ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Ανάλυση και υλοποίηση Penetration Testing: Σενάριο ιστοσελίδας φτιαγμένη με wordpress»

Του φοιτητή
Κωνσταντίνου Μποτόζη
Αρ. Μητρώου: 185242

Επιβλέπων
Αμανατιάδης Δημήτριος

Σεπτέμβριος 2025

Τίτλος Π.Ε. «Ανάλυση και υλοποίηση Penetration Testing: Σενάριο ιστοσελίδας φτιαγμένη με wordpress»

Κωδικός Π.Ε. 25113

Ονοματεπώνυμο φοιτητή Μποτόζης Κωνσταντίνος

Ονοματεπώνυμο εισηγητή Αμανατιάδης Δημήτριος

Ημερομηνία ανάληψης Π.Ε. 09-02-2025

Ημερομηνία περάτωσης Π.Ε. 11-09-2025

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.

Πρόλογος

Ο προσανατολισμός της παρούσας πτυχιακής εργασίας σε ένα σενάριο επίθεσης σε ιστοσελίδα WordPress επιλέχθηκε με γνώμονα τα προσωπικά μου ενδιαφέροντα στον τομέα των δικτύων και της κυβερνοασφάλειας και ιδιαίτερα στο πεδίο του offensive security. Η συγκεκριμένη προσέγγιση αντιμετώπισης ζητημάτων ασφάλειας, που εστιάζει στην ενεργή αναζήτηση και εκμετάλλευση αδυναμιών πριν το πράξει ένας κακόβουλος χρήστης, προσφέρει μια πρακτική και άμεσα εφαρμόσιμη οπτική στη θωράκιση των συστημάτων. Το WordPress, ως ένα από τα πιο δημοφιλή Συστήματα Διαχείρισης Περιεχομένου παγκοσμίως, αποτελεί συχνό στόχο επιθέσεων λόγω της μεγάλης χρήσης του και της πληθώρας προσθηκών και θεμάτων τρίτων κατασκευαστών, τα οποία συχνά εισάγουν κενά ασφαλείας. Μέσα από την ανάπτυξη ενός ελεγχόμενου σεναρίου penetration testing, η εργασία αποσκοπεί όχι μόνο στην κατανόηση των τεχνικών σταδίων μιας τέτοιας διαδικασίας, αλλά και στην ανάδειξη της αξίας του επιθετικού ελέγχου ως εργαλείου πρόληψης. Με αυτόν τον τρόπο, η επιλογή του θέματος συνδυάζει την προσωπική ενασχόληση με τα δίκτυα και την ασφάλεια, με ένα πρακτικό αντικείμενο υψηλής συνάφειας στον σύγχρονο κυβερνοχώρο.

Περίληψη

Η παρούσα πτυχιακή εργασία επικεντρώνεται στη διεξαγωγή ενός σεναρίου penetration testing σε μια δημοφιλή πλατφόρμα WordPress, με στόχο την αξιολόγηση της ασφάλειάς της. Αρχικά, παρουσιάζεται ιστορικά η εξέλιξη των δικτύων, ώστε να αναδειχθεί το πώς διαμορφώθηκαν οι σημερινές αρχιτεκτονικές και τεχνολογίες επικοινωνίας. Στη συνέχεια, αναλύονται οι βασικές έννοιες που διέπουν τη λειτουργία των δικτύων, προσφέροντας το απαραίτητο υπόβαθρο κατανόησης για τη μελέτη συστημάτων πληροφορικής. Έπειτα, η εργασία εστιάζει στις θεμελιώδεις αρχές της κυβερνοασφάλειας, με στόχο την κατανόηση των προκλήσεων που προκύπτουν στη σύγχρονη ψηφιακή εποχή, ενώ παράλληλα παρουσιάζονται οι συχνότερες μορφές κυβερνοεπιθέσεων που απειλούν οργανισμούς και χρήστες. Επιπλέον, εξετάζεται διεξοδικά η έννοια του penetration testing και αναλύονται τα στάδια που το απαρτίζουν, ώστε να καταστεί σαφής η μεθοδολογία που ακολουθείται σε μια ολοκληρωμένη αξιολόγηση ασφάλειας πληροφοριακών συστημάτων. Στη συνέχεια, σχεδιάζεται και υλοποιείται, σε ελεγχόμενο εργαστηριακό περιβάλλον, ένα σενάριο penetration testing σύμφωνα με καθιερωμένες μεθοδολογίες, εστιάζοντας στα στάδια του reconnaissance, της ανίχνευσης ευπαθειών και της θεωρητικής προσέγγισης τεχνικών exploitation. Η εργασία καταγράφει τις πιθανές περιοχές αδυναμίας και εξετάζει, σε θεωρητικό επίπεδο, τρόπους με τους οποίους θα μπορούσαν να αξιοποιηθούν από έναν επιτιθέμενο. Τέλος, τα συμπεράσματα υπογραμμίζουν τη σημασία της πρόληψης μέσω σωστής παραμετροποίησης και τακτικών ενημερώσεων στα Συστήματα Διαχείρισης Περιεχομένου, καθώς και τον ρόλο του ηθικού hacking ως εργαλείου ενίσχυσης της κυβερνοασφάλειας.

«Ανάλυση και υλοποίηση Penetration Testing: Σενάριο ιστοσελίδας φτιαγμένη με wordpress»

Analysis and implementation of Penetration Testing: Website built with WordPress

«Κωνσταντίνος Μποτόζης»

Botozis Konstantinos

Abstract

This thesis focuses on conducting a penetration testing scenario on a popular WordPress platform, with the aim of assessing its security. Initially, the evolution of networks is presented historically, in order to highlight how today's communication architectures and technologies were formed. Subsequently, the basic concepts governing the operation of networks are analyzed, providing the necessary background of understanding for the study of information systems. Then, the work focuses on the fundamental principles of cybersecurity, with the aim of understanding the challenges that arise in the modern digital era, while at the same time presenting the most frequent forms of cyberattacks that threaten organizations and users. In addition, the concept of penetration testing is examined in detail and the stages that comprise it are analyzed, in order to clarify the methodology followed in a comprehensive information systems security assessment. Then, a test scenario is designed and implemented, in a controlled laboratory environment, according to established methodologies, focusing on the stages of reconnaissance, vulnerability detection and theoretical approach to exploitation techniques. The work lists the possible areas of weakness and examines, at a theoretical level, ways in which they could be exploited by an attacker. Finally, the conclusions highlight the importance of prevention through proper configuration and regular updates to Content Management Systems, as well as the role of ethical hacking as a tool to enhance cybersecurity.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AI	Artificial Intelligence
ANSI	American National Standards Institute
API	Application Programming Interface
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASCII	American Standard Code for Information Interchange
BBN	Bolt, Beranek and Newman
BGP	Border Gateway Protocol
CIA	Confidentiality, Integrity, Availability
CLI	Command Line Interface
CMS	Content Management System
CNAME	Canonical Name
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNET	Computer Science Network
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Configuration Protocol
dig	Domain Information Groper
DNS	Domain Name System
DoS	Denial of Service
DRP	Disaster Recovery Plans
ENIAC	Electronic Numerical Integrator and Computer
EUnet	European UNIX Network
FTP	File Transfer Protocol
FTTH	Fiber To The Home
GDPR	General Data Protection Regulation

HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP over TLS/SSL
IBM	International Business Machines Corporation
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systems
IMAP	Internet Message Access Protocol
IMP	Interface Message Processor
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
JANET	Joint Academic NETwork
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LFI	Local File Inclusion
LTE	Long-Term Evolution
MAC	Media Access Control
Mbps	Mega Bytes Per Second
MFA	Multi-Factor Authentication
MILNET	Military Network
NCP	Network Control Protocol
NCSA	National Center for Supercomputing Applications
NIST	National Institute of Standards and Technology
NSFNET	National Science Foundation Network
OSINT	Open Source Intelligence
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OWASP	Open Worldwide Application Security Project
PCI-DSS	Payment Card Industry Data Security Standard
PoC	Proofs of Concept
PPP	Point-to-Point Protocol
RBAC	Role-Based Access Control

RFI	Remote File Inclusion
ROI	Return Of Investment
SCP	Secure Copy Protocol
SFTP	SSH File Transfer Protocol
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SRI	Stanford Research Institute
SSH	Secure Shell
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
UCLA	University of California, Los Angeles
UCSB	University of California, Santa Barbara
UDP	User Datagram Protocol
UNIVAC	Universal Automatic Computer
UPS	Uninterruptible Power Supplies
URL	Uniform Resource Locator
VDSL	Very High Bitrate DSL
VPN	Virtual Private Networks
WAF	Web Application Firewall
WWW	World Wide Web
XML	Extensible Markup Language
XSS	Cross-Site Scripting
ZTA	Zero Trust Architecture

Κεφάλαιο 1ο: Ιστορική Αναδρομή Δικτύων

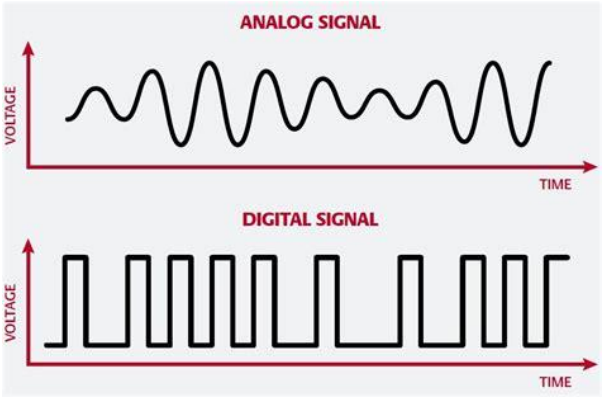
1.1 Εισαγωγή

Η εξέλιξη των δικτύων και του Διαδικτύου αποτελεί ένα από τα πλέον σημαντικά τεχνολογικά επιτεύγματα της σύγχρονης εποχής. Από τα πρώτα πειράματα στην τηλεπικοινωνία μέχρι την καθιέρωση ενός παγκόσμιου και ενοποιημένου ψηφιακού ιστού, η πορεία αυτή χαρακτηρίζεται από καινοτομίες, στρατηγικές επενδύσεις και βαθιές κοινωνικοοικονομικές επιδράσεις. Το παρόν κεφάλαιο αποσκοπεί στην αναλυτική παρουσίαση της ιστορικής διαδρομής των δικτύων, με έμφαση στη σταδιακή διαμόρφωση του Διαδικτύου.

1.2 Αναλογικά και Ψηφιακά Σήματα και Συστήματα

Η εξέλιξη των δικτύων στηρίζεται στην ανθρώπινη ανάγκη για επικοινωνία σε απόσταση. Η πρώτη πραγματική τεχνολογική ανατροπή ήρθε με την εφεύρεση του τηλέγραφου, στα μέσα του 19ου αιώνα. Ο ηλεκτρικός τηλέγραφος μετέδιδε σήματα μέσω καλωδίων με τη μορφή παλμών υψηλής ή χαμηλής τάσης, οι οποίοι κωδικοποιούσαν χαρακτήρες βάσει του κώδικα Morse. Η διαδικασία αυτή, αν και πρωτόγονη, θέτει τα πρώτα θεμέλια της ψηφιακής επικοινωνίας, καθώς βασίζεται στη δυαδική λογική, παλμός ή απουσία παλμού, δηλαδή "1" ή "0".

Η πληροφορία δεν μεταδιδόταν συνεχώς, όπως στα αναλογικά σήματα, αλλά μέσω διακριτών παλμών (σύμβολα), που σηματοδοτούν συγκεκριμένες εντολές. Έτσι, ο τηλέγραφος θεωρείται πρόδρομος της έννοιας των ψηφιακών σημάτων, παρά το ότι δεν χρησιμοποιούσε ακόμα σύγχρονα πρωτόκολλα ή ηλεκτρονικούς μετατροπείς.



Εικόνα 1.1: Αναλογικά και Ψηφιακά Σήματα [4]

Με την εφεύρεση του τηλεφώνου από τον Alexander Graham Bell το 1876, το επίκεντρο της επικοινωνίας μετακινήθηκε στην αναλογική μετάδοση φωνής μέσω συνεχών ηλεκτρικών κυμάτων. Η ανθρώπινη φωνή μετασχηματιζόταν σε ηλεκτρικό σήμα μεταβαλλόμενης έντασης και συχνότητας, γεγονός που επέτρεψε τη φυσική συνομιλία σε πραγματικό χρόνο. Ωστόσο, το τηλεφωνικό δίκτυο που βασίστηκε σε αναλογικά κυκλώματα είχε περιορισμούς σε εύρος, ποιότητα και ευστάθεια. [1]

Στη δεκαετία του 1940, εμφανίστηκαν οι πρώτοι ηλεκτρονικοί υπολογιστές, αρχικά ως τεράστιες μηχανές για στρατιωτικούς και ερευνητικούς σκοπούς. Ο ENIAC (Electronic Numerical Integrator and

Computer) συγκεκριμένα το 1945, είναι ο πρώτος γενικής χρήσης υπολογιστής, με λειτουργία βάσει δυαδικής αριθμητικής και λογικών κυκλωμάτων, χρησιμοποιώντας χιλιάδες λυχνίες κενού.

Εικόνα 1.2: ENIAC [3]

Σύντομα, μηχανές όπως ο UNIVAC (Universal Automatic Computer) το 1951 και ο IBM (International Business Machines Corporation) 701 υιοθετήθηκαν για εμπορικές και κυβερνητικές εφαρμογές. Αυτοί οι υπολογιστές λειτουργούσαν επεξεργάζοντας και μεταδίδοντας ψηφιακά δεδομένα με τη μορφή bit, μέσω ειδικών διαύλων επικοινωνίας. [2]

Η ανάγκη για διαμοιρασμό πόρων και απομακρυσμένη πρόσβαση σε δεδομένα, σε συνδυασμό με το υψηλό κόστος των υπολογιστών, δημιούργησε το ερώτημα της διασύνδεσης διαφορετικών συστημάτων σε μεγάλες αποστάσεις.

1.3 Μεταγωγή Κυκλώματος και Πακέτων

Η αρχική μορφή τηλεπικοινωνιακών συστημάτων βασιζόταν στη μεταγωγή κυκλώματος (circuit switching), όπως παρατηρείται στα παραδοσιακά τηλεφωνικά δίκτυα. Σε αυτήν την αρχιτεκτονική, κάθε σύνδεση απαιτεί αποκλειστική δέσμευση ενός φυσικού μονοπατιού μεταξύ των δύο επικοινωνούντων μερών καθ' όλη τη διάρκεια της συνομιλίας. Αν και το μοντέλο αυτό ήταν κατάλληλο για φωνητικές συνδιαλέξεις, αποδείχθηκε αναποτελεσματικό για την αποστολή δεδομένων, λόγω της αδυναμίας διαμοιρασμού των πόρων του δικτύου και της σπατάλης εύρους ζώνης κατά τις παύσεις μετάδοσης. [5]

Η ριζοσπαστική λύση προτάθηκε ανεξάρτητα από δύο επιστήμονες, τον Paul Baran στις ΗΠΑ και τον Donald Davies στο Ηνωμένο Βασίλειο. Και οι δύο ανέπτυξαν την έννοια της μεταγωγής πακέτων (packet switching), μιας μεθόδου κατά την οποία η πληροφορία τεμαχίζεται σε μικρά, αυτόνομα πακέτα, τα οποία μεταδίδονται μεμονωμένα μέσα από το δίκτυο και ανασυντίθενται στον προορισμό. Η προσέγγιση αυτή όχι μόνο μεγιστοποιεί την απόδοση του δικτύου, αλλά και ενισχύει την ανθεκτικότητά του σε βλάβες, καθώς τα πακέτα μπορούν να ακολουθήσουν εναλλακτικές διαδρομές. [6]

1.4 Το ARPANET και η Γένεση του Σύγχρονου Διαδικτύου

Η εφαρμογή της μεταγωγής πακέτων στην πράξη ξεκίνησε με τη δημιουργία του Advanced Research Projects Agency Network (ARPANET) το 1969, του πρώτου λειτουργικού δικτύου τέτοιας

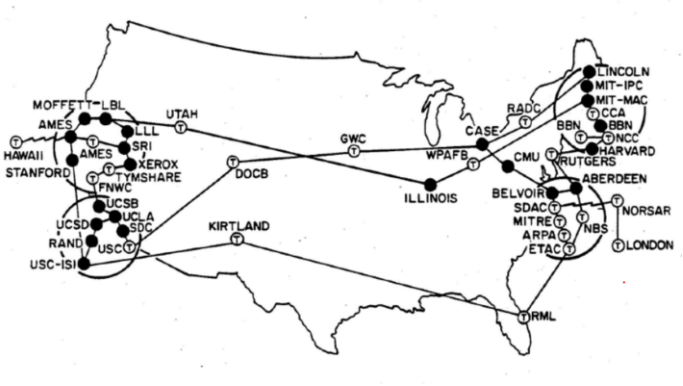
αρχιτεκτονικής. Η λειτουργία του βασίστηκε εξολοκλήρου σε ψηφιακά σήματα, καταργώντας πλήρως την ανάγκη για αναλογικές μετατροπές κατά τη μεταφορά δεδομένων.

Το ARPANET υλοποιήθηκε από την Advanced Research Projects Agency (ARPA) του Υπουργείου Άμυνας των ΗΠΑ, στο πλαίσιο της επιθυμίας δημιουργίας ενός ανθεκτικού και αποκεντρωμένου δικτύου υπολογιστών. Οι πρώτες βάσεις τέθηκαν ήδη από το 1966, όταν ο Lawrence Roberts (μετά από επιρροή από τις θεωρίες του Paul Baran για την κατανεμημένη επικοινωνία) ξεκίνησε την υλοποίηση ενός δικτύου που να βασίζεται όχι στην αποκλειστική γραμμή (όπως η μεταγωγή κυκλώματος), αλλά στη μεταγωγή πακέτων, όπου κάθε μήνυμα διασπάται σε μικρότερα πακέτα, τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου και επανενώνονται στον προορισμό.

Το αρχικό δίκτυο του ARPANET απαρτιζόταν από τέσσερις κόμβους:

- UCLA (University of California, Los Angeles)
- SRI (Stanford Research Institute)
- UCSB (University of California, Santa Barbara)
- University of Utah

Οι κόμβοι αυτοί συνδέθηκαν μεταξύ τους το 1969 και αποτέλεσαν τους πρώτους υπολογιστικούς κόμβους με δυνατότητα απομακρυσμένης επικοινωνίας μέσω ψηφιακών πακέτων. Για τη σύνδεση των υπολογιστών χρησιμοποιήθηκαν Interface Message Processors (IMPs), οι οποίοι λειτουργούσαν ως εξειδικευμένες συσκευές δρομολόγησης. Τα IMPs, σχεδιασμένα από την εταιρεία BBN Technologies (Bolt, Beranek and Newman), είχαν ως βασικό ρόλο τη λήψη, αποθήκευση και προώθηση πακέτων από κόμβο σε κόμβο. [8]



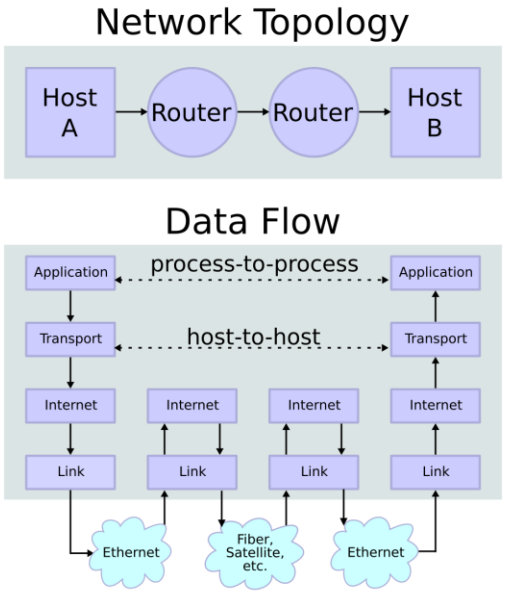
Εικόνα 1.3: Σημεία πρόσβασης του ARPANET το 1970 [11]

Οι επικοινωνίες πραγματοποιούνταν μέσω τηλεφωνικών γραμμών, ωστόσο η μεταφορά γινόταν ψηφιακά και όχι μέσω αναλογικών σημάτων, γεγονός που απαιτούσε τη χρήση modem για τη μετατροπή των σημάτων στις ενδιάμεσες γραμμές, αλλά όχι μεταξύ των IMPs ή των ίδιων των υπολογιστών. [9]

1.5 Προτυποποίηση & Πρωτόκολλα

Μετά την αρχική επιτυχία του ARPANET ως ενός πειραματικού δικτύου μεταγωγής πακέτων, η ανάγκη για ενοποίηση πολλαπλών και ετερογενών δικτυακών υποδομών έγινε άμεσα εμφανής. Το ARPANET παρείχε ένα αποδοτικό και λειτουργικό μοντέλο, ωστόσο δεν υπήρχε ένας καθολικός μηχανισμός για την επικοινωνία μεταξύ διαφορετικών τύπων δικτύων, όπως στρατιωτικά, ακαδημαϊκά ή ερευνητικά. Η

απάντηση σε αυτό το πρόβλημα ήρθε το 1974, όταν οι ερευνητές Vinton Cerf και Robert Kahn δημοσίευσαν την εργασία τους με τίτλο "A Protocol for Packet Network Intercommunication" [76]. Στην εργασία αυτή, περιέγραφαν ένα νέο πρωτόκολλο, το Transmission Control Protocol (TCP), το οποίο σχεδιάστηκε ώστε να παρέχει αξιόπιστη μεταφορά δεδομένων ανάμεσα σε διαφορετικά δίκτυα. Αρχικά, το TCP περιελάμβανε τόσο λειτουργίες αξιόπιστης μεταφοράς όσο και δρομολόγησης πακέτων. Αργότερα, διαχωρίστηκε σε δύο ξεχωριστά επίπεδα, το TCP υπεύθυνο για την ακεραιότητα της επικοινωνίας και το Internet Protocol (IP) υπεύθυνο για τη δρομολόγηση. Το σύνολο αυτό, γνωστό ως TCP/IP, αποτέλεσε το θεμέλιο για τη δημιουργία ενός "δικτύου των δικτύων", δηλαδή του Διαδικτύου. [10]



Εικόνα 1.4: TCP/IP συνδεσμολογία [13]

Το 1983, το TCP/IP καθιερώθηκε επισήμως ως το βασικό πρωτόκολλο του ARPANET, αντικαθιστώντας το παλαιότερο Network Control Protocol (NCP). Η μετάβαση αυτή σηματοδότησε την απαρχή της διαλειτουργικότητας μεταξύ ετερογενών υπολογιστικών συστημάτων, ανεξαρτήτως κατασκευαστή ή λειτουργικού συστήματος, επιτρέποντας σε πανεπιστήμια, κρατικούς οργανισμούς και αργότερα ιδιωτικές επιχειρήσεις να συνδέονται σε ένα ενιαίο παγκόσμιο δίκτυο. [9]

Ταυτόχρονα, το ARPANET άρχισε να διασυνδέεται με άλλα σημαντικά δίκτυα. Μεταξύ αυτών ήταν το Computer Science Network (CSNET), το Military Network (MILNET) και αργότερα το National Science Foundation Network (NSFNET), το οποίο διαδραμάτισε καίριο ρόλο στην ευρύτερη διάδοση του Διαδικτύου. Στην Ευρώπη, εμφανίστηκαν τα δίκτυα European UNIX Network (EUnet) και Joint Academic NETwork (JANET), τα οποία επίσης υιοθέτησαν το TCP/IP ως βασικό πρωτόκολλο. [6]

Η επιτυχία αυτών των διασυνδέσεων και η συνεχής υιοθέτηση του TCP/IP εδραίωσαν την αρχιτεκτονική του Διαδικτύου ως μια ανοικτή, αποκεντρωμένη και επεκτάσιμη πλατφόρμα. Η βασική αρχή ότι "το δίκτυο δεν γνωρίζει εφαρμογές" (end-to-end principle) επέτρεψε την ανεξάρτητη ανάπτυξη νέων υπηρεσιών και εφαρμογών πάνω από το δίκτυο, χωρίς να απαιτούνται αλλαγές στην υποδομή του. [12]

1.6 Η Δημιουργία του Παγκόσμιου Ιστού

Παρά την τεχνική ολοκλήρωση του Διαδικτύου κατά τη δεκαετία του 1980, η χρήση του περιοριζόταν κυρίως σε ερευνητικά και στρατιωτικά περιβάλλοντα. Η καθοριστική αλλαγή ήρθε το 1989, όταν ο Tim Berners-Lee, εργαζόμενος στο CERN, πρότεινε ένα νέο σύστημα ανταλλαγής και σύνδεσης εγγράφων με τη χρήση υπερκειμένου (hypertext). Η πρότασή του κατέληξε στη δημιουργία του World Wide Web (WWW), ενός συστήματος βασισμένου στο HyperText Transfer Protocol (HTTP), τη γλώσσα σήμανσης HyperText Markup Language (HTML) και τη χρήση Uniform Resource Locators (URLs) για την αναγνώριση των εγγράφων.

Το WWW δεν αντικατέστησε το Διαδίκτυο, αλλά αποτέλεσε μια υπηρεσία εντός του Διαδικτύου, επιτρέποντας στους χρήστες να αποκτούν πρόσβαση σε πληροφορίες με γραφική και διασυνδεδεμένη μορφή. Η πρώτη εφαρμογή του ήταν ο φυλλομετρητής WorldWideWeb, αργότερα μετονομασμένος σε Nexus, ο οποίος επέτρεπε την απεικόνιση εγγράφων HTML και την πλοήγηση μέσω υπερσυνδέσμων. [14]

Η μαζική αποδοχή του WWW ξεκίνησε το 1993 με την κυκλοφορία του γραφικού φυλλομετρητή Mosaic, που αναπτύχθηκε από το National Center for Supercomputing Applications (NCSA) στις ΗΠΑ. Το Mosaic και αργότερα το Netscape Navigator, αποτέλεσαν τα πρώτα προγράμματα που προσέφεραν φιλική προς τον χρήστη πλοήγηση στο Διαδίκτυο, καταργώντας την ανάγκη για εντολές σε περιβάλλον κειμένου.

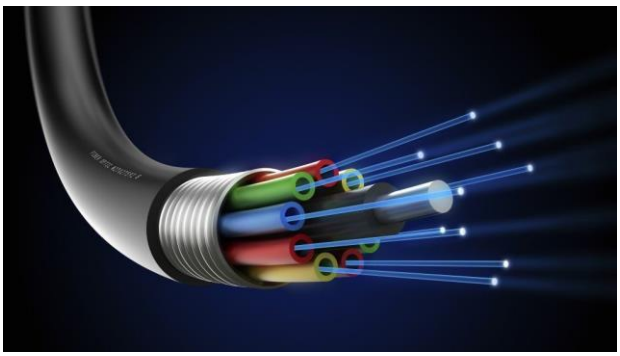
Εικόνα 1.5: Διεπαφή του φυλλομετρητή Mosaic [15]

Η ταχεία διάδοση των φυλλομετρητών συνέπεσε με την εμφάνιση των πρώτων παρόχων υπηρεσιών Διαδικτύου (Internet Service Providers - ISPs). Μέχρι τα μέσα της δεκαετίας του 1990, εταιρείες και ιδιώτες απέκτησαν τη δυνατότητα σύνδεσης στο Διαδίκτυο από το σπίτι ή το γραφείο, σηματοδοτώντας την εμπορική εκτόξευση του Ιστού και τη μετάβαση από την επιστημονική κοινότητα στο ευρύ κοινό.

Η συμβολή του Παγκόσμιου Ιστού στην παγκοσμιοποίηση της πληροφορίας υπήρξε καθοριστική. Μέσα σε λιγότερο από μία δεκαετία, το WWW μετατράπηκε από πειραματική τεχνολογία σε παγκόσμιο μέσο επικοινωνίας, ενημέρωσης και εμπορίου, ανοίγοντας τον δρόμο για τις μετέπειτα εξελίξεις στο ηλεκτρονικό εμπόριο, τις μηχανές αναζήτησης, τα κοινωνικά δίκτυα και τις πλατφόρμες πολυμέσων.[9]

1.7 Η Ψηφιακή Επανάσταση

Η μετάβαση από τις πρώτες, χαμηλής ταχύτητας dial-up συνδέσεις προς τα ευρυζωνικά δίκτυα σηματοδότησε ένα νέο κεφάλαιο στην εξέλιξη του Διαδικτύου. Οι τεχνολογίες Asymmetric Digital Subscriber Line (ADSL) και Very High-Speed DSL (VDSL) αποτέλεσαν τις πρώτες μορφές σταθερής ευρυζωνικής πρόσβασης, αντικαθιστώντας σταδιακά τις τηλεφωνικές γραμμές με γραμμές υψηλής χωρητικότητας. Η εισαγωγή των οπτικών ινών στην αστική υποδομή Fiber To The Home (FTTH) πολλαπλασίασε τις ταχύτητες πρόσβασης, επιτρέποντας την ταυτόχρονη μετάδοση δεδομένων, βίντεο και φωνής σε πραγματικό χρόνο με υψηλή αξιοπιστία. [16]



Εικόνα 1.6: Καλώδιο Οπτικών Ινών [17]

Παράλληλα, η εξέλιξη της κινητής τηλεφωνίας επηρέασε καταλυτικά τον τρόπο πρόσβασης στο Διαδίκτυο. Η υιοθέτηση των δικτύων τρίτης γενιάς (3G) στις αρχές της δεκαετίας του 2000 έδωσε τη δυνατότητα για πραγματική ασύρματη πλοήγηση στο Διαδίκτυο μέσω κινητών τηλεφώνων. Η τεχνολογική συνέχεια με τα δίκτυα 4G - Long Term Evolution (LTE) και στη συνέχεια με την εισαγωγή των δικτύων 5G, πρόσφερε όχι μόνο αυξημένες ταχύτητες (άνω των 100 Mbps) αλλά και σημαντικά μειωμένο χρόνο απόκρισης (latency). Το γεγονός αυτό επέτρεψε την ανάπτυξη εφαρμογών όπως η ζωντανή μετάδοση βίντεο, οι υπηρεσίες cloud και η επικοινωνία συσκευών μέσω του Internet of Things (IoT). [18]

Η τεχνολογική αυτή υποδομή άνοιξε τον δρόμο για την ανάδυση ενός νέου μοντέλου ιστού, του Web 2.0. Σε αντίθεση με την αρχική μορφή του Παγκόσμιου Ιστού (Web 1.0), που περιοριζόταν σε στατικές ιστοσελίδες και παθητική κατανάλωση πληροφορίας, το Web 2.0 επέτρεψε την ενεργό συμμετοχή του χρήστη. Οι χρήστες απέκτησαν τη δυνατότητα να δημιουργούν, να διαμοιράζονται και να επεξεργάζονται περιεχόμενο σε πραγματικό χρόνο. Ιστοσελίδες με δυναμικό περιεχόμενο, πλατφόρμες κοινωνικής δικτύωσης και συνεργατικά εργαλεία έφεραν το Διαδίκτυο πιο κοντά στην έννοια της συλλογικής νοημοσύνης. [19]

Στο πλαίσιο αυτό, οι πλατφόρμες όπως το Facebook (2004), το YouTube (2005) και το Twitter (2006) άλλαξαν ριζικά τον τρόπο επικοινωνίας και διάδοσης της πληροφορίας. Ο χρήστης δεν ήταν πλέον απλός παρατηρητής, αλλά συμμετοχικός παραγωγός περιεχομένου (prosumer). Οι έννοιες του "like", του "share" έγιναν κομμάτι της καθημερινότητας, ενώ η ταχύτατη διάδοση πληροφοριών επηρέασε την πολιτική, την οικονομία και τον πολιτισμό σε παγκόσμια κλίμακα. [20]

Εικόνα 1.7: Γνωστά Κοινωνικά Δίκτυα [21]

Η ευρυζωνικότητα και η φορητότητα έδρασαν συνδυαστικά ως καταλύτες για αυτή τη μεταμόρφωση. Η πρόσβαση στο Διαδίκτυο έπαψε να είναι στατική ή περιορισμένη χρονικά και έγινε μόνιμη και διαδραστική, επιτρέποντας την εμφάνιση νέων μορφών επικοινωνίας, επιχειρηματικότητας και πολιτισμικής έκφρασης.

1.8 Ψηφιακός Μετασχηματισμός

Η ραγδαία τεχνολογική πρόοδος των τελευταίων ετών οδήγησε στην είσοδο του Διαδικτύου σε όλες τις πτυχές της καθημερινής ζωής, διαμορφώνοντας ένα νέο οικοσύστημα ψηφιακής αλληλεπίδρασης. Στην καρδιά αυτής της μετάβασης βρίσκεται το IoT, το οποίο συνενώνει αισθητήρες, έξυπνες συσκευές και δίκτυα επικοινωνίας, επιτρέποντας σε αντικείμενα του φυσικού κόσμου να συνδέονται και να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο. Από τα «έξυπνα» σπίτια και τις βιομηχανίες, έως τα έξυπνα δίκτυα ενέργειας και τις εφαρμογές υγείας, το IoT λειτουργεί ως ο ψηφιακός ιστός που γεφυρώνει τον φυσικό με τον εικονικό κόσμο, επιταχύνοντας τον αυτοματισμό και την απομακρυσμένη εποπτεία.

Παράλληλα, η ολοένα και πιο εκτεταμένη υιοθέτηση του Artificial Intelligence (AI), σε συνδυασμό με τεχνολογίες όπως το υπολογιστικό νέφος (cloud computing) και η υπολογιστική αιχμής (edge computing), έχει αναδιαμορφώσει τον τρόπο με τον οποίο συλλέγεται, επεξεργάζεται και αξιοποιείται η πληροφορία. Η τεχνητή νοημοσύνη χρησιμοποιείται σήμερα σε συστήματα ανάλυσης δεδομένων σε πραγματικό χρόνο, στην αυτοματοποίηση διαδικασιών, στην αναγνώριση προτύπων και στη λήψη αποφάσεων, τόσο σε ιδιωτικές εφαρμογές όσο και σε κρίσιμες δημόσιες υποδομές. Το υπολογιστικό νέφος προσφέρει ευελιξία, κλιμάκωση και αποθήκευση τεραστίων ποσοτήτων δεδομένων, ενώ η υπολογιστική αιχμής φέρνει τη δύναμη της επεξεργασίας πιο κοντά στη συσκευή/αισθητήρα, μειώνοντας την καθυστέρηση και ενισχύοντας την αποδοτικότητα. [22]

Ωστόσο, αυτή η εκθετική αύξηση της διασυνδεσιμότητας και της επεξεργασίας δεδομένων συνοδεύεται από σοβαρές προκλήσεις στον τομέα της κυβερνοασφάλειας και της ψηφιακής κυριαρχίας. Η πολυπλοκότητα των σύγχρονων δικτύων καθιστά τις υποδομές περισσότερο ευάλωτες σε κυβερνοεπιθέσεις, οι οποίες πλέον στοχεύουν όχι μόνο ιδιωτικές εταιρείες αλλά και κρίσιμα κρατικά συστήματα, ενεργειακά δίκτυα, νοσοκομεία και μέσα μεταφοράς. Η ανάγκη για αποτελεσματικούς μηχανισμούς ανίχνευσης, πρόληψης και απόκρισης σε περιστατικά παραβίασης δεδομένων είναι πιο επιτακτική από ποτέ. Παράλληλα, ζητήματα όπως η προστασία της ιδιωτικότητας, η ψηφιακή ανεξαρτησία κρατών και η νομοθετική ρύθμιση της χρήσης της τεχνητής νοημοσύνης, απασχολούν πλέον τις κυβερνήσεις, τους οργανισμούς και την ακαδημαϊκή κοινότητα σε παγκόσμιο επίπεδο.

