Active Reconnaissance

Step 1-Host discovery:

Nmap-Network mapper

1. Host discovery
2. Post discovery
3. Vulnerability discovery

Syntax:

nmap (flags/options) target.com

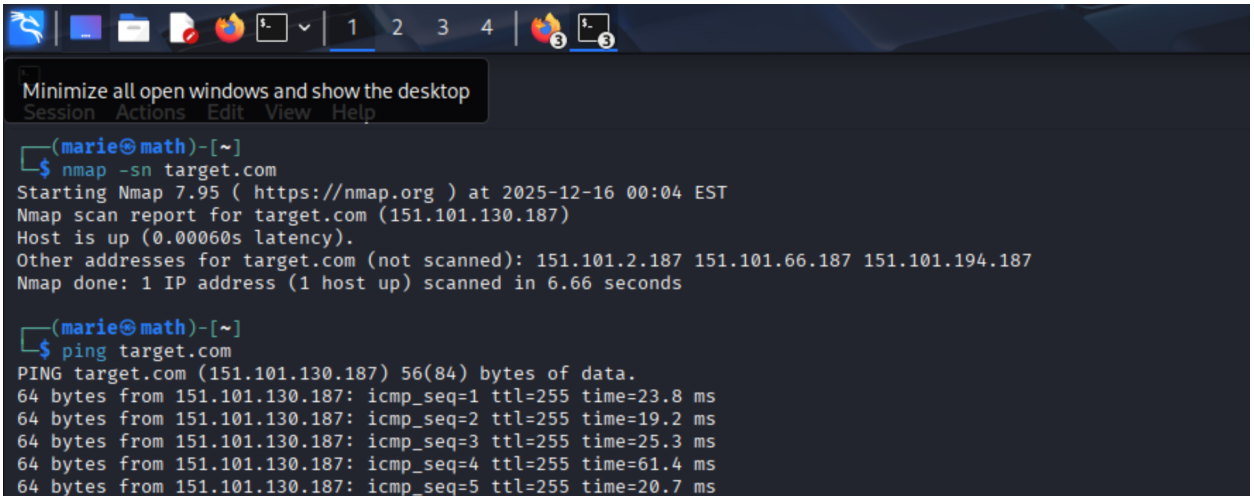
nmap (flags/options) target.com

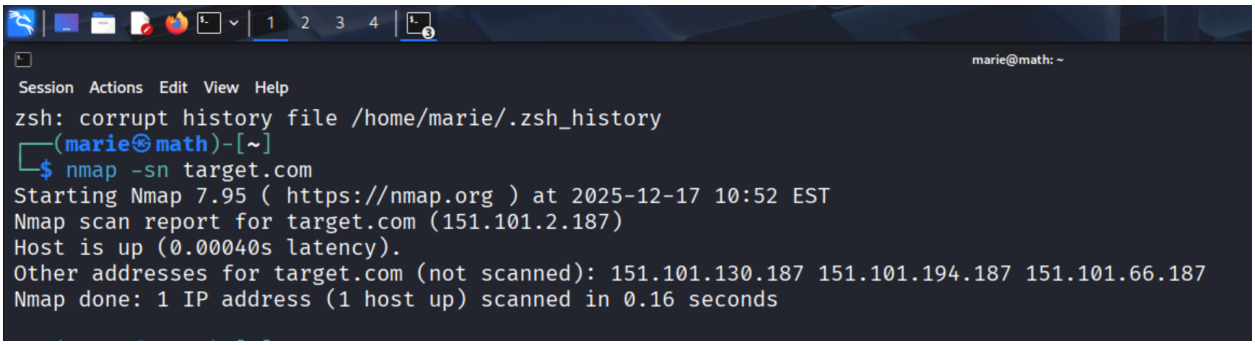
Command- nmap -sn target.com

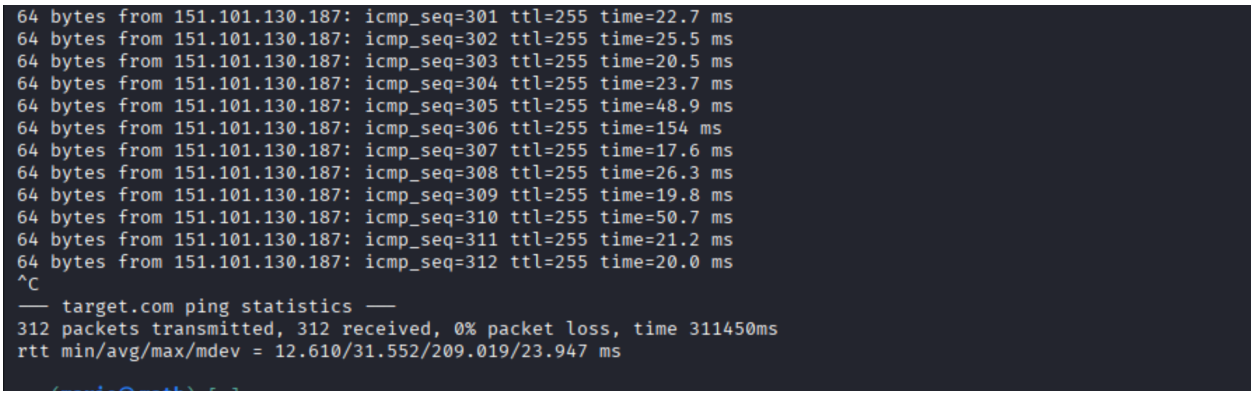
Ifconfig-for checking own ip

man nmap-nmap manual

- Identified if the target is alive and its IP.



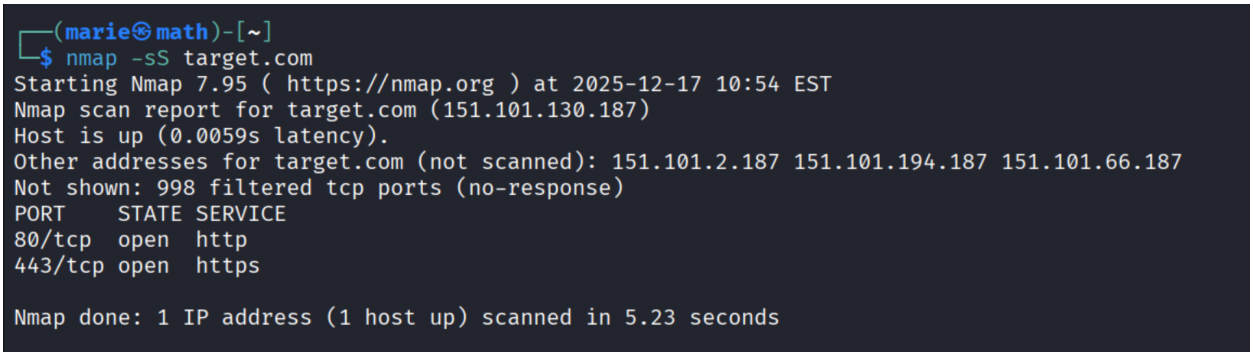




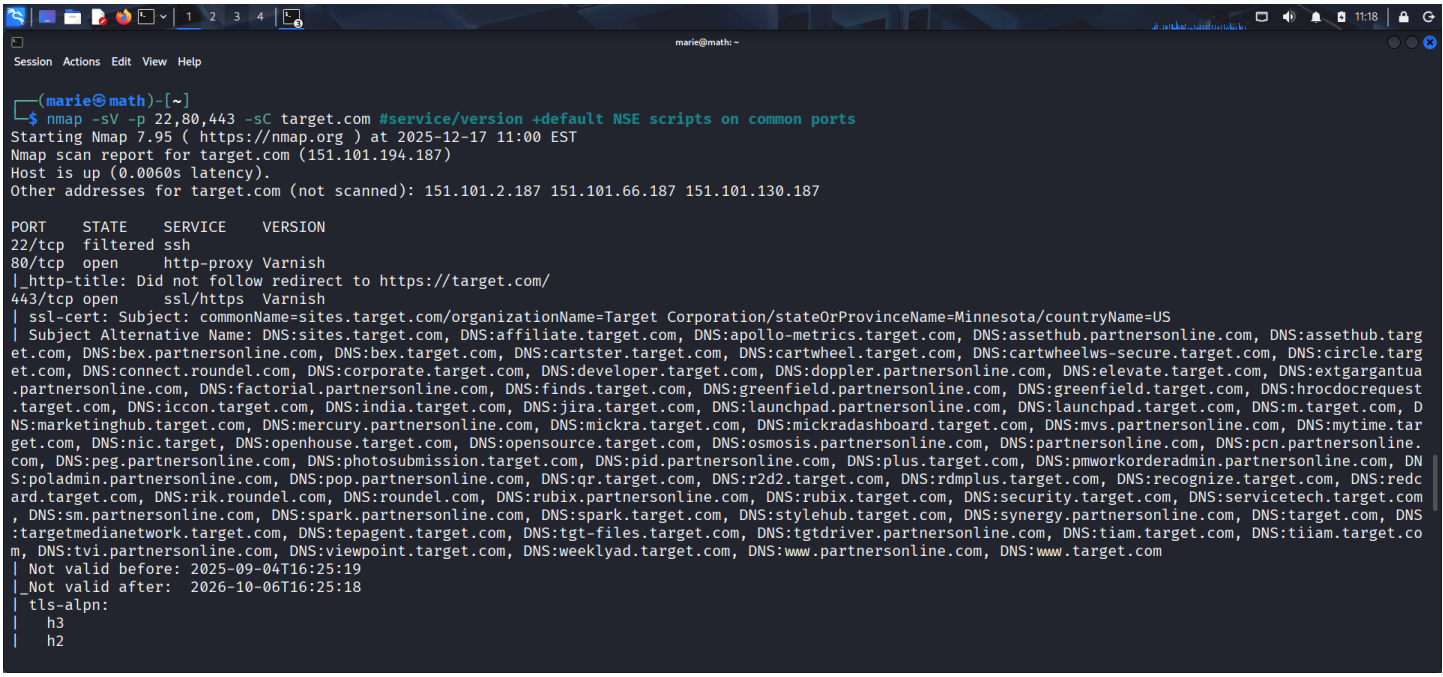
Step 2: Port & Service Scan using Nmap

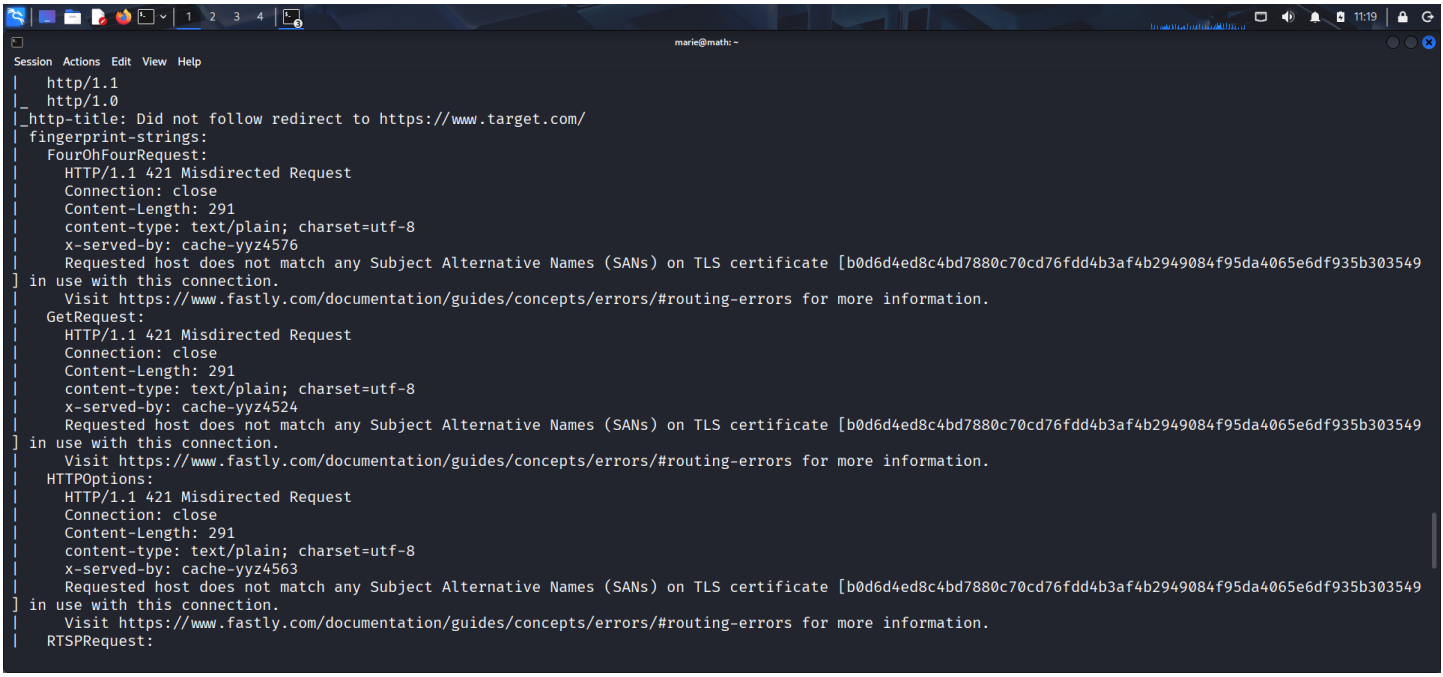
Performed staged scans: quick, then deeper.

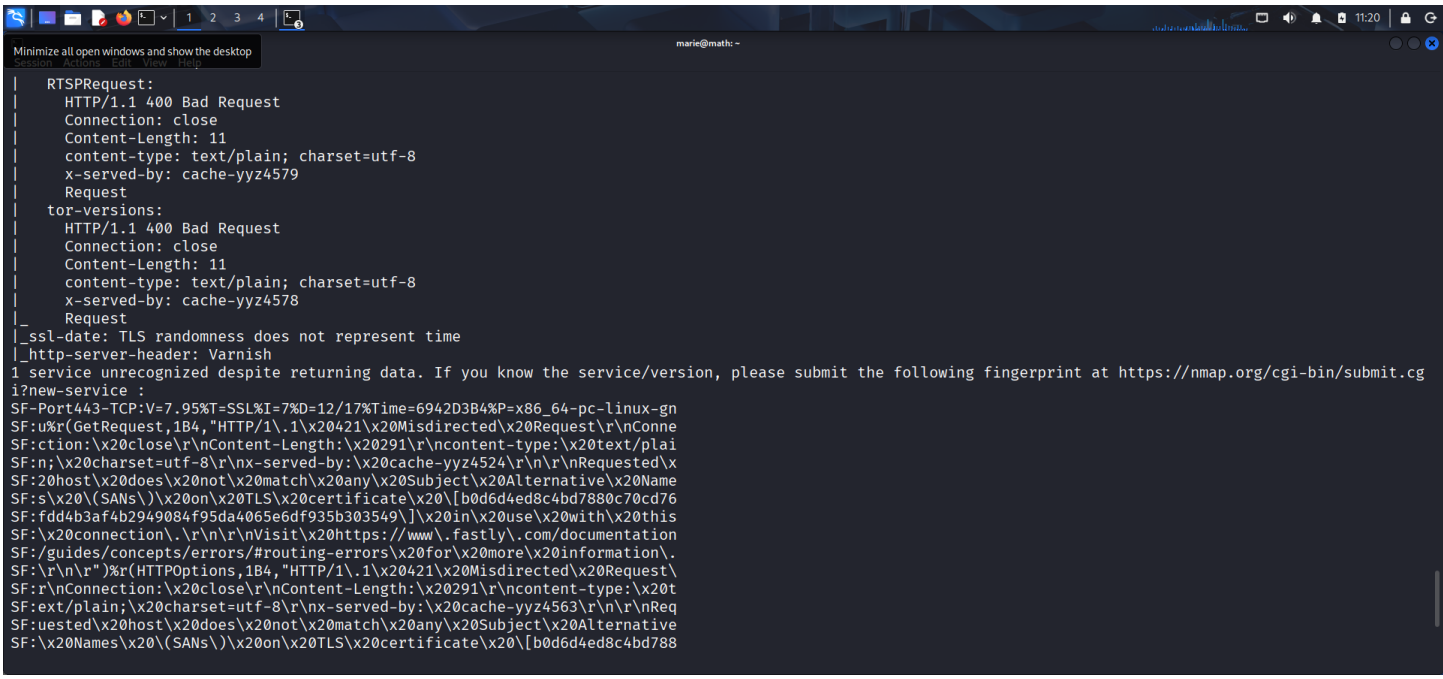
- nmap -sS target.com # TCP SYN Scan



- nmap -sV -p 22,80,443 -sC target.com # service/version + default NSE scripts on common ports



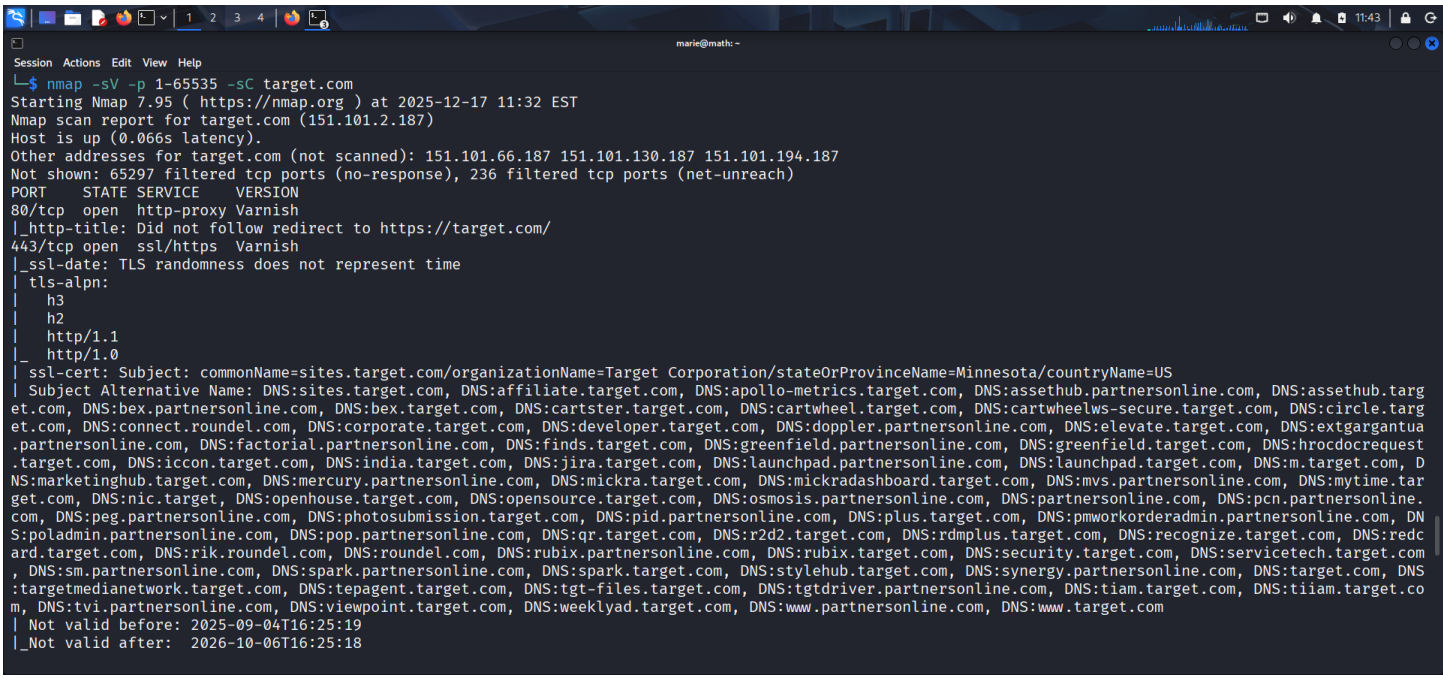


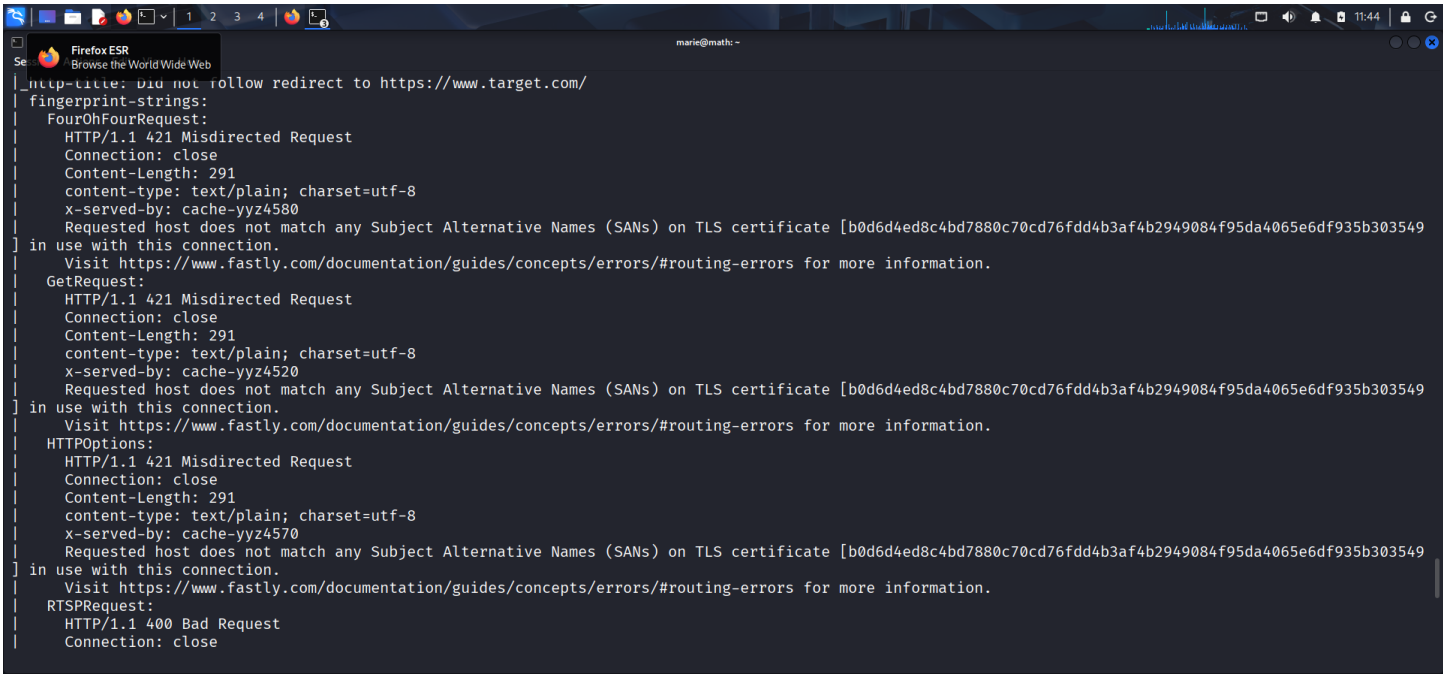

Minimize all open windows and show the desktop
marie@math: ~
| RTSPRequest:
| HTTP/1.1 400 Bad Request
| Connection: close
| Content-Length: 11
| content-type: text/plain; charset=utf-8
| x-served-by: cache-yyz4579
| Request
| tor-versions:
| HTTP/1.1 400 Bad Request
| Connection: close
| Content-Length: 11
| content-type: text/plain; charset=utf-8
| x-served-by: cache-yyz4578
|_   Request
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Varnish
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=12/17%Time=6942D3B4%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,1B4,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConne
SF:ction:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20text/plai
SF:n;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4524\r\n\r\nRequested\x
SF:20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Name
SF:s\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd7880c70cd76
SF:fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20with\x20this
SF:\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/documentation
SF:/guides/concepts/errors/#routing-errors\x20for\x20more\x20information\.
SF:\r\n\r")%r(HTTPOptions,1B4,"HTTP/1\.1\x20421\x20Misdirected\x20Request\
SF:r\nConnection:\x20close\r\nContent-Length:\x20291\r\ncontent-type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4563\r\n\r\nReq
SF:uested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative
SF:\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0d6d4ed8c4bd788

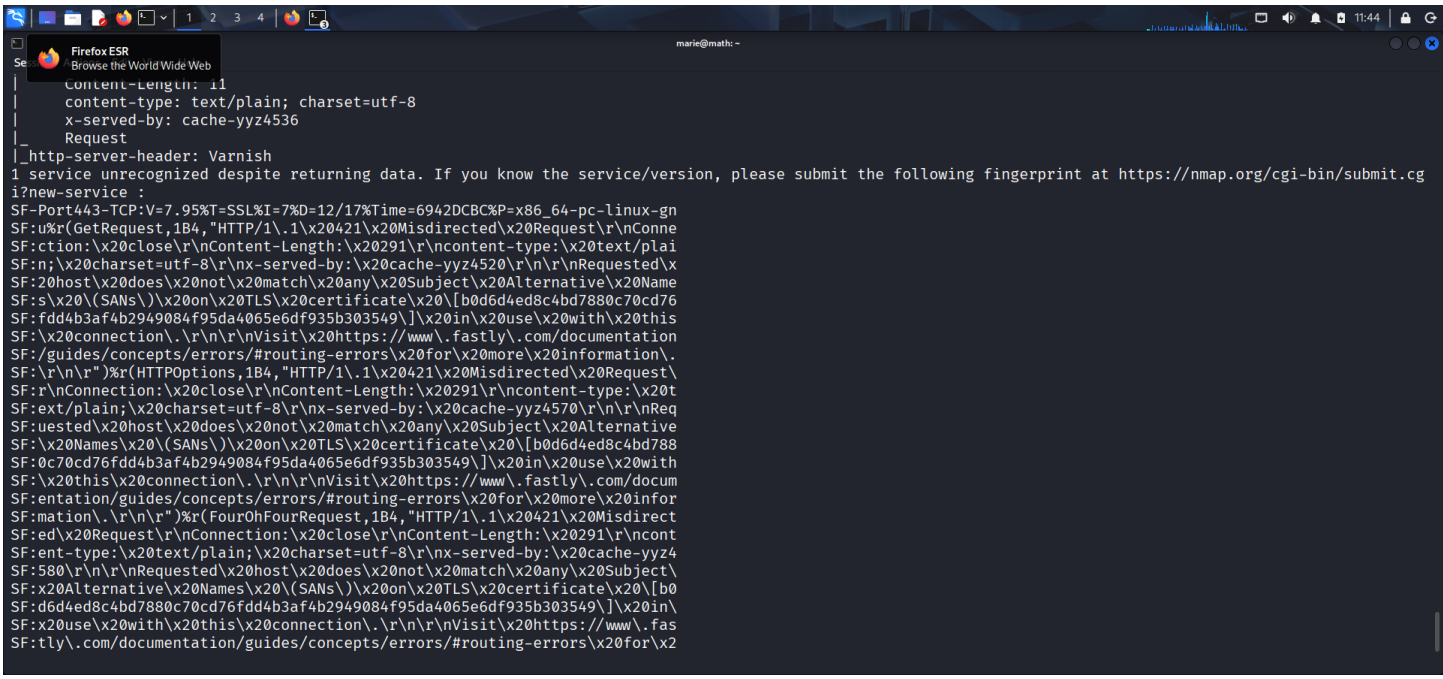

SF:0c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\x20use\x20with
SF:\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.fastly\.com/docum
SF:entation/guides/concepts/errors/#routing-errors\x20for\x20more\x20infor
SF:mation\.\r\n\r")%r(FourOhFourRequest,1B4,"HTTP/1\.1\x20421\x20Misdirect
SF:ed\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\ncont
SF:ent-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4
SF:576\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subject\
SF:x20Alternative\x20Names\x20\(SANs\)\x20on\x20TLS\x20certificate\x20\[b0
SF:d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549\]\x20in\
SF:x20use\x20with\x20this\x20connection\.\r\n\r\nVisit\x20https://www\.fas
SF:tly\.com/documentation/guides/concepts/errors/#routing-errors\x20for\x2
SF:0more\x20information\.\r\n\r")%r(tor-versions,93,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\nconte
SF:nt-type:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz45
SF:78\r\n\r\nBad\x20Request")%r(RTSPRequest,93,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\nConnection:\x20close\r\nContent-Length:\x2011\r\ncontent-ty
SF:pe:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4579\r\
SF:n\r\nBad\x20Request");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.51 seconds

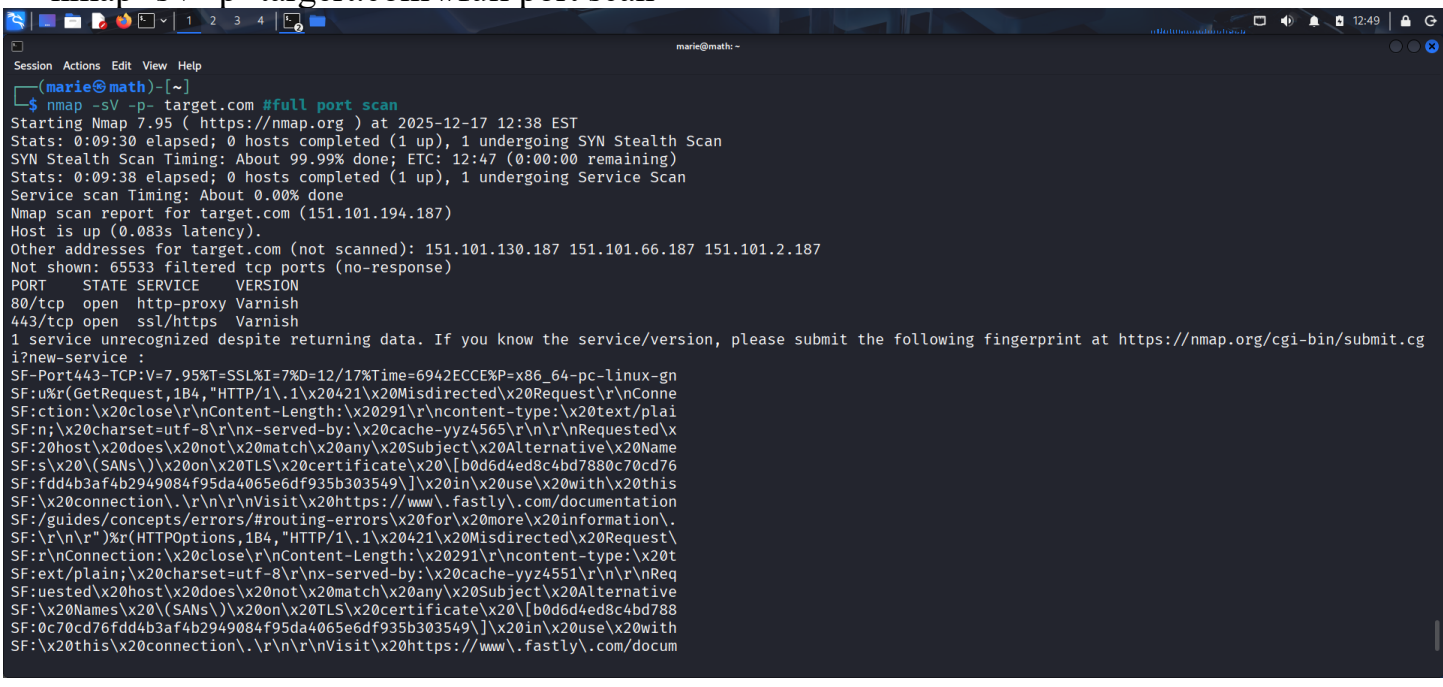
- nmap -sV -p 1-65535 -sC target.com #NSE scripts on all ports

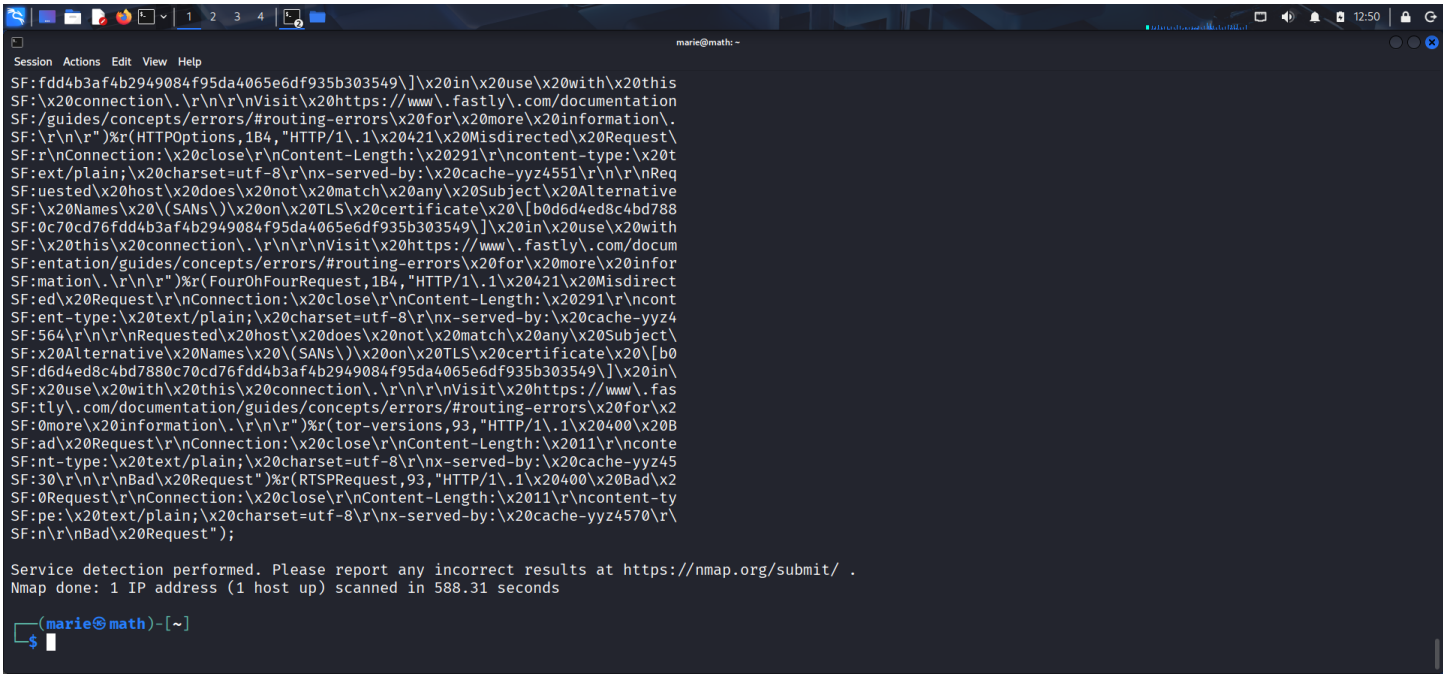




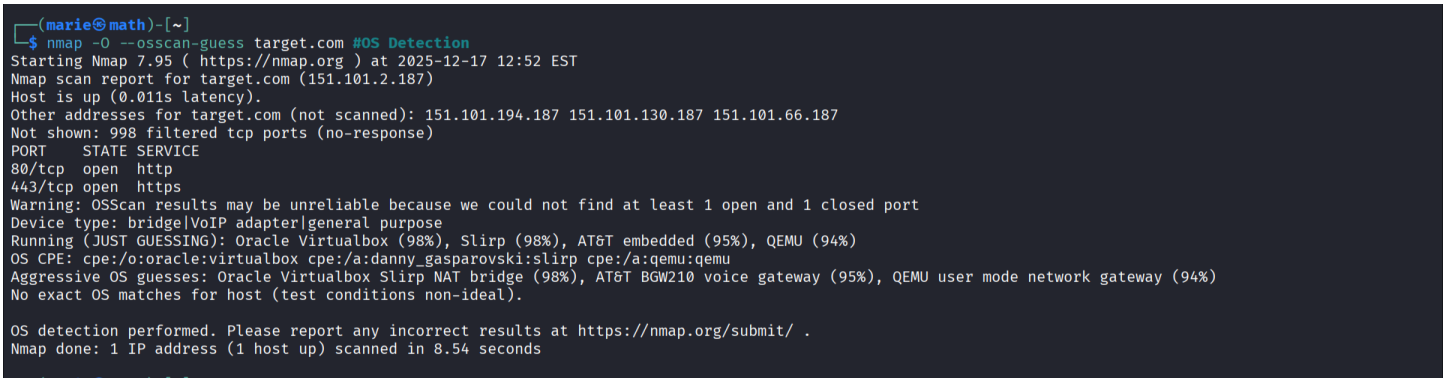


- nmap -sV -p- targert.com #full port scan





- nmap -O --osscan-guess target.com # OS detection (if allowed)



Step 3: HTTP Enumeration using Dirb

Brute-force directories & common files.

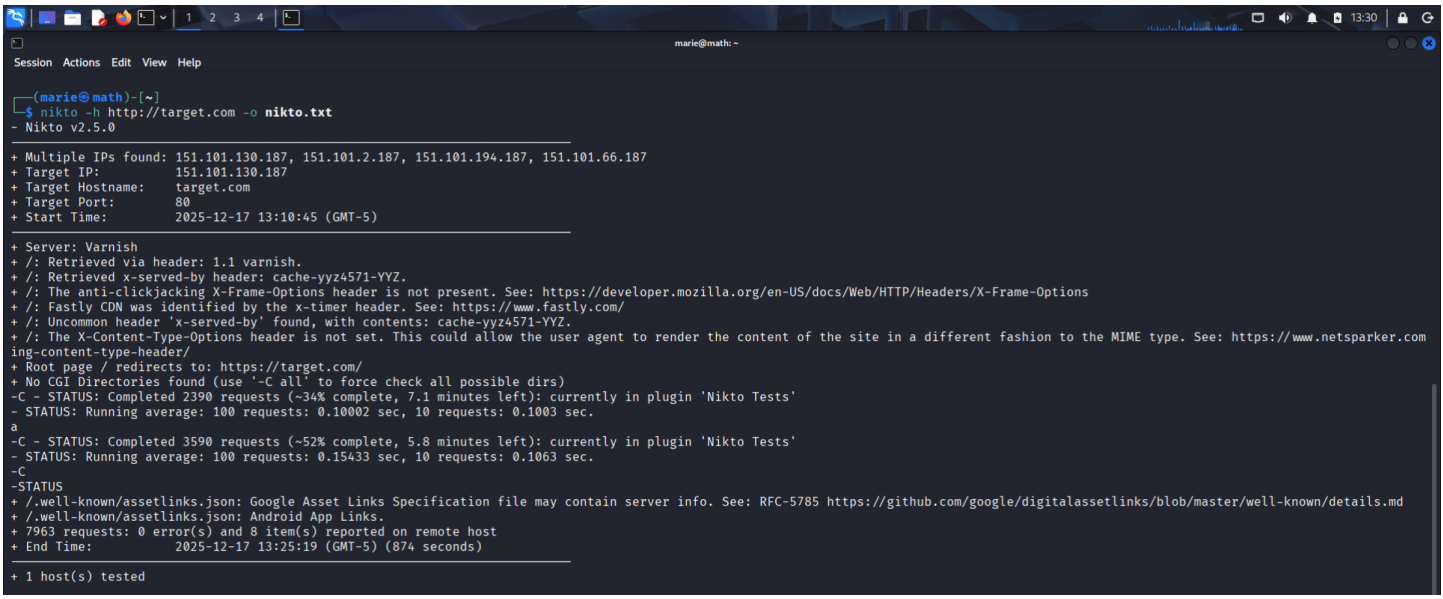
- dirb https://target.com
- dirb https://target.com /usr/share/wordlists/dirb/common.txt

```
┌──(marie㉿math)-[~]
└─$ dirb https://target.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Dec 17 12:59:20 2025
URL_BASE: https://target.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://target.com/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')

-----------------
END_TIME: Wed Dec 17 12:59:20 2025
DOWNLOADED: 0 - FOUND: 0

┌──(marie㉿math)-[~]
└─$
```

