Recon & Nmap Practice Report

Date: [DATE]

Target: https://www.hackthissite.org/

1. Tools & Resources Used

whois, nmap, dig/host, curl/wget, shodan, Google dorks, terminal commands.

2. Target Overview & Scope

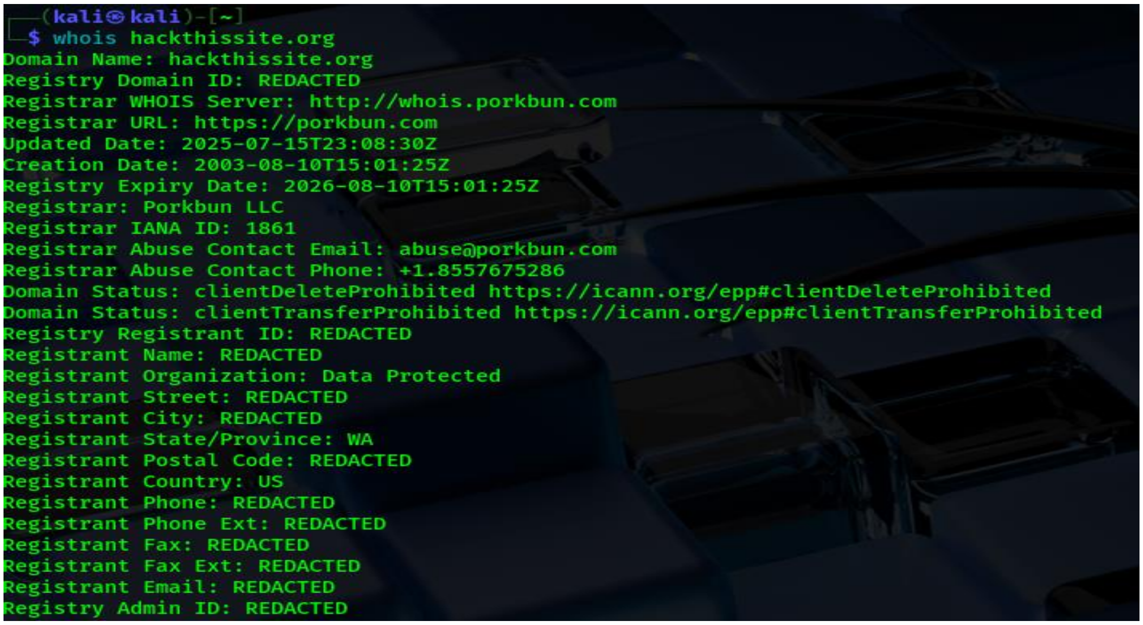
Target URL: https://www.hackthissite.org/

Scope: Passive OSINT (whois, Google, Shodan, etc) and permitted active scanning (nmap, etc). Do not attack services outside the permitted scope.

3. Whois (Domain Registration)

Command used: whois hackthissite.org

Paste the full whois output here or insert a screenshot below.

