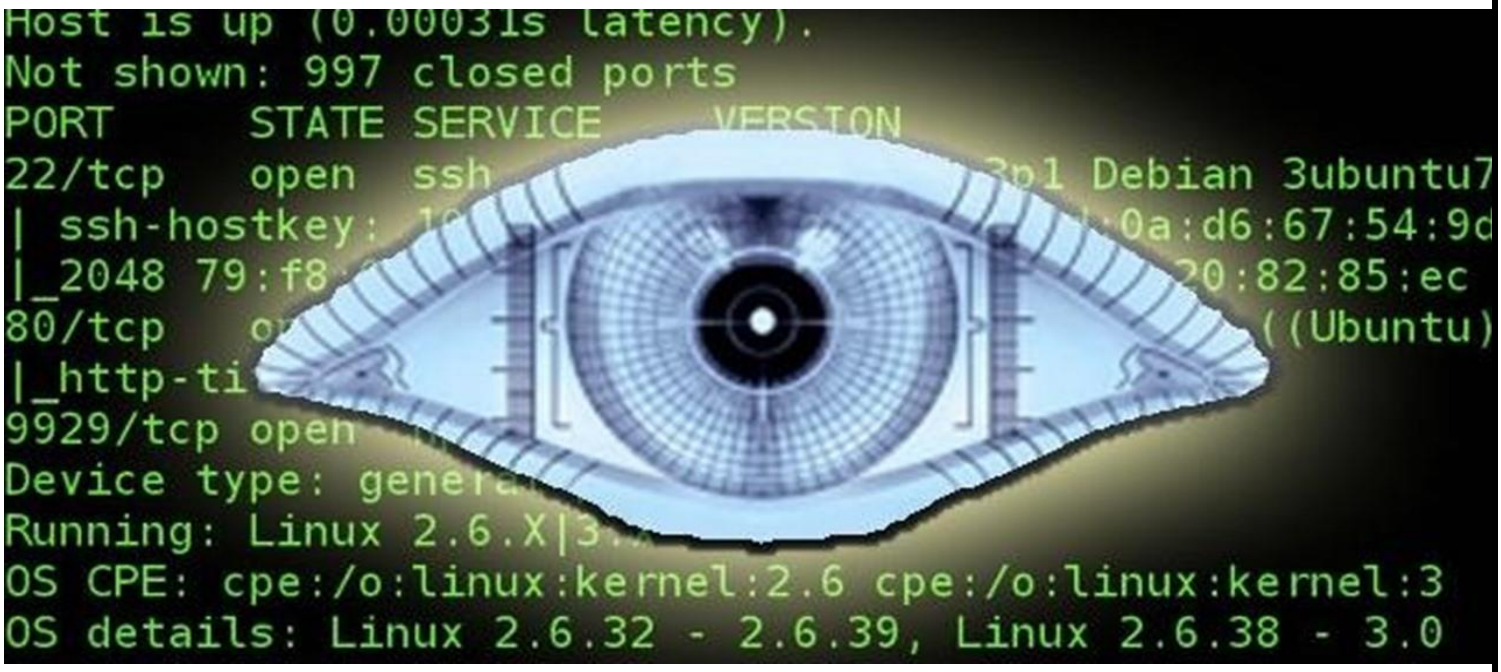
NMAP

(Network Mapper)

Sommaire :

Prepared by Younes Elbarj
LinkedIn: linkedin.com/in/younes-elbarj/



What is Nmap :

- Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

- Nmap allows network users to find which devices are running on their network, discover open ports and services, and detect vulnerabilities

- **Gordon Lyon (pseudonym Fyodor)** wrote Nmap as a tool to help map an entire network easily and to find its open ports and services.
- Nmap has become hugely popular, being featured in movies like The Matrix and the popular series Mr. Robot.

Why Use Nmap :

- Nmap is a versatile tool that simplifies network mapping with basic commands or advanced scripting through its Nmap Scripting Engine (NSE).

Key Features:

- **Device Discovery:** Quickly identifies all devices (e.g., servers, routers, switches)
- **Service Detection:** Recognizes services like web or DNS servers and detects application versions to uncover vulnerabilities.
- **OS Detection:** Determines operating systems and versions on devices
- **Security Auditing:** Leverages NSE scripts for vulnerability assessments
- **Zenmap GUI:** Offers a user-friendly graphical interface for visualizing network maps and generating reports.

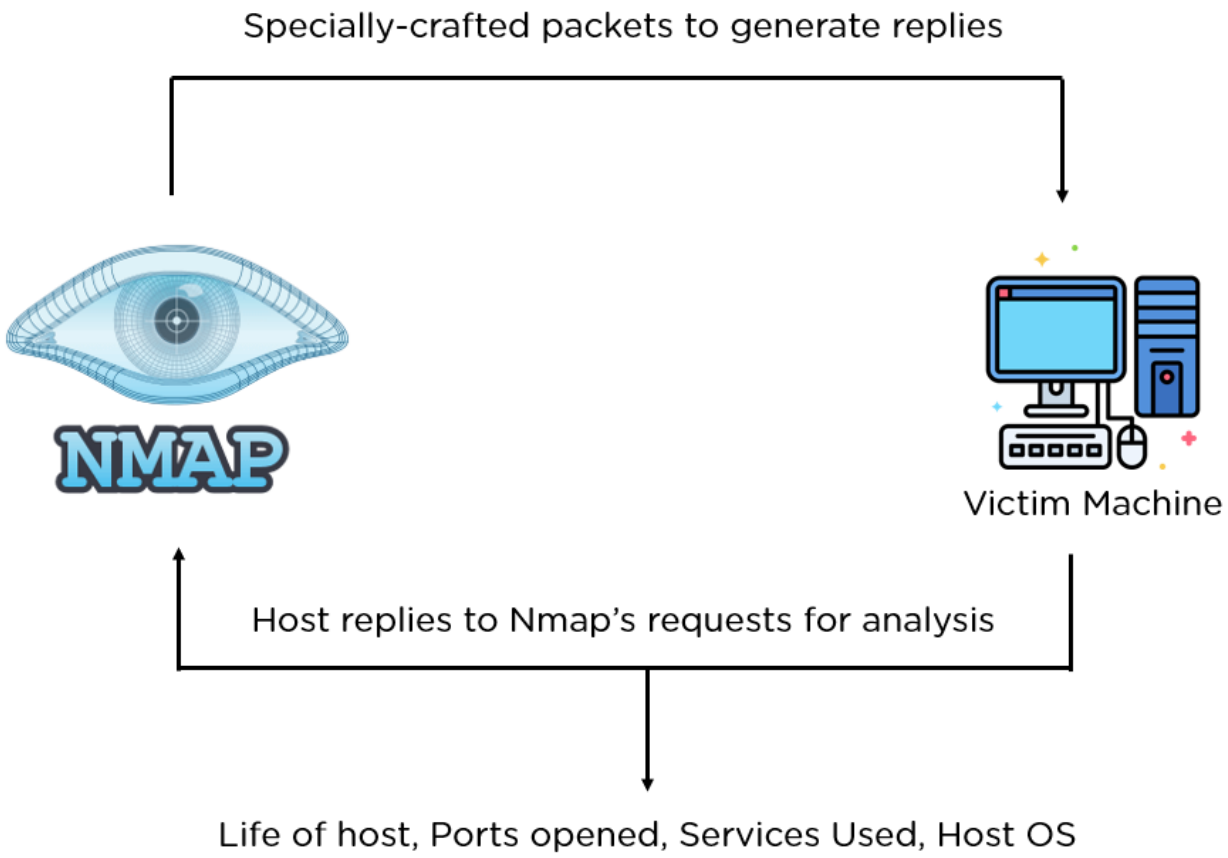
How Nmap Works :

