Question 1

According to the instruction, MITM attack (Man in the middle Attack) is the type of cyber attack that the middle attacker would secretly relay and alter the communications between two parties. Meanwhile, the attacker could intercept the message from the sender and send to the receiver after alternation, but both sides would not recognise this activity, which is called MITM. During the lab, we created a Hotspot as a proxy and seduced the users to connect to it. After users attempted to login the account name and password, the sensitive users’ data and information would be captured and extracted from the packet. However, the user got ordinary feedbacks, thus they would not recognise while the MITM happens.

Question 2

1. This command is used to start the IP forwarding based on IPv4, which has the ability to accept incoming network packets on one interface, recognise that it is not meant for the system itself. Then it should be passed on to another network, and then forwards it accordingly.
2. The command firstly sets the iptables firewall, then handles flow-in packets before routing. After the packets flow into the proxy host through NAT, then they would be redirected from port 80 to port 8080.
3. The third command line is similar to the previous one, the difference is the “Prerouting” function handles the in-put packets before routing, and redirect packets from port 443 to port 8080.

Question 3

The tool mitmproxy has been used in this question. From the command “mitmproxy -T —host”, we could know that the “-T” part is to set the transparent proxy mode, which is the proxy redirect user’s request without modify them. In addition, the “—host” part is the function of constructing URLs for display by using the host header. After the POST method succeed, we could acquire the credential to “testyou” from the URLEncoded form.

Question 4

The reason is that there is no valid certificate provided when we accessing a website with https protocol. Based on X.509 authentication services, there should be a check on certificate validity. Since the proxy is being using, the certificate could be amended originally, then the website will prompt the warning.

Question 5

C

Question 6

‘GET’ method is used to request data from server

‘POST’ method is used to send data to server. In order to get access or renew information.

Question 7

Replaying a packet means that the attacker captures data packets from network traffic, manipulates the packets and then send them back to the network. Intercepting a packet means that the attacker intercept and capture data packets, and do not send them back again. So these packets cannot be received by the destination host.

Question 8

This can be done by the attacker in the middle. When we play a game, we need to send a number of packets to the game server to update our status. The attacker can capture these data packets and manipulate some important values in packets such as score, then send these manipulated packets to game server. When the game server receives packets, it does not know these packets has been modified. So the game server will update the high score for the player.