الجامعة الافتراضية السورية

أمن الشبكات
Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Vulnerability Assessment and Mitigating Attacks

Objectives of Lecture

- Understand the meaning and the importance of vulnerability assessment and penetration testing.
- Understand the vulnerability assessment methods.
- Understanding the security Testing Methodology and be aware of some tools that are used in testing.
- Recognize some security technologies that help in vulnerability assessment and mitigating attacks

Vulnerability assessment (1)

Vulnerability assessment is responsible for highlighting security weaknesses in computer systems, applications (web, mobile, etc.), and network infrastructures.

It offers an organization a clearer understanding of their network environment and provides the information on the security flaws in it.

The primary goal of network vulnerability assessment is to reduce the probability that cybercriminals will find the weaknesses in your network and exploit them.

One of the most common uses for vulnerability assessments is their capability to validate security measures

Vulnerability assessment (2)

- The tasks of vulnerability assessment are the following:
  - Identification, quantification and ranking of vulnerabilities found in network infrastructure, software and hardware systems, and applications.
  - Explaining the consequences of a hypothetical scenario of the discovered security ‘holes’.
  - Developing a strategy to tackle the discovered threats.
  - Providing recommendations to improve a company’s security posture and help eliminate security risks.

Vulnerability Assessments and Penetration Testing(1)

Vulnerability assessment and penetration testing (or pen test) are complementary techniques.

A vulnerability assessment only identifies the potential vulnerabilities whereas a pen test tries to gain access to the network.

Vulnerability assessment and pen testing are not the equivalents to each other.

Vulnerability assessment focuses on uncovering security weaknesses, pen test means trying to get inside the network as deep as possible (“the depth over breadth approach”).

Vulnerability Assessments and Penetration Testing(2)

- A pen test is usually a better indication of the weaknesses of the network or systems but is more invasive and therefore has more potential to cause disruption to network service.

- Network vulnerability assessment is usually followed by pen testing. There's no use in conducting pen testing before the discovered vulnerabilities are patched.

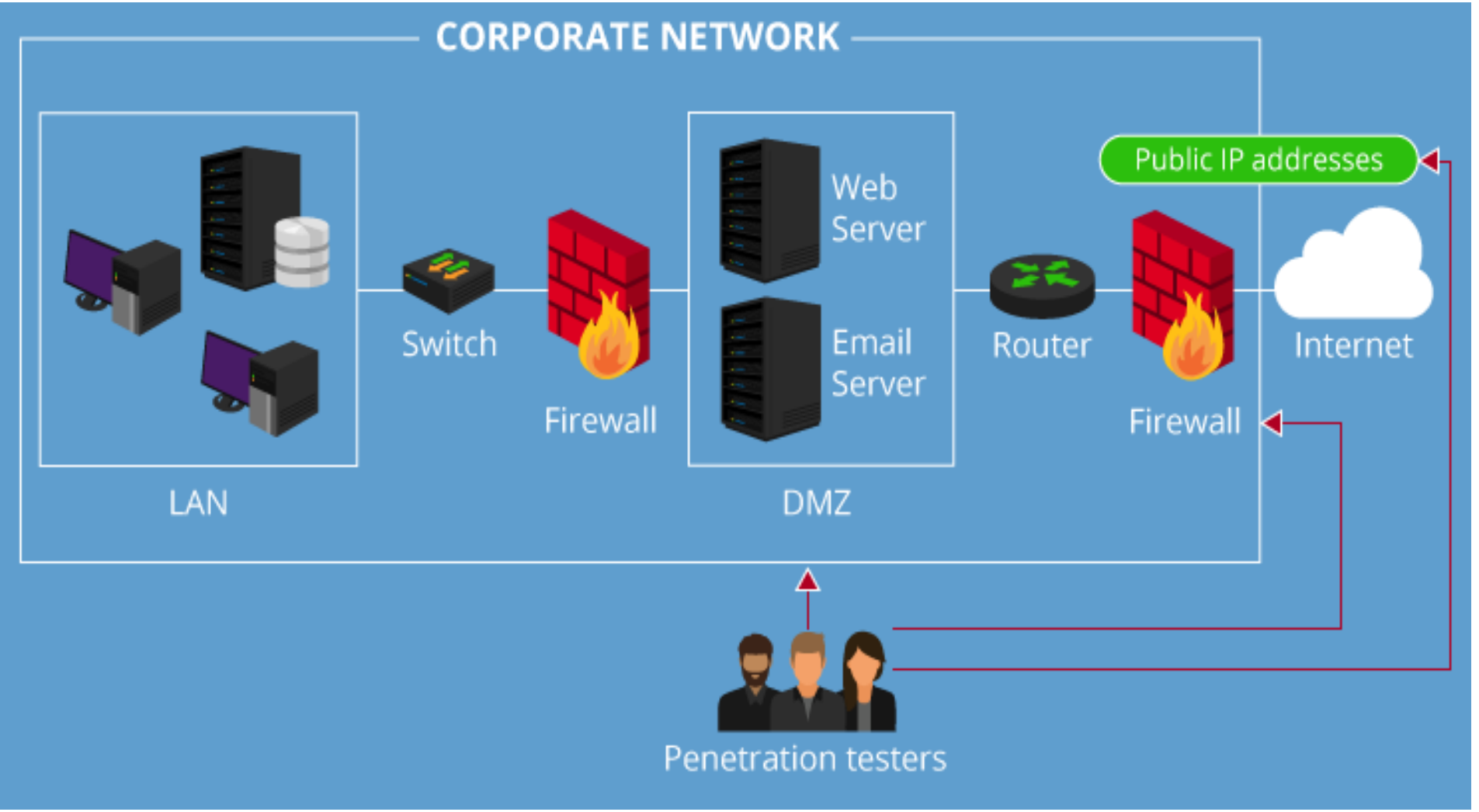
- Keep in mind that the only difference between true "hacking" and pen testing is permission. For this reason pen testing is called ethical hacking. It is critical that a person performing a pen test get written consent to perform the testing.

