6. Man-in-the-Middle(MITM) Attack

Objective: To understand how MITM attacks and manipulate network traffic
Tools: Ettercap, Wireshark

A Man-in-the-Middle (MITM) attack is a type of cyberattack where an attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. Here's a more detailed look at how it works and how to protect against it:

How MITM Attacks Work

1. **Interception**: The attacker intercepts the communication between the two parties. This can be done through various methods, such as exploiting insecure Wi-Fi networks or using malicious software to redirect traffic.
2. **Eavesdropping**: The attacker listens in on the communication, capturing sensitive information such as login credentials, personal details, or financial data.
3. **Manipulation**: In some cases, the attacker may alter the communication, injecting false information or commands that could mislead the parties involved or cause harm.
4. **Impersonation**: The attacker might impersonate one of the parties in the communication, making it seem as though they are the legitimate sender or receiver.

Common Methods of MITM Attacks

- **Wi-Fi Eavesdropping**: Attackers can set up rogue Wi-Fi hotspots to capture data from users who connect to them.
- **DNS Spoofing**: The attacker corrupts the Domain Name System (DNS) responses to redirect users to malicious websites.
- **Session Hijacking**: The attacker steals or predicts session tokens to gain unauthorized access to a user's session.
- **SSL Stripping**: The attacker downgrades a secure HTTPS connection to an unencrypted HTTP connection to intercept data.

How to Protect Against MITM Attacks

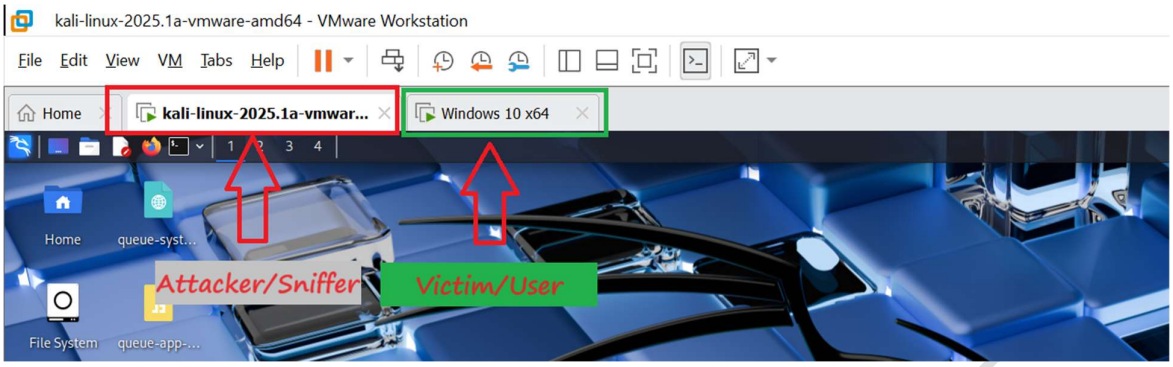
1. **Use Encryption**
2. **Verify Certificates**
3. **Avoid Unsecured Wi-Fi**
4. **Implement Strong Authentication Keep Software Updated**
5. **Educate Users**

By implementing these measures, you can significantly reduce the risk of falling victim to a MITM attack.

Man-in-the-Middle Attack MITM Using Wireshark

Step 1: Set up two virtual machines: a **Windows VM as the victim/user** and a **Kali Linux VM as the attacker/sniffer**.