Εικόνα 1.8: IoT [23]

Η συνύπαρξη του IoT, του AI και της αυξανόμενης ανάγκης για ασφάλεια διαμορφώνει έναν νέο ψηφιακό ορίζοντα, όπου η καινοτομία, η απόδοση και η εμπιστοσύνη καλούνται να συνυπάρξουν. Η πρόκληση πλέον δεν αφορά μόνο τη δημιουργία τεχνολογίας, αλλά και τη διασφάλιση ότι αυτή λειτουργεί προς όφελος των πολιτών και των κοινωνιών, διατηρώντας τον έλεγχο, την ηθική χρήση και τη διαφάνεια ως κεντρικές αξίες του ψηφιακού μετασχηματισμού.

1.9 Επίλογος

Η ιστορική αναδρομή των δικτύων ανέδειξε τη σταδιακή αλλά και καθοριστική εξέλιξη των τεχνολογιών επικοινωνίας, από τα πρώτα αναλογικά και ψηφιακά σήματα έως τον σημερινό ψηφιακό μετασχηματισμό. Η μετάβαση από τη μεταγωγή κυκλώματος στη μεταγωγή πακέτων έθεσε τα θεμέλια για την ανάπτυξη πιο αποδοτικών και ευέλικτων συστημάτων, ενώ η δημιουργία του ARPANET σηματοδότησε την απαρχή του σύγχρονου διαδικτύου. Παράλληλα, η προτυποποίηση και η ανάπτυξη πρωτοκόλλων επικοινωνίας αποτέλεσαν καθοριστικούς παράγοντες για την ενοποίηση και την καθιέρωση κοινών προδιαγραφών σε παγκόσμιο επίπεδο. Η δημιουργία του WWW διεύρυνε περαιτέρω τις δυνατότητες, καθιστώντας το διαδίκτυο εργαλείο μαζικής πληροφόρησης και επικοινωνίας. Η Ψηφιακή Επανάσταση που ακολούθησε μετέβαλε ριζικά τις κοινωνικές, οικονομικές και πολιτιστικές δομές, οδηγώντας τελικά στον σημερινό Ψηφιακό Μετασχηματισμό, ο οποίος συνεχίζει να επαναπροσδιορίζει τη σχέση του ανθρώπου με την τεχνολογία. Συνολικά, η πορεία αυτή αποδεικνύει ότι τα δίκτυα δεν αποτελούν απλώς τεχνολογικές υποδομές, αλλά έναν δυναμικό μηχανισμό που καθορίζει την εξέλιξη της ίδιας της κοινωνίας.

Κεφάλαιο 2ο: Βασικοί Όροι Δικτύων Υπολογιστών

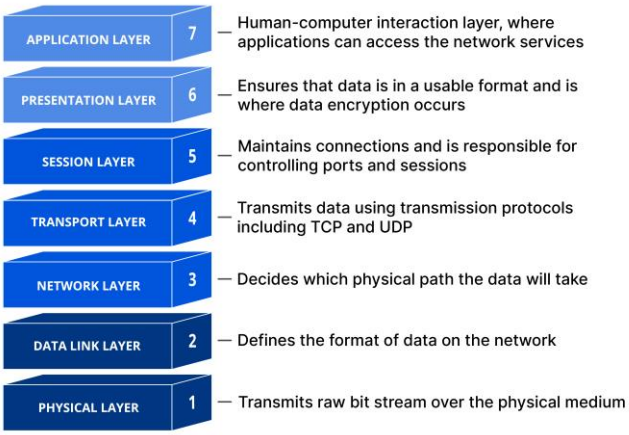
2.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί το εννοιολογικό πλαίσιο των αρχιτεκτονικών μοντέλων δικτύωσης, εστιάζοντας αρχικά στο πρότυπο Διασύνδεσης Ανοικτών Συστημάτων και στα επτά λειτουργικά του επίπεδα. Στη συνέχεια θα αναλυθεί το ευρέως υιοθετημένο μοντέλο TCP/IP, με έμφαση στις δομικές διαφορές και τις πρακτικές αποκλίσεις σε σχέση με το OSI. Τέλος, το κεφάλαιο θα επικεντρωθεί σε επιλεγμένα πρωτόκολλα του επιπέδου εφαρμογής, εξετάζοντας σε βάθος τη λειτουργικότητα, τη χρήση και τη σημασία τους στο σύγχρονο δικτυακό περιβάλλον.

2.2 Open Systems Interconnection

Η επιστήμη των δικτύων υπολογιστών αποτελεί θεμέλιο λίθο για την κατανόηση της σύγχρονης ψηφιακής εποχής. Η δυνατότητα των υπολογιστικών συστημάτων να επικοινωνούν μεταξύ τους, να ανταλλάσσουν πληροφορίες και να διαμοιράζονται πόρους σε τοπικό ή παγκόσμιο επίπεδο, βασίζεται σε ένα καλά ορισμένο σύνολο πρωτοκόλλων και προτύπων.

Η βασική ιδέα πίσω από το OSI ήταν να δημιουργηθεί ένα καθολικό, ανοιχτό μοντέλο διαλειτουργικότητας, το οποίο να επιτρέπει την ανάπτυξη πρωτοκόλλων και συστημάτων ανεξαρτήτως κατασκευαστή ή τεχνολογικής πλατφόρμας. Παρόλο που το OSI δεν υλοποιήθηκε ποτέ πλήρως ως λειτουργικό πρότυπο στην πράξη, αποτέλεσε και συνεχίζει να αποτελεί ένα πολύτιμο εννοιολογικό εργαλείο για την εκπαίδευση και την ανάλυση δικτύων.



Εικόνα 2.1: Τα επίπεδα του μοντέλου αναφοράς OSI [25]

Πριν από την εισαγωγή του OSI, η κατάσταση στα δίκτυα χαρακτηριζόταν από την ύπαρξη ιδιωτικών (proprietary) μοντέλων επικοινωνίας, τα οποία αναπτύσσονταν από μεγάλες εταιρείες όπως η IBM, η DEC και η Xerox. Κάθε κατασκευαστής υιοθετούσε το δικό του μοντέλο και τα δικά του πρωτόκολλα, με αποτέλεσμα να δημιουργείται έντονος κατακερματισμός και να καθίσταται σχεδόν αδύνατη η διασύνδεση ετερογενών συστημάτων. Οι επιχειρήσεις που επένδυαν σε συγκεκριμένες τεχνολογίες «κλειδώνονταν» ουσιαστικά σε αυτές, χωρίς τη δυνατότητα εύκολης συνεργασίας με προϊόντα άλλων κατασκευαστών. Αυτό δημιουργούσε υψηλά κόστη, περιορισμούς στην επεκτασιμότητα και σημαντικά

εμπόδια στη διάδοση των δικτύων σε ευρύτερη κλίμακα. Το OSI ήρθε να απαντήσει σε αυτές τις προκλήσεις εισάγοντας ένα ανοιχτό, τυποποιημένο πλαίσιο που προωθούσε τη διαλειτουργικότητα και έθετε κοινές βάσεις για την ανάπτυξη καινοτόμων τεχνολογιών επικοινωνίας. Έτσι, κατάφερε να αλλάξει τα δεδομένα της εποχής, ανοίγοντας τον δρόμο για την παγκόσμια διάδοση του διαδικτύου και την ευρεία συνεργασία συστημάτων διαφορετικής προέλευσης.

Το μοντέλο αναφοράς OSI προτάθηκε από τον International Organization for Standardization (ISO) τη δεκαετία του 1980, με στόχο την τυποποίηση της διαδικασίας επικοινωνίας ανάμεσα σε ετερογενή υπολογιστικά συστήματα. Πρόκειται για ένα αφηρημένο μοντέλο επτά επιπέδων, το οποίο διαχωρίζει τη λειτουργικότητα ενός δικτύου σε διακριτά επίπεδα, καθένα από τα οποία επιτελεί συγκεκριμένες λειτουργίες και αλληλεπιδρά με τα γειτονικά του.

- **Φυσικο Επίπεδο (Physical Layer):** Το φυσικό επίπεδο αποτελεί τη βάση του μοντέλου αναφοράς OSI και αφορά τη φυσική μετάδοση των δυαδικών ψηφιακών σημάτων (bits) μέσα από τα διάφορα φυσικά μέσα επικοινωνίας, όπως χαλκό, οπτικές ίνες, ασύρματα ραδιοκύματα και άλλα. Σε αυτό το επίπεδο ορίζονται τα χαρακτηριστικά των μέσων μετάδοσης, ανά είδος καλωδίου, οι τάσεις, οι ρυθμοί μετάδοσης (bit rate), τα ηλεκτρικά ή οπτικά σήματα, καθώς και οι τεχνικές διαμόρφωσης (modulation) που χρησιμοποιούνται. Επίσης καθορίζονται τα φυσικά χαρακτηριστικά των συνδέσεων, όπως οι ακροδέκτες (pinouts) και η διάταξη των καλωδίων, ώστε να επιτυγχάνεται αξιόπιστη μεταφορά των bits από τον πομπό στον δέκτη. Το φυσικό επίπεδο δεν ερμηνεύει το περιεχόμενο των δεδομένων, αλλά επικεντρώνεται αποκλειστικά στη μετάδοση των ηλεκτρικών ή οπτικών σημάτων.
- **Επίπεδο Ζεύξης Δεδομένων (Data-Link Layer):** Το επίπεδο ζεύξης δεδομένων διασφαλίζει την αξιόπιστη μεταφορά δεδομένων μεταξύ δύο γειτονικών κόμβων μέσα στο ίδιο δίκτυο. Χωρίζει τα δεδομένα σε πλαίσια (frames), ελέγχει και διορθώνει σφάλματα που προκύπτουν από το φυσικό επίπεδο και ρυθμίζει τον τρόπο με τον οποίο οι κόμβοι αποκτούν πρόσβαση στο Media Access Control (MAC). Επίσης, το επίπεδο αυτό χειρίζεται τις φυσικές διευθύνσεις (MAC addresses) που προσδιορίζουν μοναδικά κάθε συσκευή στο δίκτυο. Κλασικά πρωτόκολλα του επιπέδου σύνδεσης δεδομένων είναι το Ethernet, το Token Ring και το Point-to-Point Protocol (PPP). Μέσω αυτών διασφαλίζεται η ορθή και αδιάλειπτη ροή των δεδομένων μεταξύ γειτονικών κόμβων πριν προωθηθούν στο επόμενο επίπεδο.
- **Επίπεδο Δικτύου (Network Layer):** Το επίπεδο δικτύου έχει ως αποστολή τη δρομολόγηση των πακέτων δεδομένων ανάμεσα σε διαφορετικά δίκτυα, ώστε να φτάσουν από τον αποστολέα στον τελικό παραλήπτη μέσω των βέλτιστων διαδρομών. Εδώ γίνεται η τμηματοποίηση των δεδομένων σε πακέτα, η τοποθέτηση των διευθύνσεων IP και η λήψη αποφάσεων για τη διαδρομή που πρέπει να ακολουθήσουν. Πρωτόκολλα όπως το IP, το Internet Control Message Protocol (ICMP) για διαχείριση μηνυμάτων ελέγχου και τους αλγορίθμους που υλοποιούνται με τα πρωτόκολλα δρομολόγησης. Η αποτελεσματική δρομολόγηση εξασφαλίζει την αξιοπιστία και ευελιξία του Διαδικτύου.
- **Επίπεδο Μεταφοράς (Transport Layer):** Το επίπεδο μεταφοράς είναι υπεύθυνο για τη μεταφορά δεδομένων από την εφαρμογή πηγής στην εφαρμογή προορισμού, προσφέροντας είτε αξιόπιστη είτε μη αξιόπιστη μετάδοση. Στα πλαίσια της αξιόπιστης μεταφοράς, το TCP αναλαμβάνει τη διαχείριση της σύνδεσης, την επανεκπομπή πακέτων σε περίπτωση απώλειας και την επιβεβαίωση λήψης, εξασφαλίζοντας έτσι την ακεραιότητα των δεδομένων. Το TCP επίσης ρυθμίζει τη ροή δεδομένων και τον έλεγχο συμφόρησης. Αντίθετα, το UDP (User Datagram Protocol) παρέχει μια γρηγορότερη αλλά μη εγγυημένη μεταφορά, χρήσιμη για εφαρμογές όπως η μετάδοση πολυμέσων ή παιχνίδια.
- **Επίπεδο Συνεδρίας (Session Layer):** Το επίπεδο συνεδρίας διαχειρίζεται τις συνεδρίες επικοινωνίας ανάμεσα σε εφαρμογές, επιτρέποντας το άνοιγμα, τη διατήρηση, τον συγχρονισμό και το κλείσιμό τους. Είναι υπεύθυνο για την οργάνωση των διαλόγων, ώστε να μην υπάρχει σύγχυση στην επικοινωνία και παρέχει μηχανισμούς για την αποκατάσταση σε περίπτωση διακοπής. Παρά το ότι πολλές σύγχρονες εφαρμογές ενσωματώνουν αυτές τις λειτουργίες σε άλλα επίπεδα, το επίπεδο συνεδρίας παραμένει σημαντικό στο θεωρητικό πλαίσιο των δικτύων.
- **Επίπεδο Παρουσίασης (Presentation Layer):** Αυτό το επίπεδο λειτουργεί ως μεταφραστής δεδομένων μεταξύ διαφορετικών συστημάτων, εξασφαλίζοντας ότι τα δεδομένα που λαμβάνει μια εφαρμογή έχουν τη σωστή μορφή και κωδικοποίηση για να γίνουν κατανοητά. Υποστηρίζει λειτουργίες όπως η κωδικοποίηση χαρακτήρων (π.χ. American Standard Code for Information Interchange, Unicode

- ASCII), η συμπίεση (για μείωση του όγκου των δεδομένων) και η κρυπτογράφηση (για ασφάλεια της πληροφορίας). Το επίπεδο παρουσίασης εξασφαλίζει τη διαλειτουργικότητα μεταξύ διαφορετικών αρχιτεκτονικών και πλατφορμών.

- **Επίπεδο Εφαρμογής (Application Layer):** Το υψηλότερο επίπεδο του μοντέλου αναφοράς OSI είναι αυτό που βρίσκεται πιο κοντά στον τελικό χρήστη και περιλαμβάνει πρωτόκολλα και υπηρεσίες που υποστηρίζουν εφαρμογές, όπως η πρόσβαση στον Παγκόσμιο Ιστό, η αποστολή ηλεκτρονικού ταχυδρομείου, η μεταφορά αρχείων και η διαχείριση ονομάτων τομέα. Το επίπεδο εφαρμογής παρέχει το περιβάλλον για την επικοινωνία μεταξύ των εφαρμογών, διαμορφώνοντας τον τρόπο με τον οποίο τα δεδομένα ανταλλάσσονται και παρουσιάζονται στον χρήστη. [24]

2.3 Η Διαχρονικότητα του Μοντέλου Αναφοράς OSI

Το μοντέλο αναφοράς OSI αποτελεί έναν θεμελιώδη πυλώνα στην κατανόηση της δομής και λειτουργίας των δικτύων υπολογιστών. Μέσω της διαστρωμάτωσης των λειτουργιών σε επτά διακριτά επίπεδα, παρέχει ένα καθαρό και οργανωμένο πλαίσιο που διευκολύνει τον σχεδιασμό, την υλοποίηση και τη διαχείριση πολύπλοκων δικτυακών συστημάτων. Αν και το ίδιο το μοντέλο αναφοράς OSI δεν εφαρμόστηκε πλήρως στην πράξη, η θεωρητική του αξία παραμένει ανεκτίμητη, καθώς βοηθά στην κατανόηση των διαδικασιών επικοινωνίας, στην ανάλυση προβλημάτων και στην ανάπτυξη νέων τεχνολογιών. Η γνώση των επιπέδων και των λειτουργιών τους είναι απαραίτητη για κάθε επαγγελματία που εργάζεται στον χώρο των δικτύων, καθώς δημιουργεί τη βάση για την κατανόηση πιο πρακτικών προτύπων, όπως το TCP/IP, που κυριαρχούν στον σύγχρονο ψηφιακό κόσμο. Με αυτό το πλαίσιο, το μοντέλο αναφοράς OSI συνεχίζει να αποτελεί σημείο αναφοράς για τη μελέτη και την εξέλιξη των δικτύων επικοινωνίας.

2.4 Η Μετάβαση από το Μοντέλο Αναφοράς OSI στο TCP/IP

Παράλληλα με την ανάπτυξη του OSI, αναπτύχθηκε από την ARPA των ΗΠΑ ένα πιο πρακτικό και ευέλικτο πρότυπο, το οποίο τελικά επικράτησε στην πράξη. Το μοντέλο TCP/IP, που βασίζεται στα πρωτόκολλα TCP και IP, ήταν το λειτουργικό πρότυπο που υιοθετήθηκε από το ARPANET και εν συνεχεία από το σύνολο του παγκόσμιου Διαδικτύου.

Η μετάβαση από το μοντέλο αναφοράς OSI στο μοντέλο TCP/IP αποτελεί μια από τις σημαντικότερες εξελίξεις στην ιστορία των δικτύων υπολογιστών και του Διαδικτύου, καθώς αποτυπώνει τη διαφορά μεταξύ θεωρίας και πράξης στον σχεδιασμό δικτυακών προτύπων. Παρά το γεγονός ότι το OSI, που προτάθηκε από τον Διεθνή Οργανισμό Τυποποίησης, υπήρξε μια πολύ καλά δομημένη και αναλυτική προσέγγιση, η πραγματική υιοθέτηση και εφαρμογή του στην παγκόσμια κλίμακα δεν κατέστη εφικτή. Αντίθετα, το TCP/IP, το οποίο αναπτύχθηκε παράλληλα από την ARPA των ΗΠΑ, κατόρθωσε να επικρατήσει ως το βασικό πρότυπο επικοινωνίας, εξασφαλίζοντας την επιτυχημένη λειτουργία του ARPANET και στη συνέχεια του παγκόσμιου Διαδικτύου. [7]

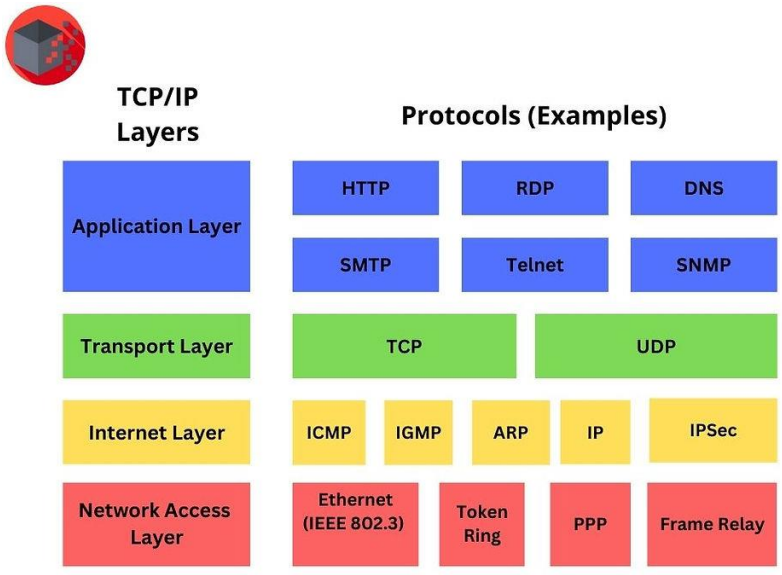
Η διαφορά των δύο μοντέλων έγκειται κατά κύριο λόγο στον σχεδιασμό και την εφαρμογή τους. Το OSI ήταν ένα καθαρά εννοιολογικό μοντέλο επτά επιπέδων, το οποίο επιδίωκε να καλύψει κάθε πτυχή της δικτυακής επικοινωνίας μέσω αυστηρής διαστρωμάτωσης και τυποποίησης. Ωστόσο, το OSI είχε ως κύριο μειονέκτημα τη θεωρητική του φύση και την πολυπλοκότητα που το καθιστούσε δυσχερές στην υλοποίηση και την ευρεία υιοθέτηση. Αντίθετα, το TCP/IP σχεδιάστηκε με γνώμονα την πρακτικότητα και την λειτουργικότητα, δοκιμαζόμενο και βελτιούμενο μέσω της συνεχούς χρήσης σε πραγματικά δίκτυα. Η ευελιξία και η προσαρμοστικότητά του επέτρεψαν τη σύνδεση διαφορετικών δικτύων με διαφορετικές τεχνολογίες και προδιαγραφές, διευκολύνοντας έτσι την ταχεία ανάπτυξη του Διαδικτύου.

Επιπλέον, η υιοθέτηση του TCP/IP έγινε με ανοιχτό και συνεργατικό τρόπο, όπου η κοινότητα των χρηστών και των προγραμματιστών συνέβαλε ενεργά στη βελτίωση και επέκταση του πρωτοκόλλου. Αυτή η συμμετοχική προσέγγιση ενίσχυσε την ευελιξία του TCP/IP, ενώ αντίστοιχα το OSI παρέμεινε ένα περισσότερο κλειστό και τυποποιημένο σύστημα, με πιο αργούς ρυθμούς εξέλιξης. Στο πλαίσιο αυτό, η μετάβαση από το OSI στο TCP/IP δεν ήταν απλώς μια τεχνική επιλογή, αλλά μια εξέλιξη που αντικατοπτρίζει τη διάθεση της τεχνολογικής κοινότητας για εφαρμοσμένες λύσεις που ανταποκρίνονται άμεσα στις ανάγκες της εποχής. [26]

Συνοπτικά, η επικράτηση του TCP/IP έναντι του OSI οφείλεται στην απλότητα, την ευελιξία, την πρακτική εφαρμοσιμότητα και την ανοικτή φύση του, που το καθιστούν το λειτουργικό πρότυπο του σύγχρονου Διαδικτύου. Η μετάβαση αυτή σηματοδότησε τη θεμελίωση ενός παγκόσμιου και διαλειτουργικού δικτύου, το οποίο συνεχίζει να εξελίσσεται και να προσαρμόζεται στις διαρκώς αυξανόμενες απαιτήσεις της ψηφιακής εποχής.

2.5 Ανάλυση του Μοντέλου TCP/IP

Στο παρόν κεφάλαιο θα αναπτυχθούν αναλυτικά τα τέσσερα επίπεδα του μοντέλου TCP/IP, εξετάζοντας τη δομή, τις λειτουργίες και τα βασικά πρωτόκολλα που τα χαρακτηρίζουν. Θα μελετηθούν οι τρόποι με τους οποίους κάθε επίπεδο συμβάλλει στην αξιόπιστη και αποδοτική μετάδοση δεδομένων μέσα από δίκτυα, από το φυσικό μέσο και την τοπική σύνδεση στο Επίπεδο Πρόσβασης Δικτύου, μέχρι τη δρομολόγηση και τη διευθυνσιοδότηση στο Επίπεδο Διαδικτύου, τη διαχείριση των συνδέσεων στο Επίπεδο Μεταφοράς και, τέλος, την υποστήριξη των εφαρμογών στο ανώτερο Επίπεδο Εφαρμογής. Μέσω αυτής της προσέγγισης θα αναδειχθεί η συνολική λειτουργία και η αλληλεπίδραση των επιπέδων που αποτελούν τη βάση του σύγχρονου Διαδικτύου.



Εικόνα 2.2: Τα επίπεδα του μοντέλου TCP/IP [27]

Στη βιβλιογραφία συναντώνται δύο διαφορετικές εκδοχές του μοντέλου TCP/IP Η πρώτη το παρουσιάζει σε πέντε επίπεδα, ενώ η δεύτερη σε τέσσερα. Η διαφοροποίηση αυτή οφείλεται κυρίως στον τρόπο με τον οποίο αντιμετωπίζεται το φυσικό και το ζεύξης δεδομένων επίπεδο. Στο πλαίσιο της

παρούσας εργασίας θα αναπτυχθεί η εκδοχή με τα τέσσερα επίπεδα, καθώς αυτή θεωρείται η πιο διαδεδομένη και απλουστευμένη προσέγγιση για την κατανόηση της λειτουργίας του διαδικτύου.

2.5.1 Επίπεδο Πρόσβασης Δικτύου (Network Access)

Το επίπεδο Πρόσβασης Δικτύου στο μοντέλο TCP/IP αποτελεί το θεμέλιο της τοπικής δικτυακής επικοινωνίας, συνδυάζοντας ουσιαστικά τα δύο πρώτα επίπεδα του μοντέλου αναφοράς OSI, το Φυσικό και το Επίπεδο Ζεύξης Δεδομένων. Στο πλαίσιο αυτό, το επίπεδο Πρόσβασης Δικτύου έχει την ευθύνη για τη μετάδοση των δεδομένων σε τοπικό επίπεδο, δηλαδή μεταξύ συσκευών που βρίσκονται στο ίδιο φυσικό δίκτυο ή στο ίδιο μέσο μετάδοσης. Η λειτουργία του είναι κρίσιμη για την ομαλή και αξιόπιστη επικοινωνία, καθώς διαχειρίζεται τη μορφοποίηση των δεδομένων σε δομημένα πλαίσια (frames), την πρόσβαση στο κοινό μέσο και τον έλεγχο της ακεραιότητας των μεταδιδόμενων δεδομένων.

Σε αυτό το επίπεδο, τα δεδομένα οργανώνονται σε πλαίσια τα οποία περιλαμβάνουν, μεταξύ άλλων, ειδικά πεδία ελέγχου και τα διευθυνσιοδοτικά στοιχεία των συσκευών, γνωστά ως διευθύνσεις MAC. Οι διευθύνσεις MAC είναι μοναδικοί 48-bit αριθμοί που αποδίδονται σε κάθε φυσική δικτυακή συσκευή και χρησιμεύουν για την αναγνώρισή της σε τοπικό επίπεδο. Αυτές οι διευθύνσεις καθιστούν δυνατή την ακριβή αποστολή και παραλαβή των δεδομένων μεταξύ συγκεκριμένων συσκευών στο ίδιο δίκτυο, εξασφαλίζοντας ότι τα πλαίσια φτάνουν στον σωστό προορισμό. Η σημασία της διευθυνσιοδότησης MAC είναι ιδιαίτερα εμφανής σε δίκτυα Ethernet, όπου κάθε πλαίσιο περιλαμβάνει πεδία πηγής και προορισμού MAC, επιτρέποντας τον εντοπισμό και την επίβλεψη της ροής των δεδομένων. Για παράδειγμα, πολλές διευθύνσεις MAC εμφανίζονται με τη μορφή έξι ζευγών δεκαεξαδικών ψηφίων, χωρισμένων με άνω και κάτω τελεία ή παύλα. Έτσι, μία τυπική διεύθυνση MAC μπορεί να είναι 00:1A:2B:3C:4D:5E, όπου τα πρώτα τρία ζεύγη (00:1A:2B) προσδιορίζουν τον κατασκευαστή της συσκευής και τα τελευταία (3C:4D:5E) είναι μοναδικός αναγνωριστικό της συσκευής.

Η διαχείριση της πρόσβασης στο μέσο μετάδοσης αποτελεί έναν από τους πιο σημαντικούς μηχανισμούς του επιπέδου Πρόσβασης Δικτύου. Σε ενσύρματα δίκτυα όπως το Ethernet, εφαρμόζεται η τεχνική Carrier Sense Multiple Access with Collision Detection (CSMA/CD), που επιτρέπει στις συσκευές να ανιχνεύουν πότε το μέσο είναι ελεύθερο και να αποφεύγουν ή να διαχειρίζονται συγκρούσεις στη μετάδοση των δεδομένων. Αντίστοιχα, στα ασύρματα δίκτυα, όπως αυτά που χρησιμοποιούν το πρότυπο Wi-Fi, εφαρμόζεται το Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), το οποίο λαμβάνει υπόψη τις ιδιαιτερότητες της ασύρματης μετάδοσης, όπου η ανίχνευση σύγκρουσης δεν είναι πάντα εφικτή. Σε αυτά τα δίκτυα, ο έλεγχος πρόσβασης γίνεται με τη βοήθεια μηχανισμών όπως η επιβεβαίωση λήψης (acknowledgment) και οι χρονικές καθυστερήσεις (backoff timers), ώστε να περιορίζεται η πιθανότητα ταυτόχρονης εκπομπής από πολλούς σταθμούς.

Η μετάδοση στο φυσικό επίπεδο, που ενσωματώνεται στο Πρόσβασης Δικτύου, περιλαμβάνει τόσο τα ενσύρματα μέσα μετάδοσης (χάλκινα καλώδια, οπτικές ίνες) όσο και τα ασύρματα κανάλια. Στα ασύρματα δίκτυα, η επικοινωνία βασίζεται σε ραδιοκύματα ή μικροκύματα, τα οποία προσφέρουν ευελιξία και κινητικότητα, αλλά ταυτόχρονα επιβάλλουν ιδιαίτερους περιορισμούς και προκλήσεις όπως η παρεμβολή, η αστάθεια σήματος και η περιορισμένη χωρητικότητα. Το επίπεδο Πρόσβασης Δικτύου ενσωματώνει τους απαραίτητους μηχανισμούς για την αντιμετώπιση αυτών των προκλήσεων, εξασφαλίζοντας την αξιοπιστία της μετάδοσης μέσα σε ένα δυναμικό και πολύπλοκο περιβάλλον.

Το επίπεδο αυτό είναι υπεύθυνο για τον έλεγχο σφαλμάτων μέσω τεχνικών όπως η Cyclic Redundancy Check (CRC), που επιτρέπει τον εντοπισμό λαθών στα πλαίσια δεδομένων πριν αυτά προωθηθούν στο επόμενο επίπεδο. Μέσω αυτών των λειτουργιών, το επίπεδο Πρόσβασης Δικτύου αποτελεί τη βάση για

την ομαλή και αποδοτική δικτυακή επικοινωνία, προετοιμάζοντας τα δεδομένα ώστε να μεταφερθούν σωστά σε υψηλότερα επίπεδα του πρωτοκόλλου TCP/IP. [28]

2.5.2 Επίπεδο Διαδικτύου (Internet Layer)

Το Επίπεδο Διαδικτύου στο μοντέλο TCP/IP αποτελεί την καρδιά της διαδικτυακής επικοινωνίας, καθώς είναι υπεύθυνο για τη διευθυνσιοδότηση και τη δρομολόγηση των δεδομένων από την πηγή στον προορισμό, ακόμα και όταν αυτά διασχίζουν πολλαπλά ανεξάρτητα δίκτυα. Σε αντίθεση με το επίπεδο Πρόσβασης Δικτύου, που λειτουργεί σε τοπικό επίπεδο, το Επίπεδο Διαδικτύου διαχειρίζεται την παγκόσμια διαλειτουργικότητα μεταξύ δικτύων, καθιστώντας δυνατή την επικοινωνία μεταξύ απομακρυσμένων συσκευών, ανεξάρτητα από τη φυσική τοπολογία ή τεχνολογία του κάθε δικτύου.

Κεντρικό στοιχείο αυτού του επιπέδου είναι το πρωτόκολλο IP, το οποίο ορίζει το βασικό πλαίσιο και τους κανόνες για τη διακίνηση πακέτων δεδομένων, γνωστών και ως datagrams. Κάθε πακέτο IP περιλαμβάνει, μεταξύ άλλων, πεδία πηγής και προορισμού που περιέχουν τις διευθύνσεις IP των αποστολέα και παραλήπτη. Οι διευθύνσεις IP αποτελούν μοναδικούς αριθμούς που ταυτοποιούν κάθε συσκευή σε ένα δίκτυο ή σε ένα σύνολο δικτύων. Υπάρχουν δύο βασικές εκδόσεις του πρωτοκόλλου IP που χρησιμοποιούνται ευρέως, η IPv4 και η IPv6. Η IPv4 χρησιμοποιεί διευθύνσεις 32-bit, επιτρέποντας περίπου 4,3 δισεκατομμύρια μοναδικές διευθύνσεις, ενώ η IPv6, με διευθύνσεις 128-bit, σχεδιάστηκε για να αντιμετωπίσει τον περιορισμό διευθύνσεων της IPv4, παρέχοντας πρακτικά απεριόριστο αριθμό μοναδικών διευθύνσεων.

Στην έκδοση IPv4, οι διευθύνσεις συνήθως εκφράζονται σε δεκαδική μορφή χωρισμένη σε τέσσερα οκτάδες, όπως για παράδειγμα η 192.168.1.10 ή η 203.0.113.25. Η νεότερη έκδοση IPv6 αποδίδεται σε δεκαεξαδική μορφή χωρισμένη με άνω και κάτω τελείες, όπως 2001:0db8:85a3:0000:0000:8a2e:0370:7334 ή, σε συντομευμένη μορφή, 2001:db8::8a2e:370:7334. Για την οργάνωση των δικτύων χρησιμοποιούνται οι μάσκες δικτύου (subnet masks), οι οποίες καθορίζουν ποιο τμήμα της διεύθυνσης IP αντιστοιχεί στο δίκτυο και ποιο στους μεμονωμένους υπολογιστές (hosts) του δικτύου. Στην IPv4, μια τυπική μάσκα μπορεί να είναι 255.255.255.0 (ή /24 σε CIDR notation), που σημαίνει ότι τα πρώτα 24 bits προσδιορίζουν το δίκτυο και τα υπόλοιπα 8 bits προσδιορίζουν τον host. Στην IPv6 η έννοια είναι παρόμοια, αλλά η μάσκα εκφράζεται σχεδόν πάντα σε CIDR μορφή, όπως /64, υποδεικνύοντας ότι τα πρώτα 64 bits είναι το τμήμα δικτύου και τα υπόλοιπα 64 το τμήμα του host.

Η δρομολόγηση των πακέτων γίνεται μέσω ειδικών δικτυακών συσκευών, των δρομολογητών (routers), που αναλαμβάνουν να κατευθύνουν κάθε πακέτο προς τον τελικό προορισμό του, λαμβάνοντας υπόψη παράγοντες όπως η τοπολογία του δικτύου, η συμφόρηση και η ποιότητα σύνδεσης. Τα πρωτόκολλα δρομολόγισης, όπως το Open Shortest Path First (OSPF) και το Border Gateway Protocol (BGP), συνεργάζονται με το IP για να καθορίσουν τις βέλτιστες διαδρομές μέσα στο δίκτυο και ανάμεσα σε διαφορετικά δίκτυα αντίστοιχα.

Επιπλέον, στο Επίπεδο Διαδικτύου ανήκουν και τα πρωτόκολλα διαχείρισης, όπως το ICMP, το οποίο χρησιμοποιείται για την αναφορά σφαλμάτων και τη διάγνωση προβλημάτων. Για παράδειγμα, το εργαλείο ping βασίζεται στο ICMP και επιτρέπει τη μέτρηση της προσβασιμότητας και της καθυστέρησης μεταξύ δύο συσκευών στο δίκτυο.

