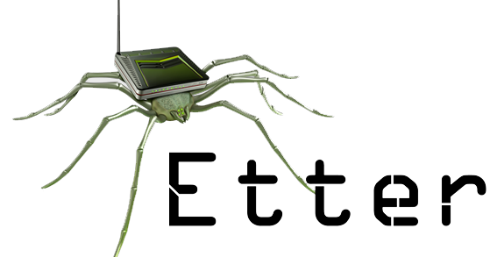
**LAB EXPERIMENT – 9**

**ARP Poisoning and 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](https://null-byte.wonderhowto.com/how-to/top-10-things-do-after-installing-kali-linux-0186450/).

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.

*Types of ARP Spoofing Attacks*

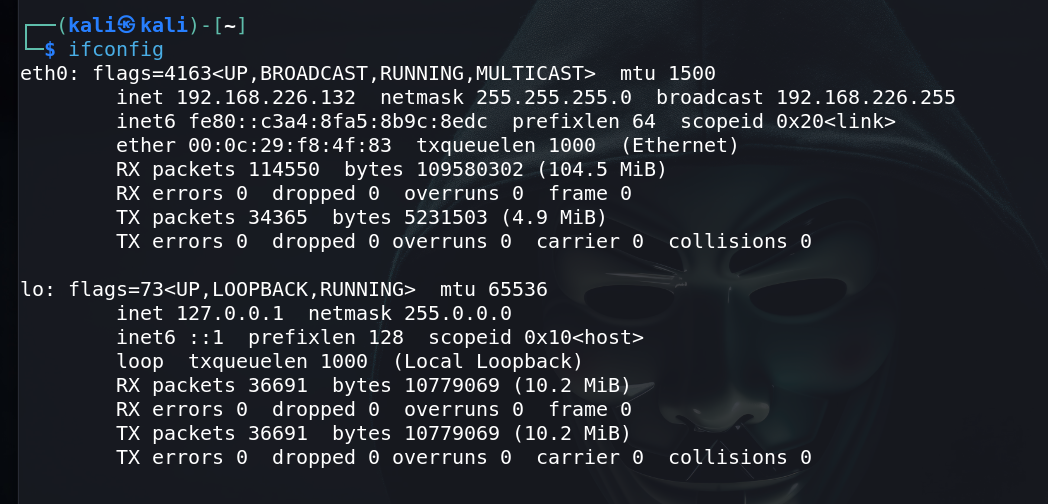
There can be three primary outcomes after an attacker gains initial success in poisoning the ARP cache of other hosts on the network:

* **The attacker can spy on traffic.** They can lurk in the shadows, seeing everything that the target user does on the network. It's pretty self-explanatory.
* **The attacker can intercept and modify the packets in a man-in-the-middle attack.** They can intercept passwords typed into an HTTP website, see DNS requests, and resolve IP addresses the target is navigating to in order to see what sites the target is visiting. In a man-in-the-middle attack, the attacker has the opportunity not only to see what's happening on the network but manipulate it as well. For instance, they can attempt to downgrade the encryption the connection is using by deliberately requesting insecure versions of webpages to make the attacker's job of sniffing passwords easier. Also, a hacker can simply be a nuisance. For example, they can replace words in the text of a website, flip or replace images, or modify other types of data flowing to and from the target.
* **The attacker can drop the packets meant for the target to create a denial-of-service attack.** This is possibly the most frustrating to a target. While a [Wi-Fi authentication attack](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/) is by far the more common cause of a Wi-Fi network being attacked, ARP spoofing can be much more challenging to figure out. If the attacker chooses not to forward on the packets now being sent to it instead of the target, the target will never receive them. The Wi-Fi network can be jammed from the inside, getting between the target and the router and then dropping the packets flowing between.

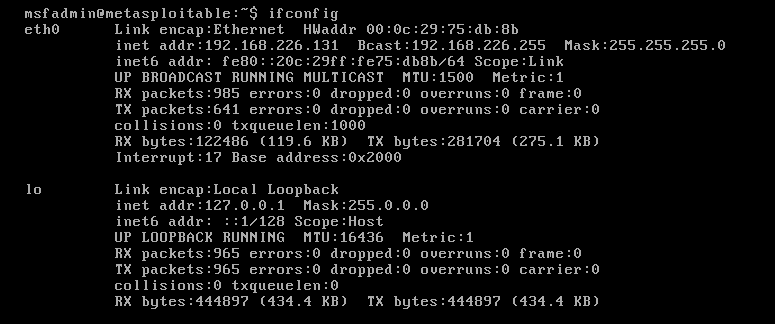
**So, we have 3 IP’s Setup for this Attack to be performed.**

* 192.168.226.132 **(KALI)** *From which the attack has to be performed*
* 192.168.226.1 **(WIN11)** *An ordinary System*
* 192.168.226.131 **(Meta server)** *Meta-exploitable 2.0 Server*
* 192.168.226.134 **(Ubuntu)** Victim OS