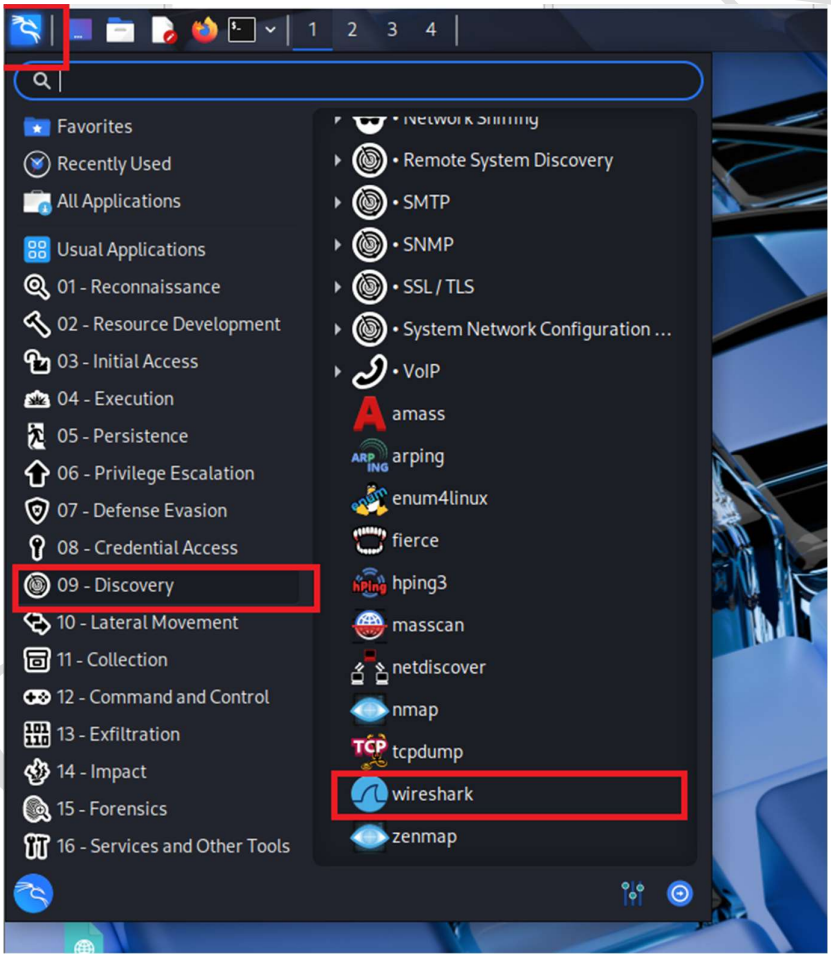
CSE(CY), RNSIT



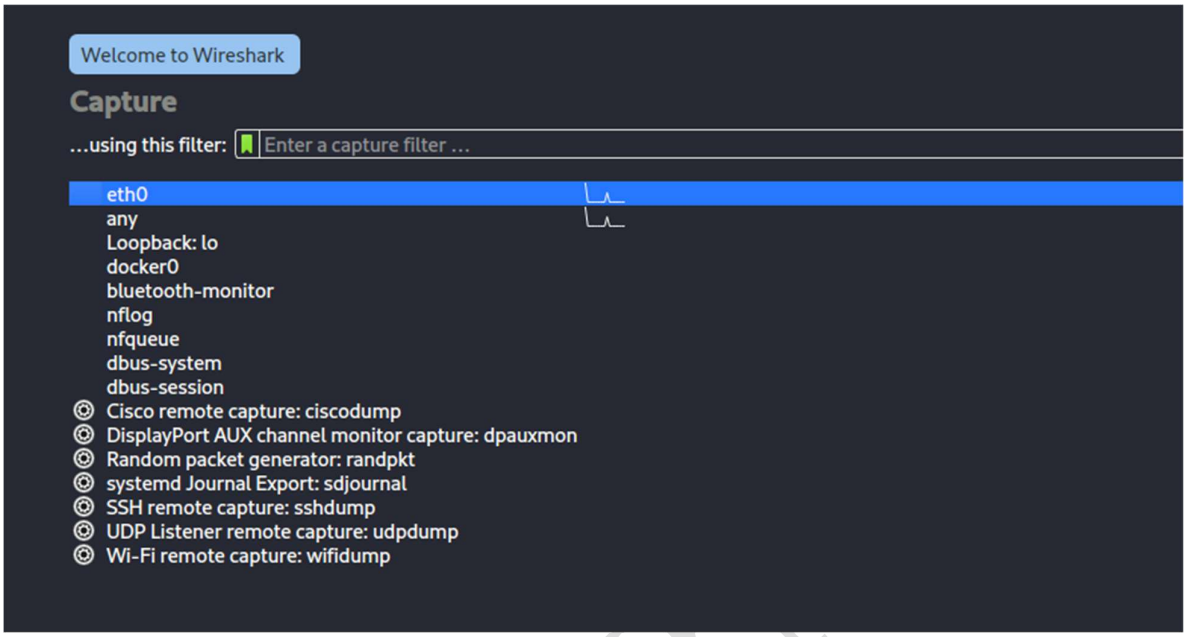
Connect both VMs to the same isolated network to simulate a **public Wi-Fi**. Take snapshots of both VMs so you can **restore them** if needed.

