Nmap Essentials Sheet

Most network servers are listening in TCP ports. Consider a port to be open if it's in a listening state, but closed if it is not.

TCP uses the three-way handshake: SYN, SYN-ACK, ACK for communications, as well as a few other flags which include FIN, RST, URGENT, PUSH

- **SYN** – (Synchronize) Initiate a connection
- **ACK** – (Acknowledge) Acknowledge that a packet has been received
- **FIN** – (Finish) The device has nothing more to send and the connection can be closed
- **RST** – (Reset) Resets a connection, often due to timeout.
- **URG** – (Urgent) Indicates that data in packet is to be processed immediately.
- **PSH** – (Push) Sends out all buffered data in the TCP sliding window.

Scan type:	Command	Flags set (Outgoing)	Response if Open	Response if closed
SYN (Stealth)	nmap -sS	SYN	SYN/ACK	RST
3 Way connect	nmap -sT	SYN	SYN/ACK	SYN/ACK
Fin	nmap -sF	FIN	none	RST
XMAS	nmap -sX	FIN,URG,PUSH	none	RST
Null	nmap -sN	None	none	RST

NOTE:

Inverse scans (Fin scan, Xmas scan, Null Scan) only work on operating systems that are compliant with RFC-793 TCP implementation. Windows systems are not compliant, so these scans have no effect.

You can scan multiple networks at once, though it takes time.
Example: nmap -sP 192.168.1-5.*

Nmap will try to determine the operating system that is present, but sometimes it cannot. You might be able to make a reasonable assumption based off which ports are open. For example, systems with 389 or 636 open may be using LDAP(S). This indicates that it's likely a Windows Domain Controller.

Additional Scans

ACK scans can tell you if there is a stateful firewall.
Command: nmap -sA
Response if stateful firewall exists: None
Response if stateful firewall is not there: RST

IDLE Scans allow you to use a device that is idle on the network for scanning. This technique allows us to forge packets to look like they came from the inactive device, and by watching the response to that device it is possible to determine information about the target. This can be done in nmap via a command such as: nmap -Pn -p 80 -sI [idle-system] [target-system]. It is important to include -Pn (no ping) to prevent sending an initial Ping to the target and disclosing your identity.

How IDLE scans work

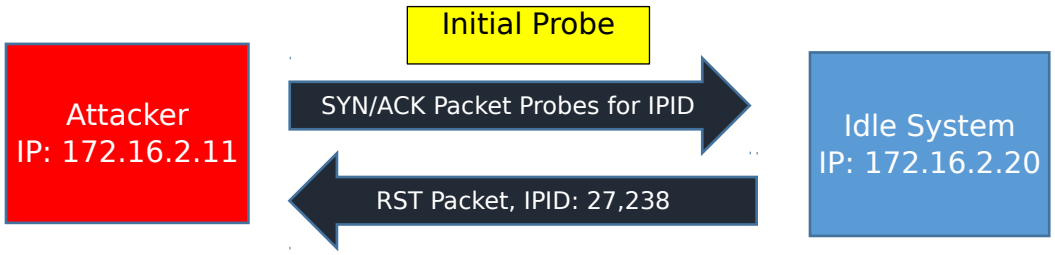
Step 1: Choose an idle system and probe for its current IPID (Sequence number)

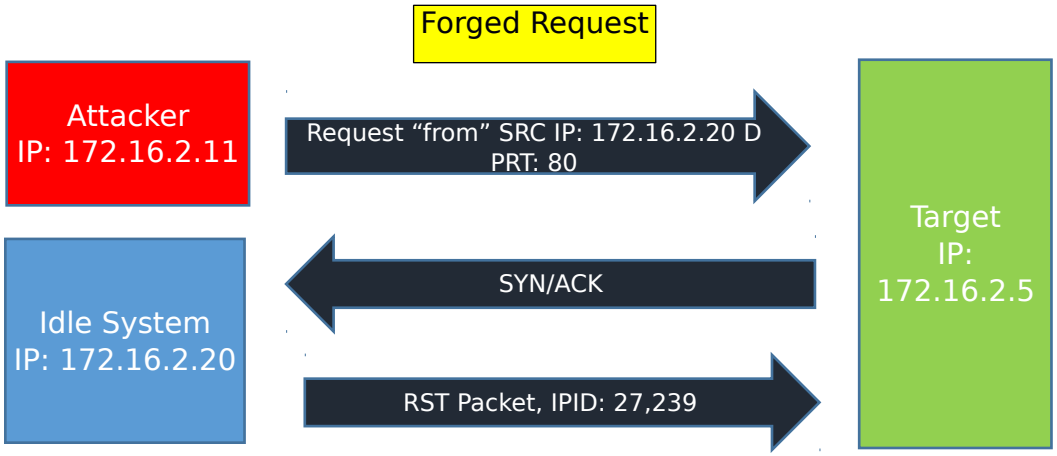
Step 2: Send the spoofed packed to the target so it looks like it came from the idle system.

