————-passive information gathering————

1. I investigated CARLETON.EDU
2. 137.22.94.116
3. 7.31.2021
4. The domain name was registered on 12.11.1989. 507-646-4841 and cdlugosz@carleton.edu can be used to contact the network manager

————-host detection———————

1. 10.0.2.1, 10.0.2.2, 10.0.2.4, 10.0.2.15
2. 10.0.2.15 is the ip address of kali. 10.0.2.1 is the localhost, 10.0.2.2 is the special alias to host loopback, 10.0.2.4 the servers. 10.0.2.4 is Metasploitable
3. From the localhost of Kali, it sends out TCP SYN packets to known destination hosts, and active hosts would reply back a RST,ACK response. It also sends out ARP requests to broadcast address to find possible ip addresses with the same first 24 bits and look for a reply.
    ———for 137.22.4.0/24———
    1. 137.22.4.5, 137.22.4.17, 137.22.4.20, 137.22.4.22
    2. They are all servers. 137.22.4.5 represents elegit.mathcs.carleton.edu, and 137.22.4.17 represents perlman.mathcs.carleton.edu
    3. Kali sends TCP SYN requests to possible destinations, showing that it wants to talk. The available servers would reply back a SYN ACK response to agree on communication. Kali would then send a RST, ACK response to not complete TCP handshake.

————port scanning————-

1. Port 21 for ftp, port 22 for ssh, port 23 for telnet, port 25 for smtp, port 53 for domain, port 80 for http, port 111 for rpcbind, port 139 for netbios-ssn, port 445 for netbios-ssn, port 512 for exec, port 513 for login, port 514 for tcpwrapped, port 1099 for java-rim, port 1524 for bindshell, port 2049 for nfs, port 2121 for ftp, port 3306 for mysql, port 5432 for postgresql, port 5900 for vnc, port 6000 for x11, port 6667 for irc, port 8009 for ajp13, port 8180 for http
2. Mysql, postgresql
3. 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3. It's the server's public key. It is for decrypting messages from the ssh host when connecting to it, so we can make sure it is the host we want to connect to.
4. Port 25/smtp server is for sending emails. Like a normal server, it can process the email we want to send and find the correct server, builds a connection with it, and send the message information. It cannot receive emails.