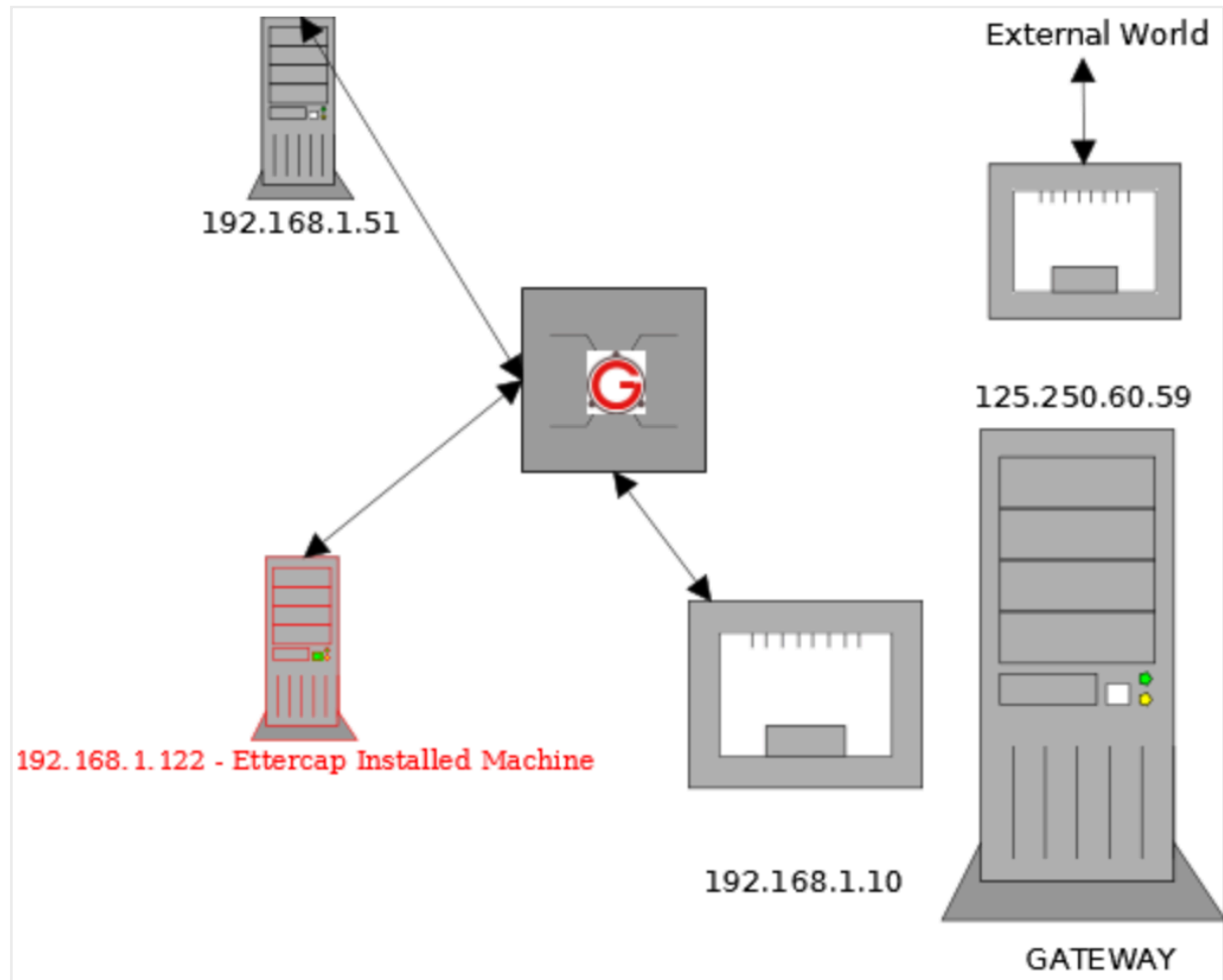


How ARP Poisoning Works (Man-in-the-Middle Attack)

Cybersecurity professionals must understand the details of how a man-in-the-middle attack works at the packet level. In this video, we will capture an ARP poisoning attack and analyze how it works with Wireshark.



In the video, I demonstrated the use of VirtualBox to host two virtual machines: a Windows 10 machine and a Kali Linux machine. Ettercap, available at ettercap-project.org, was employed to execute the Man-in-the-Middle (MiTM) attack, while Wireshark, accessible at www.wireshark.org, was utilized to analyze the captured data.



Now, let's open our virtual machines and run both Windows and Kali Linux.

Please ensure that you have Wireshark installed on both your Windows and Kali Linux virtual machines.

