LEDRA COLLEGE NICOSIA

Ethical Hacking & Penetration Testing Techniques

Ethical Hacking & Penetration Testing Techniques

Ethical hacking is meant to safeguard the interests of the innocent and ignorant tech savvy generation and combat the malicious hackers who are constantly looking to profit from someone's vulnerability.

People enrolling on this course will study the development of a structured knowledge base that enables security professionals to discover vulnerabilities and recommend solutions for tightening network and system security and protecting data from potential attackers. Focus is placed on penetration-testing tools and techniques that security testers and ethical hackers use to protect IT systems, including programmatic review and continuous improvement planning.

Course Aims

After the successful completion of this course, learners should be able to:

- Gain an in-depth knowledge and practical experience with current security mechanisms
- Recognize how intruders operate and the necessary steps to secure a system or a network
- Understand common ethical hacking topics, such as intrusion detection, policy creation, social engineering, DoS attacks, buffer overflows, and malware detection
- Identify, classify and analyze various types of malware and malicious behavior
- Utilize a standard methodology for detecting, analyzing, reverse engineering, and eradicating malware.
- Properly plan, execute and document a penetration test

Eligible Participants

This course is targeted at IT professionals, Information Security staff, auditors and system and network administrators

Course Duration

The total duration of this course is forty (40) hours. Upon completion of the course, successful participants will be awarded a certification approved by the HRDA.

Course Indicative Content

NO	INDICATIVE CONTENT	DURATION (HOURS)
1	**Introduction to Ethical Hacking** The aim is to introduce the participants to ethical hacking terminology, as well as to define the job role of an ethical hacker. Also the participant will get introduced to the different phases involved in ethical hacking, the different types of hacking technologies and the legal implications of hacking.	2
2	**Footprinting, Scanning & Enumeration** The aim is to define the term "footprinting" and describe different information gathering methodologies, as well as ways of collecting competitive intelligence. In addition, it will be explained how this intelligence can be utilized in the consequent scanning the enumeration phases.	2

NO	INDICATIVE CONTENT	DURATION (HOURS)
3	**System Hacking** The different kind of passwords and password-cracking techniques are presented, to understand escalating privilages techniques, keyloggers and other spy-ware technologies. It will also be shown how it is possible for a hacker to cover his tracks and erase possible evidence.	2
4	**Trojans, Backdoors, Viruses, Worms** The aim is to explain the functionality of Trojans, Backdoors, Viruses and Worms. Overt and covert channels are also explained, as well as differences between types of malware.	2
5	**Sniffers** The aim is to explain different active and passive sniffing techniques, as well as the protocols susceptible to sniffing. Terms such as “poisoning”, “flooding” and “spoofing” are also presented and explained.	2
6	**Denial of Service** Explain what a Denial of Service attack is, how it works, and the different types involved. Distributed Denial of Service attacks, Bots and Botnets are also introduced and explained.	2
7	**Social Engineering** The aim is to introduce the concept of social engineering and explain how a hacker can exploit the human factor to gain the information/intelligence he requires without necessarily making use of technological means.	2
8	**Session Hijacking** The aim is to introduce the concept of session hijacking, explain its different types and understand the difference between spoofing and hijacking. Also, the steps in performing session hijacking are explained, as well as possible preventive measures.	2
9	**Hacking Web Servers** The aim is to explain the different types of web server vulnerabilities and the possible attacks against web servers. An overview of how web-servers function is provided, as well as possible safety measures and “hardening” techniques.	2
10	**Web Application Vulnerabilities** The objectives of web application hacking are explained. Web application vulnerability scanners are presented as well as various web application threats and possible attacks.	2
11	**Web based Password Cracking Techniques** Analyse different web-based password cracking techniques, explain their functionality, understand the different attack classifications and present possible countermeasures	2
12	**Hacking Wireless Networks** The aim is to present an overview of wireless authentication mechanisms and protocols, understand wireless hacking techniques and describe some of the common methods used to secure networks.	2
13	**Physical Security** The aim is to present the concept of physical security, why it is necessary and how it differs from electronic safety, who is accountable for it and several non-network factors affecting the overall security of an organisation.	2
14	**Memory Analysis** Describe what is meant by “memory analysis” and explain possible ways for collecting Process Memory, Dumping Physical Memory and analyzing a Physical Memory Dump.	2
15	**File Analysis** Explain the importance and functionality of Log Files and explain related terminology such as File Metadata, Alternative Log collection methods, and Executable File Analysis	2
16	**Malware Identification and Classification** The aim is to explain the definition of malware and explain some of the possible detection methods and capabilities. Specific Malware Signatures are also presented, along with Shellcode and Rootkits.	2
17	**Malware Analysis** Explain the concept of Dynamic Analysis and show different methods for debugging Malware. De-Obfuscation is also presented, along with DLLs and Kernel debugging.	2
18	**Linux Environment** The aim is to present basic Linux kernel compilations, to understand GCC compilation commands and present LKM modules. Some Linux “hardening” methods are also presented.	2
19	**Evading Firewalls, IDSs & Honeypots** The aim is to introduce the concepts of Firewalls, Intrusion Detection Systems and Honeypots and explain their different types, functionality and possible evasion techniques.	2
20	**Penetration Testing Documentation & Reporting** The aim is to show how to properly create a penetration testing report, with a detailed list of findings, an in-depth analysis, as well as proposed remediation measures	2

