Daniel MacCarthy

CMPT_420N_111

Prof. Cannistra

February 24, 2022

A) Description:

This lab included four different tasks. In part one we took a closer look at the edge of our internal network and the risks that it could face. We identified a firewall as a useful device to help protect the edge of our network from outside attackers as well as add an extra layer against threat agents finding any vulnerabilities in our network. For part two we looked at and identified the difference between a threat and an attack. On top of that, we looked at an in-depth scenario that helped us further understand the difference between the two. Part three included building a network from scratch with 2 routers, one internal, one external, and a network of a switch and a few hosts attached to each. We had full connectivity to every host across the network as well as the servers, both internal and external. In part four (located right above the conclusion) we looked at what attack we would use to break into the network we configured in task three. We investigated how we would go about using a sniffing attack and what we would do with the information we gained from the attack.

B) Task One:

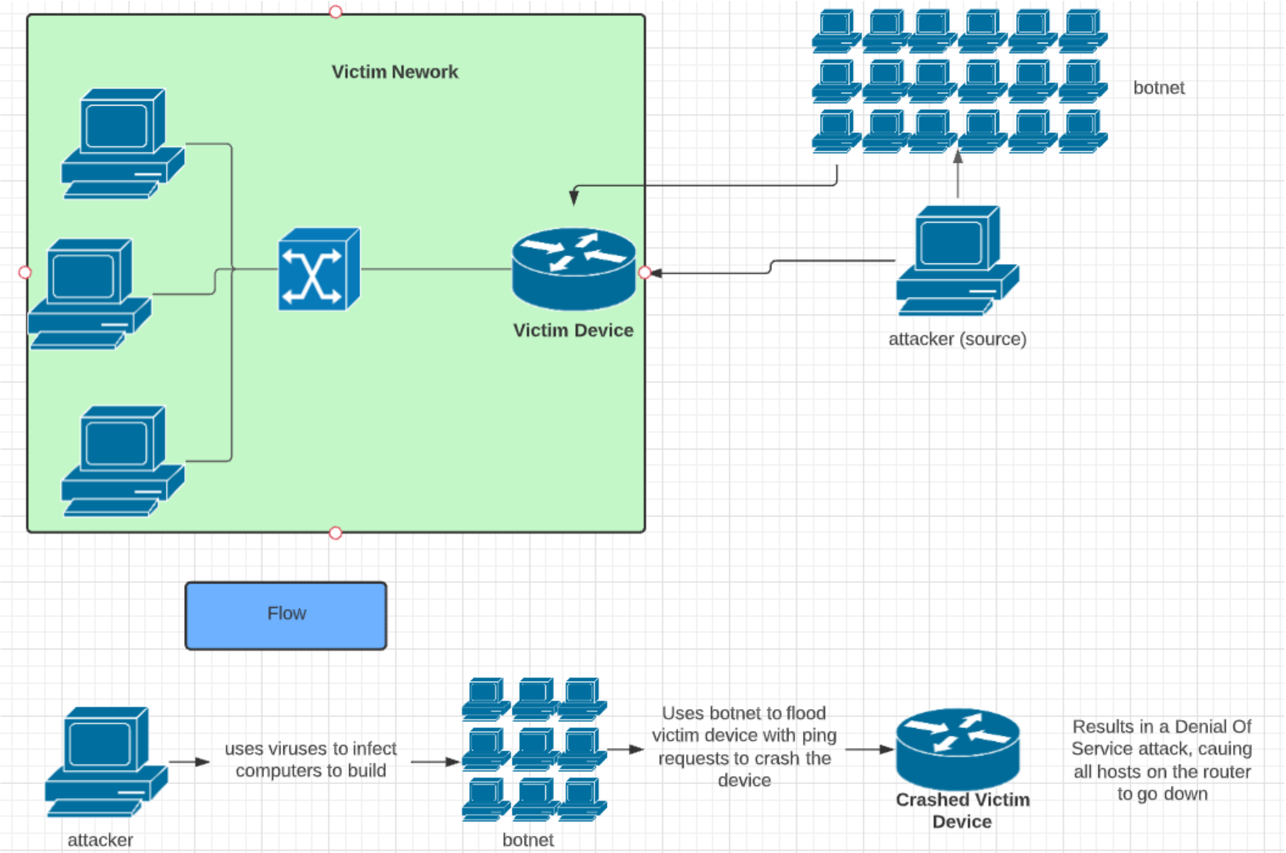
1) The perimeter of the network is where the topology changes from inside your controlled network to outside, usually the internet. At the perimeter of the network, you usually have an edge router to enable communication between your network and the internet. To increase security, it is best to have a firewall in place as well. Some routers have built-in firewall capabilities, but a firewall can also be its own device. In the case that the firewall is its own device, place it in between your edge router and the non-controlled network.

