

Forum:[Hack Forums](#)

Thread: [\[NetSec\] - Nmap Commands List - For Beginners And Experienced Hackers](#)

Sitrep - April 14, 2022, 12:09 pm

This is some common commands used for Nmap that I would like to share with you. Hope it is useful!

Tips: Copy and save it locally for quick access!

Nmap, short for "Network Mapper", is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Scan a range of IP address:

Code `nmap 192.168.1.0 0 192.168.1.2`

Scan a range of IP address using a wildcard:

Code `nmap 192.168.1.0-20`

Scan an entire subnet:

Code `nmap 192.168.1.*`

Scan a list of hosts:

Code `nmap 192.168.1.0/24`

OS and Version Detection:

Code `nmap -iL /tmp/test.txt`

Find out if a Host/Network is protected by a firewall:

Code `nmap -A 192.168.1.254`

`nmap -v -A 0`

`nmap -A -iL /tmp/scanlist.txt`

Scan a host when protected by a firewall:

Code `nmap -sA 192.168.1.254`

`nmap -sA example.com`

Scan IPV6:

Code `nmap -PN 0`

`nmap -PN example.com`

Host discovery/Ping scan:

Code ("`-6`" enables IPv6 scanning.)

`nmap -6 example.com`

`nmap -6 <IPv6 here>`

`nmap -v A -6 <IPv6 here>`

Fast Scan:

Code `nmap -sP 192.168.1.0/24`

Show only open ports:

Code `nmap -F 0`

Scan Specific Ports:

Code `nmap --open 0`

`nmap --open example.com`

Fastest way to scan:

```

Code nmap -p [port] hostName
# Scan port 80
nmap -p 80 0
# Scan TCP port 80
nmap -p T:80 0
# Scan UDP port 53
nmap -p U:53 0
# Scan two ports
nmap -p 80,443 0
# Scan port ranges
nmap -p 80-200 0
# Combine all options
nmap -p U:53,111,137,T:21-25,80,139,8080 0
nmap -p U:53,111,137,T:21-25,80,139,8080 example.com
nmap -v -sU -sT -p U:53,111,137,T:21-25,80,139,8080 192.168.1.254
# Scan all ports with * wildcard
nmap -p "*" 0
# Scan top ports i.e. scan $number most common ports
nmap --top-ports 5 0
nmap --top-ports 10 0
Identify remote host apps and OS "-O":
Code nmap -T5 192.168.1.0/24
Scan for remote services & Versions:
Code nmap -O 0
nmap -O --osscan-guess 0
nmap -v -O --osscan-guess 0
Bypass firewall ICMP ping scans:
Code nmap -sV 0
Bypass Firewalls blocking TCP scans with UDP:
Code nmap -PS 0
nmap -PS 80,21,443 0
nmap -PA 0
nmap -PA 80,21,200-512 0
Scan for UDP services:
Code nmap -PU 0
nmap -PU 2000.2001 0
Code nmap -sU nas03
nmap -sU 0
Save scan results to output file:
Code nmap -sO 0
Faster scans:
Code nmap 0 > output.txt
nmap -oN /path/to/filename 0
nmap -oN output.txt 0
Code nmap -v -sS -A -T4 <or T5> 192.168.2.0

```

SIM-5183822 - April 17, 2022, 4:38 pm

Very useful, but many use Goody versions not command line interface.

You can do even more with python3 using imports nmap, os, subprocess to force scans from everything from irc to cron jobs for mass scans to test overall security on a daily basis.

Thanks for sharing i found this thread useful and fun to read threw

Sitrep - May 6, 2022, 6:13 pm

(Apr 17, 2022 04:38 PM)ankh Wrote: [\[CITE\]](#) Very useful, but many use Gooney versions not command line interface.

You can do even more with python3 using imports nmap, os, subprocess to force scans from everything from irc to cron jobs for mass scans to test overall security on a daily basis.

Thanks for sharing i found this thread useful and fun to read threw

Thanks! Yeah, next post I make should be about nmap scripts, or you can write that one? ??

SIM-2501407 - May 6, 2022, 7:02 pm

This is nice; definitely helpful for someone that isn't a guru with nmap. I've used it once before and have used some of these commands.

If you get the chance, would you be able to also cover some popular scripts (particularly had scanners in mind, but any useful ones)?

