**PRACTICAL NO 5**

**AIM:** Network Traffic Capture and DoS Attack with Wireshark and Nemesy

Network Traffic Capture:

* Use Wireshark to capture network traffic on a specific network interface.
* Analyze the captured packets to extract relevant information and identify potential security issues.

Denial of Service (DoS) Attack:

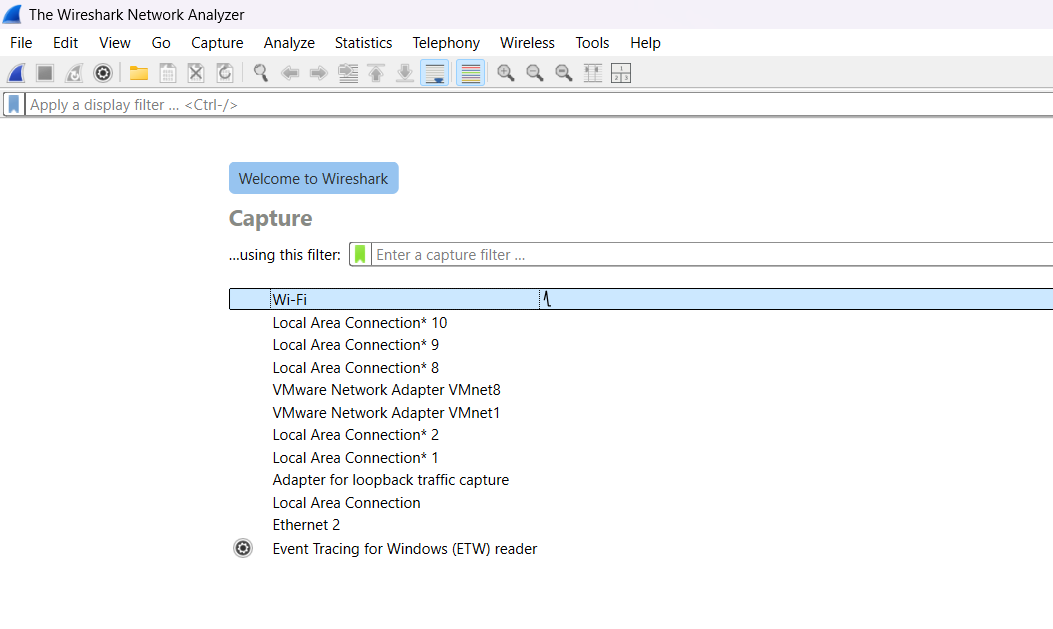
* Use Nemesy to launch a DoS attack against a target system or network.
* Observe the impact of the attack on the target's availability and performance.

**SOLUTION:**

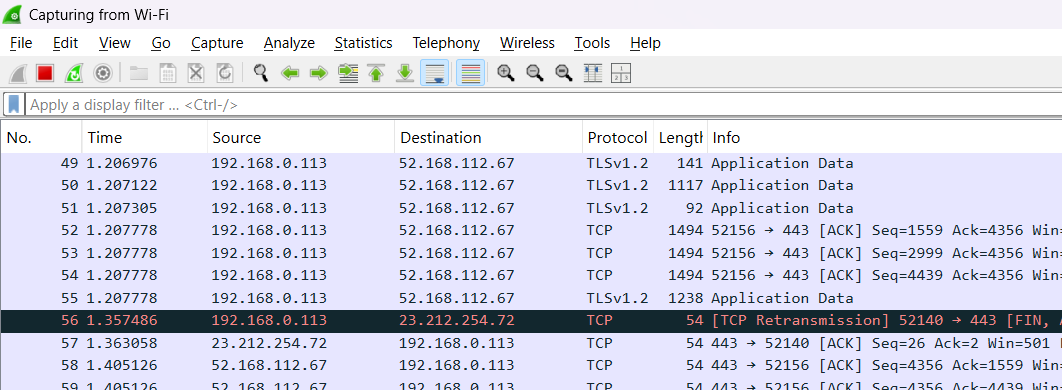
1) Network Traffic Capture:

* Use Wireshark to capture network traffic on a specific network interface.
* Analyze the captured packets to extract relevant information and identify potential security issues.

