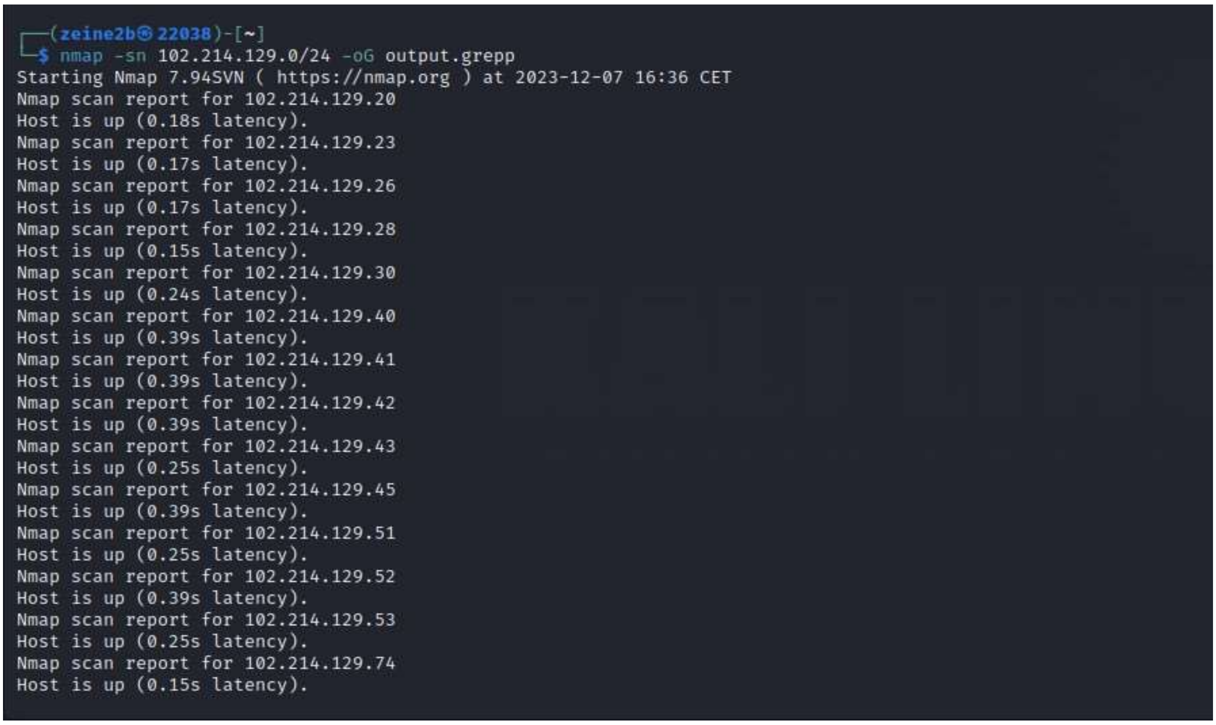
22038

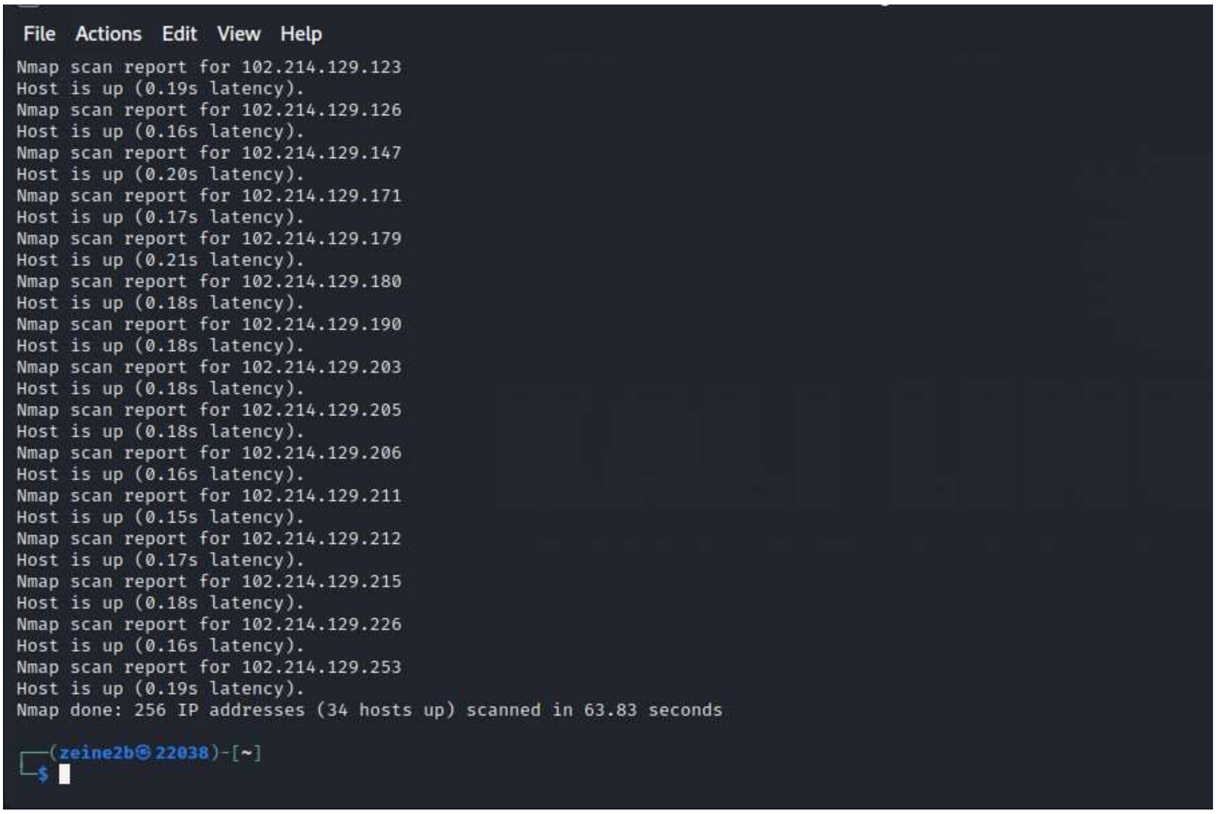
Zeinebou El Agheb

Exo2

1-nmap -sn 102.214.129.0/24 -oG output. Grepp

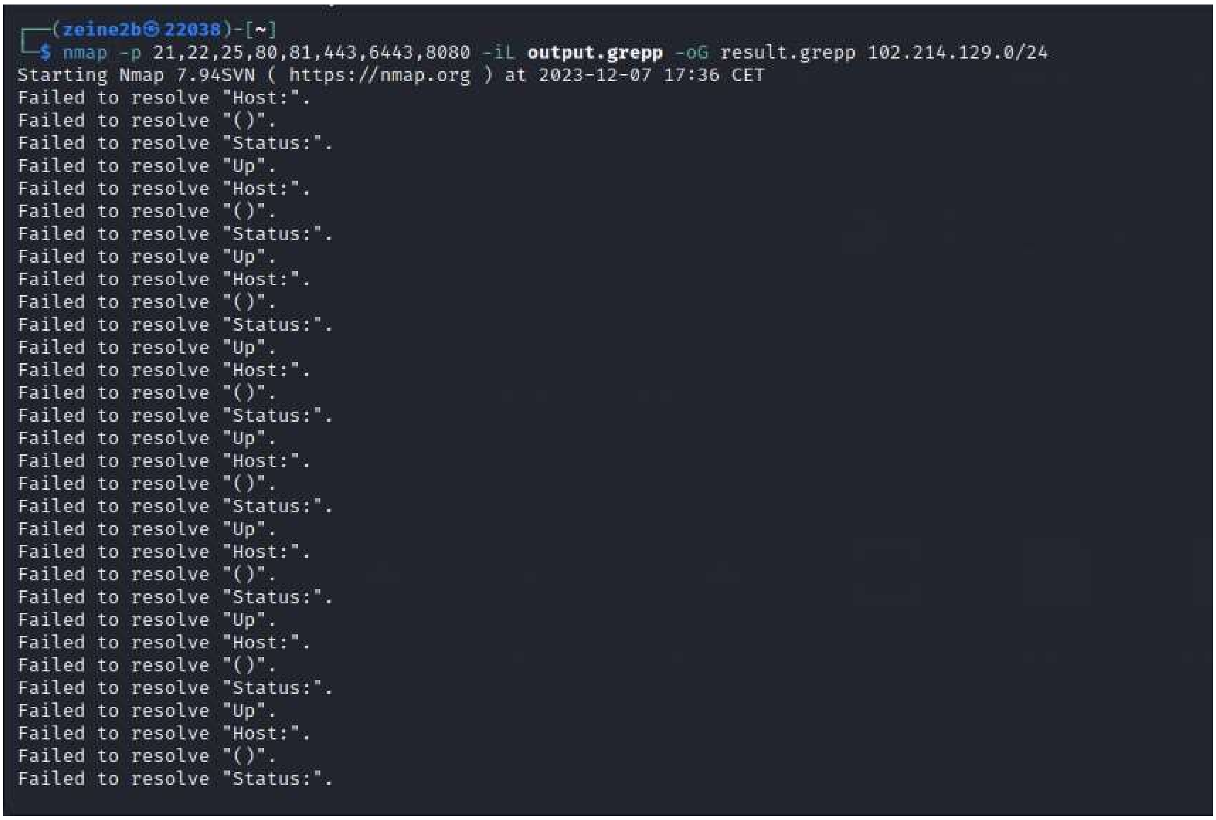


```
┌──(zeine2b㉿22038)-[~]
└─$ nmap -sn 102.214.129.0/24 -oG output.grepp
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 16:36 CET
Nmap scan report for 102.214.129.20
Host is up (0.18s latency).
Nmap scan report for 102.214.129.23
Host is up (0.17s latency).
Nmap scan report for 102.214.129.26
Host is up (0.17s latency).
Nmap scan report for 102.214.129.28
Host is up (0.15s latency).
Nmap scan report for 102.214.129.30
Host is up (0.24s latency).
Nmap scan report for 102.214.129.40
Host is up (0.39s latency).
Nmap scan report for 102.214.129.41
Host is up (0.39s latency).
Nmap scan report for 102.214.129.42
Host is up (0.39s latency).
Nmap scan report for 102.214.129.43
Host is up (0.25s latency).
Nmap scan report for 102.214.129.45
Host is up (0.39s latency).
Nmap scan report for 102.214.129.51
Host is up (0.25s latency).
Nmap scan report for 102.214.129.52
Host is up (0.39s latency).
Nmap scan report for 102.214.129.53
Host is up (0.25s latency).
Nmap scan report for 102.214.129.74
Host is up (0.15s latency).
```