Scanning networks with Nmap involves a **three-step process**, where Nmap handles the first two steps, leaving the final step to the ethical hacker

1. **Sending Requests :** Nmap sends raw IP packets to discover active hosts and accessible systems on a network
2. **Receiving Replies :** In response to the requests, active hosts send back replies. These responses indicate:

- Open Ports
- Closed Ports
- Filtered Ports

3. **Analyzing Responses :** Nmap provides detailed information about the hosts, services, and open ports



Installation :

Platforms Supported:

- Linux
- Windows
- macOS

Command to Install :

- sudo apt install nmap

Types Of Scans :

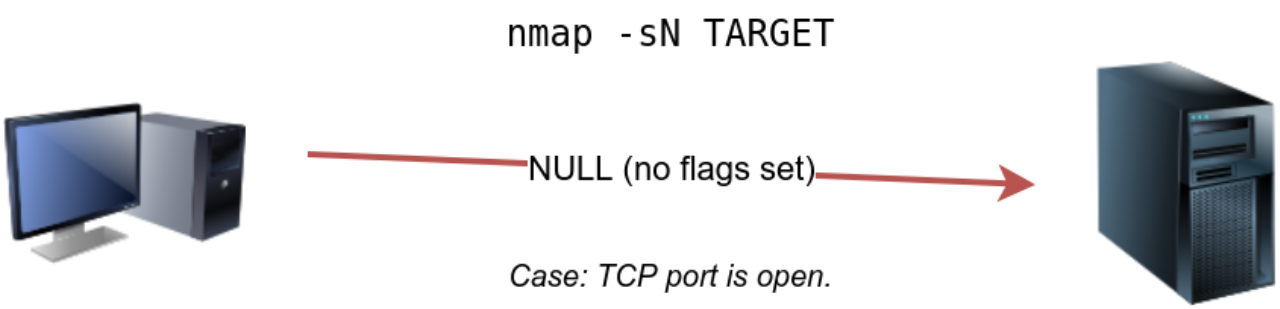
Option	Meaning
-sV	determine service/version info on open ports
-sV --version-light	try the most likely probes (2)
-sV --version-all	try all available probes (9)
-O	detect OS
--traceroute	run traceroute to target
--script=SCRIPTS	Nmap scripts to run
-sC or --script=default	run default scripts
-A	equivalent to -sV -O -sC --traceroute
-oN	save output in normal format
-oG	save output in grepable format
-oX	save output in XML format
-oA	save output in normal, XML and Grepable formats

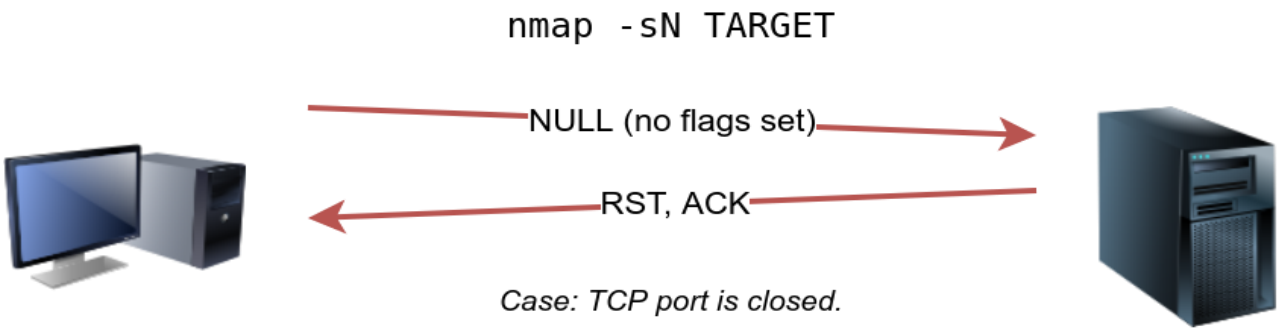
TCP Flags Table Overview :

Flag	Abbreviation	Purpose
SYN	Synchronize	Starts a connection (initiates the TCP handshake).
ACK	Acknowledgment	Acknowledges the receipt of data.
FIN	Finish	Ends a connection.
RST	Reset	Resets a connection (abortive termination).
PSH	Push	Requests immediate data delivery to the application.
URG	Urgent	Marks the data as urgent and processes it immediately.

Advanced Types Of Scans :

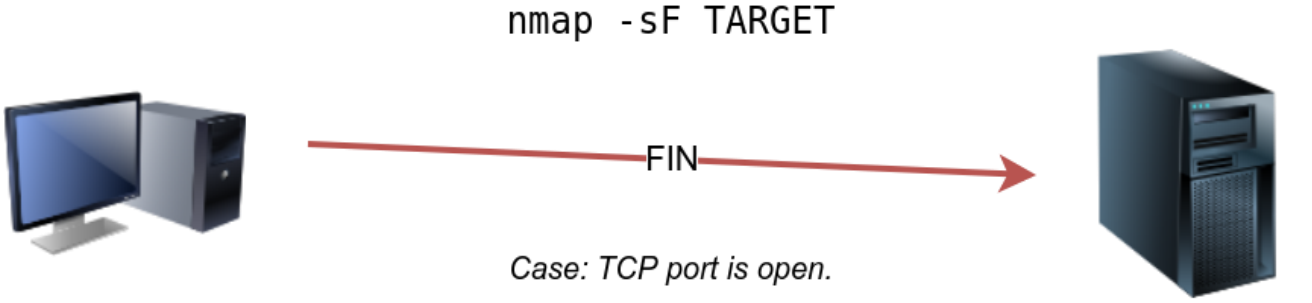
- **Null Scan :** A Null Scan sends a TCP packet without setting any flags (all six TCP flag bits are set to 0)

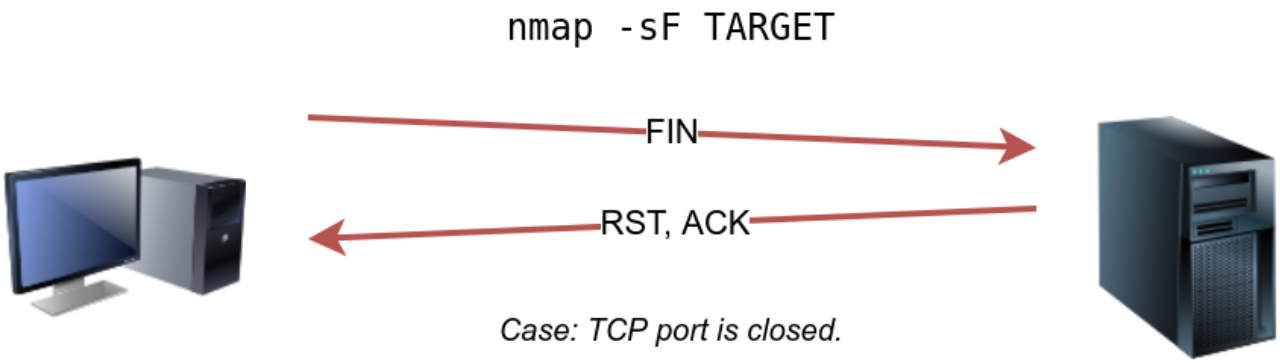




- **FIN Scan :** The FIN scan sends a TCP packet with the **FIN flag** set.

