



Nmap Security Scanning-I

Dr. Md. Mamun-or-Rashid

Professor, Dept. of CSE, University of Dhaka
mamun@cse.univdhaka.edu | www.cse.du.ac.bd

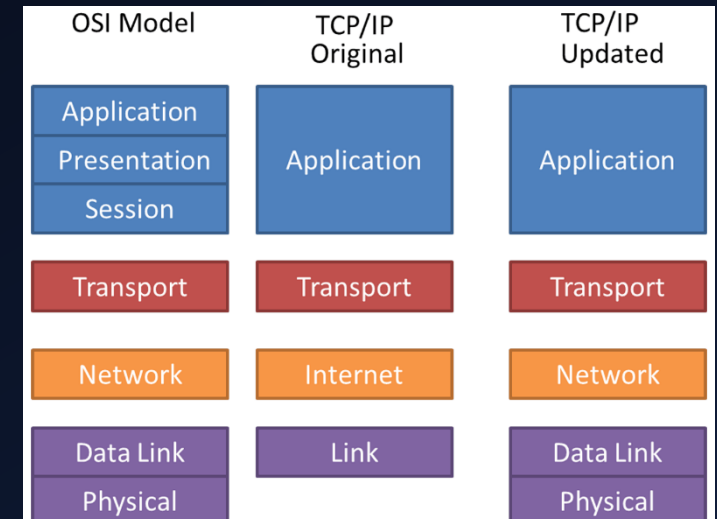
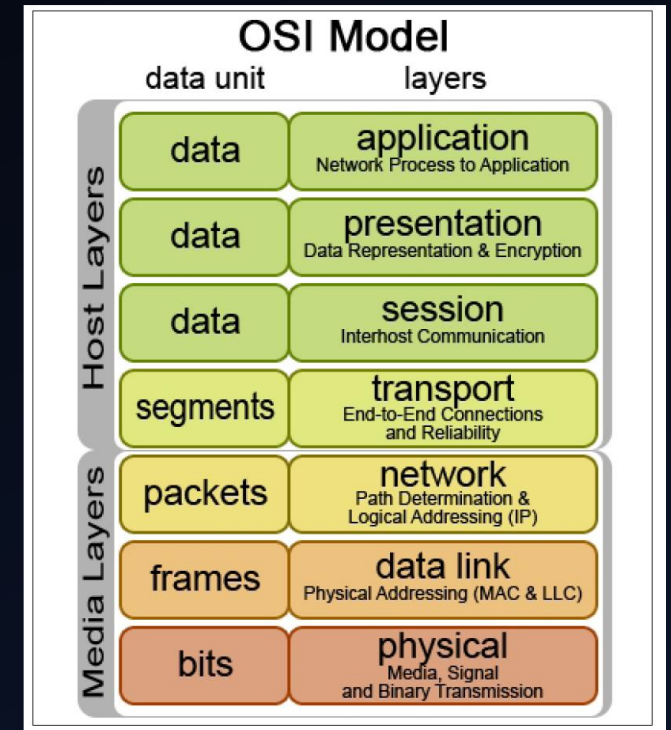
Md. Mahedi Hasan

Network Engineer, University of Dhaka
cse.mahedi@gmail.com | www.Mahedi.me

[!\[\]\(faf942dc3e59ce8eb64b4ac481eca7e0_img.jpg\) /in/mahedicse/](#) | [!\[\]\(f6b0299e0b5e4340e509b71914970da0_img.jpg\) /mahedi.cse](#)

Fundamental of Networking

- **Networking:** An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media.
- **The OSI model:** OSI stands for Open Systems Interconnection. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
- **TCP/IP Model:** TCP stands for Transmission Control Protocol a communications standard that enables application programs and computing devices to exchange messages over a network. It is designed to send packets across the internet and ensure the successful delivery of data and messages over networks
- **Protocol:** A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.



