RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT)

Jennifer Matilainen
Mackenzie Zappe and Ignacio Astaburuaga
PI: Shamik Sengupta, Co-PI: David Feil-Seifer

Introduction

In today's world and it's advancing technologies, Cybersecurity is becoming more crucial. The desire for convenience over security allows Cyber Attackers into millions of people's homes, workplace and everyday life.

Many teenagers spend multiple hours on the internet each day. Hands on activities and instruction will create an opportunity for students to see how the internet works, how a hacker seeks vulnerabilities and exploits the found information. The students will learn how to protect themselves from this attacks.

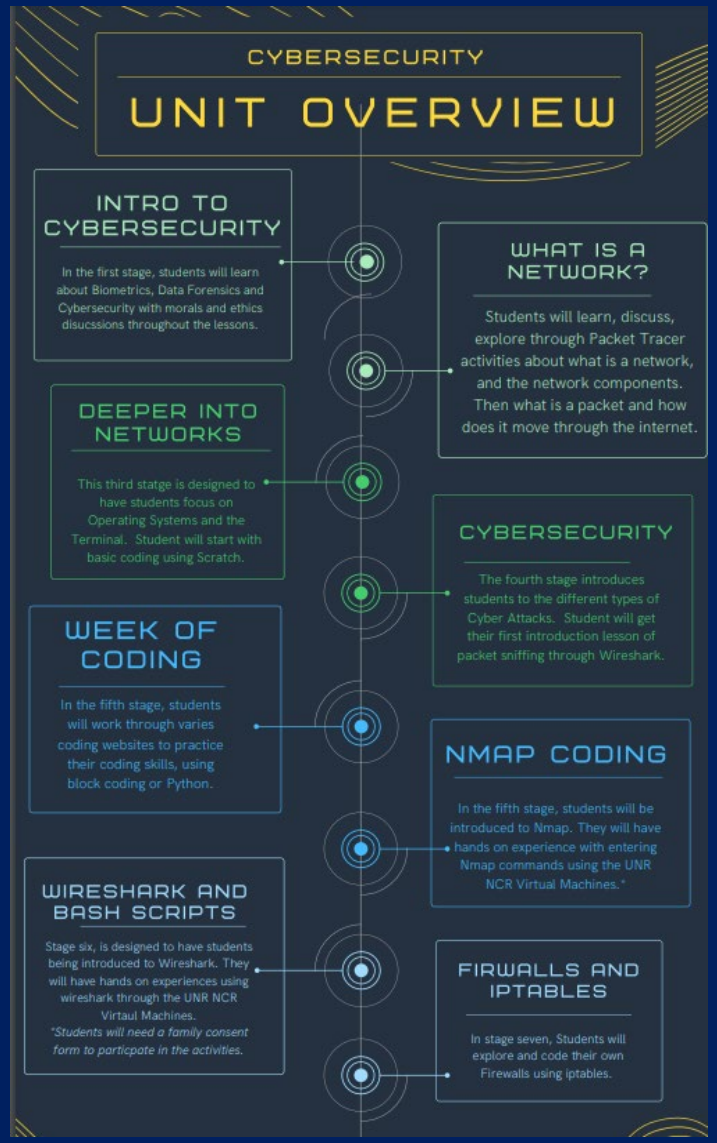
Unit Essential Questions

The essential questions students will be able to answer in this Unit are:

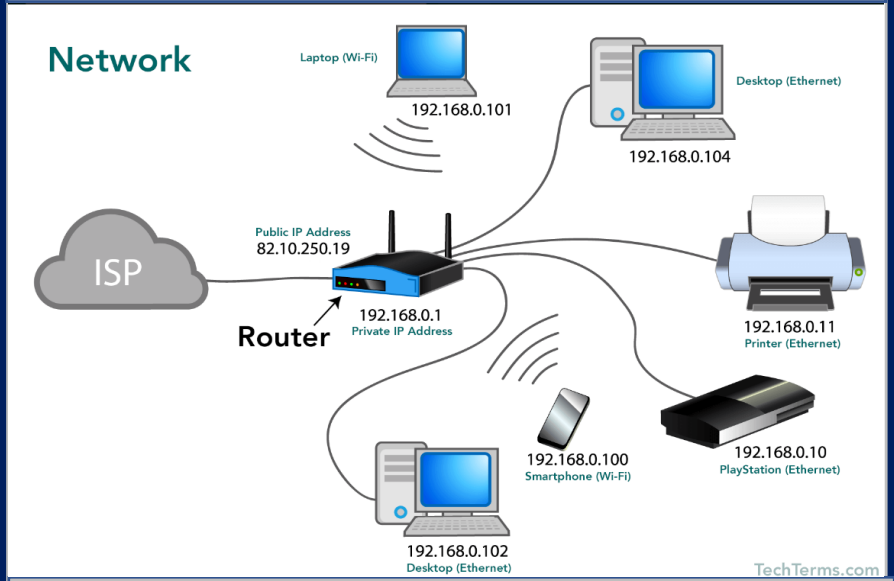
- What is a Network?
  - How does a Network function?
  - What is a packet? How does it move through the internet?
- What are the different types of coding languages?
- What is Cybersecurity?
  - What is the step-by-step procedure for a Cyber Attacker to infiltrate a network?
- Who is at risk for a cyber-attack?
  - What security measures can you put into place to protect yourself from cyber-attack?

Coding

```
GNU nano 5.4                                    ipports.sh
#!/bin/bash

#find host machine and save IP as variable
IP=$(ip addr show eth0 | grep "inet\b" | awk '{print $2}' | cut -d/ -f1)
echo Host IP $IP

#find subnet mask:
subm=$(ifconfig eth0 | awk '/netmask/{split($4,a,":"); print a[1]}')
echo Subnet Mask $subm

#find IP addresses on subnet using binanry/ bitwise AND subnet mask AND IP addreess with computer calculator
IFS=. read -r i1 i2 i3 i4 <<< "$IP"
IFS=. read -r m1 m2 m3 m4 <<< "$subm"
subn=$(printf "%d.%d.%d.%d\n" "$((i1 & m1))" "$((i2 & m2))" "$((i3 & m3))" "$((i4 & m4))")
echo Subnet ID $subn
```



Inside a Network



Assessment

Pre-Assessment:
Students will participate in a whole class discussion about what they know about Cyber Attacks. Then they will be asked to open and use the terminal to find the Host IP address, Network IP and the available open ports.

Post- Assessment:
Students will enter lines of nmap commands in a terminal to find the Host IP address, Network IP and the available open ports on the NCR virtual machines. Then students will capture PCAP files using Wireshark packet sniffing via online assessment.

RET Site: Research Experience in Cybersecurity for Nevada Teachers (RECNT)

Jennifer Matilainen
Mackenzie Zappe and Ignacio Astaburuaga
PI: Shamik Sengupta, Co-PI: David Feil-Seifer

Introduction

In today's world and it's advancing technologies, Cybersecurity is becoming more crucial. The desire for convenience over security allows Cyber Attackers into millions of people's homes, workplace and everyday life.

Many teenagers spend multiple hours on the internet each day. Hands on activities and instruction will create an opportunity for students to see how the internet works, how a hacker seeks vulnerabilities and exploits the found information. The students will learn how to protect themselves from this attacks.

Essential Questions

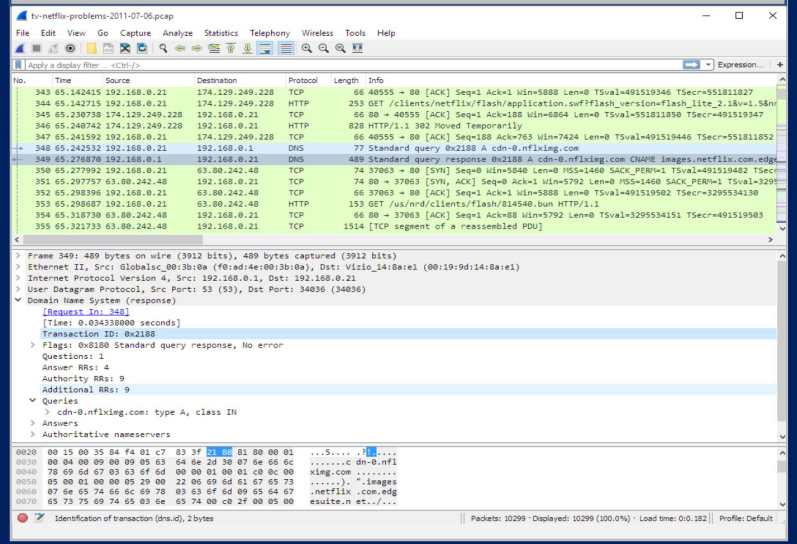
The essential questions students will be able to answer:

- What tools could Cyber Attackers use to hack into a network?
- What is the step-by-step procedure for a Cyber Attacker to infiltrate a network?
- Who is at risk for a cyber-attack?
- What security measures can you put into place to protect yourself from cyber-attack?

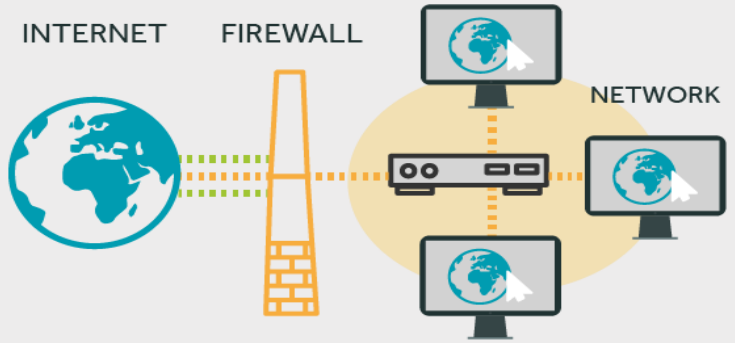
The Kill Chain- Inside the Attacker Mindset

- **Step 1: Reconnaissance.**
- **Step 2: Weaponization.** This involves using all of the collected information to craft a very specific attack.
- **Step 3: Delivery of the attack.** This usually occurs in the form of something like a text or email phishing attack or sending a malware-laden file for downloading.
- **Step 4: Exploitation.** This is where someone would actually click on a link within a phishing email or let someone in the front door who shouldn't have access to the building.
- **Step 5: Installation.** This might not be necessary with all attacks but would involve something like a rootkit installation, or some other form of malware.
- **Step 6: Establishment of command and control.** The attacker is in the system and remotely able to manage it.
- **Step 7: Acting on the attacker's objectives.** Collecting the information or causing whatever damage they had intended to cause.

Seeking Vulnerabilities



Protection through Firewalls



Firewalls are fundamental barrier between a network and the internet. They protect the network from malicious activity and filter incoming, forwarding and outgoing traffic.

Assessment

Pre-Assessment:
Students will participate in a whole class discussion about what they know about Cyber Attacks. Then they will asked to open and use the terminal to find the Host IP address, Network IP and the available open ports.

Post- Assessment:
Students will enter lines of nmap commands in a terminal to find the Host IP address, Network IP and the available open ports on the NCR virtual machines. Then students will capture PCAP files using Wireshark packet sniffing via online assessment.