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 the ‘Man-n-the middle’ AP that allows users to connect. All the HTTP, HTTPS, and Port 3000 traffic are recorded and redirected 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 mock website at Port 3000 and also enabled IPTABLES to redirect traffic to port 8080 (Proxy).

Secondly, we used a tool is called “mitmproxy” open source proxy that intercepts HTTP(S)

connections. Mitmproxy like other proxies forwards the connections to our destinsatoin website, however it also monitors and captures the packets (which may contain private information, username and password in our case) for a typical MITM attack

At last we filter out the intercepted packet by searching AUTH, so we can be able to obtain plaintext Username and password. (Plaintext already 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 a user plays a game, the server site and the client site will exchange the data to update the status. We can put a proxy (Man in the middle) that will capture when your friend gets high score, the MITM proxy can modify the POST packet and change it such that the User field is you instead of your friend.

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.

* C: sudo sysctl -w net.ipv4.ip\_forward=1 F:set up transparent proxying
* C: sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 80 -j REDIRECT --to-port 8080. F: reroute traffic from HTTP( (port 80) to mitm proxy on 8080
* sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 443 -j REDIRECT --to-port 8080 F: reroute traffic from HTTPs (port 443) to mitm proxy on 8080
* sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 3000 -j REDIRECT --to-port 8080. F: reroute traffic to local web server on port 3000 to mitm proxy on 8080
* node login.js : start login server
* mitmproxy --mode transparent –showhost (turn on transparent mode, and use the value of the host header for URL display)

User can now connect to our AP and access the login-page.

1. 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.

* Create duplicate AP with same SSID
* Initiate perpetual disconnection from the original SSID
* Eventually user will be forced to connect to the alternate SSID

1. 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.

DNS spoofing is a form of cache poisoning attack. A DNS server stores DNS records which map domain name to IP addresses. MITM attacker can intercept at the DNS server and inject fake or spoofed records effectively ‘poisoning’ the cache. When a user then tries to connect to a destination server, the DNS server will falsely route them to a different IP. In the lab a local DNS record points login-page.com to the real server. However the Evil-twin AP can hijack this record and change it so that it points to a hacked server.

1. 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?

Fluxion attack uses an Evil Access Point tool similar to our lab, it jamms the original network with disconnect commands enticing the user to join the twin evil access point. Fluxion is about 5 years old being released in 2017 having being evovled from a previous tool ‘lindset’. You would consider this attack when you can capture the WPA handshake and establish a convincing fake log-in page. Fluxion also has dependencies on aircrack-ng so one will need to ensure hardware compatibility when the network interface cards.