Laboratorul 10

> Link-uri:
>
> - https://cybermap.kaspersky.com/ -> arata atacurile cibernetice in timp real.

Task 1 | Aflare adresa IP publica

```
root@host:~# curl ifconfig.me ; echo ""
141.85.150.33
root@host:~# curl api64.ipify.org ; echo ""
141.85.150.37
root@host:~# curl ipinfo.io/ip ; echo ""
141.85.150.30
```

Pentru a vedea adresa IP publica:

- `curl ifconfig.me`
- `curl api64.ipify.org`
- `curl ipinfo.io/ip`

Adresa VM-ului este **10.9.5.29**, o adresa IP privata din **clasa A** (10.0.0.0 – 10.255.255.255).

Adresa publica este **141.85.150.30**, avand clasa **B** (128.0.0.0 – 191.255.255.255).

Task 2 | Aflare informatii despre adresa IP publica

```
root@host:~# whois 141.85.150.30
```

```
root@host:~# whois 141.85.150.30
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% 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
country:        RO
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:  2022-12-01T17:31:35Z
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

person:         Mihai Barbulescu
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:        MB6037-RIPE
mnt-by:         PUB-MNT
created:        2003-12-03T17:51:34Z
last-modified:  2008-05-23T16:40:05Z
```

```
source:         RIPE # Filtered

% Information related to '141.85.0.0/16AS2614'

route:          141.85.0.0/16
descr:          RoEduNet
descr:          "Politehnica" University of Bucharest
origin:         AS2614
mnt-by:         PUB-MNT
mnt-lower:      PUB-MNT
created:        2002-05-16T13:10:52Z
last-modified:  2003-12-07T18:32:49Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.114
(BUSA)
```

Observ subnetul (**reteaua**):

```
route:          141.85.0.0/16
```

Iar asta pare sa fie **autonomous system**:

```
origin:         AS2614
```

Task 3 | DNS Resolution

```
root@host:~# apt install dnsutils
root@host:~# which nslookup
/usr/bin/nslookup
```

```
root@host:~# nslookup -querytype=CNAME erp.codacloud.net
```

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
erp.codacloud.net   canonical name = hermes.codacloud.net.

Authoritative answers can be found from:
codacloud.net   nameserver = kiki.ns.cloudflare.com.
codacloud.net   nameserver = nitin.ns.cloudflare.com.
```

```
nitin.ns.cloudflare.com internet address = 108.162.193.215
nitin.ns.cloudflare.com internet address = 172.64.33.215
nitin.ns.cloudflare.com internet address = 173.245.59.215
nitin.ns.cloudflare.com has AAAA address 2a06:98c1:50::ac40:21d7
nitin.ns.cloudflare.com has AAAA address 2606:4700:58::adf5:3bd7
nitin.ns.cloudflare.com has AAAA address 2803:f800:50::6ca2:c1d7
kiki.ns.cloudflare.com  internet address = 173.245.58.180
kiki.ns.cloudflare.com  internet address = 108.162.192.180
kiki.ns.cloudflare.com  internet address = 172.64.32.180
kiki.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:20b4
kiki.ns.cloudflare.com  has AAAA address 2606:4700:50::adf5:3ab4
kiki.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c0b4
```

```
root@host:~# nslookup -querytype=NS cs.pub.ro
```

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
cs.pub.ro   nameserver = ns1.grid.pub.ro.
cs.pub.ro   nameserver = ns1.cs.pub.ro.
cs.pub.ro   nameserver = ns2.cs.pub.ro.

Authoritative answers can be found from:
ns1.cs.pub.ro   internet address = 141.85.226.5
ns1.grid.pub.ro internet address = 141.85.241.15
ns1.grid.pub.ro has AAAA address 2001:b30:800:f011:141:85:241:15
ns2.cs.pub.ro   internet address = 141.85.241.113
```

```
root@host:~# nslookup -querytype=MX cs.pub.ro
```

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
cs.pub.ro   mail exchanger = 10 ironport.upb.ro.

