

Chapter 5

episode 1 +

Scanning and Enumeration

Mohd Zaki Mas'ud

Content

- Scanning
- Checking For live system
- Port Scanning tool
- Port scanning Techniques
- Thwarting Scanning

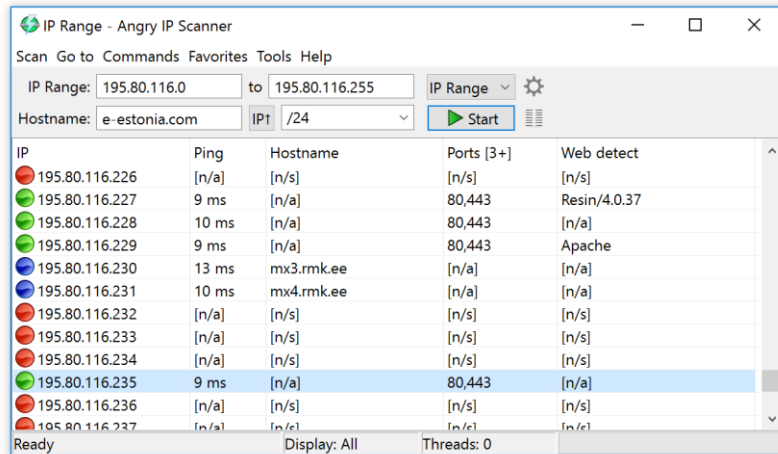
SCANNING

**HOW TO KNOW
A TARGET IS
AVAILABLE TO
BE ATTACK ?**



**IS THERE ANY
LOOP HOLE OR
VULNERABILITY
TO BE
EXPLOITED?**

Scanning answer previous Q



- Can discover more about the target system, such as what **operating system** is used, what **services are running**, and whether or not there are any **configuration lapses in the target system**.
- Types of Scanning
 - Port scanning - Open ports and services
 - Network scanning - IP addresses
 - Vulnerability scanning - Presence of known weaknesses
 - Wardialing

- Scanning is the process used to gather additional details about the target using highly complex and aggressive reconnaissance techniques
- to discover exploitable communication channels, to probe as many listeners as possible, and to keep track of the ones that are responsive or useful for hacking

```
bratchc2ddsktop bratch # nmap -T5 -sV -O localhost

Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07 GMT
Interesting ports on localhost (127.0.0.1):
Not shown: 1709 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
10000/tcp open  http     Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.241 seconds
bratchc2ddsktop bratch #
```

WarDialing



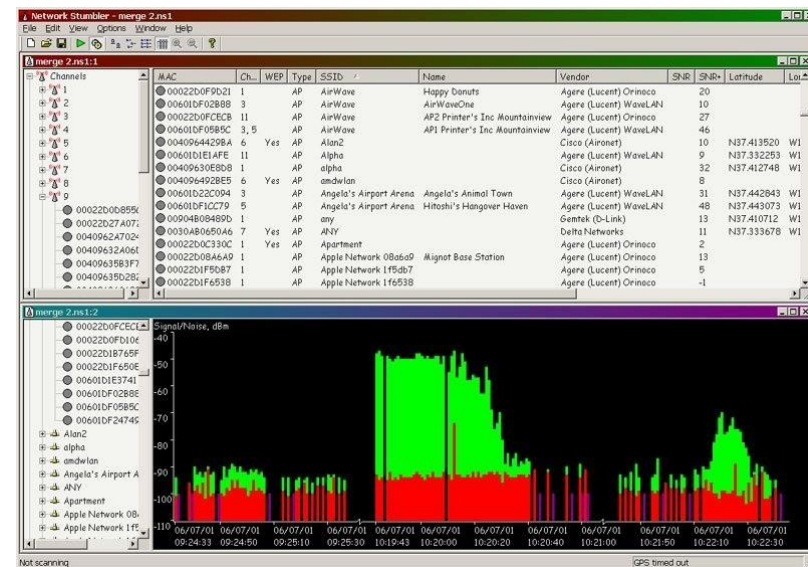
- The first type of scan
- existed in an almost unchanged state since the mid-1980s
- useful information-gathering tool.
- Once you find a modem and get a response, the question becomes what to do with that information.
- To answer that, you need to know what devices modems are commonly attached to in the modern world

- **ToneLoc** A wardialing program that looks for dial tones by randomly dialing numbers or dialing within a range. It can also look for a carrier frequency of a modem or fax. ToneLoc uses an input file that contains the area codes and number ranges you want it to dial.
- **THC-SCAN** A DOS-based program that can use a modem to dial ranges of numbers in search of a carrier frequency from a modem or fax.
- **NIKSUN's PhoneSweep** One of the few commercial options available in the wardialing market.

A number of wardialing programs have been created over the years. Here are three of the best-known ones:

WarDriving

- driving around with a wireless enabled notebook or other device.
- the goal of mapping out access points, usually with the help of a GPS device.
- can locate many access points along with their configurations and physical locations
- Some of the tool associated to this activity



AirSnort A wireless cracking tool.

AirSnare An intrusion detection system that helps you monitor your wireless networks.