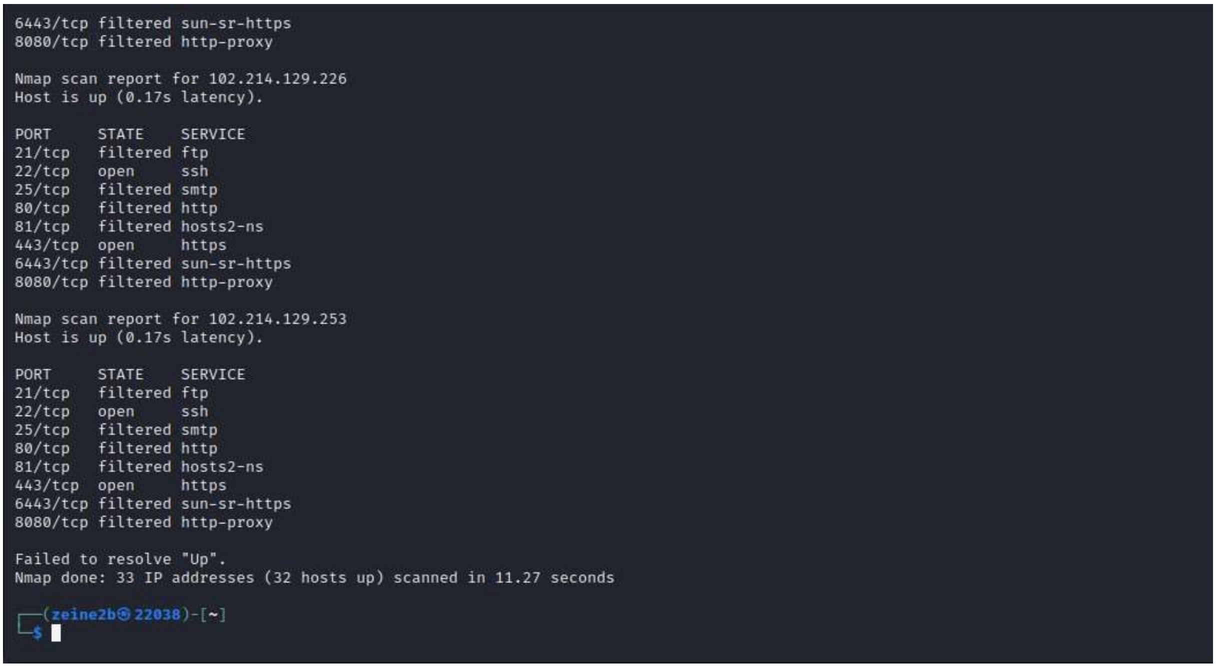


```
Nmap scan report for 102.214.129.123
Host is up (0.19s latency).
Nmap scan report for 102.214.129.126
Host is up (0.16s latency).
Nmap scan report for 102.214.129.147
Host is up (0.20s latency).
Nmap scan report for 102.214.129.171
Host is up (0.17s latency).
Nmap scan report for 102.214.129.179
Host is up (0.21s latency).
Nmap scan report for 102.214.129.180
Host is up (0.18s latency).
Nmap scan report for 102.214.129.190
Host is up (0.18s latency).
Nmap scan report for 102.214.129.203
Host is up (0.18s latency).
Nmap scan report for 102.214.129.205
Host is up (0.18s latency).
Nmap scan report for 102.214.129.206
Host is up (0.16s latency).
Nmap scan report for 102.214.129.211
Host is up (0.15s latency).
Nmap scan report for 102.214.129.212
Host is up (0.17s latency).
Nmap scan report for 102.214.129.215
Host is up (0.18s latency).
Nmap scan report for 102.214.129.226
Host is up (0.16s latency).
Nmap scan report for 102.214.129.253
Host is up (0.19s latency).
Nmap done: 256 IP addresses (34 hosts up) scanned in 63.83 seconds

┌──(zeine2b㉿22038)-[~]
└─$ 
```

2-nmap -p 21,22,25,80,81,443,6443,8080 -iL output. Grepp -oG result.grepp 102.214.129.0/24

