

Prepared by Dr. Nermin Hamza

CYB740
Penetration test and Ethical hacking

Lecture 03



Scanning

Lecture 03

CYB740

Penetration test and Ethical hacking



Prepared by
Dr. Nermin Hamza

Outlines

- Scanning
- Discover alive system
- Port scanning the system
- Banner grabbing and operating system identification
- Penetration test summary



Scanning

- One of the information gathering piece is to get IP addresses that both belonged to the target and that we were authorized to attack.



Scanning

- Network scanning refers to a set of procedures for identifying hosts , ports, and services in a network.
- Objectives of network scanning :
 - To discover live hosts, IP address, and ports of live hosts
 - To discover operating systems
 - To discover services running on hosts



Chapter

03

live hosts, IP address, and ports of live hosts

- Determining if a system is alive
- Port scanning the system with Nmap.



alive system

- A **ping** is a special type of network packet called an Internet Control Message Protocol (ICMP) packet.
- What is the Internet Control Message Protocol (ICMP)?
 - The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.
 - ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner.



alive system

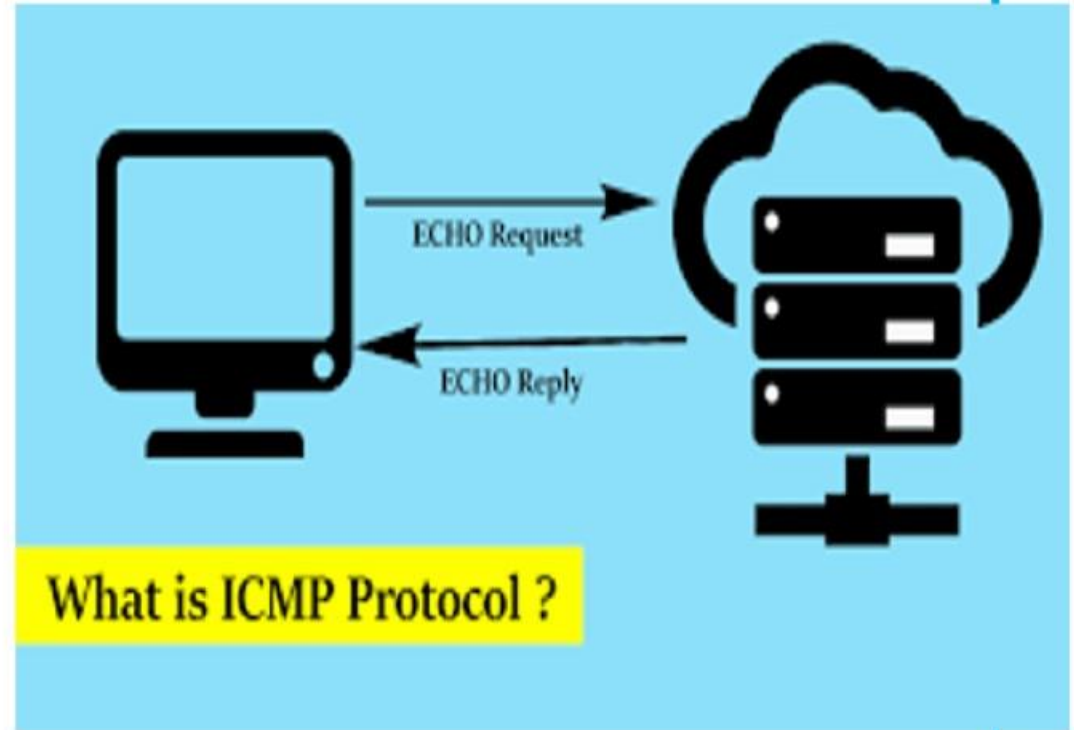
What is ICMP used for?

- The primary purpose of ICMP is for error reporting.
- A secondary use of ICMP protocol is to perform network diagnostics; the commonly used terminal utilities traceroute and ping both operate using ICMP



alive system

- Pings work by sending a particular type of network traffic, called an ICMP **echo request packet**, to a specific interface on a computer or network device.
- If the device (and the attached network card) that **received the ping packet** is turned on and not restricted from responding, the receiving machine will respond back to the originating machine with an echo reply packet.



alive system

- Aside from telling us that a host is alive and accepting traffic, pings provide other valuable information including the total time it took for the packet to travel to the target and return.
- Pings also report traffic loss that can be used to gauge the reliability of a network connection.



