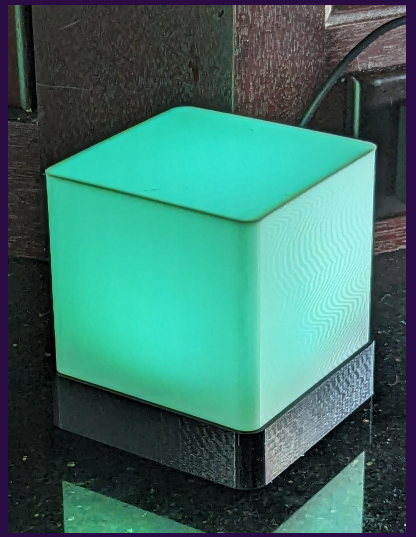
Welcome to the “Foxhunt” Game

How to use Nmap to find a hidden web server

- Fun way to learn about networks and devices.
- Find the IoT light box using different tools.
- Be the first to finish the hunt, and you’ll win a prize!
- Safety First: This is a game. Don't try this on any network without permission.
- What might you find in real life? Routers, IoT and other network devices.



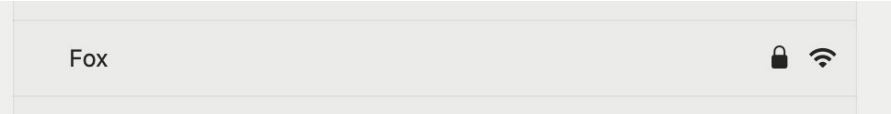
What is the IoT light box?

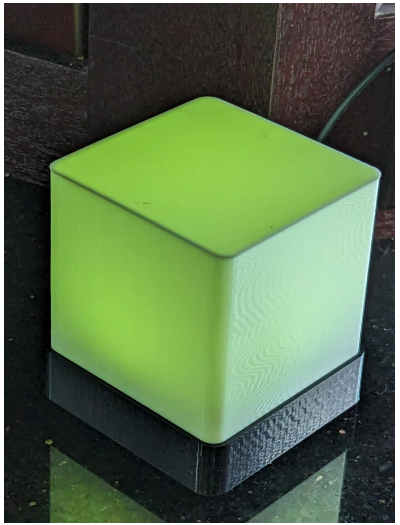
The IoT Light Box (The Fox)

- A cool device that connects to a Wi-Fi network.
- We use the WLED project to control its lights.
- We will make our own later in the class
- It gets a unique IP address on our network, which you'll need to find!

Connect to the Fox network

Now let’s join the Fox's Network with these easy steps:



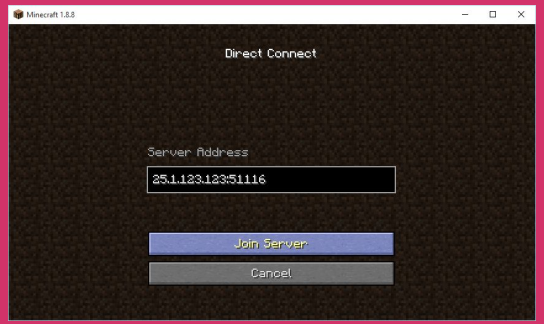


- Look for a Wi-Fi network named "**fox**"
- Connect to it with the password: **password123**

- Now, you are in the same "forest" as the fox!
- [Commonly used Windows-based network term. Often graphically presented as the border of a network with several groups of computers and entities listed or connected inside it.]

What is an IP address?

- It's like a parking space for cars, but for devices on a network.
- Or like using Direct Connect on Minecraft to access the private servers of other players
- Each device has a MAC address, a number like a license plate
- Every time a device joins a Wi-Fi network, it might get a different “parking spot”
- We'll use a tool called "arp-scan" to find all the IP addresses on this network



Using arp-scan

```
sudo apt install arp-scan
```

- This tool lists all the IP addresses in the "forest".
- ARP is a type of message we can send on a network to ask who is in each parking spot
- Devices on the network respond with their MAC address (license plate) and IP (parking space)
- It helps us see all the possible homes of the fox.