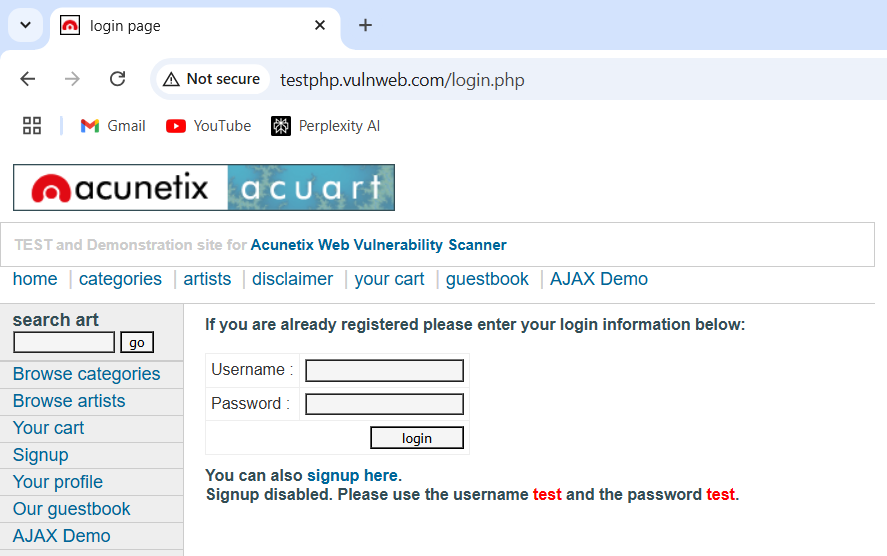
**Step 1 :** Open Wireshark and select WiFi



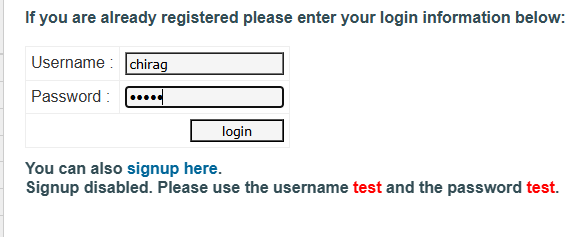
**Step 2 :** Start Capturing the Packets



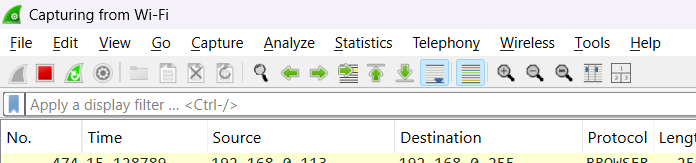
**Step 3 :** Go to chrome and visit the website : <http://testphp.vulnweb.com/login.php>



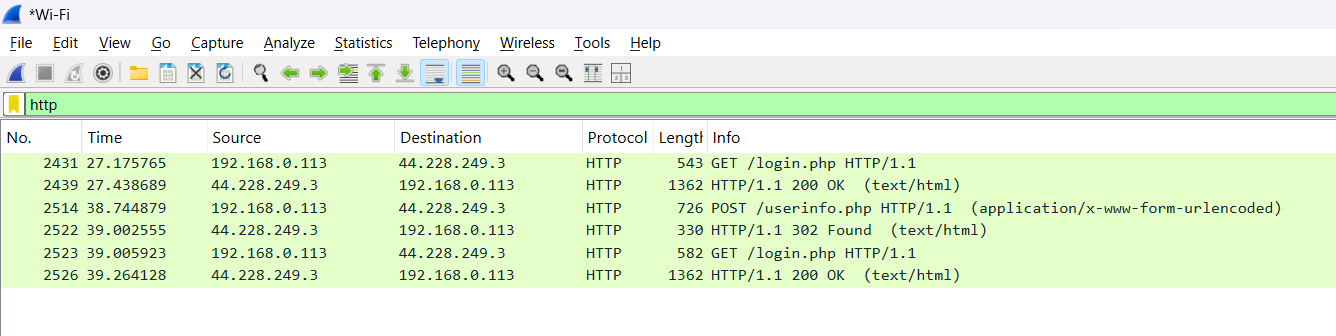
**Step 4 :** Now enter and username and password of your choice and click on login



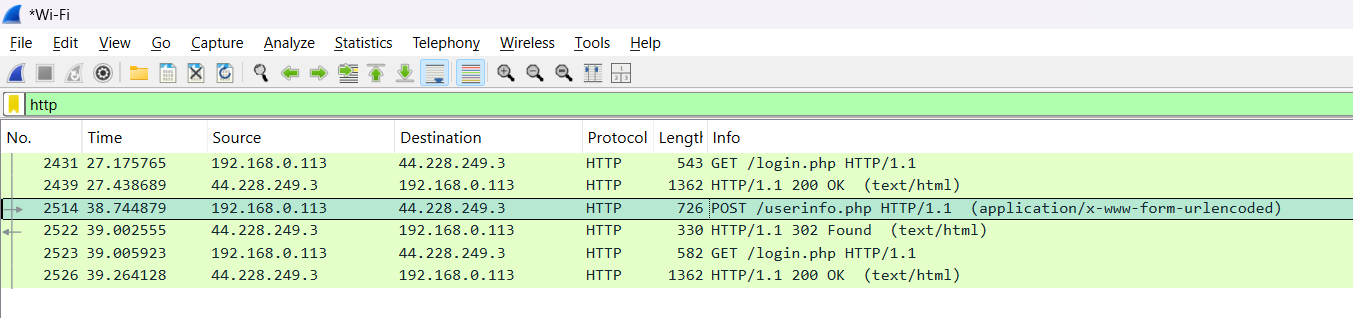
**Step 5 :** Go to wireshark and click on the Red square button to stop the capturing of packets



**Step 6 :** Type http in the search bar to retrieve only http packets



**Step 7 :** Select the below Post packet to view the username and password.



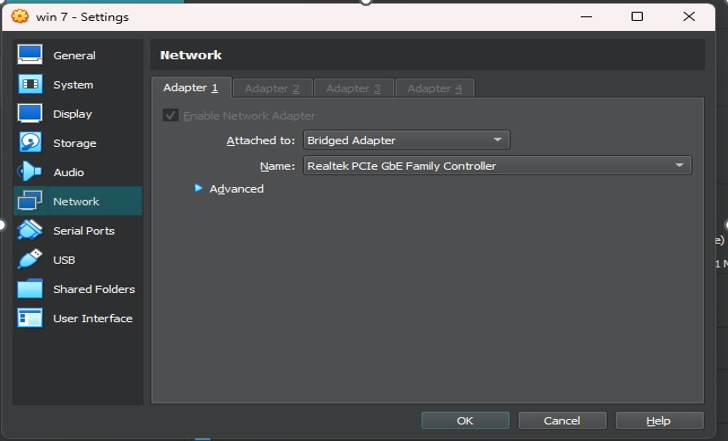
**Step 8 :** At the bottom you will get to see the username and password

****

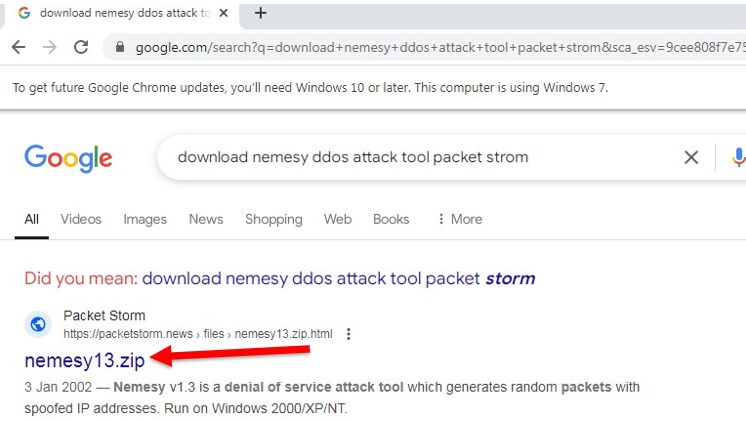
2) Denial of Service (DoS) Attack:

* Use Nemesy to launch a DoS attack against a target system or network.
* Observe the impact of the attack on the target's availability and performance.

**Step 1**: If you are using virtual windows 7 then do this setting in virtual box Setting → Network → Bridged Adapter



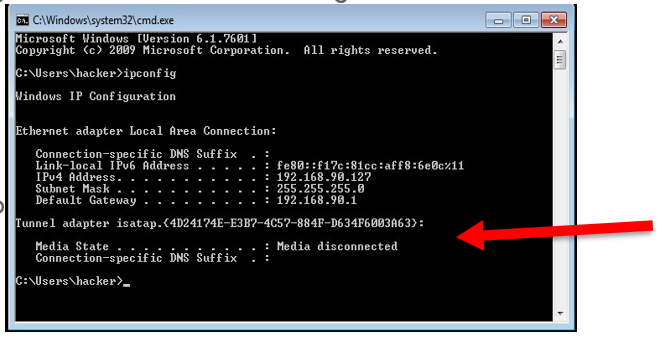
**Step 2 :** Download nemsey attack tool in windows 8



**Step 3 :** Open website and download it



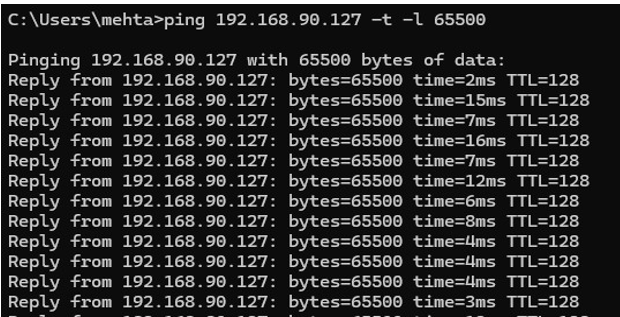
**Step 4**: Open cmd in win 7 and type ipconfig and note ip address



