Introduction to Penetration Testing

Για την επιτυχής διεξαγωγή των εργαστηρίων πρέπει να είναι διαθέσιμο το Kali Linux στην τελευταία έκδοση είτε ως primary operating system είτε στο virtual box ή στο vmware. Η γνώση βασικών εντολών linux καθώς και οι βασικές γνώσεις δικτύων (sub-netting, 3 hand shake, TCP/IP protocol) θα επεξηγηθούν πολύ σύντομα.

Module 1: Information Gathering and Enumeration

Η ενότητα "Συλλογή πληροφοριών" είναι η πιο σημαντική φάση της συνολικής διαδικασίας. Ένας pen tester θα χρησιμοποιήσει τις πληροφορίες που συλλέχθηκαν κατά τη διάρκεια αυτής της φάσης για να χαρτογραφήσει το περιβάλλον της επίθεσης (mapping) και να αυξήσει τις πιθανότητες να παραβιάσει έναν οργανισμό/σύστημα με τον ίδιο τρόπο που κάνουν οι εγκληματίες. Οι μαθητές θα μάθουν πώς να αποκτήσουν πρόσβαση σε πολύτιμα, ευαίσθητα και μερικές φορές μυστικά έγγραφα μέσω δωρεάν υπηρεσιών, βάσεων δεδομένων και εξειδικευμένων μηχανών αναζήτησης. Η συλλογή πληροφοριών ασχολείται με την απαρίθμηση των DNS, Domains, netblocks και άλλων ιστότοπων που ανήκουν στον οργανισμό καθώς και με πιθανές έμμεσες σχέσεις με άλλες οντότητες και ιστοσελίδες.

Εργαστήριο και εργαλεία

- Whois
- Waybackmachine
- TheHarvester
- Maltego
- Shodan

Module 2 : Sniffing, Phishing & MITM

Η μελέτη του ARP, του τρόπου με τον οποίο λειτουργεί και του τρόπου με τον οποίο μπορεί να γίνει χειραγώγηση για την εκπόνηση εξελιγμένων επιθέσεων καθίσταται εξαιρετικά εύκολη στην κατανόηση. Το Sniffing είναι μια τεχνική που θα μπορέσετε να κατανοήσετε πλήρως τις πιο πρακτικές πτυχές της. Θεωρούμε ότι έχετε αρκετά βασικά στοιχεία της θεωρίας του δικτύου πριν καλύψουμε πραγματικά σενάρια επίθεσης χρησιμοποιώντας τα καλύτερα διαθέσιμα εργαλεία. Οι man in the middle επιθέσεις είναι μία από τις πιο διαδεδομένες τεχνικές διείσδυσης σήμερα.

Εργαστήριο και εργαλεία

- Wireshark
- Aircrack
- Airmon
- Social Engineer Toolkit (SET)
- Wifiphisher

Module 3: Vulnerability Scanning and Exploitation

Ως ένα από τα πιο σημαντικά βήματα στη δοκιμή διείσδυσης ενός δικτύου, αυτή η ενότητα θα σας διδάξει πρώτα τη θεωρία πίσω από τη σάρωση και την ανεύρεση ευπαθειών. Θα σας δείξουμε λοιπόν πώς να χρησιμοποιείτε τα καλύτερα εργαλεία για την ανίχνευση ανοικτών θυρών (open ports) και

υπηρεσιών που εκτελούνται σε αυτά. Μέσα από το Nmap, θα μάθετε πώς να βρείτε συστήματα που παρέχουν υπηρεσίες. Οι παθητικές και ενεργές λειτουργίες αποτύπωσης του λειτουργικού συστήματος (active reconnaissance and passive reconnaissance) θα καλυφθούν επίσης σε βάθος. Επίσης θα αξιοποιηθεί το Metasploit και το nmap για την ανίχνευση ευπαθειών. Ο φοιτητής στη συνέχεια θα ενημερωθεί για τις κοινές τεχνικές exploitation που χρησιμοποιούνται από τους σημερινούς pentesters, για να εκμεταλλευτεί τις πλευρές του πελάτη και τις απομακρυσμένες ευπάθειες στους clients και στους servers.

Εργαστήριο και εργαλεία

- Nmap και λειτουργίες
- Ανίχνευση λειτουργικών συστημάτων και γνωστών υπηρεσίων (webservers, CMS κλπ)
- Nmap Scripting Engine
- Nessus
- Απαρίθμηση User Accounts και ιστοσελίδων (subdomains)
- DMitry
- Golismero
- Burbsuite
- Webgoat
- Metasploit Framework and commands

Module 4 : Anonymity

Οι pentesters συχνά πρέπει να καλύψουν τα στοιχεία και τις πληροφορίες τους. Η κάλυψη των traces είναι σημαντική λειτουργία και εντάσσεται στα πλαίσια της προσομοίωσης ρεαλιστικών επιθέσεων και τεχνικών διείσδυσης.

Εργαστήριο και εργαλεία

- Arp Spoofing
- Macchanger
- Tor
- Proxychains

Module 5 : Capture the Flag Competitions

Η διδασκαλία του Penetration Testing μπορεί να μεταβληθεί σε μια διαδικασία διαδραστικής μάθησης μέσω της ένταξης μεθοδολογιών μάθησης βασισμένων σε προκλήσεις. Διάφορες είναι οι πλατφόρμες CTF όπως το Facebook CTF, picoCTF, CTF365, hackthebox που αξιοποιούνται παγκοσμίως. Επιπλέον έχουν κατασκευαστεί ευάλωτα λειτουργικά συστήματα (vulnerable images) όπως το Metasploitable, το Webgoat και άλλα virtual images που ονομάζονται "boot2root". Τα virtual images αυτά περιέχουν ευπάθειες και αξιοποιούνται για εκπαιδευτικούς σκοπούς.

Εργαστήριο και εργαλεία

- Images από το Vulnhub
- Metasploitable
- Webgoat
- CTF platforms