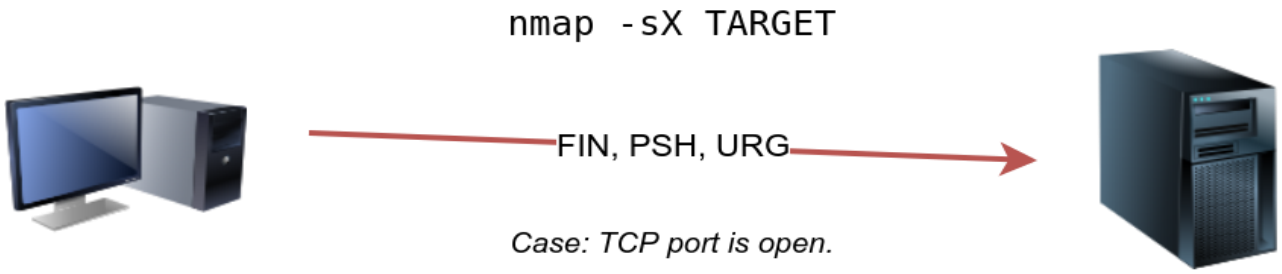
- **Open Ports**: Do not send a response.
- **Closed Ports:** Respond with a TCP RST (Reset) packet to indicate that the port is closed.

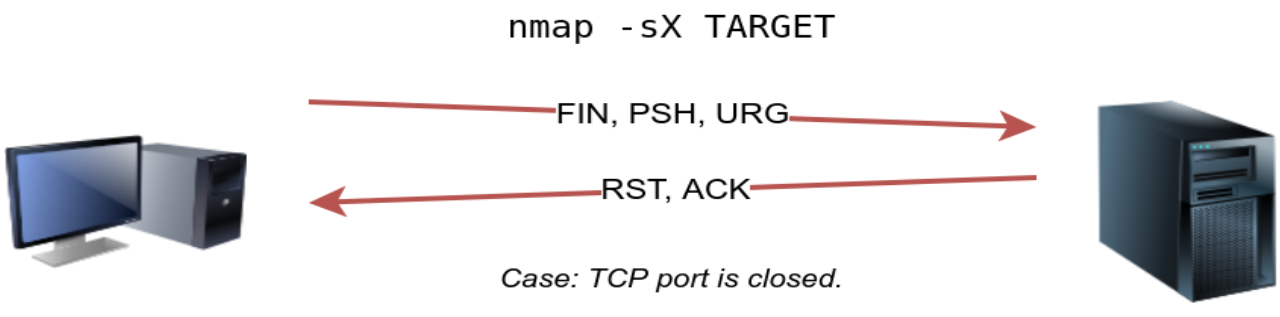




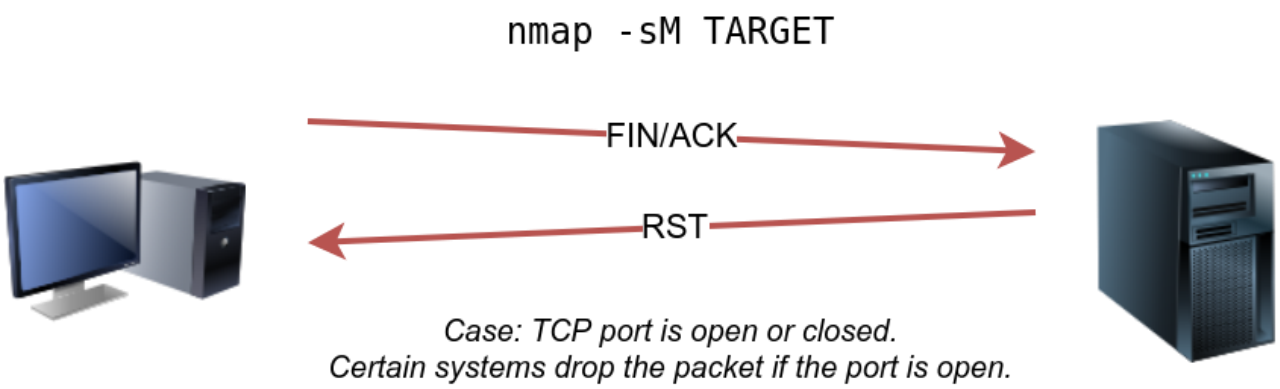
Xmas Scan :

- **Send:** A TCP packet with FIN, PSH, and URG flags set.
- **Response**: If the port is open, no response is sent. If the port is closed, an RST packet is sent.





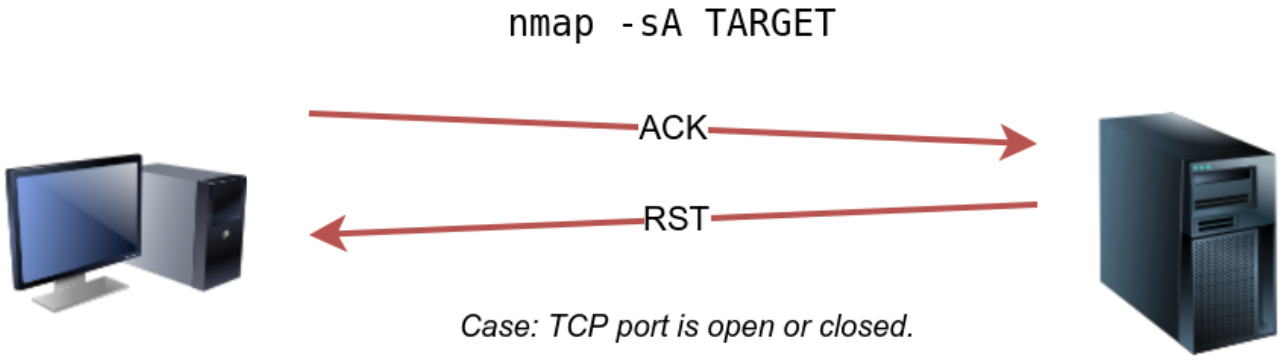
Maimon Scan : The Maimon scan sends a **TCP packet with the FIN and PSH flags** set, similar to the **Xmas scan**, but without the **URG** flag.



TCP ACK Scan :

- **Send:** A TCP packet with the ACK flag set to a target port.
- **Response:**

  - **RST Response:** If an RST packet is received, the port is likely unfiltered.
  - **No Response:** If no response is received, the port is likely filtered by a firewall or packet filter.

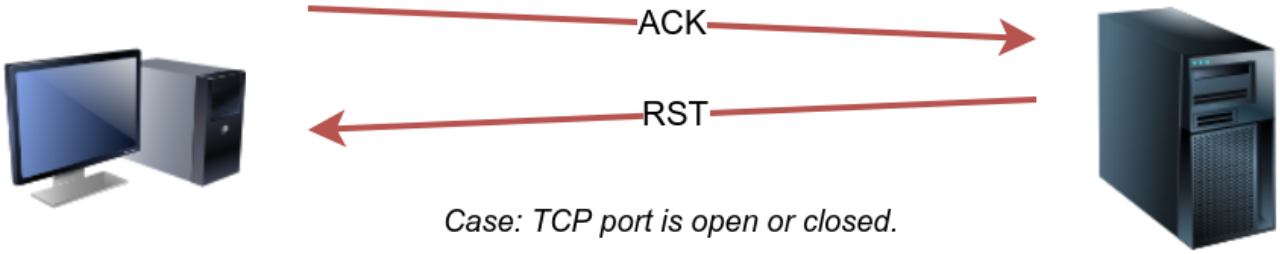


Window Scan :

- **Send:** A TCP packet with the ACK flag set to a target port.
- **Response:**

  - **Non-zero Window Size:** If the RST packet has a non-zero window size, the port might be open.
  - **Zero Window Size:** A zero window size suggests that the port is closed or filtered.