Ways to reveal network vulnerabilities

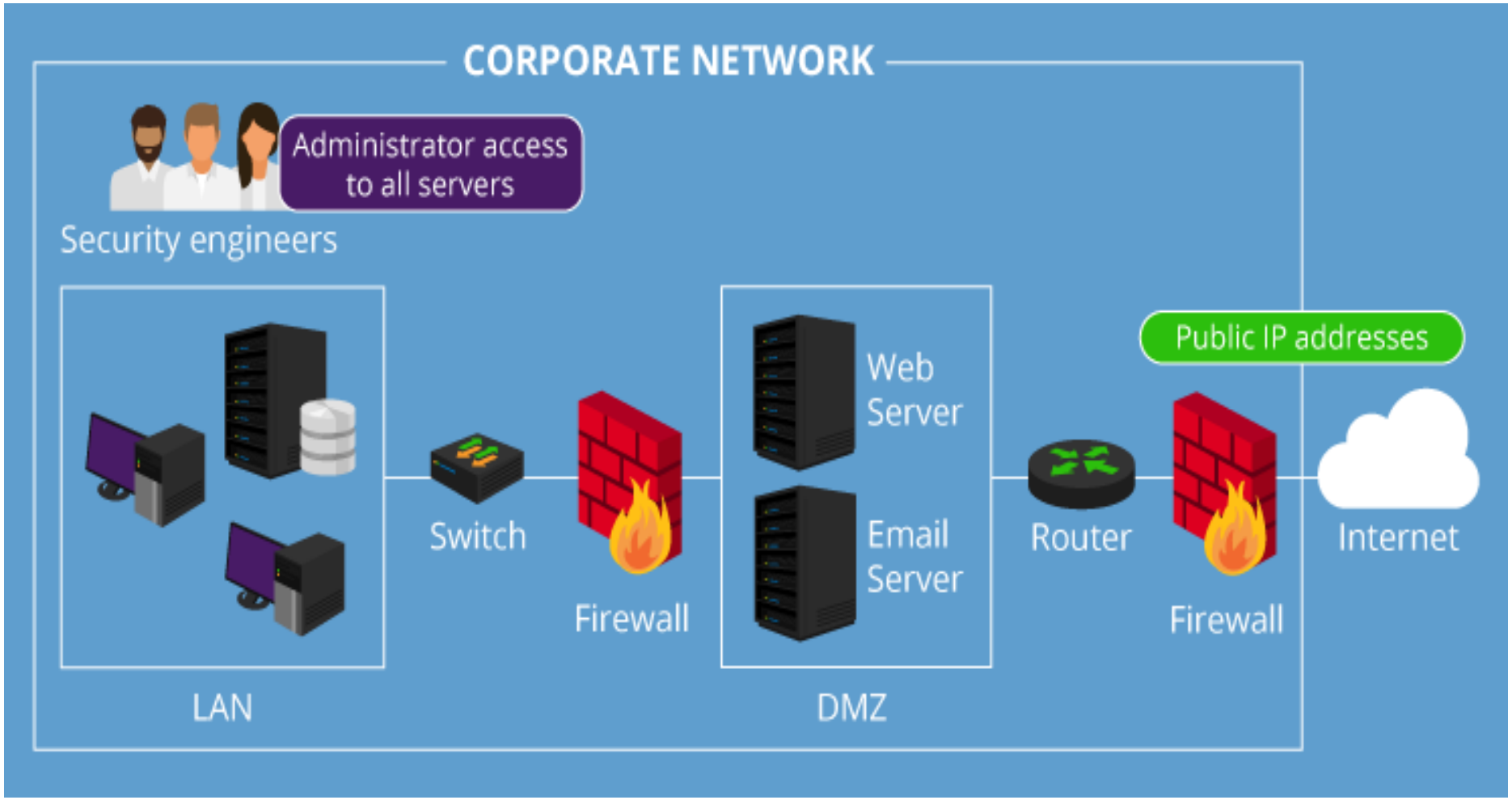
Vulnerability assessment can be conducted according to

