

Active Reconnaissance

Step 1-Host discovery:

Nmap-Network mapper

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

Syntax:

nmap (flags/options) target.com

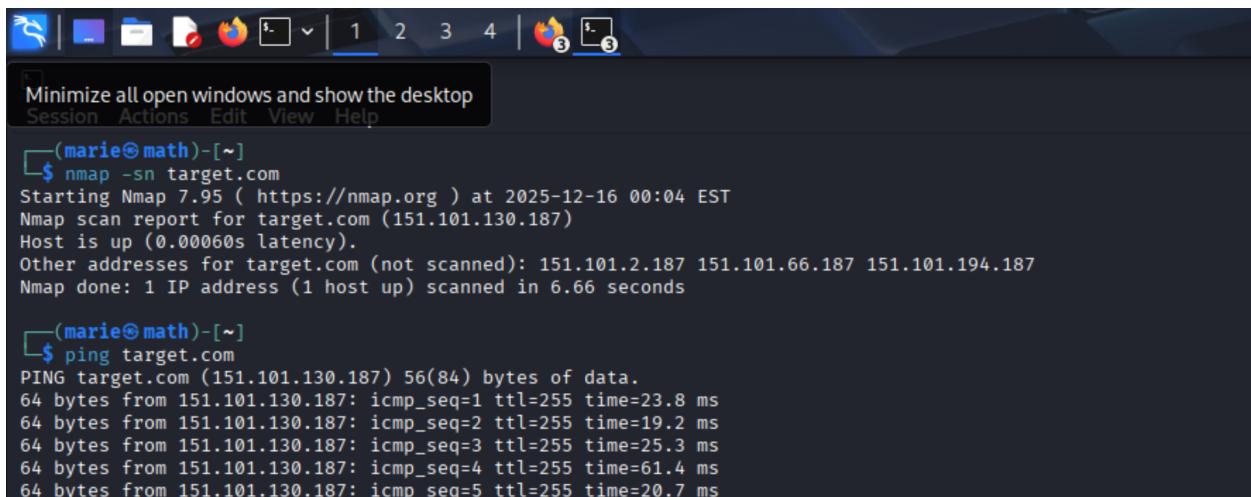
nmap (flags/options) target.com

Command- nmap -sn target.com

Ifconfig-for checking own ip

man nmap-nmap manual

- Identified if the target is alive and its IP.



```
Minimize all open windows and show the desktop
Session Actions Edit View Help

(marie@math)-[~]
$ nmap -sn target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-16 00:04 EST
Nmap scan report for target.com (151.101.130.187)
Host is up (0.00060s latency).
Other addresses for target.com (not scanned): 151.101.2.187 151.101.66.187 151.101.194.187
Nmap done: 1 IP address (1 host up) scanned in 6.66 seconds

(marie@math)-[~]
$ ping target.com
PING target.com (151.101.130.187) 56(84) bytes of data.
64 bytes from 151.101.130.187: icmp_seq=1 ttl=255 time=23.8 ms
64 bytes from 151.101.130.187: icmp_seq=2 ttl=255 time=19.2 ms
64 bytes from 151.101.130.187: icmp_seq=3 ttl=255 time=25.3 ms
64 bytes from 151.101.130.187: icmp_seq=4 ttl=255 time=61.4 ms
64 bytes from 151.101.130.187: icmp_seq=5 ttl=255 time=20.7 ms
```

```
Session Actions Edit View Help
zsh: corrupt history file /home/marie/.zsh_history
└─(marie@math)─[~]
└─$ nmap -sn target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 10:52 EST
Nmap scan report for target.com (151.101.2.187)
Host is up (0.00040s latency).
Other addresses for target.com (not scanned): 151.101.130.187 151.101.194.187 151.101.66.187
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