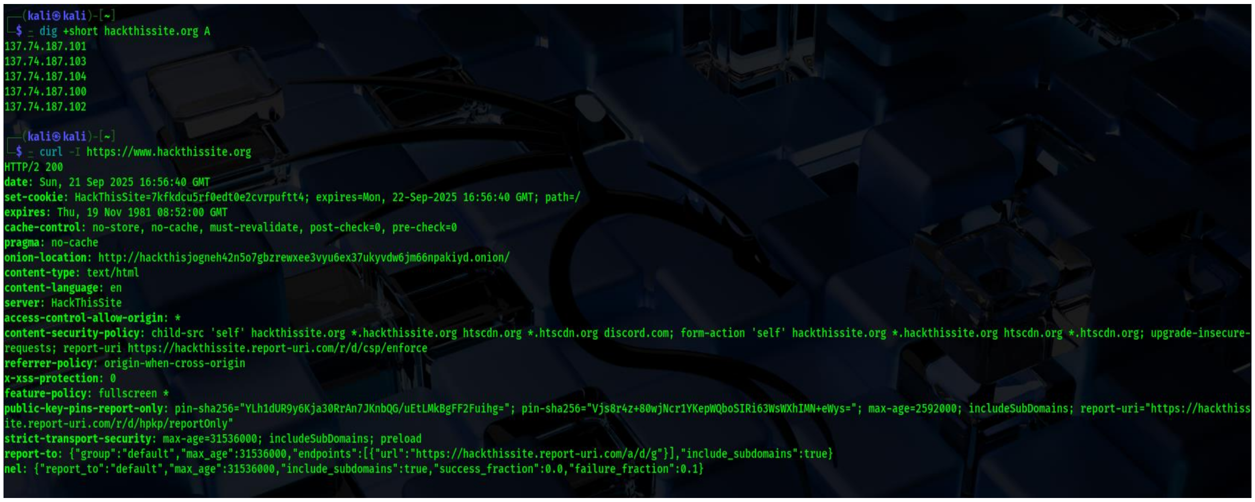


```
┌──(kali㉿kali)-[~]
└─$ whois hackthissite.org
Domain Name: hackthissite.org
Registry Domain ID: REDACTED
Registrar WHOIS Server: http://whois.porkbun.com
Registrar URL: https://porkbun.com
Updated Date: 2025-07-15T23:08:30Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2026-08-10T15:01:25Z
Registrar: Porkbun LLC
Registrar IANA ID: 1861
Registrar Abuse Contact Email: abuse@porkbun.com
Registrar Abuse Contact Phone: +1.8557675286
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED
Registrant Name: REDACTED
Registrant Organization: Data Protected
Registrant Street: REDACTED
Registrant City: REDACTED
Registrant State/Province: WA
Registrant Postal Code: REDACTED
Registrant Country: US
Registrant Phone: REDACTED
Registrant Phone Ext: REDACTED
Registrant Fax: REDACTED
Registrant Fax Ext: REDACTED
Registrant Email: REDACTED
Registry Admin ID: REDACTED
```

4. OSINT Lookups

Include any Google/Bing dork results, GitHub search hits, HaveIBeenPwned checks, and DNS lookups performed.

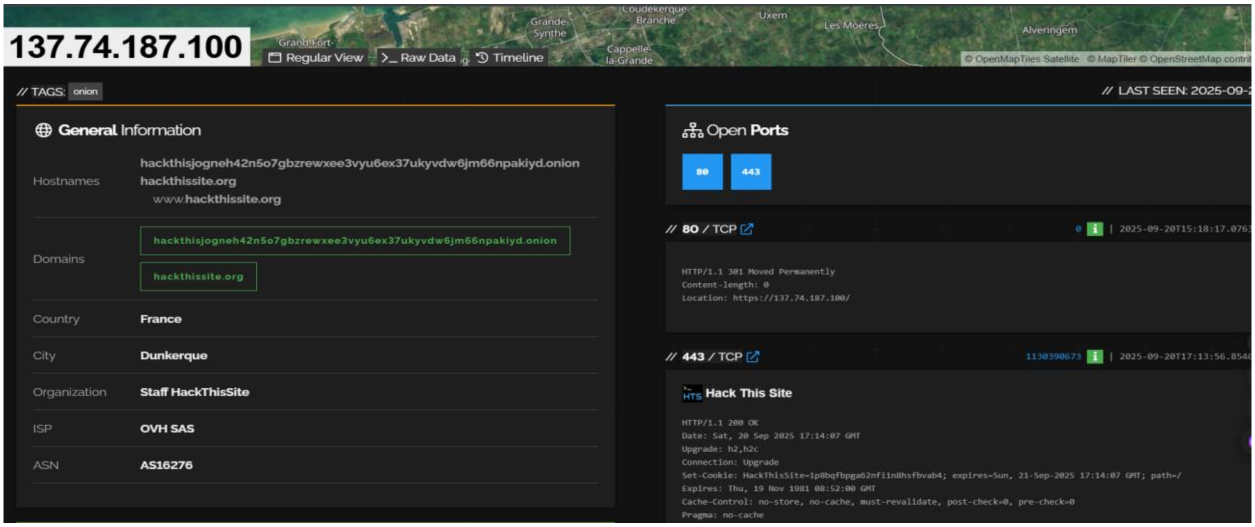
Example commands:
- dig +short hackthissite.org A
- curl -I https://www.hackthissite.org



```
┌──(kali㉿kali)-[~]
└─$ dig +short hackthissite.org A
137.74.187.101
137.74.187.103
137.74.187.104
137.74.187.100
137.74.187.102

┌──(kali㉿kali)-[~]
└─$ curl -I https://www.hackthissite.org
HTTP/2 200
date: Sun, 21 Sep 2025 16:56:40 GMT
set-cookie: HackThisSite=7kfkdcu5rf0edt0e2cvrpuftt4; expires=Mon, 22-Sep-2025 16:56:40 GMT; path=/
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
pragma: no-cache
onion-location: http://hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion/
content-type: text/html
content-language: en
server: HackThisSite
access-control-allow-origin: *
content-security-policy: child-src 'self' hackthissite.org *.hackthissite.org htscdn.org *.htscdn.org discord.com; form-action 'self' hackthissite.org *.hackthissite.org htscdn.org *.htscdn.org; upgrade-insecure-
requests; report-uri https://hackthissite.report-uri.com/r/d/csp/enforce
referrer-policy: origin-when-cross-origin
x-xss-protection: 0
feature-policy: fullscreen *
public-key-pins-report-only: pin-sha256="YLh1dUR9y6Kja30RrAn7JKnbQG/uEtLMkBgFF2Fuihg="; pin-sha256="Vjs8r4z+80wjNcr1YKepWQboSIRi63WsWXhIMN+eWys="; max-age=2592000; includeSubDomains; report-uri="https://hackthiss
ite.report-uri.com/r/d/hpkp/reportOnly"
strict-transport-security: max-age=31536000; includeSubDomains; preload
report-to: {"group":"default","max_age":31536000,"endpoints":[{"url":"https://hackthissite.report-uri.com/a/d/g"}],"include_subdomains":true}
nel: {"report_to":"default","max_age":31536000,"include_subdomains":true,"success_fraction":0.0,"failure_fraction":0.1}
```

