Chapter 1

Penetration Testing

OUTLINES

- What Is Penetration Testing
- Cybersecurity Goals
- Reasons for Penetration Testing
- Threat Hunting
- Regulatory Requirements for Penetration Testing
- CompTIA Penetration Testing Process
- Cyber Kill Chain
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
- TOOLS

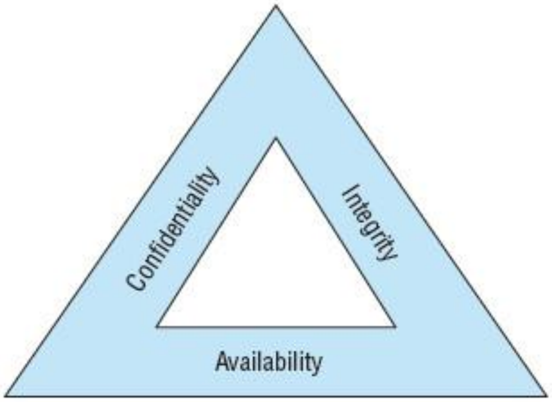
What Is Penetration Testing

Penetration testing seeks to bridge the gap between the rote uses of technical tools to test an organization's security and the **power of those tools when placed in the hands of a Skilled** and determined attacker.

Penetration tests are authorized, legal attempts to defeat
An organization's security controls and performs unauthorized activities.

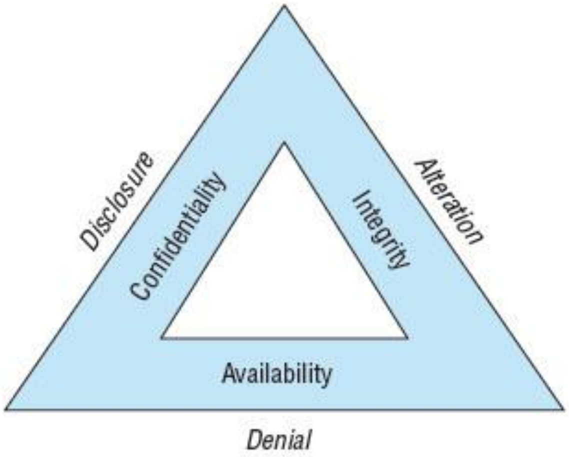
Cybersecurity Goals

- **Confidentiality** measures seek to prevent unauthorized access to information or systems.
- **Integrity** measures seek to prevent unauthorized modification of information or systems.
- **Availability** measures seek to ensure that legitimate use of information and systems remains possible.



The attackers' goals are known as the DAD triad

- Disclosure attacks seek to gain unauthorized access to information or systems.
- Alteration attacks seek to make unauthorized changes to information or systems.
- Denial attacks seek to prevent legitimate use of information and systems.



Adopting the Hacker Mind-Set

Let’s explore it using an example from the physical world. If you were responsible for the physical security of an Electronics store, you might consider a variety of threats and implement controls designed to counter those threats. You’d be worried about shoplifting, robbery, and employee embezzlement, among other threats, and you might build a system of security controls that seeks to prevent those threats from materializing. These controls might include the following items:

- Security cameras in high risk areas
- Auditing of cash register receipts
- Theft detectors at the main entrance/exit of the store
- Exit alarms on emergency exits
- Burglar alarm wired to detect the opening of doors outside of business hours

Reasons for Penetration Testing

Penetration testing provides us with visibility into the organization’s security posture that simply isn’t available by other means. Penetration testing does not seek to replace all of the other Cybersecurity activities of the organization. Instead, it complements and builds upon those efforts. Penetration testers bring their unique skills and perspective to the table and can take the output of security tools and place them within the attacker’s mind-set.

Threat Hunting

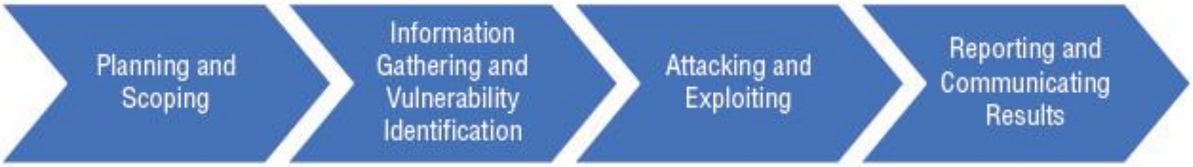
Cybersecurity professionals engaged in threat hunting seek to adopt the attacker’s mind-set and imagine how hackers might seek to defeat an organization’s security controls. The two disciplines diverge in what they accomplish with this information.

