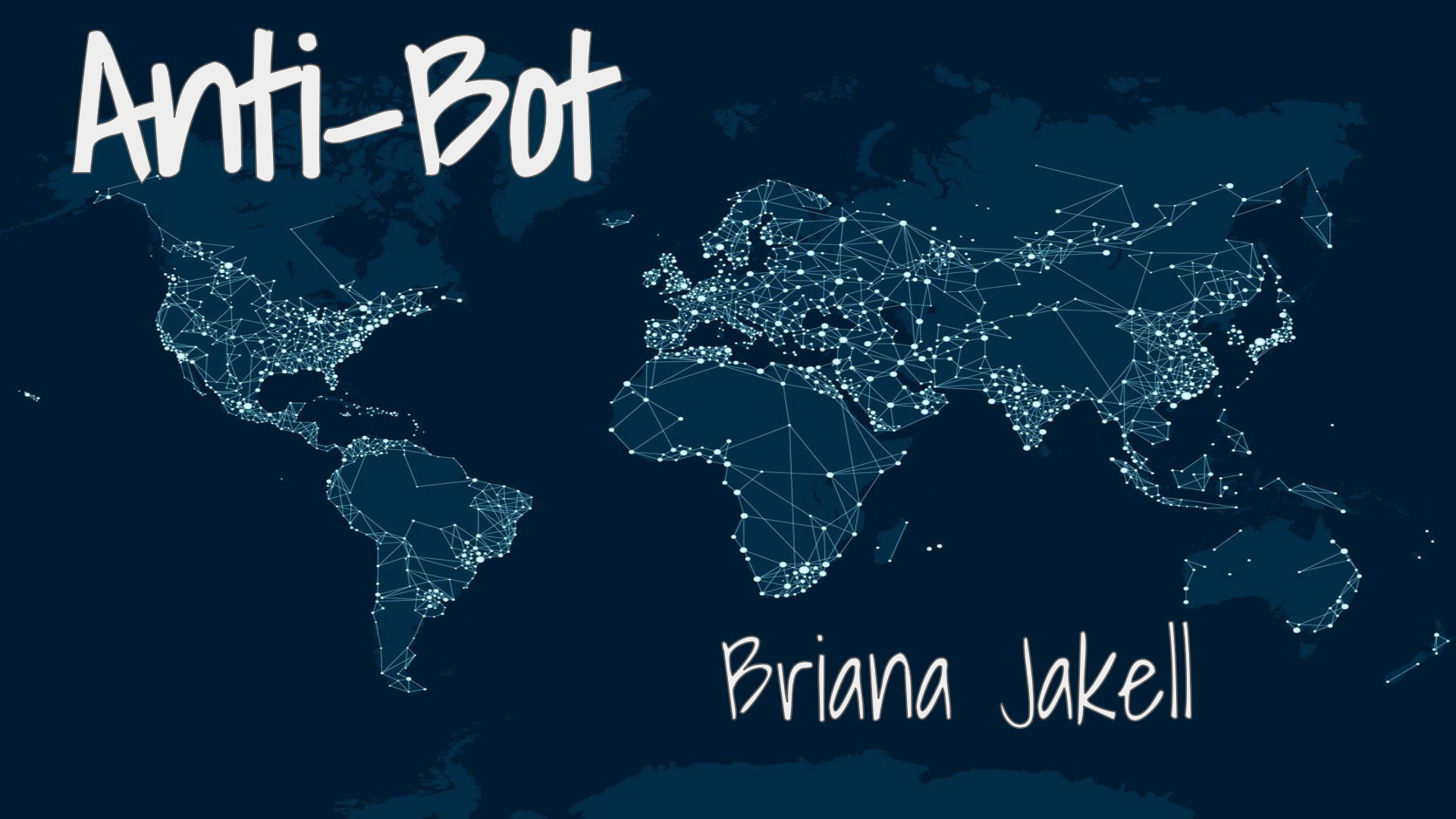