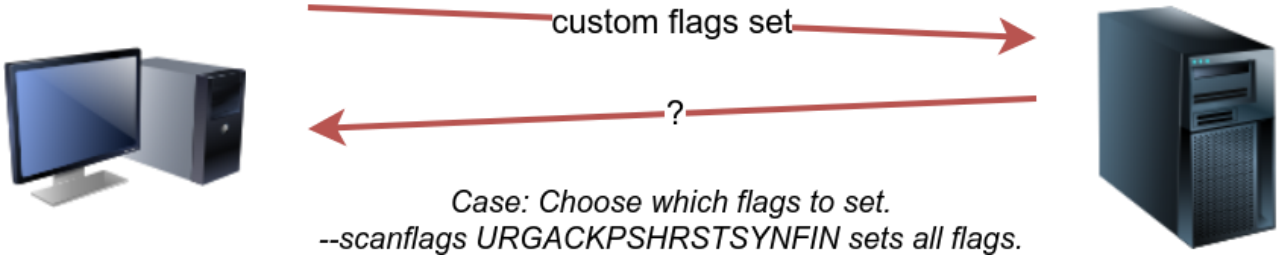
```
nmap -sW TARGET
```



Case: TCP port is open or closed.

Custom Scan: in Nmap allows you to experiment with different combinations of TCP flags using the --scanflags option. This lets you send non-standard packets to test how a target system responds. For example, you can set flags like SYN, RST, and FIN simultaneously, which is not typical in standard scans.

```
nmap --scanflags CUSTOM_FLAGS TARGET
```

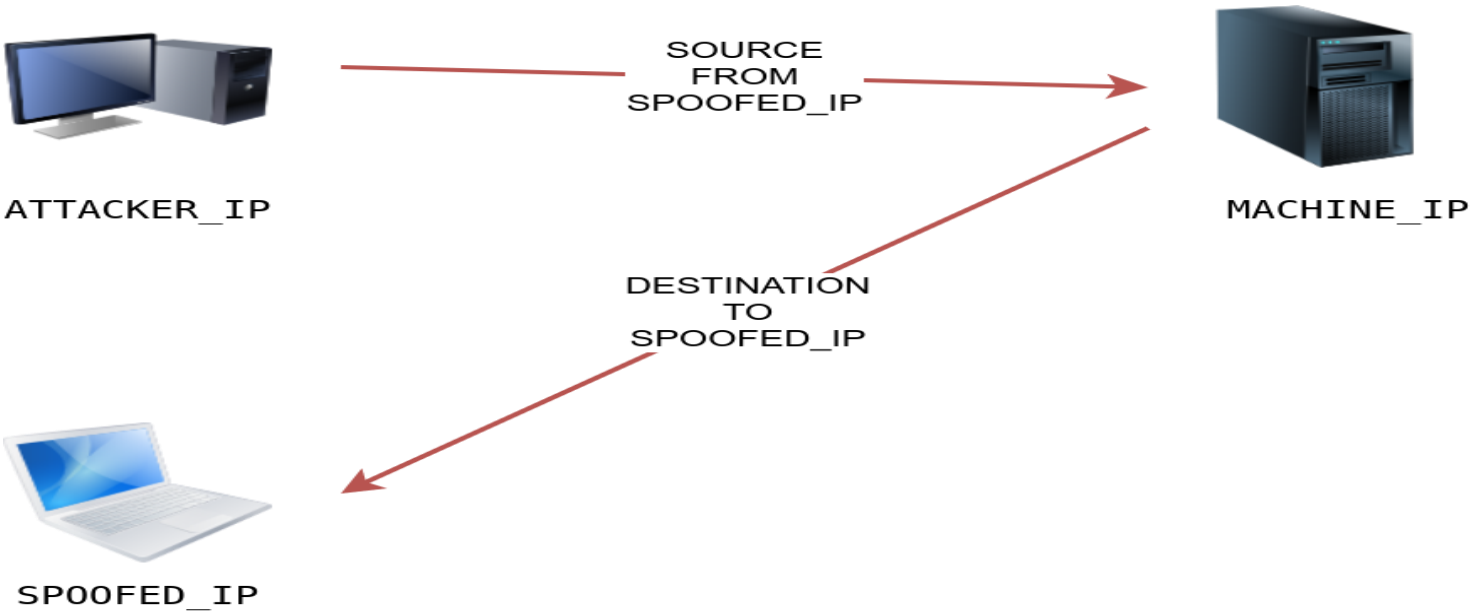


Case: Choose which flags to set.
--scanflags URGACKPSHRSTSYNFIN sets all flags.

Spoofing and Decoys in Nmap : Nmap supports **spoofing** of both IP addresses and MAC addresses during scans. This is useful when an attacker wants to hide their real identity or avoid detection by security systems like intrusion detection systems (IDS) or firewalls. However, for a spoofed scan to be effective, the attacker must be able to capture the responses sent to the spoofed address.

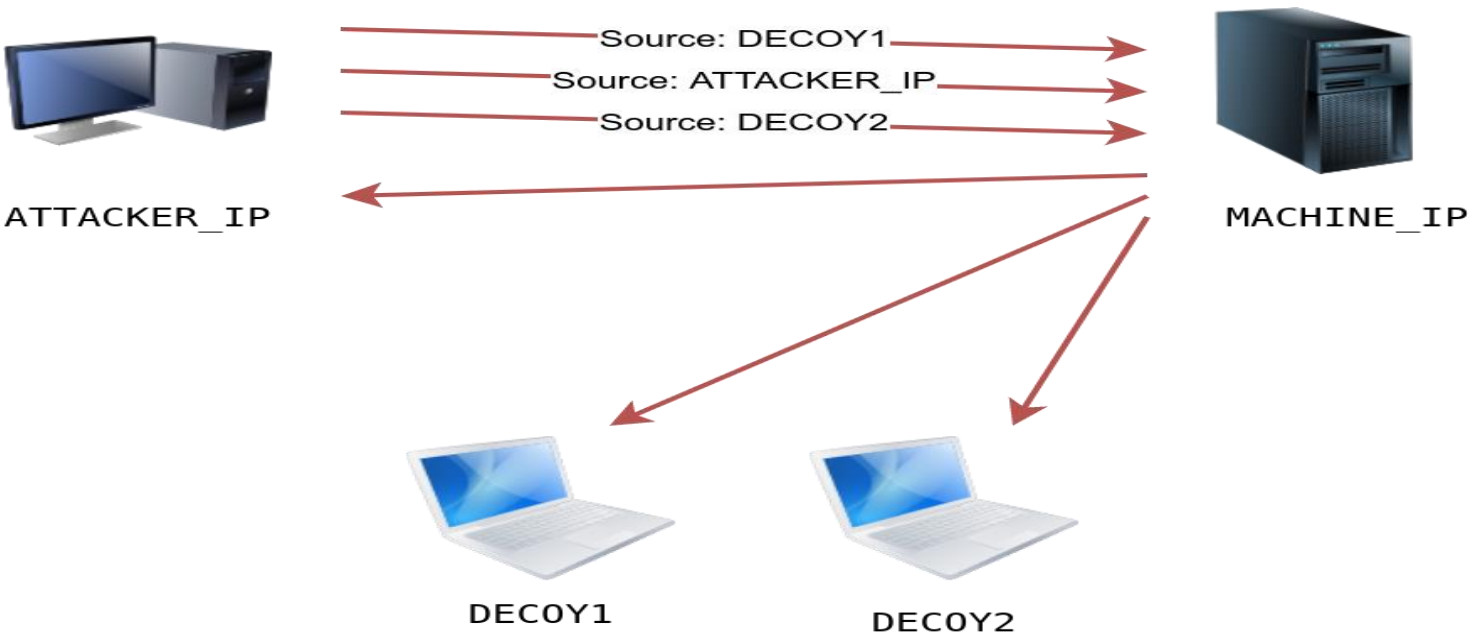
- Attacker sends a packet with a spoofed source IP address to the target machine.
- target machine replies to the spoofed IP address as the destination.
- Attacker captures the replies to figure out open ports.

nmap -S SPOOFED_IP MACHINE_IP



Using SPOOFED_IP as the source IP address for the scan.