2) The difference between a threat and an attack is quite clear. A threat is a vulnerability or circumstance that has a chance of causing damage but can be prevented by controlling the vulnerabilities. An attack is a deliberate action by a user with the intention of causing damage to a system. Think of a scenario like this, you have a system that does not limit what Ip addresses can communicate to devices inside the network. You also have an unsecured public Wi-Fi that allows anyone in the area to access it. Those are both threats, vulnerabilities that could be used to cause harm, but by themselves will not do any damage. An attack is when someone comes along and uses that public Wi-Fi to conduct a man in the middle attack and learn the login credentials of an employee to gain access to privileges on the network. An attacker can go from there, purposely harming your network from the inside, possibly ruining your company.

C) Task Two:

Attack1: Ping Flood Attack

If an attacker wanted to conduct a Denial of Service (DoS) attack on a host or network, they could build up a botnet, possibly using malware. Then, once they have their botnet, use all those hosts at once to flood the victim device with ping requests to overwhelm the system and force it to crash.

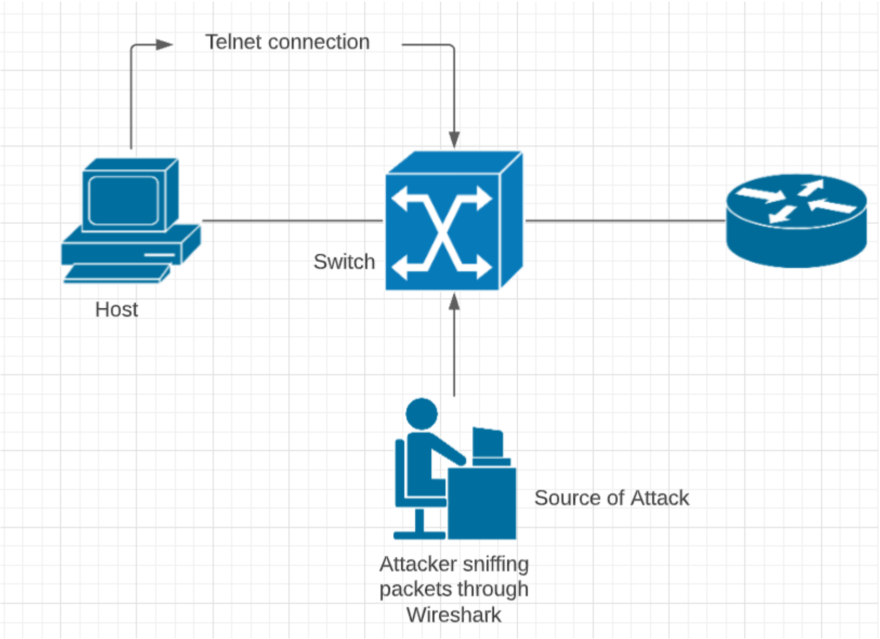

Victim Nework
Victim Device
botnet
attacker (source)
Flow
attacker
uses viruses to infect computers to build
botnet
Uses botnet to flood victim device with ping requests to crash the device
Crashed Victim Device
Results in a Denial Of Service attack, cauing all hosts on the router to go down

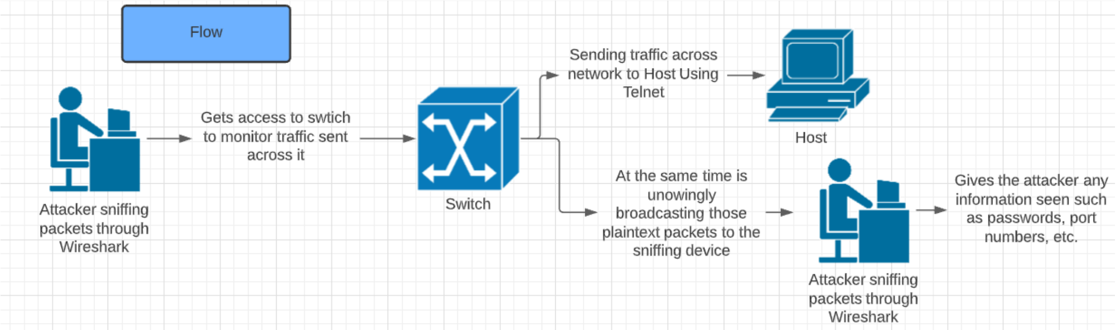
A common use of this type of attack is to disrupt communication between hosts on a network so that a cybersecurity team cannot respond to an attack as fast. If you are launching another type of attack and get found out, a ping flood can be a great attack to disrupt the users on the network from taking action to mitigate what you are doing.

