

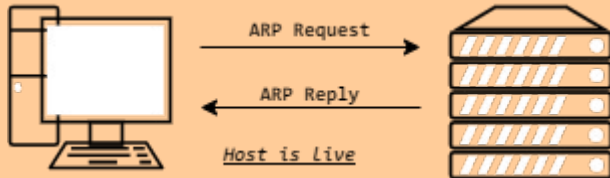
NMAP CHEAT SHEET

Basic Nmap Usage

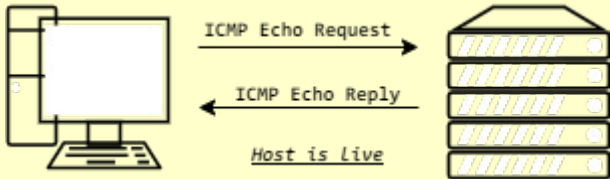
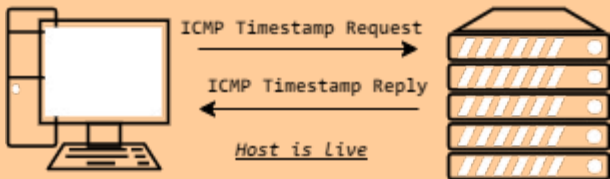
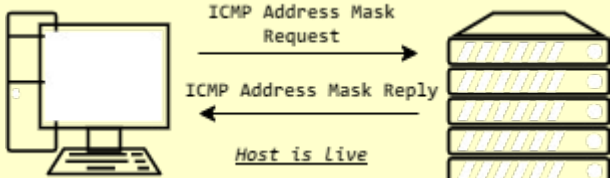
LIST: `nmap TARGET_IP example.com fake.com` (will scan 3 IP)

RANGE: `nmap 10.5.5.1-5` (will scan 5 IP address)

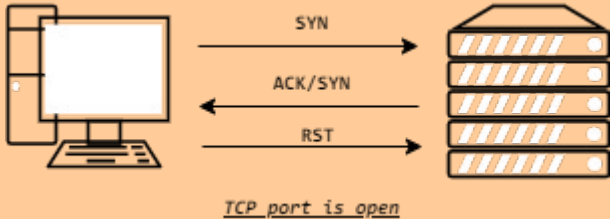
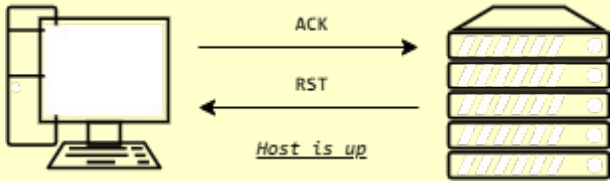
SUBNET: `nmap TARGET_IP/30` (will scan 4 IP address)

COMMAND	DESCRIPTION	USAGE
-iL	Used when you want to provide a list of targets.	<ul style="list-style-type: none"> <code>nmap -iL list_target.txt</code>
-n	No DNS lookup (DNS lookup is default for a nmap scan)	<ul style="list-style-type: none"> <code>nmap -n TARGET_IP</code>
-sL	For check the list of the host thea nmap will scan	<ul style="list-style-type: none"> <code>nmap -sL TARGET_IP/24</code>
-sn	Allow nmap to discover online hosts without port-scanning the live system	<ul style="list-style-type: none"> <code>nmap -sn TARGET_IP/24</code>
-PR	<p>Indicates we want only ARP scans. Only possible when we are on the same subnet of the target system.</p>  <pre> graph LR PC[Computer] -- ARP Request --> SRV[Server] SRV -- ARP Reply --> PC SRV --- HL[Host is Live] </pre>	<ul style="list-style-type: none"> <code>nmap -PR -sn TARGET_IP/24</code>