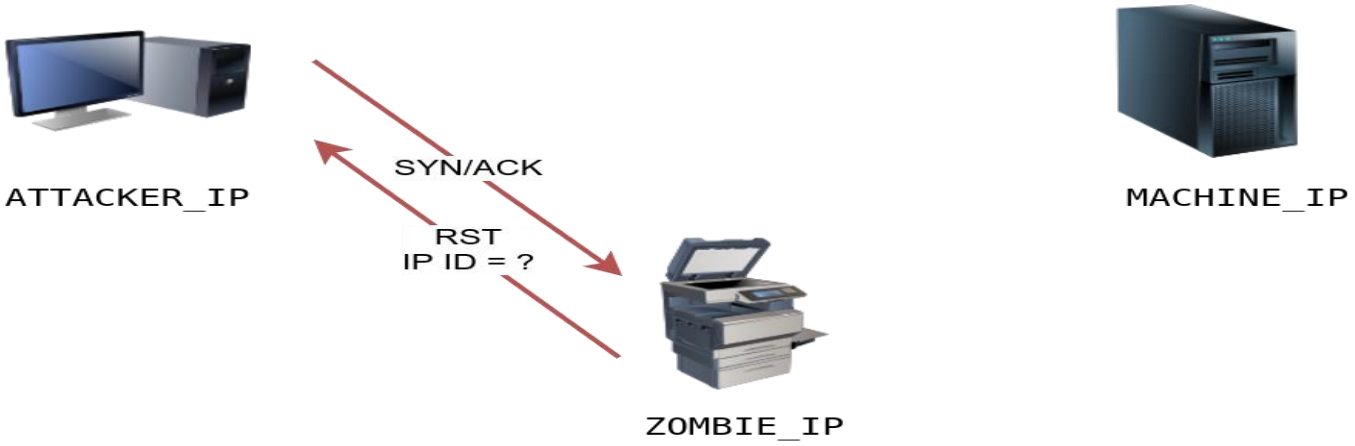
nmap -D DECOY1,ME,DECOY2 MACHINE_IP



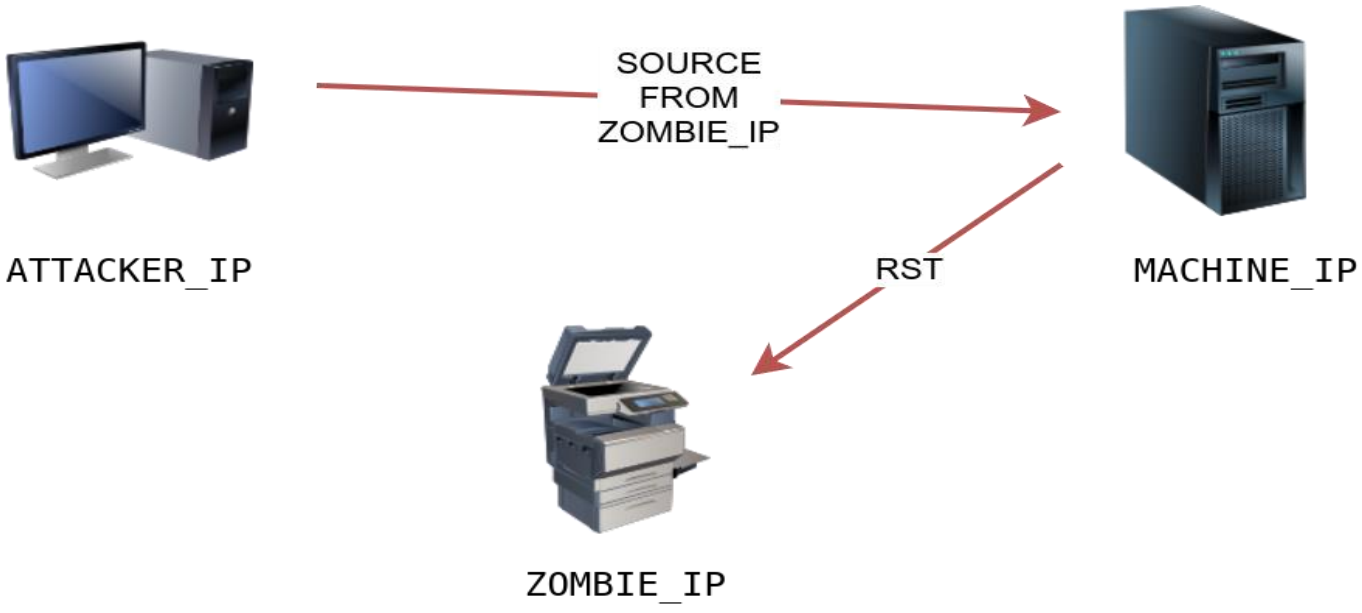
Using DECOY1, ATTACKER_IP, DECOY2 as the source IP addresses for the scan.

Idle Scan (Zombie Scan) in Nmap:

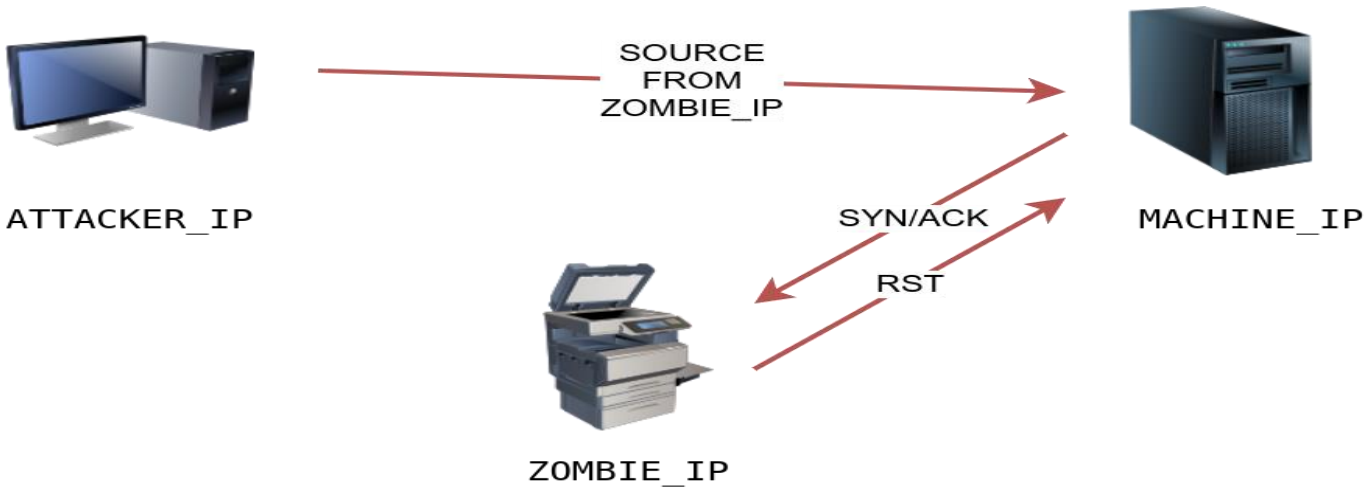
- The **idle scan** (or **zombie scan**) is a stealthy scanning technique that allows an attacker to scan a target machine without directly sending probes from their own IP address. Instead, the scan is made to appear as if the probes are coming from an **idle (zombie) host** on the network. This technique requires the attacker to have access to a system on the same network that can be used as the "zombie."



