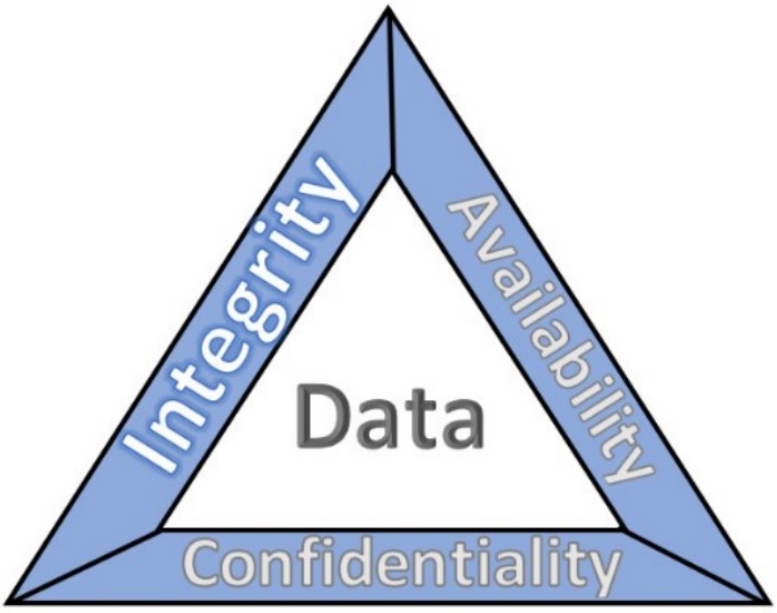
Κεφάλαιο 1ο: Εισαγωγή

1.1 Εισαγωγή

Σε αυτό το κεφάλαιο, γίνεται επισκόπηση της σημασίας της ασφάλειας στα δίκτυα υπολογιστών, παρουσιάζεται το μοντέλο OSI και εξηγείται γιατί η ασφάλεια του επιπέδου ζεύξης δεδομένων είναι ζωτικής σημασίας. Στο τέλος, αναφέρεται ο σκοπός και ο στόχος της πτυχιακής και η δομή που ακολουθεί το κείμενο.

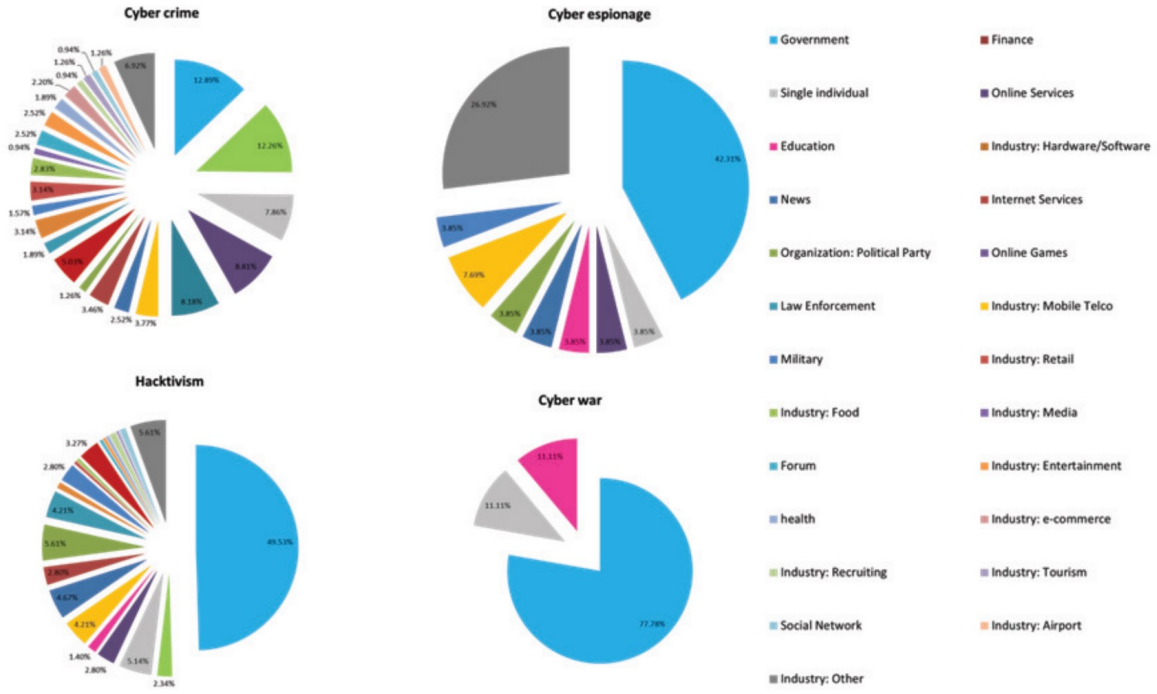
1.2 Επιθέσεις και ευπάθειες στα δίκτυα υπολογιστών

Στη σημερινή ψηφιακή εποχή, προσωπικές αλλά και εταιρικές πληροφορίες μεταδίδονται διαρκώς μέσω του δικτύου, γεγονός που καθιστά την υποκλοπή δεδομένων πρωταρχικό στόχο για τους εγκληματίες του κυβερνοχώρου. Η προστασία και η ασφάλεια των δικτύων, είναι πρωταρχικής σημασίας καθώς αποτρέπει την διαρροή ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και πιθανές παραβιάσεις. Χωρίς την εφαρμογή των κατάλληλων μέτρων ασφαλείας, οι οργανισμοί κινδυνεύουν να χάσουν εμπιστευτικές πληροφορίες, γεγονός που μπορεί να οδηγήσει σε σημαντικές οικονομικές απώλειες, ζημιά στη φήμη του οργανισμού, καθώς και νομικές επιπτώσεις. Η αποτελεσματική ασφάλεια δικτύου διασφαλίζει ότι τα δεδομένα παραμένουν εμπιστευτικά (Confidentiality), διατηρούν την ακεραιότητά (Integrity) τους και είναι διαθέσιμα σε εξουσιοδοτημένους χρήστες όταν χρειάζεται (Availability), χαρακτηριστικά που αποτελούν την τριάδα της ασφάλειας δεδομένων, Σχήμα 1.1.



Σχήμα 1.1: Μοντέλο διατήρησης ασφάλειας σε έναν οργανισμό [1].

Επιπλέον, η ασφάλεια του δικτύου είναι ζωτικής σημασίας για τη διατήρηση της λειτουργικότητας και της αξιοπιστίας της υποδομής του. Κυβερνοεπιθέσεις, όπως μολύνσεις από κακόβουλο λογισμικό, επιθέσεις άρνησης υπηρεσιών (DoS) και τα συστήματα phishing, μπορούν να διαταράξουν σοβαρά τις λειτουργίες του δικτύου, οδηγώντας σε διακοπές λειτουργίας και απώλεια παραγωγικότητας. Οι επιθέσεις προέρχονται από πληθώρα κινήτρων και στόχων. Μπορεί να αποσκοπούν στο οικονομικό κέρδος, με τους επιτιθέμενους να στοχεύουν να κλέψουν ή να εκβιάσουν πολύτιμα δεδομένα για χρήματα. Τα ιδεολογικά κίνητρα διαδραματίζουν επίσης σημαντικό ρόλο, με ομάδες χακτιβιστών να στοχεύουν οργανισμούς ή κυβερνήσεις για να προωθήσουν μια συγκεκριμένη αιτία ή ιδεολογία. Στο Σχήμα 1.2, παρουσιάζονται οι πιο συχνοί τύποι επιθέσεων καθώς και οι τομείς-οργανισμοί που επηρεάζουν. Οι κρατικές επιθέσεις γίνονται για κατασκοπεία, δολιοφθορά ή άσκηση επιρροής. Επιπλέον, υπάρχουν επιθέσεις που οδηγούνται από προσωπικές διαμάχες ή καθαρή κακόβουλη πρόθεση, επιδιώκουν να προκαλέσουν αναστάτωση ή ζημιά χωρίς ξεκάθαρο κίνητρο πέρα από το χάος. Με την εφαρμογή ισχυρών πρωτοκόλλων ασφαλείας και τη συνεχή παρακολούθηση για πιθανές απειλές, οι οργανισμοί μπορούν να αποτρέψουν διακοπές και να διασφαλίσουν ότι οι υπηρεσίες δικτύου τους παραμένουν λειτουργικές.



Σχήμα 1.2: Φορείς και τύποι επιθέσεων [2].

Η αρχιτεκτονική της μεταφοράς δεδομένων μέσα σε ένα δίκτυο, βασίζεται στο μοντέλο OSI (Open Systems Interconnection). Πιο συγκεκριμένα, το OSI αποτελεί ένα εννοιολογικό πλαίσιο το οποίο χρησιμοποιείται για την κατανόηση και την εφαρμογή τυποποιημένων λειτουργιών επικοινωνίας ενός τηλεπικοινωνιακού ή υπολογιστικού συστήματος, χωρίς να λαμβάνεται υπόψη η εσωτερική του δομή και τεχνολογία. Το μοντέλο OSI χωρίζεται σε επτά επίπεδα: Φυσικό, Ζεύξης Δεδομένων, Δικτύου, Μεταφοράς, Συνεδρίας, Παρουσίασης και Εφαρμογής. Κάθε επίπεδο εξυπηρετεί έναν συγκεκριμένο σκοπό και επικοινωνεί με τα επίπεδα ακριβώς πάνω και κάτω από αυτό, παρέχοντας μια αρθρωτή προσέγγιση στη δικτύωση που ενισχύει τη συμβατότητα και τη διαλειτουργικότητα μεταξύ διαφορετικών τεχνολογιών

και πρωτοκόλλων.

Στην παρούσα εργασία, δίνεται έμφαση στο επίπεδο Ζεύξης Δεδομένων. Η ασφάλεια του επιπέδου 2, είναι ιδιαίτερα σημαντική καθώς χειρίζεται τις άμεσες φυσικές συνδέσεις μεταξύ συσκευών εντός ενός τοπικού δικτύου. Η ασφάλιση αυτού του επιπέδου βοηθά στην αποφυγή επιθέσεων οι οποίες μπορεί να θέσουν σε κίνδυνο την ακεραιότητα και το απόρρητο του δικτύου. Τα αποτελεσματικά μέτρα ασφαλείας αυτού του επιπέδου, περιλαμβάνουν την εφαρμογή ισχυρών πρωτοκόλλων ελέγχου ταυτότητας, κρυπτογράφηση και τμηματοποίηση του δικτύου. Είναι απαραίτητα για την προστασία του εσωτερικού περιβάλλοντος δικτύου και την πρόληψη πιθανών παραβιάσεων που θα μπορούσαν να εξαπλωθούν σε υψηλότερα επίπεδα, διασφαλίζοντας έτσι τη συνολική ασφάλεια και σταθερότητα της υποδομής.

1.3 Στόχος και σκοπός της πτυχιακής εργασίας

Στόχος αυτής της πτυχιακής εργασίας είναι μία ολοκληρωμένη μελέτη μερικών από των επιθέσεων που αντιμετωπίζουμε στο δεύτερο επίπεδο του OSI, το επίπεδο ζεύξης δεδομένων. Για την υλοποίηση της εργασίας χρησιμοποιήθηκε ένα περιβάλλον προσομοίωσης, το GNS3, στο οποίο δημιουργήθηκαν οι κατάλληλες τοπολογίες δικτύων για την ρεαλιστική προσομοίωση των επιθέσεων. Εντοπίστηκαν οι ευπάθειες και τα τρωτά σημεία των τοπολογιών μέσα από μία σειρά ενεργειών, εφαρμόστηκαν οι επιθέσεις και έγινε αξιολόγηση των αποτελεσμάτων τους. Έπειτα, ακολουθήθηκε μία διαδικασία για την αναγνώριση και την εφαρμογή αντιμέτρων που θα απέτρεπαν τις εν λόγω επιθέσεις να εφαρμοστούν ξανά. Τέλος, προτάθηκαν μερικές καλές πρακτικές που πρέπει να ακολουθούνται για την δημιουργία μιας σφαιρικής ασφάλειας πάνω στα δίκτυα.

1.4 Δομή της πτυχιακής εργασίας

Η εργασία αναπτύσσεται στα παρακάτω κεφάλαια: Στο πρώτο κεφάλαιο γίνεται μία εισαγωγή στις ευπάθειες των συγχρόνων δικτύων, τους τομείς αλλά και τα κίνητρα που οδηγούν σε μία επίθεση. Στο δεύτερο κεφάλαιο περιγράφονται τα επίπεδα OSI, οι πιο κοινές επιθέσεις που συναντώνται στη σύγχρονη βιβλιογραφία καθώς και οι τεχνικές με τις οποίες μπορούν να αντιμετωπιστούν αποτελεσματικά. Στο τρίτο κεφάλαιο, παρουσιάζονται οι επιθέσεις που αφορούν το επίπεδο ζεύξης δεδομένων. Παρουσιάζονται οι τεχνικές και τα προγράμματα που χρησιμοποιήθηκαν για την προσομοίωση των επιθέσεων, καθώς και την εφαρμογή αντίμετρων.Τέλος, στο τέταρτο κεφάλαιο αναφέρονται τα συμπεράσματα των προσομοιώσεων, όπως επίσης και οι τεχνικές επιθέσεων αλλά και προστασίας, που αναμένεται να απασχολήσουν τα δίκτυα υπολογιστών τα επόμενα χρόνια.

1.5 Επίλογος

Στο κεφάλαιο αυτό, έγινε αναφορά στη σημαντικότητα της ασφάλειας στα δίκτυα υπολογιστών, το μοντέλο OSI και την ασφάλεια του επιπέδου ζεύξης δεδομένων.Ακόμη, παρουσιάστηκε η δομή της εργασίας και το πρόβλημα στο οποίο εστιάζει.

Κεφάλαιο 2ο: Απειλές στα επίπεδα OSI

2.1 Εισαγωγή

Σε αυτό το κεφάλαιο, παρουσιάζονται τα βασικά στοιχεία κάθε επιπέδου του μοντέλου OSI, οι πιο κοινές απειλές ασφαλείας που συναντώνται στην παρούσα βιβλιογραφία, καθώς και οι τρόποι που αυτές μπορούν να αντιμετωπιστούν.

2.2 Open Systems Interconnection

Το μοντέλο Open Systems Interconnection (OSI), αποτελείται από επτά επίπεδα και αφορά το βασικό πρότυπο λειτουργίας στα δίκτυα υπολογιστών. Στο μοντέλο OSI, κάθε επίπεδο εκτελεί διαφορετικές εργασίες και περνά το πακέτο στο επόμενο επίπεδο μέχρι να φτάσει στο επίπεδο προορισμού, φυσικό επίπεδο ή επίπεδο εφαρμογής.

Πιο αναλυτικά, το μοντέλο (OSI) είναι ένα framework που καθορίζει τις συμβάσεις και τις εργασίες που απαιτούνται από τα συστήματα δικτύου για να επικοινωνούν μεταξύ τους. Η έρευνα για το μοντέλο OSI ξεκίνησε στα τέλη της δεκαετίας του 1970, ως επί το πλείστον ανεξάρτητα, από τον Διεθνή Οργανισμό Τυποποίησης (ISO) και τη Διεθνή Συμβουλευτική Επιτροπή Τηλεγράφου και Τηλεφώνου ή CCITT (International Telegraph and Telephone Consultative Committee). Το CCITT διαδέχθηκε ο Τομέας Τυποποίησης Τηλεπικοινωνιών της Διεθνούς Ένωση Τηλεπικοινωνιών (ITU-TS). Το 1983 οι έρευνες των δύο οργανισμών συνδυάστηκαν και δημιουργήθηκε ένας ενιαίος οδηγός που περιγράφει το μοντέλο αναφοράς για τη Διασύνδεση Ανοικτών Συστημάτων (Open Systems Interconnection) [14].

Ο όρος «ανοικτά συστήματα» αναφέρεται στο γεγονός ότι οι προδιαγραφές είναι δημόσια διαθέσιμες σε όλους. Ο σκοπός του μοντέλου OSI ήταν να βοηθήσει τους προμηθευτές και τους προγραμματιστές λογισμικού επικοινωνίας να παράγουν διαλειτουργικά συστήματα δικτύου. Αν και το μοντέλο OSI σχεδιάστηκε για να αντικαταστήσει όλα τα προηγούμενα πρότυπα επικοινωνίας υπολογιστών, δεν θεωρείται πλέον αντικαταστάτης τους. Αντίθετα, το μοντέλο OSI αποτελεί το εργαλείο για την περιγραφή και τον καθορισμό του τρόπου με τον οποίο επικοινωνούν ετερογενή συστήματα δικτύου. Το μοντέλο OSI βασίζεται σε μια τεχνική δόμησης που ονομάζεται layering. Σύμφωνα με αυτή την προσέγγιση, οι λειτουργίες επικοινωνίας χωρίζονται σε ένα κατακόρυφο σύνολο επιπέδων. Κάθε επίπεδο εκτελεί ένα σχετικό σύνολο λειτουργιών, αξιοποιώντας και εμπλουτίζοντας τις υπηρεσίες που παρέχει το αμέσως κατώτερο στρώμα [15]. Η προσέγγιση του layering αναπτύχθηκε για την επίτευξη των ακόλουθων στόχων:

- Τον λογικό διαχωρισμό ενός πολύπλοκου δικτύου επικοινωνιών σε μικρότερα, πιο κατανοητά και διαχειρίσιμα μέρη.
- Την έμφαση στις διεπαφές των λειτουργιών δικτύου και των μονάδων τους.
- Την ύπαρξη μίας τυπικής γλώσσας, για την περιγραφή των λειτουργιών δικτύου, που μπορεί να χρησιμοποιείται από κοινού από σχεδιαστές, διαχειριστές, προμηθευτές και χρήστες δικτύου.

Επομένως, ο σημαντικότερος στόχος κατά την ανάπτυξη του μοντέλου OSI, ήταν η ομαδοποίηση παρόμοιων συναρτήσεων σε επίπεδα, διατηρώντας παράλληλα κάθε επίπεδο αρκετά μικρό ώστε να είναι διαχειρίσιμο, και ταυτόχρονα, διατηρώντας τον αριθμό των επιπέδων μικρό, καθώς ένας μεγάλος αριθμός επιπέδων θα αύξανε γενικά τα έξοδα επεξεργασίας.

Αριθμός Layer	**Όνομα Layer**	**Protocol Data Unit**
7	Application	Data
6	Presentation	Data
5	Session	Data
4	Transport	Segment / Datagram
3	Network	Packet
2	Data Link	Frame
1	Physical	Bit

Πίνακας 2.1: Πίνακας επιπέδων του OSI

Σε κάθε επίπεδο (N), δύο οντότητες (ομότιμοι επιπέδου N) ανταλλάσσουν μονάδες δεδομένων πρωτοκόλλου (protocol data units, PDUs) μέσω ενός πρωτοκόλλου επιπέδου-N. Μια μονάδα δεδομένων υπηρεσίας (service data unit, SDU) είναι το φορτίο ενός PDU, που μεταδίδεται αμετάβλητο σε μία ομότιμη οντότητα. Το SDU είναι μια μονάδα δεδομένων που μεταβιβάζεται από το ένα επίπεδο του OSI στο επόμενο χαμηλότερο επίπεδο και στο οποίο, το κατώτερο στρώμα ενσωματώνεται σε ένα PDU. Το επίπεδο N-1, προσθέτει μια κεφαλίδα (header) ή ένα υποσέλιδο (footer), ή και τα δύο, στο SDU, συνθέτοντας ένα PDU του στρώματος N-1. Τα πρόσθετα πλαίσια καθιστούν δυνατή τη μεταφορά των δεδομένων από μια πηγή σε έναν προορισμό. Με τον τρόπο αυτό, το PDU ενός επιπέδου N γίνεται το SDU επιπέδου N-1 [16]. Ορισμένες πτυχές, όπως η διαχείριση και η ασφάλεια, αφορούν κάθε επίπεδο. Για παράδειγμα, οι υπηρεσίες ασφαλείας δεν σχετίζονται με ένα συγκεκριμένο επίπεδο, μπορούν να συσχετιστούν με πολλά επίπεδα, όπως ορίζεται από τη Σύσταση ITU-T X.800 [17]. Αυτές οι υπηρεσίες στοχεύουν στη βελτίωση της τριάδας της CIA των μεταδιδόμενων δεδομένων. Στην πράξη, η διαθεσιμότητα της υπηρεσίας επικοινωνίας καθορίζεται από την αλληλεπίδραση μεταξύ σχεδίασης δικτύου και πρωτοκόλλων διαχείρισης.

2.3 Επίπεδο 1: Φυσικό επίπεδο

Το χαμηλότερο επίπεδο του μοντέλου OSI, το φυσικό επίπεδο, περιλαμβάνει φυσικά μέσα δικτύωσης όπως οι συνδέσεις καλωδίων, οι κεραίες και τα κύματα. Είναι υπεύθυνο για την κωδικοποίηση και την αποκωδικοποίηση δεδομένων σε φυσικά σήματα για μετάδοση μέσω του μέσου δικτύου. Τα πρωτόκολλα αυτού του επιπέδου διαχειρίζονται τη δημιουργία και την ανίχνευση τάσης, για τη μετάδοση και τη λήψη σημάτων δεδομένων. Διαχειρίζεται επίσης τις τεχνικές διαμόρφωσης που χρησιμοποιούνται για την αναπαράσταση ψηφιακών δεδομένων ως αναλογικά σήματα και αντίστροφα. Λαμβάνοντας υπόψη τα μηχανικά, ηλεκτρικά και λειτουργικά χαρακτηριστικά τους, όπως τάση, ρυθμός μεταφοράς δεδομένων, μέγιστη απόσταση μετάδοσης και τα φυσικά μέσα σύνδεσης, εξασφαλίζεται η ενεργοποίηση, η συντήρηση και η αποτελεσματική επικοινωνία μεταξύ των τελικών σημείων. Με τον τρόπο αυτό, διασφαλίζεται ότι τα δεδομένα αποστέλλονται και λαμβάνονται στα σωστά χρονικά διαστήματα. Η κύρια λειτουργία του φυσικού επιπέδου είναι να διευκολύνει τη μετάδοση ροών bit μεταξύ γειτονικών κόμβων. Αντιμετωπίζει ζητήματα όπως οι τύποι φυσικών σημάτων που αντιπροσωπεύουν τα δεδομένα 0 και 1, τα

συνεχή μήκη μετάδοσης, την αμφίδρομη μετάδοση δεδομένων και τη διασφάλιση της ακεραιότητας και του τερματισμού της επικοινωνίας. Το φυσικό επίπεδο ορίζει επίσης πτυχές, όπως ο αριθμός των διασυνδέσεων σε μια φυσική διεπαφή (π.χ. βύσματα και πρίζες), οι οποίες είναι ζωτικής σημασίας για τη δικτύωση, όπως για παράδειγμα, τη σύνδεση ενός επιτραπέζιου υπολογιστή σε μια κάρτα διασύνδεσης δικτύου [18].

Επιπλέον, καθορίζει τα χαρακτηριστικά του μέσου μετάδοσης, είτε είναι ενσύρματο (όπως χάλκινα καλώδια ή καλώδια οπτικών ινών) είτε ασύρματο (όπως ραδιοκύματα ή υπέρυθρα σήματα). Λαμβάνει υπόψη παράγοντες όπως η εξασθένηση του σήματος, η καταστολή θορύβου και η κατανομή εύρους ζώνης για τη βελτιστοποίηση της απόδοσης μετάδοσης δεδομένων. Αν και δεν προσφέρει υπηρεσίες διόρθωσης σφαλμάτων, παρακολουθεί τους ρυθμούς μεταφοράς δεδομένων και τα ποσοστά σφαλμάτων. Προβλήματα όπως σπασμένα καλώδια, ηλεκτρομαγνητικά κύματα, υγρασία, ακόμη και κάποια μικρά ζώα, μπορούν να επηρεάσουν σημαντικά τη λειτουργικότητα του φυσικού επιπέδου σε ένα δίκτυο.

Ακόμη, οι εξελίξεις στις τεχνολογίες φυσικών επιπέδων έχουν οδηγήσει σε καινοτομίες όπως το Ethernet, το οποίο έφερε επανάσταση στην τοπική δικτύωση και τεχνολογίες όπως το Wi-Fi και το Bluetooth, που επιτρέπουν την ασύρματη επικοινωνία μεταξύ συσκευών σε μικρές αποστάσεις. Το φυσικό επίπεδο συνεχίζει να εξελίσσεται με την ανάπτυξη νέων προτύπων και τεχνολογιών δικτύωσης για να ανταποκριθεί στις αυξανόμενες απαιτήσεις για μεγαλύτερες ταχύτητες μεταφοράς δεδομένων, υψηλότερο εύρος ζώνης και πιο αξιόπιστη επικοινωνία.

2.3.1 Επιθέσεις στο φυσικό επίπεδο

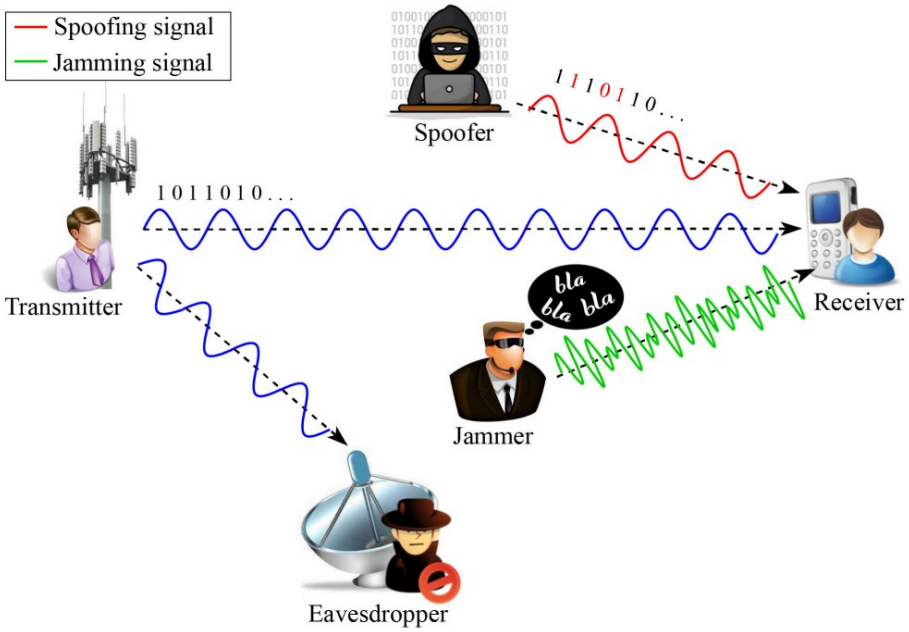
Οι κυβερνοεπιθέσεις στο φυσικό επίπεδο συνήθως περιλαμβάνουν μη εξουσιοδοτημένη πρόσβαση ή παραβίαση των φυσικών στοιχείων ενός δικτύου [19].

Ενσύρματα Δίκτυα: Στα ενσύρματα δίκτυα, οι εισβολείς μπορούν να παρακολουθούν τα φυσικά καλώδια ενός δικτύου χρησιμοποιώντας ένα "network tap ", μια μικρή συσκευή που διαχωρίζει το σήμα μεταξύ του αρχικού καλωδίου και της συσκευής ενός εισβολέα. Αυτό επιτρέπει στον εισβολέα να παρακολουθεί και να καταγράφει πακέτα δεδομένων χωρίς να διακόπτει τη σύνδεση του δικτύου. Εναλλακτικά, οι εισβολείς μπορούν να χρησιμοποιήσουν το port mirroring, μία λειτουργία που προσφέρεται από ορισμένους μεταγωγείς δικτύου, για να αντιγράψουν και να παρακολουθήσουν την κυκλοφορία δικτύου σε συγκεκριμένες θύρες.

Ασύρματα δίκτυα: Στα ασύρματα δίκτυα, οι εισβολείς μπορούν να χρησιμοποιήσουν συσκευές ανίχνευσης πακέτων και προσαρμογείς ασύρματου δικτύου για να συλλάβουν και να αναλύσουν δεδομένα που μεταδίδονται μέσω των ραδιοκυμάτων. Αυτός ο τύπος υποκλοπής είναι συχνά ευκολότερος να εκτελεστεί λόγω της φύσης των ασύρματων επικοινωνιών, οι οποίες εκπέμπουν σήματα σε μια ευρεία περιοχή. Οι εισβολείς μπορούν να αναχαιτίσουν αυτά τα σήματα από απόσταση, συχνά χωρίς την ανάγκη φυσικής πρόσβασης στο δίκτυο-στόχο [20].