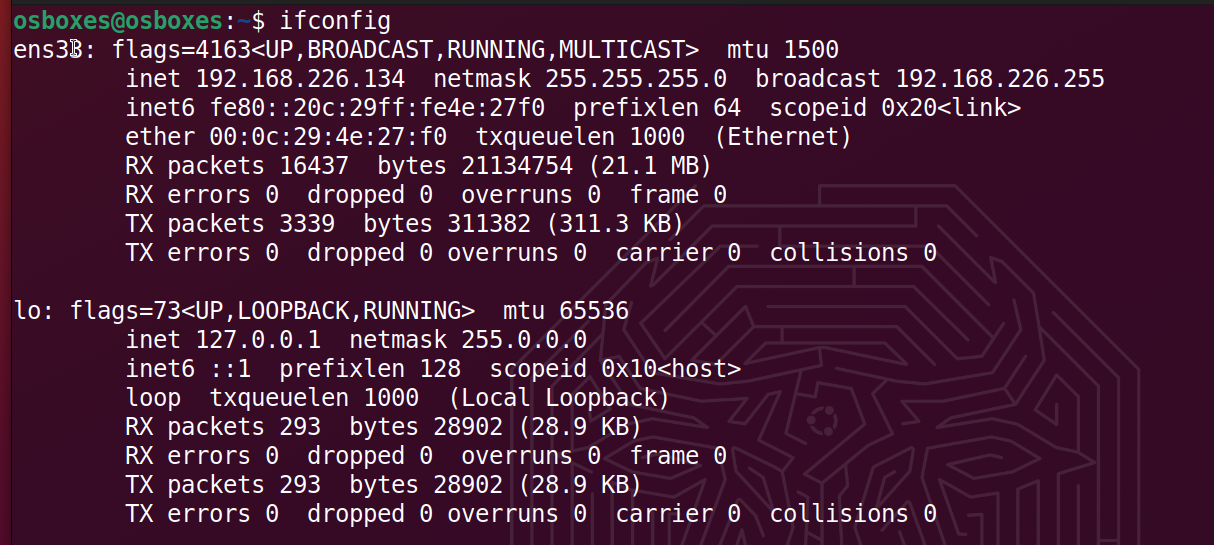
**KALI LINUX**



**Meta-exploitable 2.0 Server**



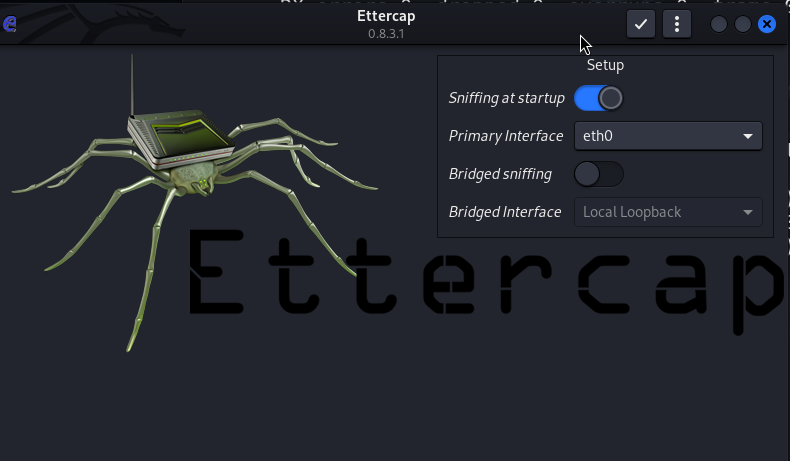
**UBUNTU**



So, 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.

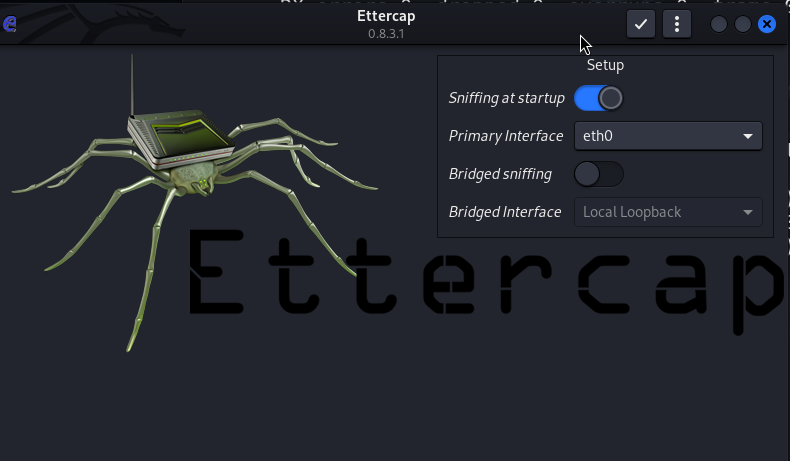
You can connect to a network for ARP spoofing in two ways. The first is to connect via Ethernet, which is very effective but may not always be practical and is rarely subtle. Instead, many people prefer to use [a wireless network adapter](https://null-byte.wonderhowto.com/how-to/buy-best-wireless-network-adapter-for-wi-fi-hacking-2018-0178550/) and perform the ARP spoofing over Wi-Fi.

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. At this point, make sure you have an active connection to the network before you continue.



Select Network Interface to Sniff On

Click on the "Sniff" menu item, and then select "Unified sniffing." A new window will be attacking.

