Question **1**
Not yet answered
Marked out of 5.00
Flag question

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, MITM (Man-in-the-Middle Attack) is a type of cyber attack that the attacker connects to both side of correspondents, then extracts the information in the middle, and forwards it as well. Both side of parties cannot recognize there's a person in the middle who has stolen their secure information, that's called MITM.
In the lab, we create a proxy that allows users to connect, then the proxy receives user's secure data (including Facebook email and password), then extract and forward it. The user gets normal message as usual thus does not recognize that MITM happens.

Question **2**
Not yet answered
Marked out of 2.50
Flag question

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

A) sysctl -w net.ipv4.ip_forward=1

B) iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 80 -j REDIRECT -- to- port 8080

C) iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 443 -j REDIRECT - -to- port 8080

[Answer template: A: Does X
B: Does Y
C: Does Z
]

A: It does start IP forward mode upon IPv4
B: It does set iptables firewall. PREROUTING is a function that handles flow-in packets before routing, let the packets flows into the proxy host via NAT, then redirect packets from port 80 to port 8080.
C: It does set iptables firewall. PREROUTING is a function that handles in-put packets before routing, let the packets flows into the proxy host via NAT, then redirect packets from port 443 to port 8080.

Question **3**
Not yet answered
Marked out of 2.00
Flag question

In the command mitmproxy -T --host, explain the options –T and --host that we passed to the tool (use the man page or the project homepage). What do they do?

-T: Set the transparent proxy mode. The transparent proxy mode is that the proxy redirect user's request without modify them.
--host: Use the host header to construct URLs for display.

Question **4**
Not yet answered
Marked out of 2.00
Flag question

Why at Step 6 when you try to access "https://www.google.com" you see the page "Your connection is not private" or "Cannot provide a secure connection"?

That is because a valid certificate is NOT provided when we try to access a HTTPS website. Based on X.509 authentication services, there should be a check on certificate validity. But as we use a proxy, the certificate origin could be amended, then the website will prompt the message.

Question **5**
Not yet answered
Marked out of 2.00
Flag question

By default, mitmproxy listens on port number _____

Select one:

- a. 80
- b. 443
- c. 8080 (selected)
- d. 23

Question **6**
Not yet answered
Marked out of 2.50
Flag question

Explain 'GET' and 'POST' methods you see in the logged data in mitmproxy console.

GET in the mitmproxy console is to request data from a specific server
POST in the mitmproxy console is to send data to the server to get access or update resource

Question **7**
Not yet answered
Marked out of 2.00
Flag question

What is the difference between a replaying a packet and intercepting a packet?

A replay attack is where the attacker captures traffic, and stores or manipulates it before sending it on.
intercepting a packet is where the attacker intercepts and capture traffic, and discard it, the packet will not able to send to it destination.

Question **8**
Not yet answered
Marked out of 7.00
Flag question

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 the man in the middle attack, as we all know when we play the game, the client(player) needs to send many packets to the server and update its status in the game, In this case, we can capture the traffic between the player and the server and manipulates some specific values which can gain more scores before we send it to the server. after the server receives those packets, they did not realize those packet has been modified, and update the score for the payer.