-- Censys (API), Shodan (CLI/API)

Shodan --



137.74.187.100

// TAGS: onion

// LAST SEEN: 2025-09-

General Information

Hostnames	hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion hackthissite.org www.hackthissite.org
Domains	hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion hackthissite.org
Country	France
City	Dunkerque
Organization	Staff HackThisSite
ISP	OVH SAS
ASN	AS16276

Open **Ports**

80 443

// 80 / TCP 0 | 2025-09-20T15:18:17.0763

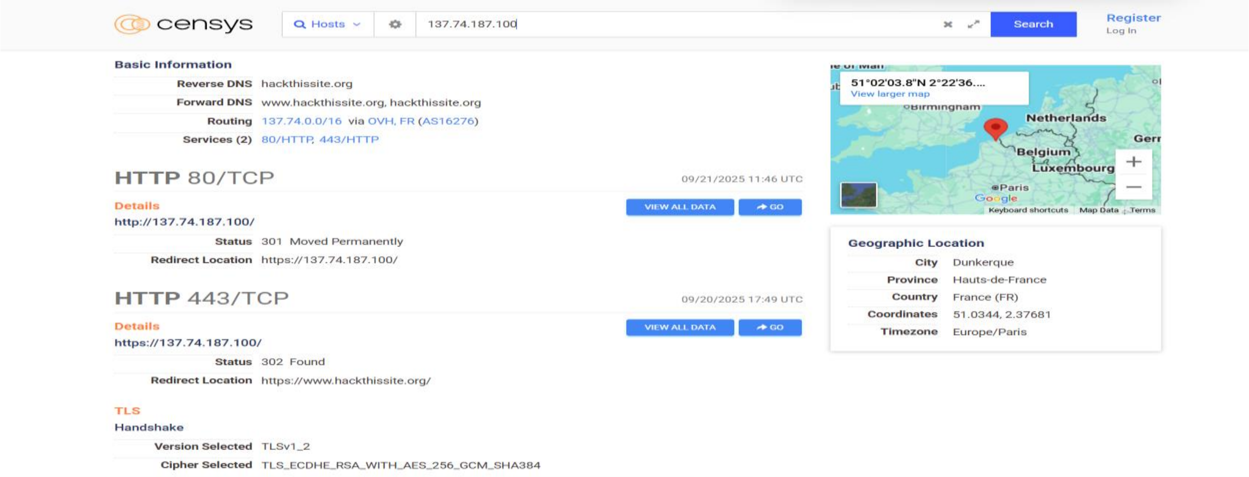
```
HTTP/1.1 301 Moved Permanently
Content-length: 0
Location: https://137.74.187.100/
```

