Lesson Plan for PenTest+ CertMaster Perform

CompTIA®

Contents

Overview

Course aggregates

Labs	45
Videos (inline videos)	24
Interactives	13
Text Topics	255
Total Assessments	49
Total Questions in Custom Quizzes Bank	409
Total Question in Course Assessments	395
Estimated Instructional Hours	44:10

1.0: Penetration Testing: Before You Begin

Overview

Summary

In this module, you will:

- Discuss ethical, legal and compliance considerations
- Describe a penetration test report
- Explain the purpose of collaboration and communication during a PenTest
- Identify and compare testing frameworks and methodologies
- Understand the use of scripting and automation in a PenTest.

As a penetration tester preparing for an engagement, next steps include addressing legal and ethical considerations to ensure compliance, protect client data, and maintain professional integrity. Defining the test's scope and obtaining authorization are essential for setting boundaries, aligning with stakeholders, and clarifying objectives. Understanding PenTest report requirements will guide clear and actionable communication of findings to the client. Effective collaboration with team members, maintaining clear communication with clients, and conducting peer reviews enhance task alignment and ensure the test meets organizational goals. Prioritizing vulnerabilities by analyzing risk, impact, and business relevance helps address the most critical issues first. Clear escalation paths, secure information handling, and client acceptance facilitate the remediation process. Selecting suitable frameworks allows the testing approach to be tailored to client needs and industry standards. Adjusting scripts for reconnaissance and enumeration improves testing efficiency and adaptability to target environments, ultimately ensuring a thorough and reliable assessment of security.

Total Time

(About 205 minutes)

1.1: Professional Conduct and Penetration Testing

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.

Video/Demo

(includes 1 inline videos.)

Topics

1.1.1 What Is Penetration Testing?
1.1.2 Ethics, Legal, and Compliance Considerations of Penetration Testing
1.1.3 Importance and Examples of Documentation
1.1.4 Scoping and Authorization
1.1.5 Overview of the PenTest Report
1.1.6 Live Lab: Exploring the Lab Environment
1.1.7 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 65 minutes)

1.2: Collaboration and Communication

Summary

Exam Objectives Covered

- 1.2 Explain collaboration and communication activities.

Topics

1.2.1 Collaboration and Communication Overview
1.2.2 PenTest Team Roles and Responsibilities
1.2.3 Communicating with Clients and Team Members
1.2.4 Peer Review
1.2.5 Stakeholder Alignment
1.2.6 Root Cause Analysis
1.2.7 Escalation Path
1.2.8 Secure Distribution
1.2.9 Articulation of Risk, Severity, and Impact
1.2.10 Goal Reprioritization
1.2.11 Business Impact Analysis
1.2.12 Client Acceptance
1.2.13 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 60 minutes)

1.3: Testing Frameworks and Methodologies

Summary

Exam Objectives Covered

- 1.3 Compare and contrast testing frameworks and methodologies.

Topics

1.3.1 Testing Frameworks and Methodologies Overview
1.3.2 Open Source Security Testing Methodology Manual (OSSTMM)
1.3.3 Council of Registered Ethical Security Testers (CREST)
1.3.4 Penetration Testing Execution Standard (PTES)
1.3.5 MITRE ATT&CK
1.3.6 Open Web Application Security Project (OWASP) Top 10
1.3.7 OWASP Mobile Application Security Verification Standard (MASVS)
1.3.8 Purdue Model
1.3.9 Threat Modeling Frameworks
1.3.10 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 45 minutes)

1.4: Introduction to Scripting for Penetration Testing

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.
- 2.3 Given a scenario, modify scripts for reconnaissance and enumeration.

Topics

1.4.1 Scripting Languages
1.4.2 Bash Shell and Bash Script
1.4.3 Python
1.4.4 PowerShell
1.4.5 Use of Libraries, Functions, and Classes
1.4.6 Logic Constructs
1.4.7 Create Logic Constructs
1.4.8 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 35 minutes)

1.5: Module Quiz

Number of Assessment Questions

20 (about 20 minutes)

2.0: Applying Pre-Engagement Activities

Overview

Summary

In this module, you will:

- Explain how to define the scope of a penetration test
- Compare and contrast agreement types used in preparing for a PenTest
- Describe the shared responsibility model
- Discuss pre-engagement documentation and planning

A penetration tester meticulously conducts pre-engagement activities to define the test's scope, objectives, and boundaries, to ensure alignment with regulations and industry standards. Establishing clear rules of engagement, securing agreements like NDAs, and selecting relevant targets are essential for an effective and legally compliant test. Different assessments—such as vulnerability, network, application, and API—will address specific security areas, providing a full view of potential risks. A clear shared responsibility model will help coordinate efforts between all parties, ensuring that each understands their role in securing the system. The PenTester must also uphold ethical and legal considerations, including obtaining authorization letters and adhering to reporting standards. Thorough documentation of these steps will lay the groundwork for a structured, transparent, and secure penetration testing process.

