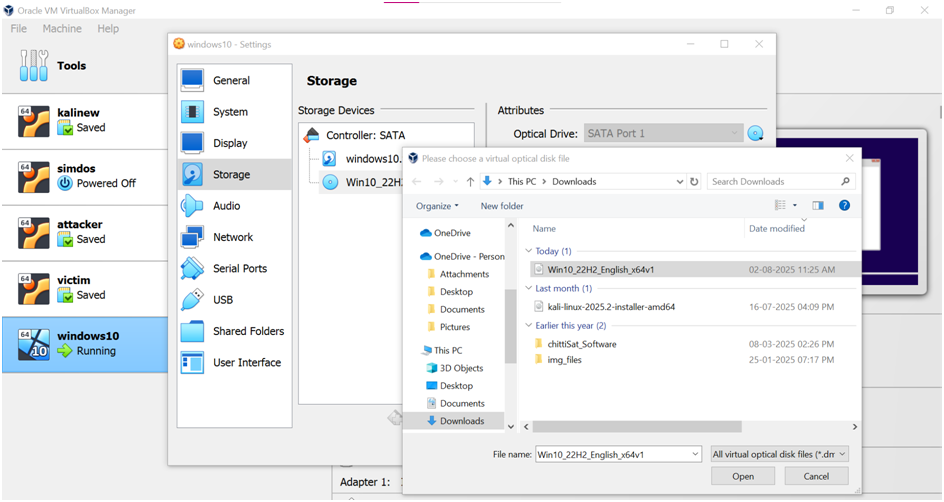
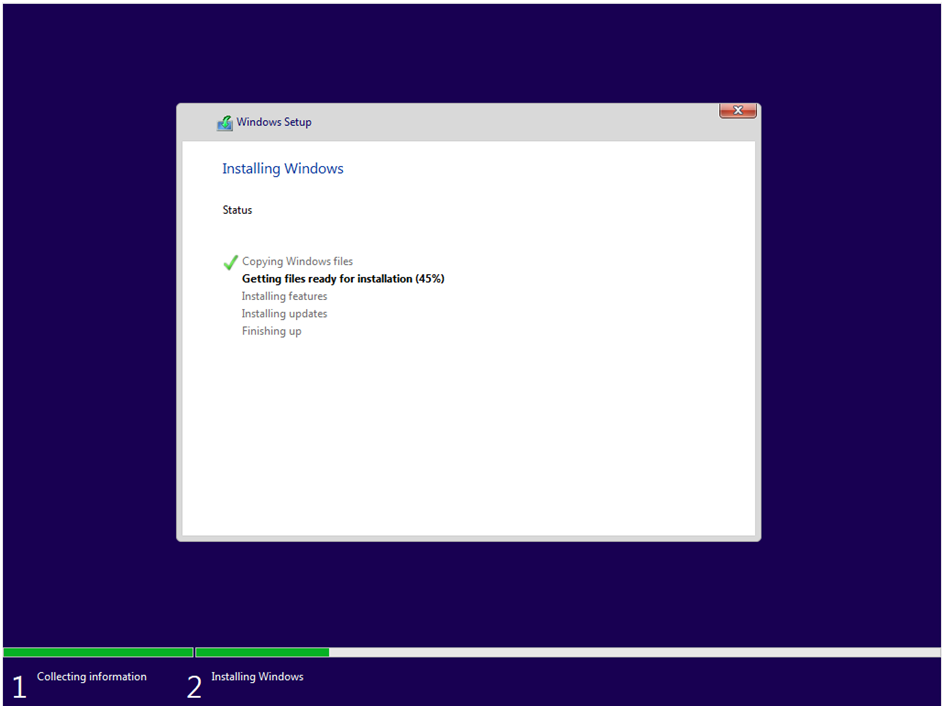
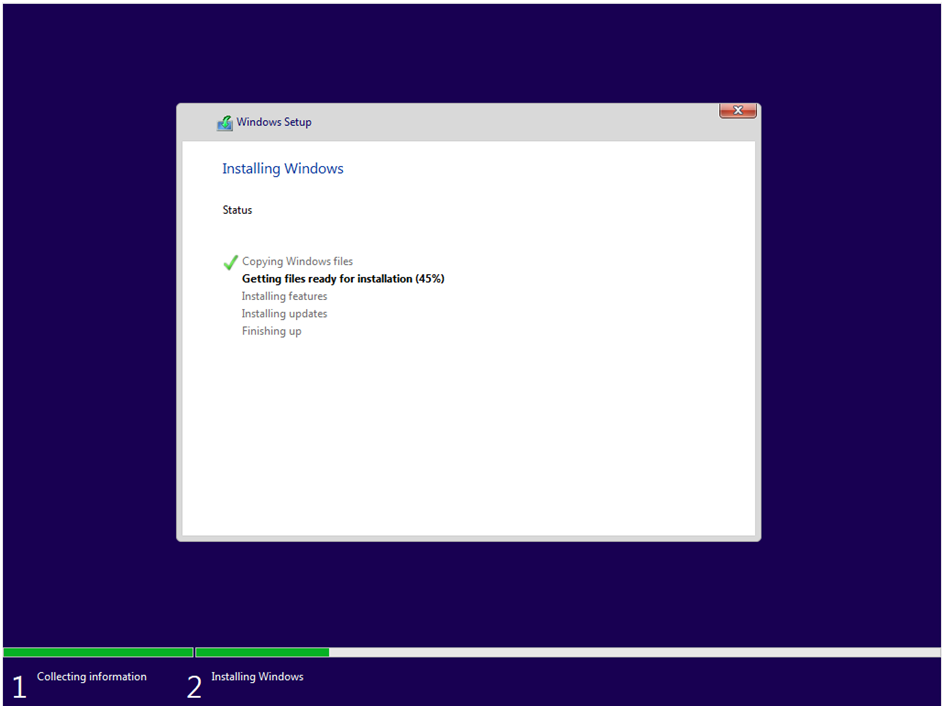
**Simulating dos attack from kali vm to windows 10 machine**.

