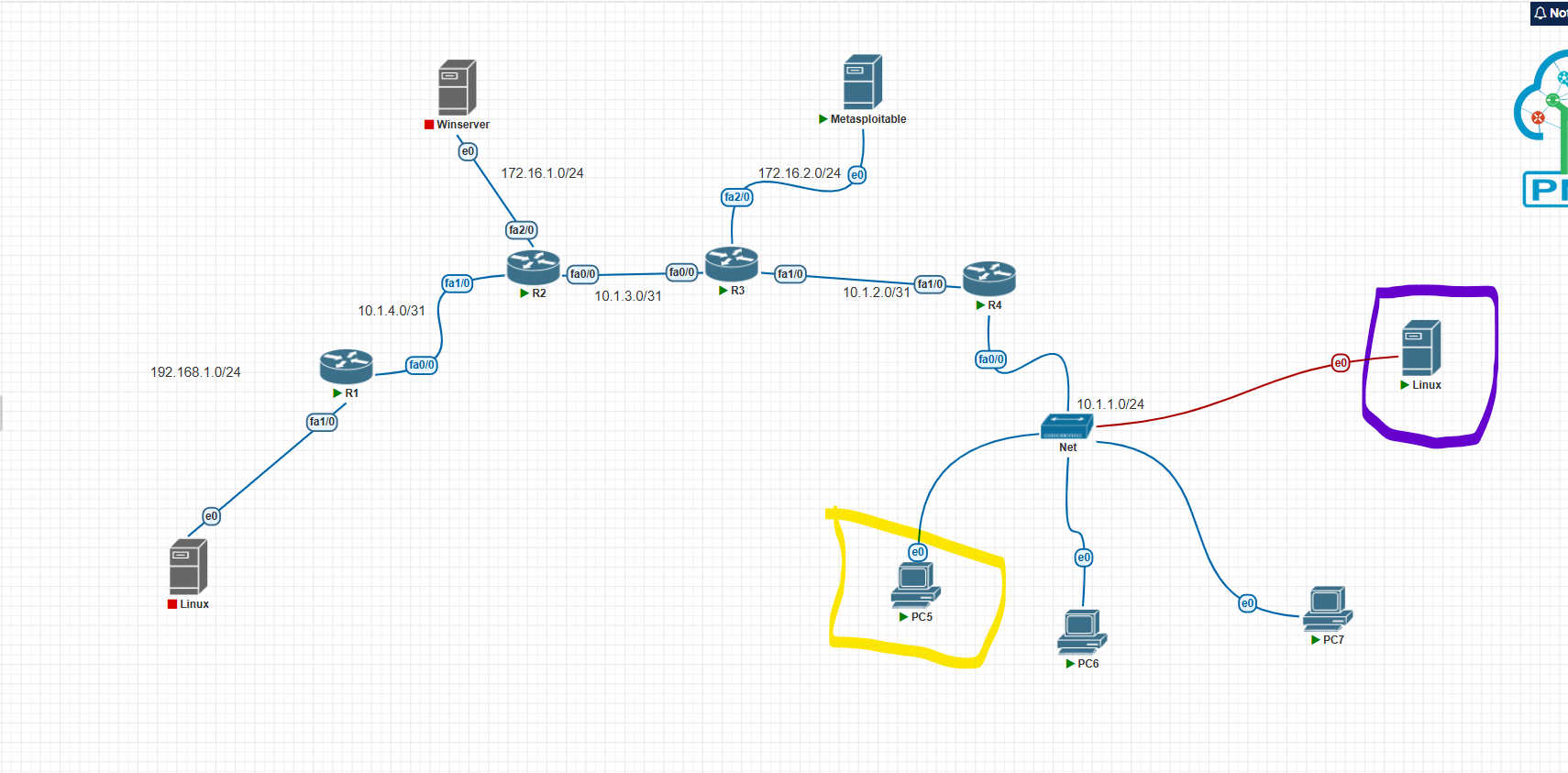
**Man-in-the-Middle Attack (MITM)**

A **Man-in-the-Middle (MITM) attack** occurs when an attacker intercepts the communication between two devices on a network, gaining unauthorized access to data. This type of attack allows the attacker to read, modify, or redirect traffic without the knowledge of the communicating parties.

