Preparation Guide

Edition 201606

Content

1. Overview

EXIN Ethical Hacking Foundation (EHF.EN)

Scope

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.

Summary

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.

Context

The certificate EXIN Ethical Hacking Foundation is part of the EXIN Ethical Hacking qualification program.

Target group

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.

Requirements for certification

- Successful completion of the name of certification exam.

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

Examination details

Examination type:	Multiple-choice questions
Number of questions:	40 questions
Pass mark:	65%
Open book/notes:	No
Electronic equipment/aides permitted:	No
Time allotted for examination:	60 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Bloom level

The EXIN Ethical Hacking Foundation certification tests candidates at Bloom Level 1 and Level 2 according to Bloom's Revised Taxonomy:

- Bloom Level 1: Remembering – relies on recall of information. Candidates will need to absorb, remember, recognize and recall. This is the building block of learning before candidates can move on to higher levels.
- Bloom Level 2: Understanding – a step beyond remembering. Understanding shows that candidates comprehend what is presented and can evaluate how the learning material may be applied in their own environment. This type of questions aims to demonstrate that the candidate is able to organize, compare, interpret and choose the correct description of facts and ideas.

Training

Contact hours

The recommended number of contact hours for this training course is 16. This includes group assignments, exam preparation and short breaks. This number of hours does not include lunch breaks, homework and the exam.

Indication study effort

60 hours, depending on existing knowledge.

Training organization

You can find a list of our accredited training organizations at www.exin.com.

2. Exam requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam requirement	Exam specification	Weight
1. Introduction to Ethical Hacking		**15%**
	1.1 Hacking Ethics	
	1.2 Basic Principles	
2. Network Sniffing		**10%**
	2.1 Tools	
	2.2 Extracting Information	
3. Hacking Wireless Networks		**10%**
	3.1 Preparation	
	3.2 Aircrack-NG	
4. System Penetration		**35%**
	4.1 Intel Gathering	
	4.2 Fingerprinting & Vulnerabilities	
	4.3 Software Tools (Nmap, Metasploit)	
	4.4 Exploitation & Post Exploitation	
5. Web-based Hacking		**30%**
	5.1 Database Attacks	
	5.2 Client Side Attacks	
	5.3 Server Side Attacks	
	Total	**100%**

Exam specifications

1 Introduction to Ethical Hacking

1.1 Hacking Ethics

The candidate can …

1.1.1 understand the legal implications of hacking.

1.1.2 describe different types of hackers.

1.2 Basic Principles

The candidate …

1.2.1 knows the difference between the white and black box test.

1.2.2 can describe different phases in the hacking process.

2 Network Sniffing

2.1 Tools

The candidate …

2.1.1 knows different kind of tools for Network Sniffing.

2.1.2 knows how to use the most common tools for Network Sniffing.

2.2 Extracting Information

The candidate …

2.2.1 knows the function of HTTP headers.

2.2.2 can extract information from HTTP headers.

3 Hacking Wireless Networks

3.1 Preparation

The candidate can …

3.1.1 find information of his own network adapter.

3.2 Aircrack-NG

The candidate …

3.2.1 can explain Airodump-NG.

3.2.2 knows the different kind of functions of tools within Aircrack.

3.2.3 knows what ESSID&BSSID means.

4 System Penetration

4.1 Intel Gathering

The candidate …

4.1.1 knows how to find information on a target online.

4.1.2 knows how to find information on a target within a network.

4.2 Software Tools (Nmap, Metasploit)

The candidate …

4.2.1 Can scan a target.

4.2.2 knows how to combine tools.

4.3 Fingerprinting and Vulnerabilities

The candidate …

4.3.1 knows how to find vulnerabilities based on scanning results.

4.3.2 knows how to perform manual fingerprinting.

4.4 Exploitation and Post Exploitation

The candidate …

4.4.1 knows how to exploit a vulnerability with Metasploit.

4.4.2 knows how to extract system information after exploitation.

5 Web-based Hacking

5.1 Database Attacks

The candidate …

5.1.1 knows the steps to test for SQLi vulnerabilities.

5.1.2 can explain how to extract data with SQLi.

