

MAN IN THE MIDDLE MANUAL



Team Members:

Muhammad Zain-ul-abideen | 201002

Abdul Moiz | 200976

Ahmad Muhammad Jaffar | 200964

Use Ettercap to Intercept Passwords with ARP Spoofing

What is ARP spoofing?

ARP spoofing is an attack against an Ethernet or Wi-Fi network to get between the router and the target user. In an ARP-spoofing attack, messages meant for the target are sent to the attacker instead, allowing the attacker to spy on, deny service to, or man-in-the-middle a target. One of the most popular tools for performing this attack is Ettercap, which comes preinstalled on Kali Linux.

On a regular network, messages are routed over Ethernet or Wi-Fi by associating the MAC address of a connected device with the IP address used to identify it by the router. Usually, this happens via an address resolution protocol (ARP) message indicating which device's MAC address goes with which IP address. It lets the rest of the network know where to send traffic – but it can be easily spoofed to change the way traffic is routed.

In an ARP-spoofing attack, a program like Ettercap will send spoofed messages attempting to get nearby devices to associate the hacker's MAC address with the IP address of the target. When successful, they're stored temporarily in a configuration setting on other network devices. If the rest of the network starts delivering packets intended for the target to the attacker instead, the attacker effectively controls the target's data connection.

Ettercap Graphical:

One of the most intriguing programs installed by default in Kali Linux is Ettercap. Unlike many of the programs that are command-line only, Ettercap features a graphical interface that's very beginner-friendly. While the results may sometimes vary, Ettercap is an excellent tool for newbies to get the hang of network attacks like ARP spoofing. If you don't already have it (like if you downloaded a light version of Kali), you can get it by typing the following into a terminal window.

```
apt install ettercap-graphical
```

Ettercap isn't the only tool for this, nor is it the most modern. Other tools, such as Bettercap, claim to do what Ettercap does but more effectively. However, Ettercap proves useful enough to feature for our demonstration. The general workflow of an

Ettercap ARP spoofing attack is to join a network you want to attack, locate hosts on the network, assign targets to a "targets" file, and then execute the attack on the targets

Once we do all of that, we can figuratively watch over the target's shoulder as they browse the internet, and we can even kill the connection from websites we want to steer them away from. We can also run various payloads, like isolating a host from the rest of the network, denying them service by dropping all packets sent to them, or running scripts to attempt to downgrade the security of the connection.

Connect to network:

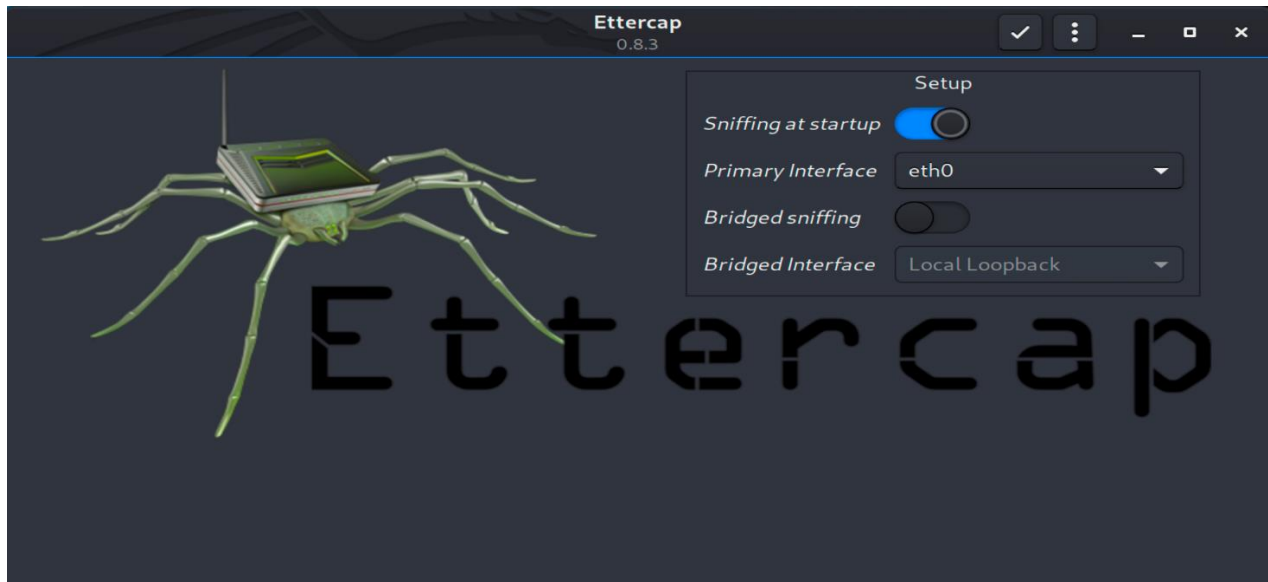
The first step of ARP spoofing is to connect to the network you want to attack. If you're attacking an encrypted WEP, WPA, or WPA2 network, you'll need to know the password. This is because we're attacking the network internally, so we need to be able to see some information about the other hosts on the network and the data passing within it. You can connect to a network for ARP spoofing in two ways. The first is to connect via Ethernet, which is very effective but may not always be practical and is rarely subtle. Instead, many people prefer to use a wireless network adapter and perform the ARP spoofing over Wi-Fi.