Sniffing και Υποκλοπή: Το sniffing και η υποκλοπή είναι παθητικές επιθέσεις στον κυβερνοχώρο που περιλαμβάνουν την παρακολούθηση της κυκλοφορίας του δικτύου. Αυτές οι επιθέσεις στοχεύουν το φυσικό επίπεδο του μοντέλου OSI, όπου τα δεδομένα μεταδίδονται μέσω καλωδίων ή ασύρματων σημά-

των.Οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές και εργαλεία για να συλλάβουν και να αναλύσουν πακέτα δεδομένων αποκτώντας με τον τρόπο αυτό, πρόσβαση σε ευαίσθητες πληροφορίες, Σχήμα 2.1.



Σχήμα 2.1: Υποκλοπή σήματος [3].

Εργαλεία και Τεχνικές Sniffing: Υπάρχουν διάφορα διαθέσιμα εργαλεία και τεχνικές που διευκολύνουν τις επιθέσεις υποκλοπής, όπως:

- Wireshark: Ένας δημοφιλής αναλυτής πακέτων, ανοιχτού κώδικα, που επιτρέπει στους χρήστες να καταγράφουν και να αναλύουν την κίνηση του δικτύου σε πραγματικό χρόνο.
- Tcpdump: Ένας αναλυτής πακέτων γραμμής εντολών που παρέχει λεπτομερείς πληροφορίες σχετικά με την κυκλοφορία δικτύου, συμπεριλαμβανομένων των IP διευθύνσεων προέλευσης και προορισμού, θύρες και πρωτόκολλα.
- AirSnort: Ένα εργαλείο ανίχνευσης ασύρματου LAN (WLAN) που καταγράφει και αποκρυπτογραφεί την κρυπτογραφημένη κίνηση ενός δικτύου Wi-Fi.

2.3.2 Στρατηγικές περιορισμού επιθέσεων στο φυσικό επίπεδο

Η εφαρμογή αποτελεσματικών στρατηγικών περιορισμού, είναι ζωτικής σημασίας για την προστασία του φυσικού επιπέδου του μοντέλου OSI από κυβερνοεπιθέσεις. Αυτές οι στρατηγικές επικεντρώνονται στη μείωση του κινδύνου μη εξουσιοδοτημένης πρόσβασης, παρεμβολών και υποκλοπής δεδομένων, διασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πόρων του δικτύου [21].

Φυσική ασφάλεια: Η διασφάλιση της φυσικής πρόσβασης στην υποδομή δικτύου είναι μια θεμελιώδης πτυχή του μετριασμού των επιθέσεων φυσικού επιπέδου. Αυτό περιλαμβάνει:

- Περιορισμός της πρόσβασης σε δωμάτια εξοπλισμού δικτύου, δωμάτια διακομιστών και κέντρα δεδομένων μέσω της χρήσης συστημάτων ελέγχου πρόσβασης, όπως κάρτες-κλειδιά, βιομετρικούς σαρωτές ή φύλακες.
- Εγκαταστάσεις συστημάτων παρακολούθησης που χρησιμοποιούν συστήματα βιντεοεπιτήρησης και ανίχνευσης εισβολής για τον εντοπισμό μη εξουσιοδοτημένων αποπειρών εισόδου ή ύποπτων δραστηριοτήτων.
- Διενέργεια τακτικών ελέγχων ασφαλείας, για τη διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας και τον εντοπισμό πιθανών τρωτών σημείων στις πολιτικές κάθε οργανισμού.

Προστασία Υποδομής Δικτύων: Η προστασία της υποδομής του δικτύου περιλαμβάνει την εφαρμογή μέτρων για τη μείωση του κινδύνου παραβίασης, υποκλοπής και παρεμβολής σήματος. Ορισμένες προσεγγίσεις περιλαμβάνουν:

- Χρήση εξοπλισμού δικτύου και συστημάτων διαχείρισης καλωδίων ανθεκτικό σε παραβιάσεις για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή τροποποιήσεων.
- Ανάπτυξη θωράκισης σήματος και φυσικών φραγμών σε ασύρματα δίκτυα για τη μείωση του κινδύνου υποκλοπής και παρεμβολών σήματος.

Προστασία τελικού σημείου: Η ασφάλεια των συσκευών που είναι συνδεδεμένες στο δίκτυο είναι μια άλλη κρίσιμη πτυχή του μετριασμού των επιθέσεων φυσικού επιπέδου. Αυτό μπορεί να επιτευχθεί μέσω:

- Εγκατάσταση λογισμικού προστασίας από ιούς, τείχη προστασίας και συστημάτων ανίχνευσης εισβολής σε συσκευές για τον εντοπισμό και την πρόληψη λογισμικού και προσπαθειών μη εξουσιοδοτημένης πρόσβασης από κακόβουλες συσκευές που συνδέονται στο δίκτυο.
- Τακτικές ενημερώσεις και αναβαθμίσεις του υλικού της συσκευής, με ενημερώσεις του BIOS, αλλαγή εξαρτημάτων με νέας γενιάς, για την αντιμετώπιση γνωστών τρωτών σημείων και τη μείωση του κινδύνου εκμετάλλευσης.
- Εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας με φυσικά μέσα, όπως ο έλεγχος ταυτότητας δύο παραγόντων (2FA), για προστασία από μη εξουσιοδοτημένη πρόσβαση.

Ενημέρωση και Εκπαίδευση Εργαζομένων: Η εκπαίδευση των εργαζομένων ενός φορέα, σχετικά με τους κινδύνους που σχετίζονται με τις επιθέσεις φυσικών επιπέδων και τη σημασία της διατήρησης ασφαλών πρακτικών, αποτελεί βασικό συστατικό μιας αποτελεσματικής στρατηγικής κατά των κυβερνοεπιθέσεων. Αυτό περιλαμβάνει:

- Διεξαγωγή τακτικών συνεδριών εκπαίδευσης για την ενημέρωση των εργαζομένων σχετικά με πιθανές απειλές, προειδοποιητικές σημάνσεις και βέλτιστες πρακτικές για τη διατήρηση της σωματικής ασφάλειας.
- Ενθάρρυνση των εργαζομένων να αναφέρουν τυχόν ύποπτες δραστηριότητες, μη εξουσιοδοτημένες απόπειρες πρόσβασης ή περιστατικά ασφαλείας.

- Εφαρμογή μιας σαφούς και ολοκληρωμένης πολιτικής ασφάλειας που περιγράφει τις προσδοκίες και τις απαιτήσεις του οργανισμού για τη διατήρηση της φυσικής ασφάλειας.

Εφαρμόζοντας αυτές τις στρατηγικές, οι οργανισμοί μπορούν να μειώσουν σημαντικά τον κίνδυνο επιθέσεων φυσικού επιπέδου και να εξασφαλίσουν την ασφάλεια και την αξιοπιστία της υποδομής του δικτύου τους.

2.4 Επίπεδο 2: Επίπεδο ζεύξης δεδομένων

Το δεύτερο επίπεδο του μοντέλου OSI, γνωστό ως επίπεδο ζεύξης δεδομένων, λειτουργεί ως ενδιάμεσος μεταξύ του δικτύου και των φυσικών επιπέδων, διασφαλίζοντας την αξιόπιστη μετάδοση στα αναξιόπιστα φυσικά μέσα. Ανεξάρτητα από το δίκτυο ή τις εφαρμογές που χρησιμοποιούνται, το επίπεδο ζεύξης δεδομένων λειτουργεί ανεξάρτητα, εστιάζοντας στη μετάδοση πλαισίων δεδομένων. Συσκευές όπως οι μεταγωγείς, λειτουργούν σε αυτό το επίπεδο για να αποκωδικοποιούν τα πλαίσια και να τα δρομολογούν στους προβλεπόμενους παραλήπτες τους. Ο πρωταρχικός ρόλος του επιπέδου ζεύξης δεδομένων είναι να παρέχει αξιόπιστη μεταφορά δεδομένων μέσω δυνητικά αναξιόπιστων φυσικών γραμμών. Αυτό περιλαμβάνει τη διαίρεση των δεδομένων που λαμβάνονται από το επίπεδο δικτύου σε συγκεκριμένα πλαίσια μετάδοσης, τα οποία ενσωματώνουν όχι μόνο τα πρωτογενή δεδομένα αλλά και τις διευθύνσεις δικτύου αποστολέα και παραλήπτη, τη διόρθωση σφαλμάτων και τις πληροφορίες ελέγχου. Τα χαρακτηριστικά αυτών των πλαισίων περιλαμβάνουν τη φυσική διεύθυνση, την τοπολογία δικτύου, τους μηχανισμούς προειδοποίησης σφαλμάτων και τον έλεγχο ροής. Η φυσική διεύθυνση χρησιμεύει ως αναγνωριστικό κόμβου μέσα στο επίπεδο ζεύξης δεδομένων, προσδιορίζοντας τον προορισμό του πλαισίου. Αυτό το επίπεδο ασχολείται με τον εντοπισμό σφαλμάτων, τη διόρθωση σφαλμάτων και τον έλεγχο ροής δεδομένων. Χωρίζεται σε δύο υποστρώματα: το υπόστρωμα Media Access Control (MAC) και το Logical Link Control (LLC) [22].

Το υποστρώμα LLC είναι υπεύθυνο για την αναγνώριση και την ενθυλάκωση των πρωτοκόλλων του επιπέδου δικτύου και τη διασφάλιση της ακεραιότητας των πλαισίων δεδομένων, εκτελώντας έλεγχο σφαλμάτων και έλεγχο ροής. Λειτουργεί ως ενδιάμεσος μεταξύ του επιπέδου δικτύου (Επίπεδο 3) και του υποστρώματος MAC. Από την άλλη, το υποστρώμα MAC ελέγχει τον τρόπο με τον οποίο οι συσκευές σε ένα δίκτυο αποκτούν πρόσβαση στο μέσο μετάδοσης, είτε πρόκειται για Ethernet, Wi-Fi ή άλλο πρωτόκολλο. Διαχειρίζεται τη διεύθυνση MAC, η οποία είναι απαραίτητη για τον προσδιορισμό του προορισμού των δεδομένων. Επιπλέον, το υποστρώμα MAC διαχειρίζεται τον εντοπισμό και την αποφυγή σύγκρουσης, ειδικά σε δίκτυα εκπομπής όπως το Ethernet, διασφαλίζοντας ότι οι συσκευές μπορούν να επικοινωνούν στο ίδιο φυσικό μέσο χωρίς παρεμβολές. Οι διευθύνσεις MAC, είναι μοναδικά αναγνωριστικά 48-bit που αντιπροσωπεύονται συνήθως σε δεκαεξαδική μορφή και κωδικοποιούνται σε κάρτες διασύνδεσης δικτύου (NIC) από τον εκάστοτε κατασκευαστή. Όταν μία συσκευή στέλνει δεδομένα μέσω του δικτύου, το επίπεδο ζεύξης δεδομένων ενσωματώνει αυτά τα δεδομένα σε πλαίσια, εμπεριέχοντας τόσο τις διευθύνσεις MAC προέλευσης όσο και προορισμού, το ωφέλιμο φορτίο (τα πραγματικά δεδομένα που μεταδίδονται) αλλά και πληροφορίες ελέγχου, κωδικούς ελέγχου σφαλμάτων και ενδείξεις έναρξης/διακοπής πλαισίου. Μηχανισμοί ανίχνευσης και διόρθωσης σφαλμάτων, όπως το CRC (Cyclic Redundancy Check) [23], εφαρμόζονται επίσης σε αυτό το επίπεδο για να διασφαλιστεί η ακεραιότητα των δεδομένων. Εάν ένα πλαίσιο καταστραφεί κατά τη μετάδοση, το επίπεδο ζεύξης δεδομένων μπορεί να το εντοπίσει και να ζητήσει αναμετάδοση, ελαχιστοποιώντας έτσι τα σφάλματα στην επικοινωνία. Αυτή η διαδικασία επιτρέπει στα πλαίσια να δρομολογούνται σωστά στον προβλεπόμενο παραλήπτη τους στο τοπικό δίκτυο, διασφαλίζοντας ότι τα δεδομένα παραδίδονται με ακρίβεια και αποτελεσματικότητα στη σωστή συσκευή.

Δυστυχώς, το επίπεδο ζεύξης δεδομένων είναι επίσης επιρρεπές σε διάφορους τύπους κυβερνοεπιθέσεων. Μερικές από τις πιο κοινές επιθέσεις του επιπέδου ζεύξης, αναλύονται παρακάτω [24]:

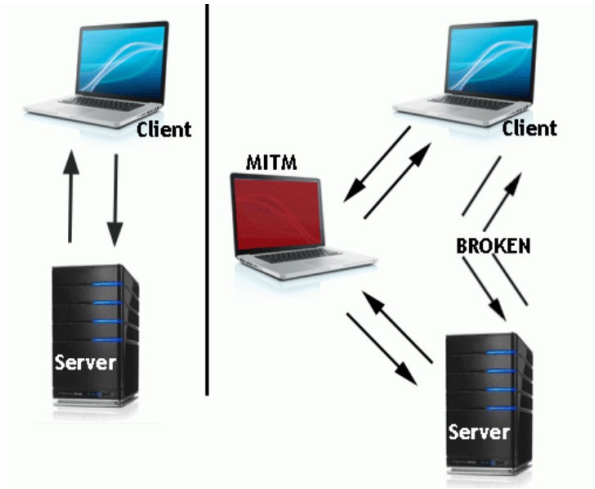
2.4.1 Επιθέσεις στο επίπεδο ζεύξης δεδομένων

MAC Spoofing: Σε αυτόν τον τύπο επίθεσης, ένας εισβολέας τροποποιεί τη διεύθυνση MAC της κάρτας διασύνδεσης δικτύου (NIC) για να μιμηθεί μια άλλη συσκευή στο δίκτυο. Αυτό μπορεί να του επιτρέψει να παρακάμψει τα στοιχεία ελέγχου πρόσβασης, να παρεμποδίσει την κυκλοφορία ή να εξαπολύσει άλλες επιθέσεις.

Επιθέσεις Spanning Tree Protocol (STP): Το STP χρησιμοποιείται για τη διατήρηση μιας τοπολογίας δικτύου χωρίς βρόχους. Ένας εισβολέας μπορεί να εκμεταλλευτεί ευπάθειες στο STP για να διακόψει το δίκτυο, να προκαλέσει βρόχους ή να δημιουργήσει άρνησης υπηρεσίας (DoS).

VLAN Hopping: Τα εικονικά τοπικά δίκτυα (VLAN) χρησιμοποιούνται για τον διαχωρισμό της κυκλοφορίας του δικτύου για λόγους ασφάλειας και διαχείρισης. Σε μια επίθεση VLAN hopping, ένας εισβολέας εκμεταλλεύεται τις αδυναμίες της υλοποίησης VLAN για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε άλλα VLAN και τους σχετικούς πόρους τους.

Παραπλάνηση πρωτοκόλλου ανάλυσης διεύθυνσης (ARP): Το ARP (Address Resolution Protocol) χρησιμοποιείται για την αντιστοίχιση διευθύνσεων IP σε διευθύνσεις MAC. Σε μια επίθεση πλαστογράφησης ARP, ένας εισβολέας στέλνει κακόβουλα πακέτα ARP σε συσκευές του δικτύου, συσχετίζοντας τη δική του διεύθυνση MAC με τη διεύθυνση IP μιας άλλης συσκευής. Αυτό μπορεί να οδηγήσει σε υποκλοπή κυκλοφορίας και επιθέσεις Man-in-the-Middle (MITM), Σχήμα 2.2.



Σχήμα 2.2: Αριστερά: Κανονική ροή δεδομένων. Δεξιά: Ροή δεδομένων κατά τη διάρκεια επίθεσης MITM. [4].

Frame Injection: Σε αυτήν την επίθεση, ένας εισβολέας εισάγει κακόβουλα πλαίσια δεδομένων στο δίκτυο, τα οποία μπορεί να οδηγήσουν σε καταστροφή δεδομένων, μη εξουσιοδοτημένη πρόσβαση ή εξάπλωση κακόβουλου λογισμικού.

2.4.2 Στρατηγικές περιορισμού επιθέσεων στο επιπέδου ζεύξης δεδομένων

Για να αμυνθούν από επιθέσεις επιπέδου ζεύξης δεδομένων, οι οργανισμοί πρέπει να εφαρμόσουν διάφορα μέτρα ασφαλείας που ενισχύουν την ανθεκτικότητα του δικτύου τους έναντι αυτών των απειλών. Μερικές από τις βασικές στρατηγικές μετριασμού περιλαμβάνουν [25]:

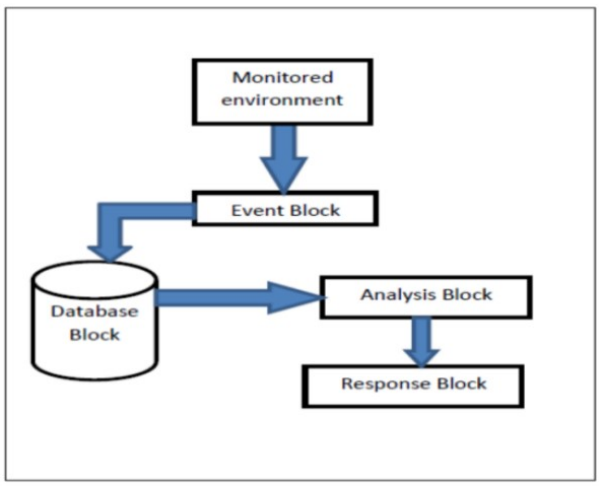
Τμηματοποίηση δικτύου: Διαχωρισμός του δικτύου σε μικρότερα τμήματα χρησιμοποιώντας VLAN (Virtual Local Area Networks) ή άλλες τεχνικές τμηματοποίησης. Αυτό μπορεί να βοηθήσει στον περιορισμό του εύρους μιας πιθανής επίθεσης και να αποτρέψει τους εισβολείς από το να μετακινούνται εύκολα μέσα στο δίκτυο.

MAC Address Filtering: Εφαρμόζοντας φιλτράρισμα διευθύνσεων MAC σε μεταγωγείς και δρομολογητές, ελέγχεται η πρόσβαση στο δίκτυο, επιτρέποντας τη σύνδεση μόνο σε εξουσιοδοτημένες συσκευές. Έτσι, οι οργανισμοί μπορούν να μειώσουν τον κίνδυνο μη εξουσιοδοτημένων συσκευών να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα ή να εξαπολύσουν επιθέσεις.

Κρυπτογράφηση: Χρησιμοποιώντας τεχνικές κρυπτογράφησης, όπως Wi-Fi Protected Access (WPA) ή WPA2, για την προστασία των δεδομένων που μεταδίδονται σε ασύρματα δίκτυα, έχουμε ως αποτέλεσμα την αποφυγή υποκλοπών και επιθέσεων Man-in-the-Middle (MITM).

Port Security: Ενεργοποιώντας τις λειτουργίες ασφαλείας θυρών στους μεταγωγείς δικτύου, περιορίζεται ο αριθμός των συσκευών που μπορούν να συνδεθούν σε μια συγκεκριμένη θύρα. Ακόμη, μπορεί να απενεργοποιηθούν οι θύρες που δεν χρησιμοποιούνται. Αυτό μπορεί να βοηθήσει στην αποτροπή μη εξουσιοδοτημένων συσκευών από τη σύνδεση στο δίκτυο και την εξαπόλυση επιθέσεων.

Ισχυρός έλεγχος ταυτότητας: Με την εφαρμογή ισχυρών μηχανισμών ελέγχου ταυτότητας, όπως το 802.1X, για συσκευές που συνδέονται στο δίκτυο, μπορεί να διασφαλιστεί ότι παρέχεται πρόσβαση μόνο σε εξουσιοδοτημένες συσκευές και να μειωθεί ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης.



Σχήμα 2.3: Γενική αρχιτεκτονική ενός συστήματος IDPS [5].

Συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS): Οι τεχνικές IDPS (Intrusion Detection and Prevention Systems) μπορούν να παρακολουθούν το δίκτυο για ενδείξεις κακόβουλης δραστηριότητας

και να αναλαμβάνουν δράση για τον αποκλεισμό ή τον μετριασμό των επιθέσεων σε πραγματικό χρόνο, Σχήμα 2.3.

Τακτικοί έλεγχοι ασφαλείας: Διεξάγοντας τακτικούς ελέγχους ασφαλείας, μπορούν να αξιολογηθούν οι πιθανές ευπάθειες και αδυναμίες στο επίπεδο ζεύξης δεδομένων. Με την εφαρμογή των απαραίτητων ενημερώσεων κώδικα ή επιδιορθώσεων μπορεί να διασφαλιστεί η ακεραιότητά τους.

Τακτικές ενημερώσεις λογισμικού: Με την διατήρηση των συσκευών δικτύου, όπως μεταγωγείς και δρομολογητές, ενημερωμένες με το πιο πρόσφατο υλικολογισμικό και με ενημερώσεις στον κώδικα α-σφαλείας, μπορεί να αντιμετωπιστούν γνωστά τρωτά σημεία και να μειωθούν οι πιθανότητες επίθεσης.

Εφαρμόζοντας αυτές τις στρατηγικές μετριασμού, οι οργανισμοί μπορούν να μειώσουν σημαντικά τον κίνδυνο επιθέσεων στο επίπεδο ζεύξης δεδομένων και να διατηρήσουν ένα ασφαλές περιβάλλον δικτύου.

2.5 Επίπεδο 3: Επίπεδο δικτύου

Το τρίτο επίπεδο του μοντέλου OSI, το επίπεδο δικτύου, παίζει καθοριστικό ρόλο στον καθορισμό της βέλτιστης διαδρομής για τη μετάδοση δεδομένων με βάση παράγοντες όπως η προτεραιότητα μετάδοσης, η συμφόρηση δικτύου, η ποιότητα της υπηρεσίας και οι επιλογές δρομολόγησης από τον έναν κόμβο δικτύου στον άλλο.
Λειτουργώντας ως ραχοκοκαλιά για τις αποφάσεις δρομολόγησης, αυτό το επίπεδο επεξεργάζεται διαδρομές και χρησιμοποιεί δρομολογητές για να καθοδηγεί έξυπνα τη μεταφορά δεδομένων στα δίκτυα. Οι αποφάσεις δρομολόγησης βασίζονται σε σχήματα διευθυνσιοδότησης και καθιερωμένα μοντέλα, για τη διευκόλυνση της αποτελεσματικής μετάδοσης δεδομένων.

Το επίπεδο δικτύου ορίζει τη μετάδοση πακέτων από άκρο σε άκρο, αναγνωρίζοντας όλους τους κόμβους με λογικές διευθύνσεις και περιγράφοντας τις υλοποιήσεις δρομολόγησης και τις στρατηγικές εκμάθησης. Επιπλέον, διαχειρίζεται την τμηματοποίηση πακέτων για να φιλοξενήσει μέγιστα μήκη μονάδας μετάδοσης μικρότερα από το μήκος πακέτων του μέσου μετάδοσης. Η κύρια λειτουργία του επιπέδου δικτύου είναι να διευκολύνει τη μετάδοση πακέτων δικτύου μεταξύ κεντρικών υπολογιστών, χρησιμοποιώντας υπηρεσίες επιπέδου ζεύξης δεδομένων για τη μετάδοση πακέτων από την πηγή στον προορισμό. Αυτό περιλαμβάνει τη δημιουργία διαδρομών από την πηγή στον προορισμό, ελαχιστοποιώντας τη συμφόρηση μέσω ενδιάμεσων σημείων του δικτύου [26].
Το επίπεδο δικτύου χειρίζεται επίσης τη μετάφραση διευθύνσεων δικτύου σε αντίστοιχες φυσικές διευθύνσεις και καθορίζει στρατηγικές δρομολόγησης για πακέτα δεδομένων μεταξύ αποστολέων και δεκτών. Τέλος, μπορεί να ελέγχει τις λειτουργίες διαδικτύου για τη βελτιστοποίηση της απόδοσης του δικτύου. Μερικές από τις πιο κοινές επιθέσεις του επιπέδου δικτύου, αναλύονται παρακάτω [27] .

2.5.1 Επιθέσεις επιπέδου δικτύου

IP Spoofing: Σε μια επίθεση πλαστογράφησης IP, ένας εισβολέας τροποποιεί τη διεύθυνση IP προέλευσης στην κεφαλίδα του πακέτου για να μιμηθεί μία άλλη συσκευή στο δίκτυο. Αυτό μπορεί να χρησιμοποιηθεί για να παρακάμψει μέτρα ασφαλείας, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση ή να εξαπολύσει άλλες επιθέσεις, όπως επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS).

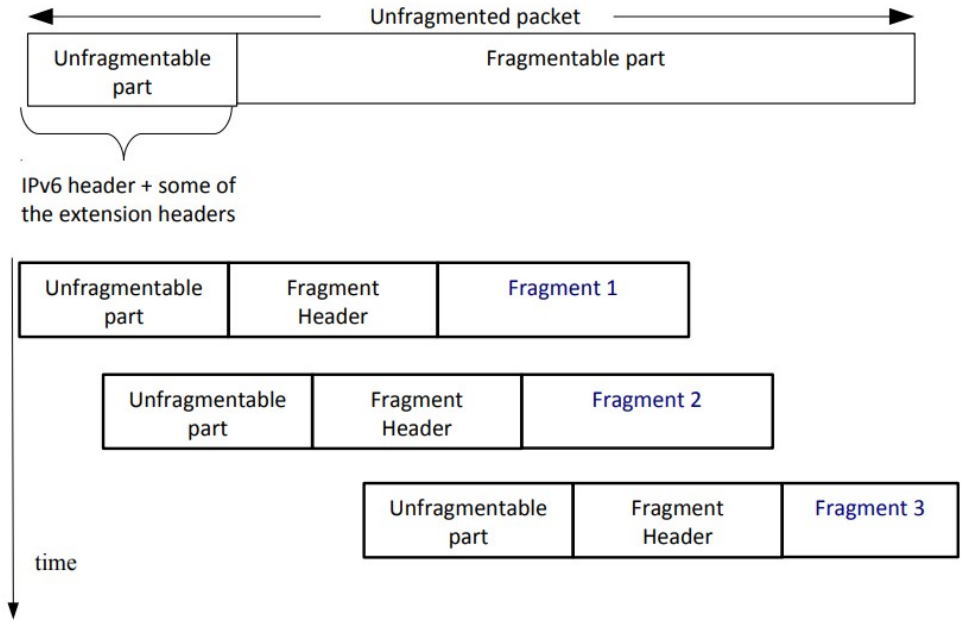
Επίθεση ICMP Flood: Το πρωτόκολλο Internet Control Message Protocol (ICMP) χρησιμοποιείται για την αναφορά σφαλμάτων και για διαγνωστικές πληροφορίες. Μια επίθεση ICMP flood, γνωστή και ως ”πλημμύρα ping”, περιλαμβάνει την αποστολή μεγάλου αριθμού πακέτων ICMP σε έναν στόχο, προκαλώντας υπερχείλιση στους πόρους του με αποτέλεσμα την άρνησης υπηρεσίας (DoS).

Επίθεση Smurf: Η επίθεση smurf, είναι ένας τύπος επίθεσης DDoS που εκμεταλλεύεται ευπάθειες στο πρωτόκολλο ICMP. Ο εισβολέας στέλνει μεγάλο αριθμό πακέτων αιτήματος echo ICMP (ping) στη διεύθυνση εκπομπής του στόχου, αναγκάζοντας όλες τις συσκευές του δικτύου να απαντούν στον στόχο με πακέτα απάντησης echo ICMP, υπερκαλύπτοντας έτσι τους πόρους του στόχου και προκαλώντας υποβάθμιση υπηρεσιών.

Επιθέσεις πρωτοκόλλου δρομολόγησης: Τα πρωτόκολλα δρομολόγησης (routing protocols), όπως το

Border Gateway Protocol (BGP) και το Open Shortest Path First (OSPF), χρησιμοποιούνται για τον προσδιορισμό της καλύτερης διαδρομής για τα πακέτα δεδομένων, ώστε να φτάσουν στον προορισμό τους. Οι εισβολείς μπορούν να στοχεύσουν αυτά τα πρωτόκολλα για να εισάγουν ψευδείς πληροφορίες δρομολόγησης, οδηγώντας σε εσφαλμένη δρομολόγηση, υποκλοπή κυκλοφορίας ή αστάθεια δικτύου.

Επιθέσεις κατακερματισμού: Σε μια επίθεση κατακερματισμού (fragmentation), ένας εισβολέας στέλνει ειδικά δημιουργημένα πακέτα IP με κατακερματισμένα τμήματα σε έναν στόχο. Αυτό μπορεί να προκαλέσει στο σύστημα-στόχο να καταναλώσει υπερβολικούς πόρους προσπαθώντας να επανασυναρμολογήσει τα πακέτα, οδηγώντας σε κατάσταση DoS ή επιτρέποντας στον εισβολέα να παρακάμψει μέτρα ασφαλείας, Σχήμα 2.4.