VM ⟶ Snapshot ⟶ Take Snapshot ⟶Name ⟶ Enter

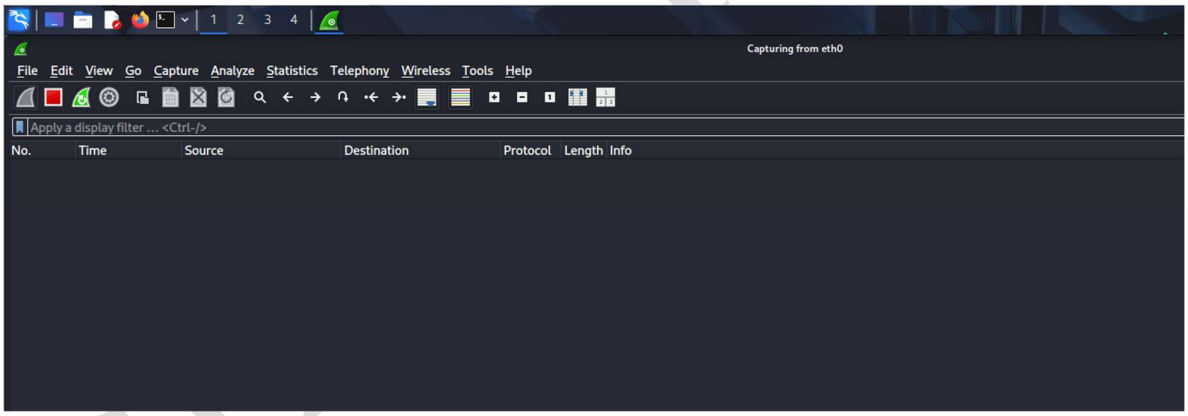
Step 2: Click on the application, select **Discovery**, and then choose **Wireshark** from the list. Click on it to open Wireshark.



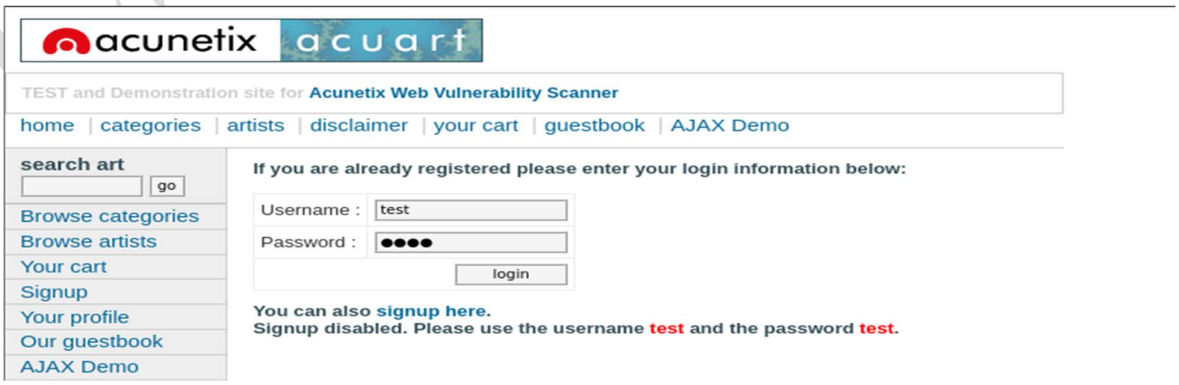
Step 3: You will see a list of network adapters; since we are working on **Ethernet 0 (eth0)**, double-click on it.



This will start capturing packets on that interface, allowing you to monitor all traffic on the subnet.