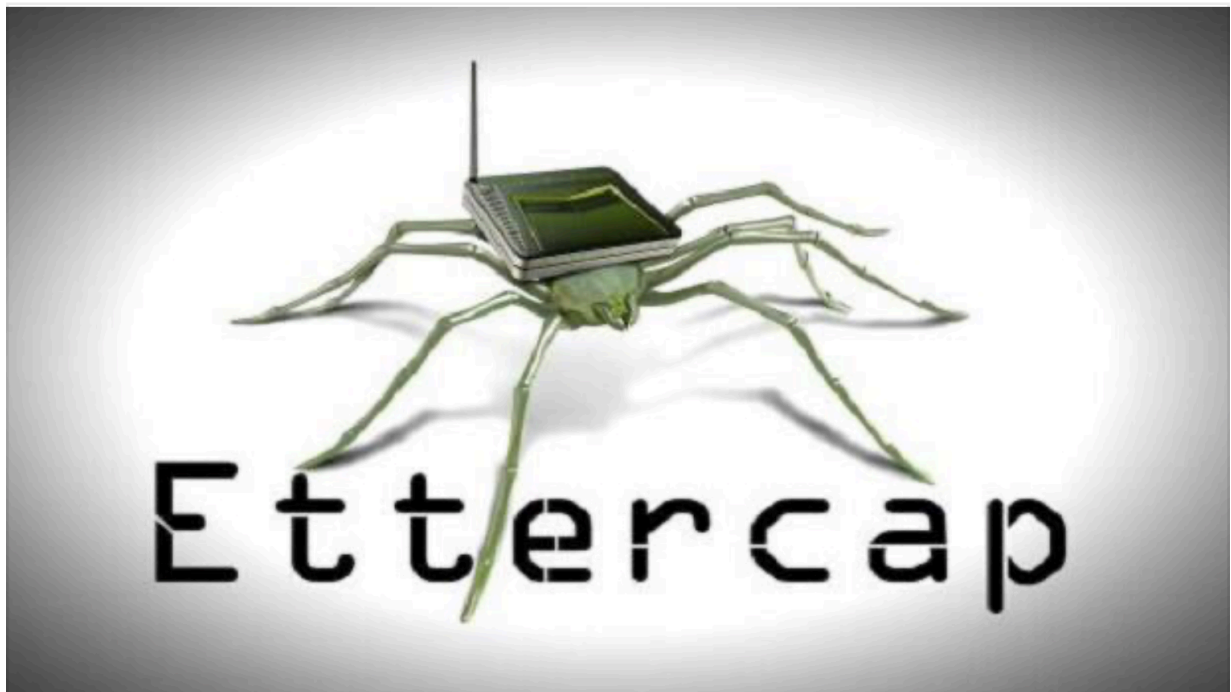
If Wireshark is not installed on your Kali Linux system, you can use the following command to download and install it. Make sure to enter this command into the terminal in your Kali Linux virtual machine:

Command:

```
sudo apt-get update  
sudo apt-get install wireshark
```

This will update the package list and install Wireshark on your Kali Linux system.

We utilized the application called Ettercap in Kali Linux to conduct our attack.



We are going to open Ettercap in Kali Linux.

Inside the "Primary Interface" section, select "eth0" in Ettercap.

If the interface only communicates with one resource (i.e., it's a one-way communication), there is no need to turn on the sniffing bridge in Ettercap.

Click the checkmark at the top of the screen to run the program.

Remember, if you are aiming for high stealth during testing or penetration testing, you might encounter issues related to ARP (Address Resolution Protocol) that could trigger alarms. This is particularly important to consider while conducting tests to avoid unnecessary detection.

Now, click on the search icon located at the top of the menu.

Next, click on "Play Hosts List" to retrieve the IP addresses on the subnet.

After retrieving the IP addresses, select and add the ones you want to target.

Once you have selected the desired targets, click on the earth icon located at the

top left corner.

The menu will give us the "Poison" option.

For our experiment, click on "ARP Poison."

You can leave the settings as default and click "OK."

In our Windows VM, if you run ``arp -a``, you will notice that your Physical Address has been changed due to the ARP poison attack in your windows VM.

Indeed, the change in the Physical Address in the ``arp -a`` command indicates the success of our attack.

ARP (Address Resolution Protocol) poisoning attacks can teach us several important lessons about network security. Here's what we can learn from ARP poisoning attacks and how to prevent them:

Lessons Learned:

1. Network Vulnerabilities: ARP poisoning attacks exploit the inherent trust in local network communications. It highlights the vulnerability of ARP, which lacks authentication mechanisms.
2. Man-in-the-Middle Attacks: ARP poisoning enables Man-in-the-Middle attacks, where an attacker intercepts and potentially alters the communication between two parties, leading to data theft or manipulation.
3. Detection Challenges: Detecting ARP poisoning attacks can be difficult because they occur at a local level within a network, making them less visible to traditional network security tools.

Preventive Measures:

1. Use ARP Spoofing Detection Tools: Deploy network intrusion detection systems (NIDS) or ARP spoofing detection tools that can identify unusual ARP activities and raise alerts.

2. Static ARP Entries: Implement static ARP entries on critical devices. This ensures that specific IP addresses are associated with predetermined MAC addresses, making it difficult for attackers to manipulate.
3. Network Segmentation: Divide your network into segments using VLANs. Restrict communication between segments to minimize the impact of ARP attacks.
4. ARP Spoofing Protection: Some modern switches and routers offer ARP spoofing protection features. Enable these features to detect and prevent ARP spoofing attempts.
5. Port Security: Implement port security on switches to restrict the number of MAC addresses allowed on a port. If an attacker tries to use multiple devices, the port can be shut down.
6. Encrypt Sensitive Traffic: Encrypt sensitive data using technologies like SSL/TLS. Even if intercepted, encrypted data is unreadable and useless to attackers.
7. Regular Security Training: Educate employees about the dangers of phishing attacks and social engineering techniques, which are often used in conjunction with ARP poisoning.
8. Regularly Update and Patch Systems: Keep all systems, including network devices, updated with the latest security patches to protect against known vulnerabilities.
9. Strong Access Controls: Implement strong access controls, including robust password policies and multi-factor authentication, to prevent unauthorized access to network devices.
10. Network Monitoring: Regularly monitor network traffic for suspicious patterns. Anomalies in network traffic could indicate ARP poisoning attempts.

By understanding the methods employed by attackers and implementing comprehensive security measures, organizations can significantly reduce the risk of falling victim to ARP poisoning attacks.