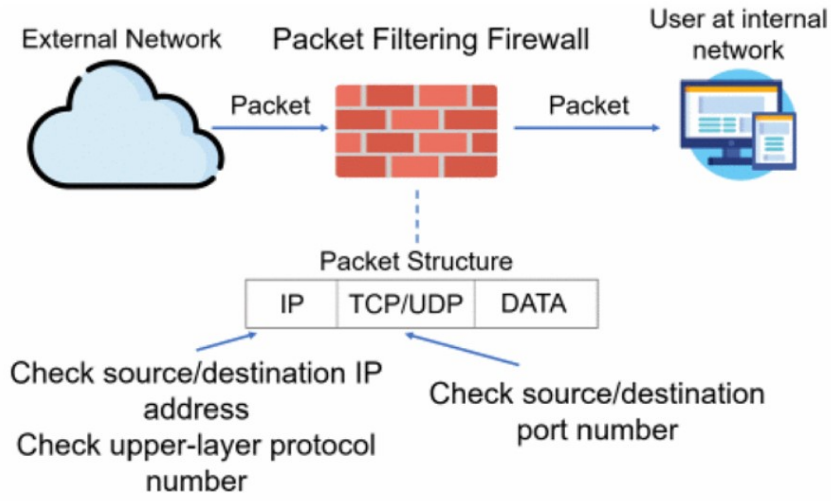
Σχήμα 2.4: Παράδειγμα κατακερματισμού ενός πακέτου IPv6 [5].

2.5.2 Στρατηγικές περιορισμού επιθέσεων στο επίπεδο δικτύου

Για την προστασία από επιθέσεις σε επίπεδο δικτύου, οι οργανισμοί θα πρέπει να υιοθετήσουν έναν συνδυασμό μέτρων ασφαλείας και βέλτιστων πρακτικών. Αυτές οι στρατηγικές μπορούν να βοηθήσουν στην πρόληψη, τον εντοπισμό και την άμεση απόκριση σε απειλές που στοχεύουν το επίπεδο δικτύου. Μερικές βασικές τεχνικές περιλαμβάνουν [28]:

Firewalls: Αναπτύσσοντας τείχη προστασίας στο δίκτυο, φιλτράρεται και ελέγχεται η εισερχόμενη και η εξερχόμενη κίνηση, Σχήμα 2.5. Τα σωστά διαμορφωμένα τείχη προστασίας μπορούν να βοηθήσουν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και να αποκλείσουν την κακόβουλη κυκλοφορία στο επίπεδο δικτύου.

Συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS): Με την εφαρμογή συστημάτων IDPS, γίνεται εύκολη η παρακολούθηση της κυκλοφορίας του δικτύου, με ενδείξεις σε περίπτωση ύποπτης δραστηριό-



Σχήμα 2.5: Παράδειγμα λειτουργίας ενός Firewall [6].

τητας και κάνοντας αυτόματο τον αποκλεισμό ή την αντιμετώπιση των απειλών που έχουν εντοπιστεί.

Λίστες ελέγχου πρόσβασης (ACL): Η χρήση των ACL (Access Control Lists) σε δρομολογητές και μεταγωγείς, δίνει την δυνατότητα να ελέγχεται και να φιλτράρεται η κυκλοφορία του δικτύου με βάση συγκεκριμένα κριτήρια, όπως διευθύνσεις IP, πρωτόκολλα ή θύρες.

Περιορισμός ρυθμού: Εφαρμόζοντας περιορισμό ρυθμού (rate) σε δρομολογητές και τείχη προστασίας, ελέγχεται η επιτρεπόμενη επισκεψιμότητα από συγκεκριμένες πηγές. Αυτό μπορεί να βοηθήσει στον περιορισμό του αντίκτυπου των επιθέσεων DoS και DDoS μειώνοντας την ποσότητα της κίνησης που μπορεί να φτάσει στον στόχο.

Ανάλυση κυκλοφορίας: Τα εργαλεία παρακολούθησης δικτύου και απειλών, μπορούν να βοηθήσουν στον εντοπισμό πιθανών επιθέσεων και στη λήψη των κατάλληλων μέτρων. Αυτό επιτυγχάνεται με την τακτική ανάλυση της κυκλοφορίας του δικτύου για ενδείξεις μη φυσιολογικής δραστηριότητας ή μοτίβα που μπορεί να υποδηλώνουν μια συνεχιζόμενη επίθεση.

Ενημερώσεις ασφαλείας: Είναι σημαντικό να παραμένουν ενημερωμένες οι συσκευές δικτύου, όπως δρομολογητές, μεταγωγείς και τείχη προστασίας, με τις πιο πρόσφατες εκδόσεις κώδικα ασφαλείας και υλικολογισμικού, για την αντιμετώπιση γνωστών τρωτών σημείων και τη μείωση της καταστροφικότητας της επίθεσης.

Redundancy και Load Balancing: Η εφαρμογή τεχνικών πλεονασμού και εξισορρόπησης φορτίου, βοηθά στην κατανομή της κυκλοφορίας δικτύου και τη μείωση του αντίκτυπου των επιθέσεων DoS και DDoS σε κρίσιμες υποδομές.

Σχέδιο Αντιμετώπισης Συμβάντων: Έχοντας ένα σχέδιο αντιμετώπισης συμβάντων, εξασφαλίζεται η ταχεία και αποτελεσματική απόκριση σε επιθέσεις επιπέδου δικτύου. Επανεξετάζοντας και κρατώντας ενημερωμένο τακτικά το σχέδιο αντιμετώπισης και με συχνές ασκήσεις εκπαίδευσης, διασφαλίζεται ότι όλο το σχετικό προσωπικό είναι εξοικειωμένο με τους ρόλους και τις ευθύνες του και μπορεί να αντα-ποκριθεί άμεσα σε μια επικείμενη απειλή.

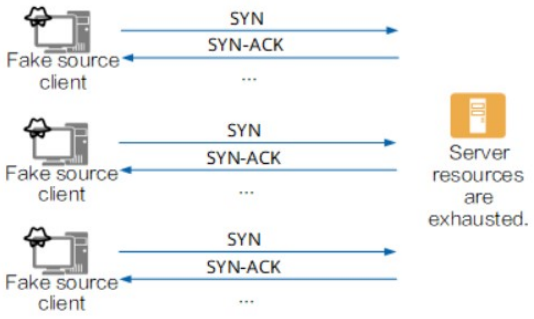
2.6 Επίπεδο 4: Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς εξασφαλίζει μετάδοση δεδομένων χωρίς σφάλματα, δημιουργώντας αξιόπιστες συνδέσεις από σημείο σε σημείο, για αποτελεσματική μεταφορά δεδομένων. Διαχειρίζεται πρωτόκολλα ελέγχου ροής για να ρυθμίζει τους ρυθμούς μεταφοράς δεδομένων με βάση τις δυνατότητες του δέκτη και τις συνθήκες δικτύου, ενώ επίσης διαιρεί μεγάλα πακέτα σύμφωνα με τους περιορισμούς μέγιστου μεγέθους του δικτύου. Μέσα στο επίπεδο μεταφοράς, υπηρεσίες όπως το TCP (Transmission Control Protocol) των πρωτοκόλλων TCP/IP και το SPX (Sequence Packet Exchange) των πρωτοκόλλων IPX/SPX, παίζουν ζωτικούς ρόλους.
Η κύρια λειτουργία του επιπέδου μεταφοράς είναι να διευκολύνει την αξιόπιστη επικοινωνία μεταξύ διεργασιών σε διαφορετικούς κεντρικούς υπολογιστές, προσφέροντας πρωτόκολλα ανάκτησης σφαλμάτων, πολυπλεξία ροών δεδομένων από διάφορες εφαρμογές στον ίδιο κεντρικό υπολογιστή και διατήρηση της σειράς πακέτων χωρίς εκ νέου ταξινόμηση. Αυτό το επίπεδο εξασφαλίζει διάφανη και αξιόπιστη μετάδοση δεδομένων μεταξύ των δικτύων, εστιάζοντας στην επικοινωνία από άκρο σε άκρο και όχι στη μετάδοση από σημείο σε σημείο. Τα χαρακτηριστικά του περιλαμβάνουν έλεγχο ροής, πολυπλεξία, διαχείριση εικονικών κυκλωμάτων, διόρθωση και ανάκτηση σφαλμάτων, επιτρέποντας σε πολλαπλές εφαρμογές να μοιράζονται έναν ενιαίο φυσικό σύνδεσμο για μετάδοση. Χρησιμοποιούνται μηχανισμοί ανίχνευσης και διόρθωσης σφαλμάτων για την αντιμετώπιση τυχόν σφαλμάτων που παρουσιάζονται κατά τη μετάδοση, διασφαλίζοντας την ακεραιότητα των δεδομένων.

2.6.1 Επιθέσεις επιπέδου μεταφοράς

Οι κυβερνοεπιθέσεις που στοχεύουν το επίπεδο μεταφοράς, αποσκοπούν κυρίως στο να διακόψουν, να υποκλέψουν ή να χειραγωγήσουν τα δεδομένα που μεταδίδονται. Ακολουθούν ορισμένοι συνήθεις τύποι επιθέσεων επιπέδου μεταφοράς [29]:

Επίθεση SYN Flood: Σε αυτή την επίθεση, ο εισβολέας στέλνει μεγάλο αριθμό πακέτων SYN (συγχρονισμός) στον διακομιστή-στόχο με σκοπό να συντρίψει τους πόρους του. Ο διακομιστής προορισμού αποκρίνεται σε κάθε πακέτο SYN με ένα πακέτο SYN-ACK (συγχρονισμός-επιβεβαίωση) και στη συνέχεια περιμένει το τελικό πακέτο ACK (επιβεβαίωση) από τον αποστολέα για να δημιουργήσει μια σύνδεση. Ωστόσο, ο εισβολέας δεν στέλνει ποτέ το πακέτο ACK, αφήνοντας τον διακομιστή να περιμένει απαντήσεις και να καταναλώνει τους πόρους του, προκαλώντας τελικά άρνηση υπηρεσίας (DoS), Σχήμα 2.6.



Σχήμα 2.6: Syn Flooding: Ο server αναμένει πακέτα ACK χωρίς ανταπόκριση [7].

UDP Flood Attack: Στην επίθεση καταιγισμού πακέτων UDP (User Datagram Protocol), ο εισβολέας στέλνει μεγάλο αριθμό πακέτων σε τυχαίες θύρες του συστήματος στόχου, αναγκάζοντάς το να ελέγξει για εφαρμογές που ακούν σε αυτές τις θύρες. Όταν το σύστημα δεν βρίσκει καμία ανταπόκριση, στέλνει ένα πακέτο ICMP (Internet Control Message Protocol) "Απρόσιτος προορισμός", στον αποστολέα. Αυτή η διαδικασία μπορεί να καταναλώσει πόρους συστήματος και εύρος ζώνης, οδηγώντας σε DoS [30].

Επιθέσεις SSL/TLS: Το Secure Sockets Layer (SSL) και το Transport Layer Security (TLS), αποτελούν πρωτόκολλα κρυπτογράφησης που παρέχουν ασφαλή επικοινωνία μεταξύ συσκευών. Ωστόσο, τα τρωτά σημεία σε αυτά τα πρωτόκολλα ή οι υλοποιήσεις τους μπορούν να αξιοποιηθούν από εισβολείς για να θέσουν σε κίνδυνο την ασφάλεια της επικοινωνίας.

Port Scanning: Η σάρωση θυρών είναι μια τεχνική που χρησιμοποιείται από τους εισβολείς για τον εντοπισμό ανοιχτών θυρών και υπηρεσιών που εκτελούνται στο σύστημα-στόχος. Αν και η σάρωση θυρών δεν είναι εγγενώς κακόβουλη, μπορεί να είναι το πρώτο βήμα για τον εντοπισμό πιθανών τρωτών σημείων προς εκμετάλλευση για περαιτέρω επιθέσεις.

2.6.2 Στρατηγικές περιορισμού επιθέσεων στο επίπεδο μεταφοράς

Ισχυρή κρυπτογράφηση και έλεγχος ταυτότητας: Η διασφάλιση της χρήσης ισχυρών αλγορίθμων κρυπτογράφησης και μεθόδων ελέγχου ταυτότητας, μπορεί να καταστήσει πιο δύσκολο για τους εισβολείς να υποκλέψουν, να χειραγωγήσουν ή να παραβιάσουν τις συνεδρίες επικοινωνίας.

Περιορισμός ρυθμού διερχόμενων πακέτων: Η εφαρμογή περιορισμού ρυθμού πακέτων μπορεί να βοηθήσει στον μετριασμό των επιθέσεων καταιγισμού αιτημάτων SYN και UDP, περιορίζοντας τον αριθμό των εισερχόμενων συνδέσεων ή πακέτων ανά δευτερόλεπτο σε ένα διαχειρίσιμο επίπεδο.

Χρονικά όρια και όρια σύνδεσης: Η διαμόρφωση μικρότερων χρονικών ορίων για ημιτελείς συνδέσεις και ο περιορισμός του αριθμού των ταυτόχρονων συνδέσεων, μπορεί να συμβάλει στη μείωση του αντίκτυπου των επιθέσεων καταιγισμού SYN.

Επιπλέον, πολλές ακόμη τεχνικές που αναφέρθηκαν και στα προηγούμενα επίπεδα, όπως η τμηματοποίηση, η εφαρμογή ενός συστήματος IDPS, οι συχνές ενημερώσεις ασφάλειας του υλικολογισμικού και η σωστή εκπαίδευση των χρηστών, αποτελούν και στο επίπεδο μεταφοράς αξιόλογες λύσεις για την προστασία του δικτύου.

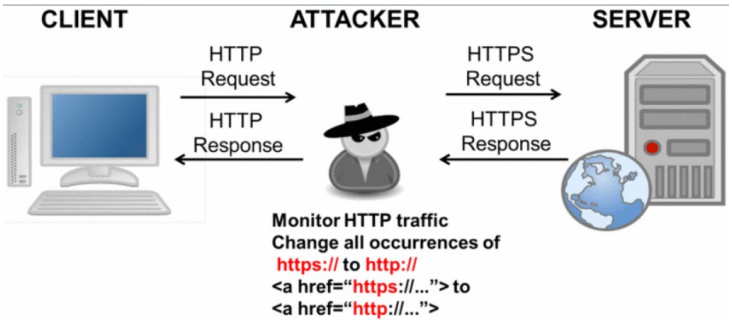
2.7 Επίπεδο 5: Επίπεδο συνεδρίας

Το επίπεδο συνεδρίας επιτρέπει σε δύο κόμβους να διατηρούν την συνέχεια στην επικοινωνία τους μέσω της σύναψης μιας συνεδρίας. Σε κάθε άκρο της επικοινωνίας, μπορούν να ανταλλάσσονται δεδομένα ή να στέλνονται πακέτα, για όσο διάστημα διαρκεί η συνεδρία. Σε μία συνεδρία μπορούν να συμμετέχουν μόνο τα καθορισμένα μέλη και μέσω υπηρεσιών ασφαλείας ελέγχεται η πρόσβαση στις πληροφορίες που μεταδίδονται. Μια συνεδρία μπορεί να χρησιμοποιηθεί για να επιτρέψει σε έναν χρήστη να συνδεθεί σε ένα απομακρυσμένο σύστημα ή να μεταφέρει ένα αρχείο μεταξύ δύο συσκευών.
Το επίπεδο συνεδρίας έχει την επιλογή παροχής μονόδρομης ή αμφίδρομης επικοινωνίας που ονομάζεται έλεγχος διαλόγου (dialogue control). Οι περίοδοι σύνδεσης μπορούν να επιτρέψουν στην κυκλοφορία να κινείται και προς τις δύο κατευθύνσεις ταυτόχρονα ή προς μία μόνο κατεύθυνση κάθε φορά. Με τη χρήση token, μπορεί να χρησιμοποιηθεί για να εμποδίσει και τις δύο πλευρές να επιχειρήσουν την ίδια λειτουργία ταυτόχρονα. Μόνο η πλευρά που κρατά το token επιτρέπεται να εκτελέσει την κρίσιμη λειτουργία. Μια άλλη υπηρεσία της συνεδρίας, είναι ο συγχρονισμός. Για παράδειγμα, εάν υπάρξει κάποια δυσλειτουργία κατά τη μεταφορά ενός αρχείου μεταξύ δύο συσκευών και το σύστημα κολλήσει χωρίς να είναι δυνατή η ολοκλήρωση της μεταφοράς, η διαδικασία θα έπρεπε να ξαναρχίσει από την αρχή. Για να αποφευχθεί αυτό το πρόβλημα, το επίπεδο συνεδρίας, παρέχει έναν τρόπο εισαγωγής σημείων ελέγχου στη ροή δεδομένων, έτσι ώστε μετά από ένα σφάλμα, να επαναλαμβάνονται μόνο τα δεδομένα μετά το τελευταίο σημείο ελέγχου. Το όνομα της μονάδας δεδομένων στο επίπεδο περιόδου συνεδρίας είναι SPDU (Session Protocol Data Unit) ή session [31].

2.7.1 Επιθέσεις επιπέδου συνεδρίας

Λόγω του κρίσιμου ρόλου του στη διαχείριση των περιόδων επικοινωνίας, το επίπεδο συνεδρίας είναι επίσης ευαίσθητο σε διάφορες επιθέσεις.

Session Hijacking: Η πειρατεία συνεδρίας, συμβαίνει όταν ένας εισβολέας καταλαμβάνει τον έλεγχο μιας συνεδρίας επικοινωνίας μεταξύ δύο συσκευών. Αυτό μπορεί να επιτευχθεί με την πρόβλεψη, την παρεμπόδιση ή τον χειρισμό των session token μιας συνεδρίας ή άλλων αναγνωριστικών που χρησιμοποιούνται για τον έλεγχο ταυτότητας και τη διατήρηση της συνεδρίας, Σχήμα 2.7. Μόλις ο εισβολέας αποκτήσει τον έλεγχο, μπορεί να πραγματοποιήσει διάφορες κακόβουλες ενέργειες, όπως η κλοπή ευαίσθητων δεδομένων ή η εισαγωγή κακόβουλου περιεχομένου στην επικοινωνία.



Σχήμα 2.7: Παράδειγμα session hijacking [8].

Επανάληψη επιθέσεων: Σε μια επίθεση επανάληψης, ο επιτιθέμενος, καταγράφει και αναμεταδίδει πακέτα δεδομένων συχνά σε μια προσπάθεια να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή να το ξεγελάσει ώστε εκτελέσει μια ενέργεια που δεν θα έπρεπε. Αυτός ο τύπος επίθεσης μπορεί να είναι ιδιαίτερα αποτελεσματικός όταν τα token ελέγχου ταυτότητας ή περιόδου λειτουργίας επαναχρησιμοποιούνται ή έχουν μεγάλη περίοδο ισχύος.

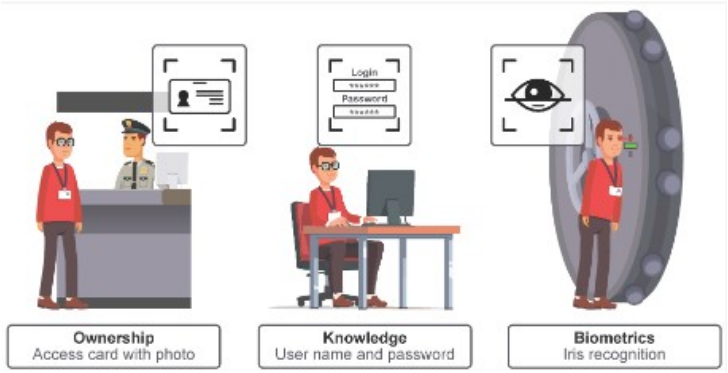
Session Fixation: Η σταθεροποίηση περιόδου λειτουργίας, είναι ένας τύπος επίθεσης κατά την οποία,ο επιτιθέμενος αναγκάζει τον χρήστη να χρησιμοποιήσει ένα συγκεκριμένο αναγνωριστικό περιόδου σύνδεσης, επιτρέποντάς του να παραβιάσει τη συνεδρία μόλις ο χρήστης έχει περάσει τον έλεγχο ταυτότητας. Αυτό συνήθως επιτυγχάνεται, εξαπατώντας τον χρήστη να κάνει κλικ σε έναν κακόβουλο σύνδεσμο ή να επισκεφτεί έναν παραποιημένο ιστότοπο.

Άρνηση υπηρεσίας (DoS): Ενώ οι επιθέσεις DoS μπορούν να στοχεύουν διάφορα επίπεδα του μοντέλου OSI, μπορούν επίσης να στοχεύουν ειδικά στη διακοπή μίας συνεδρίας, κατακλύζοντας το σύστημα διαχείρισης συνεδρίας με υπερβολικά αιτήματα σύνδεσης ή προκαλώντας σκόπιμα χρονικά όρια συνεδρίας. Με τον τρόπο αυτό, ο εισβολέας μπορεί να καταστήσει μια υπηρεσία άχρηστη για τους νόμιμους χρήστες.

2.7.2 Στρατηγικές περιορισμού επιθέσεων στο επίπεδο συνεδρίας

Ασφαλής διαχείριση συνεδρίας: Η χρήση ασφαλών μεθόδων για τη δημιουργία, την αποθήκευση και τη μετάδοση token ή cookies συνεδρίας, μπορεί να βοηθήσει στην αποτροπή επιθέσεων πειρατείας συνεδρίας. Τα αναγνωριστικά περιόδου σύνδεσης πρέπει να είναι αρκετά μεγάλα και τυχαία για να κάνουν πιο δύσκολη την εύρεσή τους. Ακόμη, με την ενεργοποίηση των ασφαλούς και HttpOnly cookie flags, μειώνεται ο κίνδυνος υποκλοπής μέσω επιθέσεων cross-site scripting (XSS).

Multi-Factor Authentication (MFA): Η ενεργοποίηση του ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), παρέχει ένα πρόσθετο επίπεδο ασφάλειας απαιτώντας από τους χρήστες να παρέχουν περισσότερες από μία μορφές ταυτοποίησης πριν παραχωρήσουν πρόσβαση σε ευαίσθητα συστήματα ή δεδομένα [9]. Αυτό μπορεί να βοηθήσει στην προστασία από διάφορες επιθέσεις επιπέδου συνεδρίας, συμπεριλαμβανομένης της πειρατείας συνεδρίας και των επιθέσεων man-in-the-middle.



Σχήμα 2.8: Πυλώνες του MFA: ιδιοκτησία, γνώση, βιομετρικά χαρακτηριστικά [9].

Transport Layer Security (TLS): Η εφαρμογή κρυπτογράφησης TLS καθ'όλη την επικοινωνία μεταξύ χρηστών και διακομιστών, συμβάλλει στην προστασία από επιθέσεις MITM και υποκλοπής, διασφαλίζοντας ότι τα δεδομένα που μεταδίδονται είναι κρυπτογραφημένα και δεν μπορούν εύκολα να υποκλαπούν ή να χειραγωγηθούν.

Session Timeout: Η εφαρμογή σύντομων χρονικών ορίων συνεδρίας και ο αυτόματος τερματισμός των συνεδριών μετά από μία περίοδο αδράνειας, μπορεί να συμβάλει στη μείωση του κινδύνου επιθέσεων. Επιπλέον, για ευαίσθητες ενέργειες ή μετά από ένα ορισμένο χρονικό διάστημα, είναι ωφέλιμο να απαιτείται από τους χρήστες να συνδέονται εκ νέου και να γίνεται ξανά ο έλεγχος ταυτότητας.

2.8 Επίπεδο 6: Επίπεδο παρουσίασης

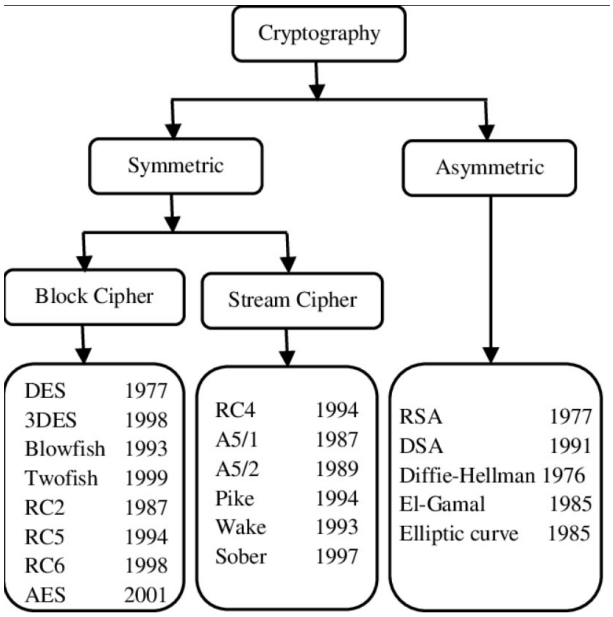
Το επίπεδο παρουσίασης μορφοποιεί τα δεδομένα που θα παρουσιαστούν στο επίπεδο εφαρμογής. Μπορεί να θεωρηθεί ως ο μεταφραστής του δικτύου. Αυτό το επίπεδο, μπορεί να μεταφράσει δεδομένα από μια μορφή που χρησιμοποιείται από το επίπεδο εφαρμογής σε μια κοινή μορφή στο σταθμό αποστολής και στη συνέχεια να μεταφράσει την κοινή μορφή σε μια μορφή γνωστή για το επίπεδο εφαρμογής στο σταθμό λήψης [32]. Το επίπεδο παρουσίασης παρέχει:

- Μετάφραση κώδικα χαρακτήρων: για παράδειγμα, ASCII σε EBCDIC.
- Μετατροπή δεδομένων: σειρά bit, CR-CR/LF, ακέραιος-κινητής υποδιαστολής, κοκ.
- Συμπίεση δεδομένων: μειώνει τον αριθμό των bit που πρέπει να μεταδοθούν στο δίκτυο.
- Κρυπτογράφηση δεδομένων.

2.8.1 Επιθέσεις επιπέδου παρουσίασης

Αν και οι επιθέσεις σε αυτό το επίπεδο είναι λιγότερο συχνές από εκείνες που στοχεύουν άλλα επίπεδα του OSI, εξακολουθούν να αποτελούν σημαντική απειλή για τα δίκτυα.

Κρυπτογραφικές επιθέσεις: Οι αδύναμοι ή ακατάλληλα εφαρμοσμένοι αλγόριθμοι κρυπτογράφησης (Σχήμα 2.9) μπορούν να αξιοποιηθούν για την αποκρυπτογράφηση ευαίσθητων δεδομένων ή την εκτέλεση επιθέσεων man-in-the-middle. Τα παραδείγματα περιλαμβάνουν επιθέσεις σε αδύναμους ή απαρχαιωμένους αλγόριθμους κρυπτογράφησης, όπως DES ή RC4.



Σχήμα 2.9: Κοινοί αλγόριθμοι κρυπτογραφίας [10].

Επιθέσεις βάσει περιεχομένου - Στεγανογραφία: Αυτές οι επιθέσεις περιλαμβάνουν την έγχυση κακό-

βουλου περιεχομένου σε ροές δεδομένων ή αρχεία, τα οποία ενεργοποιούνται κατά την εκτέλεση ή την επεξεργασία τους. Μερικά από τα παραδείγματα περιλαμβάνουν αρχεία εικόνας, PDF ή άλλες μορφές αρχείων που εκμεταλλεύονται ευπάθειες στο λογισμικό που χρησιμοποιείται για την επεξεργασία ή την εμφάνισή τους. Ακόμη, αν και δεν είναι εγγενώς κακόβουλο, η στεγανογραφία μπορεί να χρησιμοποιηθεί από επιτιθέμενους για να μεταφέρει κρυφά ευαίσθητα δεδομένα ή για να κρύψει κακόβουλα ωφέλιμα φορτία μέσα σε φαινομενικά αβλαβή αρχεία [33].

Επιθέσεις κακής μορφής δεδομένων: Οι εισβολείς ενδέχεται να στείλουν δεδομένα με λανθασμένη μορφή σε εφαρμογές ή συσκευές δικτύου, προκαλώντας απροσδόκητη συμπεριφορά ή σφάλματα. Τέτοιες επιθέσεις στοχεύουν τον τρόπο ανάλυσης και επεξεργασίας των δεδομένων στο επίπεδο παρουσίασης, οδηγώντας ενδεχομένως σε άρνηση υπηρεσίας (DoS).

2.8.2 Στρατηγικές περιορισμού επιθέσεων στο επίπεδο παρουσίασης

Μερικές από τις πιο ειδικές μεθόδους περιορισμού αντιμετώπισης για το επίπεδο 6, περιγράφονται παρακάτω:

Πρακτικές ασφαλούς κωδικοποίησης: Οι προγραμματιστές θα πρέπει να ακολουθούν ασφαλείς πρακτικές κωδικοποίησης για να αποφύγουν την εισαγωγή τρωτών σημείων που σχετίζονται με την ανάλυση και την επεξεργασία δεδομένων. Οι τακτικοί έλεγχοι κώδικα, η στατική και δυναμική ανάλυση και οι ενδελεχείς δοκιμές, μπορούν να βοηθήσουν στον εντοπισμό πιθανών ζητημάτων προτού καταστούν εκμεταλλεύσιμα.

