Ethan Li & Adela Dujsikova

1. Passive information gathering
    - What domain did you investigate?
        - wikipedia.org
    - What is its IP address?
        - 208.80.153.224
    - When does the domain's registration expire?
        - 2023-01-13T00:12:14Z
    - 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 get the names, phone numbers, and email addresses of people working in certain sectors in Wikipedia. We also got the physical address of the Wikipedia building.

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).
        - nmap -sn 10.0.2.255/24
        - Starting Nmap 7.91 (https://nmap.org) at 2021-05-09 22:18 EDT
        - Nmap scan report for **10.0.2.1**
        - Host is up (0.00050s latency).
        - Nmap scan report for **10.0.2.2**
        - Host is up (0.00085s latency).
        - Nmap scan report for **10.0.2.4**
        - Host is up (0.00090s latency).
        - Nmap scan report for **10.0.2.15**
        - Host is up (0.0016s latency).
        - Nmap done: 256 IP addresses (4 hosts up) scanned in 2.81 seconds
    - What entities do those IP addresses represent?
        - 10.0.2.1 - default router IP
        - 10.0.2.2 - VirtualBox
        - 10.0.2.4 - Metasploitable
        - 10.0.2.15 - Kali

- 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 the default router IP (10.0.2.1), a [SYN] packet is sent which is met by an [ACK, SYN] to which no [ACK] was sent. ARP packets were broadcasted asking for the MAC address of every IP address from 10.0.2.2 to 10.0.2.255. If ARP packets are sent back containing the MAC address, [SYN] packets are sent by kali (us) to initiate a TCP three-way handshake. We observed three responses to the [SYN] packets: 1) Destination unreachable (Protocol unreachable); 2) [RST, ACK]; 3) [SYN, ACK], followed by [ACK] and [RST, ACK] both responded by kali. For the latter two responses, the host at the corresponding IP address was regarded as active.
- Same question, but for the 137.22.4.0/24 network. List of active hosts IP addresses:
    - nmap -sn 137.22.4.0/24
    - Starting Nmap 7.91 (https://nmap.org) at 2021-05-09 22:41 EDT
    - Nmap scan report for elegit.mathcs.carleton.edu (**137.22.4.5**)
    - Host is up (0.0014s latency).
    - Nmap scan report for perlman.mathcs.carleton.edu (**137.22.4.17**)
    - Host is up (0.0014s latency).
    - Nmap scan report for ada.mathcs.carleton.edu (**137.22.4.19**)
    - Host is up (0.0012s latency).
    - Nmap scan report for **137.22.4.20**
    - Host is up (0.0013s latency).
    - Nmap scan report for **137.22.4.22**
    - Host is up (0.0012s latency).
    - Nmap scan report for cmc304-06.mathcs.carleton.edu (**137.22.4.111**)
    - Host is up (0.0011s latency).
    - Nmap scan report for mtietest2.mathcs.carleton.edu (**137.22.4.146**)
    - Host is up (0.0023s latency).
    - Nmap done: 256 IP addresses (7 hosts up) scanned in 3.17 seconds
- What entities?
    - 137.22.4.5 - elegit.mathcs.carleton.edu
    - 137.22.4.17 - perlman.mathcs.carleton.edu
    - 137.22.4.19 - ada.mathcs.carleton.edu

    - 137.22.4.20 - *no useful information given by nmap*
    - 137.22.4.22 - *no useful information given by nmap*
    - 137.22.4.111 - cmc304-06.mathcs.carleton.edu
    - 137.22.4.146 - mtietest2.mathcs.carleton.edu
  - Steps that nmap took:
    - First, a DHCP request is sent to 10.0.2.3 (which was unavailable in the earlier section) and ACK'ed; Then, hundreds of TCP [SYN] packets were sent from kali (10.0.2.15) to the address between 137.22.4.1 and 137.22.4.255. This time only two types of responses from the targeted IP address to the [SYN] packets were observed: 1) [RST, ACK], or 2) [SYN, ACK], followed by [ACK] and [RST, ACK] both responded by kali. A couple dozen IP addresses responded with [RST, ACK], of which only few were considered active hosts. However, it seems like every IP address that responded with [SYN, ACK] and henceforward [RST, ACK] sent by kali are listed as active

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)?
    - **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
- 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 is for authenticating computers in the SSH protocol. The host key above is the public host key, the private key is known only by the host.
- Pick one of the open ports that has a service you have never heard of, and explain what the service does.
    - ccproxy-ftp - Proxy Server CCProxy is easy-to-use and powerful Internet connection sharing software. CCProxy can support broadband, DSL, dial-up, optical fiber, satellite, ISDN and DDN connections, it helps you build your own proxy server and share Internet connection within the LAN efficiently and easily.