Auguast 15, 2015

Pin Pechdara
Network Engineer

Nmap

Agenda

- What is Nmap?
- Process of Nmap
- Scanning techniques
- Dectect OS with Nmap
- Host and Port Option
- Real Time Information
- Timing Option
- Logging Information

What is Nmap?

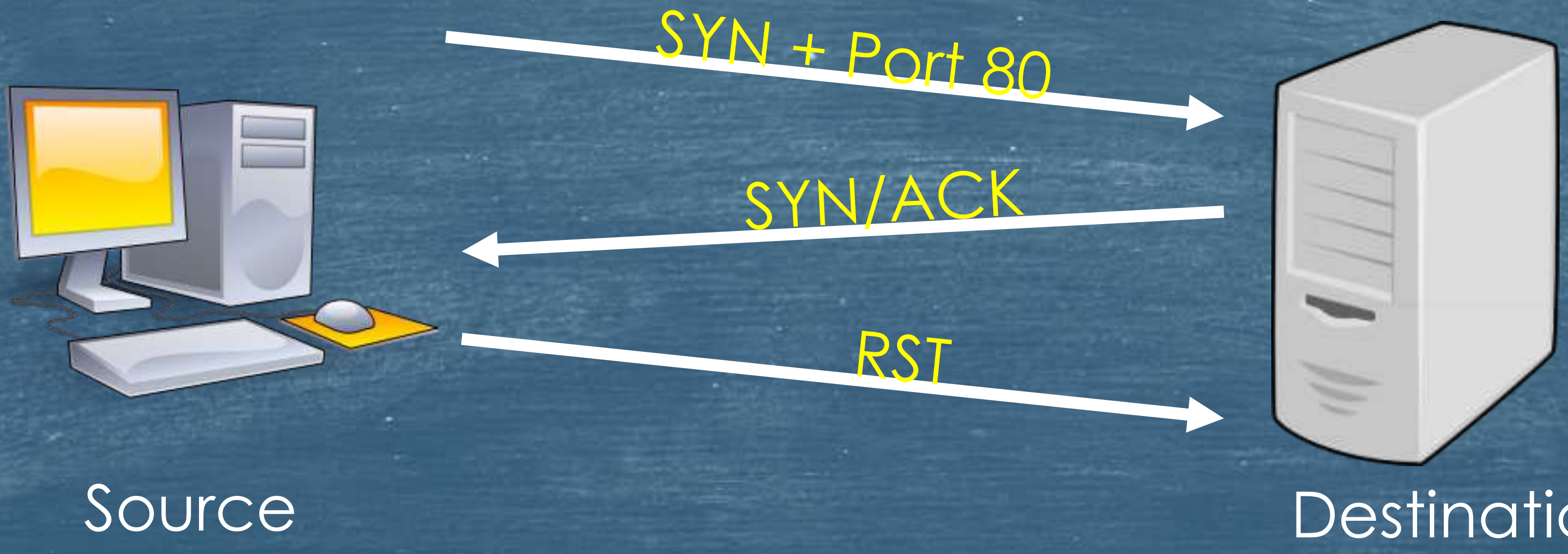
- Nmap is a free and open source utility for network discovery and security auditing.
- Latest version of nmap is 6.49BETA2
- Nmap supports all platform of OS like
  - ❑ Linux/Unix
  - ❑ Microsoft
  - ❑ Mac

Process Nmap

1. If hostname use as target, nmap will perform dns lookup to scan. But if ip address use as target, dns lookup will not process
2. Nmap pings the romote device. Can disable ping with option **(-Pn)**
3. If IP address is specified as the remote host, Reverse DNS will occur. We can use option **(-n)** to disable if we think it is not necessary
4. Nmap executes the scan.

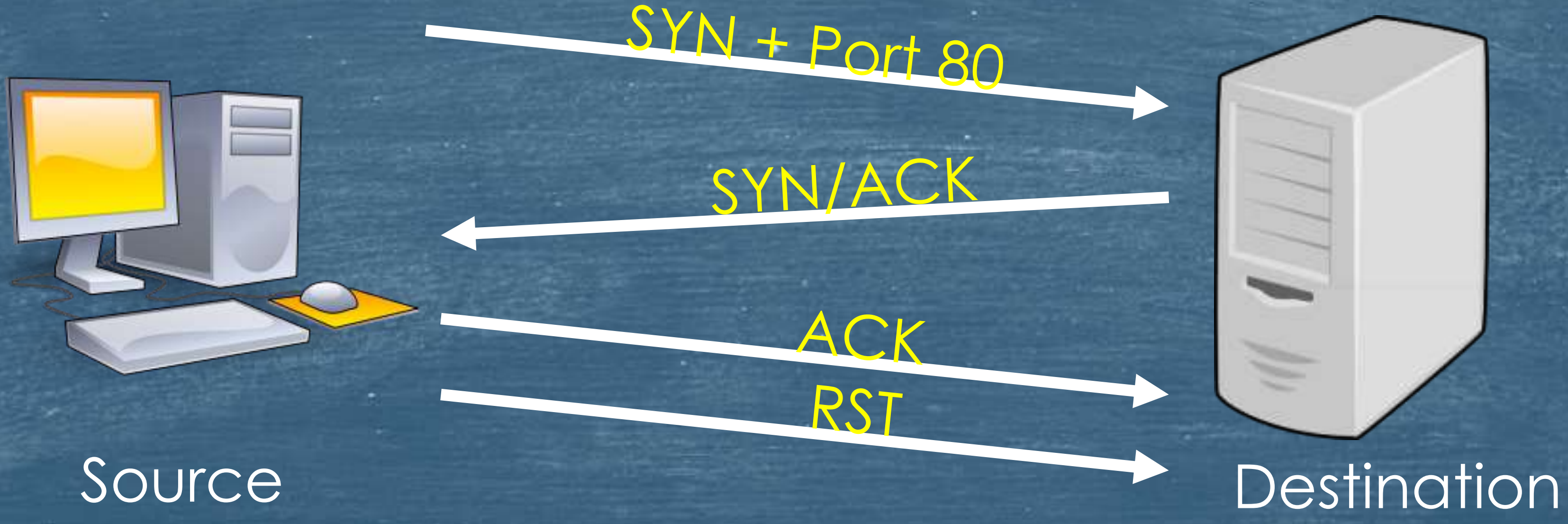
TCP SYN Scan (-sS)

