Ethical Hacking

Session 3

Network Scanning

Learning Objective 1-2

1. Describe the methodology of scanning
2. Explain and distinguish between different types of scanning
3. Describe the functions of different scanning tools
4. Explain network scanning techniques
5. Explain OS fingerprinting

Learning Objective 2-2

6. Explain banner grabbing
7. Explain vulnerability scanning
8. Explain the spoofing of IP addresses
9. Describe Scanning Pen Testing
10. Explain Scanning countermeasures

Network Scanning 1-6

- An intruder passes through five stages while progressing through a hacking attack as shown in the following figure.

Network Scanning 2-6

Reconnaissance:

- The first phase in the network scanning.
- Attacker collaborates maximum information regarding a target that would be attacked.
- Examples:
  - Dumpster diving
  - social engineering
  - network sniffing

Network Scanning 3-6

Scanning:

- The second stage in the network is scanning process.
- Considered as a logical extension of the first phase, Reconnaissance.
- The primary aim: Is to locate systems that are alive or active on the network.
- Hackers:
  - Continue to gather information about the target systems in the scanning process.
  - Gather the IP addresses of systems that are active on the network.

Network Scanning 4-6

Gaining access:

- A third phase where actual attacks are performed against the targets that are identified in the scanning and enumeration stage.
- The attacker uses tools for known vulnerabilities that were identified in the previous phases.
- In the maintaining access phase, the hacker tries to create backdoors or accesses pathways and have a way back into the system.

Network Scanning 5-6

Maintaining Access:

- The hacker tries to create backdoors or accesses pathways and have a way back into the system.
- It also performs steps to ensure that they can come back at a later date or time and access the breached resource(s).

Network Scanning 6-6

Covering Tracks:

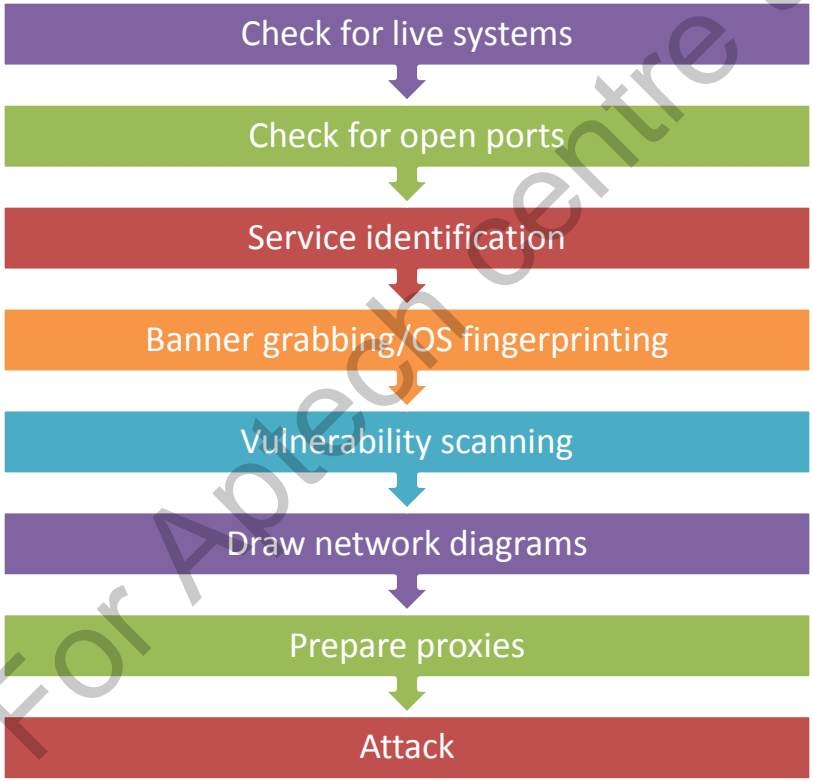
- The final stage in the network scanning.
- Hackers:
  - Have been able to gain and maintain access
  - Cover their tracks to avoid detection by security personnel to:
    - Continue to use the owned system
    - Remove evidence of hacking
    - Avoid legal action

Scanning Methodology 1-2

- The complex nature of scanning forces hackers to adopt a methodical approach so that:
  - No system or vulnerability is overlooked.
  - All necessary information to perform the attack is gathered.