**Definition and Explanation**

* **MITM Attack**: This is a type of eavesdropping attack where the attacker positions themselves between two devices, intercepting or manipulating data exchanged between them.
* **Spoofing**: The attacker uses techniques like ARP Spoofing to impersonate devices on a network by associating their MAC address with the IP addresses of the legitimate devices.

**Lab Details**

****

**Objective:**

To simulate a **Man-in-the-Middle (MITM) attack** using ARP Spoofing in a controlled lab environment to understand its methodology and impacts.

**Lab Setup:**

1. **Hacking PC**:
   * IP Address: **10.1.1.2**
   * Purpose: Simulates the attacker’s machine, launching the MITM attack.
2. **Target PC**:
   * IP Address: **10.1.1.3**
   * Purpose: Simulates the victim's machine whose traffic is intercepted.
3. **Gateway**:
   * IP Address: **10.1.1.1**
   * Purpose: The network router facilitating communication.

**Commands Used:**

To perform ARP Spoofing:

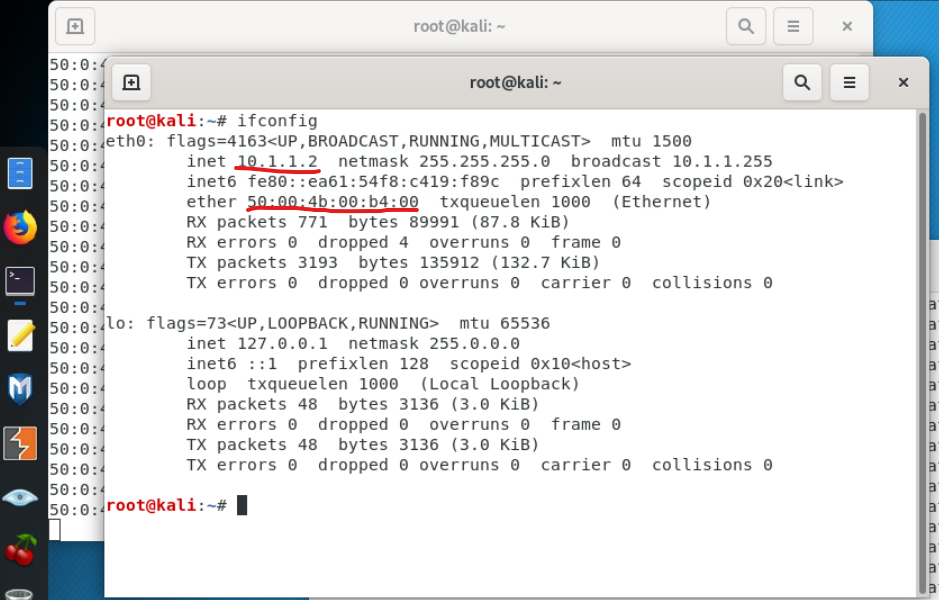
*arpspoof -i eth0 -t 10.1.1.1 10.1.1.3*

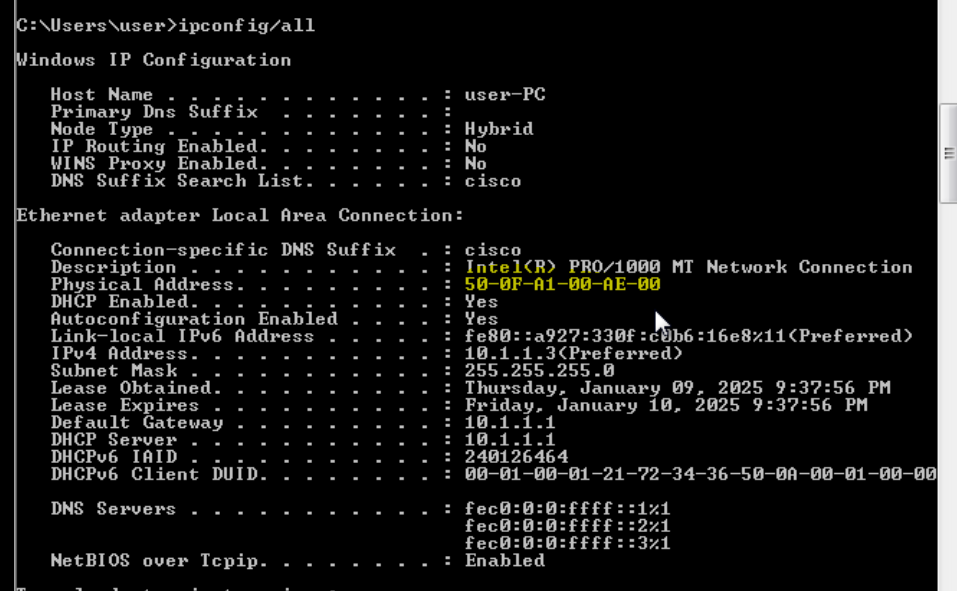
*arpspoof -i eth0 -t 10.1.1.3 10.1.1.1*

* The **first command** convinces the gateway that the attacker's MAC address belongs to the target PC.
* The **second command** convinces the target PC that the attacker's MAC address belongs to the gateway.