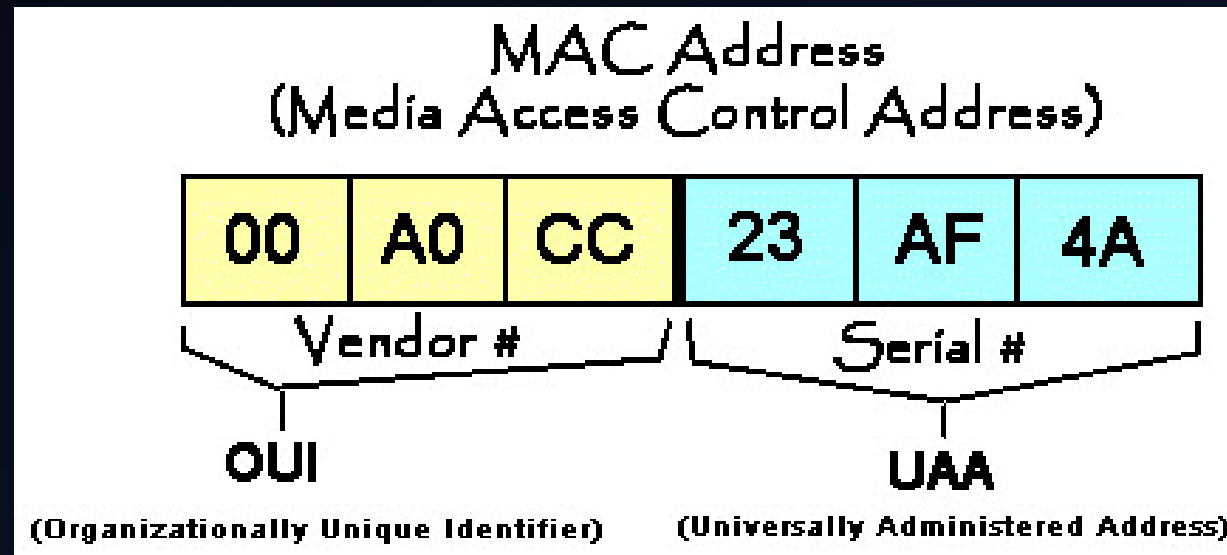
IP Address (Internet Protocol address):

- Also known as the Logical Address, the IP Address is the network address of the system across the network.
- To identify each device in the world-wide-web, assigns an IP address as a unique identifier to each device on the Internet.
- The length of an IPv4 address is 32-bits, hence, we have 2^{32} IP addresses available and the length of an IPv6 address is 128-bits.

IPv4	vs.	IPv6
Deployed 1981		Deployed 1998
32-bit IP address		128-bit IP address
4.3 billion addresses		7.9×10^{28} addresses
Addresses must be reused and masked		Every device can have a unique address
Numeric dot-decimal notation		Alphanumeric hexadecimal notation
192.168.5.18		50b2:6400:0000:0000:6c3a:b17d:0000:10a9 (Simplified - 50b2:6400::6c3a:b17d:0:10a9)
DHCP or manual configuration		Supports autoconfiguration

MAC Address (Media Access Control address):

- Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).
- A MAC address is assigned to the NIC at the time of manufacturing.
- The length of the MAC address is : 12-nibble/6 bytes/48 bits






Port Number

- A port can be referred to as a logical channel through which data can be sent/received to an application.
- Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.
- A port number is a 16-bit integer, hence, we have 65,536 ports available which are categorized as shown below:

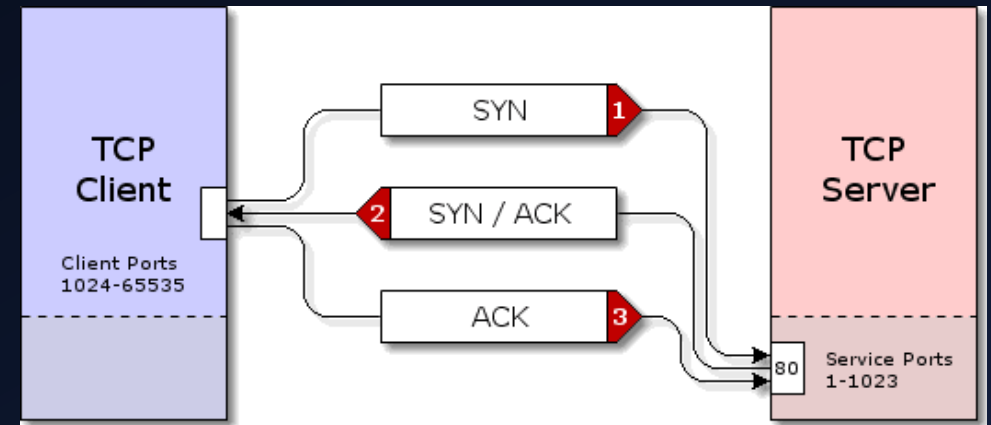
Port Types	Range
Well known Ports	0 - 1023
Registered Ports	1024 - 49151
Ephemeral Ports	49152 - 65535