Η αποτελεσματική λειτουργία του Επιπέδου Διαδικτύου είναι κρίσιμη για τη σωστή και ασφαλή λειτουργία του παγκόσμιου Διαδικτύου, καθώς διασφαλίζει τη διαλειτουργικότητα μεταξύ διαφορετικών δικτύων και τεχνολογιών. [28]

2.5.3 Επίπεδο Μεταφοράς (Transport Layer)

Το Επίπεδο Μεταφοράς του μοντέλου TCP/IP παίζει καθοριστικό ρόλο στη διαχείριση της επικοινωνίας μεταξύ δύο τερματικών συσκευών, προσφέροντας υπηρεσίες που εξασφαλίζουν τη σωστή, αποδοτική και οργανωμένη μεταφορά των δεδομένων ανεξαρτήτως της υποκείμενης δικτυακής υποδομής.

Κύρια πρωτόκολλα του επιπέδου μεταφοράς είναι το TCP και το User Datagram Protocol (UDP), τα οποία προσφέρουν διαφορετικού τύπου υπηρεσίες ανάλογα με τις απαιτήσεις της εφαρμογής. Το TCP είναι πρωτόκολλο το οποίο προϋποθέτει να έχει πραγματοποιηθεί σύνδεση, το οποίο παρέχει αξιόπιστη μεταφορά δεδομένων μέσω μηχανισμών επιβεβαίωσης λήψης (acknowledgments), επανεκπομπής πακέτων που έχουν χαθεί ή αλλοιωθεί και ελέγχου ροής ώστε να μην υπερφορτώνεται ο παραλήπτης. Αυτό το χαρακτηριστικό το καθιστά ιδανικό για εφαρμογές που απαιτούν ακεραιότητα και συνέπεια, όπως η μεταφορά αρχείων, η πρόσβαση στον Παγκόσμιο Ιστό και η ηλεκτρονική αλληλογραφία.

Αντίθετα, το UDP είναι πρωτόκολλο χωρίς σύνδεση (connectionless), το οποίο δεν παρέχει μηχανισμούς επιβεβαίωσης ή επανεκπομπής, προσφέροντας γρήγορη μετάδοση με ελάχιστη καθυστέρηση. Η έλλειψη αξιόπιστων μηχανισμών το καθιστά κατάλληλο για εφαρμογές που προτιμούν την ταχύτητα έναντι της αξιοπιστίας, όπως η ζωντανή μετάδοση πολυμέσων (streaming video και audio), τα διαδικτυακά παιχνίδια (online gaming) και η φωνητική τηλεφωνία μέσω διαδικτύου (Voice over IP - VoIP).

Μια βασική λειτουργία του Επιπέδου Μεταφοράς είναι η πολυπλεξία, δηλαδή η δυνατότητα διαχείρισης πολλαπλών ταυτόχρονων επικοινωνιών ανάμεσα σε πολλές εφαρμογές και χρήστες, που μοιράζονται την ίδια φυσική σύνδεση. Η πολυπλεξία επιτυγχάνεται μέσω της έννοιας των θυρών (ports), που αποτελούν λογικούς δείκτες στους υπολογιστές για τον διαχωρισμό και τη δρομολόγηση των δεδομένων σε συγκεκριμένες εφαρμογές ή υπηρεσίες. Κάθε πακέτο μεταφοράς περιλαμβάνει, εκτός από τις διευθύνσεις IP πηγής και προορισμού στο επίπεδο Διαδικτύου και αριθμούς θυρών πηγής και προορισμού που καθορίζουν ποια εφαρμογή θα λάβει ή θα αποστείλει τα δεδομένα.

Οι θύρες είναι αριθμημένοι από 0 έως 65535 και κατηγοριοποιούνται σε διάφορες κατηγορίες ανάλογα με τη χρήση τους. Οι "κανονικές" ή γνωστές θύρες (Well-Known Ports) καλύπτουν τους αριθμούς από 0 έως 1023 και αντιστοιχούν σε βασικές υπηρεσίες, όπως για παράδειγμα η θύρα 80 για το HTTP, η θύρα 443 για το Hypertext Transfer Protocol Secure (HTTPS), η 25 για το Simple Mail Transfer Protocol (SMTP) και η 53 για το Domain Name System (DNS). Οι θύρες από 1024 έως 49151 είναι οι εγγεγραμμένες (Registered Ports), που χρησιμοποιούνται από λιγότερο διαδεδομένες ή ειδικές εφαρμογές, ενώ οι θύρες από 49152 έως 65535 προορίζονται για δυναμική ή ιδιωτική χρήση (Dynamic/Private Ports), συνήθως από προσωρινές συνδέσεις και εφαρμογές πελάτη.

Για παράδειγμα, όταν ένας χρήστης ανοίγει μια ιστοσελίδα στο πρόγραμμα περιήγησης, η σύνδεση TCP γίνεται με προορισμό τη θύρα 80 ή 443 του απομακρυσμένου εξυπηρετητή (server), ενώ η θύρα πηγής είναι μια τυχαία δυναμική θύρα που χρησιμοποιείται για τη συγκεκριμένη σύνδεση. Με αυτόν τον τρόπο, το επίπεδο μεταφοράς διαχειρίζεται πολλαπλές ταυτόχρονες συνεδρίες, εξασφαλίζοντας ότι τα δεδομένα που αποστέλλονται και λαμβάνονται ανήκουν στη σωστή εφαρμογή ή συνεδρία.

Επιπλέον, το επίπεδο μεταφοράς αναλαμβάνει τη διάσπαση μεγάλων ροών δεδομένων σε μικρότερα τμήματα (segments) κατά την αποστολή και την επανασύνθεσή τους κατά την παραλαβή, ώστε να ανταποκριθεί στα όρια του δικτύου και να διευκολύνει τη διαχείριση της ροής. Αυτή η διαδικασία είναι ιδιαίτερα σημαντική σε δίκτυα με μεταβλητά χαρακτηριστικά καθυστέρησης και απώλειας πακέτων, όπου το TCP εφαρμόζει μηχανισμούς ελέγχου συμφόρησης για να αποφευχθεί η υπερφόρτωση του δικτύου.

Το Επίπεδο Μεταφοράς αποτελεί το κρίσιμο ενδιάμεσο στρώμα που διασφαλίζει ότι οι εφαρμογές επικοινωνούν με τον επιθυμητό βαθμό αξιοπιστίας, αποτελεσματικότητας και ταχύτητας, προσαρμόζοντας τη ροή δεδομένων στις απαιτήσεις κάθε περίπτωσης (μόνο στο TCP) και προσφέροντας ταυτόχρονα τη δυνατότητα πολυπλεξίας μέσω της χρήσης των θυρών. Η κατανόηση των μηχανισμών του επιπέδου αυτού είναι απαραίτητη για την εμβάθυνση στην αρχιτεκτονική του Διαδικτύου και τη σχεδίαση αποτελεσματικών δικτυακών υπηρεσιών. [28]

2.5.4 Επίπεδο Εφαρμογής (Application Layer)

Το Επίπεδο Εφαρμογής στο μοντέλο TCP/IP αντιπροσωπεύει το ανώτατο και πλέον άμεσα συνδεδεμένο με τον τελικό χρήστη στρώμα της δικτυακής στοίβας. Η κύρια αποστολή του είναι να λειτουργήσει ως το κρίσιμο σημείο επαφής μεταξύ των δικτυακών εφαρμογών και των υποκείμενων δικτυακών υπηρεσιών, διευκολύνοντας έτσι την ανταλλαγή δεδομένων και πληροφοριών με τρόπο κατανοητό και προσαρμοσμένο στις ανάγκες του χρήστη. Σε αντίθεση με το πιο πολύπλοκο και διακριτό σε τρία επίπεδα (Συνεδρίας, Παρουσίασης και Εφαρμογής) μοντέλο OSI, το μοντέλο TCP/IP απλοποιεί και ενοποιεί αυτές τις λειτουργίες σε ένα ενιαίο επίπεδο, όπου υλοποιούνται και συνυπάρχουν όλα τα απαραίτητα πρωτόκολλα για την παροχή διαφόρων δικτυακών υπηρεσιών.

Η συγκέντρωση αυτών των λειτουργιών σε ένα επίπεδο οφείλεται στην ανάγκη για ευελιξία, απλότητα και πρακτικότητα, καθώς το TCP/IP σχεδιάστηκε κυρίως με γνώμονα την λειτουργική υλοποίηση και την ευρεία προσαρμογή στο Διαδίκτυο, το οποίο απαιτεί την υποστήριξη ποικιλίας εφαρμογών, από απλές μεταφορές αρχείων μέχρι πολύπλοκες υπηρεσίες πολυμέσων και αλληλεπίδρασης σε πραγματικό χρόνο. Το Επίπεδο Εφαρμογής, λοιπόν, αναλαμβάνει όχι μόνο τη διαχείριση της επικοινωνίας σε επίπεδο εφαρμογών, αλλά και τον χειρισμό θεμάτων όπως η μορφοποίηση των δεδομένων, η κωδικοποίηση, η κρυπτογράφηση, η διαχείριση συνεδριών και η διαπραγμάτευση των παραμέτρων επικοινωνίας, εξασφαλίζοντας έτσι ότι οι εφαρμογές μπορούν να επικοινωνούν αποτελεσματικά και με ασφάλεια.

Η ευρεία γκάμα πρωτοκόλλων που υλοποιούνται σε αυτό το επίπεδο αντικατοπτρίζει την ποικιλία των υπηρεσιών που το σύγχρονο Διαδίκτυο προσφέρει και την ποικιλία των απαιτήσεων που αυτές επιβάλλουν. Κάθε πρωτόκολλο εξυπηρετεί συγκεκριμένους τύπους επικοινωνίας και εφαρμογών, όπως είναι η πρόσβαση σε ιστοσελίδες, η αποστολή και λήψη ηλεκτρονικής αλληλογραφίας, η μεταφορά αρχείων, η απομακρυσμένη διαχείριση συστημάτων, η αυτόματη εκχώρηση διευθύνσεων IP, η μετάδοση πολυμέσων και η διαχείριση ονομάτων τομέα. Με αυτόν τον τρόπο, το Επίπεδο Εφαρμογής λειτουργεί ως το κύριο μέσο που επιτρέπει την αλληλεπίδραση του χρήστη με το Διαδίκτυο και τις δικτυακές υποδομές, καθιστώντας το βασικό στοιχείο για τη λειτουργικότητα, την επεκτασιμότητα και την ευρωστία των σύγχρονων δικτύων.

Το Επίπεδο Εφαρμογής στο TCP/IP αποτελεί τη γέφυρα μεταξύ των τεχνολογικών υποδομών και των πρακτικών αναγκών του τελικού χρήστη, προσφέροντας ένα ευέλικτο, εκτεταμένο και λειτουργικά πλούσιο περιβάλλον για την υλοποίηση και ανάπτυξη ποικίλων δικτυακών υπηρεσιών, οι οποίες αποτελούν την καρδιά της καθημερινής ψηφιακής επικοινωνίας. [28]

2.6 Παρουσίαση Συνηθέστερων Πρωτοκόλλων του Επιπέδου Εφαρμογής

Η λειτουργία των δικτύων στηρίζεται σε μεγάλο βαθμό στα πρωτόκολλα του επιπέδου εφαρμογής, καθώς αυτά αποτελούν το σημείο αλληλεπίδρασης του χρήστη με τις παρεχόμενες υπηρεσίες. Στην ενότητα αυτή παρουσιάζονται τα συνηθέστερα πρωτόκολλα που χρησιμοποιούνται στο επίπεδο

εφαρμογής, με στόχο την κατανόηση της λειτουργίας τους, των χαρακτηριστικών τους και της συμβολής τους στη μετάδοση δεδομένων και την παροχή διαδικτυακών υπηρεσιών.

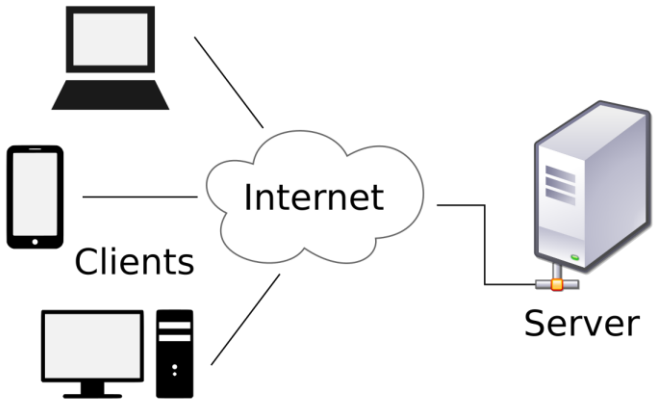
2.6.1 HTTP

Το πρωτόκολλο HTTP αποτελεί τη θεμελιώδη τεχνολογία για τη λειτουργία του Παγκόσμιου Ιστού, καθώς καθορίζει τον τρόπο με τον οποίο οι πελάτες (clients) και οι εξυπηρετητές (servers) επικοινωνούν για την ανταλλαγή υπερκειμένου και πολυμεσικών δεδομένων. Το HTTP βασίζεται στο μοντέλο πελάτη-εξυπηρετητή (client-server), όπου ο browser ενεργεί ως πελάτης, στέλνοντας αιτήματα (requests) σε έναν web server, ο οποίος, με τη σειρά του, απαντά αποστέλλοντας τους κατάλληλους πόρους, όπως ιστοσελίδες, εικόνες, βίντεο ή άλλα αρχεία.

Η λειτουργία του HTTP στηρίζεται στο πρωτόκολλο TCP για τη διασφάλιση αξιόπιστης μετάδοσης δεδομένων και χρησιμοποιεί τη θύρα 80 για μη κρυπτογραφημένη επικοινωνία. Για λόγους ασφάλειας και προστασίας της ιδιωτικότητας, έχει πλέον καθιερωθεί η χρήση της κρυπτογραφημένης έκδοσης HTTPS, η οποία λειτουργεί μέσω της θύρας 443 και εξασφαλίζει ότι τα δεδομένα που ανταλλάσσονται μεταξύ πελάτη και εξυπηρετητή είναι κρυπτογραφημένα και ασφαλή από παρακολούθηση ή αλλοίωση.

Για παράδειγμα, όταν ένας χρήστης θέλει να δει μια ιστοσελίδα, π.χ. πληκτρολογεί www.paradeigma.com στον browser, ξεκινά μια σειρά από βήματα που γίνονται αυτόματα στο παρασκήνιο:

- **Αίτημα της σελίδας:** Ο browser στέλνει ένα αίτημα με τη μέθοδο GET στον διακομιστή (server) που φιλοξενεί την ιστοσελίδα. Αυτό σημαίνει ότι ζητάει από τον server να του στείλει την αρχική σελίδα (τον κώδικα HTML).
- **Απάντηση του server:** Ο server λαμβάνει το αίτημα και στέλνει πίσω τον κώδικα της σελίδας σε μορφή HTML. Αυτά είναι «οδηγίες» για το πώς πρέπει να εμφανιστεί η σελίδα στον χρήστη.
- **Φόρτωση στοιχείων:** Ο browser διαβάζει τον HTML κώδικα και ανακαλύπτει ότι η σελίδα έχει εικόνες, βίντεο. Για κάθε τέτοιο στοιχείο, ο browser στέλνει και άλλα αιτήματα GET για να τα κατεβάσει από τον server ή από άλλους servers που τα φιλοξενούν.
- **Εμφάνιση σελίδας:** Όταν όλα τα στοιχεία φορτωθούν, ο browser συνθέτει την τελική σελίδα και τη δείχνει στον χρήστη, ο οποίος μπορεί να δει το κείμενο, τις εικόνες, τα βίντεο και να αλληλεπιδράσει με τη σελίδα.
- **Υποβολή δεδομένων:** Αν ο χρήστης συμπληρώσει μια φόρμα, όπως για παράδειγμα να γράψει το όνομά του και να πατήσει «Αποστολή», ο browser στέλνει ένα αίτημα POST στον server, μεταφέροντας τα δεδομένα της φόρμας για επεξεργασία (π.χ. αποθήκευση ή αποστολή email).



Εικόνα 2.3: Επικοινωνία συσκευών με διακομιστή [43]

Επιπλέον, το HTTP είναι ένα πρωτόκολλο χωρίς κατάσταση (stateless), που σημαίνει πως κάθε αίτημα θεωρείται ανεξάρτητο, χωρίς να διατηρείται πληροφορία για προηγούμενες επικοινωνίες. Για να ξεπεραστεί αυτή η περιορισμένη λειτουργικότητα, εφαρμόζονται μηχανισμοί όπως τα cookies και οι συνεδρίες (sessions), που επιτρέπουν την αποθήκευση προσωρινών δεδομένων και την παροχή προσωποποιημένων εμπειριών στους χρήστες. [29]

Η εξέλιξη του HTTP έχει οδηγήσει στην ανάπτυξη νεότερων εκδόσεων, όπως το HTTP/2 και HTTP/3, τα οποία βελτιώνουν σημαντικά την απόδοση και την ασφάλεια της μετάδοσης δεδομένων μέσω μηχανισμών όπως η πολυπλεξία αιτημάτων, η συμπίεση κεφαλίδων και η χρήση UDP (στο HTTP/3) αντί για TCP, μειώνοντας τους χρόνους καθυστέρησης και αυξάνοντας την αποδοτικότητα.

2.6.2 FTP

Το πρωτόκολλο FTP αποτελεί ένα από τα πρώτα και πλέον διαδεδομένα πρωτόκολλα που χρησιμοποιούνται για τη μεταφορά αρχείων μεταξύ υπολογιστών μέσω δικτύων, συμπεριλαμβανομένου και του Διαδικτύου. Η κύρια λειτουργία του FTP είναι να επιτρέπει σε χρήστες ή συστήματα να ανεβάζουν (upload) και να κατεβάζουν (download) αρχεία, καθώς και να διαχειρίζονται καταλόγους αρχείων απομακρυσμένων συστημάτων με έναν απλό και δομημένο τρόπο.

Το FTP λειτουργεί σύμφωνα με το μοντέλο client-server. Ο χρήστης εγκαθιστά στον υπολογιστή του ένα FTP client, ο οποίος συνδέεται σε έναν FTP server που φιλοξενεί τα αρχεία. Αφού πραγματοποιηθεί η σύνδεση, ο χρήστης μπορεί να πλοηγηθεί στους καταλόγους του απομακρυσμένου συστήματος, να κατεβάσει επιλεγμένα αρχεία ή να ανεβάσει αρχεία από τον τοπικό του υπολογιστή στον server. [30]

2.6.3 SMTP

Το SMTP αποτελεί το βασικό πρωτόκολλο που χρησιμοποιείται για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (email) μεταξύ διακομιστών. Η κύρια λειτουργία του είναι η προώθηση των μηνυμάτων από τον υπολογιστή ή τον mail client του αποστολέα σε έναν εξυπηρετητή αλληλογραφίας (mail server), και από εκεί σε άλλους διακομιστές, μέχρι το μήνυμα να φτάσει στον τελικό προορισμό του. Όταν ένας χρήστης στέλνει ένα email μέσω ενός mail client, το μήνυμα μεταφέρεται μέσω SMTP σε έναν εξυπηρετητή ταχυδρομείου, ο οποίος στη συνέχεια προωθεί το μήνυμα στον τελικό παραλήπτη μέσω άλλων πρωτοκόλλων όπως το POP3 ή το IMAP για τη λήψη.

Για παράδειγμα, όταν ένας χρήστης χρησιμοποιεί μια εφαρμογή ηλεκτρονικού ταχυδρομείου, όπως το Outlook ή το Thunderbird, για να στείλει ένα email, το SMTP αναλαμβάνει να μεταφέρει το μήνυμα στον κατάλληλο mail server, ο οποίος στη συνέχεια επικοινωνεί με άλλους διακομιστές μέχρι να το παραδώσει στον server του παραλήπτη. Από εκεί, ο παραλήπτης μπορεί να κατεβάσει ή να συγχρονίσει το μήνυμα με τη συσκευή του μέσω POP3 ή IMAP.

Το SMTP λειτουργεί πάνω από το TCP, εξασφαλίζοντας αξιόπιστη μεταφορά των δεδομένων, και χρησιμοποιεί συνήθως τη θύρα 25 για απλή επικοινωνία μεταξύ διακομιστών, καθώς και τις θύρες 465 ή 587 για ασφαλέστερη αποστολή και αυθεντικοποίηση μέσω κρυπτογραφημένων συνδέσεων (TLS/SSL). [31]

2.6.4 DNS

Το DNS αποτελεί έναν από τους πιο κρίσιμους μηχανισμούς λειτουργίας του Διαδικτύου, παρέχοντας τη δυνατότητα μετάφρασης φιλικών προς τον χρήστη ονομάτων τομέα (όπως www.example.com) σε αριθμητικές διευθύνσεις IP (π.χ. 93.184.216.34). Η αντιστοίχιση αυτή είναι απολύτως απαραίτητη για

την επικοινωνία μεταξύ υπολογιστικών συστημάτων μέσω των πρωτοκόλλων TCP/IP, καθώς η δικτύωση βασίζεται σε αριθμητικές διευθύνσεις. Χωρίς το DNS, οι χρήστες θα έπρεπε να θυμούνται πολύπλοκες και δύσκολες IP διευθύνσεις, γεγονός που θα καθιστούσε τη χρήση του Διαδικτύου εξαιρετικά δυσχερή.

Η αρχιτεκτονική του DNS είναι ιεραρχική και βασίζεται σε ένα κατανεμημένο σύστημα εξυπηρετητών. Στην κορυφή της ιεραρχίας αυτής βρίσκονται οι ριζικοί εξυπηρετητές (Root DNS Servers), οι οποίοι είναι συνολικά δεκατρείς λογικοί εξυπηρετητές (A έως M), τοποθετημένοι γεωγραφικά σε εκατοντάδες φυσικούς κόμβους παγκοσμίως μέσω τεχνικών όπως anycast. Οι εξυπηρετητές αυτοί δεν γνωρίζουν τις IP διευθύνσεις των ιστοσελίδων, αλλά παραπέμπουν στους Top-Level Domain (TLD) διακομιστές, όπως είναι οι .com, .org, .net, .gr κ.ά. Για παράδειγμα, όταν ζητείται η διεύθυνση της ιστοσελίδας www.example.com, ο Root Server θα απαντήσει υποδεικνύοντας τον εξυπηρετητή TLD που είναι υπεύθυνος για τον τομέα .com.

Ο εξυπηρετητής TLD, με τη σειρά του, γνωρίζει ποιοι είναι οι αυθεντικοί εξυπηρετητές (Authoritative DNS Servers) για τον συγκεκριμένο domain και παραπέμπει τον πελάτη εκεί. Οι αυθεντικοί DNS διατηρούν τα λεγόμενα αρχεία ζώνης (zone files), στα οποία περιλαμβάνονται οι ακριβείς αντιστοιχίσεις ονομάτων και διευθύνσεων IP. Σε αυτό το στάδιο, ο αυθεντικός εξυπηρετητής για το example.com επιστρέφει την πληροφορία ότι το www.example.com αντιστοιχεί στην IP διεύθυνση 93.184.216.34.

Η όλη διαδικασία ενεργοποιείται συνήθως από έναν αναδρομικό επιλυτή (Recursive Resolver), ο οποίος λειτουργεί είτε από την πλευρά του ISP, είτε από κάποιο δημόσιο DNS (όπως οι 8.8.8.8 της Google ή 1.1.1.1 της Cloudflare). Ο resolver αυτός λαμβάνει το αρχικό αίτημα από τον υπολογιστή του χρήστη και πραγματοποιεί διαδοχικά όλα τα ερωτήματα προς τους root, TLD και αυθεντικούς εξυπηρετητές, μέχρι να αποκτήσει την τελική IP διεύθυνση. Κατόπιν, αποθηκεύει το αποτέλεσμα τοπικά στην cache για μελλοντική χρήση και το επιστρέφει στο σύστημα που έκανε το αίτημα, επιτρέποντας έτσι την έναρξη επικοινωνίας με τον ζητούμενο εξυπηρετητή μέσω TCP/IP.

Το DNS χρησιμοποιεί το πρωτόκολλο UDP στην θύρα 53 για την πλειονότητα των ερωτημάτων, λόγω της ταχύτητάς του, αλλά μπορεί να χρησιμοποιήσει και TCP στην ίδια θύρα, κυρίως όταν απαιτείται μεταφορά μεγάλων πακέτων ή κατά τη μεταφορά ζωνών μεταξύ εξυπηρετητών (zone transfers).

Υπάρχουν διάφοροι τύποι DNS εγγραφών που χρησιμοποιούνται για διαφορετικές λειτουργίες:

- Η εγγραφή **A** συνδέει ένα hostname με μια IPv4 διεύθυνση.
- Η **CNAME** (Canonical Name) προσδιορίζει ψευδώνυμα (π.χ. blog.example.com → www.example.com).
- Η **MX** δηλώνει τον mail server που χειρίζεται την αλληλογραφία για τον domain.
- Η **NS** δηλώνει ποιοι nameservers είναι υπεύθυνοι για τη ζώνη ενός domain.

Το DNS λειτουργεί ως το απαραίτητο σύστημα μετάφρασης για την καθημερινή χρήση του Διαδικτύου, επιτρέποντας στους χρήστες να αλληλεπιδρούν με διαδικτυακούς πόρους μέσω ονομάτων και όχι αριθμών. Η πολυεπίπεδη και κατανεμημένη του υποδομή εξασφαλίζει καλύτερη δυνατότητα επεκτασιμότητας, ταχύτητας και αξιοπιστίας, ενώ οι σύγχρονες επεκτάσεις ασφαλείας εγγυώνται την προστασία των δεδομένων και των επικοινωνιών που βασίζονται σε αυτό. [32]

2.6.5 Telnet και SSH

Το Telnet και το Secure Shell (SSH) αποτελούν δύο πρωτόκολλα που επιτρέπουν την απομακρυσμένη πρόσβαση σε υπολογιστές, κυρίως μέσω περιβάλλοντος γραμμής εντολών. Παρόλο που εκτελούν παρόμοιες βασικές λειτουργίες, η λειτουργική τους φιλοσοφία και, κυρίως, τα χαρακτηριστικά

ασφαλείας τους διαφέρουν ουσιαστικά, καθιστώντας το SSH τον σύγχρονο και ασφαλή διάδοχο του Telnet.

Το Telnet, που αναπτύχθηκε τη δεκαετία του 1960, σχεδιάστηκε για να προσφέρει ένα βασικό πρωτόκολλο πρόσβασης σε απομακρυσμένα συστήματα, δίνοντας στον χρήστη τη δυνατότητα να εκτελεί εντολές σε έναν απομακρυσμένο υπολογιστή σαν να βρισκόταν τοπικά σε αυτόν. Η σύνδεση πραγματοποιείται μέσω της θύρας 23 και η επικοινωνία γίνεται σε απλό, μη κρυπτογραφημένο κείμενο (plaintext). Αυτό σημαίνει ότι τόσο τα διαπιστευτήρια σύνδεσης (όνομα χρήστη και κωδικός) όσο και οι εντολές που αποστέλλονται είναι ορατές σε οποιονδήποτε έχει τη δυνατότητα να παρακολουθεί το δίκτυο. Λόγω αυτής της σοβαρής αδυναμίας ασφαλείας, το Telnet έχει πλέον σχεδόν πλήρως εγκαταλειφθεί σε σύγχρονα συστήματα, ιδίως σε περιβάλλοντα που απαιτούν ελάχιστα επίπεδα προστασίας. [33]

Αντίθετα, το SSH σχεδιάστηκε με στόχο την ασφαλή απομακρυσμένη διαχείριση συστημάτων, καλύπτοντας τις αδυναμίες του Telnet. Λειτουργεί συνήθως στη θύρα 22 και υποστηρίζει κρυπτογράφηση όλων των δεδομένων που μεταφέρονται μεταξύ του πελάτη και του εξυπηρετητή. Η αυθεντικοποίηση μπορεί να γίνει είτε μέσω παραδοσιακού username/password, είτε για αυξημένη ασφάλεια μέσω δημόσιου και ιδιωτικού κλειδιού (public key authentication), όπου ο διαχειριστής διαθέτει ένα ιδιωτικό κλειδί στον τοπικό του υπολογιστή και το αντίστοιχο δημόσιο κλειδί είναι αποθηκευμένο στον server.

Ένα χαρακτηριστικό παράδειγμα χρήσης είναι η περίπτωση ενός διαχειριστή συστημάτων που επιθυμεί να συνδεθεί σε έναν server για να διαχειριστεί μια βάση δεδομένων ή να κάνει επανεκκίνηση σε μια υπηρεσία. Εισάγοντας την εντολή ssh admin@192.168.1.100 από έναν τοπικό υπολογιστή, ο διαχειριστής καθιερώνει μία ασφαλή, κρυπτογραφημένη σύνδεση προς τον server στη διεύθυνση 192.168.1.100, αποκτώντας απομακρυσμένο περιβάλλον εντολών, μέσω του οποίου μπορεί να αλληλεπιδρά με το σύστημα.

Το SSH, επιπλέον, υποστηρίζει και λειτουργίες όπως η μεταφορά αρχείων μέσω του Secure Copy Protocol (SCP) ή του SSH File Transfer Protocol (SFTP), προσφέροντας έτσι μια ενιαία, κρυπτογραφημένη πλατφόρμα για διαχείριση και μεταφορά δεδομένων. Παράλληλα, επιτρέπει και τη δημιουργία τούνελ (tunneling), δηλαδή τη διοχέτευση άλλων υπηρεσιών μέσω της ασφαλούς σύνδεσης SSH, κάτι που είναι ιδιαίτερα χρήσιμο για παρακάμψεις περιορισμών σε μη ασφαλή δίκτυα. [34]

Ενώ το Telnet αποτέλεσε σημαντικό σταθμό στην ιστορία της απομακρυσμένης πρόσβασης, η παντελής απουσία μηχανισμών ασφάλειας το καθιστά ακατάλληλο για χρήση σε οποιοδήποτε σύγχρονο περιβάλλον. Αντίθετα, το SSH έχει καθιερωθεί ως το πρότυπο πρωτόκολλο για ασφαλή απομακρυσμένη πρόσβαση, συνδυάζοντας ευκολία χρήσης, ισχυρή κρυπτογράφηση και ευελιξία στην αυθεντικοποίηση.

2.6.6 DHCP

Το Dynamic Host Configuration Protocol (DHCP) αποτελεί ένα από τα πιο κρίσιμα πρωτόκολλα για τη διαχείριση της δυναμικής παραμετροποίησης δικτυακών συσκευών σε σύγχρονα δίκτυα. Σχεδιάστηκε ώστε να αυτοματοποιεί τη διαδικασία εκχώρησης παραμέτρων δικτύου σε υπολογιστές και άλλες συσκευές όταν αυτές συνδέονται σε ένα τοπικό δίκτυο, εξαλείφοντας την ανάγκη για χειροκίνητη ρύθμιση διευθύνσεων IP, υποδικτύων, πύλης (gateway) και DNS.

Όταν μια συσκευή όπως ένας υπολογιστής, ένα smartphone ή ένας εκτυπωτής επιχειρεί να συνδεθεί σε ένα δίκτυο που χρησιμοποιεί DHCP, εκκινεί έναν κύκλο ανταλλαγής μηνυμάτων τεσσάρων βημάτων:

1. DHCP Discover: Η συσκευή εκπέμπει ένα μήνυμα broadcast στο δίκτυο ζητώντας πληροφορίες διαμόρφωσης από οποιονδήποτε διαθέσιμο DHCP server.
2. DHCP Offer: Ο DHCP server ανταποκρίνεται με μια προσφορά που περιλαμβάνει μία διαθέσιμη IP διεύθυνση και τις σχετικές παραμέτρους.
3. DHCP Request: Η συσκευή αποδέχεται την προσφορά στέλνοντας ένα αίτημα για τη συγκεκριμένη IP.
4. DHCP Acknowledgement: Ο server επιβεβαιώνει και ολοκληρώνει τη διαδικασία εκχώρησης.

Αυτός ο μηχανισμός είναι ιδιαίτερα χρήσιμος σε περιβάλλοντα με μεγάλο αριθμό συσκευών, όπως πανεπιστημιακά δίκτυα, επιχειρήσεις, δημόσιοι χώροι Wi-Fi, ή ακόμα και στο οικιακό δίκτυο, όπου συχνά πολλαπλές συσκευές συνδέονται και αποσυνδέονται συνεχώς.

Το DHCP βασίζεται στο πρωτόκολλο UDP για την επικοινωνία του. Χρησιμοποιεί τη θύρα 67 στον server και τη θύρα 68 στον πελάτη (client). Επειδή το UDP είναι connectionless, δεν απαιτεί σύσταση συνόδου, γεγονός που διευκολύνει τη γρήγορη και απλή ανταλλαγή πακέτων ανάμεσα σε συσκευές που μόλις μπήκαν στο δίκτυο και δεν έχουν ακόμα διεύθυνση IP.

Πέρα από την εκχώρηση της IP, ένα DHCP server μπορεί επίσης να παραδώσει και άλλες κρίσιμες πληροφορίες, όπως:

- Subnet mask (μάσκα υποδικτύου),
- Default gateway (προεπιλεγμένη πύλη),
- DNS server addresses,
- Lease time, δηλαδή το χρονικό διάστημα για το οποίο ισχύει η εκχωρημένη διεύθυνση IP.

Για παράδειγμα όταν ένας φορητός υπολογιστής συνδέεται σε ένα δημόσιο Wi-Fi σε ένα καφέ, αποστέλλει αυτόματα ένα DHCP Discover πακέτο. Ο router του καταστήματος, ο οποίος λειτουργεί και ως DHCP server, απαντά με μία διεύθυνση IP, π.χ. 192.168.1.35, μαζί με subnet mask 255.255.255.0, πύλη 192.168.1.1 και διευθύνσεις DNS. Ο υπολογιστής τις αποδέχεται και σε δευτερόλεπτα έχει πλήρη συνδεσιμότητα στο δίκτυο.

Σε πιο προηγμένα περιβάλλοντα, όπως εταιρικά δίκτυα, μπορούν να οριστούν και στατικές δεσμεύσεις (static leases) βάσει της MAC διεύθυνσης της συσκευής. Έτσι, κάθε φορά που μια συγκεκριμένη συσκευή συνδέεται στο δίκτυο, λαμβάνει πάντα την ίδια IP, χωρίς όμως να χρειαστεί να τη ρυθμιστεί χειροκίνητα στη συσκευή. [35]

Το DHCP αποτελεί θεμελιώδη μηχανισμό για την αυτόματη, ευέλικτη και αποτελεσματική διαχείριση της IP διαμόρφωσης σε δίκτυα κάθε κλίμακας. Χωρίς αυτό, η σύνδεση νέων συσκευών θα απαιτούσε χρονοβόρα χειροκίνητη διαδικασία, αυξάνοντας την πιθανότητα λαθών και δυσλειτουργιών στο δίκτυο.

2.7 Επίλογος

Η ανάλυση των επιπέδων του μοντέλου TCP/IP αναδεικνύει τη δομημένη και αποτελεσματική προσέγγιση που υιοθετείται για τη διαχείριση της δικτυακής επικοινωνίας σε παγκόσμιο επίπεδο. Κάθε επίπεδο, από το Πρόσβασης Δικτύου μέχρι το Επίπεδο Εφαρμογής, εκπληρώνει συγκεκριμένες λειτουργίες και συνεργάζεται αρμονικά με τα υπόλοιπα, διασφαλίζοντας την αξιόπιστη, ασφαλή και αποδοτική μεταφορά των δεδομένων. Η κατανόηση των μηχανισμών και των πρωτοκόλλων που υλοποιούνται σε κάθε στρώμα είναι ουσιώδης για την εμβάθυνση στις τεχνολογίες του Διαδικτύου, καθώς και για την ανάπτυξη, διαχείριση και βελτιστοποίηση δικτυακών υποδομών και υπηρεσιών. Συνολικά, το μοντέλο TCP/IP παραμένει το θεμέλιο λίθο της σύγχρονης ψηφιακής εποχής, προσφέροντας το πλαίσιο πάνω στο οποίο βασίζεται η παγκόσμια διασύνδεση συσκευών και υπηρεσιών.

Κεφάλαιο 3ο: Κυβερνοασφάλεια

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα εξεταστούν οι βασικές αρχές και οι κρίσιμες έννοιες της κυβερνοασφάλειας, με επίκεντρο το τρίπτυχο CIA ως θεμέλιο της σχεδίασης ασφαλών πληροφοριακών συστημάτων. Αρχικά θα οριστεί κάθε συνιστώσα του μοντέλου CIA και θα αναλυθεί ο τρόπος με τον οποίο διασφαλίζεται η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή διακοπή υπηρεσιών. Στη συνέχεια, θα παρουσιαστούν οι πιο συχνές κατηγορίες απειλών στον κυβερνοχώρο, καθώς και οι βασικοί μηχανισμοί ανίχνευσης, πρόληψης και απόκρισης που εφαρμόζονται για την αντιμετώπισή τους.

3.2 Ορισμός της Κυβερνοασφάλειας

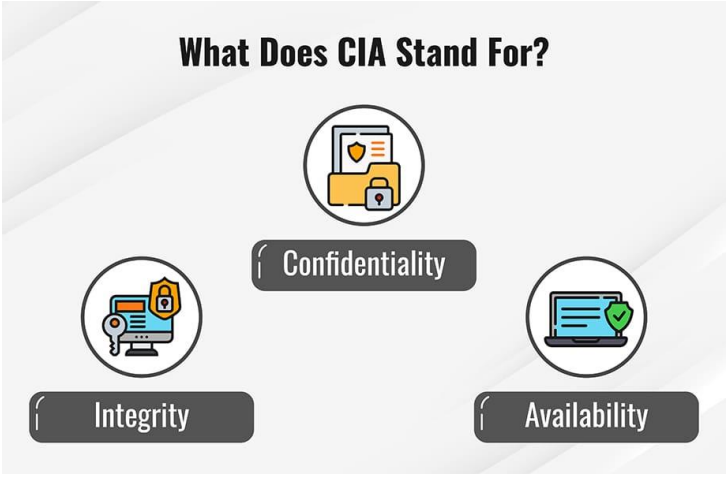
Σε μια εποχή που κυριαρχείται από τον ψηφιακό μετασχηματισμό, η σημασία της ασφάλειας των συστημάτων πληροφοριών δεν ήταν ποτέ πιο κρίσιμη. Η συνεχής εξάπλωση των τεχνολογικών υποδομών, η αυξανόμενη εξάρτηση από το Διαδίκτυο και τις υπηρεσίες cloud, καθώς και η αδιάκοπη ροή δεδομένων σε παγκόσμιο επίπεδο, έχουν δημιουργήσει νέες προκλήσεις και ευπάθειες. Καθημερινά, ιδιώτες, επιχειρήσεις και κυβερνήσεις διαχειρίζονται τεράστιους όγκους ευαίσθητων πληροφοριών, καθιστώντας την ανάγκη για αποτελεσματική προστασία από κυβερνοεπιθέσεις πιο επιτακτική από ποτέ. Η κυβερνοασφάλεια, λοιπόν, δεν αποτελεί απλώς μια επιλογή, αλλά έναν απαραίτητο μηχανισμό διασφάλισης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των ψηφιακών δεδομένων και συστημάτων απέναντι στις συνεχώς εξελισσόμενες απειλές.

Ο όρος κυβερνοασφάλεια αναφέρεται στο σύνολο των ενεργειών ως προς τη προστασία των ψηφιακών συστημάτων από κυβερνοαπειλές και τη αποτελεσματική αποκατάστασή τους μετά από μια επίθεση. Περιλαμβάνει ένα ευρύ φάσμα μέτρων, συμπεριλαμβανομένων εργαλείων υλικού (hardware) και λογισμικού (software), πολιτικών, διαδικασιών και εκπαίδευσης των χρηστών, που στοχεύουν στην άμυνα έναντι των απειλών στον κυβερνοχώρο. [36]

3.3 Βασικές Αρχές της Κυβερνοασφάλειας

Η κυβερνοασφάλεια βασίζεται σε ένα θεμελιώδες σύνολο αρχών που διασφαλίζουν την προστασία των πληροφοριών και των συστημάτων από κακόβουλες ενέργειες, τυχαία σφάλματα και τεχνικές αποτυχίες. Οι αρχές αυτές συνοψίζονται στην τριάδα Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα (Confidentiality, Integrity, Availability - CIA), η οποία αποτελεί το πρότυπο αναφοράς για τη διαχείριση της ασφάλειας των δεδομένων. [37]

Η ισορροπημένη εφαρμογή αυτών των τριών αρχών αποτελεί κρίσιμο στοιχείο της στρατηγικής κυβερνοασφάλειας για κάθε οργανισμό, καθώς η παραβίαση οποιασδήποτε από αυτές μπορεί να οδηγήσει σε σοβαρές επιπτώσεις, όπως διαρροή ευαίσθητων πληροφοριών, αλλοίωση δεδομένων ή διακοπή λειτουργίας κρίσιμων υπηρεσιών.



Εικόνα 3.1: CIA [38]

3.3.1 Εμπιστευτικότητα

Ο ρόλος της Εμπιστευτικότητας στην Κυβερνοασφάλεια είναι να διασφαλίζει ότι τα δεδομένα είναι προσβάσιμα μόνο από εξουσιοδοτημένα άτομα, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση και αποκάλυψή τους. Η εμπιστευτικότητα επιτυγχάνεται μέσω διαφόρων τεχνικών και μηχανισμών ασφαλείας, όπως η κρυπτογράφηση, οι ισχυροί έλεγχοι ταυτότητας/πρόσβασης και η χρήση ασφαλών καναλιών επικοινωνίας.

Η κρυπτογράφηση δεδομένων, τόσο κατά τη μεταφορά (transport encryption) όσο και σε κατάσταση αποθήκευσης (data-at-rest encryption), εξασφαλίζει ότι ακόμα και αν τα δεδομένα υποκλαπούν, θα παραμείνουν μη αναγνώσιμα χωρίς το κατάλληλο κλειδί αποκρυπτογράφησης. Παραδείγματα κρυπτογραφικών πρωτοκόλλων που χρησιμοποιούνται για την προστασία της εμπιστευτικότητας περιλαμβάνουν το Advanced Encryption Standard (AES) για την κρυπτογράφηση αποθηκευμένων δεδομένων και το Transport Layer Security (TLS) για την ασφαλή επικοινωνία μέσω του Διαδικτύου.

Οι έλεγχοι πρόσβασης διαδραματίζουν επίσης σημαντικό ρόλο στη διατήρηση της εμπιστευτικότητας, εφαρμόζοντας μηχανισμούς όπως πολυπαραγοντικός έλεγχος ταυτότητας (Multi-Factor Authentication), Role-Based Access Control (RBAC) και Least Privilege Access, ώστε οι χρήστες να έχουν πρόσβαση μόνο στις πληροφορίες που είναι απαραίτητες για την εκτέλεση των καθηκόντων τους. Παράλληλα, η χρήση ασφαλών Virtual Private Networks (VPN) και η υιοθέτηση τεχνολογιών Zero Trust Architecture (ZTA) ενισχύουν περαιτέρω την προστασία της εμπιστευτικότητας, διασφαλίζοντας ότι κάθε πρόσβαση ελέγχεται και επικυρώνεται δυναμικά.

Η εμπιστευτικότητα αποτελεί κρίσιμη παράμετρο στην προστασία ευαίσθητων πληροφοριών, όπως προσωπικά δεδομένα, οικονομικά αρχεία, ιατρικά ιστορικά και επιχειρηματικά μυστικά, από κακόβουλους φορείς, κυβερνοεγκληματίες ή ακόμα και εσωτερικές απειλές. Σε περιπτώσεις παραβίασης της εμπιστευτικότητας, οι επιπτώσεις μπορεί να είναι σοβαρές, περιλαμβάνοντας διαρροές δεδομένων, απώλειες πνευματικής ιδιοκτησίας, νομικές συνέπειες και σοβαρές οικονομικές ζημιές για επιχειρήσεις και οργανισμούς. Ως εκ τούτου, η διασφάλισή της αποτελεί θεμελιώδη προτεραιότητα για κάθε οργανισμό που χειρίζεται κρίσιμες ή ευαίσθητες πληροφορίες. [37]

3.3.2 Ακεραιότητα

Η ακεραιότητα διασφαλίζει ότι τα δεδομένα παραμένουν ακριβή, συνεπή και αμετάβλητα, εκτός αν υποστούν τροποποιήσεις από εξουσιοδοτημένα μέρη. Η διατήρησή της είναι ζωτικής σημασίας, καθώς

η αλλοίωση ή η μη εξουσιοδοτημένη τροποποίηση πληροφοριών μπορεί να οδηγήσει σε παραπλανητικές αποφάσεις, λειτουργικές δυσλειτουργίες και απώλεια εμπιστοσύνης στα πληροφοριακά συστήματα. Είτε πρόκειται για οικονομικά, ιατρικά ή κρατικά δεδομένα, η ακεραιότητα αποτελεί βασικό παράγοντα που εγγυάται την αξιοπιστία και την ορθότητα των πληροφοριών.

Για τη διασφάλιση της ακεραιότητας των δεδομένων, εφαρμόζονται διάφορες τεχνικές και μέθοδοι που αποτρέπουν την αλλοίωση και διασφαλίζουν την εγκυρότητα των πληροφοριών. Η χρήση αλγορίθμων κατακερματισμού (hashing), όπως SHA-256, επιτρέπει την ανίχνευση οποιασδήποτε μη εξουσιοδοτημένης τροποποίησης, ενώ η κρυπτογράφηση προστατεύει τα δεδομένα από κακόβουλες επιθέσεις. Ιδιαίτερα, η κρυπτογραφία δημοσίου κλειδιού (Public Key Cryptography - PKI) διαδραματίζει σημαντικό ρόλο στην εγγύηση της ακεραιότητας, καθώς επιτρέπει την ασφαλή υπογραφή και επαλήθευση δεδομένων μέσω ψηφιακών υπογραφών. Οι μηχανισμοί ελέγχου πρόσβασης, όπως η πολυεπίπεδη αυθεντικοποίηση και η διαχείριση δικαιωμάτων χρηστών, περιορίζουν την πρόσβαση μόνο σε εξουσιοδοτημένα άτομα. Παράλληλα, η καταγραφή και παρακολούθηση αλλαγών μέσω αρχείων καταγραφής (logs) επιτρέπει τον εντοπισμό ύποπτων δραστηριοτήτων, ενισχύοντας την ανιχνευσιμότητα και την ασφάλεια των πληροφοριακών συστημάτων.

Η ακεραιότητα διαδραματίζει κεντρικό ρόλο σε κρίσιμους τομείς, όπως η ασφάλεια των οικονομικών συναλλαγών, η προστασία ιατρικών αρχείων και η αξιοπιστία των κρατικών δεδομένων. Για παράδειγμα, στις ηλεκτρονικές τραπεζικές συναλλαγές, κάθε τροποποίηση ενός χρηματικού ποσού πρέπει να διασφαλίζεται ότι πραγματοποιείται μόνο από εξουσιοδοτημένα μέρη, ενώ στους ιατρικούς φακέλους οποιαδήποτε αλλοίωση θα μπορούσε να θέσει σε κίνδυνο την υγεία ενός ασθενούς.

Η απώλεια ακεραιότητας μπορεί να έχει σοβαρές συνέπειες, όπως η διάδοση ψευδών πληροφοριών, η πρόκληση οικονομικών ζημιών και η μείωση της εμπιστοσύνης στα πληροφοριακά συστήματα. Ως εκ τούτου, η εφαρμογή αυστηρών πολιτικών ελέγχου αλλαγών, η χρήση τεχνολογιών κατακερματισμού και κρυπτογράφησης, καθώς και η συνεχής παρακολούθηση των δεδομένων αποτελούν κρίσιμες πρακτικές για τη διατήρηση της ακεραιότητας στην κυβερνοασφάλεια. [37]

3.3.3 Διαθεσιμότητα

Ο ρόλος της Διαθεσιμότητας στην Κυβερνοασφάλεια είναι να διασφαλίζει ότι τα δεδομένα, τα πληροφοριακά συστήματα και οι υπηρεσίες είναι συνεχώς προσβάσιμα και λειτουργικά για εξουσιοδοτημένους χρήστες, όταν και όπως απαιτείται. Η διαθεσιμότητα επιτυγχάνεται μέσω της εφαρμογής μηχανισμών ανθεκτικότητας και αποκατάστασης, όπως τα πλεονάζοντα (redundant) συστήματα, οι εφεδρικές λύσεις (backup solutions) και τα σχέδια ανάκαμψης από καταστροφές (Disaster Recovery Plans - DRP). Για παράδειγμα, οι οργανισμοί χρησιμοποιούν εφεδρικούς διακομιστές (failover servers) και συστήματα ισορροπίας φορτίου (load balancers) για τη διανομή της κίνησης σε πολλαπλές υποδομές, ώστε να αποφεύγεται η υπερφόρτωση και η αποτυχία μιας και μόνο πηγής. Παράλληλα, τα συστήματα αδιάλειπτης παροχής ενέργειας (Uninterruptible Power Supplies - UPS) και τα εναλλακτικά κέντρα δεδομένων (data centers) εξασφαλίζουν ότι οι υπηρεσίες παραμένουν διαθέσιμες ακόμη και σε περιπτώσεις διακοπών ρεύματος ή φυσικών καταστροφών.

Επιπλέον, τα τακτικά backup δεδομένων και οι δοκιμές αποκατάστασης διασφαλίζουν ότι, σε περίπτωση κυβερνοεπίθεσης, αποτυχίας λογισμικού ή υλικού, τα κρίσιμα δεδομένα μπορούν να αποκατασταθούν χωρίς απώλειες. Οι οργανισμοί ακολουθούν συχνά τη στρατηγική 3-2-1 backup, η οποία συνιστά τη διατήρηση τριών αντιγράφων ασφαλείας σε δύο διαφορετικά μέσα αποθήκευσης, εκ των οποίων το ένα βρίσκεται εκτός τοποθεσίας, μειώνοντας τον κίνδυνο απώλειας δεδομένων.

Η διαθεσιμότητα είναι εξαιρετικά κρίσιμη σε τομείς όπως η υγεία, οι χρηματοοικονομικές υπηρεσίες και οι κρατικές υποδομές, όπου η διακοπή της πρόσβασης σε πληροφοριακά συστήματα μπορεί να έχει καταστροφικές συνέπειες. Για παράδειγμα, σε ένα νοσοκομείο, η απώλεια πρόσβασης σε ιατρικά αρχεία θα μπορούσε να επηρεάσει άμεσα την περίθαλψη των ασθενών, ενώ σε μια τράπεζα, η διακοπή λειτουργίας των ηλεκτρονικών συναλλαγών μπορεί να οδηγήσει σε οικονομικές απώλειες και μείωση της εμπιστοσύνης των πελατών. [37]

Η διαθεσιμότητα αποτελεί θεμελιώδη πτυχή της κυβερνοασφάλειας και απαιτεί έναν συνδυασμό προληπτικών μέτρων, εφεδρικών λύσεων και στρατηγικών αποκατάστασης για να εξασφαλιστεί η αδιάλειπτη λειτουργία κρίσιμων συστημάτων και η απρόσκοπτη παροχή υπηρεσιών στους εξουσιοδοτημένους χρήστες.

3.4 Συνήθεις Κυβερνοεπιθέσεις

Οι απειλές στον κυβερνοχώρο είναι πολλές και συνεχώς εξελισσόμενες, με νέες μεθόδους και τεχνικές να αναπτύσσονται διαρκώς. Αυτές οι απειλές αποτελούν σοβαρές προκλήσεις για τους επαγγελματίες της κυβερνοασφάλειας, καθώς επηρεάζουν την ασφάλεια των συστημάτων, των δικτύων και των δεδομένων. Η ταχεία εξέλιξη των επιθέσεων απαιτεί συνεχής παρακολούθηση, καινοτόμες λύσεις και δυναμική ανταπόκριση για την προστασία από τους διαρκώς αυξανόμενους κινδύνους. Επίσης, στην εργασία θα αναπτυχθούν οι βασικοί τύποι κυβερνοεπιθέσεων, όπως το Κακόβουλο Λογισμικό, οι επιθέσεις Άρνησης Παροχής Υπηρεσίας, καθώς και το Social Engineering. Αν και ορισμένες από αυτές τις μορφές επιθέσεων μπορεί να θεωρούνται σε κάποιο βαθμό παρωχημένες σε σχέση με τις σύγχρονες μεθόδους, η παρουσίασή τους κρίνεται αναγκαία, καθώς παρέχει ένα πληρέστερο πλαίσιο κατανόησης της εξέλιξης των κυβερνοαπειλών και συμβάλλει στη βαθύτερη ανάλυση των πιο πρόσφατων και σύνθετων τεχνικών.

3.5 Κακόβουλο Λογισμικό (Malware)

Το κακόβουλο λογισμικό, ή malware, αναφέρεται σε οποιοδήποτε λογισμικό σχεδιάζεται με σκοπό την πρόκληση βλάβης, την εκμετάλλευση ή τη διαταραχή των συστημάτων υπολογιστών, των δικτύων και των δεδομένων. Το malware εμπεριέχει διάφορους τύπους, και κάθε ένας από αυτούς έχει τον δικό του τρόπο δράσης και στόχο, αλλά όλοι οι τύποι κοινώς στοχεύουν στη διάπραξη βλαβερών ενεργειών, όπως η υποκλοπή δεδομένων, η καταστροφή αρχείων ή η κατάληψη των συστημάτων για κακόβουλους σκοπούς.

Παρακάτω βρίσκονται οι πιο γνωστοί και σημαντικοί τύποι malware:

Ιοί (Virus): Οι ιοί είναι το πιο γνωστό είδος κακόβουλου λογισμικού. Μολύνουν αρχεία ή προγράμματα και επανεγγράφουν το περιεχόμενό τους για να εκτελούν μη εξουσιοδοτημένες ενέργειες, όπως η καταστροφή δεδομένων ή η διάδοση τους σε άλλους υπολογιστές. Ένας ιός συνήθως μεταδίδεται μέσω συνημμένων αρχείων email ή κακόβουλων ιστοσελίδων.

Worm: Τα worm είναι παρόμοια με τους ιούς, αλλά έχουν τη δυνατότητα να διαδίδονται αυτόνομα μέσω δικτύων χωρίς να απαιτούν την αλληλεπίδραση του χρήστη. Αυτοί οι ιοί μπορούν να προκαλέσουν σοβαρές επιπτώσεις στα δίκτυα, καταναλώνοντας πολύτιμο εύρος ζώνης και προκαλώντας καθυστερήσεις ή διακοπές.

Ransomware: Το ransomware είναι ένα εξαιρετικά επικίνδυνο κακόβουλο λογισμικό που κλειδώνει ή κρυπτογραφεί τα δεδομένα του χρήστη και απαιτεί χρηματική πληρωμή για να τα απελευθερώσει πίσω

στους νόμιμους κάτοχούς του. Η πληρωμή συνήθως πραγματοποιείται μέσω ανώνυμων κρυπτονομισμάτων, αλλά δεν υπάρχει καμία εγγύηση ότι τα δεδομένα θα επιστραφούν στον χρήστη.

Spyware: Το spyware έχει ως στόχο την υποκλοπή προσωπικών δεδομένων χωρίς τη συγκατάθεση του χρήστη. Ενδέχεται να παρακολουθεί τη δραστηριότητα του χρήστη στο διαδίκτυο, να καταγράφει τα την πληκτρολόγηση κειμένου, όπως για παράδειγμα κωδικών πρόσβασης (keylogging) από τον χρήστη ή να παρακολουθεί τις συνήθειες πλοήγησης για να συλλέξει ευαίσθητες πληροφορίες, όπως τραπεζικά στοιχεία.

Trojan (Δούρειος Ίππος): Τα trojan είναι κακόβουλα προγράμματα που προσποιούνται ότι είναι χρήσιμα ή ακίνδυνα, προκειμένου να παραπλανήσουν τους χρήστες να τα κατεβάσουν και να τα εγκαταστήσουν. Μόλις εγκατασταθούν, επιτρέπουν στους επιτιθέμενους να αποκτήσουν απομακρυσμένη πρόσβαση στο σύστημα του χρήστη, δίνοντάς τους τη δυνατότητα να κλέψουν δεδομένα ή να εκτελέσουν άλλες κακόβουλες ενέργειες.

Rootkit: Τα rootkit είναι λογισμικά που προσπαθούν να παραμείνουν κρυμμένα στο σύστημα του χρήστη, αποκρύπτοντας την παρουσία άλλων κακόβουλων προγραμμάτων ή την ίδια τους την ύπαρξη. Μπορούν να εκτελούν δραστηριότητες χωρίς την ανίχνευσή τους, καθιστώντας δύσκολη την αφαίρεσή τους από το σύστημα. [39]

3.5.1 Μέθοδοι μετάδοσης των Malware

Αφού αναλύθηκαν οι κυριότερες κατηγορίες κακόβουλου λογισμικού και ο τρόπος με τον οποίο δρουν, είναι σημαντικό να εξεταστεί το πώς αυτά τα προγράμματα καταφέρνουν να εισχωρήσουν στα πληροφοριακά συστήματα. Η κατανόηση των μηχανισμών διάδοσης του κακόβουλου λογισμικού αποτελεί κρίσιμο βήμα για την ενίσχυση της κυβερνοασφάλειας, καθώς επιτρέπει την υιοθέτηση προληπτικών μέτρων και την ανάπτυξη στρατηγικών ανίχνευσης και αποτροπής. Οι επιτιθέμενοι εκμεταλλεύονται διάφορα μέσα, τεχνικές και ευπάθειες για να εξαπλώσουν το κακόβουλο λογισμικό, συχνά στοχεύοντας την ανθρώπινη αδυναμία και την έλλειψη ενημέρωσης. Στην ενότητα που ακολουθεί, θα παρουσιαστούν οι πιο διαδεδομένοι τρόποι διάδοσης του malware, με στόχο την κατανόηση των σημείων εισόδου και των πρακτικών που ευνοούν την εξάπλωσή του.

Το κακόβουλο λογισμικό διαδίδεται μέσα από διάφορους φορείς, καθιστώντας τη μόλυνση των συστημάτων έναν συνεχή και επικίνδυνο κίνδυνο. Μία από τις πιο συνηθισμένες μεθόδους μετάδοσης είναι μέσω συνημμένων αρχείων σε email, όπου κακόβουλα αρχεία ή σύνδεσμοι μπορούν να προσβάλλουν το σύστημα μόλις ο χρήστης τα ανοίξει. Επιπλέον, οι κακόβουλοι ιστότοποι αποτελούν σοβαρή απειλή, καθώς μπορεί να περιέχουν malware ή να εξαπατούν τους χρήστες ώστε να κατεβάσουν κακόβουλο λογισμικό μέσω ψεύτικων ενημερώσεων και άλλων μεθόδων εξαπάτησης.

Εκτός από τις διαδικτυακές απειλές, η εγκατάσταση μολυσμένου λογισμικού από μη αξιόπιστες ή ανεπίσημες πηγές αποτελεί έναν ακόμη σημαντικό τρόπο διάδοσης του κακόβουλου λογισμικού. Παράλληλα, οι συσκευές του IoT δημιουργούν νέες προκλήσεις ασφαλείας, καθώς συχνά δεν διαθέτουν επαρκή μέτρα προστασίας, γεγονός που τις καθιστά ευάλωτες σε επιθέσεις malware. Έτσι, η ανεπαρκής ασφάλεια αυτών των συσκευών διευκολύνει τη μόλυνση και τη διάδοση κακόβουλου λογισμικού σε ευρύτερα δίκτυα. [41]

3.5.2 Επιπτώσεις των Malware

Πριν εξεταστούν οι επιπτώσεις του κακόβουλου λογισμικού, είναι κρίσιμο να γίνει κατανοητό ότι η επιτυχής μετάδοσή του σε ένα σύστημα δεν αποτελεί απλώς ένα τεχνικό ζήτημα, αλλά το σημείο

εκκίνησης μιας σειράς αρνητικών συνεπειών. Η μόλυνση με malware δημιουργεί τις συνθήκες για την ενεργοποίηση κακόβουλων λειτουργιών που μπορεί να στοχεύουν στη συλλογή δεδομένων, στην κρυπτογράφηση αρχείων για λύτρα, στην παρακολούθηση δραστηριοτήτων ή ακόμη και στη χρήση του συστήματος ως μέρος ενός ευρύτερου δικτύου επιθέσεων. Ανάλογα με το είδος του malware και το επίπεδο πρόσβασης που αποκτά, οι επιδράσεις του μπορούν να κυμαίνονται από ήπιες ενοχλήσεις έως καταστροφικές συνέπειες για την ασφάλεια, την ιδιωτικότητα και την επιχειρησιακή συνέχεια. Ως εκ τούτου, η κατανόηση των επιπτώσεων που επιφέρει η παρουσία malware αποτελεί το επόμενο κρίσιμο βήμα στην πλήρη αποτίμηση των κινδύνων που σχετίζονται με αυτό το είδος κυβερνοαπειλής.

Η παρουσία κακόβουλου λογισμικού στις επιχειρήσεις και την οικονομία μπορεί να έχει καταστροφικές συνέπειες, προκαλώντας σοβαρές οικονομικές απώλειες και διαταράσσοντας τη λειτουργία των οργανισμών. Επιθέσεις ransomware και άλλες μορφές malware οδηγούν συχνά σε διακοπή των επιχειρησιακών δραστηριοτήτων, απώλεια κρίσιμων δεδομένων και υψηλά κόστη αποκατάστασης. Επιπλέον, οι εταιρείες ενδέχεται να αναγκαστούν να καταβάλουν λύτρα για την ανάκτηση των δεδομένων τους, επιβαρύνοντας περαιτέρω τον προϋπολογισμό τους. Παράλληλα, η δυσλειτουργία κρίσιμων υποδομών, όπως τραπεζικά και κυβερνητικά συστήματα, μπορεί να επηρεάσει ολόκληρους τομείς της οικονομίας, δημιουργώντας αλυσιδωτές επιπτώσεις. Η φήμη μιας επιχείρησης πλήττεται σοβαρά μετά από μια κυβερνοεπίθεση, καθώς η απώλεια εμπιστοσύνης των πελατών και των συνεργατών μπορεί να μειώσει τα έσοδα και να επηρεάσει την ανταγωνιστικότητά της στην αγορά.

Σε κοινωνικό επίπεδο, το κακόβουλο λογισμικό μπορεί να επηρεάσει την καθημερινή ζωή των πολιτών, θέτοντας σε κίνδυνο προσωπικά δεδομένα και ιδιωτικές πληροφορίες. Η κλοπή ταυτότητας, η υποκλοπή οικονομικών στοιχείων και η παραβίαση της ιδιωτικότητας αποτελούν σοβαρούς κινδύνους για τους χρήστες του Διαδικτύου, οδηγώντας σε οικονομική και ψυχολογική επιβάρυνση. Επιπλέον, οι κυβερνοεπιθέσεις σε κρίσιμες υπηρεσίες, όπως νοσοκομεία, μέσα μεταφοράς και παρόχους ενέργειας, μπορεί να προκαλέσουν διακοπή ζωτικής σημασίας λειτουργιών, θέτοντας σε κίνδυνο την ασφάλεια και την ευημερία του πληθυσμού. Συνολικά, η εξάπλωση του malware αποτελεί μια αυξανόμενη απειλή με εκτεταμένες επιπτώσεις, καθιστώντας απαραίτητη τη λήψη προληπτικών και αμυντικών μέτρων για την προστασία τόσο των επιχειρήσεων όσο και της κοινωνίας. [40]

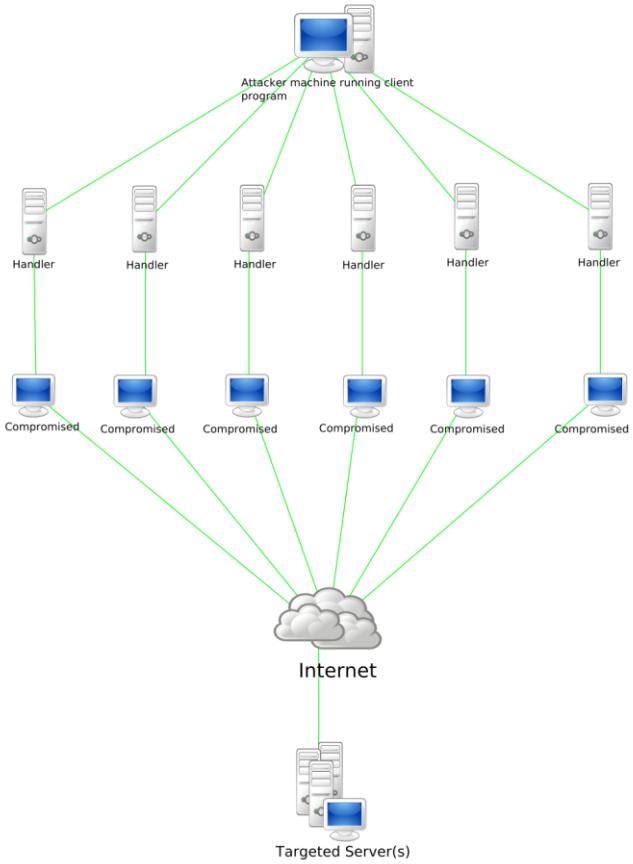
Το κακόβουλο λογισμικό αποτελεί μία από τις πλέον πολυσχιδείς και εξελισσόμενες απειλές στον ψηφιακό κόσμο, επωφελούμενο από ποικίλες τεχνικές μετάδοσης και τεχνολογικές ευπάθειες. Η κατανόηση των τύπων malware, των μηχανισμών διάδοσής τους και των επιπτώσεων που επιφέρουν σε επιχειρήσεις, κρίσιμες υποδομές και την κοινωνία ευρύτερα, είναι καθοριστική για την ανάπτυξη αποτελεσματικών στρατηγικών άμυνας. Μέσω συνδυασμού τεχνικών ελέγχου πρόσβασης, εντοπισμού και πρόληψης, καθώς και συνεχούς επιμόρφωσης των χρηστών, μπορούμε να ελαχιστοποιήσουμε τον κίνδυνο μόλυνσης και να διασφαλίσουμε την επιχειρησιακή συνέχεια και την εμπιστοσύνη των πολιτών στις ψηφιακές υπηρεσίες. Με αυτό το υπόβαθρο, είμαστε έτοιμοι να προχωρήσουμε σε ανάλυση των μεθόδων ανίχνευσης και αντιμετώπισης του malware, αλλά και των βέλτιστων πρακτικών προστασίας.

3.6 Επιθέσεις άρνησης υπηρεσίας (DoS)

Σε αυτή την ενότητα θα εστιάσουμε στις επιθέσεις Άρνησης Παροχής Υπηρεσίας (Denial of Service – DoS) και τις εξελιγμένες εκδοχές τους (Distributed DoS - DDoS). Οι επιθέσεις αυτές στοχεύουν στη διακοπή της ομαλής λειτουργίας ενός δικτυακού πόρου ή υπηρεσίας, κατακλύζοντάς τον με υπερβολικό όγκο αιτημάτων ή εκμεταλλευόμενες αδυναμίες πρωτοκόλλων, με αποτέλεσμα την αδυναμία εξυπηρέτησης νόμιμων χρηστών. Θα αναλύσουμε τον τρόπο δράσης των DoS και DDoS, τα εργαλεία

και τις τεχνικές που χρησιμοποιούν οι επιτιθέμενοι, καθώς και τη σημασία των επιθέσεων στην ασφάλεια επιχειρήσεων, οργανισμών και κρίσιμων υποδομών.

Οι επιθέσεις DoS αποτελούν μία από τις πιο σοβαρές απειλές στον τομέα της κυβερνοασφάλειας, καθώς στοχεύουν στην εξάντληση των πόρων ενός συστήματος, δικτύου ή υπηρεσίας, καθιστώντας το μη διαθέσιμο στους νόμιμους χρήστες. Μέσω τέτοιων επιθέσεων, ένας κακόβουλος παράγοντας μπορεί να προκαλέσει σοβαρές λειτουργικές και οικονομικές συνέπειες σε επιχειρήσεις, οργανισμούς και κυβερνητικές υπηρεσίες, διακόπτοντας την παροχή διαδικτυακών υπηρεσιών και δημιουργώντας σημαντικές καθυστερήσεις στη λειτουργία κρίσιμων υποδομών.



Εικόνα 3.2: Θεωρητική επίθεση DoS [83]

Οι επιθέσεις DoS βασίζονται στη μαζική αποστολή αιτημάτων ή δεδομένων προς έναν στόχο, με σκοπό την υπερφόρτωση των πόρων του και τη διακοπή της λειτουργίας του. Ο επιτιθέμενος χρησιμοποιεί μια μεμονωμένη συσκευή ή σύστημα για να επιτύχει αυτόν τον στόχο, εκμεταλλευόμενος διάφορες τεχνικές:

Flood Attacks, όπου ο επιτιθέμενος στέλνει έναν τεράστιο αριθμό αιτημάτων σύνδεσης (όπως TCP SYN Flood ή UDP Flood), με αποτέλεσμα την εξάντληση των διαθέσιμων πόρων του συστήματος.

Amplification Attacks, οι οποίες εκμεταλλεύονται υπηρεσίες όπως DNS και NTP, ώστε να αυξήσουν σημαντικά την ένταση της κακόβουλης κίνησης προς τον στόχο, δημιουργώντας μια δυσανάλογα μεγάλη επιβάρυνση.

Application Layer Attacks, που επικεντρώνονται σε συγκεκριμένες εφαρμογές ή υπηρεσίες (όπως HTTP GET/POST Flood) και στοχεύουν στην αχρήστευσή τους μέσω υπερφόρτωσης.

Οι επιθέσεις DoS μπορούν να προκαλέσουν προσωρινή ή και μακροχρόνια διακοπή των υπηρεσιών, δημιουργώντας προβλήματα τόσο στους παρόχους όσο και στους τελικούς χρήστες. Επειδή η πηγή της επίθεσης είναι μοναδική, είναι συχνά πιο εύκολο να εντοπιστεί και να μετριαστεί, για παράδειγμα μέσω φιλτραρίσματος της κακόβουλης κυκλοφορίας ή αποκλεισμού της IP του επιτιθέμενου. [42]

3.6.1 DDos

Καθώς οι επιθέσεις DoS εκμεταλλεύονται τη συγκεντρωμένη αποστολή όγκου αιτημάτων από μία μόνο πηγή, η εξέλιξή τους προς τις κατανεμημένες επιθέσεις DDoS προσθέτει ένα επιπλέον επίπεδο πολυπλοκότητας και ισχύος. Οι επιθέσεις DDoS αποτελούν μια πιο προηγμένη και ισχυρή εκδοχή των επιθέσεων DoS. Αντί να προέρχεται η επίθεση από μία μόνο συσκευή, οι DDoS επιθέσεις αξιοποιούν μεγάλο αριθμό μολυσμένων συστημάτων (botnets), τα οποία ενεργούν συντονισμένα και εξαπολύουν μαζική επίθεση στον στόχο από πολλαπλές γεωγραφικές τοποθεσίες.