// 443 / TCP 1130390673 | 2025-09-20T17:13:56.854

Hack This Site

```
HTTP/1.1 200 OK
Date: Sat, 20 Sep 2025 17:14:07 GMT
Upgrade: h2,h2c
Connection: Upgrade
Set-Cookie: HackThisSite=1p8bqfbpga62nfi1n8hsfbvab4; expires=Sun, 21-Sep-2025 17:14:07 GMT; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

Censys --



Basic Information

Reverse DNS	hackthissite.org
Forward DNS	www.hackthissite.org, hackthissite.org
Routing	137.74.0.0/16 via OVH, FR (AS16276)
Services (2)	80/HTTP, 443/HTTP

HTTP 80/TCP 09/21/2025 11:46 UTC

Details

http://137.74.187.100/

Status	301 Moved Permanently
Redirect Location	https://137.74.187.100/

HTTP 443/TCP 09/20/2025 17:49 UTC

Details

https://137.74.187.100/

Status	302 Found
Redirect Location	https://www.hackthissite.org/

TLS

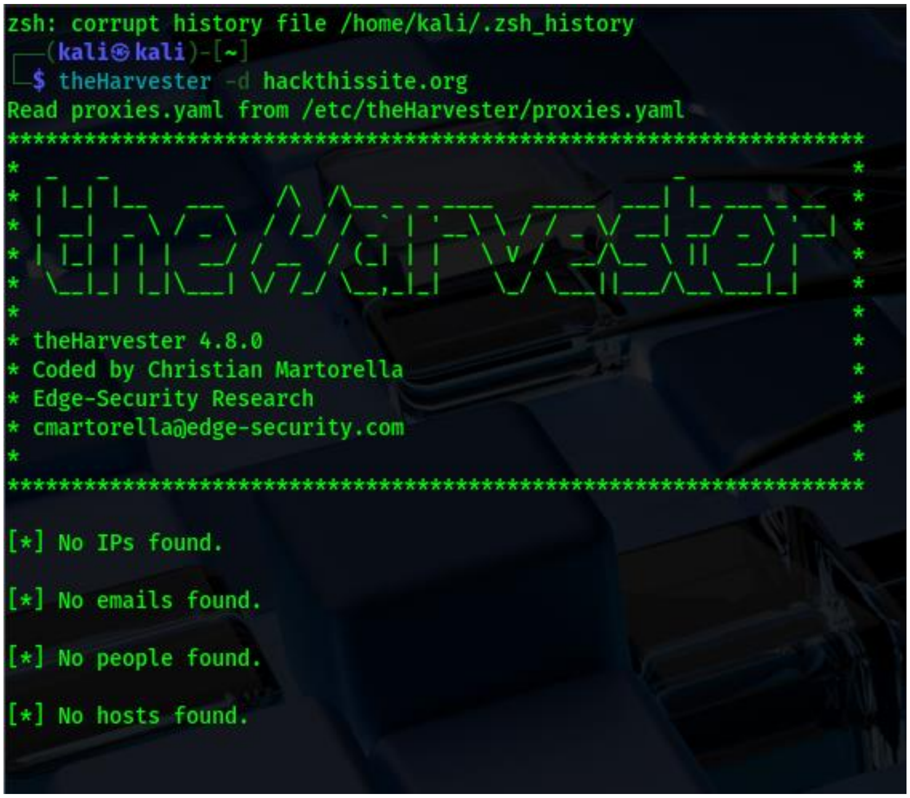
Handshake

Version Selected	TLSv1_2
Cipher Selected	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Geographic Location

City	Dunkerque
Province	Hauts-de-France
Country	France (FR)
Coordinates	51.0344, 2.37681
Timezone	Europe/Paris

5. theHarvester



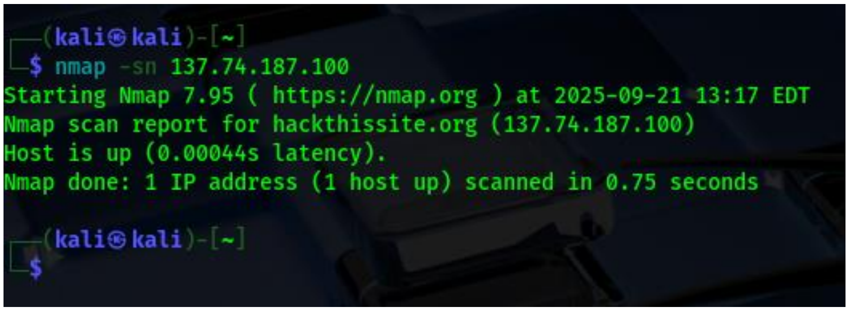
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ theHarvester -d hackthissite.org
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.8.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[*] No IPs found.

[*] No emails found.

[*] No people found.

[*] No hosts found.
```

