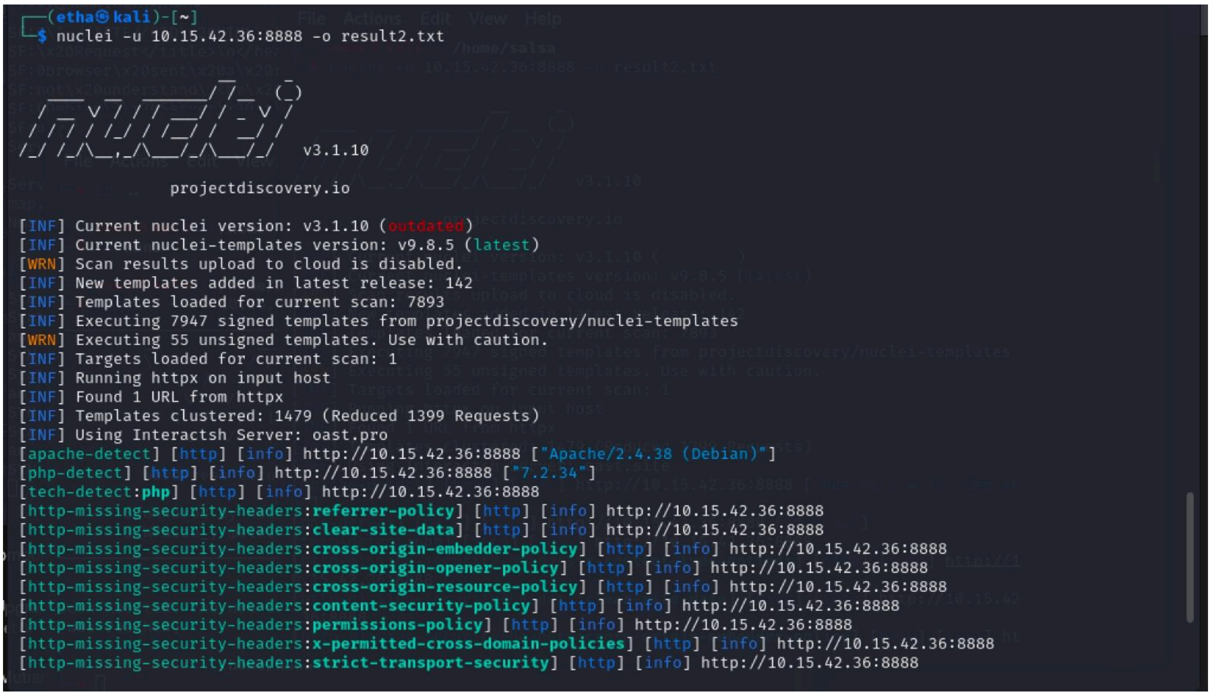
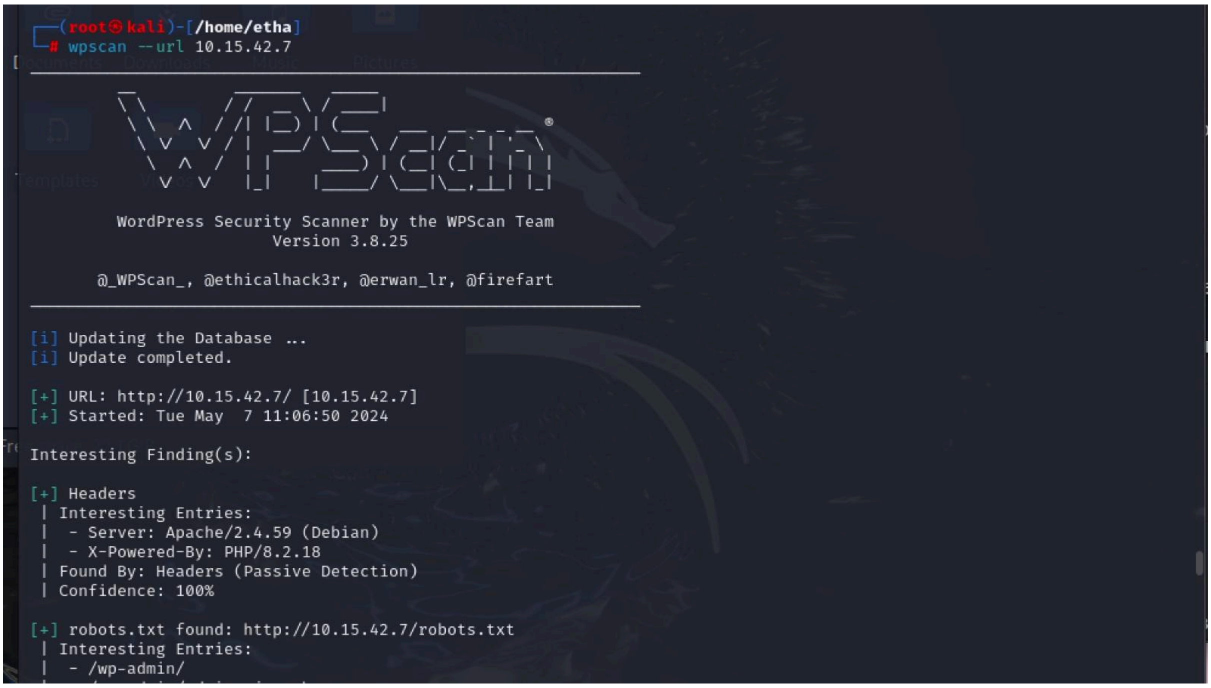
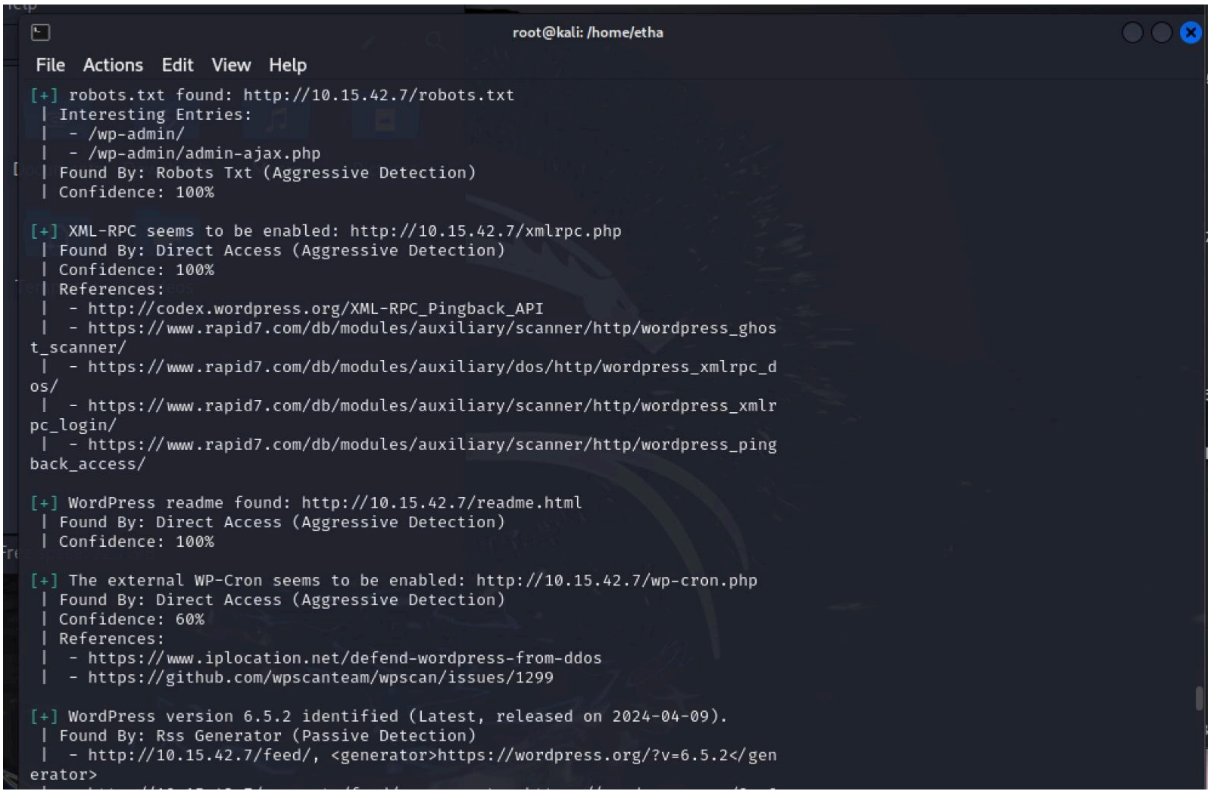