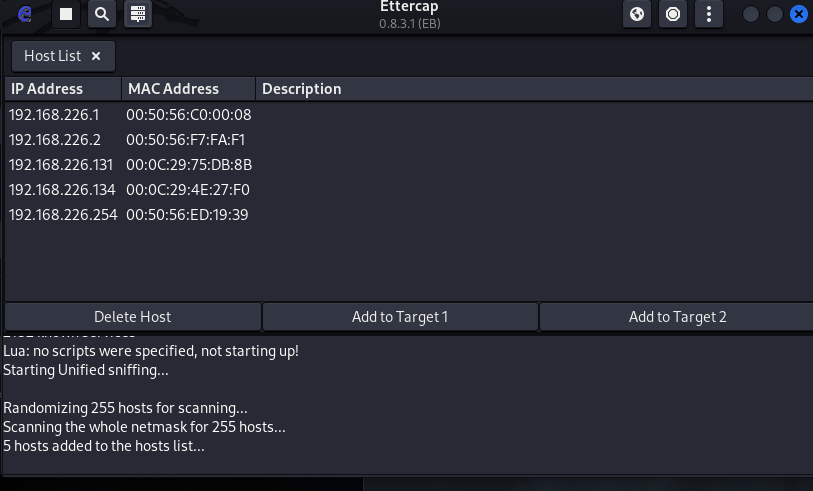


To find the device we want to attack on the network, Ettercap has a few tricks up its sleeve. First, we can do a simple scan for hosts by clicking "Hosts," then "Scan for hosts." A scan will execute, and after it finishes, you can see the resulting hosts Ettercap has identified on the network by clicking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

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."

Once in the *Connections* view, you can filter the connections by IP address, type of connection, and whether the connection is open, closed, active, or killed. This gives you a lot of snooping power, which can be augmented by clicking the "View," then "Resolve IP addresses." This means Ettercap will try to resolve the IP addresses it sees other devices on the network connecting to.

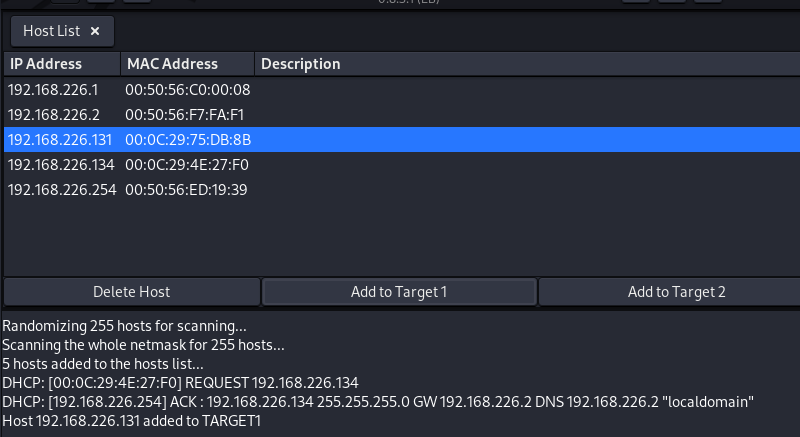


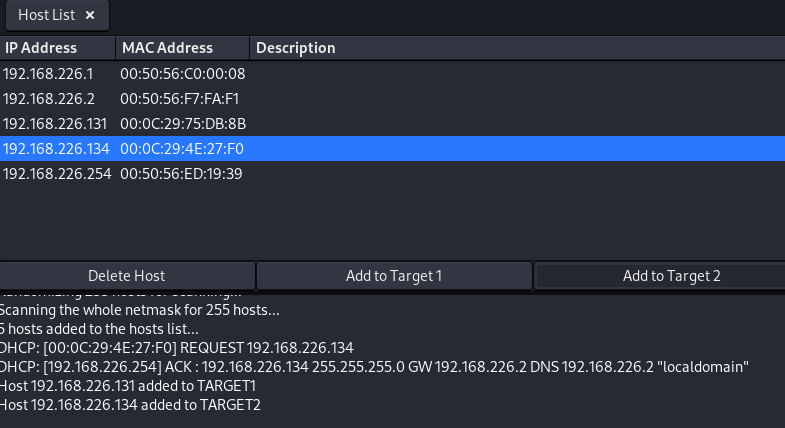
If you want to identify a target on a network and know what they're browsing, look over their shoulder at what website they're on, and match the website to an IP address with an active connection to the same website. Otherwise, you can usually tell by the MAC address, as you can [look it up online](https://macvendors.com/) to see the manufacturer.

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.

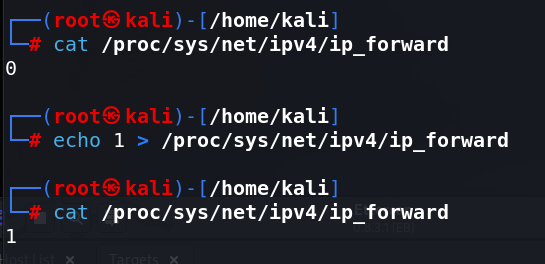
Go back to the "Hosts" screen, and select the IP address of the target you want to target. Click the IP address to highlight it, then click on “Targets," followed by "Target list," to see a list of devices that have been targeted for ARP spoofing.



