**Sniffing**

**Index:**

**Network Sniffing:**

Network sniffing is the process of intercepting and monitoring data traffic on a network to capture sensitive information, often using specialized tools, for analysis, troubleshooting, or unauthorized access.

**Packet sniffing:**

It involves monitoring and capturing all data packets passing through a given network using software or hardware device.

**How a Sniffer works:**

A sniffer works by capturing network packets transmitted over a network, analyzing data headers and payloads to extract information. It operates in promiscuous mode to intercept all traffic, not just intended packets.

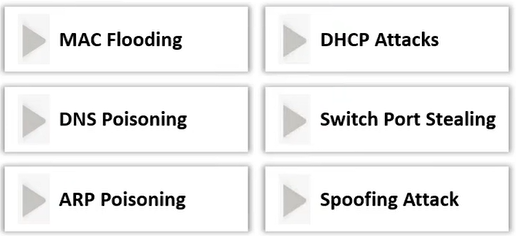
**Types of sniffing:**

1. **Passive sniffing:**

It refers through sniffing through a hub. It involves monitoring packets sent by others without sending any additional data packets in the network traffic.

1. **Active sniffing:**

It is used to sniff a switch-based network. Many techniques which can be used to do so are:



**Protocols Vulnerable to Sniffing:**

1. Telnet and Rlogin
2. HTTP
3. POP
4. IMAP
5. SMTP and NNTP
6. FTP

**SPAN Port:**

A **SPAN (Switched Port Analyzer) port** mirrors traffic from specific network ports or VLANs to a designated monitoring port, enabling network analysis. It helps sniffers capture traffic for inspection without disruption.

A SPAN port is a port that is configured to receive a copy of every packet that passes through a switch.

In sniffing, a **SPAN port** allows the sniffer to receive a copy of all network traffic passing through a switch, including packets from other devices, enabling comprehensive monitoring and analysis without affecting normal operations.

**Switching of Data in Networks:**

In networks, **switching** is the process of forwarding data packets between devices (like computers, printers, or servers) on a local area network (LAN). Switches use **MAC addresses** to make forwarding decisions. When a device sends a packet, the switch checks its **MAC address table** to find the corresponding port for that address and forwards the packet to the correct port. If the switch doesn’t know the destination, it broadcasts the packet to all ports, except the one it came from, until it learns the appropriate port.

**How a Network Learns Ports (MAC Address Learning):**

When a switch is first powered on, it doesn’t know where devices are located. The learning process begins when devices send data packets. As these packets arrive, the switch examines the **source MAC address** and records which port the data came from in its MAC address table. Over time, the switch builds a table mapping **MAC addresses to specific ports**. When future packets arrive, the switch can forward them directly to the correct port based on the destination MAC address, improving network efficiency.

**Wiretapping:**

Wiretapping is the unauthorized interception of communication, typically over phone lines or networks, to monitor, record, or eavesdrop on private conversations or data. It is often used for surveillance, espionage, or cybercrime, violating privacy and security.

Types of wiretapping:

1. Active wiretapping
2. Passive wiretapping

**MAC Address:**

A **MAC (Media Access Control) address** is a unique identifier assigned to network interfaces for communication on a local network. It consists of 48 bits, typically represented as six hexadecimal pairs.

A **MAC address** is a 48-bit identifier, typically written as six pairs of hexadecimal digits (e.g., 00:1A:2B:3C:4D:5E). It’s structured into two parts:

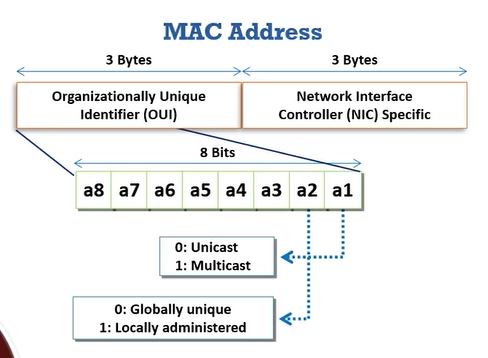
1. **Organizationally Unique Identifier (OUI)** – The first 24 bits (3 bytes) are assigned to the manufacturer or organization by the IEEE. This identifies the manufacturer or vendor of the network device.

