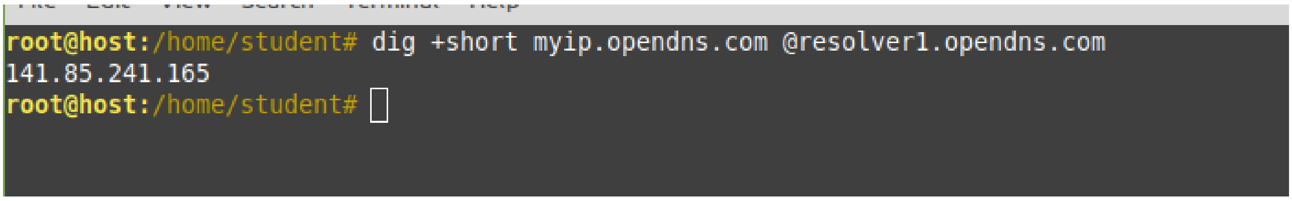
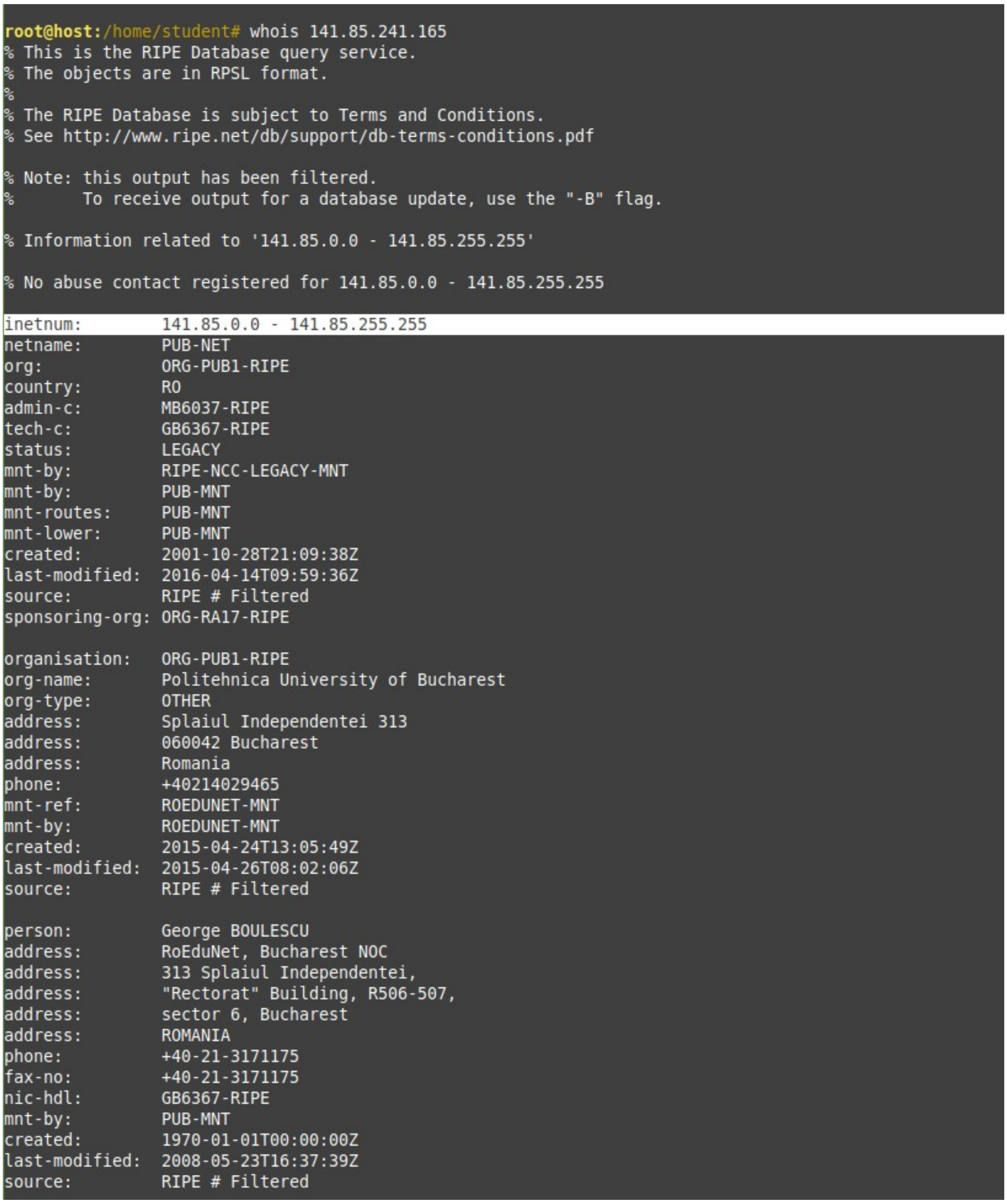
Olaru Gabriel Iulian
334CC
lab 11 RL

Ex1:



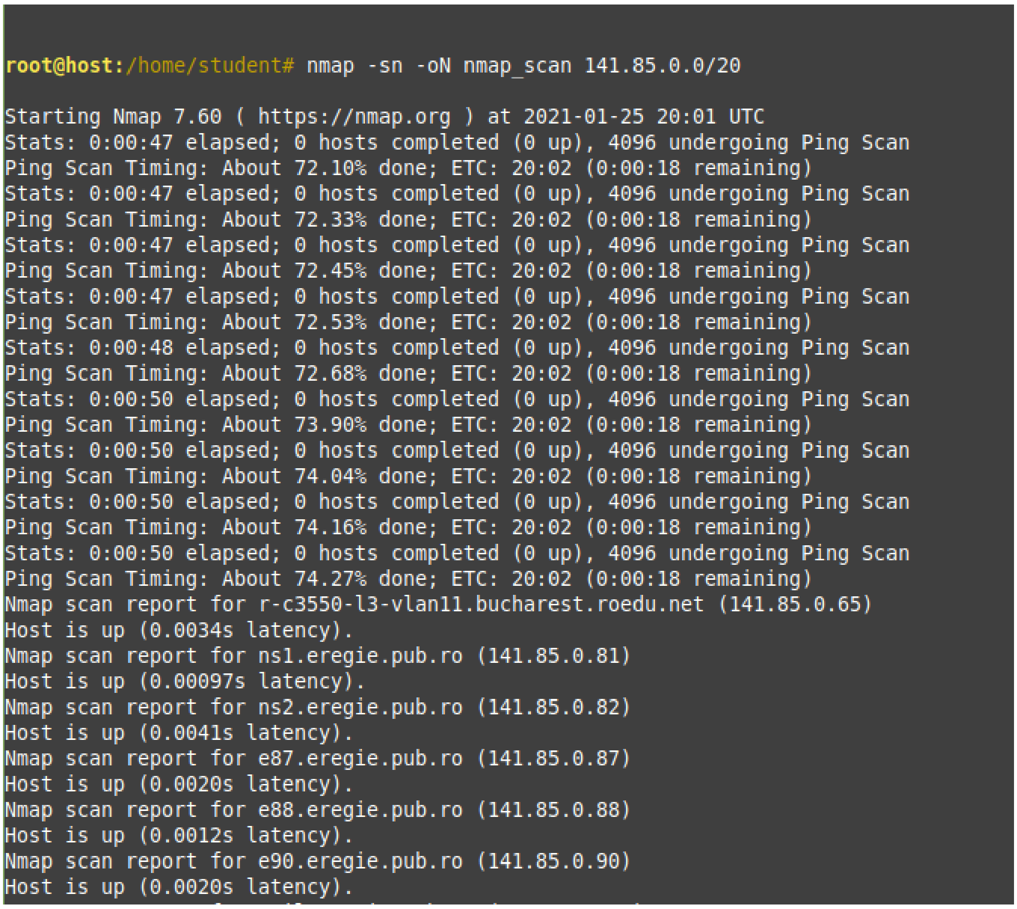
```
root@host:/home/student# dig +short myip.opendns.com @resolver1.opendns.com
141.85.241.165
root@host:/home/student# 
```

Ex2:



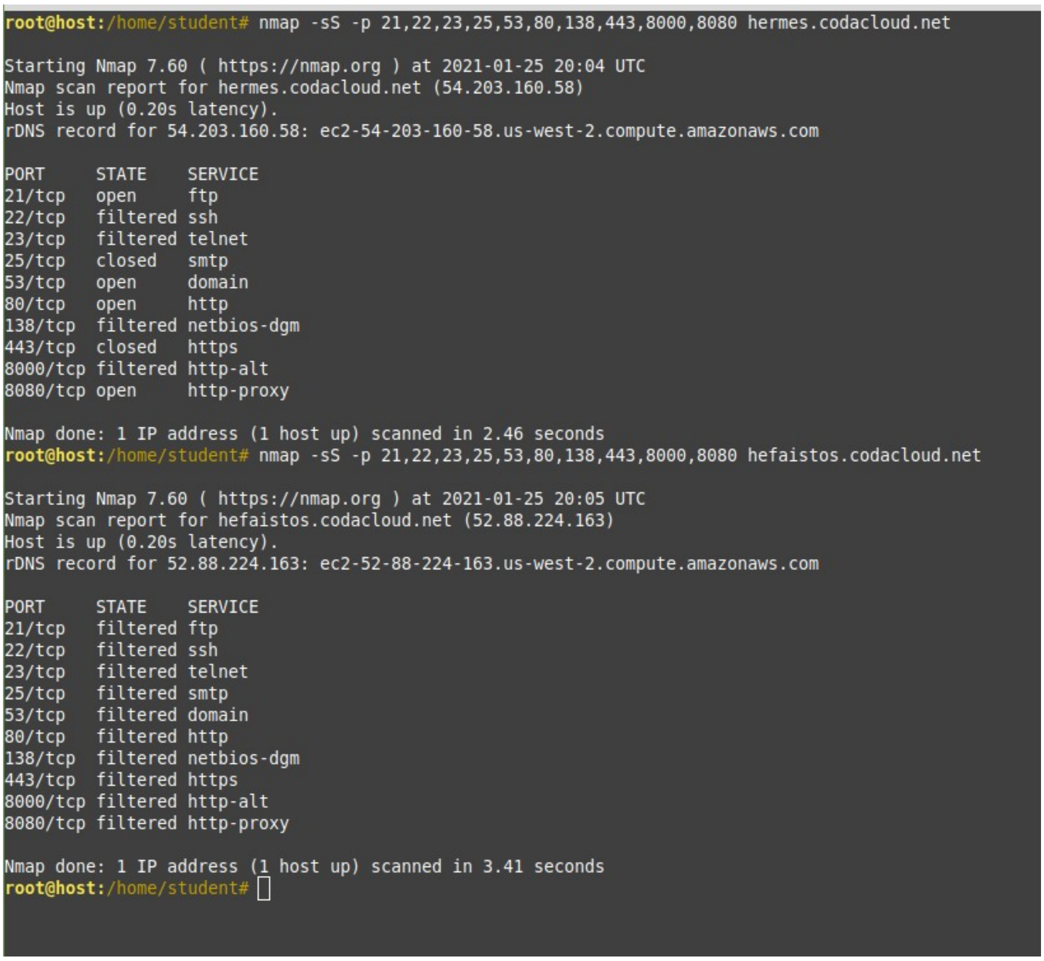
```
root@host:/home/student# whois 141.85.241.165
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '141.85.0.0 - 141.85.255.255'

% No abuse contact registered for 141.85.0.0 - 141.85.255.255

inetnum:        141.85.0.0 - 141.85.255.255
netname:        PUB-NET
org:            ORG-PUB1-RIPE
country:        RO
admin-c:        MB6037-RIPE
tech-c:         GB6367-RIPE
status:         LEGACY
mnt-by:         RIPE-NCC-LEGACY-MNT
mnt-by:         PUB-MNT
mnt-routes:     PUB-MNT
mnt-lower:      PUB-MNT
created:        2001-10-28T21:09:38Z
last-modified:  2016-04-14T09:59:36Z
source:         RIPE # Filtered
sponsoring-org: ORG-RA17-RIPE

organisation:   ORG-PUB1-RIPE
org-name:       Politehnica University of Bucharest
org-type:       OTHER
address:        Splaiul Independentei 313
address:        060042 Bucharest
address:        Romania
phone:          +40214029465
mnt-ref:        ROEDUNET-MNT
mnt-by:         ROEDUNET-MNT
created:        2015-04-24T13:05:49Z
last-modified:  2015-04-26T08:02:06Z
source:         RIPE # Filtered

person:         George BOULESCU
address:        RoEduNet, Bucharest NOC
address:        313 Splaiul Independentei,
address:        "Rectorat" Building, R506-507,
address:        sector 6, Bucharest
address:        ROMANIA
phone:          +40-21-3171175
fax-no:         +40-21-3171175
nic-hdl:        GB6367-RIPE
mnt-by:         PUB-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2008-05-23T16:37:39Z
source:         RIPE # Filtered
```

Ex3:



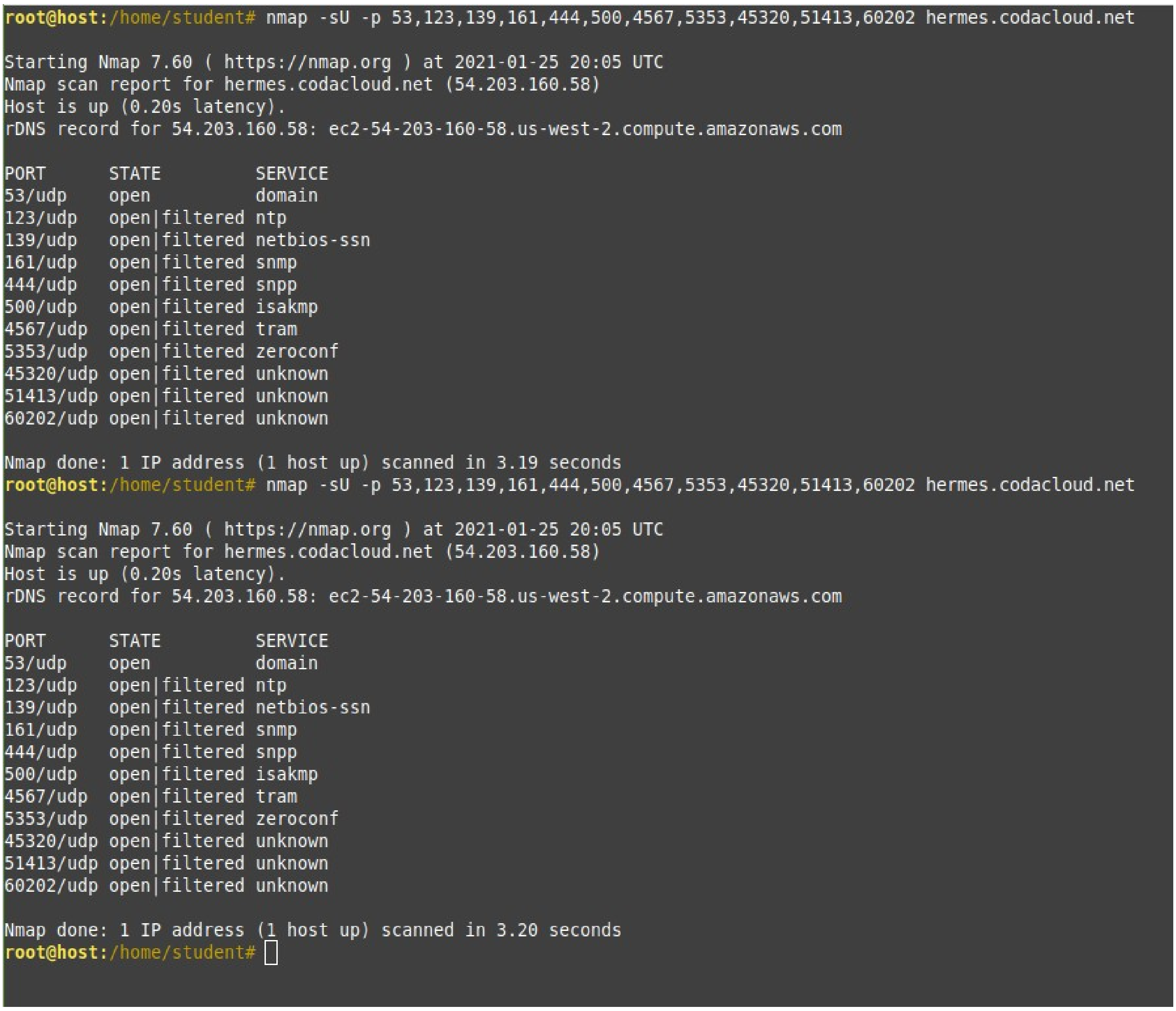
```
root@host:/home/student# nmap -sn -oN nmap_scan 141.85.0.0/20

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:01 UTC
Stats: 0:00:47 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 72.10% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 72.33% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 72.45% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 72.53% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 72.68% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 73.90% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 74.04% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 74.16% done; ETC: 20:02 (0:00:18 remaining)
Stats: 0:00:50 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 74.27% done; ETC: 20:02 (0:00:18 remaining)
Nmap scan report for r-c3550-l3-vlan11.bucharest.roedu.net (141.85.0.65)
Host is up (0.0034s latency).
Nmap scan report for ns1.eregie.pub.ro (141.85.0.81)
Host is up (0.00097s latency).
Nmap scan report for ns2.eregie.pub.ro (141.85.0.82)
Host is up (0.0041s latency).
Nmap scan report for e87.eregie.pub.ro (141.85.0.87)
Host is up (0.0020s latency).
Nmap scan report for e88.eregie.pub.ro (141.85.0.88)
Host is up (0.0012s latency).
Nmap scan report for e90.eregie.pub.ro (141.85.0.90)
Host is up (0.0020s latency).
```