Chapter

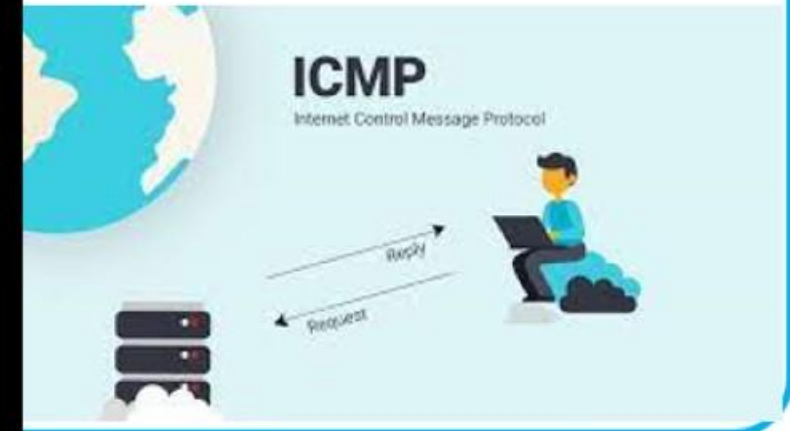
03

alive system

ping target_ip

You will need to replace the “target_ip” portion of the command with the actual IP address or hostname of the machine you are

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# ping google.com  
PING google.com (74.125.225.6) 56(84) bytes of data.  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=1 ttl=128 time=29.2 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=2 ttl=128 time=28.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=3 ttl=128 time=32.9 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=4 ttl=128 time=26.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=5 ttl=128 time=26.9 ms  
^C  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 26.475/28.800/32.940/2.312 ms  
root@bt:~#
```



alive system

- “64 bytes from”. This line is telling us that our ICMP echo request packet successfully reached the target host and that the host successfully sent a reply packet back to our machine.
- The “64 bytes” indicates the size of the response packet.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# ping google.com  
PING google.com (74.125.225.6) 56(84) bytes of data.  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=1 ttl=128 time=29.2 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=2 ttl=128 time=28.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=3 ttl=128 time=32.9 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=4 ttl=128 time=26.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=5 ttl=128 time=26.9 ms  
^C  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 26.475/28.800/32.940/2.312 ms  
root@bt:~#
```



Chapter

03

alive system

- The “from ord08s05-in-f6.1e100.net (74.125.225.6):” specifies which hostname (and IP address) responded to our google.com ping.
- The “icmp_seq=” designates the packet order.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# ping google.com  
PING google.com (74.125.225.6) 56(84) bytes of data.  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=1 ttl=128 time=29.2 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=2 ttl=128 time=28.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=3 ttl=128 time=32.9 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=4 ttl=128 time=26.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=5 ttl=128 time=26.9 ms  
^C  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 26.475/28.800/32.940/2.312 ms  
root@bt:~#
```



alive system

- The “ttl = 128” is the time to live value; this is used to determine the maximum number of hops the packet will take before automatically expiring.
- “Time = 29.2 ms” is telling you how long the entire trip took for the packets to travel to and from the target.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# ping google.com  
PING google.com (74.125.225.6) 56(84) bytes of data:  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=1 ttl=128 time=29.2 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=2 ttl=128 time=28.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=3 ttl=128 time=32.9 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=4 ttl=128 time=26.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=5 ttl=128 time=26.9 ms  
^C  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 26.475/28.800/32.940/2.312 ms  
root@bt:~#
```



alive system

- After stopping the ping command, you will be provided with an output of statistics including the number of packets transmitted, packet loss, and a series of time-based stats

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# ping google.com  
PING google.com (74.125.225.6) 56(84) bytes of data.  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=1 ttl=128 time=29.2 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=2 ttl=128 time=28.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=3 ttl=128 time=32.9 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=4 ttl=128 time=26.4 ms  
64 bytes from ord08s05-in-f6.1e100.net (74.125.225.6): icmp_seq=5 ttl=128 time=26.9 ms  
^C  
--- google.com ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 4007ms  
rtt min/avg/max/mdev = 26.475/28.800/32.940/2.312 ms  
root@bt:~#
```



Test with your self

Using a Windows Ping

To use the built-in ping command in Windows to test connectivity to another system:

1. Open a command prompt in Windows.
2. Type ping www.microsoft.com.



alive system

- A **ping sweep** is a series of pings that are automatically sent to a range of IP addresses, rather than individually entering each target's address.
- The simplest way to run a ping sweep is with a tool called **FPing**.
- FPing is built into Kali and is run from the terminal.
- The tool can also be downloaded for Windows.



