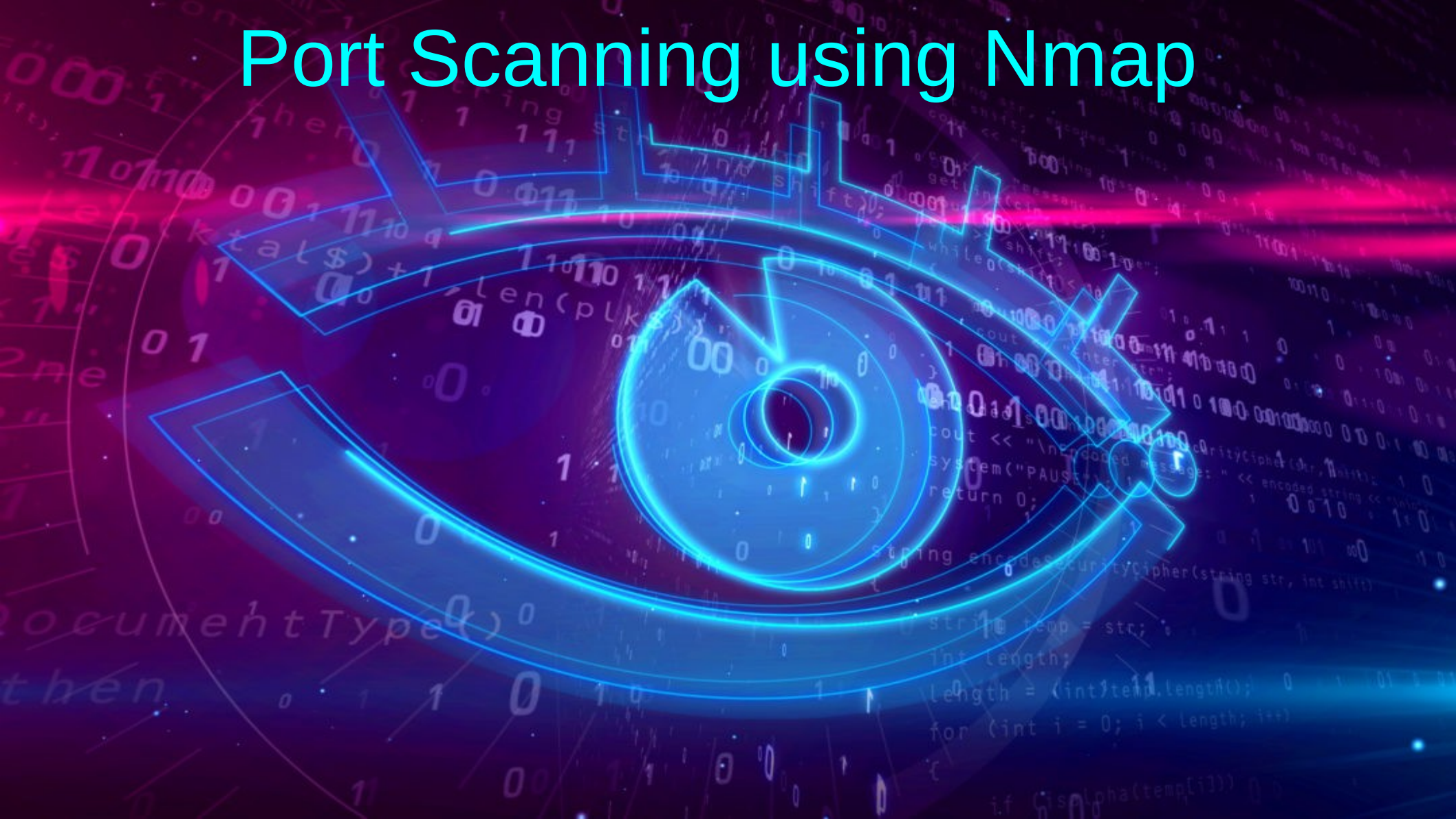
Port Scanning using Nmap



Acknowledgements

- Most of the content,photos have been taken from the below two websites.
- The second website is the official nmap website where you get to know many things about nmap.
- https://tryhackme.com/room/furthernmap
- https://nmap.org/

AGENDA

- Getting to know about ports and port scanning.
- Introduction to Nmap and its uses.
- Getting to know about the basic commands of Nmap.
- Introduction to different portscanning techniques
    - Tcp scanning.
    - Syn scanning.
    - Udp scanning.
    - Window.Fin,X-mas scanning etc.
- Getting to know about inbuilt scripts etc..where you can get to know the commands used to detect Version,OS etc..of a host.
- Demo: Here Iam going to access some files of an unsecured computer.