Η κατανεμημένη φύση των DDoS επιθέσεων καθιστά ιδιαίτερα δύσκολη την αντιμετώπισή τους, καθώς η κακόβουλη κίνηση προέρχεται από πολλές διαφορετικές πηγές, καθιστώντας αναποτελεσματικό τον αποκλεισμό μιας μεμονωμένης IP. Επιπλέον, τέτοιες επιθέσεις συχνά χρησιμοποιούνται ως μέσο συγκάλυψης άλλων κακόβουλων ενεργειών, όπως παραβιάσεις δεδομένων ή επιθέσεις ransomware. [44]

3.7 Social Engineering

Το Social Engineering αποτελεί μια από τις πιο επικίνδυνες και εκλεπτυσμένες μορφές κυβερνοεπίθεσης, καθώς εκμεταλλεύεται αδυναμίες που σχετίζονται με τον ανθρώπινο παράγοντα παρά με τεχνικές αδυναμίες των συστημάτων. Αντί να εξαρτάται από τεχνικές υποκλοπής ή κακόβουλου λογισμικού, το social engineering στοχεύει στην εξαπάτηση των ατόμων, παραπλανώντας τα έτσι ώστε να αποκαλύψουν ευαίσθητες πληροφορίες ή να πραγματοποιήσουν ενέργειες που θα επιτρέψουν στον επιτιθέμενο να αποκτήσει πρόσβαση σε συστήματα ή δεδομένα.

Η μέθοδος αυτή βασίζεται στην εκμετάλλευση της εμπιστοσύνης και των ανθρώπινων αντιδράσεων, όπως η ανάγκη για βοήθεια ή η υπερβολική εμπιστοσύνη προς έναν άγνωστο. Οι επιτιθέμενοι συχνά προσποιούνται ότι είναι κάποιο άτομο ή οργανισμός στον οποίο το στόχο εμπιστεύεται, όπως ένας υπάλληλος τεχνικής υποστήριξης, συνάδελφος ή κάποιος από τη διοίκηση. Ενδέχεται, επίσης, να δημιουργήσουν τεχνητούς εκφοβισμούς, όπως η "επείγουσα ανάγκη" για έναν κωδικό πρόσβασης, ή ακόμη και να στείλουν προσκλήσεις για "επείγοντα" έργα ή ενημερώσεις που περιλαμβάνουν κακόβουλο λογισμικό.

Η πρόληψη του social engineering απαιτεί ένα συνδυασμό εκπαίδευσης και επίγνωσης. Οι οργανισμοί πρέπει να εκπαιδεύουν τους υπαλλήλους τους να αναγνωρίζουν τις κοινές τεχνικές εξαπάτησης και να διασφαλίζουν ότι ακολουθούν αυστηρές διαδικασίες επαλήθευσης πριν αποκαλύψουν προσωπικές ή εμπιστευτικές πληροφορίες. Επίσης, η ανάπτυξη τεχνικών ασφαλείας, όπως η χρήση πολυπαραγοντικής αυθεντικοποίησης και η παρακολούθηση ύποπτων δραστηριοτήτων, μπορεί να μειώσει την πιθανότητα επιτυχίας αυτών των επιθέσεων. [84]

3.7.1 Phising

Το Phishing αποτελεί μία υποκατηγορία του Social Engineering η οποία είναι από τις πιο συχνές και αποτελεσματικές τεχνικές κυβερνοεπίθεσης, που στοχεύει στην εξαπάτηση των χρηστών ώστε να αποκαλύψουν ευαίσθητες πληροφορίες. Οι επιτιθέμενοι μεταμφιέζονται ως αξιόπιστες οντότητες μέσω ψεύτικων email, μηνυμάτων ή ιστοσελίδων, προκειμένου να πείσουν τα θύματα να παραχωρήσουν προσωπικά δεδομένα, όπως διαπιστευτήρια σύνδεσης, στοιχεία τραπεζικών λογαριασμών ή κωδικούς πρόσβασης.

Η μέθοδος αυτή χρησιμοποιείται συχνά ως αρχικό στάδιο για μεγαλύτερες κυβερνοεπιθέσεις. Μέσω της απόκτησης πρόσβασης σε κρίσιμους λογαριασμούς, οι επιτιθέμενοι μπορούν να εγκαταστήσουν κακόβουλο λογισμικό (malware), να πραγματοποιήσουν επιθέσεις ransomware ή να διεισδύσουν περαιτέρω σε δίκτυα οργανισμών, αποκτώντας πρόσβαση σε απόρρητες πληροφορίες. Επίσης, οι επιθέσεις phishing μπορούν να αξιοποιηθούν για τη διανομή trojans που παρέχουν στους εισβολείς συνεχή πρόσβαση σε συστήματα, επιτρέποντας τη μακροχρόνια εκμετάλλευσή τους.

Το phishing δεν αποτελεί μόνο μια μεμονωμένη απειλή αλλά λειτουργεί ως ένας βασικός μηχανισμός που διευκολύνει πιο σύνθετες και καταστροφικές κυβερνοεπιθέσεις, καθιστώντας την εκπαίδευση και την ευαισθητοποίηση των χρηστών κρίσιμο παράγοντα για την προστασία από τέτοιες επιθέσεις. [85]

3.8 Επίλογος

Ολοκληρώνοντας το κεφάλαιο για την κυβερνοασφάλεια, καθίσταται σαφές ότι η προστασία των πληροφοριακών συστημάτων αποτελεί θεμελιώδη προτεραιότητα στη σύγχρονη ψηφιακή εποχή. Ο ορισμός της κυβερνοασφάλειας ανέδειξε τη σημασία της ολιστικής προσέγγισης που περιλαμβάνει τεχνικά μέτρα, πολιτικές, διαδικασίες και εκπαίδευση χρηστών, με σκοπό την άμυνα απέναντι σε συνεχώς εξελισσόμενες απειλές. Επιπλέον, η παρουσίαση της αρχιτεκτονικής CIA ανέδειξε το πλαίσιο πάνω στο οποίο στηρίζεται κάθε αποτελεσματική στρατηγική προστασίας. Παράλληλα, οι κυβερνοεπιθέσεις εξελίσσονται συνεχώς και περιλαμβάνουν ποικιλία τεχνικών και μεθόδων. Επιθέσεις όπως το malware, οι επιθέσεις DDoS, το social engineering και το phishing αξιοποιούν διαφορετικές αδυναμίες των συστημάτων και των χρηστών, θέτοντας σε κίνδυνο την ασφάλεια και ακεραιότητα των δεδομένων. Η κατανόηση αυτών των επιθέσεων είναι απαραίτητη για την ανάπτυξη αποδοτικών στρατηγικών άμυνας.

Κεφάλαιο 4ο: Penetration Testing

4.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί η έννοια του penetration testing, δηλαδή της συστηματικής προσομοίωσης επιθέσεων σε ένα πληροφοριακό σύστημα με σκοπό την αξιολόγηση της ασφάλειάς του. Θα οριστεί τι ακριβώς συνιστά ένα penetration testing, θα αναδειχθούν οι σκοποί και τα οφέλη της και θα εξηγηθεί γιατί αποτελεί απαραίτητο εργαλείο για την προστασία κρίσιμων υποδομών, τη συμμόρφωση με πρότυπα και κανονισμούς, αλλά και τη διασφάλιση της εμπιστοσύνης των χρηστών και των πελατών. Μέσα από τη μεθοδολογική θεώρηση του penetration testing, ο αναγνώστης θα κατανοήσει πώς η προληπτική αξιολόγηση της ασφάλειας συμβάλλει στην ελαχιστοποίηση των κινδύνων και στην ενίσχυση της συνολικής κυβερνοασφάλειας ενός οργανισμού.

4.2 Ορισμός του Penetration Testing

Σύμφωνα με το National Institute of Standards and Technology (NIST), το penetration testing ορίζεται ως η στοχευμένη προσπάθεια προσομοίωσης επιθέσεων σε ένα πληροφοριακό σύστημα προκειμένου να αξιολογηθεί η ασφάλειά του, η ανίχνευση ευπαθειών και η εκτίμηση της δυνατότητας εκμετάλλευσής τους από κακόβουλους παράγοντες. [45]

Με άλλα λόγια, πρόκειται για μια ελεγχόμενη, συστηματική διαδικασία κατά την οποία εξειδικευμένοι επαγγελματίες αναλαμβάνουν να «χτυπήσουν» το σύστημά σας με τους ίδιους ακριβώς τρόπους που θα επιχειρούσαν οι επίδοξοι επιτιθέμενοι. Στην πράξη, ο penetration tester εξετάζει κάθε πιθανό κανάλι εισόδου. Ελέγχει κωδικούς πρόσβασης για ευκολία αποκωδικοποίησης, αναζητά λογισμικά που δεν έχουν λάβει ενημερώσεις ασφαλείας, ελέγχει παραμέτρους διακομιστών και βάσεων δεδομένων για λάθη διαμόρφωσης και καταγράφει την αντίδραση των υπαλλήλων σε πιθανά σενάρια phishing. Με αυτόν τον τρόπο προσομοιώνεται το πλήρες φάσμα των επιθέσεων, από απλές προσπάθειες αποκρυπτογράφησης έως πολύπλοκες αλυσίδες εκμετάλλευσης πολλαπλών ευπαθειών. Το τελικό προϊόν του penetration testing είναι μια αναφορά που καταγράφει αναλυτικά τις ευπάθειες, τον τρόπο εκμετάλλευσής τους και τις προτεινόμενες διορθωτικές ενέργειες, ώστε ο οργανισμός να ενισχύσει έγκαιρα την άμυνά του και να αποτρέψει πραγματικές κυβερνοεπιθέσεις.

4.3 Ο Ρόλος των Penetration Testing στην Ενίσχυση της Ασφάλειας

Η διενέργεια τακτικών penetration testing αποτελεί αναπόσπαστο στοιχείο της σύγχρονης στρατηγικής κυβερνοασφάλειας για κάθε επιχείρηση. Καταρχάς, η πρόληψη μιας επιτυχημένης παραβίασης μέσω penetration testing μπορεί να εξοικονομήσει στην εταιρεία δεκάδες ή ακόμη και εκατοντάδες εκατομμύρια ευρώ, δεδομένου ότι το μέσο κόστος μιας παραβίασης δεδομένων ανέρχεται σήμερα σε 4,4 εκατ. USD. Με τον τρόπο αυτό, το αρχικό κόστος ενός penetration testing (το οποίο συχνά κυμαίνεται μεταξύ 5 - 35 χιλ. USD) αποδεικνύεται εξαιρετικά αποδοτικό, καθώς μειώνει δραματικά τον κίνδυνο υπέρογκων δαπανών αποκατάστασης, λύτρων και δικαστικών εξόδων. [40]

Επιπλέον, τα penetration testing συμβάλλουν στην ελαχιστοποίηση των διακοπών λειτουργίας και της διακοπής των κρίσιμων υπηρεσιών. Με τον εντοπισμό και την έγκαιρη διόρθωση ευπαθειών, αποφεύγεται η αδυναμία εξυπηρέτησης νόμιμων χρηστών, που μπορεί να οδηγήσει σε σημαντική απώλεια εσόδων και υποβάθμιση της εμπιστοσύνης των πελατών. Παράλληλα, η τακτική εκτέλεση τέτοιων ελέγχων μειώνει το κόστος συμμόρφωσης με πρότυπα ασφαλείας (General Data Protection

Regulation - GDPR, Payment Card Industry Data Security Standard - PCI-DSS κ.ά.) και επιτρέπει στην επιχείρηση να διαπραγματευτεί ευνοϊκότερους όρους με τις ασφαλιστικές εταιρείες.

Η επένδυση στο penetration testing δεν είναι μόνον ένα τεχνικό μέτρο, αλλά και ισχυρό εργαλείο διατήρησης φήμης και ανταγωνιστικότητας. Η δέσμευση της διοίκησης στην ασφάλεια των δεδομένων αποτυπώνεται στην εναργή αξιολόγηση ευπαθειών και στην υλοποίηση διορθωτικών ενεργειών, ενισχύοντας την εμπιστοσύνη των συνεργατών και των τελικών χρηστών. Συνολικά, το penetration testing αναδεικνύεται ως μία στρατηγική επένδυση με υψηλό δείκτη απόδοσης (Return Of Investment - ROI), προστατεύοντας τόσο την επιχειρησιακή συνέχεια όσο και την εικόνα της εταιρείας απέναντι στις διαρκώς εξελισσόμενες κυβερνοαπειλές.

4.4 Κατηγορίες των Hacker

Μετά την επισήμανση της στρατηγικής αξίας των penetration testing για την πρόληψη οικονομικών ζημιών, τη διασφάλιση της διαθεσιμότητας υπηρεσιών και τη διατήρηση της φήμης μιας επιχείρησης, κρίνεται απαραίτητο να εξεταστεί ποιοι είναι οι ίδιοι οι εκτελεστές αυτών των ελέγχων. Οι «χακερ» δεν είναι όλοι ίδιοι. Ανάλογα με τα κίνητρα, την ηθική και το νομικό πλαίσιο δράσης τους διακρίνονται σε white hat, grey hat και black hat. Η κατανόηση των διαφορών αυτών των κατηγοριών επιτρέπει στον αναγνώστη να εξακριβώσει ποιοι εξ αυτών αναλαμβάνουν νόμιμα και υπεύθυνα τα penetration test και ποιες πρακτικές θα πρέπει να αποφεύγονται.

Οι white hat hackers είναι οι επαγγελματίες της κυβερνοασφάλειας που χρησιμοποιούν τις δεξιότητές τους για την άμυνα των πληροφοριακών συστημάτων. Κύριο κίνητρό τους είναι η προστασία των δικτύων και των δεδομένων από κακόβουλες επιθέσεις και ενεργούν νόμιμα, με τη ρητή άδεια των ιδιοκτητών των συστημάτων και συχνά εργάζονται ως σύμβουλοι ασφαλείας ή εσωτερικά σε οργανισμούς. Σ’ αυτούς ανήκουν οι ίδιοι οι penetration tester, αφού η εκτέλεση ενός pentest απαιτεί την εξουσιοδότηση και τη δεοντολογική δέσμευση που εκπροσωπούν οι white hats.

Οι grey hat hackers κινούνται σε μια γκρίζα ζώνη ανάμεσα στο νόμιμο και το παράνομο. Τυπικά, αναζητούν ευπάθειες χωρίς προηγούμενη εξουσιοδότηση, αλλά δεν έχουν κακόβουλες προθέσεις και συχνά αποκαλύπτουν τις αδυναμίες στους αρμόδιους φορείς ή στον ιδιοκτήτη του συστήματος, χωρίς όμως να ζητούν αμοιβή ή να προκαλούν ζημιά. Τα κίνητρά τους είναι κυρίως η αναγνώριση της ικανότητάς τους και η συνεισφορά στην ασφάλεια μέσα από μηχανισμούς αυτοεκπαίδευσης και κοινωνικής αναγνώρισης.

Οι black hat hackers είναι οι πραγματικά κακόβουλοι επιτιθέμενοι. Χρησιμοποιούν τις τεχνικές τους για προσωπικό κέρδος ή δολιοφθορά (π.χ. κλοπή δεδομένων, εγκατάσταση ransomware, δολιοφθορά υποδομών) χωρίς καμία άδεια ή ηθικούς φραγμούς. Τα κίνητρά τους μπορεί να περιλαμβάνουν οικονομικό όφελος, βιομηχανική κατασκοπεία ή απλώς πρόκληση ζημιάς.

Μόνο οι white hat hackers υλοποιούν συστηματικά τα penetration test, καθώς πληρούν τα ηθικά, νομικά και τεχνικά κριτήρια για τη διεξαγωγή penetration testing με άδεια και προς όφελος των οργανισμών. Οι grey hat μπορούν να πραγματοποιήσουν ad-hoc αναζητήσεις ευπαθειών, αλλά χωρίς το εύρος, τη μεθοδολογία και τη νομιμότητα των επίσημων pentests, ενώ οι black hat αποκλείονται πλήρως λόγω των κακόβουλων προθέσεών τους. [46]

4.5 Τα Στάδια του Penetration Testing

Αρχικά, η φάση του Information Gathering (Συλλογή Πληροφοριών) επιτρέπει στον ελεγκτή να αποκτήσει πολύτιμη γνώση για τον στόχο, με σκοπό τη χαρτογράφηση της επιφάνειας επίθεσης.

Ακολουθεί η Vulnerability Detection (Ανίχνευση Ευπαθειών), όπου τα ευρήματα της πρώτης φάσης αξιοποιούνται για τον εντοπισμό αδυναμιών που ενδέχεται να επιτρέψουν την είσοδο στο σύστημα. Στη συνέχεια, το Exploitation (Εκμετάλλευση) επιχειρεί να αποδείξει αν τις ευπαθειες αυτές μπορεί ο penetration tester να τις εκμεταλευτεί, ενώ οι φάσεις Persistence (Διατήρηση Πρόσβασης) και Privilege Escalation (Αναβάθμιση Δικαιωμάτων) εξετάζουν τον τρόπο με τον οποίο ένας εισβολέας θα μπορούσε να εδραιώσει την παρουσία του στο σύστημα και να αποκτήσει αυξημένα προνόμια.

Μέσα από τη λεπτομερή παρουσίαση κάθε σταδίου, αναδεικνύεται η σημασία του μεθοδικού σχεδιασμού και της τεχνικής κατάρτισης που απαιτούνται για ένα πλήρες και αξιόπιστο penetration test.

4.6 Συλλογή Πληροφοριών (Πρώτο Στάδιο)

Το στάδιο του Συλλογή Πληροφοριών (Information Gathering) αποτελεί το πρώτο και θεμελιώδες στάδιο σε κάθε διαδικασία penetration testing, καθώς θέτει τις βάσεις για όλα τα επόμενα βήματα. Σε αυτό το στάδιο, ο penetration tester επικεντρώνεται στη συγκέντρωση όσο το δυνατόν περισσότερων πληροφοριών για τον στόχο, χωρίς να έχει ακόμη προχωρήσει σε άμεσες ενέργειες εκμετάλλευσης. Η κατανόηση της υποδομής, των τεχνολογιών και των πιθανών αδυναμιών ενός οργανισμού ξεκινά με την επιμελή παρατήρηση και χαρτογράφηση του εξωτερικού του αποτυπώματος.

Η ενότητα αυτή διακρίνεται σε δύο επιμέρους προσεγγίσεις την Παθητική Συλλογή Πληροφοριών (Passive Information Gathering / OSINT - Open Source Intelligence) και την Ενεργή Συλλογή Πληροφοριών (Active Information Gathering / Enumeration).

Η σαφής διάκριση και η κατανόηση των δύο αυτών προσεγγίσεων είναι απαραίτητη για την ορθή αξιολόγηση της επιφάνειας επίθεσης και τη στρατηγική καθοδήγηση των επόμενων σταδίων του ελέγχου ασφαλείας.

4.6.1 Παθητική Συλλογή Πληροφοριών

Η παθητική συλλογή βασίζεται σε πληροφορίες που είναι διαθέσιμες δημόσια, χωρίς καμία αλληλεπίδραση με τα συστήματα του στόχου, γεγονός που την καθιστά “αθόρυβη” και μη ανιχνεύσιμη. Αυτό σημαίνει ότι οι ενέργειες του penetration tester παραμένουν «αόρατες» στα συστήματα εντοπισμού εισβολών (Intrusion Detection Systems - IDS), καθώς δεν δημιουργείται κανένα ίχνος στο δίκτυο του οργανισμού. Ουσιαστικά, ο ειδικός αξιοποιεί πόρους που βρίσκονται ήδη διαθέσιμοι στο δημόσιο περιβάλλον του διαδικτύου για να συλλέξει δεδομένα που μπορεί να είναι εξαιρετικά χρήσιμα για τα επόμενα στάδια της αξιολόγησης ασφαλείας.

Ο όρος OSINT αναφέρεται ακριβώς σε αυτό το είδος συλλογής, τη χρήση δημόσια προσβάσιμων δεδομένων από ελεύθερες ή νόμιμα διαθέσιμες πηγές. Οι πληροφορίες αυτές μπορεί να προέρχονται από ένα ευρύ φάσμα μέσων, όπως μηχανές αναζήτησης, αρχεία DNS, καταχωρήσεις WHOIS για ονόματα domain, online βάσεις δεδομένων διαρροών (data breach databases), κοινωνικά δίκτυα, κυβερνητικά μητρώα και άλλες διαδικτυακές πλατφόρμες. Ο στόχος είναι να συγκεντρωθεί κάθε είδους τεχνική ή μη πληροφορία που μπορεί να αποκαλύψει στοιχεία για την τεχνολογική υποδομή, τη γεωγραφική θέση, τις συνήθειες προσωπικού ή πιθανές αδυναμίες ασφάλειας του οργανισμού-στόχου.

Σημαντική πτυχή του OSINT αποτελεί η ανάλυση των ψηφιακών αποτυπωμάτων (digital footprint) μιας επιχείρησης ή ατόμου. Μέσα από τεχνικές αναζήτησης metadata σε αρχεία που έχουν δημοσιευθεί διαδικτυακά, ανάλυση των email addresses που χρησιμοποιούνται, αναζήτηση ιστορικών εγγραφών σε αρχεία DNS (DNS history), καθώς και αξιοποίηση εργαλείων όπως το Shodan, το Censys ή το theHarvester, ένας penetration tester μπορεί να δημιουργήσει ένα πολύ ακριβές προφίλ του στόχου.

Το πλεονέκτημα της παθητικής συλλογής πληροφοριών έγκειται στο γεγονός ότι επιτρέπει την προετοιμασία για μια πιο στοχευμένη και αποτελεσματική επίθεση (ή έλεγχο, στην περίπτωση του penetration testing), χωρίς να προκαλεί υποψίες ή να παραβιάζει νομικά όρια. Παράλληλα, συμβάλλει στη χαρτογράφηση των πιθανών επιφανειών επίθεσης, εστιάζοντας σε δημόσια προσβάσιμες πληροφορίες τις οποίες θα μπορούσε να εκμεταλλευτεί και ένας κακόβουλος χρήστης. [47]

Η φάση του Passive Information Gathering και το OSINT αποτελούν ένα ισχυρό εργαλείο για τον εντοπισμό ευπαθειών και την κατανόηση της έκθεσης ενός οργανισμού στο διαδίκτυο. Παρά την «αθόρυβη» φύση τους, οι τεχνικές αυτές προσφέρουν συχνά εξαιρετικά πολύτιμες πληροφορίες που μπορούν να καθορίσουν την πορεία και την επιτυχία ενός penetration test.

4.6.2 Ενεργή Συλλογή Πληροφοριών

Αντίθετα, η ενεργή συλλογή περιλαμβάνει άμεση επικοινωνία με τις υποδομές του στόχου, αποσκοπώντας στον εντοπισμό υπηρεσιών, θυρών και παραμέτρων συστημάτων που θα μπορούσαν να αξιοποιηθούν για τα περαιτέρω στάδια του penetration testing. Η ενεργή συλλογή πληροφοριών περιλαμβάνει όλες τις μεθόδους όπου ο penetration tester αλληλεπιδρά άμεσα με τους πόρους του στόχου, προκειμένου να αποκαλύψει λεπτομέρειες που δεν είναι διαθέσιμες μέσω παθητικής έρευνας. Σε αυτή τη φάση, ο penetration tester χρησιμοποιεί εργαλεία και τεχνικές σάρωσης (scanning) και enumeration για να χαρτογραφήσει ενεργές υπηρεσίες, ανοιχτές θύρες (ports), πρωτόκολλα που «τρέχουν» σε κάθε θύρα, εκδόσεις λογισμικού και πιθανές διαρροές αυτόματης πληροφορίας (banner grabbing).

Το enumeration αποτελεί το πιο στοχευμένο κομμάτι της ενεργής συλλογής. Εδώ ο penetration tester επιχειρεί να αντλήσει συγκεκριμένα δεδομένα από τις υπηρεσίες του στόχου όπως ονόματα χρηστών, λίστες με συνδεδεμένους λογαριασμούς, Server Message Block (SMB) shares σε αρχεία και εκτυπωτές, πληροφορίες DNS, Lightweight Directory Access Protocol (LDAP) records, Simple Network Management Protocol (SNMP) community strings και άλλες κρίσιμες παραμέτρους που μπορούν να χρησιμοποιηθούν για παραπάνω στάδια επίθεσης. Η διαδικασία ξεκινά με σάρωση θυρών (π.χ. TCP SYN scan) και συνεχίζεται με fingerprinting εργαλείων (όπως Nmap OS detection), ενώ το enumeration διευρύνει τα ευρήματα με εντοπισμό λογαριασμών (π.χ. μέσω SMB, SNMP ή LDAP queries) και άντληση πληροφοριών απευθείας από υπηρεσίες.

Στην πράξη, η ενεργή συλλογή και το enumeration απαιτούν προσοχή ώστε να μην προκαλέσουν αρνητικές επιπτώσεις στη διαθεσιμότητα της υπηρεσίας (π.χ. μεγάλοι αριθμοί αιτημάτων μπορεί να επιβραδύνουν ή ακόμη και να καταρρεύσουν τον στόχο). Παράλληλα, καταγράφονται με ακρίβεια όλα τα βήματα, οι εντολές και τα αποτελέσματα, ώστε να μπορούν να αναπαραχθούν, να τεκμηριωθούν και να αξιολογηθούν τόσο τεχνικά όσο και νομικά.

Μετά το πέρας του enumeration, ο penetration tester διαθέτει ένα πλήρες «χάρτη» των πόρων και των αδυναμιών του συστήματος, έτοιμο για τα επόμενα στάδια (Exploitation, Persistence, Privilege Escalation), όπου οι πληροφορίες αυτές θα χρησιμοποιηθούν για απόπειρες περεταίτω εμβάθυνσης στο στόχο και ενίσχυση της σφαιρικής ασφάλειας. [45]

4.7 Vulnerability Detection (Δεύτερο Στάδιο)

Το επόμενο στάδιο μετά τη Συλλογή Πληροφοριών είναι η Ανίχνευση Ευπαθειών (Vulnerability Detection), όπου οι πρώτες γενικές εικόνες για το σύστημα μετατρέπονται σε στοχευμένα τεχνικά δεδομένα. Στο στάδιο του Vulnerability Detection στοχεύεται ο εντοπισμός και την καταγραφή των αδυναμιών που μπορεί να υπάρχουν στο εξεταζόμενο σύστημα. Η διαδικασία αυτή χωρίζεται σε δύο

επιμέρους βήματα. Πρώτον, η σάρωση (scanning) των συστημάτων για την αναγνώριση του εγκατεστημένου λογισμικού και των αντίστοιχων εκδόσεών του (μία ενέργεια που αποκαλύπτει με ακρίβεια ποια πακέτα, υπηρεσίες ή πλατφόρμες λειτουργούν στον στόχο). Δεύτερον, το ταίριασμα αυτών των εκδόσεων με τα καταγεγραμμένα Common Vulnerabilities and Exposures (CVE), προκειμένου να επιβεβαιωθεί αν υπάρχουν γνωστές ευπάθειες. Το δεύτερο βήμα μπορεί να υλοποιηθεί είτε χειροκίνητα (με αναζήτηση σε επίσημες βάσεις δεδομένων) είτε αυτοματοποιημένα (μέσω εργαλείων που συγκρίνουν εκδόσεις και CVE σε πραγματικό χρόνο), προσφέροντας ευελιξία και ταχύτητα στην αξιολόγηση του κινδύνου.

4.7.1 Vulnerability Scanning

Κατά τη σάρωση για εκδόσεις (version scanning), αξιοποιούνται τα δεδομένα που συγκεντρώθηκαν κατά τη φάση του Information Gathering (όπως ονόματα υπηρεσιών, ανοιχτές θύρες και fingerprinted λειτουργικά συστήματα) για να εντοπιστούν με ακρίβεια η έκδοση κάθε λογισμικού ή υπηρεσίας που «τρέχει» στον στόχο. Αυτό μπορεί να γίνει: [45]

- Χειροκίνητα, μέσω εργαλείων γραμμής εντολών (π.χ. banner grabbing με telnet ή netcat) και αναζήτησης σε επίσημες λίστες εκδόσεων, όπου ο penetration tester στέλνει χειροκίνητα αιτήματα στις θύρες, λαμβάνει τα headers των υπηρεσιών (π.χ. HTTP headers) και ελέγχει τις εκδόσεις έναντι βάσεων δεδομένων, μια διαδικασία επίπονη αλλά χρήσιμη για επιβεβαίωση ασαφών βάσεων δεδομένων.
- Αυτόματα, με εργαλεία vulnerability scanners όπως το Nessus, που διεξάγει μαζική σάρωση θυρών και υπηρεσιών, ανιχνεύει μέσω signatures και fingerprinting τις εκδόσεις και παρουσιάζει συγκεντρωτικά αποτελέσματα. Το Nessus μπορεί, για παράδειγμα, να συνδυάσει άμεσα κάθε ανιχνευθείσα έκδοση με γνωστά CVE και να παράσχει προτεραιοποιημένη λίστα ευπαθειών.

Η ενσωμάτωση του version scanning με τα ευρήματα του Information Gathering επιτρέπει τη δημιουργία ενός πλήρους προφίλ του στόχου, από το γενικό mapping των σημείων εισόδου (θύρες, υπηρεσίες) μέχρι την ακριβή αναγνώριση ευπαθειών σε συγκεκριμένες εκδόσεις λογισμικού. Αυτό καθιστά δυνατή την αξιολόγηση του επιπέδου κινδύνου και την επιλογή κατάλληλων τεχνικών εκμετάλλευσης (Exploitation) στις επόμενες φάσεις του penetration test.

Επιπλέον, ο σχεδιασμός του vulnerability scanning διακρίνεται σε δύο βασικούς τύπους σάρωσης unauthenticated και authenticated scans. [45]

- Τα Unauthenticated Scans πραγματοποιούνται χωρίς να παρέχονται διαπιστευτήρια πρόσβασης στο σύστημα-στόχο. Ο scanner εξετάζει εξωτερικά σημεία εισόδου (όπως ανοιχτές θύρες, διαθέσιμες υπηρεσίες και banner grabbing) και συγκρίνει τις εκδόσεις λογισμικού με γνωστά ευπαθή CVE. Το πλεονέκτημά τους έγκειται στην απλότητα και στην έλλειψη ανάγκης για ειδικούς λογαριασμούς, ωστόσο συχνά περιορίζονται από την αδυναμία πρόσβασης σε εσωτερικές πληροφορίες και μπορεί να μην εντοπίζουν ευπάθειες που απαιτούν διαπιστευτήρια για να αποκαλυφθούν.
- Τα Authenticated Scans αντίθετα εκτελούνται με τη χρήση έγκυρων διαπιστευτηρίων (π.χ. λογαριασμός διαχειριστή ή χρήστη με περιορισμένα δικαιώματα) και επιτρέπουν στον scanner να εισέλθει «εντός» του συστήματος, να εξετάσει ρυθμίσεις ασφαλείας, να αναζητήσει ευπάθειες σε εσωτερικές δομές (όπως αρχεία συστήματος, registry, βιβλιοθήκες) και να εκτελέσει έλεγχο σε βάθος των εγκαταστάσεων λογισμικού. Παρέχουν πιο πλήρη εικόνα των κινδύνων, αλλά απαιτούν στενή συνεργασία με τον υπεύθυνο διαχείρισης της υποδομής, καθώς και προσεκτικό χειρισμό των διαπιστευτηρίων για να μην προκληθεί αστοχία ή αθέλητη αλλαγή στην παραγωγική λειτουργία.

Τα unauthenticated scans προσφέρουν ένα γρήγορο «εξωτερικό» προφίλ ευπαθειών, ενώ τα authenticated scans εμβαθύνουν στην ασφάλεια από το εσωτερικό, αποκαλύπτοντας ευπάθειες που

διαφορετικά παραμένουν κρυφές. Η συνδυασμένη χρήση και των δύο τύπων σάρωσης ενισχύει σημαντικά την αξιοπιστία και την κάλυψη του vulnerability assessment.