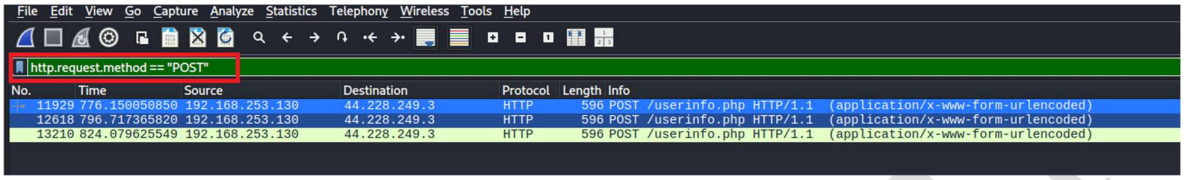
Step 3: On the Windows VM, open the browser and navigate to http://testphp.vulnweb.com/ login page. Enter the **username** and **password** as test and test, then click **Login** to submit the credentials.



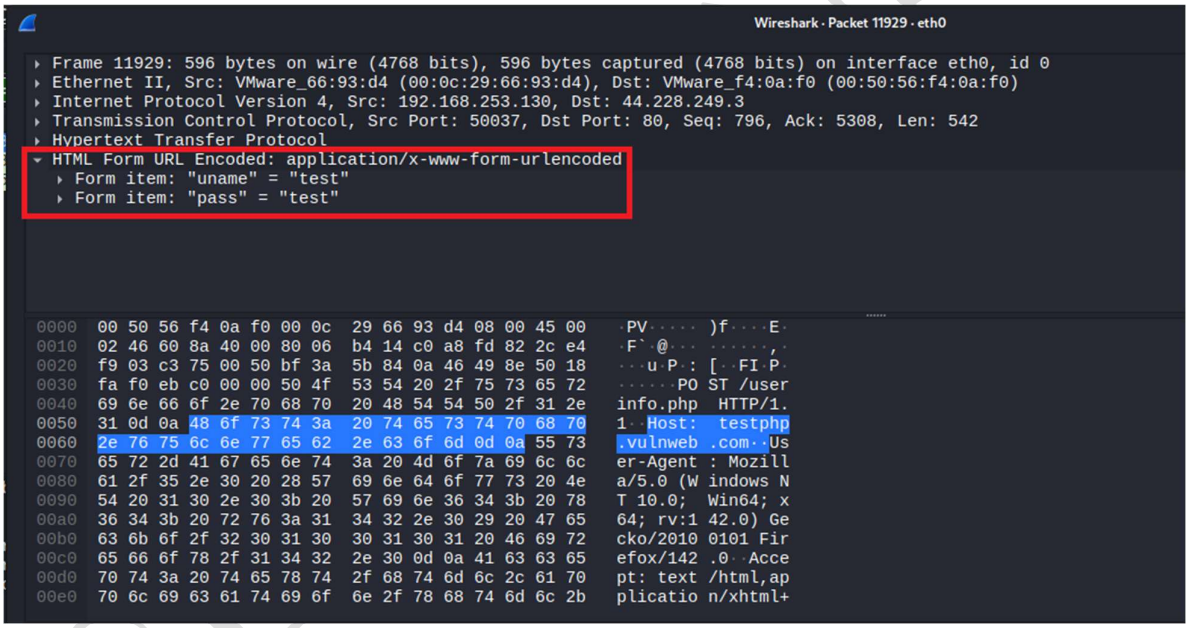
Step 4: Go back to the Kali Linux VM. After Wireshark has captured the login credentials, **stop the packet capture** by clicking on the red **Stop** button and selecting **Stop**. To find the packet containing the username and password, apply the display filter:

http.request.method == "POST"

Press **Enter** to apply the filter and isolate the POST request carrying the credentials.

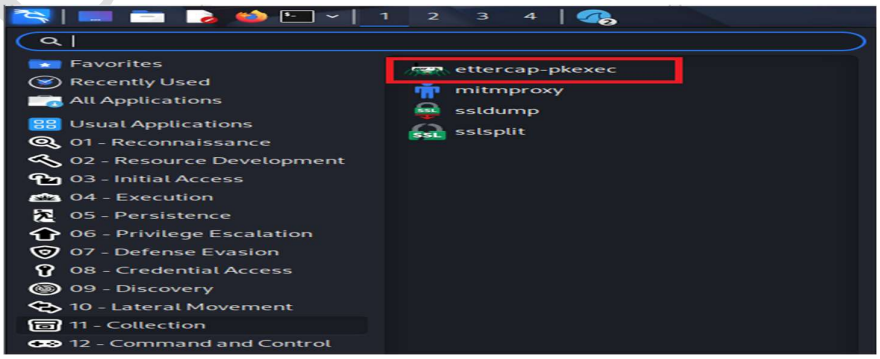


Step 5: On the Kali Linux VM, locate the POST packet in the filtered results. You can identify the packet by **double-clicking on the Windows machine's IP address** in the packet details. Expand the HTTP section and check the Request Body, where the captured credentials will appear as: **username=test & password=test**