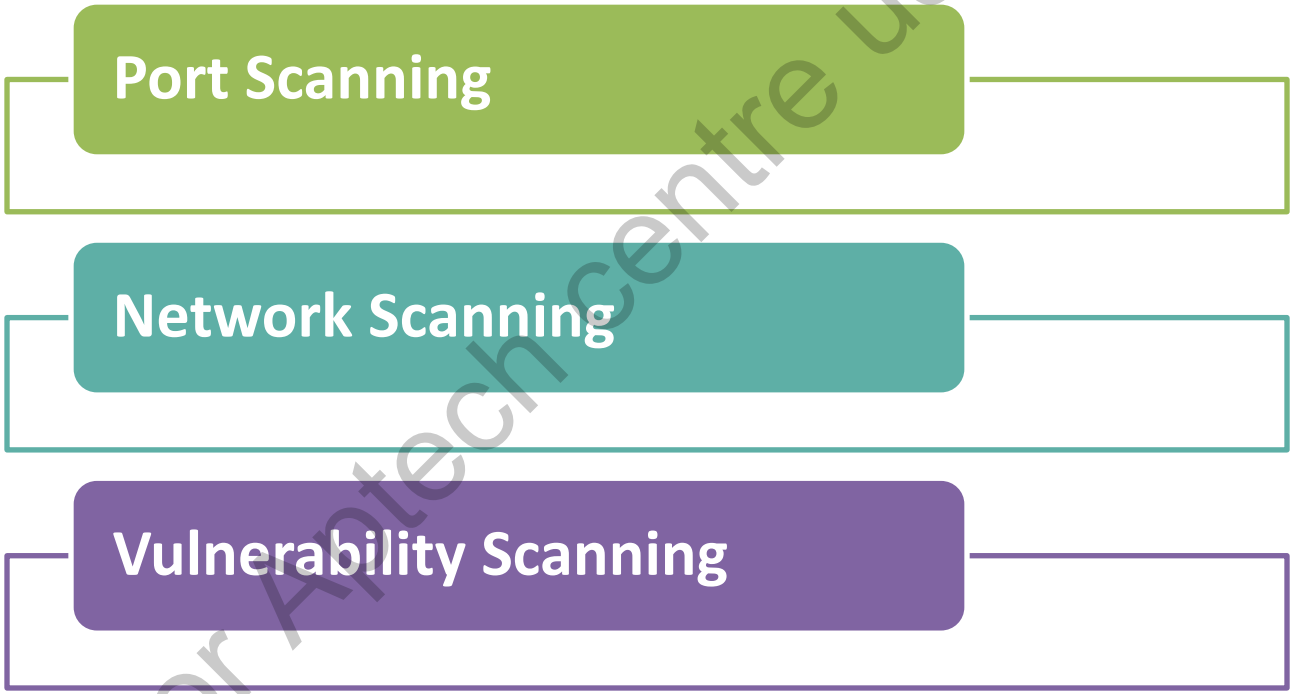
Scanning Methodology 2-2

- Following are various stages in the methodology used to gather information through scanning:



Types of Scanning 1-5

- There are three types of scanning:



Types of Scanning 2-5

Port Scanning

- Detects open TCP/IP ports and services on a system.
- Is a common practice to associate a specific port number with a specific service or application running on the computer.
- For example: On Windows operating system, it is typical to associate port number 80 with HTTP, port 21 with FTP, port 25 with SMTP and port 110 with POP3. Port numbers are usually divided into three ranges:
  - **Well known ports**: 0 to 1023
  - **Registered ports**: 1024 to 49151
  - **Dynamic ports:** 49152 to 65535

Types of Scanning 3-5

Vulnerability Scanning

- Focuses on identifying weaknesses in computer systems in a network.
- Starts by identifying operating systems and their versions, service packs installed and so on.
- Tries to identify vulnerabilities in the operating system with the help of scanner, with the intention of exploiting them later to gain access to the systems.

Types of Scanning 4-5

Network Scanning:

- Reveals IP addresses on a given network or subnet.
- The tools used for network scanning can identify the active hosts on the network or subnet by their IP addresses.

Types of Scanning 5-5

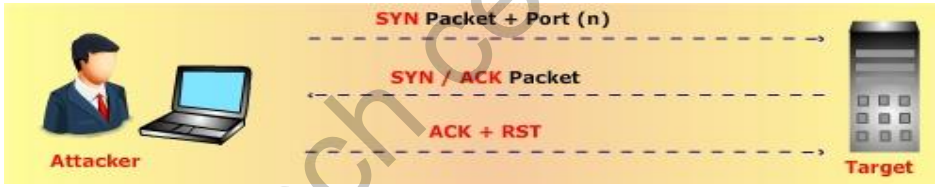
Network Scanning:

Techniques for Network Scanning:

1. TCP Connect/Full Open Scan
2. Stealth Scan (Half-open Scan)
3. Xmas Scan
4. FIN Scan
5. NULL Scan
6. IDLE Scan

Techniques for Network Scanning 1-7

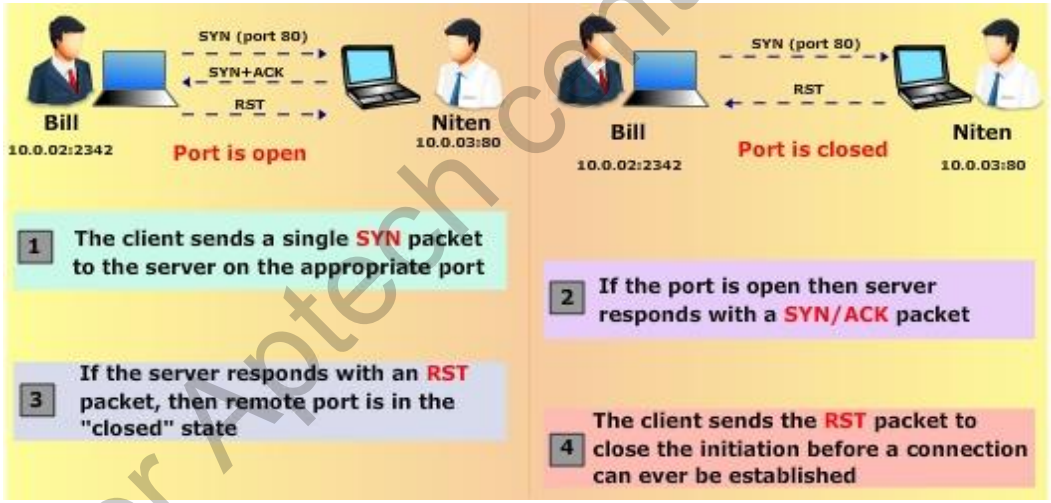
- **A TCP Connect Scan:**
  - It employs a three-way-handshake to detect whether a port is open.
  - A hacker sends a SYN packet to the target port as shown in the following figure. If the port is closed, it responds with a RST/ACK packet.
  - However, if the port is open, it responds with a SYN/ACK packet.



  - Involves establishing a full connection with the port and then, terminating it with a RST packet (reset) before further communication can happen.
  - It is one of the most reliable type of scanning.
  - It is also the most detectable.

Techniques for Network Scanning 2-7

- **Stealth Scan (Half-open Scan):**
  - Attackers use stealth scanning techniques to bypass firewall rules and logging mechanisms by disguising themselves as regular traffic as shown in the following figure:



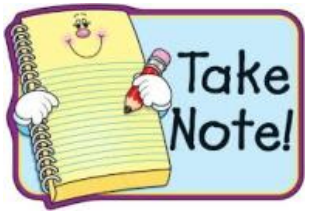
  - It is stealthy because a full TCP connection is not opened.

Techniques for Network Scanning 3-7

- **Stealth Scan (Half-open Scan):**
  - An attacker sends a SYN packet to the port on the target system.
  - A closed port responds with a RST/ACK packet, while an open port responds with a SYN/ACK packet.
  - If the port is open, the hacker immediately sends a RST packet to terminate initiation, before a full connection with the port can be established.

Techniques for Network Scanning 4-7

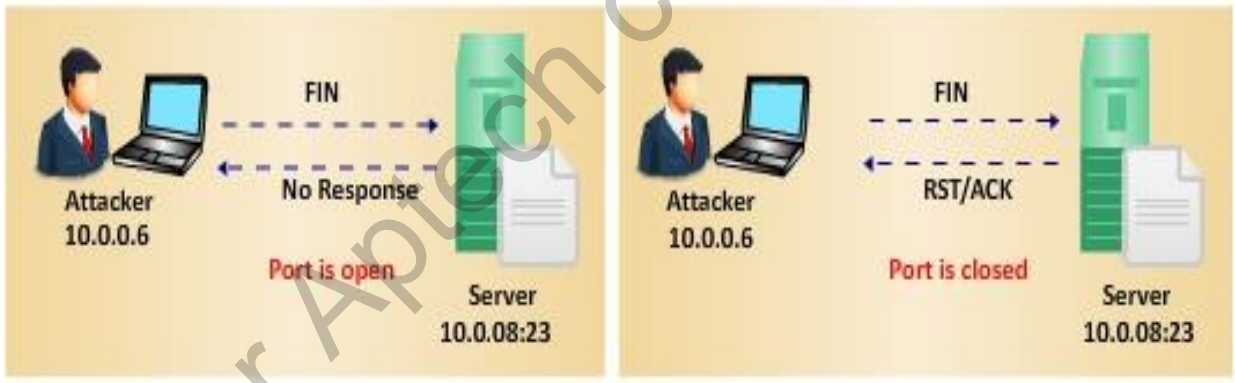
- **Xmas Scan:**
  - In this type of scanning, a hacker checks for TCP services by sending Xmas-tree packets to the target system.
  - The Xmas-tree packet signifies that the URG, ACK, RST and FIN flags are set as shown in the following figure:



This method works only with OS TCP/IP developed according to RFC 793 and does not work with Microsoft Windows.

Techniques for Network Scanning 5-7

- **FIN Scan**:
  - It sends out a TCP frame/packet to the port in the target system with only the FIN flag defined as shown in the following figure.
  - Is limited to OS TCP/IP developed according to RFC 793 and does not work with Microsoft Windows.



Techniques for Network Scanning 6-7

- **NULL scan**:
  - A hacker sends a TCP frame with no flags to the target port as shown in figure 3.28.
  - Limited to OS TCP/IP developed according to RFC 793 and does not work with Microsoft Windows.

Techniques for Network Scanning 7-7

- **IDLE Scan**:
  - Uses a spurious IP addresses.
  - Sends a SYN TCP frame to the target port using a fake IP address.
  - Receives from the target port depending upon the response, the Hacker can determine if the port is open or closed.

Scanning Tools

- Following are network scanning tools:

Global Network Inventory Scanner	Advanced Port Scanner	AQSPS: UDP Scanner	MegaPing
Net Tools Suite Pack	Netifera	AWPTA	Network Inventory Explorer

Nmap 1-5

- **Nmap**:
  - Is an open source utility for network exploration.
  - Performs ping sweeps, port scanning, service identification, IP address detection and operating system detection.
  - Is supported by most operating systems, including Windows, Unix and Linux.
  - Offers the advantage of being able to scan a large number of machines in a single session.
  - Used often by network administrators to carry out network inventory mapping tasks, monitoring host or system uptime and managing service upgrade schedules.

Nmap 2-5

- Nmap can extract the following information for a network hacker, either malicious or ethical:
  - The live (or responsive) hosts on the network
  - Operating systems (and their versions) running on hosts
  - Services running on hosts
  - Type packet, i.e., filters and firewalls
- To start Nmap scan on a Windows machine:
  - A user needs to type the command NmapIPaddress followed by any command switches in Windows command prompt and press Enter.
  - The IP address, in this case, is the address of the host on which to perform the scan.

Nmap 3-5

- Some of the commonly used switches of the Nmap command are:

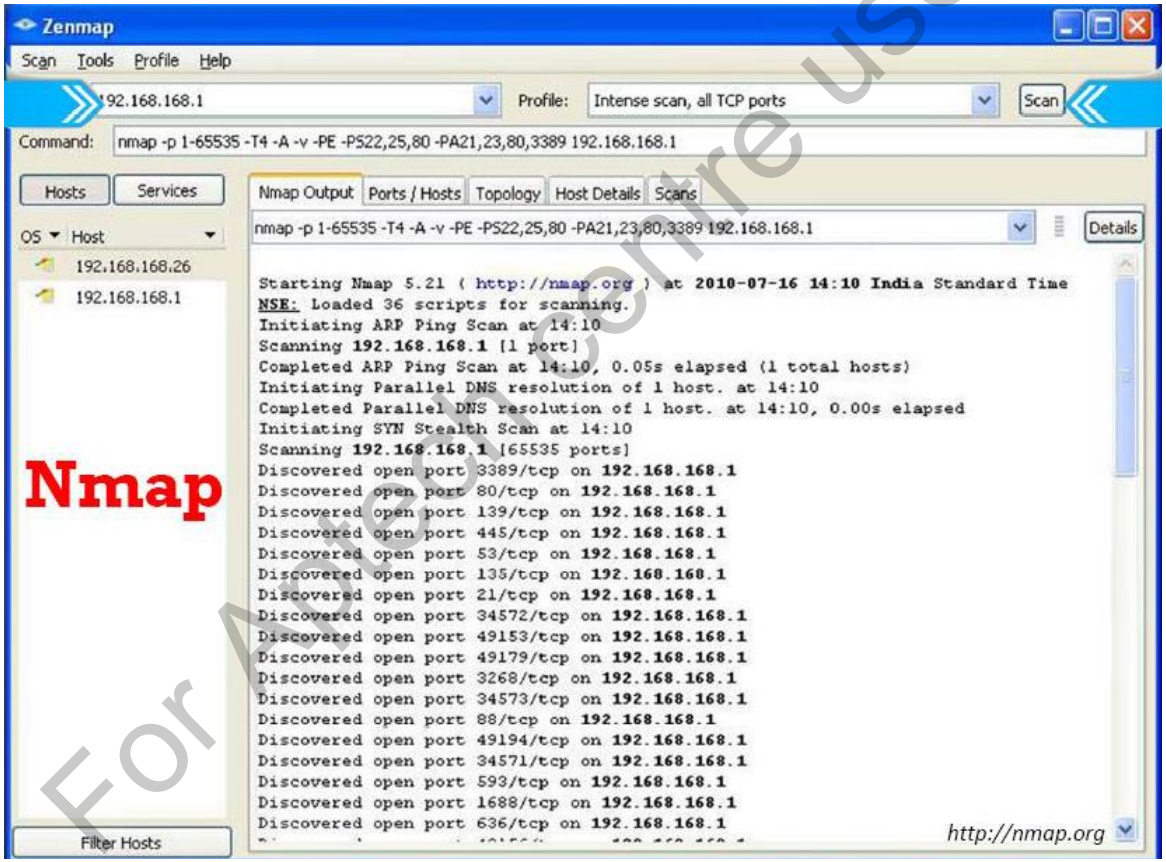
Command Switch	Scan performed
-s0	Protocol Scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan
-sL	List/DNS scan
-sI	Idle scan
-Po	Don’t ping
-PT	TCP ping
-PS	SYN ping

Nmap 4-5

Command Switch	Scan performed
-PI	ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oA	All output
-T Paranoid	Serial scan, 300 sec. between scans
-T Sneaky	Serial scan, 15 sec. between scans
-T Normal	Parallel scan
-T Aggressive	Parallel scan, 300 sec timeout, and 1.25 sec/probe

Nmap 5-5

- Following figure displays Nmap performing network scan.

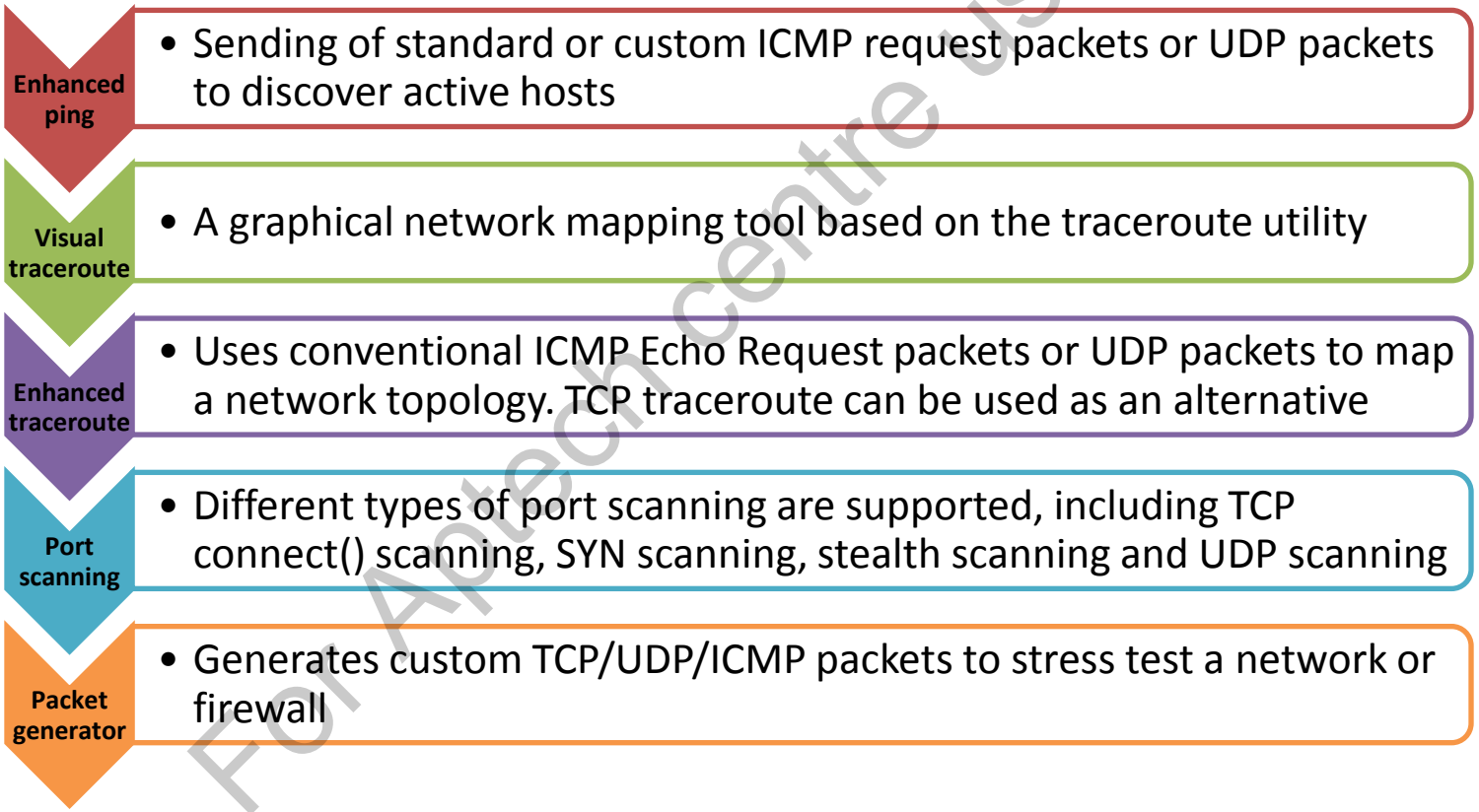


NetScanTools Pro 1-4

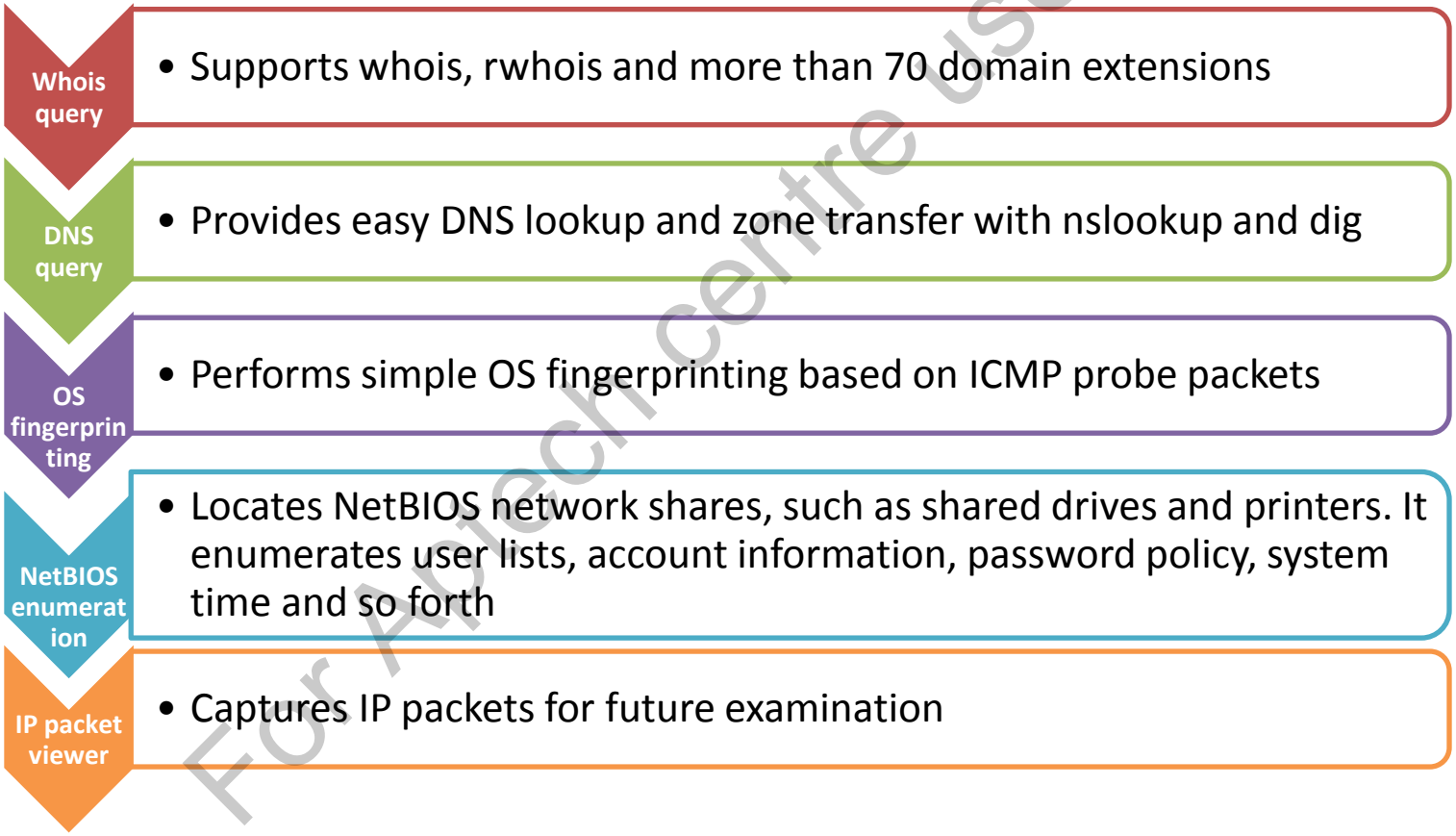
- **NetScanTools Pro**:
  - Is a sophisticated tool for network discovery and information gathering meant for the Microsoft Windows.
  - Integrates over 30 Internet and information gathering tools into a single user interface/visual package.

NetScanTools Pro 2-4

- Features of NetScanTools Pro are:

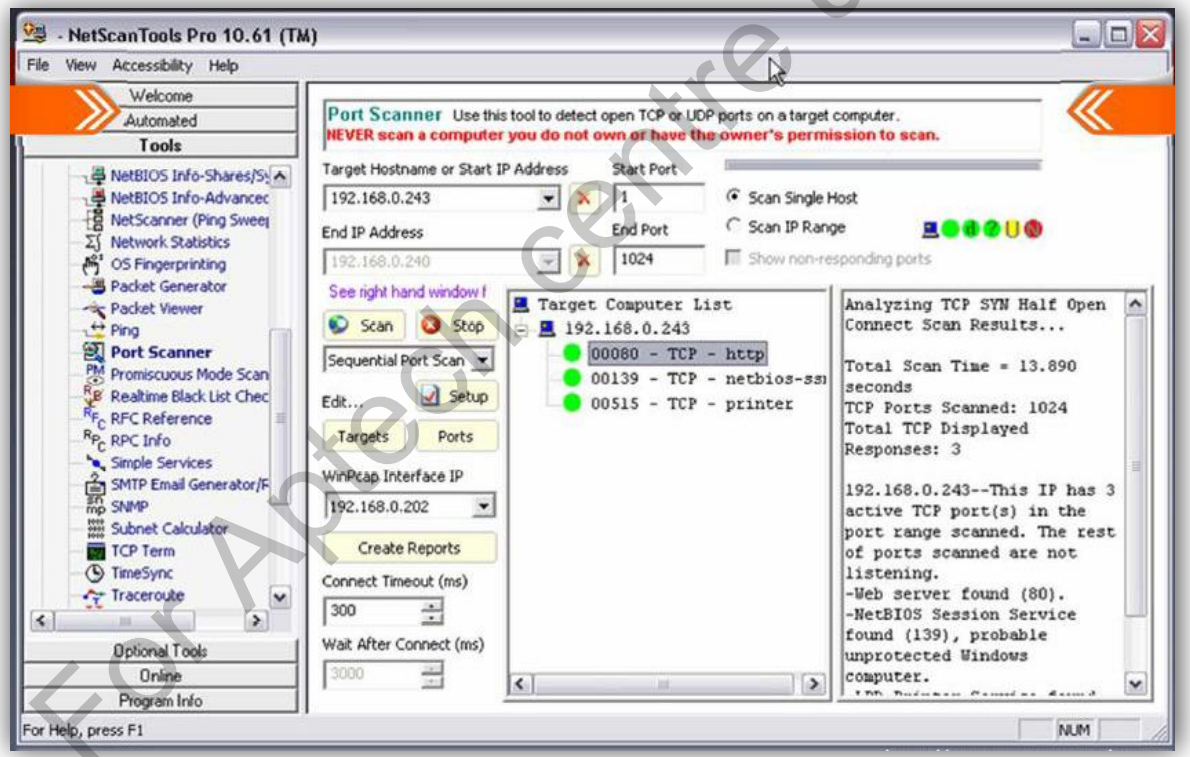


NetScanTools Pro 3-4



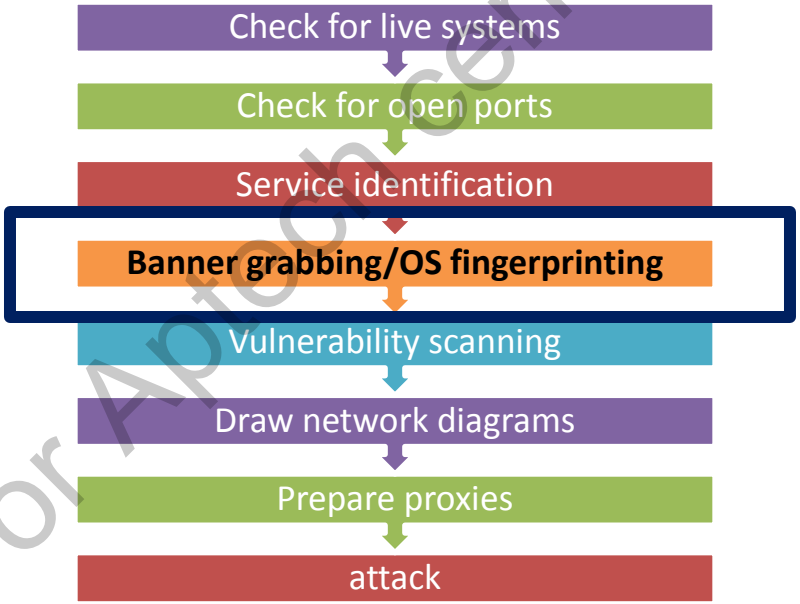
NetScanTools Pro 4-4

- Following figure displays NetScanTools Pro performing network scan:



Banner Grabbing/OS Fingerprinting 1-6

- **OS Fingerprinting**:
  - Is the fourth stage in network scanning methodology as shown in the following figure.
  - Is also known as 'Banner Grabbing.'



Banner Grabbing/OS Fingerprinting 2-6

- **OS Fingerprinting**:
  - Aimed at identifying the operating system running on the target system.
  - Many FTP, e-mail and Web servers respond to a telnet connection with the name and version of the software.
  - Is used by the attacker in fingerprinting the OS and application software.
  - There are two types of OS fingerprinting:

Banner Grabbing/OS Fingerprinting 3-6

- **Active Fingerprinting**:
  - It is also known as 'Active Stack Fingerprinting.'
  - It is based on the fact that different vendors of operating systems implement TCP stacks differently.
  - Their responses to queries and characteristic of the operating systems, they run are different.
  - A hacker can easily find out the operating system (and its version) by simply sending data to the system.
  - The response from the system reveals which operating system it runs.

Banner Grabbing/OS Fingerprinting 4-6

- **Active Fingerprinting**:
  - The general order of incidents involved in a typical active fingerprinting attempt is:
    - Specially crafted packets are sent to a target (remote) system.
    - The response from the OS is noted.
    - The response is then compared to a database in order to determine the OS.
  - It can be detected by the fact that a hacker indulging in active fingerprinting, repeatedly tries to connect to the same target system.

Banner Grabbing/OS Fingerprinting 5-6

- **Passive Fingerprinting**:
  - It differs significantly from Active fingerprinting.
  - It employs sniffing techniques instead of the scanning techniques used in Active fingerprinting.
  - Sniffing techniques involve monitoring and examining network traffic to determine an operating system.
  - It is the stealthier of the two types of fingerprinting since it uses sniffing techniques.
  - IDS and other security measures are usually unable to detect 'Passive Stack Fingerprinting'.
  - It is also less accurate when compared to Active Stack Fingerprinting.

Banner Grabbing/OS Fingerprinting 6-6

- **Passive Fingerprinting**:
  - The generic flow of events in Passive fingerprinting is as follows:
    - Sniffing techniques are used to capture packets flowing from the target system.
    - The captured packets are then analysed for information on the operating system.

Banner Grabbing Tools 1-3

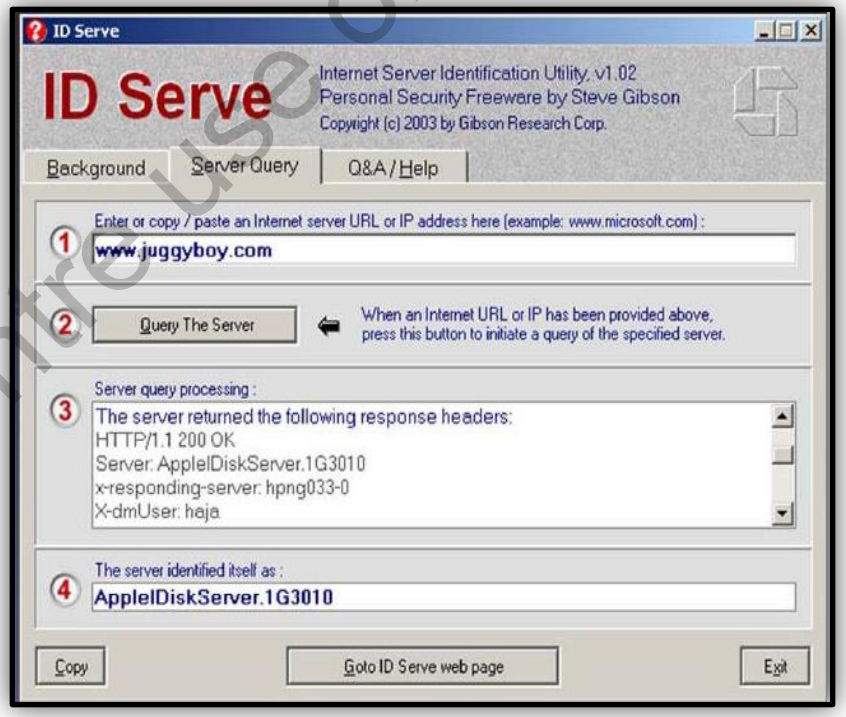
- Some Banner Grabbing tools are:

ID Serve	Netcraft	Serversiders .com	PRADS	PDF Banner Grabbing Tool
SINFP	Network Moner	Xprobe	Satori	THC-AMAP

