Ex.No: 6	Experiment Eavesdropping, Dictionary Attack, MITM Attacks.

Aim:

To experiment Eavesdropping, Dictionary Attack, MITM Attacks.

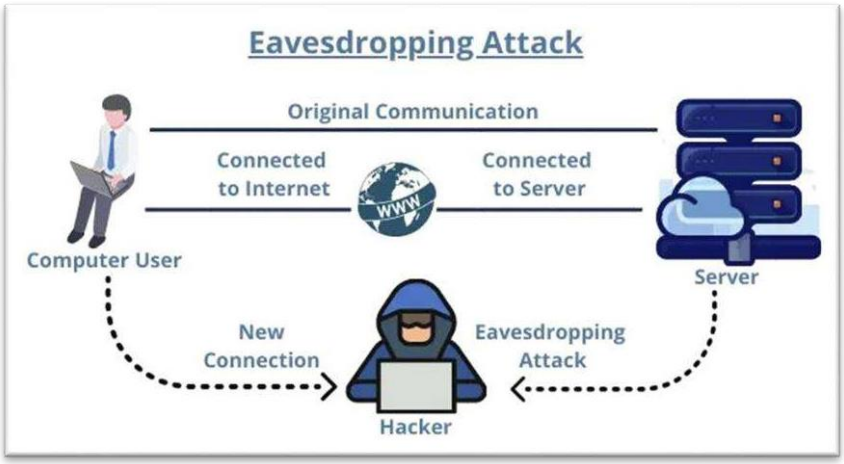
EAVESDROPPING:

Eavesdropping refers to the unauthorised and unseen intervention of a private, live conversation.

Sniffing or Eavesdropping pertains to the act of acquiring or intercepting data by capturing thecommunication flow within a network using a packet sniffer tool.

This technique involves monitoring the packets of information passing through the network,allowing unauthorized access to sensitive data, akin to theft or unauthorized interception of information.

During the transmission of data across networks, if the data packets lack encryption, they become vulnerable to interception, enabling unauthorized parties to read the contents of these network packetswith the use of a sniffer.



Categories of Network Sniffing:

Active and Passive Sniffing attacks are two distinct categories of network sniffing techniquesused by attackers to intercept and analyze data traffic.

1. **Active Sniffing:**

Active Sniffing is performed through a Switch and it is easy to detect.

It involves more direct interaction with the network traffic. Instead of just observing and capturing data, the attacker actively injects or modifies packets within the communication flow.

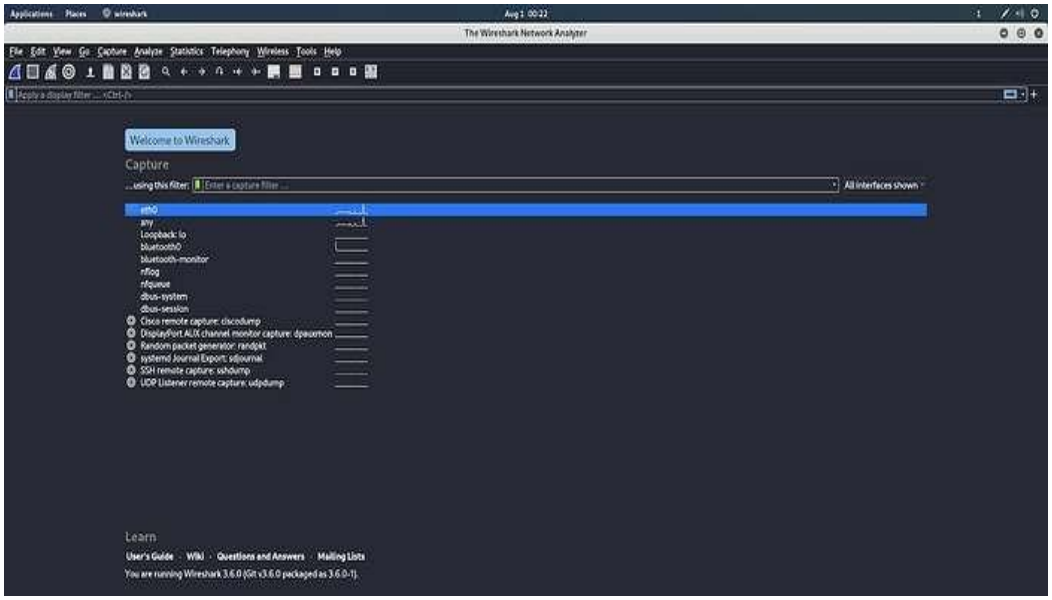
2.Passive Sniffing:

Passive Sniffing is performed through a Hub which is difficult to detect.

It involves silently capturing and monitoring network traffic without altering or modifying thedata being transmitted. The attacker's presence is relatively discreet, as they do not actively participate in the communication process. They just observe the data that flows through the network, looking for sensitive/crucial information that is not encrypted.