Ισχυροί αλγόριθμοι κρυπτογράφησης: Είναι απαραίτητη η χρήση ισχυρών, ευρέως αποδεκτών αλγορίθμων κρυπτογράφησης και πρακτικών διαχείρισης κλειδιών, για την προστασία ευαίσθητων δεδομένων. Αποφυγή της χρήσης απαρχαιωμένων ή αδύναμων μεθόδων κρυπτογράφησης και συχνό έλεγχο και ενημέρωση των κρυπτογραφικών εφαρμογών, καθώς εμφανίζονται συχνά νέες απειλές.

Φιλτράρισμα και την επικύρωση περιεχομένου: Εφαρμόζοντας αυστηρούς μηχανισμούς φιλτραρίσματος περιεχομένου και επικύρωσης για ροές δεδομένων και μεταφορτώσεις αρχείων, αποτρέπεται η εκτέλεση κακόβουλων ωφέλιμων φορτίων. Ταυτόχρονα, απαιτείται η σάρωση εισερχόμενων αρχείων και δεδομένων για γνωστές τακτικές κακόβουλου λογισμικού και η απαγόρευση μεταφορτώσεων δυνητικά επιβλαβών τύπων αρχείων.

2.9 Επίπεδο 7: Επίπεδο εφαρμογής

Τέλος, αυτό είναι το επίπεδο με το οποίο συχνά αλληλεπιδρά ο χρήστης. Εδώ τα δεδομένα μετατρέπονται σε ιστότοπους, προγράμματα συνομιλίας και ούτω καθεξής. Πολλά πρωτόκολλα τρέχουν σε αυτό το επίπεδο, όπως DNS, FTP, HTTP, HTTPS, NFS, POP3, SMTP και SSH. Η κύρια λειτουργία του επιπέδου εφαρμογής είναι η παροχή μιας διεπαφής που επιτρέπει στα προγράμματα και τους χρήστες, να χρησιμοποιούν τις υπηρεσίες του δικτύου. Δυστυχώς, λόγω της εγγύτητάς του με τον χρήστη, το επίπεδο εφαρμογής συχνά στοχοποιείται από εγκληματίες του κυβερνοχώρου [34].

2.9.1 Επιθέσεις επιπέδου εφαρμογής

Ιοί: Αποτελούν κακόβουλο λογισμικό που συνδέεται με νόμιμα προγράμματα ή αρχεία και στη συνέχεια εξαπλώνεται όταν αυτά τα αρχεία κοινοποιούνται ή εκτελούνται. Οι ιοί μπορούν να προκαλέσουν καταστροφή δεδομένων, σφάλματα συστήματος ή μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.

Worms: Πρόκειται για αυτοαναπαραγόμενο κακόβουλο λογισμικό που εκμεταλλεύεται τα τρωτά σημεία του συστήματος για να εξαπλωθεί χωρίς την παρέμβαση χρήστη. Τα σκουλήκια μπορούν να καταναλώσουν πόρους του συστήματος, να διακόψουν τις λειτουργίες του δικτύου ή να διευκολύνουν τη διάδοση άλλου κακόβουλου λογισμικού.

Phishing: Παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου, ιστότοποι ή μηνύματα που εξαπατούν τους χρήστες να αποκαλύψουν ευαίσθητες πληροφορίες ή διαπιστευτήρια. Οι επιθέσεις phishing συχνά περιλαμβάνουν τεχνικές social engineering για τη χειραγώγηση των θυμάτων, ώστε να κάνουν κλικ σε κακόβουλους συνδέσμους ή να κάνουν λήψη επιβλαβών συνημμένων.

Keyloggers: Κακόβουλα προγράμματα που καταγράφουν την πληκτρολόγηση ενός χρήστη, συχνά με σκοπό την καταγραφή κωδικών πρόσβασης, αριθμών πιστωτικών καρτών ή άλλων ευαίσθητων πληροφοριών. Τα keyloggers μπορούν να εγκατασταθούν μέσω κακόβουλου λογισμικού ή μέσω φυσικής πρόσβασης σε μια συσκευή.

Backdoors: Μη εξουσιοδοτημένα σημεία πρόσβασης σε ένα σύστημα ή ένα δίκτυο, που δημιουργούνται συνήθως από εισβολείς ή κακόβουλο λογισμικό για τη διατήρηση της μόνιμης πρόσβασης για μελλοντική εκμετάλλευση. Τα backdoors μπορούν να χρησιμοποιηθούν για την εξαγωγή δεδομένων ή τον απομακρυσμένο έλεγχο συστημάτων.

Λάθη της λογικής του προγράμματος: Ευπάθειες στον κώδικα μίας εφαρμογής που μπορούν να αξιοποιηθούν για την παράκαμψη των ελέγχων ασφαλείας, την εκτέλεση μη εξουσιοδοτημένων ενεργειών ή τον χειρισμό δεδομένων. Παραδείγματα περιλαμβάνουν SQL injections, cross-site scripting (XSS) και buffer overflow.

Bugs: Σφάλματα ή ελαττώματα στο λογισμικό που μπορούν να εκμεταλλευτούν οι εισβολείς για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση, να διακόψουν λειτουργίες ή να θέσουν σε κίνδυνο ευαίσθητα δεδομένα. Με τακτικές επιδιορθώσεις και ενημερώσεις λογισμικού, μπορούν να εντοπιστούν και

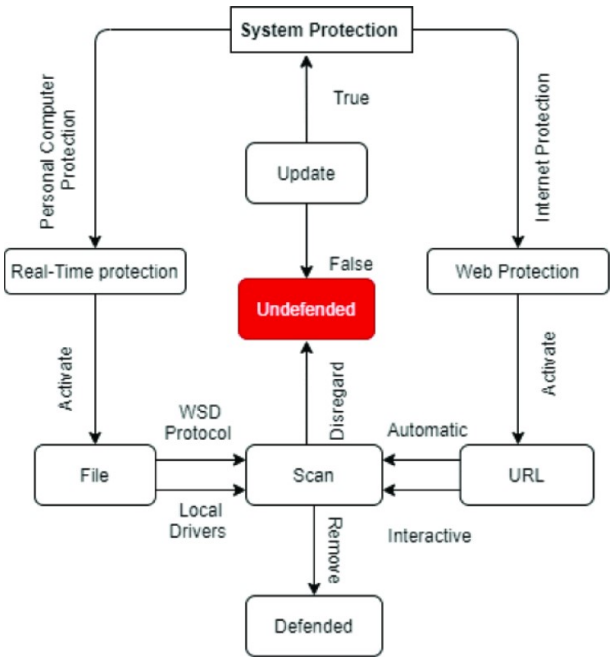
να αντιμετωπιστούν τα σφάλματα λογισμικού.

Trojan Horses: Κακόβουλα προγράμματα που μεταμφιέζονται ως νόμιμο λογισμικό ή αρχεία για να εξαπατήσουν τους χρήστες να τα εγκαταστήσουν. Μόλις εγκατασταθούν, τα Trojans μπορούν να διευκολύνουν τη μη εξουσιοδοτημένη πρόσβαση, την κλοπή δεδομένων ή την ανάπτυξη πρόσθετου κακόβουλου λογισμικού [34].

2.9.2 Στρατηγικές περιορισμού επιθέσεων στο επίπεδο εφαρμογής

Τακτικές ενημερώσεις λογισμικού και διαχείριση ενημερώσεων κώδικα: Είναι σημαντική η διατήρηση του λογισμικού στην πιο ενημερωμένη έκδοση, είτε πρόκειται για λειτουργικά συστήματα, είτε για εφαρμογές. Οι πιο πρόσφατες ενημερώσεις κώδικα, καθιστούν το σύστημα πιο ασφαλές και απωθούν τις επιθέσεις που αφορούν γνωστά ελαττώματα της προηγούμενης έκδοσης.

Λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό: Απαραίτητη κρίνεται η εγκατάσταση λογισμικού προστασίας για ιούς, σε όλες τις συσκευές ενός δικτύου. Με αυτό τον τρόπο, γίνεται άμεσα ο εντοπισμός ή η κατάργηση κάποιας απειλής, Σχήμα 2.10.



Σχήμα 2.10: Διάγραμμα λειτουργίας ενός προγράμματος antivirus [11].

Ισχυρός έλεγχος ταυτότητας και έλεγχος πρόσβασης: Με την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), τις ισχυρές πολιτικές κωδικών πρόσβασης και τον έλεγχο πρόσβασης βάσει ρόλου, περιορίζεται η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα και συστήματα.

Ασφαλείς πρακτικές ανάπτυξης λογισμικού: Ακολουθώντας ασφαλείς πρακτικές προγραμματισμού, ελαχιστοποιούνται τα τρωτά σημεία στον κώδικα μιας εφαρμογής. Δοκιμές ασφαλείας και σάρωση ευπάθειας καθ' όλη τη διάρκεια του κύκλου ανάπτυξης της εφαρμογής, μπορούν να συμβάλλουν στον εντοπισμό και την αποκατάσταση πιθανών αδυναμιών.

2.10 Επίλογος

Στο κεφάλαιο αυτό, έγινε αναφορά στα επίπεδα του μοντέλου OSI, στις ευπάθειες και τις συχνότερες επιθέσεις που εντοπίζονται σε κάθε ένα από αυτά. Επιπλέον, παρουσιάστηκαν τρόποι αντιμετώπισης που μπορούν να εφαρμοστούν σε κάθε επίπεδο για την διατήρηση της ορθής λειτουργίας ενός δικτύου.

Κεφάλαιο 3ο: Προσομοίωση επιθέσεων στο επίπεδο ζεύξης

3.1 Εισαγωγή

Στο παρακάτω κεφάλαιο, περιγράφονται οι ερευνητικές μέθοδοι και προσεγγίσεις που χρησιμοποιήθηκαν, οι προσομοιώσεις που εκτελέστηκαν για κάθε επίθεση που αναλύεται, καθώς και η επιλογή αντιμέτρων για την αντιμετώπισή τους.

3.2 Περιβάλλον προσομοίωσης

Είναι κοινώς αποδεκτό ότι, η γρήγορη ανάπτυξη και διάδοση του Διαδικτύου έχει προκαλέσει εκτεταμένες ανησυχίες για το απόρρητο, την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που διακινούνται σε αυτό. Πολλές εταιρείες χρησιμοποιούν μέτρα ασφαλείας σε υψηλότερα επίπεδα του μοντέλου OSI, από το επίπεδο εφαρμογής έως το επίπεδο πρωτοκόλλου Διαδικτύου (IP). Μια περιοχή που μπορεί να αγνοηθεί, ωστόσο, είναι η διασφάλιση του επιπέδου Data Link. Ως αποτέλεσμα αυτού, μπορεί να εξαπολυθούν διάφορες επιθέσεις εναντίον του δικτύου.

Κατά κύριο λόγο, το επίπεδο δικτύου στο μοντέλο OSI θεωρείται το πιο αδύναμο τμήμα. Αντιθέτως, το επίπεδο 2 αγνοείται και δεν αντιμετωπίζεται σωστά ενώ ταυτόχρονα μπορεί να είναι το πιο αδύναμο επίπεδο μεταξύ όλων. Οι ερευνητές έχουν επινοήσει τεχνικές για να αποτρέψουν trojans, κακόβουλα email και μολυσμένα έγγραφα από το επίπεδο μεταφοράς ή το επίπεδο δικτύου, αλλά αγνοούν το επίπεδο ζεύξης δεδομένων. Ωστόσο, η επίθεση στο επίπεδο αυτό δεν είναι εύκολη υπόθεση και τις περισσότερες φορές, οι διαχειριστές δικτύου πιστεύουν ότι είναι ασφαλές, αλλά υποτιμούν τους εισβολείς. Χρησιμοποιώντας το φιλτράρισμα των MAC διευθύνσεων, τη δημιουργία λιστών ελέγχου πρόσβασης, τον ελέγχου ταυτότητας και εφαρμόζοντας περιορισμούς πρόσβασης, μπορεί να περιοριστεί η πρόσβαση στα ανώτερα επίπεδα του δικτύου. Αλλά το επίπεδο ζεύξης δεδομένων δεν μπορεί να παρέχει φιλτράρισμα με βάση τη διεύθυνση IP, τα πρωτόκολλα ή τη συνδεσιμότητα από άκρο σε άκρο, μπορεί να παρέχει αξιοπιστία μόνο μεταξύ των άμεσα συνδεδεμένων συσκευών.

Η παρούσα εργασία εστιάζει στην ανάλυση και προσομοίωση αυτών των επιθέσεων αλλά και τον τρόπο με τον οποίο μπορούν να αντιμετωπιστούν χρησιμοποιώντας κατάλληλες τεχνικές. Για την προσομοίωση των επιθέσεων χρησιμοποιήθηκε το πρόγραμμα GNS3 [35] στην έκδοση 2.2.39, σε σύστημα Windows 7, επεξεργαστή Intel Core i5 3570K στα 3.8GHz και 16GB DDR3 RAM. Το GNS3 (Graphical Network Simulator-3), επιτρέπει το συνδυασμό εικονικών και πραγματικών συσκευών που χρησιμοποιούνται για την προσομοίωση πολύπλοκων δικτύων. Υποστηρίζει πολλές συσκευές από πολλούς προμηθευτές, όπως Cisco virtual switches, Cisco ASA, Brocade vRouters, Cumulus Linux switches, Docker instances, HPE VSRs, Linux υλοποιησεις.

Το GNS3 χρησιμοποιεί τεχνολογία server-client. Η μεριά του client αποτελείται από ένα γραφικό περιβάλλον στο οποίο δημιουργούνται οι τοπολογίες δικτύου, γίνεται προσθαφαίρεση συσκευών και συντελεί την κυρία διεπαφή με τον χρήστη. Για τον server υπάρχουν αρκετές επιλογές. Για την εργασία χρησιμοποιήθηκε η επιλογή GNS3 Virtual Machine, όπου ο server "τρέχει "σε ένα πρόγραμμα εικονικοποίησης, στην προκείμενη περίπτωσή το Oracle VirtualBox στην έκδοση 7.0.8.

Μέσα στο πρόγραμμα δημιουργήθηκαν πολλαπλά project ανάλογα τις μεταβλητές που απαιτούσε κάθε σενάριο επίθεσης. Οι βασικές συσκευές που χρησιμοποιούνται σε καθε project είναι ένας δρομολογητής που τρέχει Cisco Layer 3 IOU, ένας μεταγωγέας που τρέχει Cisco Layer 2 IOU, PC του ίδιου του προγράμματος, και ενα PC με λειτουργικό σύστημα Kali-Linux το οποίο χρησιμοποιούσε και αυτό το πρόγραμμα εικονικοποίησης Oracle VirtualBox. Το Kali Linux είναι μια διανομή Linux ανοιχτού κώδικα, η οποία δημιουργήθηκε και συντηρείτε από την Offensive Security. Βασίζεται στην διανομή Debian Testing και έχει σχεδιαστεί για να χρησιμοποιείται από επαγγελματίες του χώρου της κυβερνοασφάλειας, από ηθικούς χάκερ, αλλά και από οποιονδήποτε θέλει να χρησιμοποιήσει την πιο προηγμένη πλατφόρμα δοκιμών διείσδυσης. Αποτελείτε από πάρα πολλά προγράμματα-εργαλεία για δοκιμές διείσδυσης και ψηφιακή εγκληματολογία αλλά απαιτεί καλή κατανόηση των εννοιών της κυβερνοασφάλειας, των δικτύων και των συστημάτων Linux για την βέλτιστη και αποτελεσματική χρήση του [36].

Για την προσομοίωση των επιθέσεων υπάρχει μία νόρμα που επαναλαμβάνεται σε κάθε project. Η διαδικασία περιλαμβάνει την δημιουργία της τοπολογίας στην οποία θα εφαρμοστεί η επίθεση και την προσθήκη συσκευών δικτύου σε σωστή διάταξη και την μεταξύ τους διασύνδεση. Έπειτα ακολουθεί η ενεργοποίηση των συσκευών. Επειδή προσομοιώνεται πραγματικό λογισμικό, οι δρομολογητές και οι μεταγωγείς δεν έχουν στην μνήμη τους κάποια διαμόρφωση και τρέχουν τις προεπιλεγμένες εργοστασιακές ρυθμίσεις. Για τον λόγο αυτό χρειάζεται να "τρέξουμε"κάποιες εντολές σε κάθε συσκευή για να δημιουργήσουμε τις απαραίτητες ρυθμίσεις που θα ορίζουν την λειτουργία της. Εφόσον ολοκληρωθεί η παραμετροποίηση των συσκευών, πραγματοποιείται ένας έλεγχος για την ομαλή λειτουργία και την επικοινωνία μεταξύ τους. Στην συνέχεια, χρησιμοποιώντας το Kali-Linux και τα κατάλληλα εργαλεία-εφαρμογές που διαθέτει, υλοποιούνται οι επιθέσεις. Τέλος, είτε χρησιμοποιώντας τα ίδια εργαλεία, είτε με άλλα προγράμματα παρακολούθησης, λαμβάνουμε πληροφορίες για το δίκτυο και ελέγχεται αν η επίθεση ήταν επιτυχής ή όχι.

Για την αντιμετώπιση των επιθέσεων απαιτείται η αναγνώριση της πηγής της επίθεσης. Ελέγχεται αν δουλεύουν σωστά τα πρωτόκολλα που χρησιμοποιούνται καθώς και οι συσκευές στις οποίες εμφανίστηκε και πραγματοποιήθηκε η επίθεση. Έπειτα πραγματοποιείται η σύσταση αντιμέτρων η οποία περιλαμβάνει συνήθως την προσθήκη ή παραμετροποίηση κάποιων εντολών της συσκευής ωστέ να αποφευχθεί η επίθεση.

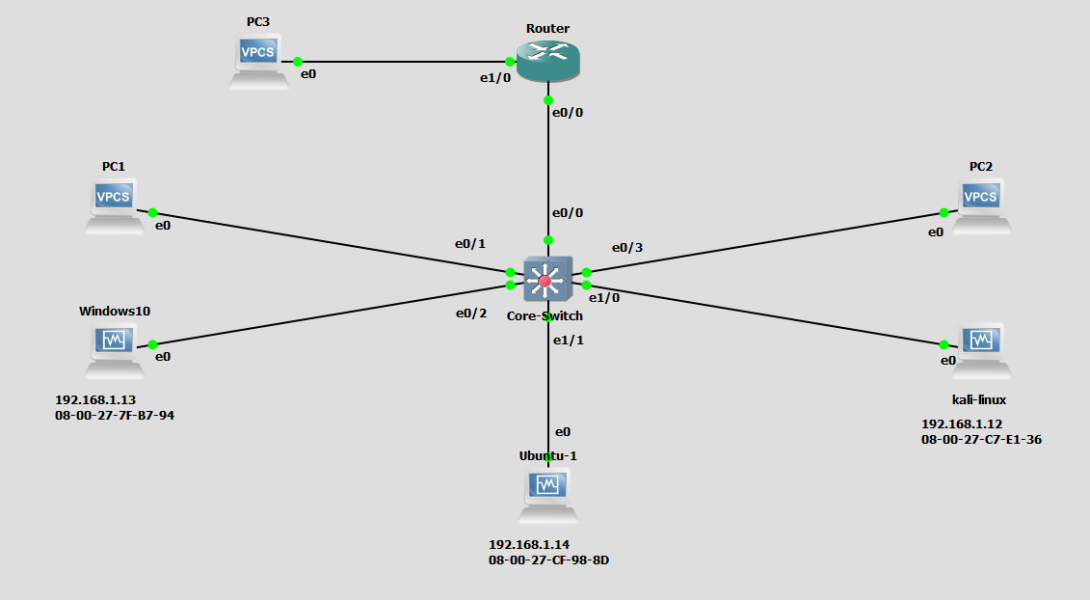
Οι επιθέσεις που προσομοιώθηκαν παρουσιάζονται αναλυτικά στις παρακάτω ενότητες:

3.3 Επιθέσεις ARP

Κατά τη μετάδοση δεδομένων εντός ενός τοπικού δικτύου (LAN), οι συσκευές χρησιμοποιούν το Πρωτόκολλο Ανάλυσης Διευθύνσεων (ARP) [37] για να μεταφράσουν τις διευθύνσεις IP σε διευθύνσεις MAC. Οι διευθύνσεις IP αποτελούν τα λογικά αναγνωριστικά για τις συσκευές που είναι συνδεδεμένες στο διαδίκτυο, ενώ οι διευθύνσεις MAC είναι τα φυσικά αναγνωριστικά που είναι αποθηκευμένα στις κάρτες δικτύου των συσκευών. Το ARP λειτουργεί μέσω αιτημάτων και απαντήσεων ARP και οι συσκευές, ενημερώνουν τους πίνακες ARP αντίστοιχα. Ωστόσο, η stateless φύση του ARP το καθιστά επηρεπές σε επιθέσεις, συμπεριλαμβανομένης της πλαστογράφησης (spoofing) ARP, όπου οι εισβολείς μπορούν να εκτελέσουν επιθέσεις Man-in-the-Middle (MiTM) για να υποκλέψουν και να χειριστούν τα δεδομένα

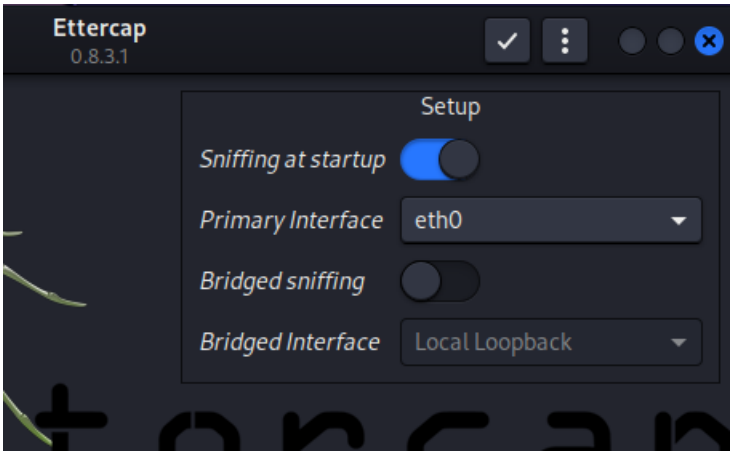
που μεταδίδονται [38].

Η τοπολογία της συγκεκριμένης προσομοίωσης απεικονίζεται στο Σχήμα 3.1.



Σχήμα 3.1: Τοπολογία επίθεσης.

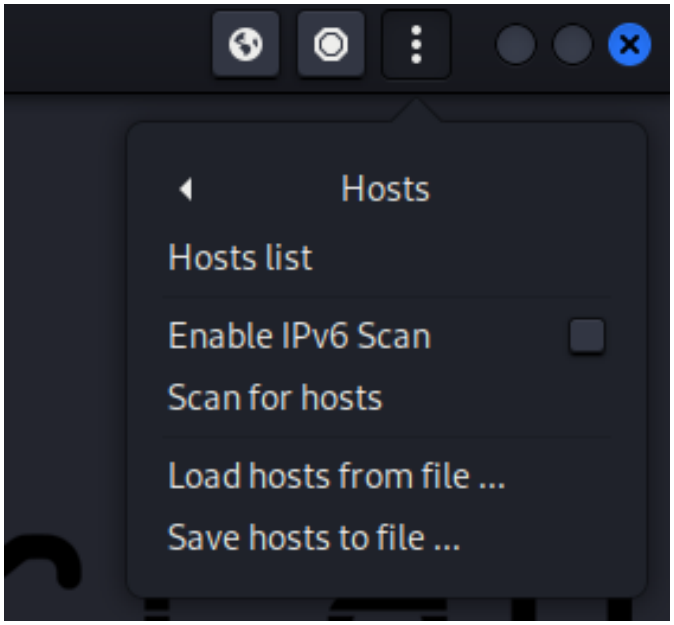
Για την προσομοίωση αυτής της επίθεσης, χρησιμοποιήθηκε το γραφικό περιβάλλον του προγράμματος Ettercap. Στο Σχήμα 3.2, απεικονίζεται η αρχική σελίδα του Ettercap, όπου μπορούν να αλλαχτούν συγκεκριμένες παράμετροι για να εξυπηρετήσουν τον σκοπό της προσομοίωσης. Στη συγκεκριμένη περίπτωση, οι παράμετροι παρέμειναν στις default επιλογές και με κλικ στο ✓αποθηκεύονται.



Σχήμα 3.2: Ρυθμίσεις του προγράμματος Ettercap.

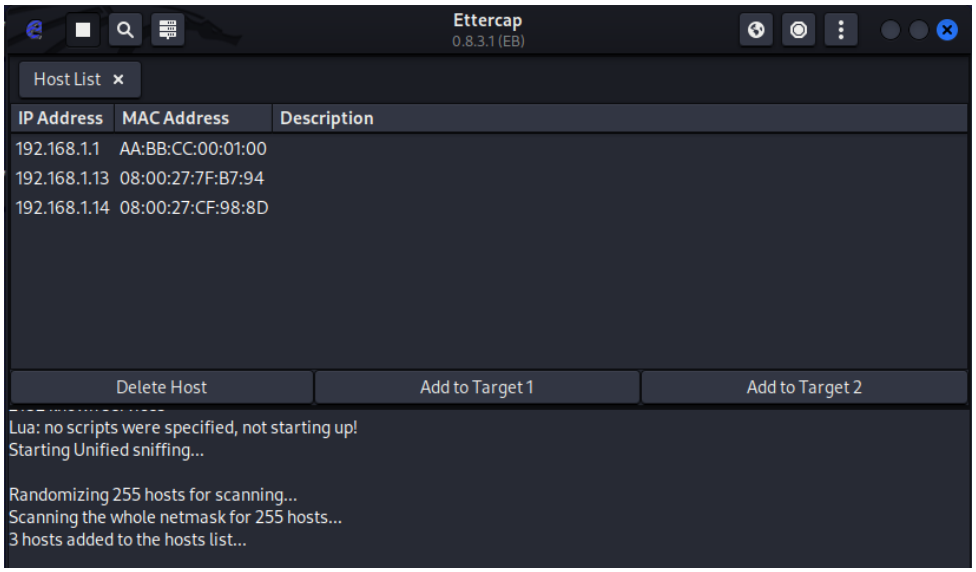
Έπειτα, επιλέγοντας τις τρεις κουκκίδες του μενού, εμφανίζεται η επιλογή “Hosts”και επιλέγεται το

“Scan for hosts”, όπως φαίνεται στο Σχήμα3.3, ώστε να εμφανιστεί η λίστα με όλους τους ενεργούς host που υπάρχουν στο δίκτυο.



Σχήμα 3.3: Hosts μενού.

Εφόσον εμφανιστούν οι διαθέσιμοι host, όπως φαίνεται στο Σχήμα 3.4, επιλέγεται αυτός στον οποίο θα γίνει η επίθεση κάνοντας κλικ στο “Add to Target1”. Στο παράδειγμα επιλέγουμε τον host με IP 192.168.1.13 και MAC 08:00:27:7F:B7:94.

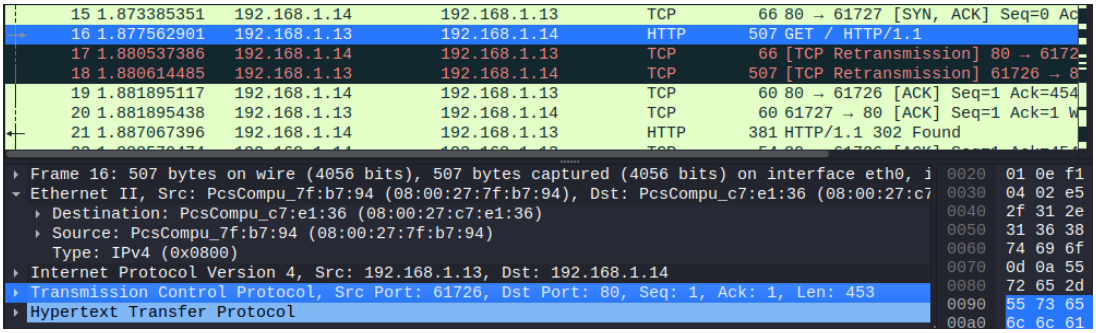


Σχήμα 3.4: Λίστα με τους διαθέσιμους host.

