Sean Lee
Nacho Rodriguez-Cortes

1.

Question: after nslookup -query=any, the terminal said: server can't find ultralingua.com: NOTIMP -- what does this mean?

Question: what is the difference between server and address in nslookup? Address had a #53 after the ip address

Performing whois with the IP address gave us information on the Internet Assigned Numbers Authority whereas using the whois command on the ultralingua domain gave us information directly about ultralingua.

What domain did you investigate?

Domain: ultralingua.com

What is its IP address?

IP address: 192.168.1.1

When does the domain's registration expire?

Expiration date: 2024-12-23T07:48:00Z

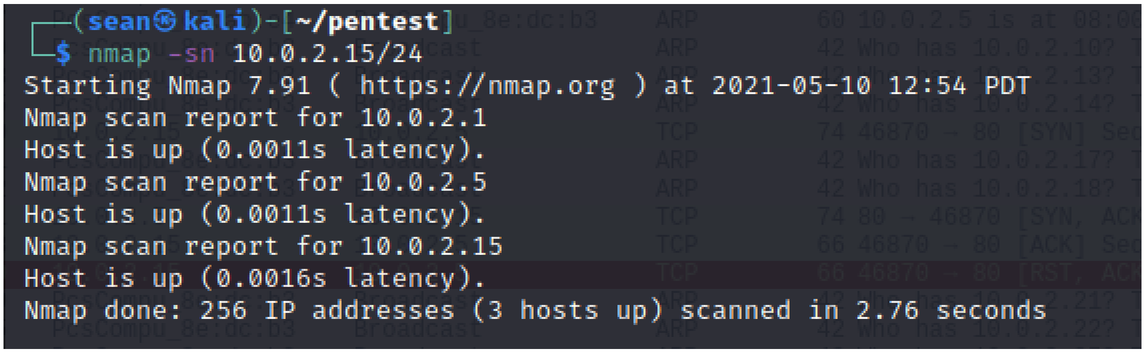
What information, if any, did you learn about the people or corporation responsible for the domain in question? (Your answer could be less interesting than you had hoped due to the increasingly common use of domain privacy services. In that case, at least give me information about what you learned about the relevant domain privacy service.)

Information about corporations responsible for domain: Typical business contact information pertaining to Tucows.

2.

List the IP addresses for all the active hosts you found on the local network (i.e. the hosts whose IP addresses have the same first 24 bits--i.e. the same W.X.Y of the IP address W.X.Y.Z--as Kali's IP address).

IP addresses:



```
┌──(sean㉿kali)-[~/pentest]
└─$ nmap -sn 10.0.2.15/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:54 PDT
Nmap scan report for 10.0.2.1
Host is up (0.0011s latency).
Nmap scan report for 10.0.2.5
Host is up (0.0011s latency).
Nmap scan report for 10.0.2.15
Host is up (0.0016s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.76 seconds
```

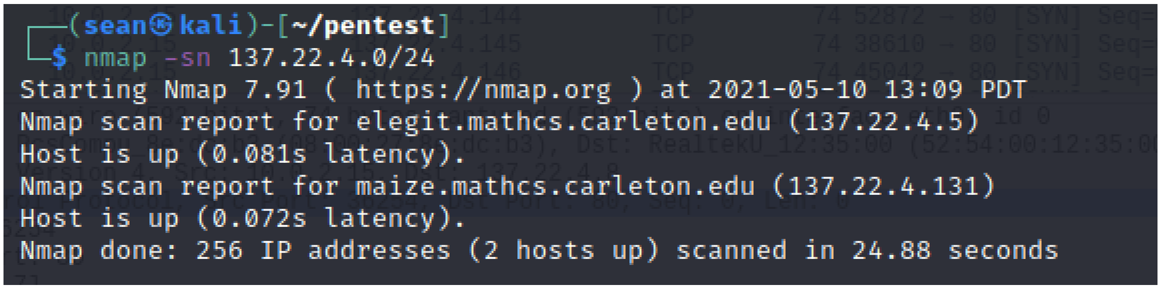
What entities do those IP addresses represent?

> We used sudo nmap -O -v on the ip addresses to gather more information about them.
> 10.0.2.1 didn't return any identifying information aside from a MAC address
> 10.0.2.5 pertains to the linux virtual box
> 10.0.2.15 didn't return any identifying information, but interestingly it stated that too many fingerprints match this host to give specific OS information

For each possible candidate IP address it was searching in the local network, what steps did nmap take? (You can answer this question by examining the Wireshark captured packets. If you want to make it easier to read the relevant packets, try doing "nmap -sn [just-one-ip-address]" instead of the /24 thing.)
Same question, but for the 137.22.4.0/24 network

> It appears that nmap attempted to set up a TCP handshake with each of the entities, the ones it reported being those that actually completed the handshake.

For the 137.22.4.0/24 network.



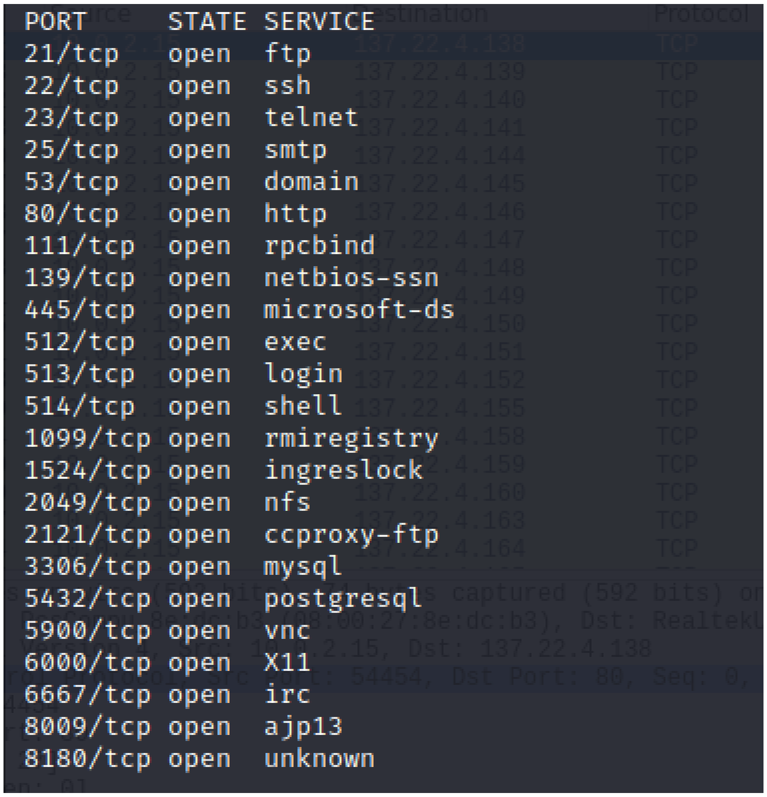
```
┌──(sean㉿kali)-[~/pentest]
└─$ nmap -sn 137.22.4.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 13:09 PDT
Nmap scan report for elegit.mathcs.carleton.edu (137.22.4.5)
Host is up (0.081s latency).
Nmap scan report for maize.mathcs.carleton.edu (137.22.4.131)
Host is up (0.072s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 24.88 seconds
```

For the Carleton IP address, it appeared that it was still performing TCP handshakes, but there were a couple of DNS protocols that appeared.

137.22.4.5 appears to be some sort of storage server running some sort of (a guess) British Gas OS.
137.22.4.131 appears to also be some sort of storage server running (a guess) British Gas OS.

3.

Which ports does Metasploitable have open, and what services do they correspond to (e.g. port 22 / SSH or port 80 / HTTP)?



```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
```

What database server(s) is/are available on Metasploitable?

FTP server is open.
IRC server is open.
There are also 2 http ports available, one being associated with port 80, the other associated with port 8180.

What is the value of the RSA SSH host key? What is the host key for?

2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

The RSA SSH key is used to authenticate a user when creating a TLS session. Specifically, the host key is used by the client to decrypt an authentication message from the server when attempting to connect. It is used to ensure that the host you are connect to is actually the one you intended to connect to.

Pick one of the open ports that has a service you have never heard of, and explain what the service does.

SMTP port 25. This is the oldest of the SMTP ports, established in 1982. It is used to send and receive emails, SMTP representing Simple Mail Transfer Protocol. Interestingly, the SMTP port 25 specifically is most commonly abused to send spam from compromised computers.