Another use of this version of a Denial of Service (DoS) attack is to try to bring down a whole network. If you have a network that you want to launch an attack on, and they have a connection to a network that hosts most of their security measures, you could target certain devices to bring down, leaving the target network vulnerable to attack.

Attack 2: Sniffing Attack

If someone can get a sniffing device or a PC that runs Wireshark on your network, then they can see any packets sent across a network. This becomes a huge problem when using something like Telnet, which sends traffic as plaintext.



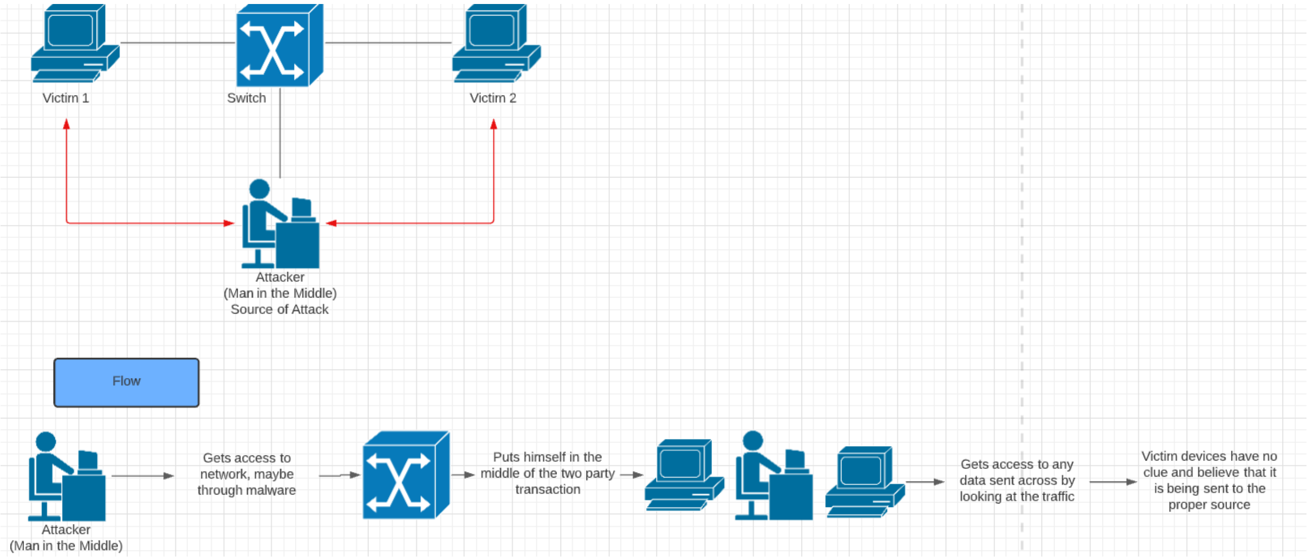

Flow
Attacker sniffing packets through Wireshark
Gets access to swtich to monitor traffic sent across it
Switch
Sending traffic across network to Host Using Telnet
Host
At the same time is unowingly broadcasting those plaintext packets to the sniffing device
Attacker sniffing packets through Wireshark
Gives the attacker any information seen such as passwords, port numbers, etc.

A popular way for this attack to be used is for an attacker to try to gain login credentials for a company or website. If someone was to get a new job at a company and they decided to send them their login credentials in an email the attacker can see the SMTP packets sent in an email, then use that data to gain deeper access to their network.

Another use of a sniffing attack is what is depicted in the flow diagram. If the attacker was able to get some access to the network and is sniffing traffic sent across the network, they would be able to capture any telnet traffic on the network. Once they capture the telnet packets, they will be able to see all data that appeared for the host that used the telnet connection, whether it be passwords to get onto the devices or other information.

Attack 3: Man in the Middle Attack

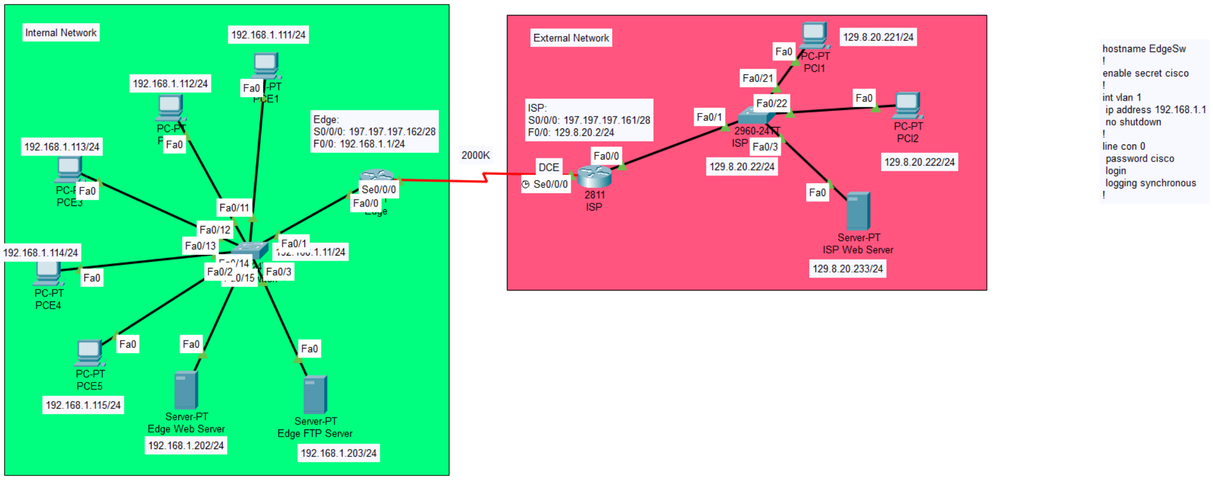
Man in the Middle Attacks can happen if an attacker takes advantage of a vulnerability, such as unsecured public Wi-Fi, to insert themselves in between a transaction. They can access any data sent across this transaction, such as bank account information if you are accessing your banking.


Victim 1
Switch
Victim 2
Attacker
(Man in the Middle)
Source of Attack
Flow
Attacker
(Man in the Middle)
Gets access to network, maybe through malware
Puts himself in the middle of the two party transaction
Gets access to any data sent across by looking at the traffic
Victim devices have no clue and believe that it is being sent to the proper source

One reason for an attacker to use this was highlighted before, say an attacker is trying to get access to your bank account. If you are logging in to your banking website on unsecured public Wi-Fi, they can insert themselves between the connection from you to your bank's website, and with this see any data you send across that transaction. If you log in with your credentials, they now have them and therefore can gain access to your bank account.

Another reason for an attacker to use the man in the middle attack is if a worker at a company they are planning an attack on is using unsecured Wi-Fi to work remotely. Especially now in a post-covid, work-from-home environment, people may try to get some work done at a local coffee shop, which can work to the benefit of an attacker. If the attacker can intercept the traffic between the victim host and the website that they are trying to connect to, then they once again can gain access to your login credentials. Once they have that, they can do more reconnaissance on your company to help with their cyber-attack. Things like this are why VPNs are a great tool.

D) Topology:



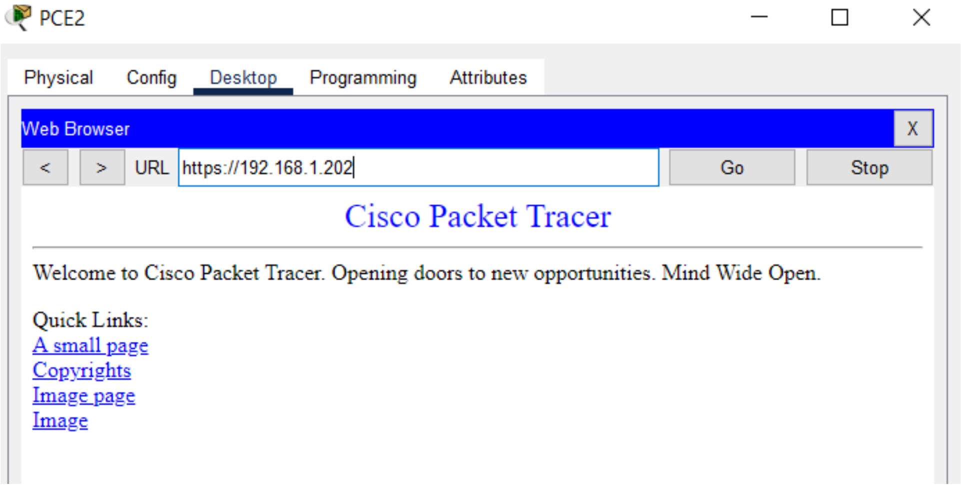
```
hostname EdgeSw
!
enable secret cisco
!
int vlan 1
 ip address 192.168.1.1
 no shutdown
!
line con 0
 password cisco
 login
 logging synchronous
!
```

E) Key Syntax:

Command	Description	IOS Mode
hostname	Sets the name of the device	Global Configuration mode
enable	Enables privilege mode	User Mode
configure terminal	Enters Global Configuration mode	Privilege Mode
login	Prompts the user to enter a password to gain access	Line Configuration mode
logging synchronous	Synchronizes the console line	Line Configuration modeP
int x/x	Accesses and interface	Global Configuration mode
ip config	Verifies the ip address and subnet mask of a host	CMD User mode
ping	Verify connectivity to another entity on the network through the IP address	CMD User mode
ip default-gateway	Sete the address to forward packets to on a switch	Global Configuration mode
ip route 0.0.0.0 0.0.0.0	Sets default static route to forward all packets across a connection	Global Configuration mode

F) Verification:

PCE2 accessing Internal Web Server



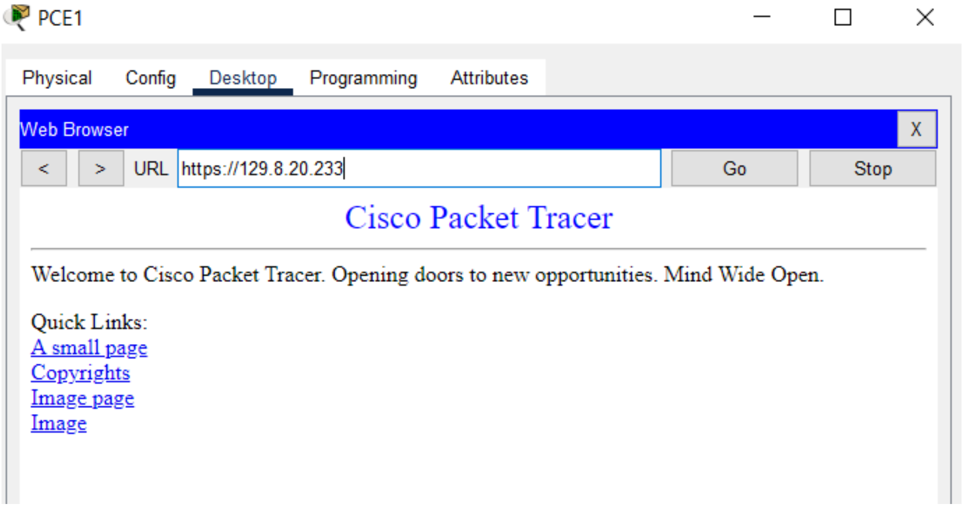
URL https://192.168.1.202

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

PCE1 accessing Internet Web Server



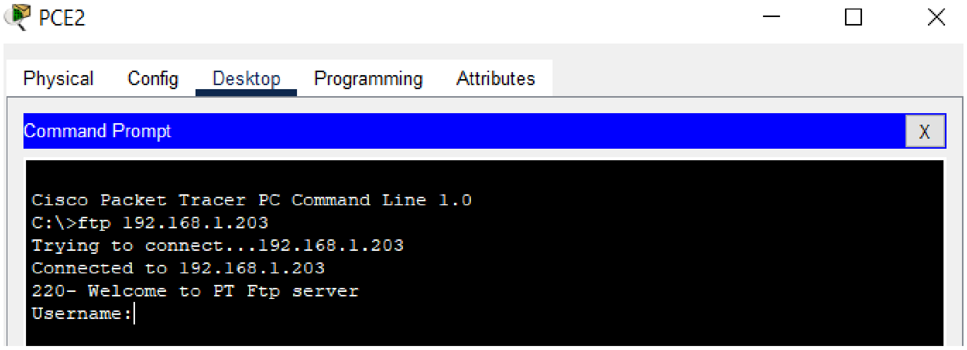
URL https://129.8.20.233

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

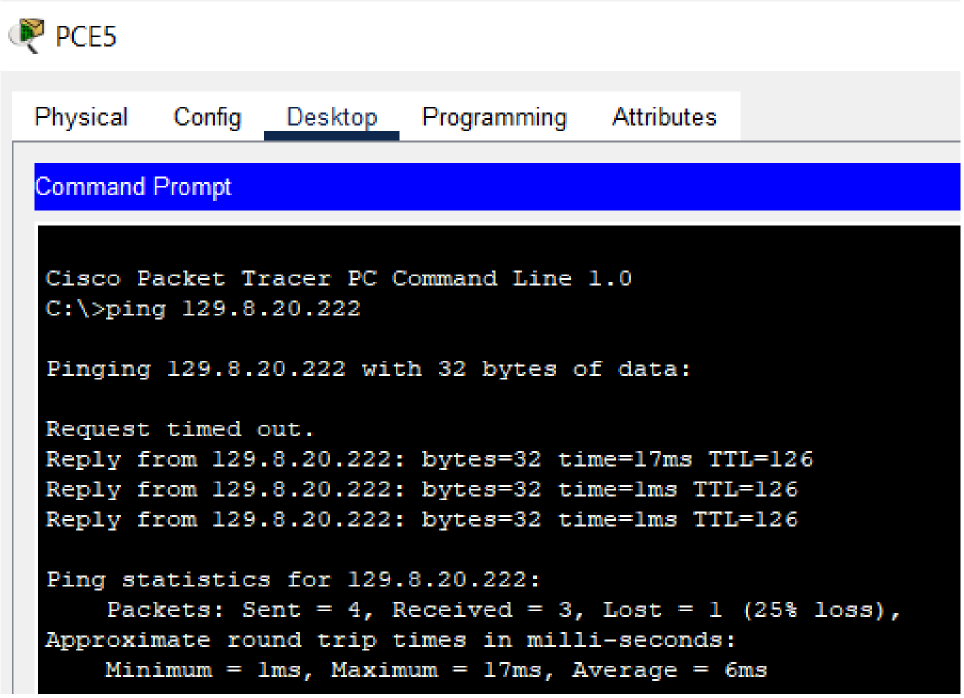
Quick Links:
A small page
Copyrights
Image page
Image

PCE2 using FTP to FTP to the Internal FTP Server



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.203
Trying to connect...192.168.1.203
Connected to 192.168.1.203
220- Welcome to PT Ftp server
Username:
```

PCE5 pinging PCI2



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 129.8.20.222

Pinging 129.8.20.222 with 32 bytes of data:

Request timed out.
Reply from 129.8.20.222: bytes=32 time=17ms TTL=126
Reply from 129.8.20.222: bytes=32 time=1ms TTL=126
Reply from 129.8.20.222: bytes=32 time=1ms TTL=126

Ping statistics for 129.8.20.222:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 17ms, Average = 6ms
```

Configuration Thoughts:

A) No, if the internet PC’s have access to FTP on the internal FTP server then they can transfer private documents to themselves and possibly steal data. Even if they can only transfer to the FTP server and not from it is still a risk that is not necessary.

B) No, an internal web server could contain important hardware used to keep their website running and allowing public access to that part could risk your devices and your network.

Task Four:

To get into the topology that we configured in task three I would use a sniffing attack. Since any ISP device has full connectivity to the devices on the internal network, this is not a secure network. Using Wireshark on my end device I would sniff all traffic going across the network until I eventually got useful data, whether it be in the form of Telnet traffic through a telnet session or something like SMTP from an email. If I were to get the password to get on a switch, router, or even an internal server through this method I could potentially bring the whole network down, whether that be by shutting down all ports on the devices or changing the Ip addressing in the devices. If this was a company with data tables on its users, I could get access to that data and possibly sell it online for money. That data could also lead me to launch another attack on a different company if they have a worker that re-uses passwords.

G) Conclusion:

The lab went as planned. Every part of the lab was done properly. I used Lucid Chart to make the diagrams for task two. All devices were working properly in task three with every device having full connectivity. This lab stressed the importance of Internet Security and that if a network has even a slight vulnerability, there are a million ways a threat can turn into an attack, and even more ways an attacker will try to get into the system.

H) References:

https://www.datto.com/blog/cybersecurity-101-intro-to-the-top-10-common-types-of-cybersecurity-attacks

https://www.imperva.com/learn/ddos/ping-icmp-flood/