Understanding the IP range

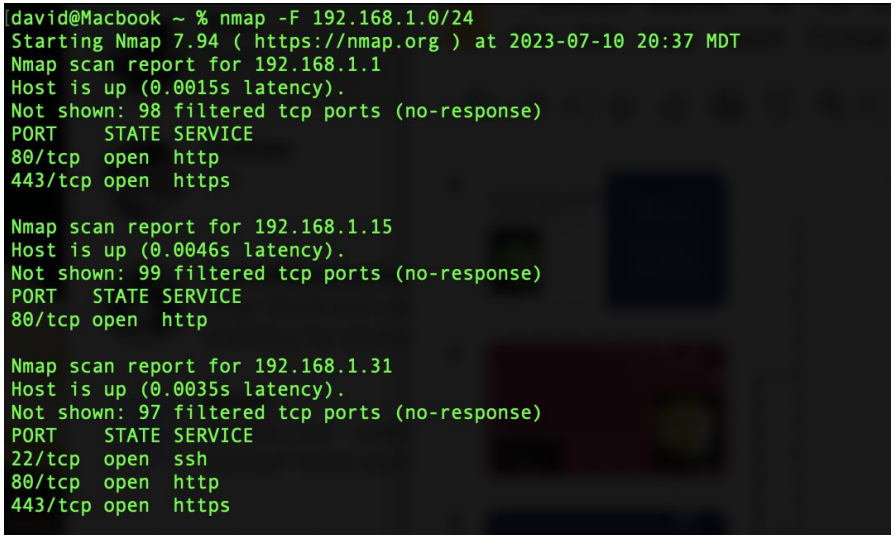
```
sudo apt install ipcalc
```

- To use the next tool, we need to find how big the network can be
- IPcalc tool helps us know the size of our "forest".
- It tells us the range of possible IP addresses.
- It's like knowing the boundary of the fox's habitat!
- Install IPcalc and take an IP address from our ARP scan
- Run “ipcalc (ip address)” to find the network range

```
david@Macbook ~ % ipcalc 192.168.1.151
Address:   192.168.1.151        11000000.10101000.00000001. 10010111
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.1.0/24       11000000.10101000.00000001. 00000000
HostMin:   192.168.1.1          11000000.10101000.00000001. 00000001
HostMax:   192.168.1.254        11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255        11000000.10101000.00000001. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

NMAP: The Fox Finder!

```
sudo apt install nmap
```



- NMAP is a tool that helps find devices in a network.
- It can tell if a device, like our fox, has an "open door" (port 80).
- In order to use it, we need to tell it where to look
- If we don’t it will check everywhere, and take a very long time

Using Nmap

- We tell NMAP to look for anything with port 80 open.
- It's like finding a fox's den with an open entrance!
- Now we use the network range we found with IPcalc
- The command for doing this is “sudo nmap (NetworkRange) -p open”

```
david@Macbook ~ % ipcalc 192.168.1.151
Address:   192.168.1.151          11000000.10101000.00000001. 10010111
Netmask:   255.255.255.0 = 24     11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255              00000000.00000000.00000000. 11111111
=>
Network:   192.168.1.0/24         11000000.10101000.00000001. 00000000
HostMin:   192.168.1.1            11000000.10101000.00000001. 00000001
HostMax:   192.168.1.254          11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255          11000000.10101000.00000001. 11111111
Hosts/Net: 254                    Class C, Private Internet
```

Different Doors: Ports

- Sometimes, devices have more than one "open door".
- We can also search for port 8080, 81, and 8081.
- Using --open with NMAP will only show us "dens" with open entrances!
- The command for this is “sudo nmap (IPRange) -p 80,8080,8081,81 --open”

Wrapping Up

Ready for the Foxhunt?

- Now you know how to find the fox's "home" on the network.
- You can use these tools to explore, but remember, only on allowed networks!
- Time to start the game. Happy Hunting!