What are ports and port numbers ?

- Port is a virtual point which connects transport layer to the application layers and vice versa. It has a bi-directional flow.

What are Port numbers and why should we use them ?

- There are a total of 2^16 ports ranging from 0-65,536.
- Each of the port is numbered and that number is called port number.
- Each port is numbered in order to differentiate the function performed by an application which helps in segregating different programs which helps in speeding up the processes.
- Ports 0 to 1023 are well known port numbers that are designed for Internet use and are reservered for certain processes.
- Numbers 1024 through 49151 are considered “registered ports” meaning they are registered by software corporations. Ports 49,151 through 65,536 are dynamic and private ports - and can be used by nearly everyone.

Some of the well known port numbers

- Port 21 holds File Transfer Protocol (FTP) used for data transfer.
- Port 22 holds Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding.
- Port 53 is the Domain Name System (DNS) which translates names to IP addresses.
- Port 80 is the World Wide Web HTTP.
- Port 443 is for HTTPS.

PORT SCANNING

What is port scanning ?

- Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process of sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

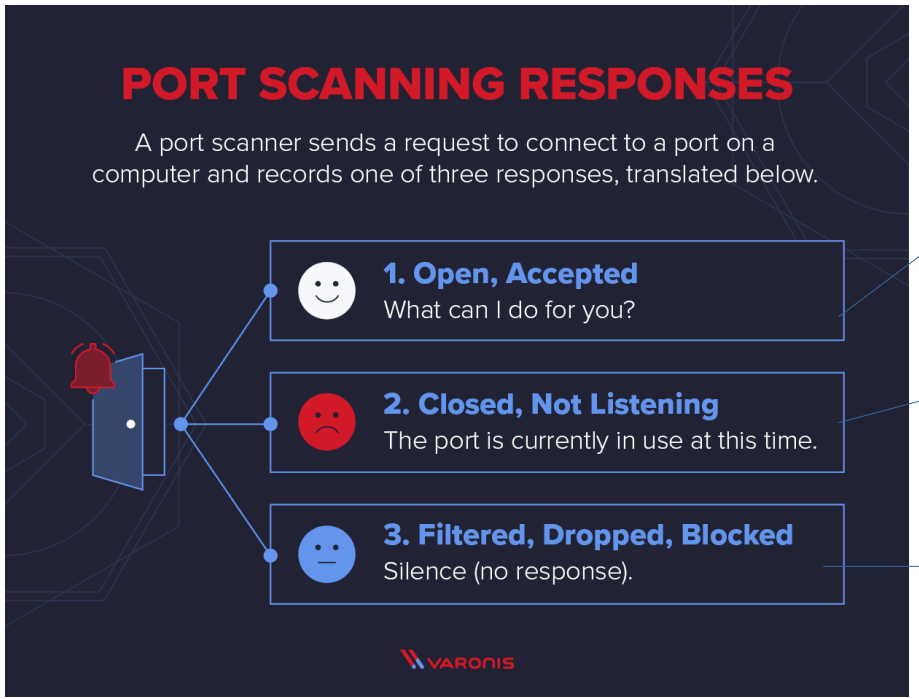
Goal of port scanning ?

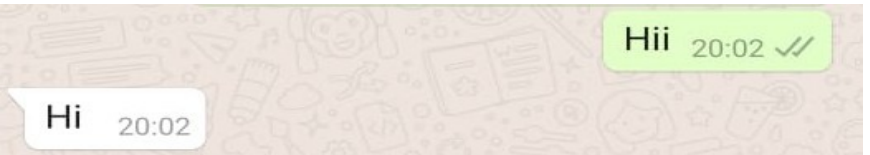
- Used to find working ports (open), closed ports etc.. on a network.
- Can be used to find vulnerabilities on a host/server.It is widely used in small networks to analyse ports and find vulnerabilities.
- The above point implies that we can improve the security level of a particular system by getting rid of the known vulnerabiliteies.