Ταχύρυθμα επιχορηγημένα μαθήματα
Αρχής Ανάπτυξης Ανθρώπινου Δυναμικού (ΑΝΑΔ) 2014

Το LEDRA COLLEGE προσφέρει ταχύρυθμα επιχορηγημένα πολυεπιχειρησιακά προγράμματα σε άτομα που επιθυμούν να εμπλουτίσουν τις γνώσεις και τα επαγγελματικά τους προσόντα.

Σημαντικές πληροφορίες & κριτήρια για τα επιχορηγημένα προγράμματα της ΑΝΑΔ

- Τα μαθήματα δικαιούνται να τα παρακολουθήσουν άτομα που εργάζονται στον ιδιωτικό τομέα, σε ημικρατικούς οργανισμούς και σε δημοτικές αρχές. Εξαιρούνται από την επιχορήγηση οι κυβερνητικοί υπάλληλοι.

- Για να δικαιούται ένα άτομο να παρακολουθήσει κάποιο από τα επιχορηγημένα προγράμματα της ΑΝΑΔ, θα πρέπει να καταβάλλει εισφορές στο Ταμείο Κοινωνικών Ασφαλίσεων

- Για κάθε πρόγραμμα υπάρχουν επιπλέον συγκεκριμένα κριτήρια εισδοχής, τα οποία αναγράφονται στον οδηγό κάθε προγράμματος.

- Το ποσοστό της επιχορήγησης διαφέρει ανάλογα με το μέγεθος της επιχείρησης/οργανισμού: Αν η επιχείρηση είναι μικρού μεγέθους (κάτω των 50 ατόμων), η επιχορήγηση ανέρχεται στο 80%, αν η επιχείρηση είναι μεσαίου μεγέθους (κάτω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 70% και αν είναι μεγάλου μεγέθους (άνω των 250 ατόμων), η επιχορήγηση ανέρχεται στο 60%.

- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των εργοδοτουμενων που μπορεί να στείλει κάθε εταιρεία για κάθε πρόγραμμα.

- Δεν υπάρχει περιορισμός όσο αφορά τον συνολικό αριθμό των προγραμμάτων που μπορεί να παρακολουθήσει κάθε ενδιαφερόμενος.

- Όλα τα μαθήματα ξεκινούν την εβδομάδα 10-16 Φεβρουαρίου 2014

LEDRA COLLEGE
NICOSIA

13 Lankada Street, Strovolos, 2023 Nicosia, Cyprus
+357 22514044 I www.ledra.ac.cy I info@ledra.ac.cy