CS 231
Nathan Hayes-Rich and Peter McCrea
Pen testing #1: host detection & port scanning

Passive information gathering

1. What domain did you investigate?
    a. xkcd.com
2. What is its IP address?
    a. 151.101.192.67, 151.101.64.67, 151.101.128.67, 151.101.0.67
3. When does the domain's registration expire?
    a. Registrar Registration Expiration Date: 2024-01-25T21:25:10Z
4. 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.)
    a. xkcd.com uses DomainsByProxy, LLC (based in Scottsdale, AZ) to hide their identity.
    b. The whois does list fax number (+1.4806242598), registrant phone number (+1.4806242599), and tech/admin email for the domain (XKCD.COM@domainsbyproxy.com).
    c. The domain is also owned / registered by godaddy.com

Host detection

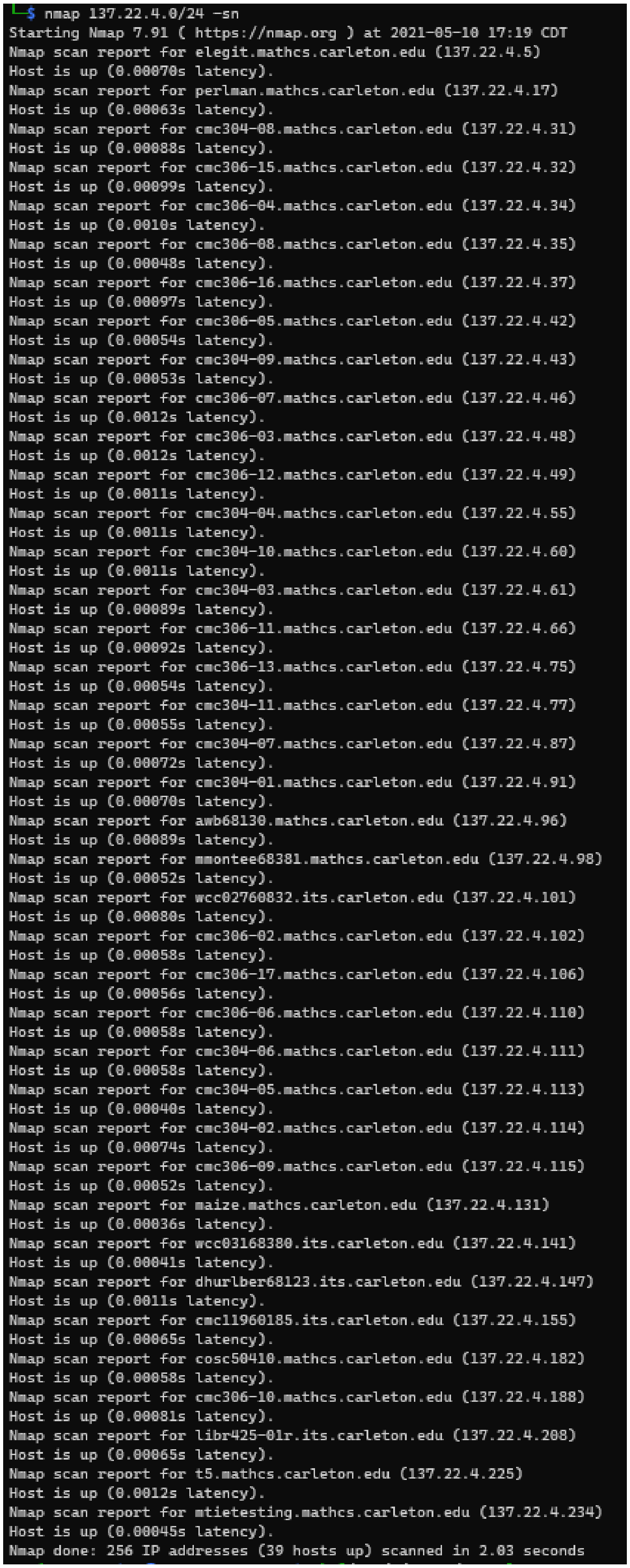
1. List the IP addresses for all the active hosts you found on the local network (i.e. the hosts whose IP addresses have the same first 24 bits--i.e. the same W.X.Y of the IP address W.X.Y.Z--as Kali's IP address).
    a. 10.0.2.1, 10.0.2.2, 10.0.2.4, 10.0.2.15
2. What entities do those IP addresses represent?
    a. 10.0.2.1 (DNS), 10.0.2.2 (DNS), 10.0.2.4 (Metasploitable VM), 10.0.2.15 (Kali VM).
3. 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.)

a. First, nmap issues an arp request for the IP address (if it’s not already stored in the arp cache). Second, nmap initiates a TCP handshake with the device associated with the ip address we are nmapping. Third, it performs a DNS query on the IP address.