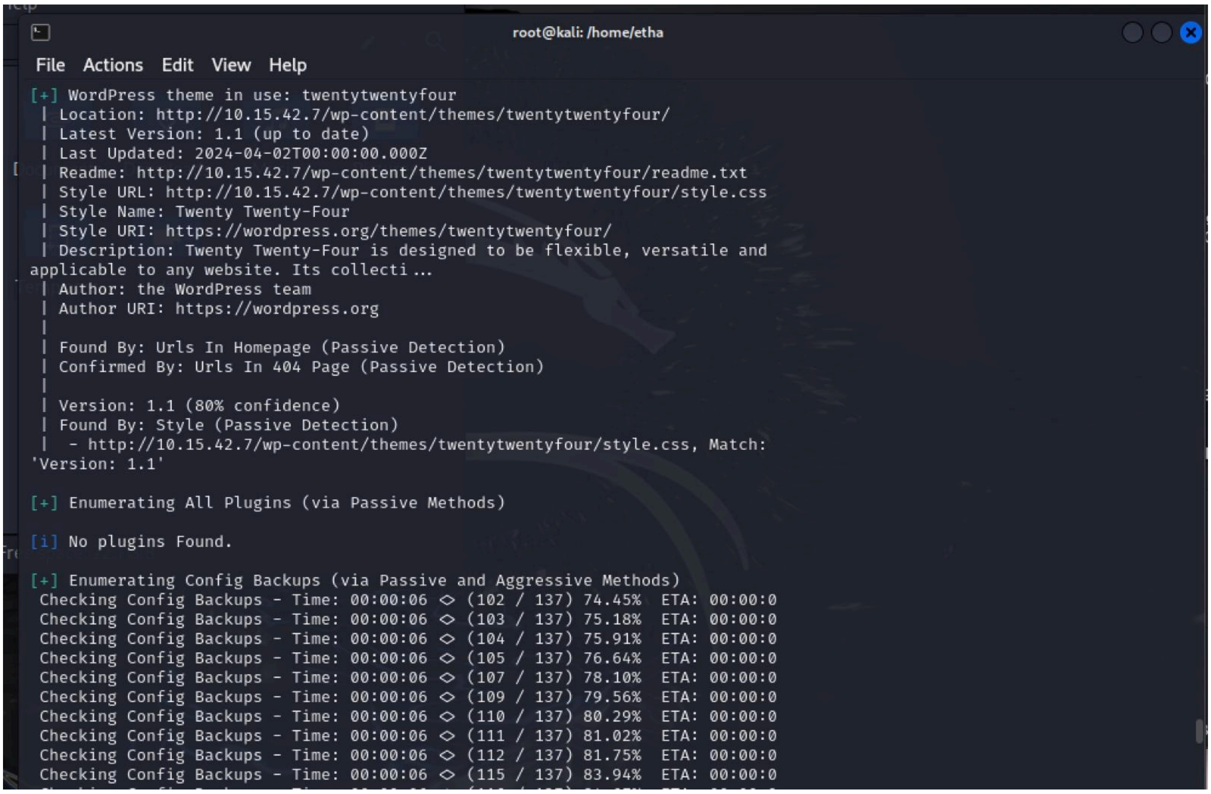
```
┌──(etha㉿kali)-[~]
└─$ nuclei -u 10.15.42.36:8888 -o result2.txt

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.1.10

                projectdiscovery.io

[INF] Current nuclei version: v3.1.10 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
[INF] Executing 7947 signed templates from projectdiscovery/nuclei-templates
[WRN] Executing 55 unsigned templates. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Running httpx on input host
[INF] Found 1 URL from httpx
[INF] Templates clustered: 1479 (Reduced 1399 Requests)
[INF] Using Interactsh Server: oast.pro
[apache-detect] [http] [info] http://10.15.42.36:8888 ["Apache/2.4.38 (Debian)"]
[php-detect] [http] [info] http://10.15.42.36:8888 ["7.2.34"]
[tech-detect:php] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.36:8888
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.36:8888
```