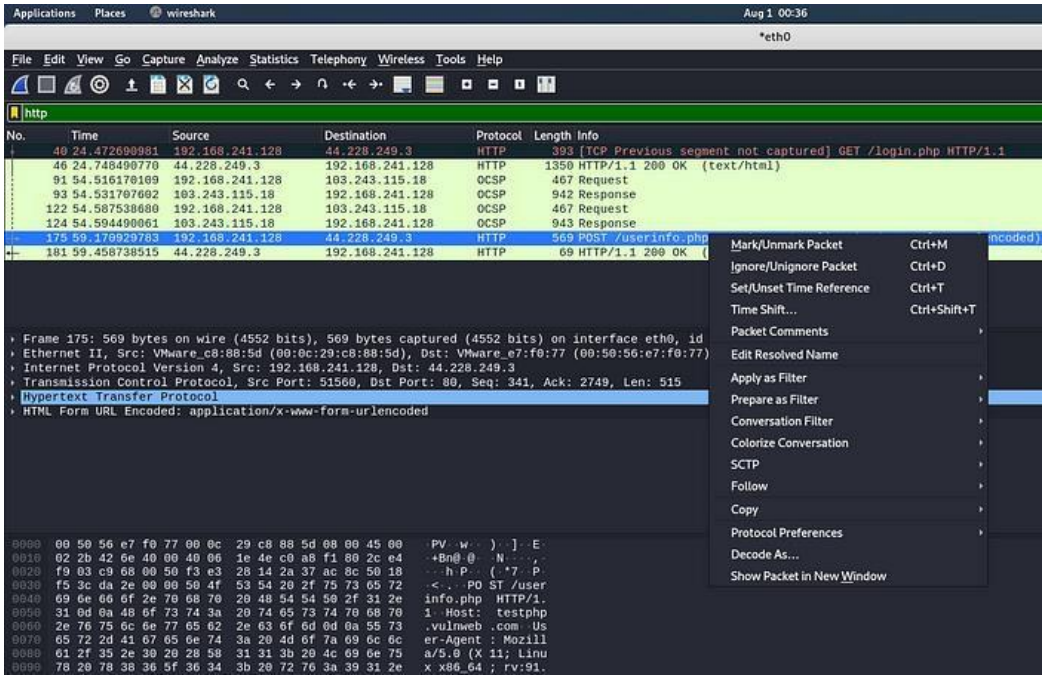
Experimenting Eavesdropping:

Step 1: Launch the Wireshark software on your computer and choose the 'eth0' option, In your webbrowser, input the URL we want to capture login credentials from.



Step 2: Input the login credentials, which are 'test', and then click on the login button.

Step 3: Then by entering 'http' in the filter section, the captured packets using the HTTP protocol willbe shown. Choose 'Follow' to access additional options, then select 'http stream' from the available choices.



Step 4: Explore the provided information, and you will uncover the login credentials.

Output:

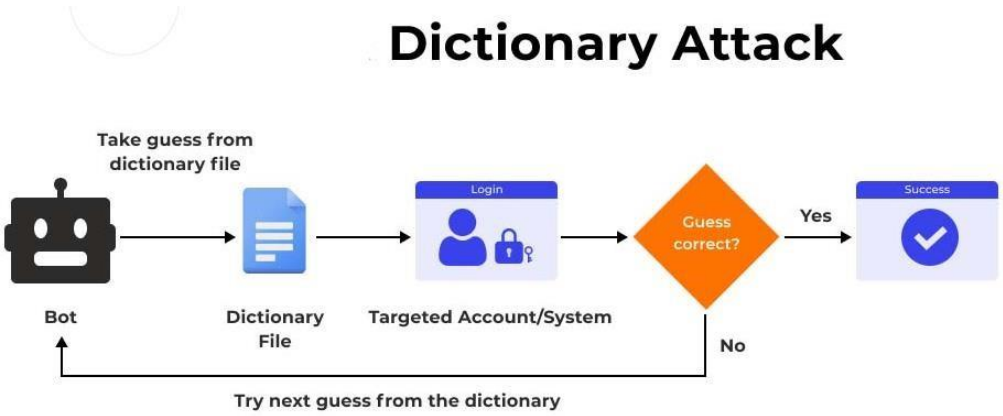
DICTIONARY ATTACK:

A Dictionary Attack is an attack vector used by the attacker to break in a system, which is password protected, by putting technically every word in a dictionary as a form of password for thatsystem. This attack vector is a form of Brute Force Attack.

Like the brute force attack, the dictionary attack aims to break in by logging in using usernameand password combinations. It is only inefficient as far as its overall success rate: automated scriptscan do this in a matter of seconds.

A hacker will look for applications and websites that don't lock a user out quickly for incorrectusername and password combinations and don't require other forms of authentication when signing in. Sites that allow simple passwords are especially vulnerable.

Suppose the target website or application does not adequately monitor suspicious behavior likethis or has lax password rules. In that case, the website runs a high risk of data disclosure resulting from a dictionary attack. Leaked password databases have become a common feature of modern dictionary attacks. Attempting to log in with username and password combinations used multiple times elsewhere makes these dictionary attacks much more successful and potentially harder to detect on the application or website's end.



Result:

Thus, Eavesdropping and Dictionary Attack have been implemented successfully.