Threat hunting builds upon a Cybersecurity philosophy known as the “presumption of compromise.” This approach assumes that attackers have already successfully breached an organization and searches out the evidence of successful attacks.

Regulatory Requirements for Penetration Testing

- **Is based on industry accepted penetration testing approaches (for example, NIST SP800-115**
- **Includes coverage for the entire CDE perimeter and critical systems Reasons for Penetration Testing 7**
- **Includes testing from both inside and outside the network**
- **Includes testing to validate any segmentation and scope-reduction controls**
- **Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5**
- **Defines network-layer penetration tests to include components that support network functions as well as operating systems**
- **Includes review and consideration of threats and vulnerabilities experienced in the last 12 months**
- **Specifies retention of penetration testing results and remediation activities results**

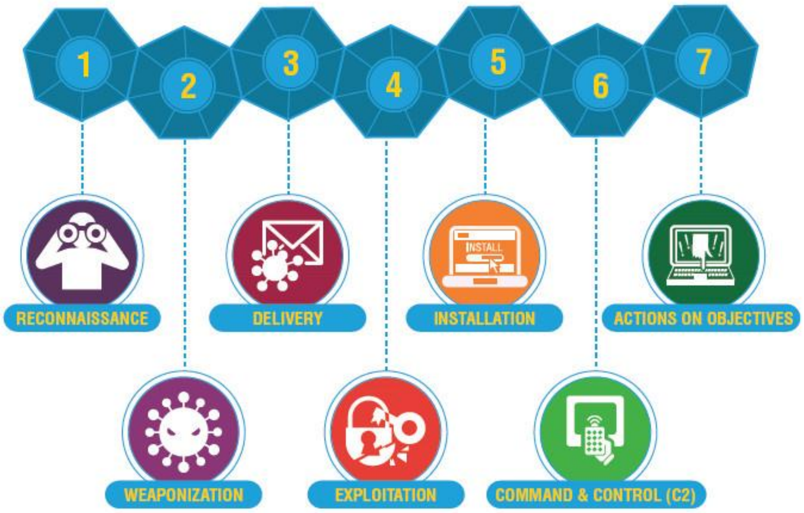
The CompTIA Penetration Testing Process


Planning and Scoping
Information Gathering and Vulnerability Identification
Attacking and Exploiting
Reporting and Communicating Results

- Planning and Scoping
- Information Gathering and Vulnerability Identification
- Attacking and Exploiting
- Reporting and Communicating Results

The Cyber Kill Chain

Describes how sophisticated attackers typically organize their work: the Cyber Kill Chain model. This approach, pioneered by Lockheed Martin, consists of the seven stages



Reconnaissance

The reconnaissance phase of the Cyber Kill Chain maps directly to the Information Gathering and Vulnerability Identification phase of the penetration testing process.
During this phase, attackers gather open-source intelligence and conduct initial scans of the target environment to detect potential avenues of exploitation.

Weaponization

After completing the Reconnaissance phase of an attack, attackers move into the remaining six steps, which expand upon the Attacking and Exploiting phase of the penetration testing process.

The first of these phases is Weaponization. During this stage, the attackers develop a Specific attack tool designed to exploit the vulnerabilities identified during reconnaissance.
They often use automated toolkits to develop a malware strain specifically tailored to infiltrate their target.

Delivery

After developing and testing their malware weapon, attackers next must deliver that malware to the target. This may occur through a variety of means, including exploiting a network or application vulnerability, conducting a social engineering attack, distributing malware on an infected USB drive or other media, sending it as an email attachment, or through other means.

Exploitation

Once the malware is delivered to the target organization, the attacker or the victim takes some action that triggers the malware’s payload, beginning the Exploitation phase of the Cyber Kill Chain. During this phase, the malware gains access to the targeted system. This may occur when the victim opens a malicious file or when the attacker exploits vulnerability over the network or otherwise gains a foothold on the target network.

