Vicente Riquelme

Seth Romanenko

1. Passive information gathering

- What domain did you investigate? We investigated Bing.com
- What is its IP address? 204.79.197.200
- When does the domain's registration expire? It expires 2023-01-30T00:00:00+0000x
- 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.)

  We were able to find that markmoniter.com is involved with bing.

  The following report goes into detail about the Microsoft corp, the owners of bing.com

  Registrant Name: Domain Administrator

  Registrant Organization: Microsoft Corporation

  Registrant Street: One Microsoft Way,

  Registrant City: Redmond

  Registrant State/Province: WA

  Registrant Postal Code: 98052

  Registrant Country: US

  Registrant Phone: +1.4258828080

  Registrant Phone Ext:

  Registrant Fax: +1.4259367329

  Registrant Fax Ext:

  Registrant Email: domains@microsoft.com

  Registry Admin ID:

  Admin Name: Domain Administrator

Admin Organization: Microsoft Corporation

Admin Street: One Microsoft Way,

Admin City: Redmond

Admin State/Province: WA

Admin Postal Code: 98052

Admin Country: US

Admin Phone: +1.4258828080

Admin Phone Ext:

Admin Fax: +1.4259367329

Admin Fax Ext:

Admin Email: domains@microsoft.com

Registry Tech ID:

Tech Name: MSN Hostmaster

Tech Organization: Microsoft Corporation

Tech Street: One Microsoft Way,

Tech City: Redmond

Tech State/Province: WA

Tech Postal Code: 98052

Tech Country: US

Tech Phone: +1.4258828080

Tech Phone Ext:

Tech Fax: +1.4259367329

Tech Fax Ext:

Tech Email: msnhst@microsoft.com

Name Server: dns1.p09.nsone.net

Name Server: dns4.p09.nsone.net

Name Server: ns3-204.azure-dns.org

Name Server: ns2-204.azure-dns.net

Name Server: ns1-204.azure-dns.com

Name Server: dns3.p09.nsone.net

Name Server: ns4-204.azure-dns.info

Name Server: dns2.p09.nsone.net

Thus, bing.com is owned by the Microsoft corporation.

2. Host Detection

- 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).
- 172.16.138.1
- 172.16.138.2
- 172.16.138.128

3 hosts were found.

Metasploitable is at ip address 192.168.64.1. It had a different range of addresses since my computer uses the M1 chip and thus was not within the 172.xx.xxx.x range.

What entities do those IP addresses represent?

.1 is my mac.

.2 is the vm router address.

.128 is kali, which is why is the tell address.

Metasploitable is 192.168.64.1

- 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.)

  Nmap sends an ARP packet asking the ip address to tell 172. 16.138.128

  Nmap tries to connect using TCP, both as http and syn/ack

  Then there two DNS packet sent between the two. One from either source.

  Then there is another ARP packet asking the ip address to tell 172. 16.138.128

  When run on the 137.22.4.0/24 network, the following ip addresses are in use.

  - Nmap scan report for elegit.mathcs.carleton.edu (137.22.4.5)
  - Nmap scan report for olin310-18.mathcs.carleton.edu (137.22.4.15)
  - Nmap scan report for perlman.mathcs.carleton.edu (137.22.4.17)
  - Nmap scan report for ada.mathcs.carleton.edu (137.22.4.19)
  - Nmap scan report for olin310-23.mathcs.carleton.edu (137.22.4.21)
  - Nmap scan report for olin302-01.mathcs.carleton.edu (137.22.4.30)
  - Nmap scan report for olin312-02.mathcs.carleton.edu (137.22.4.31)
  - Nmap scan report for olin304-07.mathcs.carleton.edu (137.22.4.32)
  - Nmap scan report for olin210cs70692.mathcs.carleton.edu (137.22.4.34)
  - Nmap scan report for olin210cs70686.mathcs.carleton.edu (137.22.4.35)
  - Nmap scan report for olin304-08.mathcs.carleton.edu (137.22.4.37)
  - Nmap scan report for olin304-06.mathcs.carleton.edu (137.22.4.38)
  - Nmap scan report for olin310-19.mathcs.carleton.edu (137.22.4.39)
  - Nmap scan report for olin310-17.mathcs.carleton.edu (137.22.4.40)
  - Nmap scan report for olin310-22.mathcs.carleton.edu (137.22.4.41)
  - Nmap scan report for olin210cs70687.mathcs.carleton.edu (137.22.4.42)
  - Nmap scan report for olin312-03.mathcs.carleton.edu (137.22.4.43)
  - Nmap scan report for olin210cs70691.mathcs.carleton.edu (137.22.4.46)
  - Nmap scan report for olin304-04.mathcs.carleton.edu (137.22.4.49)
  - Nmap scan report for olin310-21.mathcs.carleton.edu (137.22.4.54)
  - Nmap scan report for olin310-24.mathcs.carleton.edu (137.22.4.56)
  - Nmap scan report for olin310-20.mathcs.carleton.edu (137.22.4.57)
  - Nmap scan report for olin310-11.mathcs.carleton.edu (137.22.4.58)
  - Nmap scan report for olin310-15.mathcs.carleton.edu (137.22.4.59)
  - Nmap scan report for olin312-04.mathcs.carleton.edu (137.22.4.60)
  - Nmap scan report for olin312-06.mathcs.carleton.edu (137.22.4.61)
  - Nmap scan report for olin310-12.mathcs.carleton.edu (137.22.4.63)

