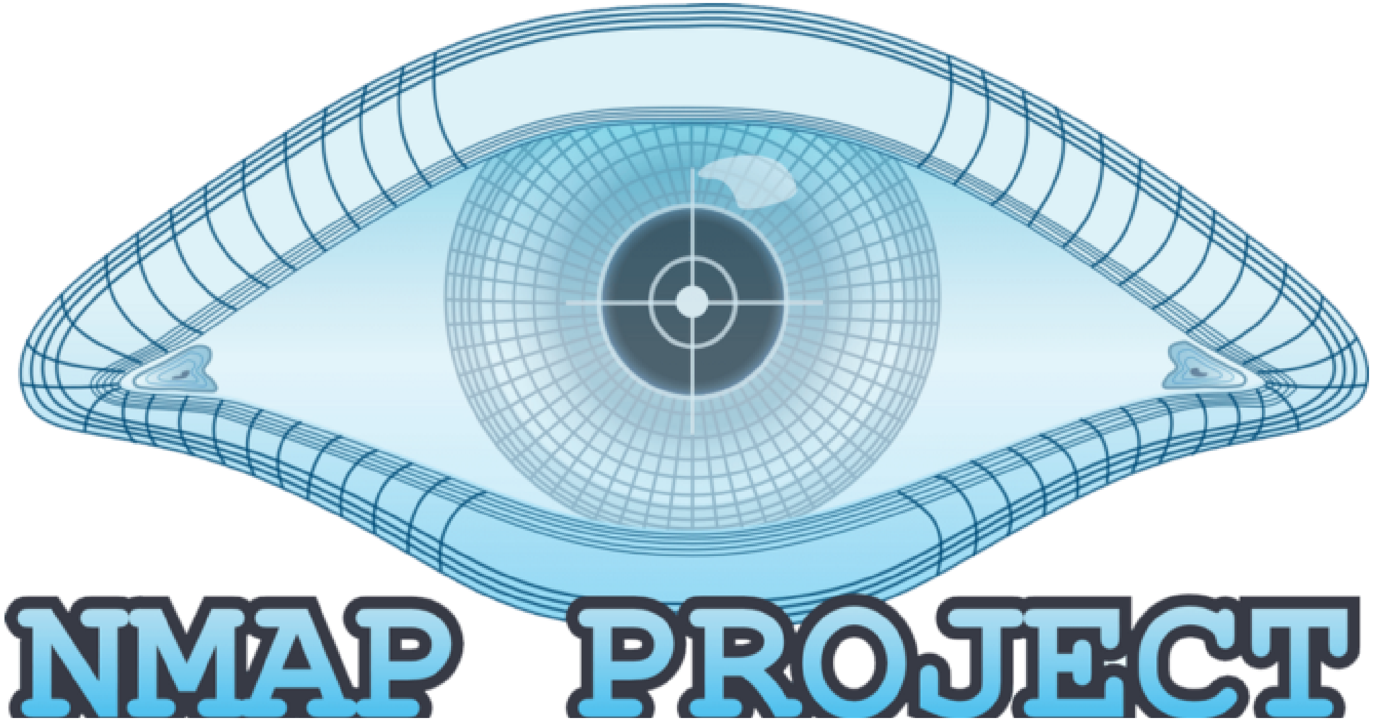
NMAP How-To

Miguel Sampaio da Veiga Follow

Feb 26 · 2 min read



Quick scans

nmap -sV target — scan 1000 ports of ‘target’ (target1 target2) (target#first-target#last) and obtain service version number

nmap -p- target -scan all ports of ‘target’

Comands Help

Target Specification

- Single host: nmap 192.168.0.1
- Specific hosts: nmap 192.168.0.1 192.168.0.2
- Range: nmap 192.168.0.1–254
- Domain: nmap mydomain.org
- CIDR notation: nmap 192.168.0.1/24
- Targets from file (-iL): nmap -iL targets.txt

- Random 100 ports (-iR): nmap -iR 100
- Exclude hosts (--exclude): nmap --exlude 192.168.0.1

Scan techniques

- TCP SYN port scan (-sS): nmap -sS 192.168.0.1
- TCP connect port scan (-sT): nmap -sT 192.168.0.1
- UDP port scan (-sU): nmap -sU 192.168.0.1
- TCP ACK port scan (-sA): nmap -sA 192.168.0.1
- TCP Window port scan (-sW): nmap -sW 192.168.0.1
- TCP Maimon port scan (-sM): nmap -sM 192.168.0.1

Host Discovery

- Only list targets (-sL): nmap -sL 192.168.0.1
- Host discovery only (-sn): nmap -sn 192.168.0.1
- Port scan only (-Pn): nmap -Pn 192.168.0.1