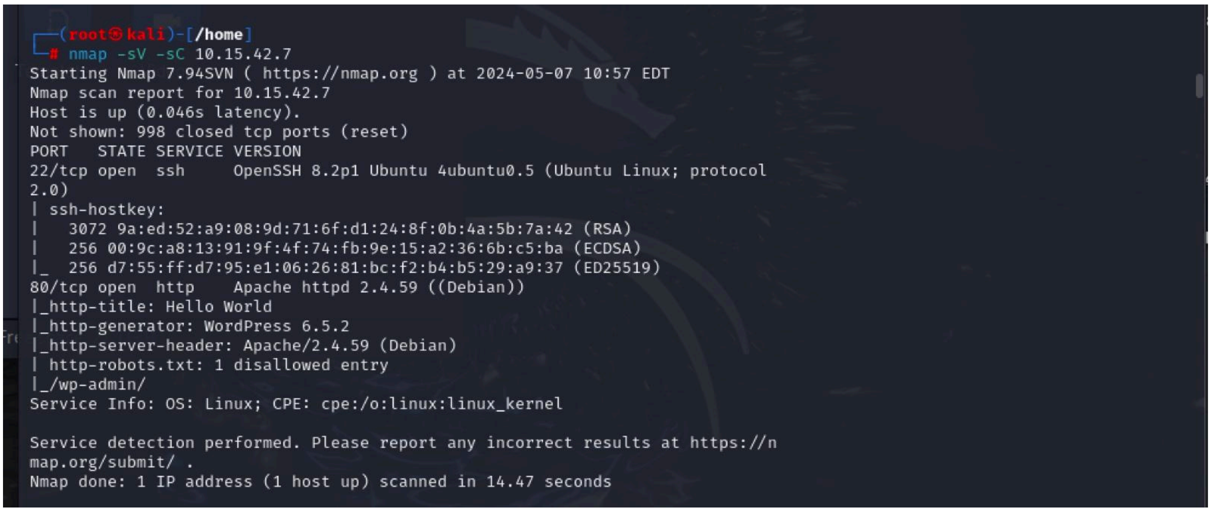
```
┌──(root㉿kali)-[/home/etha]
└─# wpscan --url 10.15.42.7
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25

       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://10.15.42.7/ [10.15.42.7]
[+] Started: Tue May  7 11:06:50 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.59 (Debian)
 |  - X-Powered-By: PHP/8.2.18
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://10.15.42.7/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
```