- Nmap scan report for olin310-16.mathcs.carleton.edu (137.22.4.65)
- Nmap scan report for olin304-03.mathcs.carleton.edu (137.22.4.66)
- Nmap scan report for olin310-02.mathcs.carleton.edu (137.22.4.67)
- Nmap scan report for olin310-06.mathcs.carleton.edu (137.22.4.70)
- Nmap scan report for olin310-03.mathcs.carleton.edu (137.22.4.71)
- Nmap scan report for olin310-07.mathcs.carleton.edu (137.22.4.72)
- Nmap scan report for olin310-04.mathcs.carleton.edu (137.22.4.73)
- Nmap scan report for olin304-05.mathcs.carleton.edu (137.22.4.75)
- Nmap scan report for olin312-05.mathcs.carleton.edu (137.22.4.77)
- Nmap scan report for olin208-01.mathcs.carleton.edu (137.22.4.78)
- Nmap scan report for olin310-08.mathcs.carleton.edu (137.22.4.79)
- Nmap scan report for olin310-01.mathcs.carleton.edu (137.22.4.80)
- Nmap scan report for olin310-05.mathcs.carleton.edu (137.22.4.82)
- Nmap scan report for olin310-14.mathcs.carleton.edu (137.22.4.83)
- Nmap scan report for olin310-10.mathcs.carleton.edu (137.22.4.85)
- Nmap scan report for olin312-01.mathcs.carleton.edu (137.22.4.87)
- Nmap scan report for olin310-09.mathcs.carleton.edu (137.22.4.88)
- Nmap scan report for olin310-13.mathcs.carleton.edu (137.22.4.94)
- Nmap scan report for olin310-is.mathcs.carleton.edu (137.22.4.95)
- Nmap scan report for awb68130.mathcs.carleton.edu (137.22.4.96)
- Nmap scan report for mmontee68381.mathcs.carleton.edu (137.22.4.98)
- Nmap scan report for olin308-10.mathcs.carleton.edu (137.22.4.100)
- Nmap scan report for olin208-02.mathcs.carleton.edu (137.22.4.102)
- Nmap scan report for olin308-09.mathcs.carleton.edu (137.22.4.105)
- Nmap scan report for olin304-09.mathcs.carleton.edu (137.22.4.106)
- Nmap scan report for olin308-08.mathcs.carleton.edu (137.22.4.107)
- Nmap scan report for olin210cs70693.mathcs.carleton.edu (137.22.4.110)
- Nmap scan report for olin302-03.mathcs.carleton.edu (137.22.4.111)
- Nmap scan report for olin302-02.mathcs.carleton.edu (137.22.4.113)
- Nmap scan report for olin304-01.mathcs.carleton.edu (137.22.4.115)
- Nmap scan report for olin308-06.mathcs.carleton.edu (137.22.4.118)
- Nmap scan report for olin308-02.mathcs.carleton.edu (137.22.4.121)
- Nmap scan report for olin308-01.mathcs.carleton.edu (137.22.4.122)
- Nmap scan report for olin308-03.mathcs.carleton.edu (137.22.4.125)
- Nmap scan report for olin308-05.mathcs.carleton.edu (137.22.4.127)
- Nmap scan report for maize.mathcs.carleton.edu (137.22.4.131)
- Nmap scan report for olin312-07.mathcs.carleton.edu (137.22.4.133)
- Nmap scan report for olin321-62195.mathcs.carleton.edu (137.22.4.139)
- Nmap scan report for wcc03168380.its.carleton.edu (137.22.4.141)
- Nmap scan report for olin335-01.mathcs.carleton.edu (137.22.4.142)

- Nmap scan report for dhurlber68123.its.carleton.edu (137.22.4.147)
- Nmap scan report for olin319-62183.mathcs.carleton.edu (137.22.4.148)
- Nmap scan report for olin327-62232.mathcs.carleton.edu (137.22.4.149)
- Nmap scan report for olin339-62200.mathcs.carleton.edu (137.22.4.157)
- Nmap scan report for awb1.mathcs.carleton.edu (137.22.4.175)
- Nmap scan report for dmusicant67927.mathcs.carleton.edu (137.22.4.185)
- Nmap scan report for olin304-02.mathcs.carleton.edu (137.22.4.188)
- Nmap scan report for olin335-02.mathcs.carleton.edu (137.22.4.191)
- Nmap scan report for t5.mathcs.carleton.edu (137.22.4.225)
- Nmap scan report for mtietesting.mathcs.carleton.edu (137.22.4.234)
- Nmap done: 256 IP addresses (77 hosts up) scanned in 1.89 seconds

  Quite a few ports open.

  In fact, there appears to be different ip addresses for each room and certain users in Olin and the CS dept.

- Here we see a similar level of interactions that nmap does.

  ARP, followed by TCP, DNS.

3. Port Scanning

- 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?

  MySQL and postgreSQL are both open on Metasploitable.

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

  22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)

  | 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)

RSA public key for that server, which enables secure messaging to the SSH port.

One service I've never heard of before is rpcbind.

- 111/tcp open rpcbind   2 (RPC #100000)
- | rpcinfo:
- | program version   port/proto service
- | 100000 2   111/tcp   rpcbind
- | 100000 2   111/udp   rpcbind
- | 100003 2,3,4   2049/tcp   nfs
- | 100003 2,3,4   2049/udp   nfs
- | 100005 1,2,3   40743/udp   mountd
- | 100005 1,2,3   42937/tcp   mountd
- | 100021 1,3,4   39627/tcp   nlockmgr
- | 100021 1,3,4   41421/udp   nlockmgr
- | 100024 1   33484/udp   status
- |_ 100024 1   37874/tcp   status

> RPC is an inter-process communication technique that allows for client and server software to communicate on a network. IRpcbind accepts port reservations from local RPC services. rpcbind manages the addresses that are listening and the RPC program numbers it is prepared to serve.