EEHF: EXIN Ethical Hacking Foundation

Course Code: EEHF
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

The purpose of ethical hacking is to evaluate the security of a computer system or network through the discovery and exploitation of vulnerabilities in a legal manner.

Today's technology is moving fast and changing the way we do business. Companies digitize all information by default, store their data in the cloud and use open source software. This raises information security issues related to network and system infrastructure.

The EXIN Ethical Hacking Foundation module covers the basic steps of ethical hacking: intelligence gathering, scanning computer network/systems, and penetrating systems. Candidates are expected to be very aware of the difference between legal and illegal hacking, and the consequences of misuse.

In more detail the candidate will develop an understanding of the following topics:

- Network sniffing (gathering information from network traffic)
- Cracking a WEP and WPA(2) key from a wireless network
- Network vulnerability scanning
- Basic penetration of computer systems
- Password cracking
- Web-based hacking, containing SQL Injections (SQLi), Cross-Site Scripting (XSS), Remote File Inclusions (RFI)

The EXIN Ethical Hacking Foundation exam tests the knowledge of the candidate on:

- the basics of Ethical Hacking, and
- the practice of Ethical Hacking.

SKILLS COVERED

- Introduction to Ethical Hacking
- Network Sniffing
- Hacking Wireless Networks
- System Penetration
- Web-based Hacking

WHO SHOULD ATTEND?

This certificate is meant for security officers, network architects, network administrators, security auditors, security professionals, computer programmers and networking experts, managers working in the field of ethical hacking and anyone who is interested in improving and/or testing the security of an IT infrastructure. The module is also meant for (beginning) ethical hackers who want to get certified and verify their knowledge.

PREREQUISITES

- Successful completion of the name of certification exam.

However, a training Ethical Hacking Foundation and knowledge of Linux is highly recommended.

MODULES

Module 1: Introduction to Ethical Hacking

1.1 Hacking Ethics

- Understand the legal implications of hacking.
- Different types of hackers.

1.2 Basic Principles

- The difference between the white and black box test.
- Different phases in the hacking process.

Module 2: Network Sniffing

2.1 Tools

- Different kind of tools for Network Sniffing.
- The most common tools for Network Sniffing.

2.2 Extracting Information

- The function of HTTP headers.
- Extract information from HTTP headers.

Module 3: Hacking Wireless Networks

3.1 Preparation

- Find information of his own network adapter.

3.2 Aircrack-NG

- Airodump-NG.
- The different kind of functions of tools within Aircrack.
- What ESSID&BSSID means.

Module 4: System Penetration

4.1 Intel Gathering

- Knows how to find information on a target online.
- Knows how to find information on a target within a network.

4.2 Software Tools (Nmap, Metasploit)

- Can scan a target.
- Knows how to combine tools.

4.3 Fingerprinting and Vulnerabilities

- Knows how to find vulnerabilities based on scanning results.
- Knows how to perform manual fingerprinting.

4.4 Exploitation and Post Exploitation

- Knows how to exploit a vulnerability with Metasploit.
- Knows how to extract system information after exploitation

Module 5: Web-based Hacking

5.1 Database Attacks

- Knows the steps to test for SQLi vulnerabilities.
- How to extract data with SQLi.
- Functions: CONCAT, LOAD_FILE, UNION, SELECT,
  @@version, ORDER BY, LIMIT
  what they do.

5.2 Client Side Attacks

- Knows how to create an XSS PoC (Proof of Concept).
- Knows the basics of session hijacking i/c/w XSS.
- Knows how to bypass basic XSS filters.

5.3 Server Side Attacks

- Knows how RFI is performed.
- Knows basic functionalities of php shells such as r57 and c99.
- Knows the difference between Bind & Back connect shells and what they do.

END OF PAGE