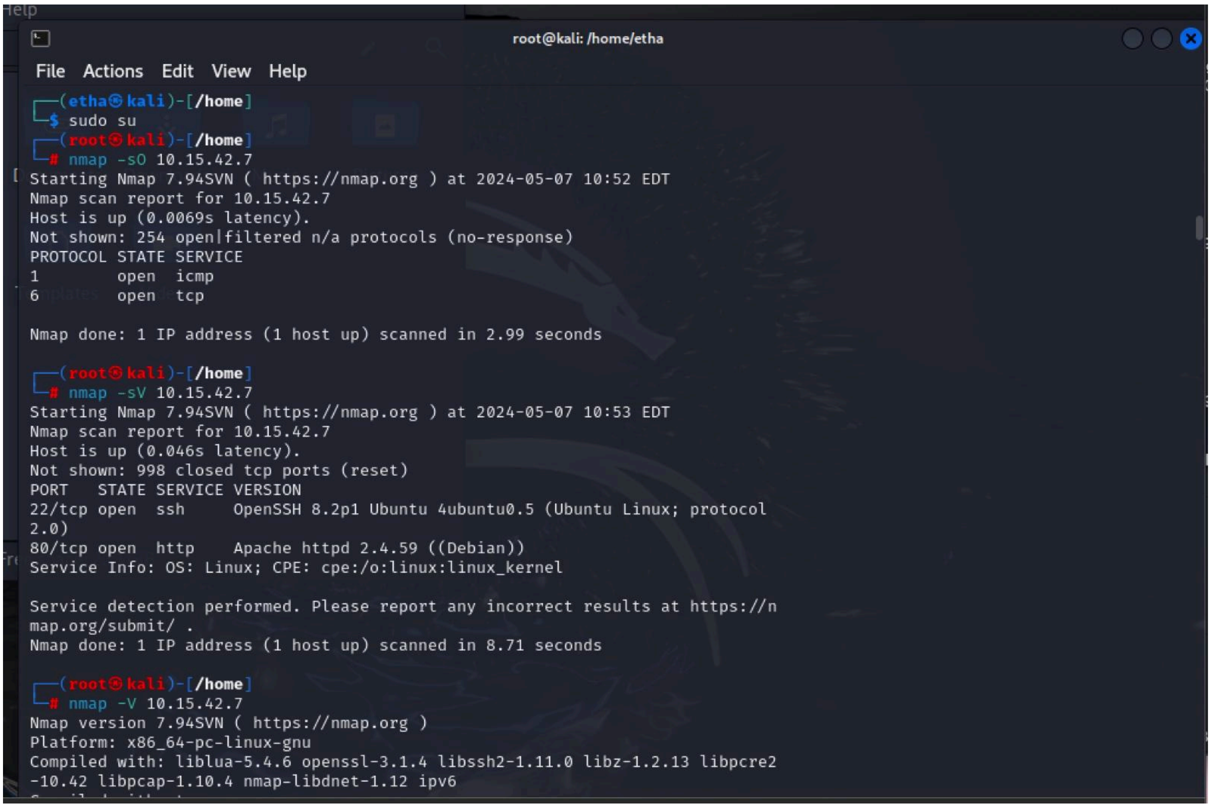
```
[+] robots.txt found: http://10.15.42.7/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.15.42.7/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghos
t_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_d
os/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlr
pc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ping
back_access/

[+] WordPress readme found: http://10.15.42.7/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.15.42.7/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.5.2 identified (Latest, released on 2024-04-09).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.org/?v=6.5.2</gen
erator>
```



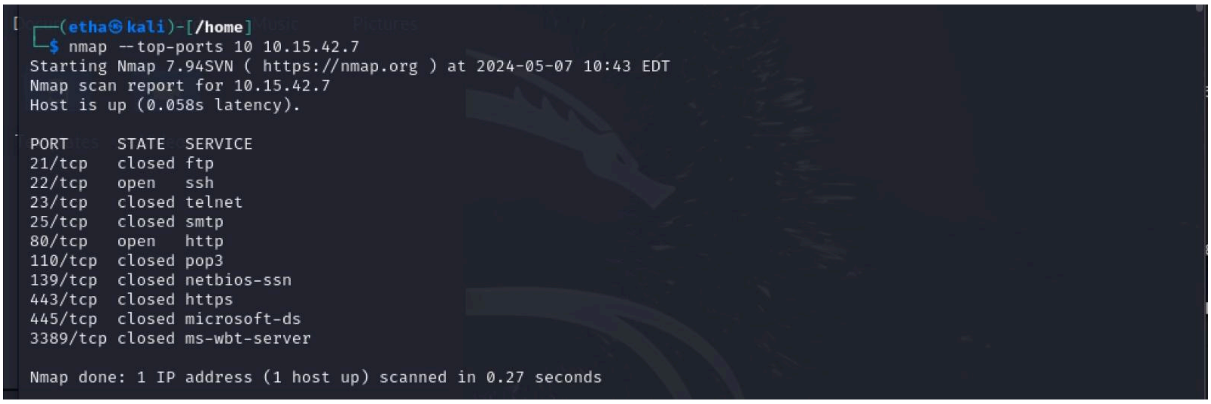
```
[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfour/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and
applicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/style.css, Match:
'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:06 <> (102 / 137) 74.45%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (103 / 137) 75.18%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (104 / 137) 75.91%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (105 / 137) 76.64%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (107 / 137) 78.10%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (109 / 137) 79.56%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (110 / 137) 80.29%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (111 / 137) 81.02%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (112 / 137) 81.75%  ETA: 00:00:0
 Checking Config Backups - Time: 00:00:06 <> (115 / 137) 83.94%  ETA: 00:00:0
```



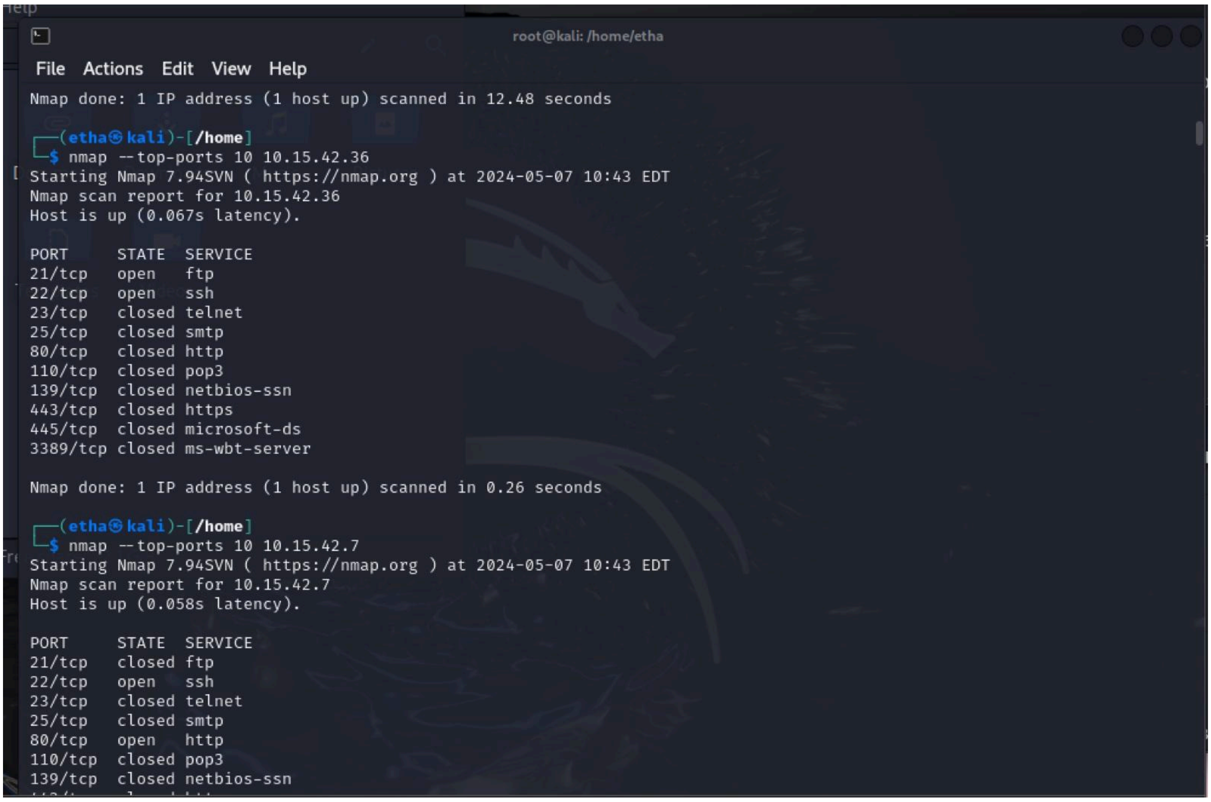
```
┌──(root㉿kali)-[/home]
└─# nmap -sV -sC 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:57 EDT
Nmap scan report for 10.15.42.7
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|   256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_  256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-title: Hello World
|_http-generator: WordPress 6.5.2
|_http-server-header: Apache/2.4.59 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
```



