Emma Roskopf and Lily Haas
Worked with Ashok, to troubleshoot and discuss

**1. Passive information gathering**
Domain picked: MINECRAFT.NET
What is its IP address: 99.86.60.51
When does the domain's registration expire: 2023 05 18, May 18th, 2023

Other things

- We have their fax number. I don't know what to do with this information.
    - We can also send them letters (They live on One Microsoft Way, Redmond, WA, 98052)
    - I really didn't think we'd be able to pull information like phone numbers and addresses from just a domain name. Seems like weird information to store there
- Using IP address instead
    - We've got even more weird data on Minecraft
        - They have an Abuse Phone? Probably just a complaint line, but what a weird name
    - They're using Amazon web services
- Using netcraft
    - Minecraft has two web trackers that are both by Adobe, and both are considered analytics (one of them have advertising in the name also)
    - It's not using HTTPS
    - The server location pointed to the UK/Ireland/very western Europe and the US

**2. Host detection**
The nmap tries to communicate with all the other IP addresses on the local network by pinging them.[1] It goes through them sequentially (the last 8 bits) and figures out what's running at that address. It is looking for active ones (the ones that respond to the ping), that it then has a quick interaction with them (TCP SYN, they return TCP ACK) to make sure it's actually active.

List the IP addresses for the active hosts we found on the local network: 192.168.178.1, 192.168.178.2, 192.168.178.129 (myself)
What entities do these represent: We can't figure out what the first two are, we pinged them and it returned NODOMAIN. The third one is myself, because I'm on the local network. The 192.168.178.2 is doing DNS communications (queries). Both of the others are doing TCP acknowledgements of each other.
For each IP address what steps did nmap take?

- It seems like it sends a packet and sees if it responds

[1] nmap.org

- If it doesn't, it broadcasts that there's nothing there
- If it gets a response, it both will acknowledge the connection and nmap returns it as an open host

Repeat for 137.22.4.0/24 network

- We got a lot of active hosts, perlman, the olin machines, maize, t5, mtietesting (Mike Tie), wcc (weitz lab computers), and mmontee68381 (MurphyKate Montee)
    - We got 74 hosts up
    - There was too many to list all of the olin machines so we settled for listing the unique ones and just stating there's a LOT of olin machines on the local network
- We got a lot more TCP responses here, and some DNS here too

**3. Port scanning**

Testing hosts and seeing which one is metasploitable

- 192.168.178.1
    - Only 4 ports are open which seems fair
    - It's AirTunes (found out through nmap -A), so definitely not metasploitable
- 192.168.178.2
    - There are 1000 closed tcp ports
    - Probably not metasploitable
- 192.168.178.129
    - This one is my program, and it also has 1000 closed tcp ports
    - Probably not metasploitable
- We figured out at this step that Metasploitable on Lily's computer isn't visible from the /24 search. The last 16 bits of the IP address are different, not just the last 8. We didn't know that at the time, so we found out the IP address using ifconfig in metasploitable and confirmed this in kali (nmap of the suspected metasploitable address). The IP address is 192.168.64.2
    - Also in the details of "nmap -A 192.168.64.2" it states that various names of things are metasploitable

Metasploitable Info

- Metasploitable has 23 ports open (977 closed TCP ports)
    - 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
- Database servers
    - mysql, postgresql, domain (DNS) (seemed like there is a database of the domain names), rmiregistry (allows clients to get a reference to a remote service from a name, some searching mechanism at play), ingreslock (ingres is a database so ingreslock has something to do with ingres)
    - I found information by looking up the port name and looking through websites that explained what it was because with just the acronyms it's hard to figure out what it is. I tried to verify information with several sites after I figured out the full name of what's running on the port
        - I did find out which ports could have different attacks run on them, like botnet runs through irc which was kinda cool to learn, and ingreslock is a backdoor exploit
- Value of RSA SSH host key? What is the host key for?
    - Value: 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3
    - It's half of a public private key pair using RSA and this host key is the host's public key so that communications are authenticated and secure in SSH[2]
    - SSH clients store the public/host keys of hosts so that they can communicate with known entities
- Port 8180

---

2 https://www.ssh.com/academy/ssh/host-key#:~:text=A%20host%20key%20is%20a,are%20stored%20on%20SSH%20servers.

    - This just seems to be an open TCP port that has no real specified function. I'm assuming this is just to make metasploitable more vulnerable. I looked it up because it's the only one that's not labeled
- Port 8009 ajp13
    - This stands for Apache Jserv Protocol[3]
    - This is a protocol that allows communications between a web server through an application server
    - AJP has a lot of sensitive information, and things could be run on the application server via malicious requests if the port is not protected
    - This also makes sense because Apache is a web server software, so AJP has something to do with web servers

[3] https://en.wikipedia.org/wiki/Apache_JServ_Protocol