For details: <http://www.iana.org/assignments/port-numbers/>

- **Socket:** The unique combination of IP address and Port number together are termed as Socket.
- 

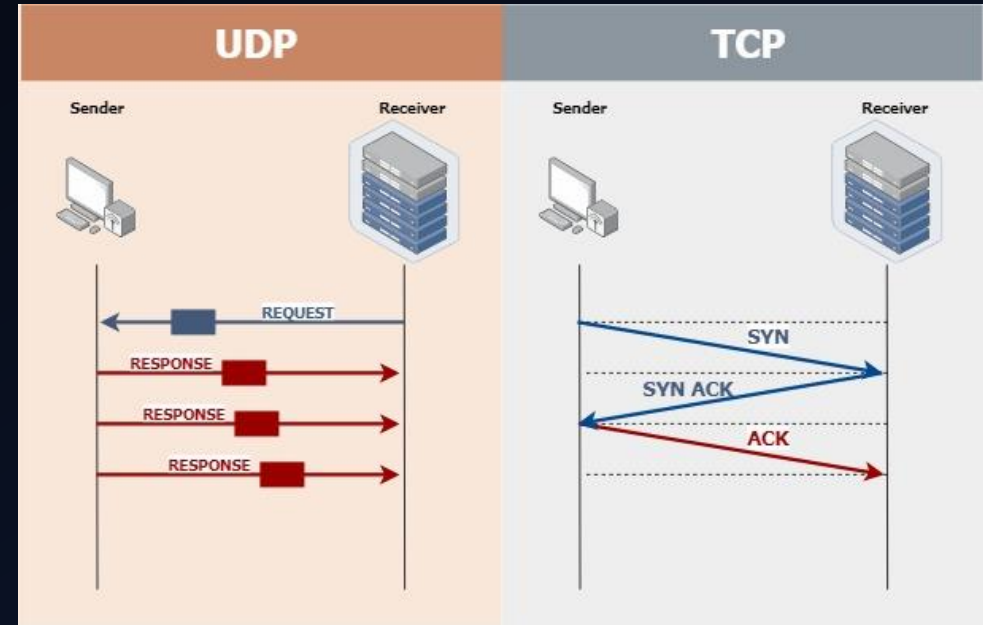
The TCP Handshake

- Before TCP can begin the process of sending data across the network, TCP relies on a “handshake” to set up the conversation between point A and point B.
- This handshake makes TCP “connection oriented,” which means that a connection must be created between the end-stations before TCP communication can proceed.
- This handshake is often referred to as the “three way handshake” because of the three frames that pass back and forth:
- **The First Frame** - The initial synchronize (SYN) frame is sent from the station initiating the conversation to the destination station. The SYN frame includes initial sequence numbers and the port that will be used for the conversation, as well as other initialization parameters
- **The Second Frame** - The destination station receives the SYN frame. If everything is in agreement, it sends an acknowledgement to the SYN (called an ACK) and its own SYN parameters.
- **The Third Frame** - The original station receives the ACK to its original SYN, as well as the SYN from the destination device. Assuming everything is in order, the source station sends an ACK to the destination station’s SYN.
- This handshake occurs every time a TCP session is established. It’s this three-way handshake that allows nmap to gather so much information about the ports on a device.



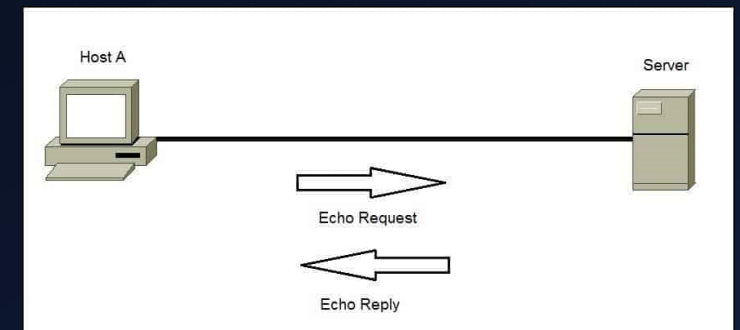
User Datagram Protocol (UDP)

- Datagram protocol also built on top of IP.
- Has the same packet-size limit (64Kb) as IP, but allows for port number specification.
- Provides also 65,536 different ports.
- Hence, every machine has two sets of 65,536 ports: one for TCP and the other for UDP.
- Connectionless protocol, without any error detection facility.
- Provides only support for data transmission from one end to the other, without any further verification.
- The main interest of UDP is that since it does not make further verification, it is very fast.
- Useful for sending small size data in a repetitive way such as time information.



