Network-Security

Exercise 1: Secure a wireless network

This is a multistep attack and protect exercise in which you must do the following:

1. identify the passphrase to connect to the WEP network "to_break_educational"
2. If you have successfully identified the passphrase (anyone else can also) so the network is compromised and you should find a way to secure the network. You are allowed to do a network reconnaissance.

IMPORTANT: if you find a way to secure to network do not change the existing passphrase or any existing protocols in the network but only mention the steps to secure it. Remember, if you change any protocol or passphrases others will not be able to identify the passphrase so please avoid it.

In the exercise 1 answer you must include:

1. describe the step by step process of how the passphrase was obtained ?
2. Identify and state what was the exact weakness in the protocol due to which you were able to identify the passphrase of the wireless network ?
3. state your methods of network reconnaissance and identified steps to secure the network ?

Hint: Below is the QR code to join the network. Please note trying to find the password from the QR code / by trying to find the password from Wifi settings / by accessing the routers homeppage after using the QR codes are not valid methods.

Exercise 2: Man in the middle attack

Once you have obtained access to the "to_break_educational" network perform a man in the middle ARP attack. The ARP poison may require multiple machines and you are allowed to use virtual machines or physical devices from members in the group.

You are also free to perform any other man in the middle attacks other than ARP if you wish to do so.

If you are unable to get to access to "to_break_educational" network you can do the man in the middle attacks on virtual machines.

In the exercise 2 answer you must include:

1. describe which tools or languages are used to perform the man in the middle attack and screenshots of the poisoned ARP cache ?
2. how to could the man in the middle attack be prevented ?

Exercise 3: BEAST SLL vulnerability

BEAST SLL threat was a vulnerability that existed in TLS 1.0 and earlier protocols. You should explain in details what the vulnerability was and how to prevent BEAST SSL attacks.