Automating Reconnaissance Workflows for Effective Penetration Testing

Rizwan Syed

@_r12w4n

Agenda

- Introduction
- Reconnaissance
- Enumeration
- Scanning
- Assessment

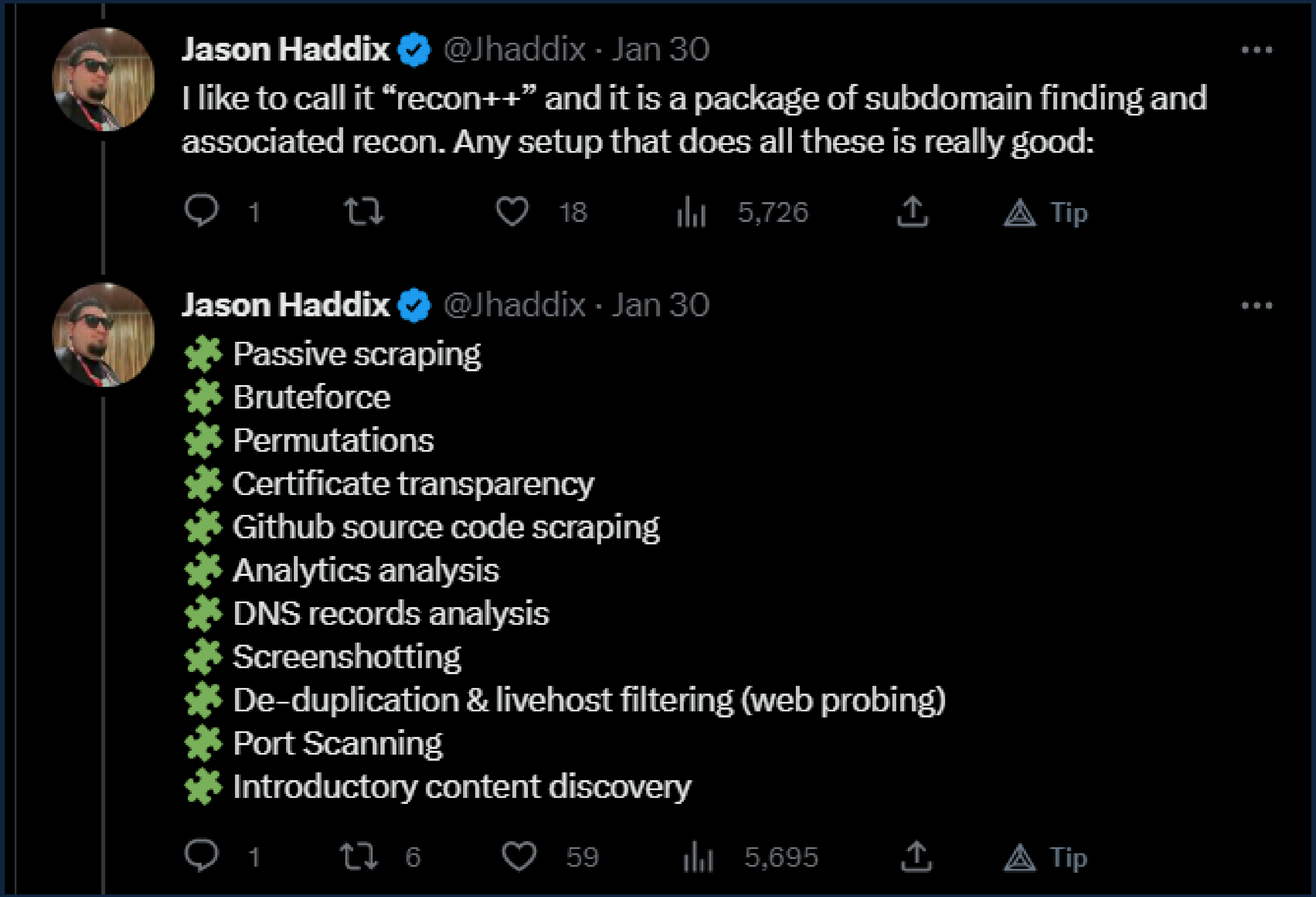
About Me

Consultant - Cyber Risk Advisory

Certified Red Team Professional - CRTP

Penetration Tester| Offensive Cyber Security Enthusiast

"Without reconnaissance, you're shooting in the dark."
- Unknown

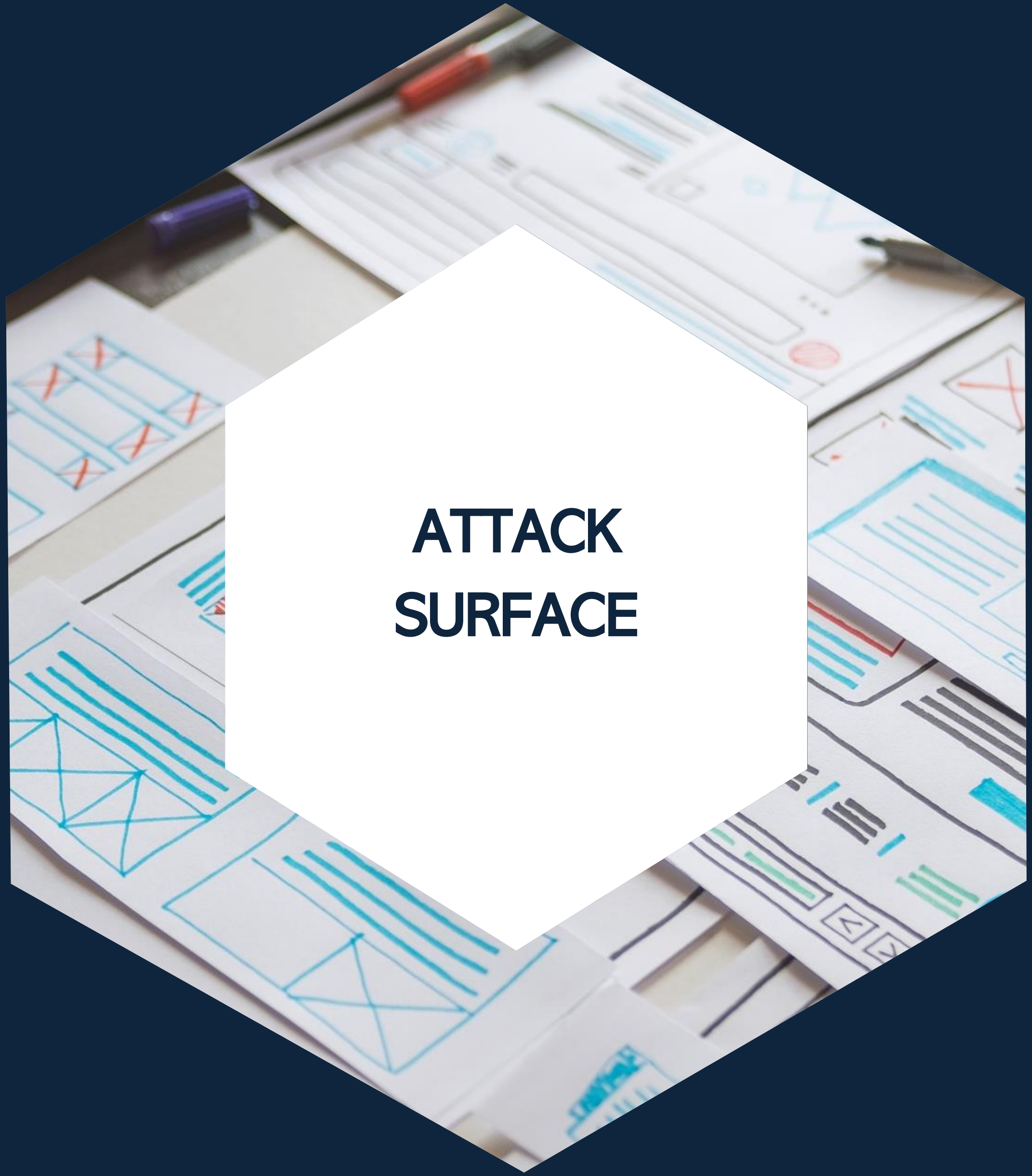


Jason Haddix @Jhaddix · Jan 30

I like to call it "recon++" and it is a package of subdomain finding and associated recon. Any setup that does all these is really good:

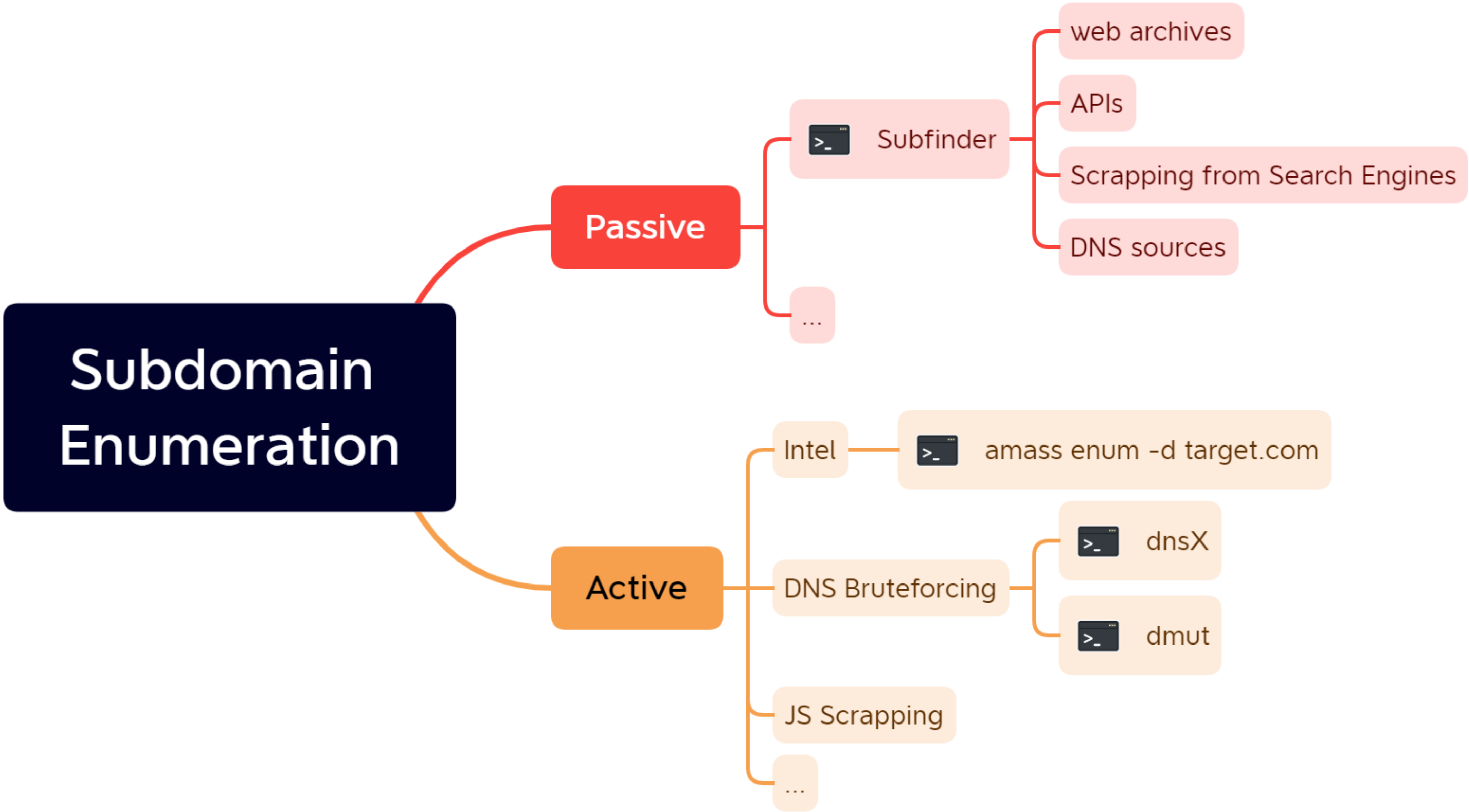
Jason Haddix @Jhaddix · Jan 30

🧩 Passive scraping
🧩 Bruteforce
🧩 Permutations
🧩 Certificate transparency
🧩 Github source code scraping
🧩 Analytics analysis
🧩 DNS records analysis
🧩 Screenshotting
🧩 De-duplication & livehost filtering (web probing)
🧩 Port Scanning
🧩 Introductory content discovery



ATTACK
SURFACE

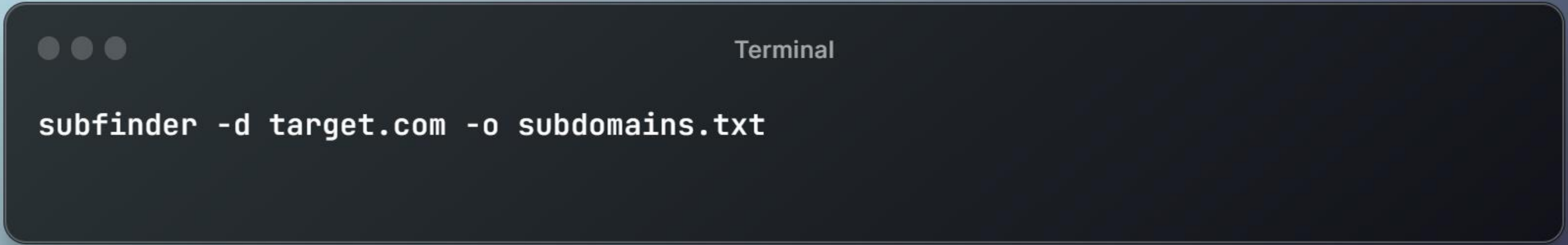
Subdomain Enumeration



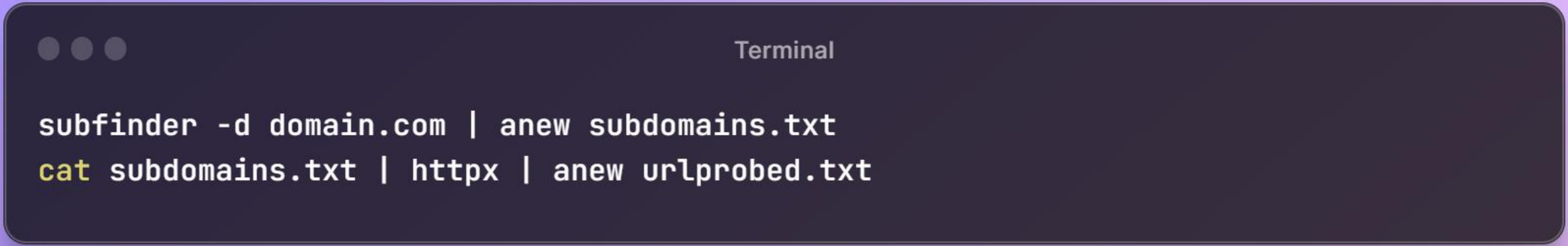
- Subdomain Enumeration
  - Passive
    - Subfinder
      - web archives
      - APIs
      - Scrapping from Search Engines
      - DNS sources
    - ...
  - Active
    - Intel
      - `amass enum -d target.com`
    - DNS Bruteforcing
      - dnsX
      - dmut
    - JS Scrapping
    - ...