- Allow nmap to gather information about open ports without completing the TCP handshake process.
- By default if nmap scan option isn't specified on the command line, TCP SYN scan is use
  #namp --sS -v 192.168.1.100



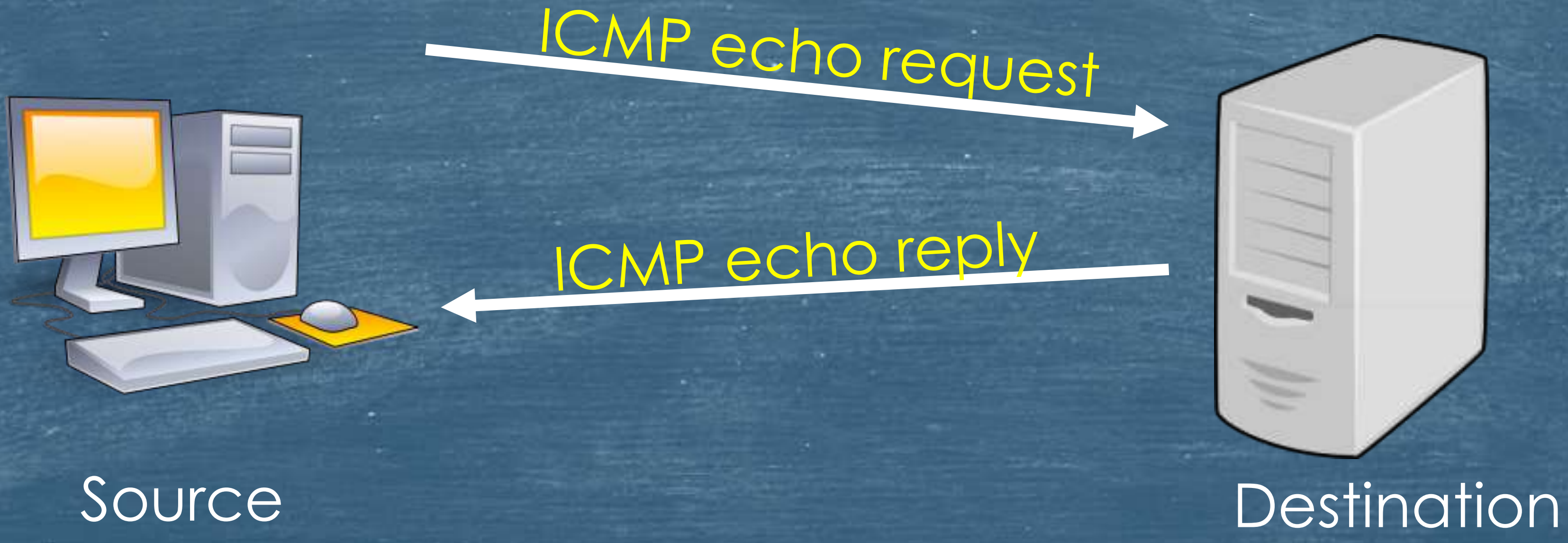
TCP SYN Scan (-sT)

- Allow nmap to gather information about open ports with completing the TCP handshake process.
- nmap –sT –v 192.168.1.100



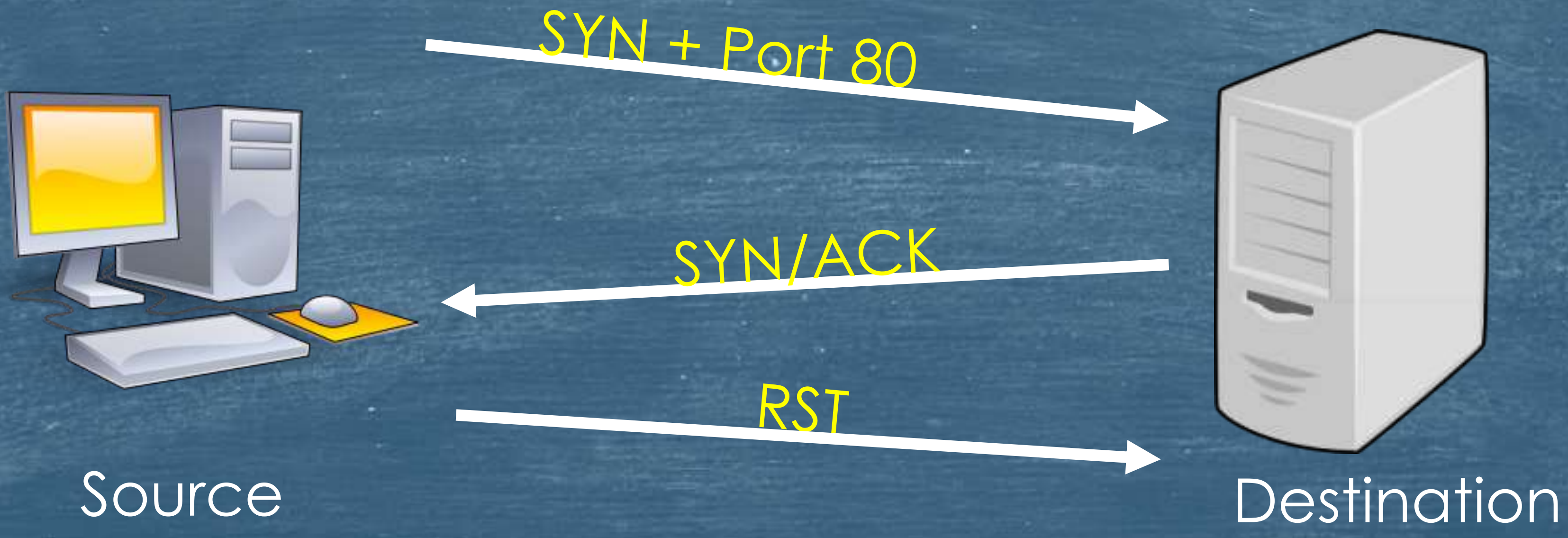
Ping Scan (-sP)