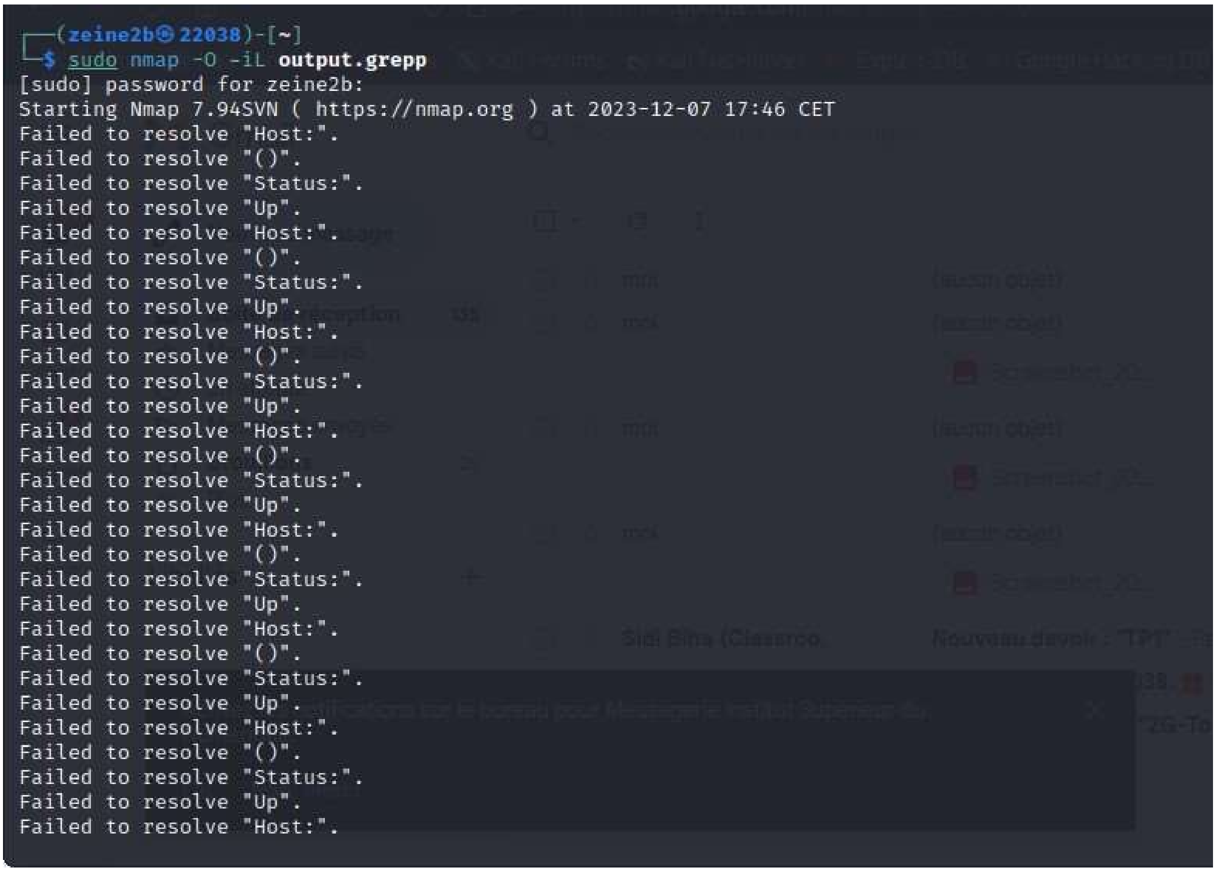


```
┌──(zeine2b㉿22038)-[~]
└─$ nmap -p 21,22,25,80,81,443,6443,8080 -iL output.grepp -oG result.grepp 102.214.129.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 17:36 CET
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
```



```
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Nmap scan report for 102.214.129.226
Host is up (0.17s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
25/tcp   filtered smtp
80/tcp   filtered http
81/tcp   filtered hosts2-ns
443/tcp  open     https
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Nmap scan report for 102.214.129.253
Host is up (0.17s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   open     ssh
25/tcp   filtered smtp
80/tcp   filtered http
81/tcp   filtered hosts2-ns
443/tcp  open     https
6443/tcp filtered sun-sr-https
8080/tcp filtered http-proxy

Failed to resolve "Up".
Nmap done: 33 IP addresses (32 hosts up) scanned in 11.27 seconds

┌──(zeine2b㉿22038)-[~]
└─$ █
```