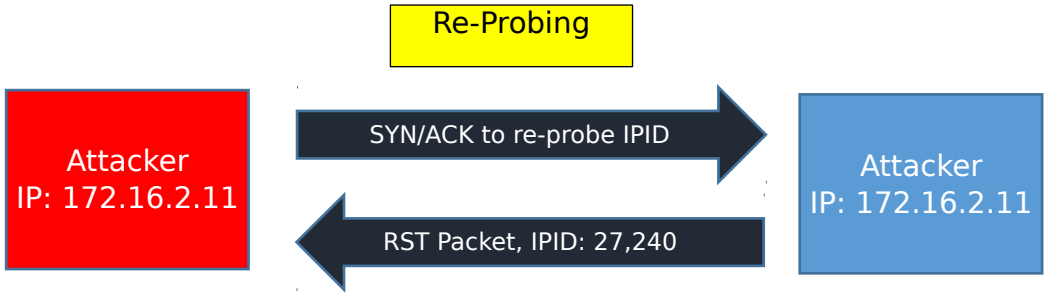
Step 3: If target responds with SYN/ACK, the port is open. The idle system will not be expecting anything from the target, and so sends a RST packet, incrementing it's IPID by 1. If the port is closed, a RST is sent from target to idle system, which the idle system ignores.

Step 4:Re-probe the idle system. If it's IPID incremented by 2, the target systems port is open. For example, let's say our initial probe of the idle system revealed an IPID of 27,238. After Step 2, if the target responds with SYN/ACK, the idle system responds with a RST and an IPID of 27,239. Now when we re-probe we should see an IPID of 27,240. Had target port been closed, the idle system would never have done anything to increment its IPID and so we would see it increment by 1.

See the visual representation on the next page.







IPID incremented by 2. Then the port is open. Had the target sen a RST instead of SYN/ACK, the idle system would not have incremented its sequence number, so when re-probing we should see it increment by a value of 1.

Additional nmap options

Don't ping: -P0 -PN -Pn -PD

Operating System Detection

- Fingerprinting: -O
- Aggressive: -A

Service Version Detection

- Version: -sV
- Windows Scan: -sW

Select port or port range

- single port: -p 53
- specific ports: -p 23, 53, 80, 445
- range + specific ports: -p 1-1024, 3389
- range of ports: -p 1-1024
- all 65,535 ports: -p-
- 100 most popular ports: -F
- Specify ports NOT to scan: --exclude-ports
- All ports equal to or less than a number: -p [-1024]
- All ports equal to or greater than a number: -p [1024-]

Example: nmap -sS -O -p 1-1024, 1701, 3306, 3389 192.168.1.10-100

This executes a stealth scan with OS fingerprinting on ports 1-1024, 1701, 3306, and 3389. It scans the IP address range of 192.168.1.10 through 192.168.1.100.

UDP Scan -sU
Note: UDP scans take longer than TCP because if the port is open there should be no response. If the port is closed we expect an ICMP message with "destination unreachable"

but sometimes this never shows up. If there is no reply nmap will re-try in case the packet was lost. Linux systems in particular limit this message to 1 per second so UDP scans can take a very long time. Try using a –F for “fast scan”, as this will only search the most popular ports.

Timing Options

Set time to live: --ttl

Timing: --timing -T use 0-5 after these options to set how aggressive the scan is. The format is as follows: 0 = paranoid, 1= sneaky, 2=polite, 3=normal, 4=aggressive, 5=insane Timing differences come down to milliseconds but can mean the difference between a scan being discovered or remaining undetected.

Note: This is not an all-inclusive guide, but a good starting point. Refer to the nmap web site or manual pages for more advanced options and information on the nmap scripting engine.