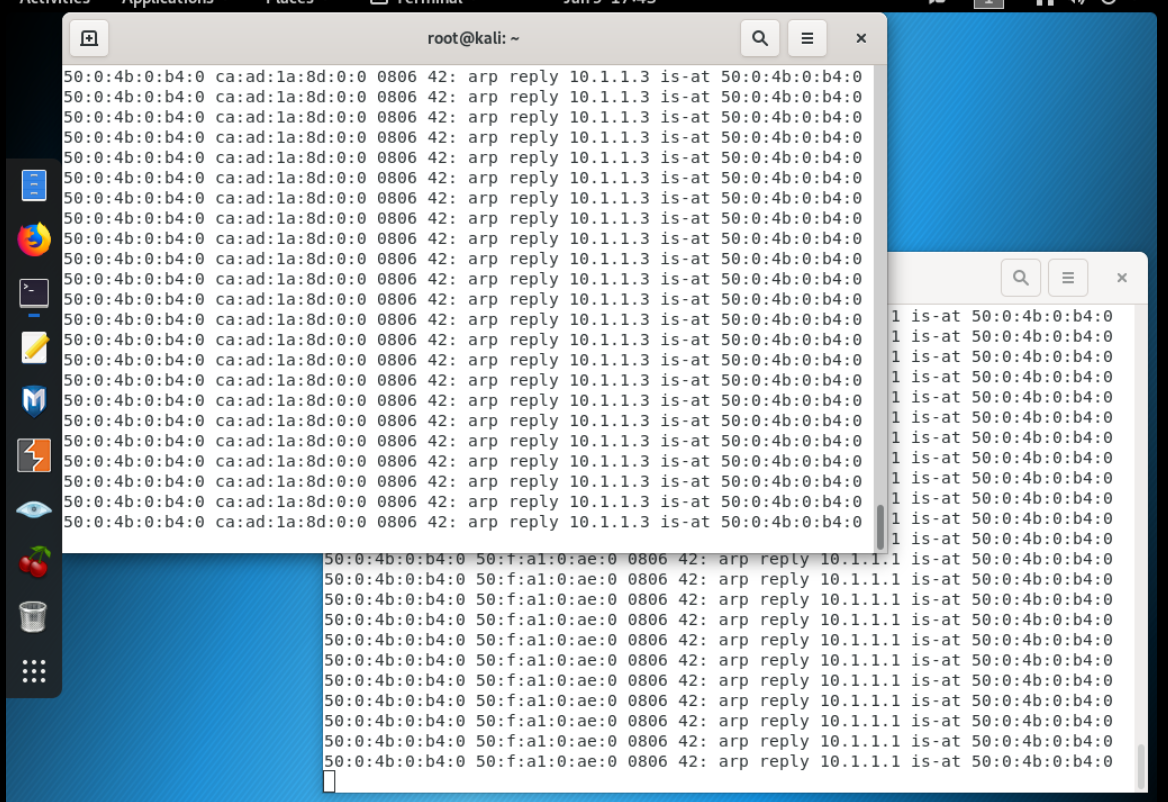
**Lab Diagrams:**

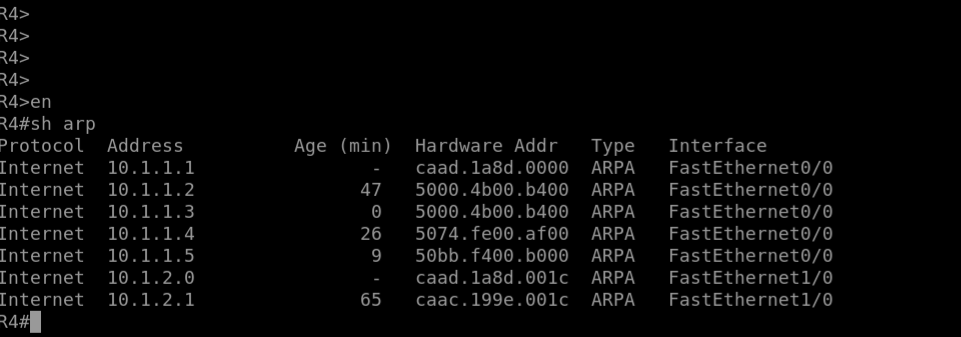
1. **Network Setup Diagram**:
   * Illustrates the relationship between the Hacking PC, Target PC, and Gateway.





1. **ARP Table Screenshots**:
   * Show the spoofed MAC address of the hacker on both the gateway and the target PC.





**Vulnerability Exploited**

* **ARP (Address Resolution Protocol)**:
  + ARP is used to map IP addresses to MAC addresses for communication within a local network.
  + ARP requests and replies are not authenticated, making them vulnerable to spoofing attacks.

**Methods Used**

1. **ARP Spoofing**:
   * The attacker sends falsified ARP responses to associate their MAC address with the IP addresses of the target and the gateway.
2. **Traffic Interception**:
   * Once ARP Spoofing is successful, all traffic between the target and the gateway is redirected through the attacker’s machine.

**What an Attacker Can Do**

By successfully exploiting a MITM attack, an attacker can:

* **Eavesdrop**: Intercept and read sensitive data such as login credentials and personal messages.
* **Modify Data**: Alter the content of transmitted data, such as redirecting a banking transaction.
* **Inject Malware**: Introduce malicious code or payloads into the communication.
* **Denial of Service (DoS)**: Interrupt or degrade network communication by dropping packets.

**How to Mitigate MITM Attacks**

1. **Enable ARP Spoofing Detection**:
   * Use intrusion detection systems (IDS) or intrusion prevention systems (IPS) that monitor and flag ARP anomalies.
2. **Implement Secure Communication**:
   * Use encryption protocols such as HTTPS, TLS, or VPNs to protect data even if intercepted.
3. **Static ARP Entries**:
   * Configure static ARP tables to ensure IP-MAC bindings are fixed and cannot be altered.
4. **Network Segmentation**:
   * Separate sensitive systems into isolated network segments to minimize exposure.
5. **Regular Updates**:
   * Keep network devices and firmware up to date to patch vulnerabilities.

**Note**

This lab is for **educational purposes only** and aims to demonstrate how attackers exploit network vulnerabilities to improve awareness and strengthen defenses. It is not intended for unauthorized or malicious activities.