```
64 bytes from 151.101.130.187: icmp_seq=301 ttl=255 time=22.7 ms
64 bytes from 151.101.130.187: icmp_seq=302 ttl=255 time=25.5 ms
64 bytes from 151.101.130.187: icmp_seq=303 ttl=255 time=20.5 ms
64 bytes from 151.101.130.187: icmp_seq=304 ttl=255 time=23.7 ms
64 bytes from 151.101.130.187: icmp_seq=305 ttl=255 time=48.9 ms
64 bytes from 151.101.130.187: icmp_seq=306 ttl=255 time=154 ms
64 bytes from 151.101.130.187: icmp_seq=307 ttl=255 time=17.6 ms
64 bytes from 151.101.130.187: icmp_seq=308 ttl=255 time=26.3 ms
64 bytes from 151.101.130.187: icmp_seq=309 ttl=255 time=19.8 ms
64 bytes from 151.101.130.187: icmp_seq=310 ttl=255 time=50.7 ms
64 bytes from 151.101.130.187: icmp_seq=311 ttl=255 time=21.2 ms
64 bytes from 151.101.130.187: icmp_seq=312 ttl=255 time=20.0 ms
^C
--- target.com ping statistics ---
312 packets transmitted, 312 received, 0% packet loss, time 311450ms
rtt min/avg/max/mdev = 12.610/31.552/209.019/23.947 ms
```

Step 2: Port & Service Scan using Nmap

Performed staged scans: quick, then deeper.

- nmap -sS target.com # TCP SYN Scan

```
└─(marie@math)─[~]
└─$ nmap -sS target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 10:54 EST
Nmap scan report for target.com (151.101.130.187)
Host is up (0.0059s latency).
Other addresses for target.com (not scanned): 151.101.2.187 151.101.194.187 151.101.66.187
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 5.23 seconds
```

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

```
(marie@math) [~]
$ nmap -sV -p 22,80,443 -sC target.com #service/version +default NSE scripts on common ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 11:00 EST
Nmap scan report for target.com (151.101.194.187)
Host is up (0.0060s latency).
Other addresses for target.com (not scanned): 151.101.2.187 151.101.66.187 151.101.130.187

PORT      STATE    SERVICE      VERSION
22/tcp    filtered  ssh
80/tcp    open     http-proxy  Varnish
|_http-title: Did not follow redirect to https://target.com/
443/tcp   open     ssl/https  Varnish
| ssl-cert: Subject: commonName=sites.target.com/organizationName=Target Corporation/stateOrProvinceName=Minnesota/countryName=US
| Subject Alternative Name: DNS:sites.target.com, DNS:affiliate.target.com, DNS:apollo-metrics.target.com, DNS:assethub.partnersonline.com, DNS:assethub.target.com, DNS:bex.partnersonline.com, DNS:bex.target.com, DNS:cartsster.target.com, DNS:cartwheel.target.com, DNS:cartwheelws-secure.target.com, DNS:circle.target.com, DNS:connect.roundel.com, DNS:corporate.target.com, DNS:developer.target.com, DNS:doppler.partnersonline.com, DNS:elevate.target.com, DNS:extgargantua.partnersonline.com, DNS:factorial.partnersonline.com, DNS:finds.target.com, DNS:greenfield.partnersonline.com, DNS:greenfield.target.com, DNS:hroddorequest.target.com, DNS:iccon.target.com, DNS:india.target.com, DNS:jira.target.com, DNS:launchpad.partnersonline.com, DNS:launchpad.target.com, DNS:m.target.com, DNS:marketinghub.target.com, DNS:mercury.partnersonline.com, DNS:mickra.target.com, DNS:mickradashboard.target.com, DNS:mvs.partnersonline.com, DNS:mytime.target.com, DNS:nic.target, DNS:openhouse.target.com, DNS:opensource.target.com, DNS:osmosis.partnersonline.com, DNS:partneronline.com, DNS:pcn.partnersonline.com, DNS:peg.partnersonline.com, DNS:photosubmission.target.com, DNS:pid.partnersonline.com, DNS:plus.target.com, DNS:pmworkorderadmin.partnersonline.com, DNS:poladmin.partnersonline.com, DNS:pop.partnersonline.com, DNS:qr.target.com, DNS:r2d.target.com, DNS:rdmplus.target.com, DNS:recognize.target.com, DNS:redcard.target.com, DNS:rik.roundel.com, DNS:roundel.com, DNS:rubix.partnersonline.com, DNS:rubix.target.com, DNS:security.target.com, DNS:servicetech.target.com, DNS:sm.partnersonline.com, DNS:spark.partnersonline.com, DNS:spark.target.com, DNS:stylehub.target.com, DNS:synergy.partnersonline.com, DNS:target.com, DNS:taiam.target.com, DNS:taiam.target.com, DNS:tv1.partnersonline.com, DNS:viewpoint.target.com, DNS:tgt-files.target.com, DNS:tgtdriver.partnersonline.com, DNS:tiams.target.com, DNS:www.partnersonline.com, DNS:www.target.com
| Not valid before: 2025-09-04T16:25:19
| Not valid after: 2026-10-06T16:25:18
| tls-alpn:
|_ h3
|_ h2
```