Attacker system communicates with an idle system to find its current IP ID



Attacker system sends to target machine a SYN packet spoofed as sent by the idle system.
Case: Port is closed



Attacker system sends to target machine
a SYN packet spoofed as sent by the idle system.
Case: Port is open

Port Scan Type	Example Command
TCP Null Scan	sudo nmap -sN MACHINE_IP
TCP FIN Scan	sudo nmap -sF MACHINE_IP
TCP Xmas Scan	sudo nmap -sX MACHINE_IP
TCP Maimon Scan	sudo nmap -sM MACHINE_IP
TCP ACK Scan	sudo nmap -sA MACHINE_IP
TCP Window Scan	sudo nmap -sW MACHINE_IP
Custom TCP Scan	sudo nmap --scanflags URGACKPSHRSTSYNFIN MACHINE_IP
Spoofed Source IP	sudo nmap -S SPOOFED_IP MACHINE_IP
Spoofed MAC Address	--spoof-mac SPOOFED_MAC
Decoy Scan	nmap -D DECOY_IP,ME MACHINE_IP
Idle (Zombie) Scan	sudo nmap -sI ZOMBIE_IP MACHINE_IP
Fragment IP data into 8 bytes	-f
Fragment IP data into 16 bytes	-ff

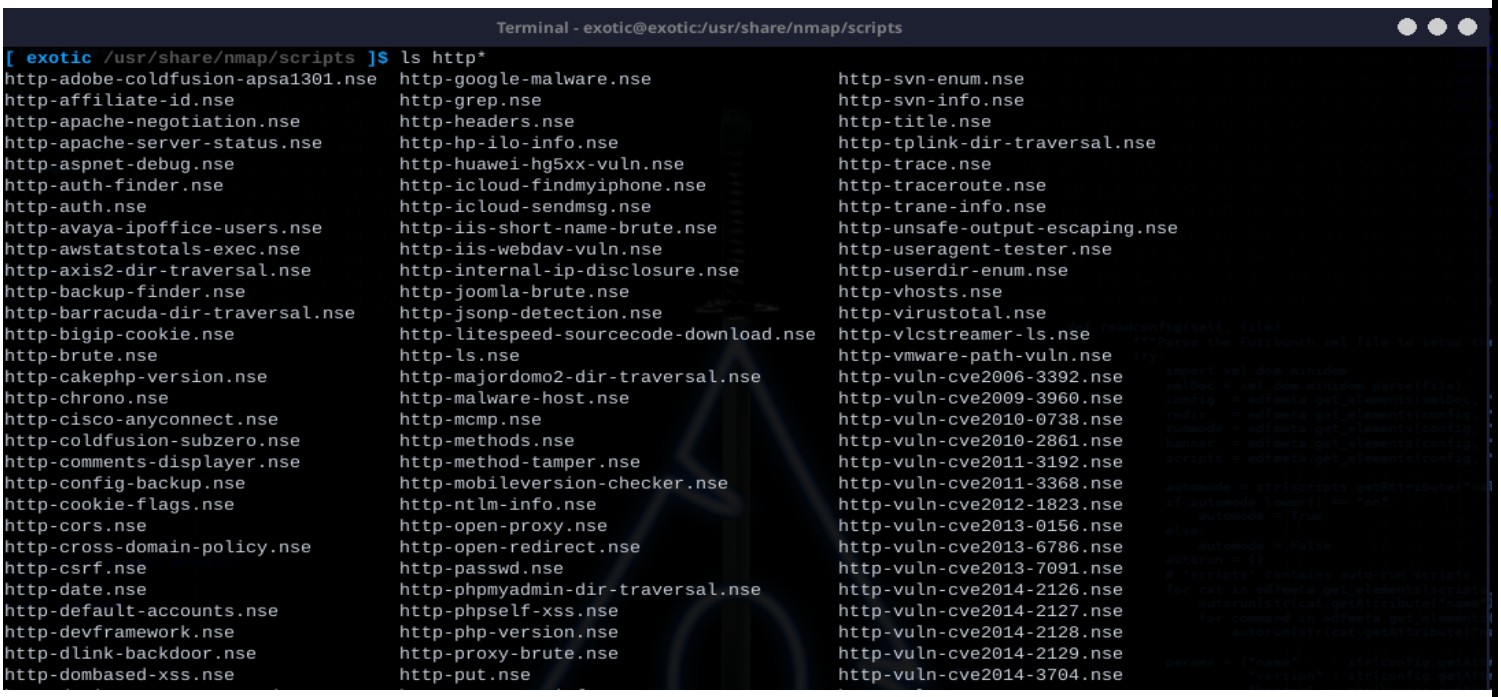
Nmap Scripting Engine (NSE):

- The **Nmap Scripting Engine (NSE)** is a powerful feature of Nmap that allows users to automate a wide range of tasks using scripts written in the **Lua programming language**
- A **script** is a piece of code that remains in human-readable form and does not require compilation. It can provide custom functionality or extend existing capabilities.

Key Features of NSE:

Pre-Built Scripts:

- Nmap installations typically include **hundreds of scripts**, with names indicating their purpose (http-* scripts target HTTP protocols).
- Scripts are stored in the directory /usr/share/nmap/scripts on Linux systems



Categorization of Scripts:

NSE scripts are grouped into categories, such as:

- **Auth:** Authentication-related tasks.
- **Default:** Basic scripts included in standard scans.
- **Discovery:** Finding hosts, services, or information.
- **Vuln:** Detecting vulnerabilities.
- **Exploit:** Exploiting vulnerabilities to test systems.

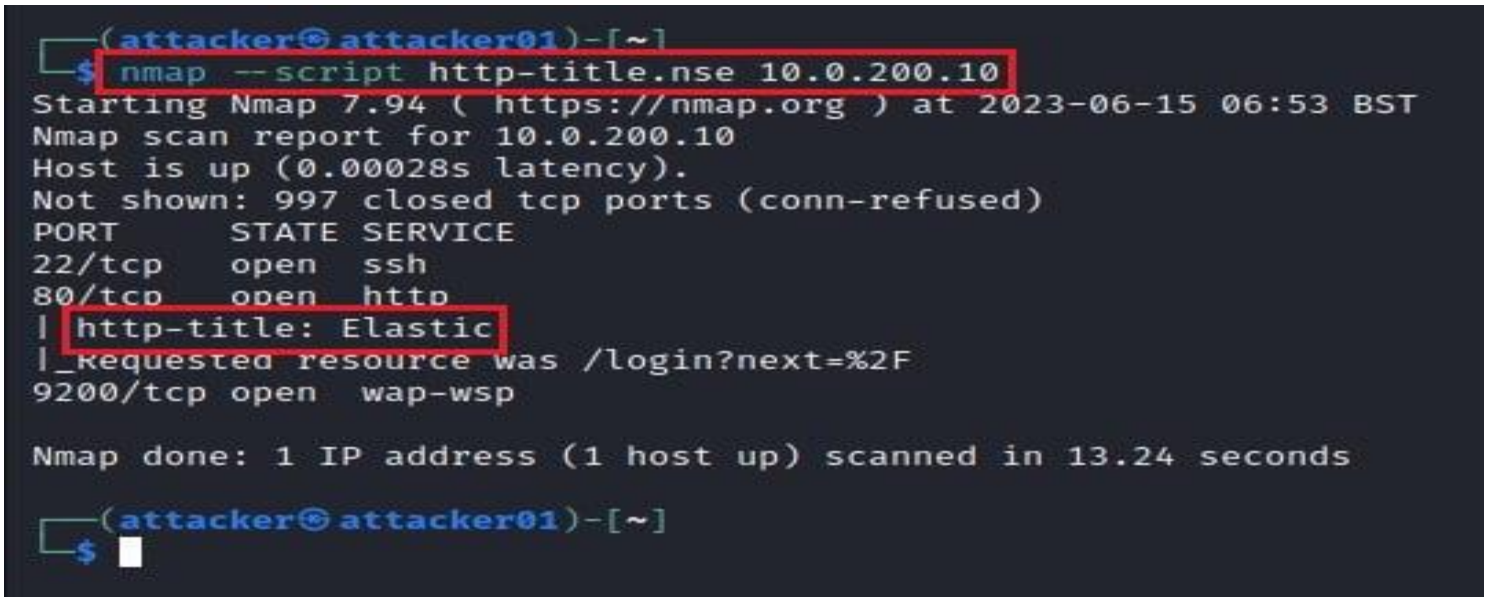
Users can run scripts from a specific category using options like **--script=category.**