Tools of Trade

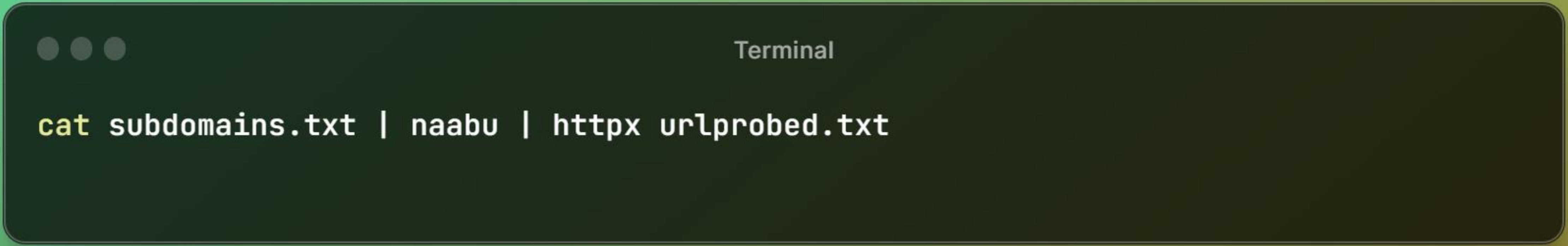
Tool Name	Category	From
subfinder	Subdomain Enumeration	ProjectDiscovery
dnsx	Domain Resolution	ProjectDiscovery
naabu	Quick Port Scanner	ProjectDiscovery
httpx	HTTP Probing	ProjectDiscovery



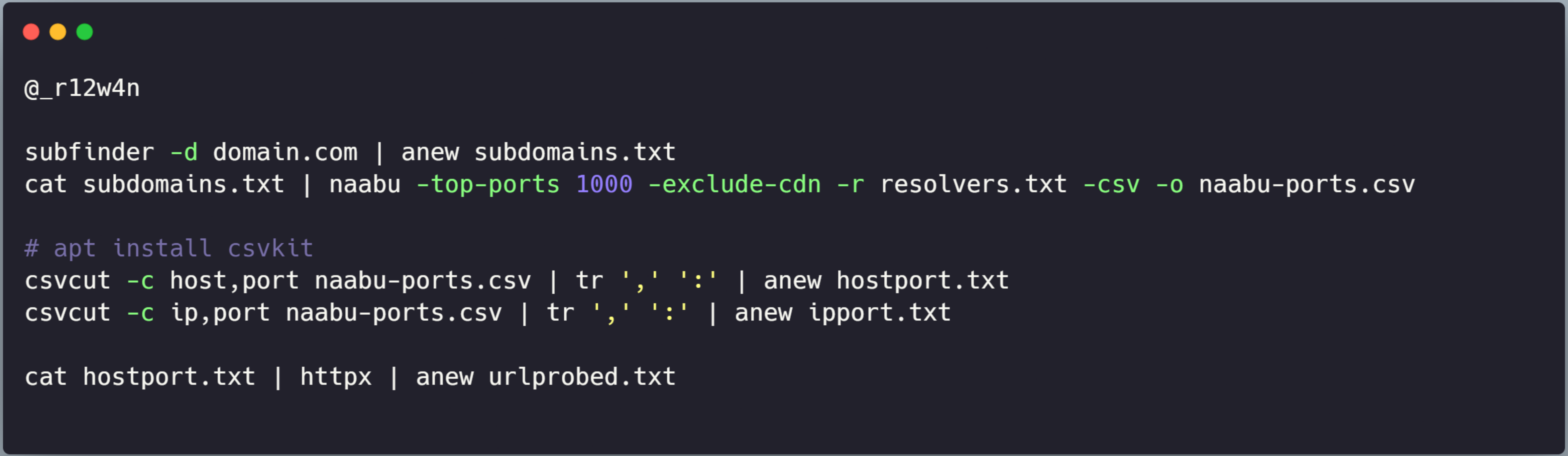
```
subfinder -d target.com -o subdomains.txt
```



```
subfinder -d domain.com | anew subdomains.txt
cat subdomains.txt | httpx | anew urlprobed.txt
```

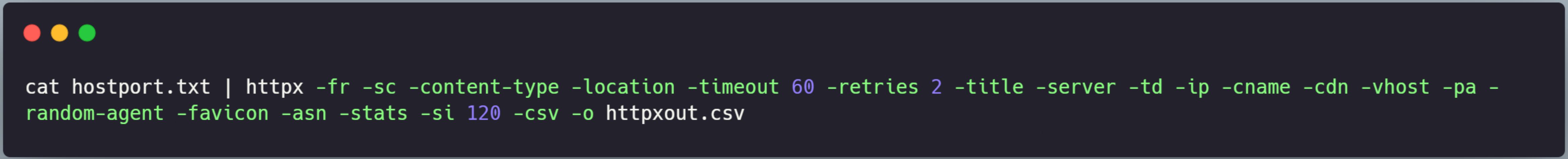


```
cat subdomains.txt | naabu | httpx urlprobed.txt
```

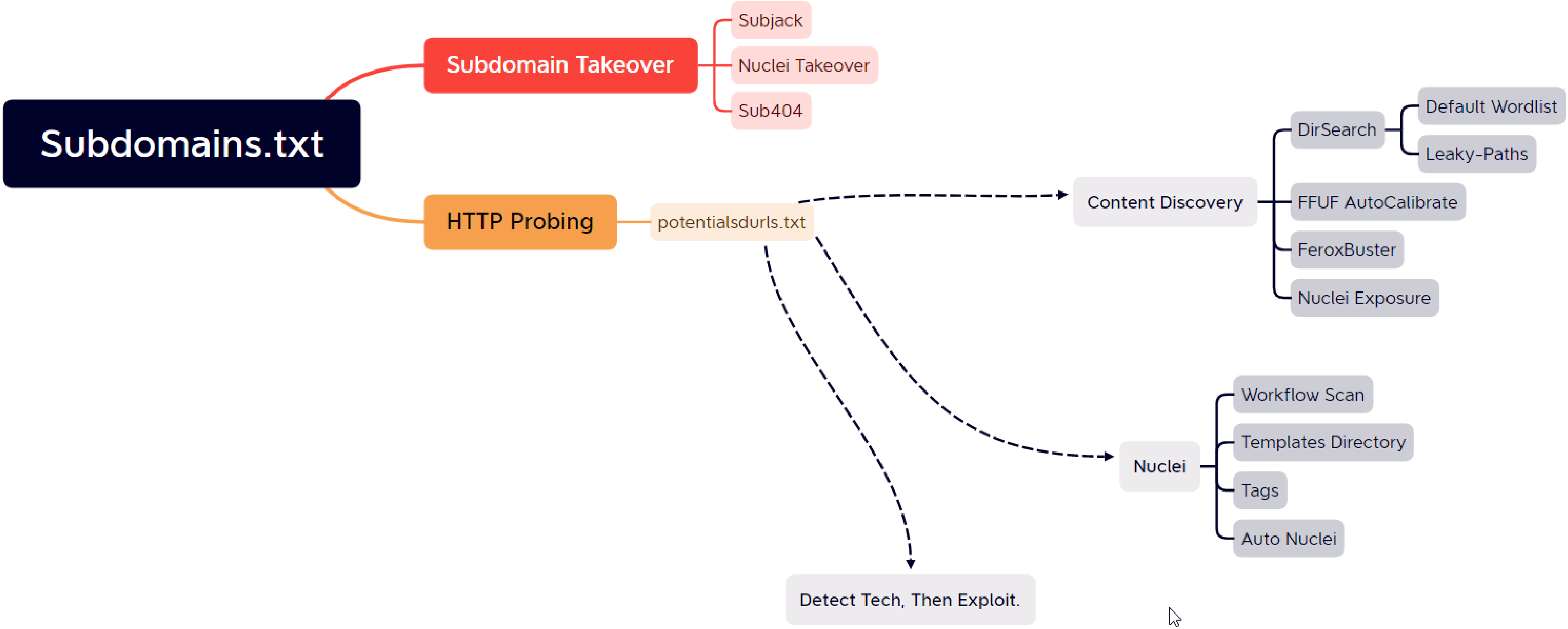


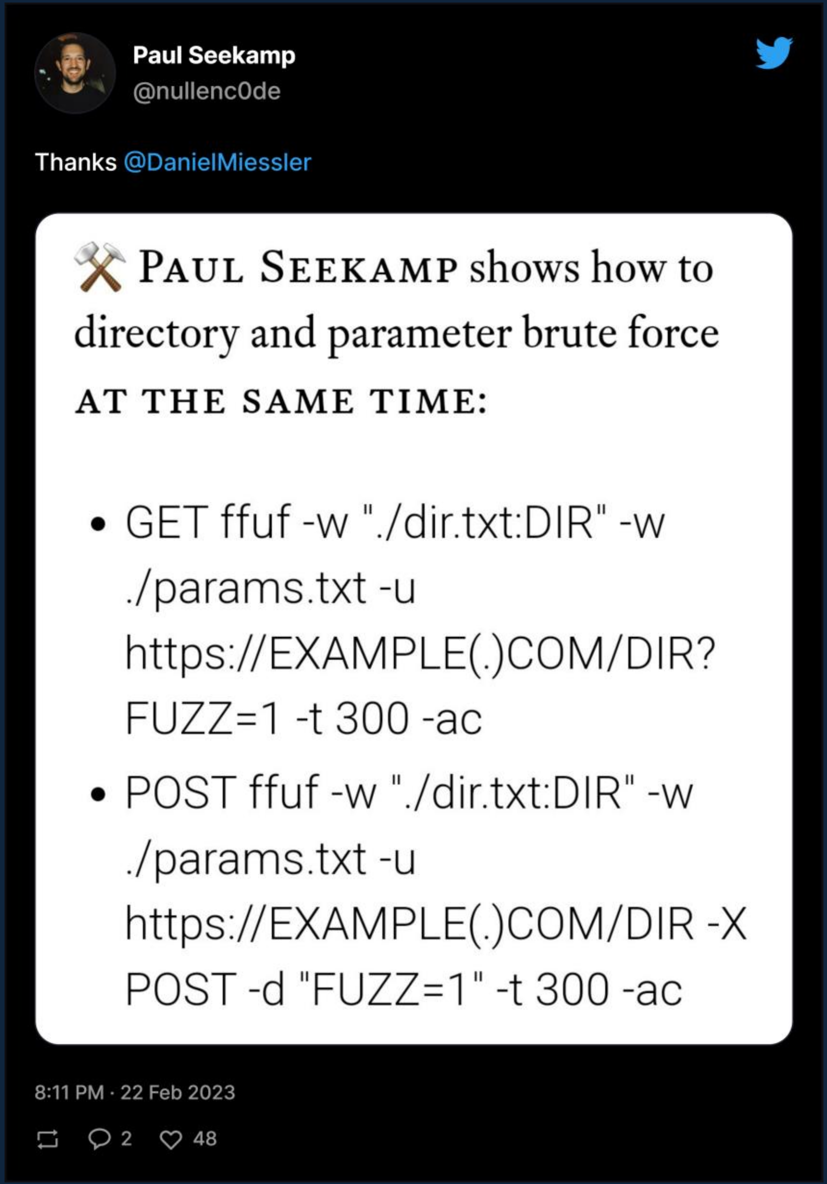
```
@_r12w4n

subfinder -d domain.com | anew subdomains.txt
cat subdomains.txt | naabu -top-ports 1000 -exclude-cdn -r resolvers.txt -csv -o naabu-ports.csv

# apt install csvkit
csvcut -c host,port naabu-ports.csv | tr ',' ':' | anew hostport.txt
csvcut -c ip,port naabu-ports.csv | tr ',' ':' | anew ipport.txt

cat hostport.txt | httpx | anew urlprobed.txt
```

HTTPX - PIVOT



```
cat hostport.txt | httpx -fr -sc -content-type -location -timeout 60 -retries 2 -title -server -td -ip -cname -cdn -vhost -pa -random-agent -favicon -asn -stats -si 120 -csv -o httpxout.csv
```


Subdomains.txt
Subdomain Takeover
Subjack
Nuclei Takeover
Sub404
HTTP Probing
potentialsdurls.txt
Content Discovery
DirSearch
Default Wordlist
Leaky-Paths
FFUF AutoCalibrate
FeroxBuster
Nuclei Exposure
Nuclei
Workflow Scan
Templates Directory
Tags
Auto Nuclei
Detect Tech, Then Exploit.



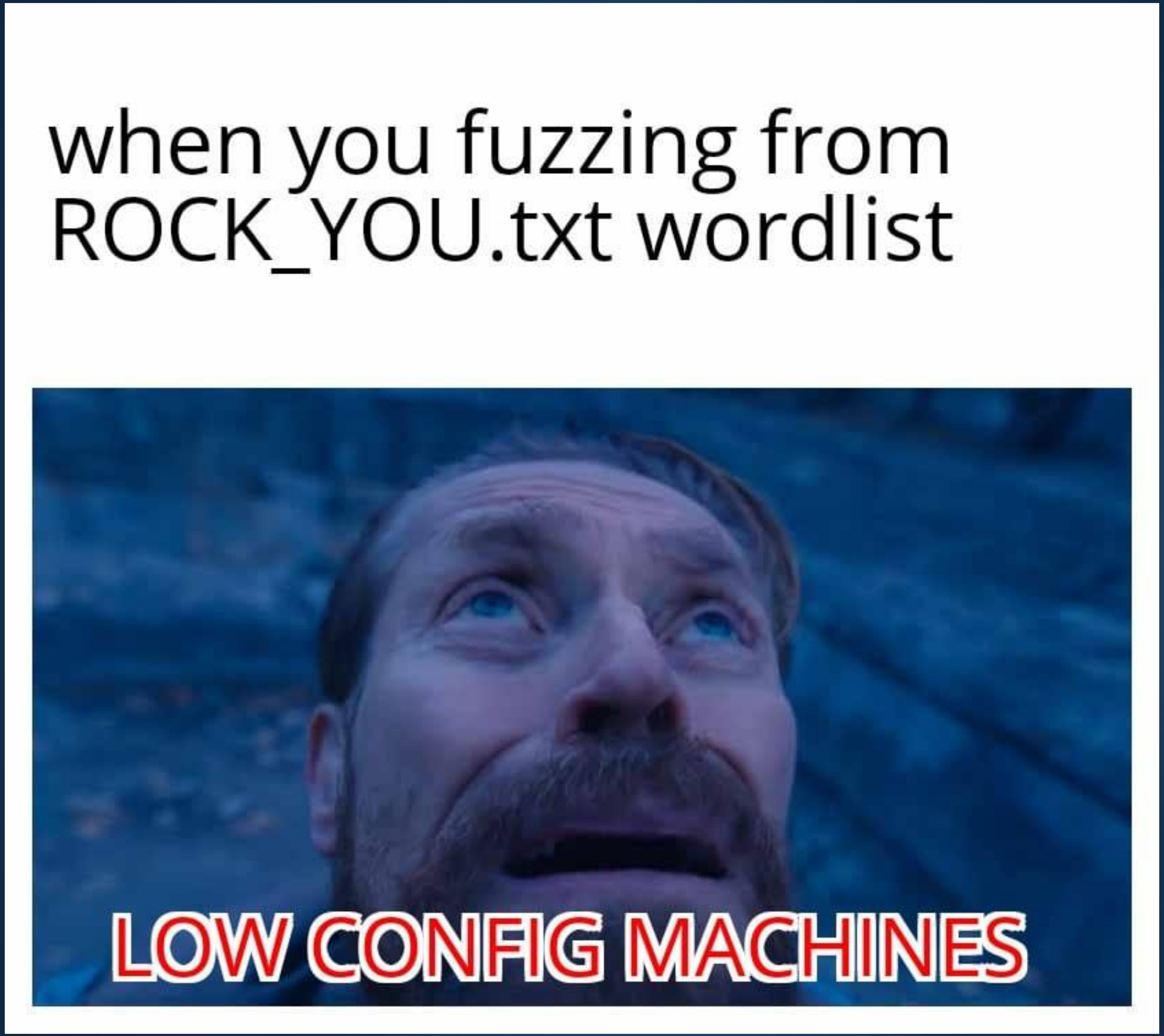
Paul Seekamp
@nullenc0de

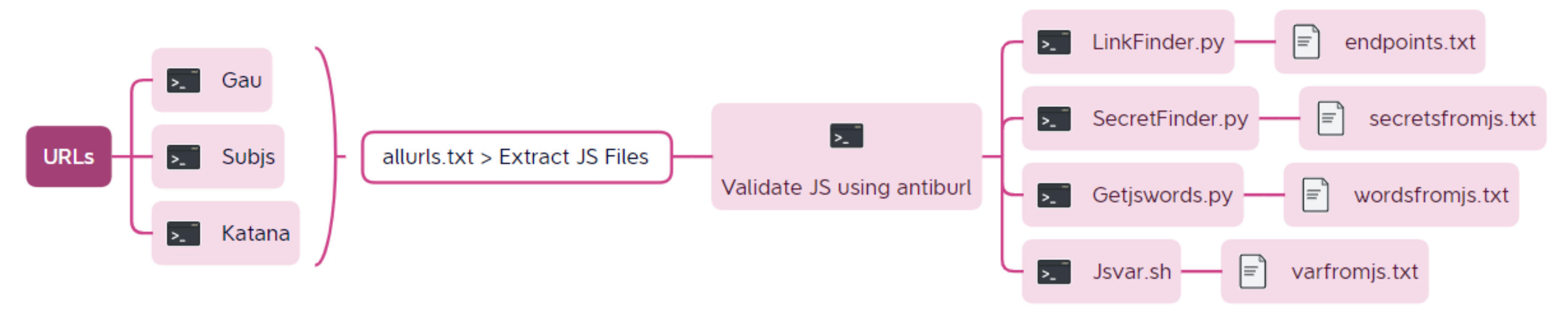
Thanks @DanielMiessler

⚒️ PAUL SEEKAMP shows how to directory and parameter brute force AT THE SAME TIME:

- GET `ffuf -w "./dir.txt:DIR" -w ./params.txt -u https://EXAMPLE(.)COM/DIR?FUZZ=1 -t 300 -ac`
- POST `ffuf -w "./dir.txt:DIR" -w ./params.txt -u https://EXAMPLE(.)COM/DIR -X POST -d "FUZZ=1" -t 300 -ac`

8:11 PM · 22 Feb 2023


when you fuzzing from ROCK_YOU.txt wordlist
LOW CONFIG MACHINES



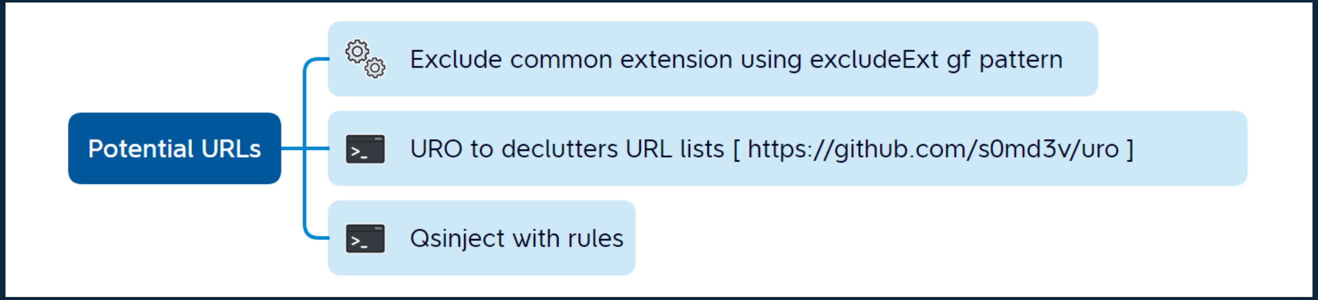
URLs

- Gau
- Subjs
- Katana

allurls.txt > Extract JS Files

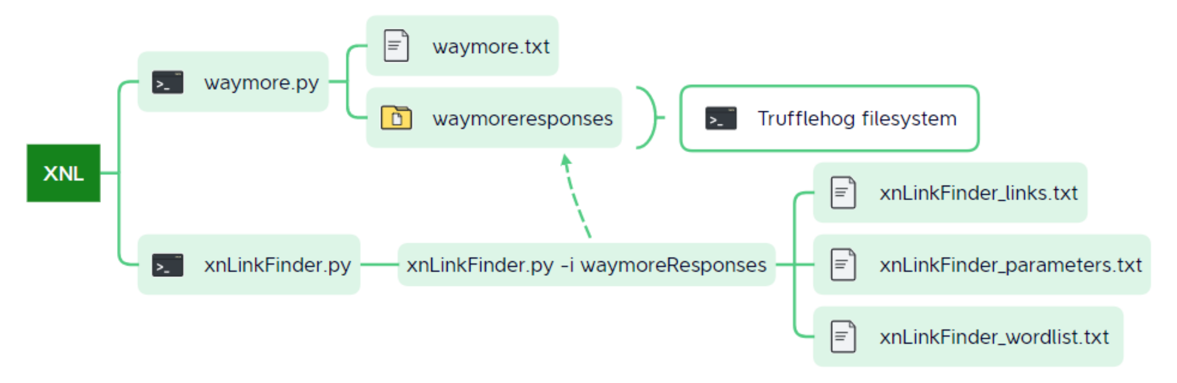
Validate JS using antiburl

- LinkFinder.py — endpoints.txt
- SecretFinder.py — secretsfromjs.txt
- Getjswords.py — wordsfromjs.txt
- Jsvar.sh — varfromjs.txt



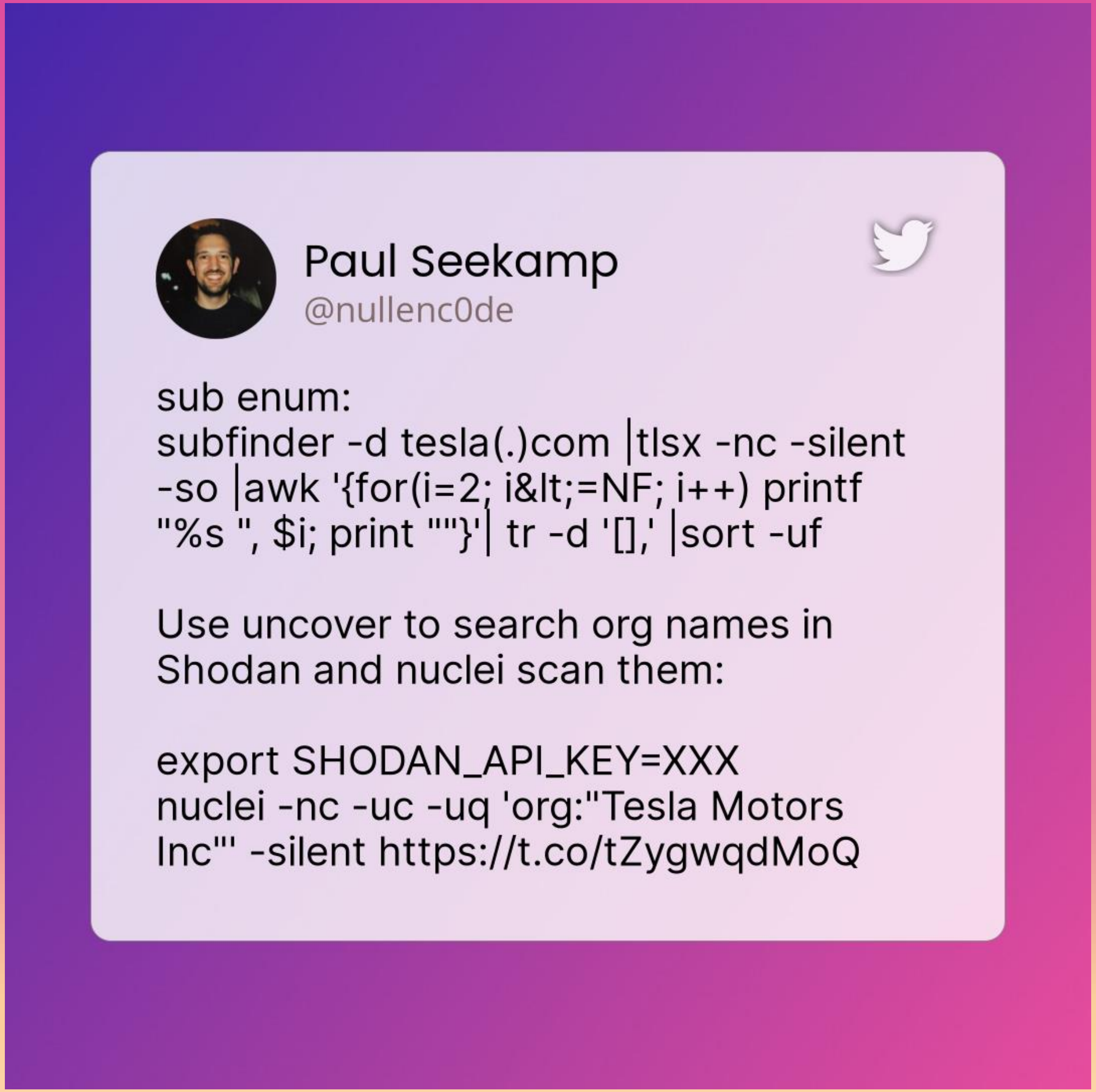
Potential URLs

- Exclude common extension using excludeExt gf pattern
- URO to declutters URL lists [https://github.com/s0md3v/uro]
- Qsinject with rules