Authoritative answers can be found from:
cs.pub.ro   nameserver = ns1.grid.pub.ro.
cs.pub.ro   nameserver = ns2.cs.pub.ro.
cs.pub.ro   nameserver = ns1.cs.pub.ro.
ironport.upb.ro internet address = 141.85.13.12
ns1.cs.pub.ro   internet address = 141.85.226.5
ns1.grid.pub.ro internet address = 141.85.241.15
```

```
ns1.grid.pub.ro has AAAA address 2001:b30:800:f011:141:85:241:15
ns2.cs.pub.ro   internet address = 141.85.241.113
```

```
root@host:~# nslookup -querytype=A erp.codacloud.net
```

```
Server:     127.0.0.53
Address:    127.0.0.53#53

Non-authoritative answer:
erp.codacloud.net   canonical name = hermes.codacloud.net.
Name:   hermes.codacloud.net
Address: 35.231.129.40
```

Task 4 | Descoperirea porturiloe TCP deschise

```
root@host:~# nmap -sT -p 21,22,23,25,53,80,138,443,8000,8080
hermes.codacloud.net hefaistos.codacloud.net
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-12-11 23:03 EET
Nmap scan report for hermes.codacloud.net (35.231.129.40)
Host is up (0.061s latency).
rDNS record for 35.231.129.40: 40.129.231.35.bc.googleusercontent.com

PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
53/tcp   filtered 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 scan report for hefaistos.codacloud.net (34.148.182.155)
Host is up (0.029s latency).
rDNS record for 34.148.182.155: 155.182.148.34.bc.googleusercontent.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   open     http
138/tcp  filtered netbios-dgm
443/tcp  filtered https
8000/tcp filtered http-alt
8080/tcp filtered http-proxy

