

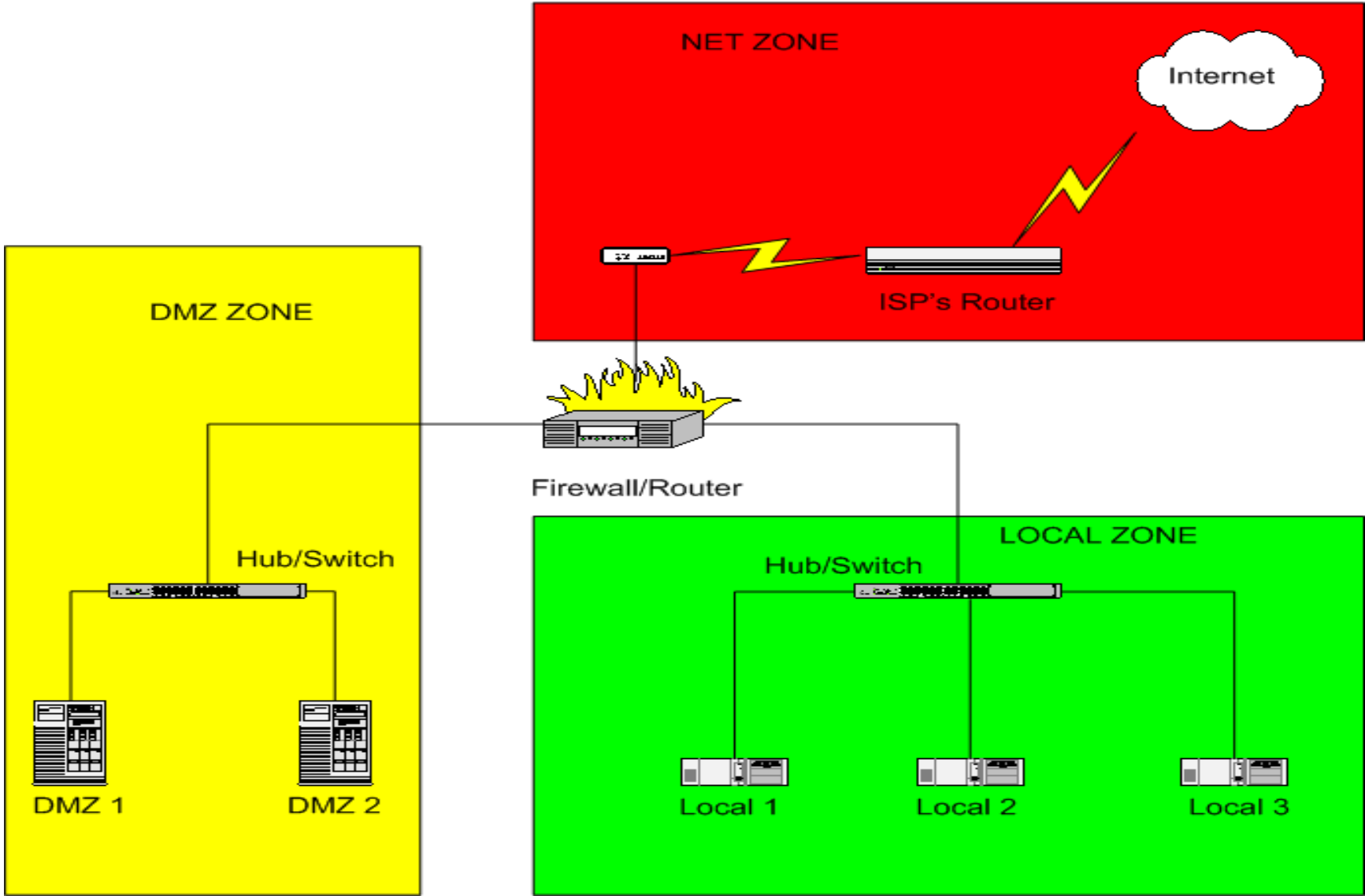
Computer Security

- By Indra Tobing
- @ STMIK Putera Batam

Computer Security

- Security Testing Techniques
 - (Picture: Typical Network with Firewall)
 1. Network / Port Scanning
 2. Vulnerability Scanning
 3. Log Reviews
 4. Anti Virus Detectors

Typical Network with Firewall



Network/Port Scanning

A **port scanner** is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to compromise it.