Script Category	Description
auth	Authentication related scripts
broadcast	Discover hosts by sending broadcast messages
brute	Performs brute-force password auditing against logins
default	Default scripts, same as -sC
discovery	Retrieve accessible information, such as database tables and DNS names
dos	Detects servers vulnerable to Denial of Service (DoS)
exploit	Attempts to exploit various vulnerable services
external	Checks using a third-party service, such as Geoplugin and Virustotal
fuzzer	Launch fuzzing attacks
intrusive	Intrusive scripts such as brute-force attacks and exploitation
malware	Scans for backdoors
safe	Safe scripts that won't crash the target
version	Retrieve service versions
vuln	Checks for vulnerabilities or exploit vulnerable services

Practical Scenarios :

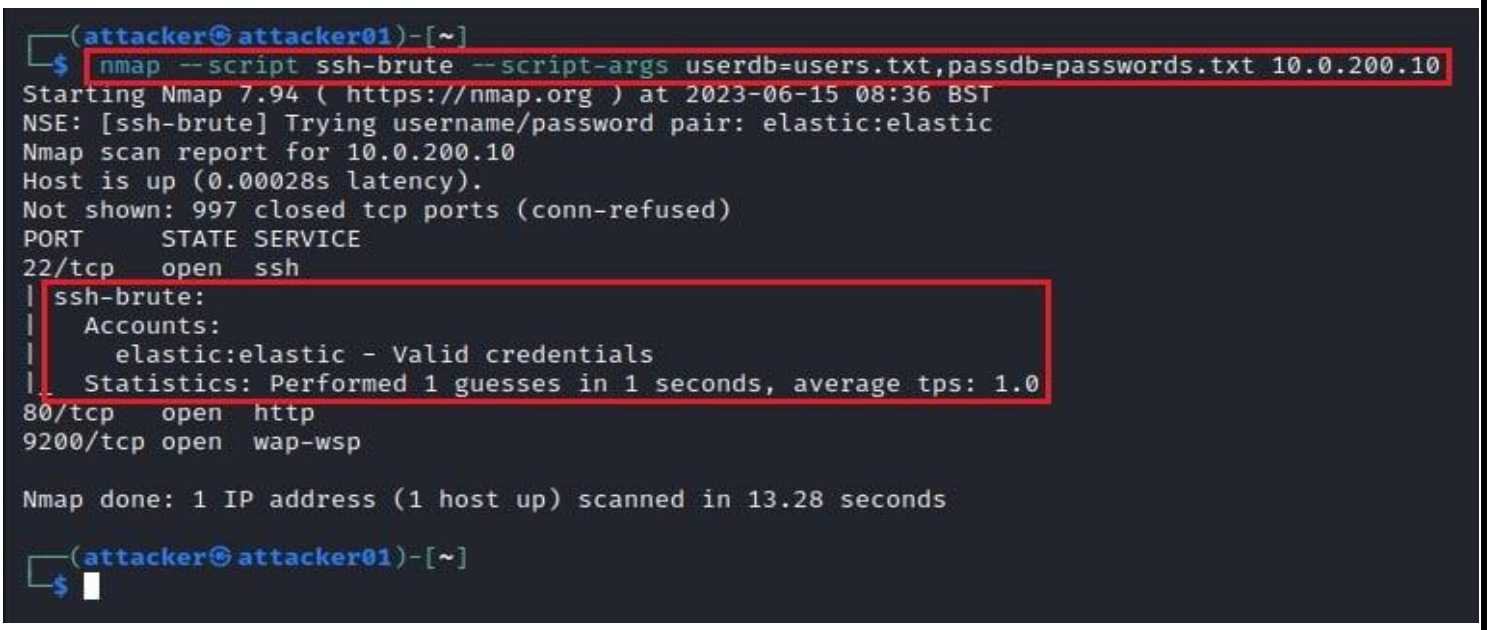
Executing a Specific Nmap Script :

```
nmap --script http-title.nse 10.0.200.10
```



Executing Nmap Scripts With Arguments :

Some scripts require you to specify arguments so they can execute correctly. This can be done with the argument **--script-args** followed by a list of arguments you want to pass to the script or with --scripts-args-file followed by a file containing the arguments you want to pass.



Executing a Nmap Script Category :

If you wanted to run all the scripts that fall under the vuln category against a machine whose IP address is 10.0.200.3, you would run the command:

```
nmap --script vuln 10.0.200.3
```

```
┌──(attacker㉿attacker01)-[~]
└─$ nmap --script vuln 10.0.200.10
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-15 07:11 BST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.0.200.10
Host is up (0.00029s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-vuln-cve2010-0738:
|_  /jmx-console/: Authentication was not required
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /api/: Potentially interesting folder (401 Unauthorized)
|_  /internal/: Potentially interesting folder (401 Unauthorized)
9200/tcp open  wap-wsp

Nmap done: 1 IP address (1 host up) scanned in 112.30 seconds
```

Executing All Nmap Scripts :

```
nmap -sC 10.0.200.3
```

```
┌──(attacker㉿attacker01)-[~]
└─$ nmap -sC 10.0.200.3
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-15 07:55 BST
Nmap scan report for 10.0.200.3
Host is up (0.00076s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
| rdp-ntlm-info:
|   Target_Name: milkyway
|   NetBIOS_Domain_Name: milkyway
|   NetBIOS_Computer_Name: WORKSTATION01
|   DNS_Domain_Name: milkyway.local
|   DNS_Computer_Name: WORKSTATION01.milkyway.local
|   DNS_Tree_Name: milkyway.local
|   Product_Version: 10.0.19041
|_  System_Time: 2023-06-15T06:55:34+00:00
| ssl-cert: Subject: commonName=WORKSTATION01.milkyway.local
| Not valid before: 2023-05-22T16:46:51
|_Not valid after:  2023-11-21T16:46:51
|_ssl-date: 2023-06-15T06:55:34+00:00; 0s from scanner time.
5357/tcp open  wsdapi

Host script results:
|_nbstat: NetBIOS name: WORKSTATION01, NetBIOS user: <unknown>, NetBIOS MAC: 4a:05:86:b5:c7:7d (unknown)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-06-15T06:55:34
|_  start_date: N/A

Nmap done: 1 IP address (1 host up) scanned in 30.37 seconds

┌──(attacker㉿attacker01)-[~]
└─$
```

Conclusion :

The Nmap Scripting Engine (NSE) is a game-changing feature of the powerful network scanning tool Nmap. It allows hackers to create and execute scripts that automate everything from scanning for vulnerabilities to exploitation.

The NSE is used by professional, ethical hackers and penetration testers worldwide to automate their hacking workflows.