Installation

The initial malware installation is designed only to enable temporary access to the target system. During the next phase of the Cyber Kill Chain, Installation, the attacker uses the initial access provided by the malware to establish permanent, or persistent, access to the target system. For this reason, many people describe the objective of this phase as establishing persistence in the target environment. Attackers may establish persistence by creating a back door that allows them to return to the system at a later date, by creating Registry entries that reopen access once an administrator closes it, or by installing a web shell that allows them to access the system over a standard HTTPS connection.

Command and Control

After establishing persistent access to a target system and network, the attacker may then use a remote shell or other means to remotely control the compromised system. The attacker may manually control the system using the shell or may connect it to anautomated command-and-control (C2C) network that provides it instructions. This automated approach is common in distributed denial of service (DDoS) attacks where the attacker simultaneously directs the actions of thousands of compromised systems, known as a botnet.

Tools:

Reconnaissance Tools:

- WHOIS tools gather information from public records about domain ownership.
- Nslookup tools help identify the IP addresses associated with an organization.
- TheHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.
- Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.
- Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.
- FOCA (Fingerprinting Organizations with Collected Archives) is an open-source tool used to find metadata within Office documents, PDFs, and other common file formats.
- Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.
- Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.

Vulnerability Scanners:

- Nessus is a commercial vulnerability scanning tool used to scan a wide variety of devices.
- OpenVAS is an open-source alternative to commercial tools such as Nessus OpenVAS also performs network vulnerability scans.
- Sqlmap is an open-source tool used to automate SQL injection attacks against web applications with database backends.
- Nikto and W3AF are open-source web application vulnerability scanners.

Social Engineering:

- The Social Engineer Toolkit (SET) provides a framework for automating the social engineering process, including sending spear phishing messages, hosting fake websites, and collecting credentials.

- The Browser Exploitation Framework (BeEF) provides an automated toolkit for using social engineering to take over a victim's web browser.

Credential-Testing:

- Hashcat, John the Ripper, Hydra, Medusa, Patator, and Cain and Abel are password cracking tools used to reverse engineer hashed passwords stored in files.
- CeWL is a custom wordlist generator that searches websites for keywords that may be used in password guessing attacks.
- Mimikatz retrieves sensitive credential information from memory on Windows systems.
- DirBuster is a brute-forcing tool used to enumerate files and directories on a webserver.

Debuggers:

- Immunity Debugger is designed specifically to support penetration testing and the reverse engineering of malware.
- GDB is a widely used open-source debugger for Linux that works with a variety of programming languages.
- OllyDbg is a Windows debugger that works on binary code at the assembly language level.
- WinDbg is another Windows-specific debugging tool that was created by Microsoft.
- IDA is a commercial debugging tool that works on Windows, Mac, and Linux platforms.

  In addition to decompiling traditional applications, penetration testers also may find themselves attempting to exploit vulnerabilities on mobile devices. You should be familiar with three mobile device security tools for the exam.
- Drozer is a security audit and attack framework for Android devices and apps.
- APKX and APK Studio decompile Android application packages (APKs).

Software Assurance:

- FindBugs and find-sec-bugs are Java software testing tools that perform static analysis of code.
- Peach and AFL are fuzzing tools that generate artificial input designed to test applications.
- SonarQube is an open-source continuous inspection tool for software testing.
- YASCA (Yet Another Source Code Analyzer) is another open-source software testing tool that includes scanners for a wide variety of languages. YASCA leverages FindBugs, among other tools.

Network Testing:

- Wireshark is a protocol analyzer that allows penetration testers to eavesdrop on and dissect network traffic.
- Hping is a command-line tool that allows testers to artificially generate network traffic.
- Aircrack-ng, WiFite, and Kismet are wireless network security testing tools.

Remote Access:

- Secure Shell (SSH) provides secure encrypted connections between systems.
- Ncat Netcat provides an easy way to read and write data over network connections.
- Proxychains allows testers to force connections through a proxy server where they may be inspected and altered before being passed on to their final destination.

Exploitation:

- Metasploit is, by far, the most popular exploitation framework and supports thousands of plug-ins covering different exploits.
- SearchSploit is a command-line tool that allows you to search through a database of known exploits.
- PowerSploit and Empire are Windows-centric sets of PowerShell scripts that may be used to automate penetration testing tasks.
- Responder is a toolkit used to answer NetBIOS queries from Windows systems on a network.
- Impacket is a set of network tools that provide low-level access to network protocols.

