Kaeden Berg, Kitty Tyree

Passive information gathering

- What domain did you investigate?
    - https://jeffondich.com/
- What is its IP address?
    - 45.79.89.123
- When does the domain's registration expire?
    - March 23, 2022
- 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 learned the website was created in 2015
    - It was registered by a company called Contact Privacy Inc. based in Toronto, which is a company that helps hide a registered user's data
        - Does Contact Privacy Inc technically own the domain? Could they change or sell it legally? I'm guessing the users have a contract.
        - If it wasn't for this, we could find a person's address, phone number, email, and even fax!
    - The website's server is based through Linode, a cloud computing server host

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).
    - 10.0.2.1
    - 10.0.2.4
    - 10.0.2.15
- What entities do those IP addresses represent?
    - 10.0.2.1 - Our virtual machine's NIC
    - 10.0.2.4 - metasploitable
    - 10.0.2.15 - our machine
- 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 began sending out ARP protocols to determine if there are any hosts at the IP addresses. It sends one for each of the 256 variations of the IP address.
    - When there was a response, there was a SYN, ACK interaction.
    - On occasion, there were some resets sent [RST,ACK]

    - Then they performed DNS lookups for each device
- Same question, but for the 137.22.4.0/24 network.
    - 137.22.4.5, and we know it is a subserver at Carleton and it is believed (with 92% certainty) that the OS it runs is " British Gas GS-Z3 data logger" and this IP address has 2 open ports
    - 137.22.4.131, and we know it is a subserver at Carleton and it is believed (with 92% certainty as well) that the OS it runs is "British Gas GS-Z3 data logger" But this IP address has 3 open ports
    - Both of these OS detections are unreliable, so it's doubtful that the servers are actually running British Gas Embedded
    - Steps:
        - TCP Handshake
        - A reset when successful(for reasons we do not understand yet, one guess is to cover our tracks?)
        - Our machine sent a whole lot of SYN packets from different ports to the same port (80)
        - There were listening in on a few ports

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?
    - ftp, ssh, smtp, rpcbind, mysql, postgresql,vnc,irc,http
- What is the value of the RSA SSH host key? What is the host key for?
    - We should not tell you this normally, but it should be safe for metasploitable, 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. (It's not possible to hack through a virtual machine right?)
    - The host key is used as a private key in RSA
- Pick one of the open ports that has a service you have never heard of, and explain what the service does.
    - Port 25 has smtp, which is the simple mail transfer protocol, used to send and receive e-mail between servers. You send it to a specific address at a specific server, and the server provider, such as gmail or AOL, will download it and put it in the recipient's mailbox. It will send the message back if it can't be delivered. Source: https://sendgrid.com/blog/what-is-an-smtp-server/