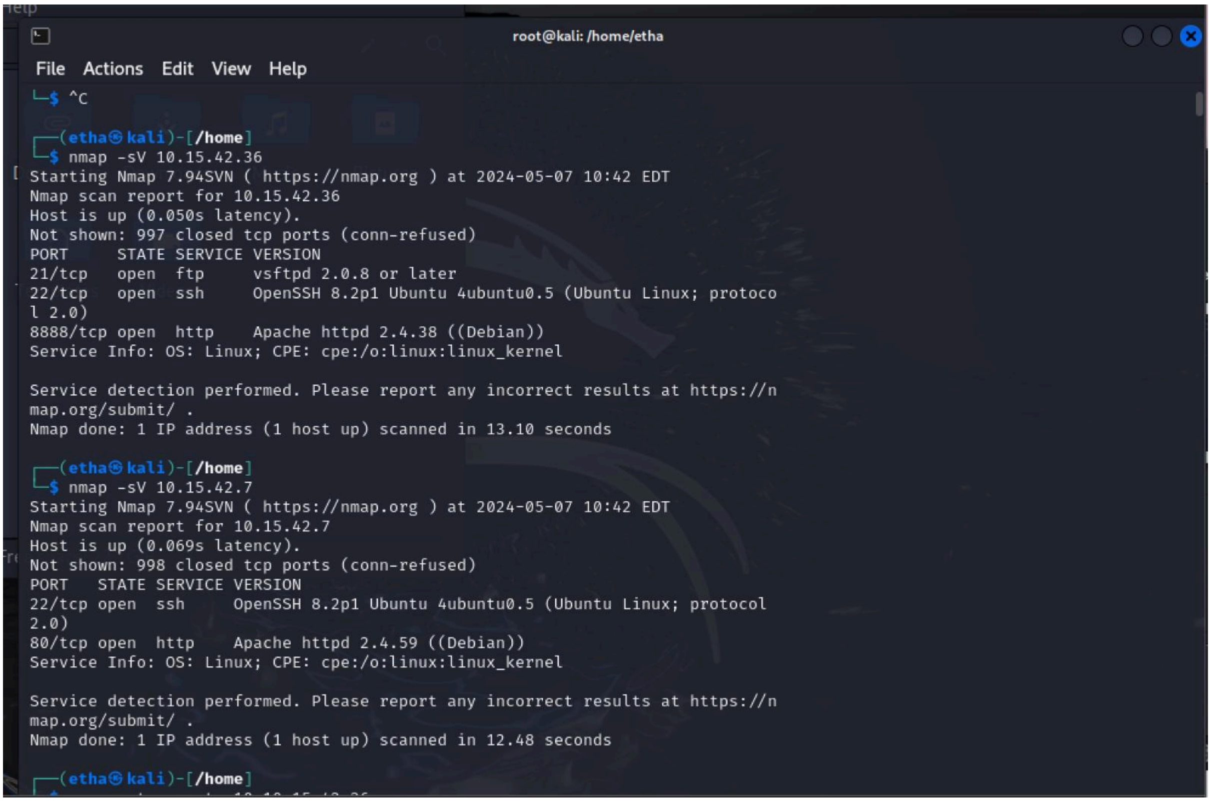
```
┌──(etha㉿kali)-[/home]
└─$ sudo su
┌──(root㉿kali)-[/home]
└─# nmap -sO 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:52 EDT
Nmap scan report for 10.15.42.7
Host is up (0.0069s latency).
Not shown: 254 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp

Nmap done: 1 IP address (1 host up) scanned in 2.99 seconds

┌──(root㉿kali)-[/home]
└─# nmap -sV 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:53 EDT
Nmap scan report for 10.15.42.7
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds

┌──(root㉿kali)-[/home]
└─# nmap -V 10.15.42.7
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.1.4 libssh2-1.11.0 libz-1.2.13 libpcre2
-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
```