XNL

- waymore.py
  - waymore.txt
  - waymoreresponses
- Trufflehog filesystem
- xnLinkFinder.py
  - xnLinkFinder.py -i waymoreResponses
    - xnLinkFinder_links.txt
    - xnLinkFinder_parameters.txt
    - xnLinkFinder_wordlist.txt



Paul Seekamp
@nullenc0de

sub enum:

```
subfinder -d tesla(.)com |tlsx -nc -silent
-so |awk '{for(i=2; i&lt;=NF; i++) printf
"%s ", $i; print ""}'| tr -d '[],' |sort -uf
```

Use uncover to search org names in Shodan and nuclei scan them:

```
export SHODAN_API_KEY=XXX
nuclei -nc -uc -uq 'org:"Tesla Motors
Inc"' -silent https://t.co/tZygwqdMoQ
```

KingOfBugbounty / KingOfBugBountyTips

3477 ★

Our main goal is to share tips from some well-known bughunters. Using recon methodology, we are able to find subdomains, apis, and tokens that are already exploitable, so we can report them. We wish to influence Onelinetips and explain the commands, for the better understanding of new hunters..

12 Contributors

Recon Script –

1. Gather Subdomains
2. Domain to IP resolution of subdomains
3. Scanning for open ports resolved IP
4. Map the open ports to their corresponding subdomains
5. Perform an HTTP probing of each subdomain : port
6. Content discovery
7. Tech detect – run custom scan based on running technology
8. Gather URL, JS mining, potential URLs, param, secrets
9. Service enumeration using Nmap
10. Nmap report generation x3

https://github.com/mr-rizwan-syed/chomtesh

SWISS ARMY KNIFE

Scanning Large Scale Networks

NMAP
(Swiss army knife)

Identify the network range

- Determine the range of IP addresses that you want to scan.
- This could be a single subnet or multiple subnets.
- You can use tools like ipcalc or subnet calculators to help you determine the IP range.

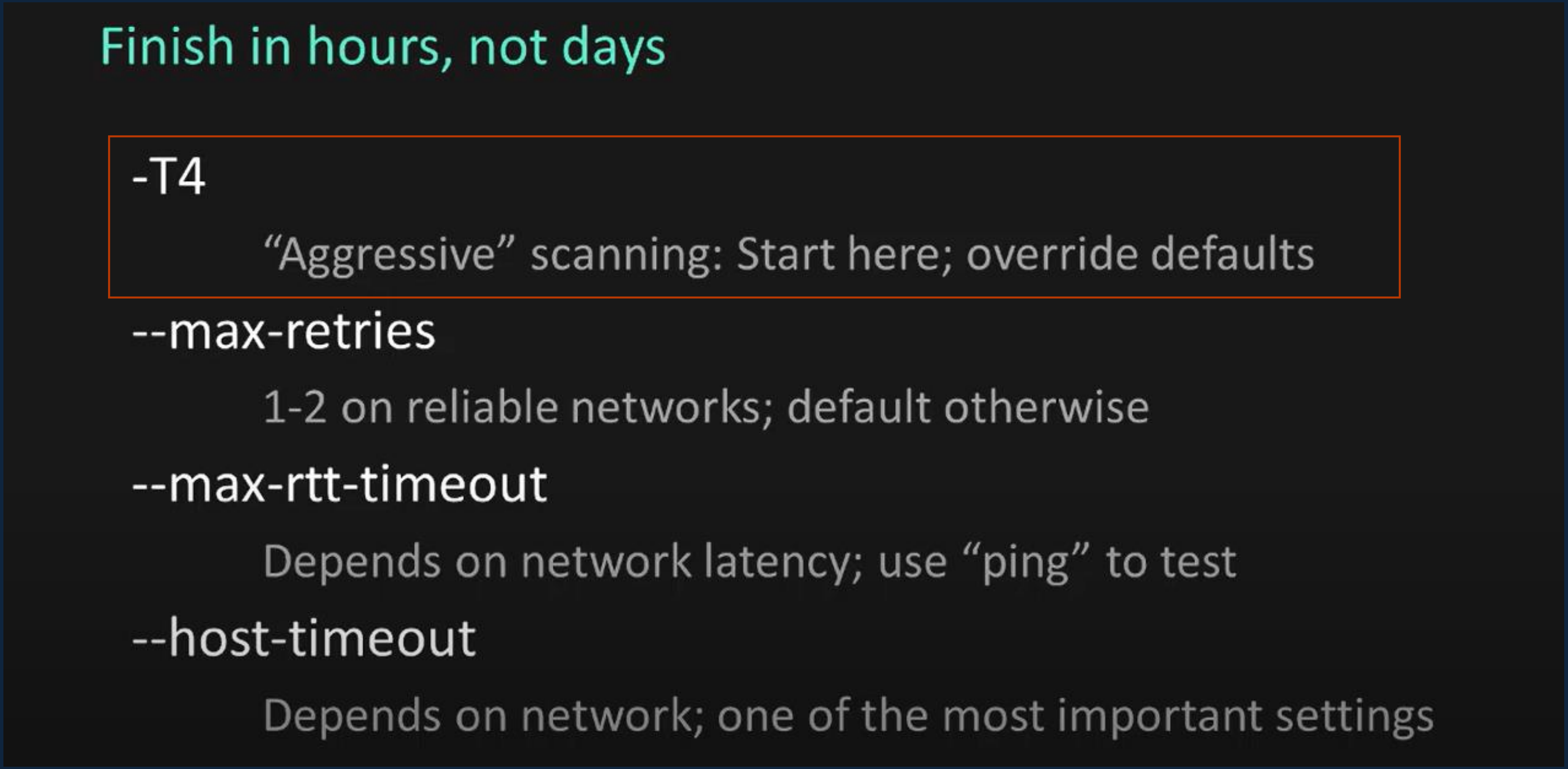
Choose your scan options:

- Nmap offers a wide range of scan options to choose from depending on what you want to achieve
- For example, you may want to use the -sP option to perform a ping sweep and identify live hosts or use the -sS option to perform a SYN scan and identify open ports.

Performance Tuning

- Depending on the results of your initial scan, you may want to fine-tune your scan options to get more detailed information or to speed up the scan.

Nmap Performance Tuning



Finish in hours, not days

-T4

“Aggressive” scanning: Start here; override defaults

--max-retries

1-2 on reliable networks; default otherwise

--max-rtt-timeout

Depends on network latency; use “ping” to test

--host-timeout

Depends on network; one of the most important settings

Nmap –Pn 192.168.1.0/24

Queue	Hosts	Alive
1	192.168.1.1	Yes
2	192.168.1.2	No
3	192.168.1.3	Yes
4	192.168.1.4	No
5	192.168.1.5	Yes
6	192.168.1.6	No
7	192.168.1.7	Yes
8	192.168.1.8	No
9	192.168.1.9	Yes
10	192.168.1.10	No