- Ping Scan is a quickest scan that nmap perform.
- It is useful to determine remote hosts are up or down.
  #nmap -v -sP 192.168.1.100 --packet_trace



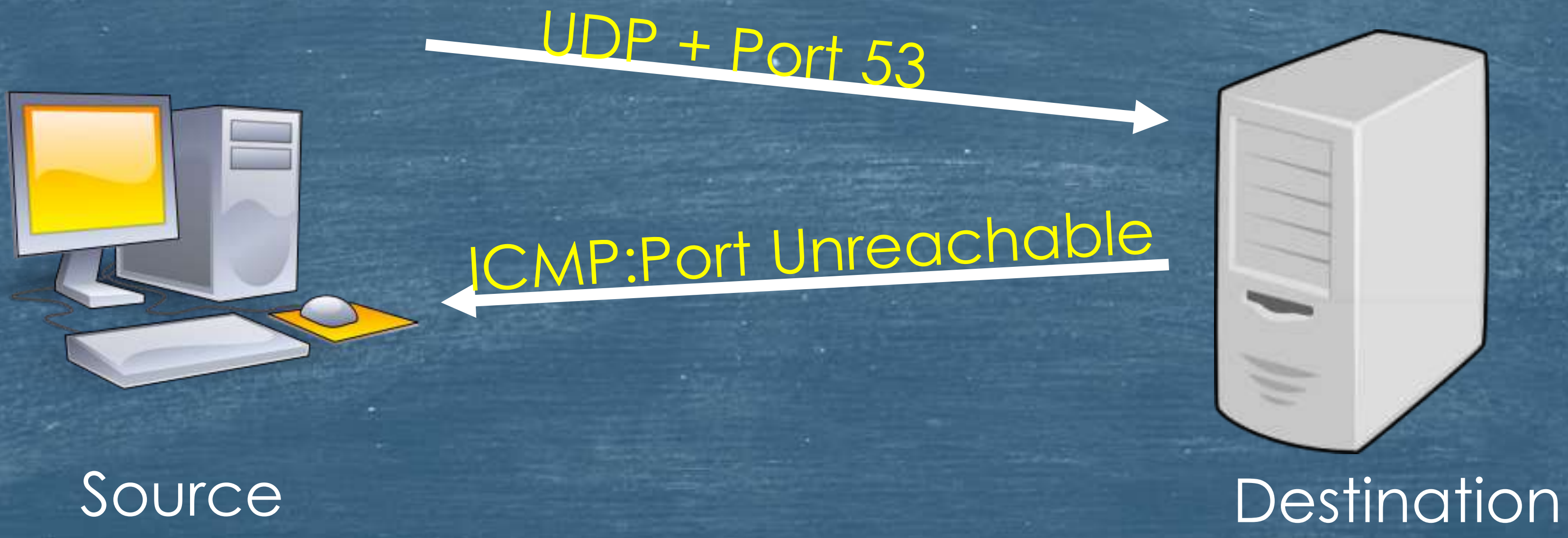
Version Detection (-sV)

- Allow nmap to gather version of application of remote host
- The version detection scan runs automatically if the Aggressive Scan (-A) is selected.
- -sP, -sL, -sO will not run the same command line with version detection



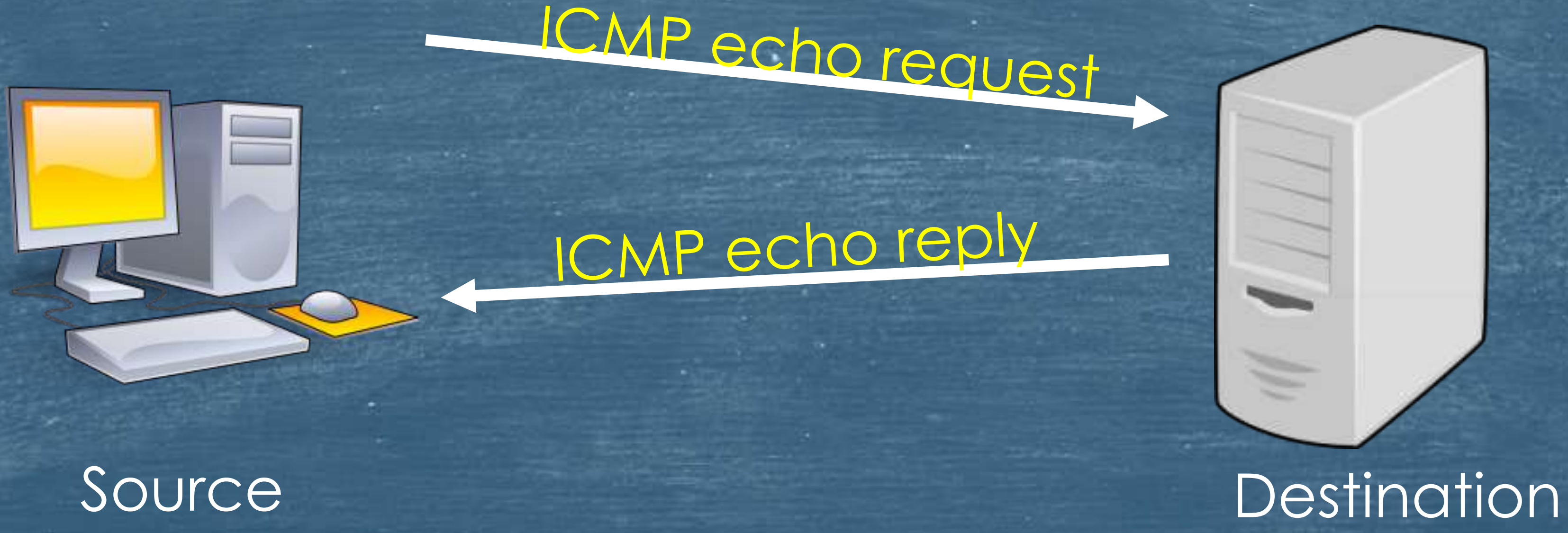
UDP Scan (-sU)

- UDP has no need to process 3 way handshake or SYN, FIN, and RST.
  #nmap -sU -v 192.168.1.100 --packet_trace



