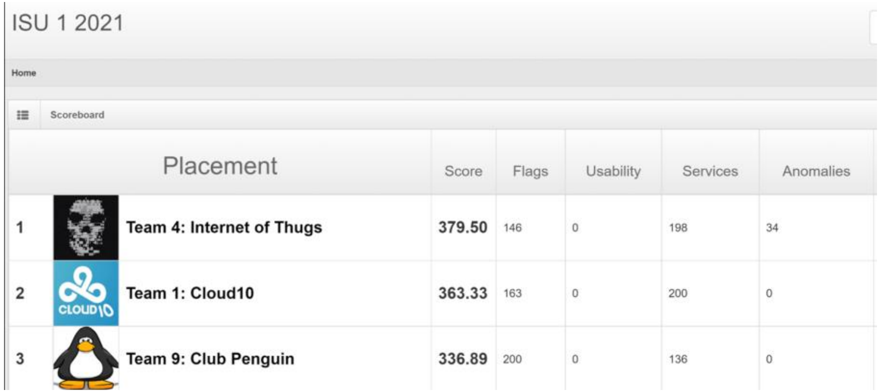
Week 6 Brief

10/19/21

Team Activities

- Participated in CDC
- Met with Doug Jacobson
- Created initial Design Document
- Researched bash scripting and possible initial setup steps for spinning up our VM

CDC summary



ISU 1 2021

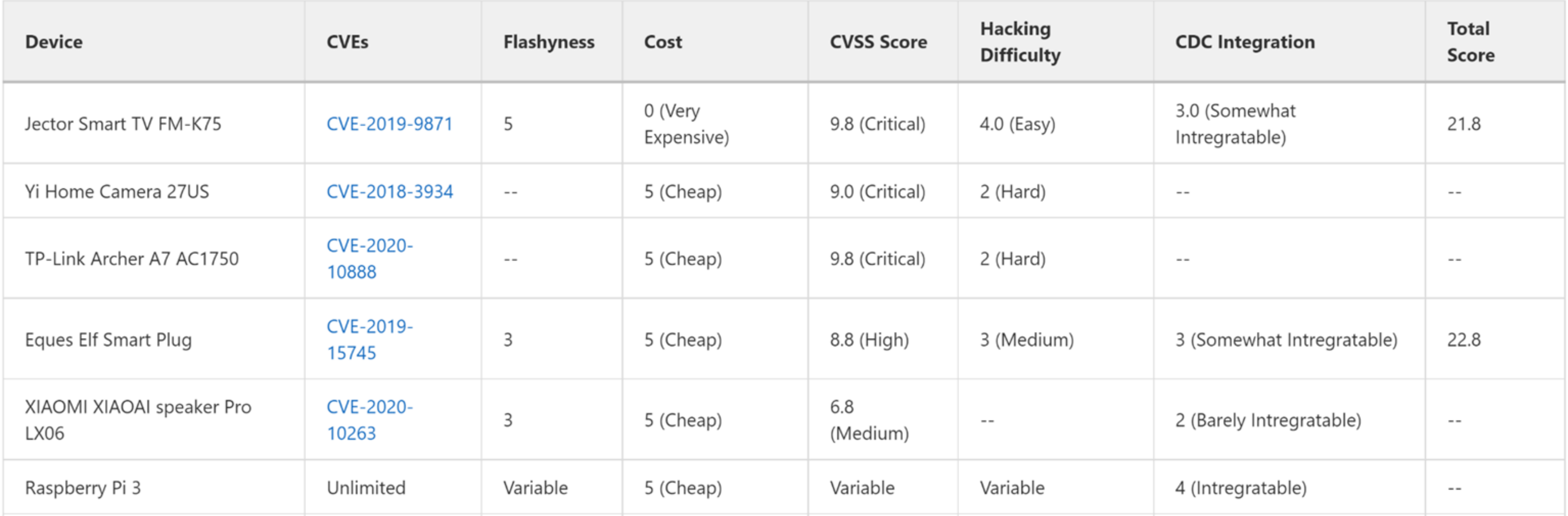
Placement		Score	Flags	Usability	Services	Anomalies
1	Team 4: Internet of Thugs	379.50	146	0	198	34
2	Team 1: Cloud10	363.33	163	0	200	0
3	Team 9: Club Penguin	336.89	200	0	136	0