• 1.Install windows 10\_english\_64bit. Create an instance in virtualbox,in storage->click empty disk->choose disk file->then ok.



• Setup windows10







• In settings of attacker(kali) and windows 10, for adapter 1-> enable and choose NAT

• Start both

• If the kali vm shows error: temporary not able to name resolution.Do,

• in terminal of attacker,

sudo systemctl restart NetworkManager

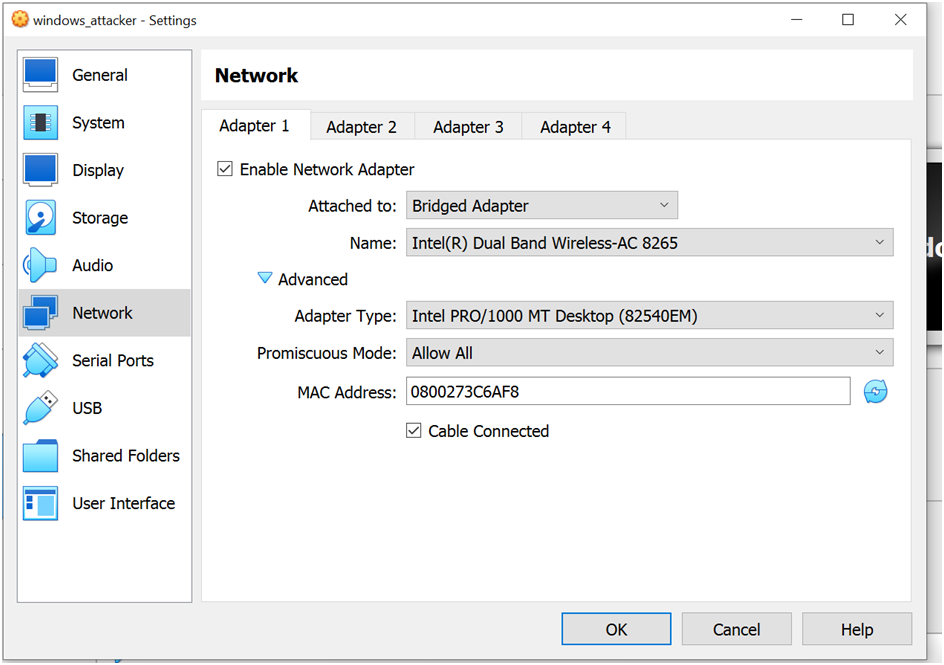
sudo nano /etc/resolv.conf

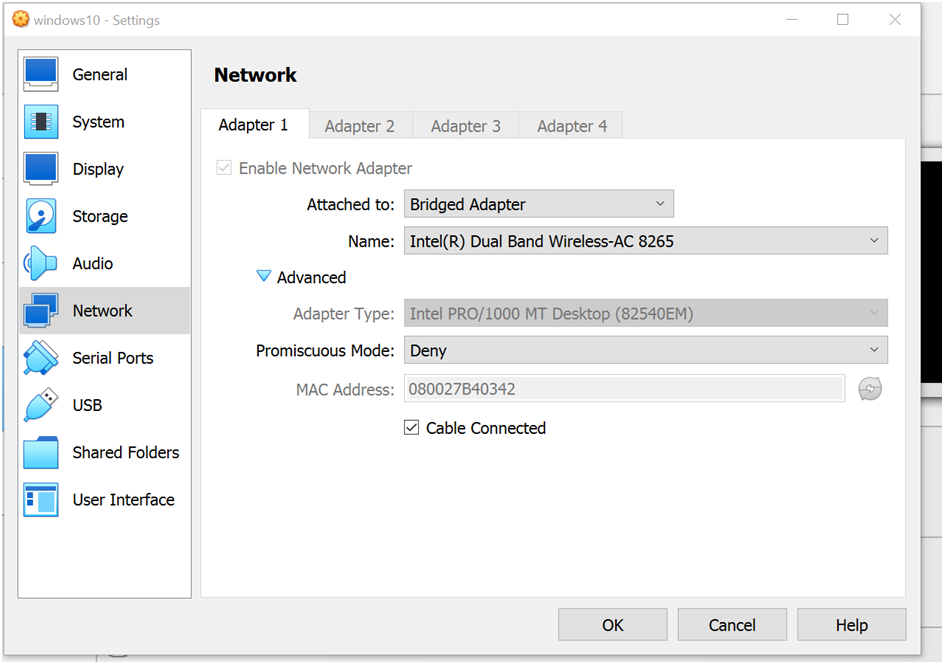
nameserver 8.8.8.8 ->add at first

the ctrl+o->enter->ctrl+x

• shutdown and start kali vm

• attacker and victim should present in same network and how different ip.





• In attacker, o cd Desktop

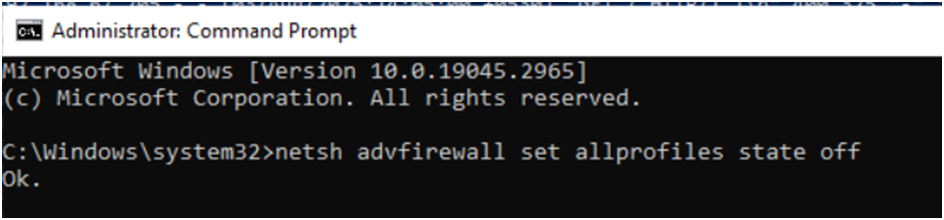
get hammer.git using,

git clone <https://github.com/cyweb/hammer.git> o

then cd hammer

• in victim,

Windows have firewall first off using , netsh advfirewall set allprofiles state off