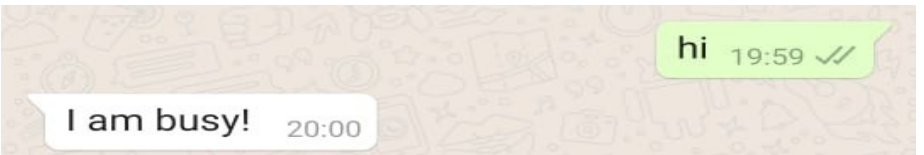
Port scanning

https://ccna-200-301.online/wp-content/uploads/2020/08/Performing-Port-Scans.gif

Port scanning responses







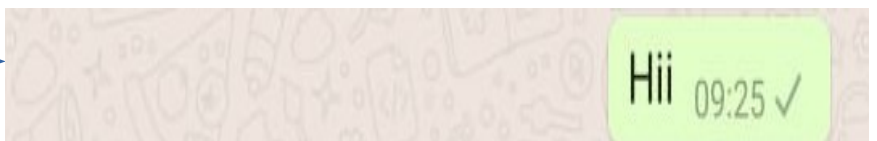


Image : https://blogvaronis2.wpengine.com/wp-content/uploads/2020/11/how-a-port-scanner-works.png

What type of results can you get from port scanning?

Port scan results reveal the status of the network or server and can be described in one of three categories: open, closed, or filtered.

Open ports: Open ports indicate that the target server or network is **actively accepting connections or datagrams and has responded with a packet that indicates it is listening.** It also indicates that the service used for the scan (typically TCP or UDP) is in use as well.Finding open ports is important to do any kind of activity.

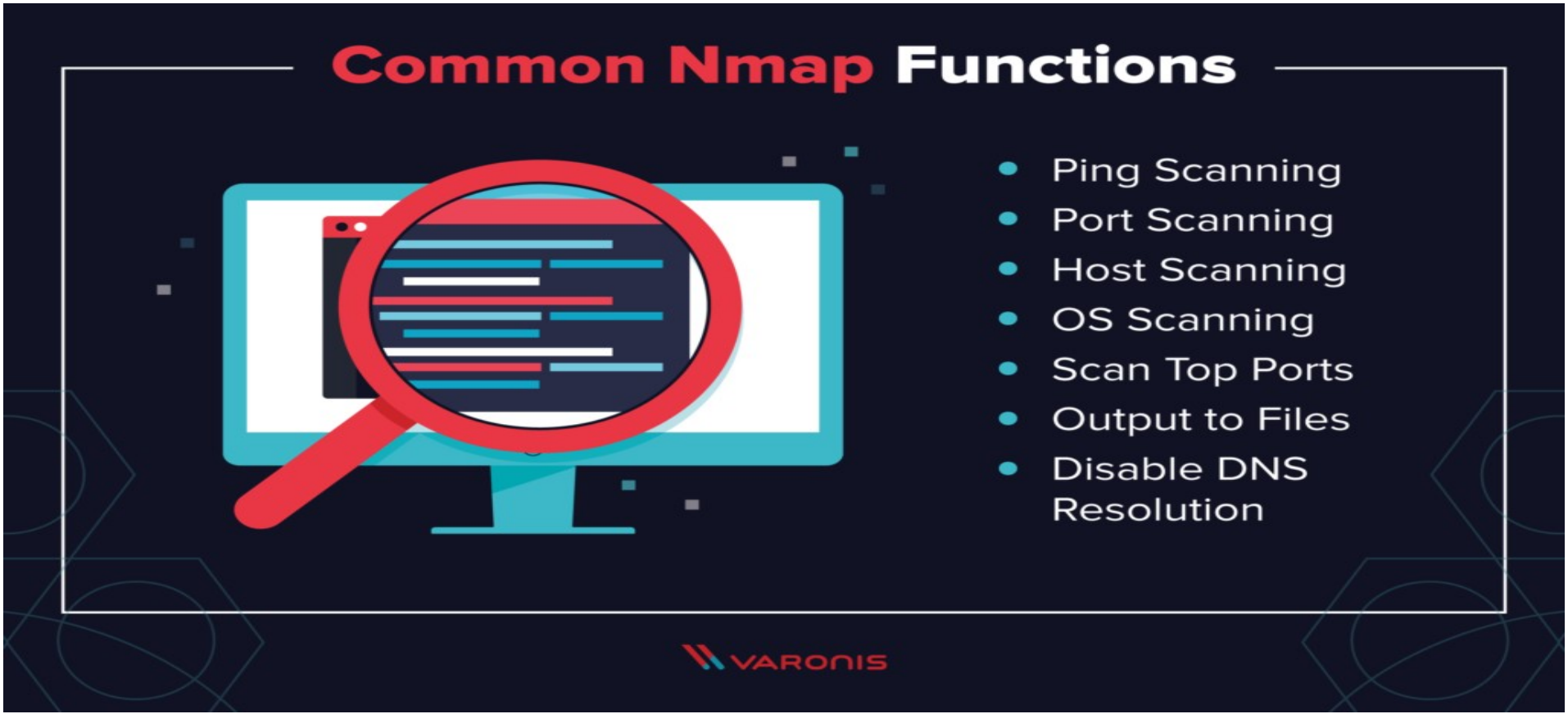
Closed ports: Closed ports indicate that the server or network received the request, **but there is no service "listening" on that port.** A closed port is still accessible and can be useful in showing that a host is on an IP address.