Step 4: Web fingerprinting & vulnerability checks using whatweb & nikto

Command:whatweb http://target.com

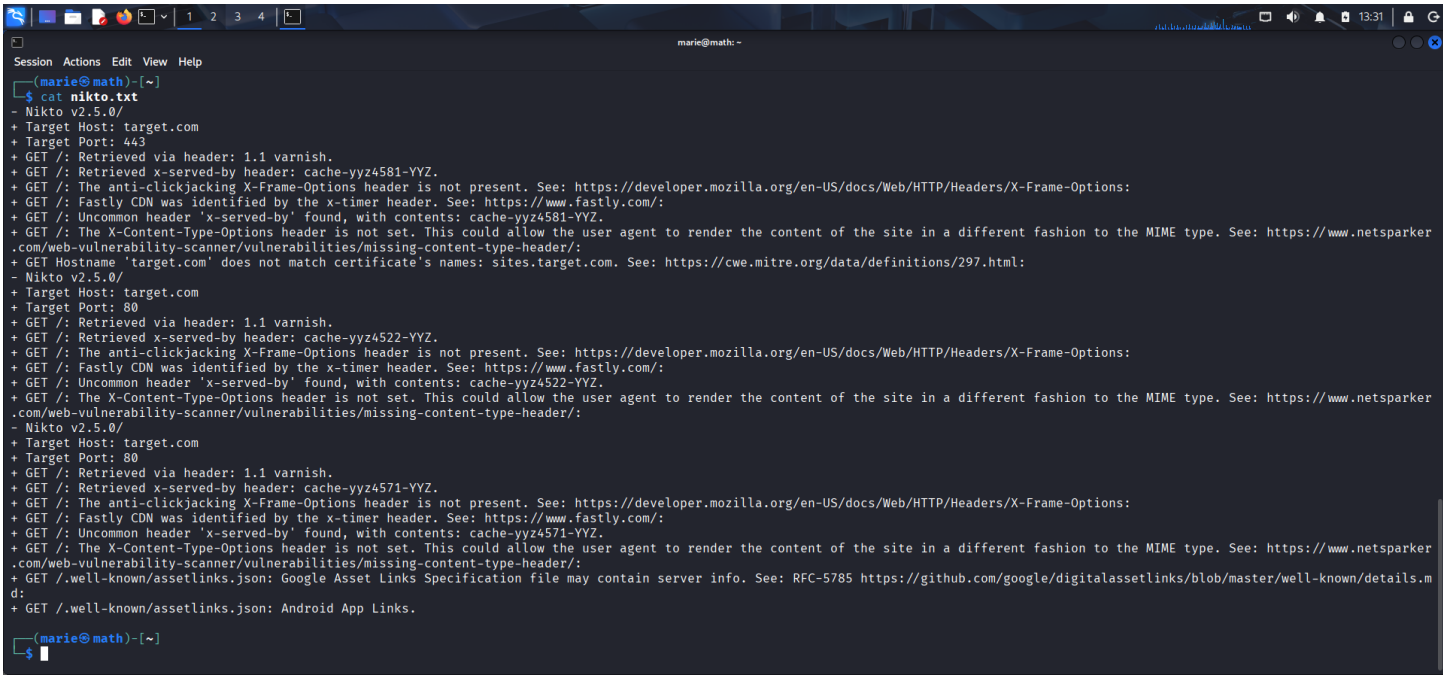
nikto -h http://target.com -o nikto.txt


marie@math: ~
Session Actions Edit View Help
┌──(marie㉿math)-[~]
└─$ nikto -h http://target.com -o nikto.txt
- Nikto v2.5.0

+ Multiple IPs found: 151.101.130.187, 151.101.2.187, 151.101.194.187, 151.101.66.187
+ Target IP: 151.101.130.187
+ Target Hostname: target.com
+ Target Port: 80
+ Start Time: 2025-12-17 13:10:45 (GMT-5)

+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-yyz4571-YYZ.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-yyz4571-YYZ.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com
ing-content-type-header/
+ Root page / redirects to: https://target.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
-C - STATUS: Completed 2390 requests (~34% complete, 7.1 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.10002 sec, 10 requests: 0.1003 sec.
a
-C - STATUS: Completed 3590 requests (~52% complete, 5.8 minutes left): currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.15433 sec, 10 requests: 0.1063 sec.
-C
-STATUS
+ /.well-known/assetlinks.json: Google Asset Links Specification file may contain server info. See: RFC-5785 https://github.com/google/digitalassetlinks/blob/master/well-known/details.md
+ /.well-known/assetlinks.json: Android App Links.
+ 7963 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time: 2025-12-17 13:25:19 (GMT-5) (874 seconds)

+ 1 host(s) tested


marie@math: ~
Session Actions Edit View Help
┌──(marie㉿math)-[~]
└─$ cat nikto.txt
- Nikto v2.5.0/
+ Target Host: target.com
+ Target Port: 443
+ GET /: Retrieved via header: 1.1 varnish.
+ GET /: Retrieved x-served-by header: cache-yyz4581-YYZ.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/:
+ GET /: Uncommon header 'x-served-by' found, with contents: cache-yyz4581-YYZ.
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker
.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET Hostname 'target.com' does not match certificate's names: sites.target.com. See: https://cwe.mitre.org/data/definitions/297.html:
- Nikto v2.5.0/
+ Target Host: target.com
+ Target Port: 80
+ GET /: Retrieved via header: 1.1 varnish.
+ GET /: Retrieved x-served-by header: cache-yyz4522-YYZ.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/:
+ GET /: Uncommon header 'x-served-by' found, with contents: cache-yyz4522-YYZ.
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker
.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
- Nikto v2.5.0/
+ Target Host: target.com
+ Target Port: 80
+ GET /: Retrieved via header: 1.1 varnish.
+ GET /: Retrieved x-served-by header: cache-yyz4571-YYZ.
+ GET /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options:
+ GET /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/:
+ GET /: Uncommon header 'x-served-by' found, with contents: cache-yyz4571-YYZ.
+ GET /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker
.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/:
+ GET /.well-known/assetlinks.json: Google Asset Links Specification file may contain server info. See: RFC-5785 https://github.com/google/digitalassetlinks/blob/master/well-known/details.m
d:
+ GET /.well-known/assetlinks.json: Android App Links.
┌──(marie㉿math)-[~]
└─$