

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

Aim:

To experiment Eavesdropping, Dictionary Attack, MITM Attacks.

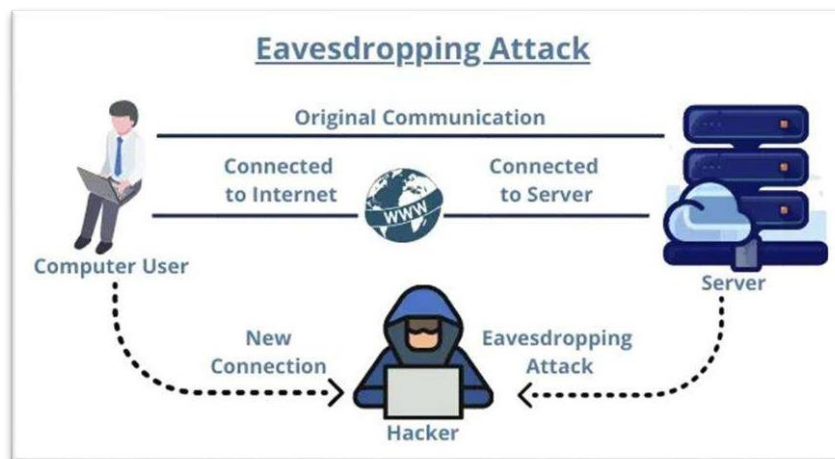
EAVESDROPPING:

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 the communication 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 packets with the use of a sniffer.

**Categories of Network Sniffing:**

Active and Passive Sniffing attacks are two distinct categories of network sniffing techniques used 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.

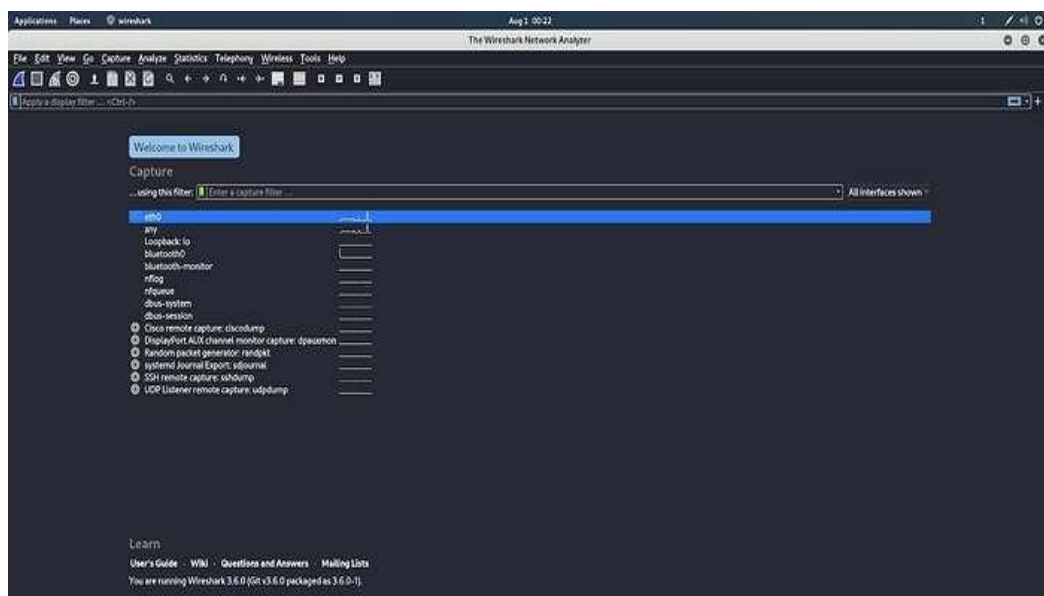
2.Passive Sniffing:

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

It involves silently capturing and monitoring network traffic without altering or modifying the data 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.