Example: 00:1A:2B (indicating the manufacturer)

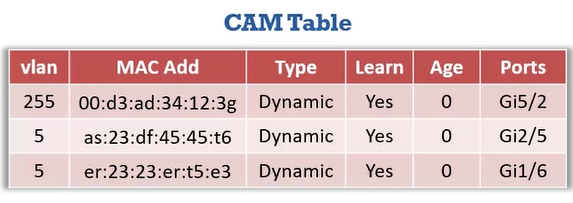
1. **Network Interface Controller (NIC) Specific** – The last 24 bits (3 bytes) are assigned by the manufacturer and are unique to each device. This portion identifies the specific network interface card or device.

Example: 3C:4D:5E (unique to the device)

Thus, the MAC address is globally unique and can be used to identify a device on a local network.



**CAM tables:**A **CAM (Content Addressable Memory) table** is a switch's database that stores MAC addresses and their associated switch ports. It helps determine where to forward frames by mapping MAC addresses to specific ports.



**MAC flooding:**

**MAC flooding** is an attack where a malicious device sends numerous fake MAC addresses to a switch, overwhelming its CAM table. This causes the switch to broadcast traffic to all ports, enabling potential eavesdropping.

Tools to do so:

1. Macof
2. Yersinia
3. Ettercap
4. Scapy

**Switch Port Stealing:**

The Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets. The attacker floods the switch with forged gratuitous ARP packets with the target MAC address as the source and his/her own MAC address as the destination. A race condition of the attacker's flooded packets and the target host's packets occurs; thus, the switch must change its MAC address, binding constantly between two different ports. In such a case, if the attacker is fast enough, he/she will able to direct the packets intended for the target host toward his/her switch port. The attacker now manages to steal the target host's switch port and sends ARP requests to the stolen switch port to discover the target host's IP address. When the attacker gets an ARP reply, this indicates that the target host's switch port binding has been restored, and the attacker can now sniff the packets sent toward the targeted host.

**How to defend against MAC attacks?**

To defend against MAC (Message Authentication Code) attacks, use strong cryptographic algorithms, regularly update keys, implement secure key management, utilize hardware security modules (HSMs), and enable multi-factor authentication for added security.

Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attacks.

**DHCP starvation attack:**

The DoS attack on the DHCP servers where the attacker broadcast forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope.

Tools for it:

1. Yersinia
2. Hyenae
3. Dhcpstarv

**Rogue DHCP server attack:**

A rogue DHCP server attack occurs when an unauthorized server provides incorrect IP configuration to clients, potentially redirecting traffic, intercepting data, or causing denial of service. Countermeasures include network monitoring and DHCP snooping.

**How to defend against DHCP starvation Rogue DHCP server attack?**

Enable port security to defend against DHCP starvation attacks.

Enable DHCP snooping, which allows the switch to accept a DHCP transaction directed from a trusted port.

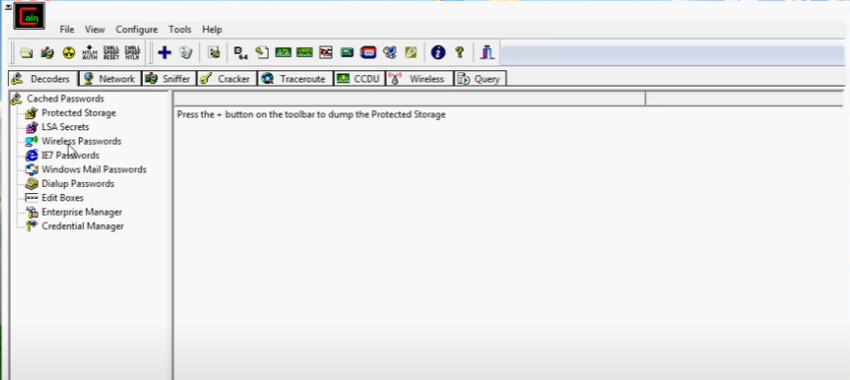
**ARP spoofing attack:**

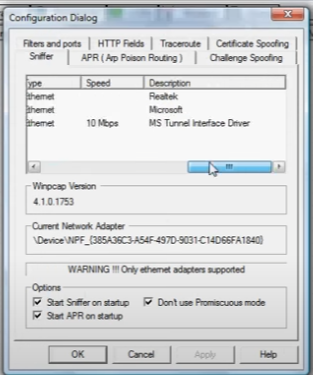
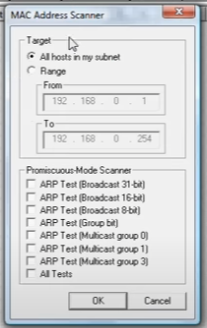
ARP spoofing is a network attack where an attacker sends falsified ARP (Address Resolution Protocol) messages, associating their MAC address with a legitimate IP address. This can lead to man-in-the-middle attacks, data interception, or network disruption.

