CERTIFICATION

CertiProf

Professional Knowledge

ETHICAL HACKING

CEHPC™

ETHICAL HACKING

PROFESSIONAL CERTIFICATION

CEHPC™ Version 022024

CertiProf®

Ethical Hacking

Syllabus V022024

CERTIPROF ETHICAL HACKING PROFESSIONAL CERTIFICATION CEHPC™

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

Introduction

With the Ethical Hacking certification, you will learn the techniques of Ethical Hacking, its characteristics, functionalities and scope in order to defend organizations against cyber-attacks. You will use the tools, methodologies and techniques most commonly used in Social Engineering, in order to detect this type of attacks in real environments through case studies. You will learn how to search for information in different public sources, as well as the use of security tools to find confidential information. You will perform network analysis to identify network mapping, operating systems, versions and open ports, identifying assets. You will learn how to analyze the most common vulnerabilities of operating systems exploiting in a controlled environment. You will learn the techniques of Ethical Hacking, its characteristics, functionalities and scope in order to defend organizations against cyber-attacks. You will learn the techniques of Ethical Hacking, its characteristics, functionalities and scopes in order to defend organizations against cyber-attacks. And you will learn how to write an executive and technical report for the presentation of the findings found, where you will generate value with mitigation recommendations.

Objetivos

The objective of the course is to learn to perform Pentesting in a professional manner following methodologies with an ethical approach, knowing the attack techniques that a cybercriminal performs to prevent security gaps, you will learn to identify vulnerabilities in technological assets, giving recommendations for their mitigation.

Specific points

- Understand current security trends.
- Know the elements of information security.
- Understand the concepts, types and phases of ethical hacking.
- Manage information security threats.
- Develop strategies for the understanding, management and protocols of attack vectors.
- Master the concepts, types and phases of pentesting.
- Understand the pentesting process.
- Master information security controls.

At the end of the course, the student will have the necessary knowledge to be able to perform penetration tests in a professional way in the technological infrastructure, following methodologies with 100% ethical approach being a high value professional with one of the most demanded profiles by companies.

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

Exam format and duration

This syllabus has an exam in which the candidate must achieve a score to obtain the Ethical Hacking certification.

- Type: Multiple Choice; 40 Questions.
- Duration: 60 minutes maximum, for all candidates in their respective language.
- Prerequisite: None.
- Supervised: At the discretion of the Partner.
- Open book: No.
- Passing Score: 32/40 or 80%.
- Delivery: This exam is available online.

Certification eligibility

Students, auditors, security analysts, audit and internal control and risk management consultants or advisors, and professionals related to the world of cybersecurity.

Content

1. Fundamentals of Pentesting and Ethical Hacking

1.1 Introduction to Ethical Hacking

- What is a Hacker
- Types of Hackers
- Classification of Hackers
- Hacking vs. Ethical Hacking
- The Proceedings of a Hacker
- How Do They Do It?

1.2 Penetration Testing

- What is Penetration Testing
- Importance of Pentesting
- Knowledge of the Pentester
- Types of Pentesting Tests
- Categorization of a Pentesting
- Pentesting Methodologies
- Pentesting Phases

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

1.3 Metodologías y Buenas Practicas

- PETS
- OWASP
- MITRE ATT&CK

1.4 Security Technologies and Tools

- IPS / IDS
- VPN
- Content Filtering Systems
- Routers
- Switches
- Firewall
- HoneyPot
- Information Security Incident Response
- SIEM
- Backup and Recovery

2. Social Engineering

2.1 History of Social Engineering

- What Is Social Engineering?
- How Does Social Engineering Work?
- Channels Used by Attackers
- Methods Used by Attackers
- Factors that Make Companies Vulnerable to Attacks

2.2 Types of Social Engineering

- Phishing
- Phishing Planning
- What Does it Look Like?
- Spear Phishing
- Vishing
- Smishing
- Whaling
- Baiting
- Scareware
- Pretexting

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

2.3 Protection and Control Measures

- Acceptable Use Policy
- Preliminary Review Measures
- Awareness and Training
- Phishing Campaigns

3. Active and Passive Reconnaissance

3.1 Passive Reconnaissance

- Framework OSINT
- Google Hacking
- DNS Collection
- Whois
- Shodan

3.2 Active Reconnaissance

- Network Scanning and Enumeration
- Ports and Services
- Classification of Port Scanning Response Type

4. Network Scanning and Analysis

4.1 Introduction to Network Analysis

- Ping
- Traceroute
- Ping Sweep
- Port Types
- Internet Control Message Protocol (ICMP)
- SYN /ACK
- TCP Communication Indicators
- TCP Communication Flags
- Three-wayhandshake Method

4.2 Installation Working Environment

- Wmware Installation
- Installation of Kali Linux.
- System Upgrade
- User Creation
- Installation Metasploitable 2 and 3

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

4.3 Introduction to NMAP
- What is NMAP?
- Basic Nmap Scanning
- NMAP Options

4.4 NMAP Categories
- Host Discovery
- Scan Techniques
- Port Specification and Scan Order
- Service/Version Detection
- OS Detection
- Timing and Performance
- Firewall/IDS Evasion and Spoofing
- Output

5. Vulnerability Analysis

5.1 Introduction to Vulnerabilities
- What is Vulnerability Analysis?
- What are Vulnerabilities?
- What is CVSS?

5.2 Automated Vulnerability Scanning
- Nessus
- ZAP

5.3 Manual Vulnerability Scanning
- Scanning with NMAP Scripts

6. Exploitation

6.1 Metasploit
- What is Metasploit?
- Basic Commands
- Searching for Sploit
- Execution of Meterpreter

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.

7. Attack Techniques

7.1 Attack Types

- Malware
- Spoofing
- Man-in-the-middle
- Distributed Denial of Service (Ddos)
- PiggyBacking
- SQL Code Injection
- Phishing

8. Results Report

8.1 Types of Reports

- Technical Report
- Executive Report

8.2 Results presentation

CERTIPROF ETHICAL HACKING PROFESSIONAL CERTIFICATION CEHPC™

CERTIPROF® is a registered trademark of CertiProf, LLC in the United States and/or other countries.