Start Ettercap

In Kali, click on "Applications," then "Sniffing & Spoofing," followed by "ettercap-graphical." Alternatively, click on the "Show Applications" option in the dock, then search for and select "Ettercap."



Once it starts up, you should find yourself on the Ettercap main screen. You'll see the spooky Ettercap logo, and a few drop-down menus to start the attack from. In the next step, we'll start exploring the "Sniff" menu.



Select Network Interface to Sniff On:

Click on the "Sniff" menu item, and then select "Unified sniffing." A new window will open asking you to select which network interface you want to sniff on. You should select the network interface that is currently connected to the network you're attacking. In my case it was eth0.

Now, you'll see some text confirming that sniffing has started, and you'll be able to access more advanced menu options such as Targets, Hosts, Mitm, Plugins, etc. Before we get started using any of them, we'll need to identify our target on the network.

```
Listening on:
eth0 -> 00:0C:29:84:1C:37
192.168.171.136/255.255.255.0
fe80::20c:29ff:fe84:1c37/64

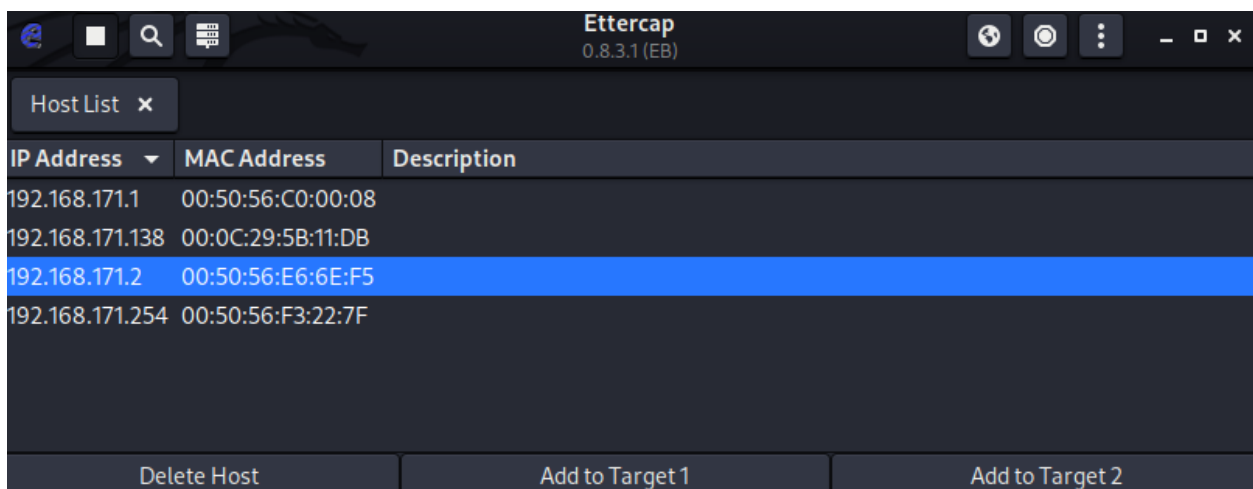
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534 EGID 65534...

34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
Host 192.168.171.2 added to TARGET1
Host 192.168.171.138 added to TARGET2
```

Identify Hosts on a Network:

To find the device we want to attack on the network, Ettercap has a few tricks up its sleeve. First, we can do a simple scan for hosts by clicking "Hosts," then "Scan for hosts." A scan will execute, and after it finishes, you can see the resulting hosts Ettercap has identified on the network by clicking "Hosts," then "Hosts list."