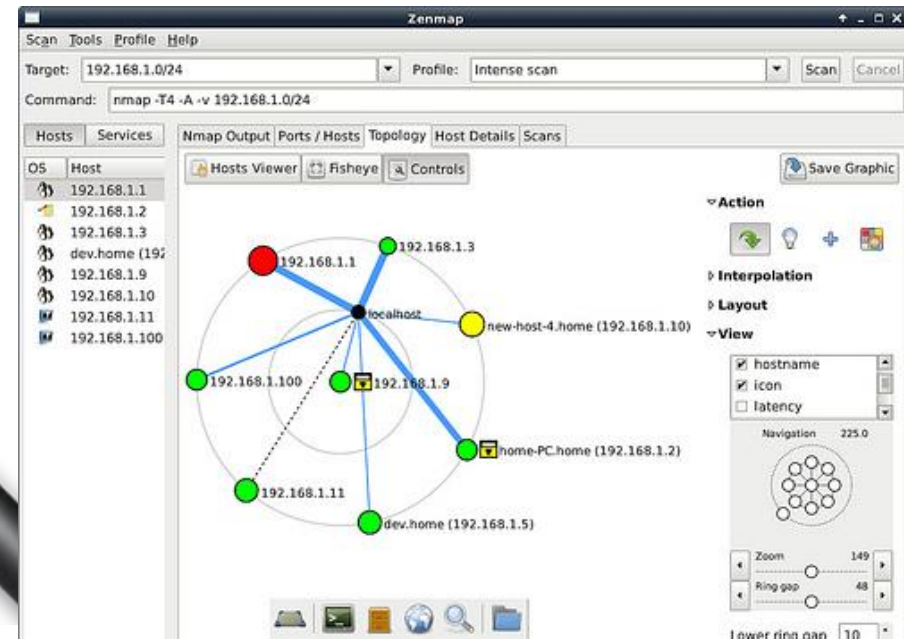
Kismet A wireless network detector, sniffer, and intrusion detection system commonly found on Linux.

NetStumbler A wireless network detector; also available for Mac and for handhelds.

inSSIDer A wireless network detector and mapper of access points.

Network Scanning

- During the network scanning process, you can gather information about specific IP addresses that can be accessed over the Internet, their targets' operating systems, system architecture, and the services running on each computer
- In addition, the attacker also gathers details about the networks and their individual host systems.



- The most common objectives that are encountered during the hacking phase:
 - Discovering live hosts, IP address, and open ports of live hosts running on the network.
 - Discovering open ports:
 - the best means to break into a system or network.
 - Discovering operating systems and system architecture
 - referred to as fingerprinting.
 - attacker will try to launch the attack based on the operating system's vulnerabilities.
 - Identifying the vulnerabilities and threats:
 - the security risks present in any system. You can compromise the system or network by exploiting these vulnerabilities and threats.
 - Detecting the associated network service of each port

CHECKING FOR LIVE SYSTEM (TCP & UDP)

Check for Live Systems

- ICMP
 - Can be gathered by sending ICMP packets to target.



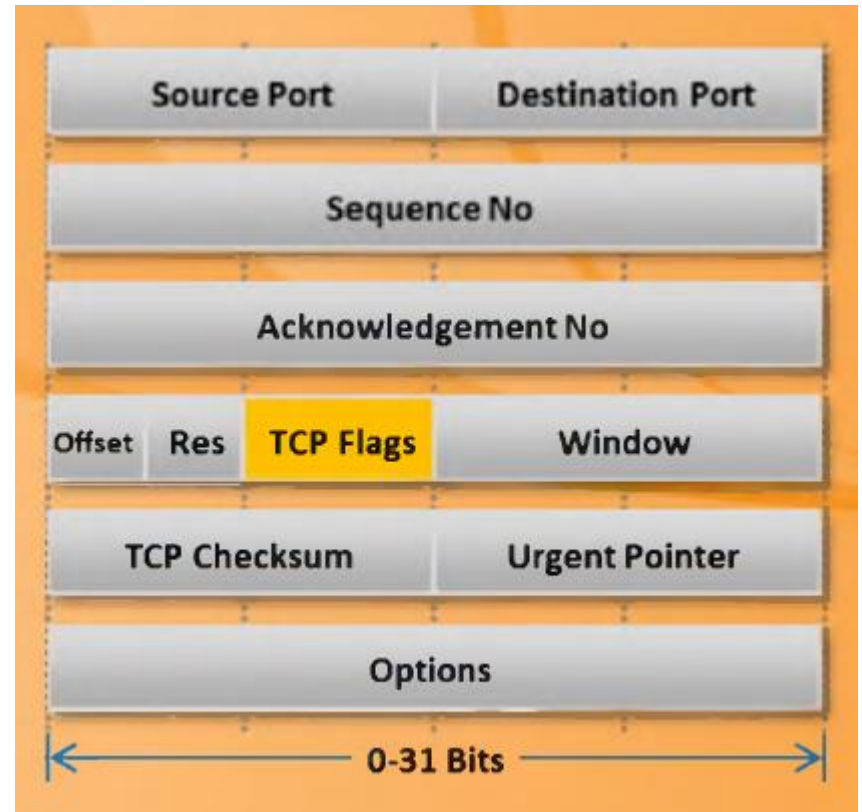
- Ping Scan Output Using Nmap
 - Nmap is a tool that can be used for ping scans, also known as host discovery.
 - can determine the live hosts on a network.
 - It performs ping scans by sending the ICMP ECHO requests to all the hosts on the network.
 - If the host is live, then the host sends an ICMP ECHO reply.
 - This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