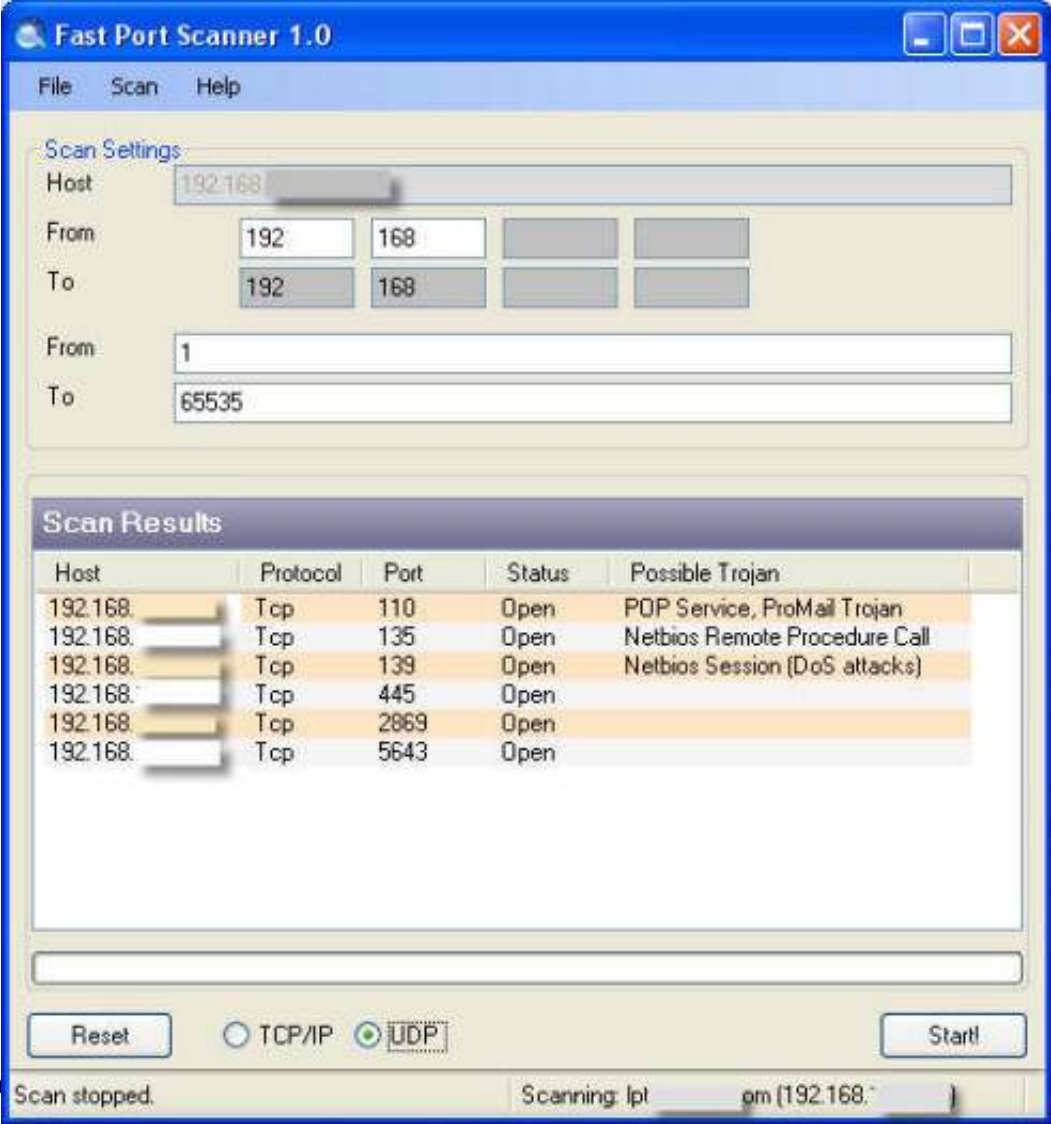
Network/Port Scanning (cont.)

1. Identify active hosts in the address range specified by the user using Transport Control Protocol/Internet Protocol (TCP/IP) Internet Control Message Protocol (ICMP) .
2. Scanned identified active hosts for open (available) TCP and User Datagram Protocol (UDP) ports.
3. Identify the network services operating on that port of the host by sending a message to each port. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

Network/Port Scanning (cont.)