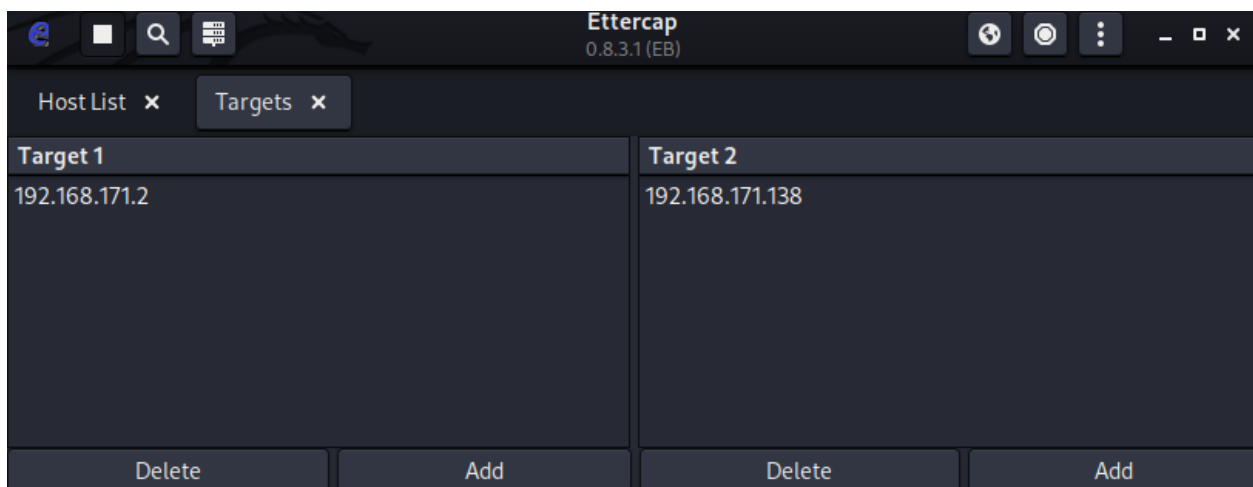
IP Address	MAC Address	Description
192.168.171.1	00:50:56:C0:00:08	
192.168.171.138	00:0C:29:5B:11:DB	
192.168.171.2	00:50:56:E6:6E:F5	
192.168.171.254	00:50:56:F3:22:7F	

FYI the ip addresses 192.168.171.2 and 192.168.171.138 are of my virtual router and windows virtual machine respectively.

Select Hosts to Target with ARP Spoofing:

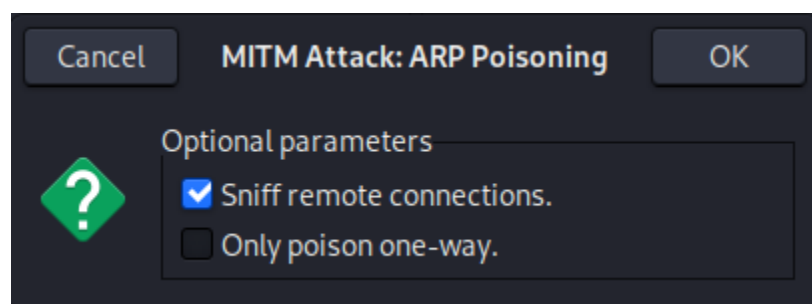
Now that we've identified our target's IP address, it's time to add them to a target list. Once we do this, we'll be telling Ettercap that we want to designate that IP address as one we want to pretend to be, so that we're receiving messages from the router that were meant to be sent to the target.

Go back to the "Hosts" screen, and select the IP address of the target you want to target. Click the IP address to highlight it, then click on "Targets," followed by "Target list," to see a list of devices that have been targeted for ARP spoofing.



Launch Attack on Targets:

Click on the "Mitm" menu, and select "ARP poisoning." A popup will open, and you'll select "Sniff remote connections" to begin the sniffing attack.



Once this attack has begun, you'll be able to intercept login credentials if the user you're targeting enters them into a website that doesn't use HTTPS. This could be a router or a device on the network or even a website that uses poor security.