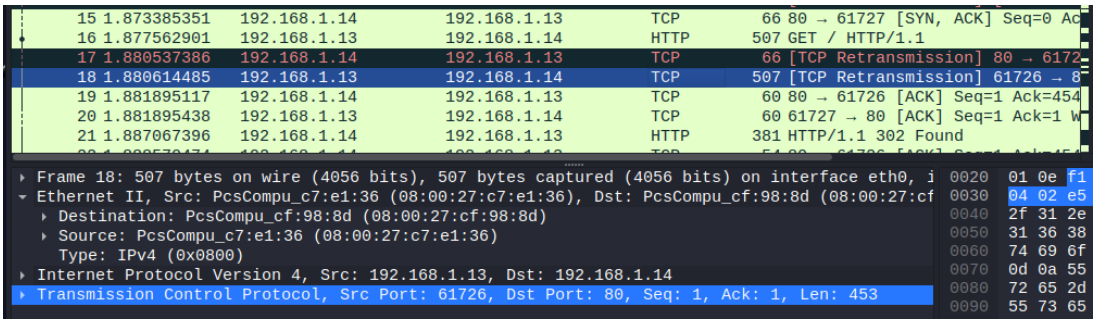
Έπειτα κάνοντας κλικ στο εικονίδιο με την υδρόγειο, βρίσκονται οι τύποι επιθέσεων που μπορούν να

εκτελεστούν. Στην παρόν παράδειγμα, επιλέγεται το “Arp poisoning”και έπειτα OK.

Η πλαστογράφηση του ARP ξεκινάει. Αν δεν επιλεγεί άλλος host στο “Add to Target2”, τότε χρησιμοποιούνται όλοι οι host στην επίθεση, διαφορετικά εάν επιλεγεί ένας συγκεκριμένος host, το spoofing γίνεται μόνο ανάμεσα στους “στόχους”που επιλέχθηκαν. Συγκεκριμένα, μέσω του Wireshark (Σχήμα 3.5 και 3.6) παρατηρούμε ότι για τις επικοινωνίες που προσπαθούν να γίνουν μεταξύ των χρηστών με IP 192.168.1.13 και 192.168.1.14, τα πακέτα προωθούνται πρώτα στον host που εκτελεί την επίθεση (08:00:27:C7:E1:36) και έπειτα καταφθάνουν στον τελικό χρήστη. Αυτό γίνεται γιατί ο επιτιθέμενος διαφημίζει την MAC του με την IP του στόχου με αποτέλεσμα τα πακέτα να δρομολογούνται σε αυτόν.



Σχήμα 3.5: Wireshark-Στιγμιότυπο των επικοινωνιών.



Σχήμα 3.6: Wireshark-Στιγμιότυπο των επικοινωνιών.

Η επίθεση μπορεί να αποφευχθεί ορίζοντας τις κατάλληλες παραμέτρους στο switch που διασυνδέει τις συσκευές. Πιο συγκεκριμένα, ενεργοποιώντας το arp inspection (Σχήμα 3.7). Ταυτόχρονα, η θύρα που συνδέεται ο δρομολογητής πρέπει να γίνει trust ώστε τα πακέτα να μην περνάνε από έλεγχο.

```
Core-Switch#
Core-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch(config)#ip arp inspection vlan 1
Core-Switch(config)#int eth 0/0
Core-Switch(config-if)#ip arp inspection trust
Core-Switch(config-if)#
```

Σχήμα 3.7: Ενεργοποίηση του ARP Inspection στον μεταγωγέα.

Στην επόμενη προσπάθεια που θα γίνει για επίθεση, το Switch αντιλαμβάνεται τον μεγάλο αριθμό από πακέτα ARP Request [39] σε σύντομο χρονικό διάστημα και λαμβάνει τα απαραίτητα μέτρα απενεργοποιώντας την θύρα του επιτιθέμενου, Σχήμα 3.8.

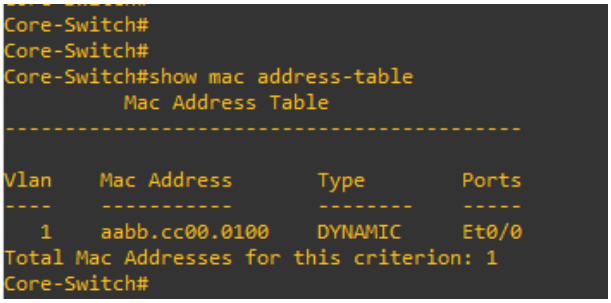
```
Core-Switch#
Nov 20 20:33:34.060: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 154 milliseconds on Et1/0.
Nov 20 20:33:34.060: %PM-4-ERR_DISABLE: arp-inspection error detected on Et1/0, putting Et1/0 in err-disable state
Nov 20 20:33:34.131: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.1/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:34.131: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.213/20:33:33 UTC Mon Nov 20 2023])
Core-Switch#
Nov 20 20:33:34.131: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.160/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:34.131: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.245/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:34.131: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.132/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:35.066: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
Nov 20 20:33:35.132: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.211/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:35.132: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.176/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:35.132: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.151/20:33:33 UTC Mon Nov 20 2023])
Core-Switch#
Nov 20 20:33:35.132: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.141/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:35.132: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.107/20:33:33 UTC Mon Nov 20 2023])
Nov 20 20:33:36.063: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
Nov 20 20:33:36.134: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.126/20:33:34 UTC Mon Nov 20 2023])
Nov 20 20:33:36.134: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.54/20:33:34 UTC Mon Nov 20 2023])
Nov 20 20:33:36.134: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.25/20:33:34 UTC Mon Nov 20 2023])
Core-Switch#
Nov 20 20:33:36.134: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.13/20:33:34 UTC Mon Nov 20 2023])
Nov 20 20:33:36.134: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et1/0, vlan 1.([0800.27c7.e136/192.168.1.12/0000.0000.0000/192.168.1.9/20:33:34 UTC Mon Nov 20 2023])
Core-Switch#
```

Σχήμα 3.8: Το μήνυμα που εμφανίζεται στον μεταγωγέα κατά την προσπάθεια νέας επίθεσης.

3.4 MAC Flooding

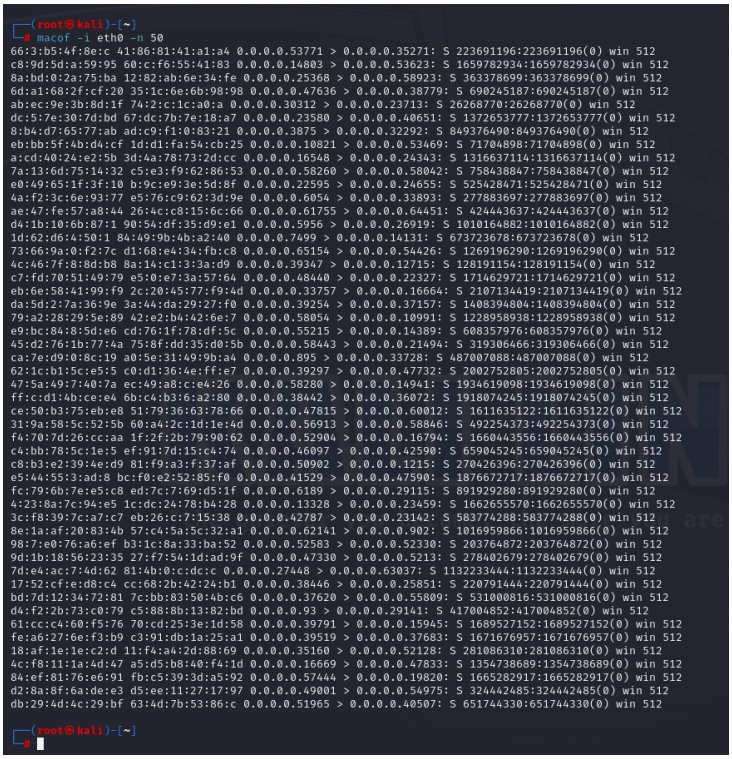
Και αυτή η προσομοίωση εκτελείται στο δίκτυο του Σχήματος 3.1.

Με την εντολή show mac address-table (Σχήμα 3.9), εμφανίζονται οι φυσικές διευθύνσεις που αναγνωρίζει ο μεταγωγέας καθώς και ο τρόπος με τον οποίο της έμαθε. Σύμφωνα με την κίνηση που διερχόταν από αυτόν, αποθηκεύει τις διευθύνσεις αυτές σε αντιστοιχία με το interface που συνδέονταν.



Σχήμα 3.9: Αποτέλεσμα της εντολής show mac address-table.

Στο terminal του επιτιθέμενου, γίνεται χρήση του εργαλείου macof, όπου επιλέγοντας ένα συγκεκριμένο Interface, γίνεται ταυτόχρονη προώθηση μεγάλου αριθμού διαφορετικών mac διευθύνσεων ώστε να προκληθεί άρνηση υπηρεσίας. Αρχικά, στο Σχήμα 3.10 φαίνεται ότι επιλέχθηκε το interface (eth0) και ο αριθμός των MAC που θα προωθηθούν (50). Άμεσα, με την εκτέλεση της εντολής, ο αριθμός MAC που δηλώθηκε, αρχίζει να κατακλύζει το interface που επιλέχθηκε.



Σχήμα 3.10: Αποστολή 50 MAC διευθύνσεων.

Για την επαλήθευση των εγγραφών, εκτελώντας ξανά την εντολή show mac address-table [40], φαίνεται πλέον στο Σχήμα 3.11, ότι και οι 50 διευθύνσεις έχουν εγγραφεί επιτυχώς στον πίνακα.

```
Core-Switch#
Core-Switch#
Core-Switch#show mac address-table
          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0423.8a7c.94e5    DYNAMIC     Et1/0
   1    08b4.d765.77ab    DYNAMIC     Et1/0
   1    0acd.4024.e25b    DYNAMIC     Et1/0
   1    1752.cf0e.d8c4    DYNAMIC     Et1/0
   1    18af.1e1e.c20d    DYNAMIC     Et1/0
   1    1d62.d604.5001    DYNAMIC     Et1/0
   1    319a.585c.525b    DYNAMIC     Et1/0
   1    3cf8.397c.a7c7    DYNAMIC     Et1/0
   1    45d2.761b.774a    DYNAMIC     Et1/0
   1    475a.4907.407a    DYNAMIC     Et1/0
   1    4af2.3c6e.9377    DYNAMIC     Et1/0
   1    4c46.7f08.8db8    DYNAMIC     Et1/0
   1    4cf8.111a.4d47    DYNAMIC     Et1/0
   1    61cc.c460.f576    DYNAMIC     Et1/0
   1    621c.b15c.e505    DYNAMIC     Et1/0
   1    6603.b54f.8e0c    DYNAMIC     Et1/0
   1    6da1.682f.cf20    DYNAMIC     Et1/0
   1    7366.9a00.f27c    DYNAMIC     Et1/0
   1    79a2.2829.5e89    DYNAMIC     Et1/0
   1    7a13.6d75.1432    DYNAMIC     Et1/0
   1    7de4.ac07.4d62    DYNAMIC     Et1/0
   1    84ef.8176.e691    DYNAMIC     Et1/0
   1    8abd.002a.75ba    DYNAMIC     Et1/0
   1    8e1a.af20.834b    DYNAMIC     Et1/0
   1    9807.e076.a6ef    DYNAMIC     Et1/0
   1    9d1b.1856.2335    DYNAMIC     Et1/0
   1    aabb.cc00.0100    DYNAMIC     Et0/0
   1    abec.9e3b.8d1f    DYNAMIC     Et1/0
   1    ae47.fe57.a844    DYNAMIC     Et1/0
   1    bd7d.1234.7281    DYNAMIC     Et1/0
   1    c4bb.785c.1e05    DYNAMIC     Et1/0
   1    c7fd.7051.4979    DYNAMIC     Et1/0
   1    c89d.5d0a.5995    DYNAMIC     Et1/0
   1    c8b3.e239.4ed9    DYNAMIC     Et1/0
   1    ca7e.d900.8c19    DYNAMIC     Et1/0
   1    ce50.b375.ebe8    DYNAMIC     Et1/0
   1    d28a.8f6a.dee3    DYNAMIC     Et1/0
   1    d41b.106b.8701    DYNAMIC     Et1/0
   1    d4f2.2b73.c079    DYNAMIC     Et1/0
   1    da5d.027a.369e    DYNAMIC     Et1/0
   1    db29.4d4c.29bf    DYNAMIC     Et1/0
   1    dc05.7e30.7dbd    DYNAMIC     Et1/0
   1    e049.651f.3f10    DYNAMIC     Et1/0
   1    e544.5503.ad08    DYNAMIC     Et1/0
   1    e9bc.8408.5de6    DYNAMIC     Et1/0
   1    eb6e.5841.99f9    DYNAMIC     Et1/0
   1    ebbb.5f4b.d4cf    DYNAMIC     Et1/0
   1    f470.7d26.ccaa    DYNAMIC     Et1/0
   1    fc79.6b7e.e5c8    DYNAMIC     Et1/0
   1    fea6.276e.f3b9    DYNAMIC     Et1/0
   1    ff0c.d14b.cee4    DYNAMIC     Et1/0
Total Mac Addresses for this criterion: 51
Core-Switch#
```

Σχήμα 3.11: Αποστολή 50 MAC διευθύνσεων.

Όμως ο αριθμός των 50 διευθύνσεων, δεν επαρκεί για να προκαλέσει άρνηση υπηρεσίας. Αφαιρώντας το φίλτρο -n 50 από την εντολή του macof, η αποστολή των MAC παύει να έχει όριο και στέλνει διαρκώς νέες διευθύνσεις. Στο στιγμιότυπο που φαίνεται στο Σχήμα 3.12, οι εγγραφές έχουν φτάσει τις 13.417 διευθύνσεις. Ο αριθμός των διευθύνσεων που μπορεί να δεχτεί ένας πίνακας MAC διευθύνσεων, εξαρτάται από το μοντέλο του μεταγωγέα και τις δυνατότητές του [41]. Συνήθως, τα πιο εμπορικά switch έχουν την δυνατότητα να αποθηκεύσουν έως 8.000 εγγραφές [42], ενώ τα switch υψηλότερων κατηγο-

ριών δίνουν ένα εύρος 8.000 μέχρι 32.000 διευθύνσεις [43].

```
  1    ffd2.e72a.f46a    DYNAMIC     Et1/0
  1    ffd3.1e5d.cfe1    DYNAMIC     Et1/0
  1    ffd4.ab14.ef03    DYNAMIC     Et1/0
  1    ffd5.6f70.9d38    DYNAMIC     Et1/0
  1    ffd5.846d.726f    DYNAMIC     Et1/0
  1    ffd6.362b.f313    DYNAMIC     Et1/0
  1    ffda.9554.9f2e    DYNAMIC     Et1/0
  1    ffdc.1465.e2d4    DYNAMIC     Et1/0
  1    ffde.515a.8cb4    DYNAMIC     Et1/0
  1    ffde.b765.f30f    DYNAMIC     Et1/0
  1    ffdf.b91b.da98    DYNAMIC     Et1/0
  1    ffe6.5046.8d69    DYNAMIC     Et1/0
  1    ffe9.b719.cba3    DYNAMIC     Et1/0
  1    ffea.a906.e22d    DYNAMIC     Et1/0
  1    ffed.2637.f017    DYNAMIC     Et1/0
  1    fffa.db73.465e    DYNAMIC     Et1/0
  1    ffff.711e.8fb7    DYNAMIC     Et1/0
otal Mac Addresses for this criterion: 13417
ore-Switch#
```

Σχήμα 3.12: Στιγμιότυπο MAC Flooding.

Εφόσον υπερβεί το όριο των MAC διευθύνσεων, το switch σταματά να ανταποκρίνεται σωστά, γεγονός που επιβεβαιώνεται στο Σχήμα 3.13, όπου φαίνεται ότι το PC1 δεν μπορεί να αποκτήσει διεύθυνση IP καθώς το switch δεν δρομολογεί σωστά την κίνηση.

```
Welcome to Virtual PC Simulator, version 0.8.2
Dedicated to Daling.
Build time: Aug 23 2021 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file


DDDO
Can't find dhcp server

PC1>
PC1> ip dhcp
DORA IP 192.168.1.12/24 GW 192.168.1.1

PC1>
```

Σχήμα 3.13: Αποτέλεσμα της επίθεσης MAC Flooding.

Για να αποτραπεί η παραπάνω επίθεση, χρειάζεται να γίνουν οι απαραίτητες ρυθμίσεις στο switch. Συγκεκριμένα, με το ip arp inspection, η κίνηση των ARP πακέτων από και προς το VLAN που επιλέχθηκε θα ελέγχεται. Επαληθεύεται ότι η διεύθυνση MAC στο πακέτο ARP ταιριάζει με τη διεύθυνση IP. Εάν ένα πακέτο ARP αποτύχει στη διαδικασία επαλήθευσης, ο μεταγωγέας θα απορρίψει το πακέτο, εμποδίζοντάς το να φτάσει σε άλλες συσκευές στο δίκτυο. Στο interface που συνδέεται ο μεταγωγέας με τον δρομολογητή, δίνεται η εντολή ip arp inspection trust ώστε να επιτρέπεται η ομαλή κίνηση στο δίκτυο και ταυτόχρονα ενεργοποιείται το ip dhcp snooping, όπως φαίνεται στο Σχήμα 3.14

```
Core-Switch#
Core-Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch(config)#
Core-Switch(config)#
Core-Switch(config)#
Core-Switch(config)#
Core-Switch(config)#ip arp inspection vlan 1
Core-Switch(config)#
Core-Switch(config)#interface eth0/0
Core-Switch(config-if)#ip arp inspection trust
Core-Switch(config-if)#exit
Core-Switch(config)#
Core-Switch(config)#ip dhcp snooping
Core-Switch(config)#
Core-Switch(config)#
Core-Switch(config)#
```

Σχήμα 3.14: Ενεργοποίηση του ARP Inspection και του DHCP Spoofing.

Για να επαληθευτεί η αποτελεσματικότητα των ρυθμίσεων και η ακεραιότητα του δικτύου, επιχειρώντας να γίνει η ίδια επίθεση, το switch πλεόν αντιτίθεται στις κακόβουλες ενέργειες. Στο Σχήμα 3.15, φαίνεται ότι ο μεταγωγέας αναγνωρίζει τον φόρτο των πακέτων που προέρχονται από μία μόνο θύρα με αποτέλεσμα να την απενεργοποιεί αυτόματα ώστε να προστατευτεί το δίκτυο.

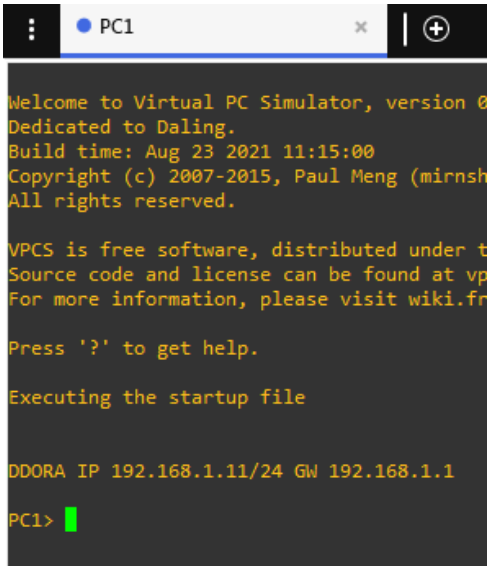
```
Core-Switch#
*May 11 16:24:51.919: %SW_DAI-4-PACKET_RATE_EXCEEDED: 16 packets received in 153 milliseconds on Et1/0.
*May 11 16:24:51.919: %PM-4-ERR_DISABLE: arp-inspection error detected on Et1/0, putting Et1/0 in err-disable state
*May 11 16:24:52.925: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to down
Core-Switch#
*May 11 16:24:53.924: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to down
Core-Switch#
```

Σχήμα 3.15: Αποτέλεσμα του DAI μετά από προσπάθεια για νέα επίθεση

3.5 Επιθέσεις DHCP

Και αυτή η προσομοίωση εκτελείται στο δίκτυο του Σχήματος 3.1.

Στο δίκτυο αυτής της επίθεσης, ο router έχει τον ρόλο του DHCP server και διαμοιράζει τις IP διευθύνσεις [44] στις συσκευές. Ο υπολογιστής PC1 μέσω του μηχανισμού DORA (Discover Offer Request Acknowledge) παίρνει και αυτός την IP του όπως φαίνεται στο Σχήμα 3.16.



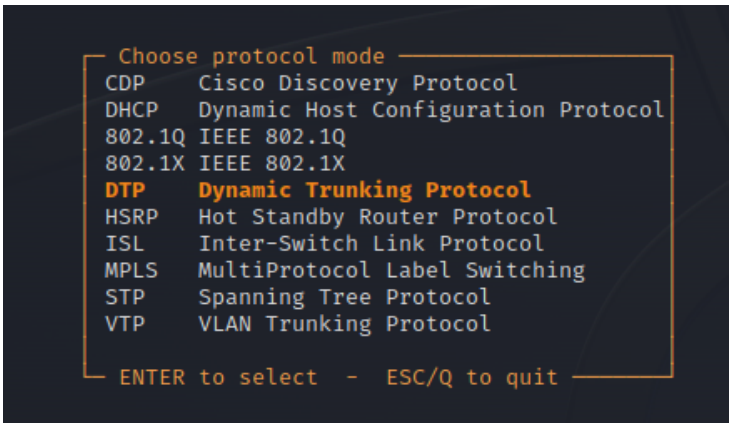
Σχήμα 3.16: Η διεύθυνση IP του PC1.

Αντίστοιχα, στον δρομολογητή εκτελώντας την εντολή show ip dhcp binding [45], εμφανίζεται η ip που πήρε ο υπολογιστής, η φυσική του διεύθυνση καθώς και το lease expiration time, Σχήμα 3.17.

```
Router#
Router#
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.11        0100.5079.6668.00       Sep 26 2020 02:35 PM    Automatic
Router#
```

Σχήμα 3.17: Οι διευθύνσεις IP που έχουν δεσμευτεί μέσω του DHCP.

Χρησιμοποιώντας την εφαρμογή Yersinia (Σχήμα 3.18) και επιλέγοντας το πρωτόκολλο DHCP με την επίθεση “Flood Discovery packets”, ξεκινάει η επίθεση. Με τον κατακλυσμό αιτημάτων Discovery, δεσμεύονται όλες οι διαθέσιμες ip διευθύνσεις από το εύρος του DHCP pool του δρομολογητή.



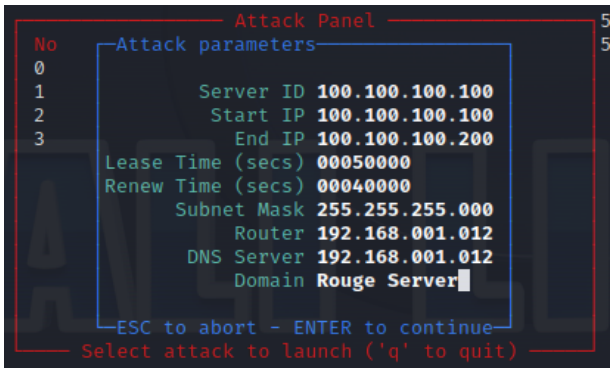
Σχήμα 3.18: Μενού πρωτοκόλλων στο πρόγραμμα Yersinia.

Με την εντολή show ip dhcp binding, στον δρομολογητή, επιβεβαιώνεται ότι πράγματι έχουν γίνει lease όλες οι IP με διαφορετικές MAC διευθύνσεις, Σχήμα 3.19.

```
Router#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.1.11        0100.5079.6668.00       Sep 26 2020 02:35 PM    Automatic
192.168.1.12        1d3a.5b58.e1e6          Sep 19 2020 02:43 PM    Automatic
192.168.1.13        c717.b63f.ec81          Sep 19 2020 02:43 PM    Automatic
192.168.1.14        2f6e.a674.ea29          Sep 19 2020 02:43 PM    Automatic
192.168.1.15        25c2.6445.c66d          Sep 19 2020 02:43 PM    Automatic
192.168.1.16        63d2.9064.b4ef          Sep 19 2020 02:43 PM    Automatic
192.168.1.17        078a.5a6d.4ffe          Sep 19 2020 02:43 PM    Automatic
192.168.1.18        c06e.5227.c932          Sep 19 2020 02:43 PM    Automatic
192.168.1.19        79f2.204c.ad6f          Sep 19 2020 02:43 PM    Automatic
192.168.1.20        3f95.e174.b0bc          Sep 19 2020 02:43 PM    Automatic
192.168.1.21        76de.5413.2743          Sep 19 2020 02:43 PM    Automatic
192.168.1.22        fdf4.5004.90fc          Sep 19 2020 02:43 PM    Automatic
192.168.1.23        7eab.0053.9869          Sep 19 2020 02:43 PM    Automatic
192.168.1.24        5b4a.c80b.6305          Sep 19 2020 02:43 PM    Automatic
192.168.1.25        bcc0.3d14.12c4          Sep 19 2020 02:43 PM    Automatic
192.168.1.26        7e8d.d039.80fa          Sep 19 2020 02:43 PM    Automatic
192.168.1.27        7080.f01e.c6d9          Sep 19 2020 02:43 PM    Automatic
192.168.1.28        7f69.e377.ddf6          Sep 19 2020 02:43 PM    Automatic
192.168.1.29        2dce.860d.3844          Sep 19 2020 02:43 PM    Automatic
192.168.1.30        a1b9.2767.3de3          Sep 19 2020 02:43 PM    Automatic
192.168.1.31        1830.e701.bcd7          Sep 19 2020 02:43 PM    Automatic
192.168.1.32        d30a.1f48.6129          Sep 19 2020 02:43 PM    Automatic
192.168.1.33        6689.a74c.04e9          Sep 19 2020 02:43 PM    Automatic
192.168.1.34        72cb.b810.a794          Sep 19 2020 02:43 PM    Automatic
192.168.1.35        4b8d.674b.4b66          Sep 19 2020 02:43 PM    Automatic
192.168.1.36        00e0.5771.7dca          Sep 19 2020 02:43 PM    Automatic
192.168.1.37        0645.6c64.a64a          Sep 19 2020 02:43 PM    Automatic
192.168.1.38        115c.fd6a.f227          Sep 19 2020 02:43 PM    Automatic
192.168.1.39        bc15.821e.321d          Sep 19 2020 02:43 PM    Automatic
192.168.1.40        2f9d.2510.3809          Sep 19 2020 02:43 PM    Automatic
192.168.1.41        3f3b.0526.a374          Sep 19 2020 02:43 PM    Automatic
192.168.1.42        5299.666a.a500          Sep 19 2020 02:43 PM    Automatic
192.168.1.43        49f2.215c.1b65          Sep 19 2020 02:43 PM    Automatic
192.168.1.44        e653.9c23.1f2a          Sep 19 2020 02:43 PM    Automatic
192.168.1.45        80da.d34e.4b18          Sep 19 2020 02:43 PM    Automatic
192.168.1.46        c850.943c.535b          Sep 19 2020 02:43 PM    Automatic
192.168.1.47        8c99.7c56.4f60          Sep 19 2020 02:43 PM    Automatic
```

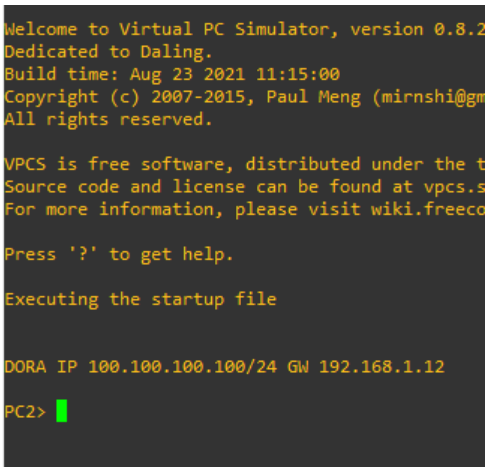
Σχήμα 3.19: Οι διευθύνσεις IP που έχουν δεσμευτεί μέσω του DHCP, μετά το flooding.

Πίσω στο Yersinia, επιλέγοντας την επίθεση “creating DHCP rogue server”, δημιουργείται ένας εικονικός DHCP server, ο οποίος έχει ψεύτικες παραμέτρους. Στο παράδειγμα του Σχήματος 3.20, απεικονίζονται οι παράμετροι ip, subnet mask, router που επιλέχθηκαν.



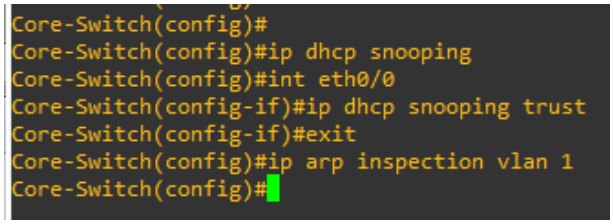
Σχήμα 3.20: Οι παράμετροι του κακόβουλου server.

Ορίζοντας ένα τυχαίο δίκτυο διαφορετικό από το υπάρχον, όποιος client (PC) ζητήσει IP θα την λάβει πλέον από τον εικονικό DHCP Server. Σαν router IP μπορούμε να βάλουμε την πραγματική IP του router και τα πακέτα να δρομολογούνται κανονικά προς την default gateway. Εναλλακτικά μπορούμε να βάλουμε την IP διεύθυνση του επιτιθέμενου με σκοπό όλα τα πακέτα να περνάνε προς αυτόν πρώτα. Μπορούμε να επιβεβαιώσουμε την λειτουργία του κακόβουλου DHCP Server βλέποντας την IP που έχει δοθεί στο PC2 μέσω DHCP, Σχήμα 3.21.