- Ping Sweep
 - basic network scanning technique to determine which range of IP addresses map to live hosts (computers)



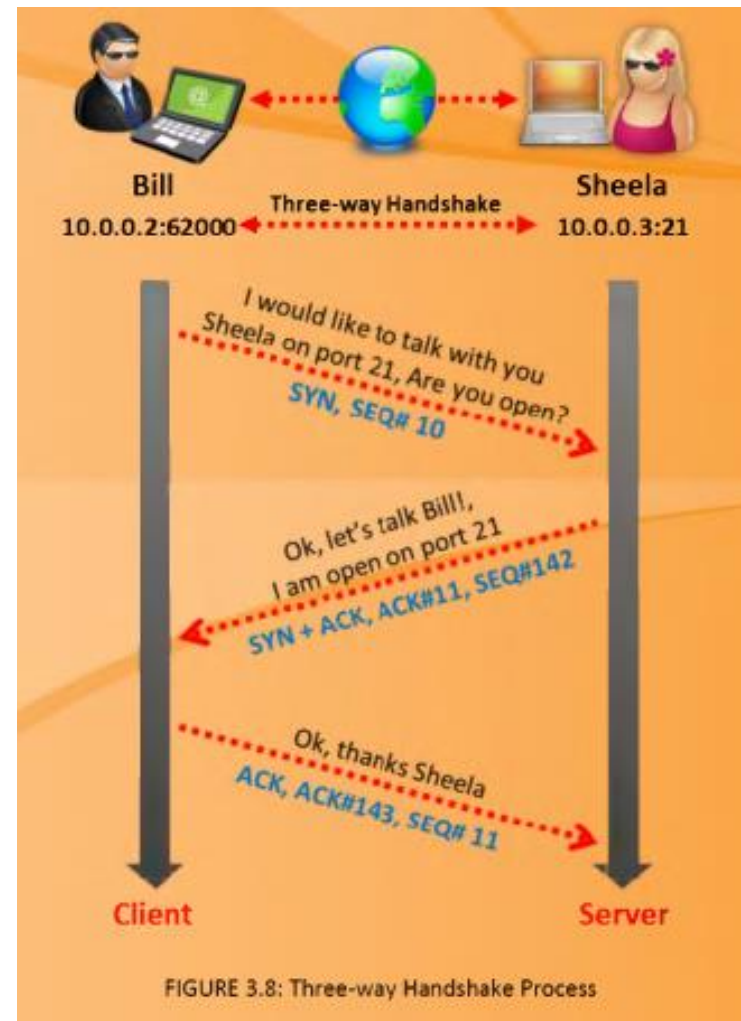
Check for Open Ports

- TCP is connection-oriented, which implies connection establishment is principal prior to data transfer between applications.
- This connection is possible through the process of the three-way handshake.
- The three-way handshake is implemented for establishing the connection between protocols