[Features]

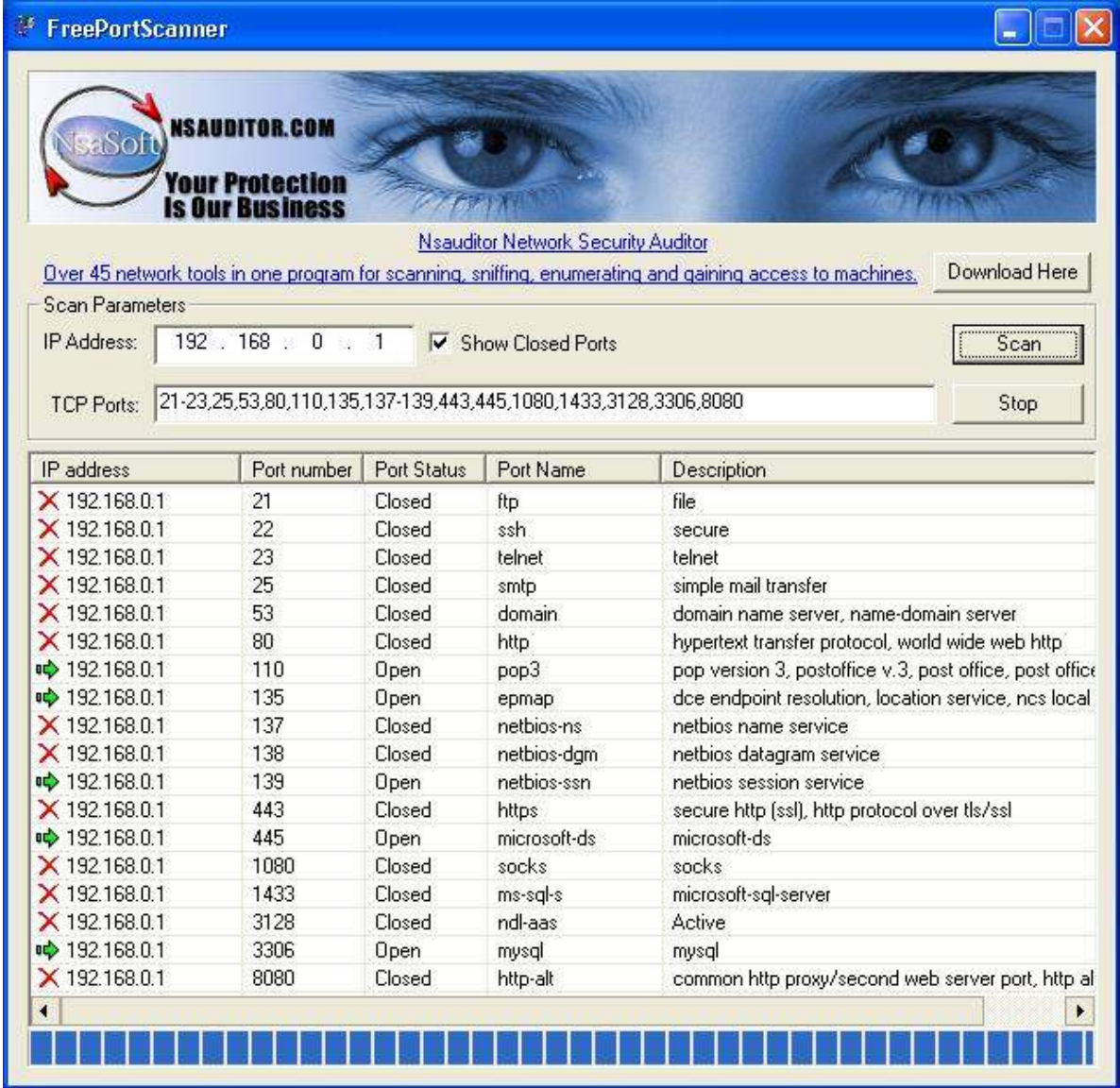
- 1. Able to find open ports of a host on a network.
- 2. Able to identify services provides on each open/available ports.



Network/Port Scanning (cont.)

[Features]

- 1. Able to identify the operating system of the host.
- 2. Able to identify the application available on the host.



Network/Port Scanning (cont.)