Σχήμα 3.21: Η διεύθυνση IP του PC2.

Για την αποφυγή αυτής της επίθεσης, αρκεί να εκτελεστούν οι εντολές “ip dhcp snooping”, “ip arp inspection vlan 1”και τέλος στο Interface που καταλήγει στον router/DHCP Server, “ip dhcp snooping trust”, όπως φαίνεται στο στιγμιότυπο του Σχήματος 3.22. Πλεόν, το switch θα δέχεται πακέτα μόνο από έμπιστα (trusted) interface,δηλαδή όπως δηλώθηκε στις εντολές, μόνο από αυτό του δρομολογητή.



Σχήμα 3.22: Η διεύθυνση IP του PC2.

3.6 Επιθέσεις CDP

Και αυτή η προσομοίωση εκτελείται στο δίκτυο του Σχήματος 3.1.

Το CDP-Cisco Discovery Protocol, αποτελεί ένα πρωτόκολλο το οποίο επιτρέπει τις συσκευές Cisco να επικοινωνούν μεταξύ τους και να διαμοιράζονται πληροφορίες σχετικές με την κατάστασή τους. Επιλέγοντας το core switch της τοπολογίας και εκτελώντας την εντολή "show cdp neighbors" [46], εμφανίζονται μόνο τα στοιχεία του δρομολογητή καθώς αυτός αποτελεί τη μόνη συσκευή που υπάρχει στο δίκτυο (Σχήμα 3.23).

```
Core-Switch#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router           Eth 0/0           157              R B   Linux Uni Eth 0/0
```

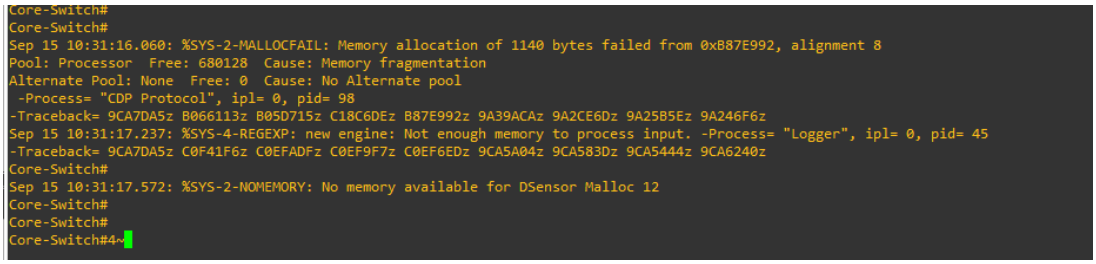
Σχήμα 3.23: Αποτέλεσμα της εντολής show cdp neighbors.

Επιλέγοντας πάλι το πρόγραμμα Yersinia, αυτή τη φορά με το πρωτόκολλο CDP και με την επίθεση flood cdp table. Έτσι ξεκινάει ο καταιγισμός του πίνακα CDP με στοιχεία πλαστών συσκευών με διαφορετικά id/capabilities, μέχρι να γίνει χειροκίνητα παύση της αποστολής. Η μνήμη του CDP table γεμίζει με τις εγγραφές που στάλθηκαν μέχρι να γίνει η παύση. Στο στιγμιότυπο του Σχήματος 3.24 ο συνολικός αριθμός των εγγραφών, φαίνεται να έχει φτάσει τις 864.

```
Core-Switch#
Core-Switch#sho cd n
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Router           Eth 0/0           50               R B   Linux Uni Eth 0/0
OOOOO6I          Eth 1/0           243            B H I r yersinia  Eth 0
WWWW000          Eth 1/0           242              R T I  yersinia  Eth 0
000QQQQ          Eth 1/0           74               S I r  yersinia  Eth 0
0MMMMMM          Eth 1/0           245              B H r  yersinia  Eth 0
0NNNNNN          Eth 1/0           75               R B S  yersinia  Eth 0
WW00000          Eth 1/0           58             R T S I  yersinia  Eth 0
VVVV000          Eth 1/0           245              R T I  yersinia  Eth 0
WWWWWW0          Eth 1/0           240              R T I  yersinia  Eth 0
000RRRR          Eth 1/0           242              R B r  yersinia  Eth 0
SS00000          Eth 1/0           243            R T H I yersinia  Eth 0
RRRR000          Eth 1/0           241            R T B S yersinia  Eth 0
RRRRRR0          Eth 1/0           244            R T H I yersinia  Eth 0
VV00000          Eth 1/0           244            R T S I  yersinia  Eth 0
SSSSSS0          Eth 1/0           44             R T H I yersinia  Eth 0
00000RR          Eth 1/0           241            R S I r yersinia  Eth 0
0RRRRRR          Eth 1/0           241            R S I r yersinia  Eth 0
VVVVVV0          Eth 1/0           240            R T S I  yersinia  Eth 0
00000MM          Eth 1/0           46               H I   yersinia  Eth 0
RR00000          Eth 1/0           244            R T B H  yersinia  Eth 0
000NNNN          Eth 1/0           240              R B H r yersinia  Eth 0
000MMMM          Eth 1/0           240              B H r  yersinia  Eth 0
00000QQ          Eth 1/0           240              S I r  yersinia  Eth 0


Total cdp entries displayed : 864
Core-Switch#
```

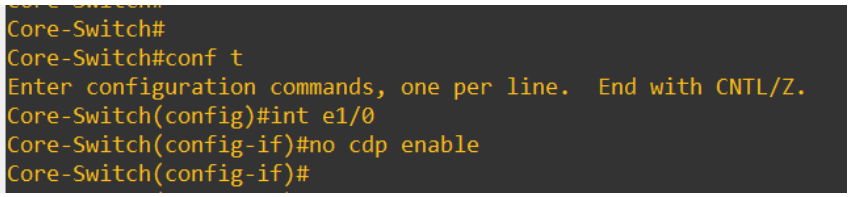
Σχήμα 3.24: Αποτέλεσμα της εντολής show cdp neighbors.

Το switch εμφανίζει error καθώς δεν διαθέτει επιπλέον πόρους μνήμης για να εκτελέσει άλλες διεργασίες, όπως φαίνεται στο Σχήμα 3.25, στο μήνυμα που εμφανίζει. Συνεπώς, το αποτέλεσμα της επίθεσης είναι η άρνηση υπηρεσίας καθώς ο μεταγωγέας παύει να είναι λειτουργικός και να ανταποκρίνεται.



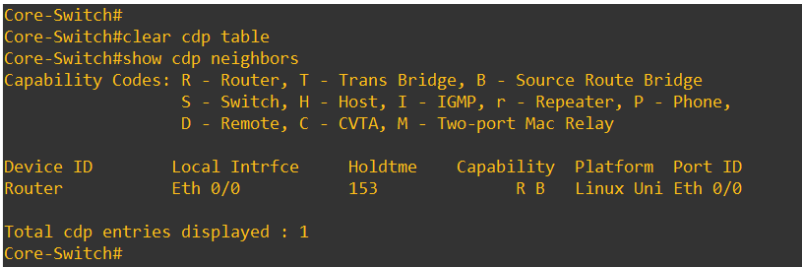
Σχήμα 3.25: Πρόβλημα μνήμης στο switch.

Για την αποφυγή της επίθεσης, χρειάζεται να προστατευτούν οι θύρες που δεν χρησιμοποιούνται. Δηλαδή, στις θύρες όπου δεν συνδέεται δικτυακός εξοπλισμός όπως router ή switch, αλλά συνδέονται μόνο τελικοί χρήστες, πρέπει να αποκλείεται η μεταφορά των CDP πληροφοριών. Στα interface του switch που πρέπει να απενεργοποιηθεί το πρωτόκολλο, γίνεται εκτέλεση της εντολής no cdp enable, Σχήμα 3.26.



Σχήμα 3.26: Απενεργοποίηση του CDP.

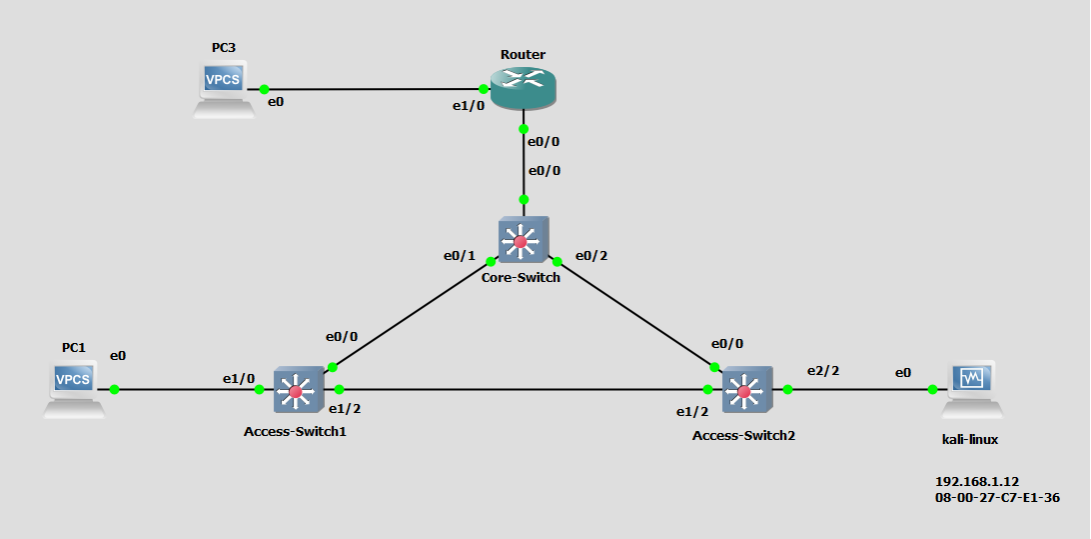
Επιβεβαιώνεται η σωστή καταγραφή στον πίνακα cdp, κάνοντας αρχικά clear cdp table για να διαγραφούν οι υπάρχουσες εγγραφές και έπειτα με το show cdp neighbors, εμφανίζονται οι σωστές εγγραφές, δηλαδή μόνο τα στοιχεία του δρομολογητή που είναι συνδεδεμένος, Σχήμα 3.27.



Σχήμα 3.27: Αποκατάσταση λειτουργίας του switch.

3.7 Επιθέσεις STP

Η τοπολογία της συγκεκριμένης προσομοίωσης απεικονίζεται στο Σχήμα 3.28.



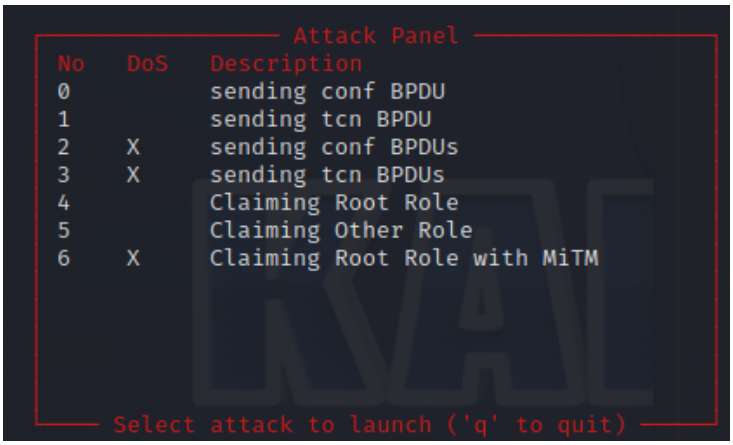
Σχήμα 3.28: Τοπολογία επίθεσης.

Το STP - Spanning Tree Protocol [47], παρέχει πλεονάζουσες διαδρομές ενώ ταυτόχρονα αποτρέπει την δημιουργία βρόγχων στο δίκτυο. Λειτουργεί ορίζοντας έναν μεταγώγεα ως ρίζα(root) μέσω μιας διαδικασίας εκλογών, κρατώντας λειτουργικές μόνο τις διαδρομές-συνδέσεις που οδηγούν προς αυτόν και έχοντας ως εφεδρικές τις υπόλοιπες συνδέσεις. Σε συσκευές Cisco χρησιμοποιείται και το PVST (Per VLAN Spanning Tree), το οποίο λειτουργεί με όμοιο τρόπο. Το STP είναι αυτόματα ενεργό κατά την εκκίνηση της συσκευής. Από την διαδικασία των εκλογών που συμβαίνει, ορίζεται σαν root το Core Switch, Σχήμα 3.29.

```
Core-Switch#
Core-Switch#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID    Priority    32769
             Address     aabb.cc00.0200
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
             Address     aabb.cc00.0200
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr
Et1/2               Desg FWD 100       128.7    Shr
Et1/3               Desg FWD 100       128.8    Shr
Et2/0               Desg FWD 100       128.9    Shr
Et2/1               Desg FWD 100       128.10   Shr
Et2/2               Desg FWD 100       128.11   Shr
Et2/3               Desg FWD 100       128.12   Shr
Et3/0               Desg FWD 100       128.13   Shr
Et3/1               Desg FWD 100       128.14   Shr
Et3/2               Desg FWD 100       128.15   Shr
Et3/3               Desg FWD 100       128.16   Shr
```

Σχήμα 3.29: Το core Switch έχει το ρόλο του root στο STP.

Για την επιλογή του τύπου επίθεσης, χρησιμοποιήθηκε και εδώ το πρόγραμμα Yersinia. Οι επιθέσεις που μπορούν να υλοποιηθούν, απεικονίζονται στο Σχήμα 3.30.



Σχήμα 3.30: Πανελ επιθέσεων στο Yersinia.

Στην παρούσα υλοποίηση, αρχικά επιλέχθηκε η επίθεση 4:Claiming Root Role, στην οποία αφαιρείται ο ρόλος του root από το core switch. Στο root id, δεν εμφανίζεται το μήνυμα “This bridge is the root”, αλλά υποδικνύεται η θύρα στην οποία βρισκεται ο root, Σχήμα 3.31.

```
Core-Switch#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     aabb.cc00.0000
              Cost        300
              Port        3 (Ethernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     aabb.cc00.0200
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Root FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
```

Σχήμα 3.31: Το core switch δεν εμφανίζεται πλέον σαν root.

Παράλληλα, εκτελείται και η επίθεση 3: Sending tcn BPDUs με αποτέλεσμα να μειώνεται η απόδοση του switch και να υπολειτουργεί. Αργότερα, γίνεται παύση της επίθεσης 4 και ξανά προσπάθεια για την εκλογή νέου root, όμως τα switch συνεχίζουν να μην ανταποκρίνονται και να δρομολογούν την κίνηση σωστά Σχήμα 3.32.

```
PC1>
PC1> ping 192.168.1.1

host (192.168.1.1) not reachable

PC1>
PC1>
```

Σχήμα 3.32: Το switch δεν δρομολογεί κίνηση.

Τέλος, εκτελείται και η επίθεση 2: Sending conf BPDUs, γεγονός που προκαλεί σε όλα τα switch της τοπολογίας να μην λειτουργούν σωστά με αποτέλεσμα άρνηση υπηρεσίας. Με αυτή την επίθεση, τα switch αλλάζουν διαρκώς την κατάσταση των θυρών τους σε Blocking, Listening, Learning ή Forwarding και γίνονται διαρκώς εκλογές για το ποια συσκευή θα αναλάβει τον ρόλο του root με αποτέλεσμα να ξοδεύονται οι πόροι τους και να μην ανταποκρίνονται σωστά.

Για να προστατευτεί ένα σύστημα από τις παραπάνω επιθέσεις, αρκεί να διασφαλιστούν τα interface τα οποία δεν συνδέουν μεταγωγείς μεταξύ τους, με τις εντολές που φαίνονται στο Σχήμα 3.33, ώστε κατά τον εντοπισμό ενός κακόβουλου BPDU, να γίνεται αυτόματα αποκλεισμός του συγκεκριμένου Interface για να διατηρηθεί η λειτουργικότητα του δικτύου, Σχήμα 3.34.

```
Access-Switch2#
Access-Switch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Access-Switch2(config)#int e2/2
Access-Switch2(config-if)#spanning-tree bpduguard enable
Access-Switch2(config-if)#spanning-tree portfast edge
Access-Switch2(config-if)#
Access-Switch2(config-if)#
Access-Switch2(config-if)#
```

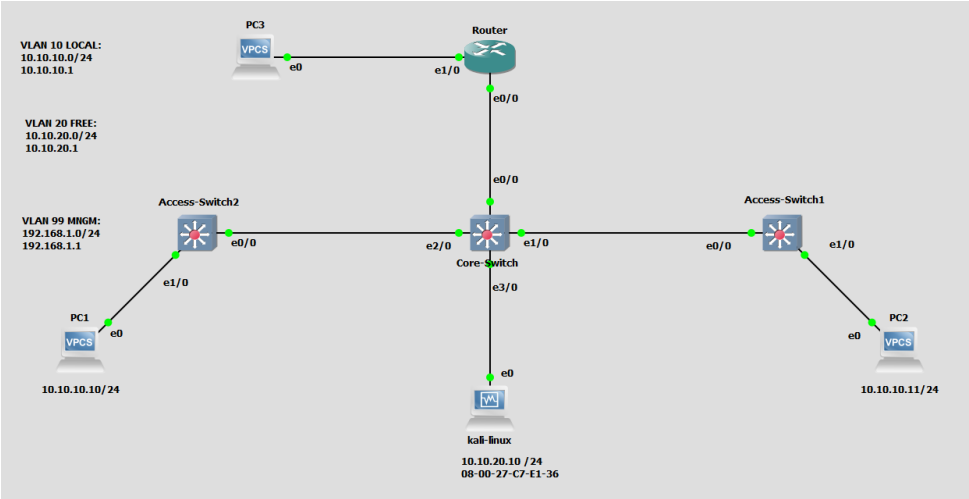
Σχήμα 3.33: Ενεργοποίηση του BPDU Guard.

```
Access-Switch2#
Sep  5 15:17:13.626: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Et2/2 with BPDU Guard enabled. Disabling port.
Access-Switch2#
Sep  5 15:17:13.626: %PM-4-ERR_DISABLE: bpduguard error detected on Et2/2, putting Et2/2 in err-disable state
Sep  5 15:17:14.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/2, changed state to down
Access-Switch2#
Sep  5 15:17:15.632: %LINK-3-UPDOWN: Interface Ethernet2/2, changed state to down
Access-Switch2#
```

Σχήμα 3.34: Αποκλεισμός Interface με το BPDU Guard.

3.8 Επιθέσεις VTP

Η τοπολογία της συγκεκριμένης προσομοίωσης απεικονίζεται στο Σχήμα 3.35.



Σχήμα 3.35: Τοπολογία VTP.

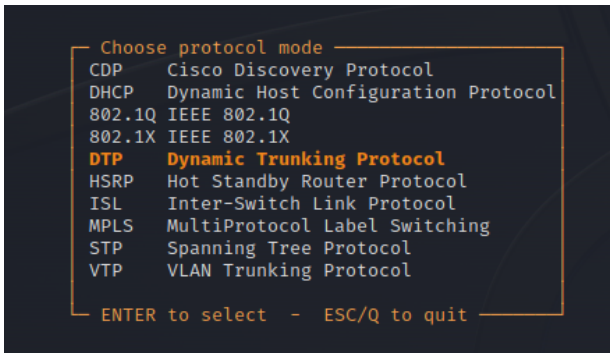
Σε αυτή την προσομοίωση, το core switch έχει το ρόλο ενός VTP (VLAN Trunk Protocol) [48] Server. Στον server υπάρχουν 2 VLAN για χρήστες και ένα διαχειριστικό (management). Εκτελώντας την εντολή show interface status, εμφανίζεται η θύρα Eth3/0 που είναι συνδεδεμένη με τον Host Kali Linux, η κατάστασή της "connected"και το VLAN στο οποίο ανήκει, VLAN 20, Σχήμα 3.36.

```
Core-Switch#show int status

Port      Name               Status       Vlan       Duplex  Speed Type
Et0/0                        connected    trunk        auto   auto unknown
Et0/1                        connected    1            auto   auto unknown
Et0/2                        connected    1            auto   auto unknown
Et0/3                        connected    1            auto   auto unknown
Et1/0                        connected    trunk        auto   auto unknown
Et1/1                        connected    1            auto   auto unknown
Et1/2                        connected    1            auto   auto unknown
Et1/3                        connected    1            auto   auto unknown
Et2/0                        connected    trunk        auto   auto unknown
Et2/1                        connected    1            auto   auto unknown
Et2/2                        connected    1            auto   auto unknown
Et2/3                        connected    1            auto   auto unknown
Et3/0                        connected    20           auto   auto unknown
Et3/1                        connected    1            auto   auto unknown
Et3/2                        connected    1            auto   auto unknown
Et3/3                        connected    1            auto   auto unknown
Core-Switch#
```

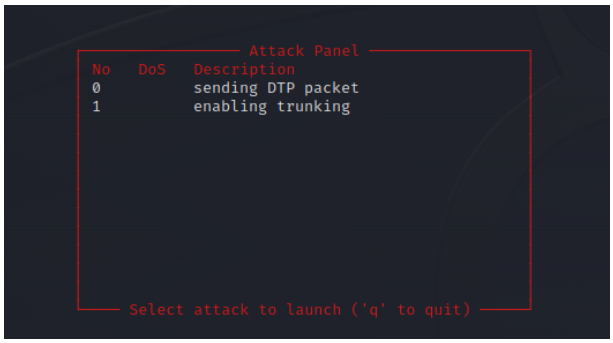
Σχήμα 3.36: Αποτέλεσμα της εντολής show interface status.

Χρησιμοποιώντας στο Yersinia το πρωτόκολλο DTP-Dynamic Trunking Protocol και την επίθεση 1: enabling trucking, Σχήμα 3.37 και 3.38, το πρόγραμμα εκμεταλλεύεται την ευπάθεια της θύρας Eth3/0,

Σχήμα 3.39, να διαπραγματεύεται την κατάστασή της και την κάνει trunk port.



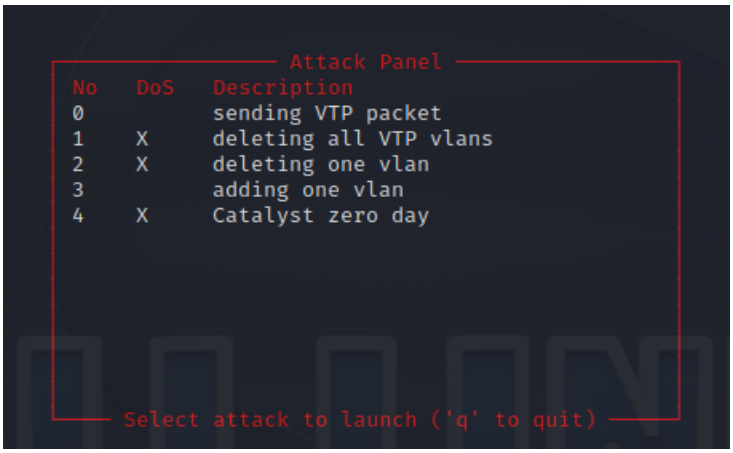
Σχήμα 3.37: Yersinia-Μενού επιλογών.



Σχήμα 3.38: Επιλογή τύπου επίθεσης.

Σχήμα 3.39: Αλλαγή στο VLAN της port Et3/0.

Οι επιθέσεις συνεχίζονται, καθώς όπως φαίνεται και στο Σχήμα 3.40, επιλέγεται η επίθεση deleting all VTP vlans.



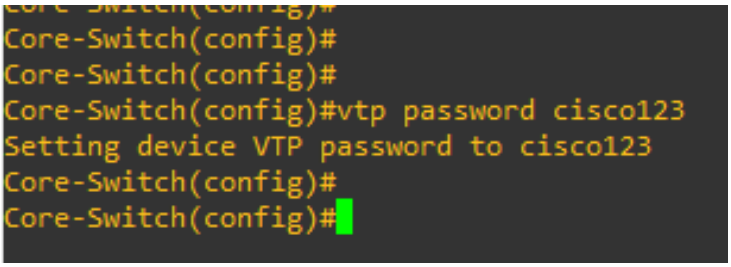
Σχήμα 3.40: Μενού επιλογής επιπλέον επιθέσεων.

Μετά από την επίθεση, όντως διαπιστώνεται με την εντολή show vlan, ότι έχουν διαγραφεί όλα τα VLAN που είχαν οριστεί, Σχήμα 3.41, και έχει απομείνει μόνο το VLAN 1 - default.

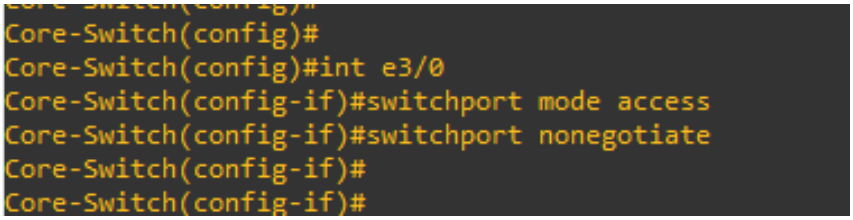
```
Core-Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/1, Et0/2, Et0/3, Et1/1
                                                Et1/2, Et1/3, Et2/1, Et2/2
                                                Et2/3, Et3/1, Et3/2, Et3/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Σχήμα 3.41: VLAN που έχουν απομείνει στο switch.

Για να αποφευχθεί μία τέτοια επίθεση, αρχικά είναι απαραίτητο να προστατευτεί ο VTP Server ορίζοντας έναν κωδικό πρόσβασης, πχ Σχήμα 3.42. Έπειτα, πρέπει να απενεργοποιηθεί το DTP από τα interface του switch τα οποία θα γίνουν access. Αυτό γίνεται εκτελώντας τις εντολές switchport mode access και έπειτα, switchport nonegotiate,Σχήμα 3.43. Με τις εντολές αυτές, η συγκεκριμένη θύρα γίνεται στατική και δεν διαπραγματεύεται την κατάστασή της ώστε να γίνει trunk, αλλά παραμένει access.



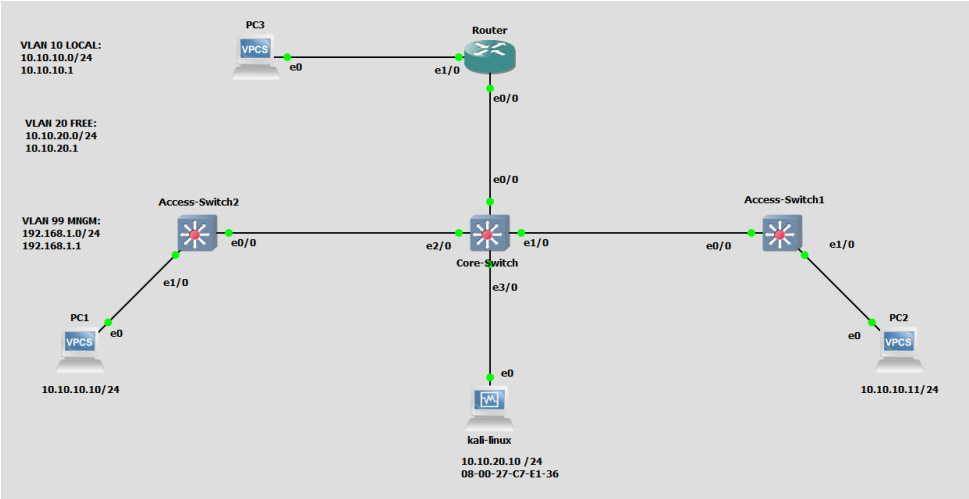
Σχήμα 3.42: Ορισμός κωδικού πρόσβασης στον VTP Server.



Σχήμα 3.43: Απενεργοποίηση του DTP.

3.9 VLAN Hopping

Η τοπολογία της συγκεκριμένης προσομοίωσης απεικονίζεται στο Σχήμα 3.44.



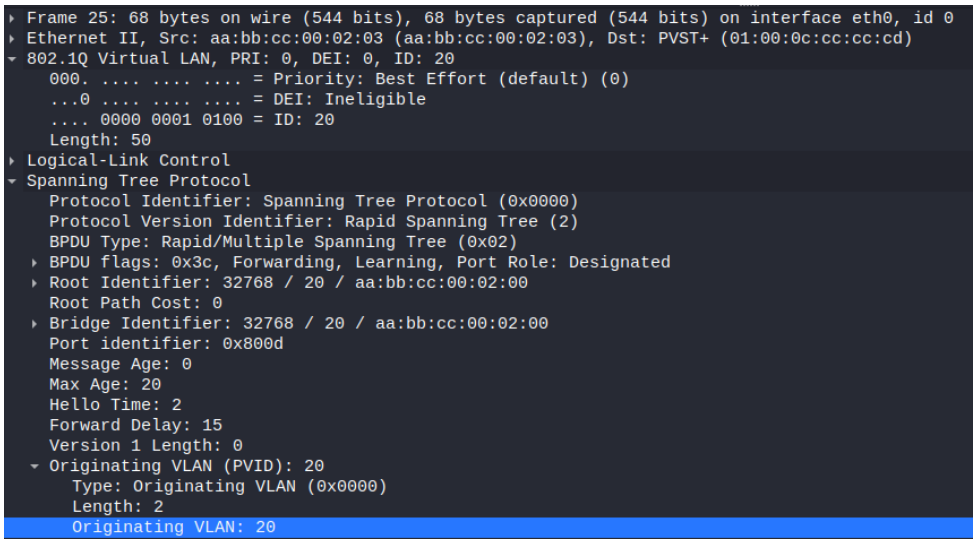
Σχήμα 3.44: Τοπολογία επίθεσης.

Για την προσομοίωση αυτής της ευπάθειας, αρχικά ακολουθείται η ίδια διαδικασία με αυτή στην επίθεση VTP, καθώς χρειάζεται να μετατραπεί σε trunk η θύρα στην οποία είναι συνδεδεμένος ο κακόβουλος χρήστης, ώστε να έχει πρόσβαση και σε άλλα vlan. Έχοντας σε trunk αυτή τη θύρα, μπορούν να μεταδοθούν περισσότερα δεδομένα αναφορικά με την κίνηση του δικτύου, όπως για παράδειγμα πακέτα STP και broadcast ICMP [49].

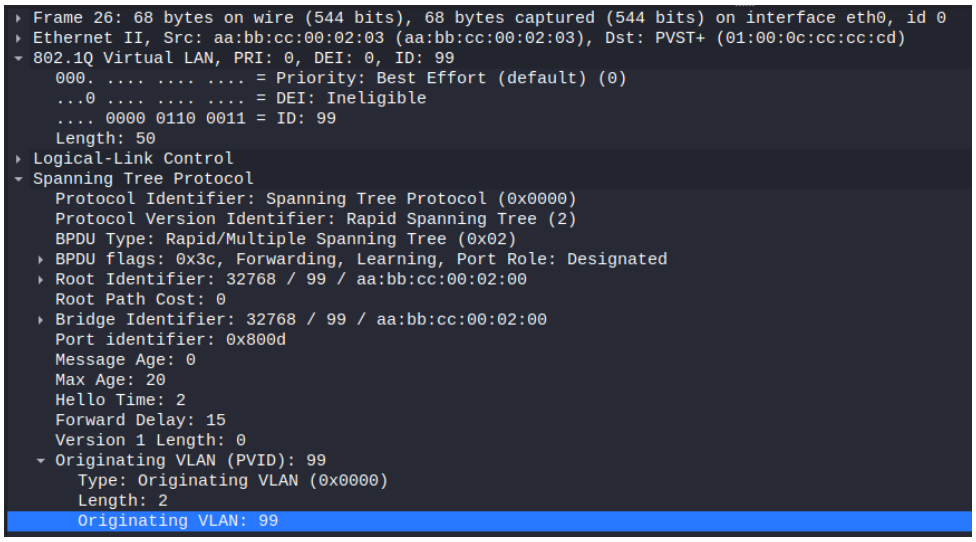
Με την χρήση του προγράμματος Wireshark, διαβάζονται τα πακέτα που μεταδίδονται. Από τα STP πακέτα, εμφανίζονται οι πληροφορίες για τα VLAN του δικτύου, Σχήμα 3.45, 3.46 και 3.47, ενώ από τα πακέτα ARP εντοπίζεται το δίκτυο, Σχήμα3.48.

