Soren DeHaan and Carl Tankersley

Part 1

1. carleton.edu
2. 137.22.94.116
3. 31 July 2021
4. The registrant is Carleton College (complete with full street address), the administrative contact is Chris Dlugosz, and their phone number is (507) 222 5999. The domain record was activated on 2 June 1986, and the ip address was registered 11 October 1989.

Part 2

1. IP addresses on the network:
    a. 10.0.2.1 (Default gateway)
    b. 10.0.2.4 (Metasploitable)
    c. 10.0.2.15 (Kali)
2. Nmap sends a SYN request to ports 80 and 443, responding to a SYN ACK if present, for the TCP handshake. It then resets both ports, and sends a DNS query to the network authority to check if the address has a name (for instance, maize.mathcs.carleton.edu), which it would then display.
3. The following are the 3 results that turned up for both of Soren's runs of "nmap -sn 137.22.4.0/24"- Carl had a full 256 hosts that showed up with the identical command. We're uncertain what caused the difference, but it may be due to VPN?
    a. 137.22.4.5 (elegit.mathcs.carleton.edu)
    b. 137.22.4.17 (perlman.mathcs.carleton.edu)
    c. 137.22.4.131 (maize.mathcs.carleton.edu)

Part 3

1. Here they be:
    a. 21/tcp open ftp
    b. 22/tcp open ssh
    c. 23/tcp open telnet
    d. 25/tcp open smtp
    e. 53/tcp open domain
    f. 80/tcp open http
    g. 111/tcp open rpcbind
    h. 139/tcp open netbios-ssn
    i. 445/tcp open microsoft-ds
    j. 512/tcp open exec
    k. 513/tcp open login
    l. 514/tcp open shell
    m. 1099/tcp open rmiregistry
    n. 1524/tcp open ingreslock
    o. 2049/tcp open nfs
    p. 2121/tcp open ccproxy-ftp

    q. 3306/tcp open mysql
    r. 5432/tcp open postgresql
    s. 5900/tcp open vnc
    t. 6000/tcp open X11
    u. 6667/tcp open irc
    v. 8009/tcp open ajp13
    w. 8180/tcp open unknown
2. MySQL and PostgreSQL on ports 3306 and 5432, respectively
3. The RSA SSH host key is 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3, which is used to establish a secure SSH connection with the host. It can be used for a symmetric key exchange, after which point the host will be trusted.
4. The smtp (Simple Mail Transfer Protocol) service on port 25 corresponds with a mail server. Port 25 is common, but not always used, and port 587 is generally used for outgoing mail. There used to be no authentication process, allowing for trivial spoofing, and now additional systems are required for verification, including DKIM, as seen in all those “e2ma-verification=” things.