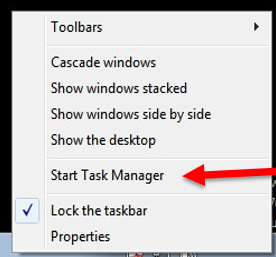
**Step 5**: Open cmd in targeted /main host and type ipconfig and note ip address in my case there we are considering “Ethernet adapter Ethernet”.



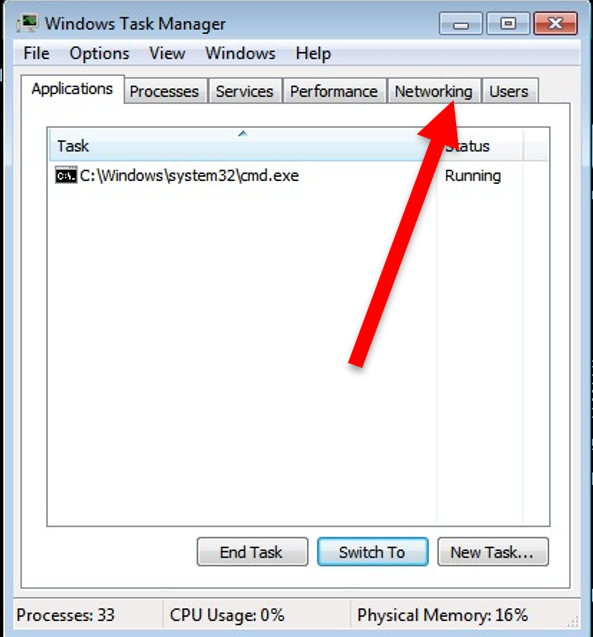
**Step 6**: Check connectivity between win 7 & host machine by sending packets to win 7 enter “ping [win 7 ip address] -t -l 65500”



**Step 7 :** Go to win 7 and right click on taskbar and Start Task Manager



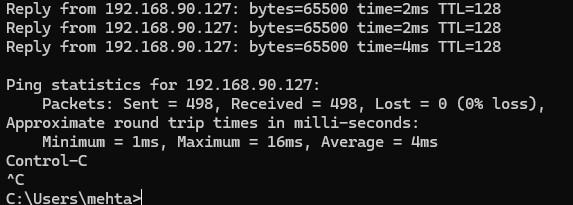
**Step 8 :** Go To networking



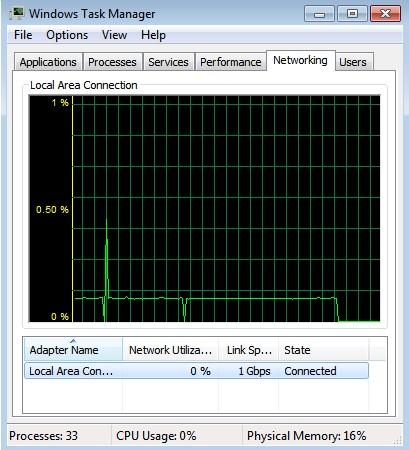
Now here you we are receiving packets in win 7