Nmap Practice -

Run the commands listed below. For each command: include the full command line, a one-line explanation of what the command does, and a screenshot of the output.

Command: nmap -sn 137.74.187.100

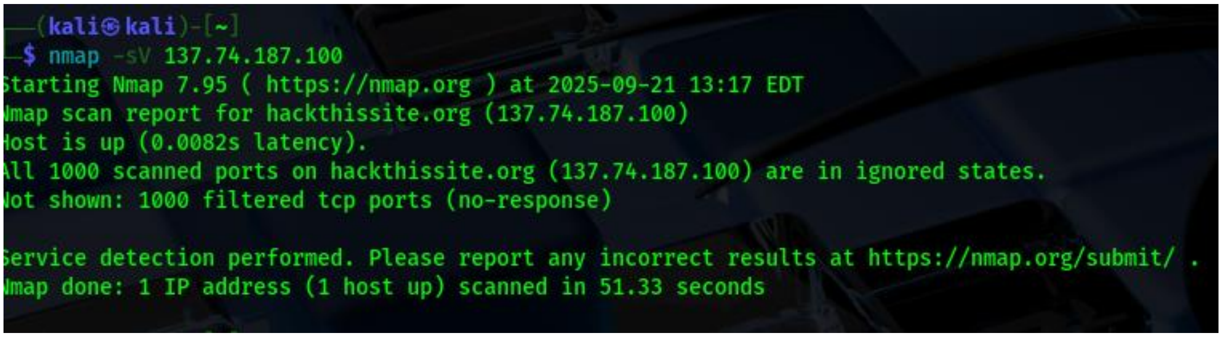
One-line explanation: Host discovery (ping scan) - checks if host is up.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 137.74.187.100
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 13:17 EDT
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.00044s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.75 seconds

┌──(kali㉿kali)-[~]
└─$
```

Command: nmap -sV 137.74.187.100

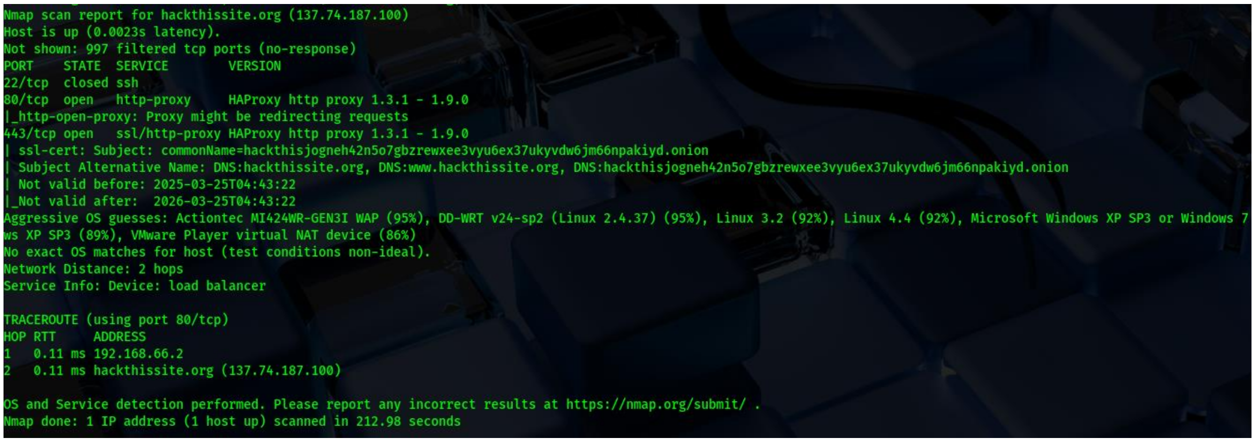
One-line explanation: Top 1000 ports with service detection.