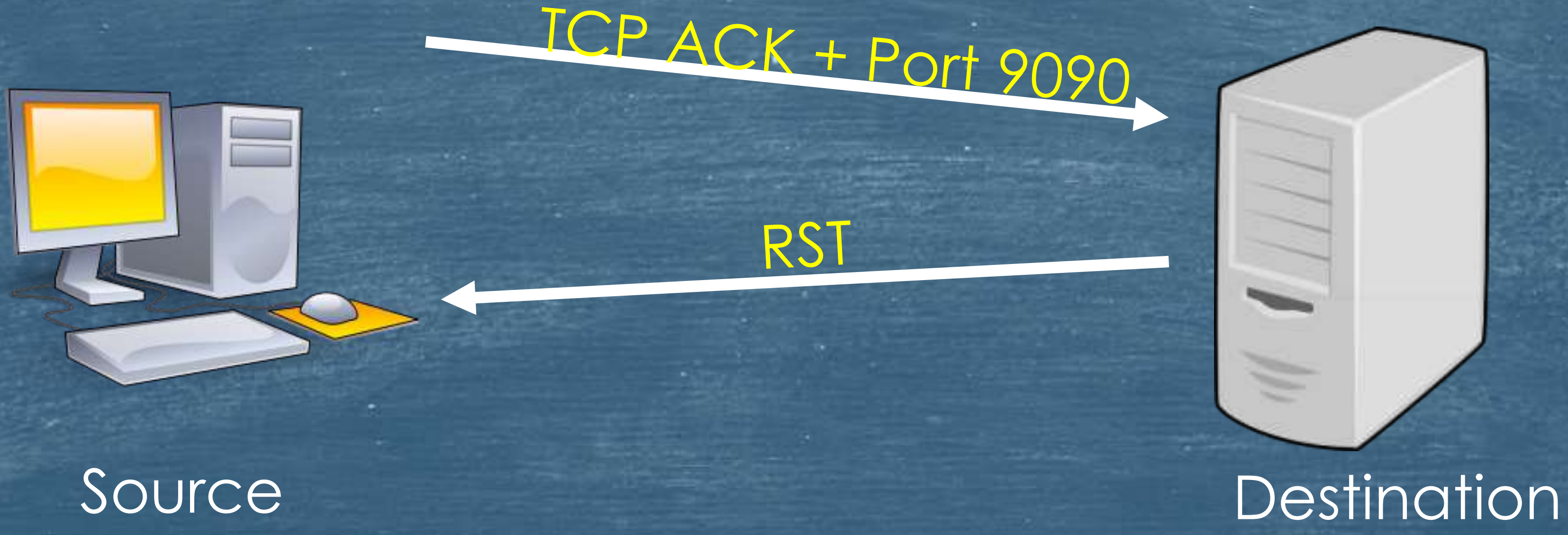
IP Protocol Scan (-sO)

- The IP Protocol Scan attempt to determine IP Protocol support on target.
  #nmap -v -sO 192.168.1.100 --packet_trace



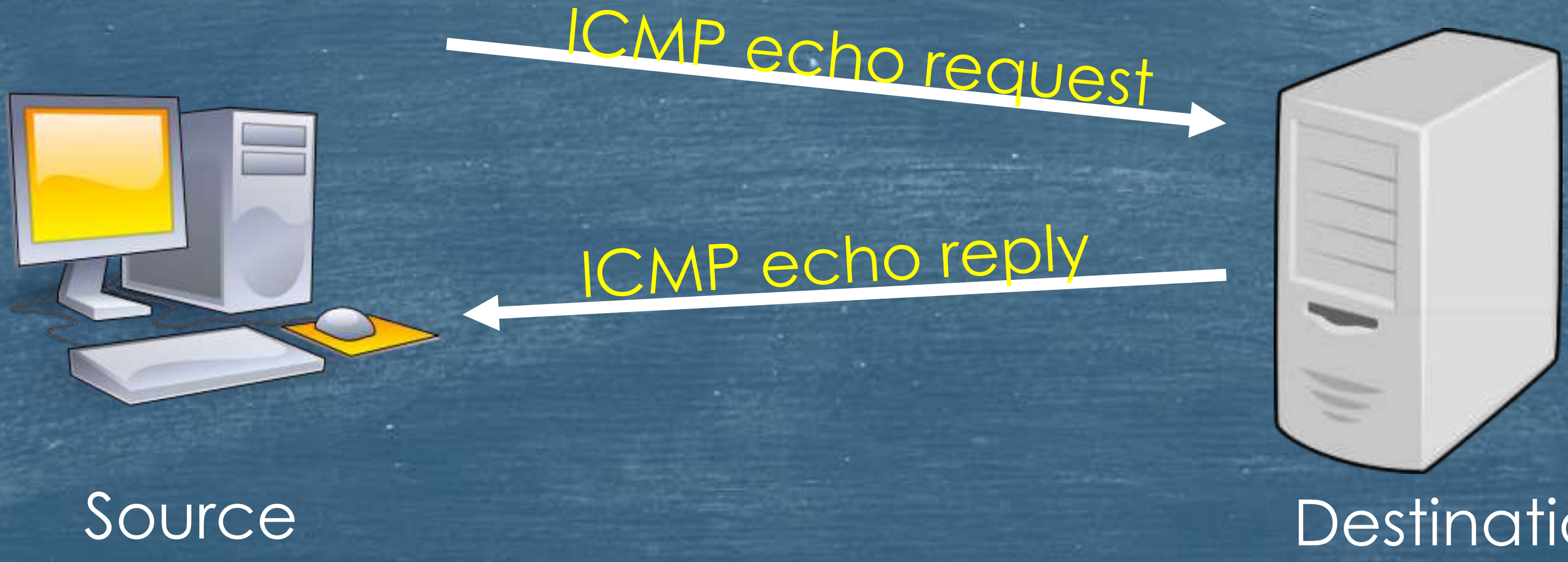
ACK Scan (-sA)

- ACK Scan to determine port filter or unfilter
  #nmap -sA -v 192.168.1.100



Window Scan (-sA)

