Kevin Cleland and Jake Martens

Part 1
1. carleton.edu
2. 137.22.198.41
3. 31-July-2021
4. The whois command returned contact info for the registrant, administrative contact, technical contact, and the educause database, which registers .edu domains. nslookup also returned info for abuse handling, tech handling, and the range of IP addresses.

Part 2
Local Network:
1. The Ip addresses (for active hosts) are 10.0.2.1, 10.0.2.2, 10.0.2.4, and 10.0.2.15.
2. The addresses 10.0.2.1 and 10.0.2.2 are other devices connected to the same network as our virtual Kali machine. They could be the network gateway or a server of some sort. 10.0.2.4 is the metasploitable machine, and the other address (10.0.2.15) is our own machine.
3. For every possible IP address it send out a who has (IP address) broadcast, and says to tell (Our IP address). If it gets a response from the IP adress it concludes the server is up.

Carleton's 137.22.4.0 network:
1.137.22.4.5, 137.22.4.17, 137.22.4.19, 137.22.4.20, 137.22.4.22
, 137.22.4.31, 137.22.4.32, 137.22.4.34
, 137.22.4.35, 137.22.4.37, 137.22.4.42, 137.22.4.46, 137.22.4.48, 137.22.4.49, 137.22.4.60, 137.22.4.61, 137.22.4.66, 137.22.4.75, 137.22.4.77, 137.22.4.87, 137.22.4.91, 137.22.4.96, 137.22.4.98, 137.22.4.101, 137.22.4.102, 137.22.4.106, 137.22.4.110, 137.22.4.113, 137.22.4.114, 137.22.4.147, 137.22.4.155, 137.22.4.175, 137.22.4.182, 137.22.4.188
2. These represent various devices connected to Carleton's Math/CS server. Most of them appear to be lab computers, although we also noticed two professors who were online as well as connections in the Weitz and the Perlman museum.
3. This time our machine attempted the threeway TCP handshake with each IP address on the desired network. The ones that were active responded with a TCP [RST, ACK] packet. The server then sends DNS querry back to the servers that responded (except we noticed that they seem to all be going through two servers that we're guessing are routers for the department), and finally they send back DNS responses.

Part 3
1. 21/tcp - 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

2. There's an SSH server on 22, there's an HTTP server on port 80, irc.Metasploitable.LAN is on 6667, and maybe a mySQL server on port 3306. There's a lot of things listed on these ports, and we're not entirely sure if anything else constitutes a server.
3. 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. The host key is needed to authenticate the idneitty of the server using the PKI structure we've talked about. It's also theoretically for people who want to send something encrypted to the server.
4. We looked at port 1099 (rmiregistry). It's purpose is to allow java programs on different servers to communicate with each other over the connection. It seems to only be for java problems though.