Banner Grabbing Tools 2-3

ID Serve

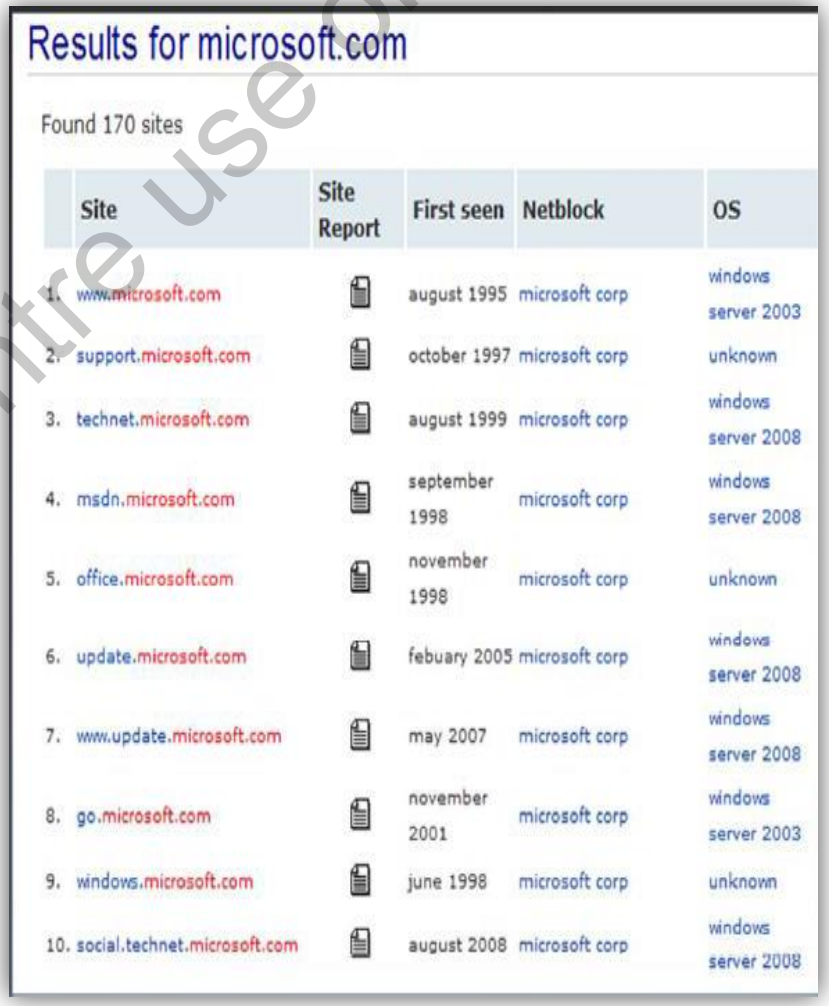
- Can identify the make and version of any Website's server software.
- Can also be used to identify non-Web (non-HTTP) Internet servers such as:
  - FTP servers
  - SMTP servers
  - POP servers
  - NEWS servers



Banner Grabbing Tools 3-3

Netcraft

- Can detect:
  - Website's operating system
  - Web server
  - Netblock owner
- Can report, if available, a graphical view of the time since last reboot for each of the computers serving the Website as shown in figure.



Results for microsoft.com

Found 170 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.microsoft.com		august 1995	microsoft corp	windows server 2003
2.	support.microsoft.com		october 1997	microsoft corp	unknown
3.	technet.microsoft.com		august 1999	microsoft corp	windows server 2008
4.	msdn.microsoft.com		september 1998	microsoft corp	windows server 2008
5.	office.microsoft.com		november 1998	microsoft corp	unknown
6.	update.microsoft.com		febuary 2005	microsoft corp	windows server 2008
7.	www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
8.	go.microsoft.com		november 2001	microsoft corp	windows server 2003
9.	windows.microsoft.com		june 1998	microsoft corp	unknown
10.	social.technet.microsoft.com		august 2008	microsoft corp	windows server 2008

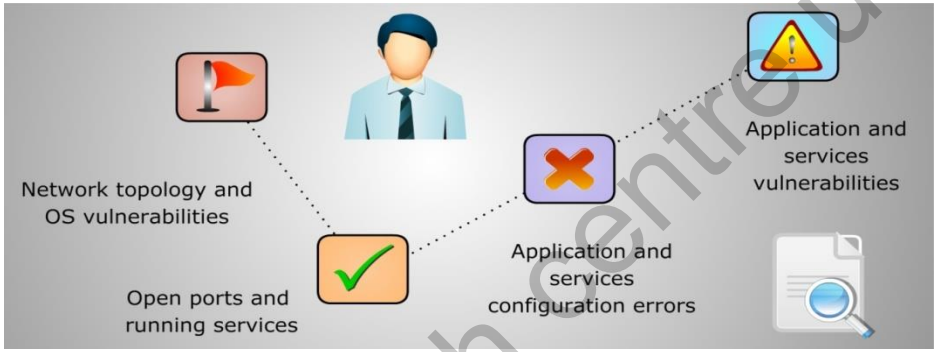
Vulnerability Scanning 1-3

Vulnerability scanning:

- Proactively focuses on identifying weaknesses in computer systems in a network.
- Starts by identifying an operating system and its version, service packs installed and so on.
- Tries to identify vulnerabilities in the operating system to gain access to the systems.

Vulnerability Scanning 2-3

- The following figure displays the vulnerability scanning illustration:



- The tools available for performing vulnerability scanning provide:
  - A slew of remedies
  - Data and fixes such as patches
  - Configuration
  - Compliance auditing
  - Malware
  - Botnet discovery
  - Sensitive data identification

Vulnerability Scanning 3-3

- Following are the tools for performing vulnerability scanning:

SAINT	GFI LANguard	Retina	Nsauditor	Core Impact
Network Security Inspector	MBSA	OpenVAS	Shadow Security Scanner	Security Manager Plus

- Security Administrator's Integrated Network Tool (SAINT):
  - Gathers information about the type of operating system running on the target and the ports that are open.
  - Helps attackers to detect the vulnerabilities in a network without being intrusive.