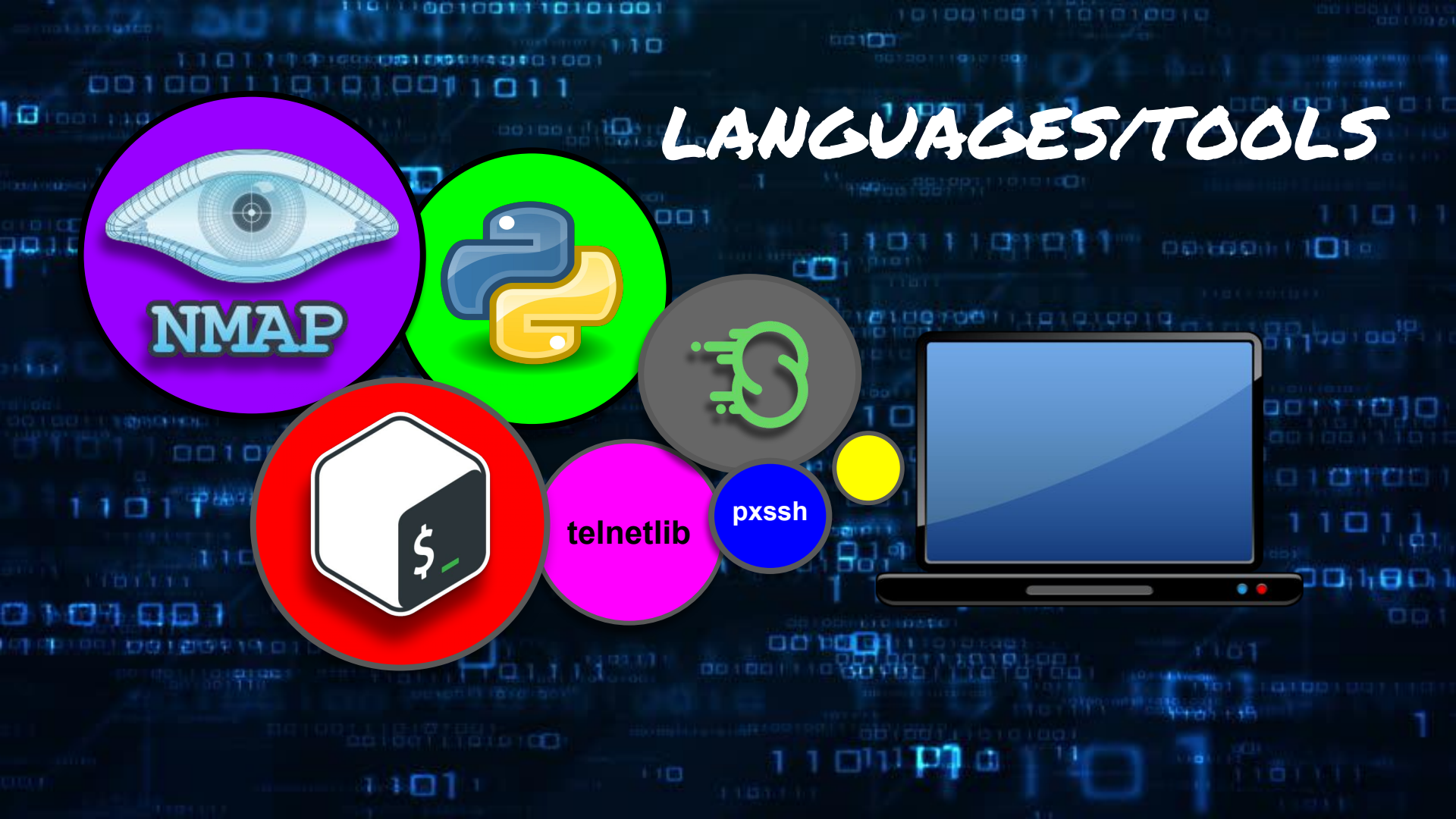
Anti-Bot



Briana Jakell

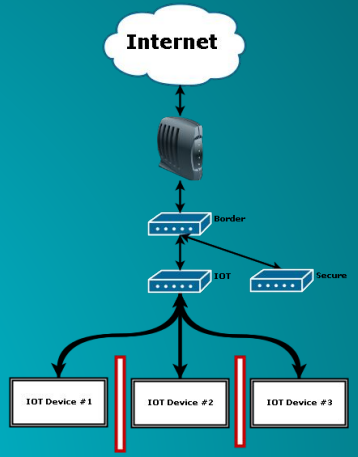
Inspiration

LANGUAGES/TOOLS



Challenges

- Which approach to take:
  - Do I reinvent the wheel?
  - Do I show better understanding?
- Finding hosts to exploit - Cost
  - Firmware updates
  - How much to spend to get new devices
- Efficiency
  - Scanning large number of hosts
  - Brute forcing
- Setting up VLAN with CLI/Script
  - Switch - no CLI
  - Mini router - Couldn't implement in a script



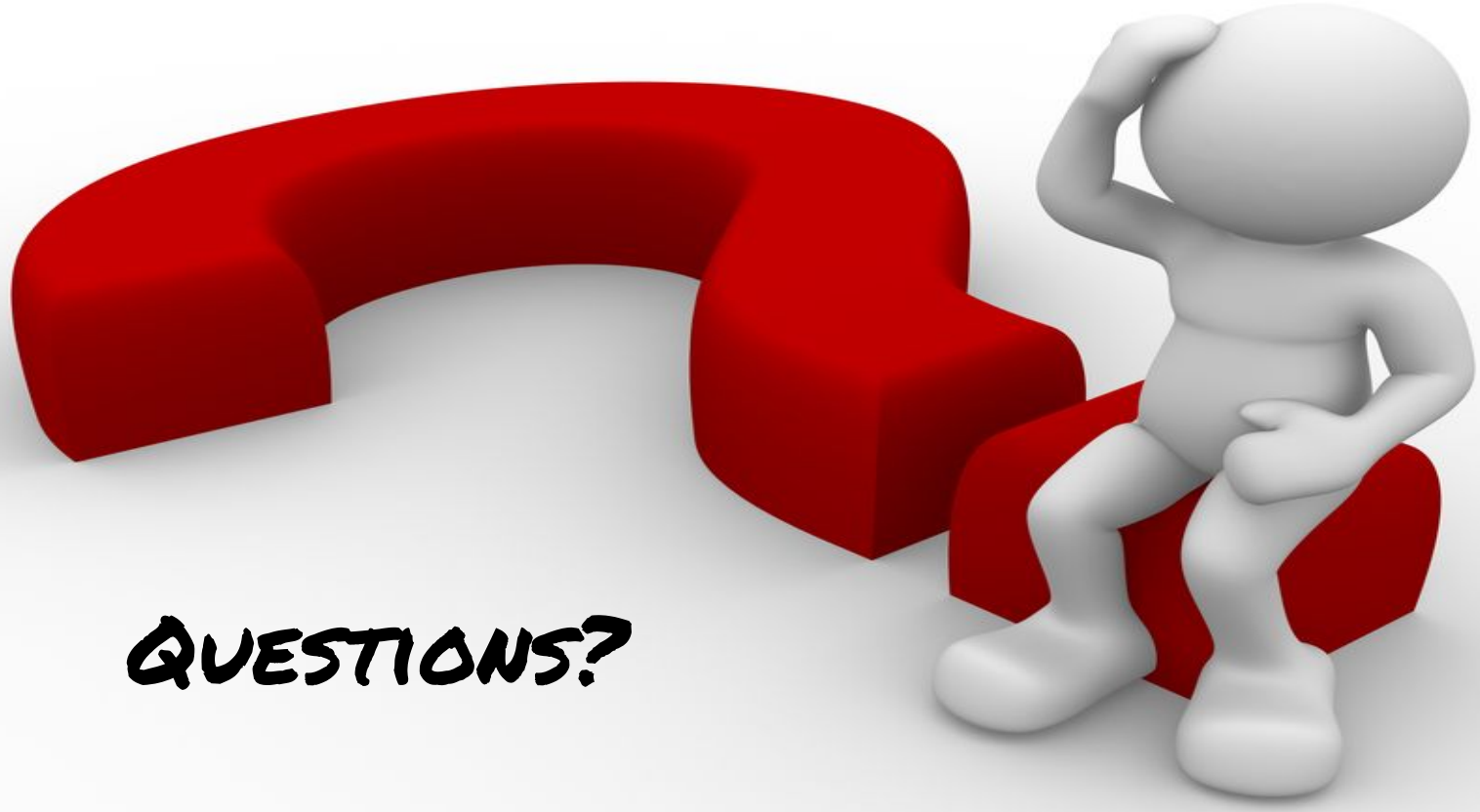
Demos

```
bjakell@HP-Spectre: ~/SeniorProject
bjakell@HP-Spectre:~$ cd SeniorProject/
bjakell@HP-Spectre:~/SeniorProject$ sudo python portScanner.py
[sudo] password for bjakell:
Enter target IP address: 192.168.1.22
Enter minimum port number: 1
Enter maximum port number: 25
Target is up, beginning scan...
Scan started at 23:50:18
```


```
bjakell@HP-Spectre:~/SeniorProject$ nmap -p 1-25 192.168.1.22

Starting Nmap 7.60 ( https://nmap.org ) at 2018-05-10 23:54 PDT
Nmap scan report for 192.168.1.22
Host is up (0.011s latency).

PORT   STATE  SERVICE
1/tcp  closed tcpmux
2/tcp  closed compressnet
3/tcp  closed compressnet
4/tcp  closed unknown
5/tcp  closed rje
6/tcp  closed unknown
7/tcp  closed echo
8/tcp  closed unknown
9/tcp  closed discard
10/tcp closed unknown
11/tcp closed systat
12/tcp closed unknown
13/tcp closed daytime
14/tcp closed unknown
15/tcp closed netstat
16/tcp closed unknown
17/tcp closed qotd
18/tcp closed msp
19/tcp closed chargen
20/tcp closed ftp-data
21/tcp closed ftp
22/tcp open   ssh
23/tcp open   telnet
24/tcp closed priv-mail
25/tcp closed smtp

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

What's Next

VLAN


Questions?