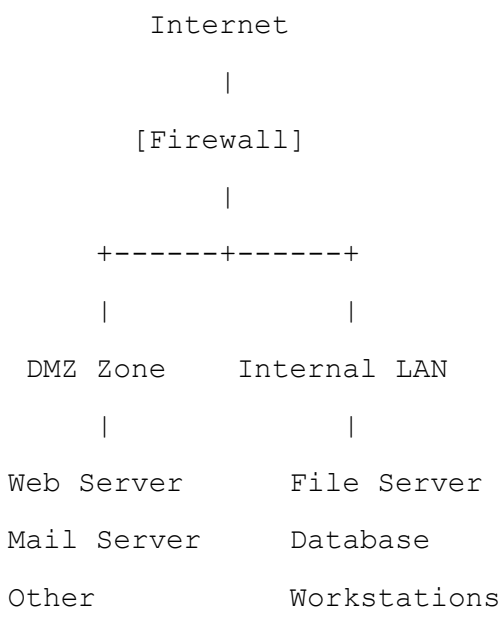
Σχεδίαση και υλοποίηση εργαστηριακών ασκήσεων κυβερνοασφάλειας σε εικονικοποιημένη υποδομή

Στόχος της παρούσας διπλωματικής είναι να αναπτυχθεί ένα σύνολο εργαστηριακών ασκήσεων που θα προσφέρουν το κατάλληλο περιβάλλον για τη διαχείριση και την προστασία δικτύων υπολογιστών και πληροφοριακών συστημάτων. Στο πλαίσιο της διπλωματικής θα διερευνούν θέματα ασφάλειας πληροφοριακών συστημάτων, με χρήση μιας σειράς εργαλείων ασφάλειας και δοκιμών διείσδυσης (hacking). Οι εργαστηριακές ασκήσεις θα εκτελούνται σε ένα απομονωμένο δίκτυο που θα περιλαμβάνει εικονικές υποδομές. Ακολουθεί μία ενδεικτική υποδομή που προσομοιώνει ένα μικρό εταιρικό δίκτυο:



Α. Θα διερευνηθούν λύσεις ως προς τον τρόπο παροχής της υποδομής, ενδεικτικά:

- Περιβάλλοντα πλήρους εικονικοποίησης όλης της υποδομής, π.χ. virtual box, containerlab ώστε η άσκηση να εκτελείται αποκλειστικά σε προσωπικό υπολογιστή.
- Μικτή υποδομή με χρήση VMs σε εξυπηρετητές που διαθέτει το εργαστήριο.

Για κάθε περίπτωση θα μελετηθούν θέματα απαιτήσεων σε υπολογιστικούς πόρους.

Β. Θα υλοποιηθούν ενδεικτικές εργαστηριακές ασκήσεις, όπως:

Αναγνώριση δικτύου και υπηρεσιών. Εξοικείωση με την αναγνώριση δικτύου και την καταγραφή διαθέσιμων υπηρεσιών με χρήση εργαλείων Nmap, Netcat, Wireshark.

Σχεδίαση και υλοποίηση πολιτικών Firewall. Υλοποίηση ασφαλούς διαχωρισμού μεταξύ Internet, DMZ και Internal LAN.

Ανίχνευση επιθέσεων με IDS. Εγκατάσταση και παραμετροποίηση ενός IDS.

Ανίχνευση και αντιμετώπιση επίθεσης τύπου Ransomware

Ασφάλεια Web Server. Εντοπισμός και αντιμετώπιση ευπαθειών.

Επίθεση και προστασία βάσης δεδομένων.

Capture The Flag (CTF). Συνδυαστική εφαρμογή όλων των γνώσεων.

Επικοινωνία: Ε. Συκάς (sykas@cn.ntua.gr), Κ. Σακκά (nsakka@cn.ntua.gr)

Χρήσιμοι σύνδεσμοι: Εργαλεία προς διερεύνηση

Virtualization

Oracle VM VirtualBox Documentation

Docker Documentation

containerlab Documentation

Network Scanning

Nmap Network Scanning (Official Book)

https://github.com/owasp-amass

Networking utilities

Wireshark

https://linuxcommandlibrary.com/man/netcat

Ethical Hacking

Kali Linux Documentation

Metasploit Documentation

https://hashcat.net/hashcat/

https://www.openwall.com/john/

Firewall

pfSense Documentation

Intrusion Detection

Snort 3 Documentation

Suricata Documentation