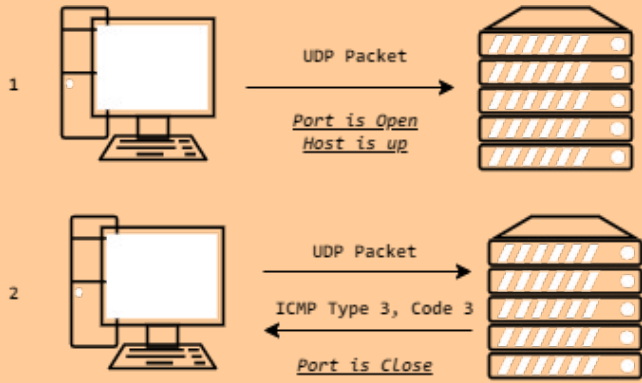
NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-PE	<p>Use a ICMP echo request (ping) to discover live host. ICMP echo request tend to be blocked.</p>  <pre> graph LR Host[Host] -- "ICMP Echo Request" --> Server[Server] Server -- "ICMP Echo Reply" --> Host Host --- Live[Host is Live] </pre>	<ul style="list-style-type: none"> • <code>nmap -PE -sn TARGET_IP</code> • <code>nmap -PE -sn TARGET_IP/24</code>
-PP	<p>Use ICMP Timestamp request to discover live host</p>  <pre> graph LR Host[Host] -- "ICMP Timestamp Request" --> Server[Server] Server -- "ICMP Timestamp Reply" --> Host Host --- Live[Host is Live] </pre>	<ul style="list-style-type: none"> • <code>nmap -PP -sn TARGET_IP</code> • <code>nmap -PP -sn TARGET_IP/24</code>
-PM	<p>Use ICMP Address Mask Request to discover live host</p>  <pre> graph LR Host[Host] -- "ICMP Address Mask Request" --> Server[Server] Server -- "ICMP Address Mask Reply" --> Host Host --- Live[Host is Live] </pre>	<ul style="list-style-type: none"> • <code>nmap -PM -sn TARGET_IP</code> • <code>nmap -PM -sn TARGET_IP/24</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-PS<ports>	<p>TCP SYN Ping. Send a packet with the SYN flag set. If not specify, -PS will use port 80 as default.</p> 	<ul style="list-style-type: none"> • <code>nmap -PS -sn TARGET_IP</code> • <code>nmap -PS -sn TARGET_IP/24</code> • <code>nmap -PS21 -sn TARGET_IP</code> • <code>nmap -PS21 -sn TARGET_IP/24</code> • <code>nmap -PS21-25 -sn TARGET_IP</code> • <code>nmap -PS21-25 -sn TARGET_IP/24</code> • <code>nmap -PS80,443,8080 -sn TARGET_IP</code> • <code>nmap -PS80,443,8080 -sn TARGET_IP/24</code>
-PA<ports>	<p>TCP ACK Ping. Send a packet with the ACK flag set. If not specify, -PS will use port 80 as default.</p> 	<ul style="list-style-type: none"> • <code>nmap -PA -sn TARGET_IP</code> • <code>nmap -PA -sn TARGET_IP/24</code> • <code>nmap -PA21 -sn TARGET_IP</code> • <code>nmap -PA21 -sn TARGET_IP/24</code> • <code>nmap -PA21-25 -sn TARGET_IP</code> • <code>nmap -PA21-25 -sn TARGET_IP/24</code> • <code>nmap -PA80,443,8080 -sn TARGET_IP</code> • <code>nmap -PA80,443,8080 -sn TARGET_IP/24</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-PU	<p>UDP Ping. Use a UDP packet to discover live hosts or open port. If we do not</p> 	<ul style="list-style-type: none"> • <code>nmap -PU -sn TARGET_IP</code> • <code>nmap -PU -sn TARGET_IP/24</code>
-R	Query DNS Server for also for offline hosts	<ul style="list-style-type: none"> • <code>nmap -R -sn TARGET_IP</code> • <code>nmap -R -sn TARGET_IP/24</code>
--dns-server <DNS SERVER>	For specify a DNS server	<ul style="list-style-type: none"> • <code>nmap -dns-server DNS_SERVER -sn TARGET_IP</code> • <code>nmap -dns-server DNS_SERVER -sn TARGET_IP/24</code>