Filtered ports: Filtered ports indicate that a request packet was sent, but the host **did not respond and is not listening.** This usually means that a request packet was filtered out and/or **blocked** by a **firewall**. If packets do not reach their target location, attackers cannot find out more information. Filtered ports often respond with error messages reading "destination unreachable" or "communication prohibited.

NMAP src-Wikipedia

- Nmap (Network Mapper) is a free and open-source network scanner released in 1997.
- created by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich).
- Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses.

Functions of NMAP



https://blogvaronis2.wpengine.com/wp-content/uploads/2019/12/nmap-commands-1024x640.png

Host discovery

- nmap 192.168.0.1 - Scanning a specific host
- nmap 192.168.1.1-254 - Scanning a range of hosts
- nmap google.com - Scanning a specific domain
- nmap 192.168.1.1/24 - Scanning a range of IP’S using CIDR
- nmap –iR 100 - Scan 100 random hosts

Port Scanning

- nmap 192.168.1.1 -p 21-100 - scan ports of this range
- nmap 192.168.1.1 -p- - scan all ports of the host
- nmap 192.168.1.1 -F - Fast scan (scan 100 ports)
- nmap 192.168.1.1 -T5 - This is used to speed up the process of scanning

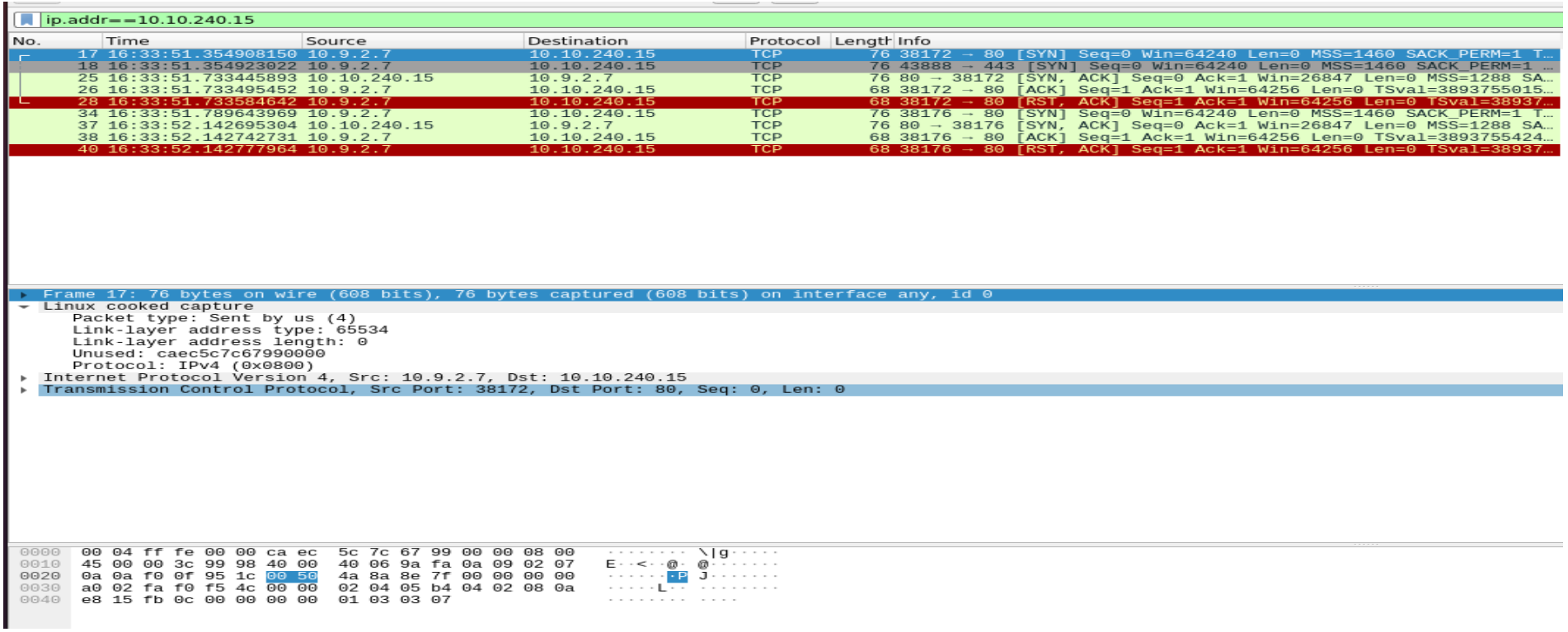
DIFFERENT PORT SCANNING TECHNIQUES

- Tcp scanning.
- Syn scanning.
- Udp scanning.
- Window,Fin,X-mas scanning etc

TCP Scanning

- This process of scanning a port takes place through a threeway TCP handshake process.
- In the first step host sends a syn packet .
- In the next step If the server is open It send SYN,ACK packet else it sends RST(reset) packet.
- After recieving a syn,ack packet host sends RST,ACK packet and resets or closes the connection.
- Command to perform this on a host :
  nmap -sT 192.168.0.0

TCP scanning results in wireshark



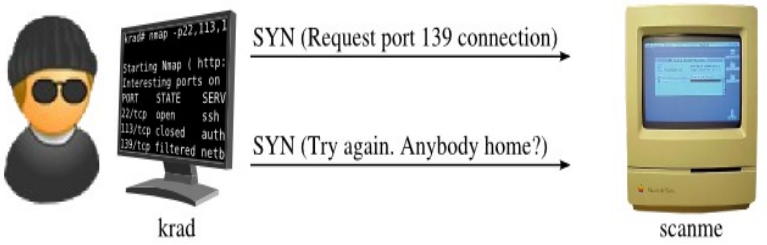
SYN Scanning

- This is a type of TCP scan also called as half open scanning or "Stealth" scans.
- First source sends a SYN packet.
- The server responds with a SYN,ACK packet.
- Then the source sends a RST packet without creating a connection.
- Command to perform this on a host :