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.
- Commonly, the ICMP protocol is used on network devices, such as routers. ICMP is crucial for error reporting and testing, but it can also be used in distributed denial-of-service (DDoS) attacks.



What are the ICMP message codes?

- ICMP offers feedback and information regarding errors, control messages and management queries.
- The first code field in the **ICMP block** singlehandedly manages to convey a great deal of information.
- Below you can find some of the most relevant values **the first code field** can have and their meaning:
 - 0: **Echo Reply**. It is used for ping.
 - 3: Destination is unreachable.
 - 4: **Source quench**. It means that the router is overloaded.
 - 5: Redirect. It denotes the use of another router.
 - 8: **Echo Request**. Similar to 0, it is used for ping.
 - 9: Router advertisement reply.
 - 10: **Router solicitation**.
 - 11: Time Exceeded. It is used for traceroute.

Scan Types

- **Passive Scan:**
 - Network Traffic Analysis: Wireshark, TCPDump
 - ARP Tables
- **Active Scan:**
 - Nmap
 - Hping
 - Scapy
 - Ping, Tracert etc,



Wireshark

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
45	22.254614682	192.168.56.1	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
46	23.255228685	192.168.56.1	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
47	24.255946708	192.168.56.1	239.255.255.250	SSDP	213	M-SEARCH * HTTP/1.1
48	47.385717018	192.168.56.1	192.168.56.4	SSH	134	Client: Encrypted packet (len=80)
49	47.427566144	192.168.56.4	192.168.56.1	TCP	54	22 → 1074 [ACK] Seq=1697 Ack=593
50	52.158464607	0a:00:27:00:00:17	PcsCompu_21:00:10	ARP	60	Who has 192.168.56.4? Tell 192.168.56.1
51	52.158503859	PcsCompu_21:00:10	0a:00:27:00:00:17	ARP	42	192.168.56.4 is at 08:00:27:21:00:10
52	52.518758829	PcsCompu_21:00:10	0a:00:27:00:00:17	ARP	42	Who has 192.168.56.1? Tell 192.168.56.4
53	52.519084816	0a:00:27:00:00:17	PcsCompu_21:00:10	ARP	60	192.168.56.1 is at 0a:00:27:00:00:17

Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface eth1, id 0

- Ethernet II, Src: 0a:00:27:00:00:17 (0a:00:27:00:00:17), Dst: PcsCompu_21:00:10 (08:00:27:21:00:10)
- Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.4
- Transmission Control Protocol, Src Port: 1074, Dst Port: 22, Seq: 1, Ack: 1, Len: 64
- SSH Protocol

0000 08 00 27 21 00 10 0a 00 27 00 00 17 08 00 45 00 ...!...E.
0010 00 68 89 d0 40 00 80 06 7f 69 c0 a8 38 01 c0 a8 ...h...i...8...
0020 38 04 04 32 00 16 88 8d a2 14 04 97 5b 19 50 18 ...8...2...[...P...
0030 20 10 7e 1e 00 00 eb 07 36 c5 36 b3 e6 63 b9 86 ...6...6...c...
0040 a9 af 81 a6 9b ce 29 73 a7 ca b7 c4 1b 76 1c ec ...)...s)...v...
0050 d5 d8 2a d5 ed b7 72 03 58 78 71 4b 8e 89 0c 66 ...*...r...XxqK...f...
0060 5f 41 a1 31 44 b5 b3 cb 86 ea ce e7 b9 76 00 48 ..._A...1D...v...H...
0070 48 98 88 f1 71 4d H...qM

eth1: <live capture in progress> Packets: 53 · Displayed: 53 (100.0%) Profile

Wireshark - Conversations - eth1

Ethernet · 3 IPv4 · 3 IPv6 TCP · 1 UDP · 4

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
01:00:5e:7f:ff:fa	0a:00:27:00:00:17	12	2,556	0	0	12	2,556	21.252978	243.0046
08:00:27:21:00:10	0a:00:27:00:00:17	67	6,176	34	3,436	33	2,740	0.000000	232.4875
08:00:27:21:00:10	08:00:27:b4:29:fd	4	1,016	2	366	2	650	109.526698	5.2005

