Nmap

https://nmap.org/

Written by Alireza Liaghat || linkedin.com/in/alireza-lia/
Reviewed by Dale Hobbs || linkedin.com/in/dale-hobbs/

Nmap + Target + Type + Port + Detection + Timing + Scripts + Evasion

The Nmap Formula

TARGET | What do you want to scan?

- Scan the specified IP address: `192.168.x.x`
  Used when there is only one target IP address.
- Scan the specified domain: `domain.com`
  Used when there is only one target domain.
- Scan from a list of host addresses: `-iL target.txt`
  Used when searching a known range of hosts.
- Scans each address only once: `--unique`
  Used in combination with lists. Avoids duplicate scans to speed up the scan.
- No DNS resolution: `-n`
  Speeds up scanning by skipping reverse DNS resolution.

TYPE | How do you want to scan?

- Full TCP 3-Way Handshake Scan: `-sT`
  Most reliable scan. Use when not worried about firewalls.
- "Stealth" scan. Impartial 3-Way Handshake: `-sS`
  Does not establish a full handshake. "Dumb" firewalls will only see this as regular poor connection.
- Scan using UDP: `-sU`
  Preferred for scanning DNS (53), SNMP (161), DHCP (67), TFTP (69), etc.

PORT | What port do you want to scan?

- Scans only the comma-separated ports: `-p 80,443`
  Useful for when scanning a host for a specific attack surface.
- Scans all possible ports: `-p 1-65535`
  Useful for all ports in use, including ephemeral (temporary) ports.

DETECTION | What do you want to detect?

- Probe for service/version: `-sV`
  Useful for when mapping and identifying a network.
- Try the most likely probes for detection: `--version-light`
  Useful for when mapping and identifying a network.
- Try every available probe (max intensity): `--version-all`
  Useful for when mapping and identifying a network.
- OS Detection: `-O`
  Useful for when mapping and identifying a network.

TIMING | How fast do you want to scan?

- Sends a maximum of 5 probes per second: `--max-rate 5`
  Limits network traffic to avoid disruptions to the network.
- Adds 1 second delay between probes: `--scan-delay 1`
  Limits network traffic to avoid disruptions to the network.
- Give up on a particular port after 1 second: `--host-timeout 1`
  Limits network traffic and useful for slow responding devices.

SCRIPTS | What additional scripts do you want?

- Performs a WHOIS lookup of domains and IP addresses: `--script=whois`
  Used when mapping a network.
- Enumerates SMB shares: `--scripts=smb-enum-shares`
  Identifies SMB shares that might be exposed.
- Searches for known vulnerabilities: `--script=vulners`
  Identifies known/unpatched vulnerabilities in a network.

EVASION | How sneaky do you want to be?

- Spoofs the source MAC address: `-spoof-mac 00:0C:29:6F:F3:6B`
  Useful for when the network switch restricts connectivity using MAC addresses.
- Spoofs the source IP address: `S 192.168.1.1`
  Useful for when the network switch restricts connectivity using IP addresses.
- Adds random data to packets: `--data-length 5`
  Useful for when trying to camouflage the network traffic caused by the scan.
- Uses a proxy to scan: `--proxies 192.168.5.5`
  Useful for when navigating a scan through an IP-based filter.

Example formula of a slow and thorough search

Common Port States	
`open`	An application is actively accepting TCP connections or UDP datagrams on this port.
`closed`	The port is accessible. Nmap probes received a response but was indicated that there is no application listening.
`filtered`	Nmap cannot determine if the port is open. This could be caused by firewalls dropping packets or by network congestion.