Total Time

(About 110 minutes)

2.1: Define the Scope

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.

Topics

2.1.1 Regulations, Frameworks, and Standards

2.1.2 Rules of Engagement
2.1.3 Agreement Types
2.1.4 Target Selection
2.1.5 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 20 minutes)

2.2: Compare Types of Assessments

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.

Topics

2.2.1 Types of Assessments Overview
2.2.2 Web and Application Assessments
2.2.3 Network Assessments
2.2.4 Activity: Assess Environmental Considerations
2.2.5 Mobile Assessments
2.2.6 Cloud Assessments
2.2.7 Wireless Assessments
2.2.8 IoT Devices and Penetration Testing
2.2.9 Information Technology Versus Operational Technology
2.2.10 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 45 minutes)

2.3: Utilize the Shared Responsibility Model

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.

Topics

2.3.1 The Shared Responsibility Model Overview
2.3.2 Hosting Provider Responsibilities
2.3.3 Customer Responsibilities
2.3.4 Penetration Tester Responsibilities
2.3.5 Third-Party Responsibilities
2.3.6 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 25 minutes)

2.4: Identify Legal and Ethical Considerations

Summary

Exam Objectives Covered

- 1.1 Summarize pre-engagement activities.

Topics

2.4.1 Authorization Letters
2.4.2 Mandatory Reporting Requirements
2.4.3 Risk to the Penetration Tester
2.4.4 Documenting Pre-Engagement Activities
2.4.5 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 20 minutes)

2.5: Module Quiz

Number of Assessment Questions

20 (about 20 minutes)

3.0: Enumeration and Reconnaissance

Overview

Summary

In this module, you will:

- Perform Recon with Nmap
- Perform Enumeration with Nmap
- DNS Enumeration and Reconnaissance
- Perform a Decoy Scan

Before any pentest can commence, the pentester should spend the time to gather as much information as possible on the target. The more information that is learned about the target prior to starting the pentest, the easier the test will be.

Because having more information will lead to greater success in the pentest, the pentester should spend ample time in this phase of the pentest.

The process of gathering this information is known as Enumeration and Reconnaissance.

Total Time

(About 295 minutes)

3.1: Information Gathering Techniques

Summary

Exam Objectives Covered

- 2.1 Given a scenario, apply information gathering techniques.
- 2.3 Given a scenario, modify scripts for reconnaissance and enumeration.

Video/Demo

(includes 3 inline videos.)

Topics

3.1.1 Active and Passive Reconnaissance
3.1.2 Tools for Reconnaissance
3.1.3 Open-Source Intelligence (OSINT)
3.1.4 Using Shodan
3.1.5 Previously Breached Password Lists
3.1.6 Network Reconnaissance
3.1.7 Basics of Scanning
3.1.8 Perform Recon with Nmap
3.1.9 Certificate Transparency Logs
3.1.10 Information Disclosure
3.1.11 Search Engine Analysis/Enumeration
3.1.12 Network Sniffing
3.1.13 Data Manipulation
3.1.14 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 90 minutes)

3.2: Host and Service Discovery Techniques

Summary

Exam Objectives Covered

- 2.1 Given a scenario, apply information gathering techniques.
- 2.2 Given a scenario, apply enumeration techniques.
- 2.3 Given a scenario, modify scripts for reconnaissance and enumeration.
- 2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

Video/Demo

(includes 3 inline videos.)

Topics

3.2.1 What Is Enumeration?
3.2.2 Host Discovery
3.2.3 Scripting with Nmap
3.2.4 Activity: Scripting with Nmap
3.2.5 Banner Grabbing
3.2.6 Protocol Enumeration
3.2.7 Service Discovery

3.2.8 DNS Enumeration
3.2.9 Operating System (OS) Fingerprinting
3.2.10 Perform Enumeration with Nmap
3.2.11 Live Lab: DNS Enumeration and Reconnaissance
3.2.12 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 105 minutes)

3.3: Enumeration for Attack Planning

Summary

Exam Objectives Covered

- 2.2 Given a scenario, apply enumeration techniques.
- 2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.

Topics

3.3.1 Attack Path Mapping
3.3.2 Manual Enumeration
3.3.3 Simple Network Management Protocol
3.3.4 Documenting Enumeration Activities
3.3.5 Activity: Document Enumeration Activities
3.3.6 Lesson Review

Number of Assessment Questions

5 (about 5 minutes)

Total Time

(About 30 minutes)

3.4: Enumeration for Specific Assets

Summary

Exam Objectives Covered

- 2.2 Given a scenario, apply enumeration techniques.

- 2.4 Given a scenario, use the appropriate tools for reconnaissance and enumeration.
- 3.1 Given a scenario, conduct vulnerability discovery using various techniques.

Video/Demo

(includes 2 inline videos.)

Topics

3.4.1 Directory Enumeration
3.4.2 User Enumeration
3.4.3 Wireless Enumeration
3.4.4 Permission Enumeration
3.4.5 Secrets Enumeration
3.4.6 Share Enumeration
3.4.7 Web Application Firewall (WAF) Enumeration
3.4.8 Perform a Decoy Scan
3.4.9 Industrial Control Systems (ICS) Vulnerability Assessment
3.4.10 Web Crawling/HTML Scraping
3.4.11 Lesson Review

Number of Assessment Questions

5 (about 5 minutes)

Total Time

(About 70 minutes)

3.5: Module Quiz

Number of Assessment Questions

20 (about 20 minutes)

4.0: Scanning and Identifying Vulnerabilities

Overview

Summary

In this module, you will:

- Scan for Cleartext Vulnerabilities
- Use Metasploit
- Use aircrack-ng to Discover Hidden Networks
- Locate a Rogue Access Point
- Network Reconnaissance
- Scan for Linux Vulnerabilities

To gain access to a target device during the pentest, vulnerabilities will need to be identified. The pentester will then exploit these vulnerabilities in an attempt to gain access to the network resource. Using the information that was gathered during the reconnaissance and enumeration phases, the pentester will begin to scan for and identify potential vulnerabilities.

Total Time

(About 175 minutes)

4.1: Vulnerability Discovery Techniques

Summary

Exam Objectives Covered:

- 3.1 Given a scenario, conduct vulnerability discovery using various techniques.
- 3.2 Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Video/Demo

(includes 2 inline videos.)

Topics

4.1.1 Tools for Vulnerability Discovery
4.1.2 Types of Scans
4.1.3 Container Scans
4.1.4 Application Scans
4.1.5 Scan for Cleartext Vulnerabilities
4.1.6 Network Scans
4.1.7 Activity: Scan Identified Targets
4.1.8 Host-Based Scans
4.1.9 Live Lab: Using Metasploit
4.1.10 Secrets Scanning
4.1.11 Wireless Scans
4.1.12 Use aircrack-ng to Discover Hidden Networks
4.1.13 Locate a Rogue Wireless Access Point
4.1.14 Validate Scan, Reconnaissance, and Enumeration Results
4.1.15 Applied Live Lab: Network Reconnaissance
4.1.16 Scan for Linux Vulnerabilities
4.1.17 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 130 minutes)

4.2: Analyzing Reconnaissance Scanning and Enumeration

Summary

Exam Objectives Covered:

- 3.2 Given a scenario, analyze output from reconnaissance, scanning, and enumeration phases.

Topics

4.2.1 Public Exploit Selection
4.2.2 Use Scripting to Validate Results
4.2.3 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 10 minutes)

4.3: Physical Security Concepts

Summary

Exam Objectives Covered:

- 3.3 Explain physical security concepts.

Topics

4.3.1 Tailgating
4.3.2 Site Surveys
4.3.3 Universal Serial Bus (USB) Drops
4.3.4 Badge Cloning
4.3.5 Lock Picking
4.3.6 Documenting Scanning and Identifying Vulnerabilities Activities
4.3.7 Activity: Identify Physical Security Concepts
4.3.8 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 35 minutes)

4.4: Module Quiz

Number of Assessment Questions

15 (about 15 minutes)

4.5: Checkpoint Review

Number of Assessment Questions

20 (about 20 minutes)

5.0: Conducting Pentest Attacks

Overview

Summary

In this module, you will:

- Evaluate EOL Software and Systems
- Exploit Default Configurations with Responder
- Execute Scripts to Automate Tasks

Once the pentester has gathered information on the target and identified potential vulnerabilities, they will need to prioritize which vulnerabilities they want to exploit. The prioritization will be based on the goals of the pentest and the network devices that the pentester has discovered.

Once the pentester has determined which network resources to start exploiting, they will use the information that has been gathered to carry out their exploits on the target machines.

Total Time

(About 195 minutes)

5.1: Prepare and Prioritize Attacks

Summary

Exam Objectives Covered

- 4.1 Given a scenario, analyze output to prioritize and prepare attacks.

Video/Demo

(includes 1 inline videos.)

Topics

5.1.1 Target Prioritization
5.1.2 High-Value Asset Identification
5.1.3 Descriptors and Metrics
5.1.4 End-of-Life Software and Systems
5.1.5 Default Configurations
5.1.6 Running Services
5.1.7 Vulnerable Encryption Methods
5.1.8 Defensive Capabilities
5.1.9 Capability Selection
5.1.10 Exploit Selection and Customization
5.1.11 Documentation Procedures for Attacks
5.1.12 Dependencies
5.1.13 Consideration of Scope Limitations
5.1.14 Activity: Customize Exploits
5.1.15 Live Lab: Evaluate EOL Software & Systems
5.1.16 Applied Live Lab: Exploiting Default Configurations with Responder
5.1.17 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 140 minutes)

5.2: Scripting Automation

Summary

Exam Objectives Covered

- 4.10 Given a scenario, use scripting to automate attacks.

Topics

5.2.1 Types of Scripting Automation
5.2.2 PowerShell
5.2.3 Bash
5.2.4 Python
5.2.5 Breach and Attack Simulation (BAS)
5.2.6 Live Lab: Executing Scripts to Automate Tasks
5.2.7 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 55 minutes)

5.3: Module Quiz

Number of Assessment Questions

10 (about 10 minutes)

6.0: Web-based Attacks

Overview

Summary

In this module, you will:

- Evaluate a Database using SQLMap
- Exploit Directory Traversal
- Perform XSS
- Abuse Insecure Direct Object Reference
- Perform Lateral Movement
- Perform RFI and LFI Exploitation
- Perform and Analyze a SYN Flood Attack

Many of the systems that the pentester will be exploiting use web applications and cloud resources to perform their specified functions. because of this, web applications and cloud resources are a prime target that can be exploited to gain access to the system. The pentester needs to be knowledgeable on the different attacks that can be carried out against these systems.

Total Time

(About 350 minutes)

6.1: Web-based Attacks

Summary

Exam Objectives Covered

- 4.5 Given a scenario, perform web application attacks using the appropriate tools.

Video/Demo

(includes 2 inline videos.)

Topics

6.1.1 Web Application Attacks Overview
6.1.2 Types of Web Application Attacks
6.1.3 Tools for Performing Web Application Attacks
6.1.4 Brute-Force Attack
6.1.5 Collision Attack
6.1.6 Directory Traversal
6.1.7 Request Forgery Attacks
6.1.8 Deserialization Attack
6.1.9 Injection Attacks
6.1.10 Activity: Injection Attacks
6.1.11 Insecure Direct Object Reference
6.1.12 Session Hijacking
6.1.13 Arbitrary Code Execution
6.1.14 File Inclusions
6.1.15 API Abuse
6.1.16 JSON Web Token (JWT) Manipulation
6.1.17 Live Lab: Evaluating a Database Using SQLMap
6.1.18 Live Lab: Exploiting Directory Traversal
6.1.19 Live Lab: Performing XSS
6.1.20 Live Lab: Abusing Insecure Direct Object References
6.1.21 Live Lab: Performing Lateral Movement
6.1.22 Live Lab: Performing RFI and LFI Exploitation
6.1.23 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 280 minutes)

6.2: Cloud-based Attacks

Summary

Exam Objectives Covered

- 4.6 Given a scenario, perform cloud-based attacks using the appropriate tools.

Topics

6.2.1 Cloud-based Attacks Overview
6.2.2 Types of Cloud-based Attacks
6.2.3 Tools for Performing Cloud-based Attacks
6.2.4 Metadata Service Attacks
6.2.5 Access Management Misconfigurations
6.2.6 Third-party Integrations

6.2.7 Resource Misconfiguration
6.2.8 Activity: Conduct Resource Misconfiguration Attacks
6.2.9 Logging Information Exposure
6.2.10 Image and Artifact Tampering
6.2.11 Supply Chain Attacks
6.2.12 Workload Runtime Attacks
6.2.13 Container Escape
6.2.14 Trust Relationship Abuse
6.2.15 Perform and Analyze a SYN Flood Attack
6.2.16 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 70 minutes)

6.3: Module Quiz

Number of Assessment Questions

10 (about 10 minutes)

7.0: Enterprise Attacks

Overview

Summary

In this module, you will:

- Sniff Network Traffic
- Explore Nmap NSE
- Discover Vulnerabilities with Netcat
- Perform a Relay Attack
- Crack a Password with John the Ripper
- Crack Passwords
- Clear Audit Policies
- Perform Privilege Escalation
- Implement Payload Obfuscation
- Perform SQL Injection
- Investigate with Evil-WinRM
- Exploit LOLBins
- Implement Credential Dumping

When the pentester has identified their targets and researched and discovered potential vulnerabilities, they will begin attempting to exploit the targets. Depending on the resource, this can involve network based attacks or host based attacks. The pentester will want to attempt to authenticate themselves on the devices so they can navigate and carry out attacks as needed.

Total Time

(About 610 minutes)

7.1: Perform Network Attacks

Summary

Exam Objectives Covered

- 4.2 Given a scenario, perform network attacks using the appropriate tools.

Topics

7.1.1 Network Attack Types
7.1.2 Tools for Performing Network Attacks
7.1.3 Default Credentials
7.1.4 On-Path Attack
7.1.5 Certificate Services
7.1.6 Misconfigured Services Exploitation
7.1.7 Virtual Local Area Network (VLAN) Hopping
7.1.8 Multihomed Hosts
7.1.9 Relay Attack
7.1.10 IDS Evasion
7.1.11 Live Lab: Sniffing Network Traffic
7.1.12 Applied Live Lab: Exploring the Power of Nmap NSE
7.1.13 Live Lab: Discovering Vulnerabilities with Netcat
7.1.14 Applied Live Lab: Performing a Relay Attack
7.1.15 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 170 minutes)

7.2: Perform Authentication Attacks

Summary

Exam Objectives Covered

- 4.3 Given a scenario, perform authentication attacks using the appropriate tools.

Video/Demo

(includes 2 inline videos.)

Topics

7.2.1 Authentication Attack Types
7.2.2 Tools for Performing Authentication Attacks
7.2.3 Multifactor Authentication (MFA) Fatigue
7.2.4 Pass-the-Hash Attacks
7.2.5 Pass-the-Ticket Attacks
7.2.6 Pass-the-Token Attacks
7.2.7 Kerberos Attacks
7.2.8 Lightweight Directory Access Protocol (LDAP) Injection
7.2.9 Dictionary Attacks

7.2.10 Crack a Password with John the Ripper
7.2.11 Brute-Force Attacks
7.2.12 Mask Attacks
7.2.13 Password Spraying
7.2.14 Credential Stuffing
7.2.15 OpenID Connect (OIDC) Attacks
7.2.16 Security Assertion Markup Language (SAML) Attacks
7.2.17 Live Lab: Cracking Passwords
7.2.18 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 125 minutes)

7.3: Perform Host-Based Attacks

Summary

Exam Objectives Covered

- 4.4 Given a scenario, perform host-based attacks using the appropriate tools.

Video/Demo

(includes 3 inline videos.)

Topics

7.3.1 Types of Host-Based Attacks
7.3.2 Tools for Performing Host-Based Attacks
7.3.3 Privilege Escalation
7.3.4 Credential Dumping
7.3.5 Circumventing Security Tools
7.3.6 Clear Audit Policies
7.3.7 Misconfigured Endpoints
7.3.8 Payload Obfuscation
7.3.9 User-Controlled Access Bypass
7.3.10 Shell Escape
7.3.11 Kiosk Escape
7.3.12 Library Injection
7.3.13 Process Hollowing and Injection
7.3.14 Log Tampering
7.3.15 Unquoted Service Path Injection
7.3.16 Documenting Enterprise Attacks
7.3.17 Applied Live Lab: Performing an On-Path (AiTM) Attack

7.3.18 Live Lab: Performing Privilege Escalation
7.3.19 Live Lab: Implementing Payload Obfuscation
7.3.20 Live Lab: Performing SQL Injection
7.3.21 Live Lab: Investigating with Evil-WinRM
7.3.22 Live Lab: Exploiting LOLBins
7.3.23 Live Lab: Implementing Credential Dumping
7.3.24 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 315 minutes)

7.4: Module Quiz

Number of Assessment Questions

15 (about 15 minutes)

7.5: Checkpoint Review

Number of Assessment Questions

20 (about 20 minutes)

8.0: Specialized Attacks

Overview

Summary

In this module, you will:

- Perform wireless attacks
- Perform social engineering using SET
- Perform specialized system attacks

Oftentimes, the pentester will need to carry out specialized attacks against different targets. This can involve attacking the wireless network to sniff traffic, carrying out social engineering attacks to exploit the human element, or attempting to gain access to non-standard devices, such as vehicles. These systems are all integrated into the main network and can be exploited to gain access. The pentester needs to be aware of these systems and how to exploit them if they are to be successful.

Total Time

(About 180 minutes)

8.1: Wireless Attacks

Summary

Exam Objectives Covered

- 4.7 Given a scenario, perform wireless attacks using the appropriate tools.

Video/Demo

(includes 1 inline videos.)

Topics

8.1.1 Types of Wireless Attacks
8.1.2 Tools for Performing Wireless Attacks

8.1.3 Activity: Explore Wireless Tools
8.1.4 Wardriving
8.1.5 Bluetooth
8.1.6 Evil Twin Attack
8.1.7 Signal Jamming
8.1.8 Protocol Fuzzing
8.1.9 Packet Crafting
8.1.10 Deauthentication
8.1.11 Captive Portal
8.1.12 Wi-Fi Protected Setup (WPS) and Personal Identification (PIN) Attack
8.1.13 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 70 minutes)

8.2: Social Engineering Attacks

Summary

Exam Objectives Covered

- 4.8 Given a scenario, perform social engineering attacks using the appropriate tools.

Video/Demo

(includes 1 inline videos.)

Topics

8.2.1 Types of Social Engineering Attacks
8.2.2 Tools for Performing Social Engineering Attacks
8.2.3 Phishing, Whaling, Spear phishing, and Smishing
8.2.4 Social Engineering Techniques for Gathering Information
8.2.5 Watering Hole
8.2.6 Credential Harvesting
8.2.7 Live Lab: Performing Social Engineering using SET
8.2.8 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 70 minutes)

8.3: Specialized System Attacks

Summary

Exam Objectives Covered

- 4.9 Explain common attacks against specialized systems.

Topics

8.3.1 Types of Specialized System Attacks
8.3.2 Tools for Performing Specialized System Attacks
8.3.3 Mobile Attacks
8.3.4 AI Attacks
8.3.5 Operational Technology (OT)
8.3.6 Radio-Frequency Identification (RFID) and Near-Field Communication (NFC)
8.3.7 Bluejacking
8.3.8 Conducting Specialized Penetration Testing Attacks
8.3.9 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 40 minutes)

8.4: Module Quiz

Number of Assessment Questions

15 (about 15 minutes)

9.0: Performing Penetration Testing Tasks

Overview

Summary

In this module, you will:

- Create a Backdoor with Metasploit
- Configure Reverse and Bind Shells
- Establish Persistence and Other Post-Exploitation Activities
- Scan for Open Ports from a Remote Computer
- Perform Enumeration of MSSQL with Metasploit
- Perform a Scan using Zenmap
- Bypass Windows Firewall
- Hide Files with OpenStego
- Stage and Exfiltrate Using ADS

Once the pentester has gained access to their targets, they will want to establish persistence. This simply means that a method is established that will allow the pentester to quickly and easily reconnect to the system at a later time. This may mean installing a backdoor into the system, adding a user account with appropriate credentials, or other methods. The pentester will use these methods to move throughout the network establishing connections and persistence across multiple machines so data can be exfiltrated safely and without detection. Once the pentester has completed their tasks, they will want to clear out any evidence that they were in the systems.

Total Time

(About 250 minutes)

9.1: Establish and Maintain Persistence

Summary

Exam Objectives Covered

- 5.1 Given a scenario, perform tasks to establish and maintain persistence.

Video/Demo

(includes 1 inline videos.)

Topics

9.1.1 Principles of Establishing and Maintaining Persistence
9.1.2 Scheduled Tasks/cron Jobs
9.1.3 Service Creation
9.1.4 Reverse and Bind Shells
9.1.5 Add New Accounts
9.1.6 Obtain Valid Account Credentials
9.1.7 Registry Keys
9.1.8 Command and Control (C2) Frameworks
9.1.9 Backdoor
9.1.10 Activity: Maintain Persistence
9.1.11 Create a Backdoor with Metasploit
9.1.12 Rootkit
9.1.13 Browser Extensions
9.1.14 Tampering Security Controls
9.1.15 Live Lab: Configuring Reverse and Bind Shells
9.1.16 Live Lab: Establishing Persistence and Other Post-Exploitation Activities
9.1.17 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 135 minutes)

9.2: Move Laterally through Environments

Summary

Exam Objectives Covered

- 5.2 Given a scenario, perform tasks to move laterally throughout the environment.

Topics

9.2.1 Lateral and Horizontal Movement
9.2.2 Scan for Open Ports from a Remote Computer
9.2.3 Techniques for Moving Laterally through Environments
9.2.4 Tools for Moving Laterally through Environments
9.2.5 Pivoting
9.2.6 Relay Creation
9.2.7 Enumeration

9.2.8 Perform Enumeration of MSSQL with Metasploit
9.2.9 Service Discovery
9.2.10 Perform a Scan Using Zenmap
9.2.11 Bypass Windows Firewall
9.2.12 Windows Management Instrumentation (WMI)
9.2.13 Window Remote Management (WinRM)
9.2.14 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 45 minutes)

9.3: Staging and Exfiltration

Summary

Exam Objectives Covered

- 5.3 Summarize concepts related to staging and exfiltration.

Video/Demo

(includes 1 inline videos.)

Topics

9.3.1 Fundamentals of Staging and Exfiltration
9.3.2 Getting Data from a Target
9.3.3 Hide Files with OpenStego
9.3.4 Alternate Data Streams
9.3.5 Applied Live Lab: Staging and Exfiltration Using ADS
9.3.6 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 55 minutes)

9.4: Cleanup and Restoration

Summary

Exam Objectives Covered

- 5.4 Explain cleanup and restoration activities.

Topics

9.4.1 Cleanup and Restoration Procedures
9.4.2 Activity: Implement Cleanup and Restoration Activities
9.4.3 Documenting Penetration Testing Tasks
9.4.4 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 15 minutes)

9.5: Module Quiz

Number of Assessment Questions

20 (about 20 minutes)

10.0: Reporting and Recommendations

Overview

Summary

In this module, you will:

- Identify and describe components used to create a penetration report
- Understand the importance of using risk scoring in a penetration report
- Explain the importance of administrative controls
- Discuss the process of analyzing findings and developing recommendations

The next steps in preparing the report involve compiling all key components—executive summary, methodology, detailed findings, attack narrative, and tailored recommendations—to give stakeholders a clear understanding of the security assessment's results and suggested actions. The PenTester ensures that the report respects privacy and complies with legal standards while incorporating quality control measures and possibly AI tools to improve clarity and accuracy. The PenTester's recommendations will address vulnerabilities through technical measures like patch management, as well as administrative policies, operational safeguards, and physical controls, creating a multi-layered defense strategy to reduce attack risks and improve overall security.

Total Time

(About 70 minutes)

10.1: Penetration Test Report Components

Summary

Exam Objectives Covered

- 1.4 Explain the components of a penetration test report.

Topics

10.1.1 Creating the Penetration Test Report

10.1.2 Reporting Considerations
10.1.3 Report Components and Definitions
10.1.4 Documentation Specifications and Format Alignment
10.1.5 Risk Scoring
10.1.6 Test Limitations and Assumptions
10.1.7 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 30 minutes)

10.2: Analyze Findings and Remediation Recommendations

Summary

Exam Objectives Covered

- 1.5 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.

Video/Demo

(includes 1 inline videos.)

Topics

10.2.1 Analyzing Findings and Developing Recommendations Overview
10.2.2 Technical Controls
10.2.3 Administrative Controls
10.2.4 Operational Controls
10.2.5 Physical Controls
10.2.6 Activity: Administrative and Operational Controls
10.2.7 Lesson Review

Number of Assessment Questions

0 (about 0 minutes)

Total Time

(About 40 minutes)

10.3: Module Quiz

Number of Assessment Questions

10 (about 10 minutes)

A.0: PenTest+ PT0-003 Practice Exams

Overview

Summary

Learning Outcomes:

- Explain the value of a certification.
- Understand the structure and format of the certification exam.
- Know what objectives the exam covers.
- Feel prepared to sit for a certification exam.

With your certification in hand, you're joining a community of more than 2 million IT professionals who are CompTIA certified. You've earned a powerful, globally-recognized IT certification that will showcase your skills and help you advance your career.

Total Time

(About 210 minutes)

A.1: Prepare for CompTIA PenTest+ Certification

Summary

Topics

A.1.1 Why Should I Take a Certification Exam?
A.1.2 Exam Details for PenTest+ (PT0-003)
A.1.3 How to Take the Certification Exam
A.1.4 Tips for Taking the Exam

Total Time

(About 20 minutes)

A.2: Practice Exams

Summary

Topics

A.2.1 Exam Practice 1: Engagement Management
A.2.2 Exam Practice 2: Reconnaissance and Enumeration
A.2.3 Exam Practice 3: Vulnerability Discovery, and Analysis
A.2.4 Exam Practice 4: Attacks and Exploits
A.2.5 Exam Practice 5: Post-exploitation and Lateral Movement
A.2.6 PenTest+ PT0-003 Exam Practice

Number of Assessment Questions

190 (about 190 minutes)

Total Time

(About 190 minutes)

Approximate Time for the Course

The total time for the PenTest+ CertMaster Perform course is approximately 44 hours and 10 minutes. Time is calculated by adding the approximate time for each section which is calculated using the following elements:

- Video/demo (10 minutes assigned per video or demo)
- Live Labs (30 minutes assigned per lab)
- Simulation Labs (12 minutes assigned per lab)
- Text Lessons (5 minutes assigned per text lesson)
- Questions (1 minute per question)
- Interactives (5 minutes assigned per interactive)

The breakdown for this course is as follows:

Module	Lessons	Totals	Videos	Labs	Text	Questions	Interactives
1.0: Penetration Testing: Before You Begin							
	1.1: Professional Conduct and Penetration Testing	6	1	1	5	0	0
	1.2: Collaboration and Communication	12	0	0	12	0	0
	1.3: Testing Frameworks and Methodologies	9	0	0	9	0	0
	1.4: Introduction to Scripting for Penetration Testing	7	0	0	6	0	1
	1.6: Module Quiz	20	0	0	0	20	0
	Total time	03:40	00:10	00:30	02:40	00:20	00:00
2.0: Applying Pre-Engagement Activities							
	2.1: Define the Scope	4	0	0	4	0	0
	2.2: Compare Types of Assessments	9	0	0	8	0	1
	2.3: Utilize the Shared Responsibility Model	5	0	0	5	0	0
	2.4: Identify Legal and Ethical Considerations	4	0	0	4	0	0
	2.6: Module Quiz	20	0	0	0	20	0

Module	Lessons	Totals	Videos	Labs	Text	Questions	Interactives
	Total time	02:05	00:00	00:00	01:45	00:20	00:00
3.0: Enumeration and Reconnaissance							
	3.1: Information Gathering Techniques	13	3	1	12	0	0
	3.2: Host and Service Discovery Techniques	11	3	2	8	0	1
	3.3: Enumeration for Attack Planning	10	0	0	4	5	1
	3.4: Enumeration for Specific Assets	15	2	1	9	5	0
	3.6: Module Quiz	20	0	0	0	20	0
	Total time	05:41	01:20	01:06	02:45	00:30	00:00
4.0: Scanning and Identifying Vulnerabilities							
	4.1: Vulnerability Discovery Techniques	16	2	6	9	0	1
	4.2: Analyzing Reconnaissance Scanning and Enumeration	2	0	0	2	0	0
	4.3: Physical Security Concepts	7	0	0	6	0	1
	4.5: Module Quiz	15	0	0	0	15	0
	4.6: Checkpoint Review	20	0	0	0	20	0
	Total time	04:08	00:20	01:48	01:25	00:35	00:00
5.0: Conducting Pentest Attacks							
	5.1: Prepare and Prioritize Attacks	16	1	2	13	0	1
	5.2: Scripting Automation	6	0	1	5	0	0
	5.4: Module Quiz	10	0	0	0	10	0
	Total time	03:20	00:10	01:30	01:30	00:10	00:00
6.0: Web-based Attacks							
	6.1: Web-based Attacks	22	2	6	15	0	1
	6.2: Cloud-based Attacks	15	0	1	13	0	1
	6.4: Module Quiz	10	0	0	0	10	0
	Total time	06:02	00:20	03:12	02:20	00:10	00:00
7.0: Enterprise Attacks							
	7.1: Perform Network Attacks	14	0	4	10	0	0
	7.2: Perform Authentication Attacks	17	2	2	15	0	0
	7.3: Perform Host-Based Attacks	23	3	8	15	0	0

Module	Lessons	Totals	Videos	Labs	Text	Questions	Interactives
	7.5: Module Quiz	15	0	0	0	15	0
	7.6: Checkpoint Review	20	0	0	0	20	0
	Total time	11:09	00:50	06:24	03:20	00:35	00:00
8.0: Specialized Attacks							
	8.1: Wireless Attacks	12	1	0	11	0	1
	8.2: Social Engineering Attacks	7	1	1	6	0	0
	8.3: Specialized System Attacks	8	0	0	8	0	0
	8.5: Module Quiz	15	0	0	0	15	0
	Total time	03:10	00:20	00:30	02:05	00:15	00:00
9.0: Performing Penetration Testing Tasks							
	9.1: Establish and Maintain Persistence	16	1	3	12	0	1
	9.2: Move Laterally through Environments	13	0	4	9	0	0
	9.3: Staging and Exfiltration	5	1	2	3	0	0
	9.4: Cleanup and Restoration	3	0	0	2	0	1
	9.6: Module Quiz	20	0	0	0	20	0
	Total time	05:32	00:20	02:42	02:10	00:20	00:00
10.0: Reporting and Recommendations							
	10.1: Penetration Test Report Components	6	0	0	6	0	0
	10.2: Analyze Findings and Remediation Recommendations	6	1	0	5	0	1
	10.4: Module Quiz	10	0	0	0	10	0
	Total time	01:15	00:10	00:00	00:55	00:10	00:00
A.0: PenTest+ PT0-003 Practice Exams							
	A.1: Prepare for CompTIA PenTest+ Certification	4	0	0	4	0	0
	A.2: Practice Exams	190	0	0	0	190	0
	Total time	03:30	00:00	00:00	00:20	03:10	00:00