4.7.2 Αντιστοίχιση Εκδόσεων Λογισμικού σε CVE

Στο στάδιο της Αντιστοίχισης Εκδόσεων Λογισμικού σε CVE αξιοποιούνται τα αποτελέσματα του version scanning —δηλαδή οι ακριβείς εκδόσεις λογισμικού και υπηρεσιών που έχουν εντοπιστεί (π.χ. Apache HTTP Server 2.4.49, OpenSSL 1.1.1k, MySQL 5.7.36) — ώστε να εντοπιστούν οι αντίστοιχες γνωστές ευπάθειες. Κάθε έκδοση μπορεί να συγκριθεί είτε χειροκίνητα, μέσω αναζήτησης στον κατάλογο CVE της εταιρίας MITRE, είτε αυτόματα με εργαλεία σάρωσης όπως το Nessus ή το OpenVAS, τα οποία αντιστοιχούν αυτόματα τις εκδόσεις σε καταγεγραμμένα CVE (π.χ. το Apache 2.4.49 σχετίζεται με το CVE-2021-41773, το OpenSSL 1.1.1k με το CVE-2021-23840 και η MySQL 5.7.36 με το CVE-2021-27928). Στη συνέχεια, οι εντοπισμένοι CVE κατηγοριοποιούνται ανάλογα με τον τύπο της ευπάθειας (remote code execution, information disclosure, denial of service κ.ά.), το CVSS score (βαθμός σοβαρότητας) και τις απαιτούμενες συνθήκες εκμετάλλευσης (authentication, local/remote). Αυτή η διαδικασία επιτρέπει την προτεραιοποίηση των ευπαθειών με υψηλό ρίσκο ή χαμηλές απαιτήσεις δικαιωμάτων, τον σχεδιασμό κατάλληλων διορθωτικών ενεργειών (όπως αναβάθμιση σε ασφαλέστερες εκδόσεις ή εφαρμογή εξειδικευμένων ρυθμίσεων) και την έγκαιρη ενημέρωση των αρμόδιων ομάδων για την υλοποίηση των επιδιορθώσεων. Ο συνδυασμός version scanning και αντιστοίχισης σε CVE δημιουργεί έναν δομημένο κατάλογο πραγματικών και επιβεβαιωμένων αδυναμιών, προσφέροντας στις ομάδες ασφαλείας σαφή εικόνα των κινδύνων και των απαιτούμενων βημάτων θωράκισης των συστημάτων. [48]

4.7.3 Κοινές Ευπάθειες

Σε αυτό το σημείο κρίνεται ιδιαίτερα χρήσιμο να παρουσιαστούν οι ευπάθειες που απαντώνται συχνότερα σε web εφαρμογές, όπως τις καταγράφει ο οργανισμός Open Worldwide Application Security Project (OWASP) στο Top 10 των κρίσιμων κινδύνων ασφάλειας. Η αναφορά σε αυτές τις κατηγορίες ευπαθειών θα βοηθήσουν τον αναγνώστη να κατανοήσει καλύτερα τα κοινά λάθη υλοποίησης και τις πρακτικές που πρέπει να αποφεύγονται, προκειμένου να ενισχυθεί η ασφάλεια των πληροφοριακών συστημάτων. [49]

Εικόνα 4.1: Λογότυπο του Οργανισμού OWASP [50]

Παρακάτω παρουσιάζονται συνοπτικά οι βασικές κατηγορίες μαζί με σύντομη περιγραφή του τρόπου λειτουργίας τους:

Injection

Οι επιθέσεις τύπου injection συμβαίνουν όταν ένας επιτιθέμενος εκμεταλλεύεται την έλλειψη κατάλληλου φιλτραρίσματος ή εξαγωγής ειδικών χαρακτήρων από τις εισόδους (inputs) μιας εφαρμογής, εισάγοντας κακόβουλο κώδικα (όπως SQL statements, LDAP queries ή ακόμα και shell

commands) που εκτελούνται από τον διακομιστή. Στην περίπτωση του SQL Injection, για παράδειγμα, μια αδύναμη φόρμα αναζήτησης μπορεί να επιτρέψει σε έναν επιτιθέμενο να διαβάσει, να τροποποιήσει ή να διαγράψει δεδομένα της βάσης σε πραγματικό χρόνο, παρακάμπτοντας οποιαδήποτε λογική ελέγχου πρόσβασης. [51]

Broken Authentication

Όταν ο μηχανισμός πιστοποίησης και διαχείρισης συνεδριών μιας εφαρμογής δεν έχει σχεδιαστεί με ασφάλεια, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αδύναμους ή προβληματικούς αλγορίθμους δημιουργίας session IDs, επαναχρησιμοποίηση tokens ή ελλιπή έλεγχο χρονου ζωής (session timeout). Αυτό οδηγεί σε περιπτώσεις όπως session hijacking ή credential stuffing, όπου ένας κακόβουλος χρήστης αποκτά πρόσβαση σε λογαριασμούς άλλων χρηστών χωρίς να απαιτείται η γνώση του πραγματικού τους κωδικού. [52]

Sensitive Data Exposure

Οι εφαρμογές που δεν προστατεύουν επαρκώς ευαίσθητα δεδομένα, είτε κατά τη μετάδοσή τους είτε κατά την αποθήκευσή τους, επιτρέπουν την υποκλοπή προσωπικών πληροφοριών, όπως στοιχεία πιστωτικών καρτών ή ιατρικά δεδομένα, από ενδιάμεσους επιτιθέμενους (Man in the Middle attacks - MITM) ή μέσω διαρροών σε μη κρυπτογραφημένη βάση. Η μη χρήση πρωτοκόλλων TLS/SSL, αδύναμοι αλγόριθμοι κρυπτογράφησης ή αποθήκευση passwords σε plain text αυξάνει δραματικά τον κίνδυνο έκθεσης. [53]

XML External Entities (XXE)

Όταν εφαρμογές που αναλύουν XML (Extensible Markup Language) κώδικα εισάγουν εγγενώς εξωτερικές οντότητες χωρίς ασφάλεια, ένας επιτιθέμενος μπορεί να καθοδηγήσει τον XML parser στην ανάκτηση ή εκτέλεση κακόβουλου περιεχομένου (όπως τοπικών αρχείων ή υπηρεσιών δικτύου) αποκτώντας πρόσβαση σε ευαίσθητα αρχεία ή προκαλώντας denial-of-service μέσω υπερφόρτωσης πόρων. [54]

Broken Access Control

Οι ανεπαρκείς έλεγχοι πρόσβασης επιτρέπουν σε χρήστες να εκτελέσουν ενέργειες ή να δουν δεδομένα για τα οποία δεν έχουν άδεια. Παραδείγματα περιλαμβάνουν την παραβίαση URL ή Application Programming Interface (API) endpoints, όπου ένας χρήστης με κατώτερο ρόλο επιχειρεί να αποκτήσει διοικητικά δικαιώματα ή να δει ευαίσθητες πληροφορίες προοριζόμενες για υψηλότερα προνόμια. [55]

Security Misconfiguration

Λανθασμένες ρυθμίσεις σε servers, βάσεις δεδομένων ή πλατφόρμες, όπως ανοιχτά διαχειριστικά interfaces, ξεχασμένα default credentials, ενεργοποίηση debug modes ή έκθεση εσωτερικών endpoints, δημιουργούν εύκολους στόχους για επιτιθέμενους που εκμεταλλεύονται αυτές τις απροσεξίες για να αποκτήσουν πρόσβαση ή να προκαλέσουν υπηρεσιακές διαταραχές. [56]

Cross-Site Scripting (XSS)

Σε ευπάθειες XSS, οι επιτιθέμενοι εισάγουν κακόβουλο JavaScript κώδικα σε σελίδες που επισκέπτονται άλλοι χρήστες. Αυτό επιτυγχάνεται συνήθως μέσω ανεπαρκούς απολύμανσης (sanitization) inputs, επιτρέποντας την εκτέλεση κώδικα στον browser του θύματος για κλοπή cookies, εμφύτευση phishing forms ή redirection σε κακόβουλους ιστοτόπους. [57]

Insecure Deserialization

Η αποκωδικοποίηση μη αξιόπιστων serialized objects μπορεί να οδηγήσει σε απρόβλεπτες ενέργειες, όπως remote code execution ή denial-of-service, εάν ο κώδικας που διαχειρίζεται την απεικόνιση αντικειμένων δεν ελέγχει την ακεραιότητα ή την προέλευσή τους. [58]

Using Components with Known Vulnerabilities

Η εκτέλεση βιβλιοθηκών, frameworks ή πακέτων open-source με ήδη αναγνωρισμένες ευπάθειες (όπως παλαιές εκδόσεις jQuery ή Log4j) ευνοεί επιθέσεις χωρίς την ανάγκη για zero-day εκμεταλλεύσεις, καθώς οι πληροφορίες και τα Proof of Concept (PoC) είναι διαθέσιμα σε ευρεία κλίμακα. [59]

Insufficient Logging & Monitoring

Η έλλειψη ή η ανεπαρκής καταγραφή και παρακολούθηση των συμβάντων ασφαλείας (όπως αποτυχημένες προσπάθειες login, αλλαγές σε κρίσιμες ρυθμίσεις ή ανεξήγητη δικτυακή κίνηση) οδηγεί σε καθυστερημένη ανίχνευση επιθέσεων και αδυναμία ουσιαστικής αντίδρασης, επιτρέποντας στους επιτιθέμενους να παραμείνουν αόρατοι για εκτεταμένο διάστημα. [60]

4.8 Εκμετάλλευση Ευπαθιών (Τρίτο Στάδιο)

Σε αυτό το σημείο της διαδικασίας του penetration testing, έχοντας ήδη αναγνωρίσει το λογισμικό και τις εκδόσεις που χρησιμοποιούνται στον στόχο και έχοντας διασταυρώσει αυτές τις πληροφορίες με γνωστές ευπάθειες όπως αυτές που περιγράφονται στο OWASP Top 10, ο penetration tester μπορεί να μεταφερθεί πλέον στο επόμενο καθοριστικό στάδιο, την εκμετάλλευση (exploitation). Σε αυτό το στάδιο, ο penetration tester επιχειρεί να αξιοποιήσει ενεργά τις εντοπισμένες ευπάθειες με σκοπό να επιβεβαιώσει την ύπαρξή τους, να εξετάσει τον βαθμό σοβαρότητάς τους και να μετρήσει τις πιθανές επιπτώσεις που θα μπορούσαν να έχουν εάν γίνονταν αντικείμενο κακόβουλης χρήσης.

Οι ευπάθειες που έχουν εντοπιστεί μέχρι τώρα, όπως η ανεπαρκής έλεγχος ταυτότητας (broken authentication), ο ανεπαρκής έλεγχος πρόσβασης (broken access control), ή η χρήση ευάλωτων βιβλιοθηκών (vulnerable components), δεν αποτελούν απλώς θεωρητικά σημεία αδυναμίας. Αντιθέτως, είναι πλέον οι «πύλες εισόδου» τις οποίες ο επιτιθέμενος μπορεί να χρησιμοποιήσει για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση, να παρακάμψει κρίσιμους μηχανισμούς ασφαλείας, να διαρρεύσει δεδομένα ή να εκτελέσει κακόβουλο κώδικα. Το exploitation αποτελεί, λοιπόν, την εφαρμοσμένη επαλήθευση του κινδύνου, εκεί όπου η πληροφορία μετατρέπεται σε δράση και τα θεωρητικά σενάρια απειλής αποκτούν πρακτική υπόσταση.

Η σημασία αυτού του σταδίου δεν έγκειται μόνο στην ανάδειξη της ευπάθειας, αλλά και στην αξιολόγηση των πραγματικών συνεπειών που μπορεί να έχει μία παραβίαση στην υποδομή του στόχου. Με γνώμονα τη δεοντολογική διάσταση του white-hat hacking, στόχος δεν είναι η πρόκληση βλάβης, αλλά η παροχή αποδείξεων που θα επιτρέψουν στην εκάστοτε επιχείρηση να ενισχύσει την ασφάλειά της προτού υπάρξει πραγματική απειλή. [62]

4.8.1 Τεχνικές Εκμετάλλευσης Ευπαθιών

Στον πραγματικό κόσμο των επιθέσεων, η ύπαρξη ευπαθειών σε συστήματα, εφαρμογές ή δικτυακές υποδομές δεν αποτελεί απλώς ένα θεωρητικό ζήτημα ασφάλειας, αλλά το σημείο εκκίνησης για στοχευμένες και συστηματικές προσπάθειες παραβίασης. Οι τεχνικές εκμετάλλευσης ευπαθειών (vulnerability exploitation techniques) αποτελούν το στάδιο όπου οι πληροφορίες που έχουν συλλεχθεί κατά την αναγνώριση και ανάλυση των αδυναμιών μετατρέπονται σε πρακτικά βήματα επίθεσης, με σκοπό την απόκτηση μη εξουσιοδοτημένης πρόσβασης, την παράκαμψη μηχανισμών ασφαλείας ή την εκτέλεση κακόβουλου κώδικα. Η διαδικασία αυτή περιλαμβάνει τη χρήση εξειδικευμένων εργαλείων

και μεθόδων, από αυτοματοποιημένα scripts μέχρι χειροκίνητες τεχνικές και καλύπτει ένα ευρύ φάσμα σεναρίων, ανάλογα με τη φύση και τη σοβαρότητα της ευπάθειας. Παρακάτω παρουσιάζονται ορισμένες χαρακτηριστικές τεχνικές εκμετάλλευσης, οι οποίες καταδεικνύουν πώς οι θεωρητικές αδυναμίες μπορούν να μετατραπούν σε απτές παραβιάσεις με σημαντικές επιχειρησιακές και τεχνικές συνέπειες:

Password Cracking

Το Password Cracking αποτελεί τεχνική εκμετάλλευσης ευπαθειών που στοχεύει στη διάρρηξη μηχανισμών αυθεντικοποίησης μέσω αποκρυπτογράφησης ή ανεύρεσης κωδικών πρόσβασης χρηστών και διαχειριστών. Η διαδικασία βασίζεται σε μεθόδους όπως οι επιθέσεις brute force, όπου δοκιμάζονται συστηματικά όλοι οι πιθανοί συνδυασμοί χαρακτήρων, οι dictionary attacks που χρησιμοποιούν προκαθορισμένες λίστες λέξεων και οι hybrid επιθέσεις που συνδυάζουν τα δύο. Προηγμένα εργαλεία όπως τα John the Ripper[77], Hydra[78] και Hashcat[79] μπορούν να αυτοματοποιήσουν αυτές τις διαδικασίες, ενώ τεχνικές όπως τα rainbow tables επιταχύνουν την αποκρυπτογράφηση hash τιμών, εκτός αν εφαρμόζεται salting, το οποίο προσθέτει τυχαία δεδομένα πριν την κωδικοποίηση για να αποτρέψει τέτοιες επιθέσεις. Η επιτυχής διάρρηξη κωδικών μπορεί να επιτρέψει στον επιτιθέμενο την πρόσβαση σε κρίσιμους λογαριασμούς, την κλιμάκωση προνομίων και, τελικά, τον πλήρη έλεγχο του συστήματος, καθιστώντας το password cracking ένα από τα πιο αποτελεσματικά αλλά και επικίνδυνα εργαλεία στο οπλοστάσιο του exploitation. [63]

Remote Code Execution (RCE)

Το Remote Code Execution αποτελεί μία από τις πιο επικίνδυνες τεχνικές εκμετάλλευσης ευπαθειών, καθώς δίνει τη δυνατότητα σε έναν επιτιθέμενο να εκτελεί αυθαίρετο κώδικα σε απομακρυσμένο σύστημα χωρίς φυσική πρόσβαση. Η εμφάνισή του συνήθως οφείλεται σε ανεπαρκή έλεγχο και φιλτράρισμα εισόδου δεδομένων, σε ευπάθειες τύπου injection (π.χ. command injection, SQL injection), σε μη ασφαλή διαδικασία deserialization ή σε χρήση ευάλωτων βιβλιοθηκών και frameworks. Μέσω της αποστολής κατάλληλα διαμορφωμένων αιτημάτων (payloads), ο επιτιθέμενος μπορεί να προκαλέσει την εκτέλεση εντολών ή scripts στο περιβάλλον του server, αποκτώντας έτσι δυνατότητα για ενέργειες όπως εγκατάσταση backdoors, άνοιγμα reverse shells, παραβίαση μηχανισμών ασφαλείας ή πλήρη έλεγχο του συστήματος. Λόγω της κρισιμότητάς του, το RCE θεωρείται κορυφαία απειλή στο πλαίσιο του penetration testing και η ανίχνευση ή επιβεβαίωσή του απαιτεί αυστηρά ελεγχόμενες και δεοντολογικές μεθόδους. [64]

File Inclusion

Το File Inclusion (τοπικό - Local File Inclusion / απομακρυσμένο - Remote File Inclusion) είναι τεχνική εκμετάλλευσης ευπαθειών που εμφανίζεται κυρίως σε εφαρμογές web όταν ο κώδικας επιτρέπει τη δυναμική φόρτωση αρχείων χωρίς επαρκή έλεγχο και επικύρωση της διαδρομής τους. Στην περίπτωση του Local File Inclusion (LFI), ο επιτιθέμενος αξιοποιεί τη δυνατότητα πρόσβασης σε αρχεία που βρίσκονται τοπικά στον server, με σκοπό την ανάγνωση ευαίσθητων δεδομένων (π.χ. αρχείων ρυθμίσεων ή αρχείων κωδικών) ή την εκτέλεση τοπικών scripts. Στο Remote File Inclusion (RFI), η ευπάθεια επιτρέπει τη φόρτωση και εκτέλεση αρχείων από απομακρυσμένο διακομιστή, κάτι που μπορεί να οδηγήσει στην εισαγωγή και εκτέλεση κακόβουλου κώδικα, εγκατάσταση backdoors ή πλήρη παραβίαση του συστήματος. Και οι δύο μορφές συνήθως προκύπτουν από ελλιπή φιλτράρισμα παραμέτρων σε συναρτήσεις όπως η include() ή η require() σε γλώσσες όπως η PHP και αποτελούν ιδιαίτερα κρίσιμες απειλές, αφού μπορούν να μετατραπούν σε σημεία εισόδου για περαιτέρω επιθέσεις, όπως privilege escalation ή Remote Code Execution. [65]

4.8.2 PoC/Public Exploits

Στο στάδιο του exploitation οι επιτιθέμενοι σπάνια γράφουν από την αρχή τον δικό τους κακόβουλο κώδικα αντίθετα, αξιοποιούν συχνά ήδη διαθέσιμα PoC και public exploits για να εκμεταλλευτούν τις ευπάθειες που έχουν εντοπιστεί. Τα PoC είναι μικρά σενάρια ή προγράμματα που αποδεικνύουν πειραματικά τη δυνατότητα εκμετάλλευσης μίας ευπάθειας, επιτρέποντας στον ερευνητή ή επιτιθέμενο να κατανοήσει τη λογική πίσω από το σφάλμα χωρίς απαραιτήτως να φτάσει σε πλήρη κατάληψη συστήματος. Τα public exploits, από την άλλη, είναι πιο ολοκληρωμένες υλοποιήσεις αυτών των PoC, οι οποίες συχνά περιλαμβάνουν και ένα ή περισσότερα payloads (κομμάτια εκτελέσιμου κώδικα ή scripts) τα οποία, μόλις μεταφερθούν στο μηχάνημα-θύμα, εγκαθιστούν έναν reverse shell, ένα backdoor, επιτρέπουν αυξημένα προνόμια ή εξάγουν ευαίσθητα δεδομένα.

Τέτοιες υλοποιήσεις μπορεί κανείς να βρει σε βάσεις δεδομένων όπως το Exploit-DB ή στο Metasploit Framework, ενώ πλήθος PoC δημοσιεύονται επίσης σε δημοφιλή repositories στο GitHub και σε security forums και mailing lists όπως το Full Disclosure. Για να χρησιμοποιήσει κάποιος ένα public exploit, επιλέγει το κατάλληλο module ή σενάριο που ταιριάζει στην έκδοση του λογισμικού-στόχου, διαμορφώνει τις παραμέτρους σύνδεσης (διεύθυνση, θύρα, HTTP headers κ.λπ.) και εκκινεί το payload, το οποίο στη συνέχεια ανοίγει ένα κανάλι επικοινωνίας με τον επιτιθέμενο. Μέσω αυτής της διαδικασίας, ένας επιτιθέμενος μπορεί να επιβεβαιώσει την αξιοποίηση της ευπάθειας γρήγορα και αποτελεσματικά, επιταχύνοντας δραστικά το συνολικό χρόνο και το κόστος μίας πλήρους επίθεσης. [66]

4.8.3 Metasploit Framework

Μετά την αξιοποίηση των PoC και public exploits για την κατανόηση και επίδειξη των ευπαθειών, η διαδικασία μπορεί να γίνει πολύ πιο αποτελεσματική με τη χρήση του Metasploit Framework. Το Metasploit αυτοματοποιεί μεγάλο μέρος των βημάτων (από την αναζήτηση και επιλογή του κατάλληλου exploit μέχρι την επιλογή και ενσωμάτωση του κατάλληλου payload) συνδυάζοντας exploits, auxiliary modules και post-exploitation εργαλεία σε ένα ενιαίο περιβάλλον. Με αυτόν τον τρόπο, ο penetration tester μπορεί να εστιάσει στην ανάλυση των αποτελεσμάτων και στη βελτιστοποίηση των τεχνικών, ενώ το Metasploit αναλαμβάνει την εκτέλεση και παρακολούθηση πολλών από τις πιο χρονοβόρες και επαναλαμβανόμενες διαδικασίες.

Το Metasploit Framework αποτελεί ένα από τα πιο δημοφιλή και ολοκληρωμένα εργαλεία για την αυτοματοποίηση του σταδίου του exploitation στο penetration testing. Αναπτύχθηκε αρχικά από τον Mati Aharoni και εξελίχθηκε σε μια κοινότητα υπό την αιγίδα της Rapid7, παρέχοντας ένα ενιαίο περιβάλλον όπου συνδυάζονται exploits, payloads και βοηθητικά modules για την εκμετάλλευση ευπαθειών.

Καθένα από τα διαθέσιμα exploit modules στο Metasploit είναι σχεδιασμένο να στοχεύει συγκεκριμένες ευπάθειες (π.χ. CVE-2021-41773 για Apache 2.4.49) και περιλαμβάνει τον κώδικα που απαιτείται για να προκαλέσει το σφάλμα. Μαζί με αυτά υπάρχουν payload modules (π.χ. Meterpreter ή reverse TCP shells) τα οποία εγκαθίστανται αυτόματα στο σύστημα-θύμα μόλις το exploit πετύχει. Ο penetration tester απλώς φορτώνει το κατάλληλο exploit, ορίζει τις παραμέτρους του στόχου (RHOST, RPORT) και επιλέγει το payload που επιθυμεί. Με μία εντολή εκκίνησης (exploit), το Metasploit αναλαμβάνει τη διαχείριση του αιτήματος, την αποστολή του κακόβουλου κώδικα και την εγκατάσταση του payload.

Χρησιμοποιώντας το msfconsole, ο penetration tester έχει πρόσβαση σε εργαλείο αυτόματης αναζήτησης κατάλληλων exploits (command search), δυνατότητα δοκιμής διαφορετικών payloads

(command set PAYLOAD), καθώς και παρακολούθησης της σύνδεσης σε πραγματικό χρόνο. Επιπλέον, το Metasploit ενσωματώνει auxiliary modules για σάρωση θυρών ή brute-forcing credentials, διευκολύνοντας τη μεταφορά δεδομένων από το Vulnerability Detection στο exploitation.

Μόλις εγκατασταθεί το Meterpreter session, ο penetration tester αποκτά ένα πλήρες εργαλείο post-exploitation με εντολές για ανύψωση δικαιωμάτων (mimikatz, getsystem), εξαγωγή κρυπτογραφημένων αρχείων, keylogging και persistence. Μέσα από αυτό το πλαίσιο, το Metasploit αυξάνει δραστικά την ταχύτητα και την αξιοπιστία των penetration testing, επιτρέποντας στον penetration tester να επαληθεύσει και να αποδείξει με αντικειμενικά παραδοτέα τη σοβαρότητα των ευπαθειών. [61]

4.9 Persistance (Τέταρτο Στάδιο)

Μόλις αποκτιθεί αρχική πρόσβαση στο σύστημα-θύμα μέσω ενός exploit και επιτευχθεί το πρώτο reverse shell, συνήθως ο penetration tester βρίσκεται αντιμέτωπος με ένα έστω λειτουργικό, αλλά περιορισμένο περιβάλλον. Το shell αυτό δεν υποστηρίζει συχνά βασικές λειτουργίες (π.χ. history, tab-completion και control sequences), καθιστώντας την περαιτέρω εργασία δύσκολη. Για να μπορέσει να γίνει πιο σταθερό, θα χρειαστεί για παράδειγμα να εκτελεστεί η παρακάτω ακολουθία εντολών στον τρέχοντα αμειβόμενο interpreter:

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
Ctrl+Z
```

```
stty raw -echo; fg
```

```
export TERM=xterm
```

Με αυτά τα βήματα εκκινείται στην απομακρυσμένη συσκευή ένα πλήρες διαδραστικό Bash shell, “σπάζοντας” τους περιορισμούς του αρχικού τερματικού και απολαμβάνοντας λειτουργίες όπως arrow-key navigation και λειτουργία ιστορικού εντολών.

Παράλληλα, δεδομένου ότι ένα reverse shell μπορεί να εντοπιστεί και να τερματιστεί από διαχειριστές ασφαλείας ή IDS/IPS, συχνά δημιουργούνται backdoor για μόνιμη πρόσβαση. Αυτό μπορεί να γίνει είτε με την εγκατάσταση ενός μόνιμου listener (π.χ. με netcat σε background) και την επανασύνδεση σε τακτά διαστήματα, είτε με την εμφύτευση ενός μικρού web shell ή cron job που δέχεται εντολές από τον penetration tester. Με αυτόν τον τρόπο, ακόμα κι αν το αρχικό session χαθεί, διατηρείται διακριτικά έναν κρυφό δίαυλο επικοινωνίας με το μηχάνημα, εξασφαλίζοντας συνεχή πρόσβαση για monitoring, data exfiltration ή περαιτέρω κινήσεις. [67]

4.10 Privilege Escalation (Πέμπτο Στάδιο)

Εφόσον έχει αποκτηθεί αρχική πρόσβαση στο σύστημα εκμεταλεύοντας μια ευπάθεια στο στάδιο του exploitation, συνήθως ο penetration tester βρίσκεται μπροστά σε ένα περιβάλλον με χαμηλά δικαιώματα χρήστη. Σε αυτό το επίπεδο πρόσβασης δεν μπορούν να εκτελεστούν κρίσιμες εντολές διαχείρισης, να τροποποιηθούν σημαντικές ρυθμίσεις του λειτουργικού συστήματος ή να εγκαταστηθούν μόνιμα εργαλεία υποστήριξης. Για να μπορεί να επιτευχθεί πλήρη αξιολόγηση των κινδύνων και να αναδειχθεί η επιθετική δυνατότητα ενός εισβολέα, απαιτείται Privilege Escalation, το οποίο θα επιτρέψει την απόκτιση δικαιωμάτων διαχειριστή ή root.

Η φάση αυτή είναι κομβικής σημασίας για τον εντοπισμό των πραγματικών επιπτώσεων μιας πιθανής παραβίασης, καθώς αποκαλύπτει εάν ο εισβολέας θα μπορούσε να αποκτήσει πλήρη έλεγχο του συστήματος, να παρακάμψει μηχανισμούς ασφαλείας, ή να κινείται ανεξέλεγκτα εντός του δικτύου.

Μέσα από τεχνικές, ο penetration tester επιδιώκει να αναδείξει τα αδύναμα σημεία που επιτρέπουν την ανεπιθύμητη αναβάθμιση δικαιωμάτων, με σκοπό την έγκαιρη αντιμετώπισή τους από την εκάστοτε επιχείρηση ή οργανισμό.

Για να μπορέσει ο αναγνώστης να κατανοήσει ολοκληρωμένα τις ανάγκες αναβάθμισης δικαιωμάτων, θα μελετιθούν τόσο οι χειροκίνητες τεχνικές, όπου η εμπειρία και η λεπτομερής ανάλυση του συστήματος οδηγούν στον εντοπισμό ειδικών αδυναμιών, όσο και τις αυτόματες μεθόδους, που αξιοποιούν εργαλεία για γρήγορη και συστηματική αναγνώριση και εκμετάλλευση κοινών ευπαθειών. Με αυτόν τον τρόπο διασφαλίζεται ότι κάθε περιβάλλον ελέγχου αποκτά την κατάλληλη προσέγγιση, συνδυάζοντας την ευελιξία του χειροκίνητου ελέγχου με την ταχύτητα της αυτοματοποίησης. [68]

4.10.1 Χειροκίνητες Μέθοδοι Privilege Escalation

Στη φάση της χειροκίνητης αναβάθμισης δικαιωμάτων (manual privilege escalation), ο penetration tester αξιοποιεί την άμεση αλληλεπίδραση με το υποκείμενο λειτουργικό σύστημα για να εντοπίσει και να εκμεταλλεύσει αδυναμίες που δεν απαιτούν αυτοματοποιημένα εργαλεία. Αρχικά, ο έλεγχος των διαπιστευτηρίων (credentials) συχνά φέρνει αποτελέσματα, με τεχνικές όπως το password cracking και το password spraying δοκιμάζονται μεθοδικά επιθέσεις brute-force εναντίον hashes από τα αρχεία `/etc/shadow`, ενώ default ή ξεχασμένα credentials σε υπηρεσίες SSH, βάσεις δεδομένων ή εφαρμογές δίνουν άμεση πρόσβαση σε λογαριασμούς με υψηλότερα προνόμια. Μετά την επίτευξη πρόσβασης, βασικές εντολές όπως id, whoami και hostname επιβεβαιώνουν το τρέχον επίπεδο δικαιωμάτων και τον ρόλο του μηχανήματος στο περιβάλλον, ενώ μέσω της εντολής passwd σε Linux μπορεί, υπό ορισμένες συνθήκες, να αλλάξει ο κωδικός ενός λογαριασμού αν εντοπιστεί ευπάθεια στα αρχεία `/etc/passwd` και `/etc/shadow`.

Εξετάζοντας τα αρχεία ρυθμίσεων (dotfiles) στον προσωπικό φάκελο του χρήστη, όπως το `.bashrc` συχνά εντοπίζονται αποθηκευμένα clear-text passwords ή scripts που τρέχουν με αυξημένα δικαιώματα. Η αναζήτηση σε `/etc/passwd` μπορεί να αποκαλύψει ευκαιρίες: σε συστήματα που για λόγους συμβατότητας αφήνουν hash μέσα σε αυτόν τον δημόσιο φάκελο, ένα απλό append ενός νέου χρήστη με UID/GID 0 επιτρέπει τη δημιουργία additional superuser.

Η αναγνώριση τρέχουσας έκδοσης λειτουργικού (`uname -a`) και πακέτων (`dpkg -l` ή `rpm -qa`), σε συνδυασμό με σάρωση για φορτωμένα kernel modules (`lsmod` + `modinfo`), μπορεί να αποκαλύψει παλαιά ή ευάλωτα στοιχεία. Σε αυτή τη φάση, ο penetration tester εντοπίζει κατάλληλο πηγαίο κώδικα exploit (π.χ. μέσω searchsploit) και τον μεταφέρει στο θύμα για τοπική αντιγραφή, compilation (`gcc exploit.c -o exploit`) και εκτέλεση, εκμεταλλευόμενος αστοχίες στον πυρήνα ή σε συσκευαστές συσκευών.

Παράλληλα, μηχανισμοί Set-UID/Set-GID (SUID/SGID) σε εκτελέσιμα αρχεία αποτελούν κλασική μέθοδο όπου με `find / -perm -u=s -type f` εντοπίζονται προγράμματα που τρέχουν ως root ανεξάρτητα από τον καλούντα χρήστη. Η κατάλληλη χρήση του δικαιώματος `-exec` σε misconfigured SUID binaries (όπως το `find` ή `perl`) παρέχει άμεση αναβάθμιση σε root shell.

Η ανάλυση των διεργασιών που τρέχουν ως root (π.χ. μέσω `ps aux`) μπορεί να αποκαλύψει custom daemons ή κρυφές κλήσεις σε scripts με credentials ή περιβάλλον που επιτρέπει την τροποποίηση. Παράλληλα, ο έλεγχος των εγγραφών στο crontab (`crontab -l` και `/etc/cron.*`) φέρνει στο φως scripts με αδύναμες άδειες, στα οποία αρκεί μια τροποποίηση για να τρέξουν κακόβουλο κώδικα σε υψηλό privilege level.

Τέλος, η διερεύνηση των συστημάτων αρχείων (με `mount`, `lsblk` ή ανάγνωση του `/etc/fstab`) μπορεί να αποκαλύψει μη προσαρτημένα volumes που περιέχουν backups ή configuration files με ευαίσθητες πληροφορίες. Αν τοποθετηθούν με write-permissions, επιτρέπουν την τροποποίηση ή την εμφύτευση εκτελέσιμων αρχείων στο σύστημα.

Μέσα από αυτές τις χειροκίνητες τεχνικές, ο penetration tester αναδεικνύει την πλήρη διαδρομή αναβάθμισης δικαιωμάτων, επιβεβαιώνοντας ότι ένας πραγματικός επιτιθέμενος θα μπορούσε όχι απλώς να εισέλθει, αλλά και να κυριαρχήσει στο σύστημα. [69]

4.10.2 Αυτόματες Μέθοδοι Privilege Escalation

Σε αντίθεση με τις χειροκίνητες τεχνικές αναβάθμισης δικαιωμάτων, που στηρίζονται στην εμπειρία του penetration tester και στην προσεκτική ανάλυση κάθε στοιχείου του συστήματος, οι αυτόματες μέθοδοι επιδιώκουν να αυτοματοποιήσουν τη διαδικασία ανεύρεσης αδυναμιών για privilege escalation, ελαχιστοποιώντας τον χρόνο και εξαλείφοντας κάποιες ανθρώπινες παραλείψεις. Τρεις από τα πιο διαδεδομένα σενάρια εργαλείων σε περιβάλλοντα Linux είναι το unix-privesc-check, το LinEnum και το LinPEAS.

Το unix-privesc-check αποτελεί ένα απλό, αλλά ισχυρό script γραμμένο σε Bash, το οποίο εκτελείται με ένα μόνο κλικ και παράγει αναφορά με τα πιο κρίσιμα σημεία που μπορεί να εκμεταλλευτεί ένας επιτιθέμενος. Κατά την εκτέλεσή του, ελέγχει για λειτουργικά προνόμια σε αρχεία εκτελέσιμων με SUID bit, αναζητεί στο σύστημα αρχεία ρυθμίσεων με αδύναμες άδειες, καταγράφει τις εκδόσεις πυρήνα και εγκατεστημένων πακέτων και επισκοπεί περιβαλλοντικές μεταβλητές που μπορεί να περιέχουν credentials. Το τελικό παραδοτέο είναι ένα απλό `.txt` αρχείο που συνοψίζει τις πιθανές οδούς privilege escalation, επιτρέποντας στον penetration tester να επικεντρωθεί άμεσα στις πιο επικίνδυνες ευπάθειες.

Το LinEnum αποτελεί εξέλιξη της ιδέας του unix-privesc-check, προσθέτοντας πολύ πιο λεπτομερή enumeration. Χρησιμοποιώντας σκριπτάκια και εντολές όπως `lsmod`, `getcap`, `crontab -l`, `df -h` και πολλαπλές αναζητήσεις σε αρχεία συστήματος, το LinEnum συγκεντρώνει όχι μόνο τα SUID/SGID binaries αλλά και όλα τα cron jobs, τις εγκατεστημένες Python ή Perl βιβλιοθήκες με ειδικά δικαιώματα, τις ατομικές ρυθμίσεις του χρήστη και στοιχεία configuración firewalls. Επιπλέον, προσπαθεί να συγκρίνει kernel version με γνωστά exploits, δίνοντας σαν output βαθμολογία κινδύνου για κάθε ευπάθεια.

Το πλέον δημοφιλές εργαλείο στη σύγχρονη κοινότητα penetration testing, το LinPEAS, προχωρά ακόμη παραπέρα, ενοποιώντας πολλαπλούς έλεγχους σε ένα μόνο script που εντοπίζει configuration weaknesses, misconfigured services, ενεργά network sockets, καθώς και δημοφιλείς attack vectors, όπως writable mounts, world-readable secrets και παλαιές εκδόσεις docker images. Το LinPEAS παρέχει και χρωματισμένη έξοδο (American National Standards Institute - ANSI colors) για άμεση αντίληψη κρίσιμων ευρημάτων, ενώ υποστηρίζει και προσαρμοσμένα modules για συγκεκριμένα περιβάλλοντα (systemd, AppArmor, SELinux). Με ένα απλό `chmod +x linpeas.sh && ./linpeas.sh`, ο penetration tester αποκτά πλήρη εικόνα των δυνατοτήτων privilege escalation, συνοδευόμενη από links σε PoC και public exploits που μπορεί να κατεβάσει και να εκτελέσει επιτόπου.

Συνολικά, αυτά τα εργαλεία αυτοματοποιούν τη μαζική έρευνα για ευπάθειες, επιταγχύνουν την αξιολόγηση κινδύνου και αποδεσμεύουν τον penetration tester από χρονοβόρα manual βήματα, ενώ παράλληλα δεν υποκαθιστούν την κρίση και την εμπειρία που απαιτούνται για την τελική αξιολόγηση και επιβεβαίωση κάθε πιθανού path privilege escalation. [70]

4.11 Τελική Αναφορά (Έκτο Στάδιο)

Στο τελικό στάδιο ενός penetration testing, η σύνταξη της αναλυτικής τελικής αναφοράς καθορίζει σε μεγάλο βαθμό την αξία και την πρακτική χρησιμότητα της διαδικασίας για τον οργανισμό. Η αναφορά πρέπει να ξεκινά με μια σύντομη εισαγωγή, στην οποία περιγράφεται ο στόχος της δοκιμής, το πλαίσιο και το εύρος (scope) των συστημάτων που εξετάστηκαν, καθώς και η μεθοδολογία που ακολουθήθηκε, με αναφορά στα βασικά στάδια (Reconnaissance, Vulnerability Detection, Exploitation, Persistence, Privilege Escalation).

Ακολουθεί μια μη τεχνική «εκτελεστική σύνοψη» (Executive Summary), η οποία απευθύνεται στη διοίκηση και τα ανώτερα στελέχη, παρουσιάζοντας με συνοπτικό τρόπο τα πιο κρίσιμα ευρήματα, το συνολικό επίπεδο κινδύνου και τις προτεινόμενες στρατηγικές δράσεις. Στο κείμενο αυτό τονίζεται εξαρχής το αντίστοιχο επιχειρηματικό κόστος αποκατάστασης σε περίπτωση επιτυχημένης επίθεσης, καθώς και το όφελος που προσφέρει η έγκαιρη διόρθωση.

Το κύριο σώμα της αναφοράς αναλύει κάθε ευπάθεια με τεχνική ακρίβεια, για κάθε σημείο αδυναμίας καταγράφεται ο τίτλος της, η περιγραφή της (π.χ. SQL Injection ή misconfigured SUID binary), οι αποδείξεις (screenshots, output εντολών), η αξιολόγηση του αντίκτυπου βάσει της τριάδας CIA και το Risk Rating score, Common Vulnerability Scoring System (CVSS). Στη συνέχεια, παρατίθενται αναλυτικές οδηγίες remediation, δηλαδή συγκεκριμένα βήματα (όπως εγκατάσταση security patch, αλλαγή παραμέτρων ή αναβάθμιση εκδόσεων) που επιτρέπουν στον τεχνικό υπεύθυνο να διορθώσει την ευπάθεια άμεσα και με ασφάλεια.

Για να διευκολυνθεί η διαχείριση των ευρημάτων, η αναφορά συμπληρώνεται με έναν συγκεντρωτικό πίνακα προτεραιοτήτων. Παρουσιάζονται όλες οι ευπάθειες με μοναδικό κωδικό αναφοράς, βαθμό σοβαρότητας, χρονικό πλαίσιο επιδιόρθωσης (π.χ. κρίσιμες μέσα σε μία εβδομάδα) και τον υπεύθυνο τμήμα ή άτομο για την υλοποίηση. Τέλος, η αναφορά κλείνει με συμπεράσματα που τονίζουν την ανάγκη επαναληπτικού penetration testing μετά την εφαρμογή των διορθωτικών ενεργειών και προτάσεις για θεσμοθέτηση τακτικών ελέγχων ασφαλείας, ώστε ο οργανισμός να διατηρεί συνεχή ανοσία απέναντι στις εξελισσόμενες κυβερνοαπειλές. [71]

4.12 Επίλογος

Το penetration testing, εστιάζοντας στην εφαρμογή πρακτικών τεχνικών και μεθόδων, προσφέρει πολύτιμες πληροφορίες για τον εντοπισμό αδυναμιών που μπορεί να εκμεταλλευτούν κακόβουλοι επιτιθέμενοι, ενώ βοηθά στον εντοπισμό των δυνατών σημείων που απαιτούν ενίσχυση και βελτίωση. Ολοκληρώνοντας την ανάλυση των σταδίων του penetration testing, γίνεται καλύτερα κατανοητή η σημασία κάθε σταδίου στην ολοκληρωμένη διαδικασία ελέγχου ασφαλείας. Από την αρχική αναγνώριση του στόχου και την ανίχνευση πιθανών ευπαθειών, έως την εκμετάλλευση και την τελική αναφορά, κάθε στάδιο έχει τον δικό του ρόλο στη συνολική αξιολόγηση της ασφάλειας του συστήματος.

Κεφάλαιο 5ο: Σενάριο Επίθεσης σε Ιστοσελίδα WordPress

5.1 Εισαγωγή

Σε αυτό το κεφάλαιο θα παρουσιαστεί ένα σενάριο επίθεσης στην ιστοσελίδα "***https://people.iee.ihu.gr/~dima/***" που βασίζεται στο σύστημα διαχείρισης περιεχομένου WordPress, με στόχο την πρακτική απεικόνιση των θεωρητικών γνώσεων που αναλύθηκαν στα προηγούμενα μέρη.

Λόγω των περιορισμών που υπήρχαν στην υποδομή του συστήματος και της ανάγκης αποφυγής ενδεχόμενων δυσλειτουργιών στην παραγωγική υπηρεσία, η εφαρμογή της μεθοδολογίας περιορίστηκε στα δύο πρώτα στάδια, την Συλλογή Πληροφοριών και τον Εντοπισμό Ευπαθειών. Στο πλαίσιο της Αναγνώρισης συγκεντρώθηκαν πληροφορίες για το περιβάλλον-στόχο μέσω παθητικών και ενεργών τεχνικών συλλογής δεδομένων, ενώ στο στάδιο του Εντοπισμού Ευπαθειών εντοπίστηκαν και αξιολογήθηκαν πιθανές αδυναμίες του συστήματος, βασιζόμενοι στα αποτελέσματα της προηγούμενης φάσης. Τα περαιτέρω παρεμβατικά στάδια δεν πραγματοποιήθηκαν, όπως η εκμετάλλευση ευπαθειών, η διατήρηση πρόσβασης ή η αναβάθμιση δικαιωμάτων, ώστε να διασφαλιστεί η ακεραιότητα και η ομαλή λειτουργία της ιστοσελίδας.

5.2 Συλλογή Πληροφοριών

Στο πρακτικό μέρος της παρούσας εργασίας, η φάση της παθητικής και ενεργής συλλογής δεδομένων αποτελεί το θεμέλιο για την περαιτέρω αξιολόγηση της ασφάλειας του στόχου. Μέσα από παθητικές τεχνικές, συγκεντρώνονται πληροφορίες από δημόσιες πηγές και διαθέσιμα αρχεία, χωρίς άμεση αλληλεπίδραση με το σύστημα, μειώνοντας τον κίνδυνο εντοπισμού. Στη συνέχεια, οι ενεργές μέθοδοι επιτρέπουν την άμεση επικοινωνία με τον στόχο, αποκαλύπτοντας λεπτομέρειες για τις υπηρεσίες, τις εκδόσεις λογισμικού και τα διαθέσιμα σημεία πρόσβασης. Ο συνδυασμός αυτών των δύο προσεγγίσεων δημιουργεί μια πλήρη και αξιόπιστη εικόνα του περιβάλλοντος, θέτοντας τη βάση για τον εντοπισμό και την αξιολόγηση πιθανών ευπαθειών στα επόμενα στάδια της διαδικασίας.

5.2.1 Παθητική Συλλογή Πληροφοριών

Η φάση του παθητικού εντοπισμού πληροφοριών αποτελεί το πρώτο βήμα συλλογής δεδομένων για τον στόχο, όπου ο penetration tester συγκεντρώνει πληροφορίες χωρίς να εκτελεί παρεμβατικές ενέργειες που θα μπορούσαν να επηρεάσουν τη λειτουργία του συστήματος ή να προσελκύσουν την προσοχή των διαχειριστών. Σε αυτήν τη φάση, αξιοποιούνται εργαλεία και πηγές που παρέχουν πληροφορίες για την υποδομή του στόχου χωρίς απευθείας επίθεση ή σάρωση.

Αρχικά, χρησιμοποιήθηκε η εντολή `dig` για την ανάλυση DNS του στόχου, με σκοπό την εξαγωγή της διεύθυνσης IP της ιστοσελίδας. Το `dig` αποτελεί ένα ισχυρό εργαλείο γραμμής εντολών, ικανό να ανακτά εγγραφές DNS όπως A, MX και CNAME, επιτρέποντας την ακριβή ταυτοποίηση της IP που εξυπηρετεί τον συγκεκριμένο τομέα. Η εντολή που χρησιμοποιήθηκε για την εύρεση της IP είναι η παρακάτω:

```
dig A people.iee.ihu.gr
```

Τα πιο σημαντικά από τα αποτελέσματα της εντολής αυτής φαίνονται παρακάτω (η πλήρης ανάπτυξη των αποτελεσμάτων της εντολής φαίνεται στο Παράρτημα Α):

```
people.iee.ihu.gr.      85796   IN      CNAME   aetos.iee.ihu.gr.
aetos.iee.ihu.gr.       20996   IN      A       195.251.123.232
```

Στο αποτέλεσμα του ερωτήματος dig για τον τομέα people.iee.ihu.gr παρατηρείται ότι δεν επιστρέφεται απευθείας μια εγγραφή τύπου A, αλλά πρώτα μια εγγραφή ως CNAME, η οποία δηλώνει ότι το people.iee.ihu.gr είναι στην πραγματικότητα ψευδώνυμο (alias) του aetos.iee.ihu.gr. Στη συνέχεια, το σύστημα DNS ακολουθεί αυτήν την αντιστοίχιση και αναζητά την A record του κανονικού ονόματος (aetos.iee.ihu.gr), η οποία αντιστοιχεί στην IPv4 διεύθυνση 195.251.123.232. Με άλλα λόγια, η IP που τελικά χρησιμοποιείται για την πρόσβαση στο people.iee.ihu.gr είναι αυτή του aetos.iee.ihu.gr, καθώς το πρώτο όνομα είναι απλώς ένα alias που ανακατευθύνει στον κανονικό (canonical) host.

Η επιβεβαίωση της αντιστοίχισης της διεύθυνσης IP 195.251.123.232 για την ιστοσελίδα https://people.iee.ihu.gr/~dima/ πραγματοποιήθηκε όχι μόνο μέσω της ανάλυσης DNS με την εντολή `dig`, αλλά και με χρήση των Developer Tools του browser. Συγκεκριμένα, από την καρτέλα Network εντοπίθηκαν τα αιτήματα που αποστέλλονται κατά τη φόρτωση της σελίδας και εξετάστηκαν οι πληροφορίες σύνδεσης (Remote Address), όπου εμφανίστηκε η ίδια IP. Με αυτόν τον τρόπο διασταυρώθηκε ότι η ιστοσελίδα εξυπηρετείται πράγματι από τον εξυπηρετητή που αντιστοιχεί στην 195.251.123.232, επιβεβαιώνοντας πλήρως το αποτέλεσμα της ανάλυσης DNS.

Τέλος, έγινε χρήση του εργαλείου Wappalyzer [72], το οποίο αναλύει τις τεχνολογίες που χρησιμοποιεί ο ιστότοπος, όπως το σύστημα διαχείρισης περιεχομένου (Content Management System - CMS), οι βιβλιοθήκες JavaScript, τα frameworks, τα εργαλεία ανάλυσης επισκεψιμότητας και οι τύποι διακομιστών. Το συγκεκριμένο εργαλείο αποτελεί πρόσθετο στον Browser το οποίο αναλύει την ιστοσελίδα με το άνοιγμά της. Η αναγνώριση των τεχνολογιών αυτών είναι κρίσιμη, καθώς μπορεί να αποκαλύψει πιθανά σημεία ευπάθειας. Τα αποτελέσματα της ανάλυσης παρουσιάζονται στον παρακάτω πίνακα:

Κατηγορία	**Τεχνολογίες / Εκδόσεις**
CMS	WordPress 6.8.2
Databases	MySQL
Blogs	WordPress 6.8.2
Page Builder	SiteOrigin Page Builder 2.31.8
Font Scripts	Twitter Emoji (Twemoji), Font Awesome
Javascript Libraries	jQuery 3.7.1, jQuery Migrate 3.4.1, jQuery UI 1.13.3
Miscellaneous	RSS
Web Servers	Apache 2.4.62
WordPress Plugins	Contact Form 7 6.0.6, SiteOrigin Page Builder 2.31.8, SiteOrigin Widgets Bundle 1.68.5, TablePress
Operating System	Debian

Πίνακας 5.1: Αποτελέσματα Wappalyzer

5.2.2 Ενεργή Συλλογή Πληροφοριών

Μετά την ολοκλήρωση της φάσης της παθητικής συλλογής πληροφοριών, επέρχεται το ενεργό στάδιο συλλογής, στο οποίο εκτελούνται άμεσες αλληλεπιδράσεις με το σύστημα-στόχο με σκοπό τη συλλογή πιο εξειδικευμένων και τεχνικών πληροφοριών. Σε αντίθεση με το παθητικό στάδιο, εδώ πραγματοποιούνται ενέργειες που ενδέχεται να εντοπιστούν από μηχανισμούς παρακολούθησης και ασφάλειας, καθώς η επικοινωνία με τον διακομιστή είναι πιο εμφανής.

Αρχικά, χρησιμοποιήθηκε το εργαλείο Nmap για την εκτέλεση port scanning στη διεύθυνση IP που είχε εντοπιστεί στο προηγούμενο στάδιο. Η διαδικασία αυτή επιτρέπει την ανακάλυψη των ανοιχτών θυρών και των υπηρεσιών που εκτελούνται στον διακομιστή, παρέχοντας κρίσιμες πληροφορίες για το πιθανό

πεδίο επίθεσης. Το Nmap[80] δίνει επίσης τη δυνατότητα προσδιορισμού εκδόσεων υπηρεσιών και λειτουργικών συστημάτων, κάτι που μπορεί να συμβάλει στον εντοπισμό συγκεκριμένων ευπαθειών. Παρακάτω παρουσιάζεται η εντολή που χρησιμοποιήθηκε για τον έλεγχο:

```
sudo nmap -sVC 195.251.123.232 -A
```

Τα πιο σημαντικά από τα αποτελέσματα της εντολής αυτής φαίνονται παρακάτω (η πλήρης ανάπτυξη των αποτελεσμάτων της εντολής φαίνεται στο Παράρτημα Β):

```
22/tcp   open  ssh      OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
25/tcp   open  smtp     Postfix smtpd
53/tcp   open  domain   NLnet Labs NSD
80/tcp   open  http     Apache httpd 2.4.62
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Did not follow redirect to https://aetos.iee.ihu.gr/
143/tcp  open  imap     Dovecot imapd
443/tcp  open  ssl/http Apache httpd 2.4.62
|_http-title: Did not follow redirect to http://people.iee.ihu.gr/
|_http-server-header: Apache/2.4.62 (Debian)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=aetos.iee.ihu.gr
|      Subject      Alternative      Name:      DNS:aetos.iee.ihu.gr,
DNS:aetos.it.teithe.gr, DNS:people.iee.ihu.gr
| Not valid before: 2025-06-17T04:03:04
|_Not valid after:  2025-09-15T04:03:03
465/tcp  open  ssl/smtp Postfix smtpd
993/tcp  open  ssl/imap Dovecot imapd
995/tcp  open  ssl/pop3 Dovecot pop3d
8008/tcp open  http?
```

Στη συνέχεια, για τον εντοπισμό κρυφών ή μη ευρέως γνωστών καταλόγων και αρχείων της ιστοσελίδας, εφαρμόστηκε η τεχνική directory fuzzing με χρήση του εργαλείου `ffuf`[81]. Μέσω της διαδικασίας αυτής, πραγματοποιούνται μαζικά αιτήματα HTTP σε διαφορετικές διαδρομές (paths), με σκοπό την ανίχνευση πιθανών πόρων που δεν είναι εμφανείς μέσω της κύριας πλοήγησης αλλά παραμένουν προσβάσιμοι από τον ιστό. Η ανακάλυψη τέτοιων καταλόγων μπορεί να οδηγήσει σε ευρήματα υψηλής σημασίας, όπως σελίδες διαχείρισης, αποθηκευμένα αρχεία ρυθμίσεων ή προσωρινά αντίγραφα δεδομένων. Παρακάτω παρουσιάζεται η εντολή που χρησιμοποιήθηκε για τον έλεγχο:

```
ffuf -c -w /usr/share/seclists/Discovery/Web-Content/big.txt -u
https://people.iee.ihu.gr/~dima/FUZZ
```

Τα πιο σημαντικά από τα αποτελέσματα της εντολής αυτής φαίνονται παρακάτω (η πλήρης ανάπτυξη των αποτελεσμάτων της εντολής φαίνεται στο Παράρτημα C):

```
.htaccess               [Status: 200, Size: 458, Words: 36, Lines:
7, Duration: 57ms]
mrtg                    [Status: 403, Size: 345, Words: 30, Lines:
10, Duration: 59ms]
mysql                   [Status: 301, Size: 330, Words: 20, Lines:
10, Duration: 54ms]
phpmyadmin              [Status: 301, Size: 335, Words: 20, Lines:
10, Duration: 56ms]
wp-admin                [Status: 301, Size: 333, Words: 20, Lines:
10, Duration: 52ms]
wp-content              [Status: 301, Size: 335, Words: 20, Lines:
10, Duration: 53ms]
wp-includes             [Status: 301, Size: 336, Words: 20, Lines:
10, Duration: 54ms]
www                     [Status: 403, Size: 345, Words: 30, Lines:
10, Duration: 51ms]
```

Μετά την εκτέλεση του αρχικού ελέγχου για την ανίχνευση γενικών καταλόγων και αρχείων, πραγματοποιήθηκε ένας πιο εξειδικευμένος έλεγχος προσανατολισμένος στο WordPress, το οποίο είχε ήδη εντοπιστεί στο προηγούμενο στάδιο αναγνώρισης. Για τον σκοπό αυτό χρησιμοποιήθηκε η παρακάτω εντολή:

```
ffuf -c -w /usr/share/seclists/Discovery/Web-
Content/CMS/wordpress.fuzz.txt -u
https://people.iee.ihu.gr/~dima/FUZZ
```

Η συγκεκριμένη εντολή αξιοποιεί το αρχείο λίστας `wordpress.fuzz.txt` από τη συλλογή SecLists[82], το οποίο περιλαμβάνει τυπικές και συχνά χρησιμοποιούμενες διαδρομές, αρχεία και καταλόγους που σχετίζονται με την εγκατάσταση και τη διαχείριση ενός ιστότοπου WordPress. Με αυτόν τον τρόπο, στοχεύονται ειδικά σημεία της πλατφόρμας που μπορεί να εκθέτουν πληροφορίες ή λειτουργίες προς εκμετάλλευση, όπως καταλόγοι διαχείρισης, αρχεία ρυθμίσεων, ή σημεία εισαγωγής προσθηκών (plugins).

Το αποτέλεσμα (output) της εντολής, καθώς ήταν αρκετά μεγάλο, έχει περιοριστεί μόνο στα ευρήματα τα οποία είναι άξια προσοχής στη διαδικασία του penetration testing. Παρακάτω φαίνονται οι σελίδες οι οποίες αφορούν θέματα ασφαλείας για την εγκατάσταση του WordPress και επιστρέφουν κωδικό HTTP Status 200:

```
readme.html             [Status: 200, Size: 7425, Words: 752, Lines:
99, Duration: 68ms]
license.txt            [Status: 200, Size: 19903, Words: 3331, Lines:
385, Duration: 57ms]
wp-admin/maint/repair.php [Status: 200, Size: 1726, Words: 86, Lines:
19, Duration: 184ms]
```

```
wp-admin/install.php     [Status: 200, Size: 1518, Words: 69, Lines:
17, Duration: 1094ms]

wp-includes/ID3/license.txt [Status: 200, Size: 1396, Words: 235,
Lines: 31, Duration: 63ms]

wp-admin/upgrade.php     [Status: 200, Size: 1430, Words: 62, Lines:
24, Duration: 1121ms]

wp-config.php            [Status: 200, Size: 0, Words: 1, Lines: 1,
Duration: 1112ms]

wp-includes/js/plupload/license.txt [Status: 200, Size: 17987, Words:
3013, Lines: 340, Duration: 58ms]

wp-includes/js/swfupload/license.txt [Status: 200, Size: 1540, Words:
207, Lines: 32, Duration: 65ms]

wp-includes/js/tinymce/license.txt [Status: 200, Size: 26441, Words:
4467, Lines: 505, Duration: 63ms]

wp-cron.php              [Status: 200, Size: 0, Words: 1, Lines: 1,
Duration: 1119ms]

wp-includes/version.php [Status: 200, Size: 0, Words: 1, Lines: 1,
Duration: 59ms]

wp-links-opml.php       [Status: 200, Size: 272, Words: 13, Lines: 12,
Duration: 1118ms]

wp-load.php              [Status: 200, Size: 0, Words: 1, Lines: 1,
Duration: 1145ms]

wp-trackback.php        [Status: 200, Size: 188, Words: 10, Lines: 5,
Duration: 1141ms]

wp-login.php            [Status: 200, Size: 11850, Words: 489, Lines:
146, Duration: 1867ms]

wp-admin/upgrade.php     [Status: 200, Size: 1430, Words: 62, Lines:
24, Duration: 1121ms]
```

Από τα παραπάνω συνολικά αποτελέσματα προκύπτει ότι οι σημαντικότεροι κίνδυνοι για την ασφάλεια της υπό εξέταση ιστοσελίδας εντοπίζονται σε αρχεία τα οποία, εάν παραμείνουν προσβάσιμα χωρίς περιορισμούς, μπορούν να δώσουν σε έναν επιτιθέμενο κρίσιμες πληροφορίες ή να του επιτρέψουν την εκτέλεση κακόβουλων ενεργειών. Ειδικότερα, αρχεία όπως τα `readme.html`, `license.txt` και `wp-includes/version.php` αποκαλύπτουν την ακριβή έκδοση του WordPress που χρησιμοποιείται, διευκολύνοντας έτσι την αντιστοίχιση με γνωστά CVE και την επιλογή κατάλληλων exploits. Το αρχείο wp-config.php αποτελεί έναν από τους πιο ευαίσθητους στόχους, καθώς περιέχει διαπιστευτήρια σύνδεσης με τη βάση δεδομένων και άλλες κρίσιμες ρυθμίσεις. Ακόμη και αν εμφανίζεται κενό λόγω ρυθμίσεων ασφαλείας, η διαρροή του θα μπορούσε να έχει καταστροφικές συνέπειες. Επιπλέον, αρχεία εγκατάστασης, αναβάθμισης ή συντήρησης όπως τα `wp-admin/install.php`, `wp-admin/upgrade.php` και `wp-admin/maint/repair.php` μπορούν να χρησιμοποιηθούν για την εκ νέου διαμόρφωση ή παραβίαση του συστήματος. Σημαντικό

ρόλο παίζουν και λειτουργικά endpoints όπως τα `wp-cron.php`, `wp-trackback.php`, `wp-links-opml.php`, `wp-load.php` και `wp-login.php`, τα οποία μπορεί να αποτελέσουν στόχο επιθέσεων brute force ή DoS. Ακόμα, η προσβασιμότητα του αρχείου `.htaccess` αποτελεί σοβαρή αδυναμία, καθώς μπορεί να αποκαλύψει ευαίσθητες ρυθμίσεις ασφαλείας και δομής του διακομιστή, διευκολύνοντας την παράκαμψη μηχανισμών προστασίας. Τέλος, η άμεση πρόσβαση σε αρχεία PHP εντός των φακέλων `wp-admin` και `wp-includes` χωρίς αυθεντικοποίηση ενέχει τον κίνδυνο εκτέλεσης μη εξουσιοδοτημένων εντολών ή αποκάλυψης εσωτερικών λειτουργιών, ιδιαίτερα σε περιπτώσεις λανθασμένης παραμετροποίησης. Συνεπώς, η περιορισμένη πρόσβαση ή η πλήρης απόκρυψη αυτών των αρχείων μέσω κατάλληλων ρυθμίσεων αποτελεί κρίσιμο μέτρο προστασίας για την ασφάλεια της πλατφόρμας.

Παρόλο που η πρόσβαση στα παραπάνω αρχεία και σελίδες δεν αποκαλύπτει άμεσα το περιεχόμενό τους (καθώς η φόρτωσή τους εμφανίζει απλώς μια λευκή σελίδα) η ύπαρξη ανοικτής, μη αυθεντικοποιημένης πρόσβασης εξακολουθεί να αποτελεί σημαντικό κίνδυνο ασφάλειας. Ακόμη και χωρίς ορατό περιεχόμενο, οι επιτιθέμενοι μπορούν να αξιοποιήσουν την πληροφορία ύπαρξης αυτών των αρχείων ή να εκμεταλλευτούν πιθανά σφάλματα παραμετροποίησης για να αποκτήσουν πρόσβαση ή να εκτελέσουν κακόβουλες ενέργειες. Για τον λόγο αυτό, η απαγόρευση πρόσβασης χωρίς αυθεντικοποίηση σε αυτά τα αρχεία και endpoints θα πρέπει να θεωρείται απαραίτητο μέτρο προστασίας σε κάθε εγκατάσταση WordPress.

Μία από τις μεθόδους που μπορούν να αξιοποιηθούν για την προστασία αυτών των αρχείων είναι η προσθήκη κατάλληλων κανόνων στο αρχείο `.htaccess` του Apache, μέσω των οποίων ελέγχεται η ύπαρξη cookies σύνδεσης του WordPress. Σε περίπτωση που δεν εντοπιστούν αντίστοιχα cookies, η πρόσβαση απορρίπτεται με κωδικό κατάστασης HTTP 403.

Παράδειγμα σχετικής υλοποίησης φαίνεται παρακάτω: [87][88]

```
<Files "upgrade.php">
    <IfModule mod_rewrite.c>
        RewriteEngine On
        RewriteCond %{HTTP_COOKIE} !wordpress_logged_in_
        RewriteRule .* - [R=403,L]
    </IfModule>
</Files>
```

Εναλλακτικά, η πρόσβαση μπορεί να περιοριστεί σε επίπεδο WordPress, αξιοποιώντας το αρχείο `functions.php` του θέματος. Μέσω της συνάρτησης `is_user_logged_in()`, πραγματοποιείται έλεγχος ώστε να διασφαλιστεί ότι μόνο συνδεδεμένοι χρήστες μπορούν να έχουν πρόσβαση σε συγκεκριμένα αρχεία.

Η υλοποίηση αυτής της μεθόδου παρουσιάζεται στο ακόλουθο παράδειγμα: [86]

```
function restrict_wp_admin() {
      if (!current_user_can('administrator') && !is_admin()) {
            if (strpos($_SERVER['REQUEST_URI'], 'wp-admin/') === 0){
                  wp_redirect(home_url('/login'));
```

```
            }
        }
}
add_action('admin_init', 'restrict_wp_admin');
```

Επιπλέον, για μεγαλύτερη ευελιξία και ευκολία διαχείρισης, μπορούν να χρησιμοποιηθούν εξειδικευμένα πρόσθετα ασφαλείας (security plugins), όπως το Wordfence, το οποία παρέχει δυνατότητες καθορισμού κανόνων πρόσβασης με βάση τον ρόλο του χρήστη.

Η συνδυαστική χρήση ελέγχων τόσο στο επίπεδο του διακομιστή (server-level restrictions) όσο και στο επίπεδο του WordPress (application-level checks) ενισχύει την προστασία της ιστοσελίδας και μειώνει σημαντικά τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.

Αφού εντοπίστηκαν και αναλύθηκαν οι σελίδες που επιστρέφουν κωδικό κατάστασης 200 (OK), οι οποίες είναι πλήρως προσβάσιμες χωρίς αυθεντικοποίηση και παρουσιάζουν άμεσο κίνδυνο, η επόμενη φάση της αξιολόγησης εστιάζει στα αποτελέσματα με κωδικό 302 (Found). Παρότι η ανακατεύθυνση συνήθως υποδεικνύει την ύπαρξη μηχανισμού αυθεντικοποίησης, στην πράξη δεν διασφαλίζει πάντα την προστασία του περιεχομένου, καθώς ορισμένα endpoints ενδέχεται να είναι προσβάσιμα ή λειτουργικά ακόμη και χωρίς έγκυρα διαπιστευτήρια, γεγονός που απαιτεί περαιτέρω διερεύνηση. Παρακάτω φαίνονται τα αποτελέσματα των σελίδων με κωδικό 302 απο το εργαλείο `ffuf` και τη wordlist του WordPress και συγκεκριμένα οι πιο κρίσιμες σελίδες που αφορούν ζητήματα ασφάλειας:

```
wp-activate.php           [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 1102ms]
wp-admin/import.php       [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 149ms]
wp-admin/ms-options.php [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 190ms]
wp-admin/network/plugin-install.php [Status: 302, Size: 0, Words: 1,
Lines: 1, Duration: 237ms]
wp-admin/network/plugin-editor.php [Status: 302, Size: 0, Words: 1,
Lines: 1, Duration: 285ms]
wp-admin/network/theme-install.php [Status: 302, Size: 0, Words: 1,
Lines: 1, Duration: 201ms]
wp-admin/network/theme-editor.php [Status: 302, Size: 0, Words: 1,
Lines: 1, Duration: 228ms]
wp-admin/plugin-editor.php [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 109ms]
wp-admin/plugin-install.php [Status: 302, Size: 0, Words: 1, Lines:
1, Duration: 159ms]
wp-admin/options.php      [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 192ms]
```

```
wp-admin/theme-editor.php [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 164ms]

wp-admin/theme-install.php [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 161ms]

wp-signup.php             [Status: 302, Size: 0, Words: 1, Lines: 1,
Duration: 1142ms]
```

Από την ανάλυση της λίστας των εντοπισμένων διευθύνσεων, η πλειοψηφία τους ανήκει στον φάκελο `wp-admin/`, ο οποίος αποτελεί τον διαχειριστικό πίνακα του WordPress. Η επιστροφή κωδικού 302 (redirect) προς τη σελίδα σύνδεσης είναι η αναμενόμενη συμπεριφορά για μη αυθεντικοποιημένους χρήστες και από μόνη της δεν υποδηλώνει ευπάθεια. Ωστόσο, ελλιπής αυθεντικοποίηση ή ανεπαρκείς μηχανισμοί προστασίας (π.χ. αδύναμοι κωδικοί, απουσία rate limiting σε login) μπορούν να καταστήσουν τις σελίδες αυτές ελκυστικούς στόχους για επιθέσεις. Ιδιαίτερα κρίσιμα αρχεία, όπως `plugin-editor.php` και `theme-editor.php`, επιτρέπουν την άμεση επεξεργασία κώδικα, ενώ τα `plugin-install.php` και `theme-install.php` μπορούν να χρησιμοποιηθούν για εγκατάσταση κακόβουλων πρόσθετων ή θεμάτων. Το `options.php` δίνει πρόσβαση σε κρίσιμες ρυθμίσεις, ενώ τα `wp-activate.php` και `wp-signup.php` μπορούν να αξιοποιηθούν για τη δημιουργία κακόβουλων λογαριασμών αν η εγγραφή είναι ενεργή χωρίς κατάλληλο έλεγχο. Επιπλέον, το `import.php` μπορεί να επιτρέψει την εισαγωγή κακόβουλων δεδομένων. Αξίζει να σημειωθεί ότι ορισμένες σελίδες, όπως το `wp-admin/upgrade.php`, παρότι επιστρέφουν 302 κατά τη σάρωση, στην πράξη είναι πλήρως προσβάσιμες και λειτουργικές χωρίς αυθεντικοποίηση, γεγονός που αυξάνει σημαντικά τον κίνδυνο αν χρησιμοποιηθούν από μη εξουσιοδοτημένους χρήστες.

5.2.3 Σύνοψη Συλογής Πληροφοριών

Η συνδυαστική εφαρμογή παθητικών και ενεργών τεχνικών συλλογής δεδομένων επέτρεψε τη διαμόρφωση μιας ολοκληρωμένης εικόνας για την υποδομή και τις πιθανές αδυναμίες του στόχου. Οι παθητικές μέθοδοι παρείχαν χρήσιμες πληροφορίες χωρίς άμεση αλληλεπίδραση με το σύστημα, περιορίζοντας τον κίνδυνο ανίχνευσης, ενώ οι ενεργές τεχνικές αποκάλυψαν κρίσιμες λεπτομέρειες σχετικά με τις υπηρεσίες, τις εκδόσεις λογισμικού και τα διαθέσιμα endpoints. Η ανάλυση αυτών των δεδομένων αποτέλεσε τη βάση για τον εντοπισμό πιθανών ευπαθειών και τη στοχευμένη συνέχιση της διαδικασίας του penetration testing, επιβεβαιώνοντας τη σημασία μιας καλά σχεδιασμένης και ισορροπημένης προσέγγισης στη φάση της αναγνώρισης.

5.3 Vulnerability Detection

Το στάδιο της ανίχνευσης ευπαθειών επικεντρώνεται στον εντοπισμό αδυναμιών που μπορούν να αποτελέσουν σημεία εισόδου για έναν πιθανό επιτιθέμενο. Για τις ανάγκες της παρούσας εργασίας, αξιοποιήθηκε το εξειδικευμένο εργαλείο WPScan, το οποίο είναι σχεδιασμένο αποκλειστικά για την ανάλυση ιστοσελίδων που βασίζονται στην πλατφόρμα WordPress. Μέσω της χρήσης του, πραγματοποιήθηκε σάρωση για τον εντοπισμό γνωστών ευπαθειών σε θέματα (themes), πρόσθετα (plugins) και στην ίδια την εγκατάσταση του WordPress, καθώς και για τον έλεγχο λανθασμένων ρυθμίσεων ή εκδόσεων λογισμικού που έχουν συσχετιστεί με δημοσιευμένα CVE. Η διαδικασία αυτή παρείχε στοχευμένες και τεκμηριωμένες πληροφορίες, οι οποίες αποτέλεσαν τη βάση για την αξιολόγηση του επιπέδου ασφάλειας της ιστοσελίδας και τη διαμόρφωση προτάσεων για τη μείωση των εντοπισμένων κινδύνων.

Αρχικά, για την εκτέλεση της διαδικασίας ανίχνευσης ευπαθειών χρησιμοποιήθηκε η εντολή:

```
wpscan --url https://people.iee.ihu.gr/~dima/ --enumerate p --plugins-detection aggressive
```

Ωστόσο, το εργαλείο επέστρεψε το ακόλουθο μήνυμα στο output:

```
Scan Aborted: The target is responding with a 403, this might be due to a WAF. Please re-try with --random-user-agent
```

Όπως φαίνεται και από τα παραπάνω αποτελέσματα, η απόκριση 403 υποδεικνύει την ύπαρξη μηχανισμών φιλτραρίσματος, πιθανόν μέσω Web Application Firewall (WAF), οι οποίοι αποτρέπουν τέτοιου είδους αυτοματοποιημένους ελέγχους, προστατεύοντας το σύστημα από μη εξουσιοδοτημένες προσπάθειες εντοπισμού ευπαθειών. Παρόλα αυτά, όταν προστέθηκε το option `--random-user-agent`, ο έλεγχος πραγματοποιήθηκε χωρίς κάποια παρεμπόδιση, παρακάμπτοντας ουσιαστικά τον περιορισμό. Αυτό καταδεικνύει ότι, παρά την ύπαρξη μέτρων προστασίας, απαιτείται η υλοποίηση πιο ισχυρών μηχανισμών αποτροπής τέτοιου είδους enumeration, ώστε να μην είναι εφικτή η συλλογή κρίσιμων πληροφοριών από πιθανούς επιτιθέμενους.

Με την εκτέλεση της εντολής με την προσθήκη της παραμέτρου:

```
wpscan --url https://people.iee.ihu.gr/~dima/ --enumerate p --plugins-detection aggressive --random-user-agent
```

ο έλεγχος ολοκληρώθηκε επιτυχώς, παρακάμπτοντας τον μηχανισμό που προηγουμένως απαντούσε με 403 Forbidden. Τα πιο σημαντικά από τα αποτελέσματα της εντολής αυτής φαίνονται παρακάτω (η πλήρης ανάπτυξη των αποτελεσμάτων της εντολής φαίνεται στο Παράρτημα D):

```
[+] XML-RPC seems to be enabled: https://people.iee.ihu.gr/~dima/xmlrpc.php
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API