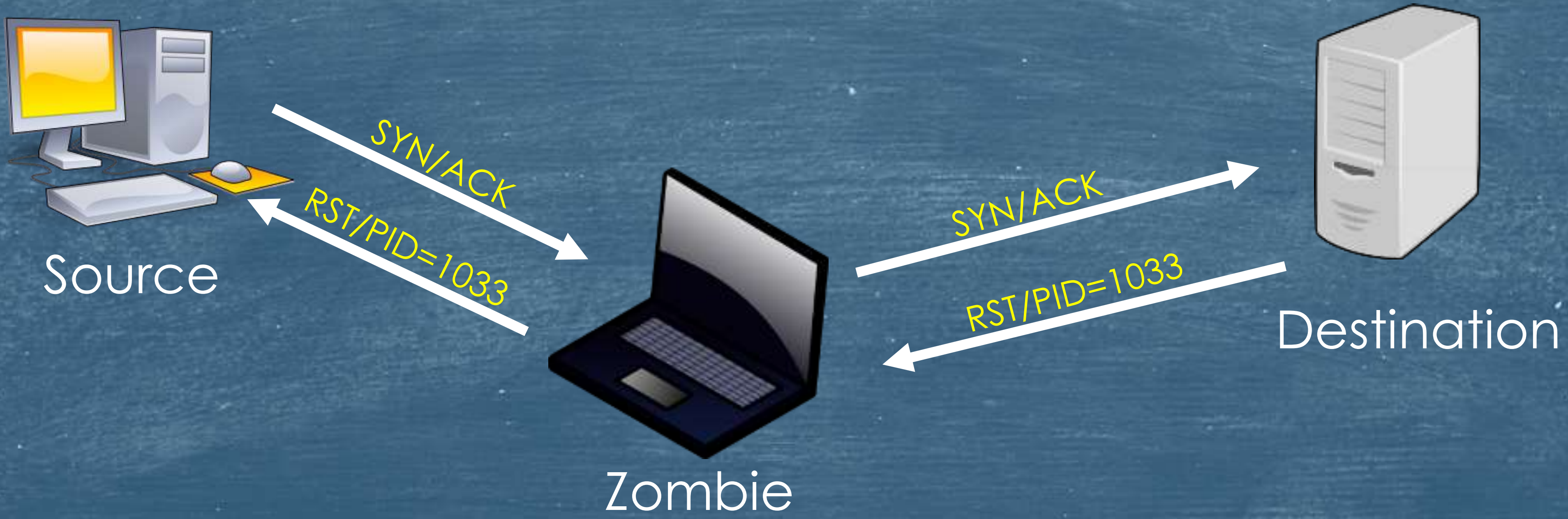
- Allow nmap to gather information about open ports without completing the TCP handshake process.
- The version detection scan runs automatically if the Aggressive Scan (-A) is selected.
- -sP, -sL, -sO will not run the same command line with version detection



Idlescan (-sI)

- Idle Scan use other station to scan remote host device

```
#nmap -sI -v 192.168.1.50 192.168.1.100
```



How to Detect OS with Nmap

- Technically, nmap provide the rich feature that offer us to dectect what OS that remote devices are used.
- By using below additional options we can get what OS of remote host
  - ❑ OS fingerprint with option (-O)

    ```
    #nmap -sS -O 192.168.1.100
    ```

  - ❑ Additional, Advance, and Aggressive (-A)
    Note: shortcut for running (-O) & (-sV)

    ```
    #nmap -sS -A 192.168.1.100
    ```

Host and Port options

- Except Target
  - ❑ Exclude Targets (--exclude host1,host2,….)
    This option provide nmap to avoid scanning specific hosts that are not necessary
    #nmap -v -sS 192.168.1.0/24 --exclude 192.168.1.1-10
  - ❑ Exclude Targets in File (--excludefile <filename>)
    This option provide nmap to avoid scanning specific hosts from file.
    #nmap -v -sS 192.168.1.0/24 --ecludefile except_IP.txt

- Include Target
  - ❑ Read Targets from File (-iL <filename>)
    This option provide name to scan specific host from file.
    #nmap -v -sS 192.168.1.0/24 -iL IP_Scan.txt

Host and Port options (Cont)

- Specify Port Protocol or Port Number (-p <port_range>)
  by using this option, it provides nmap to scan specific port rather than scan all port (1000 ports)
  #nmap -v -sS -p 80 192.168.1.100 (-p dedicate to TCP port number)
  #nmap -v -sO -p 6 192.168.1.100 (-p dedicate to protocol number)
  #nmap -v -sU -p 6 192.168.1.100 (-p dedicate UDP Port number)

Real Time Information

- While Nmap is processing to scan remote host device, there are a lot of activities behind what we seen on screen.
- So we use additional option to see slightly with :
  - ❑ Verbose Mode (--verbose, -v)
    #nmap -sS -v 192.168.1.100
  - ❑ Packet Trace (--packet_trace)
    #nmap -sS -v 192.168.1.100 --packet_trace

Timing Option (--timing, -T <0-5>)

Category	Initial_rtt_timeout	Min_rtt_timeout	Max_rtt_timeout	Max_parallelism	Scan_delay	Max_scan_delay
T0/Paranoid	5 min	Default 100ms	Default 10 sec	serial	5 min	Default 1 sec
T1/Sneaky	15 Sec	Default 100ms	Default 10 sec	serial	15 sec	Default 1 sec
T2/Polite	Default (1 Sec)	Default 100ms	Default 10 sec	serial	400ms	Default 1 sec
T3/Normal	Default (1 Sec)	Default 100ms	Default 10 sec	parallel	0 sec	Default 1 sec
T4/Aggressive	500ms	100ms	1,250ms	parallel	0 sec	10ms
T5/Insane	200ms	50ms	300ms	parallel	0 sec	5ms