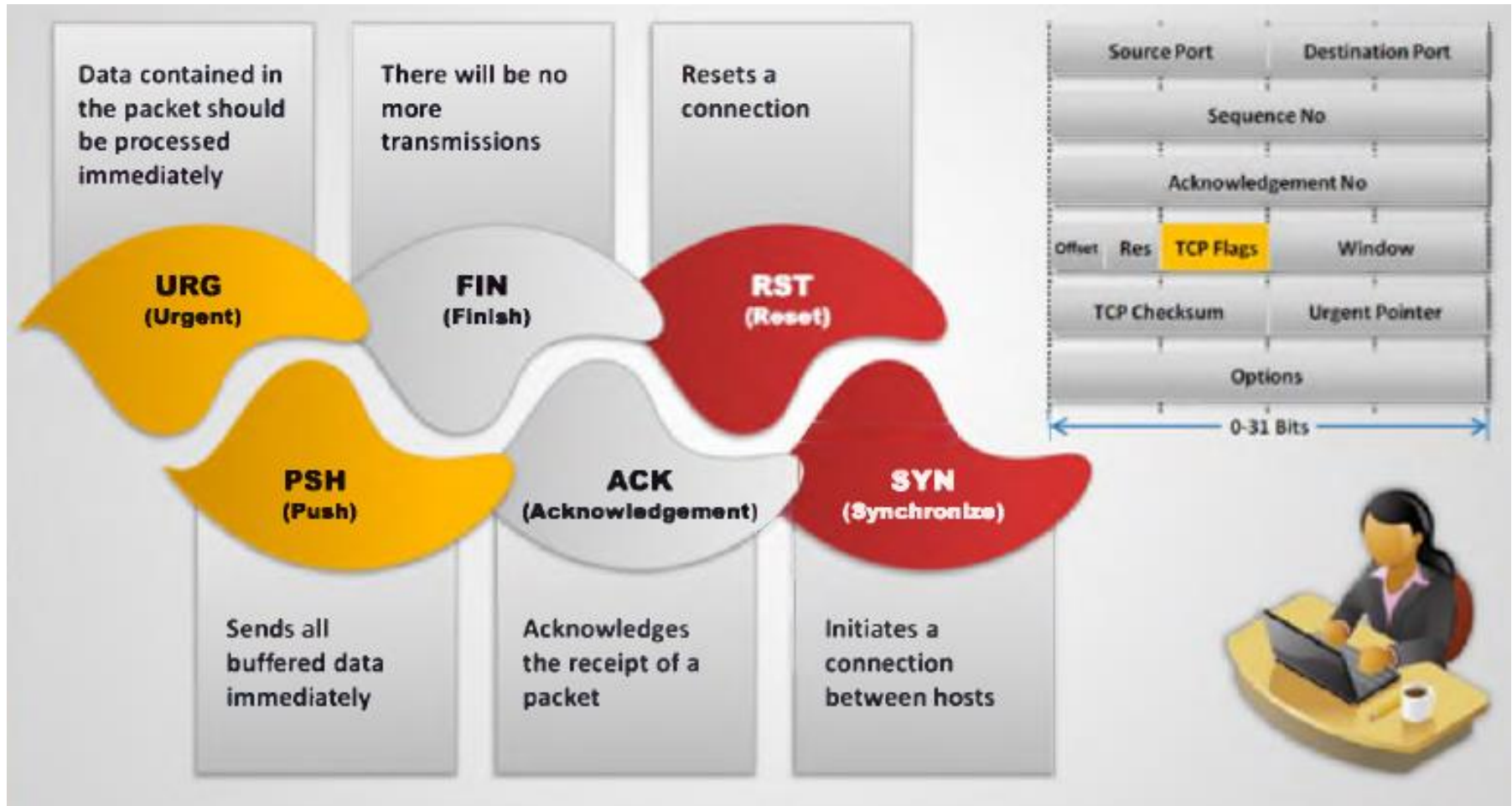


- **The three-way handshake process goes as follows:**

- To launch a TCP connection, the source (10.0.0.2:62000) sends a SYN packet to the destination (10.0.0.3:21).
- The destination, on receiving the SYN packet, i.e., sent by the source, responds by sending a SYN/ACK packet back to the source.
- This ACK packet confirms the arrival of the first SYN packet to the source.
- In conclusion, the source sends an ACK packet for the ACK/SYN packet sent by the destination.
- This triggers an "OPEN" connection allowing communication between the source and the destination, until either of them issues a "FIN" packet or a "RST" packet to close the connection.



TCP Flags



- TCP communication flags:
 - Synchronize alias "**SYN**": SYN notifies transmission of a new sequence number
 - Acknowledgement alias "**ACK**": ACK confirms receipt of transmission, and identifies next expected sequence number
 - Push alias "**PSH**": System accepting requests and forwarding buffered data
 - Urgent alias "**URG**": Instructs data contained in packets to be processed as soon as possible
 - Finish alias "**FIN**": Announces no more transmissions will be sent to remote system
 - Reset alias "**RST**": Resets a connection

SCANNING TOOL (EXAMPLE)

Tool

Hping

Scan	Commands
ICMP ping	<code>hping3 -1 10.0.0.25</code>
ACK scan on port 80	<code>hping3 -A 10.0.0.25 -p 80</code>
UDP scan on port 80	<code>hping3 -2 10.0.0.25 -p 80</code>
Collecting initial sequence number	<code>hping3 192.168.1.103 -Q -p 139 -s</code>
Firewalls and time stamps	<code>hping3 -S 72.14.207.99 -p 80 --tcp-timestamp</code>
SYN scan on port 50-60	<code>hping3 -8 50-56 -S 10.0.0.25 -v</code>
FIN, PUSH and URG scan on port 80	<code>hping3 -F -p -U 10.0.0.25 -p 80</code>
Scan entire subnet for live host	<code>hping3 -1 10.0.1.x --rand-dest -I eth0</code>
Intercept all traffic containing HTTP signature	<code>hping3 -9 HTTP -I eth0</code>
SYN flooding a victim	<code>hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood</code>

Port Scanning Tools

- nmap
 - Widely known port scanner.
 - Utility for port scanning large networks, although it works fine for single hosts.
 - The guiding philosophy for the creation of nmap was TMTOWTDI (There's More Than One Way To Do It).
 - CMD: `nmap -sS 192.168.1.1`
 - Output:

Port	State	Protocol	Service
21	open	tcp	ftp
 -

- NMAP
 - Demo

Port Scanning Tools

- netcat
 - The Swiss army knife in our security toolkit.
 - Provides basic TCP and UDP port scanning capabilities. By default, netcat uses TCP ports, so for UDP scanning, we need to specify the `-u` option. For example,
 - CMD: `netcat -v -z -w2 192.168.1.1 1-140`
 - Output: `[192.168.1.1] 25 (smtp) open`

SCANNING TECHNIQUES

SCANNING TECHNIQUES

- The port scanning techniques are designed to identify the open ports on a targeted server or host.
- This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the intent of compromising it.
- Different types of scanning techniques employed include:
 - TCP Connect / Full Open Scan
 - Stealth Scans: SYN Scan (Half-open Scan); XMAS Scan, FIN Scan, NULL Scan
 - IDLE Scan
 - ICMP Echo Scanning/List Scan
 - SYN/FIN Scanning Using IP Fragments
 - UDP Scanning
 - Inverse TCP Flag Scanning
 - ACK Flag Scanning

Port Number

- An abstraction of the OS + Net Stds
- Part of UDP and TCP packets
 - UDP and TCP port numbers are disjoint
 - Typical to use the same port number for both UDP and TCP service
 - E.g., 80/TCP and 80/UDP for www
- 16-bit unsigned integer
- Well Known Ports (0 .. 1023)
- Registered Ports (1024 .. 49151)
- Dynamic and/or Private Ports (49152 .. 65535).
- <http://www.iana.org/assignments/port-numbers>

Name	Port/Protocol	Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	
daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
smtp	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nicname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client

bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service
audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
Name	Port/Protocol	Description
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol

imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	
snmp-trap	162/tcp	
snmp-trap	162/udp	
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo
at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zie	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk

at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	
ipx	213/udp	
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
Name	Port/Protocol	Description
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
54erberos54-ds	445/tcp	
54erberos54-ds	445/udp	
isakmp	500/udp	ISAKMP/IKE
fcpx	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	Talk
ntalk	518/udp	New Talk (ntalk)

ntalk	518/udp	SunOS talkd(8)
netnews	532/tcp	Readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)
klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell -kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
56erberos-adm	749/tcp	Kerberos Administration
56erberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication—tcp
kerberos	750/udp	Kerberos
56erberos_mas ter	751/udp	Kerberos authentication
56erberos_mas ter	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation

	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos
ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
Name	Port/Protocol	Description
pptp	1723/tcp	Pptp
pptp	1723/udp	Pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin
rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/udp	
afs	7000-7009/udp	

State of a Port

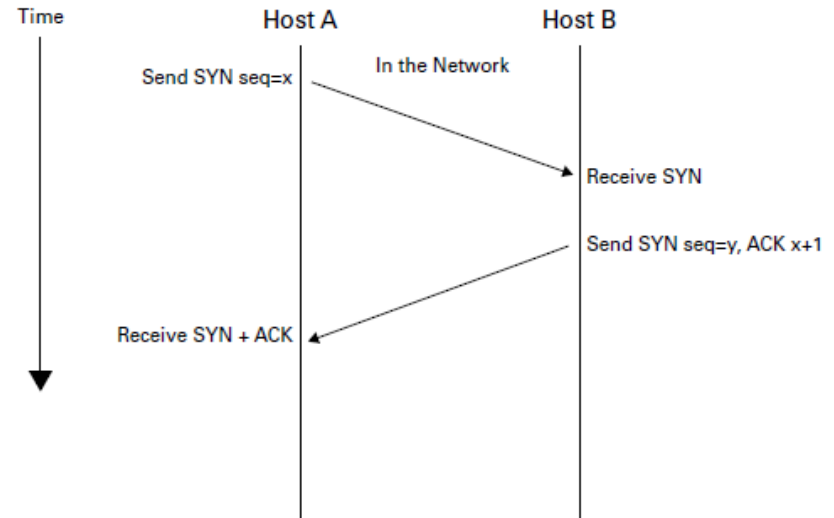
- Open
 - A service process is listening at the port. The OS receives packets arriving at this port and gives the messages to the service process. If the OS receives a SYN at an open port, this is the first packet of the three way handshake.
- Closed
 - No process is listening at the port. If the OS receives a SYN at a closed port, an RST is sent.
- Filtered
 - A packet filter is listening at the port.

Full Open Scan

- The first type of scan is known as a *full open scan*, which is a fancy way of saying that the systems involved initiated and completed the three-way handshake.
- The advantage of a full open scan is that you have positive feedback that the host is up and the connection is complete.
- However, with everything there is a downside, and in this case since you complete the three-way handshake you have confirmed that you as the scanning party are there. W
- hen this connection is no longer required, the initiating party will change the three-way handshake, and the last step will be an ACK+RST (which tears down the connection).

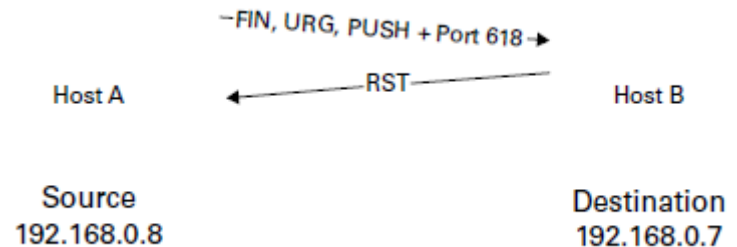
Stealth Scan, or Half-open Scan

- In this type of scan, the process is similar to the full open scan with a few important, but minor, differences. In this case, the attacker scans a system, but instead of sending the final ACK packet the attacker sends an RST packet, tearing down the connection.
- However, if the victim port is closed rather than open, the three-way handshake starts with the attacker sending a SYN, only to have the victim fire back an RST packet indicating that the port is closed and not taking connections.
- The advantage of this type of scanning is that it is less likely to trigger detection mechanisms, but the downside is that it is a little less reliable than a full open scan, because confirmation is not received during this process.



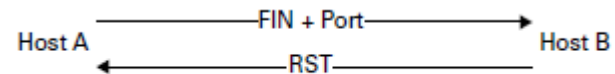
Xmas Tree Scan

- This next scan gets its name from the phrase “Lit up like a Christmas (Xmas) tree,” meaning that everything is turned on. In this type of scan, all the flags are set except PSH.
- That is, a single packet is sent to the client with ACK, SYN, URG, RST, and FIN all set.
- Having all the flags set creates an illogical or illegal combination, and the receiving system has to determine what to do.
- In most modern systems this simply means that the packet is ignored or dropped, but on some systems the lack of response tells you a port is open whereas a single RST packet tells you the port is closed.