Supported Protocols

TCP/IP (Transmission Control Protocol) is a connection-oriented protocol between two computers, built on top of Internet Protocol (IP) and is nearly always seen in the combination TCP/IP (TCP over IP). It adds reliable communication and flow-control and provides full-duplex, process-to-process connections. It is used for normal internet applications such as web servers, FTP servers, etc.

UDP (User Datagram Protocol) is a protocol based on connectionless datagram service that offers best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams. UDP is ideal for things like Video Streams and Multi-Player Gaming, where a few lost and disordered packets are not a big deal, and where speed is very important.

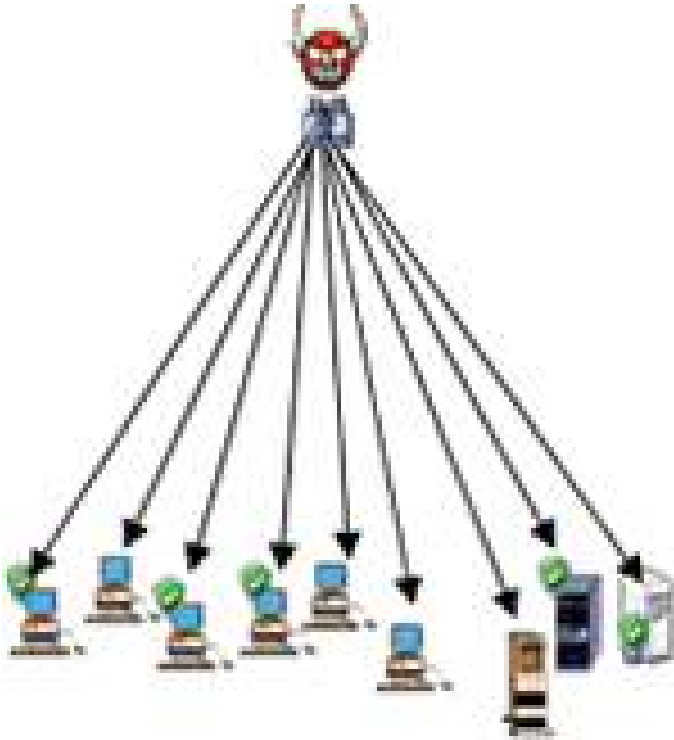
Network/Port Scanning (cont.)

[Weaknesses]

- Port Scanning do NOT identify vulnerabilities (beyond some common Trojan ports).
- Vulnerabilities can only be identified by a human who interprets the mapping and scanning results.
- From these results, a qualified individual can ascertain what services are vulnerable and the presence of Trojans. Although the scanning process itself is highly automated, the interpretation of scanned data is not.
- The scanning can also disrupt network operations by consuming bandwidth and slowing network response times.

Network/Port Scanning

[performed by attacker]