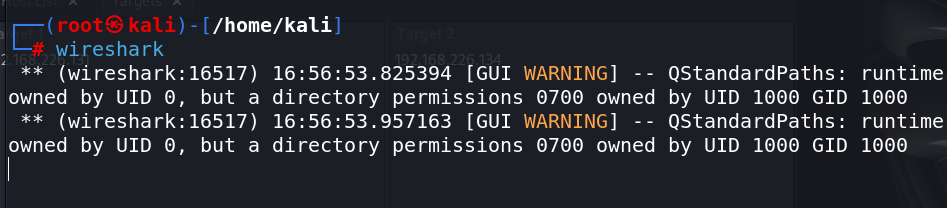


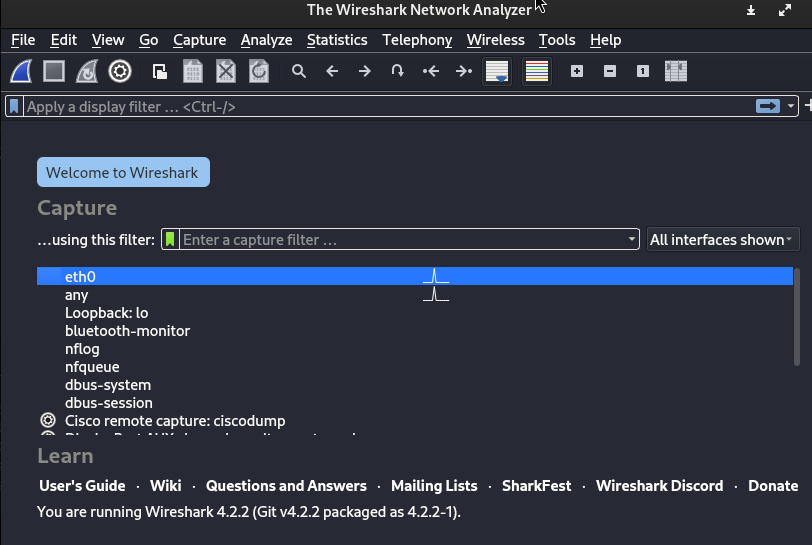
**NOTICE**

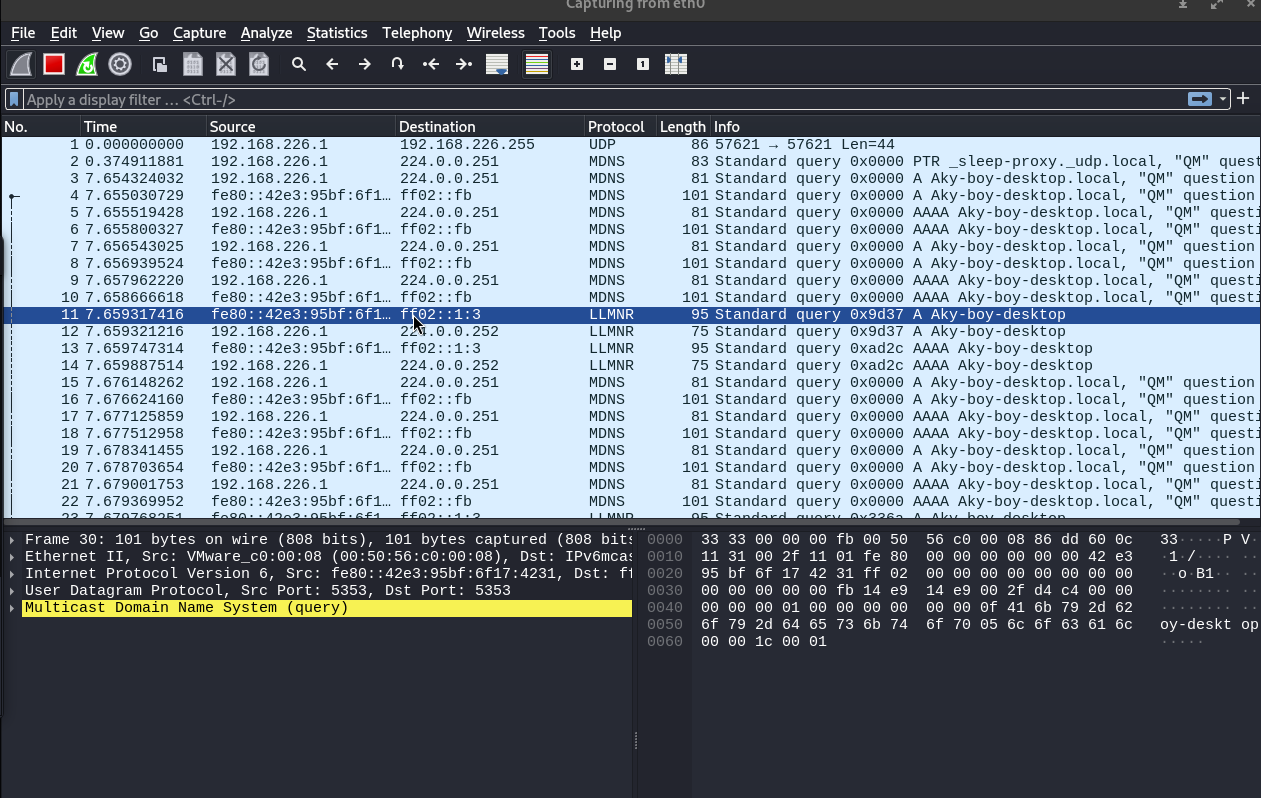
**Before Being Started with the Spoofing make sure these configurations must be done.**