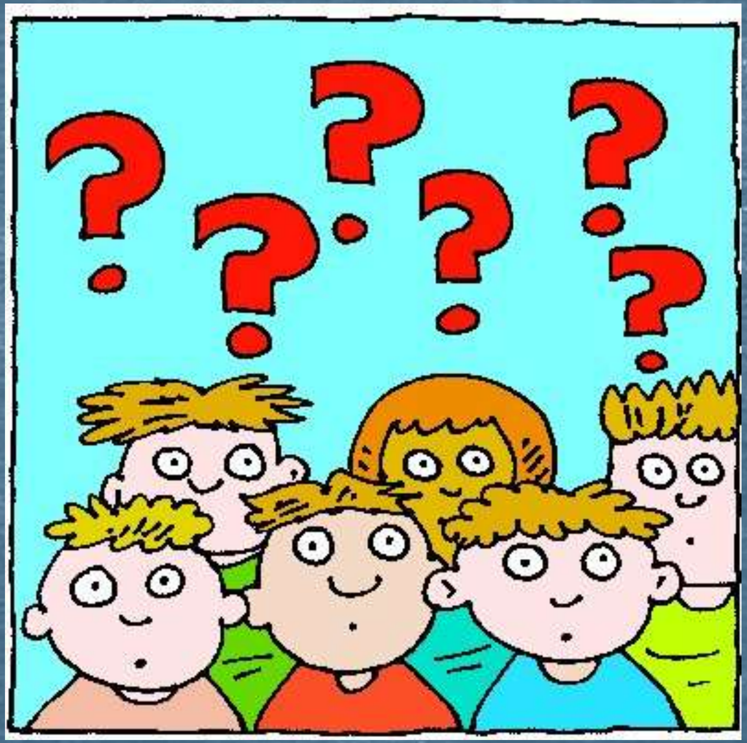
```
#nmap -sS -v 192.168.1.100 -T5
```

Logging Information

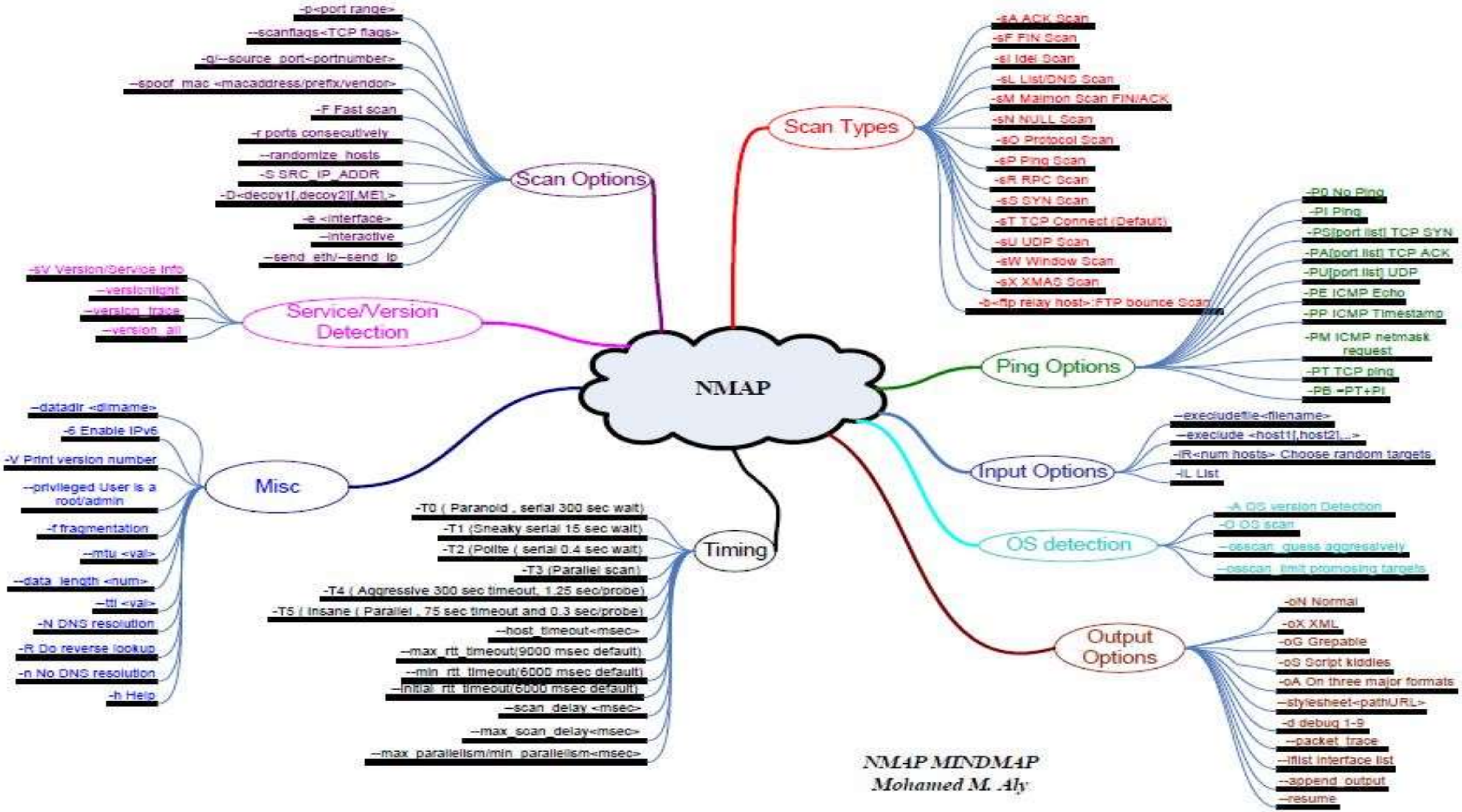
- Nmap provide many options of logging the scan result.
  - Normal Format (-oN <Logfilename>)
    ```
    #nmap -sS -v 192.168.1.100 --packet_trace -oN nmap_output
    ```
  - XML Format (-oX <Logfilenmae>)
    ```
    #nmap -sS -v 192.168.1.100 --packet_trace -oN nmap_output
    ```
  - Grepable Format (-oG <filename>)
    ```
    #nmap -sS -v 192.168.1.100 --packet_trace -oG nmap_output
    ```
  - All Formats (-oA <filename>)
    this option will create 3 different output (Normal, XML, grepable output)
    ```
    #nmap -sS -v 192.168.1.100 --packet_trace -oA nmap_output
    ```

Nmap sample command

Nmap command	Description
Nmap 192.168.1.100	Perform nmap scan default on host 192.168.1.100
Nmap 192.168.1.0/24	Scan default nmap on network 192.168.1.0
Nmap –sP 192.168.1.100	Just ping to identify remote host alive or not
Nmap –sS –O –p 22,80,443 192.168.1.100	Perform SYN scan on port 22, 80, and 443 on remote host and dectect operation system
nmap -sS -Pn -sV -O nmap.org	Syn scan, no ping, identify version, and operating system detection.
nmap -v -n -sS -sU -Pn -A -oA scan nmap.org	**-v** invokes verbosity. **-n** skips name resolution. **-sS** is a SYN scan. **-sU** scans UDP ports. **-Pn** skips pinging. **-A** enables both OS fingerprinting and version detection (tries to verify what is listening on found ports). **-oA scan** creates reports as **scan.nmap**, **scan.gnmap**, and **scan.xml**.