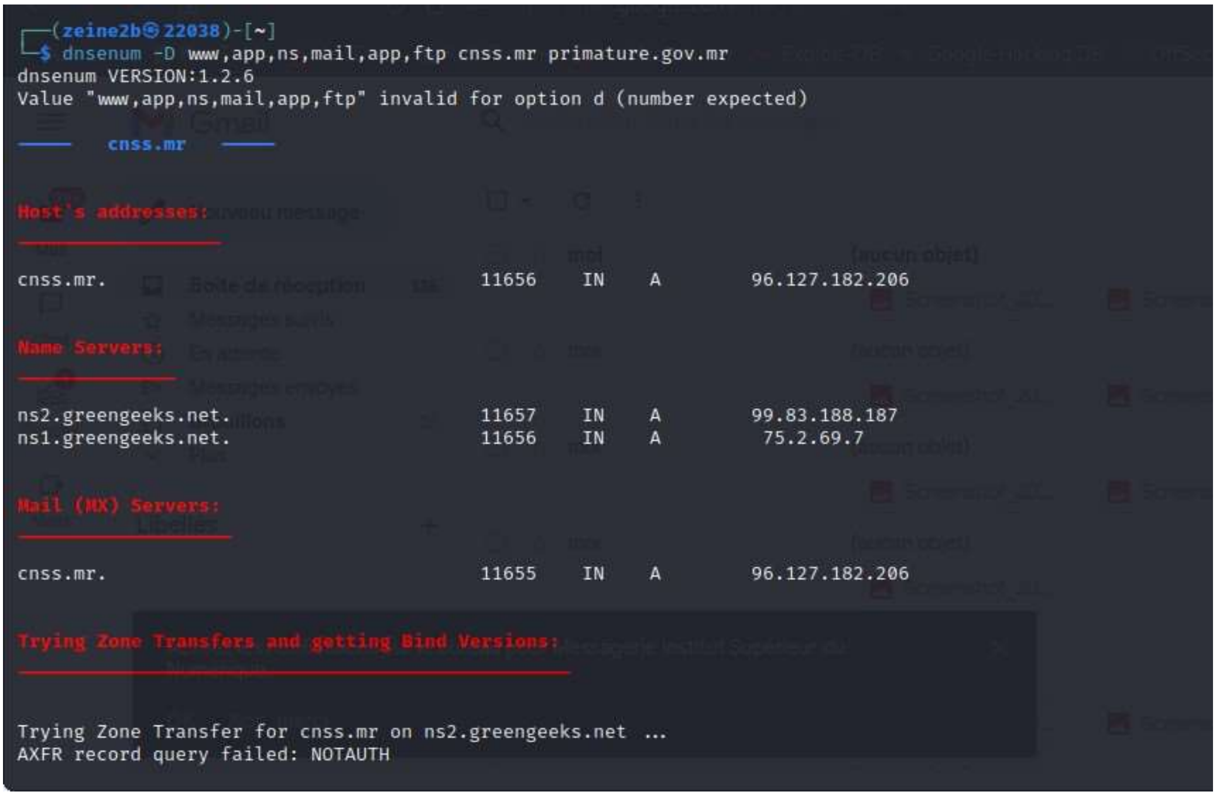
3-sudo nmap -O -iL output.grepp



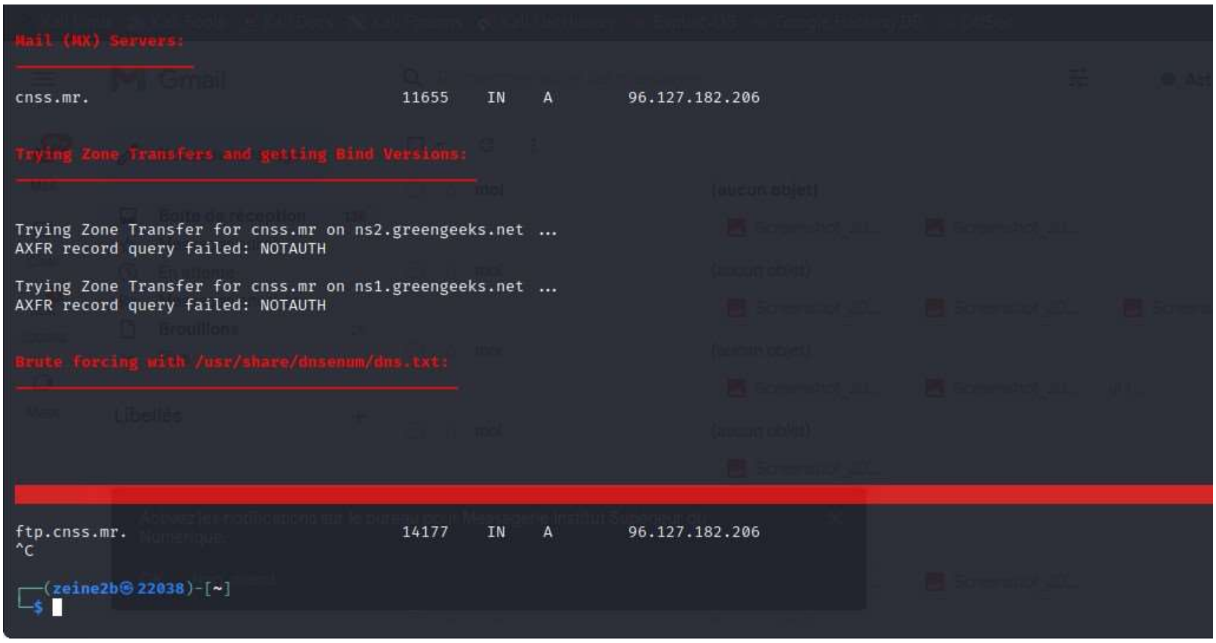
```
┌──(zeine2b㉿22038)-[~]
└─$ sudo nmap -O -iL output.grepp
[sudo] password for zeine2b:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 17:46 CET
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
Failed to resolve "()".
Failed to resolve "Status:".
Failed to resolve "Up".
Failed to resolve "Host:".
```

Exo3

1-dnsenum -d www,app,ns,mail,ftp,zmail,vpn cnss.mr primature.gov.mr

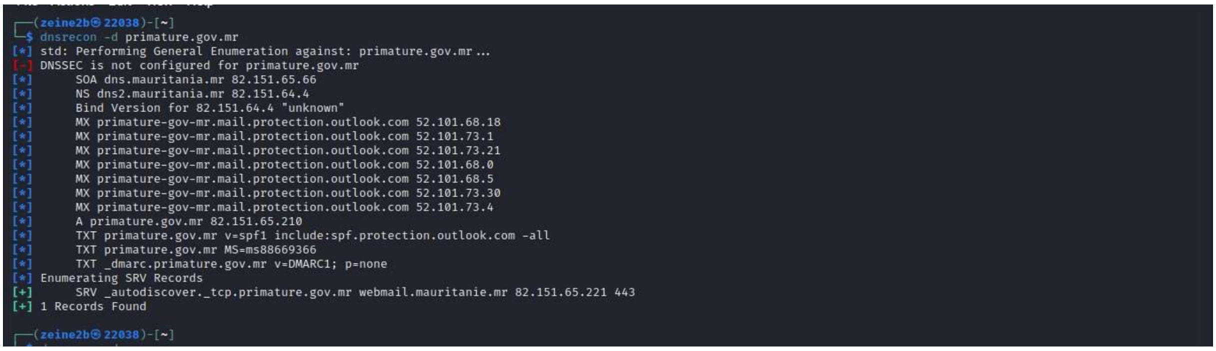


```
┌──(zeine2b㉿22038)-[~]
└─$ dnsenum -D www,app,ns,mail,app,ftp cnss.mr primature.gov.mr
dnsenum VERSION:1.2.6
Value "www,app,ns,mail,app,ftp" invalid for option d (number expected)
-----   cnss.mr   -----


Host's addresses:
__________________

cnss.mr.                                 11656    IN    A        96.127.182.206


Name Servers:
______________

ns2.greengeeks.net.                      11657    IN    A        99.83.188.187
ns1.greengeeks.net.                      11656    IN    A         75.2.69.7


Mail (MX) Servers:
___________________

cnss.mr.                                 11655    IN    A        96.127.182.206


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for cnss.mr on ns2.greengeeks.net ...
AXFR record query failed: NOTAUTH
```



```
Mail (MX) Servers:
___________________

cnss.mr.                                 11655    IN    A        96.127.182.206


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for cnss.mr on ns2.greengeeks.net ...
AXFR record query failed: NOTAUTH

Trying Zone Transfer for cnss.mr on ns1.greengeeks.net ...
AXFR record query failed: NOTAUTH


Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________




ftp.cnss.mr.                             14177    IN    A        96.127.182.206
^C

┌──(zeine2b㉿22038)-[~]
└─$ 
```