**You can Take a use of Wireshark to capture and have and analysis of captured packets over the network.**



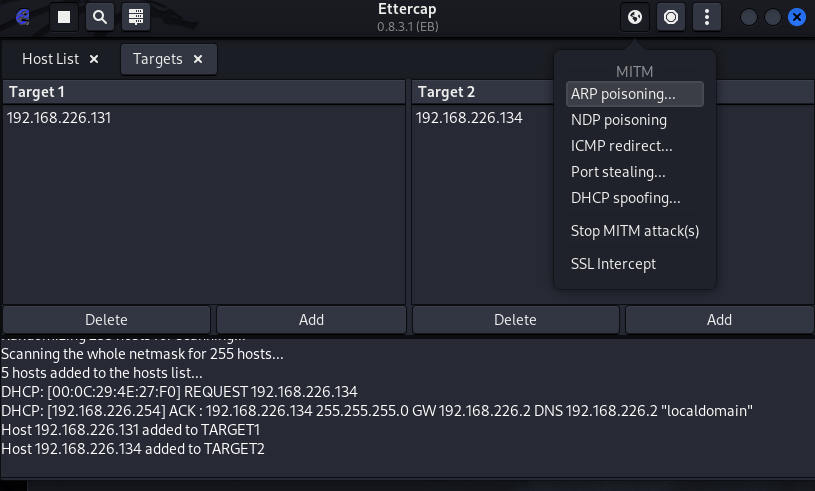




Now, we can go to the "MITM" menu to start our attack on this target.

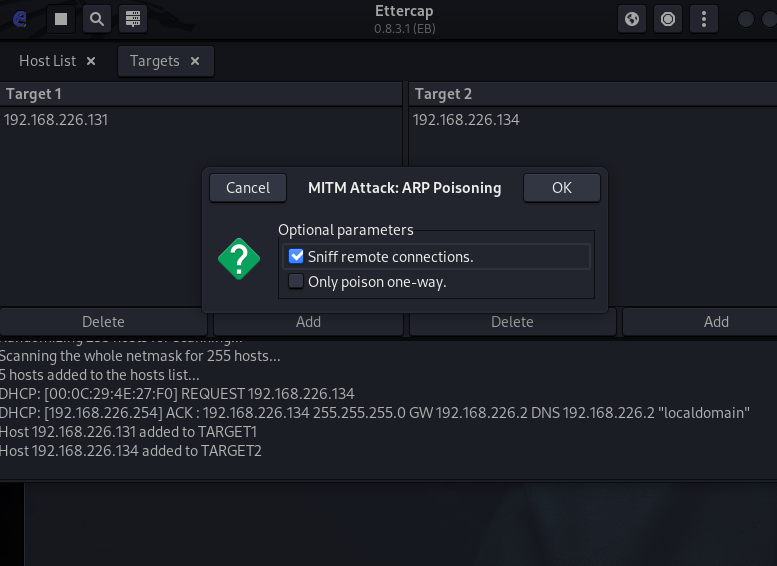
Launch Attack on Targets

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.

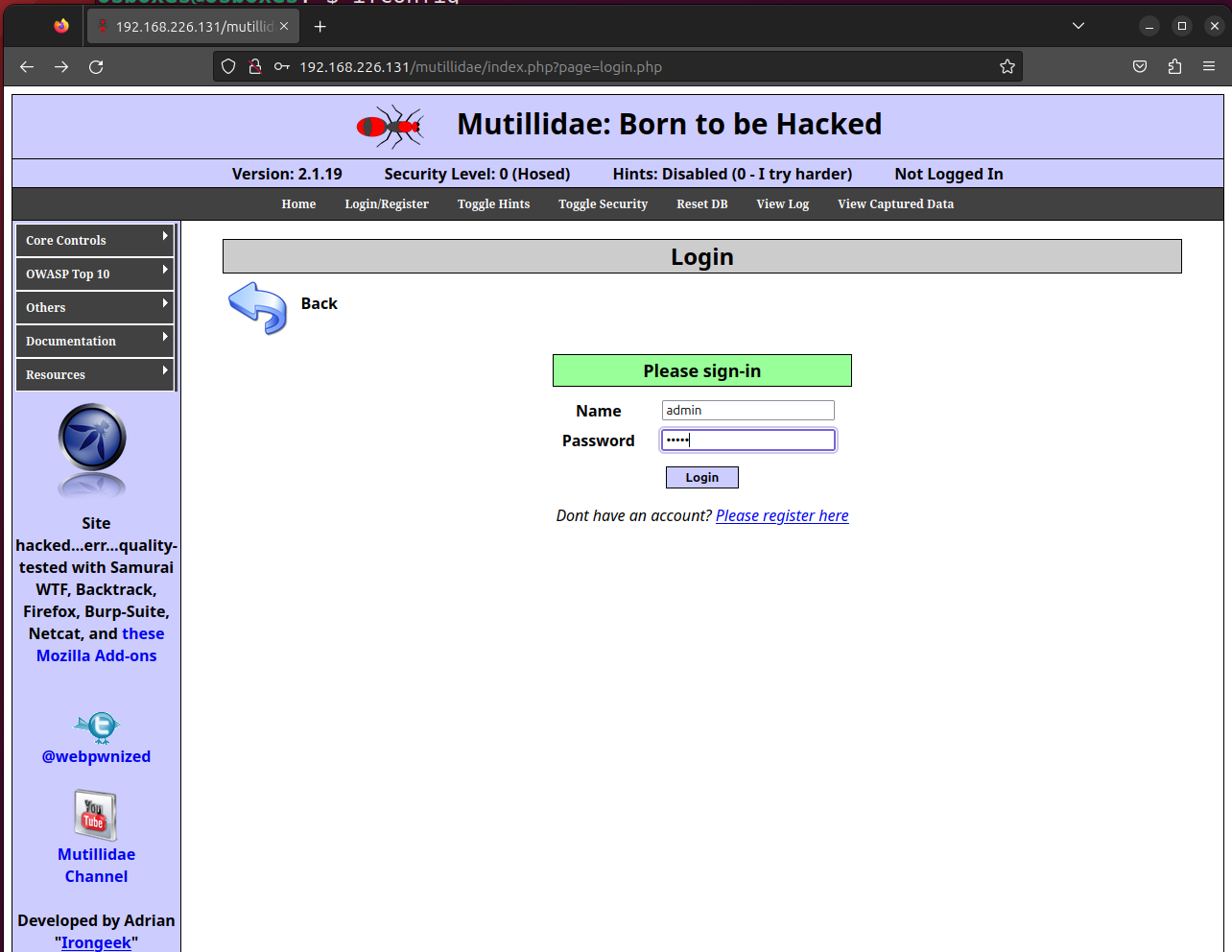
To try another attack, you can click on "Plugins," then "Load plugins," to show the plugin menu. If you select the DOS attack, it will begin dropping the packets sent to this target, cutting off their internet access.