```
fping -a -g 216.58.209.46 216.58.209.200 >hosts.txt
```



Port scanning the system



Port scanning the system with

What Does Port Number Mean?

- A port number is the **logical address** of each application or process that uses a network or the Internet to communicate.
- A port number **uniquely identifies** a network-based application on a computer.
- Each application/program is allocated a **16-bit** integer port number.
- This number is assigned automatically by the OS, manually by the user or is set as a default for some popular applications.



Port scanning the system

What is the difference between an IP address and a port number?

- An **IP address** identifies a machine in an IP network and is used to determine the destination of a data packet.
- **Port numbers** identify a particular application or service on a system.

Question : what is MAC address?



Port scanning the system

- There are 65,535 port numbers, but not all are used every day.
- Restricted port numbers or well-known port numbers are reserved by prominent companies and range from 0 to 1023.
- Those who want to register a specific port number can choose from 1024 to 49151. Software companies typically register these port numbers
- Dynamic or private ports ranging from 49152 to 65535 are available for anyone to use.



Port scanning the system

Well-Known Ports	0-1023
NN Registered Ports	1024-49151
NN Dynamic Ports	49152-65535



Port scanning the system: well-know

Port no.	Echo	Echo service
20	FTP-data	File Transfer Protocol data transfer
21	FTP	File Transfer Protocol (FTP) control connection
22	SSH	Secure Shell, secure logins, file transfers (scp, sftp), and port forwarding
23	Telnet	Telnet protocol—unencrypted text communications
25	SMTP	Simple Mail Transfer Protocol, used for email routing between mail servers
53	DNS	Domain Name System name resolver
80	HTTP	Hypertext Transfer Protocol (HTTP) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP
88	Kerberos	Network authentication system
443	HTTPS (HTTP over SSL)	Hypertext Transfer Protocol Secure (HTTPS) uses TCP in versions 1.x and 2. HTTP/3 uses QUIC, a transport protocol on top of UDP.

Port scanning the system: registered

1194	OpenVPN	OpenVPN
1589	Cisco VQP	Cisco VLAN Query Protocol (VQP)
2483	Oracle DB	Oracle database listening for insecure client connections to the listener, replaces port 1521
2484	Oracle DB	Oracle database listening for SSL client connections to the listener
2967	Symantec AV	Symantec System Center agent (SSC-AGENT)



Port scanning the system

When we conduct a port scan, our tool will literally create a packet and send it to each designated port on the machine.

- The goal is to determine what kind of a response we get from the target port.
- Different types of port scans can produce different results.
- It is important to understand the type of scan you are running as well as the expected output of that scan.



Port scanning the system with Nmap

- Nmap is a free, open source tool that quickly and efficiently performs ping sweeps, port scanning, service identification, IP address detection, and operating system detection.
- Nmap has the benefit of scanning a large number of machines in a single session.
- It's supported by many operating systems, including Unix, Windows, and Linux.



Port scanning the system with Nmap

- The state of the port as determined by an nmap scan can be open, filtered, or unfiltered.
- Open means that the target machine accepts incoming request on that port.
- Filtered means a firewall or network filter is screening the port and preventing nmap from discovering whether it's open.
- Unfiltered mean the port is determined to be closed, and no firewall or filter is interfering with the nmap requests.



Port scanning the system with Nmap