Question



NMAP

Scan Options
- -p<port range>
- --scanflags<TCP flags>
- -g/--source_port<portnumber>
- --spoof_mac <macaddress/prefix/vendor>
- -F Fast scan
- -r ports consecutively
- --randomize_hosts
- -S SRC_IP_ADDR
- -D<decoy1[,decoy2][,ME],>
- -e <interface>
- --interactive
- --send_eth/--send_ip

Service/Version Detection
- -sV Version/Service Info
- --versionlight
- --version_trace
- --version_all

Misc
- --datadir <dirname>
- -6 Enable IPv6
- -V Print version number
- --privileged User is a root/admin
- -f fragmentation
- --mtu <val>
- --data_length <num>
- --ttl <val>
- -N DNS resolution
- -R Do reverse lookup
- -n No DNS resolution
- -h Help

Timing
- -T0 (Paranoid , serial 300 sec wait)
- -T1 (Sneaky serial 15 sec wait)
- -T2 (Polite (serial 0.4 sec wait)
- -T3 (Parallel scan)
- -T4 (Aggressive 300 sec timeout, 1.25 sec/probe)
- -T5 (Insane (Parallel , 75 sec timeout and 0.3 sec/probe)
- --host_timeout<msec>
- --max_rtt_timeout(9000 msec default)
- --min_rtt_timeout(6000 msec default)
- --initial_rtt_timeout(6000 msec default)
- --scan_delay <msec>
- --max_scan_delay<msec>
- --max_parallelism/min_parallelism<msec>

Scan Types
- -sA ACK Scan
- -sF FIN Scan
- -sI Idel Scan
- -sL List/DNS Scan
- -sM Maimon Scan FIN/ACK
- -sN NULL Scan
- -sO Protocol Scan
- -sP Ping Scan
- -sR RPC Scan
- -sS SYN Scan
- -sT TCP Connect (Default)
- -sU UDP Scan
- -sW Window Scan
- -sX XMAS Scan
- -b<ftp relay host>:FTP bounce Scan

Ping Options
- -P0 No Ping
- -PI Ping
- -PS[port list] TCP SYN
- -PA[port list] TCP ACK
- -PU[port list] UDP
- -PE ICMP Echo
- -PP ICMP Timestamp
- -PM ICMP netmask request
- -PT TCP ping
- -PB =PT+PI

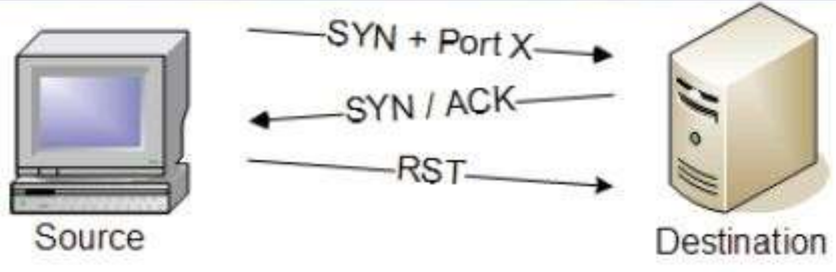
Input Options
- --execiudefile<filename>
- --execlude <host1[,host2],...>
- -iR<num hosts> Choose random targets
- -iL List

OS detection
- -A OS version Detection
- -O OS scan
- --osscan_guess aggresaively
- --osscan_limit promosing targets

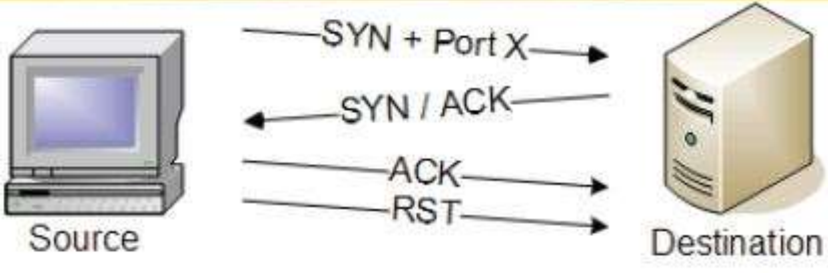
Output Options
- -oN Normal
- -oX XML
- -oG Grepable
- -oS Script kiddies
- -oA On three major formats
- --stylesheet<pathURL>
- -d debug 1-9
- --packet_trace
- --iflist interface list
- --append_output
- --resume

NMAP MINDMAP
Mohamed M. Aly

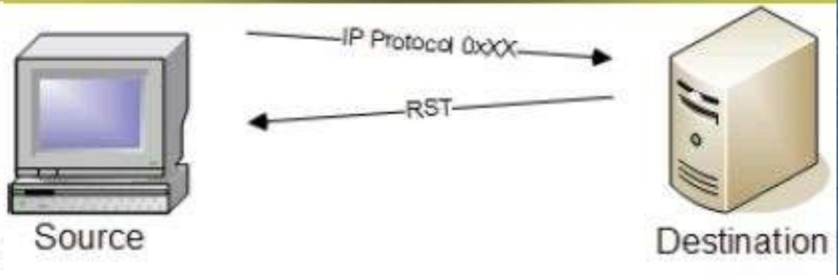
TCP SYN SCAN (-sS)