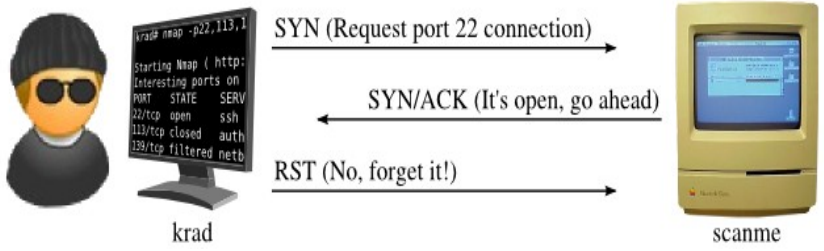
  nmap -sS 192.168.0.0

SYN Scanning

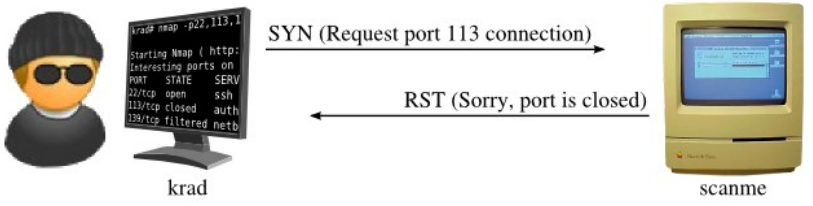
- SYN scan of filtered port 139



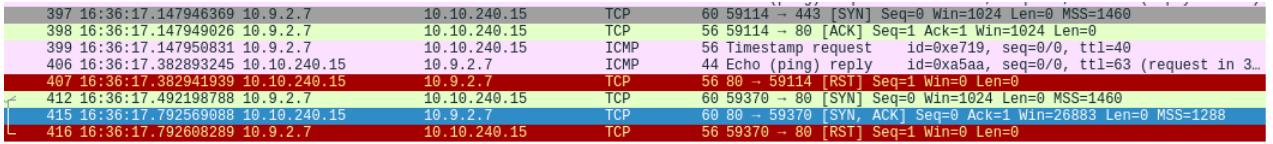
- SYN scan of open port22

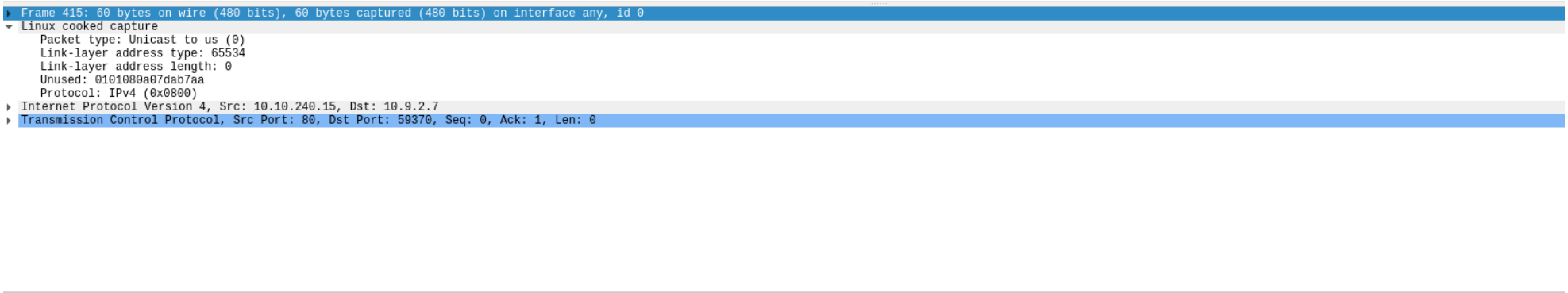


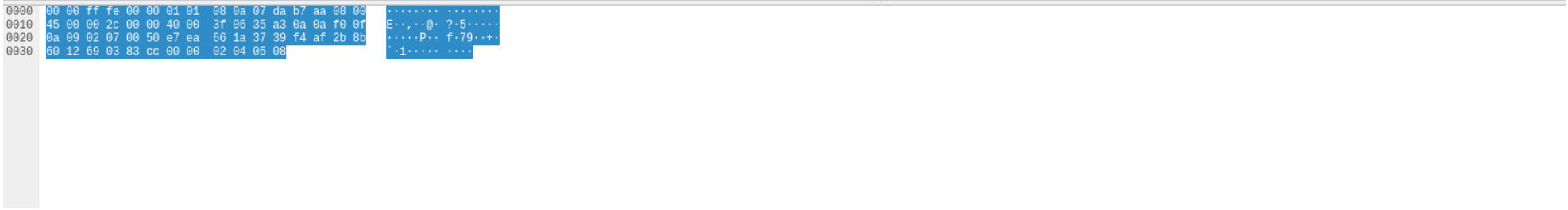
- SYN scan of closed port 113



SYN scanning results in wireshark







UDP Scanning

- It’s a connectionless protocol.
- The source sends a UDP packet and gets a response if a port is open.
- If the port is closed it sends a ICMP port unreachable message.
- Command to perform this on a host : nmap -sU 192.168.0.0