```
nmap <Scan Type> <Option> <Target Specification>
```



Port scanning the system with Nmap

- Nmap has server scan types such as :
 - TCP scan
 - UDP scan
 - Specific port scan



Port scanning the system with Nmap

TCP scan

- The first scan we will look at is called the TCP Connect scan.
- This scan is often considered the most basic and stable of all the port scans because Nmap attempts to complete the three-way handshake on each port specified in the Nmap command.



Port scanning the system

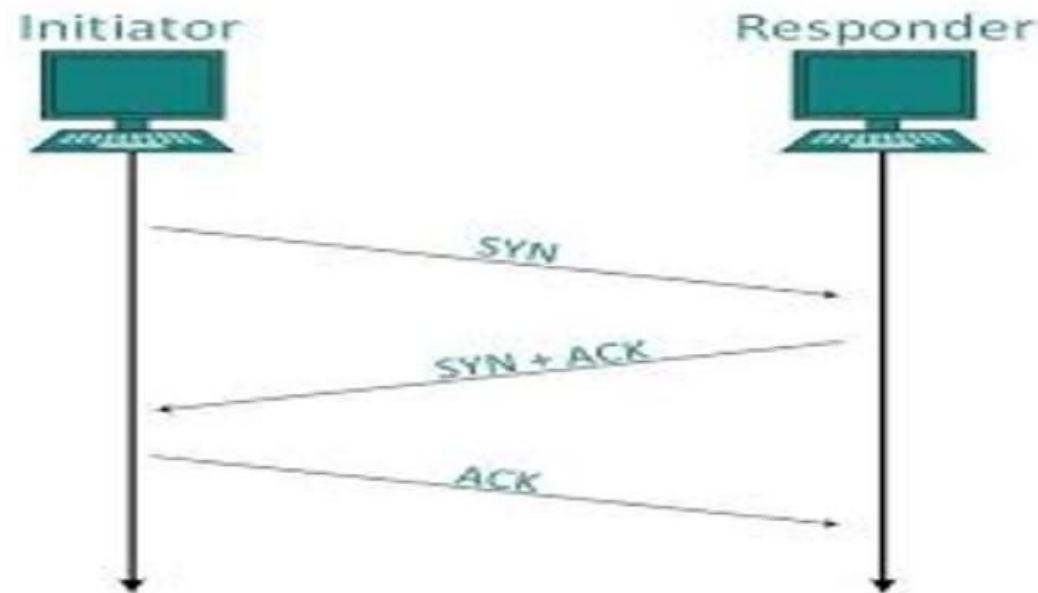
- **What is TCP protocol?**
- TCP stands for Transmission Control Protocol. It is a transport layer protocol that facilitates the transmission of packets from source to destination. It is a connection-oriented protocol that means it establishes the connection prior to the communication that occurs between the computing devices in a network. This protocol is used with an IP protocol, so together, they are referred to as a TCP/IP.

7 Layers of the OSI Model



Port scanning the system with Nmap

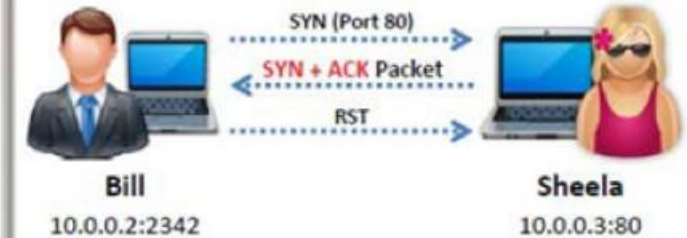
- TCP connect scan detects when a port is open by completing the **three-way handshake**.



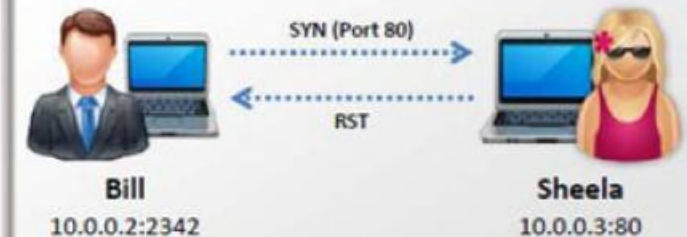
Port scanning the system with Nmap

- The client sends a single **SYN** packet to the server on the appropriate port
- If the port is open then the server responds with a **SYN/ACK** packet
- The client sends the **RST** packet to close the initiation before a connection can ever be established
- If the server responds with an **RST** packet then the remote port is in the closed state

Port is open



Port is closed



Port scanning the system with Nmap

- **nmap** <target Ip Address>
- Nmap is very simple to use, this would return us the ports that are opened upon the target host
- Lets test with google IP address
- If you do not specify a specific port range, Nmap will scan the 1000 most common ports.