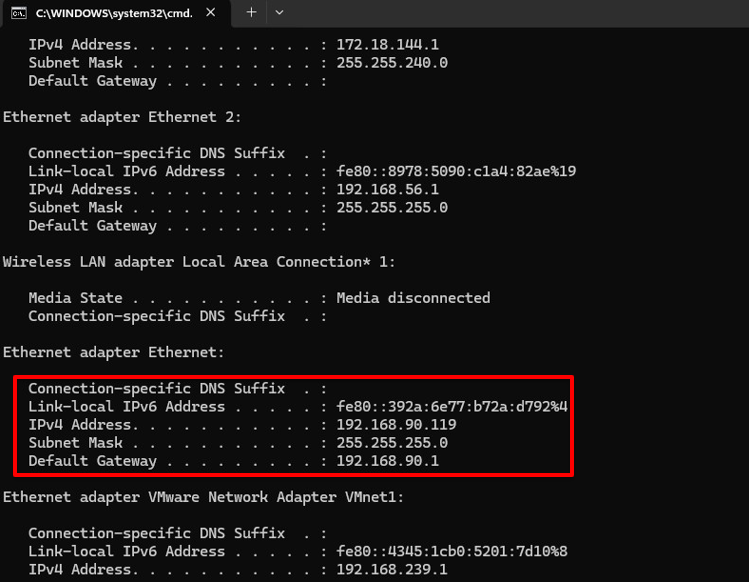
**Step 9**: Control – c to stop



After stop see the result



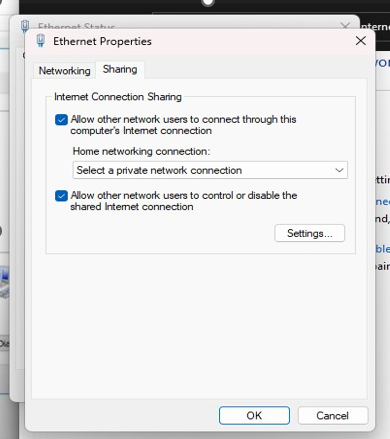
Note this details



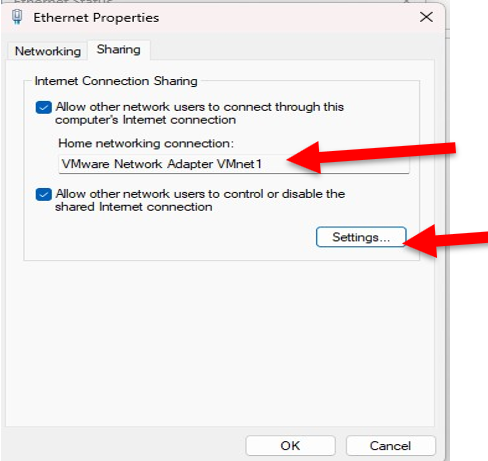
**Step 10:** Open control Panel



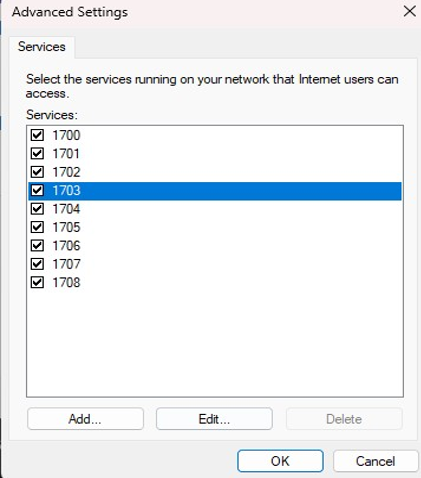
**Step 11**: Go to Network & Internet →Ethernet right click → select Properties → Sharing & Mark Checkbox & Change Home networking connection



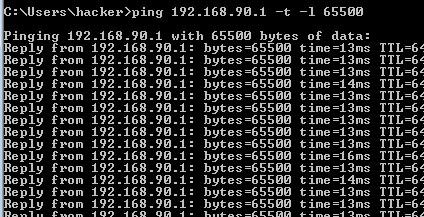
**Step 12 :** Select VMware network adaptor & After that click on setting

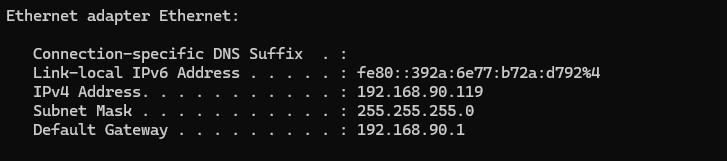


**Step 13 :** select all the services

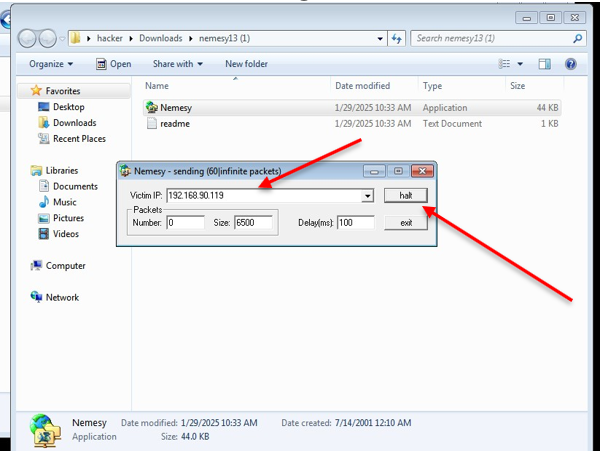


**Step 14**: Go to Win 7 open cmd Enter : ping [Default Gateway] -t -l 65500





**Step 15**: Install Nemesy in Win 7 & Enter Victim IP Address & no of packets size and time



Observe the impact of the attack on the target's availability and performance.