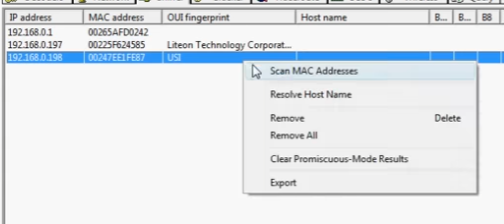
ARP poisoning tools:

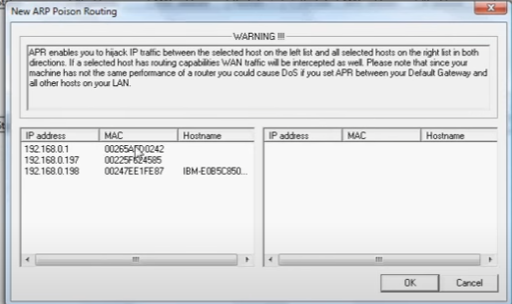
1. Arpspoof
2. Habu
3. BetterCAP
4. Ettercap
5. Dsniff
6. MITMf
7. Arpoison
8. Habu

Network spoofing using Cain and Abel:







We can defend against ARP poisoning using DHCP Snooping Binding table.

ARP spoofing Detection tools:

1. Wireshark
2. ArpON
3. Capsa Portable Network Analyzer
4. sharp

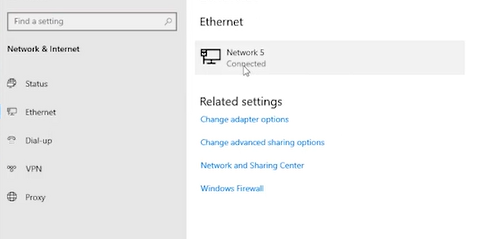
**MAC Spoofing/ Duplicating:**

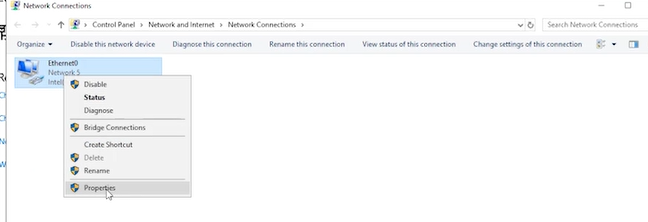
A MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses. By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address to receive all the traffic destined for the user. This attack allows an attacker to gain access to the network and take over someone's identity on the network.

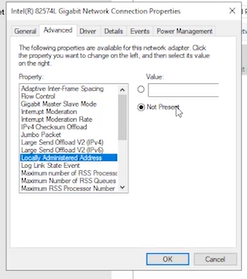
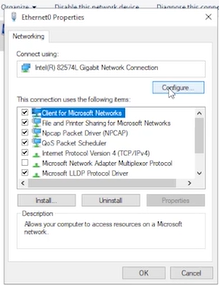
This technique can be used to bypass Wireless Access Points’ MAC filtering.

MAC Spoofing tools:

1. Technitium MAC Address changer
2. SMAC
3. MAC address changer







To defend against MAC spoofing, use DHCP Snooping binding table, dynami ARP inspection, and IP source guard.

**VLAN Hopping:**

VLAN hopping is an attack technique targeting network resources on a virtual LAN, allowing attackers to traverse VLAN boundaries and access restricted areas, ultimately undermining network security by exploiting VLAN infrastructure vulnerabilities.

**Techniques**:  
VLAN hopping can be performed using two primary methods - Switch Spoofing and Double Tagging, each targeting specific vulnerabilities in VLAN implementation to access unauthorized network segments.

Attackers execute VLAN hopping to steal passwords, modify or delete data, and install malicious programs, facilitating the spread of malware such as viruses, Trojans, and worms across the network.

**SwitchSpoofing**:  
Through switch spoofing, attackers connect a rogue switch to the network, deceiving a legitimate switch into establishing a trunk link, which allows unauthorized access to traffic from multiple VLANs.

Doubletagging:  
Double tagging involves attackers adding and modifying Ethernet frame tags, tricking the network to redirect packets into unauthorized VLANs, bypassing security barriers designed to contain VLAN traffic.