Scanning Methodology

Scanning in phases

```
nmap -Pn –iL <full-list> -oA phase1
```

Top 1k ports – [no ping]

```
nmap –sn –iL <full-list> -oA phase2
```

Ping only – no scan

```
nmap –p- –iL <filtered-list> -oA phase3
```

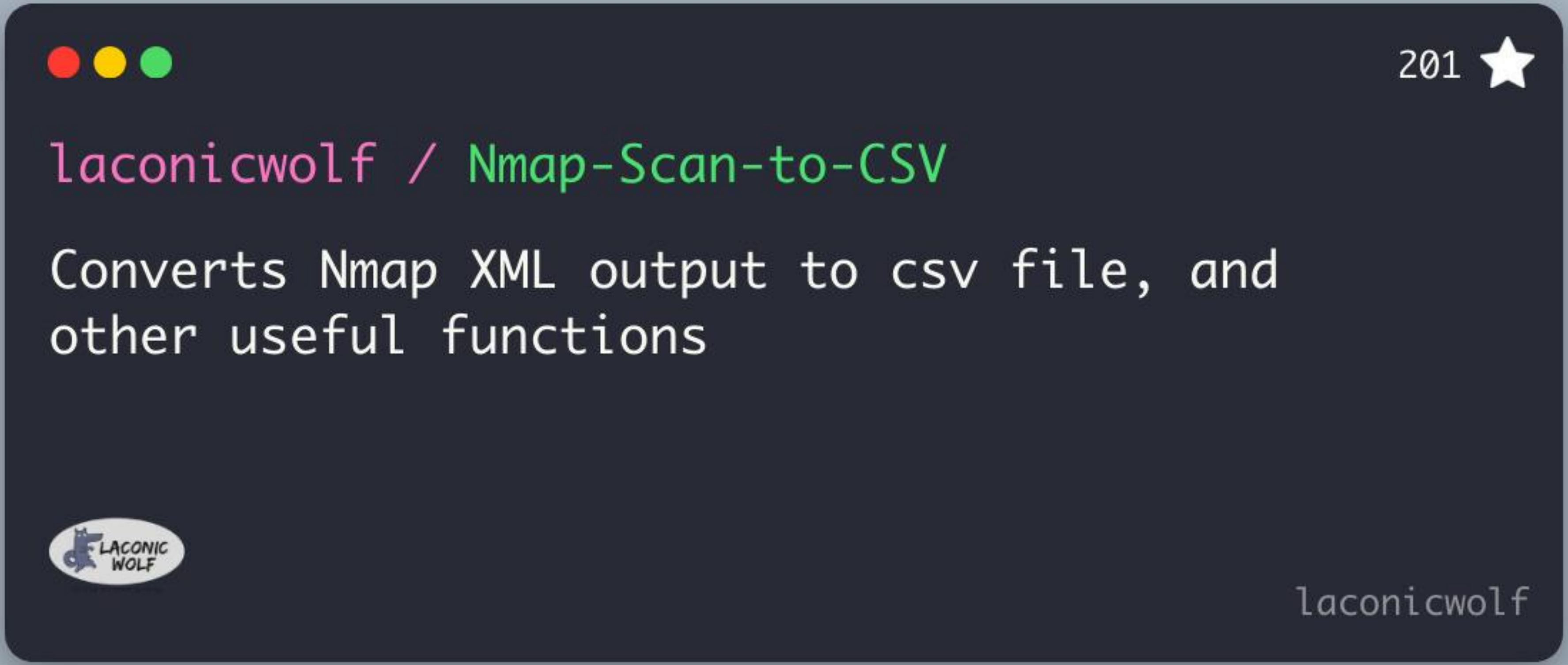
(Optional) Full 65K port scan - breadth

```
nmap –p <filtered-ports> -iL <filtered-list> -A –oA phase4
```

Detailed service scan - depth

Scanning Methodology

Report Conversion and Analysis

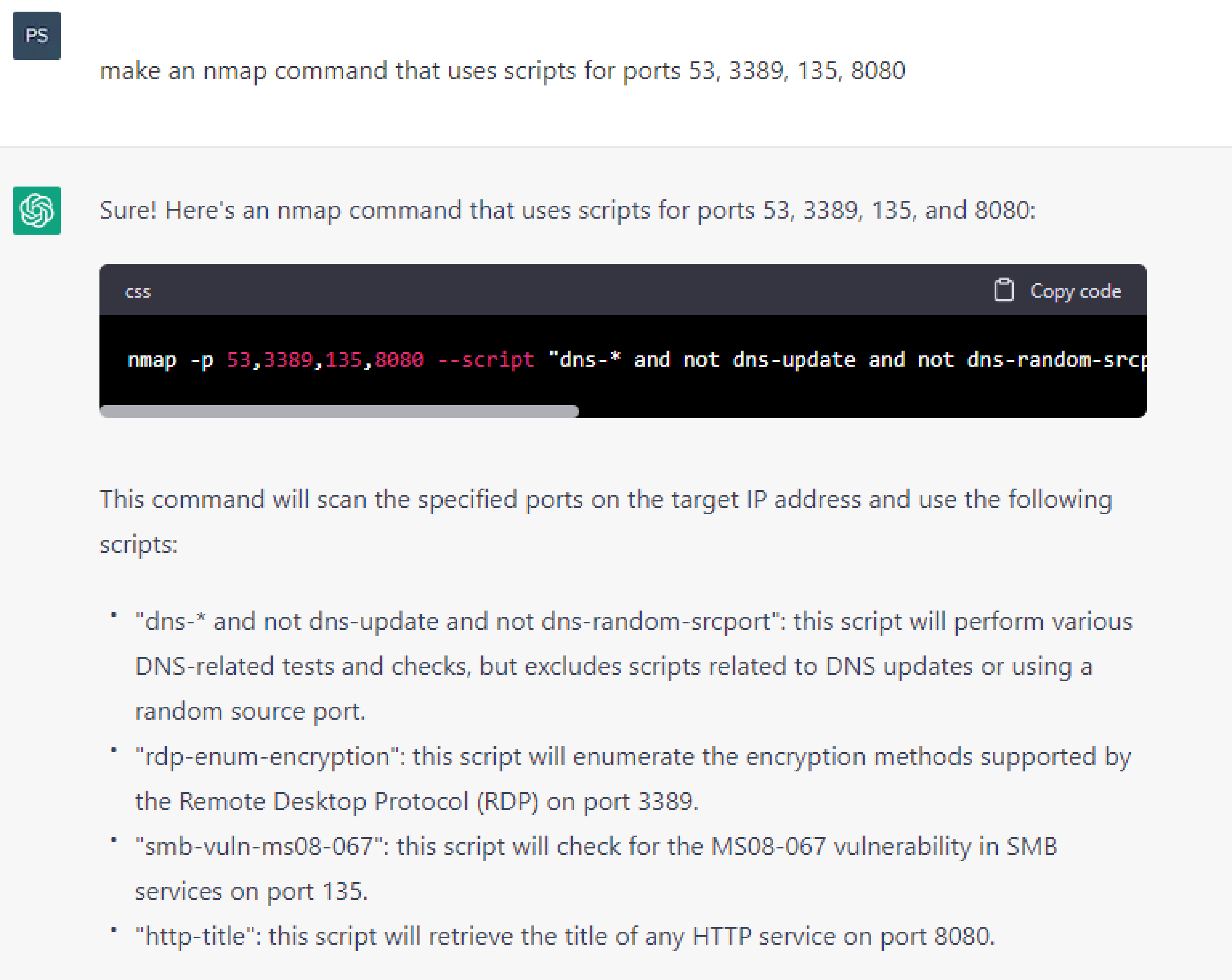


201

laconicwolf / Nmap-Scan-to-CSV

Converts Nmap XML output to csv file, and other useful functions

laconicwolf



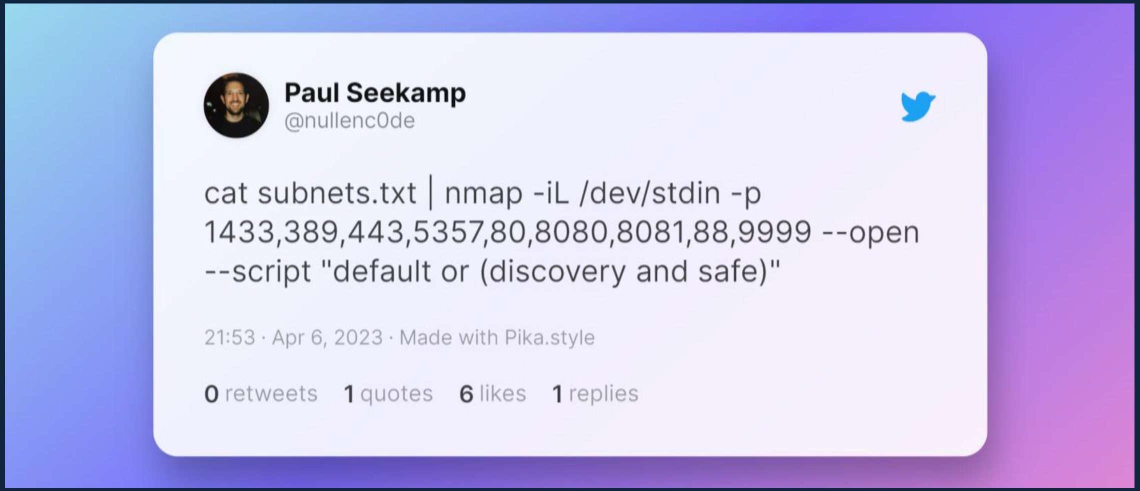
make an nmap command that uses scripts for ports 53, 3389, 135, 8080

Sure! Here's an nmap command that uses scripts for ports 53, 3389, 135, and 8080:

```css
nmap -p 53,3389,135,8080 --script "dns-* and not dns-update and not dns-random-srcp
```

This command will scan the specified ports on the target IP address and use the following scripts:

- "dns-* and not dns-update and not dns-random-srcport": this script will perform various DNS-related tests and checks, but excludes scripts related to DNS updates or using a random source port.
- "rdp-enum-encryption": this script will enumerate the encryption methods supported by the Remote Desktop Protocol (RDP) on port 3389.
- "smb-vuln-ms08-067": this script will check for the MS08-067 vulnerability in SMB services on port 135.
- "http-title": this script will retrieve the title of any HTTP service on port 8080.

