CS338 Pen Test 1

Kuo Wang

May 2022

1 PASSIVE INFORMATION GATHERING

1. What domain did you investigate?
   - https://stmtuned.com

2. What is its IP address?
   - 23.227.38.32

3. When does the domain's registration expire?
   - 2023-02-09T18:45:32Z

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.)
   - Being that the website itself is shabby and I expect some poor security practices, I got some interesting information.
   - STMTuned is a small business ran by a Shawna Susice from Spencerport, NY.
   - The server is hosted by a very basic looking hosting/address service aplus.net
   - Furthermore, aplus.net is contracted by Shopify, which Shawna probably deals with.

2 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).

   - kuo-homePC (192.168.88.1)
   - 192.168.88.2
   - 192.168.88.128
   - 192.168.88.129

2. What entities do those IP addresses represent?
   - Each entity represent a "machine" that's on the local machine. The device could be my computer itself or some virtual machines.

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.)
   - For each address x that follows 192.168.88.¡0-255¿, nmap asks if anyone has address x, through a broadcast.
   - If there is a hit on the network for x, the machine on x will do TCP handshake to Kali to establish connection. Then, the machine on x sends a series of TCP query responses to Kali.

4. Repeat the previous three bullets, but for the 137.22.4.0/24 network. (Note that your results will be different if you execute nmap while connected to the Carleton network than if you're not connected. Either choice is fine with me.)

5. List of hosts up (77 of them):
   137.22.4.5
   137.22.4.15
   137.22.4.21
   137.22.4.30
   137.22.4.31
   137.22.4.32
   137.22.4.34
   137.22.4.35
   137.22.4.37
   137.22.4.38
   137.22.4.39
   137.22.4.40
   137.22.4.41
   137.22.4.42
   137.22.4.43
   137.22.4.46
   137.22.4.49
   137.22.4.54

137.22.4.56
137.22.4.57
137.22.4.58
137.22.4.59
137.22.4.60
137.22.4.61
137.22.4.63
137.22.4.65
137.22.4.66
137.22.4.67
137.22.4.70
137.22.4.71
137.22.4.72
137.22.4.73
137.22.4.75
137.22.4.77
137.22.4.78
137.22.4.79
137.22.4.80
137.22.4.82
137.22.4.83
137.22.4.85
olin312-01.mathcs.carleton.edu (137.22.4.87)
olin310-09.mathcs.carleton.edu (137.22.4.88)
olin310-13.mathcs.carleton.edu (137.22.4.94)
olin310-is.mathcs.carleton.edu (137.22.4.95)
mmontee68381.mathcs.carleton.edu (137.22.4.98)
137.22.4.100
olin208-02.mathcs.carleton.edu (137.22.4.102)
olin308-09.mathcs.carleton.edu (137.22.4.105)
olin304-09.mathcs.carleton.edu (137.22.4.106)
olin308-08.mathcs.carleton.edu (137.22.4.107)
olin210cs70693.mathcs.carleton.edu (137.22.4.110)
olin302-03.mathcs.carleton.edu (137.22.4.111)
olin308-07.mathcs.carleton.edu (137.22.4.112)
olin302-02.mathcs.carleton.edu (137.22.4.113)
olin304-01.mathcs.carleton.edu (137.22.4.115)
137.22.4.118
olin308-02.mathcs.carleton.edu (137.22.4.121)
olin308-01.mathcs.carleton.edu (137.22.4.122)
137.22.4.123
olin308-03.mathcs.carleton.edu (137.22.4.125)
olin308-05.mathcs.carleton.edu (137.22.4.127)
olin312-07.mathcs.carleton.edu (137.22.4.133)
olin321-62195.mathcs.carleton.edu (137.22.4.139)
wcc03168380.its.carleton.edu (137.22.4.141)
137.22.4.142
olin319-62183.mathcs.carleton.edu (137.22.4.148)

olin327-62232.mathcs.carleton.edu (137.22.4.149)
olin339-62200.mathcs.carleton.edu (137.22.4.157)
137.22.4.164
wcc138-04r.its.carleton.edu (137.22.4.165)
wcc138-03r.its.carleton.edu (137.22.4.173)
wcc138-02r.its.carleton.edu (137.22.4.174)
awb1.mathcs.carleton.edu (137.22.4.175)
olin304-02.mathcs.carleton.edu (137.22.4.188)
137.22.4.191
t5.mathcs.carleton.edu (137.22.4.225)
137.22.4.234

6. Entities:
   - Each address represent a machine on the network of 137.22.4.0, which is Carleton's network.

7. What does nmap do?
   - For each address x on 137.22.4.0, nmap sends a TCP SYN request.
   - When there is a hit, address x's machine will produce a response in time, be it SYN RST or SYN ACK.

3 PORT SCANNING

1. Ports opened on MSF:

    - 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

2. What database server(s) is/are available on Metasploitable?
   - postgreSQL and mySQL

3. 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
   - SSH server uses a host key to verify that the correct host is being connected to by the client. It is an authentication device.

4. Describe a service
   - microsoft-ds
   - microsoft-ds is a service that enables Windows networks to share resources such as a printer or some files through Server Message Block protocol.
   - It can also enable commands to be executed remotely, sometimes without authorization.