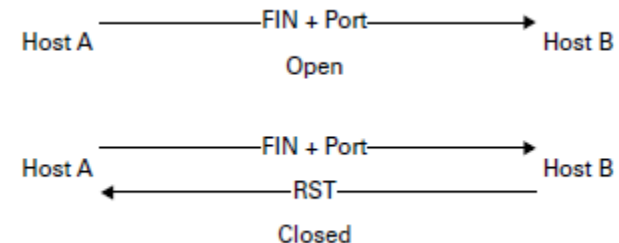
FIN Scan

- In this type of scan, the attacker sends frames to the victim with the FIN flag set. The result is somewhat similar to what happens in a Xmas tree scan. The victim's response depends
- on whether the port is open or closed. Much like the Xmas tree scan, if an FIN is sent to an open port there is no response, but if the port is closed the victim returns an RST.



NULL Scan

- In this type of scan, the attacker sends frames to the victim with no flag set.
- The result is somewhat similar to what happens in an FIN scan. The victim's response depends on whether the port is open or closed.
- Much like the FIN and Xmas tree scans, if no flags are set on a frame that is sent to an open port there is no response, but if the port is closed, the victim returns an RST



ACK scan

- Another interesting variation of setting flags is the ACK scan, which is used to test whether any filtering is being done on a port.
- Filtering indicates that a stateful firewall is present between the attacker and the target.
- The results that come back from the probe tell the attacker whether a firewall or router is in use.
- *fragmenting* works by breaking a packet into multiple pieces with the goal of preventing detection devices from seeing what the original unfragmented packet intends to do.

Fragmentation scanning

- Not a new scanning method in and of itself. A modification of other techniques.
- Split the probe packet into IP fragments.
- By splitting up the TCP header over several packets, it is harder for packet filters to detect a probe.

TCP reverse identd scanning

- *identd* protocol (rfc1413): Disclose the username of the owner of any process connected via TCP, even if that process didn't initiate the connection.
- Example: connect to the http port (80), and then use identd to find out whether the server is running as root.
- Must have full TCP connection to the port.

FTP Bounce Scan

- A port scanner can exploit this to scan TCP ports from a proxy ftp server.
- Connect to an FTP server behind a firewall, and then scan ports that are more likely to be blocked.
- If the ftp server allows reading from and writing to a directory (such as /incoming), you can send arbitrary data to ports that you do find open.

FTP Bounce Scan

- Take advantage of a vulnerability of FTP protocol.
- Requires support for proxy ftp connections.
- For example, evil.com can establish a control communication connection to FTP server-PI (protocol interpreter) of target.com.
- Then it is able to request the server-PI to initiate an active server-DTP (data transfer process) to send a file anywhere on the Internet.

FTP Bounce Scan

- Use the PORT command (of FTP) to declare that our passive user-DTP is listening on the target box at a certain port number.
- LIST the current directory, and the results is sent over the server-DTP channel.
- If our target host is listening on the port, the transfer will be successful.
- Otherwise, connection will be refused.
- Then issue another PORT command to try the next port on the target.

FTP Bounce Scan

- Advantages
 - Harder to trace
 - Potential to bypass firewalls.
- Disadvantages
 - Slow
 - Many FTP servers have (finally) disabled the proxy feature.

UDP Scans

- UDP is simpler, but the scanning is more difficult
- Open ports do not have to send an ACK.
- Closed ports are not *required* to send an error packet.
 - Most hosts send an ICMP_PORT_UNREACH error when you send a packet to a closed UDP port.
 - Can find out if a port is NOT open.

UDP Scans

- Neither UDP packets, nor the ICMP errors are guaranteed to arrive.
- Slow: the ICMP error message rate is limited.
- Need to be root for access to raw ICMP socket.
- Non-root users cannot read port unreachable errors directly.

UDP Scans

- But users can learn it indirectly.
- For example, a second `write()` call to a closed port will usually fail.
- `recvfrom()` on non-blocking UDP sockets usually return `EAGAIN` (try again), if the ICMP error hasn't been received.
- It will return `ECONNREFUSED` (connection refuse), if ICMP error has been received.

Stealth Scan

- Simple port scanning can be easily logged by the services listening at the ports.
 - E.g. they see an incoming connection with no data, thus they log an error.
- Stealth scan refers to scanning techniques that can avoid being logged.
- These techniques include fragmented packets, SYN scanning, FIN scanning etc.

Stealth Scan

- Scan slowly
 - A port scanner typically scans a host too rapidly
 - Some detectors recognize these “signatures”.
 - So, scanning very slowly (e.g., over several days) is a stealth technique.
- Firing packets with fake IPs
 - Flood with spoofed scans and embed one scan from the real source (network) address.

Signatures of a port scan

- Several packets to different destination ports from the same source within a “short period” of time.
- SYN to a non-listening port

THWARTING SCANNING

Detection of Port Scanning

- Open a socket
 - SOCK_RAW mode.
 - protocol type IPPROTO_IP
- recvfrom() to capture the packets
- Discovering stealth scans requires kernel level work.
- A detector can inform us that we have been port-scanned, but the source address may have been spoofed.

Scanner Leaks

- If the packets we received have an IP TTL of 255, we can conclude that it was sent from or local network, regardless of what the source address field says.
- if TTL is 250, we can only tell that the attacker was no more than 5 hops away.

OS FINGERPRINTING

OS Fingerprinting

- Much like individuals, operating systems have unique fingerprints that help identify them.
- have to know how to look for these unique details and determine what each means.

TABLE 5.3 Active vs. passive fingerprinting

	Active	Passive
How it works	Uses specially crafted packets.	Uses sniffing techniques to capture packets coming from a system.
Analysis	Responses are compared to a database of known responses.	Responses are analyzed looking for details of OS.
Chance of detection	High, because it introduces traffic to the network.	Low, because sniffing does not introduce traffic to the network.

Banner Grabbing

- is designed to determine information about the services running on a system
- useful to ethical hackers during their assessment process
- undertaken using Telnet to retrieve banner information about the target that reveals the nature of the service
- *banner* is what a service returns to the requesting program to give information about the service itself
 - in the case of HTTP it can include the type of server software, version number, when it was modified last, and similar information
- Safeguard by disable or change the banner that the server is exposing and hide file extensions on systems such as web servers

- For instance, in Nmap, the OS finger print or banner grabbing is done through eight tests.
 - T1: In this test, a TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.
 - T2: It involves sending a TCP packet with the no flags enabled to an open TCP port. This type of packet is known as a NULL packet.
 - T3: It involves sending a TCP packet with the URG, PSH, SYN, and FIN flags enabled to an open TCP port.
 - T4: It involves sending a TCP packet with the ACK flag enabled to an open TCP port.
 - T5: It involves sending a TCP packet with the SYN flag enabled to a closed TCP port.
 - T6: It involves sending a TCP packet with the ACK flag enabled to a closed TCP port.
 - T7: It involves sending a TCP packet with the URG, PSH, and FIN flags enabled to a closed TCP port.
 - PU (Port Unreachable): It involves sending a UDP packet to a closed UDP port. The objective is to extract an "ICMP port unreachable " message from the target machine.

Example command





- Netcat
 - nc - vv www.juggyboy.com 80
- Nmap
- NMAP -sF <target IP address> (Fin scan)
- NMAP -sN <target IP address> (Nul Scan)
- NMAP -sA -P0 <target IP address> (Ack Scan)
- NMAP -sS -T4 -A -f -v <target IP address>
(fragment Scan)

VULNERABILITY SCANNING

Vulnerability scanning

- Vulnerability scanning identifies vulnerabilities and weaknesses of a system
- Network in order to determine how a system can be exploited.
- Vulnerability scanning can find the vulnerabilities in:
 - Network topology and OS vulnerabilities
 - Open ports and running services
 - Application and services configuration errors
 - Application and services vulnerabilities
- Nessus, Owasp ZAP, burpsuit, acunetix is among the tool for VS

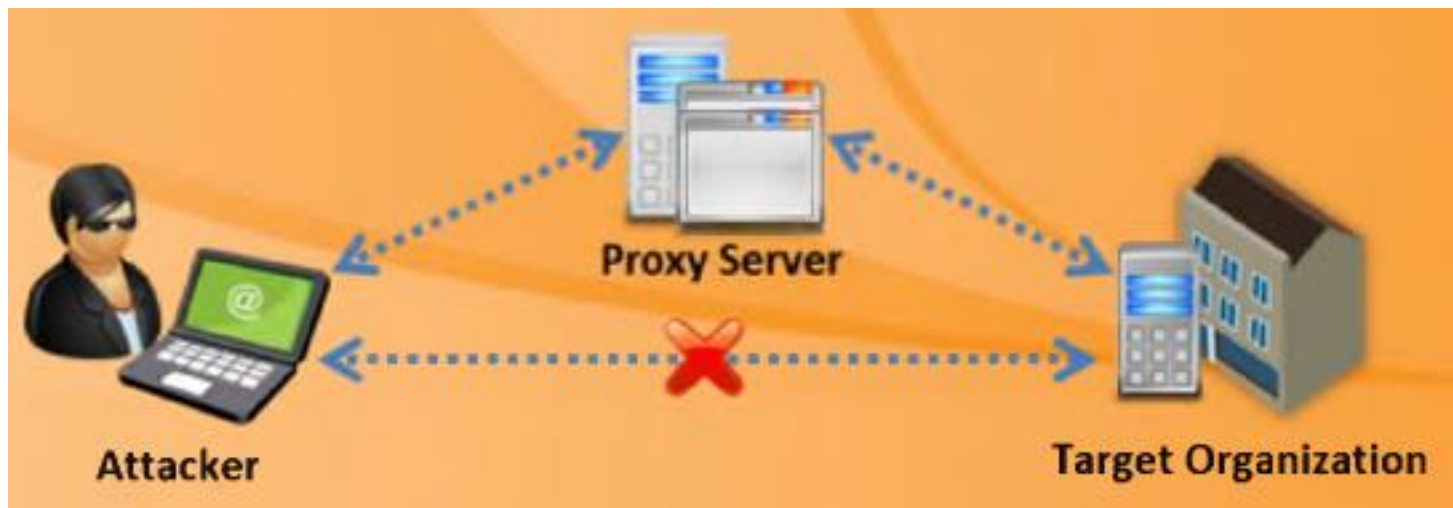
Tool

 Retina CS http://go.eeye.com	 OpenVAS http://www.openvas.org
 Core Impact Professional http://www.coresecurity.com	 Security Manager Plus http://www.manageengine.com
 MBSA http://www.microsoft.com	 Nexpose http://www.rapid7.com
 Shadow Security Scanner http://www.safety-lab.com	 QualysGuard http://www.qualys.com
 Nsauditor Network Security Auditor http://www.nsauditor.com	 Security Auditor's Research Assistant (SARA) http://www-arc.com

COVERING YOUR SCANNING ACTIVITY

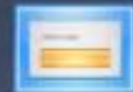
Proxy Servers

- A *proxy* is a system acting as a stand-in between the scanner and the target.
- The proxy acts as an agent for the scanning party, thus providing a degree of anonymity for the scanning party.
- Proxy servers can perform several functions, including:
 - Filtering traffic in and out of the network
 - Anonymizing web traffic
 - Providing a layer of protection between the outside world and the internal network
- A vigilant network administrator who is checking logs and systems will see the agent or proxy, but not the actual scanning party behind the proxy



1

To hide the **source IP address** so that an attacker can hack without any legal corollary



2

To **mask the actual source** of the attack by impersonating a fake source address of the proxy



3

To **remotely access intranets** and other **website resources** that are normally off limits



4

To **interrupt all the requests** sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address



5

Attackers chain **multiple proxy servers** to avoid detection





tool



Burp Suite

<http://www.portswigger.net>



Proxy Commander

<http://www.dlao.com>



Proxy Tool Windows App

<http://webproxylst.com>



Gproxy

<http://gpass1.com>



Fiddler

<http://www.fiddler2.com>



Proxy

<http://www.analogx.com>



Protoport Proxy Chain

<http://www.protoport.com>



Proxy+

<http://www.proxyplus.cz>



FastProxySwitch

<http://affinity-tools.com>



ProxyFinder

<http://www.proxy-tool.com>



ProxyFinder Enterprise

<http://www.proxy-tool.com>



Socks Proxy Scanner

<http://www.mylanviewer.com>



ezProxy

<http://www.oclc.org>



Charles

<http://www.charlesproxy.com>



JAP Anonymity and Privacy

http://anon.inf.tu-dresden.de/index_en.html



UltraSurf

<http://www.ultrasurf.us>



CC Proxy Server

<http://www.youngsoft.net>



WideCap

<http://widecap.ru>



FoxyProxy Standard











<https://addons.mozilla.org>



ProxyCap

<http://www.proxycap.com>

IP spoofing Counter Measure

 <p>Limit access to configuration information on a machine</p>	<p>Do not rely on IP-based authentication</p> 
 <p>Use random initial sequence numbers</p>	<p>Strictly filter use of ICMP</p> 
 <p>Ingress Filtering - Use router filters to prevent packets from entering your network</p>	<p>Reduce TTLs in TCP/IP requests</p> 
 <p>Egress Filtering - Use filters to prevent packets from leaving your network</p>	<p>Block private or unauthorized IP addresses using access control lists</p> 
 <p>Encrypt all network traffic</p>	<p>Use multiple firewalls providing multi-layered depth of protection</p> 

Scanning PentTest

- Pen testing a network for scanning vulnerabilities determines the network's **security posture** by identifying **live systems**, discovering **open ports**, associating **services** and grabbing **system banners** to simulate a network hacking attempt
- The penetration testing report will help **system administrators** to:





START

Perform host
discovery

Perform port
scanning

Perform banner grabbing
/OS fingerprinting

Scan for
vulnerability



Use tools such as Nmap,
Angry IP Scanner, etc.

Use tools such as Nmap,
Netscan Tools Pro, etc.

Use tools such as Telnet,
Netcraft, ID Serve, etc.

Use tools such as Nessus,
SAINTscanner,
GFI-LANGuard, etc.



- ❖ Check for the live hosts using tools such as Nmap, Angry IP Scanner, SolarWinds Engineer's toolset, Colasoft Ping Tool, etc.
- ❖ Check for open ports using tools such as Nmap, Netscan Tools Pro, PRTG Network Monitor, Net Tools, etc.
- ❖ Perform banner grabbing/OS fingerprinting using tools such as Telnet, Netcraft, ID Serve, etc.
- ❖ Scan for vulnerabilities using tools such as Nessus, GFI LANGuard, SAINTscanner, Core Impact Professional, Retina CS Management, MBSA, etc.





- Draw network diagrams of the vulnerable hosts using tools such as LAN surveyor, OpManager, NetworkView, The Dude, FriendlyPinger, etc.
- Prepare proxies using tools such as Proxy Workbench, Proxifier, Proxy Switcher, SocksChain, TOR, etc.
- Document all the findings

SUMMARY

Summary

- The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network.
- Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts.
- Attackers use various scanning techniques to bypass firewall rules, logging mechanism, and hide themselves as usual network traffic.
- Banner Grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system.
- HTTP Tunneling technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls.
- Proxy is a network computer that can serve as an intermediary for connecting with other computers.
- A chain of proxies can be created to evade a traceback to the attacker.