Proxy Servers 1-3

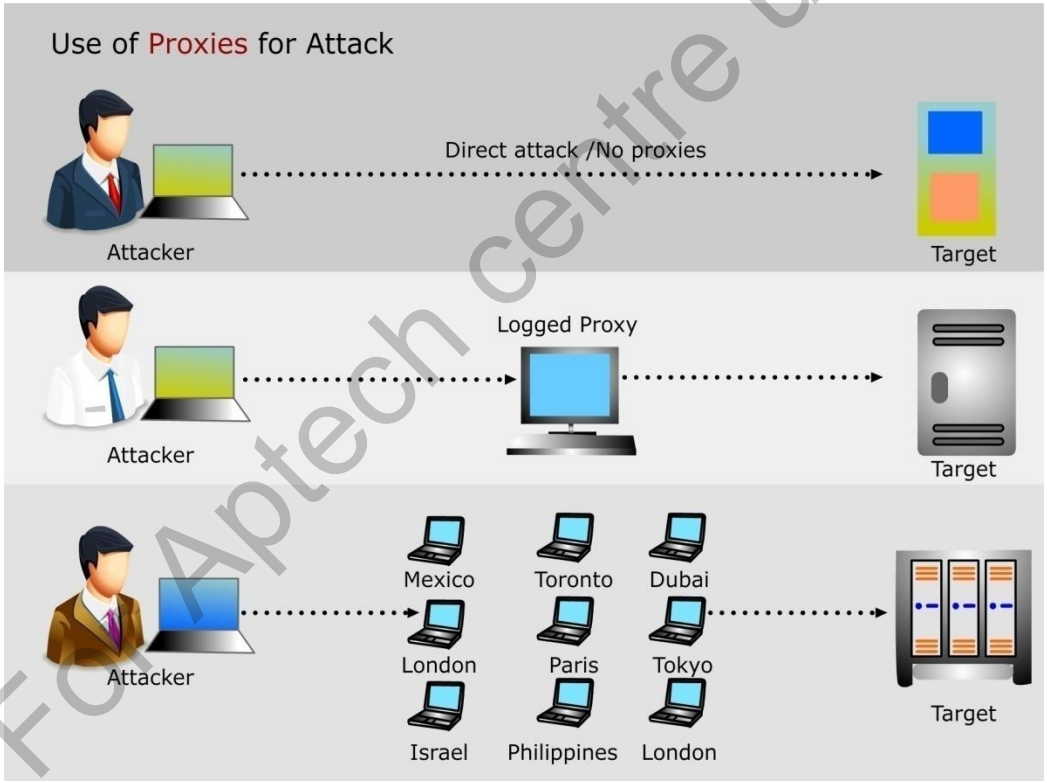
- **Proxy Servers**:
  - Are included in networks to provide structure and encapsulation to distributed and therefore, complex systems.
  - Act as intermediaries between clients looking for resources and servers that store those resources.
  - For example: A client may request a Web page from a proxy server, which then locates the page from the Internet and passes it on to the client.
  - Can be used as a shared Internet connection.

Proxy Servers 2-3

- **Proxy Servers**:
  - Are also good targets for hackers and is also known as proxy hijacking.
  - Provide anonymity to hackers because the logs in a target server record the IP address of the proxy server used by the attacker rather than the attacker's IP address.
  - An attacker supplants an authentic Web page in a search engine's index and search results pages.
  - In this way, the attacker can redirect users/clients to malicious and fraudulent Web sites.

Proxy Servers 3-3

- The following figure shows the relative benefits when a hacker uses a proxy server(s):



Scanning Pen Testing

- **Penetration Testing**:
  - Is performed on systems and networks to identify any weaknesses that might be exploited by hackers to compromise the system or network.
  - Helps system administrators and others responsible for the security of the systems in:
    - Identifying and closing any unused ports.
    - Identifying and disabling any unnecessary services.
    - Hiding or customising banners.
    - Troubleshooting service configuration errors and calibrating firewall rules.

Scanning Countermeasures 1-4

- To protect itself from hacking attacks, an organisation can implement the following countermeasures:

1. Border routers and firewalls should filter all inbound Internet Control Message Protocol (ICMP) message types. This forces attackers to use full-blown TCP port scans against all IP addresses to map a network correctly, but reveal themselves in the process.

2. Border routers and firewalls should filter all outbound ICMP type 3 unreachable messages to prevent UDP port scanning and firewalling from being effective.

Scanning Countermeasures 2-4

3

- Internet firewalls need to be configured such that they can identify port scans and choke connections accordingly. Commercial firewall appliances (such as those from Check Point, NetScreen and WatchGuard) can be configured to prevent fast port scans and SYN floods being launched against an organisation's networks.

4

- While performing scanning and probing exercises, the manner in which network firewall and IDS devices are configured to handle fragmented IP packets should be assessed. Some devices crash or fail under conditions where there is a high volume of fragmented packets in the network traffic.

Scanning Countermeasures 3-4

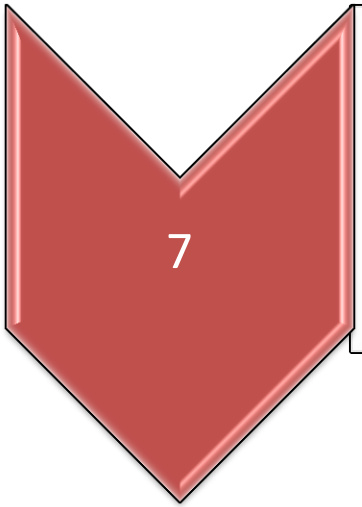
5

- It is important to ensure that the routing and filtering mechanisms (both firewalls and routers) cannot be bypassed by the use of specific source ports or by employing source-routing techniques.

6

- If an organisation's network publicly hosts accessible FTP services, the firewalls need to be configured and strengthened against malformed PORT and PASV commands that can cause stateful circumvention attacks.

Scanning Countermeasures 4-4



If a commercial firewall is in use, the following needs to be ensured:

- The latest service pack is installed.
- The firewall does not accept, at its external interface, packets that have private spoofed-source addresses. However, to ensure this, anti-spoofing rules must be adequately defined.
- Check Point Firewall-1 environments do not use Fastmode services.

Summary 1-2

In this session, you learned that:

- Network scanning is the second phase in the process of hacking a system or network.
- Hackers adopt a methodical approach so that no system or vulnerability is overlooked and that all necessary information to perform the attack is gathered.
- There are three types of scanning:
  - Port scanning
  - Network scanning
  - Vulnerability scanning

Summary 2-2

- There are several tools available for scanning.
- There are various techniques for implementing scans.
- There is slew or countermeasures available for preventing hackers from scanning a system of network.