☐ Name resolution ☐ Limit to display filter ☐ Absolute start time

Conversation Types

Copy Follow Stream... Graph... Close Help

ARP

```
(mahedi@kali)~$ arp -a
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on eth0
? (192.168.56.1) at 0a:00:27:00:00:17 [ether] on eth1
? (192.168.56.2) at 08:00:27:b4:29:fd [ether] on eth1

(mahedi@kali)~$
```

```
Microsoft Windows [Version 10.0.19041.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Md Mahedi Hasan>arp -a

Interface: 192.168.68.107 --- 0x9
Internet Address      Physical Address      Type
192.168.68.1          e4-c3-2a-1c-e4-1c    dynamic
192.168.68.101        28-3a-4d-1d-0a-a5    dynamic
192.168.68.114        00-21-6a-ff-73-46    dynamic
192.168.68.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
224.0.0.253           01-00-5e-00-00-fd    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0x17
Internet Address      Physical Address      Type
192.168.56.4          08-00-27-21-00-10    dynamic
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Md Mahedi Hasan>
```



What is nmap?

- nmap is a network mapping utility. It will identify any open “doors” or ports that might be available on that remote device.
- Nmap uses TCP/IP protocols to query workstations and the responses are interpreted into useful security information.
- All computers using the TCP/IP family of protocols follow standard processes when initiating network conversations.
- Ideally, these processes would be identical regardless of operating system, software version, or hardware manufacturer.
- In the networking world, however, not every system works exactly the same way. Although these minor differences would usually be considered problematic, nmap takes advantage of these anomalies to provide additional information about the remote system.



History of nmap

- The very first Nmap was only about 2,000 lines of code—and was released in 1997 in issue 51 of Phrack, a hacker "zine" that was started in 1985.
- The general timeline of Nmap development is as follows:
 - At the time of release, Nmap did not have many features; There was no version number attached to this release of Nmap because the developers did not plan to release any future versions. Nmap was designed only to scan for open ports on a target machine, and only worked when run from a Linux host and compiled with gcc.
 - Only four days after the initial release of Nmap, a slightly improved version was released (also through Phrack)—version 1.25
 - By March 1998, about six months after the initial Nmap release, the scanner had become the de facto port scanner of the underground hacker community and information security industry
 - By September 2003, when Nmap 3.45 was released, there had been many major changes to the project. The tool has many new features—such as service detection, OS detection, timing configuration, and optimization flags.
 - In December 2006, one of the most important aspects of the Nmap project was integrated into all Nmap builds: Nmap Scripting Engine (NSE). The NSE allows users of Nmap to write their own modules (in a programming language called Lua) to trigger on certain ports being open, or certain services—or even specific versions of services—found listening. This release allows the elevation of Nmap from a simple networking tool to a fully robust and customizable vulnerability assessment engine, suitable for a wide variety of tasks

The Nmap Scanning Process

- Nmap performs four steps during a normal device scan. Some of these steps can be modified or disabled using options on the nmap command line.
- **Step-1:**
 - If a hostname is used as a remote device specification, nmap will perform a DNS lookup prior to the scan.
 - This isn't really an nmap function, but it's useful to mention since this DNS traffic will appear as network traffic and the query will eventually be noted in the DNS logs.
 - If an IP address is used to specify the remote device, this step never occurs.
 - There's no way to disable a DNS lookup when a hostname is specified, unless the hostname and IP address is found in a locally maintained name resolution file such as hosts or lmhosts.

The Nmap Scanning Process

– Step-2:

- Nmap pings the remote device. This refers to the nmap “ping” process, not (necessarily) a traditional ICMP echo request.
- This ping process can be disabled with the `-P0` option.