- Everyone attended
- Did some very basic firewall securing
    - Ufw firewall configuring
    - Denied all incoming besides SSH and HTTP
    - Denied all outgoing (reverse shell)
- Mostly worked on anomalies
- Overall a good experience

Doug Meeting Summary

- Virtual IoT device (VM)
  - Will be created directly in ISEAGE 2.0 environment
  - Directly involved with CDC scenario
  - Available in a month
- Physical IoT device
  - Use multiple raspberry pis(1 for each team)
  - Could potentially be used as an anomaly
- Physical Camera from last year’s group
  - Try to get working or replace with raspberry pi

Current Physical IoT list



Device	CVEs	Flashyness	Cost	CVSS Score	Hacking Difficulty	CDC Integration	Total Score
Jector Smart TV FM-K75	CVE-2019-9871	5	0 (Very Expensive)	9.8 (Critical)	4.0 (Easy)	3.0 (Somewhat Intregratable)	21.8
Yi Home Camera 27US	CVE-2018-3934	--	5 (Cheap)	9.0 (Critical)	2 (Hard)	--	--
TP-Link Archer A7 AC1750	CVE-2020-10888	--	5 (Cheap)	9.8 (Critical)	2 (Hard)	--	--
Eques Elf Smart Plug	CVE-2019-15745	3	5 (Cheap)	8.8 (High)	3 (Medium)	3 (Somewhat Intregratable)	22.8
XIAOMI XIAOAI speaker Pro LX06	CVE-2020-10263	3	5 (Cheap)	6.8 (Medium)	--	2 (Barely Intregratable)	--
Raspberry Pi 3	Unlimited	Variable	5 (Cheap)	Variable	Variable	4 (Intregratable)	--

Prioritized Task: Virtual Machine

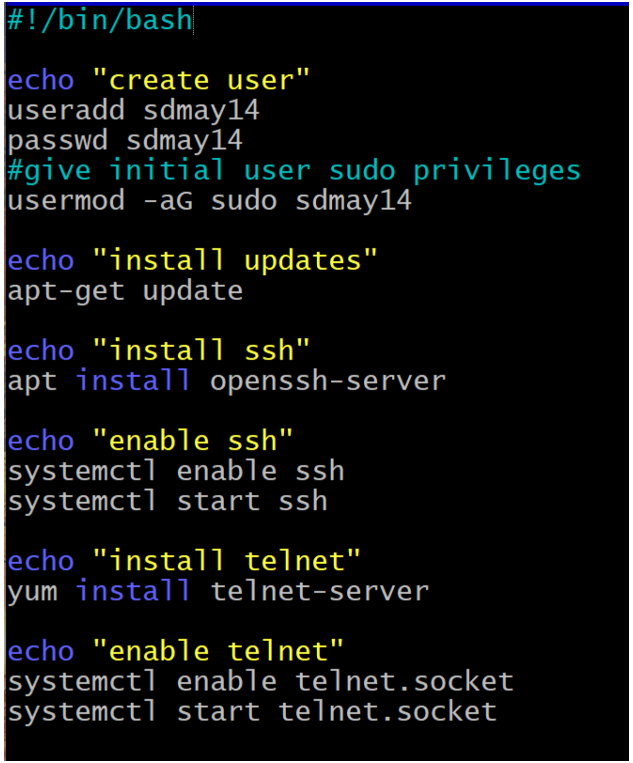
- Develop an IoT configuration script
    - Jake, Justin

- Develop a vulnerable web interface
    - Megan, Jacob

IoT VM initial setup (with script)

- Create a non-root user(with sudo permissions)
- SSH
  - Configure firewall to allow SSH
- Telnet
- … more to come

Basic Configuration Script(will expand)



```
#!/bin/bash

echo "create user"
useradd sdmay14
passwd sdmay14
#give initial user sudo privileges
usermod -aG sudo sdmay14

echo "install updates"
apt-get update

echo "install ssh"
apt install openssh-server

echo "enable ssh"
systemctl enable ssh
systemctl start ssh

echo "install telnet"
yum install telnet-server

echo "enable telnet"
systemctl enable telnet.socket
systemctl start telnet.socket
```

This week “To Do”

- Continue expanding and researching scripting
- Create services for VM (i.e. web server)
- Testing assignment and lightning talk