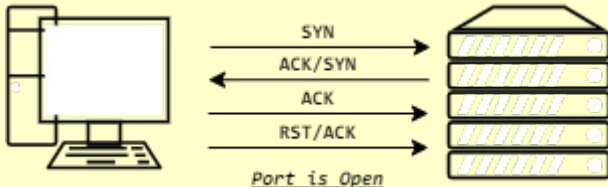
NMAP CHEAT SHEET

Port States

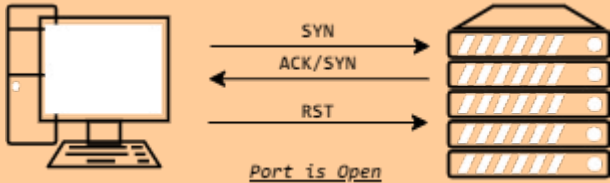
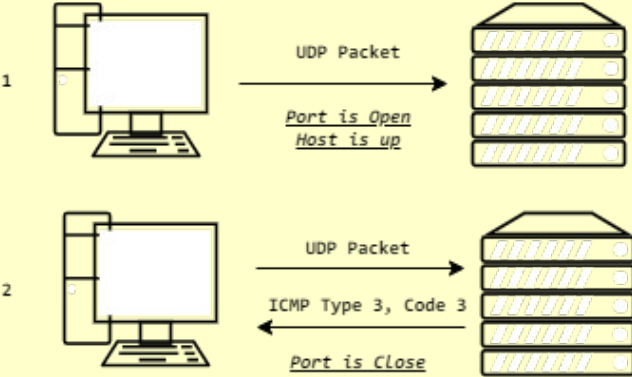
1. **OPEN**: service is listening on a specific port
2. **CLOSED**: No service is listening. Port is not blocked by a firewall
3. **FILTERED**: Port is not accessible due to a firewall.
4. **UNFILTERED**: Port is accessible, but nmap can't determine if the port is open or closed.
5. **OPEN|FILTERED**: nmap can't determine if the port is open or filtered
6. **CLOSED|FILTERED**: nmap can't determine if the port is closed or filtered

TCP Flags

1. **SYN**: Synchronize flag. Used to initiate the TCP 3-way handshake and synchronize the sequence numbers with the host.
2. **ACK**: Acknowledgment flag indicates that the acknowledgment number is significant.
3. **RST**: Reset flag is used to reset the connection. Also used when data is sent to a host and there is no service.
4. **URG**: Urgent flag indicates that the incoming data is urgent, so the segment is processed immediately.
5. **PSH**: Push flag asking TCP to pass the data to the application promptly.
6. **FIN**: The sender has no more data to send.

COMMAND	DESCRIPTION	USAGE
-F	Enable the fast mode scanning only the 100 most common ports instead of 1000.	<ul style="list-style-type: none">• <code>nmap -F TARGET_IP</code>
-r	Scan the port in consecutive order.	<ul style="list-style-type: none">• <code>nmap -r TARGET_IP</code>
-sT	<p>TCP scan. Complete the TCP 3-way handshake</p>  <pre>graph LR Client[Laptop] -- SYN --> Server[Server Rack] Server -- ACK/SYN --> Client Client -- ACK --> Server Note[Port is Open]</pre>	<ul style="list-style-type: none">• <code>nmap -sT TARGET_IP</code>