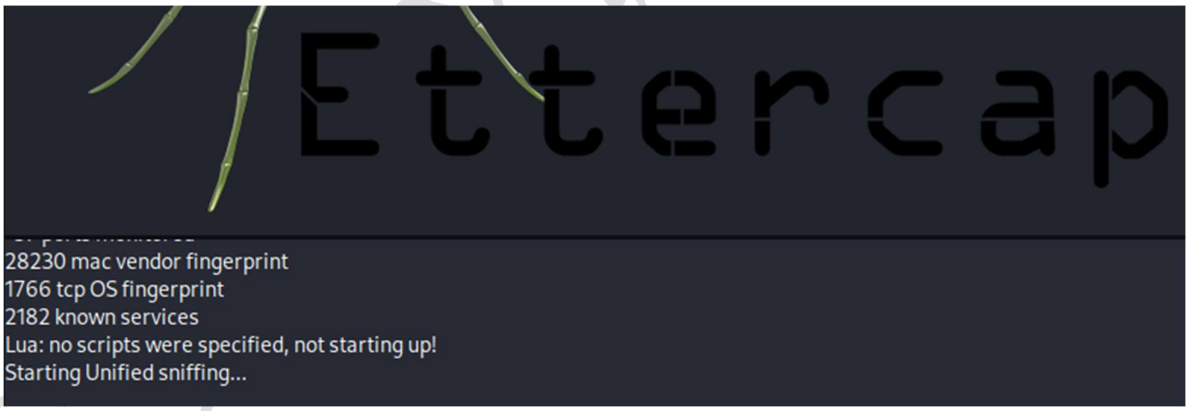
Man-in-the-Middle Attack MITM Using Ettercap

Step 1: Open Kali Linux VM. Click on the application, select **Collection**, and then choose **Ettercap** from the list. Click on it to open Ettercap.

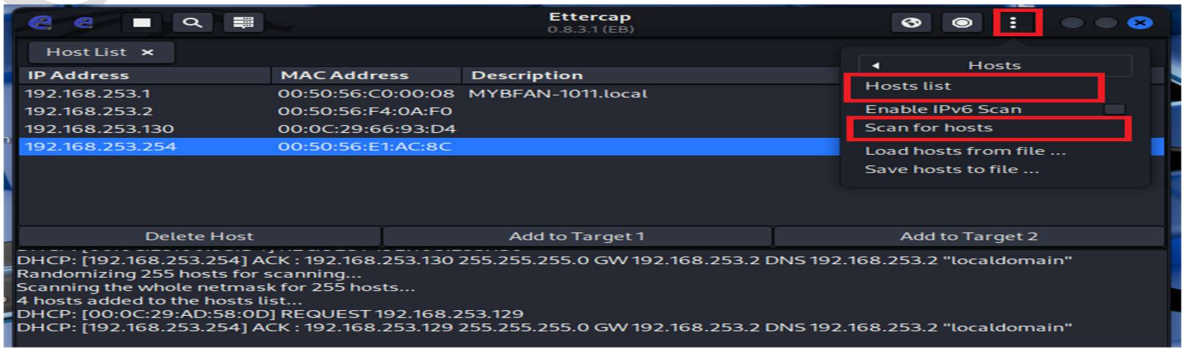


Step 2: Go to the **Setup** section in Ettercap. Under Primary Interface, select the network adapter connected to the internet, which is **Ethernet 0 (eth0)**. On the right side, click the **checkmark (✓) symbol** to confirm.

