6.13.2 Penetration Testing Facts

Penetration testing (also called a pen test) is an organization's attempt to circumvent security controls to identify vulnerabilities in their information systems. It simulates an actual attack on the network and is conducted from outside the organization's security perimeter. Penetration testing helps assure the effectiveness of an organization's security policy, security mechanism implementations, and deployed countermeasures. In general, the following steps are included in the penetration testing process:

- Verifying that a threat exists
- Bypassing security controls
- Actively testing security controls
- Exploiting vulnerabilities

Before starting a penetration test, it is important to define the Rules of Engagement (ROE), or the test's scope. The ROE defines the parameters and limits of the test; however, it usually does not include a complete list of all vulnerabilities. Important actions to take when preparing for a pen test include:

- Obtaining a written and signed authorization from the highest possible senior management
- Delegating personnel who are experts in the areas being tested.
- Gaining approval from the internet provider to perform the penetration test.
- Making sure that all tools or programs used in the testing are legal and ethical. It is important to verify this yourself, even if management approves your penetration testing plan.
- Establishing the scope and timeline.
- Identifying systems that will not be included in the test.
- Including in the authorization a statement that limits the tester's liability.
- Reviewing test findings with administrative personnel.

Types of penetration testing include:

Test	Examples
Physical Penetration	In a physical penetration test, the tester attempts to: - Enter a building without authorization - Access servers or workstations without authorization - Access wiring closets - Shut down power or other services
Operations Penetration	In an operations penetration test, the tester attempts to gain as much information as possible using the following methods: - Dumpster diving: attackers look through discarded papers or media for sensitive information. - Over-the-shoulder reconnaissance: attackers eavesdrop or obtain sensitive information from items that are not properly stored. - Social engineering: attackers act as imposters with the intent to gain access or information.
Electronic Penetration	In an electronic penetration test, the tester attempts to gain access and information about computer systems and the data on those systems. Definitions of the types of electronic penetration testing are as follows: - *System scanning* is using discovery protocols such as ICMP and SNMP to get as much information as possible from a system. - *Port scanning* is scanning various ports on remote hosts looking for well known services. - *Network monitoring* is using specialized tools to watch and log network activities. - *Sniffing* is the duplication of captured packets without altering or interfering with the flow of traffic on that medium. - *Fingerprinting* (also called footprinting) is scanning the system to identify the operating system, the patch level, and the applications and services available on it. For example, you can identify the operating system used by examining the format of the response to specific probes or messages.

Penetration testing is classified by the knowledge that the attacker and system personnel have prior to the attack.

- In a zero knowledge test (also called a black box test), the tester has no prior knowledge of the target system.
- In a full knowledge test (also called a white box test), the tester has detailed information prior to starting the test.
- In a partial knowledge test (also called the grey box test), the tester has the same amount of information that would be available to a typical insider in the organization.
- A single-blind test is one in which one side has advanced knowledge. For example, either the attacker has prior knowledge about the target system, or the defender has knowledge about the impending attack.
- A double-blind test is one in which the penetration tester does not have prior information about the system and the defender has no knowledge that the test is being performed. The double-blind test provides more accurate information about the security of the system.

The Open Source Security Testing Methodology Manual (OSSTMM) is a manual of a peer-reviewed methodology for performing security tests and metrics. It analyzes an organization's security in five categories:

- Personnel security
- Fraud and social engineering
- Computer and telecommunications networks
- Wireless and mobile devices
- Physical security

Penetration testing progresses in stages. Descriptions of these stages are presented in the table below:

Stage	Description
Passive Reconnaissance	*Passive reconnaissance* is characterized by gathering data. Passive reconnaissance does not directly affect the target. Examples of this stage include: - Putting a sniffer on the wire - Eavesdropping on employee conversations - Dumpster diving - Browsing the organization's website
Network Enumeration	*Network enumeration* (also called *network mapping*) involves a thorough and systematic discovery of as much of the corporate network as possible. Enumeration methods include: - Social engineering - *Wardriving*: Scanning for wireless access points within the organization - *War dialing*: Trying to access phone lines that will answer a calling modem - *Banner grabbing*: Capturing information transmitted by the remote host (including the application type, application version, and even operating system type and version) - *Firewalking*: Using traceroute techniques to discover which services can pass through a firewall or a router (common firewalking tools are Hping and Firewalk) - Probing the corporate network with scanning tools, often using the same tools used by hackers, such as SATAN and Nessus - Monitoring the network (usually performed from a remote site) - Soliciting host-specific banners to identify the function of a remote host *Vulnerability scanners* are an important part of network enumeration. There are several methods of scanning that can be employed for network enumeration: - *Ping scans* identify open ports using ping (ICMP) messages. - *UDP scans* determine which UDP service ports are open on a host by sending UDP packets to a target port. If an ICMP port unreachable message is returned, then the target does not use that port. - *TCP connect scans* discover TCP servers that are running on a host even if ICMP is blocked. Basic TCP connect scans are considered noisy because they can be noticed by logging and intrusion detection systems. To improve the stealth of TCP scans, the following types of TCP scans are used: - *TCP SYN scans* are less noisy because they do not require a fully open TCP session. TCP SYN packets are directed to a particular port by a test host. If the target responds RST, then the target is not listening. If a target responds SYN/ACK, then the target is listening on that port, and a test host will send an immediate RST to cut the connection. - *TCP FIN scans* are considered stealthy. A TCP packet with a FIN bit is sent to the target port by your test host. If the target responds with an RST packet, you may assume that the port is not being used. If there is no response, there's a possibility that the port is being used. - *TCP XMAS scans* are much like TCP FIN scans, but they also turn on the URG and PSH flags. - *TCP NULL scans* are much like the TCP FIN scans, but they turn off all flags. *Always* obtain senior management approval before scanning. This activity is a form of system intrusion and can cause undue alarm.
System Enumeration	*System enumeration* is the process of gaining as much information about a specific computer as possible. System enumeration initiates *fingerprinting*. Important facts about fingerprinting are: - Passive fingerprinting analyzes communications to and from a remote host. - Active fingerprinting analyzes the response to a stimulus. The analysis can determine the operating system and even the patch level. - Fingerprinting identifies an operating system or network service based on its ICMP message quoting characteristics. - With ICMP message quoting, portions of the original ICMP request are repeated (or quoted) within the response. - Each operating system quotes this information back in a slightly different manner.
Target Selection	*Target selection* is the process of identifying servers that appear available. An attack typically involves targeted servers that: - Present the path of least resistance - Are the easiest to exploit

Gaining Access	*Gaining access* is the act of performing the exploit. A successful exploit on a service or application typically leads to an attempt to: - Elevate privilege to local administrator or domain administrator - Grant more privileges to the system or entire network
Control and Reporting	*Control and reporting* is the process of documenting the following with as much detail as possible: - The level of access or control that was gained during the testing. - Methods used during the penetration test. - Services and systems exploited.

Penetration testing should attempt to breach system security in ways a hacker might. Penetration testing should be performed regularly to evaluate the effectiveness of safeguards and countermeasures used to protect information systems. The typical steps a hacker would take after gaining access to the system are as follows:

- Attempt to maintain access through the installation of root kits, backdoors, and perhaps Trojan horse applications used to capture information.
- Harden the system to prevent another attacker from gaining access.
- Attempt to cover the tracks by scrubbing the logs, hiding root kit files, and hiding the services and ports that may have been made available on the system.
- Attempt to modify existing permissions to grant the hacker further access to the system.
- Browse the system.
- Perform data theft.
- Launch attacks deeper into the corporate network from this system.