Updated 04/11/2024

Sign up

Comptia Pentest+© Certification Training (PT0-002)

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

Presentation

Our Comptia Pentest+© training course will prepare you effectively for certification. This certification will enable you to prove your skills in penetration testing and IT security, reinforcing your credibility and value on the professional market.

Our course curriculum covers various modules, including test planning and scope, information gathering and vulnerability scanning, attacks and exploits, reporting, as well as tool usage and code analysis.

Our training prepares you to pass the exam by providing in-depth knowledge of governance concepts, compliance regulations, attack methods, and penetration testing best practices.

We are constantly updating our program to reflect the latest developments in the industry and ensure that our learners have the most up-to-date skills.

Objectives

- Gain an in-depth understanding of regulatory compliance requirements
- Master the concepts of test planning and scope definition
- Apply recognized standards and methodologies
- Develop communication and report writing skills
- Familiarize yourself with a variety of vulnerability and code analysis tools

Target audience

- Pentesters
- Cybersecurity Analysts
- Security Consultants
- System administrators

Prerequisites

- 3 to 4 years' practical experience in performing penetration tests, vulnerability assessments and code analysis
- Solid knowledge of IT security
- Basic knowledge of penetration testing
- Knowledge of scripting languages such as Python or Ruby

Software requirements

- Virtualization environment (VMware or VirtualBox)
- Vulnerability testing tools (Nmap, Metasploit, Burp Suite, OWASP ZAP, SQLmap...)
- Tools for password management and secure storage of sensitive information

Note: Ambient IT is not the owner of Comptia Certifications©, this certification belongs to Comptia®, Inc.

Pentest+© Certification Preparation Program

Planning and Scoping (14%)

- Regulatory compliance considerations
  - Payment Card Industry Data
  - Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
- Location restrictions
  - Country limitations
  - Tool restrictions
  - Local laws
- Legal concepts
  - ALS
  - Privacy
  - Non-disclosure agreement (NDA)

- Standards and methodology
  - MITRE ATT&CK
  - Open Web Application
  - Security Project (OWASP)
  - National Institute of Standards
  - and Technology (NIST)
  - Open-source Security Testing
  - Methodology Manual (OSSTMM)
  - Penetration Testing
  - Execution Standard (PTES)
  - Information Systems Security
  - Assessment Framework (ISSAF)
- Rules of engagement
    - Time of day
  - Permitted/prohibited test types
  - Other restrictions
- Environmental considerations
  - NetworkApplicationCloud
- Target list/in-scope assets
  - Wireless networks
  - Internet Protocol (IP) ranges
  - Domains
  - Application programming interfaces (APIs)
  - Physical locations
  - Domain name system (DNS)
  - External vs. internal targets
  - First-party vs. third-party hosted
- Validate the scope of the mission
  - Interviewing customers/reviewing contracts
  - Time management
  - Strategy
  - Unknown vs. known environment testing
- Background checks on penetration testing team
- Identifying criminal activity
- Limiting the use of tools to a specific mission
- Maintain data/information confidentiality

Information gathering and vulnerability analysis (22%)

- DNS lookups
- Identify technical contacts
- Administrator contacts
- Cloud vs. self-hosted
- Scraping social networks
- Cryptographic faults
- Safety posture
- Data
  - Password dumps
  - Metadata files
  - Website archiving / caching
  - Public source code repositories
- OSINT
  - Tools (Shodan, Recon-ng)
  - Sources (CWE, CVE...)

- Website recognition
  - Crawling
  - Scraping
- Packet crafting (Scapy)
- Defense detection
- Tokens
- Wardriving
- Network traffic
- Cloud asset discovery
- Fingerprinting
- Analyse output from
- Analysis methods
- Nmap
- Vulnerability testing tools

Attacks and exploits (30%)

- Stress testing for availability
- Exploit resources (DB, Packet storm)
- Attacks
  - ARP poisoning
  - Exploit chaining
  - Password attacks
  - On-path (previously knownas man-in-the-middle)
  - Kerberoasting
  - DNS cache poisoning
  - Virtual local area network
  - (VLAN) hopping
  - Network access control (NAC) bypass
  - Media access control (MAC) spoofing
  - Link-Local Multicast Name
  - Resolution (LLMNR)/NetBIOS-
  - Name Service (NBT-NS) poisoning
  - New Technology LAN Manager
  - (NTLM) relay attacks
- Tools (Metasploit, Netcat, Nmap)
- Attack methods
- Falsifying server-side requests
- Attacks injections
- Application vulnerabilities
- API Attacks
- Directory traversal
- Tools (Web proxies, SQLmap, DirBuster)
- Mobile
  - Vulnerabilities
  - Attacks
  - Tools
  - IoT devices
  - BLE attacks
  - Vulnerabilities
- Vulnerabilities in data storage systems
- Management interface vulnerabilities
- Control and data acquisition system vulnerabilities
  - SCADA
  - IIoT
  - ICS

- Social engineering attacks
- Methods of influence
- Post-exploitation of tools
- Network segmentation tests
- Establish / maintain

Reporting and communication (18%)

- Report hearing
- Report contents
- report retention
- Secure distribution
- Technical inspections
  - System hardening
  - Clean up user input/parameterize queriesImplemented multifactor
  - authentication
  - Encrypt passwords
  - Process-level remediation
  - Patch management
  - Key rotation
- Administrative controls
  - Role-based access control
  - Secure software
  - Development cycle
  - Password requirements
  - Policies and procedures
- Operational controls
  - Job rotation
  - Time-of-day restrictions
  - Mandatory vacations
  - User training
- Physical controls
  - Access control vestibule
  - Biometric controls
  - Video surveillance
- Communication channel
- Communication triggers
- Reasons for communication
- Redefining priorities and objectives
- Post-engagement cleanup
- Follow-up actions / retest

Code analysis and tools (16%)

- Logical constructs
  - Loops
  - Conditions
  - Boolean operator
  - String operator
  - Arithmetic operator

- Data structures
  - JavaScript Object Notation (JSON)
  - Key value
  - Arrays
  - Dictionaries
  - Comma-separated values (CSV)
  - Lists
  - Trees
- Libraries
- Classes
- Procedures
- Functions
- Shells
- Programming languages (Python, Ruby, Perl, Javascript)
- Code analysis
  - Download files
  - Launch remote access
  - Enumerate users
  - Enumerate assets
- Automation options
  - Automate the penetration testing process
- Scripting to modify IP addresses during a test run
- Nmap script for enumerating and reporting

Strategy and methods for exam success Mock

exam

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.