Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Lab 4: Let's go F(ph)ishing

Always know:

Trusting is bursting in security

Nitheesh Murugan Kaliyamurthy – n.kaliyamurthy@uwtsd.ac.uk

What we do?

Part 1

1. Set up your Lab
2. Go Phishing
3. Record your reflections to mitigate these types of vulnerabilities

Part 2

4. Observe the demonstration by your Instructor (Using Telnet and SSH)
5. Identify the vulnerability and record your reflections to mitigate it

Part 3

6. Use Packet Tracer Exercise and investigate the FTP Traffic and record your reflections to mitigate the vulnerability.

What you need?

- Host computer with a minimum of 8 GB of RAM and 40GB of free disk space
- Internet access

Part 1:

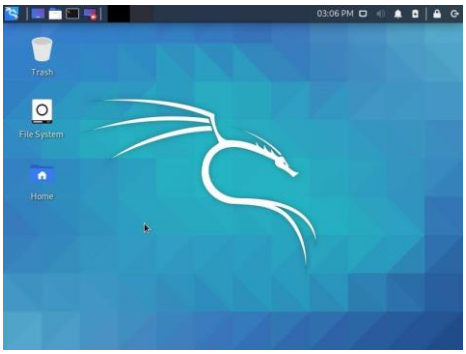
Set up your Lab

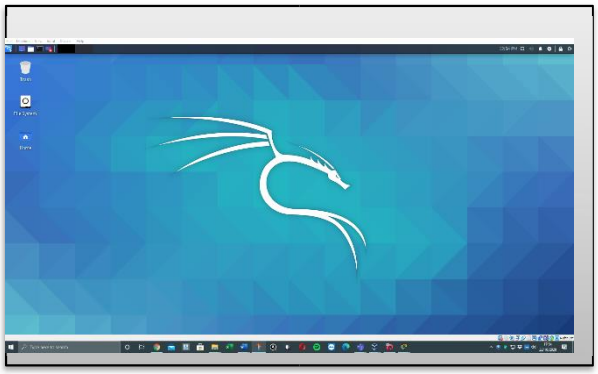
Download Kali Linux 2020.3 version from https://www.kali.org/downloads/. (Based on your Operating System, Select the version and install) Start Kali Linux and login.

(Based on your previous lab exercises, if you come across any issues in starting kali Linux, troubleshoot it on your own. Recommendations: You should have created a "Lab Manual/Reference Document" to record all your previous errors/ issues and its troubleshooting steps. Refer the document to troubleshoot. If not done, please start now.)

You should now know the username and password to login into Kali Linux 2020.3. If you don't know, search and find as a warm up activity to go Phishing!!!

Login and record your screen:





Go to https://github.com/trustedsec/social-engineer-toolkit or any other websites, which you find better. List out the other website links here (Add additional lines)

_____

https://securityonline.info/install-social-engineering-toolkit-set-windows/

https://sourceforge.net/directory/os:windows/?q=social+engineering+toolkit

https://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/

http://exploitsrevealed.com/the-social-engineer-toolkit-free-download/

_____ Record your reflections/ understanding about SE Toolkit

I was surprised how many toolkits there are for performing Social Engineering, and how easy it is for anyone to setup. I initially thought it would be very hard for someone to recreate a false website that steals your data, but with the toolkit, all the hard work is already done.

Now, let's go Phishing. The idea is to clone a social media website and use the template to harvest the user credentials. It could be done in many ways. This lab is to help you understand the use of Social Engineering Toolkit. Warning: Be Ethical. After learning the functions of SE Toolkit, you could try other options and record them in your manual for further learning.

Let's get into a scenario:

Scene 1: You are receiving a link from your friend asking to look at his post in linkedin. You click on the link and it takes you to the official login page. You enter your credentials and login. It loads and asks for the login credentials again. No doubts for you, (maybe thinking of some internet/ application issue) and logging in again. It takes into your account. But you could not see your friends post. You think it is not working and focus on other interesting posts.

Behind the scene: Your friend actually sets you a trap by sending the link. It is to harvest your credentials. Your user name and password is now with your friend. (No worries ahh!!! Its your friend. He/She will not do any harm to you)

Just deeper behind the scene: Your friend's account has been compromised and actually it was some real time criminal (hacker) who sent you a link in the name of your friend setting you a trap through the link. Now your user name and password is with some criminal.

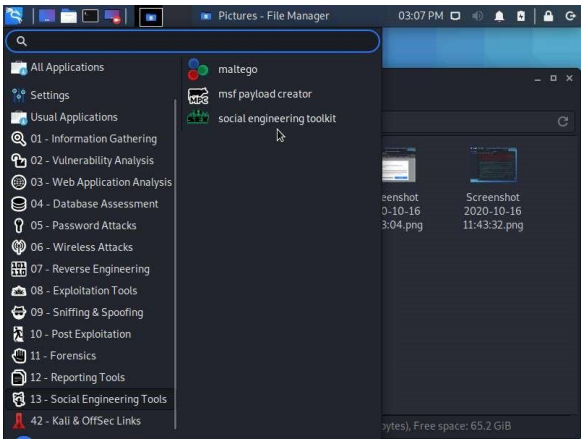
Imagine the next day morning. You wake up anddddddd…..

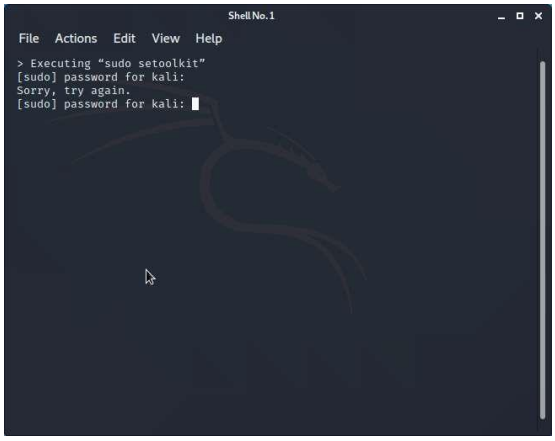
It is a nice story. But, is it really possible? How?

Let's go phishing….

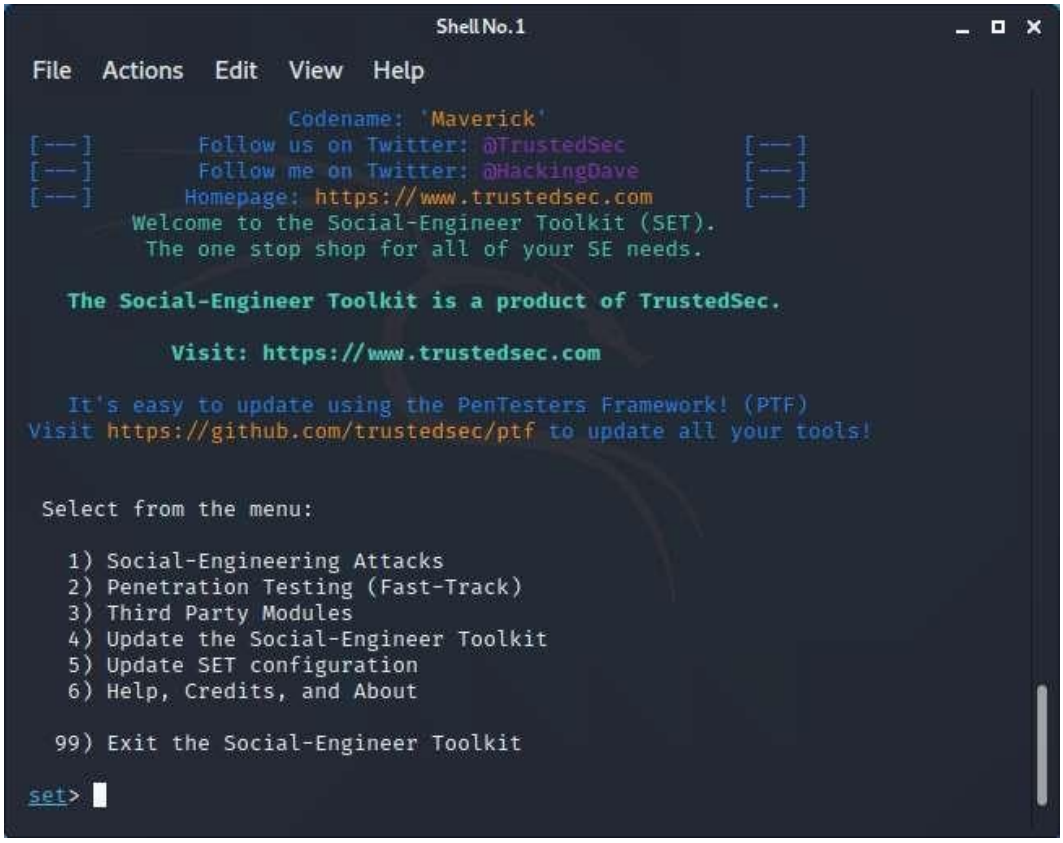
Click on Programs□ Social Engineering Tools □ social engineering toolkit

It prompts for your password. Give your password

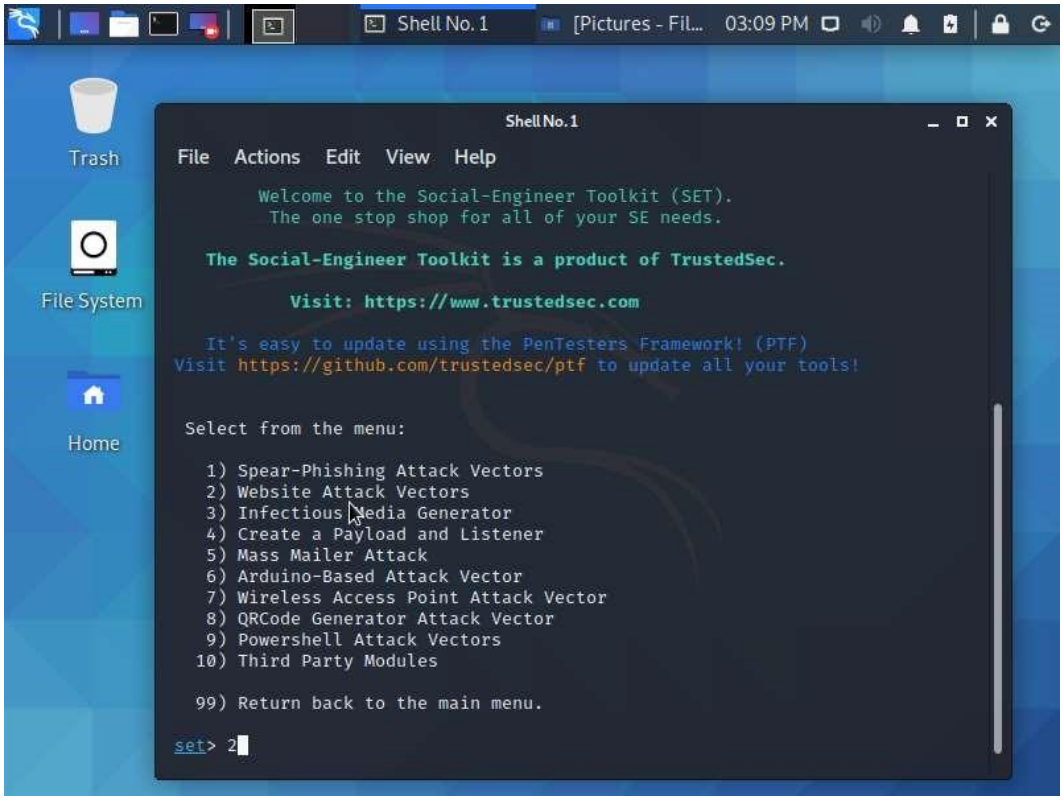




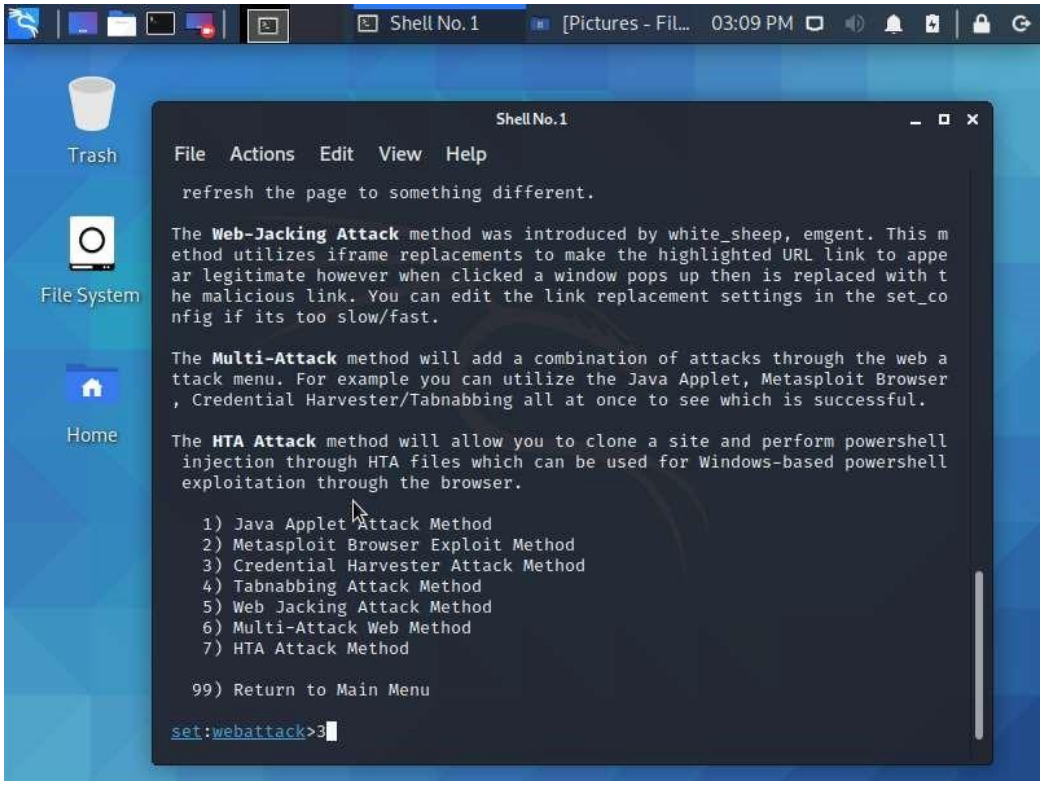
Select Social Engineering Attacks □ 1



Select Website Attack Vectors □ 2



Select Credential Harvester Attack Method □ 3



Select Web Templates □ 1

It will ask for an IP Address □ Give your Local IP Address. (In cases, if you are phishing outside the network, you might need a Public IP Address)

It will ask for the website to clone/ use: Give, https://www.twitter.com

Open the Web Browser and click the Local IP Address, which you had set. It should take you to the twitter login page.

Give dummy credentials to check. After login, it will take you to the original twitter login page.

Go back to the SETools Editor and check for the harvest. You should find out the credentials listed.

You could also try to set this link (Local IP Address) and send via emails/ Embed it with some image and send it to get a professional look. But, remember, this lab is just to practice and identify the vulnerabilities as a Cybersecurity Analyst.

You could also embed this into a pdf or other applications (.jpg., .png etc). Try them out within the Virtual Machine !!!

Record your reflections/ understanding about using the SE Toolkit

I was amazed by how quick and easy this makes it for someone to trick people out of their details, but also how little time it takes. Very often people would be attempting to log into a website and not even realising that they are giving away their password to a scammer.

What is the security vulnerability you identified when using the link to login the social media page? This social engineering scam relies exploiting human psychology, rather than technical hacking techniques, this can be employed many different ways.

What is your recommendations to mitigate the above identified vulnerability? (Like, when you click on a link, what should you check for?) I always recommend people should examine the link carefully before clicking on it, because if someone receives an email supposedly from amazon or paypal etc, it can look quite convincing, but by checking the url of the link to see if it really is www.amazon.co.uk or www.paypal.co.uk etc If its an unrelated addresses then no doubt it's a scam no matter how realistic it looks.

Part 2:

Observe and identify

The Lecturer has demonstrated about the Telnet and SSH configuration. How it works? Its advantages and disadvantages.

(Link is available in Moodle)

Record your reflections/ understanding about the vulnerabilities you identified when using Telnet.

The problem with telnet is that everything is sent in plain text, nothing is encrypted. If anyone is 'listening' using some kind of packet sniffer such as wireshark, then they can see everything that has been typed, including usernames and passwords.

Record your reflections/ understanding about any vulnerabilities you identified when using SSH.

Ssh is more secure, especially if using version 2. All text is encrypted before being sent so even if someone has somehow got access to the packets being sent, they wouldn't be able to make any sense of them anyway.

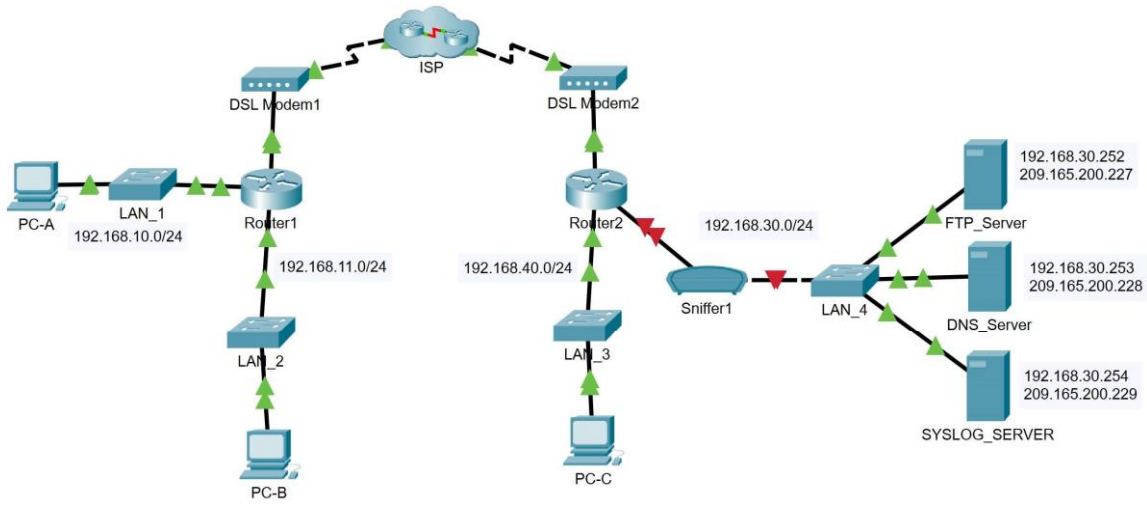
What is your recommendations to mitigate the above identified vulnerabilities?

To never use an unsecure connection, never use a protocol that doesn't employ an encryption method. In cisco equipment, the option to use telnet can be turned off, so only secure methods can be used – but it is often more about training staff, developing good habits and making sure the weaknesses and vulnerabilities are minimised.

Part 3:

Use Packet Tracer to investigate the FTP Traffic

Packet Tracer is available in Moodle and Teams File Channel



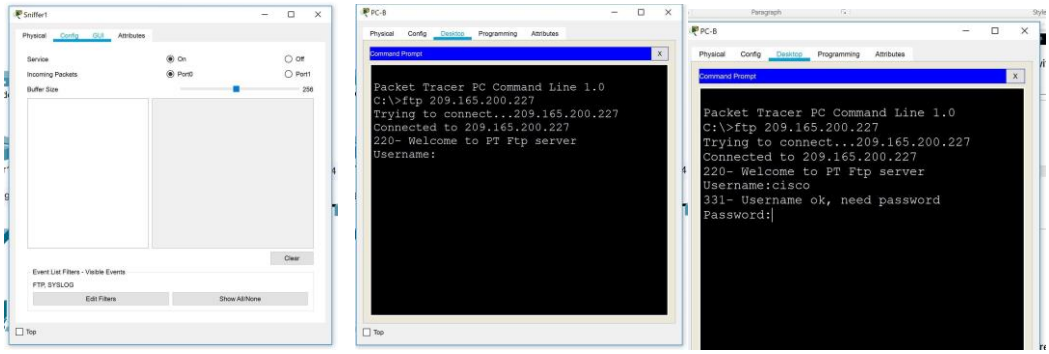
Addressing Table

Device	Private IP Address	Public IP Address
FTP_Server	192.168.30.253	209.165.200.227
SYSLOG_SERVER	192.168.11.254	209.165.200.229
Router2	N/A	209.165.200.226

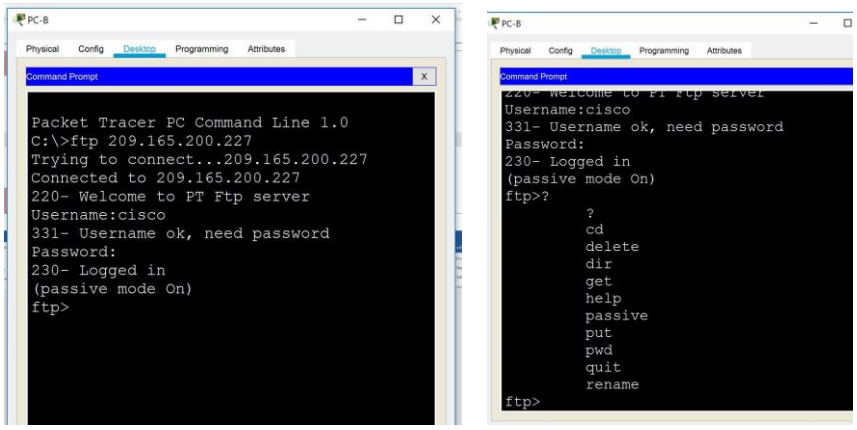
- Create FTP traffic.
- Activate the sniffing device.
  - Click on sniffer device Sniffer1.
  - Go to the Physical tab and turn on the power to the sniffer.
  - Go to the GUI tab and turn the sniffer service on. o Select the appropriate port to sniff.

  Note that the FTP and syslog packets entering the sniffer from Router2 are being monitored.

- Remotely connect to the FTP server.
- Click on PC-B and go to the desktop.
- Click Command Prompt. From the command prompt, open an FTP session with FTP_SERVER using its public IP address.

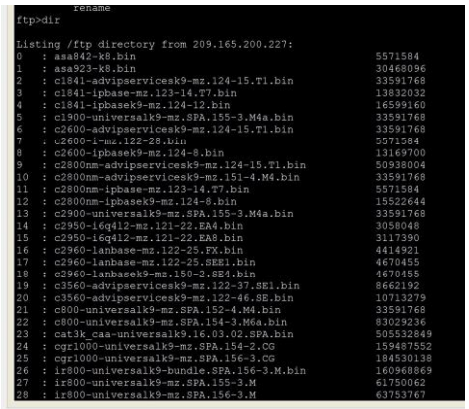


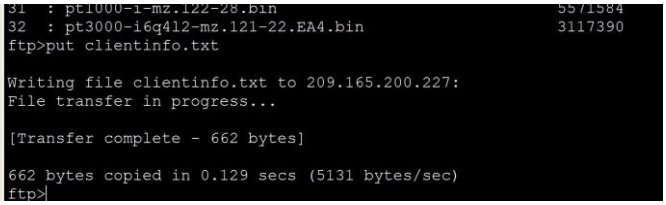
☐ Enter the username of cisco and password of cisco to authenticate with the FTP_Server.



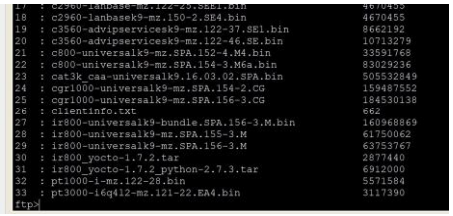
☐ Upload a file to the FTP server.

- At the ftp> prompt, enter the command dir to view the current files stored on the remote FTP server.
- Upload the clientinfo.txt file to the FTP server by entering the command put clientinfo.txt.
- At the ftp> prompt, enter the command dir and verify that the clientinfo.txt file is now on the FTP server.



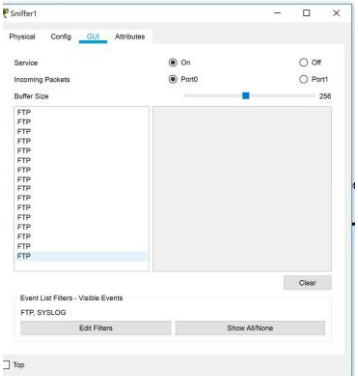


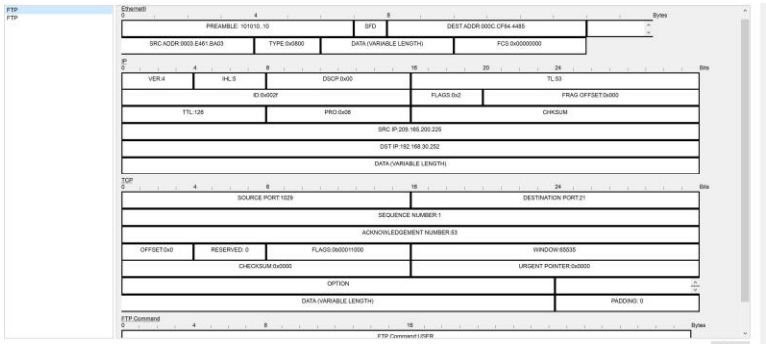
☐ Enter quit at the FTP prompt to close the session.

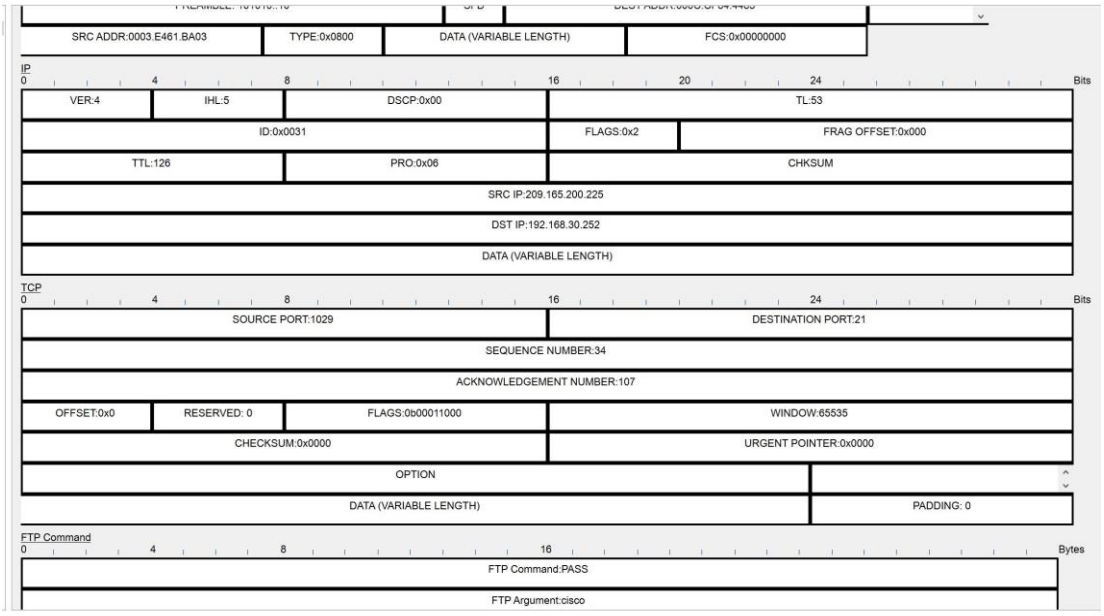


Investigate the FTP Traffic

- Click the Sniffer1 device and then click the GUI tab.
- Click through some of the first FTP packets in the session.
  - Be sure to scroll down to view the application layer protocol information in the packet details for each.
  - (This assumes this is your first FTP session. If you have opened other sessions, clear the window and repeat the login and file transfer process.)







Record your reflections/ understanding about the vulnerabilities you identified when using FTP. FTP is not encrypted, and because all of the data is transferred as plain-text, any intercepted traffic can be read easily.

What is your recommendations to mitigate the above identified vulnerabilities?

I would recommend encrypting all traffic using Secure variants of FTP such as FTPS Implicit SSL and FTPS Explicit SSL. Both utilize SSL encryption. Another protocol that could be used instead is SFTP, which is based on SSH (Secure Shell).

Using all unencrypted protocols such as POP and Telnet should be avoided in today's networks.

The example above had a physical device planted in the network to monitor traffic, so another tip to avoid this happening would be to physically secure the servers and data room.

Also scanning and monitoring the network regularly, for any kind of intrusion attempt or rogue devices that may be setup to capture traffic.

Learnings from this lab:

- Understand Cyberattacks, Updates about recent attacks.
- Analyse the Cyberattacks to find out the target, outcome, vulnerabilities and exploits.
- Available Certifications and Job Opportunities in Cybersecurity domain.
- Setup various lab environments (Virtual Machines with Cyberops, Kali Linux etc), modify settings and troubleshoot compatibility issues with Operating Systems.
- Use MiniNet, trace the routes and examine the packets using Wireshark.
- Contributing and working as a part of a Team (Blue Team) and to share responsibilities of a demonstrated SOC.
- Analyse various Malwares and Social Engineering methods to gain access.
- Using tools like TCPView to identify the process running in the machine to establish a connection.
- Use Social Engineering Toolkit to harvest credentials of users.
- Using a sniffer and sniff the packets and analyse its vulnerabilities.