2-dnsrecon -d primature.gov.mr

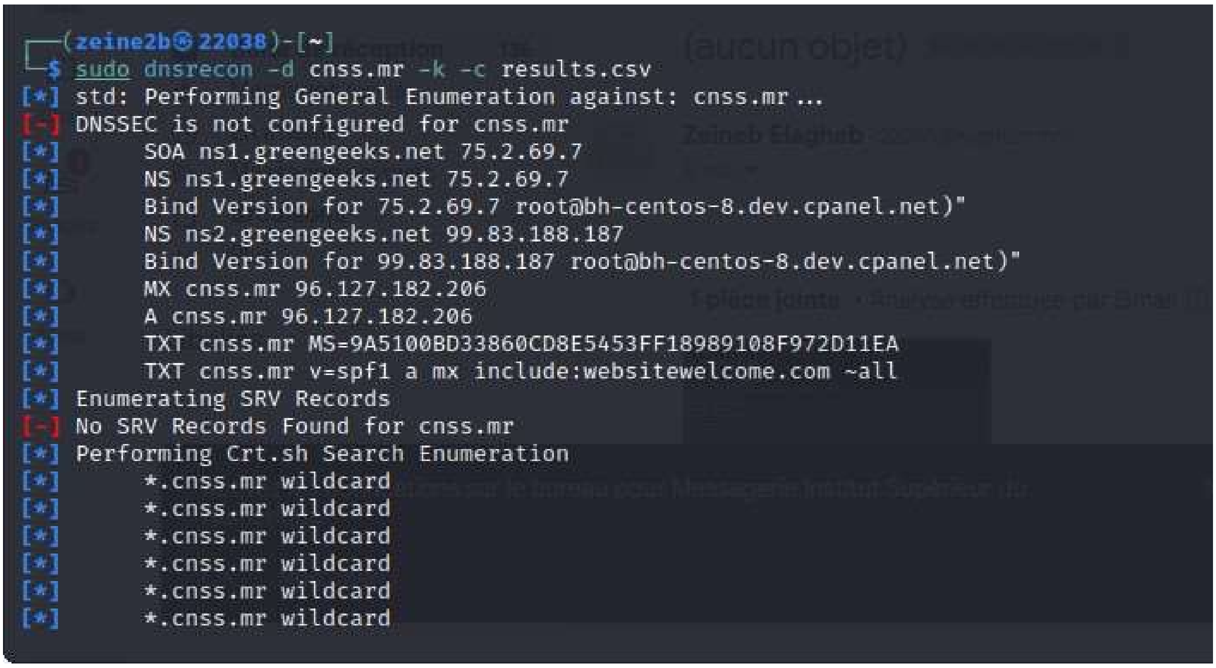


```
┌──(zeine2b㉿22038)-[~]
└─$ dnsrecon -d primature.gov.mr
[*] std: Performing General Enumeration against: primature.gov.mr...
[-] DNSSEC is not configured for primature.gov.mr
[*]      SOA dns.mauritania.mr 82.151.65.66
[*]      NS dns2.mauritania.mr 82.151.64.4
[*]      Bind Version for 82.151.64.4 "unknown"
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.18
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.1
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.21
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.0
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.5
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.30
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.4
[*]      A primature.gov.mr 82.151.65.210
[*]      TXT primature.gov.mr v=spf1 include:spf.protection.outlook.com -all
[*]      TXT primature.gov.mr MS=ms88669366
[*]      TXT _dmarc.primature.gov.mr v=DMARC1; p=none
[*] Enumerating SRV Records
[+]      SRV _autodiscover._tcp.primature.gov.mr webmail.mauritanie.mr 82.151.65.221 443
[+] 1 Records Found

┌──(zeine2b㉿22038)-[~]
```