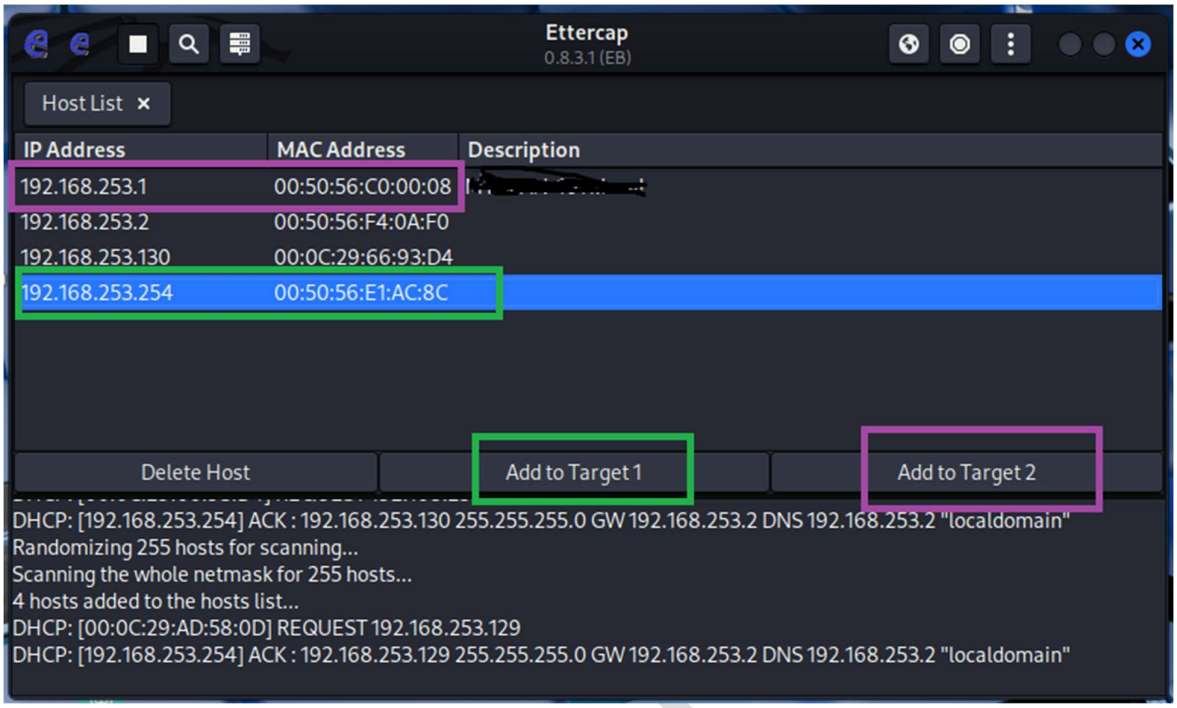
This will start **unified sniffing** on the selected interface.



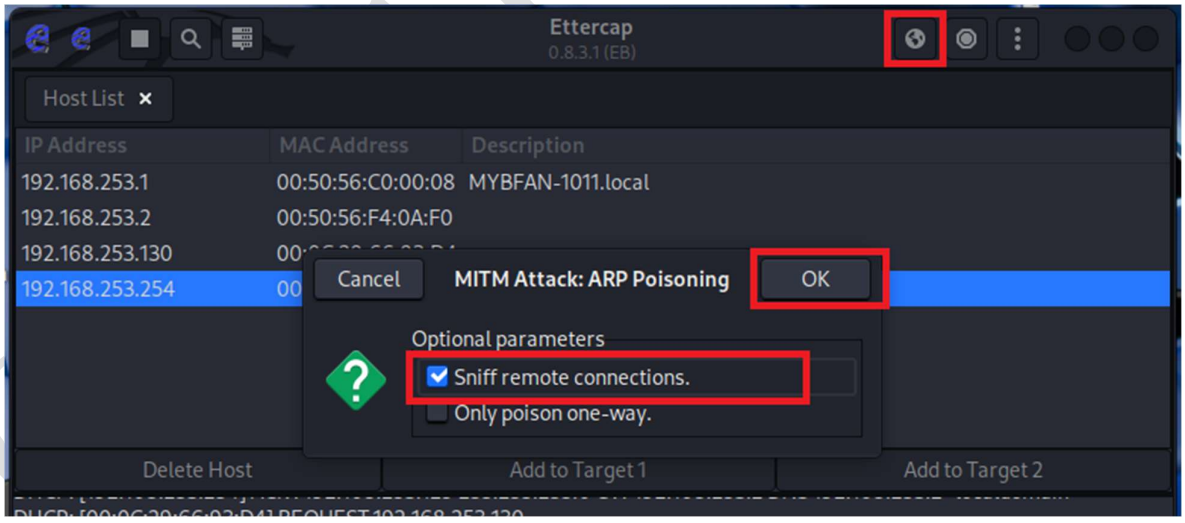
Step 3: In Ettercap, go to the **Host** menu and select **Host List**. Click on **Scan for Hosts** to detect all devices connected to the network. After scanning for hosts,



