Kiefer Lord
16 May 2022

1. Passive Information Gathering

The IP address for carleton.edu is 137.22.94.116. The domain expires on July 31, 2024. I found the following information about the owners of the domain:

Registrant:

Carleton College
One North College Street
Northfield, MN 55057-4040
USA

Administrative Contact:

Chris Dlugosz
Carleton College
One North College Street
Northfield, MN 55057
USA
+1.5072225999
network-manager@carleton.edu

Technical Contact:

Webmasters Sysadmins
Carleton College
One North College Street
Northfield, MN 55057-4040
USA
+1.5072225999
nic-tech-contact@carleton.edu

2. Host Detection

Active IP addresses on the local network: 192.168.205.129, 192.168.205.128, 192.168.205.1, 192.168.205.2. I couldn't find which hosts those IP addresses correspond to, but 192.168.205.129 is the Metasploitable address (used ifconfig locally). Nmap broadcasts to all hosts on the network, asking who has the given IP address. Then, the host with that IP address responds, saying that it has the given IP address.

Nmap output for the 137.22.4.0/24 network (contains IP addresses and host names):
Nmap scan report for elegit.mathcs.carleton.edu (137.22.4.5)

Host is up (0.0018s latency).
Nmap scan report for perlman.mathcs.carleton.edu (137.22.4.17)
Host is up (0.0019s latency).
Nmap scan report for olin312-02.mathcs.carleton.edu (137.22.4.31)
Host is up (0.0017s latency).
Nmap scan report for olin210cs70686.mathcs.carleton.edu (137.22.4.35)
Host is up (0.0023s latency).
Nmap scan report for olin304-06.mathcs.carleton.edu (137.22.4.38)
Host is up (0.0028s latency).
Nmap scan report for olin310-19.mathcs.carleton.edu (137.22.4.39)
Host is up (0.0019s latency).
Nmap scan report for olin310-17.mathcs.carleton.edu (137.22.4.40)
Host is up (0.0026s latency).
Nmap scan report for olin310-22.mathcs.carleton.edu (137.22.4.41)
Host is up (0.0026s latency).
Nmap scan report for olin208-01.mathcs.carleton.edu (137.22.4.78)
Host is up (0.014s latency).
Nmap scan report for mmontee68381.mathcs.carleton.edu (137.22.4.98)
Host is up (0.0042s latency).
Nmap scan report for olin304-09.mathcs.carleton.edu (137.22.4.106)
Host is up (0.0048s latency).
Nmap scan report for olin308-08.mathcs.carleton.edu (137.22.4.107)
Host is up (0.0047s latency).
Nmap scan report for olin210cs70693.mathcs.carleton.edu (137.22.4.110)
Host is up (0.0055s latency).
Nmap scan report for olin302-03.mathcs.carleton.edu (137.22.4.111)
Host is up (0.0062s latency).
Nmap scan report for olin308-05.mathcs.carleton.edu (137.22.4.127)
Host is up (0.0077s latency).
Nmap scan report for olin327-62232.mathcs.carleton.edu (137.22.4.149)
Host is up (0.0098s latency).

It looks like nmap asks each individual IP address on that network for its host name, and the host sends a message back containing its host name.

3. Port Scanning

Ports for the Metasploitable machine:

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

mysql and postgresql are database servers.

RSA SSH key: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. This key is used to authenticate entities trying to SSH into the machine.

Port 23 is for Telnet, which seems to be an earlier and less secure version of SSH, as it gives other devices a remote terminal connection to the host offering Telnet (https://www.grc.com/port_23.htm)