Owen Barnett and Nick Pandelakis
CS231
10 May 2021

1. We investigated carleton.edu. The IP address is 137.22.94.116. The domain's registration expires July 31, 2021. We found out that this domain was registered in 1989, they are located at 300 N College St in (beautiful) Northfield, MN. We also received the phone numbers and email addresses of the network abuse manager and network manager of the owner of this domain.

2. Kali's ip address is 10.0.2.15. We found four hosts: 10.0.2.1, 10.0.2.2, 10.0.2.4, and 10.0.2.15. These addresses are the router (1 and 2), Kali, and Metasploitable. To get these ip addresses, nmap used the address resolution protocol and asked every ip address in the range 10.0.2.1-10.0.2.255 on the network to identify themselves. When these devices responded, nmap logged their existence and ip address. When using nmap on the Carleton math/cs network, it attempts to do a tcp handshake with each ip address of the form 137.22.4.*. If the handshake was successful, then nmap logged that ip address as existing and up.

3. The database servers on Metasploitable are mysql and postgresql.

```
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
```

2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. The host key is used to authenticate the computer when using ssh. The port 8009 is associated with Apache JServ Protocol version 1.3. This service is similar to https but improves efficiency by passing binary representations of header from a proxy server to an application server (assuming you have a proxy server "in front of" your application server).