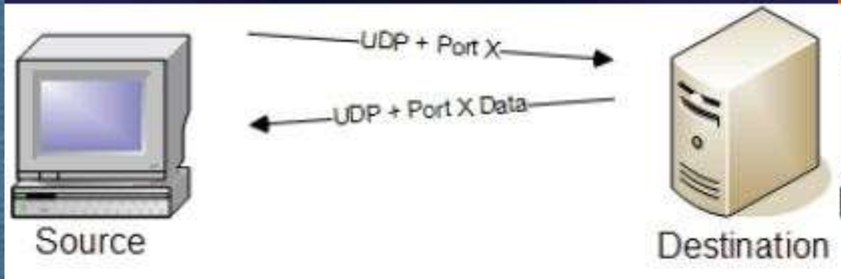
TCP connect() SCAN (-sT)



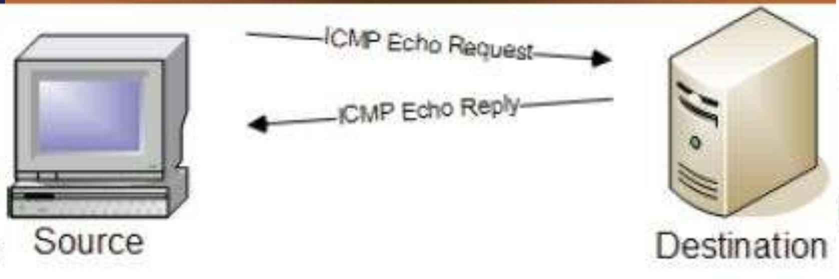
IP PROTOCOL SCAN (-sO)



UDP SCAN (-sU)

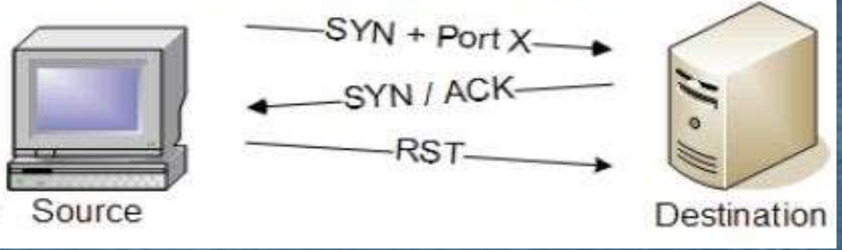


TCP PING SCAN (-sP)



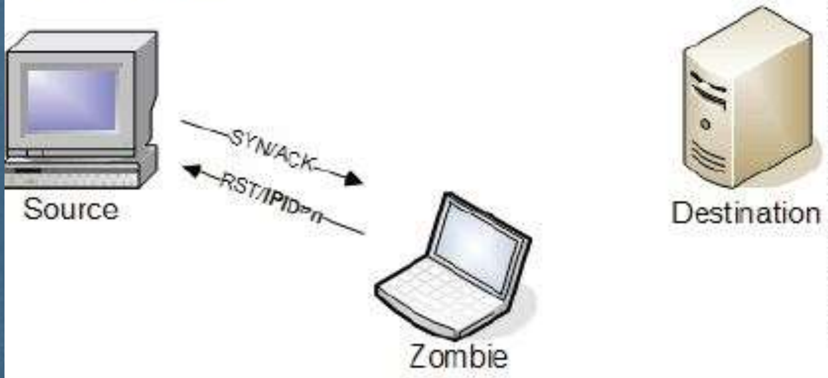
VERSION DETECTION SCAN (-sV)

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

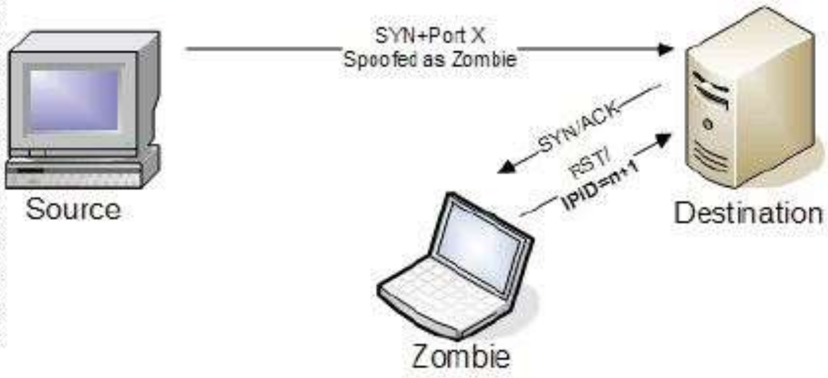


IDLESCAN (-sI <zombie host:[probeport]>)

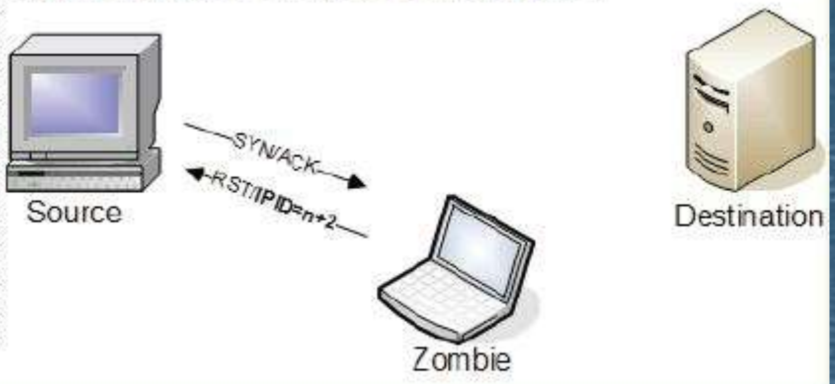
Step 1: Nmap sends a SYN/ACK to the zombie workstation to induce a RST in return. This RST frame contains the initial IPID that nmap will remember for later.



Step 2: Nmap sends a SYN frame to the destination address, but nmap spoofs the IP address to make it seem as if the SYN frame was sent from the zombie workstation.



Step 3: Nmap repeats the original SYN/ACK probe of the zombie station. If the IPID has incremented, then the port that was spoofed in the original SYN frame is open on the destination device.


SYN/ACK
RST/IPID=n+2
Source
Destination
Zombie