```
▸ Frame 24: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface eth0, id 0
▸ Ethernet II, Src: aa:bb:cc:00:02:03 (aa:bb:cc:00:02:03), Dst: PVST+ (01:00:0c:cc:cc:cd)
▾ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0000 1010 = ID: 10
    Length: 50
▸ Logical-Link Control
▾ Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Rapid Spanning Tree (2)
    BPDU Type: Rapid/Multiple Spanning Tree (0x02)
  ▸ BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated
  ▸ Root Identifier: 32768 / 10 / aa:bb:cc:00:02:00
    Root Path Cost: 0
  ▸ Bridge Identifier: 32768 / 10 / aa:bb:cc:00:02:00
    Port identifier: 0x800d
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
    Version 1 Length: 0
  ▾ Originating VLAN (PVID): 10
      Type: Originating VLAN (0x0000)
      Length: 2
      Originating VLAN: 10
```

Σχήμα 3.45: Πληροφορίες για το VLAN 10.



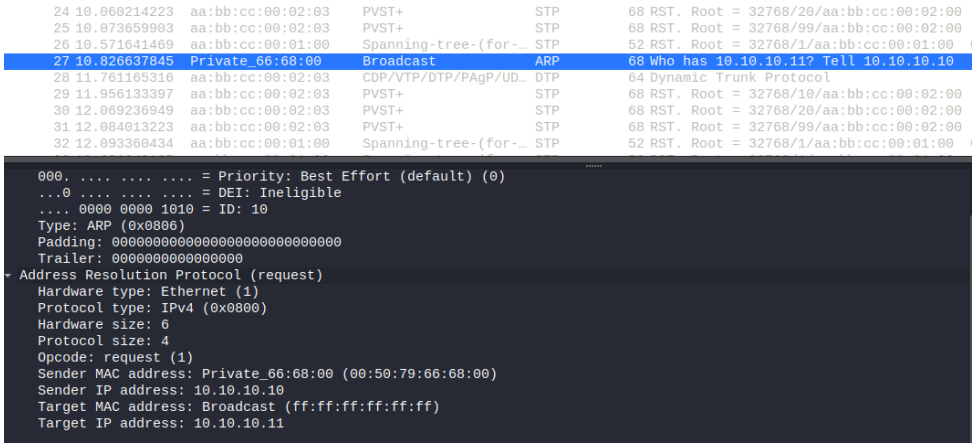
Σχήμα 3.46: Πληροφορίες για το VLAN 20.



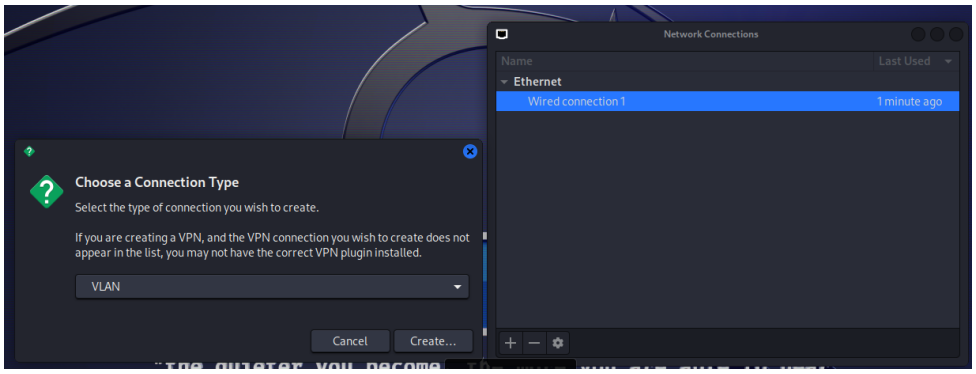
Σχήμα 3.47: Πληροφορίες για το VLAN 99.

Στο περιβάλλον του Kali Linux, πηγαίνοντας στις ρυθμίσεις δικτύων, προστίθεται μία νέα σύνδεση VLAN, Σχήμα 3.49.

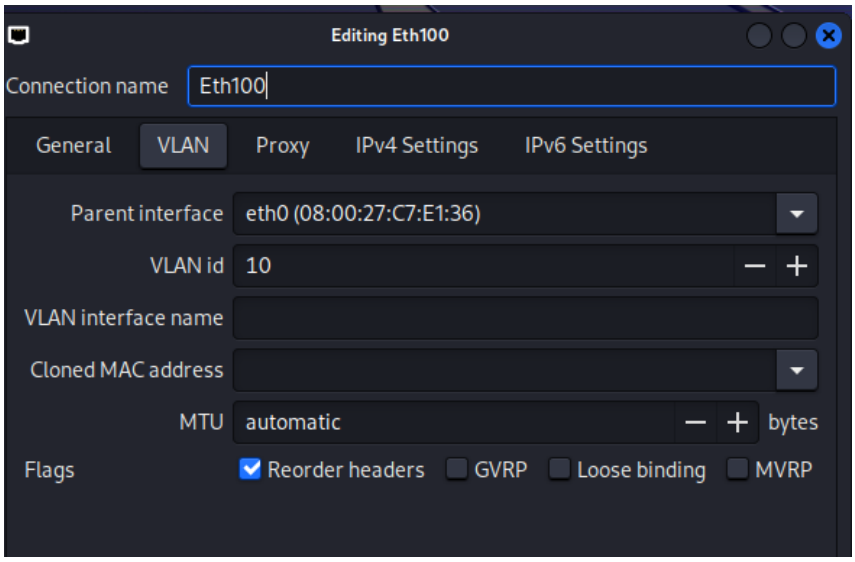
Δίνεται το όνομα Eth100 στη νέα σύνδεση, και με την επιλογή Parent interface ορίζεται το interface Eth0. Έπειτα δηλώνεται το VLAN στο οποίο θα γίνει η μεταπήδηση, στη συγκεκριμένη περίπτωση το VLAN10 και ορίζεται η IP του δικτύου που εντοπίστηκε πιο πριν, Σχήμα 3.50.



Σχήμα 3.48: Πληροφορίες για το δίκτυο.



Σχήμα 3.49: Ρύθμιση νέας σύνδεσης VLAN.



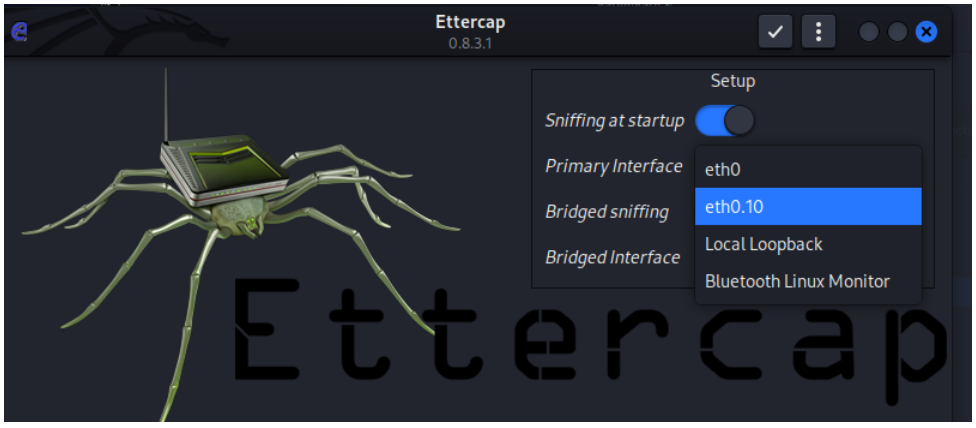
Σχήμα 3.50: Ορισμός παραμέτρων νέας σύνδεσης.

Χρησιμοποιώντας την εντολή ifconfig, επαληθεύονται τα στοιχεία των VLAN, Σχήμα 3.51.

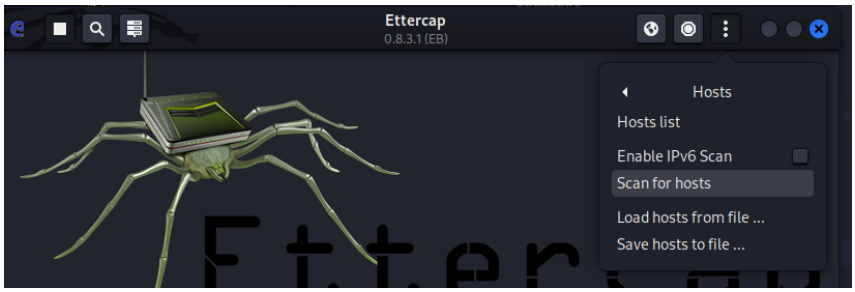
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.20.10  netmask 255.255.255.0  broadcast 10.10.20.255
        inet6 fe80::ea8e:f1b5:3b3c:e7fd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 6891  bytes 466472 (455.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 510389  bytes 30647282 (29.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0.10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.10  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::6b50:3a5:e2f:b586  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 484 (484.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11  bytes 738 (738.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 872  bytes 43904 (42.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 872  bytes 43904 (42.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Σχήμα 3.51: Αποτέλεσμα της εντολής iconfig.

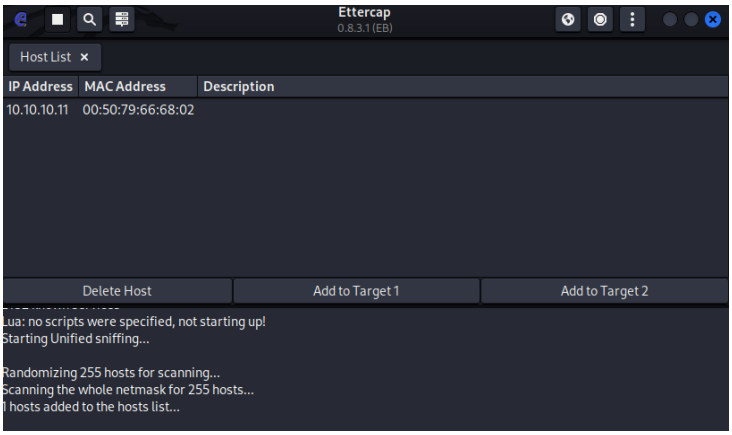
Έπειτα γίνεται η χρήση του προγράμματος Ettercap. Επιλέγεται το interface Eth0.10 (Σχήμα 3.52) και το πρόγραμμα αναζητά (Σχήμα 3.53) και εμφανίζει όλους τους host (Σχήμα 3.54).



Σχήμα 3.52: Επιλογή interface στο Ettercap.

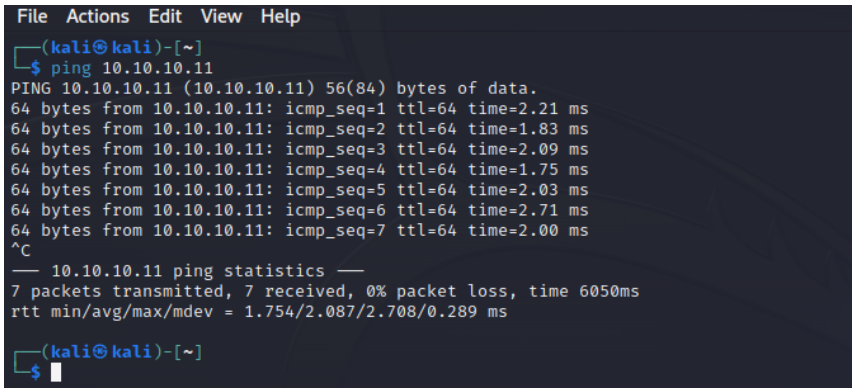


Σχήμα 3.53: Επιλογή scan for hosts στο Ettercap.



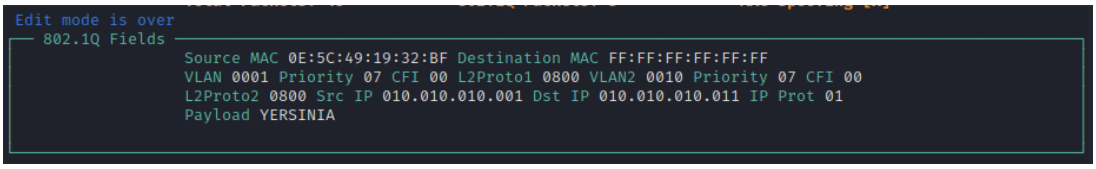
Σχήμα 3.54: Λίστα με τους διαθέσιμους host.

Για να επαληθευτεί η εισβολή στο VLAN 10, γίνεται έλεγχος επικοινωνίας με ping στην ip 10.10.10.11 του PC2, Σχήμα 3.55 .



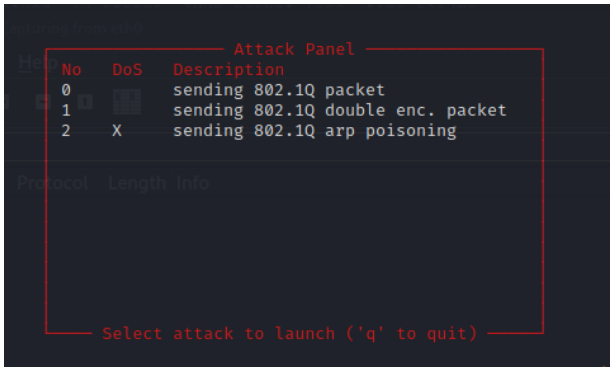
Σχήμα 3.55: Λίστα με τους διαθέσιμους host.

Αντίστοιχη διαδικασία ακολουθείται και για την επίθεση Double Encapsulated 802.1Q. Στο μενού του Yersinia, επιλέγεται το αντίστιχο πρωτόκολλο 802.1Q και έπειτα ορίζονται οι παράμετροι του πακέτου. Στην επιλογή VLAN2 τοποθετούμε το VLAN10, στις διευθύνσεις IP χρησιμοποιούμε την IP που βρήκαμε σαν διεύθυνση προορισμού καθώς και την IP του δρομολογητή αυτού του δικτύου σαν IP αποστολέα, όπως φαίνονται στο Σχήμα 3.56. Το συγκεκριμένο πακέτο χρησιμοποιεί το ICMP πρωτόκολλο.

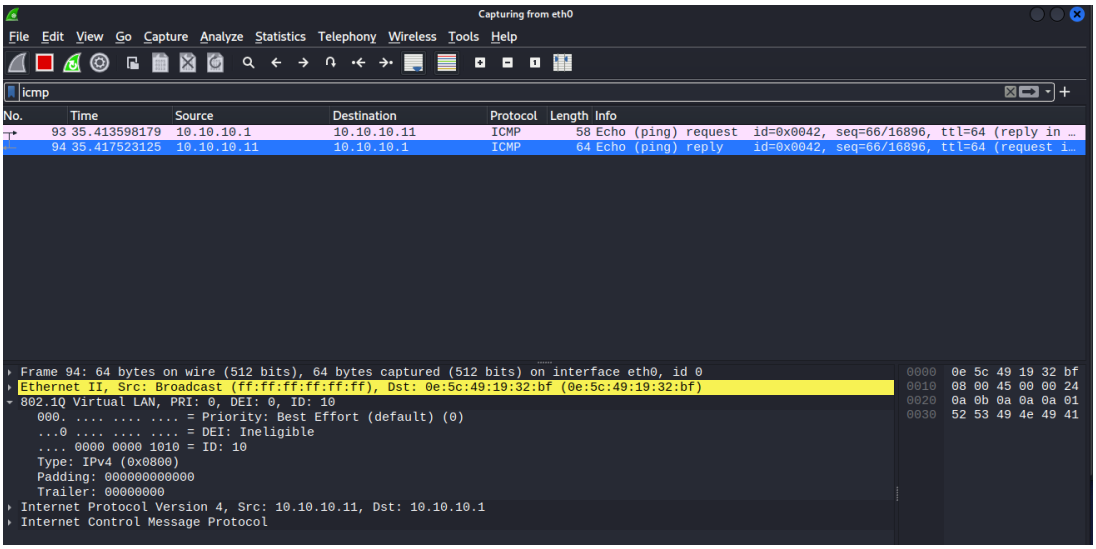


Σχήμα 3.56: Παράμετροι πακέτου ICMP.

Έπειτα, με την επιλογή της επίθεσης 2: sending 802.1Q double enc packet (Σχήμα 3.57), παρακάμπτεται το VLAN και γίνεται ping στην ip που επιλέχθηκε, όμως το πακέτο φαίνεται ότι προέρχεται από τον router (Σχήμα 3.58) και το pc απαντάει αυτόματα.



Σχήμα 3.57: Λίστα επιλογής επιθέσεων.



Σχήμα 3.58: Στιγμιότυπο πακέτου στο Wireshark.

Για την αποφυγή τέτοιου τύπου επιθέσεων, αρκεί η απενεργοποίηση του DTP όπως αναφέρθηκε και στο κεφάλαιο Επιθέσεις VTP. Επομένως, σε όσα interface είναι σε access mode γίνεται η απαραίτητη ρύθμιση που περιγράφεται παρακάτω στο Σχήμα 3.59, ώστε να μην επιτρέπεται να διαπραγματευτούν το status τους.

```
Core-Switch(config)#
Core-Switch(config)#int e3/0
Core-Switch(config-if)#switchport mode access
Core-Switch(config-if)#switchport nonegotiate
Core-Switch(config-if)#
Core-Switch(config-if)#
```

Σχήμα 3.59: Εντολές απενεργοποίησης του DTP.

3.10 Επιθέσεις σε ασύρματα δίκτυα

Τα ασύρματα δίκτυα βρίσκονται παντού γύρω μας και η ασφάλειά τους έχει εξελιχθεί με την πάροδο του χρόνου. Τα παλιότερα δίκτυα χρησιμοποιούσαν το πρωτόκολλο WEP(Wired Equivalent Privacy) το οποίο θεωρείται απαρχαιωμένο πρωτόκολλο και μπορεί να παραβιαστεί πολύ εύκολα. Η εξελιξη του είναι το πρωτόκολλο WPA(Wi-Fi Protected Access) και WPA2(Wi-Fi Protected Access II) εν συνεχεία, με το πρώτο να αρκετά ευάλωτο ακόμα σε επιθέσεις και τον διάδοχό του να έχει επικρατήσει ως το πιο κοινό και ασφαλές πρωτόκολλο επί του παρόντος. Στην κορυφή του επιπέδου ασφάλειας βρίσκεται το πιο πρόσφατο πρωτόκολλο το WPA3 [50].

Οι επιθέσεις ασύρματου δικτύου Wi-Fi περιλαμβάνουν πολλαπλές τεχνικές που εκμεταλλεύονται διάφορες ευπάθειες σε ασύρματα δίκτυα για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Μερικές από τις πιο συνηθισμένες επιθέσεις περιλαμβάμνουν ARP/MAC spoofing, Deauthentication επιθέσεις, δημιουργία Evil Twin, Brute Force επιθέσεις και αρκετές ακόμη. Χρησιμοποιώντας πλαστογράφηση της φυσικής διεύθυνσης ή της διεύθυνσης δικτύου, ο επιτηθέμενος προσποιείται έναν πραγματικό χρήστη του δικτύου με αποτέλεσμα να υποκλέψει, τροποποιήσει ή να αποκλίσει δεδομένα. Με την επίθεση κατάργησης ταυτότητας δημιουργήται μια μορφή άρνησης υπηρεσίας. Κακόβουλα πακέτα αναγκάζουν τους χρήστες που είναι συνδεδεμένοι στο δίκτυο να αποσυνδεθούν με σκοπό την επανασύνδεσή τους στο δίκτυο. Κατά την επανασύνδεση ο εισβολέας υποκλέπτει το WPA/WPA2 four-way handshake, το οποίο είναι απαραίτητο για το σπάσιμο του κωδικού πρόσβασης. Η δημιουργία ενός "Διαβολικού Διδύμου "αποτελεί μία απλή επίθεση κατά την οποία δημιουργούμε ένα κλώνο ενός σημείου πρόσβασης, με αποτέλεσμα να καταγράψουμε την κίνηση του δικτύου. Τέλος, η πιο ευθύς επίθεση είναι η Brute Force, δηλαδή επίθεση ωμής βίας. Σε αυτού του τύπου τις επιθέσεις χρησιμοποιείται συνήθως ένα αρχείο με τους πιο γνωστούς κωδικούς οι οποίοι δοκιμάζονται συστηματικά μέχρι να βρεθεί ο σωστός [51].

Για τις ανάγκες της εργασίας χρησιμοποιήθηκε ένα ιδιωτικό σημείο πρόσβασης και το λογισμικό Kali-Linux με έναν ασύρματο αντάπτορα δικτύου. Το πρωτόκολλο που χρησιμοποιήθηκε στο σημείο πρόσβασης είναι το WEP και σαν κωδικός πρόσβασης το λεκτικό "1234567890". Ένα από τα πιο δυνατά και αυτοματοποιημένα εργαλεία για επιθέσεις Wi-Fi είναι το wifite. Αποτελεί μία ολοκληρωμένη σουίτα εργαλείων που παρουσιάζονται με φιλικό τρόπο στην γραμμή εργαλειών. Ξεκινώντας, το πρόγραμμα μας εμφανίζει σε μορφή λίστας όλα τα διαθέσιμα δίκτυα της περιοχής. Επιλέγωντας τον αύξων αριθμό του δικτύου που θέλουμε να επιτεθούμε, το πρόγραμμα ξεκινάει μία σειρά επιθέσων προς το δίκτυο-στόχο. Μέσω της διαδικασίας του Deauthentication το πρόγραμμα κατάφερε και "έσπασε"τον κωδικό σε πολύ μικρό χρονικό διάστημα, Σχήμα 3.60.

Για να αποφευχθούν οι επιθέσεις και η μη εξουσιοδοτημένη πρόσβαση στα ασύρματα δίκτυα, μπορούν να εφαρμοστούν διάφορα αμυντικά μέτρα. Η βασική και πιο σημαντική άμυνα είναι η χρήση πρωτοκόλλου κρυπτογράφησης όπως το WPA2 και το WPA3. Σε συνδιασμό μαζί με έναν ισχυρό κωδικό πρόσβασης ο οποίος αποτελείται από πολλά ψηφία, νούμερα και σύμβολα δημιουργείται μια πρωταρχική "ασπίδα"απέναντι σε επιθέσεις. Προσθέτοντας την απενεργοποίηση του WPS(Wi-Fi Protected Setup) για αποτροπή Brute Force επιθέσεων, και παρακολουθώντας τακτιτά το δίκτυο για ασυνήθιστες και ύποπτες δραστηριότητες μπορούμε να έχουμε μια ολοκληρωμένη προστασία του ασύρματου δικτύου μας.