```
──(kali㉿kali)-[~]
─$ nmap -sV 137.74.187.100
tarting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 13:17 EDT
map scan report for hackthissite.org (137.74.187.100)
ost is up (0.0082s latency).
ll 1000 scanned ports on hackthissite.org (137.74.187.100) are in ignored states.
ot shown: 1000 filtered tcp ports (no-response)

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 51.33 seconds
```

Command: sudo nmap -A -T4 137.74.187.100

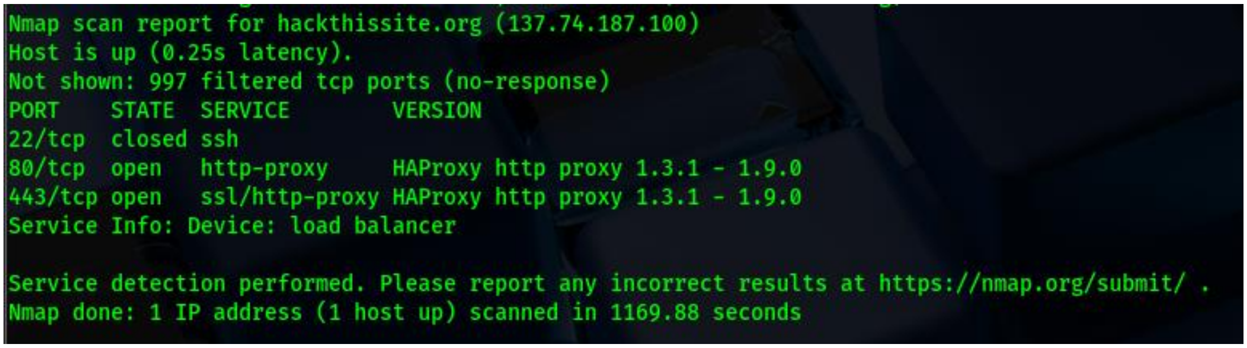
One-line explanation: Aggressive scan: OS, versions, scripts, traceroute.



```
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.0023s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE        VERSION
22/tcp  closed ssh
80/tcp  open   http-proxy     HAProxy http proxy 1.3.1 - 1.9.0
|_http-open-proxy: Proxy might be redirecting requests
443/tcp open   ssl/http-proxy HAProxy http proxy 1.3.1 - 1.9.0
| ssl-cert: Subject: commonName=hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
| Subject Alternative Name: DNS:hackthissite.org, DNS:www.hackthissite.org, DNS:hackthisjogneh42n5o7gbzrewxee3vyu6ex37ukyvdw6jm66npakiyd.onion
| Not valid before: 2025-03-25T04:43:22
|_Not valid after:  2026-03-25T04:43:22
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (95%), DD-WRT v24-sp2 (Linux 2.4.37) (95%), Linux 3.2 (92%), Linux 4.4 (92%), Microsoft Windows XP SP3 or Windows 7
ws XP SP3 (89%), VMware Player virtual NAT device (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Device: load balancer