recover using, netsh advfirewall set allprofiles state on

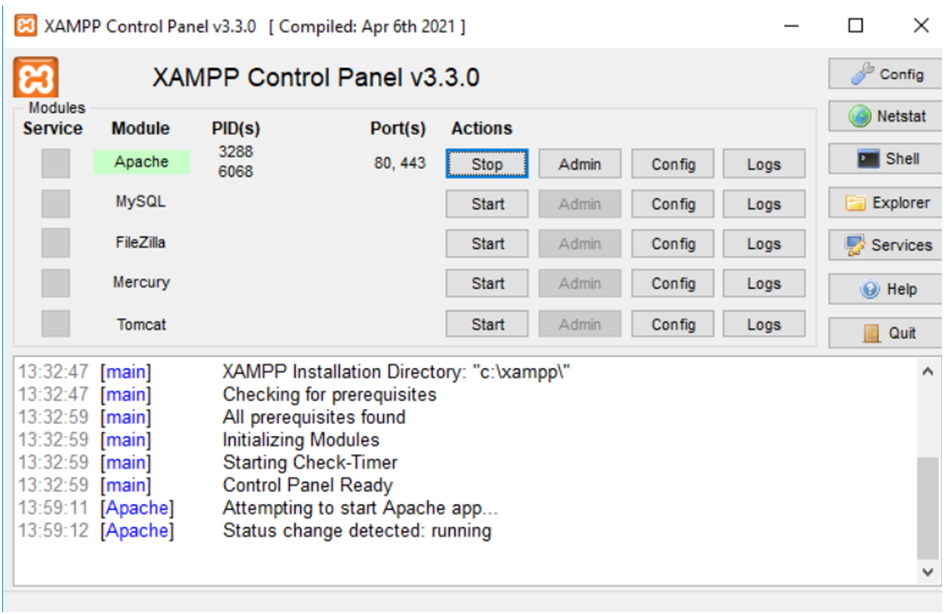
• Download and Install XAMPP o Go to: <https://www.apachefriends.org/index.html> Download XAMPP for Windows

Run the installer → Choose Apache (and optionally MySQL, PHP)

