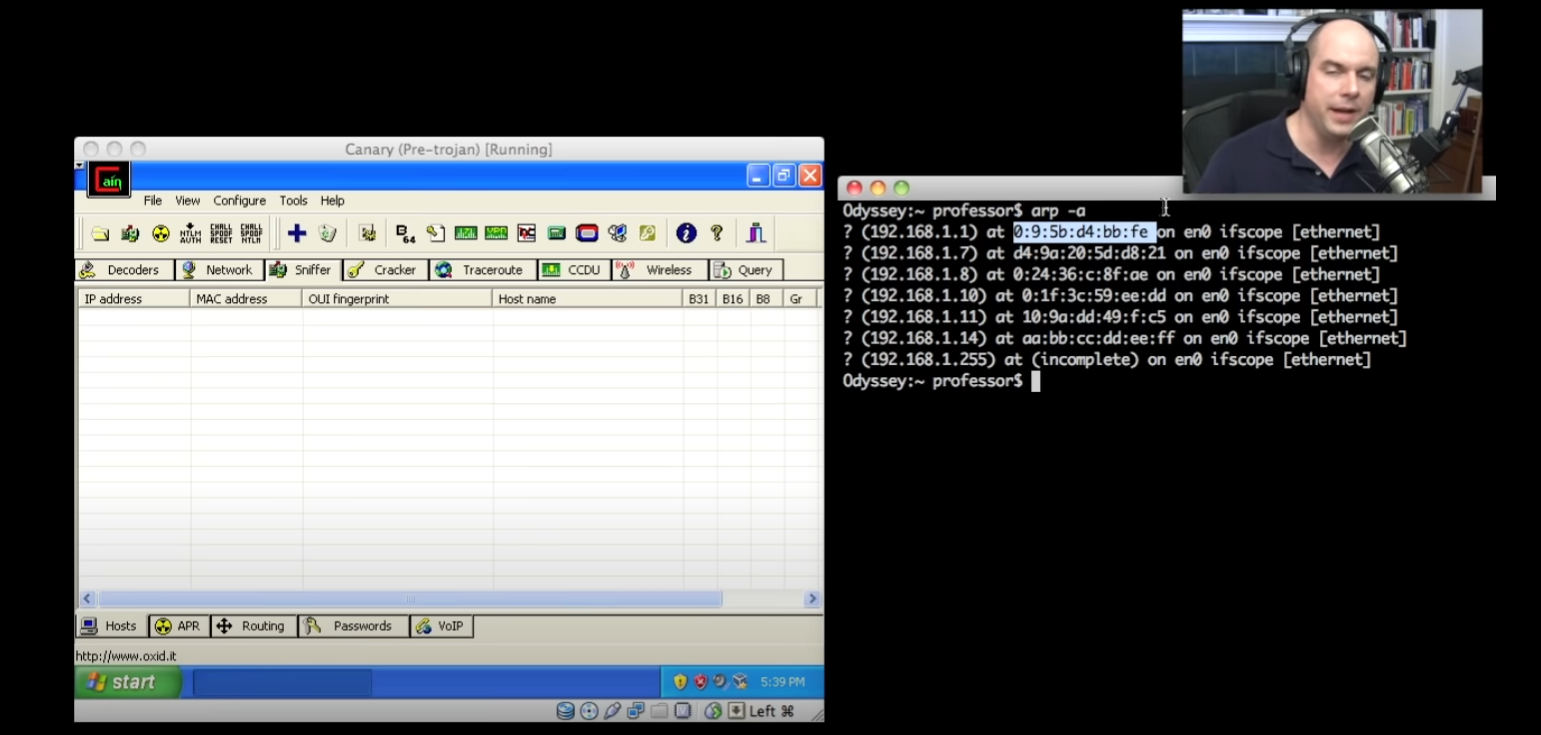
**IOT & Cyber Security**

~Week 3-4~

Man In the Middle Attack

**Reflection based on two videos:**

In the first video it shows the details and basically steps of the attack and implements it using a third-party application. A man-in-the-middle (MITM) attack is a type of cyber-attack where an attacker intercepts communication between two parties and can manipulate or view the data being transmitted. Here are the steps that an attacker might follow to perform a MITM attack:

1. The attacker first needs to find a way to intercept the communication between the two parties. This can be done through various methods such as using a rogue access point, ARP spoofing, or DNS spoofing.
2. Once the attacker has intercepted the communication, they can start manipulating or viewing the data being transmitted. For example, the attacker might alter messages being sent between the two parties, or they might simply listen in on the conversation to gather sensitive information.
3. The attacker can then continue to intercept and manipulate the communication until they are satisfied with the amount of information they have gathered or the damage they have caused.
4. The attacker may also choose to relay the communication between the two parties, pretending to be one of the parties to remain undetected.
5. Diagram

   Description automatically generatedGraphical user interface, application

   Description automatically generatedEventually, the attacker may decide to end the attack and stop intercepting the communication. They might do this either because they have achieved their goal or because they have been detected and are trying to cover their tracks.

It is important to note that MITM attacks can be difficult to detect, as communication between the two parties may appear normal and no errors may be reported. Therefore, it is important to take steps to protect against these types of attacks, such as using encryption and secure protocols.

Graphical user interface, application

Description automatically generatedIn the second video, the scenario was simpler and more usual than the first one. It gave real world examples such as a hacker who brings his laptop to café and creates a bait Wi-Fi to let other customers connect to internet via himself. When customers hit their credentials on any website using hacker’s Wi-Fi, hackers can see their credentials because of Network sniffing tool.

**Operation of man-in-the-middle attacks in the context of enterprise networks:**

In the context of an enterprise network, an MITM attack could be carried out by an employee who has access to the network, or by an outsider who has gained access to the network through, for example, a phishing attack or by exploiting a vulnerability in the network.

Once the attacker has positioned themselves in the middle of the communication, they can potentially read, alter, or block the communication as they see fit. For example, an attacker could intercept and alter an email being sent from one employee to another, or they could intercept and read sensitive information being transmitted between systems on the network.

To protect against MITM attacks, it is important for organizations to use secure communication protocols, such as SSL/TLS, and to use strong authentication methods to verify the identity of parties involved in a communication. It is also important to regularly update and patch systems and to educate employees on how to recognize and avoid phishing attacks.

17330118 – Mustafa Guner