```
(kali㉿kali)-[~]  
$ nmap 216.58.209.46  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-12 18:15 EST  
Nmap scan report for mil07s12-in-f14.1e100.net (216.58.209.46)  
Host is up (0.088s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 13.04 seconds
```



Chapter

03

Port scanning the

- “-sT” is used to run a scan type of TCP Connect.
- We use the “-p-” to tell Nmap to scan all the ports not just the default 1000
- “-Pn” switch will cause Nmap to disable host discovery and force the tool to scan every system as if it were alive.

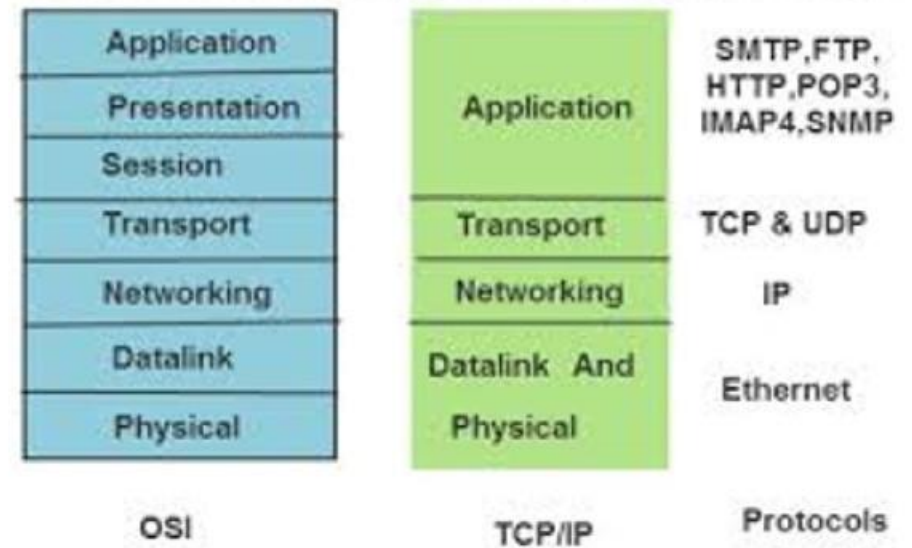
```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# nmap -sT -p- -Pn 192.168.18.132  
  