**STP Attack:**

A STP (Spanning Tree Protocol) attack involves manipulating network topology by sending false Bridge Protocol Data Units (BPDU) to disrupt normal spanning tree operations. This can cause network loops, downtime, or unauthorized network access by altering switch roles.

**DNS Poisoning Techniques:**

DNS poisoning, or cache poisoning, occurs when malicious data is inserted into a DNS resolver's cache, redirecting traffic to fraudulent websites. This can lead to phishing attacks, data interception, or the spread of malware by compromising domain name resolution.

**Internet DNS Spoofing:**

Internet DNS spoofing involves sending falsified DNS responses to a resolver, causing it to cache incorrect IP addresses. This redirects users to malicious websites, enabling phishing, malware distribution, or other cyberattacks by manipulating domain name resolution.

**Proxy server DNS Poisoning:**

Proxy server DNS poisoning occurs when malicious data is injected into a proxy's DNS cache. This redirects users' web traffic to fraudulent sites or intercepts communications, potentially enabling phishing, data theft, or malware distribution by compromising domain resolution.

**DNS Cache Poisoning:**

DNS cache poisoning involves injecting malicious data into a DNS resolver’s cache, causing it to return incorrect IP addresses. This misdirects users to fraudulent or malicious websites, enabling attacks like phishing, malware distribution, or data interception.

**Sniffing Tool: Wireshark**

**Wireshark** is a widely-used network protocol analyzer and sniffing tool that allows users to capture and inspect data packets traveling through a network. It is used for troubleshooting, network analysis, and security monitoring. Here's a brief overview:

* **Packet Capture**: Wireshark captures network traffic in real time, enabling detailed inspection of each packet, including headers, protocols, and payloads.
* **Protocol Analysis**: Supports hundreds of protocols, allowing users to dissect and understand the data exchange between devices.
* **Filters**: Wireshark offers powerful filtering capabilities to isolate specific traffic based on protocols, IP addresses, ports, and other criteria.
* **User-Friendly Interface**: Provides a graphical interface to display captured data and offer insights into network behavior.
* **Security and Troubleshooting**: Often used by network administrators and security professionals to detect vulnerabilities, troubleshoot performance issues, or investigate suspicious activity.
* **Cross-Platform**: Available for Windows, macOS, and Linux.

While it's an invaluable tool for legitimate network analysis, it can also be misused for malicious sniffing, capturing sensitive information like passwords or credit card details on unsecured networks.

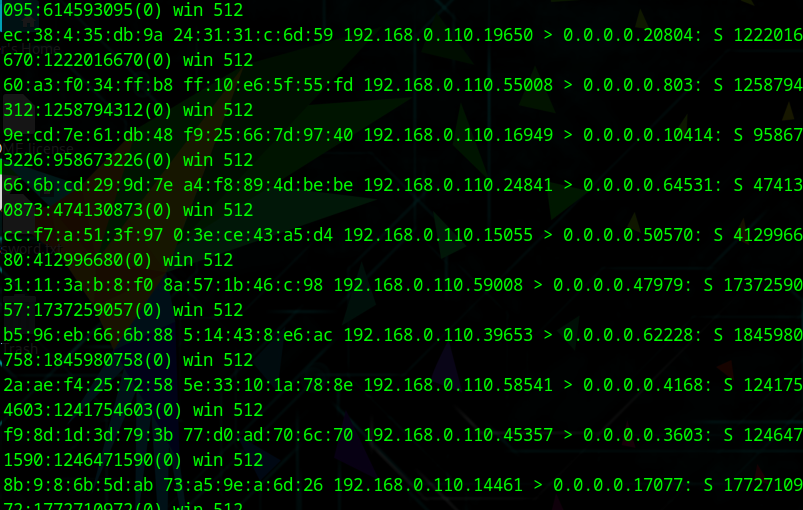
**Detecting network sniffing involves several techniques:**