- Black box method
- White box method
- Gray box method

Black box method



White box method



A scenario of network vulnerability assessment

- To get a clearer understanding of the vulnerability assessment process, let us consider its stages:
  1. Step 1. Planning and defining the scope
  2. Step 2. Gathering information on the network infrastructure
  3. Step 3. Scanning, detection and assessment of network vulnerabilities
  4. Step 4. Reporting the final results and identifying countermeasures

Understanding the security Testing Methodology(1)

We can use any of the following techniques to conduct ethical hacking. These ethical hacking steps are not always followed in the same order and might involve some iteration:

- Reconnaissance
- Network and Port Scanning
- Policy Scanning
- Vulnerability Probes and Fingerprinting
- Penetration
- Enumeration and Cracking
- Escalation
- Backdoors and Rootkits
- Exfiltration and Abuse

Understanding the security Testing Methodology(2)

In addition to the ethical hacking process, there are many alternatives available for security testers, for example:

- The Open Web Application Security Project method
- The Open Source Security Testing Methodology Manual
- The Penetration Testing Framework.

Intrusion prevention systems (IPS)

- The intrusion prevention system (IPS), is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity.

- Like an IDS, an IPS can be host-based, network-based, It can use anomaly detection or signature detection.

- Once an IDS has detected malicious activity, it can respond by modifying or blocking network packets across a perimeter or into a host.

- Thus, a network IPS can block traffic, as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so.

Host-Based IPS (HIPS)

A host-based IPS (HIPS) can make use of either signature or anomaly detection techniques to identify attacks.

In the signature detection, the focus is on the specific content of application, or of sequences of system calls, that have been identified as malicious.

In the anomaly detection, the IPS is looking for behavior patterns that indicate malware, such as:

- Modification of system resources
- Privilege-escalation exploits
- Buffer-overflow exploits
- Access to e-mail contact list
- Directory traversal

Sandbox HIPS

HIPS can use a sandbox approach.

Sandboxes are especially suited to mobile code, such as Java applets and scripting languages.

The HIPS quarantines such code in an isolated system area, then runs the code and monitors its behavior. If the code violates predefined policies or matches predefined behavior signatures, it is halted and prevented from executing in the normal system environment

Network-Based IPS (NIPS) (1)

A network-based IPS (NIPS) is in essence an inline NIDS with the authority to modify or discard packets and tear down TCP connections.

NIPS makes use of techniques such as signature detection and anomaly detection.

Network-Based IPS (2)

To identify malicious packets, NIPS can use:

- Pattern matching: Scans incoming packets for specific byte sequences (the signature) stored in a database of known attacks.
- Stateful matching: Scans for attack signatures in the context of a traffic stream rather than individual packets.
- Protocol anomaly: Looks for deviation from standards set forth in RFCs.
- Traffic anomaly: Watches for unusual traffic activities, such as a flood of UDP packets or a new service appearing on the network.
- Statistical anomaly: Develops baselines of normal traffic activity and throughput, and alerts on deviations from those baselines.

Honeypots

- Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.
- Honeypots are designed to:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond

These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access. Thus, any access to the honeypot is suspect.

The system is instrumented with sensitive monitors and event loggers that detect these accesses and collect information about the attacker's activities.