```
(marie@math) [~]
Session Actions Edit View Help
| http/1.1
| http/1.0
|_http-title: Did not follow redirect to https://www.target.com/
| fingerprint-strings:
| FourOhFourRequest:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4576
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| GetRequest:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4524
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| HTTPOptions:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4563
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549] in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| RTSPRequest:
```

```
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-yyz4579  
| 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.cgi?new-service :  
SF-Port443-TCP:V=7.95%T=SSL%I=7%D=12/17%Time=6942D3B4%P=x86_64-pc-linux-gnu  
SF:u$(`GetRequest,1B4,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nContent-Type:\x20text/plain\x20charset=utf-8\r\nnx-served-by:\x20cache-yyz4524\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Name\x20(SANs)\x20on\x20TLS\x20certificate\x20[b0d6d4ed8c4bd7880c70cd76\x20fdd4b3af4b2949084f95da4065e6df935b303549]\x20in\x20use\x20with\x20this\x20connection.\r\nVisit\x20https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20information.\r\nHTTPOptions,1B4,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nContent-Type:\x20text/plain\x20charset=utf-8\r\nnx-served-by:\x20cache-yyz4563\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Names\x20(\SANs)\x20on\x20TLS\x20certificate\x20[b0d6d4ed8c4bd7880c70cd76\x20fdd4b3af4b2949084f95da4065e6df935b303549]\x20in\x20use\x20with\x20this\x20connection.\r\nVisit\x20https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20information.\r\nHTTPRequest,1B4,"HTTP/1\.1\x20421\x20Misdirected\x20Request\r\nConnection:\x20close\r\nContent-Length:\x20291\r\nContent-Type:\x20text/plain\x20charset=utf-8\r\nnx-served-by:\x20cache-yyz4563\r\n\r\nRequested\x20host\x20does\x20not\x20match\x20any\x20Subject\x20Alternative\x20Names\x20(\SANs)\x20on\x20TLS\x20certificate\x20[b0d6d4ed8c4bd7880c70cd76\x20fdd4b3af4b2949084f95da4065e6df935b303549]\x20in\x20use\x20with\x20this\x20connection.\r\nVisit\x20https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors\x20for\x20more\x20information.\r\nHTTPResponse,1B4,"HTTP/1\.1\x20400\x20Bad Request\r\nConnection:\x20close\r\nContent-Length:\x20201\r\nContent-Type:\x20text/plain\x20charset=utf-8\r\nnx-served-by:\x20cache-yyz4579\r\n\r\nBad Request")`  
SF:0Request\r\nConnection:\x20close\r\nContent-Length:\x20201\r\nContent-Type:\x20text/plain\x20charset=utf-8\r\nnx-served-by:\x20cache-yyz4579";  
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

```

Session Actions Edit View Help
└$ nmap -sV -p 1-65535 -sC target.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 11:32 EST
Nmap scan report for target.com (151.101.2.187)
Host is up (0.066s latency).
Other addresses for target.com (not scanned): 151.101.66.187 151.101.130.187 151.101.194.187
Not shown: 65297 filtered tcp ports (no-response), 236 filtered tcp ports (net-unreach)
PORT      STATE SERVICE VERSION
80/tcp    open  http-proxy Varnish
|_http-title: Did not follow redirect to https://target.com/
443/tcp   open  ssl/https Varnish
|_ssl-date: TLS randomness does not represent time
|_tls-alpn:
|   h3
|   h2
|   http/1.1
|   http/1.0
| ssl-cert: Subject: commonName=sites.target.com/organizationName=Target Corporation/stateOrProvinceName=Minnesota/countryName=US
| Subject Alternative Name: DNS:sites.target.com, DNS:affiliate.target.com, DNS:apollo-metrics.target.com, DNS:assethub.partnersonline.com, DNS:assethub.targ
| et.com, DNS:bex.partnersonline.com, DNS:bex.target.com, DNS:cartsster.target.com, DNS:cartwheel.target.com, DNS:cartwheelws-secure.target.com, DNS:circle.targ
| et.com, DNS:connect.roundel.com, DNS:corporate.target.com, DNS:developer.target.com, DNS:doppler.partnersonline.com, DNS:elevate.target.com, DNS:extgargantua
| .partnersonline.com, DNS:factorial.partnersonline.com, DNS:finds.target.com, DNS:greenfield.partnersonline.com, DNS:greenfield.target.com, DNS:hrocdocrequest
| .target.com, DNS:iccon.target.com, DNS:india.target.com, DNS:jira.target.com, DNS:launchpad.partnersonline.com, DNS:launchpad.target.com, DNS:m.target.com, D
| NS:marketinghub.target.com, DNS:mercury.partnersonline.com, DNS:mickra.target.com, DNS:mickradashboard.target.com, DNS:mvs.partnersonline.com, DNS:mytime.tar
| get.com, DNS:nic.target, DNS:openhouse.target.com, DNS:opensource.target.com, DNS:osmosis.partnersonline.com, DNS:partnersonline.com, DNS:pcn.partnersonline.
| com, DNS:peg.partnersonline.com, DNS:photosubmission.target.com, DNS:pid.partnersonline.com, DNS:plus.target.com, DNS:pmworkorderadmin.partnersonline.com, DN
| S:poladmin.partnersonline.com, DNS:pop.partnersonline.com, DNS:qr.target.com, DNS:r2d2.target.com, DNS:rdmplus.target.com, DNS:recognize.target.com, DNS:redc
| ard.target.com, DNS:rik.roundel.com, DNS:roundel.com, DNS:rubix.partnersonline.com, DNS:rubix.target.com, DNS:security.target.com, DNS:servicetech.target.com
| , DNS:sm.partnersonline.com, DNS:spark.partnersonline.com, DNS:spark.target.com, DNS:stylehub.target.com, DNS:synergy.partnersonline.com, DNS:target.com, DNS:t
| :targetmedianetwork.target.com, DNS:tepagent.target.com, DNS:tgt-files.target.com, DNS:tgtdriver.partnersonline.com, DNS:tiam.target.com, DNS:tiam.target.co
| m, DNS:tv1.partnersonline.com, DNS:viewpoint.target.com, DNS:weeklyad.target.com, DNS:www.partnersonline.com, DNS:www.target.com
| Not valid before: 2025-09-04T16:25:19
| Not valid after: 2026-10-06T16:25:18

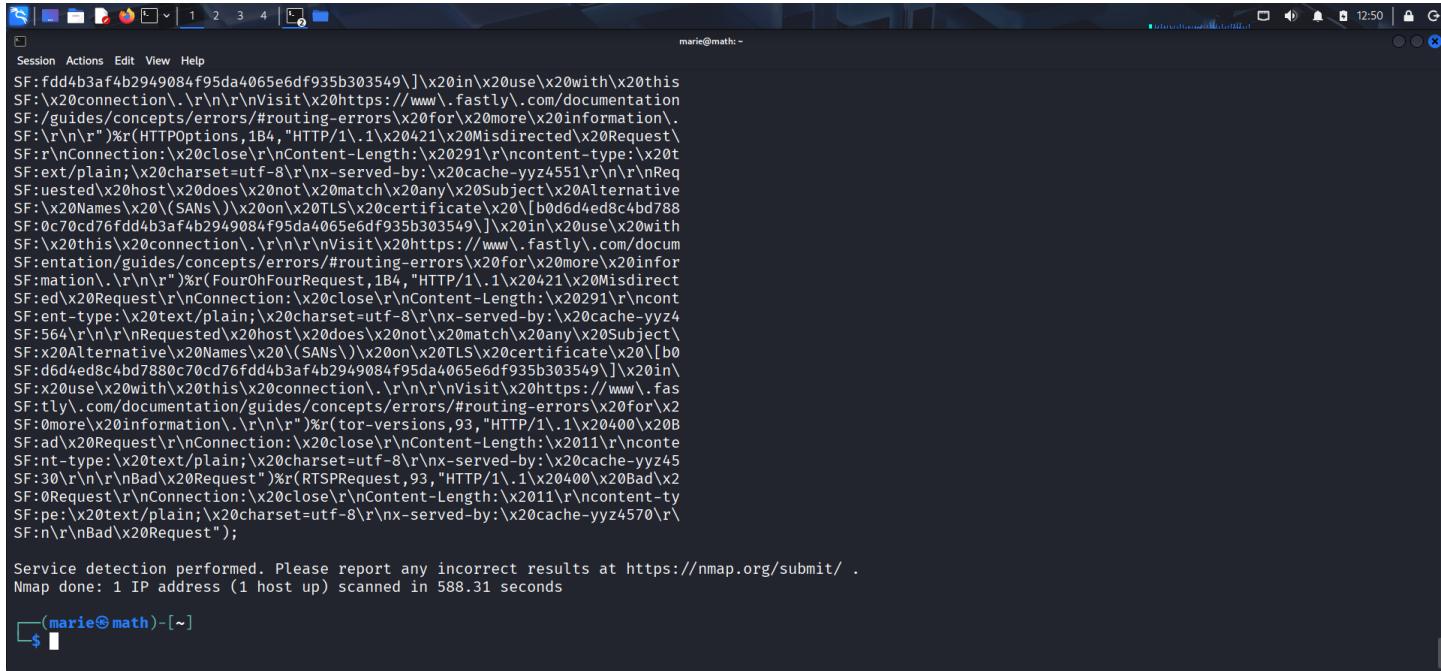
```

```

Session Actions Edit View Help
Se Firefox ESR
Browse the World Wide Web
|_http-title: Did not follow redirect to https://www.target.com/
| fingerprint-strings:
| FourOhFourRequest:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4580
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549]
| in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| GetRequest:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4520
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549]
| in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| HTTPOptions:
|   HTTP/1.1 421 Misdirected Request
|   Connection: close
|   Content-Length: 291
|   content-type: text/plain; charset=utf-8
|   x-served-by: cache-yyz4570
|   Requested host does not match any Subject Alternative Names (SANs) on TLS certificate [b0d6d4ed8c4bd7880c70cd76fdd4b3af4b2949084f95da4065e6df935b303549]
| in use with this connection.
|   Visit https://www.fastly.com/documentation/guides/concepts/errors/#routing-errors for more information.
| RTSPRequest:
|   HTTP/1.1 400 Bad Request
|   Connection: close