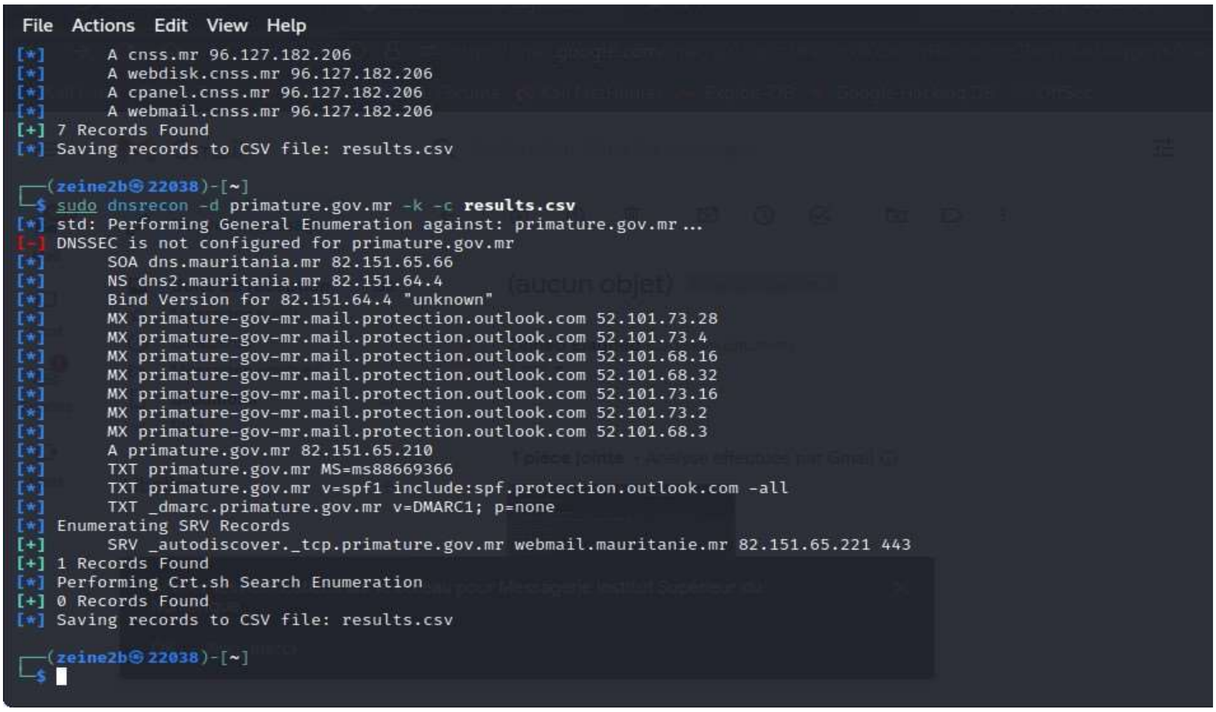
- *dnsrecon -d cnss.mr*

```
┌──(zeine2b㉿22038)-[~]
└─$ dnsrecon -d cnss.mr
[*] std: Performing General Enumeration against: cnss.mr...
[-] DNSSEC is not configured for cnss.mr
[*]      SOA ns1.greengeeks.net 75.2.69.7
[*]      NS ns1.greengeeks.net 75.2.69.7
[*]      Bind Version for 75.2.69.7 root@bh-centos-8.dev.cpanel.net)"
[*]      NS ns2.greengeeks.net 99.83.188.187
[*]      Bind Version for 99.83.188.187 root@bh-centos-8.dev.cpanel.net)"
[*]      MX cnss.mr 96.127.182.206
[*]      A cnss.mr 96.127.182.206
[*]      TXT cnss.mr v=spf1 a mx include:websitewelcome.com ~all
[*]      TXT cnss.mr MS=9A5100BD33860CD8E5453FF18989108F972D11EA
[*] Enumerating SRV Records
[-] No SRV Records Found for cnss.mr

┌──(zeine2b㉿22038)-[~]
```

