

Basic Scanning with Nmap		Output Options (cont)		Version Detection with Nmap		Ndiff	
Scan a single target	nmap [target]	133t output	nmap -oS [scan.txt] [target]	Operating system detection	nmap -O [target]	Comparison using Ndiff	ndiff [scan1.xml] [scan2.xml]
Scan multiple targets	nmap [target1,-target2,etc]	Nmap Scripting Engine		Attempt to guess an unknown	nmap -O -ossan-guess [target]	Ndiff verbose mode	ndiff -v [scan1.xml] [scan2.xml]
Scan a list of targets	nmap -iL [hacklist.txt]	Execute individual scripts		Service version detection	nmap -sV [target]	XML output mode	ndiff -xml [scan1.xml] [scan2.xml]
Scan a range of hosts	nmap [range of IP addresses]	Execute multiple scripts		Troubleshooting version scans	nmap -sV -version-trace [target]	About me	
Scan an entire subnet	nmap [IP address/cdir]	Execute scripts by category		Perform a RPC scan	nmap -sR [target]	Name	netwrkspider
Scan random hosts	nmap -iR [number]	Execute multiple scripts categories		Firewall Evasion Techniques with Nmap		website	http://www.netwrkspider.org
Excluding targets from a scan	nmap [targets] -exclude [targets]	Troubleshoot scripts		Fragment packets	nmap -f [target]	Job Profile	Security Researcher & Developers
Excluding targets using a list	nmap [targets] -excludefile [list.txt]	Update the script database		Specify a specific MTU	nm ap -mtu [MTU] [target]	Nmap Discovery Options	
Perform an aggressive scan	nmap -A [target]	Script categories		Use a decoy	nmap -D RND: [number] [target]	Perform a ping scan only	nmap -sP [target]
Scan an IPv6 target	nmap -6 [target]	a auth default discovery external intrusive malware safe vuln		Idle zombie scan	nmap -sl [zombie] [target]	Don't ping	nmap -PN [target]
Output Options				Manually specify a source port	nmap --source-port [port] [target]	TCP SYN Ping	nmap -PS [target]
Save output to a text file	nmap -oN [scan.txt] [target]			Append random data	nmap --data--length [size] [target]	TCP ACK ping	nmap -PA [target]
Save output to a xml file	nmap -oX [scan.xml] [target]			Randomize target scan order	nmap --randomize-hosts [target]	UDP ping	nmap -PU [target]
Grepable output	nmap -oG [scan.txt] [target]			Spoof MAC Address	nmap --spoof-mac [MAC 0 vendor] [target]	SCTP Init Ping	nmap -PY [target]
Output all supported file types	nmap -oA [path/filename] [target]			Send bad checksums	nmap --badsum [target]	ICMP echo ping	nmap -PE [target]
Periodically display statistics	nmap --stats-every [time] [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]



By **Abhisek** (netwrkspider)

Published 3rd September, 2015.

Last updated 11th May, 2016.

Page 1 of 2.

Sponsored by **Readable.com**

Measure your website readability!

<https://readable.com>

Nmap Discovery Options (cont)

Traceroute	<code>nmap -trace-route [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>



By **Abhisek** (netwrkspider)

cheatography.com/netwrkspider/
www.netwrkspider.org

Published 3rd September, 2015.
Last updated 11th May, 2016.
Page 2 of 2.

Sponsored by **Readable.com**
Measure your website readability!
<https://readable.com>