5.1.3 knows the following functions: CONCAT, LOAD_FILE, UNION, SELECT, @@version, ORDER BY, LIMIT

5.2 Client Side Attacks

The candidate …

5.2.1 knows how to create an XSS PoC (Proof of Concept).

5.2.2 knows the basics of session hijacking i/c/w XSS.

5.2.3 knows how to bypass basic XSS filters.

5.3 Server Side Attacks

The candidate …

5.3.1 knows how RFI is performed.

5.3.2 knows basic functionalities of php shells such as r57 and c99.

5.3.3 knows the difference between Bind & Back connect shells and what they do.

3. List of Basic Concepts

This chapter contains the terms and abbreviations with which candidates should be familiar.

Please note that knowledge of these terms alone does not suffice for the exam; the candidate must understand the concepts and be able to provide examples.

@@ version
+x eXecute
Aircrack-ng
Aireplay-ng
Airodump-ng
arpspoof
BackTrack
Bind & Back (Reverse) connect shells
Black box testing
BSSID & ESSID
Command line Interface (CLI)
CONCAT
Cross-Site Scripting (XSS)
Default Gateway
Dynamic Host Configuration Protocol (DHCP)
Domain Name System (DNS)
Fingerprinting
FTP server
Graphical User Interface (GUI)
Hackers
- Black hat hackers
- Grey hat hackers
- Hacktivists
- White hat hackers

Hashdump
HTTP
ipconfig /all
iwconfig
John The Ripper (JTR)
Kali Linux
Keyloggers
Kismet
LIMIT
LOAD_FILE
Local File Inclusion (LFI)
MAC address
Metasploit
Meterpreter payload
Nessus
Netcat
Network File System (NFS)
Nikto
Nmap
Nonce
ORDER BY
Packet sniffers
Penetration test
php-shell
- c99shell
- r57shell

Ping
Privilege Escalation Exploit / Kernel exploit
Proof of Concept (PoC)
Reconnaissance
Remote File Inclusion (RFI)
Scanning
SELECT
Session Hijacking
Shell
Spoofing
SQL- MySQL
SQL injection (SQLi)
sqlmap
SSH server
SYN scan
TCPdump
TCP three-way handshake
Tshark
UNION
VNC Injection payload
WEP key
White box testing
WPA2

4. Literature

Exam literature

The knowledge required for the exam is covered in the following literature:

A. Georgia Weidman
Penetration Testing: A Hands-On Introduction to Hacking
ISBN-13: 978-1593275648

B. **Exam literature EXIN Ethical Hacking Foundation**
Free download on www.exin.com.

Additional literature

C. Stuart McClure, Joel Scambray, George Kurtz
Hacking Exposed 7: Network Security Secrets & Solutions (Hacking Exposed: Network Security Secrets & Solutions)
ISBN-13: 978-0071780285

D. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

E. **Prosecuting Computer Crimes Manual**
http://www.justice.gov/criminal/cybercrime
Documents and reports - Manuals
Chapter 1

Comment

Additional literature is for reference and depth of knowledge only. Additional literature (**C**) can be read by the candidate to obtain deeper knowledge of the subject. **D** (EU legislation) and **E** (US legislation) cover the legal consequences of misuse of computer systems and computer data.

Literature matrix

Exam requirement	Exam specification	Literature
1. Introduction to Ethical Hacking		
	1.1 Hacking Ethics	B: Ch. 1, 2
	1.2 Basic Principles	B: Ch. 3
2. Network Sniffing		
	2.1 Tools	A: Ch. 7
	2.2 Extracting Information	A: Ch. 7
3. Hacking Wireless Networks		
	3.1 Preparation	A: Ch. 15
	3.2 Aircrack-NG	A: Ch. 15
4. System Penetration		
	4.1 Intel Gathering	A: Ch. 5, 7
	4.2 Fingerprinting & Vulnerabilities	A: Ch. 5
	4.3 Software Tools (Nmap, Metasploit)	A: Ch. 6, 10
	4.4 Exploitation & Post Exploitation	A: Ch. 4
5. Web-based Hacking		
	5.1 Database Attacks	A: Ch. 14
	5.2 Client Side Attacks	A: Ch. 14
	5.3 Server Side Attacks	A: Ch. 14

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER