CompTIA PenTest+

Exam PT0-002

CompTIA PenTest+ Exam PT0-002

Lesson 1

Scoping Organizational/Customer Requirements

Objectives

- Compare and contrast governance, risk, and compliance reports.
- Explain the importance of scoping and organizational/customer requirements
- Explain the importance of communication during the penetration testing process
- Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity
- Given a scenario, perform passive reconnaissance

Lesson 1

Topic 1A

Define Organizational PenTesting

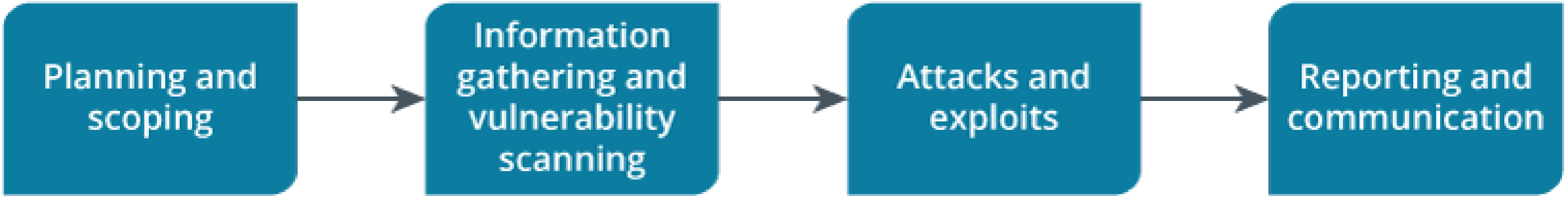
Assessing Cyber Health and Resiliency

- Companies recognize the need to secure their systems
- Many employ controls to ensure the CIA of data
  - Administrative controls
  - Physical controls
  - Technical or logical controls
- All controls should adhere to the Principle of Least Privilege

Reducing Overall Risk

- One of the primary goals of a PenTest is to reduce overall risk
- Formula for determining risk:
    - RISK = THREAT * VULNERABILITY
    - Threats include malware or natural disasters
    - Vulnerabilities – a weakness or flaw
- **Risk management** - process of identifying, assessing, analyzing, and responding to risks.

Recognizing the CompTIA Process


Planning and scoping
Information gathering and vulnerability scanning
Attacks and exploits
Reporting and communication

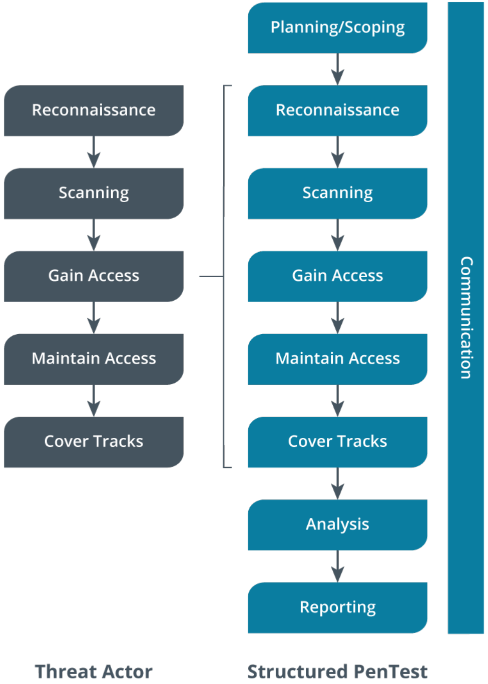
CompTIA Structured PenTest Process

Steps in the PenTest Process

- **Planning and scoping -** outline a plan for the PenTest.
- **Reconnaissance** gather information about the target.
- **Scanning -** identify live hosts, listening ports, and running services.
- **Gaining access -** see how deep into the network they can travel.
- **Maintaining access -** maintain access undetected for as long as possible
- **Covering tracks -** removes any evidence that the team was in the system
- **Analysis** - analyze the findings and derive a summary of the risk rating
- **Reporting -** deliver the results

Comparing Steps Taken During PenTesting

- PenTesting Team
  - Main goal – test an infrastructure’s defenses
- Threat Actor
  - Main goal - alter the integrity of the system



Review Activity: Organizational PenTesting

- Explain the process of scoping and organizational requirements.
- Outline the main steps of the structured PenTesting process
- Describe the importance of communication during the penetration testing process.

Lesson 1

Topic 1B

Acknowledge Compliance Requirements

Outlining PCI DSS

- Specifies controls that must be in place to handle credit card data.
  - Create and maintain a secure infrastructure.
  - Employ good practice strategies.
  - Continuously monitor for vulnerabilities
  - Employ appropriate anti-malware protection
  - Provide strong access control methods
  - Routinely monitor and test networks.

Assess, remediate, and report

- A company must be vigilant with efforts to secure the data.
- Testing ensures they are compliant
  - Complete an assessment and then report the results.
- Merchant level defines whether they must complete a ROC
  - **Level 1**—must have an external auditor perform the assessment by an approved Qualified Security Assessor (QSA).
  - **Levels 1 and 2** must complete a Report on Compliance
  - **Levels 2–4**—can either have an external auditor or submit a self-test that proves they are taking active steps to secure the infrastructure.

General Data Protection Regulation (GDPR)

- Focuses on the privacy of consumer data
  - Affects anyone who does business with residents of EU and Britain.
- Components include:
  - **Require consent** – ask permission for each data source
  - **Rescind consent** – consumer can opt out at any time
  - **Global reach** - anyone who does business with residents of EU and Britain.
  - **Restrict data collection** - collect only what is needed
  - **Violation reporting** – companies must report a breach within 72 hours.

Other Privacy Laws

- Stop Hacks and Improve Electronic Data Security (SHIELD)
  - Enacted in New York state to protect citizens data.
- California Consumer Privacy Act (CCPA)
  - Outlines specific guidelines on how to appropriately handle consumer data.
- Health Insurance Portability and Accountability Act (HIPAA)
  - Rigorous requirements for anyone that deals with patient information.

Review Activity: Define Organizational PenTesting

- Describe the components of PCI DSS
- List the main topics of GDPR
- Discuss other privacy laws that govern the protection of data:
    - SHIELD, CCPA and HIPAA

Lesson 1

Topic 1C

Compare Standards and Methodologies

Identifying Pentesting Frameworks

- A complete assessment will discover system weaknesses
- Many resources available that provide guidance on how to conduct an effective PenTesting exercise:
  - The Open Web Application Security Project (OWASP)
  - National Institute of Science and Technology (NIST)
  - Open-source Security Testing Methodology Manual (OSSTMM)

Providing Structure and Guidance

- Several organizations have developed structured guidelines and best practices to accomplish a PenTesting exercise.
  - **ISSAF** - open-source resource available to cybersecurity professionals.
  - **PTES** - provide a comprehensive overview of the proper structure of a complete PenTest.
  - **MITRE** provides research, publications, and tools at no charge for anyone who accesses the site.

MITRE ATT&CK

- ATT&CK - Adversarial Tactics, Techniques & Common Knowledge
- Provides tools and techniques specific to PenTesting.
- Contains categories that list tasks completed during a PenTest:
    - **Initial Access** lists attack vectors used to gain access to a network.
    - **Persistence** provides details on how to remain in a system.
    - **Credential access** provides solutions on how to obtain credentials,

Investigating CVE and CWE

- **CVE** - Common Vulnerabilities and Exposures is a listing of all publicly disclosed vulnerabilities.
  - Each entry refers to specific vulnerability of a particular product
  - Is cataloged with the name and description of the vulnerability
- **CWE** - Common Weakness Enumeration is a database of software-related weaknesses maintained by the MITRE Corporation

Review Activity: Compare Standards and Methodologies

- Identify Pentesting Frameworks
- List organizations have developed Pentest guidelines
- Describe the key elements of MITRE ATT&CK
- Compare and contrast CVE and CWE

Lesson 1

Topic 1D

Describe Ways to Maintain Professionalism

Validating the Team

- Each member of a PenTesting team needs to prove they can work in a secure environment:
  - Provide credentials, such as certifications that prove they have the appropriate skills to conduct PenTesting.
  - Produce recent background checks, that can include credit scores and driving records. Make sure no one has a criminal record or felony conviction.
- Stress how it's essential to identify and report criminal activity – even if the activity occurred by accident

Maintaining Confidentiality

- Everyone on the PenTest team must agree to conform to the policy on handling proprietary and sensitive information.
- The team should explicitly state to the client that the testers will protect information they discover during testing

Avoiding Prosecution

- Prior to beginning any testing, the team should outline the terms of the contract
  - Review all possible legal considerations that might be applicable.
- Carefully think through all scenarios.
  - Step though how they will complete the testing, along with possible conflicts that might occur.

Review Activity: Describe Ways to Maintain Professionalism

- List ways to assure the organization that the team has the appropriate experience and an excellent reputation.
- Explain the importance of maintaining confidentiality.
- Describe possible legal considerations that might be applicable during the PenTest process.

Lesson 1

Summary