Install to: C:\xampp o Start Apache

Open XAMPP Control Panel

Click Start next to Apache

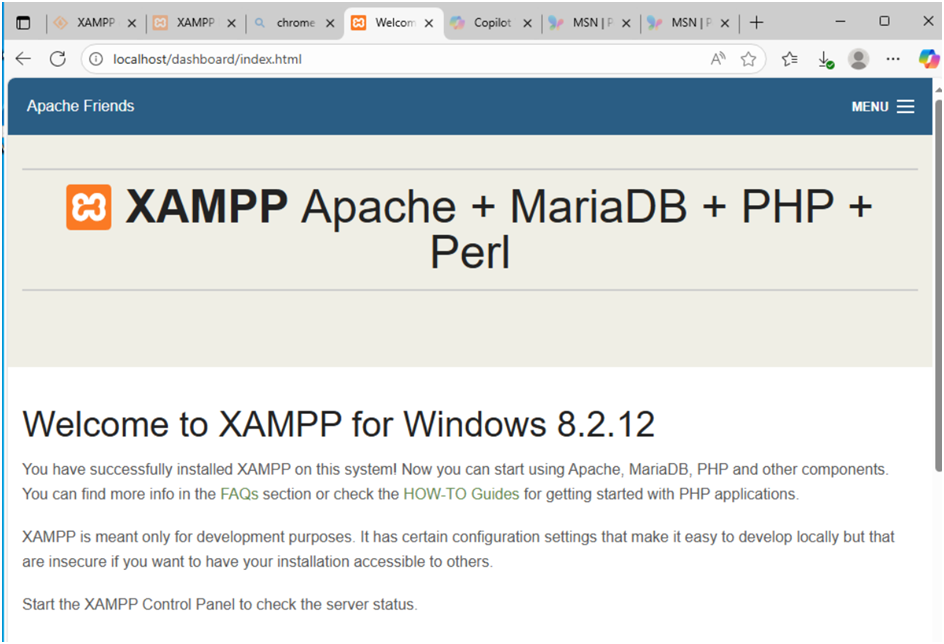


You should see the Apache icon turn green

Confirm Apache is running

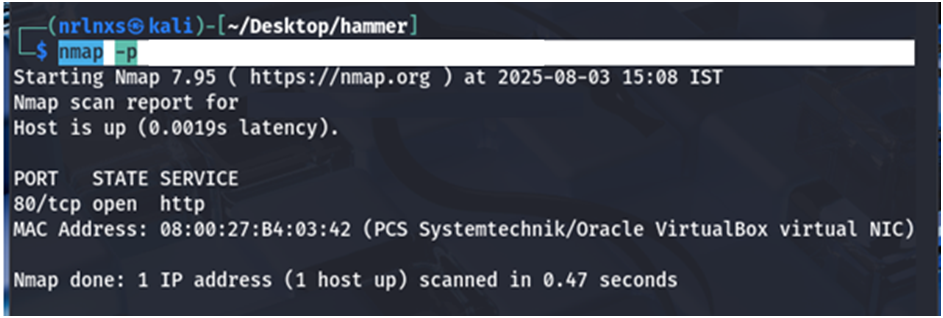
Open a browser on Windows:

Use:[http://localhost](http://localhost/)



• In attacker,

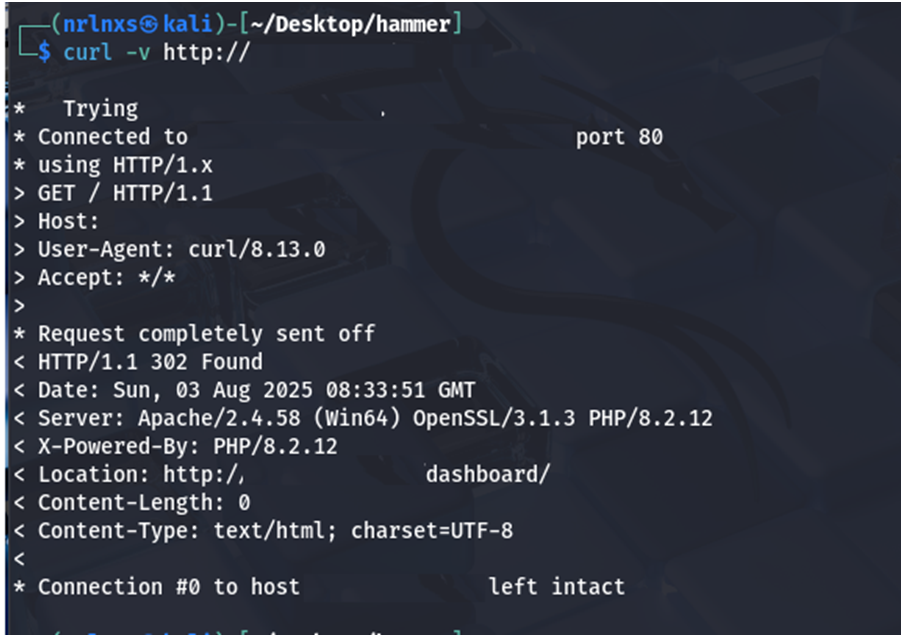
Ping the victim and use this command: nmap -p 80 ip of victim