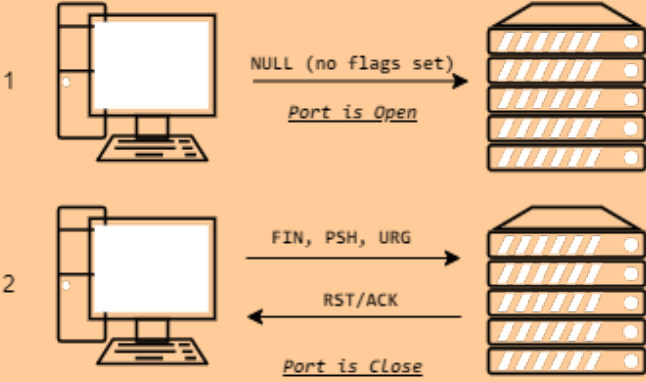
NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-sS	<p>TCP SYN scan. SYN scan does not need to complete the TCP 3-way handshake; instead, it tears down the connection once it receives a response from the server. Because we didn't establish a TCP connection, this decreases the chances of the scan being logged.</p>  <pre> sequenceDiagram participant Client participant Server Client->>Server: SYN Server-->>Client: ACK/SYN Client->>Server: RST Server-->>Client: Port is Open </pre>	<ul style="list-style-type: none"> <code>nmap -sS TARGET_IP</code>
-sU	<p>UDP Scan. UDP protocol does not require any handshake. If UDP port is close, an ICMP port is close ICMP error is returned.</p>  <pre> sequenceDiagram participant Client participant Server Note over Client: 1 Client->>Server: UDP Packet Server-->>Client: Port is Open Host is up Note over Client: 2 Client->>Server: UDP Packet Server-->>Client: ICMP Type 3, Code 3 Port is Close </pre>	<ul style="list-style-type: none"> <code>nmap -sU TARGET_IP</code>

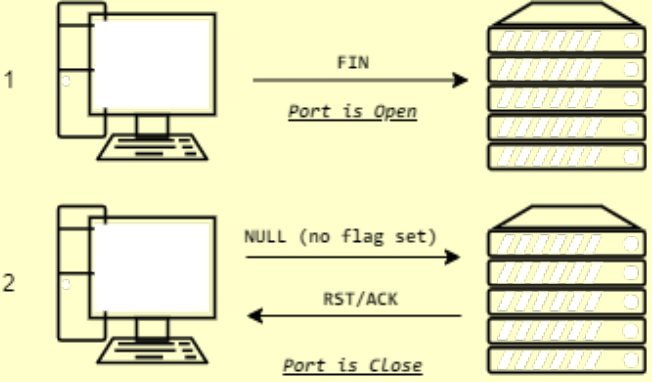
NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-p<ports>	Specify the port number to scan. If is not specify the 1000 most common ports are scanned	<ul style="list-style-type: none"> • nmap -p22 TARGET_IP • nmap -p22,80,443 TARGET_IP • nmap -p1-1000 TARGET_IP
-p-	All 65535 ports are scanned	<ul style="list-style-type: none"> • nmap -p- TARGET_IP
--top-ports <number port>	Specify the quantity of the most common port to scan. In the example on the right only the top 50 ports will be scanned	<ul style="list-style-type: none"> • nmap --top-ports 50 TARGET_IP
-T<0-5>	<p>Controlling the scan timing used. Default -T3.</p> <ul style="list-style-type: none"> • -T0 Paranoid (Slowest. Scan one port at a time and wait 5 minutes between the scanning) • -T1 Sneaky (Most used during real engagements) • -T2 Polite • -T3 Normal (Nmap Default scan timing) • -T4 Aggressive (often used during CTFs and when learning to scan on practice targets) • -T5 Insane (Most aggressive in terms of speed; however, this can affect the accuracy of the scan results due to the increased likelihood of packet loss) 	<ul style="list-style-type: none"> • nmap -T0 TARGET_IP
--min-rate <number> --max-rate <number>	Controlling the packet rate. Indicate the number of packet send it per second.	<ul style="list-style-type: none"> • nmap --min-rate 50 TARGET_IP • nmap --min-rate=50 TARGET_IP • nmap --max-rate 50 TARGET_IP • nmap --max-rate=50 TARGET_IP

