Scanning techniques

- ▶Xmas scan
- ▶-sX
- ▶TCP SYN scan
 - ▶-sS
- ►Connect scan
 - ▶-sT
- ▶ACK scan
- ▶Window scan
 - ►-sW
- ▶Maimon scan
 - ► SM
- ►UDP scan
- ▶TCP Null scan
- ▶FIN scan
- ►SCTP INIT scan
 - ►-sY
- ►C00KIE-ECH0 scan
 - ▶-sZ
- ▶IP protocol scan
 - **▶**-s0

Host discovery

- ▶List scan
- ▶Ping scan
- ▶Treat all hosts as online
- ▶Discovery to given ports: TCP SYN/ ACK, UDP, SCTP
- ►-PS/PA/PU/PY <port list> ►ICMP echo, timestamp, and netmask
- request discovery probes
- ►-PE/PP/PM
- ▶IP Protocol ping
 - ►-P0 protocol list>
- ▶DNS resolution: never/always (default: sometimes)
- ▶-n/R

OS detection

- ▶Enable OS detection
- ►Limit detection to promising targets
- ▶--osscan-limit
- ▶Guess OS more aggressively
 - ▶--osscan-guess

Timing & performance

- ▶Serial. slowest
- ►-T0
- ▶Serial, slow
- ▶-T1
- ▶Serial
- ▶-T2
- ▶Parallel
- ▶-T3
- ▶Parallel, fast
- ▶-T4

Target specification

- ▶Input list of hosts/Networks from file
- ▶-iL <fileName.txt> ▶Scan Random Hosts
- ▶-iR <number>
- ▶Exclude host/Networks
- ►--exclude <host>
- ▶Exclude host/Networks from file
- ▶--excludefile <hostFile.txt>

Port specification & scan order

- ▶Specify ports
 - ►-p <port>,<port>,<...>/<1-65535>
- ▶Scan UDP ports
 - ▶-p U:<port>
- ▶Fast mode, scans few ports
- ►Scan ports consecutively
- ►Scan number of top ports
 - ►--top-ports <number>
- ▶Scan ports more common than ratio
- ▶-port-ratio <number>

NMAP output options

- ▶Output normal
- ▶Output XML
- ►Output greppable
 - ►-oG
- ▶Output all 3 formats
- ▶Verbose
- ▶ Debuggung
 - ►-d/-dd

Service version detection

- ▶Probe open ports to determine service/ version info
 - ▶-sV
- ▶Version intensity
 - ▶--version-intensity <0-9>
- ▶Limit to most likely probes (intensity 2)
- ▶Try all probes (intensity 9)
 - ▶--version-all
- ▶Show scan activity
- ▶--version-trace

Firewall/IDS evasion & spoofing

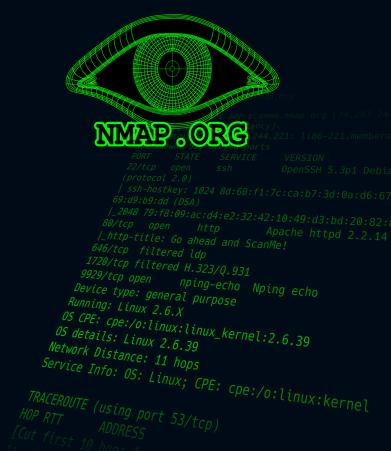
- ▶Fragment IP packets (including ping scans). Can add offset size
 - ►-f [--mtu <value>]
- ▶Cloak scanwith decoys
 - ►-D <decoy>,<decoy>
- ▶Spoof source address
- ▶Use specified interface
- ▶Send packets with specified ip option
- ▶--ip-options <option>
- ▶Set IP time to live field
- ▶--ttl <value>

HTTP service information

- ▶ Gather page titles from HTTP services
- ▶--script=http-title <host>
- ▶Get HTTP headers of web services
- ▶--script=http-headers <host>
- ▶Find web apps from known paths ▶--script=http-enum <host>
- Script scan
- ▶Script default
- ▶Provide NSE script args in a file
- ▶-script-args-file=<filename>
- ▶Show all data sent and received
- ▶--script-trace ▶Show script help

▶--script-args=unsafe=1

▶Potential to crash servers/service



Various TCP/IP protocols

Application layer:

▶FTP, HTTP, SNMP, BOOTP, DHCP

Transport layer: ▶TCP, UDP, ICMP, IGMP

Network layer:

►ARP, IP, RARP

►SLIP, PPP

Data link layer:

Script categories

- **►**ALL
- **►**AUTH
- **▶**DEFAULT
- **▶**DISCOVERY
- **►**EXTERNAL **▶INTRUSIVE**
- **►**MALWARE
- **►**SAFE
- ►VULN, etc

https://github.com/cuanknaggs/nmap-docs