Ex4:



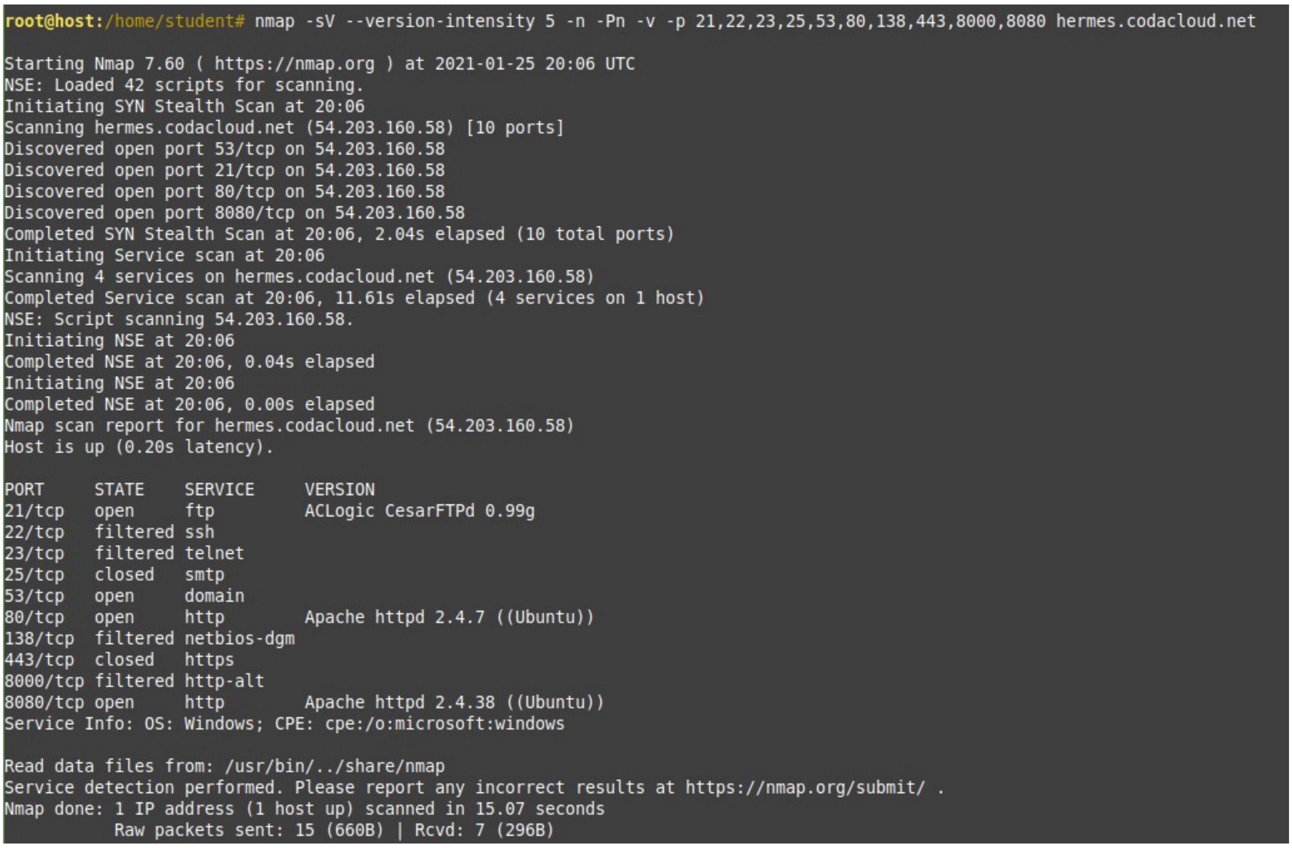
```
root@host:/home/student# nmap -sS -p 21,22,23,25,53,80,138,443,8000,8080 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:04 UTC
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).
rDNS record for 54.203.160.58: ec2-54-203-160-58.us-west-2.compute.amazonaws.com

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   closed   smtp
53/tcp   open     domain
80/tcp   open     http
138/tcp  filtered netbios-dgm
443/tcp  closed   https
8000/tcp filtered http-alt
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.46 seconds
root@host:/home/student# nmap -sS -p 21,22,23,25,53,80,138,443,8000,8080 hefaistos.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:05 UTC
Nmap scan report for hefaistos.codacloud.net (52.88.224.163)
Host is up (0.20s latency).
rDNS record for 52.88.224.163: ec2-52-88-224-163.us-west-2.compute.amazonaws.com

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
138/tcp  filtered netbios-dgm
443/tcp  filtered https
8000/tcp filtered http-alt
8080/tcp filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 3.41 seconds
root@host:/home/student# 
```

Ex5:

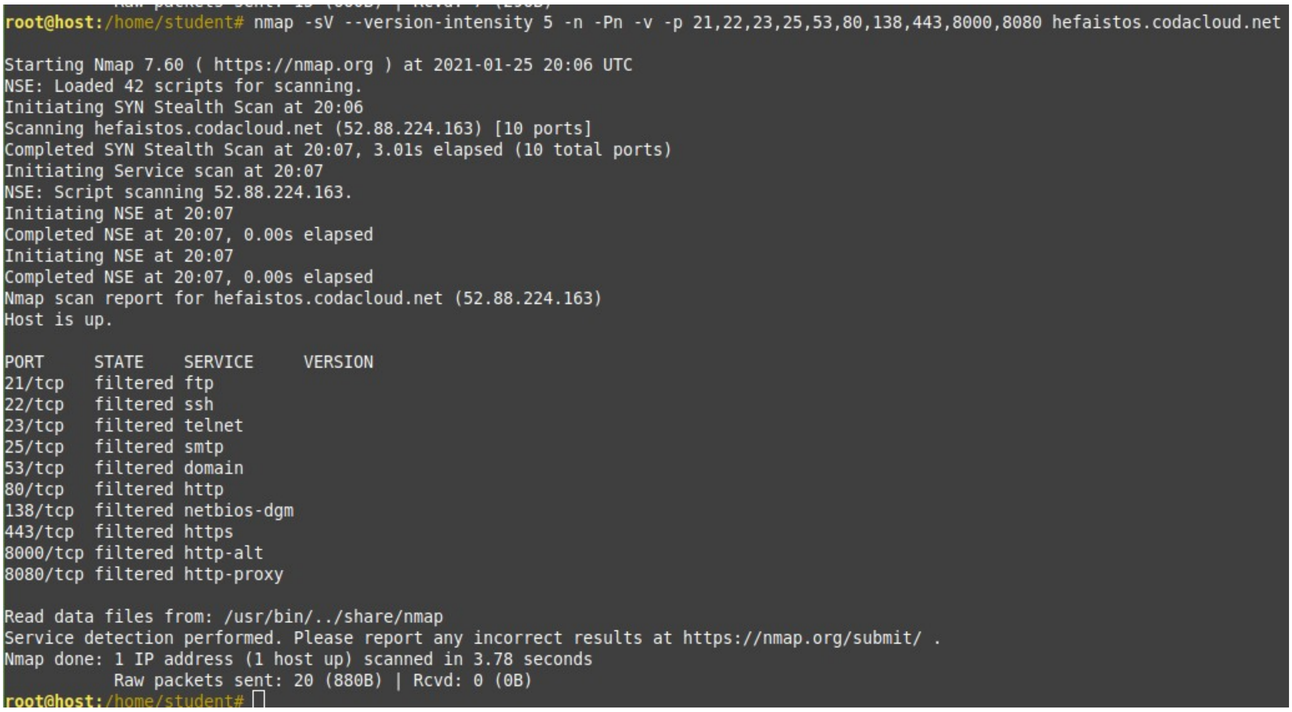


```
root@host:/home/student# nmap -sU -p 53,123,139,161,444,500,4567,5353,45320,51413,60202 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:05 UTC
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).
rDNS record for 54.203.160.58: ec2-54-203-160-58.us-west-2.compute.amazonaws.com

PORT      STATE         SERVICE
53/udp    open          domain
123/udp   open|filtered ntp
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
444/udp   open|filtered snpp
500/udp   open|filtered isakmp
4567/udp  open|filtered tram
5353/udp  open|filtered zeroconf
45320/udp open|filtered unknown
51413/udp open|filtered unknown
60202/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.19 seconds
root@host:/home/student# nmap -sU -p 53,123,139,161,444,500,4567,5353,45320,51413,60202 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:05 UTC
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).
rDNS record for 54.203.160.58: ec2-54-203-160-58.us-west-2.compute.amazonaws.com

PORT      STATE         SERVICE
53/udp    open          domain
123/udp   open|filtered ntp
139/udp   open|filtered netbios-ssn
161/udp   open|filtered snmp
444/udp   open|filtered snpp
500/udp   open|filtered isakmp
4567/udp  open|filtered tram
5353/udp  open|filtered zeroconf
45320/udp open|filtered unknown
51413/udp open|filtered unknown
60202/udp open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds
root@host:/home/student# 
```

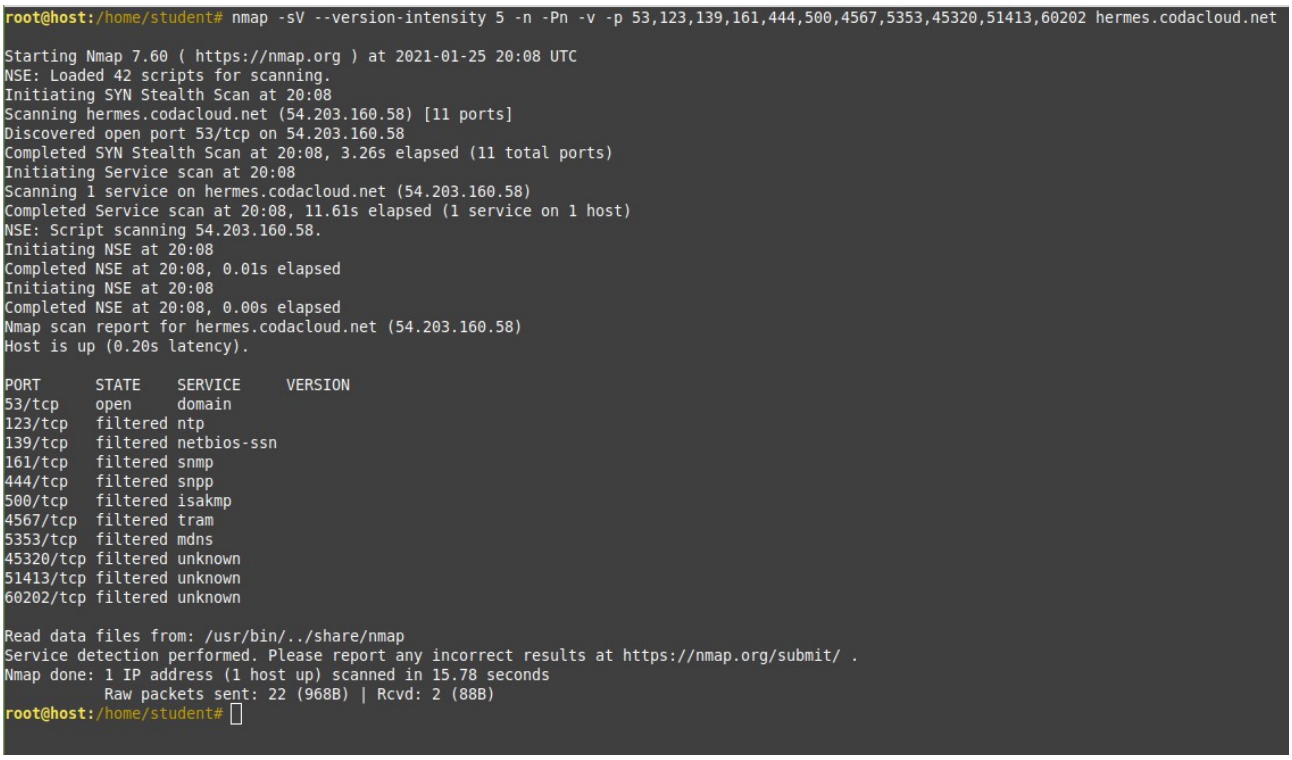
Ex6:



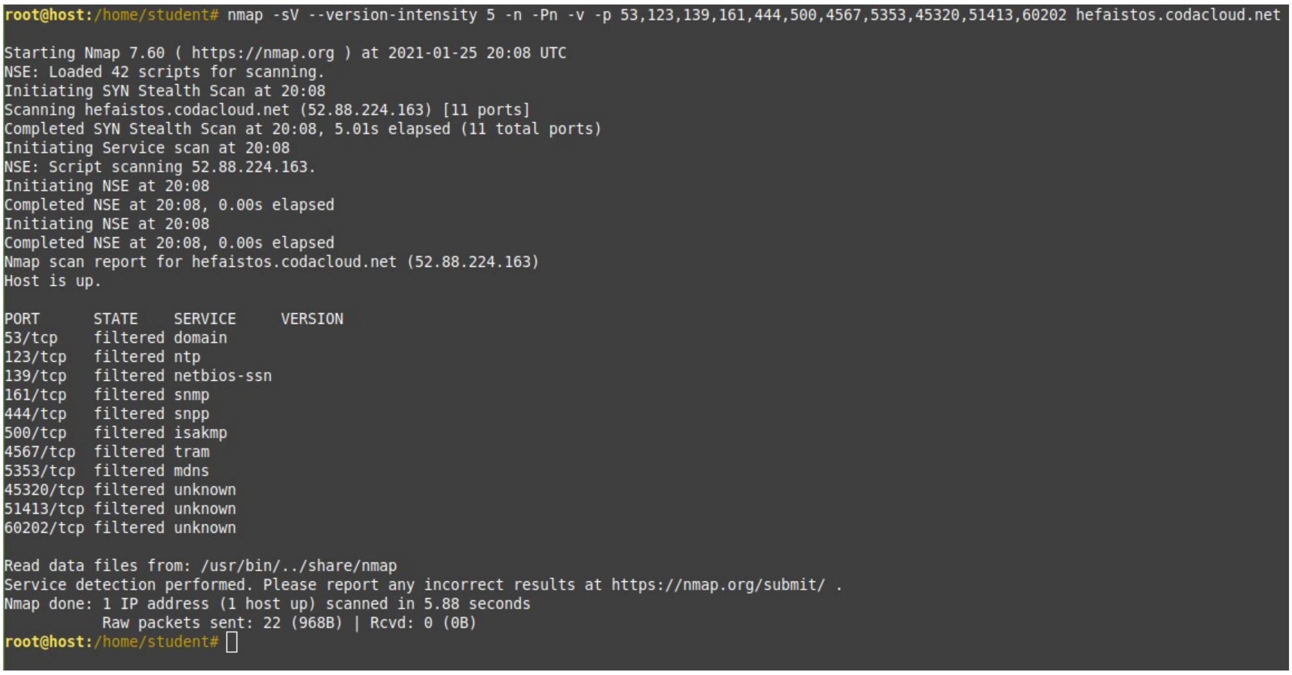
```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v -p 21,22,23,25,53,80,138,443,8000,8080 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:06 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:06
Scanning hermes.codacloud.net (54.203.160.58) [10 ports]
Discovered open port 53/tcp on 54.203.160.58
Discovered open port 21/tcp on 54.203.160.58
Discovered open port 80/tcp on 54.203.160.58
Discovered open port 8080/tcp on 54.203.160.58
Completed SYN Stealth Scan at 20:06, 2.04s elapsed (10 total ports)
Initiating Service scan at 20:06
Scanning 4 services on hermes.codacloud.net (54.203.160.58)
Completed Service scan at 20:06, 11.61s elapsed (4 services on 1 host)
NSE: Script scanning 54.203.160.58.
Initiating NSE at 20:06
Completed NSE at 20:06, 0.04s elapsed
Initiating NSE at 20:06
Completed NSE at 20:06, 0.00s elapsed
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).

PORT     STATE    SERVICE     VERSION
21/tcp   open     ftp         ACLogic CesarFTPd 0.99g
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   closed   smtp
53/tcp   open     domain
80/tcp   open     http        Apache httpd 2.4.7 ((Ubuntu))
138/tcp  filtered netbios-dgm
443/tcp  closed   https
8000/tcp filtered http-alt
8080/tcp open     http        Apache httpd 2.4.38 ((Ubuntu))
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.07 seconds
           Raw packets sent: 15 (660B) | Rcvd: 7 (296B)
```



```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v -p 21,22,23,25,53,80,138,443,8000,8080 hefaistos.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:06 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:06
Scanning hefaistos.codacloud.net (52.88.224.163) [10 ports]
Completed SYN Stealth Scan at 20:07, 3.01s elapsed (10 total ports)
Initiating Service scan at 20:07
NSE: Script scanning 52.88.224.163.
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
Initiating NSE at 20:07
Completed NSE at 20:07, 0.00s elapsed
Nmap scan report for hefaistos.codacloud.net (52.88.224.163)
Host is up.

PORT     STATE    SERVICE     VERSION
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered domain
80/tcp   filtered http
138/tcp  filtered netbios-dgm
443/tcp  filtered https
8000/tcp filtered http-alt
8080/tcp filtered http-proxy

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.78 seconds
           Raw packets sent: 20 (880B) | Rcvd: 0 (0B)
root@host:/home/student# 
```

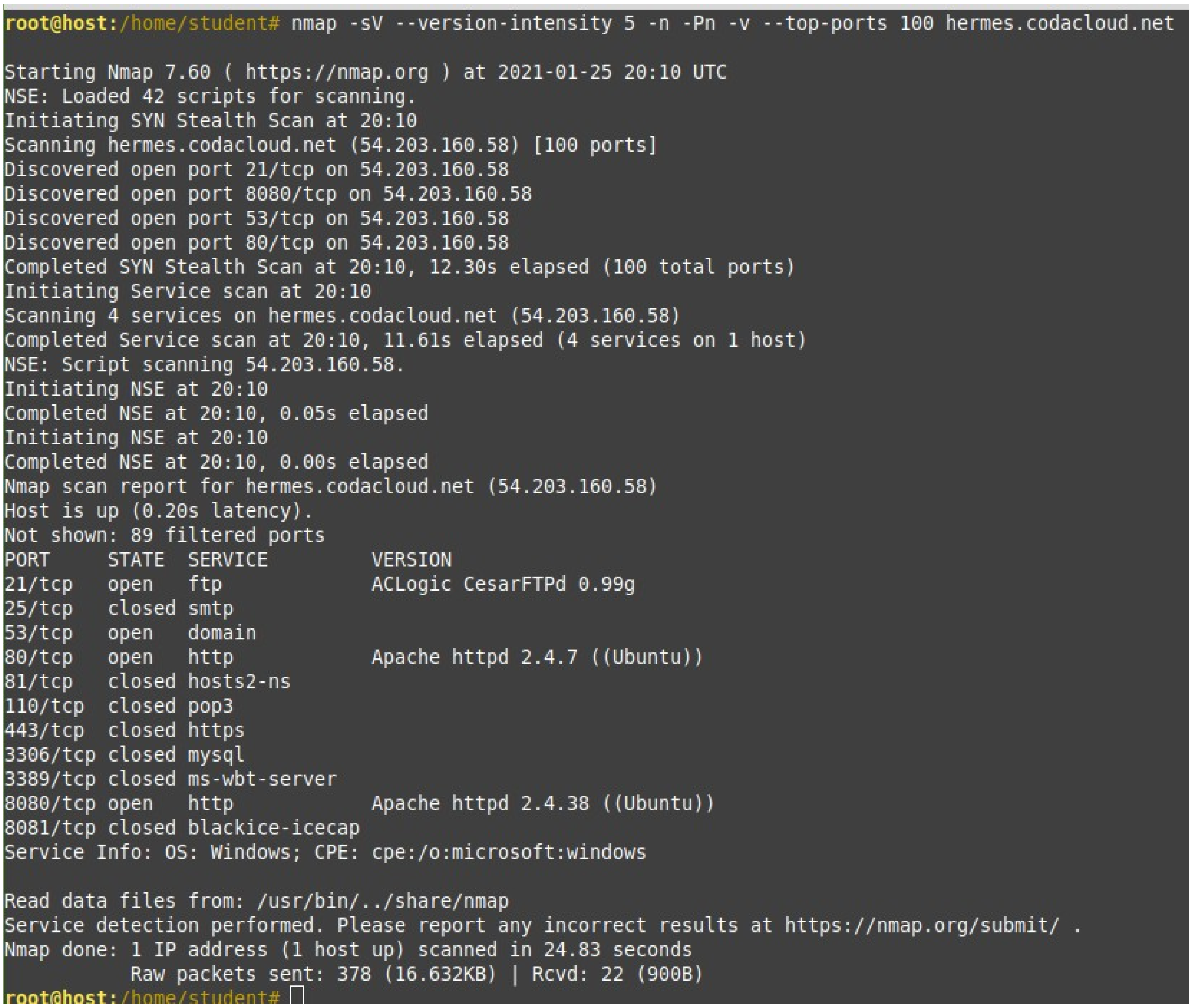


```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v -p 53,123,139,161,444,500,4567,5353,45320,51413,60202 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:08 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:08
Scanning hermes.codacloud.net (54.203.160.58) [11 ports]
Discovered open port 53/tcp on 54.203.160.58
Completed SYN Stealth Scan at 20:08, 3.26s elapsed (11 total ports)
Initiating Service scan at 20:08
Scanning 1 service on hermes.codacloud.net (54.203.160.58)
Completed Service scan at 20:08, 11.61s elapsed (1 service on 1 host)
NSE: Script scanning 54.203.160.58.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.01s elapsed
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).

PORT      STATE    SERVICE     VERSION
53/tcp    open     domain
123/tcp   filtered ntp
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
444/tcp   filtered snpp
500/tcp   filtered isakmp
4567/tcp  filtered tram
5353/tcp  filtered mdns
45320/tcp filtered unknown
51413/tcp filtered unknown
60202/tcp filtered unknown

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.78 seconds
           Raw packets sent: 22 (968B) | Rcvd: 2 (88B)
root@host:/home/student# 
```