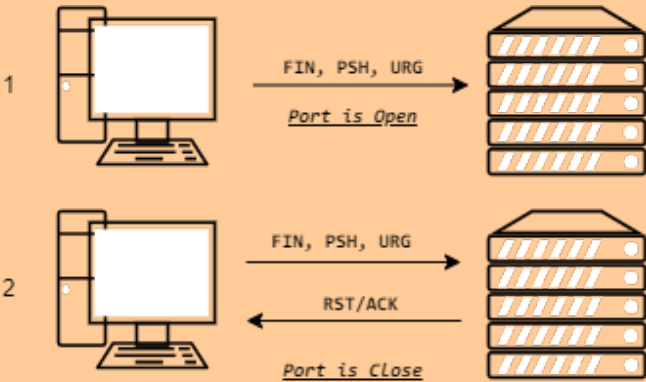
NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
--min-parallelism <probes> --max-parallelism <probes>	Controlling the Probing parallelization. Nmap probes the targets to discover which hosts are live and which ports are open; probing parallelization specifies the number of such probes that can be run in parallel.	<ul style="list-style-type: none"> • <code>nmap --min-parallelism 512 TARGET_IP</code> • <code>nmap --min-parallelism=512 TARGET_IP</code> • <code>nmap --max-parallelism 512 TARGET_IP</code> • <code>nmap --max-parallelism=512 TARGET_IP</code>
-sN	<p>NULL scan. Does not set any flag. A TCP packet with no flag will not trigger any response when reaches a open port. For nmap a no response indicate that the port is open or a firewall is blocking the packet. So the result will be OPEN FILTERED.</p>  <pre> sequenceDiagram participant Client participant Server Note over Client: 1 Client->>Server: NULL (no flags set) Server-->>Client: Port is Open Note over Client: 2 Client->>Server: FIN, PSH, URG Server-->>Client: RST/ACK Note over Client: Port is Close </pre>	<ul style="list-style-type: none"> • <code>nmap -sN TARGET_IP</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-sF	<p>FIN Scan. FIN flag set. Similar a NULL scan, no response will be sent if the TCP port is open. For nmap a no response indicate that the port is open or a firewall is blocking the packet. So the result will be OPEN FILTERED.</p>  <p>The diagram illustrates the FIN scan process in two steps. In step 1, a client (represented by a computer icon) sends a FIN packet to a server (represented by a server rack icon). The packet is labeled 'FIN' and 'Port is Open'. In step 2, the client sends a NULL packet (no flag set) to the server. The server responds with an RST/ACK packet, labeled 'RST/ACK' and 'Port is Close'.</p>	<ul style="list-style-type: none"> <code>nmap -sF TARGET_IP</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-sX	<p>XMAS Scan. FIN, PSF and URG flags are set. Similar a NULL and FIN scans, no response will be sent if the TCP port is open. For nmap a no response indicate that the port is open or a firewall is blocking the packet. So the result will be OPEN FILTERED.</p>  <p>The diagram illustrates the XMAS Scan process in two scenarios. In scenario 1, a host (represented by a computer icon) sends a packet with FIN, PSF, and URG flags to a server (represented by a server rack icon). The server responds with 'Port is Open'. In scenario 2, the host sends a similar packet, but the server responds with 'RST/ACK' and 'Port is Close'.</p>	<ul style="list-style-type: none"> <code>nmap -sX TARGET_IP</code>
-sA	<p>TCP ACK Scan. The packet has the ACK flag set. This type of scan is more suitable to discover firewall rule sets and configuration. If we scan a target that doesn't have a firewall in the front, all ports will response to our ACK with a RST, no matter if the port is open or close. If a firewall is sitting in front of our target the result can be different. It can show some port as UNFILTERED, meaning that the firewall is not blocking those ports.</p>	<ul style="list-style-type: none"> <code>nmap -sA TARGET_IP</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-sW	Window Scan. Also this scan send a TCP packet with the ACK flag set, but examines the TCP Window field of the RST packets returned, because this can reveal that the port is open. However, also this scan is more suitable to discover firewall rule sets and configuration. Against target without firewall we will not get any result. On the contrary, with a firewall we can get some result showing us that some ports are CLOSED . We don't know that those port are really close or not, but we know that responded differently because the firewall does not block them.	<ul style="list-style-type: none"> <code>nmap -sW TARGET_IP</code>
--scanflags <CUSTOM_FLAGS>	Custom scan. We can customize the flag to set on our TCP packet. We need to know how the different ports will responde, to interpret correctly the results in different scenarios.	<ul style="list-style-type: none"> <code>nmap --scanflags RSTACKFIN TARGET_IP</code>
-Pn	Disable Ping scan.	<ul style="list-style-type: none"> <code>nmap -Pn TARGET_IP</code>
-e <NETWORK_INTERFACE>	Specify the network interface to use	<ul style="list-style-type: none"> <code>nmap -e NETWORK_INTERFACE TARGET_IP</code>
-S <SPOOFED_IP>	For spoofing the IP address. Such a scan is reliable only if we can guarantee to capture the response.	<ul style="list-style-type: none"> <code>nmap -e NETWORK_INTERFACE -Pn -S SPOOFED_IP TARGET_IP</code>
--spoof-mac <SPOOFED_MAC>	For spoofing the MAC address. Such a scan is reliable only if we are on the same subnet as the target machine. This address spoofing is only possible if the attacker and the target machine are on the same Ethernet (802.3) network or same WiFi (802.11).	<ul style="list-style-type: none"> <code>nmap -e NETWORK_INTERFACE -Pn --spoof-mac SPOOFED_MAC TARGET_IP</code>