– Step-3:

- If an IP address is specified as the remote device, nmap will perform a reverse DNS lookup in an effort to identify a name that might be associated with the IP address.
- This is the opposite process of what happens in step 1, where an IP address is found from a hostname specification.
- If this reverse lookup process isn’t required or desired, it can be disabled with the `-r` option.

– Step-4:

- Nmap executes the scan. Once the scan is over, this four-step process is completed
- If the scan is interrupted (with CTRL-C), an “interrupt” process performs a cleanup to close any log files and halt nmap. If the scan is resumed (with the `--resume` option), nmap uses the log file information to begin scanning from the previous location. A normal (`-oN`) or grepable log file (`-oG`) option must be specified to resume the scanning process

Using nmap from the Command Line

- The command line syntax for nmap is similar to any other command line-based utility.
- Each option is specified one after another on the same line, separated by a space and in no particular order.
- Nmap uses Unix-style command line syntax by preceding option abbreviations with a single hyphen (-) and non-abbreviated options with two hyphens (--).
- The nmap command:

```
(mahedi@kali)-[~]  
└─$ nmap scan.nmap.org  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-16 23:57 +06  
Nmap scan report for scan.nmap.org (45.33.49.119)  
Host is up (0.26s latency).  
Other addresses for scan.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061  
Not shown: 996 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
25/tcp    open  smtp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 13.96 seconds
```



Nmap Target Specifications

- Nmap provides many methods of specifying a scan target. The target specification can be placed anywhere on the command line.
- A single IP address or hostname can be specified on the command line without any wildcards or lists. For example, the command `nmap 192.168.1.5` will perform an nmap scan to the 192.168.1.5 address.
- A group of hosts can be specified in “slash notation,” sometimes referred to as a Classless Inter-Domain Routing (CIDR, pronounced “cider”) block notation.
- The term slash notation refers to the forward-slash that is placed between the IP network address and the number of subnet mask bits.
- A host specification of `192.168.1.5/24` references a subnet mask of 24 bits, which would scan everything between 192.168.1.0 and 192.168.1.255.

Nmap Target Specifications

- Hyphens, commas, and asterisks can also be used to create a list of hosts. The nmap host specification of 192.168.1-2.* would scan everything between 192.168.1.0 and 192.168.2.255.
- This could also be specified as 192.168.1,2.0-255, or as 192.168.1-2.1,2-5,6-255.
- The nmap man page throws another twist to the target specification by specifying the networks as the variable values. For example, *.*.1.5 would scan all devices between 1.0.1.5 and 255.255.1.5 (that's a total of 65,535 possible devices!).



Privileged Access

- To have access to all possible options, nmap should always be run by a privileged user.
- A system's privileged users can create custom Ethernet packets that bypass the checks that are normally done by the operating system.
- With these custom “raw” packets, nmap can manufacture packet header combinations that induce unique responses from the remote stations.
- These responses then provide nmap with much more information than would normally be available to a non-privileged user
- On a Unix-based system, privileged access means that nmap should run as root, and on Windows-based systems nmap should have Administrator rights.
- Lack of privileged access doesn't mean that nmap won't work, but certain scanning methods and program options will not be available

Nmap Scan Summary

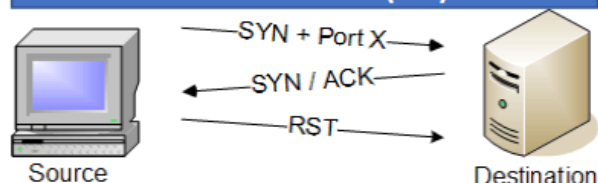
- This chart summarizes the nmap scans and compares the usability for privileged users. The chart also includes a summary of which scans identify TCP ports, and which identify UDP ports.

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

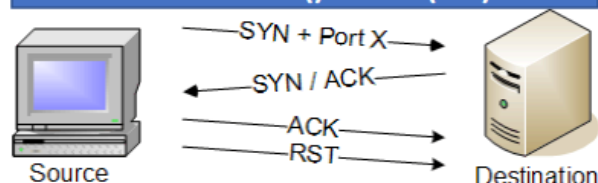
Nmap Scan Summary

Identifying Open Ports with Nmap

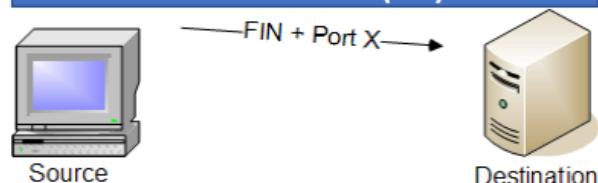
TCP SYN SCAN (-sS)