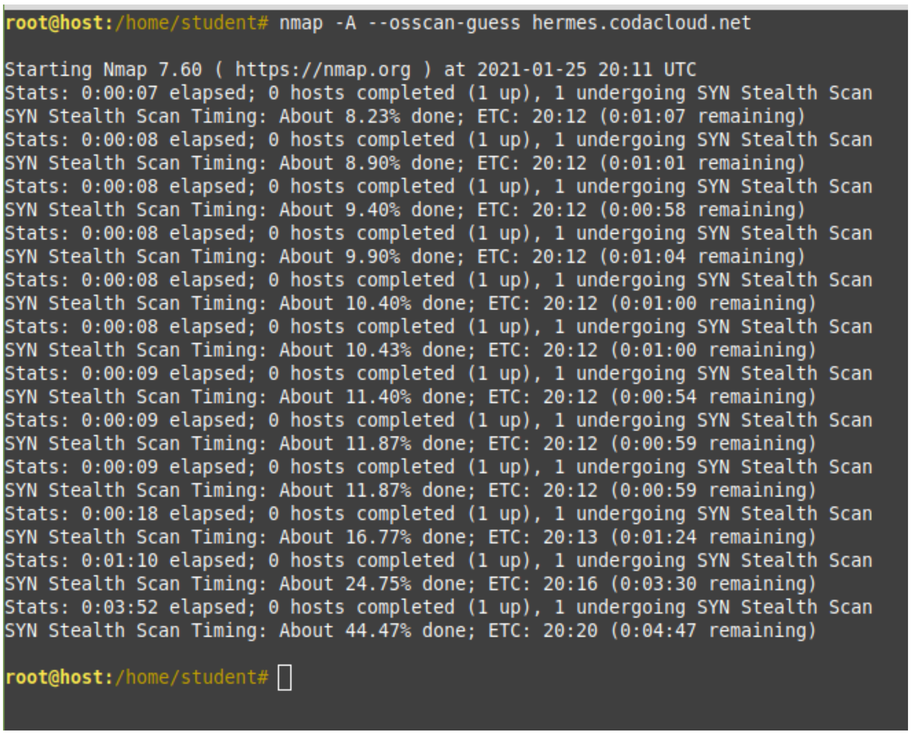
```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v -p 53,123,139,161,444,500,4567,5353,45320,51413,60202 hefaistos.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:08 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:08
Scanning hefaistos.codacloud.net (52.88.224.163) [11 ports]
Completed SYN Stealth Scan at 20:08, 5.01s elapsed (11 total ports)
Initiating Service scan at 20:08
NSE: Script scanning 52.88.224.163.
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Initiating NSE at 20:08
Completed NSE at 20:08, 0.00s elapsed
Nmap scan report for hefaistos.codacloud.net (52.88.224.163)
Host is up.

PORT      STATE    SERVICE     VERSION
53/tcp    filtered domain
123/tcp   filtered ntp
139/tcp   filtered netbios-ssn
161/tcp   filtered snmp
444/tcp   filtered snpp
500/tcp   filtered isakmp
4567/tcp  filtered tram
5353/tcp  filtered mdns
45320/tcp filtered unknown
51413/tcp filtered unknown
60202/tcp filtered unknown

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.88 seconds
           Raw packets sent: 22 (968B) | Rcvd: 0 (0B)
root@host:/home/student# 
```

Ex7:



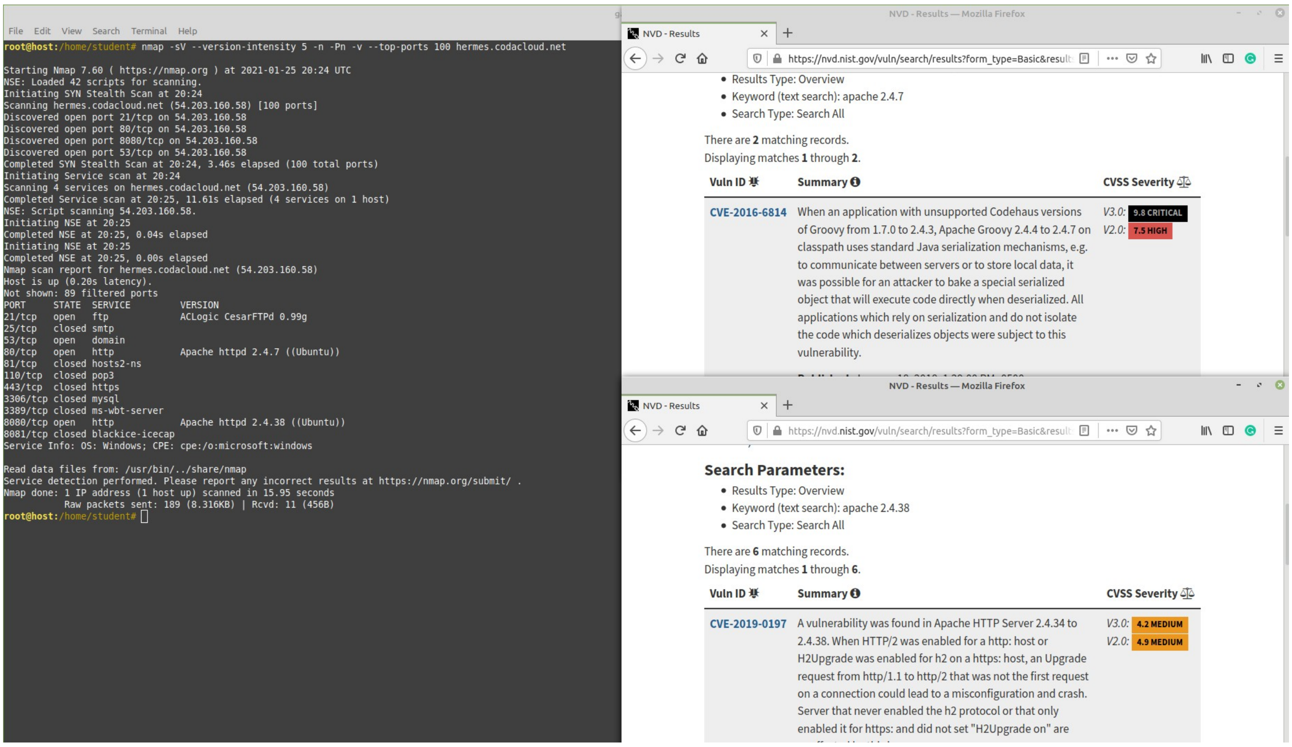
```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v --top-ports 100 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:10 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:10
Scanning hermes.codacloud.net (54.203.160.58) [100 ports]
Discovered open port 21/tcp on 54.203.160.58
Discovered open port 8080/tcp on 54.203.160.58
Discovered open port 53/tcp on 54.203.160.58
Discovered open port 80/tcp on 54.203.160.58
Completed SYN Stealth Scan at 20:10, 12.30s elapsed (100 total ports)
Initiating Service scan at 20:10
Scanning 4 services on hermes.codacloud.net (54.203.160.58)
Completed Service scan at 20:10, 11.61s elapsed (4 services on 1 host)
NSE: Script scanning 54.203.160.58.
Initiating NSE at 20:10
Completed NSE at 20:10, 0.05s elapsed
Initiating NSE at 20:10
Completed NSE at 20:10, 0.00s elapsed
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).
Not shown: 89 filtered ports
PORT     STATE  SERVICE         VERSION
21/tcp   open   ftp             ACLogic CesarFTPd 0.99g
25/tcp   closed smtp
53/tcp   open   domain
80/tcp   open   http            Apache httpd 2.4.7 ((Ubuntu))
81/tcp   closed hosts2-ns
110/tcp  closed pop3
443/tcp  closed https
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
8080/tcp open   http            Apache httpd 2.4.38 ((Ubuntu))
8081/tcp closed blackice-icecap
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.83 seconds
           Raw packets sent: 378 (16.632KB) | Rcvd: 22 (900B)
root@host:/home/student# 
```

Ex8: (nu l-am lasat pana la capat...)



```
root@host:/home/student# nmap -A --osscan-guess hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:11 UTC
Stats: 0:00:07 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.23% done; ETC: 20:12 (0:01:07 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.90% done; ETC: 20:12 (0:01:01 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.40% done; ETC: 20:12 (0:00:58 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 9.90% done; ETC: 20:12 (0:01:04 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.40% done; ETC: 20:12 (0:01:00 remaining)
Stats: 0:00:08 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 10.43% done; ETC: 20:12 (0:01:00 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.40% done; ETC: 20:12 (0:00:54 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.87% done; ETC: 20:12 (0:00:59 remaining)
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.87% done; ETC: 20:12 (0:00:59 remaining)
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 16.77% done; ETC: 20:13 (0:01:24 remaining)
Stats: 0:01:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 24.75% done; ETC: 20:16 (0:03:30 remaining)
Stats: 0:03:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 44.47% done; ETC: 20:20 (0:04:47 remaining)

root@host:/home/student# 
```