```
┌──(root㉿kali)-[~]
└─# wifite

                                   wifite2 2.6.6
                                   a wireless auditor by derv82
                                   maintained by kimocoder
                                   https://github.com/kimocoder/wifite2

[!] Conflicting processes: NetworkManager (PID 503), wpa_supplicant (PID 2899)
[!] If you have problems: kill -9 PID or re-run wifite with --kill

[+] Using wlan0 already in monitor mode

  NUM                       ESSID   CH  ENCR    PWR    WPS  CLIENT
  ---   -------------------------   --  -----   ----   ---  ------
    1       ([redacted])            6  WPA     99db    no    1
    2       ([redacted])           11  WPA     99db    no    1
    3                  MyNetwork    6  WEP    59db    no
    4       [redacted]              1  WPA-P   39db   yes    10
    5                  [redacted]   6  WPA-P   21db   yes
    6                  [redacted]  11  WPA-P   20db   yes
    7       [redacted]              8  WPA-P   20db  lock    4
    8                  [redacted]   5  WPA-P   18db   yes
    9                  [redacted]  11  WPA-P   17db   yes
   10                  [redacted]   1  WEP    16db    no
   11                  [redacted]  10  WPA-P   14db   yes
   12                  [redacted]  11  WPA-P   12db   yes
   13                  [redacted]  13  WPA-P   12db    no
   14                  [redacted]   3  WPA-P   10db   yes
   15                  [redacted]   6  WPA-P    9db   yes
   16                  [redacted]   4  WPA-P    8db   yes
[+] Select target(s) (1-16) separated by commas, dashes or all: 3

[+] (1/1) Starting attacks against C4:EA:1D:A7:44:4B (MyNetwork)
[+] attempting fake-authentication with C4:EA:1D:A7:44:4B... success
[+] MyNetwork (63db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (61db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (61db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (62db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (68db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (62db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (61db) WEP replay: 0/10000 IVs, fakeauth, Waiting for packet...
[!] Restarting aireplay after 11 seconds of no new IVs
[+] MyNetwork (66db) WEP replay: 10128/10000 IVs, fakeauth, Replaying @ 599/sec
[+] replay WEP attack successful

[+]      ESSID: MyNetwork
[+]      BSSID: C4:EA:1D:A7:44:4B
[+] Encryption: WEP
[+]    Hex Key: 12:34:56:78:90
[+] saved crack result to cracked.json (2 total)
[+] Finished attacking 1 target(s), exiting
```

Σχήμα 3.60: Επίθεση σε ασύρματο δίκτυο.

3.11 Authentication Authorization Accounting

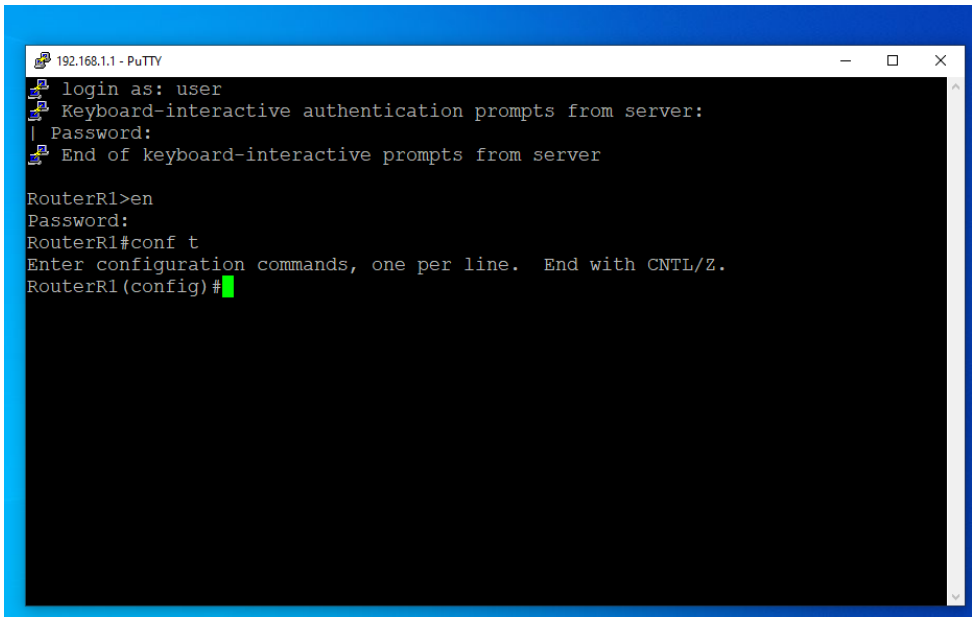
Για την αποτελεσματική άμυνα κατά των επιθέσεων στα δίκτυα επικοινωνιών, είναι απαραίτητη η εφαρμογή της AAA τεχνικής. Οι μηχανισμοί πιστοποίησης ταυτότητας, εξουσιοδότησης και ελέγχου πρόσβασης, καθορίζουν τους τομείς τους οποίους οφείλουν να προστατεύουν οι οργανισμοί. Αρχικά, για να εξασφαλιστεί η πιστοποίηση ταυτότητας, πρέπει να εφαρμοστούν τεχνικές που θα επαληθεύουν κάθε προσπάθεια πρόσβασης μέσα σε ένα σύστημα, όπως κωδικούς πρόσβασης, βιομετρικά χαρακτηριστικά, μηχανισμούς OTP (One Time Password) ή ψηφιακα πιστοποιητικά. Η εξουσιοδότηση, καθορίζει το περιεχόμενο στο οποίο μπορούν να έχουν πρόσβαση οι χρήστες και τα δικαιώματά τους, ανάλογα με τον ρόλο τους εντός του οργανισμού. Τέλος, ο έλεγχος πρόσβασης αφορά την καταγραφή δεδομένων αναφορικά με τις κινήσεις των χρηστών σε ένα σύστημα. Αυτό περιλαμβάνει την καταγραφή λεπτομερειών όπως ο χρόνος σύνδεσης, οι πόροι στους οποίους έγινε η πρόσβαση, καθώς και οι ενέργειες που πραγματοποιήθηκαν.

Για την προσομοίωση των μηχανισμών αυτών, εκτελούνται οι εντολές που φαίνονται στο Σχήμα 3.61.

```
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RouterR1
RouterR1(config)#enable secret cisco
RouterR1(config)#username local privilege 15 secret local
RouterR1(config)#username admin privilege 15 secret admin
RouterR1(config)#username user privilege 1 secret user
RouterR1(config)#ip domain-name lab.com
RouterR1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: RouterR1.lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

RouterR1(config)#aaa new-model
RouterR1(config)#aaa authentication login default local
RouterR1(config)#aaa authorization exec default local
RouterR1(config)#aaa accounting exec default none
RouterR1(config)#line vty 0 4
RouterR1(config-line)#login authentication default
RouterR1(config-line)#transport input ssh
RouterR1(config-line)#exit
RouterR1(config)#
RouterR1(config)#
*May 23 15:02:07.211: %SSH-5-ENABLED: SSH 1.99 has been enabled
RouterR1(config)#
```

Σχήμα 3.61: Ενεργοποίηση μηχανισμών προστασίας σε ένα router.

Εφόσον έχουν ενεργοποιηθεί όλοι οι μηχανισμοί ελέγχου πρόσβασης, κατά την προσπάθεια σύνδεσης ενός χρήστη, εμφανίζονται τα αντίστοιχα πεδία ταυτότητας και κωδικού πρόσβασης, όπως φαίνεται στο Σχήμα 3.62 για τον χρήστη user. Εφόσον επαληθευτούν τα στοιχεία του χρήστη, του επιτρέπεται η είσοδος. Σε περίπτωση που γινόταν προσπάθεια σύνδεσης από χρήστη που δεν διαθέτει τις απαραίτητες πληροφορίες σύνδεσης, το σύστημα θα παρέμενε ασφαλές και ακέραιο.



Σχήμα 3.62: Ενεργοποίηση μηχανισμών προστασίας σε ένα router.

3.12 Επίλογος

Στο παραπάνω κεφάλαιο, παρουσιάστηκαν οι προσομοιώσεις που εκτελέστηκαν για την παρουσίαση των επιθέσεων δικτύου, καθώς και οι μηχανισμοί που συντελούν στην προστασία και την αποφυγή των επιθέσεων από μη εξουσιοδοτημένους χρήστες.

Κεφάλαιο 4ο: Συμπεράσματα και προτάσεις βελτίωσης

4.1 Εισαγωγή

Στο κεφάλαιο αυτό, ανακεφαλαιώνονται τα ευρήματα των προσομοιώσεων, γίνεται αναφορά για το μέλλον των επιθέσεων στο επίπεδο ζεύξης, καθώς και για τους τρόπους βελτίωσης της ασφάλειας του επιπέδου.

4.2 Τεχνικές ασφάλειας και AI

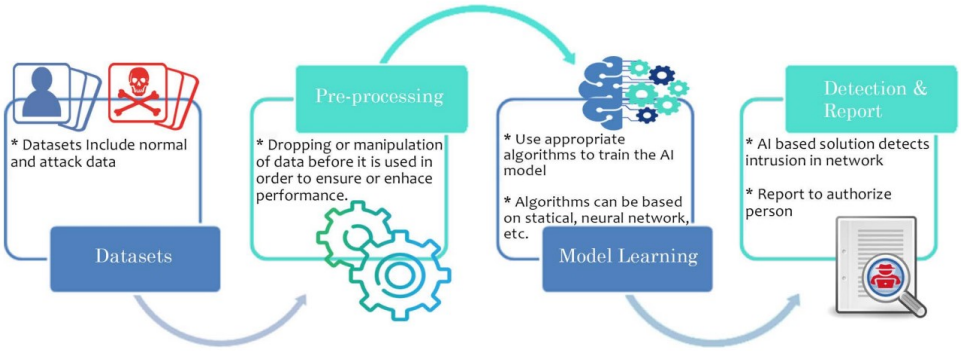
Η ασφάλεια δικτύου είναι μια σημαντική πτυχή της σύγχρονης τεχνολογίας πληροφοριών, η οποία εστιάζει στην προστασία δεδομένων, συσκευών και υποδομών από μη εξουσιοδοτημένη πρόσβαση και επιθέσεις. Καθώς οι οργανισμοί βασίζονται όλο και περισσότερο σε ψηφιακά συστήματα και διασυνδεδεμένα δίκτυα, η αξία των ισχυρών μέτρων ασφάλειας στα δίκτυα δεν μπορεί να αποφευχθεί. Από το χαμηλότερο επίπεδο του μοντέλου OSI έως και το υψηλότερο πρέπει να λαμβάνονται μέτρα και βέλτιστες πρακτικές για την ασφάλεια του δικτύου.

Έχοντας σαν κεντρικό άξονα το επίπεδο ζεύξης δεδομένων, θα έρθουμε αντιμέτωποι με επιθέσεις όπως το ARP spoofing, το MAC flooding, και το VLAN hopping. Εφαρμόζοντας τις άμυνες που αναφέραμε παραπάνω μπορούμε να αποκτήσουμε μια άμεση ασφάλεια στον εξοπλισμό μας και στο δίκτυο. Παρόλα αυτά είναι σημαντικό να προσπαθούμε να διατηρούμε και να βελτιώνουμε το επίπεδο της ασφάλειας. Χρησιμοποιώντας ισχυρές τεχνικές κρυπτογράφησης διασφαλίζουμε την ακεραιότητα των δεδομένων που μεταδίδονται μέσω των δικτύων. Ο διαχωρισμός και η τμηματοποίηση του δικτύου σε μικρότερα εικονικά δίκτυα περιορίζει πιθανές παραβιάσεις και την εξάπλωσή τους, καθώς και καθιστά το δίκτυο πιο διαχειρίσιμο.

Έπειτα είναι κρίσιμο να ασφαλίσουμε τις συσκευές που χρησιμοποιούνται στο δίκτυο. Αξιοποιώντας λογισμικό προστασίας από ιούς και τείχη προστασίας σε τερματικές συσκευές του δικτύου, τις προστατεύουμε απο κακόβουλο λογισμικό και μη εξουσιοδοτημένη πρόσβαση. Μέσω μηχανισμών φιλτραρίσματος διευθύνσεων MAC και ελέγχου ταυτότητας δίνουμε πρόσβαση μόνο σε εξουσιοδοτημένες και έμπιστες συσκευές. Σε αυτό βοηθάει και η εφαρμογή συστημάτων ανίχνευσης και πρόληψης εισβολών [52].

Όλο και περισσότεροι οργανισμοί προστατεύουν την ψηφιακή τους υποδομή με αποτέλεσμα να καθίσταται επιτακτική η ανάγκη για εξέλιξη. Η ενίσχυση της ασφάλειας του δικτύου με την Τεχνητή Νοημοσύνη αποτελεί μία καινοτόμος ιδέα. Τα συστήματα ασφαλείας που λειτουργούν με AI αξιοποιούν αλγόριθμους μηχανικής μάθησης και αναλύσεις δεδομένων για τον εντοπισμό και την αντιμετώπιση απειλών με πρωτοφανή ταχύτητα και ακρίβεια. Αυτά τα συστήματα αναλύουν συνεχώς τεράστιες ποσότητες δεδομένων κίνησης δικτύου σε πραγματικό χρόνο, εντοπίζοντας μοτίβα και ανωμαλίες που θα μπορούσαν να υποδεικνύουν πιθανές παραβιάσεις της ασφάλειας [53]. Με την αυτοματοποίηση των διαδικασιών εντοπισμού και ανταπόκρισης, η τεχνητή νοημοσύνη μειώνει σημαντικά τον χρόνο που απαιτείται για τον μετριασμό των απειλών, ελαχιστοποιώντας έτσι πιθανές παραβιάσεις και κρατώντας ακέραιη την λειτουργία του οργανισμού, Σχήμα 4.1.

Οι δυνατότητες συνεχούς μάθησης επιτρέπουν στα συστήματα που χρησιμοποιούν Τεχνητή Νοημοσύνη να προσαρμόζονται σε νέες και εξελισσόμενες απειλές, διασφαλίζοντας ότι τα μέτρα ασφαλείας παραμένουν αποτελεσματικά έναντι των πιο πρόσφατων επιθέσεων. Με την ενσωμάτωση της τεχνητής νοημοσύνης στις στρατηγικές ασφάλειας δικτύων, οι οργανισμοί μπορούν να ενισχύσουν τις αμυντικές τους ικανότητες, διασφαλίζοντας μια πιο ισχυρή και ανθεκτική στάση ασφαλείας απέναντι σε ολοένα και πιο εξελιγμένες απειλές στον κυβερνοχώρο.



Σχήμα 4.1: Σύστημα εντοπισμού επιθέσεων με χρήση AI [12].

4.3 Συμπεράσματα και η εξέλιξη των επιθέσεων

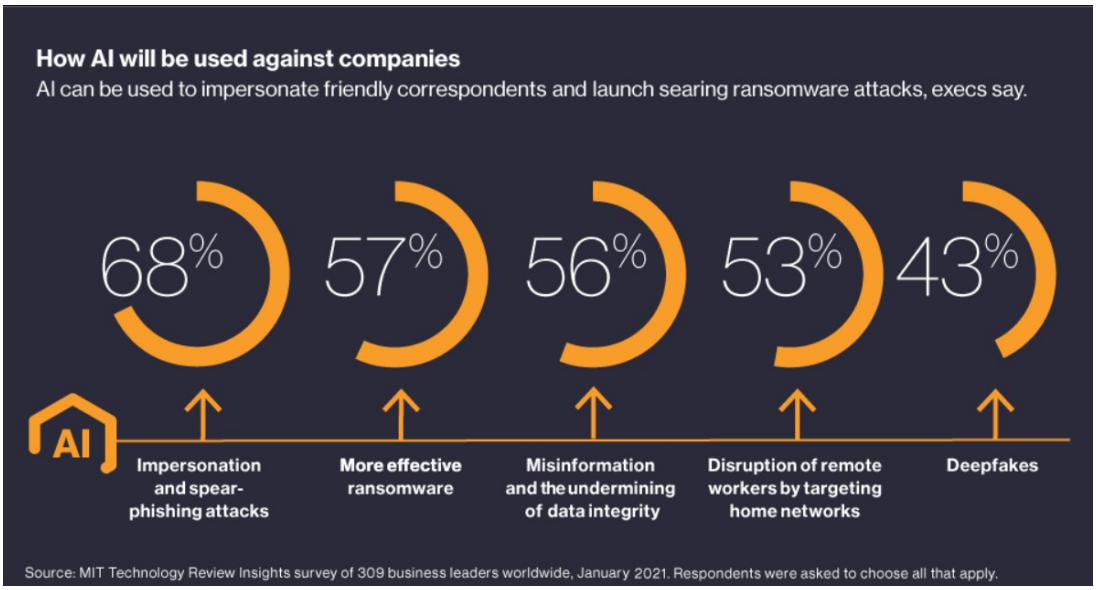
Από τις επιθέσεις που αναφέρθηκαν στο κείμενο, είναι σημαντικό να γίνει αντιληπτή η διασφάλιση κάθε πτυχής και παραμέτρου μέσα σε ένα δίκτυο. Οι επιτιθέμενοι αναζητούν διαρκώς τρωτά σημεία και ευκαιρίες για να εισβάλλουν σε ένα σύστημα. Επομένως αρκεί να εντοπιστούν όλες οι παράμετροι που καθιστούν μοναδικό κάθε επίπεδο του OSI και να εξεταστούν για τυχόν ευπάθειες ξεχωριστά.

Οι επιθέσεις που προσομοιώθηκαν στην παρούσα εργασία αποτελούν μία μορφή υλοποίησης. Στην πραγματικότητα, υπάρχουν αρκέτες δεκάδες ακόμα τρόποι οι οποίοι μπορούν να επιφέρουν ίδια αποτελέσματα. Η επιλογή των συγκεκριμένων τεχνικών έγινε χάριν εξοικονόμησης στον χρόνο εκτέλεσης, την διαθεσιμότητα του υλικολογισμικού και την γρήγορη εκμάθηση των τρόπων εκτέλεσης. Σε διαφορετική περίπτωση, στην οποία υπάρχει μία οργανωμένη ομάδα από επιτιθέμενους, τα εργαλεία και οι τεχνικές που χρησιμοποιούνται είναι πιο εξεζητημένα και τα αποτελέσματα των επιθέσεών τους, μπορεί να είναι ολέθρια για έναν οργανισμό ή ακόμη και να περάσουν απαρατήρητα από απαρχαιωμένα συστήματα εντοπισμού των επιθέσεων. Αναμένεται να εμφανιστούν περισσότερες επιθέσεις, σχεδιασμένες για να "ανακατεύουν τα δίκτυα", να προκαλούν χάος και να κάνουν τους ανθρώπους να χάσουν την εμπιστοσύνη στα συστήματα που χρησιμοποιούν. Παράγοντες όπως ο πολλαπλασιασμός των συσκευών Internet of Things (IoT), η αυξημένη συνδεσιμότητα και ο γρήγορος ρυθμός ανάπτυξης της τεχνολογικής καινοτομίας, παρέχουν περισσότερους στόχους και πιθανές ευπάθειες για εκμετάλλευση [54].

Ακόμη, η εξέλιξη της τεχνολογίας ενισχύει την σφοδρότητα των επιθέσεων στο επίπεδο ζεύξης δεδομένων, καθώς τα μοντέλα τεχνητής νοημοσύνης και αυτοματισμών μπορούν να δημιουργήσουν κώδικα για να εξυπηρετήσουν σχεδόν οποιαδήποτε ανάγκη. Η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την αυτοματοποίηση της ανακάλυψης τρωτών σημείων σε πρωτόκολλα και συσκευές δικτύου, κα-

θώς μαθαίνοντας από προηγούμενες επιθέσεις, μπορούν να δημιουργήσουν νέες στρατηγικές επίθεσης, να προσαρμόζονται και να εξελίσσονται για να παρακάμπτουν τα μέτρα ασφαλείας. Ακόμη, η τεχνητή νοημοσύνη μπορεί να χρησιμοποιηθεί για την ανακάλυψη και την εκμετάλλευση τρωτών σημείων zero-day.

Επιπλέον, η AI μπορεί να βελτιώσει τον συντονισμό και την αποτελεσματικότητα των botnet [55] που λειτουργούν στο επίπεδο ζεύξης δεδομένων. Οι αλγόριθμοι μηχανικής μάθησης μπορούν να βελτιστοποιήσουν την κατανομή των εντολών και των πόρων μεταξύ των παραβιασμένων συσκευών, καθιστώντας τα botnet πιο ανθεκτικά στις προσπάθειες κατάργησης και ικανά να εξαπολύουν επιθέσεις μεγάλης κλίμακας. Τέλος, τα συστήματα που λειτουργούν με AI μπορούν να ενισχύσουν τις επιθέσεις phishing [56] και social engineering [57], δημιουργώντας πιο πειστικά και εξατομικευμένα μηνύματα προσαρμοσμένα στα χαρακτηριστικά των μεμονωμένων στόχων, Σχήμα 4.2. Οι αλγόριθμοι μηχανικής μάθησης μπορούν να αναλύσουν τεράστιες ποσότητες δεδομένων που έχουν αφαιρεθεί από τα μέσα κοινωνικής δικτύωσης και άλλες πηγές για να δημιουργήσουν εξαιρετικά στοχευμένες παγίδες.



Σχήμα 4.2: Τύποι επιθέσεων που αναμένονται, κάνοντας χρήση της AI [13].

4.4 Επίλογος

Σε αυτό το κεφάλαιο έγινε λόγος για τις κύριες και βέλτιστες τεχνικές ασφάλειας, τους τρόπους βελτίωσής τους, καθώς και για την εξέλιξη των επιθέσεων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] "Executive summary — NIST SP 1800-25 documentation." `https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html`. Accessed Mar. 30, 2023.

[2] F. Aloul, A. Shaikh, and A. Chaudhry, "Cyber attacks: Prevention and proactive responses," *Procedia Computer Science*, vol. 83, pp. 1419–1426, 2016.

[3] M. S. J. Solaija, H. Salman, and H. Arslan, "Towards a unified framework for physical layer security in 5g and beyond networks," *IEEE Open Journal of Vehicular Technology*, vol. 3, pp. 321–343, 2022.

[4] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-world man-in-the-middle (mitm) attack implementation using open source tools for instructional use," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, pp. 0192–0197, 2018.

[5] D. Mudzingwa and R. Agrawal, "A study of methodologies used in intrusion detection and prevention systems (idps)," in *2012 Proceedings of IEEE Southeastcon*, pp. 1–6, 2012.

[6] J. Liang and Y. Kim, "Evolution of firewalls: Toward securer network using next generation firewall," in *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0752–0759, 2022.

[7] "Syn flood." Huawei Support, 2024.

[8] M. A. Jonas, M. S. Hossain, R. Islam, H. S. Narman, and M. Atiquzzaman, "An intelligent system for preventing ssl stripping-based session hijacking attacks," in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, pp. 1–6, 2019.

[9] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018.

[10] "A comparative analysis of symmetric algorithms in cloud computing: A survey," *International Journal of Computer Applications*, vol. 182, pp. 7–16, April 2019.

[11] C. Rohith and G. Kaur, "A comprehensive study on malware detection and prevention techniques used by anti-virus," in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, pp. 429–434, 2021.

[12] S. Rizvi, M. Scanlon, J. Mcgibney, and J. Sheppard, "Application of artificial intelligence to network forensics: Survey, challenges and future directions," *IEEE Access*, vol. 10, pp. 110362–110384, 2022.

[13] "Preparing for ai-enabled cyberattacks," 2021.

[14] V. D. Sumit Kumar, Sumit Dalal, "The osi model: Overview on the seven layers of computer networks," *International Journal of Computer Science and Information Technology Research*, vol. 2, no. Issue 3, pp. 461–466, 2014.

[15] H. Zimmermann, "Osi reference model - the iso model of architecture for open systems interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425–432, 1980.

[16] M. V. Salvi and M. P. Bapat, "Mode of data flow in the osi model," *International Journal of Innovations in Engineering Research and Technology*, vol. 2, no. 3, pp. 1–7, 2015.

[17] A. M. Shaaban, O. Jung, and C. Schmittner, "A proposed x.800-based security architecture framework for unmanned aircraft system," in *IDIMT-2022: Digitalization of Society, Business and Management in a Pandemic: 30th Interdisciplinary Information Management Talks* (G. Chroust, P. Doucek, and V. Oškrdal, eds.), no. 51. Universität in Schriftenreihe Informatik, (Linz), pp. 389–398, Trauner Verlag, 2022.

[18] P. V. Jasud, "The osi model: Overview on the seven layers of computer networks," *International Journal for Innovative Research in Science & Technology*, vol. 4, p. 116, August 2017.

[19] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.

[20] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, dec 2012.

[21] W. Fumy and J. Sauerbrey, eds., *Enterprise Security: IT Security Solutions – Concepts, Practical Experiences, Technologies*. 1st ed., 2014.

[22] G. Bora, S. Bora, S. Singh, and S. M. Arsalan, "Osi reference model: An overview," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 7, p. 214, January 2014. Page 214.

[23] A. K. Singh, "Comprehensive study of error detection by cyclic redundancy check," in *2017 2nd International Conference for Convergence in Technology (I2CT)*, pp. 556–558, 2017.

[24] G. M. Marro, "Attacks at the data link layer," thesis, University of California, Davis, 1996.

[25] T. O'Connor, "Detecting and responding to data link layer attacks." GIAC (GCIA) Gold Certification, 2010. Author: TJ O'Connor, terrence.oconnor@usma.edu, Advisor: Joel Esler, Accepted: October 13, 2010.

[26] M. Alani, "Osi model," in *Guide to OSI and TCP/IP Models*, SpringerBriefs in Computer Science, Springer, 2014.

[27] S. Pandey, "Modern network security: Issues and challenges," *Technology*, vol. 3, p. 4351, May 2011. Mr. Reza Beshghi, Iran, and Pin-227105.

[28] G. Marin, "Network security basics," *IEEE Security Privacy*, vol. 3, no. 6, pp. 68–72, 2005.

[29] S. Joshna and N. Nishanth, "A study on different attacks on transport, network and data link layer in tcp/ip," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, June 2017.

[30] K. Treseangrat, S. S. Kolahi, and B. Sarrafpour, "Analysis of udp ddos cyber flood attack and defense mechanisms on windows server 2012 and linux ubuntu 13," in *2015 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, 2015.

[31] W. Emmons and A. Chandler, "Osi session layer: Services and protocols," *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1397–1400, 1983.

[32] P. Boait, G. Neville, R. Norris, M. Pickman, M. Tolhurst, and J. Walmsley, "Presentation layer — layer 6," in *Open Systems Interconnection* (M. Tolhurst, ed.), Macmillan Computer Science Series, Palgrave, 1988.

[33] R. Mishra and P. Bhanodiya, "A review on steganography and cryptography," in *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 119–122, 2015.

[34] M. Hosseini, D. T. Ahmed, S. Shirmohammadi, and N. D. Georganas, "A survey of application-layer multicast protocols," *IEEE Communications Surveys Tutorials*, vol. 9, no. 3, pp. 58–74, 2007.

[35] Graphical Network Simulator-3, "Graphical Network Simulator-3 (GNS3)." `https://www.gns3.com/`. 2024.

[36] M. Tigner, H. Wimmer, and C. M. Rebman, "Analysis of kali linux penetration tools: A survey of hacking tools," in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, pp. 1–6, 2021.

[37] Cisco Networking Academy, "Cisco Networking Academy (NetAcad)." `http://www.netacad.com`. 2024.

[38] M. Data, "The defense against arp spoofing attack using semi-static arp cache table," in *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, pp. 206–210, 2018.

[39] Cisco Networking Academy, *Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7)*. Cisco Press, 2020.

[40] A. Johnson, *31 Days Before Your CCNA Routing & Switching Exam: A Day-By-Day Review Guide for the ICND1/CCENT (100-105), ICND2 (200-105), and CCNA (200-125) Certification Exams*. Cisco Press, 2017.

[41] S. S. Ray, K. Das, and S. Ghosh, "A ram-based mac table with two-tier security at layer 2," *IETE Journal of Research*, vol. 62, no. 4, pp. 435–445, 2016.

[42] Y. Tzang, H. Chang, and C. Tzang, "Enhancing the performance and security against media-access-control table overflow vulnerability attacks," *Security and Communication Networks*, vol. 8, pp. 1780–1793, 2015.

[43] Cisco Systems, Inc., *Configuring the MAC Address Table, Cisco Nexus 1000V Layer 2 Switching Configuration Guide, Release 4.2(1)SV2(1.1)*. Cisco Systems, San Jose, CA.

[44] Cisco Networking Academy, *Connecting Networks v6 Companion Guide*. Cisco Press, 2017.

[45] W. Odom and S. Wilkins, *CCNA Routing and Switching 200-125 Official Cert Guide and Network Simulator Library*. Cisco Press, 2017.

[46] R. Nastase, *Cisco CCNA Command Guide (Volume 2)*. CreateSpace Independent Publishing Platform, 2018.

[47] W. Odom and S. Wilkins, *CCNA Routing and Switching ICND2 200-105 Pearson uCertify Course, Network Simulator, and Textbook Academic Edition Bundle*. Cisco Press, 2017.

[48] W. Odom, *CCNA 200-301 Official Cert Guide, Volume 2*. Cisco Press, 2020.

[49] A. Johnson and Cisco Networking Academy, *Enterprise Networking, Security, and Automation Labs and Study Guide (CCNAv7)*. Cisco Press, 2020.

[50] M. Alhamry and A. Alomary, "Exploring wi-fi wpa2-psk protocol weaknesses," in *2022 International Conference on Data Analytics for Business and Industry (ICDABI)*, pp. 190–195, 2022.

[51] T. Radivilova and H. A. Hassan, "Test for penetration in wi-fi network: Attacks on wpa2-psk and wpa2-enterprise," in *2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, pp. 1–4, 2017.

[52] T. AlMasri, M. A. Snober, and Q. A. Al-Haija, "Idps-sdn-ml: An intrusion detection and prevention system using software-defined networks and machine learning," in *2022 1st International Conference on Smart Technology, Applied Informatics, and Engineering (APICS)*, pp. 133–137, 2022.

[53] R. Madala, N. Vijayakumar, N. N, S. Verma, S. D. Chandvekar, and D. P. Singh, "Automated ai research on cyber attack prediction and security design," in *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 6, pp. 1391–1395, 2023.

[54] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in iot networks," in *2019 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, 2019.

[55] R. M. Baazeem, "Cybersecurity: Botnet threat detection across the seven-layer iso-osi model using machine learning techniques," *COMPUTING AND INFORMATICS*, vol. 42, no. 5, pp. 1060–1090, 2024.

[56] A. Basit, M. Zafar, X. Liu, and et al., "A comprehensive survey of ai-enabled phishing attacks detection techniques," *Telecommunication Systems*, vol. 76, pp. 139–154, 2021.

[57] N. Mashtalyar, U. Ntaganzwa, T. Santos, S. Hakak, and S. Ray, "Social engineering attacks: Recent advances and challenges," in *HCI for Cybersecurity, Privacy and Trust. HCII 2021* (A. Moallem, ed.), vol. 12788 of *Lecture Notes in Computer Science*, Springer, Cham, 2021.

[58] D. Kriz, "Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity," in *2011 Second Worldwide Cybersecurity Summit (WCS)*, pp. 1–3, 2011.

[59] A. Atlasis, “Attacking ipv6 implementation using fragmentation,” *Centre for Strategic Cyberspace + Security Science*, 2013.

[60] S. Mayukha and R. Vadivel, “Various possible attacks and mitigations of the osi model layers through pentesting – an overview,” in *New Frontiers in Communication and Intelligent Systems* (R. Srivastava and A. K. S. Pundir, eds.), Computing & Intelligent Systems, pp. 799–809, SCRS, India, 2021.