



Course Outline for PenTest+ (PT0-002) CertMaster Learn, Student Guide and CertMaster Labs

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
Overview	Each of the bulleted activities below is a separate study task within the CertMaster Learn learning plan. Students are encouraged to complete a certain number of tasks in each login session based on their desired course completion date.	Review Activities are embedded within the eBook. Videos and Practice Questions are found in the CompTIA Learning Center, the platform through which the eBook is delivered.	Labs are available at the course level or integrated as study tasks within CertMaster Learn.
Lesson 1: Scoping Organizational/Customer Requirements			
Topic 1A: Define Organizational PenTesting <i>Exam objectives covered:</i> 1.2 Explain the importance of scoping and organizational/customer requirements. 4.3 Explain the importance of communication during the penetration testing process.	<ul style="list-style-type: none"> • Video: Job Roles Using PenTest+ • Review Activity: Organizational PenTesting 	<ul style="list-style-type: none"> • Video: Job Roles Using PenTest+ • Review Activity: Organizational PenTesting 	
Topic 1B: Acknowledge Compliance Requirements <i>Exam objectives covered:</i> 1.1 Compare and contrast governance, risk, and compliance reports.	<ul style="list-style-type: none"> • Review Activity: Compliance Requirements 	<ul style="list-style-type: none"> • Review Activity: Compliance Requirements 	
Topic 1C: Compare Standards and Methodologies	<ul style="list-style-type: none"> • Review Activity: Standards and Methodologies 	<ul style="list-style-type: none"> • Review Activity: Standards and Methodologies 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p><i>Exam objectives covered:</i> 1.2 Explain the importance of scoping and organizational/customer requirements.</p> <p>2.1 Given a scenario, perform passive reconnaissance.</p>			
<p>Topic 1D: Describe Ways to Maintain Professionalism</p> <p><i>Exam objectives covered:</i> 1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.</p>	<ul style="list-style-type: none"> Review Activity: Professionalism 	<ul style="list-style-type: none"> Review Activity: Professionalism 	
	<ul style="list-style-type: none"> Lesson 1: Practice Questions 	<ul style="list-style-type: none"> Lesson 1: Practice Questions 	<ul style="list-style-type: none"> Assisted Lab: Explore the Lab Environment
<p>Lesson 2: Defining the Rules of Engagement</p>			
<p>Topic 2A: Assess Environmental Considerations</p> <p><i>Exam objectives covered:</i> 1.1 Compare and contrast governance, risk, and compliance reports.</p> <p>1.2 Explain the importance of scoping and organizational/customer requirements.</p>	<ul style="list-style-type: none"> Review Activity: Environmental Considerations PBQ: Assess Environmental Considerations 	<ul style="list-style-type: none"> Review Activity: Environmental Considerations 	
<p>Topic 2B: Outline the Rules of Engagement</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> Review Activity: The Rules of Engagement 	<ul style="list-style-type: none"> Review Activity: The Rules of Engagement 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p><i>1.2 Explain the importance of scoping and organizational/customer requirements.</i></p> <p><i>1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.</i></p>			
<p>Topic 2C: Prepare Legal Documents</p> <p><i>Exam objectives covered: 1.1 Compare and contrast governance, risk, and compliance reports.</i></p>	<ul style="list-style-type: none"> Review Activity: Legal Documents 	<ul style="list-style-type: none"> Review Activity: Legal Documents 	
	<ul style="list-style-type: none"> Lesson 2: Practice Questions 	<ul style="list-style-type: none"> Lesson 2: Practice Questions 	
<p>Lesson 3: Footprinting and Gathering Intelligence</p>			
<p>Topic 3A: Discover the Target</p> <p><i>Exam objectives covered: 2.1 Given a scenario, perform passive reconnaissance.</i></p> <p><i>5.3 Explain use cases of the following tools during the phases of a penetration test.</i></p>	<ul style="list-style-type: none"> Video: Performing Passive Reconnaissance Review Activity: The Target 	<ul style="list-style-type: none"> Video: Performing Passive Review Activity: The Target 	
<p>Topic 3B: Gather Essential Data</p> <p><i>Exam objectives covered: 2.1 Given a scenario, perform passive reconnaissance.</i></p>	<ul style="list-style-type: none"> Review Activity: Essential Data 	<ul style="list-style-type: none"> Review Activity: Essential Data 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p><i>5.3 Explain use cases of the following tools during the phases of a penetration test.</i></p>			
<p>Topic 3C: Compile Website Information</p> <p><i>Exam objectives covered:</i></p> <p><i>2.1 Given a scenario, perform passive reconnaissance.</i></p> <p><i>2.2 Given a scenario, perform active reconnaissance.</i></p> <p><i>2.3 Given a scenario, analyze the results of a reconnaissance exercise.</i></p> <p><i>5.3 Explain use cases of the following tools during the phases of a penetration test.</i></p>	<ul style="list-style-type: none"> • Video: Performing Passive Reconnaissance • Review Activity: Website Information 	<ul style="list-style-type: none"> • Video: Performing Passive Reconnaissance • Review Activity: Website Information 	<ul style="list-style-type: none"> • Assisted Lab: Exploring the Domain Tools: Nslookup, Dig and Whois
<p>Topic 3D: Discover Open-Source Intelligence Tools</p> <p><i>Exam objectives covered:</i></p> <p><i>2.1 Given a scenario, perform passive reconnaissance.</i></p> <p><i>5.3 Explain use cases of the following tools during the phases of a penetration test.</i></p>	<ul style="list-style-type: none"> • Review Activity: Open-Source Intelligence Tools • PBQ: Footprinting and Gathering Intelligence 	<ul style="list-style-type: none"> • Review Activity: Open-Source Intelligence Tools 	<ul style="list-style-type: none"> • Assisted Lab: Navigating Open-Source Intelligence Tools
	<ul style="list-style-type: none"> • Lesson 3: Practice Questions 	<ul style="list-style-type: none"> • Lesson 3: Practice Questions 	
<p>Lesson 4: Evaluating Human and Physical Vulnerabilities</p>			
<p>Topic 4A: Exploit the Human Psyche</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> • Review Activity: The Human Psyche • PBQ: Exploit the Human Psyche 	<ul style="list-style-type: none"> • Review Activity: The Human Psyche 	<ul style="list-style-type: none"> • Assisted Lab: Understanding Social Engineering Toolkit (SET)

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>3.6 Given a scenario, perform a social engineering or physical attack.</p>			
<p>Topic 4B: Summarize Physical Attacks</p> <p><i>Exam objectives covered:</i> 3.6 Given a scenario, perform a social engineering or physical attack.</p>	<ul style="list-style-type: none"> Review Activity: Physical Attacks PBQ: Configure Cloud Storage Solutions 	<ul style="list-style-type: none"> Review Activity: Physical Attacks 	
<p>Topic 4C: Use Tools to Launch a Social Engineering Attack</p> <p><i>Exam objectives covered:</i> 5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Tools to Launch a Social Engineering Attack PBQ: Use Tools to Launch a Social Engineering Attack 	<ul style="list-style-type: none"> Review Activity: Tools to Launch a Social Engineering Attack 	<ul style="list-style-type: none"> APPLIED Lab: Understanding Spear Phishing and Credentials Attack
	<ul style="list-style-type: none"> Lesson 4: Practice Questions 	<ul style="list-style-type: none"> Lesson 4: Practice Questions 	
<p>Lesson 5: Preparing the Vulnerability Scan</p>			
<p>Topic 5A: Plan the Vulnerability Scan</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p> <p>2.4 Given a scenario, perform vulnerability scanning.</p> <p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p>	<ul style="list-style-type: none"> Video: Performing Vulnerability Scanning Review Activity: The Vulnerability Scan 	<ul style="list-style-type: none"> Video: Performing Vulnerability Scanning Review Activity: The Vulnerability Scan 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
3.7 Given a scenario, perform post-exploitation techniques.			
<p>Topic 5B: Detect Defenses</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p>	<ul style="list-style-type: none"> Review Activity: Defenses 	<ul style="list-style-type: none"> Review Activity: Defenses 	<ul style="list-style-type: none"> Assisted Lab: Exploring OpenVAS
<p>Topic 5C: Utilize Scanning Tools</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Scanning Tools 	<ul style="list-style-type: none"> Review Activity: Scanning Tools 	<ul style="list-style-type: none"> Assisted Lab: Using Web Scanners
	<ul style="list-style-type: none"> Lesson 5: Practice Questions 	<ul style="list-style-type: none"> Lesson 5: Practice Questions 	
Lesson 6: Scanning Logical Vulnerabilities			
<p>Topic 6A: Scan Identified Targets</p> <p><i>Exam objectives covered:</i> 2.4 Given a scenario, perform vulnerability scanning.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Identified Targets PBQ: Compare Different Types of Scans 	<ul style="list-style-type: none"> Review Activity: Identified Targets 	
<p>Topic 6B: Evaluate Network Traffic</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p>	<ul style="list-style-type: none"> Review Activity: Network Traffic 	<ul style="list-style-type: none"> Review Activity: Network Traffic 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>2.3 Given a scenario, analyze the results of a reconnaissance exercise.</p> <p>3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>			
<p>Topic 6C: Uncover Wireless Assets</p> <p><i>Exam objectives covered:</i></p> <p>2.2 Given a scenario, perform active reconnaissance.</p> <p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Wireless Assets 	<ul style="list-style-type: none"> Review Activity: Wireless Assets 	
	<ul style="list-style-type: none"> Lesson 6: Practice Questions 	<ul style="list-style-type: none"> Lesson 6: Practice Questions 	
<p>Lesson 7: Analyzing Scanning Results</p>			
<p>Topic 7A: Discover Nmap and NSE</p> <p><i>Exam objectives covered:</i></p> <p>2.3 Given a scenario, analyze the results of a reconnaissance exercise.</p> <p>2.4 Given a scenario, perform vulnerability scanning.</p>	<ul style="list-style-type: none"> Review Activity: Nmap and NSE 	<ul style="list-style-type: none"> Review Activity: Nmap and NSE 	<ul style="list-style-type: none"> Assisted Lab: Understanding Nmap Common Usage

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p>			
<p>Topic 7B: Enumerate Network Hosts</p> <p><i>Exam objectives covered:</i> 2.4 Given a scenario, perform vulnerability scanning.</p> <p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p>	<ul style="list-style-type: none"> Review Activity: Network Hosts 	<ul style="list-style-type: none"> Review Activity: Network Hosts 	<ul style="list-style-type: none"> Assisted Lab: Understanding Scan Output
<p>Topic 7C: Analyze Output from Scans</p> <p><i>Exam objectives covered:</i> 2.3 Given a scenario, analyze the results of a reconnaissance exercise.</p> <p>3.1 Given a scenario, research attack vectors and perform wireless attacks.</p>	<ul style="list-style-type: none"> Review Activity: Output from Scans PBQ: Analyzing Scanning Results 	<ul style="list-style-type: none"> Review Activity: Output from Scans 	<ul style="list-style-type: none"> APPLIED Lab: Scanning a Vulnerable System
	<ul style="list-style-type: none"> Lesson 7: Practice Questions 	<ul style="list-style-type: none"> Lesson 7: Practice Questions 	
<p>Lesson 8: Avoiding Detection and Covering Tracks</p>			
<p>Topic 8A: Evade Detection</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p> <p>3.7 Given a scenario, perform post-exploitation techniques.</p>	<ul style="list-style-type: none"> Review Activity: Detection PBQ: Understand Cloud Automation and Orchestration Techniques 	<ul style="list-style-type: none"> Review Activity: Detection 	<ul style="list-style-type: none"> Assisted Lab: Using ProxyChains

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>			
<p>Topic 8B: Use Steganography to Hide and Conceal</p> <p><i>Exam objectives covered:</i> 3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Steganography to Hide and Conceal 	<ul style="list-style-type: none"> Review Activity: Steganography to Hide and Conceal 	<ul style="list-style-type: none"> Assisted Lab: Navigating Steganography Tools
<p>Topic 8C: Establish a Covert Channel</p> <p><i>Exam objectives covered:</i> 3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: A Covert Channel PBQ: Avoiding Detection and Covering Tracks 	<ul style="list-style-type: none"> Review Activity: A Covert Channel 	
	<ul style="list-style-type: none"> Lesson 8: Practice Questions 	<ul style="list-style-type: none"> Lesson 8: Practice Questions 	
<p>Lesson 9: Exploiting the LAN and Cloud</p>			
<p>Topic 9A: Enumerating Hosts</p> <p><i>Exam objectives covered:</i> 2.2 Given a scenario, perform active reconnaissance.</p> <p>3.7 Given a scenario, perform post-exploitation techniques.</p>	<ul style="list-style-type: none"> Review Activity: The LAN and Cloud 	<ul style="list-style-type: none"> Review Activity: The LAN and Cloud 	<ul style="list-style-type: none"> Assisted Lab: Demonstrating Enumeration Techniques

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>Topic 9B: Attack LAN Protocols</p> <p><i>Exam objectives covered:</i></p> <p>2.2 Given a scenario, perform active reconnaissance.</p> <p>3.1 Given a scenario, research attack vectors and perform network attacks.</p>	<ul style="list-style-type: none"> • Video: Researching Attack Vectors and Performing Network Attacks • Review Activity: LAN Protocols 	<ul style="list-style-type: none"> • Video: Researching Attack Vectors and Performing Network Attacks • Review Activity: LAN Protocols 	
<p>Topic 9C: Compare Exploit Tools</p> <p><i>Exam objectives covered:</i></p> <p>3.1 Given a scenario, research attack vectors and perform network attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> • Review Activity: Exploit Tools • PBQ: Compare Exploit Tools 	<ul style="list-style-type: none"> • Review Activity: Exploit Tools 	<ul style="list-style-type: none"> • Assisted Lab: Exploring the Basics of Metasploit
<p>Topic 9D: Discover Cloud Vulnerabilities</p> <p><i>Exam objectives covered:</i></p> <p>2.2 Given a scenario, perform active reconnaissance.</p> <p>3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> • Review Activity: Cloud Vulnerabilities 	<ul style="list-style-type: none"> • Review Activity: Cloud Vulnerabilities 	
<p>Topic 9E: Explore Cloud-Based Attacks</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> • Review Activity: Cloud-Based Attacks • PBQ: Explore Cloud-Based Attacks 	<ul style="list-style-type: none"> • Review Activity: Cloud-Based Attacks 	<ul style="list-style-type: none"> • APPLIED Lab: Using VSFTP Manual and Metasploit

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies.			
	<ul style="list-style-type: none"> Lesson 9: Practice Questions 	<ul style="list-style-type: none"> Lesson 9: Practice Questions 	
Lesson 10: Testing Wireless Networks			
<p>Topic 10A: Discover Wireless Attacks</p> <p><i>Exam objectives covered:</i></p> <p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Video: Researching Attack Vectors and Performing Wireless Attacks Review Activity: Wireless Attacks 	<ul style="list-style-type: none"> Video: Researching Attack Vectors and Performing Wireless Attacks Review Activity: Wireless Attacks 	
<p>Topic 10B: Explore Wireless Tools</p> <p><i>Exam objectives covered:</i></p> <p>3.2 Given a scenario, research attack vectors and perform wireless attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Wireless Tools PBQ: Compare Wireless Tools 	<ul style="list-style-type: none"> Review Activity: Wireless Tools 	<ul style="list-style-type: none"> Assisted Lab: Monitoring with Aircrack-ng
	<ul style="list-style-type: none"> Lesson 10: Practice Questions 	<ul style="list-style-type: none"> Lesson 10: Practice Questions 	
Lesson 11: Targeting Mobile Devices			
<p>Topic 11A: Recognize Mobile Device Vulnerabilities</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> Review Activity: Mobile Device Vulnerabilities 	<ul style="list-style-type: none"> Review Activity: Mobile Device Vulnerabilities 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<i>3.5 Explain common attacks and vulnerabilities against specialized systems.</i>			
<p>Topic 11B: Launch Attacks on Mobile Devices</p> <p><i>Exam objectives covered:</i> 3.2 Given a scenario, research attack vectors and perform wireless attacks.</p> <p><i>3.5 Explain common attacks and vulnerabilities against specialized systems.</i></p>	<ul style="list-style-type: none"> Review Activity: Attacks on Mobile Devices PBQ: Compare Attacks on Mobile Devices 	<ul style="list-style-type: none"> Review Activity: Attacks on Mobile Devices 	
<p>Topic 11C: Outline Assessment Tools for Mobile Devices</p> <p><i>Exam objectives covered:</i> 3.5 Explain common attacks and vulnerabilities against specialized systems.</p>	<ul style="list-style-type: none"> Review Activity: Assessment Tools for Mobile Devices 	<ul style="list-style-type: none"> Review Activity: Assessment Tools for Mobile Devices 	
	<ul style="list-style-type: none"> Lesson 11: Practice Questions 	<ul style="list-style-type: none"> Lesson 11: Practice Questions 	
Lesson 12: Attacking Specialized Systems			
<p>Topic 12A: Identify Attacks on the IoT</p> <p><i>Exam objectives covered:</i> 3.5 Explain common attacks and vulnerabilities against specialized systems.</p>	<ul style="list-style-type: none"> Review Activity: Attacks on the IoT 	<ul style="list-style-type: none"> Review Activity: Attacks on the IoT 	<ul style="list-style-type: none"> Assisted Lab: Discovering IoT devices with Shodan
<p>Topic 12B: Recognize Other Vulnerable Systems</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> Review Activity: Other Vulnerable Systems 	<ul style="list-style-type: none"> Review Activity: Other Vulnerable Systems 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<i>3.5 Explain common attacks and vulnerabilities against specialized systems.</i>			
<p>Topic 12C: Explain Virtual Machine Vulnerabilities</p> <p><i>Exam objectives covered: 3.5 Explain common attacks and vulnerabilities against specialized systems.</i></p>	<ul style="list-style-type: none"> Review Activity: Virtual Machine Vulnerabilities 	<ul style="list-style-type: none"> Review Activity: Virtual Machine Vulnerabilities 	
	<ul style="list-style-type: none"> Lesson 12: Practice Questions 	<ul style="list-style-type: none"> Lesson 12: Practice Questions 	
Lesson 13: Web Application-Based Attacks			
<p>Topic 13A: Recognize Web Vulnerabilities</p> <p><i>Exam objectives covered: 3.3 Given a scenario, research attack vectors and perform application-based attacks.</i></p> <p><i>3.5 Explain common attacks and vulnerabilities against specialized systems.</i></p>	<ul style="list-style-type: none"> Review Activity: Web Vulnerabilities 	<ul style="list-style-type: none"> Review Activity: Web Vulnerabilities 	
<p>Topic 13B: Launch Session Attacks</p> <p><i>Exam objectives covered: 3.3 Given a scenario, research attack vectors and perform application-based attacks.</i></p> <p><i>3.7 Given a scenario, perform post-exploitation techniques.</i></p>	<ul style="list-style-type: none"> Video: Researching Attack Vectors and Performing Application-Based Attacks Review Activity: Session Attacks 	<ul style="list-style-type: none"> Video: Researching Attack Vectors and Performing Application-Based Attacks Review Activity: Session Attacks 	
<p>Topic 13C: Plan Injection Attacks</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> Review Activity: Injection Attacks PBQ: Recognize Injection Attacks 	<ul style="list-style-type: none"> Review Activity: Injection Attacks 	<ul style="list-style-type: none"> Assisted Lab: Using SQL Injection

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>2.2 Given a scenario, perform active reconnaissance.</p> <p>3.3 Given a scenario, research attack vectors and perform application-based attacks.</p>			
<p>Topic 13D: Identify Tools</p> <p><i>Exam objectives covered:</i> 3.3 Given a scenario, research attack vectors and perform application-based attacks.</p> <p>3.6 Given a scenario, perform a social engineering or physical attack.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> • Video: Performing a Social Engineering Attack • Review Activity: Tools 	<ul style="list-style-type: none"> • Video: Performing a Social Engineering Attack • Review Activity: Tools 	
	Lesson 13: Practice Questions	Lesson 13: Practice Questions	
<p>Lesson 14: Performing System Hacking</p>			
<p>Topic 14A: System Hacking</p> <p><i>Exam objectives covered:</i> 3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> • Review Activity: System Hacking 	<ul style="list-style-type: none"> • Review Activity: System Hacking 	<ul style="list-style-type: none"> • Assisted Lab: Using Reverse and Bind Shells
<p>Topic 14B: Use Remote Access Tools</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> • Review Activity: Remote Access Tools 	<ul style="list-style-type: none"> • Review Activity: Remote Access Tools 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<p>3.1 Given a scenario, research attack vectors and perform network attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>			
<p>Topic 14C: Analyze Exploit Code</p> <p><i>Exam objectives covered:</i> 3.1 Given a scenario, research attack vectors and perform attacks on cloud technologies.</p> <p>5.2 Given a scenario, analyze script or code sample for use in a penetration test.</p>	<ul style="list-style-type: none"> • Video: Researching Attack Vectors and Performing Attacks on Cloud Technologies • Review Activity: Exploit Code • PBQ: Analyze Exploit Code and Logic Constructs 	<ul style="list-style-type: none"> • Video: Researching Attack Vectors and Performing Attacks on Cloud Technologies • Review Activity: Exploit Code 	<ul style="list-style-type: none"> • Assisted Lab: Analyzing Exploit Code
	Lesson 14: Practice Questions	Lesson 14: Practice Questions	
Lesson 15: Scripting and Software Development			
<p>Topic 15A: Analyzing Scripts and Code Samples</p> <p><i>Exam objectives covered:</i> 5.2 Given a scenario, analyze a script or code sample for use in a penetration test.</p>	<ul style="list-style-type: none"> • Video: Analyzing a Script or Code Sample • Review Activity: Scripts and Code Samples 	<ul style="list-style-type: none"> • Video: Analyzing a Script or Code Sample • Review Activity: Scripts and Code Samples 	<ul style="list-style-type: none"> • Assisted Lab: Exploring Programming Shells
<p>Topic 15B: Create Logic Constructs</p> <p><i>Exam objectives covered:</i> 5.1 Explain the basic concepts of scripting and software development.</p>	<ul style="list-style-type: none"> • Review Activity: Logic Constructs • PBQ: Compare Various Logic Constructs 	<ul style="list-style-type: none"> • Review Activity: Logic Constructs 	
<p>Topic 15C: Automate Penetration Testing</p> <p><i>Exam objectives covered:</i></p>	<ul style="list-style-type: none"> • Review Activity: Penetration Testing 	<ul style="list-style-type: none"> • Review Activity: Penetration Testing 	<ul style="list-style-type: none"> • Assisted Lab: Applying PenTest Automation

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
5.2 Given a scenario, analyze a script or code sample for use in a penetration test.			
	Lesson 15: Practice Questions	Lesson 15: Practice Questions	
Lesson 16: Leveraging the Attack: Pivot and Penetrate			
<p>Topic 16A: Test Credentials</p> <p><i>Exam objectives covered:</i> 3.1 Given a scenario, research attack vectors and perform network attacks.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: Credentials 	<ul style="list-style-type: none"> Review Activity: Credentials 	<ul style="list-style-type: none"> Assisted Lab: Exploring Password Attacks with john the Ripper and Hydra
<p>Topic 16B: Move Throughout the System</p> <p><i>Exam objectives covered:</i> 3.7 Given a scenario, perform post-exploitation techniques.</p> <p>5.3 Explain use cases of the following tools during the phases of a penetration test.</p>	<ul style="list-style-type: none"> Review Activity: The System 	<ul style="list-style-type: none"> Review Activity: The System 	<ul style="list-style-type: none"> Assisted Lab: Using MimiKatz and Hashes
<p>Topic 16C: Maintain Persistence</p> <p><i>Exam objectives covered:</i> 3.7 Given a scenario, perform post-exploitation techniques.</p>	<ul style="list-style-type: none"> Review Activity: Persistence PBQ: Maintain Persistence 	<ul style="list-style-type: none"> Review Activity: Persistence 	
	Lesson 16: Practice Questions	Lesson 16: Practice Questions	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
Lesson 17: Communicating During the PenTesting Process			
Topic 17A: Define the Communication Path <i>Exam objectives covered: 4.3 Explain the importance of communication during the penetration testing process.</i>	<ul style="list-style-type: none"> Review Activity: The Communication Path 	<ul style="list-style-type: none"> Review Activity: The Communication Path 	
Topic 17B: Communication Triggers <i>Exam objectives covered: 4.3 Explain the importance of communication during the penetration testing process</i>	<ul style="list-style-type: none"> Review Activity: Communication Triggers PBQ: Recognize Communication Triggers 	<ul style="list-style-type: none"> Review Activity: Communication Triggers 	
Topic 17C: Use Built-In Tools for Reporting <i>Exam objectives covered: 4.3 Explain the importance of communication during the penetration testing process.</i>	<ul style="list-style-type: none"> Review Activity: Built-In Tools for Reporting 	<ul style="list-style-type: none"> Review Activity: Built-In Tools for Reporting 	
	Lesson 17: Practice Questions	Lesson 17: Practice Questions	
Lesson 18: Summarizing Report Components			
Topic 18A: Identify Report Audience <i>Exam objectives covered: 4.1 Compare and contrast important components of written reports.</i>	<ul style="list-style-type: none"> Review Activity: Report Audience 	<ul style="list-style-type: none"> Review Activity: Report Audience 	
Topic 18B: List Report Contents <i>Exam objectives covered:</i>	<ul style="list-style-type: none"> Review Activity: Report Contents 	<ul style="list-style-type: none"> Review Activity: Report Contents 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
<i>4.1 Compare and contrast important components of written reports.</i>			
<p>Topic 18C: Define Best Practices for Reports</p> <p><i>Exam objectives covered: 4.1 Compare and contrast important components of written reports.</i></p>	<ul style="list-style-type: none"> Review Activity: Best Practices for Reports 	<ul style="list-style-type: none"> Review Activity: Best Practices for Reports 	<ul style="list-style-type: none"> Assisted Lab: Exploring a Sample PenTest Report
	<ul style="list-style-type: none"> Lesson 18: Practice Questions 	<ul style="list-style-type: none"> Lesson 18: Practice Questions 	
Lesson 19: Recommending Remediation			
<p>Topic 19A: Employ Technical Controls</p> <p><i>Exam objectives covered: 3.5 Explain common attacks and vulnerabilities against specialized systems.</i></p> <p><i>4.2 Given a scenario, analyze the findings and recommend the appropriate.</i></p>	<ul style="list-style-type: none"> Review Activity: Technical Controls 	<ul style="list-style-type: none"> Review Activity: Technical Controls 	<ul style="list-style-type: none"> APPLIED Lab: Recommending Controls
<p>Topic 19B: Administrative and Operational Controls</p> <p><i>Exam objectives covered: 4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.</i></p>	<ul style="list-style-type: none"> Video: Analyzing the Finding and Recommending the Appropriate Remediation Review Activity: Administrative and Operational Controls 	<ul style="list-style-type: none"> Video: Analyzing the Finding and Recommending the Appropriate Remediation Review Activity: Administrative and Operational Controls 	
<p>Topic 19C: Physical Controls</p> <p><i>Exam objectives covered: 4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report.</i></p>	<ul style="list-style-type: none"> Review Activity: Physical Controls PBQ: Recommending Remediation 	<ul style="list-style-type: none"> Review Activity: Physical Controls 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
	<ul style="list-style-type: none"> Lesson 19: Practice Questions 	<ul style="list-style-type: none"> Lesson 19: Practice Questions 	
Lesson 20: Performing Post-Report Delivery Activities			
Topic 20A: Post-Engagement Cleanup <i>Exam objectives covered: 4.4 Explain post-report delivery activities.</i>	<ul style="list-style-type: none"> Review Activity: Post-Engagement Cleanup 	<ul style="list-style-type: none"> Review Activity: Post-Engagement Cleanup 	
Topic 20B: Follow-Up Actions <i>Exam objectives covered: 4.4 Explain post-report delivery activities.</i>	<ul style="list-style-type: none"> Review Activity: Follow-Up Actions 	<ul style="list-style-type: none"> Review Activity: Follow-Up Actions 	
	<ul style="list-style-type: none"> Lesson 20: Practice Questions 	<ul style="list-style-type: none"> Lesson 20: Practice Questions 	
	<ul style="list-style-type: none"> Final Assessment 	<ul style="list-style-type: none"> Final Assessment 	
	<ul style="list-style-type: none"> Strengths and Weaknesses Dashboard Flashcards Game Center 	<ul style="list-style-type: none"> Strengths and Weaknesses Dashboard 	
Student Resources	<ul style="list-style-type: none"> Mapping Course Content to CompTIA PenTest+ PT0-002 (pdf) 	<ul style="list-style-type: none"> Mapping Course Content to CompTIA PenTest+ PT0-002 (pdf) 	
Instructor Resources	<ul style="list-style-type: none"> Presentation Planner for PenTest+ PT0-002 (xlsx) Transition Guide for Official CompTIA PenTest+ PT0-002 001 to Official CompTIA PenTest+ PT0-002 (pdf) Onboarding Guide for Official CompTIA PenTest+ PT0-002 Content (pdf) Mapping Course Content to CompTIA 	<ul style="list-style-type: none"> Presentation Planner for PenTest+ PT0-002 (xlsx) Transition Guide for Official CompTIA PenTest+ PT0-002 to Official CompTIA PenTest+ PT0-002 (pdf) Onboarding Guide for Official CompTIA PenTest+ PT0-002 Content (pdf) Mapping Course Content to CompTIA PenTest+ PT0-002 (pdf) 	

Course Outline	CertMaster Learn	Student Guide eBook	CertMaster Labs
	PenTest+ PT0-002 (pdf) <ul style="list-style-type: none"> • Instructor PowerPoint Presentations for PenTest+ PT0-002 (zip) 	<ul style="list-style-type: none"> • Instructor PowerPoint Presentations for PenTest+ PT0-002 (zip) 	



©2021 CompTIA Properties, LLC, used under license by CompTIA Certifications, LLC. All rights reserved. All certification programs and education related to such programs are operated exclusively by CompTIA Certifications, LLC. CompTIA is a registered trademark of CompTIA Properties, LLC in the U.S. and internationally. Other brands and company names mentioned herein may be trademarks or service marks of CompTIA Properties, LLC or of their respective owners. Reproduction or dissemination prohibited without written consent of CompTIA Properties, LLC.