Ex9:



```
root@host:/home/student# nmap -sV --version-intensity 5 -n -Pn -v --top-ports 100 hermes.codacloud.net

Starting Nmap 7.60 ( https://nmap.org ) at 2021-01-25 20:24 UTC
NSE: Loaded 42 scripts for scanning.
Initiating SYN Stealth Scan at 20:24
Scanning hermes.codacloud.net (54.203.160.58) [100 ports]
Discovered open port 21/tcp on 54.203.160.58
Discovered open port 80/tcp on 54.203.160.58
Discovered open port 8080/tcp on 54.203.160.58
Discovered open port 53/tcp on 54.203.160.58
Completed SYN Stealth Scan at 20:24, 3.46s elapsed (100 total ports)
Initiating Service scan at 20:24
Scanning 4 services on hermes.codacloud.net (54.203.160.58)
Completed Service scan at 20:25, 11.61s elapsed (4 services on 1 host)
NSE: Script scanning 54.203.160.58.
Initiating NSE at 20:25
Completed NSE at 20:25, 0.04s elapsed
Initiating NSE at 20:25
Completed NSE at 20:25, 0.00s elapsed
Nmap scan report for hermes.codacloud.net (54.203.160.58)
Host is up (0.20s latency).
Not shown: 89 filtered ports
PORT     STATE  SERVICE         VERSION
21/tcp   open   ftp             ACLogic CesarFTPd 0.99g
25/tcp   closed smtp
53/tcp   open   domain
80/tcp   open   http            Apache httpd 2.4.7 ((Ubuntu))
81/tcp   closed hosts2-ns
110/tcp  closed pop3
443/tcp  closed https
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
8080/tcp open   http            Apache httpd 2.4.38 ((Ubuntu))
8081/tcp closed blackice-icecap
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.95 seconds
           Raw packets sent: 189 (8.316KB) | Rcvd: 11 (456B)
root@host:/home/student# 
```

NVD - Results — Mozilla Firefox
NVD - Results
https://nvd.nist.gov/vuln/search/results?form_type=Basic&result

- Results Type: Overview
- Keyword (text search): apache 2.4.7
- Search Type: Search All

There are **2** matching records.
Displaying matches **1** through **2**.

Vuln ID	Summary	CVSS Severity
CVE-2016-6814	When an application with unsupported Codehaus versions of Groovy from 1.7.0 to 2.4.3, Apache Groovy 2.4.4 to 2.4.7 on classpath uses standard Java serialization mechanisms, e.g. to communicate between servers or to store local data, it was possible for an attacker to bake a special serialized object that will execute code directly when deserialized. All applications which rely on serialization and do not isolate the code which deserializes objects were subject to this vulnerability.	V3.0: 9.8 CRITICAL V2.0: 7.5 HIGH

NVD - Results — Mozilla Firefox
NVD - Results
https://nvd.nist.gov/vuln/search/results?form_type=Basic&result

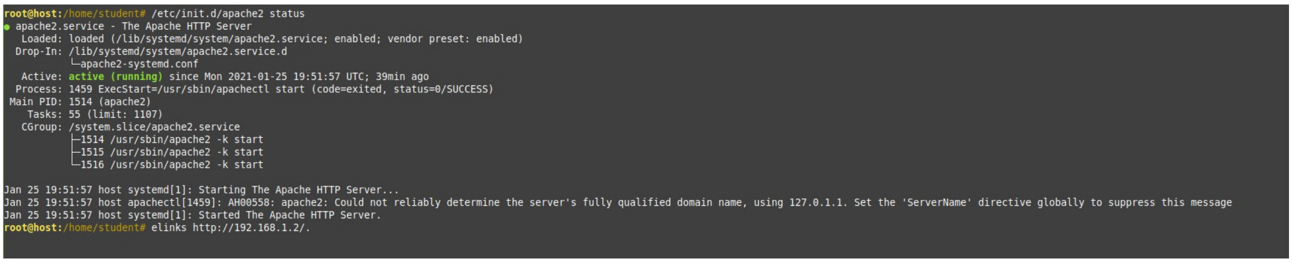
Search Parameters:

- Results Type: Overview
- Keyword (text search): apache 2.4.38
- Search Type: Search All

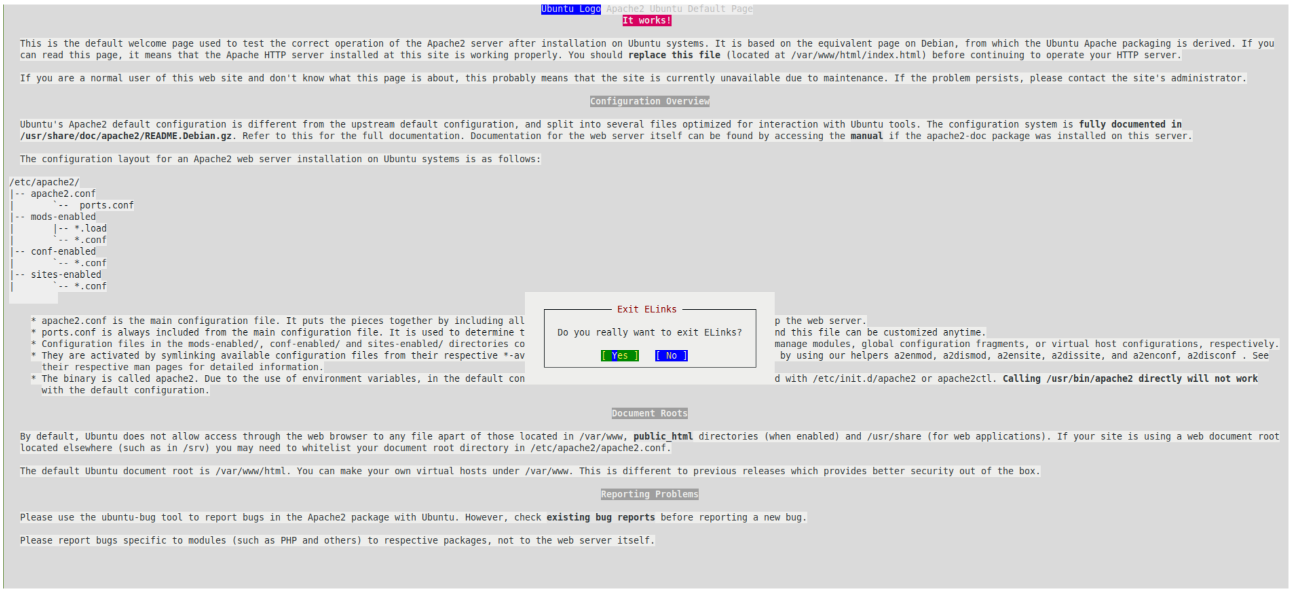
There are **6** matching records.
Displaying matches **1** through **6**.