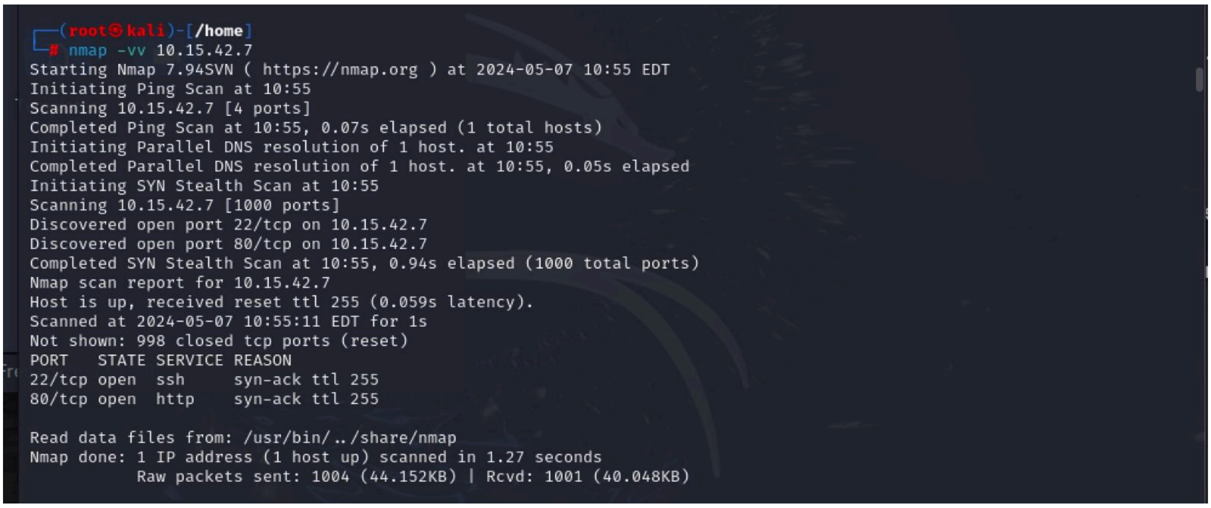
```
┌──(etha㉿kali)-[/home]
└─$ nmap --top-ports 10 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:43 EDT
Nmap scan report for 10.15.42.7
Host is up (0.058s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```



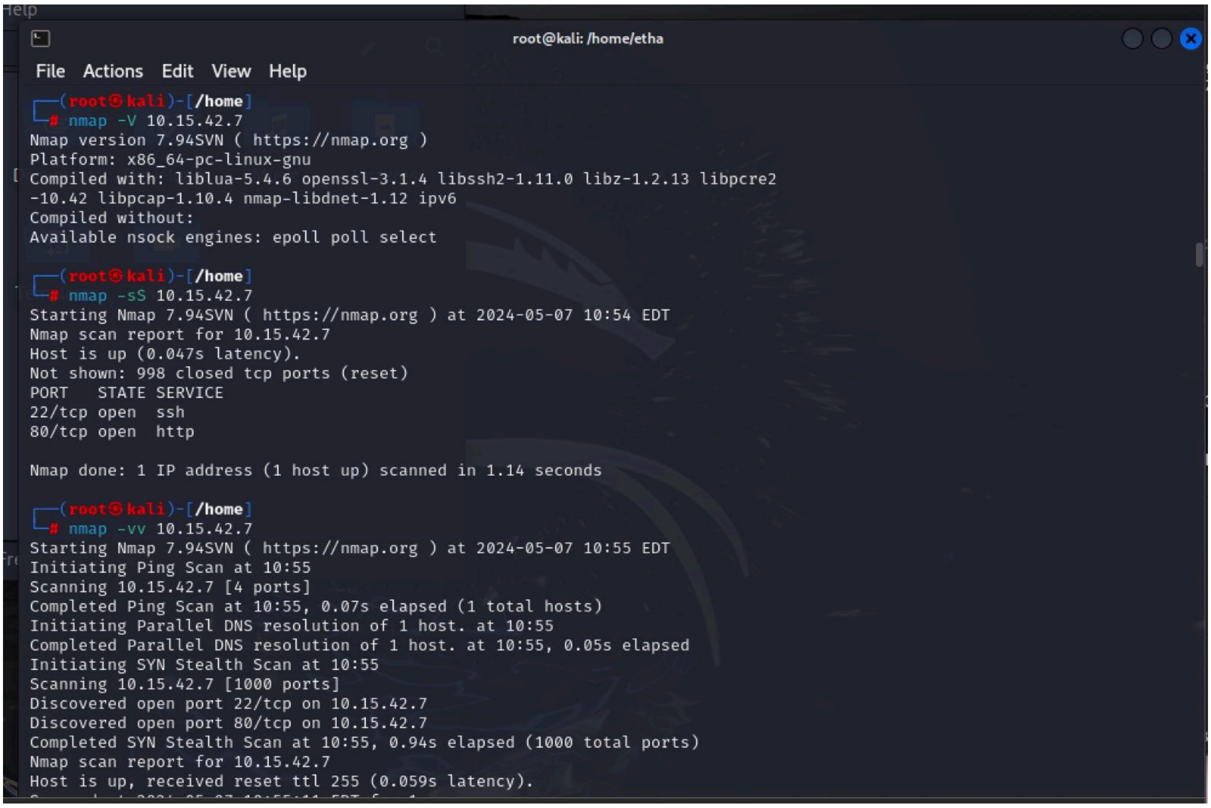
```
Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds

┌──(etha㉿kali)-[/home]
└─$ nmap --top-ports 10 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:43 EDT
Nmap scan report for 10.15.42.36
Host is up (0.067s latency).

PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds

┌──(etha㉿kali)-[/home]
└─$ nmap --top-ports 10 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:43 EDT
Nmap scan report for 10.15.42.7
Host is up (0.058s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
```



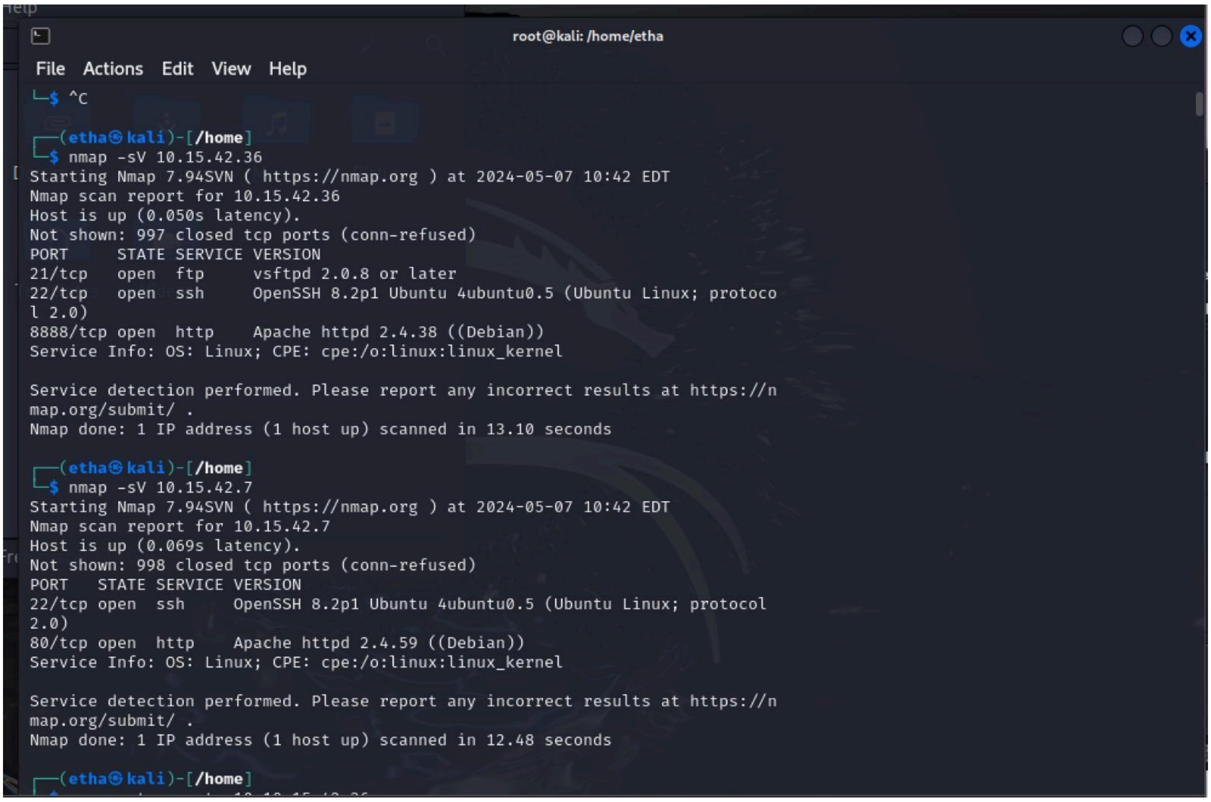
```
└─$ ^C

┌──(etha㉿kali)-[/home]
└─$ nmap -sV 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:42 EDT
Nmap scan report for 10.15.42.36
Host is up (0.050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

┌──(etha㉿kali)-[/home]
└─$ nmap -sV 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:42 EDT
Nmap scan report for 10.15.42.7
Host is up (0.069s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds

┌──(etha㉿kali)-[/home]
```



```
┌──(root㉿kali)-[/home]
└─# nmap -vv 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:55 EDT
Initiating Ping Scan at 10:55
Scanning 10.15.42.7 [4 ports]
Completed Ping Scan at 10:55, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:55
Completed Parallel DNS resolution of 1 host. at 10:55, 0.05s elapsed
Initiating SYN Stealth Scan at 10:55
Scanning 10.15.42.7 [1000 ports]
Discovered open port 22/tcp on 10.15.42.7
Discovered open port 80/tcp on 10.15.42.7
Completed SYN Stealth Scan at 10:55, 0.94s elapsed (1000 total ports)
Nmap scan report for 10.15.42.7
Host is up, received reset ttl 255 (0.059s latency).
Scanned at 2024-05-07 10:55:11 EDT for 1s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 255
80/tcp open  http    syn-ack ttl 255

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
           Raw packets sent: 1004 (44.152KB) | Rcvd: 1001 (40.048KB)
```



```
┌──(root㉿kali)-[/home]
└─# nmap -V 10.15.42.7
Nmap version 7.94SVN ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.1.4 libssh2-1.11.0 libz-1.2.13 libpcre2
-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(root㉿kali)-[/home]
└─# nmap -sS 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:54 EDT
Nmap scan report for 10.15.42.7
Host is up (0.047s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.14 seconds

┌──(root㉿kali)-[/home]
└─# nmap -vv 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:55 EDT
Initiating Ping Scan at 10:55
Scanning 10.15.42.7 [4 ports]
Completed Ping Scan at 10:55, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:55
Completed Parallel DNS resolution of 1 host. at 10:55, 0.05s elapsed
Initiating SYN Stealth Scan at 10:55
Scanning 10.15.42.7 [1000 ports]
Discovered open port 22/tcp on 10.15.42.7
Discovered open port 80/tcp on 10.15.42.7
Completed SYN Stealth Scan at 10:55, 0.94s elapsed (1000 total ports)
Nmap scan report for 10.15.42.7
Host is up, received reset ttl 255 (0.059s latency).
```



```
└─$ ^C

┌──(etha㉿kali)-[/home]
└─$ nmap -sV 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:42 EDT
Nmap scan report for 10.15.42.36
Host is up (0.050s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 2.0.8 or later
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protoco
l 2.0)
8888/tcp open  http    Apache httpd 2.4.38 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.10 seconds

┌──(etha㉿kali)-[/home]
└─$ nmap -sV 10.15.42.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:42 EDT
Nmap scan report for 10.15.42.7
Host is up (0.069s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol
2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.48 seconds

┌──(etha㉿kali)-[/home]
```