Starting Nmap 6.01 ( http://nmap.org ) at 2013-02-17 14:42 EST  
Nmap scan report for 192.168.18.132  
Host is up (0.00042s latency).  
Not shown: 65522 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
3632/tcp  open  distccd  
5432/tcp  open  postgresql  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds  
root@bt:~#
```

Port scanning the system with Nmap

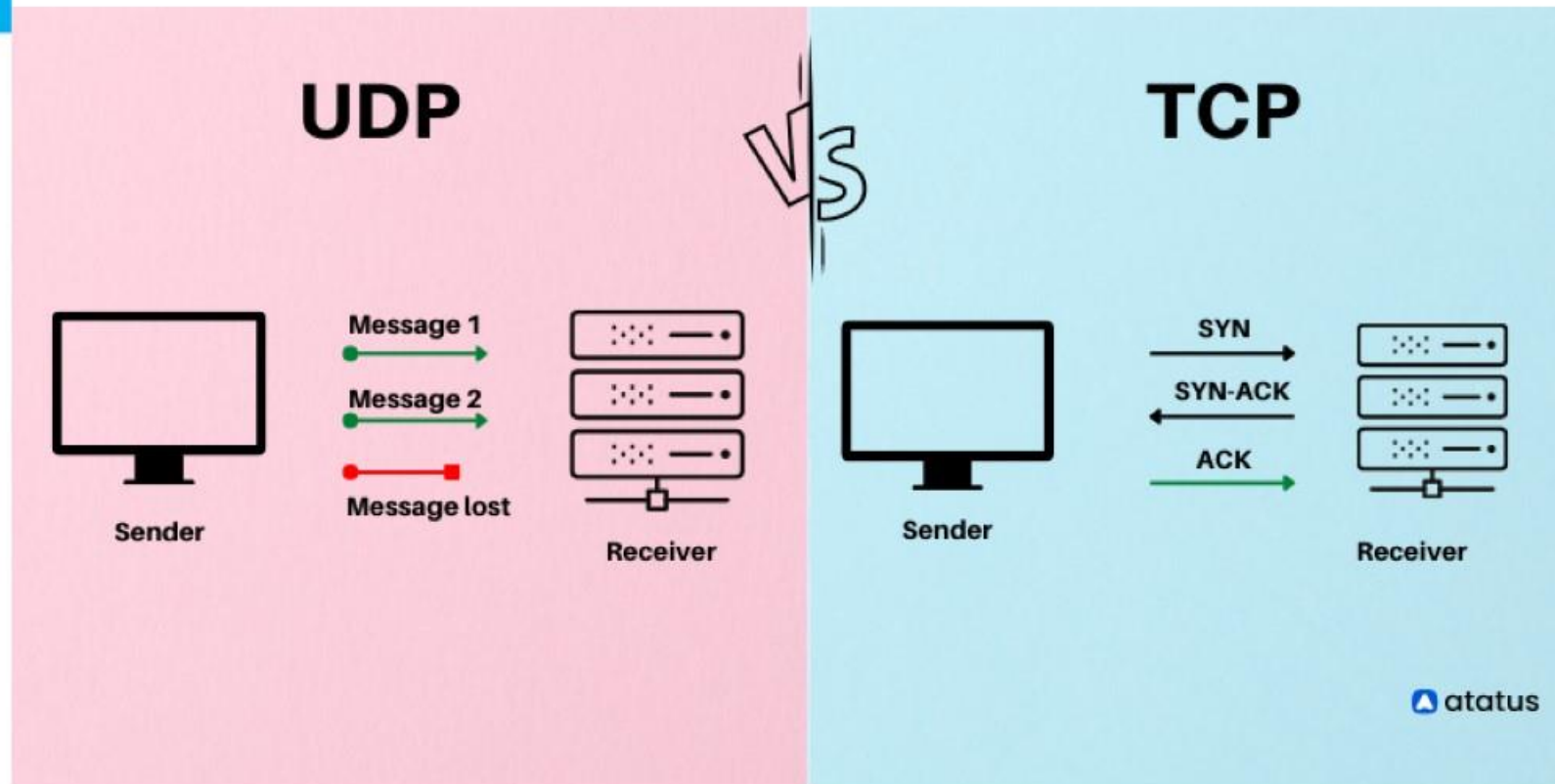
UDP scan

- User Datagram Protocol (UDP) refers to a protocol used for communication throughout the internet. It is specifically chosen for time-sensitive applications like gaming, playing videos, or Domain Name System (DNS) lookups.
- UDP results in speedier communication because it does not spend time forming a firm connection with the destination before transferring the data.

OSI & TCP/IP Protocol-Stacks and Protocols

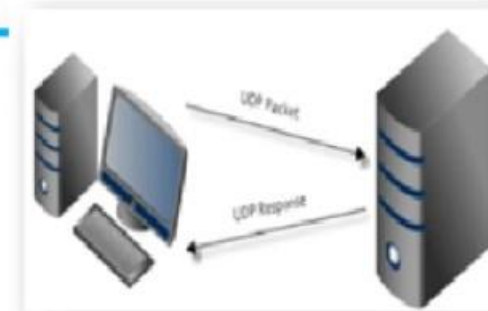


Port scanning the system



Port scanning the system with Nmap

- Nmap sends a UDP packet to a port.
- Depending **on the port**, the packet sent is protocol specific.
- If it receives a response, the port is considered open.
- If the port is closed, Nmap will receive an ICMP Port Unreachable message.
- If Nmap receives no response whatsoever, then either the port is open and the program listening does not respond to Nmap's query, or the traffic is being filtered.

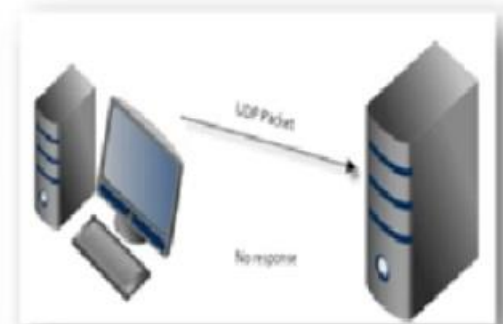


OPEN



CLOSED

OPEN | FILTERED



Port scanning the system with Nmap

- Because UDP is connectionless, the scanning logic is a bit different.
- In a UDP scan (-sU),

```
root@kali:~# nmap -sU 192.168.20.10-12 -oA bookudp

Starting Nmap 6.40 ( http://nmap.org ) at 2015-12-18 08:39 EST
Stats: 0:11:43 elapsed; 0 hosts completed (3 up), 3 undergoing UDP Sc:
UDP Scan Timing: About 89.42% done; ETC: 08:52 (0:01:23 remaining)
Nmap scan report for 192.168.20.10
Host is up (0.00027s latency).
Not shown: 990 closed ports
PORT      STATE      SERVICE
69/udp    open|filtered  tftp
123/udp   open          ntp
135/udp   open          msrpc
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
1026/udp  open          win-rpc
1065/udp  open|filtered syscomlan
1900/udp  open|filtered upnp
MAC Address: 00:0C:29:A5:C1:24 (VMware)