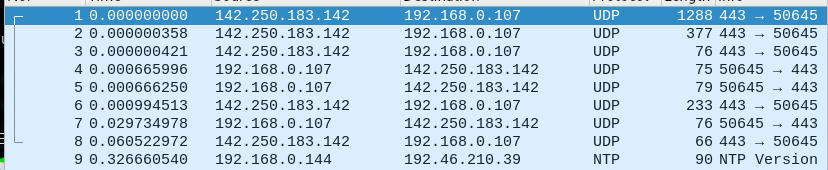
1. **Unusual Network Traffic**: Monitor for unexpected spikes in network activity or unknown devices accessing the network.
2. **ARP Spoofing Detection**: Use tools to check for ARP spoofing or poisoning attacks.
3. **Packet Inspection**: Analyze network traffic for signs of interception using intrusion detection systems (IDS).
4. **Use Encrypted Protocols**: Ensure encrypted communication (HTTPS, SSH) to prevent sniffed data from being readable.
5. **Monitor Wireless Networks**: Check for rogue access points or unusual wireless devices intercepting traffic.
6. **Network Segmentation**: Implement VLANs or other techniques to limit access to sensitive data.

**MAC flooding attacks:**

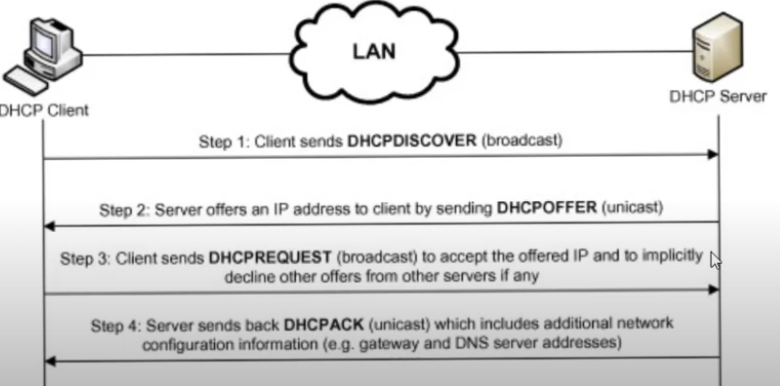
Using macof:



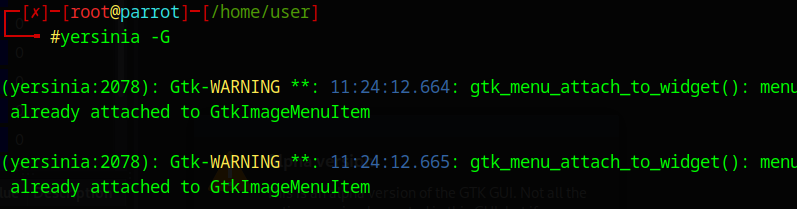


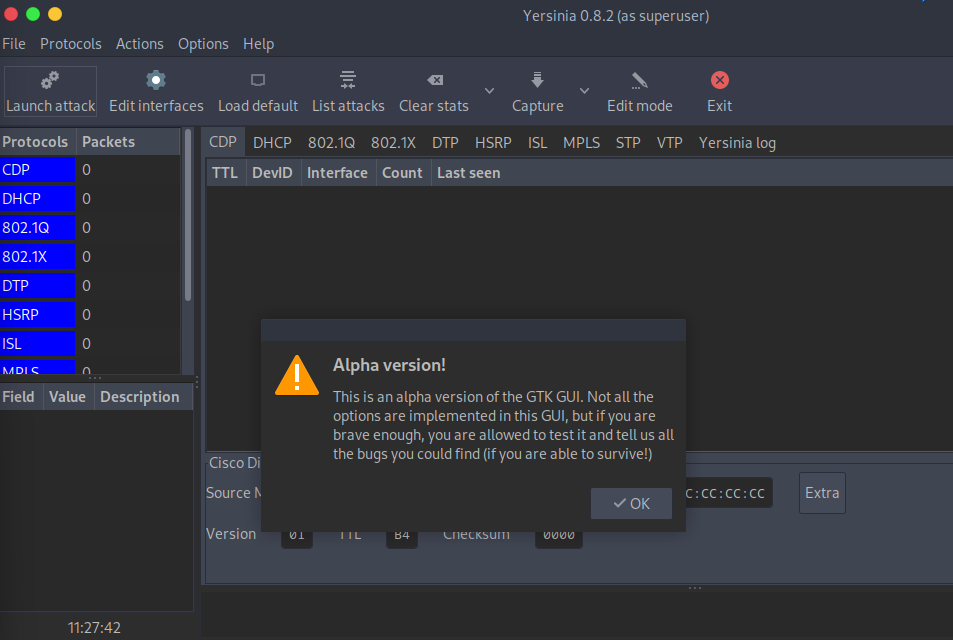


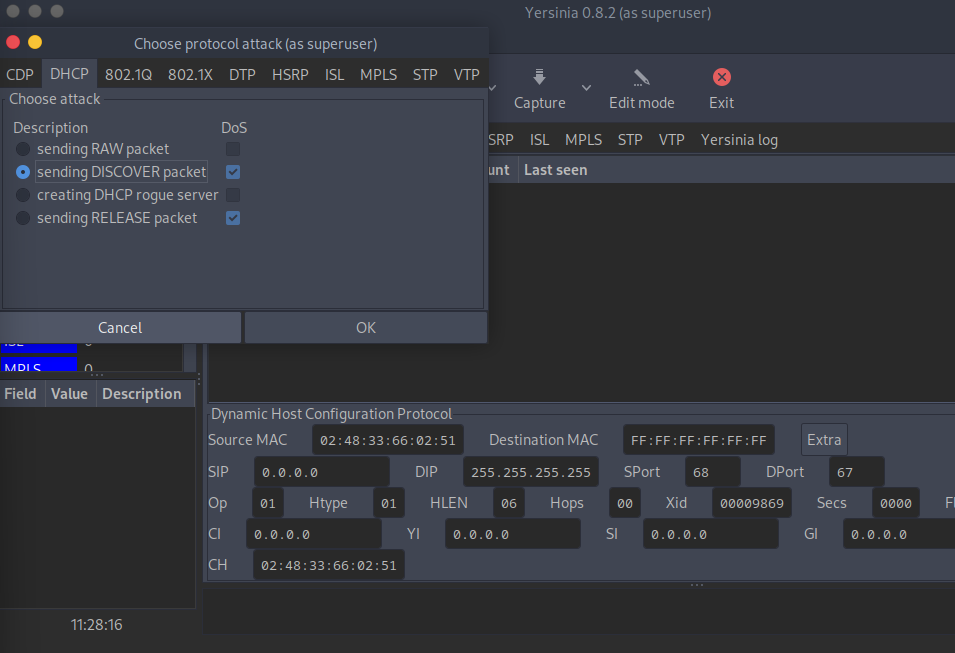
**DHCP starvation attack:**

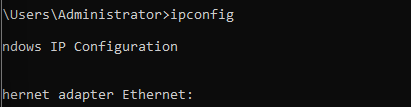
****

Using Yersinia:

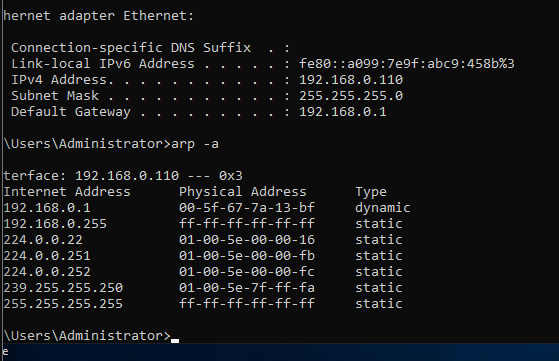


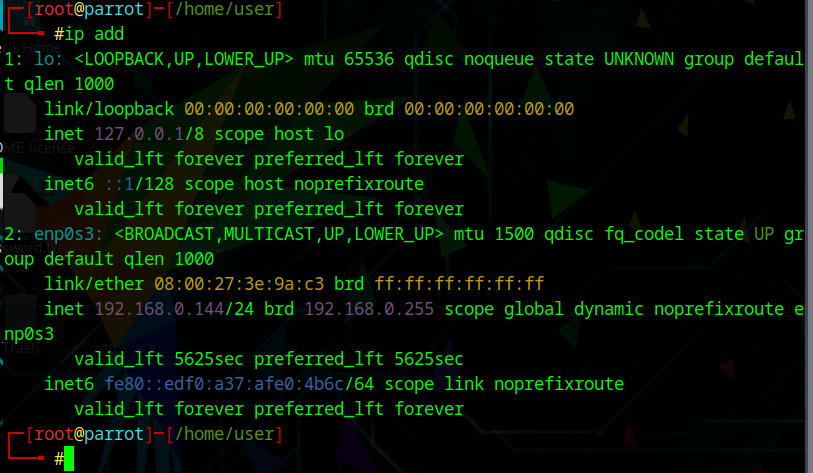


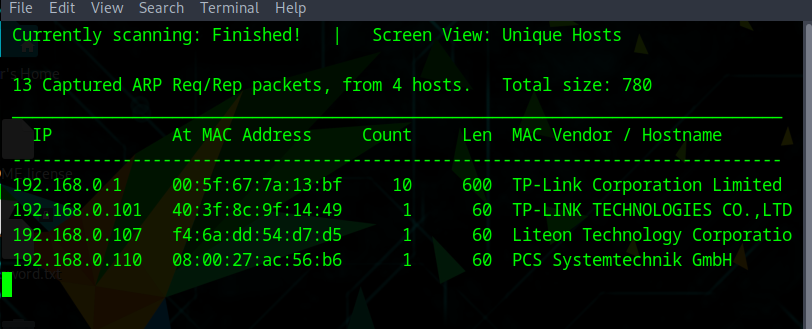


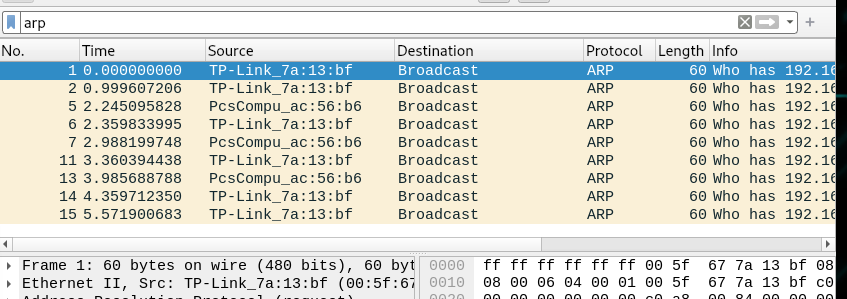


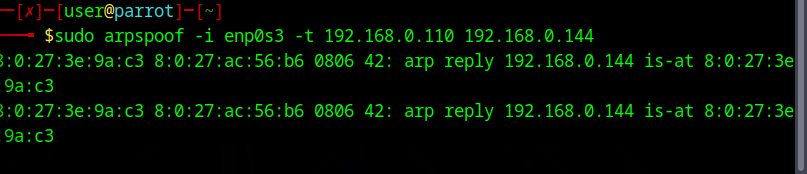
**ARP spoofing:**

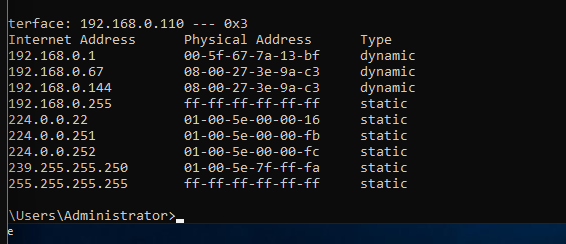


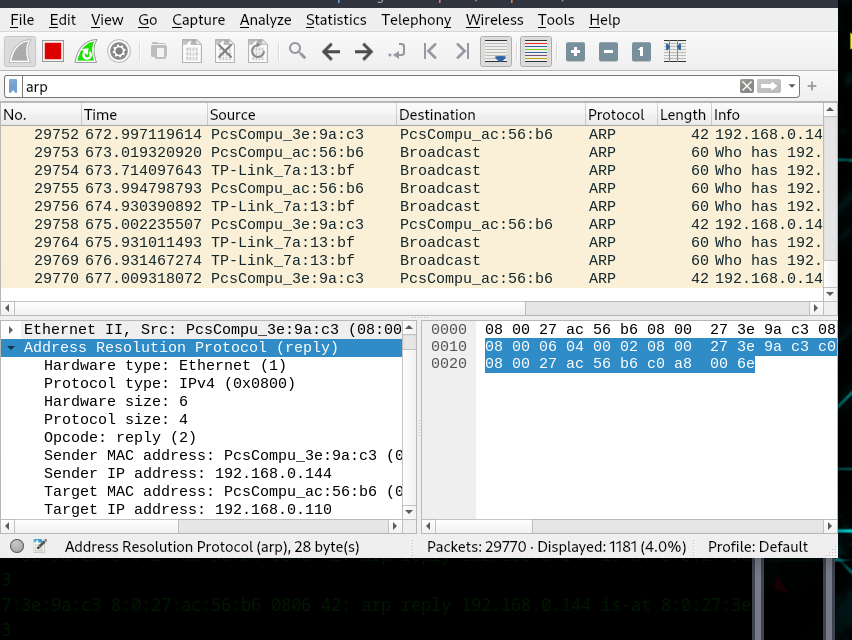












Using habu:

