1. ***In your own words, summarise a MITM attack. (Don't need to Google, just refer to your lab instruction sheet document for this)***

According to the instruction, the Man-In-The-Middle Attack (MIMT) is a cyber-attack method to connect both ends (Network and End User). Since it connects in between, it can receive and obtain information from all the traffic flow between users and the network.

In the Lab, we created a proxy at the raspberry pi and the Raspberry PI also acts as an AP that allows users to connect. All the HTTP, HTTPS, and Port 3000 traffic are recorded so we can be able to obtain information from those packets.

1. ***In few words, explain what does each of the following command do. Please follow the answer template provided and be succinct.***

Graphical user interface, text

Description automatically generated

A) Is to enable the Kernel for IPv4 forwarding.

B) IPTABLES is used to set filter traffic rules. PREROUTING is handling the flowing traffic at Port 80 (HTTP Request) from WLAN0 Interface and Redirecting them to Port 8080 (Proxy Host) immediately via NAT before routing.

C) IPTABLES is used to set filter traffic rules. PREROUTING is handling the flowing traffic at Port 443 (HTTPS Request) from WLAN0 Interface and Redirecting them to Port 8080 (Proxy Host) immediately via NAT before routing.

1. ***As the “man in the middle”, what tools and method did you use to obtain the credential to obtain the username and password?***

Firstly, we host a website at Port 3000 and also enabled IPTABLES to redirect traffic to port 8080 (Proxy).

Secondly, we used a tool is called “mitmproxy” records the traffic flow and waits for the victim to put a username and password to the provided website.

At least we filter out the intercepted packet by searching AUTH, so we can be able to obtain plaintext Username and password. (Only it’s because the Website use HTTP Protocol without any encryption method in use)

1. **Explain ‘GET’ and ‘POST’ methods you see in the logged data in mitmproxy console.**

GET Method in the mitmproxy console is to request data from specific Server.

POST Method in the mitmproxy console is to send data to specific Server (Get Login Access in this scenario).

1. **What is the difference between a replaying a packet and intercepting a packet?**

Both attacks are required to intercept packets. But intercepting a packet is to analyze, obtain information from the packet. But Replaying a packet is one step further by storing the packet and manipulating it before sending it to its destination.

1. ***You have successfully captured login credentials over unencrypted HTTP traffic. Although HTTPS enforces end-to-end encryption, it is still possible to perform MITM attack and sniff the network traffic under certain condition. Can you elaborate? Hint: It has something to do with SSL Certificates.***

Since HTTPS enforces end-to-end encryption, so for an established HTTPS connection the MITM attack can only receive unreadable context from the packets. But the attack can be done when the user initiates an HTTPS connection. Basically, when a user sends to start an HTTPS request, the attacker can use its own key to replace the user’s key to establish a connection to the server to exchange data. So send HTTPS requests to the server will be decrypted at the attacker’s end and encrypted and send to the server, when the server sends back the HTTPS packet and will be decrypted by the attacker and re-encrypt the data send back to users (simulate a secure HTTPS connection).

1. ***You have made a 1000 dollar bet with your friends that you can reach the highest score on Apple Game Centre for this game. Other than mastering the game and reaching the highest record, how do you think todays lab can help you win this bet. Discuss your solution.***

This can be done by Man-In-The-Middle Attack. This is because when user plays a game, the server site and the client site will exchange the data to update the status. The MITM attack can be able to capture the traffic from the client and change the data value before send to the server. So we can easily get a very high score.

1. List all commands used to setup a working Evil Twin AP (as per the instruction sheet document). Briefly, describe each command's function as well.
2. You just walked into a cafe, which you frequently visit, and would like to connect to the Internet via public WiFi and answer your course assignments. How would you detect an Evil Twin attack, in an environment like the one shown in Figure 1 of Lab 3 instruction sheet? In other words, how would you know "Starbucks WiFi" is not an Evil Twin and is trustworthy.
3. What is DNS Spoofing attack? Can Evil Twin attack be used as part of a DNS Spoofing attack? If so, please provide a succinct summary.
4. What is Fluxion Attack? When was it released? (i.e. how old is this attack?) if you were to target a network, when would you consider this attack?