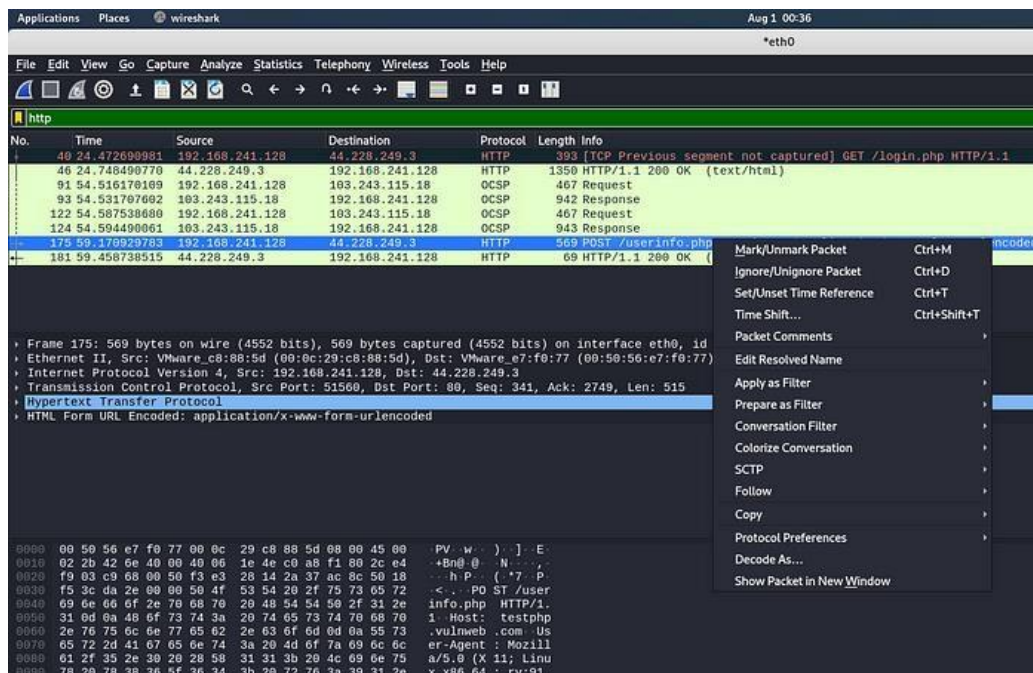
Experimenting Eavesdropping:

Step 1: Launch the Wireshark software on your computer and choose the 'eth0' option, In your web browser, 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 will be 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:

```
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:12px;padding:1px">
<p style="padding-left:5%;padding-right:5%;<b>Warning</b><b>: This is not a real shop. This is an example PHP application, which is
intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and
bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well.
Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.</p>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.6
Date: Tue, 01 Aug 2023 05:34:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideLocked="false" -->
<head>
```

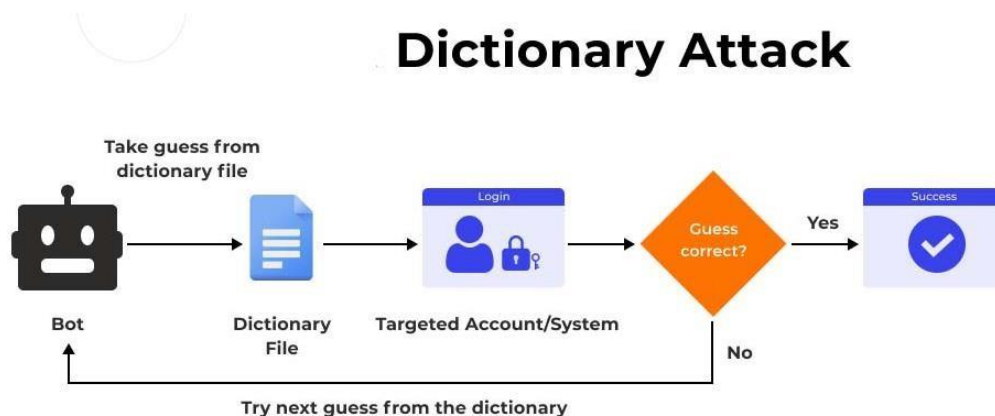
DICTIONARY ATTACK:

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 that system. 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 username and password combinations. It is only inefficient as far as its overall success rate: automated scripts can do this in a matter of seconds.

A hacker will look for applications and websites that don't lock a user out quickly for incorrect username 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 like this 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.