• 80/tcp open

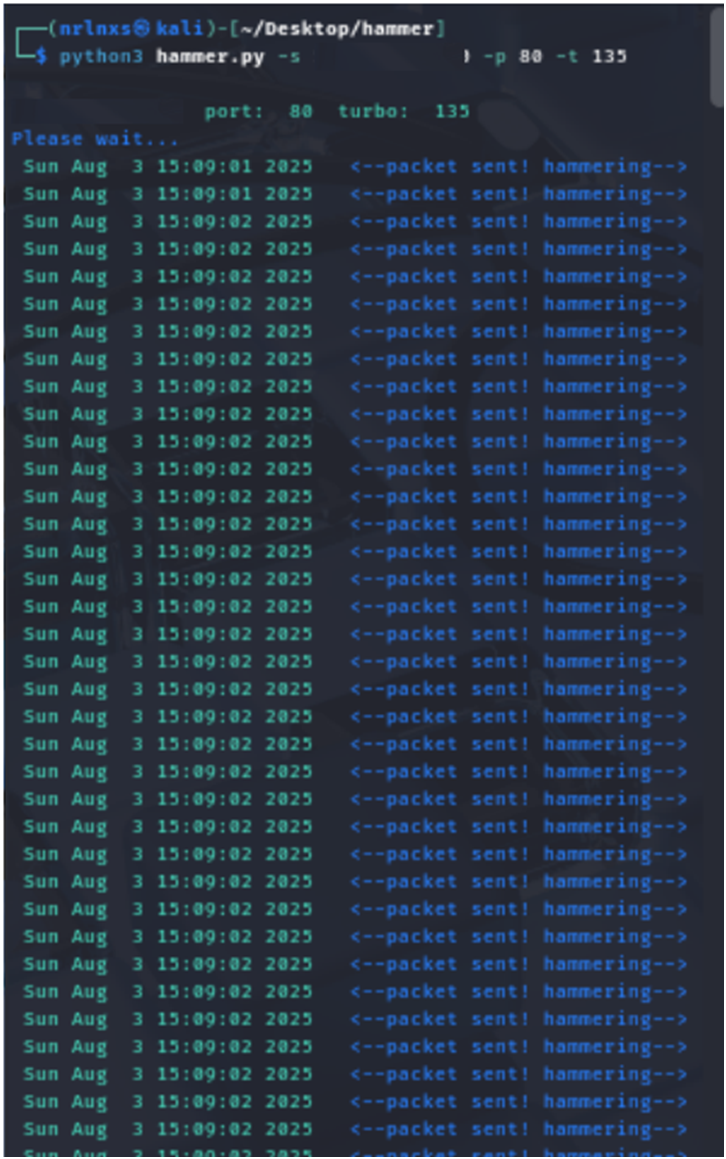
• Then we can simulate packets to victim

curl -v [http://victim\_ip](http://victim_ip/)