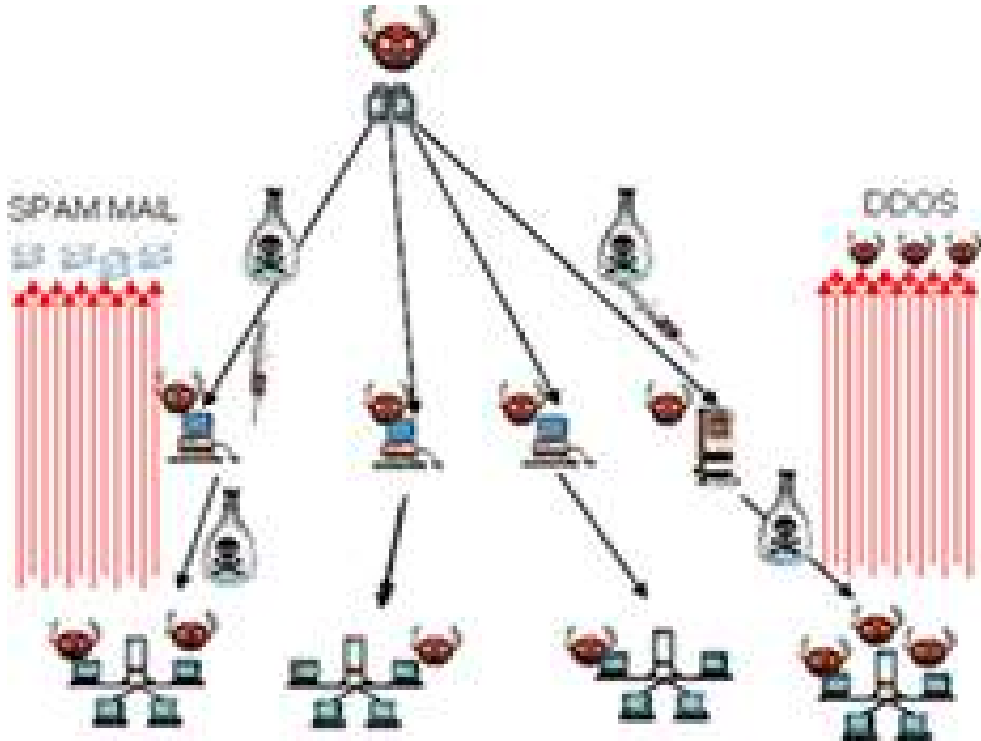
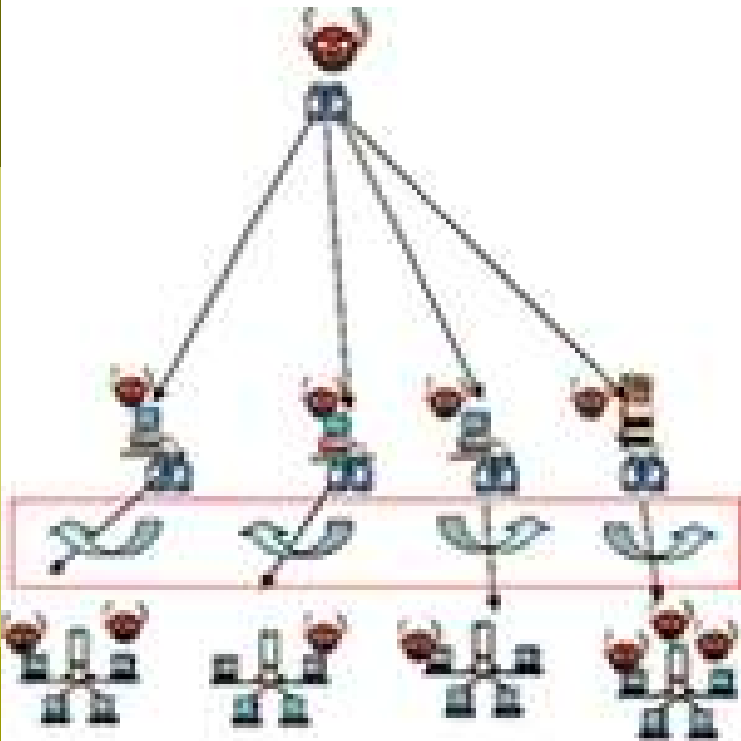
Step 1. Hacker performs Port Scanning techniques to find targets with vulnerabilities



Step 2. Hacker can inject virus, trojan to targets with vulnerabilities found

Network/Port Scanning

[performed by attacker] (cont.)



Step 3. The infected machines further SCAN and INFECT for vulnerable hosts within INTERNAL network

Step 4. The hacker can issue commands to hosts with virus/trojan installed to perform further attacks. e.g. Sending of SPAM MAIL or DDOS attacks

Vulnerability Scanning

A **vulnerability scanner** is a **computer program** designed to search for and map systems for weaknesses of a host, in a network.

The steps:

1. Look for an active host or active IP addresses.
2. Locate open ports.
3. Look at the OSes and any applications running.
4. Create a report or move to the next step.
5. Try to determine the patch level of the OS or applications (In this process the scanner can cause an exploit of the vulnerability such as crash the OS or application).
6. Attempt to exploit the vulnerability.

Note:

- The Scanners may either be malicious or friendly.
- The Friendly scanners usually stop at step 2 and occasionally step 3 but never go to step

Vulnerability Scanning

[also...]

- Provides information on the associated vulnerabilities (not just relying on human interpretation of the results).
- Attempt to provide information on mitigating discovered vulnerabilities.
- Provide proactive tools that can be used to identify vulnerabilities before an adversary can find them.
- A relatively fast and easy way to quantify an organization's exposure to surface vulnerabilities.
- Identify operating systems and major software applications running on hosts and match them with known exposures.
- Identify out-of-date software versions, applicable patches or system upgrades, and validate compliance with, or deviations from, the organization's security policy.
- Employ large databases of vulnerabilities to identify flaws associated with commonly used operating systems and applications.