Vuln ID	Summary	CVSS Severity
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are	V3.0: 4.2 MEDIUM V2.0: 4.9 MEDIUM

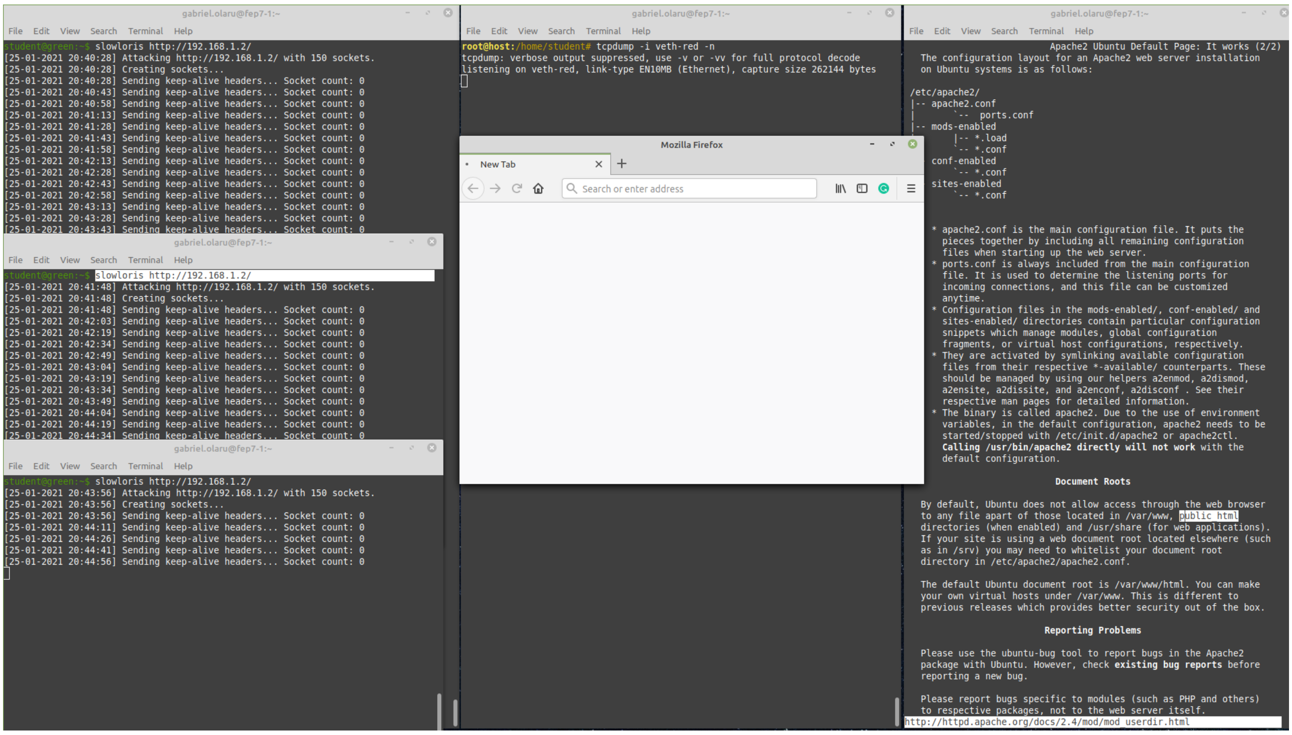
Ex10:



```
root@host:/home/student# /etc/init.d/apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Mon 2021-01-25 19:51:57 UTC; 39min ago
  Process: 1459 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 1514 (apache2)
    Tasks: 55 (limit: 1107)
   CGroup: /system.slice/apache2.service
           ├─1514 /usr/sbin/apache2 -k start
           ├─1515 /usr/sbin/apache2 -k start
           └─1516 /usr/sbin/apache2 -k start

Jan 25 19:51:57 host systemd[1]: Starting The Apache HTTP Server...
Jan 25 19:51:57 host apachectl[1459]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Jan 25 19:51:57 host systemd[1]: Started The Apache HTTP Server.
root@host:/home/student# elinks http://192.168.1.2/.
```



```
                                   Ubuntu Logo Apache2 Ubuntu Default Page
                                                It works!

  This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you
  can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.

  If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

                                          Configuration Overview

  Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in
  /usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the apache2-doc package was installed on this server.

  The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

 /etc/apache2/
 |-- apache2.conf
 |       `--  ports.conf
 |-- mods-enabled
 |       |-- *.load
 |       `-- *.conf
 |-- conf-enabled
 |       `-- *.conf
 |-- sites-enabled
 |       `-- *.conf

                                          ┌── Exit ELinks ──────┐
    * apache2.conf is the main configuration file. It puts the pieces together by including all            p the web server.
    * ports.conf is always included from the main configuration file. It is used to determine t  Do you really want to exit ELinks?  nd this file can be customized anytime.
    * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories co            manage modules, global configuration fragments, or virtual host configurations, respectively.
    * They are activated by symlinking available configuration files from their respective *-av  [ Yes ]  [ No ]  by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See
      their respective man pages for detailed information.
    * The binary is called apache2. Due to the use of environment variables, in the default con            d with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work
      with the default configuration.

                                             Document Roots

  By default, Ubuntu does not allow access through the web browser to any file apart of those located in /var/www, public_html directories (when enabled) and /usr/share (for web applications). If your site is using a web document root
  located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

  The default Ubuntu document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

                                           Reporting Problems

  Please use the ubuntu-bug tool to report bugs in the Apache2 package with Ubuntu. However, check existing bug reports before reporting a new bug.

  Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.
```



```
student@green:~$ slowloris http://192.168.1.2/
[25-01-2021 20:40:28] Attacking http://192.168.1.2/ with 150 sockets.
[25-01-2021 20:40:28] Creating sockets...
[25-01-2021 20:40:28] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:40:43] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:40:58] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:41:13] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:41:28] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:41:43] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:41:58] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:13] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:28] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:43] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:58] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:13] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:28] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:43] Sending keep-alive headers... Socket count: 0
```

```
student@green:~$ slowloris http://192.168.1.2/
[25-01-2021 20:41:48] Attacking http://192.168.1.2/ with 150 sockets.
[25-01-2021 20:41:48] Creating sockets...
[25-01-2021 20:41:48] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:03] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:19] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:34] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:42:49] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:04] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:19] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:34] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:43:49] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:04] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:19] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:34] Sending keep-alive headers... Socket count: 0
```

```
student@green:~$ slowloris http://192.168.1.2/
[25-01-2021 20:43:56] Attacking http://192.168.1.2/ with 150 sockets.
[25-01-2021 20:43:56] Creating sockets...
[25-01-2021 20:43:56] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:11] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:26] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:41] Sending keep-alive headers... Socket count: 0
[25-01-2021 20:44:56] Sending keep-alive headers... Socket count: 0
```

```
root@host:/home/student# tcpdump -i veth-red -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on veth-red, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
                             Apache2 Ubuntu Default Page: It works (2/2)
   The configuration layout for an Apache2 web server installation
   on Ubuntu systems is as follows:

 /etc/apache2/
 |-- apache2.conf
 |       `--  ports.conf
 |-- mods-enabled
 |       |-- *.load
 |       `-- *.conf
     conf-enabled
         `-- *.conf
     sites-enabled
         `-- *.conf


     * apache2.conf is the main configuration file. It puts the
       pieces together by including all remaining configuration
       files when starting up the web server.
     * ports.conf is always included from the main configuration
       file. It is used to determine the listening ports for
       incoming connections, and this file can be customized
       anytime.
     * Configuration files in the mods-enabled/, conf-enabled/ and
       sites-enabled/ directories contain particular configuration
       snippets which manage modules, global configuration
       fragments, or virtual host configurations, respectively.
     * They are activated by symlinking available configuration
       files from their respective *-available/ counterparts. These
       should be managed by using our helpers a2enmod, a2dismod,
       a2ensite, a2dissite, and a2enconf, a2disconf . See their
       respective man pages for detailed information.
     * The binary is called apache2. Due to the use of environment
       variables, in the default configuration, apache2 needs to be
       started/stopped with /etc/init.d/apache2 or apache2ctl.
       Calling /usr/bin/apache2 directly will not work with the
       default configuration.

                             Document Roots

   By default, Ubuntu does not allow access through the web browser
   to any file apart of those located in /var/www, public_html
   directories (when enabled) and /usr/share (for web applications).
   If your site is using a web document root located elsewhere (such
   as in /srv) you may need to whitelist your document root
   directory in /etc/apache2/apache2.conf.

   The default Ubuntu document root is /var/www/html. You can make
   your own virtual hosts under /var/www. This is different to
   previous releases which provides better security out of the box.

                           Reporting Problems

   Please use the ubuntu-bug tool to report bugs in the Apache2
   package with Ubuntu. However, check existing bug reports before
   reporting a new bug.

   Please report bugs specific to modules (such as PHP and others)
   to respective packages, not to the web server itself.
http://httpd.apache.org/docs/2.4/mod/mod_userdir.html
```