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
-D	DECOY. The concept is simple, make the scan appears to be coming from many IP addresses so that the attacker's IP address would be lost among them. RDN assign randomly IP address.	<ul style="list-style-type: none"> <code>nmap -D 10.5.5.1,10.5.5.2,ATTACKER_IP TARGET_IP</code> <code>nmap -D RDN,RDN,ATTACKER_IP TARGET_IP</code>
-f -f -f -ff	Fragmented Packet. We can get some benefit, using the fragmentation, depending from the firewall and IDS. The IP data will be split in 8 bytes (-f), or in 16 bytes (-f -f, -ff)	<ul style="list-style-type: none"> <code>nmap -sS -p80 -f TARGET_IP</code> <code>nmap -sS -p80 -f -f TARGET_IP</code> <code>nmap -sS -p80 -ff TARGET_IP</code>
-mtu <VALUE>	Choose manually the value of the fragmentation. However, a multiple of 8 should always be used	<ul style="list-style-type: none"> <code>nmap -sS -p80 -mtu 24 TARGET_IP</code>
--data-length <VALUE>	To increase the size of the packet. It may look innocuous.	<ul style="list-style-type: none"> <code>nmap -sS -p80 --data-length 512 TARGET_IP</code>

NMAP CHEAT SHEET

COMMAND

```
-sI <ZOMBIE_IP>
```

USAGE

```
nmap -sI ZOMBIE_IP MACHINE_IP
```

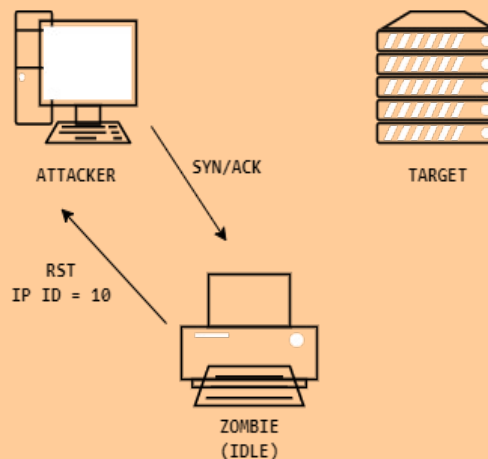
DESCRIPTION

IDLE/ZOMBIE Scan. This scan requires an idle(zombie) system connected to the network that we can communicate with. Practically, Nmap will make each probe appear as if coming from the idle (zombie) host, then it will check for indicators whether the idle (zombie) host received any response to the spoofed probe. This is accomplished by checking the IP identification (IP ID) value in the IP header.

