

Basic Scanning Techniques

Nmap Query	Nmap Command
Scan a single target	<code>nmap [target]</code>
Scan multiple targets	<code>nmap [target1,target-2,etc]</code>
Scan a list of targets	<code>nmap -iL [list.txt]</code>
Scan a range of hosts	<code>nmap [range of IP addresses]</code>
Scan an entire subnet	<code>nmap [IP address/cdir]</code>
Scan random hosts	<code>nmap -iR [number]</code>
Excluding targets from a scan	<code>nmap [targets] -exclude [targets]</code>
Excluding targets using a list	<code>nmap [targets] --exclude-file [list.txt]</code>
Perform an aggressive scan	<code>nmap -A [target]</code>
Scan an IPv6 target	<code>nmap -6 [target]</code>

Version Detection

Nmap Query	Nmap Command
Operating system detection	<code>nmap -O [target]</code>
Attempt to guess an unknown	<code>nmap -O --osscan-guess [target]</code>
Service version detection	<code>nmap -sV [target]</code>
Troubleshooting version scans	<code>nmap -sV --version-trace [target]</code>
Perform a RPC scan	<code>nmap -sR [target]</code>

Discover Options

Nmap Query	Nmap Command
Perform a ping scan only	<code>nmap -sP [target]</code>
Don't ping	<code>nmap -PN [target]</code>

Discover Options (cont)

TCP SYN Ping	<code>nmap -PS [target]</code>
TCP ACK ping	<code>nmap -PA [target]</code>
UDP ping	<code>nmap -PU [target]</code>
SCTP Init Ping	<code>nmap -PY [target]</code>
ICMP echo ping	<code>nmap -PE [target]</code>
ICMP Timestamp ping	<code>nmap -PP [target]</code>
ICMP address mask ping	<code>nmap -PM [target]</code>
IP protocol ping	<code>nmap -PO [target]</code>
ARP ping	<code>nmap -PR [target]</code>
Traceroute	<code>nmap --traceroute [target]</code>
Force reverse DNS resolution	<code>nmap -R [target]</code>
Disable reverse DNS resolution	<code>nmap -n [target]</code>
Alternative DNS lookup	<code>nmap --system-dns [target]</code>
Manually specify DNS servers	<code>nmap --dns-servers [servers] [target]</code>
Create a host list	<code>nmap -sL [targets]</code>

Scripting Engine

Nmap Query	Nmap Command
Execute individual scripts	<code>nmap --script [script.t.nse] [target]</code>
Execute multiple scripts	<code>nmap --script [expression] [target]</code>
Execute scripts by category	<code>nmap --script [cat] [target]</code>
Execute multiple scripts categories	<code>nmap --script [cat1,-cat2, etc]</code>
Troubleshoot scripts	<code>nmap --script [script] --script-trace [target]</code>

Scripting Engine (cont)

Update the script database	<code>nmap --script-updatedb</code>
----------------------------	-------------------------------------

Firewall Evasion Techniques

Nmap Query	Nmap Command
Fragment packets	<code>nmap -f [target]</code>
Specify a specific MTU	<code>nmap --mtu [MTU] [target]</code>
Use a decoy	<code>nmap -D RND:[number] [target]</code>
Idle zombie scan	<code>nmap -sl [zombie] [target]</code>
Manually specify a source port	<code>nmap --source-port [port] [target]</code>
Append random data	<code>nmap --data-length [size] [target]</code>
Randomize target scan order	<code>nmap --randomize-hosts [target]</code>
Spoof MAC Address	<code>nmap --spooof-mac [MAC 0 vendor] [target]</code>
Send bad checksums	<code>nmap --badsum [target]</code>

Output Options

Nmap Query	Nmap Command
Save output to a text file	<code>nmap -oN [scan.txt] [target]</code>
Save output to a xml file	<code>nmap -oX [scan.xml] [target]</code>
Grepable output	<code>nmap -oG [scan.txt] [target]</code>
Output all supported file types	<code>nmap -oA [path/filename] [target]</code>
Periodically display statistics	<code>nmap --stats-every [time] [target]</code>
133t output	<code>nmap -oS [scan.txt] [target]</code>