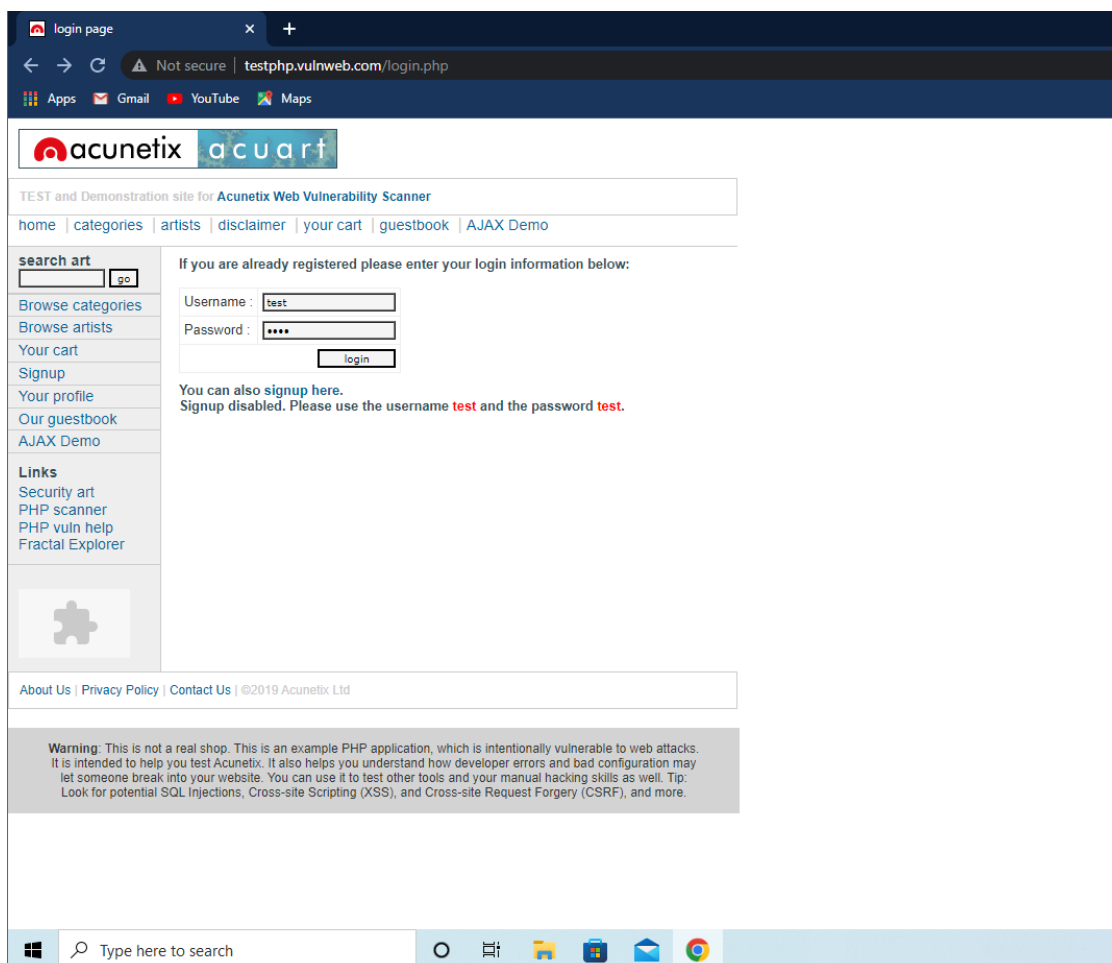
```
ARP poisoning victims:

GROUP 1 : 192.168.171.2 00:50:56:E6:6E:F5

GROUP 2 : 192.168.171.138 00:0C:29:5B:11:DB
```

Try Intercepting a Password:

Now, let's actually try intercepting a password. A website that's great for testing is aavtain.com, which deliberately uses bad security so that you can intercept credentials. On the target device, navigate to <http://testphp.vulnweb.com/> Once it loads, you'll see a login screen you can enter a fake login and password into.



Enter a username and password, then hit "Submit." If Ettercap is successful, you should see the login and password you typed appear on the attacker's screen!

```
GROUP 2 : 192.168.171.138 00:0C:29:5B:11:DB  
HTTP : 44.228.249.3:80 -> USER: test PASS: test INFO: http://testphp.vulnweb.com/login.php  
CONTENT: uname=test&pass=test
```

In this result above, we can see that Ettercap successfully ARP poisoned the target and intercepted an HTTP login request the target was sending to an insecure website.

AND THAT'S HOW YOU DEMONSTRATE MITM ATTACK BY ARP POISONING USING ETTERCAP.