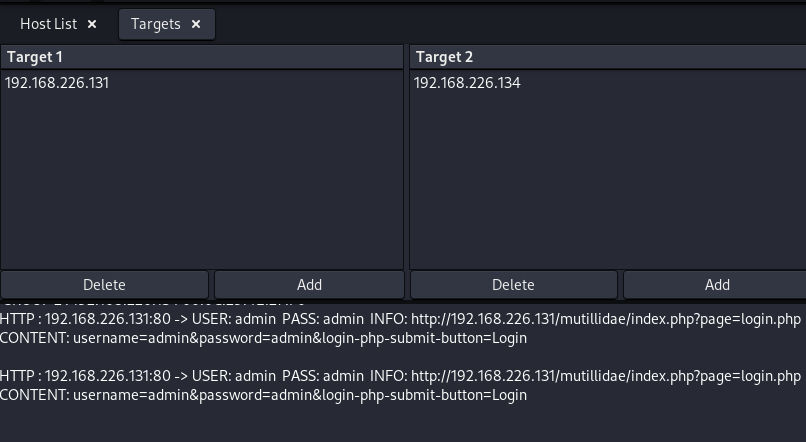
Try Intercepting a Password

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 [aavtrain.com](http://aavtrain.com/). Once it loads, you'll see a login screen you can enter a fake login and password into.

Tested on Mutillidae Website



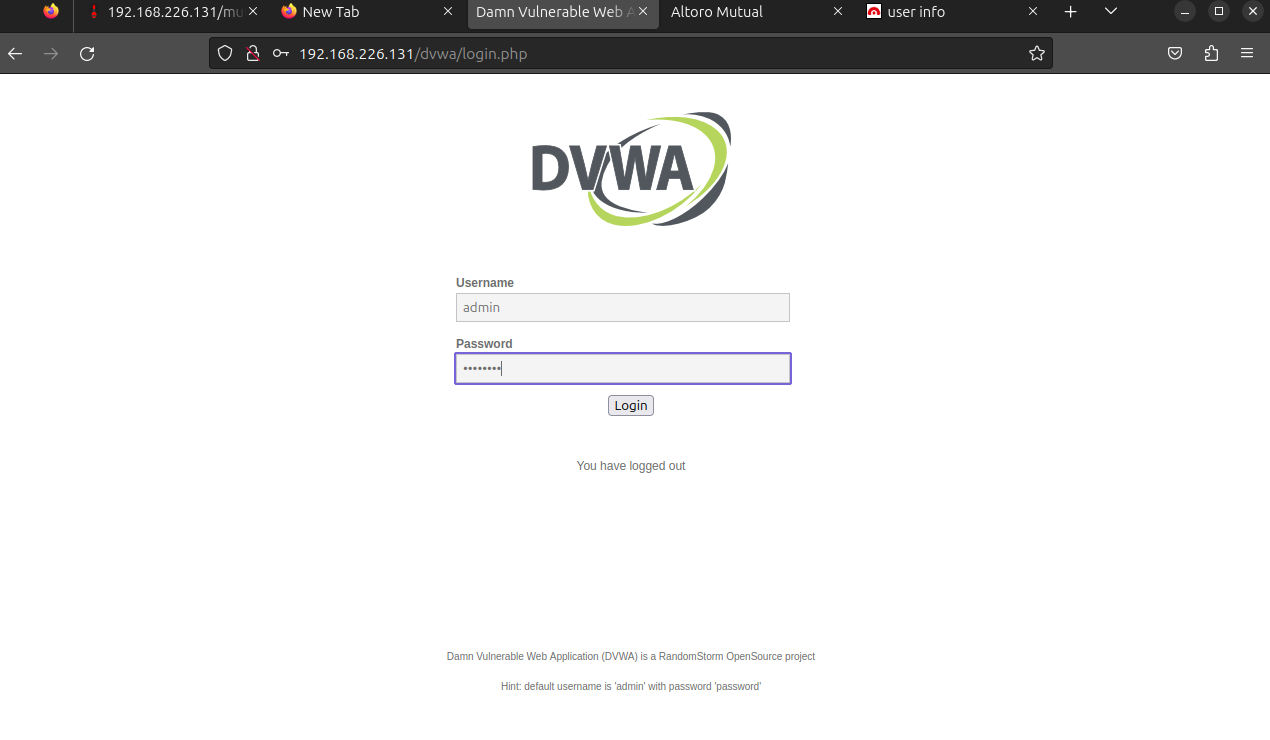
Enter a username and password, then hit "Submit." If Ettercap is successful, you should see the login and password you typed appear on the attacker's screen!