Nmap scan report for 192.168.20.11
Host is up (0.00031s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
111/udp   open          rpcbind
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open          nfs
5353/udp  open          zeroconf
MAC Address: 00:0C:29:FD:0E:40 (VMware)

Nmap scan report for 192.168.20.12
Host is up (0.072s latency).
Not shown: 999 open|filtered ports
PORT      STATE      SERVICE
137/udp   open          netbios-ns
MAC Address: 00:0C:29:62:D5:C8 (VMware)

Nmap done: 3 IP addresses (3 hosts up) scanned in 1073.86 seconds
```



Port scanning the system with Nmap

Scanning a Specific Port

- Nmap scans only the 1,000 ports it considers the most “interesting,” not the 65,535 possible TCP or UDP ports.
- The default Nmap scan will catch common running services, but in some cases it will miss a listening port or two. To scan specific ports, use the -p flag with Nmap

```
root@kali:~# nmap -p 3232 -sV 192.168.20.10
Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-28 10:19 EDT
Nmap scan report for 192.168.20.10
Host is up (0.00031s latency).
PORT      STATE SERVICE VERSION
3232/tcp  open  unknown
1 service unrecognized despite returning data❶. If you know the service/
version, please submit the following fingerprint at http://www.insecure.org/
```



Test by yourself

To use a port scan tool to determine listening ports of active hosts:

1. Download Angry IP Scanner from www.angryip.org
2. Enter the IP address of the target system in the Host or IP Address field or enter a range or IP address for your lab systems and click Start to perform a conventional (full connect) scan of standard ports.



Discover operating systems



Discover operating systems

- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system.



Banner grabbing and operating system identification

- Banner grabbing is the process of opening a connection and reading the banner or response sent by the application.
- The process of fingerprinting allows the hacker to identify particularly vulnerable or high-value targets on the network.
- Hackers are looking for the easiest way to gain access to a system or network.



Banner grabbing and operating system identification

- Many email, FTP, and web servers will respond to a telnet connection with the name and version of the software.
- This aids a hacker in fingerprinting the OS and application software.
- For example, a Microsoft Exchange email server would only be installed on a Windows OS.



- Identifying the OS used on the target host allows an attacker to figure out vulnerabilities the system possesses and the exploits that might work on a system to further carry out additional attack.
- There are two types of banner grabbing : **active and passive** .



- Active stack fingerprinting is the most common form of fingerprinting.
- It involves sending data to a system to see how the system responds.
- It's based on the fact that various operating system vendors implement the TCP stack differently, and responses will differ based on the operating system.
- The responses are then compared to a database to determine the operating system.
- Active stack fingerprinting is detectable because it repeatedly attempts to connect with the same target system.



- Passive stack fingerprinting is stealthier and involves examining traffic on the network to determine the operating system.
- It uses sniffing techniques instead of scanning techniques.