Nmap done: 2 IP addresses (2 hosts up) scanned in 1.96 seconds
```

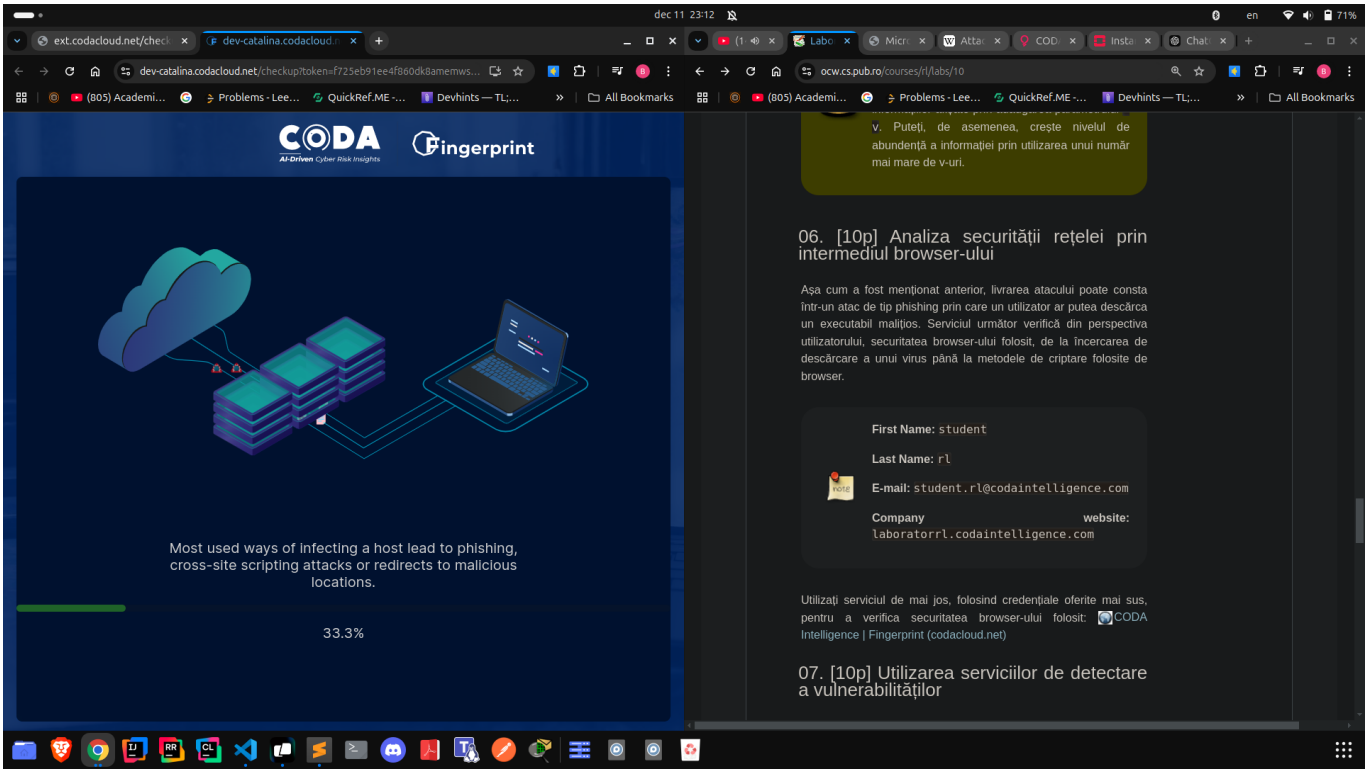
Task 5 | Determinarea versiunilor aplicatiilor descoperite

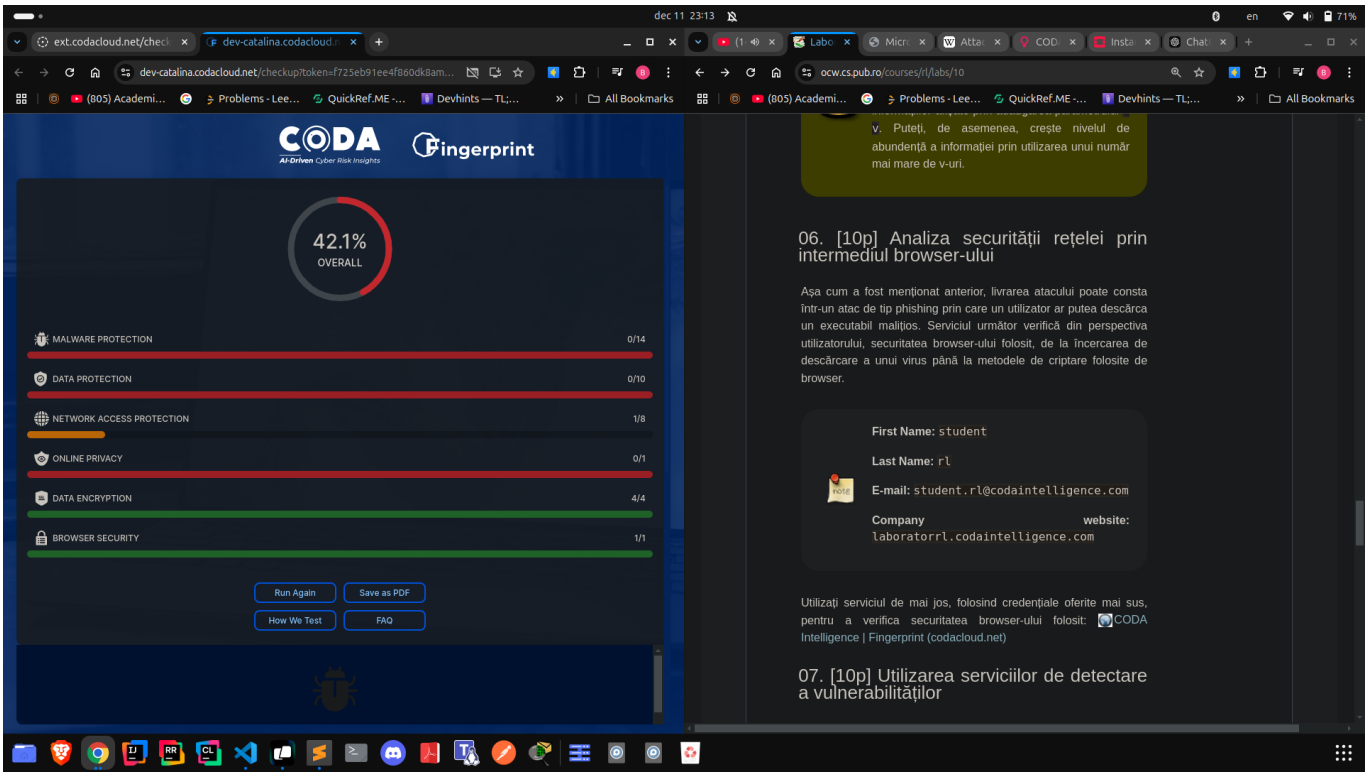
```
# Nu va scana versiuni
root@host:~# nmap -sT -T5 -Pn -v -v -p 21,22,23,25,53,80,138,443,8000,8080
hermes.codacloud.net hefaistos.codacloud.net
```

> Flag-ul **-sV** detecteaza versiuni de aplicatie.

```
# Va scana versiunile aplicatiilor ce ruleaza pe aceste porturi
root@host:~# nmap -sT -sV -T5 -Pn -v -v -p
21,22,23,25,53,80,138,443,8000,8080 hermes.codacloud.net
hefaistos.codacloud.net
```

Task 6 | Analiza securiatii retelei prin intermediului browser-ului





Task 7 | Utilizarea serviciilor de detectare a vulnerabilitatilor

Platforme:

- https://dnsdumpster.com/
- https://www.shodan.io/

Scriind **hermes.codacloud.net** in prompt-ul de input al lui https://dnsdumpster.com/, am obtinut adresa IP **35.231.129.40**, despre care pot afla mai multe la URL-ul https://www.shodan.io/host/35.231.129.40.

Task 8 | Rulare **Dos** (Denial of Service) pe un server web

TODO: