Brian Rhee

- What domain did you investigate?
    - CVS.COM
- What is its IP address?
    - 23.46.189.181
- When does the domain's registration expire?
    - Registry Expiry Date: 2023-01-31T05:00:00Z
    - Registrar Registration Expiration Date: 2023-01-31T00:00:00+0000
- 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.)
    - The whois command allowed me to identify the registrant organization, CVS Pharmacy, Inc., and the street, city, state, and postal code of the registrant. Also, I was able to find out the phone and fax number of the CVS Health Corporate Office, which is presumably the entity that applied for the cvs.com domain. Finally, I was able to identify the email the registrant used to apply for the cvs domain.
    - I also learned that the netblock owner (who apparently is the "datacenter/ISP which owns that range of IP address for which the site is hosted with" according to https://www.webhostingtalk.com/showthread.php?t=142611) of cvs.com is Akamai International, BV, which is a company based in the Netherlands
- List the IP addresses for all the active hosts you found on the local network
    - 192.168.237.1
    - 192.168.237.2
    - 192.168.237.128
    - 192.168.237.129
- What entities do those IP addresses represent?
    - 192.168.237.129 must represent Metasploitable on my machine because the IP address did not appear in the nmap report when Metasploitable was closed, and only appeared after I opened Metasploitable.
    - 192.168.237.128 represents our server
    - Because the ".1" ending on an IP address often represents "a gateway or router on a particular network" (https://www.iusmentis.com/technology/tcpip/ipaddress/), I believe 192.168.237.1 represents the gateway in our local network.
    - 192.168.237.2 remains a mystery
- 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.)
    - First, nmap pings each possible IP address in the local network. "Each possible IP address" in our case is all the IP addresses with the same first 24 bits. Pinging occurs by our server sending out ARP broadcasts to each of these addresses.

    - If an address is responsive, our server will establish a TCP connection by sending a [SYN] request to the host. Afterwards, the connection will be closed by way of a [RST, ACK] response sent back to our server.
    - One thing I am unsure of is how the process of pinging works, since the ARP broadcasts for the IP addresses that we end up sending [SYN] requests to don't show up in Kali
- List the IP addresses for all the active hosts you found on the local network
    - 137.22.4.5
    - 137.22.4.17
    - 137.22.4.20
    - 137.22.4.22
    - 137.22.4.72
    - 137.22.4.131
    - 137.22.4.175
- What entities do those IP addresses represent?
    - 137.22.4.5
        - elegit.mathcs.carleton.edu
    - 137.22.4.17
        - perlman.mathcs.carleton.edu.
    - 137.22.4.20
        - *Unavailable*
    - 137.22.4.22
        - *Unavailable*
    - 137.22.4.72
        - olin310-07.mathcs.carleton.edu
    - 137.22.4.131
        - maize.mathcs.carleton.edu
    - 137.22.4.175
        - awb1.mathcs.carleton.edu
- 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.)
    - Unlike the previous wireshark nmap recording, this recording contained no ARP packets. Instead, there were a total of 1366 packets containing a mixture of DNS, MDNS, and TCP protocols.
    - In this wireshark recording, we can see that our server sends out TCP [SYN] requests to every possible host with endings between 137.22.4.1 to 137.22.4.256.
    - We then receive [RST, ACK] TCP packets back from each of the hosts we reach out to. This confuses me, because in the previous nmap, we only received [RST, ACK] packets from the hosts that we were able to successfully ping.

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

    - 22/tcp – ssh
    - 23/tcp – telnet
    - 25/tcp – smtp
    - 53/tcp – domain
    - 80/tcp – http
    - 111/tcp – rpcbind
    - 139/tcp – netbios-ssn
    - 445/tcp – microsoft-ds
    - 512/tcp – exec
    - 513/tcp – login
    - 514/tcp – shell
    - 1099/tcp – rmiregistry
    - 1524/tcp – ingreslock
    - 2049/tcp – nfs
    - 2121/tcp – ccproxy-ftp
    - 3306/tcp – mysql
    - 5432/tcp – postgresql
    - 5900/tcp – vnc
    - 6000/tcp – X11
    - 6667/tcp – irc
    - 8009/tcp – ajp13
    - 8180/tcp – unknown

- What database server(s) is/are available on Metasploitable?
    - Mysql, postgresql, and (possibly) ingreslock. Ingreslock is used as a tool in conjunction with the Ingres database, so it is not technically a database server itself.
- What is the value of the RSA SSH host key? What is the host key for?
    - 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    - The host key allows a client to identify and ensure that they are connecting to their intended host. In this sense, the host key is a unique identifier for a specific host.
- Pick one of the open ports that has a service you have never heard of, and explain what the service does.
    - Smtp stands for Simple Mail Transfer Protocol. The service simply allows two servers to interact by sending and receiving mail. Apparently, this service is valuable because it can be used to resolve issues like “email deliverability” and “IP blacklisting” (https://www.duocircle.com/content/smtp-email/smtp-server-example)