- Passive stack fingerprinting usually goes undetected by an IDS or other security system but is less accurate than active fingerprinting.



Active Banner Grabbing

- **Specially crafted packets** are sent to remote OS and the responses are noted
- The responses are then compared with a database to **determine the OS**
- Response from different OSes varies due to differences in **TCP/IP stack implementation**



Passive Banner Grabbing

- **Banner grabbing from error messages**
Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system
- **Sniffing the network traffic**
Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system
- **Banner grabbing from page extensions**
Looking for an extension in the URL may assist in determining the application version
Example: .aspx => IIS server and Windows platform



Hostnames matching google.com

► Q Search with another pattern?

First 500 results (showing 1 to 20)

Rank	Site	First seen	Netblock	OS
	www.google.com ↗	November 1998	Google LLC	Linux
	mail.google.com ↗	June 2004	Google LLC	Linux
	docs.google.com ↗	December 2006	Google LLC	Linux
0	accounts.google.com ↗	March 2011	Google LLC	Linux
5	drive.google.com ↗	January 2012	Google LLC	Linux
0	translate.google.com ↗	October 2008	Google LLC	Linux

- Netcraft reports a site's operating system, web server and netblock owner together with, if available, a graphical view of the time since last reboot for each of the computer serving the site.



Chapter

03

ID Server

Banner grabbing and operating system identification

- ID Server is used to identify the make, model, and version of any web site; server software.
- It is also used to identify non-HTTP internet servers such as FTP, SMTP, POP NEWs etc.



Chapter
03

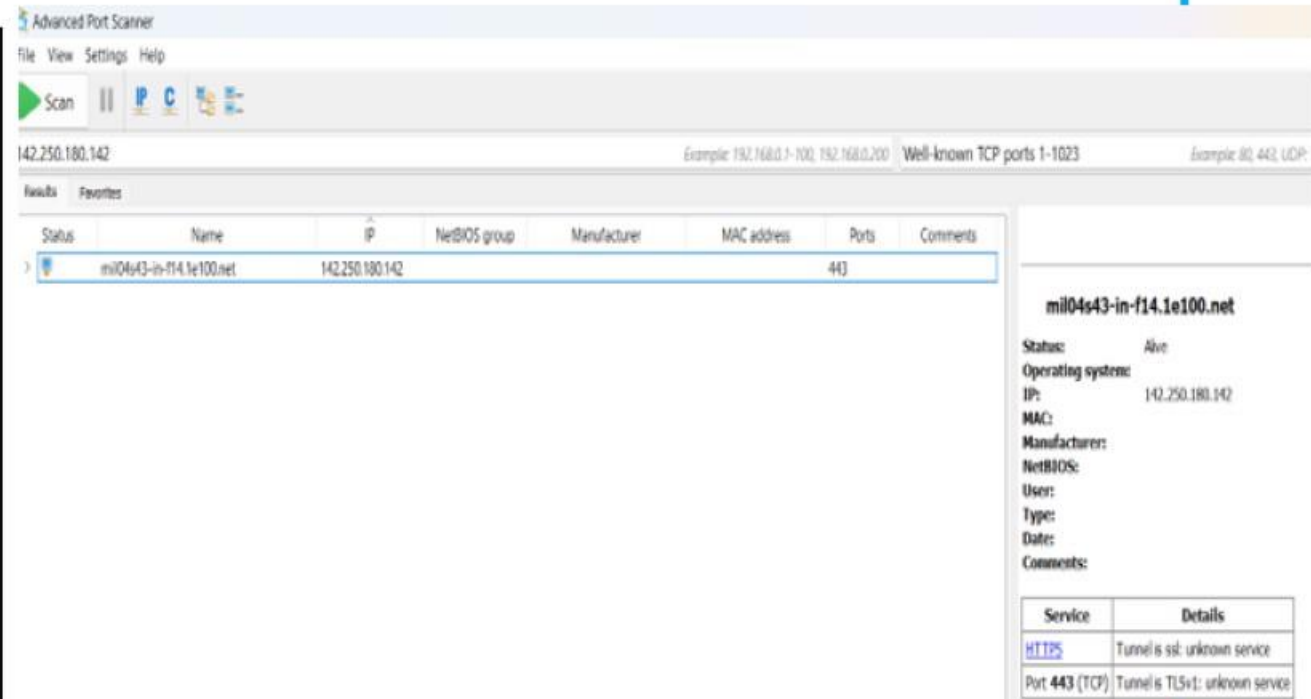
Services and ports

- What about services and ports numbers ?

```
C:\Users\Nermin>netstat
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:49313	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49340	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49347	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49350	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49364	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49366	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49388	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49389	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49390	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49391	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49392	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49400	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49404	DESKTOP-UAC9DLD:49676	ESTABLISHED
TCP	127.0.0.1:49406	DESKTOP-UAC9DLD:49676	ESTABLISHED



Advanced Port Scanner

File View Settings Help

Scan || IP C

142.250.180.142 Example: 192.168.0.1-100, 192.168.0.200 Well-known TCP ports 1-1023 Example: 80, 443, UDP: 1

Status	Name	IP	NetBIOS group	Manufacturer	MAC address	Ports	Comments
Alive	mil04s43-in-f14.1e100.net	142.250.180.142				443	

mil04s43-in-f14.1e100.net

Status: Alive

Operating system: 142.250.180.142

IP: 142.250.180.142

MAC:

Manufacturer:

NetBIOS:

User:

Type:

Date:

Comments:

Service	Details
HTTPS	Tunnel is ssl; unknown service
Port 443 (TCP)	Tunnel is TLSv1; unknown service



Penetration test summary

- 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.



Penetration test countermeasure

The penetration testing report will help system administrators to:





Thank You