[i] Plugin(s) Identified:
[+] contact-form-7
 | [!] The version is out of date, the latest version is 6.1
 | [!] Directory listing is enabled
 | Version: 6.0.6 (90% confidence)


[+] livemesh-siteorigin-widgets
 | Latest Version: 3.9.1 (up to date)
 | [!] Directory listing is enabled
 | Version: 3.9.1 (100% confidence)
```

```
[+] siteorigin-panels
 | [!] The version is out of date, the latest version is 2.32.1
 | [!] Directory listing is enabled
 | Version: 2.31.8 (80% confidence)

[+] so-css
 | Latest Version: 1.6.4 (up to date)
 | [!] Directory listing is enabled
 | Version: 1.6.4 (100% confidence)

[+] so-widgets-bundle
 | [!] The version is out of date, the latest version is 1.69.2
 | [!] Directory listing is enabled
 | Version: 1.68.5 (80% confidence)
```

Στα αποτελέσματα εμφανίστηκε πλήρης λίστα των ανιχνευμένων plugins της εγκατάστασης WordPress, συνοδευόμενη από τις εκδόσεις τους και σχετικές πληροφορίες για γνωστές ευπάθειες, όπου αυτές υπήρχαν. Η δυνατότητα αυτή του WPScan να παρακάμπτει βασικούς μηχανισμούς φιλτραρίσματος δείχνει ότι η υπάρχουσα προστασία του συστήματος δεν επαρκεί απέναντι σε πιο στοχευμένες τεχνικές enumeration. Συνεπώς, καθίσταται σαφές ότι απαιτείται ενίσχυση των μέτρων ασφαλείας, όπως αυστηρότεροι κανόνες στο WAF, περιορισμός των HTTP headers, ή και δυναμικά φίλτρα εντοπισμού ύποπτης συμπεριφοράς, ώστε να μειωθεί η έκθεση πληροφοριών που μπορούν να αξιοποιηθούν σε μετέπειτα στάδια επίθεσης.

Από τα αποτελέσματα του WPScan προκύπτουν αρκετά σημεία που μπορούν να αποτελέσουν πεδίο εκμετάλλευσης από έναν κακόβουλο χρήστη. Πρώτον, η ενεργοποίηση του `XML-RPC` (`xmlrpc.php`) αποτελεί γνωστό σημείο τρωτότητας στο WordPress, καθώς επιτρέπει σε έναν επιτιθέμενο να πραγματοποιήσει μαζικές προσπάθειες σύνδεσης (brute-force) ή να εκτελέσει pingback επιθέσεις DDoS, χρησιμοποιώντας τον ιστότοπο ως ενδιάμεσο. [73]

Σχετικά με τα plugins, η ύπαρξη του Contact Form 7 σε έκδοση 6.0.6, σε συνδυασμό με ενεργοποιημένο directory listing στον φάκελό του `/wp-content/plugins/contact-form-7/`, αποκαλύπτει δημόσια τη δομή και τα αρχεία του plugin. Αυτό διευκολύνει έναν επιτιθέμενο να αναγνωρίσει ακριβώς την έκδοση και να αναζητήσει γνωστές ευπάθειες, όπως η CVE που αφορά XSS επιθέσεις.[74] Το ίδιο πρόβλημα ισχύει και για το plugin `livemesh-siteorigin-widgets`, όπου η ενεργοποίηση directory listing παρέχει ορατότητα στον κώδικα και τις βιβλιοθήκες που χρησιμοποιούνται, κάτι που μπορεί να αξιοποιηθεί για αναγνώριση και εκμετάλλευση πιθανών κενών ασφαλείας.

Στο SiteOrigin Panels (έκδοση 2.31.8, παλαιότερη από την τρέχουσα) η συνύπαρξη outdated έκδοσης και directory listing αυξάνει τον κίνδυνο, καθώς τυχόν γνωστά exploits για παλαιότερες εκδόσεις είναι πιθανό να παραμένουν ενεργά. Παρόμοια εικόνα παρατηρείται στο `so-css`, όπου, αν και είναι ενημερωμένο, η δυνατότητα καταλόγου δίνει πληροφορίες που ιδανικά δεν θα έπρεπε να είναι ορατές.

Το πιο σοβαρό εύρημα είναι στο SiteOrigin Widgets Bundle (έκδοση 1.68.5), το οποίο είναι εκτός ενημέρωσης και ευάλωτο σε Stored XSS μέσω του attribute `data-url` σε DOM elements, όπως αναφέρεται στο WPScan advisory. Η ευπάθεια αυτή επιτρέπει σε χρήστες με ρόλο τουλάχιστον Contributor να εισάγουν κακόβουλο JavaScript, το οποίο εκτελείται στους browsers άλλων χρηστών, ανοίγοντας τον δρόμο για κλοπή cookies, λογαριασμών ή ακόμα και εκτέλεση διοικητικών ενεργειών χωρίς άδεια. [75]

Συνολικά, η συνύπαρξη παλαιών εκδόσεων, ενεργοποιημένου directory listing και γνωστών ευπαθειών δημιουργεί ένα επικίνδυνο περιβάλλον όπου ένας επιτιθέμενος μπορεί να πραγματοποιήσει enumeration, να ταυτοποιήσει εκδόσεις, να αναζητήσει public exploits και να εκτελέσει επιθέσεις με ελάχιστη προσπάθεια. Μέτρα όπως η απενεργοποίηση του directory listing, η άμεση ενημέρωση των plugins και η απενεργοποίηση του `XML-RPC` είναι κρίσιμα για τη μείωση αυτών των κινδύνων.

5.4 Επίλογος

Ολοκληρώνοντας το κεφάλαιο του πρακτικού σεναρίου επίθεσης στην ιστοσελίδα WordPress, γίνεται σαφές ότι ακόμη και σε ένα περιβάλλον ελεγχόμενης δοκιμής, η αναγνώριση και η εκμετάλλευση ευπαθειών μπορούν να αποκαλύψουν σημαντικές αδυναμίες στην ασφάλεια ενός συστήματος. Μέσα από τα στάδια παθητικής και ενεργής συλλογής πληροφοριών, ανίχνευσης ευπαθειών και θεωρητικής αξιολόγησης πιθανών εκμεταλλεύσεων, καταδείχθηκε πως ο συνδυασμός παρωχημένων εκδόσεων λογισμικού, μη ασφαλών ρυθμίσεων (όπως η ενεργοποίηση directory listing και `XML-RPC`) και γνωστών τρωτοτήτων σε δημοφιλή plugins, μπορεί να επιτρέψει σε έναν κακόβουλο χρήστη να προχωρήσει σε στοχευμένες και αποτελεσματικές επιθέσεις. Παρά το γεγονός ότι το σενάριο εκτελέστηκε σε ερευνητικό πλαίσιο, τα αποτελέσματα αντικατοπτρίζουν ρεαλιστικούς κινδύνους που συναντώνται σε πραγματικές εγκαταστάσεις WordPress, υπογραμμίζοντας την ανάγκη για συστηματική εφαρμογή ενημερώσεων, βέλτιστων πρακτικών ασφάλειας και περιορισμό της έκθεσης κρίσιμων πόρων στο διαδίκτυο. Το συγκεκριμένο πρακτικό μέρος απέδειξε ότι η προληπτική ανίχνευση και αξιολόγηση ευπαθειών αποτελεί καθοριστικό παράγοντα για την έγκαιρη αντιμετώπιση κυβερνοαπειλών και την ενίσχυση της συνολικής θωράκισης ενός ιστότοπου.

Κεφάλαιο 6ο: Συμπεράσματα και προτάσεις βελτίωσης

Η πτυχιακή εργασία ανέπτυξε ένα ενιαίο σύνολο θεωρητικών και πρακτικών γνώσεων, εστιάζοντας σε τομείς όπως η δικτύωση, η κυβερνοασφάλεια, το penetration testing και η εφαρμογή ενός ρεαλιστικού σεναρίου επίθεσης σε ιστοσελίδα WordPress. Αρχικά, εξετάστηκαν οι βασικές αρχές των δικτύων και η λειτουργία τους, παρέχοντας το τεχνικό υπόβαθρο που απαιτείται για την κατανόηση της ασφάλειας συστημάτων. Στη συνέχεια, αναλύθηκαν κρίσιμες έννοιες της κυβερνοασφάλειας, δίνοντας έμφαση στο πώς οι απειλές, οι αδυναμίες και οι μηχανισμοί άμυνας αλληλεπιδρούν στο σύγχρονο ψηφιακό περιβάλλον. Ένα ιδιαίτερο βάρος δόθηκε στη μεθοδολογία του penetration testing, τόσο θεωρητικά όσο και μέσα από την πρακτική προσέγγιση, η οποία περιλάμβανε παθητική και ενεργή συλλογή πληροφοριών, ανίχνευση ευπαθειών και θεωρητική αξιολόγηση πιθανών εκμεταλλεύσεων.

Παρά την ολοκληρωμένη προετοιμασία και την αναλυτική διερεύνηση των αρχικών σταδίων, η υλοποίηση του πλήρους κύκλου του penetration testing αντιμετώπισε περιορισμούς. Δεν ήταν εφικτή η πρακτική εφαρμογή πιο προχωρημένων σταδίων, όπως η εκμετάλλευση ευπαθειών (exploitation), η διατήρηση πρόσβασης (persistence) και η αναβάθμιση δικαιωμάτων (privilege escalation), καθώς η παραμετροποίηση σχετικών ρυθμίσεων μπορούσε μόνο να πραγματοποιηθεί από τον διαχειριστή του διακομιστή και όχι τον διαχειριστή της ιστοσελίδας. Ως εκ τούτου, δεν υπήρχε δυνατότητα επέμβασης σε κρίσιμες ρυθμίσεις ή προσαρμογής του περιβάλλοντος ώστε να επιτραπεί η πλήρης προσομοίωση επιθέσεων. Επιπλέον, η ύπαρξη ενεργού firewall περιόριζε σημαντικά την υλοποίηση επιθέσεων, δεδομένου ότι θα έπρεπε να έχει ρυθμιστεί με τέτοιον τρόπο ώστε να δέχεται αιτήματα από συγκεκριμένη διεύθυνση IP για να καταστεί εφικτή η συνέχιση της δοκιμής. Οι περιορισμοί αυτοί οδήγησαν στην εστίαση στα πρώτα στάδια της διαδικασίας, με έμφαση στην καταγραφή, τεκμηρίωση και ανάλυση των εντοπισμένων ευπαθειών, χωρίς την επιβεβαίωση μέσω πλήρους αλυσίδας επίθεσης.

Η μελλοντική ενασχόληση με το ίδιο περιβάλλον ή με παρόμοιο σενάριο θα μπορούσε να επεκτείνει την εργασία, καλύπτοντας τα στάδια που παρέμειναν σε θεωρητικό επίπεδο. Σε μεταγενέστερη χρονική στιγμή, για παράδειγμα κατά τη θερινή περίοδο όπου η ιστοσελίδα δεν χρησιμοποιείται ενεργά για τις ανάγκες μαθημάτων, θα ήταν εφικτή η υλοποίηση των βημάτων που δεν κατέστη δυνατό να πραγματοποιηθούν στο παρόν πλαίσιο. Μια τέτοια συνέχεια θα επέτρεπε την εμπειρική επαλήθευση των ευρημάτων, την πλήρη αξιολόγηση του κινδύνου και τη διαμόρφωση πιο στοχευμένων προτάσεων για την ενίσχυση της ασφάλειας. Με αυτόν τον τρόπο, η μελέτη θα αποκτούσε ακόμη μεγαλύτερη αξία τόσο ερευνητικά όσο και πρακτικά, συμβάλλοντας ουσιαστικά στην κατανόηση και αντιμετώπιση των σύγχρονων κυβερνοαπειλών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Standage, T. (1998). The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers.

[2] Ceruzzi, Paul E. *A history of modern computing*. MIT press, 2003.

[3] https://en.wikipedia.org/wiki/ENIAC#/media/File:ENIAC_Penn1.jpg

[4] https://www.valuerworld.com/wp-content/uploads/2022/01/signal.jpg

[5] Kurose, James, and Keith Ross. "Computer networks: A top down approach featuring the internet." (2010).

[6] Abbate, Janet, and Joel McKim. "Inventing the internet." *Canadian Journal of Communication* 26.1 (2001): 155.

[7] Comer, Douglas E. *Internetworking with tcp/ip*. Addison-Wesley Professional, 2013.

[8] Hafner, Katie, and Matthew Lyon. *Where wizards stay up late: The origins of the Internet*. Simon and Schuster, 1998.

[9] Leiner, Barry M., et al. "A brief history of the Internet." *ACM SIGCOMM computer communication review* 39.5 (2009): 22-31.

[10] Cerf, Vinton, and Robert Kahn. "A protocol for packet network intercommunication." *IEEE Transactions on communications* 22.5 (1974): 637-648.

[11] https://en.wikipedia.org/wiki/ARPANET#/media/File:Arpanet_in_the_1970s.png

[12] Saltzer, Jerome H., David P. Reed, and David D. Clark. "End-to-end arguments in system design." *ACM Transactions on Computer Systems (TOCS)* 2.4 (1984): 277-288.

[13] https://en.wikipedia.org/wiki/Internet_protocol_suite#/media/File:IP_stack_connections.svg

[14] Berners-Lee, Tim, et al. "The world-wide web." *Linking the World's Information: Essays on Tim Berners-Lee's Invention of the World Wide Web*. 2023. 51-65.

[15] https://en.wikipedia.org/wiki/NCSA_Mosaic#/media/File:NCSA_Mosaic_Browser_Screenshot.png

[16] Mukherjee, Biswanath. "WDM optical communication networks: progress and challenges." *IEEE Journal on Selected Areas in communications* 18.10 (2002): 1810-1824.

[17] https://itel.com/blog/how-fibre-optic-internet-works/

[18] Andrews, Jeffrey G., et al. "What will 5G be?." *IEEE Journal on selected areas in communications* 32.6 (2014): 1065-1082.

[19] O'reilly, Tim. *What is web 2.0*. " O'Reilly Media, Inc.", 2009.

[20] Kaplan, Andreas M., and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media." *Business horizons* 53.1 (2010): 59-68.

[21] https://en.wikipedia.org/wiki/Social_media#/media/File:Social_media_collection_2020s.png

[22] Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7 (2013): 1645-1660.

[23] https://vtcnetviet.com/iot-la-gi/

[24] Day, John D., and Hubert Zimmermann. "The OSI reference model." *Proceedings of the IEEE* 71.12 (1983): 1334-1340.

[25] https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

[26] ANDREW STANENBAUM and WETHERALL DAVID J. "COMPUTER NETWORKS FIFTH EDITION." (2011).

[27] https://www.darkrelay.com/post/tcp-ip-model

[28] Kurose, James F., and Keith W. Ross. "Computer networking: A top-down approach edition." *Addision Wesley* 12 (2007).

[29] Fielding, Roy, et al. *Hypertext transfer protocol--HTTP/1.1*. No. rfc2616. 1999.

[30] Postel, Jon, and Joyce Reynolds. *File transfer protocol*. No. rfc959. 1985.

[31] Klensin, John. *Simple mail transfer protocol*. No. rfc5321. 2008.

[32] Mockapetris, Paul. *Domain names-concepts and facilities*. No. rfc1034. 1987.

[33] Postel, Jon, and Joyce K. Reynolds. *Telnet protocol specification*. No. rfc854. 1983.

[34] Ylonen, Tatu, and Chris Lonvick. *The secure shell (SSH) transport layer protocol*. No. rfc4253. 2006.

[35] Droms, Ralph. *Dynamic host configuration protocol*. No. rfc2131. 1997.

[36] Guttman, Barbara. *An introduction to computer security: the NIST handbook*. Vol. 800. No. 12. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 1995.

[37] Whitman, Michael E., and Herbert J. Mattord. *Principles of information security*. Boston, MA: Thomson Course Technology, 2009.

[38] https://www.fortinet.com/resources/cyberglossary/cia-triad

[39] Souppaya, Murugiah, and Karen Scarfone. "Guide to malware incident prevention and handling for desktops and laptops." NIST Special Publication 800 (2013): 83.

[40] Cost of a Data Breach Report 2025

[41] Farhat, Danyal, and Malik Shahzad Awan. "A brief survey on ransomware with the perspective of internet security threat reports." 2021 9th international symposium on digital forensics and security (ISDFS). IEEE, 2021.

[42] Handley, Mark, and Eric Rescorla. Internet denial-of-service considerations. No. rfc4732. 2006.

[43] https://en.wikipedia.org/wiki/Client%E2%80%93server_model#/media/File:Client-server-model.svg

[44] Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.

[45] Scarfone, Karen, et al. "Technical guide to information security testing and assessment." *NIST Special Publication* 800.115 (2008).

[46] Whitman, Michael E., and Herbert J. Mattord. *Principles of information security*. Boston, MA: Thomson Course Technology, 2009.

[47] Bazzell, Michael. *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform, 2016.

[48] Kuppa, Aditya, Lamine Aouad, and Nhien-An Le-Khac. "Linking cve's to mitre att&ck techniques." *Proceedings of the 16th International Conference on Availability, Reliability and Security*. 2021.

[49] OWASP Top Ten

[50] https://owasp.org/

[51] A03:2021 - Injection

[52] API2:2023 Broken Authentication

[53] A3:2017-Sensitive Data Exposure

[54] XML External Entity (XXE) Processing

[55] A01:2021 - Broken Access Control

[56] A05:2021 - Security Misconfiguration

[57] A7:2017-Cross-Site Scripting (XSS)

[58] A8:2017-Insecure Deserialization

[59] A9:2017-Using Components with Known Vulnerabilities

[60] A10:2017-Insufficient Logging & Monitoring

[61] Kennedy, David, et al. Metasploit: the penetration tester's guide. No Starch Press, 2011.

[62] Zhang, Wei, Ju Xing, and Xiaoqi Li. "Penetration Testing for System Security: Methods and Practical Approaches." arXiv preprint arXiv:2505.19174 (2025).

[63] Yisa, Victor, Meshach Baba, and Emmanuel Olaniyi. "A review of top open source password cracking tools." International Conference on Information and Communication Technology and Its Applications (ICTA 2016), 2016.

[64] Sayar, Imen, et al. "An in-depth study of java deserialization remote-code execution exploits and vulnerabilities." ACM Transactions on Software Engineering and Methodology 32.1 (2023): 1-45.

[65] Hubczyk, Michal, Adam Domanski, and Joanna Domanska. "Local and remote file inclusion." Internet-Technical Developments and Applications 2. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. 189-200.

[66] Yadmani, Soufian El, Robin The, and Olga Gadyatskaya. "Beyond the Surface: Investigating Malicious CVE Proof of Concept Exploits on GitHub." arXiv preprint arXiv:2210.08374 (2022).

[67] Kaushik, Keshav, et al. "A novel approach to generate a reverse shell: Exploitation and Prevention." International Journal of Intelligent Communication, Computing and Networks Open Access Journal (2021): 2582-7707.

[68] Mohammad Ali Pour, Fazel, and Mohammadreza Rashidi. "The Art of Post-Exploitation." The Art of Post-Exploitation (2024).

[69] Happe, Andreas, and Jürgen Cito. "Got root? a linux priv-esc benchmark." arXiv preprint arXiv:2405.02106 (2024).

[70] Kowira, Evander Marvel, N. Nik Suki, and Yogeswaran Nathan. "Automated privilege escalation enumeration and execution script for linux." AIP Conference Proceedings. Vol. 2802. No. 1. AIP Publishing LLC, 2024.

[71] Alghamdi, Abdulrahman A. "Effective penetration testing report writing." 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). IEEE, 2021.

[72] https://www.wappalyzer.com/

[73] https://www.hostinger.com/tutorials/xmlrpc-wordpress

[74] https://wpscan.com/vulnerability/7dbafbe2-abbc-4191-a587-afa89c2f7421/

[75] https://wpscan.com/vulnerability/9338a598-8f61-4aee-b9fb-f3c88966efad/

[76] Cerf, Vinton, and Robert Kahn. "A protocol for packet network intercommunication." IEEE Transactions on communications 22.5 (1974)

[77] https://github.com/openwall/john

[78] https://github.com/vanhauser-thc/thc-hydra

[79] https://github.com/hashcat/hashcat

[80] https://nmap.org

[81] https://github.com/ffuf/ffuf

[82] https://github.com/danielmiessler/SecLists

[83] https://en.wikipedia.org/wiki/Denial-of-service_attack#/media/File:Stachledraht_DDos_Attack.svg

[84] Washo, Amy Hetro. "An interdisciplinary view of social engineering: A call to action for research." Computers in Human Behavior Reports 4 (2021): 100126.

[85] Alabdan, Rana. "Phishing attacks survey: Types, vectors, and technical approaches." Future internet 12.10 (2020): 168.

[86] https://wordpress.org/support/topic/restrict-and-block-access-to-wp-login-php-and-wp-admin-to-non-admins/

[87] https://developer.wordpress.org/advanced-administration/wordpress/cookies/

[88] https://httpd.apache.org/docs/2.4/rewrite/flags.html

ΠΑΡΑΡΤΗΜΑ Α : Πλήρη Αποτελέσματα Εντολής `dig`

```
dig A people.iee.ihu.gr
; <<>> DiG 9.20.9-1-Debian <<>> A people.iee.ihu.gr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5712
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 6

;; QUESTION SECTION:
;people.iee.ihu.gr.             IN      A

;; ANSWER SECTION:
people.iee.ihu.gr.      85796   IN      CNAME   aetos.iee.ihu.gr.
aetos.iee.ihu.gr.       20996   IN      A       195.251.123.232

;; AUTHORITY SECTION:
gr.                     31321   IN      NS      gr-at.ics.forth.gr.
gr.                     31321   IN      NS      gr-m.ics.forth.gr.
gr.                     31321   IN      NS      gr-c.ics.forth.gr.
gr.                     31321   IN      NS      gr-d.ics.forth.gr.
gr.                     31321   IN      NS      grdns.ics.forth.gr.
gr.                     31321   IN      NS      estia.ics.forth.gr.

;; ADDITIONAL SECTION:
gr-at.ics.forth.gr.     31321   IN      A       78.104.145.227
gr-m.ics.forth.gr.      31321   IN      A       194.0.4.10
gr-c.ics.forth.gr.      47317   IN      A       194.0.1.25
gr-d.ics.forth.gr.      31321   IN      A       194.0.11.102
grdns.ics.forth.gr.     47317   IN      A       139.91.1.1
estia.ics.forth.gr.     47317   IN      A       139.91.191.3

;; Query time: 8 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Sat Jul 26 06:56:36 EDT 2025
;; MSG SIZE  rcvd: 304
```

ΠΑΡΑΡΤΗΜΑ Β : Πλήρη Αποτελέσματα Εντολής nmap

```
sudo nmap -sSVC 195.251.123.232 -A


Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 07:28 EDT
Nmap scan report for aetos.iee.ihu.gr (195.251.123.232)
Host is up (0.0064s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 9.2p1 Debian 2+deb12u6 (protocol 2.0)
| ssh-hostkey:
|   256 8d:dc:14:66:55:9f:e9:85:b1:40:ea:d3:8d:27:1f:16 (ECDSA)
|_  256 96:27:7e:e8:2c:bd:ab:b3:b9:f1:25:f1:77:ef:61:81 (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: aetos.it.teithe.gr, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
| ssl-cert: Subject: commonName=aetos.it.teithe.gr
| Subject Alternative Name: DNS:aetos.it.teithe.gr
| Not valid before: 2025-07-03T21:01:26
|_Not valid after:  2025-10-01T21:01:25
|_ssl-date: TLS randomness does not represent time
53/tcp   open  domain   NLnet Labs NSD
80/tcp   open  http     Apache httpd 2.4.62
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Did not follow redirect to https://aetos.iee.ihu.gr/
143/tcp  open  imap     Dovecot imapd
|_ssl-date: TLS randomness does not represent time
|_imap-capabilities: have STARTTLS IDLE OK more IMAP4rev1 LOGIN-REFERRALS
post-login SASL-IR listed capabilities Pre-login ENABLE LOGINDISABLEDA0001
ID LITERAL+
| ssl-cert: Subject: commonName=aetos.it.teithe.gr
| Subject Alternative Name: DNS:aetos.it.teithe.gr
| Not valid before: 2025-05-04T19:40:25
|_Not valid after:  2025-08-02T19:40:24
443/tcp  open  ssl/http Apache httpd 2.4.62
|_http-title: Did not follow redirect to http://people.iee.ihu.gr/
|_http-server-header: Apache/2.4.62 (Debian)
```

|_ssl-date: TLS randomness does not represent time

| ssl-cert: Subject: commonName=aetos.iee.ihu.gr

| Subject Alternative Name: DNS:aetos.iee.ihu.gr, DNS:aetos.it.teithe.gr, DNS:people.iee.ihu.gr

| Not valid before: 2025-06-17T04:03:04

|_Not valid after: 2025-09-15T04:03:03

465/tcp open ssl/smtp Postfix smtpd

|_smtp-commands: aetos.it.teithe.gr, PIPELINING, SIZE 10240000, VRFY, ETRN, AUTH PLAIN, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING

| ssl-cert: Subject: commonName=aetos.it.teithe.gr

| Subject Alternative Name: DNS:aetos.it.teithe.gr

| Not valid before: 2025-07-03T21:01:26

|_Not valid after: 2025-10-01T21:01:25

|_ssl-date: TLS randomness does not represent time

993/tcp open ssl/imap Dovecot imapd

| ssl-cert: Subject: commonName=aetos.it.teithe.gr

| Subject Alternative Name: DNS:aetos.it.teithe.gr

| Not valid before: 2025-05-04T19:40:25

|_Not valid after: 2025-08-02T19:40:24

|_ssl-date: TLS randomness does not represent time

|_imap-capabilities: AUTH=PLAINA0001 listed IDLE OK more IMAP4rev1 LOGIN-REFERRALS SASL-IR have post-login Pre-login ENABLE capabilities ID LITERAL+

995/tcp open ssl/pop3 Dovecot pop3d

|_pop3-capabilities: SASL(PLAIN) CAPA TOP AUTH-RESP-CODE UIDL USER RESP-CODES PIPELINING

| ssl-cert: Subject: commonName=aetos.it.teithe.gr

| Subject Alternative Name: DNS:aetos.it.teithe.gr

| Not valid before: 2025-05-04T19:40:25

|_Not valid after: 2025-08-02T19:40:24

|_ssl-date: TLS randomness does not represent time

8008/tcp open http?

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: bridge|VoIP adapter|general purpose

Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (94%), QEMU (93%)

OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu

```
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&amp;amp;T
BGW210 voice gateway (94%), QEMU user mode network gateway (93%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 1 hop

Service Info: Hosts:  aetos.it.teithe.gr, aetos.it.teithe.gr; OS: Linux; CPE:
cpe:/o:linux:linux_kernel


TRACEROUTE (using port 80/tcp)

HOP RTT     ADDRESS

1   0.12 ms aetos.iee.ihu.gr (195.251.123.232)


OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 171.02 seconds
```

ΠΑΡΑΡΤΗΜΑ C : Πλήρη Αποτελέσματα Εντολής ffuf

```
ffuf -c -w /usr/share/seclists/Discovery/Web-Content/big.txt -u https://people.iee.ihu.gr/~dima/FUZZ
```

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://people.iee.ihu.gr/~dima/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 200, Size: 458, Words: 36, Lines: 7, Duration: 57ms]
mrtg                    [Status: 403, Size: 345, Words: 30, Lines: 10, Duration: 59ms]
mysql                   [Status: 301, Size: 330, Words: 20, Lines: 10, Duration: 54ms]
phpmyadmin              [Status: 301, Size: 335, Words: 20, Lines: 10, Duration: 56ms]
wp-admin                [Status: 301, Size: 333, Words: 20, Lines: 10, Duration: 52ms]
wp-content              [Status: 301, Size: 335, Words: 20, Lines: 10, Duration: 53ms]
```

```
wp-includes                 [Status: 301, Size: 336, Words: 20, Lines: 10,
Duration: 54ms]
www                         [Status: 403, Size: 345, Words: 30, Lines: 10,
Duration: 51ms]
:: Progress: [20478/20478] :: Job [1/1] :: 754 req/sec :: Duration: [0:00:31]
:: Errors: 0 ::
```

ΠΑΡΑΡΤΗΜΑ D : Πλήρη Αποτελέσματα Εντολής `wpscan`

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://people.iee.ihu.gr/~dima/ [195.251.123.232]
[+] Started: Sat Jul 26 07:51:26 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.62 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: https://people.iee.ihu.gr/~dima/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |                                                              -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_sc
anner/
 |                                                              -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
```

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/

| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://people.iee.ihu.gr/~dima/readme.html

| Found By: Direct Access (Aggressive Detection)

| Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://people.iee.ihu.gr/~dima/wp-cron.php

| Found By: Direct Access (Aggressive Detection)

| Confidence: 60%

| References:

| - https://www.iplocation.net/defend-wordpress-from-ddos

| - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.8.2 identified (Latest, released on 2025-07-15).

| Found By: Rss Generator (Passive Detection)

| - https://people.iee.ihu.gr/~dima/?feed=rss2, <generator>https://wordpress.org/?v=6.8.2</generator>

| - https://people.iee.ihu.gr/~dima/?feed=comments-rss2, <generator>https://wordpress.org/?v=6.8.2</generator>

[+] WordPress theme in use: travel-eye

| Location: https://people.iee.ihu.gr/~dima/wp-content/themes/travel-eye/

| Last Updated: 2025-07-10T00:00:00.000Z

| Readme: https://people.iee.ihu.gr/~dima/wp-content/themes/travel-eye/readme.txt

| [!] The version is out of date, the latest version is 2.0

| Style URL: https://people.iee.ihu.gr/~dima/wp-content/themes/travel-eye/style.css?ver=1.9.3

| Style Name: Travel Eye

| Style URI: https://wenthemes.com/item/wordpress-themes/travel-eye/

| Description: Travel Eye is a clean and professional Travel WordPress Theme. This Theme is ideal for travel agenci...

```
 | Author: WEN Themes
 | Author URI: https://wenthemes.com/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.9.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |           -     https://people.iee.ihu.gr/~dima/wp-content/themes/travel-
eye/style.css?ver=1.9.3, Match: 'Version: 1.9.3'



[i] Plugin(s) Identified:


[+] contact-form-7
 |   Location:   https://people.iee.ihu.gr/~dima/wp-content/plugins/contact-
form-7/
 | Last Updated: 2025-06-26T09:17:00.000Z
 | Readme: https://people.iee.ihu.gr/~dima/wp-content/plugins/contact-form-
7/readme.txt
 | [!] The version is out of date, the latest version is 6.1
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |    -  https://people.iee.ihu.gr/~dima/wp-content/plugins/contact-form-7/,
status: 200
 |
 | Version: 6.0.6 (90% confidence)
 | Found By: Query Parameter (Passive Detection)
 |      -   https://people.iee.ihu.gr/~dima/wp-content/plugins/contact-form-
7/includes/css/styles.css?ver=6.0.6
 | Confirmed By: Readme - Stable Tag (Aggressive Detection)
 |      -   https://people.iee.ihu.gr/~dima/wp-content/plugins/contact-form-
7/readme.txt


[+] livemesh-siteorigin-widgets
 |  Location:  https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-
siteorigin-widgets/
```

```
 | Latest Version: 3.9.1 (up to date)
 | Last Updated: 2025-03-07T12:41:00.000Z
 |   Readme:   https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-siteorigin-widgets/readme.txt
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |         -    https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-siteorigin-widgets/, status: 200
 |
 | Version: 3.9.1 (100% confidence)
 | Found By: Query Parameter (Passive Detection)
 |         -    https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-siteorigin-widgets/assets/js/lsow-frontend.min.js?ver=3.9.1
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |          -   https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-siteorigin-widgets/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |          -   https://people.iee.ihu.gr/~dima/wp-content/plugins/livemesh-siteorigin-widgets/readme.txt


[+] siteorigin-panels
 | Location: https://people.iee.ihu.gr/~dima/wp-content/plugins/siteorigin-panels/
 | Last Updated: 2025-06-29T20:40:00.000Z
 |  Readme:  https://people.iee.ihu.gr/~dima/wp-content/plugins/siteorigin-panels/readme.txt
 | [!] The version is out of date, the latest version is 2.32.1
 | [!] Directory listing is enabled
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://people.iee.ihu.gr/~dima/wp-content/plugins/siteorigin-panels/, status: 200
 |
 | Version: 2.31.8 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
```

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/siteorigin-panels/readme.txt

[+] so-css

| Location: https://people.iee.ihu.gr/~dima/wp-content/plugins/so-css/

| Latest Version: 1.6.4 (up to date)

| Last Updated: 2025-05-26T21:25:00.000Z

| Readme: https://people.iee.ihu.gr/~dima/wp-content/plugins/so-css/readme.txt

| [!] Directory listing is enabled

|

| Found By: Known Locations (Aggressive Detection)

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/so-css/, status: 200

|

| Version: 1.6.4 (100% confidence)

| Found By: Readme - Stable Tag (Aggressive Detection)

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/so-css/readme.txt

| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/so-css/readme.txt

[+] so-widgets-bundle

| Location: https://people.iee.ihu.gr/~dima/wp-content/plugins/so-widgets-bundle/

| Last Updated: 2025-07-19T22:45:00.000Z

| Readme: https://people.iee.ihu.gr/~dima/wp-content/plugins/so-widgets-bundle/readme.txt

| [!] The version is out of date, the latest version is 1.69.2

| [!] Directory listing is enabled

|

| Found By: Known Locations (Aggressive Detection)

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/so-widgets-bundle/, status: 200

|

| Version: 1.68.5 (80% confidence)

| Found By: Readme - Stable Tag (Aggressive Detection)

| - https://people.iee.ihu.gr/~dima/wp-content/plugins/so-widgets-bundle/readme.txt

```
[+] tablepress
 | Location: https://people.iee.ihu.gr/~dima/wp-content/plugins/tablepress/
 | Latest Version: 3.1.3 (up to date)
 | Last Updated: 2025-05-22T05:08:00.000Z
 |                Readme:                https://people.iee.ihu.gr/~dima/wp-
content/plugins/tablepress/readme.txt
 |
 | Found By: Known Locations (Aggressive Detection)
 |       -   https://people.iee.ihu.gr/~dima/wp-content/plugins/tablepress/,
status: 200
 |
 | Version: 3.1.3 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |                           -            https://people.iee.ihu.gr/~dima/wp-
content/plugins/tablepress/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |                           -            https://people.iee.ihu.gr/~dima/wp-
content/plugins/tablepress/readme.txt


[+] wordfence
 | Location: https://people.iee.ihu.gr/~dima/wp-content/plugins/wordfence/
 | Latest Version: 8.0.4 (up to date)
 | Last Updated: 2025-03-19T18:03:00.000Z
 |                Readme:                https://people.iee.ihu.gr/~dima/wp-
content/plugins/wordfence/readme.txt
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - https://people.iee.ihu.gr/~dima/wp-content/plugins/wordfence/, status:
200
 |
 | Version: 8.0.5 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |                           -            https://people.iee.ihu.gr/~dima/wp-
content/plugins/wordfence/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |                           -            https://people.iee.ihu.gr/~dima/wp-
content/plugins/wordfence/readme.txt
```

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Jul 26 07:51:50 2025

[+] Requests Done: 1558

[+] Cached Requests: 19

[+] Data Sent: 467.231 KB

[+] Data Received: 773.667 KB

[+] Memory used: 244.359 MB

[+] Elapsed time: 00:00:23