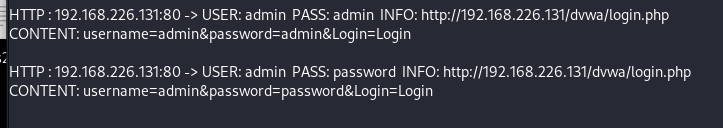


In this result above, we can see that Ettercap successfully ARP poisoned the target and intercepted an HTTP login request the target was sending to an insecure website.

Tested on DVWA Website

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!

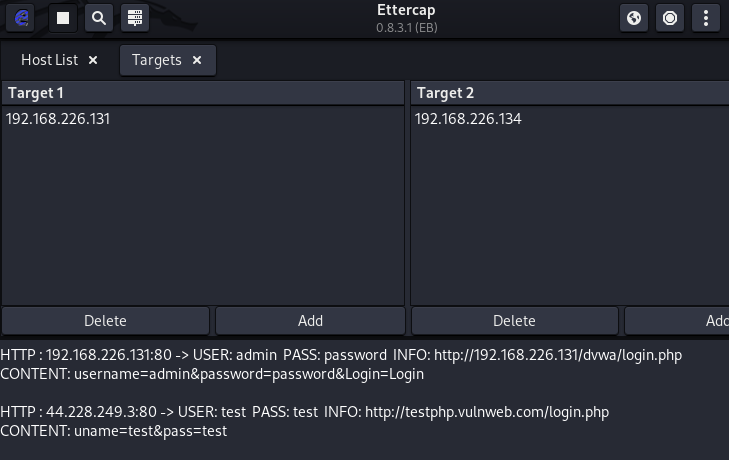


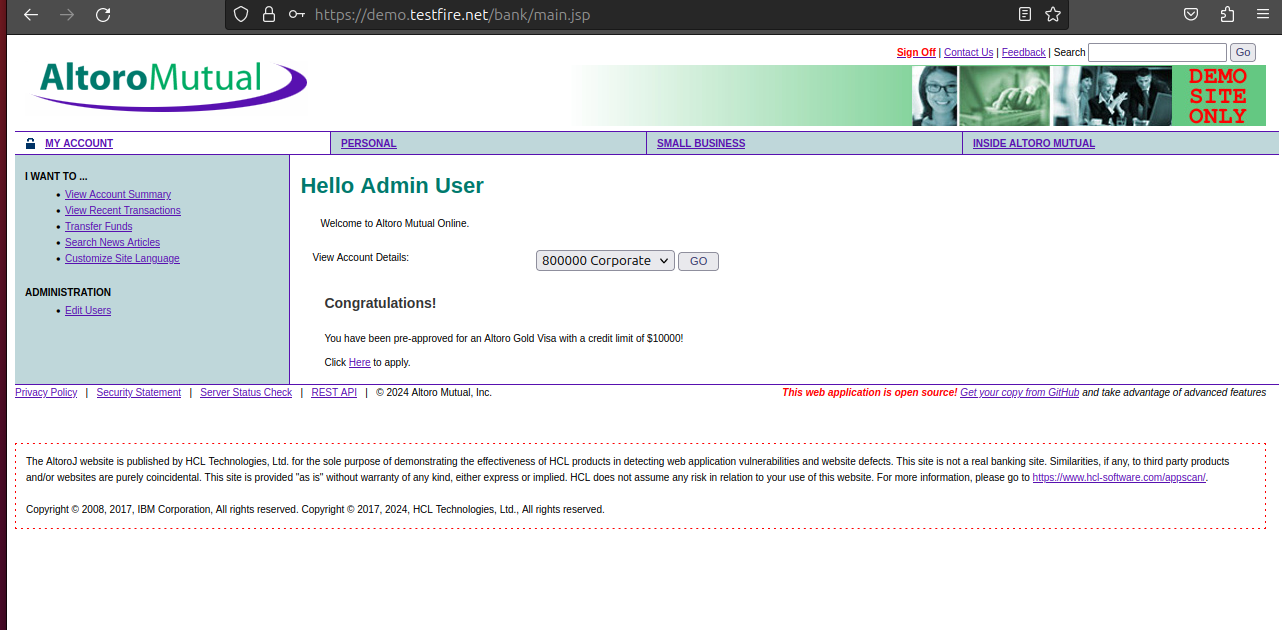


Tested on ACUNETIX Website

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!