4. Same question, but for the 137.22.4.0/24 network.

a.



```
└─$ nmap 137.22.4.0/24 -sn
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 17:19 CDT
Nmap scan report for elegit.mathcs.carleton.edu (137.22.4.5)
Host is up (0.00070s latency).
Nmap scan report for perlman.mathcs.carleton.edu (137.22.4.17)
Host is up (0.00063s latency).
Nmap scan report for cmc304-08.mathcs.carleton.edu (137.22.4.31)
Host is up (0.00088s latency).
Nmap scan report for cmc306-15.mathcs.carleton.edu (137.22.4.32)
Host is up (0.00099s latency).
Nmap scan report for cmc306-04.mathcs.carleton.edu (137.22.4.34)
Host is up (0.0010s latency).
Nmap scan report for cmc306-08.mathcs.carleton.edu (137.22.4.35)
Host is up (0.00048s latency).
Nmap scan report for cmc306-16.mathcs.carleton.edu (137.22.4.37)
Host is up (0.00097s latency).
Nmap scan report for cmc306-05.mathcs.carleton.edu (137.22.4.42)
Host is up (0.00054s latency).
Nmap scan report for cmc304-09.mathcs.carleton.edu (137.22.4.43)
Host is up (0.00053s latency).
Nmap scan report for cmc306-07.mathcs.carleton.edu (137.22.4.46)
Host is up (0.0012s latency).
Nmap scan report for cmc306-03.mathcs.carleton.edu (137.22.4.48)
Host is up (0.0012s latency).
Nmap scan report for cmc306-12.mathcs.carleton.edu (137.22.4.49)
Host is up (0.0011s latency).
Nmap scan report for cmc304-04.mathcs.carleton.edu (137.22.4.55)
Host is up (0.0011s latency).
Nmap scan report for cmc304-10.mathcs.carleton.edu (137.22.4.60)
Host is up (0.0011s latency).
Nmap scan report for cmc304-03.mathcs.carleton.edu (137.22.4.61)
Host is up (0.00089s latency).
Nmap scan report for cmc306-11.mathcs.carleton.edu (137.22.4.66)
Host is up (0.00092s latency).
Nmap scan report for cmc306-13.mathcs.carleton.edu (137.22.4.75)
Host is up (0.00054s latency).
Nmap scan report for cmc304-11.mathcs.carleton.edu (137.22.4.77)
Host is up (0.00055s latency).
Nmap scan report for cmc304-07.mathcs.carleton.edu (137.22.4.87)
Host is up (0.00072s latency).
Nmap scan report for cmc304-01.mathcs.carleton.edu (137.22.4.91)
Host is up (0.00070s latency).
Nmap scan report for awb68130.mathcs.carleton.edu (137.22.4.96)
Host is up (0.00089s latency).
Nmap scan report for mmontee68381.mathcs.carleton.edu (137.22.4.98)
Host is up (0.00052s latency).
Nmap scan report for wcc02760832.its.carleton.edu (137.22.4.101)
Host is up (0.00080s latency).
Nmap scan report for cmc306-02.mathcs.carleton.edu (137.22.4.102)
Host is up (0.00058s latency).
Nmap scan report for cmc306-17.mathcs.carleton.edu (137.22.4.106)
Host is up (0.00056s latency).
Nmap scan report for cmc306-06.mathcs.carleton.edu (137.22.4.110)
Host is up (0.00058s latency).
Nmap scan report for cmc304-06.mathcs.carleton.edu (137.22.4.111)
Host is up (0.00058s latency).
Nmap scan report for cmc304-05.mathcs.carleton.edu (137.22.4.113)
Host is up (0.00040s latency).
Nmap scan report for cmc304-02.mathcs.carleton.edu (137.22.4.114)
Host is up (0.00074s latency).
Nmap scan report for cmc306-09.mathcs.carleton.edu (137.22.4.115)
Host is up (0.00052s latency).
Nmap scan report for maize.mathcs.carleton.edu (137.22.4.131)
Host is up (0.00036s latency).
Nmap scan report for wcc03168380.its.carleton.edu (137.22.4.141)
Host is up (0.00041s latency).
Nmap scan report for dhurlber68123.its.carleton.edu (137.22.4.147)
Host is up (0.0011s latency).
Nmap scan report for cmc11960185.its.carleton.edu (137.22.4.155)
Host is up (0.00065s latency).
Nmap scan report for cosc50410.mathcs.carleton.edu (137.22.4.182)
Host is up (0.00058s latency).
Nmap scan report for cmc306-10.mathcs.carleton.edu (137.22.4.188)
Host is up (0.00081s latency).
Nmap scan report for libr425-01r.its.carleton.edu (137.22.4.208)
Host is up (0.00065s latency).
Nmap scan report for t5.mathcs.carleton.edu (137.22.4.225)
Host is up (0.0012s latency).
Nmap scan report for mtietesting.mathcs.carleton.edu (137.22.4.234)
Host is up (0.00045s latency).
Nmap done: 256 IP addresses (39 hosts up) scanned in 2.03 seconds
```

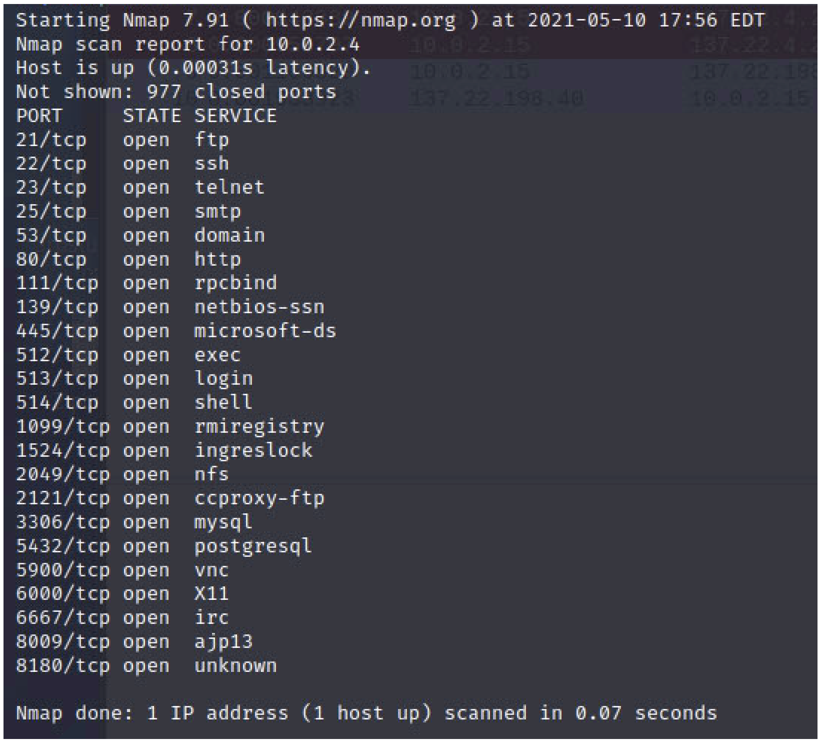
b.

   i. Elegit is Dave Musicant's project to create a GUI-based Git client!!!
   ii. Perlman, maize, and ada are all Carleton servers for various CS (and Stats) related tasks.
   iii. mtietesting looks like a Mike Tie test machine
   iv. The cmc-prefixed machines are CMC labs. The libr-prefixed machines are in the library. The wcc-prefixed machines are in the Weitz.
   v. There are a few named machines which belong to CS professors.

c. First, nmap issues an arp request for the IP address (if it's not already stored in the arp cache). Second, nmap initiates a TCP handshake with the device associated with the ip address we are nmapping. Third, it performs a DNS query on the IP address.

Port scanning

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

   a. 

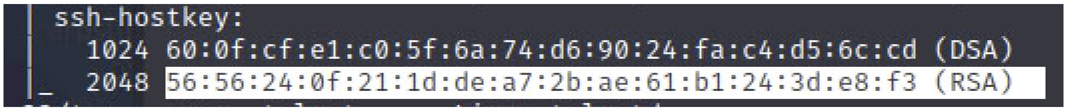
```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 17:56 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00031s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
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

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

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

a. mysql

b. postgresql

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

   a. 

   ```
   | ssh-hostkey:
   |   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
   |_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
   ```

   b. The RSA host key is Metasploitable's public RSA key used for SSH connections. In combined use with the VM's private RSA key, it can be used to establish a secure connection (i.e. some form of encrypted session using AES) and simultaneously verify the identity of the VM for any outside connection. (This is the same key that gets saved to the known hosts file of a remote connection upon successfully connecting).

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

   a. smtp is the simple mail transfer protocol. This port is used to send and receive mail messages. When you want to send or receive a mail message you use this port. Using this port the client can submit mail data to a mail server to be processed and sent to its destination.