Nmap Cheat Sheet

pentestlab.blog/category/general-lab-notes/page/14

August 17, 2012

Basic Scanning Techniques

Scan a single target —> **nmap [target]**

Scan multiple targets —> **nmap [target1,target2,etc]**

Scan a list of targets —-> **nmap -iL [list.txt]**

Scan a range of hosts —-> **nmap [range of IP addresses]**

Scan an entire subnet —-> **nmap [IP address/cdir]**

Scan random hosts —-> **nmap -iR [number]**

Excluding targets from a scan —> **nmap [targets] –exclude [targets]**

Excluding targets using a list —> **nmap [targets] –excludefile [list.txt]**

Perform an aggressive scan —> **nmap -A [target]**

Scan an IPv6 target —> **nmap -6 [target]**

Discovery Options

Perform a ping scan only —> **nmap -sP [target]**

Don’t ping —> **nmap -PN [target]**

TCP SYN Ping —> **nmap -PS [target]**

TCP ACK ping —-> **nmap -PA [target]**

UDP ping —-> **nmap -PU [target]**

SCTP Init Ping —> **nmap -PY [target]**

ICMP echo ping —-> **nmap -PE [target]**

ICMP Timestamp ping —> **nmap -PP [target]**

ICMP address mask ping —> **nmap -PM [target]**

IP protocol ping —-> **nmap -PO [target]**

ARP ping —> **nmap -PR [target]**

Traceroute —> **nmap –traceroute [target]**

Force reverse DNS resolution —> **nmap -R [target]**

Disable reverse DNS resolution —> **nmap -n [target]**

Alternative DNS lookup —> **nmap –system-dns [target]**

Manually specify DNS servers —> **nmap –dns-servers [servers] [target]**

Create a host list —-> **nmap -sL [targets]**

Advanced Scanning Options

TCP SYN Scan —> **nmap -sS [target]**

TCP connect scan —-> **nmap -sT [target]**

UDP scan —-> **nmap -sU [target]**

TCP Null scan —-> **nmap -sN [target]**

TCP Fin scan —> **nmap -sF [target]**

Xmas scan —-> **nmap -sX [target]**

TCP ACK scan —> **nmap -sA [target]**

Custom TCP scan —-> **nmap –scanflags [flags] [target]**

IP protocol scan —-> **nmap -sO [target]**

Send Raw Ethernet packets —-> **nmap –send-eth [target]**

Send IP packets —-> **nmap –send-ip [target]**

Port Scanning Options

Perform a fast scan —> **nmap -F [target]**

Scan specific ports —-> **nmap -p [ports] [target]**

Scan ports by name —-> **nmap -p [port name] [target]**

Scan ports by protocol —-> **nmap -sU -sT -p U:[ports],T:[ports] [target]**

Scan all ports —-> **nmap -p “*” [target]**

Scan top ports ——> **nmap –top-ports [number] [target]**

Perform a sequential port scan —-> **nmap -r [target]**

Version Detection

Operating system detection —-> **nmap -O [target]**

Submit TCP/IP Fingerprints —-> **http://www.nmap.org/submit/**

Attempt to guess an unknown —-> **nmap -O –osscan-guess [target]**

Service version detection —-> **nmap -sV [target]**

Troubleshooting version scans —-> **nmap -sV –version-trace [target]**

Perform a RPC scan —-> **nmap -sR [target]**

Timing Options

Timing Templates —-> **nmap -T [0-5] [target]**

Set the packet TTL —-> **nmap –ttl [time] [target]**

Minimum of parallel connections —-> **nmap –min-parallelism [number] [target]**

Maximum of parallel connection —-> **nmap –max-parallelism [number] [target]**

Minimum host group size ——> **nmap –min-hostgroup [number] [targets]**

Maximum host group size —-> **nmap –max-hostgroup [number] [targets]**

Maximum RTT timeout ——> **nmap –initial-rtt-timeout [time] [target]**

Initial RTT timeout —-> **nmap –max-rtt-timeout [TTL] [target]**

Maximum retries —-> **nmap –max-retries [number] [target]**

Host timeout —-> **nmap –host-timeout [time] [target]**

Minimum Scan delay —-> **nmap –scan-delay [time] [target]**

Maximum scan delay —-> **nmap –max-scan-delay [time] [target]**

Minimum packet rate —-> **nmap –min-rate [number] [target]**

Maximum packet rate —-> **nmap –max-rate [number] [target]**

Defeat reset rate limits —-> **nmap –defeat-rst-ratelimit [target]**

Firewall Evasion Techniques

Fragment packets —-> **nmap -f [target]**

Specify a specific MTU —-> **nmap –mtu [MTU] [target]**

Use a decoy —-> **nmap -D RND: [number] [target]**

Idle zombie scan —> **nmap -sI [zombie] [target]**

Manually specify a source port —-> **nmap –source-port [port] [target]**

Append random data —-> **nmap –data-length [size] [target]**

Randomize target scan order —-> **nmap –randomize-hosts [target]**

Spoof MAC Address —-> **nmap –spoof-mac [MAC|0|vendor] [target]**

Send bad checksums —-> **nmap –badsum [target]**

Output Options

Save output to a text file —-> **nmap -oN [scan.txt] [target]**

Save output to a xml file —> **nmap -oX [scan.xml] [target]**

Grepable output —-> **nmap -oG [scan.txt] [target]**

Output all supported file types —-> **nmap -oA [path/filename] [target]**

Periodically display statistics —-> **nmap –stats-every [time] [target]**

133t output —-> **nmap -oS [scan.txt] [target]**

Troubleshooting and debugging

Help —> **nmap -h**

Display Nmap version —-> **nmap -V**

Verbose output —-> **nmap -v [target]**

Debugging —-> **nmap -d [target]**

Display port state reason —-> **nmap –reason [target]**

Only display open ports —-> **nmap –open [target]**

Trace packets —> **nmap –packet-trace [target]**

Display host networking —> **nmap –iflist**

Specify a network interface —> **nmap -e [interface] [target]**

Nmap Scripting Engine

Execute individual scripts —> **nmap –script [script.nse] [target]**

Execute multiple scripts —-> **nmap –script [expression] [target]**

Script categories —-> **all, auth, default, discovery, external, intrusive, malware, safe, vuln**

Execute scripts by category —-> **nmap –script [category] [target]**

Execute multiple scripts categories —-> **nmap –script [category1,category2, etc]**

Troubleshoot scripts —-> **nmap –script [script] –script-trace [target]**

Update the script database —-> **nmap –script-updatedb**

Ndiff

Comparison using Ndiff —-> **ndiff [scan1.xml] [scan2.xml]**

Ndiff verbose mode —-> **ndiff -v [scan1.xml] [scan2.xml]**

XML output mode —-> **ndiff –xml [scan1.xm] [scan2.xml]**