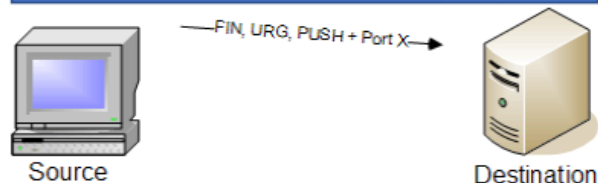
TCP connect() SCAN (-sT)



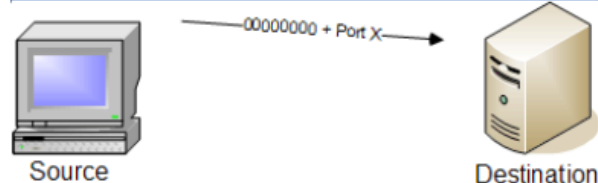
TCP FIN SCAN (-sF)



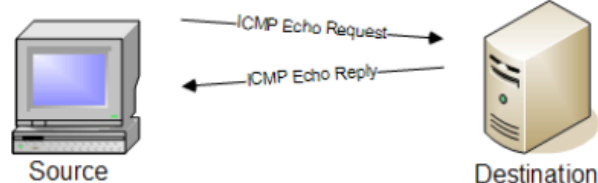
TCP XMAS TREE SCAN (-sX)



TCP NULL SCAN (-sN)

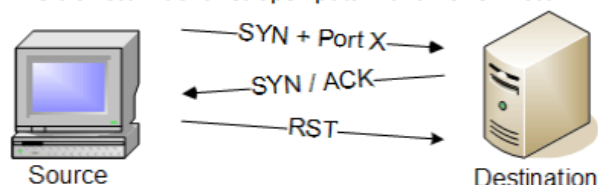


TCP PING SCAN (-sP)

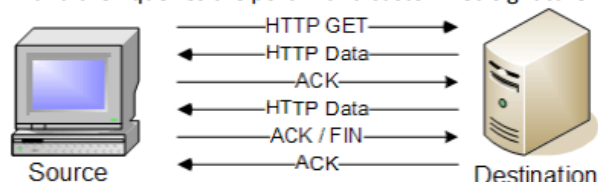


VERSION DETECTION SCAN (-sV)

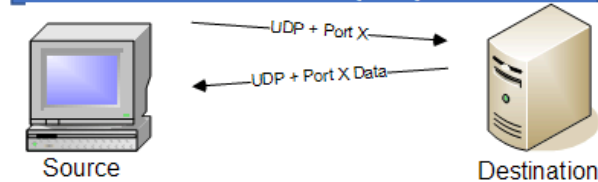
Version scan identifies open ports with a TCP SYN scan...



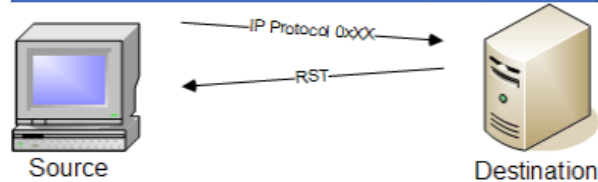
...and then queries the port with a customized signature.



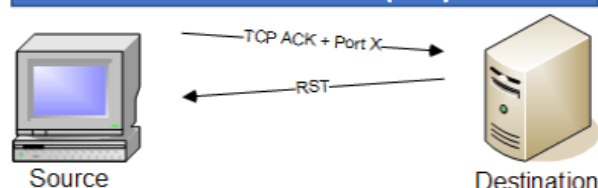
UDP SCAN (-sU)



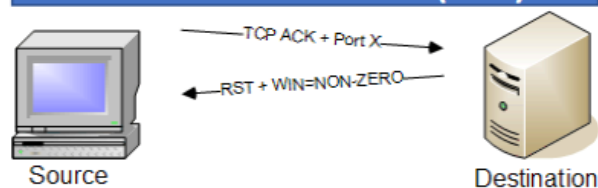
IP PROTOCOL SCAN (-sO)



TCP ACK SCAN (-sA)



TCP WINDOW SCAN (-sW)





Thank You

?