Nmap Cheat Sheet :

Target Specification

Switch	Example	Description
	nmap 192.168.1.1	Scan a single IP
	nmap 192.168.1.1 192.168.2.1	Scan specific IPs
	nmap 192.168.1.1-254	Scan a range
	nmap scanme.nmap.org	Scan a domain
	nmap 192.168.1.0/24	Scan using CIDR notation
-iL	nmap -iL targets.txt	Scan targets from a file
-iR	nmap -iR 100	Scan 100 random hosts
--exclude	nmap --exclude 192.168.1.1	Exclude listed hosts

Scan Techniques

Switch	Example	Description
-sS	nmap 192.168.1.1 -sS	TCP SYN port scan (Default)
-sT	nmap 192.168.1.1 -sT	TCP connect port scan (Default without root privilege)
-sU	nmap 192.168.1.1 -sU	UDP port scan
-sA	nmap 192.168.1.1 -sA	TCP ACK port scan
-sW	nmap 192.168.1.1 -sW	TCP Window port scan
-sM	nmap 192.168.1.1 -sM	TCP Maimon port scan

Host Discovery

Switch	Example	Description
-sL	nmap 192.168.1.1-3 -sL	No Scan. List targets only
-sn	nmap 192.168.1.1/24 -sn	Disable port scanning
-Pn	nmap 192.168.1.1-5 -Pn	Disable host discovery. Port scan only
-PS	nmap 192.168.1.1-5 -PS22-25,80	TCP SYN discovery on port x. Port 80 by default
-PA	nmap 192.168.1.1-5 -PA22-25,80	TCP ACK discovery on port x. Port 80 by default
-PU	nmap 192.168.1.1-5 -PU53	UDP discovery on port x. Port 40125 by default
-PR	nmap 192.168.1.1-1/24 -PR	ARP discovery on local network
-n	nmap 192.168.1.1 -n	Never do DNS resolution

Port Specification

Switch	Example	Description
-p	nmap 192.168.1.1 -p 21	Port scan for port x
-p	nmap 192.168.1.1 -p 21-100	Port range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	Port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	Port scan all ports
-p	nmap 192.168.1.1 -p http,https	Port scan from service name
-F	nmap 192.168.1.1 -F	Fast port scan (100 ports)
--top-ports	nmap 192.168.1.1 --top-ports 2000	Port scan the top x ports
-p-65535	nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
-p0-	nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535

Service and Version Detection

Switch	Example	Description
sV	nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port
sV --version-intensity	nmap 192.168.1.1 -sV --version-intensity 8	Intensity level 0 to 9. Higher number increases possibility of correctness
sV --version-light	nmap 192.168.1.1 -sV --version-light	Enable light mode. Lower possibility of correctness. Faster
sV --version-all	nmap 192.168.1.1 -sV --version-all	Enable intensity level 9. Higher possibility of correctness. Slower
A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Switch	Example	Description
-O	nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
-O --osscan-limit	nmap 192.168.1.1 -O --osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O --osscan-guess	nmap 192.168.1.1 -O --osscan-guess	Makes Nmap guess more aggressively
-O --max-os-tries	nmap 192.168.1.1 -O --max-os-tries 1	Set the maximum number x of OS detection tries against a target
-A	nmap 192.168.1.1 -A	Enables OS detection, version detection, script scanning, and traceroute

Timing and Performance

Switch	Example	Description
-T0	nmap 192.168.1.1 -T0	Paranoid (0) Intrusion Detection System evasion
-T1	nmap 192.168.1.1 -T1	Sneaky (1) Intrusion Detection System evasion
-T2	nmap 192.168.1.1 -T2	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	nmap 192.168.1.1 -T3	Normal (3) which is default speed
-T4	nmap 192.168.1.1 -T4	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	nmap 192.168.1.1 -T5	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

Switch	Example input	Description
--host-timeout <time>	1s; 4m; 2h	Give up on target after this long
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
--min-hostgroup/max-hostgroup <size>	50; 1024	Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelization
--scan-delay/--max-scan-delay <time>	20ms; 2s; 4m; 5h	Adjust delay between probes
--max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
--min-rate <number>	100	Send packets no slower than <number> per second
--max-rate <number>	100	Send packets no faster than <number> per second

NSE Scripts

Switch	Example	Description
-sC	nmap 192.168.1.1 -sC	Scan with default NSE scripts. Considered useful for discovery and safe
--script default	nmap 192.168.1.1 --script default	Scan with default NSE scripts. Considered useful for discovery and safe
--script	nmap 192.168.1.1 --script=banner	Scan with a single script. Example banner
--script	nmap 192.168.1.1 --script=http*	Scan with a wildcard. Example http
--script	nmap 192.168.1.1 --script=http,banner	Scan with two scripts. Example http and banner
--script	nmap 192.168.1.1 --script "not intrusive"	Scan default, but remove intrusive scripts
--script-args	nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1	NSE script with arguments

Useful NSE Script Examples

Command	Description
nmap -Pn --script=http-sitemap-generator scanme.nmap.org	http site map generator
nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000	Fast search for random web servers
nmap -Pn --script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1	Safe SMB scripts to run
nmap --script whois* domain.com	Whois query
nmap -p80 --script http-unsafe-output-escaping scanme.nmap.org	Detect cross site scripting vulnerabilities.
nmap -p80 --script http-sql-injection scanme.nmap.org	Check for SQL injections

Firewall / IDS Evasion and Spoofing

Switch	Example	Description
-f	nmap 192.168.1.1 -f	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
--mtu	nmap 192.168.1.1 --mtu 32	Set your own offset size
-D	nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1	Send scans from spoofed IPs
-D	nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip	Above example explained
-S	nmap -S www.microsoft.com www.facebook.com	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
-g	nmap -g 53 192.168.1.1	Use given source port number
--proxies	nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1	Relay connections through HTTP/SOCKS4 proxies
--data-length	nmap --data-length 200 192.168.1.1	Appends random data to sent packets

Example IDS Evasion command

nmap -f -t 0 -n -Pn --data-length 200 -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1

Output

Switch	Example	Description
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once
-oG -	nmap 192.168.1.1 -oG -	Grepable output to screen. -oN -, -oX - also usable
--append-output	nmap 192.168.1.1 -oN file.file --append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
--reason	nmap 192.168.1.1 --reason	Display the reason a port is in a particular state, same output as -vv
--open	nmap 192.168.1.1 --open	Only show open (or possibly open) ports
--packet-trace	nmap 192.168.1.1 -T4 --packet-trace	Show all packets sent and received
--iflist	nmap --iflist	Shows the host interfaces and routes
--resume	nmap --resume results.file	Resume a scan

Helpful Nmap Output examples

Command	Description
nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open	Scan for web servers and grep to show which IPs are running web servers
nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 > live-hosts.txt	Generate a list of the IPs of live hosts
nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " " -f5 >> live-hosts.txt	Append IP to the list of live hosts
ndiff scanl.xml scan2.xml	Compare output from nmap using the ndiff
xsltproc nmap.xml -o nmap.html	Convert nmap xml files to html files
grep " open " results.nmap | sed -r 's/ +/ /g' | sort | uniq -c | sort -rn | less	Reverse sorted list of how often ports turn up

Miscellaneous Options

Switch	Example	Description
-6	nmap -6 2607:f0d0:1002:51::4	Enable IPv6 scanning
-h	nmap -h	nmap help screen

Other Useful Nmap Commands

Command	Description
hmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn	Discovery only on ports x, no port scan
hmap 192.168.1.1-1/24 -PR -sn -vv	Arp discovery only on local network, no port scan
hmap -iR 10 -sn -traceroute	Traceroute to random targets, no port scan
hmap 192.168.1.1-50 -sL --dns-server 192.168.1.1	Query the Internal DNS for hosts, list targets only

Ethical Considerations for Using Nmap:

- Always obtain permission before scanning a network. Respect laws and policies, avoid disruptive scans, and protect sensitive data. Use Nmap only for legitimate purposes, ensuring transparency and integrity throughout.