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.11 ms 192.168.66.2
2   0.11 ms hackthissite.org (137.74.187.100)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 212.98 seconds
```

Command: sudo nmap -sS -sV -Pn -T4 137.74.187.100

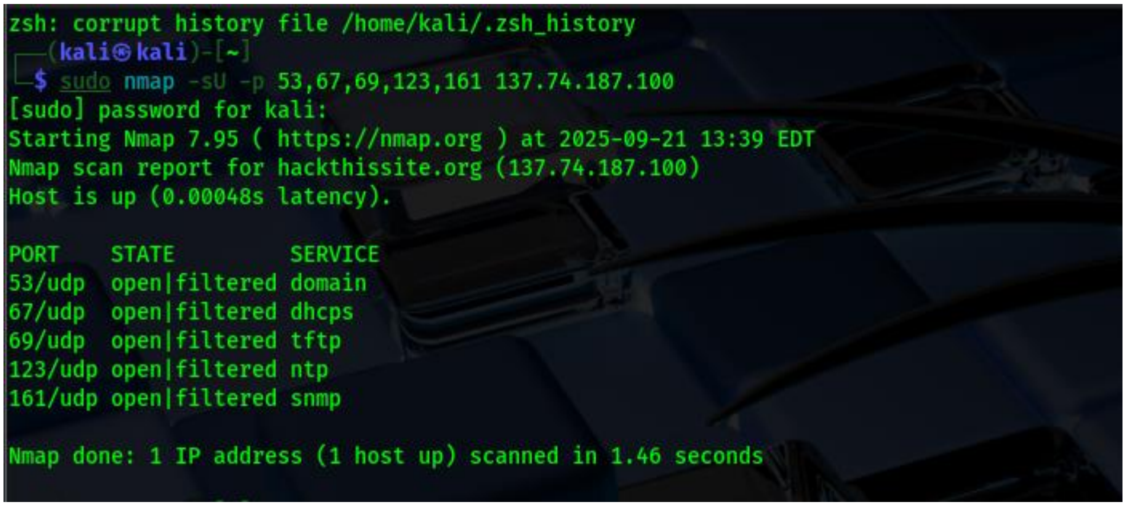
One-line explanation: SYN stealth scan with service detection;



```
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.25s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE        VERSION
22/tcp  closed ssh
80/tcp  open   http-proxy     HAProxy http proxy 1.3.1 - 1.9.0
443/tcp open   ssl/http-proxy HAProxy http proxy 1.3.1 - 1.9.0
Service Info: Device: load balancer

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1169.88 seconds
```

Command: sudo nmap -sU -p 53,67,69,123,161 137.74.187.100

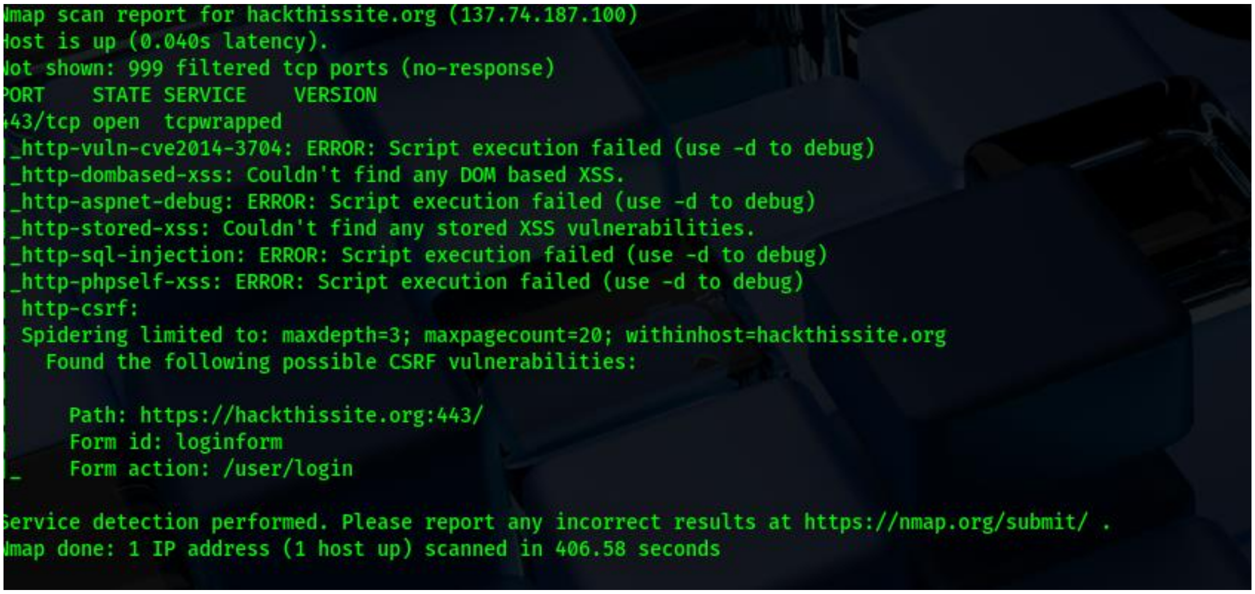
One-line explanation: UDP scan for common UDP services (DNS, DHCP, TFTP, NTP, SNMP).



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU -p 53,67,69,123,161 137.74.187.100
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 13:39 EDT
Nmap scan report for hackthissite.org (137.74.187.100)
Host is up (0.00048s latency).

PORT    STATE         SERVICE
53/udp  open|filtered domain
67/udp  open|filtered dhcps
69/udp  open|filtered tftp
123/udp open|filtered ntp
161/udp open|filtered snmp

Nmap done: 1 IP address (1 host up) scanned in 1.46 seconds
```