Sitrep - May 19, 2022, 2:49 pm

(May 6, 2022 07:02 PM)Spy Wrote: [\[CITE\]](#) This is nice; definitely helpful for someone that isn't a guru with nmap. I've used it once before and have used some of these commands.

If you get the chance, would you be able to also cover some popular scripts (particularly had scanners in mind, but any useful ones)?

Thanks, I am glad you liked it! And yes, I will return with some useful scripts as well!

Joseph Ducreux - May 19, 2022, 3:39 pm

decent introductory lesson but I recomend throwing in some of the nmap nse scripts... thats where the fun is at... I broke into a very large corporate secure network (had nids/wids protection / Suricata etc) by doing a very slow scan 1-255x on 4rth ip sequence, than changing 3rd ip sequence up digit up and repeating eventually found a single vulnerable computer and got in relatively easy from their ..

I was hired at time to do red/blue team penetrations I was not well liked because I could always overcome their current security team through increasingly alternative and anoying ways that were not considered "operationally relevant" they were also pissed cuz i was basically hired under the table and yet almost on a daily basis I was bringing a team of college educated 'professionals' down to their fucking knees in constant headahce..... I only did a single nmap scan and from data I got from that fueled the entire next months worth of exploitation vectors and operandi

nmap scans should be the FIRST thing anybody does in a security assesment, do the scan slow as possable. add as much relevant scripts and service discovery modules as you can, and make it as verbose as you can.. most people HATE this, as it makes you have an output that in some cases is literally 100x larger and mostly useless but sifting through it carefully is where you find a tiny key... I also highly recomend to save your outputs to a file (I am glad you included that) so you dont have to repeat scans, for some reason alot of people even blue team side would run a scan, not like the output, so modify parameters to be more specific than run an entire nmap scan again... (never do that, do one nmap scan and never do it again on thatnetwork),,, make a highly verbose and inclusive single nmap scan and save the output

nmap scans are generally recognized to be very obvious, that networks can generally tell easily when an attacker is doing it. however doing the scan slow and only once in most cases is mild enough to get you through especially in large networks or very busy ones that have have a mcfuckton of network traffic anyway....

nmap has a fragmentation option that can split request that is very stealthy, it has a false ip option that is very stealthy, and I beleive it even has a proxy option.... I never even had to use those...

dont use nmap in tor... I tried it for stealth but it is basically unstable for various reasons

I highly recomend vulscan / vulner for the nmap nse suite

One last thing (sorry for tryng so much) the recursive-DNS and traceroute options in NMAP are extremely hecking useful..... I prefer people to use Zenmap which is basically nmap with a gui... and it has a tab that will draw you the network in a beautiful hierarchial fashion. with the recursive dns option it has a unique ability to show you secret "intro ips" into the network.. ie "internet facing" ones that are the key from the outside internet to a networks internal private intranet ... this is insanely helpful as usually you will find some corporate employee login portal as the usual gateway but than all this sudden secretly they had an old router on other side of network that is also internet connected and has a stupid simple rce but basically its not commonly used will never show up publically when trying to find intropoints the usual way

from everything i learned if i had to teach a beginner nmap is the first one i would choose to teach, because instead of trying to break into things with a particular skillset you are used to (I liked sql injections and uri exploits) it will tell you what it is vulnerbale too.. and forces you to adapt to the true security landscape enviroment... this is much more improntan because you will learn techniques you never previously studied, and in my opinion that is TRUE hacking..... things that sound very boring and alternative... such as vauge ones like some ancient apache directory traversal that in most cases you will use once and never use again ut but still very rapidly you develop a large and broad skillset that in the long run is much more versatile than being skilled in a single particular style

Swejeji2485 - May 20, 2022, 4:22 pm

Damn! I didn't even know nmap had this many commands, many thanks!

2xTheTap115 - May 21, 2022, 4:55 am

Useful list. in my opinion it would be nice to add Nmap Script Engine here. It's also a handy tool. After all, a mega thread. good job OP??

Sitrep - July 1, 2022, 5:17 pm

(May 20, 2022 04:22 PM)Swejeji2485 Wrote: [\[CITE\]](#) Damn! I didn't even know nmap had this many commands, many thanks!

That's just the beginning as well! Nmap has scripts too that you can run!