Vulnerability Scanning

[**simply...**]

1. Identify active hosts on network.
2. Identify active and vulnerable services (ports) on hosts.
3. Identify applications and banner grabbing.
4. Identify operating systems.
5. Identify vulnerabilities associated with discovered operating systems and applications.
6. Identify misconfigured settings.
7. Test compliance with host application usage/security policies.
8. Establish a foundation for penetration testing.

Vulnerability Scanning

[weaknesses]

1. Identify only surface vulnerabilities and are unable to address the overall risk level of a scanned network.
2. Although the scan process itself is highly automated, the scanners can have a high false positive error rate (reporting vulnerabilities when none exist). This means an individual with expertise in networking and operating system security and in administration must interpret the results.
3. Generate significantly more network traffic than port scanners. This may have a negative impact on the hosts or network being scanned or network segments through which scanning traffic is traversing.

Vulnerability Scanning

[weaknesses] (cont.)

1. Tests for denial of service (DoS) attacks that, in the hands of an inexperienced tester, can have a considerable negative impact on scanned hosts.
2. Relies on constant updating of the vulnerability database in order to recognize the latest vulnerabilities. Before running any scanner, the latest updates should be installed to its vulnerability database.
3. Vulnerability scanners are better at detecting well-known vulnerabilities than the more esoteric ones, primarily because it is difficult to incorporate all known vulnerabilities in a timely manner.
4. More vulnerabilities detected requires more tests which slows the overall scanning process.

Log Reviews

Various system logs that are collecting audit data on systems and Networks, such as;

- firewall logs,
- IDS logs,
- server logs,
- and any other logs,

Can;

- be used to identify deviations from the organization's security policy.
- provide a dynamic picture of ongoing system activities that can be compared with the intent and content of the security policy.

Essentially, audit logs can be used to validate that the system is operating according to policies.

Log Reviews

[Example]

If an IDS sensor is placed behind the firewall (within the enclave), its logs can be used to examine the service requests and communications that are allowed into the network by the firewall. If this sensor registers unauthorized activities beyond the firewall, it indicates that the firewall is no longer configured securely and a backdoor exists on the network.

Log Reviews (cont.)

The following actions can be taken if a system is not configured according to policies:

- Remove vulnerable services if they are not needed.
- Reconfigure the system as required to reduce the chance of compromise.
- Change firewall policy to limit access to the vulnerable system or service.
- Change firewall policy to limit accesses from the IP subnet that is the source of compromise.

Anti Virus Detectors

All organizations are at risk of engaging computer viruses, Trojans and worms if they;

- connect to the Internet,
- use removable media (e.g., floppy disks and CD-ROMs),
- use shareware/freeware software.

The impact of a virus, Trojan, or worm can be:

as harmless as a pop-up message on a computer screen, or as destructive as deleting all the files on a hard drive.

With any malicious code, there is also the risk of exposing or destroying sensitive or confidential information.

Anti Virus Detectors (cont.)

There are two primary types of anti-virus programs available;

- those that are installed on the network infrastructure, and
- those that are installed on end-user machines.

Each has advantages and disadvantages, but the use of both types of programs is generally required for the highest level of security.

Anti Virus Detectors (cont.)

The virus detector installed on the network infrastructure

This is usually installed on mail servers or in conjunction with firewalls at the network border of an organization. Server based virus detection programs can detect viruses before they enter the network or before users download their e-mail. Another advantage of server based virus detection is that all virus detectors require frequent updating to remain effective. This is much easier to accomplish on the server-based programs due to their limited number relative to client hosts.

Anti Virus Detectors (cont.)

The virus detector installed on end-user machines

This software detects malicious code in e-mails, floppies, hard disks, documents and the like but only for the local host. The software also sometimes detects malicious code from web sites. This type of virus detection program has less impact on network performance but generally relies on end-users to update their signatures, a practice that is not always reliable. Most anti-virus software is now able to automatically update the list of virus signatures.

Anti Virus Detectors (cont.)

Security Testing Techniques

The following preliminary steps are recommended to minimize the chances of a major virus infection.

- + Virus definition files should be updated at least weekly and whenever a major outbreak of a new virus occurs.
- + The anti-virus software should be configured to run continuously in the background and use heuristics, if available to look for viruses.
- + After the virus definition files are updated, a full system scan should be performed.