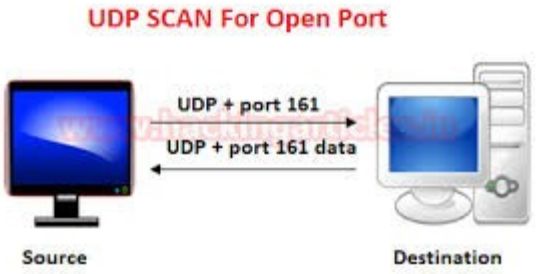
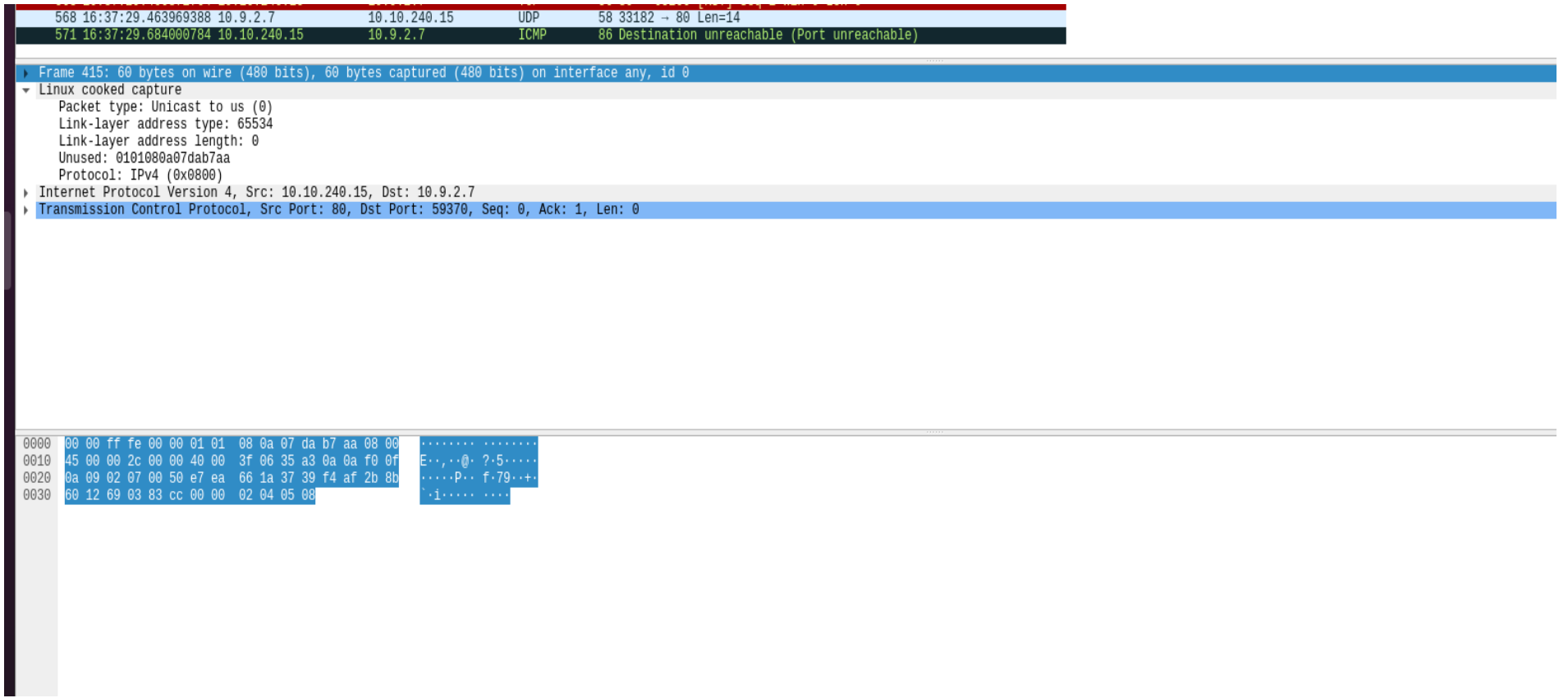