- *Dnsrecon -d cnss.mr -k -c results.csv*

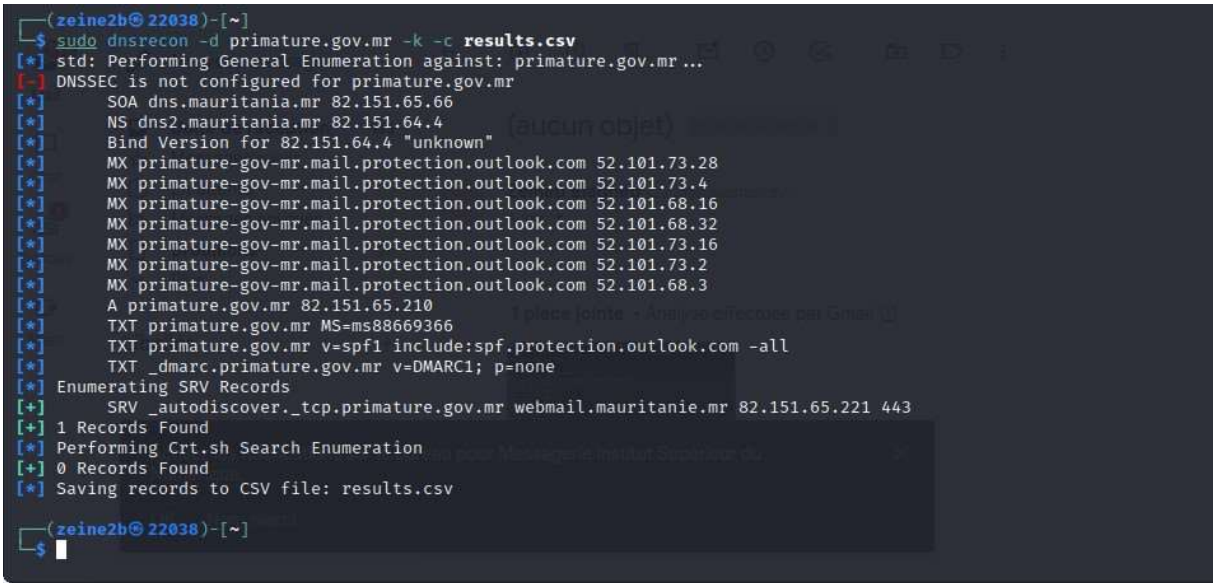


```
┌──(zeine2b㉿22038)-[~]
└─$ sudo dnsrecon -d cnss.mr -k -c results.csv
[*] std: Performing General Enumeration against: cnss.mr...
[-] DNSSEC is not configured for cnss.mr
[*]      SOA ns1.greengeeks.net 75.2.69.7
[*]      NS ns1.greengeeks.net 75.2.69.7
[*]      Bind Version for 75.2.69.7 root@bh-centos-8.dev.cpanel.net)"
[*]      NS ns2.greengeeks.net 99.83.188.187
[*]      Bind Version for 99.83.188.187 root@bh-centos-8.dev.cpanel.net)"
[*]      MX cnss.mr 96.127.182.206
[*]      A cnss.mr 96.127.182.206
[*]      TXT cnss.mr MS=9A5100BD33860CD8E5453FF18989108F972D11EA
[*]      TXT cnss.mr v=spf1 a mx include:websitewelcome.com ~all
[*] Enumerating SRV Records
[-] No SRV Records Found for cnss.mr
[*] Performing Crt.sh Search Enumeration
[*]      *.cnss.mr wildcard
[*]      *.cnss.mr wildcard
[*]      *.cnss.mr wildcard
[*]      *.cnss.mr wildcard
[*]      *.cnss.mr wildcard
[*]      *.cnss.mr wildcard
```



```
[*]      A cnss.mr 96.127.182.206
[*]      A webdisk.cnss.mr 96.127.182.206
[*]      A cpanel.cnss.mr 96.127.182.206
[*]      A webmail.cnss.mr 96.127.182.206
[+] 7 Records Found
[*] Saving records to CSV file: results.csv

┌──(zeine2b㉿22038)-[~]
└─$ sudo dnsrecon -d primature.gov.mr -k -c results.csv
[*] std: Performing General Enumeration against: primature.gov.mr ...
[-] DNSSEC is not configured for primature.gov.mr
[*]      SOA dns.mauritania.mr 82.151.65.66
[*]      NS dns2.mauritania.mr 82.151.64.4
[*]      Bind Version for 82.151.64.4 "unknown"
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.28
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.4
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.16
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.32
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.16
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.2
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.3
[*]      A primature.gov.mr 82.151.65.210
[*]      TXT primature.gov.mr MS=ms88669366
[*]      TXT primature.gov.mr v=spf1 include:spf.protection.outlook.com -all
[*]      TXT _dmarc.primature.gov.mr v=DMARC1; p=none
[*] Enumerating SRV Records
[+]      SRV _autodiscover._tcp.primature.gov.mr webmail.mauritanie.mr 82.151.65.221 443
[+] 1 Records Found
[*] Performing Crt.sh Search Enumeration
[+] 0 Records Found
[*] Saving records to CSV file: results.csv

┌──(zeine2b㉿22038)-[~]
└─$ █
```

Dnsrecon -d primature.gov.mr -k -c results.csv



```
┌──(zeine2b㉿22038)-[~]
└─$ sudo dnsrecon -d primature.gov.mr -k -c results.csv
[*] std: Performing General Enumeration against: primature.gov.mr ...
[-] DNSSEC is not configured for primature.gov.mr
[*]      SOA dns.mauritania.mr 82.151.65.66
[*]      NS dns2.mauritania.mr 82.151.64.4
[*]      Bind Version for 82.151.64.4 "unknown"
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.28
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.4
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.16
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.32
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.16
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.73.2
[*]      MX primature-gov-mr.mail.protection.outlook.com 52.101.68.3
[*]      A primature.gov.mr 82.151.65.210
[*]      TXT primature.gov.mr MS=ms88669366
[*]      TXT primature.gov.mr v=spf1 include:spf.protection.outlook.com -all
[*]      TXT _dmarc.primature.gov.mr v=DMARC1; p=none
[*] Enumerating SRV Records
[+]      SRV _autodiscover._tcp.primature.gov.mr webmail.mauritanie.mr 82.151.65.221 443
[+] 1 Records Found
[*] Performing Crt.sh Search Enumeration
[+] 0 Records Found
[*] Saving records to CSV file: results.csv

┌──(zeine2b㉿22038)-[~]
└─$ █
```

3-whatweb cnss .mr

```
[+] 0 Records Found
[*] Saving records to CSV file: results.csv

┌──(zeine2b㉿22038)-[~]
└─$ whatweb cnss.mr
http://cnss.mr [403 Forbidden] Country[UNITED STATES][US], HTML5, IP[96.127.182.206], Title[403 Forbidden][Title element contains newline(s)!], UncommonHeaders[x-cont
ent-type-options], X-Frame-Options[SAMEORIGIN]

┌──(zeine2b㉿22038)-[~]
└─$ █
```