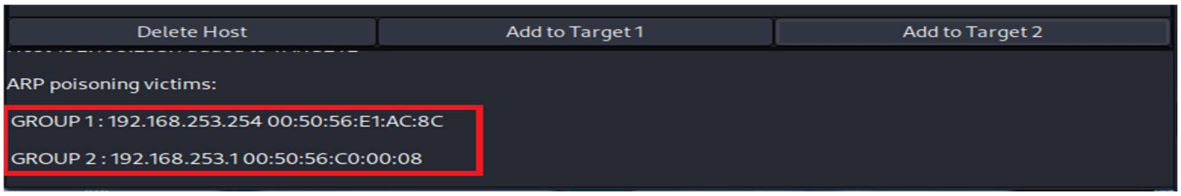
select the **victim machine's IP address** and click **Add to Target 1**(.). Then, select the **gateway IP address** and click **Add to Target 2** (.). Both the victim and gateway are now set as targets for the MITM attack.



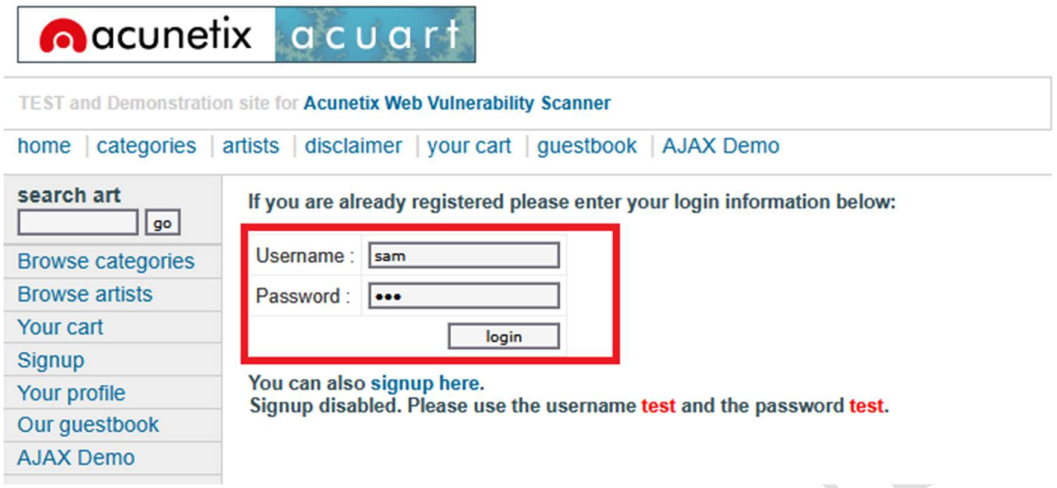
Step 4: Open the **MITM** menu and choose **ARP Poisoning** (Address Resolution Protocol poisoning). In the ARP Poisoning dialog, check **Sniff remote connections** (or **Sniff remote hosts**) and click **OK** to begin.



Ettercap will now poison ARP caches for Target 1 (victim) and Target 2 (gateway) and start intercepting their traffic.