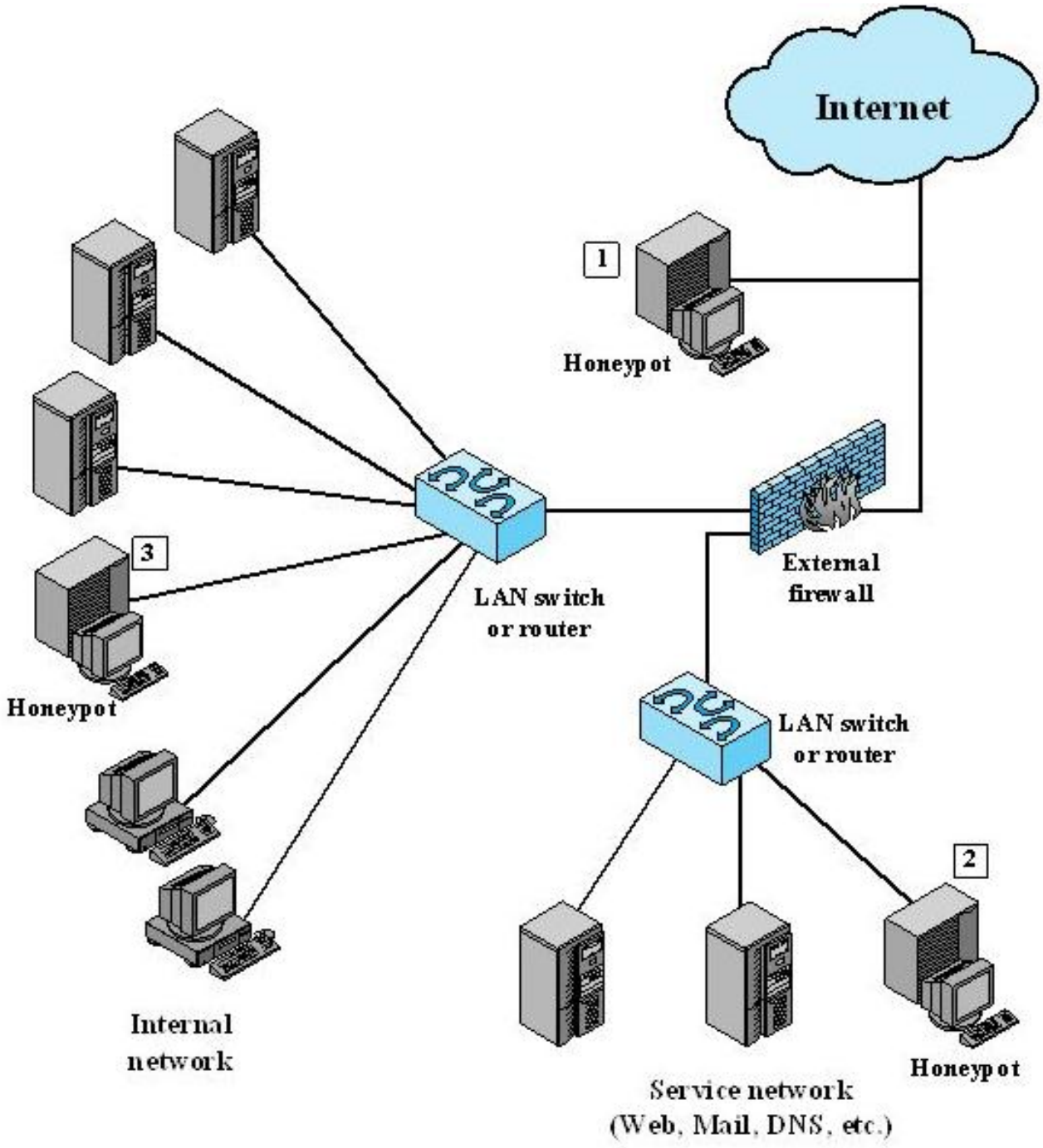
Honeypot locations

The location depends on a number of factors, such as the type of information the organization is interested in gathering and the level of risk that organizations can tolerate to obtain the maximum amount of data.

Location 1: A honeypot outside the external firewall is useful for tracking attempts to connect to unused IP addresses within the scope of the network.

Location 2: The DMZ (demilitarized zone), is another candidate for locating a honeypot.

Location 3: A fully internal honeypot has several advantages. Its most important advantage is that it can catch internal attacks. A honeypot at this location can also detect a misconfigured firewall that forwards impermissible traffic from the Internet to the internal network


Internet
1
Honeypot
External
firewall
LAN switch
or router
3
Honeypot
LAN switch
or router
2
Internal
network
Service network
(Web, Mail, DNS, etc.)
Honeypot