```

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



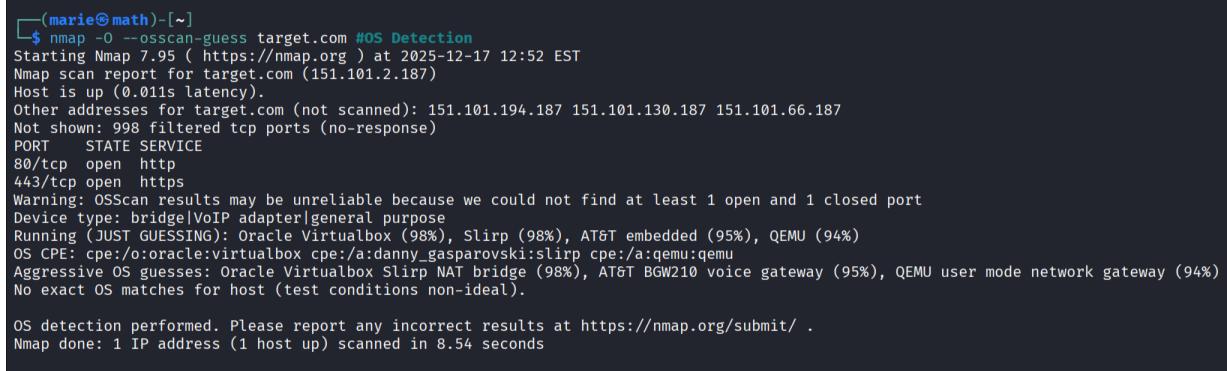
```

Session Actions Edit View Help
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:text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4551\r\n\r\nReq
SF:uested\x20does\x20not\x20match\x20any\x20Subject\x20Alternative
SF:\x20Names\x20(SANs\x20on\x20TLS\x20certificate\x20[b0d6d4ed8c4bd788
SF:0cd76fdd4b3af4b2949084f95da4065e6df935b303549]\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:564\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\x20
SF:more\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:30\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-t
SF:pe:\x20text/plain;\x20charset=utf-8\r\nx-served-by:\x20cache-yyz4570\r\n
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 588.31 seconds

```

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



```

(marie@math)-[~]
$ nmap -O --osscan-guess target.com #OS Detection
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-17 12:52 EST
Nmap scan report for target.com (151.101.2.187)
Host is up (0.011s latency).
Other addresses for target.com (not scanned): 151.101.194.187 151.101.130.187 151.101.66.187
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.54 seconds

```

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

```

└─$ whatweb http://target.com
http://target.com [301 Moved Permanently] Country[UNITED STATES][us], HTTPServer[Varnish], IP[151.101.130.187], RedirectLocation[https://target.com/], UncommonHeaders[retry-after,x-served-by,x-cache-rl], Varnish, Via-Proxy[1.1 varnish]
https://target.com/ [301 Moved Permanently] Country[UNITED STATES][us], HTTPServer[Varnish], IP[151.101.2.187], RedirectLocation[https://www.target.com/], Strict-Transport-Security[max-age=31536000], domains; preload, UncommonHeaders[retry-after,x-served-by,x-cache-hits,x-timer], Varnish, Via-Proxy[1.1 varnish]
https://www.target.com/ [200 OK] Cookies[GuestLocation,TeleafAkAsid,accessToken,adScriptData,egsSessionId,idToken,onboardingGuest,refreshToken,sapphire,visitorId], Country[UNITED STATES][us], HTMLAccessToken,egsSessionId,refreshToken], IP[199.232.22.187], Open-Graph-Protocol, OpenSearch[https://assets.targetimg1.com/webui/top-of-funnel/opensearchdescription.xml], Script[application/json,application/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], UncommonHeaders[referrer-policy,x-content-type-options,content-security-policy], X-Frame-Options[SAMEORIGIN]

```

```
(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-yzz4571-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-yzz4571-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) [~]
$ 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-yzz4581-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-yzz4581-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-yzz4522-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-yzz4522-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-yzz4571-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-yzz4571-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.md:
d:
+ GET /.well-known/assetlinks.json: Android App Links.

(marie@math) [~]
```