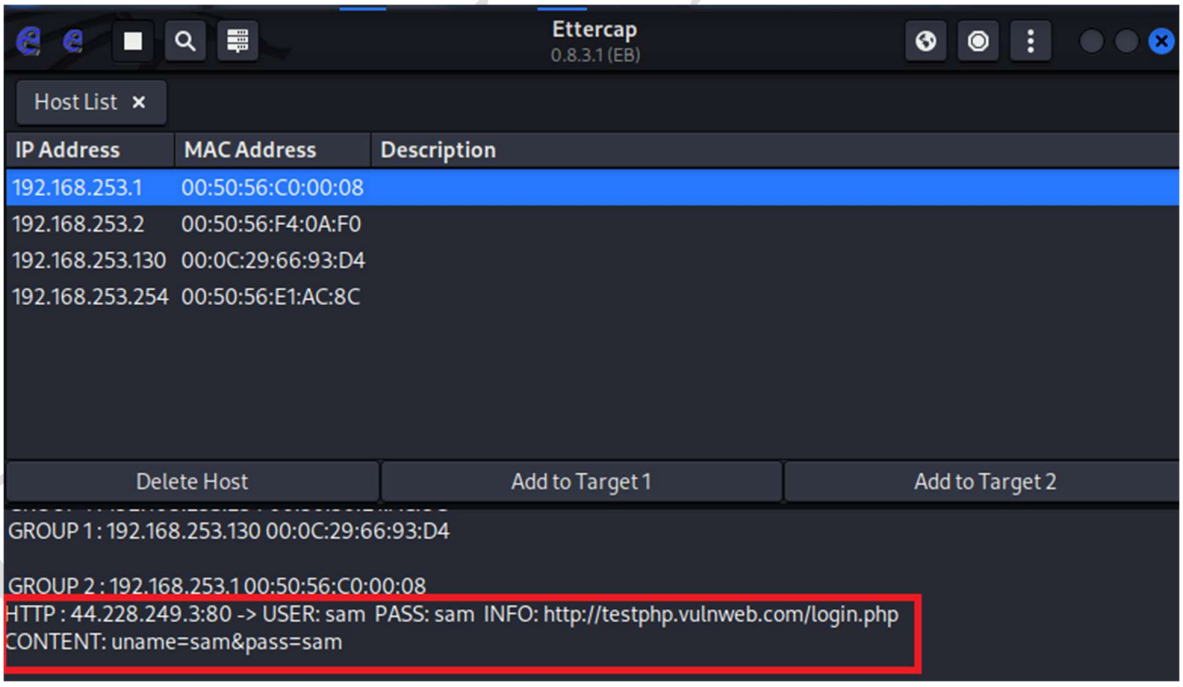


Step 5: On the **Windows VM**, open the browser and navigate to the vulnerable login page http://testphp.vulnweb.com/. Enter example credentials (e.g. **username:** sam, **password:** sam) and click **Login** to submit the form.



Switch back to the **Kali VM** and check Ettercap for the intercepted traffic. In Ettercap look at the **Connections / Logs / Hosts** window or the packet console — you should see the HTTP POST request from the victim. The request body will contain the submitted credentials (for example):

username=sam & password=sam



Ref: **https://www.youtube.com/watch?v=DElzWHWDG9Q&ab_channel=UbuntuManiac**

Viva Questions:

1. **What is a Man-in-the-Middle (MITM) attack?**
   A MITM attack occurs when an attacker secretly intercepts and manipulates communication between two parties.
2. **How does a MITM attack work?**
   The attacker positions themselves between the sender and receiver to eavesdrop, alter, or inject malicious data into the communication.
3. **What are common tools used for MITM attacks?**
   Ettercap, Wireshark, BetterCAP, and ARP spoofing tools can be used to perform and analyze MITM attacks.
4. **What role does Ettercap play in a MITM attack?**
   Ettercap is used for ARP poisoning, DNS spoofing, and intercepting network traffic in real time.
5. **How does ARP spoofing help in MITM attacks?**
   ARP spoofing tricks devices into sending data to the attacker instead of the legitimate recipient by poisoning the ARP cache.
6. **How can attackers use Wireshark in a MITM attack?**
   Wireshark captures and analyzes network packets to extract sensitive information like credentials or session cookies.
7. **What are the consequences of a MITM attack?**
   Attackers can steal credentials, alter messages, inject malware, or hijack user sessions.
8. **How can MITM attacks be prevented?**
   Use HTTPS, VPNs, encrypted protocols, ARP inspection, and avoid unsecured Wi-Fi networks.
9. **What is SSL stripping in MITM attacks?**
   SSL stripping downgrades HTTPS connections to HTTP, allowing attackers to intercept and read unencrypted traffic.
10. **How does HSTS help prevent MITM attacks?**
    HTTP Strict Transport Security (HSTS) forces browsers to use HTTPS, preventing SSL stripping attacks.

CSE-CY, RNSIT