MITM Attack

⚠️ **Important:** MITM attacks are **illegal** if done on real networks or without permission. You **must only** practice this in a **controlled lab environment** (like a virtual lab or simulation) where all devices involved are yours or you're authorized to test.

What is MITM Attack?

MITM Attack is a type of cyber attack where attacker attack your devices to gather information like email, messages, photos, videos, bank details and other personal information from your devices. A **MITM attack** (short for **Man-in-the-Middle attack**) is like someone secretly eavesdropping on a conversation between two people and sometimes even changing what's being said — but in the digital world.

Simple Example:

Imagine you're talking to your friend on the phone about a secret. But without you knowing, someone taps into the line and listens in. Worse, they might change what your friend says before it reaches you.

In a **MITM attack**, this happens between two computers or a user and a website. The attacker sits in the middle of your connection — for example, between your phone and a bank website — and can gather information that you done in bank website like money transaction, password change and other activities. Attacker will capture information from the device and you will be unknown about that.

Common Places it Happens:

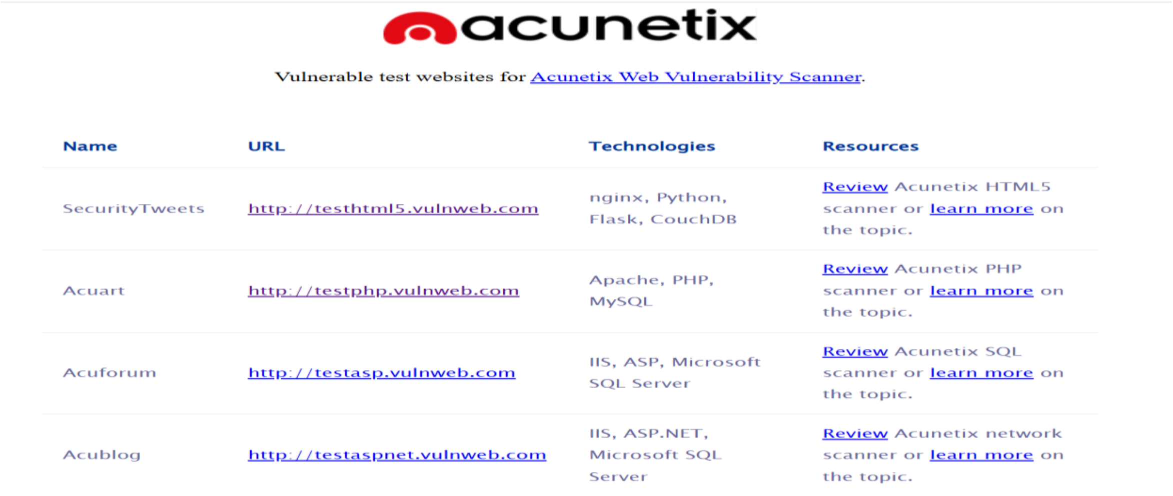
- Public Wi-Fi (coffee shops, airports)
- Fake websites
- Unsecured networks (no HTTPS)

Sure! Here's the grammatically corrected version of your instructions with clearer wording:

MITM Attack Using Ettercap and Wireshark (For Educational Purposes in a Lab Environment Only)

1. On the **attacker machine**, open **Ettercap**.
2. Select the **network interface** based on your OS environment (e.g., eth0, wlan0).
3. After setting the interface, click on the **Accept** icon.
4. Scan the IP addresses connected to the internet.

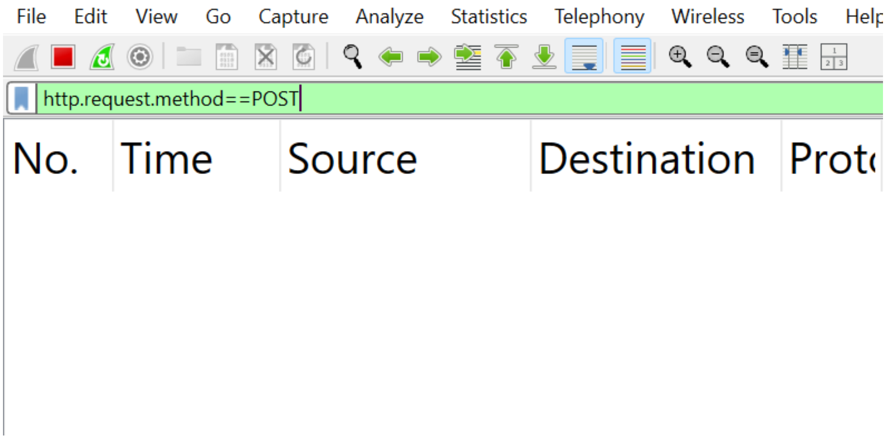
5. Once scanning is complete, it will display a message like "16 hosts added to the host list."
6. Click on the **Host List** icon (located near the search icon).
7. In the host list, set the **victim's IP address as Target 1** and the **router's IP address as Target 2**.
8. After setting the targets, click on the **Menu** icon.
9. Under the list of attacks, choose **ARP Poisoning**.
10. After starting ARP poisoning, open **Wireshark** for packet analysis.
11. Select the same network interface (e.g., eth0) in Wireshark.
12. Now packets will start appearing in Wireshark.
13. While packet analysis is ongoing, go to the **victim system** and open a browser.
14. Visit http://www.vulnweb.com.
15. Click on the **second link** on the page (as shown in your reference image).
16. Once the page opens, click on **Sign Up**.
17. Enter a **username** and **password**, then submit the form.
18. Go back to the **attacker machine** and search in Wireshark using the filter:
19. http.request.method == POST
20. Click the matching packet from the list.
21. Click the **arrow icon** to expand the details.
22. Look under the **HTML Form URL** section to see the captured **username and password**.



acunetix

Vulnerable test websites for Acunetix Web Vulnerability Scanner.

Name	URL	Technologies	Resources
SecurityTweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB	Review Acunetix HTML5 scanner or learn more on the topic.
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL	Review Acunetix PHP scanner or learn more on the topic.
Acuforum	http://testasp.vulnweb.com	IIS, ASP, Microsoft SQL Server	Review Acunetix SQL scanner or learn more on the topic.
Acublog	http://testaspnet.vulnweb.com	IIS, ASP.NET, Microsoft SQL Server	Review Acunetix network scanner or learn more on the topic.



http.request.method==POST

No.	Time	Source	Destination	Prot