Questions

1. Tom is running a penetration test in a web application and discovers a flaw that allows him to shut down the web server remotely. What goal of penetration testing has Tom most directly achieved?
A. Disclosure
B. Integrity
C. Alteration
D. Denial

2. Brian ran a penetration test against a school's grading system and discovered a flaw that would allow students to alter their grades by exploiting a SQL injection vulnerability. What type of control should he recommend to the school's Cybersecurity team to prevent students from engaging in this type of activity?
A. Confidentiality
B. Integrity
C. Alteration
D. Availability

3. Edward Snowden gathered a massive quantity of sensitive information from the National Security Agency and released it to the media. What type of attack did he wage?
A. Disclosure
B. Denial
C. Alteration
D. Availability

4. Assuming no significant changes in an organization's cardholder data environment, how Often does PCI DSS require that a merchant accepting credit cards conduct penetration testing?
A. Monthly
B. Semiannually
C. Annually
D. Biannually

5. Which one of the following is NOT a benefit of using an internal penetration testing team?
A. Contextual knowledge
B. Cost
C. Subject matter expertise
D. Independence

6. Which one of the following is NOT a reason to conduct periodic penetration tests of systems and applications?
A. Changes in the environment
B. Cost
C. Evolving threats
D. New team members

7. Rich recently got into trouble with a client for using an attack tool during a penetration test that caused a system outage. During what stage of the penetration testing process should Rich and his clients have agreed upon the tools and techniques that he would use during the test?
A. Planning and Scoping
B. Information Gathering and Vulnerability Identification
C. Attacking and Exploiting
D. Reporting and Communication Results

8. Which one of the following steps of the Cyber Kill Chain does not map to the Attacking and Exploiting stage of the penetration testing process?
A. Weaponization
B. Reconnaissance
C. Installation
D. Actions on Objectives

9. Beth recently conducted a phishing attack against a penetration testing target in an attempt to gather credentials that she might use in later attacks. What stage of the penetration testing process is Beth in?
A. Planning and Scoping
B. Attacking and Exploiting
C. Information Gathering and Vulnerability Identification
D. Reporting and Communication Results

10. Which one of the following security assessment tools is not commonly used during the Information Gathering and Vulnerability Identification phase of a penetration test?
A. Nmap
B. Nessus
C. Metasploit
D. Nslookup

11. During what phase of the Cyber Kill Chain does an attacker steal information, use computing resources, or alter information without permission?
A. Weaponization
B. Installation
C. Actions on Objectives
D. Command and Control

12. Grace is investigating a security incident where the attackers left USB drives containing infected files in the parking lot of an office building. What stage in the Cyber Kill Chain describes this action?
A. Weaponization
B. Installation
C. Delivery
D. Command and Control

13. Which one of the following is not an open-source intelligence gathering tool?
A. WHOIS
B. Nslookup
C. Nessus
D. FOCA

14. Which one of the following tools is an exploitation framework commonly used by penetration testers?
A. Metasploit
B. Wireshark
C. Aircrack-ng
D. SET

15. Which one of the following tools is NOT a password cracking utility?
A. OWASP ZAP
B. Cain and Abel
C. Hashcat
D. Jack the Ripper

16. Which one of the following vulnerability scanners is specifically designed to test the security of web applications against a wide variety of attacks?
A. OpenVAS
B. Nessus
C. sqlmap
D. Nikto

17. Which one of the following debugging tools does not support Windows systems?
A. GDB
B. OllyDbg
C. WinDbg
D. IDA

18. What is the final stage of the Cyber Kill Chain?
A. Weaponization
B. Installation
C. Actions on Objectives
D. Command and Control

19. Which one of the following activities assumes that an organization has already been compromised?
A. Penetration testing
B. Threat hunting
C. Vulnerability scanning
D. Software testing

20. Alan is creating a list of recommendations that his organization can follow to remediate issues identified during a penetration test. In what phase of the testing process is Alan participating?

A. Planning and Scoping
B. Reporting and Communicating Results
C. Attacking and Exploiting
D. Information Gathering and Vulnerability Identification