Command: sudo nmap --script=vuln -sV 137.74.187.100

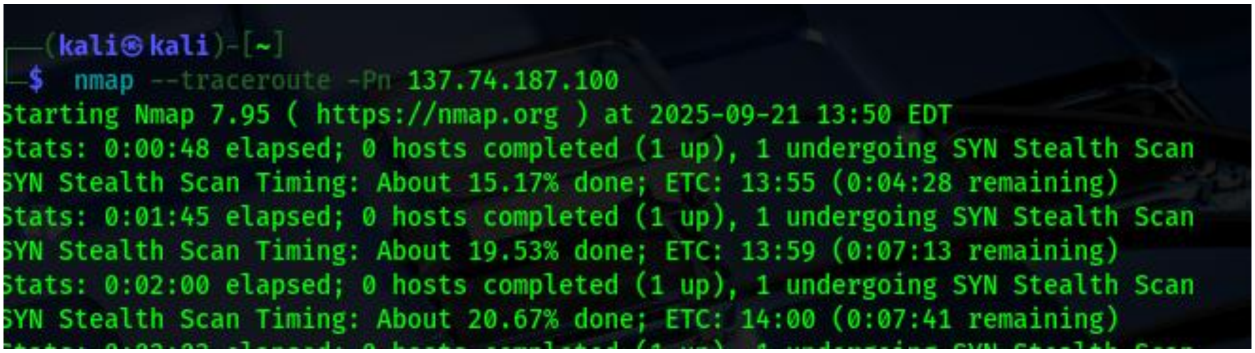
One-line explanation: Run NSE vulnerability scripts against discovered services.



```
map scan report for hackthissite.org (137.74.187.100)
ost is up (0.040s latency).
ot shown: 999 filtered tcp ports (no-response)
ORT    STATE SERVICE    VERSION
43/tcp open  tcpwrapped
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-sql-injection: ERROR: Script execution failed (use -d to debug)
|_http-phpself-xss: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=hackthissite.org
|   Found the following possible CSRF vulnerabilities:
|
|     Path: https://hackthissite.org:443/
|     Form id: loginform
|_    Form action: /user/login

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 406.58 seconds
```

Command: nmap --traceroute -Pn 137.74.187.100

One-line explanation: Show network path (traceroute) to target.



```
──(kali㉿kali)-[~]
─$ nmap --traceroute -Pn 137.74.187.100
tarting Nmap 7.95 ( https://nmap.org ) at 2025-09-21 13:50 EDT
tats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
YN Stealth Scan Timing: About 15.17% done; ETC: 13:55 (0:04:28 remaining)
tats: 0:01:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
YN Stealth Scan Timing: About 19.53% done; ETC: 13:59 (0:07:13 remaining)
tats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
YN Stealth Scan Timing: About 20.67% done; ETC: 14:00 (0:07:41 remaining)
```