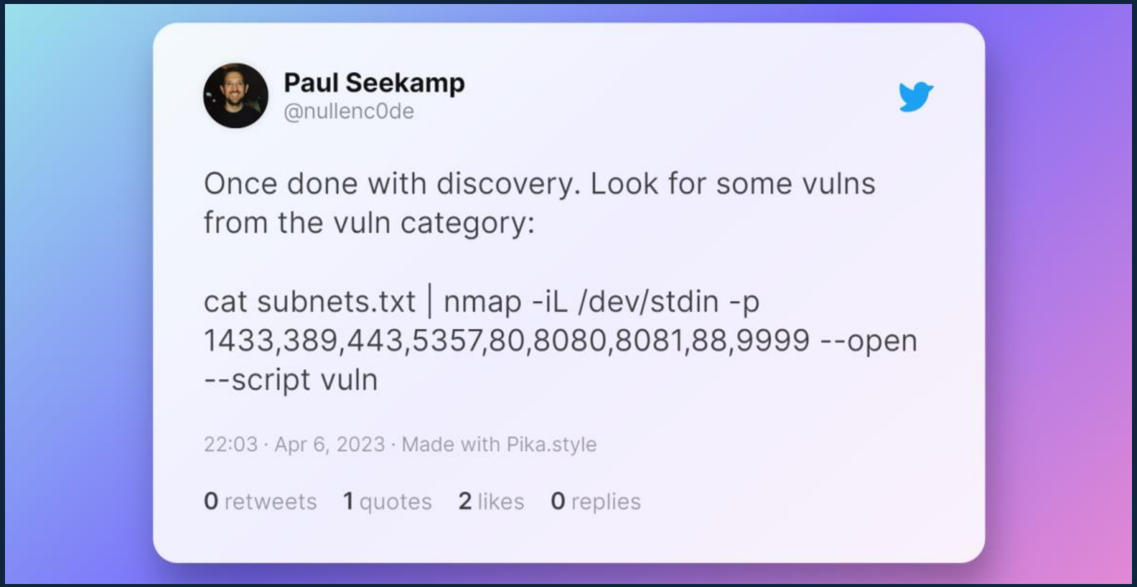


Paul Seekamp
@nullenc0de

```
cat subnets.txt | nmap -iL /dev/stdin -p 1433,389,443,5357,80,8080,8081,88,9999 --open --script "default or (discovery and safe)"
```

21:53 · Apr 6, 2023 · Made with Pika.style

0 retweets **1** quotes **6** likes **1** replies



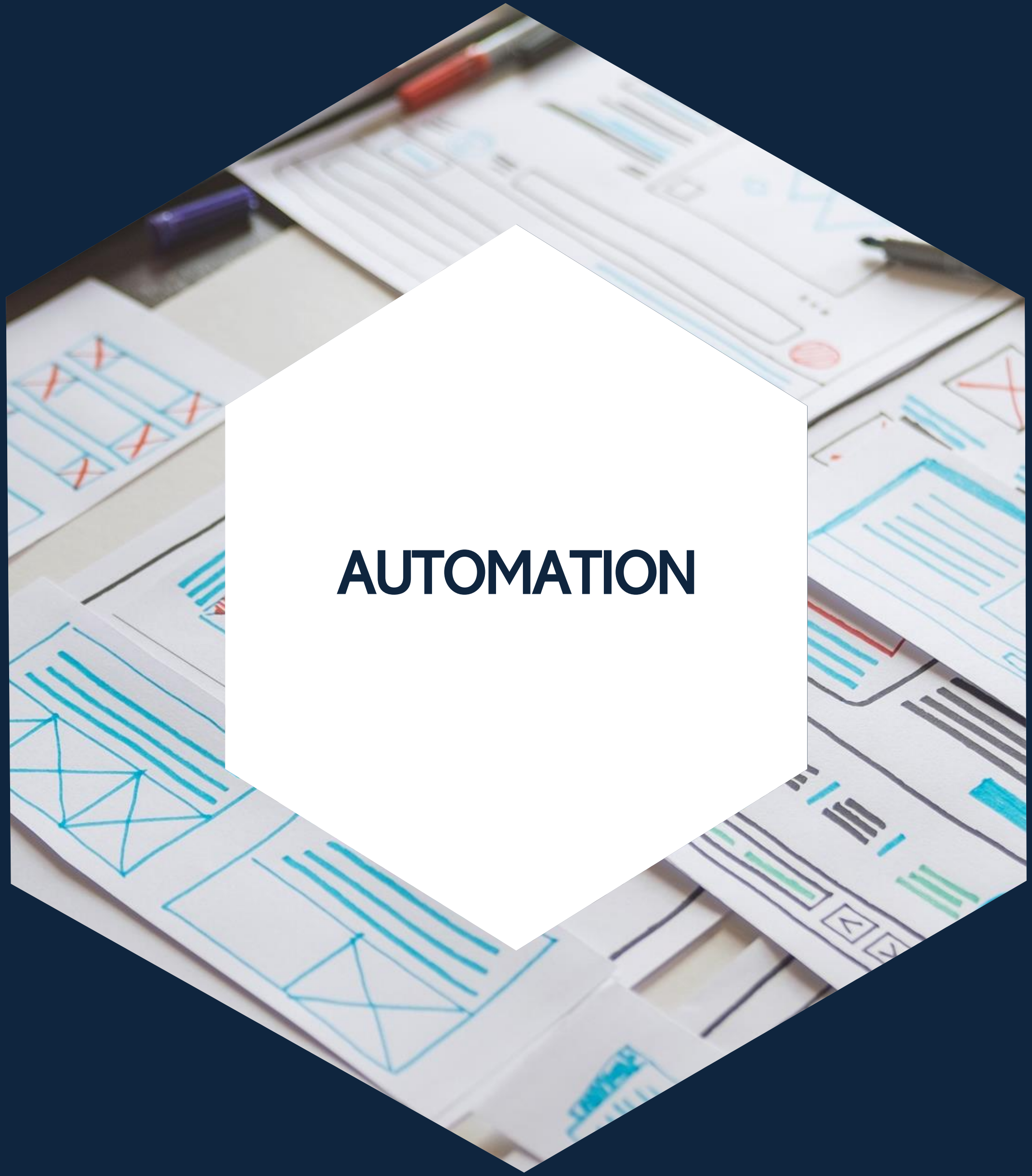
Paul Seekamp
@nullenc0de

Once done with discovery. Look for some vulns from the vuln category:

```
cat subnets.txt | nmap -iL /dev/stdin -p 1433,389,443,5357,80,8080,8081,88,9999 --open --script vuln
```

22:03 · Apr 6, 2023 · Made with Pika.style

0 retweets **1** quotes **2** likes **0** replies



AUTOMATION

Shell Scripting

Resources

1. https://www.shellscript.sh
2. https://betterdev.blog/minimal-safe-bash-script-template/
3. https://github.com/mr-rizwan-syed/chomtesh

Resources

Web Application Penetration Testing Checklist ~ Nitesh Gupta
https://capricious-typhoon-db6.notion.site/Web-Application-Penetration-Testing-Checklist-baa90cb760664e3094c1cff299511858

Thank you

Rizwan Syed

https://www.linkedin.com/in/r12w4n/

https://twitter.com/_r12w4n