Port specification

- port X scan (-p X): nmap -p 21 192.168.0.1
- port range scan (-p X-Y): nmap -p 21–150 192.168.0.1
- multiple UDP and TCP port scan (-p U:X,T:Y-Z): nmap -p U:53,T:80–100 192.168.0.1
- scan all ports (-p-): nmap -p- 192.168.0.1
- scan ports by service name (-p service_name): nmap -p http 192.168.0.1
- Fast port scan (-F): nmap -F 192.168.0.1
- Scan top ports (— top-ports X): nmap --top-ports 1000 192.168.0.1

Service and Version Detection

- Service version detection (-sV): nmap -sV 192.168.0.1
- Service version detection light [faster] (-sV --version-light): nmap -sV — version-light 192.168.0.1
- Service version detection all[slower] (-sV --version-light): nmap -sV — version-all 192.168.0.1

OS Detection

- OS detection with TCP/IP stack (-O): nmap -O 192.168.0.1
- Limit detection to promising targets (-O --osscan-limit): nmap -O --osscan-limit 192.168.0.1
- Aggressive detection (-O --osscan-guest): nmap -O --osscan-guest 192.168.0.1
- Maximum number of tries (-O -a-max-os-tries X): nmap -O --max-os-tries 5 192.168.0.1
- OS, version, script scanning, traceroute (-A): nmap -A 192.168.0.1

Firewall/IDS Evasion and Spoofing

- Use fragmented IP packages (-f): nmap -f 192.168.0.1
- Mask scan with decoys(-D decoy1, decoy2,…): nmap -D 192.168.0.253,192.168.0.254 192.168.0.1
- Spoof address (-S IP): nmap -S 192.168.0.250 192.168.0.1

Output formats

- Output to file (-oN): nmap -oN scan.file 192.168.0.1

- Output XML to file (-oX): nmap -oX scan.xml 192.168.0.1
- Output grepable to file (-oG): nmap -oG grep.file 192.168.0.1
- Output 3 formats in once (-oA): nmap -oA scan 192.168.0.1
- Increase verbose output (-v): nmap -v 192.168.0.1

Scripts

- Default set of scripts (-sC): nmap -sC 192.168.0.1
- Run safe scripts (--script safe): nmap --script safe 192.168.0.1
- View scripts help (--script-help XXX): nmap --script-help whois-domain
- nmap scripts path: /usr/share/nmap/scripts

Nmap Pentesting Reconnaissance How To

1 clap

WRITTEN BY

Miguel Sampaio da Veiga

Follow

Freelance writer, tech enthusiast

Hacker Toolbelt

Follow

Hacking tools and how-to

Write the first response

More From Medium

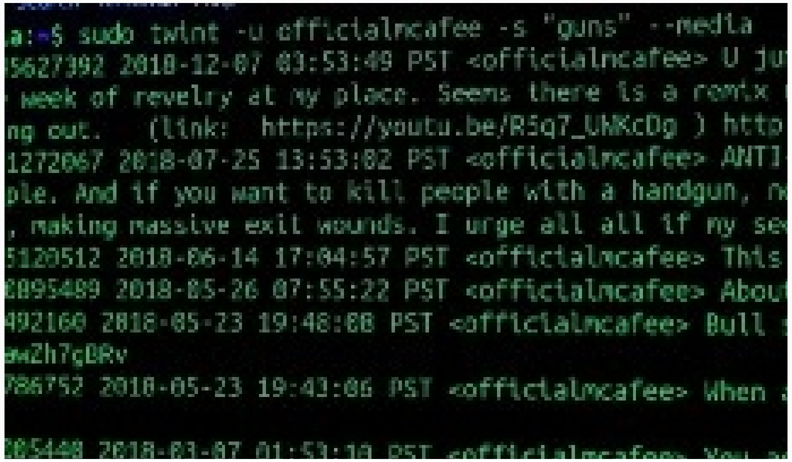
Also tagged Reconnaissance

How to Mine Twitter for Targeted Information with Twint

Null Byte

May 2 · 20 min read ★

123



```
a:~$ sudo twint -u officialmcafee -s "guns" --media
5627392 2018-12-07 03:53:49 PST <officialmcafee> U ju
 week of revelry at my place. Seems there is a remix
ng out.   (link:  https://youtu.be/R5q7_UNKcDg ) http
1272067 2018-07-25 13:53:02 PST <officialmcafee> ANTI
ple. And if you want to kill people with a handgun, n
, making massive exit wounds. I urge all all if my se
5120512 2018-06-14 17:04:57 PST <officialmcafee> This
2895489 2018-05-26 07:55:22 PST <officialmcafee> About
492160 2018-05-23 19:48:08 PST <officialmcafee> Bull
mwZh7gBRv
786752 2018-05-23 19:43:06 PST <officialmcafee> When

205448 2018-03-07 01:53:10 PST <officialmcafee> You a
```

```
ttp://www.nbcnews.com/video/dateline/58515382 ..  News
```

Top on Medium

10 Bad Habits of Unsuccessful People

Darius Foroux in Forge

Jul 9 · 5 min read ★

46K

Top on Medium

The Uncanny Power of Incompetent Men

Danny Wallace in Forge

Jul 25 · 9 min read ★

5.8K