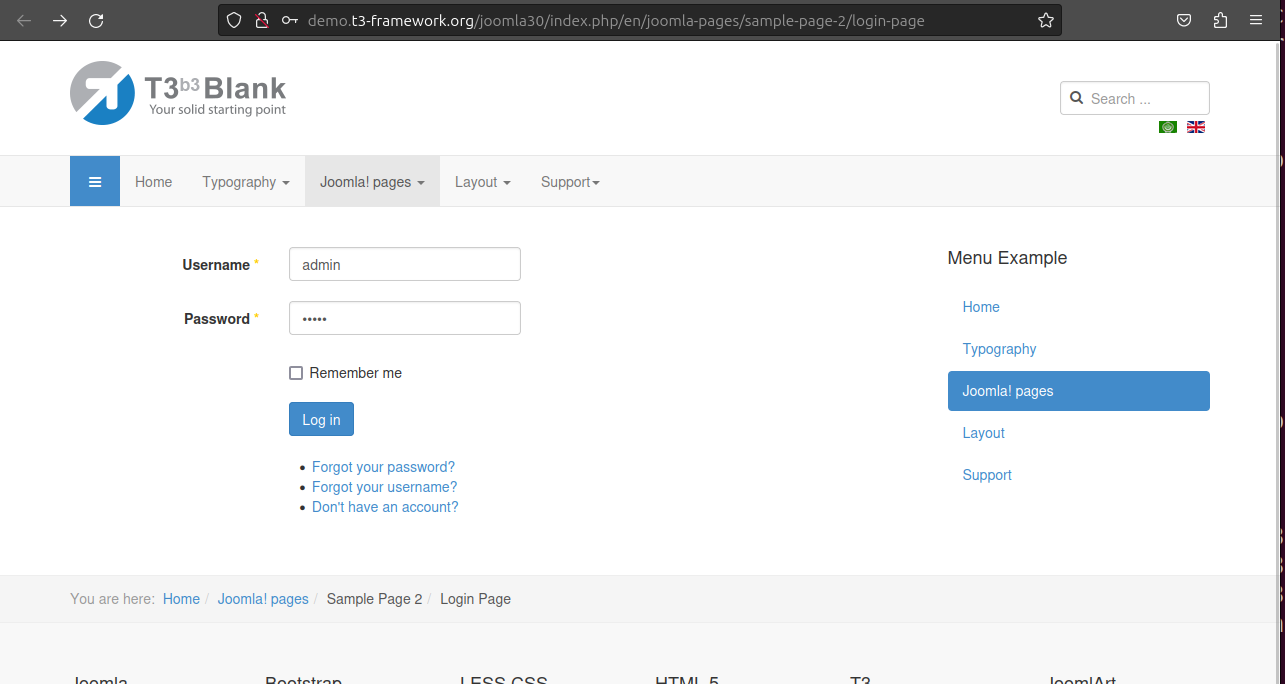


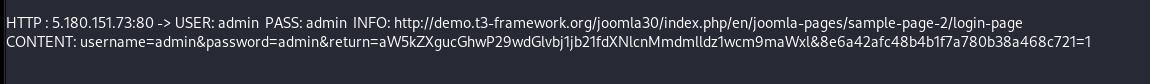


NOT WORKED!

Tested on NEW Website

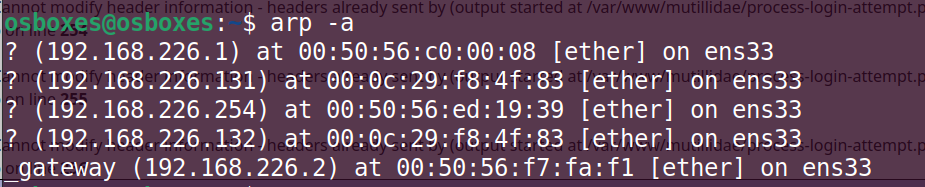
Enter a username and password, then hit "Submit." If Ettercap is successful, you should see the login and password you typed appear on the attacker's screen!





**NOTICE**

**FROM VICTIM’S SIDE VICTIM CAN MONTIOR, THE SPOOF IF HE IS AWARE OF THIS ATTACK**



ARP Poisoning Is a Powerful Tool with Some Limitations

The major obvious limitation of ARP spoofing is that it only works if you're connected to a Wi-Fi network. This means it works on open networks but may not work well against networks that have more sophisticated monitoring or firewalls that may detect this sort of behavior.

ARP spoofing attacks are another example of why it's so essential to [pick strong passwords](https://null-byte.wonderhowto.com/how-to/advice-from-real-hacker-create-stronger-passwords-0156907/) for your networks and limit access to those you trust. You're giving away a lot of trust when you give someone your network password or an Ethernet connection, so remember to pick your passwords carefully and who you share them with.