Table 5.3. How Nmap interprets responses to a UDP probe

Probe Response	Assigned State
Any UDP response from target port (unusual)	`open`
No response received (even after retransmissions)	`open|filtered`
ICMP port unreachable error (type 3, code 3)	`closed`
Other ICMP unreachable errors (type 3, code 1, 2, 9, 10, or 13)	`filtered`

UDP scanning results in wireshark



ACK Scanning

- It is mainly use to find whether there is a firewall or to know if any sources are blocking the packet from reaching the server.
- open and closed ports will both return a RST response.
- So we cannot differentiate open and close packets.
- Command to perform this on a host :
  nmap -sA 192.168.0.0

Table 5.5. How Nmap interprets responses to an ACK scan probe

Probe Response	Assigned State
TCP RST response	`unfiltered`
No response received (even after retransmissions)	`filtered`
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	`filtered`

Window Scanning

- Window scan is exactly the same as ACK scan except that it returns open and closed ports. It does this by examining the TCP Window value of the RST packets returned. On some systems, open ports use a positive window size (even for RST packets) while closed ones have a zero window.

Probe Response	Assigned State
TCP RST response with non-zero window field	open
TCP RST response with zero window field	closed
No response received (even after retransmissions)	filtered
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	filtered

Null Scan

- Sends a packet with no flag and host responds with RST if closed.

FIN scan

- Same as above but sends a FIN flag

Table 5.4. How Nmap interprets responses to a NULL, FIN, or Xmas scan probe

Probe Response	Assigned State
No response received (even after retransmissions)	`open|filtered`
TCP RST packet	`closed`
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13)	`filtered`

Version,OS detection

- nmap 192.168.1.1 –sV - Used to detect version of the service running on port.
- nmap 192.168.1.1 –A - Enables os detection ,version detection,script scanning, traceroute.
- nmap 192.168.1.1 -O - Remote OS detection using TCP/IP stack fingerprinting

How is OS detected?

- In this process we send different kinds of packets with different flags at different intervels.

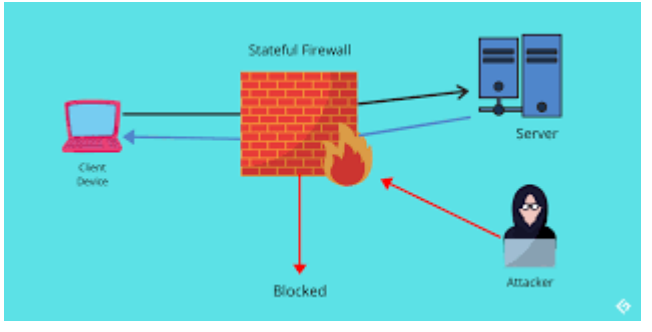
- It analyses all the data and format received from these packets(TTL,Window size,Packet size,DF bit,TOS) and tries to match these with a database that is nmap-os-db database of more than 2,600 known OS fingerprints and prints the one which matches the most.

NSE
NMAP Scripting Engine

- NSE scripts are very powerful.
- These are mostly written in Lua programming language.
- These scripts can perform different processes which are used to know vulnerabilities of a host ,os,version
- These scripts are found in /usr/share/nmap/scripts. In a computer installed with nmap.

How to prevent port scanning

- Install a Firewall: A firewall can help prevent unauthorized access to your private network. It controls the ports that are exposed and their visibility. Firewalls can also detect a port scan in progress and shut them down.



- TCP Wrappers: TCP wrapper can give administrators the flexibility to permit or deny access to the servers based on IP addresses or domain names.
- One of the best and foremost thing is to perform a NMAP scan on yourself and find vulnerabilities by yourself and solve them.“prevention is better than cure”.


THE END