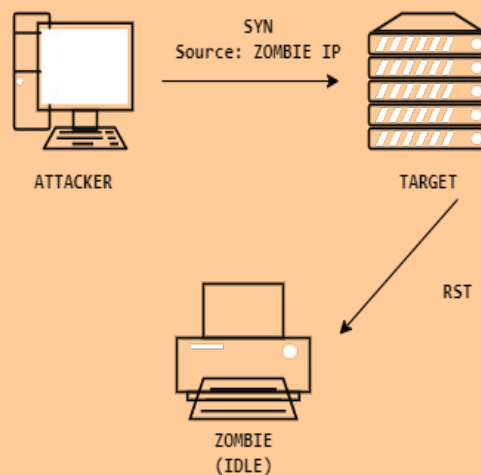
The idle (zombie) scan requires the following three steps to discover whether a port is open:

1. Trigger the idle host to respond so that you can record the current IP ID on the idle host.
2. Send a SYN packet to a TCP port on the target. The packet should be spoofed to appear as if it was coming from the idle host (zombie) IP address.
3. Trigger the idle machine again to respond so that you can compare the new IP ID with the one received earlier.

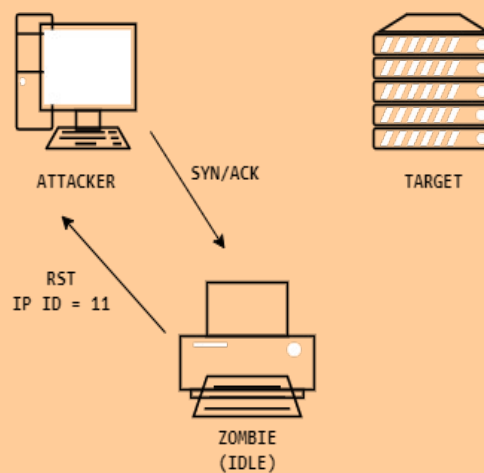
Discover the IP ID on the idle host



NMAP CHEAT SHEET

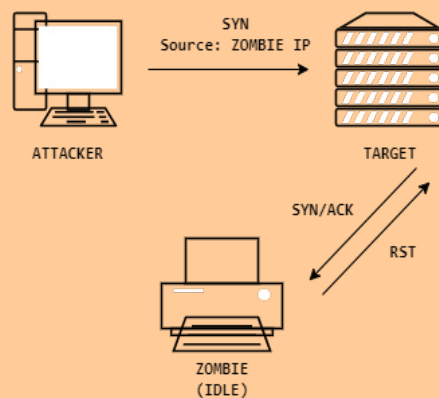


We send another SYN/ACK to the Zombie and we see that the IP ID increase only by 1. The RST received from the target did not trigger a response so the IP ID did not increase.

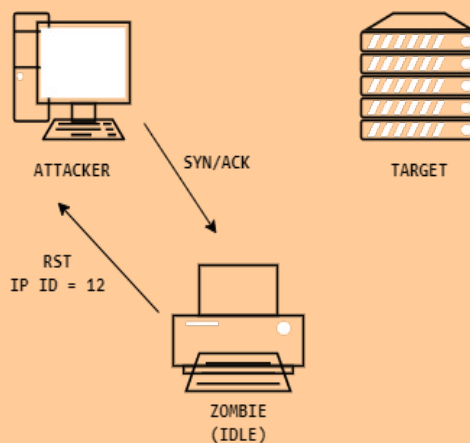


NMAP CHEAT SHEET

Second Scenario: Port Open



We send another SYN/ACK to the Zombie and we see that the IP ID increase by 2. The SYN/ACK received from the target did trigger a response so the IP ID increased of 1.



The attacker needs to compare the IP ID of the RST packet received in the first step with the IP ID of the RST packet received in the third step. If the difference is 1, it means the port on the target was closed or filtered, if the difference is 2, it means that the port on the target was open.

NMAP CHEAT SHEET

COMMAND	DESCRIPTION	USAGE
--reason	Give us the reason why Nmap concluded a port is open or a host is up.	<ul style="list-style-type: none"> <code>nmap -sS --reason TARGET_IP</code>
-v	For verbose output	<ul style="list-style-type: none"> <code>nmap -sS --reason -v TARGET_IP</code>
-v -v -vv	Even more verbose	<ul style="list-style-type: none"> <code>nmap -sS --reason -v - v TARGET_IP</code> <code>nmap -sS --reason -vv TARGET_IP</code>
-d	Debugging details	<ul style="list-style-type: none"> <code>nmap -sS -d TARGET_IP</code>
-dd	Even more Debugging details	<ul style="list-style-type: none"> <code>nmap -sS -dd TARGET_IP</code>
-sV <i>Options:</i> --version-intensity <LEVEL> --version-light --version-all	Collect information about the services running on the port. -sV will force 3-way handshake. No possible with -sS. Intensity level from 0 (lightest) to 9. --version-light is set on 2, while --version-all is set on 9.	<ul style="list-style-type: none"> <code>nmap -sV TARGET_IP</code> <code>nmap -sV --version-intensity 5 TARGET_IP</code> <code>nmap -sV --version-light TARGET_IP</code> <code>nmap -sV --version-all TARGET_IP</code>
-O	Try to detect the Operating System,	<ul style="list-style-type: none"> <code>nmap -sS -O TARGET_IP</code>
--traceroute	Find the routers between us and the target.	<ul style="list-style-type: none"> <code>nmap -sS --traceroute TARGET_IP</code>

NMAP CHEAT SHEET

The Script folder can be found at /use/share/nmap/scripts.

There are almost 600 scripts divided in the following categories:

- auth – authentication related scripts
- broadcast – discover hosts
- brute – for brute-force password auditing against logins
- default – default scripts
- discovery – try to get accessible information (example: DNS names, database name and tables)
- dos – check for server vulnerable to DoS attack
- exploit – try to exploit vulnerable services
- external – check and use a third party service
- fuzzer – for fuzzing attacks
- intrusive – intrusive scripts. Include brute-force and exploitation
- malware – backdoor scanner
- safe – script that won't crash the target
- version – check version service
- vuln – check for vulnerability or vulnerable services

COMMAND	DESCRIPTION	USAGE
-sC --script=default	Run the default script	<ul style="list-style-type: none"> • nmap -sS -sC TARGET_IP • nmap -sS --script=default TARGET_IP
--script <"SCRIPT_NAME"> --script <"SCRIPT_NAME*">	To run a specific script(s), using the name or a pattern	<ul style="list-style-type: none"> • nmap -sS -n --script "SCRIPT" TARGET_IP • nmap -sS -n --script "SCR*" TARGET_IP
-oN <FILE_NAME>	Save output in normal format	<ul style="list-style-type: none"> • nmap -sS TARGET_IP -oN FILE_NAME
-oG <FILE_NAME>	Save output in grepable format	<ul style="list-style-type: none"> • nmap -sS TARGET_IP -oG FILE_NAME
-oX <FILE_NAME>	Save output in XML format	<ul style="list-style-type: none"> • nmap -sS TARGET_IP -oX FILE_NAME
-oA <FILE_NAME>	Save 3 outputs in normal, grepable and XML format.	<ul style="list-style-type: none"> • nmap -sS TARGET_IP -oA FILE_NAME
-oS <FILE_NAME>	Save output in script kiddie format. NOT USEFUL	<ul style="list-style-type: none"> • nmap -sS TARGET_IP -oS FILE_NAME