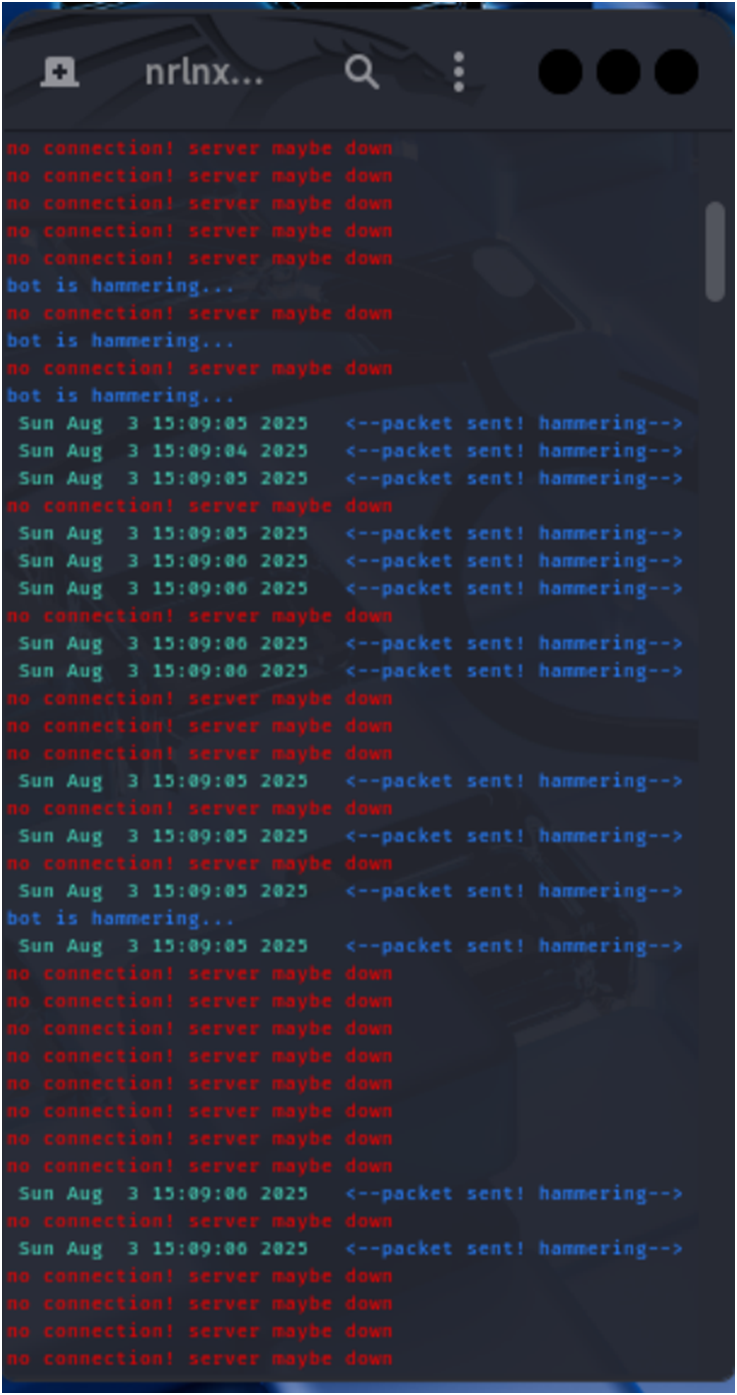


is used to make an HTTP request to a server at ip of victim and display verbose output about the request and response.

• Use python3 hammer.py –s ip of victim –p 80 –t 135

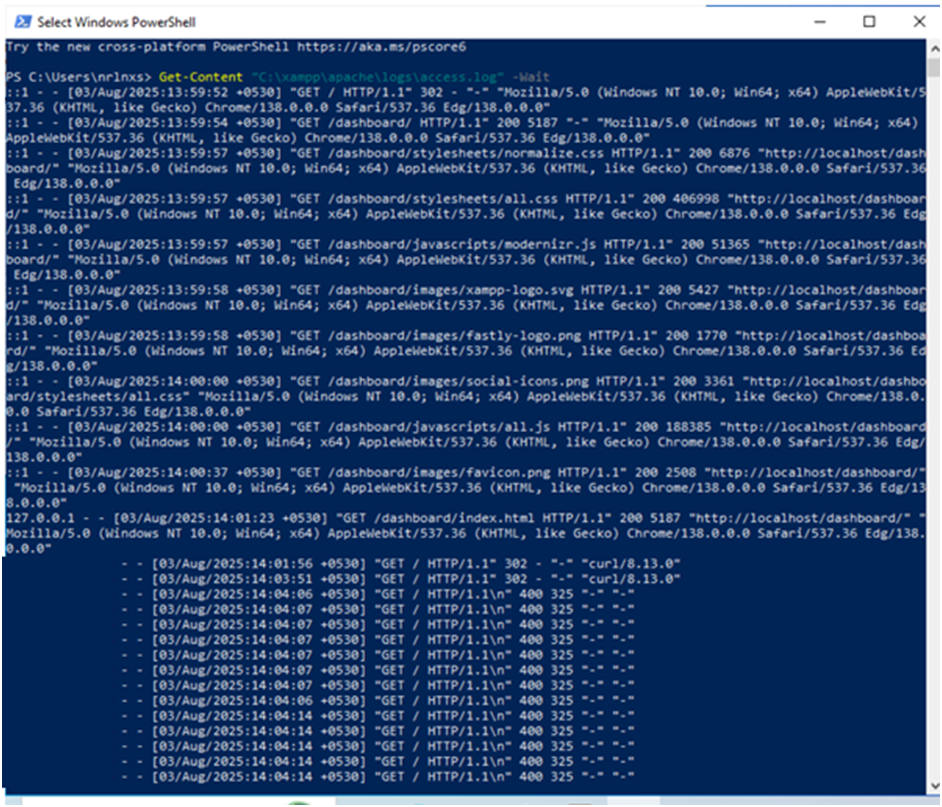


• In 3 minutes 24 seconds, 926 packets were transmitted and make the victim server down and the system started hang not working properly.

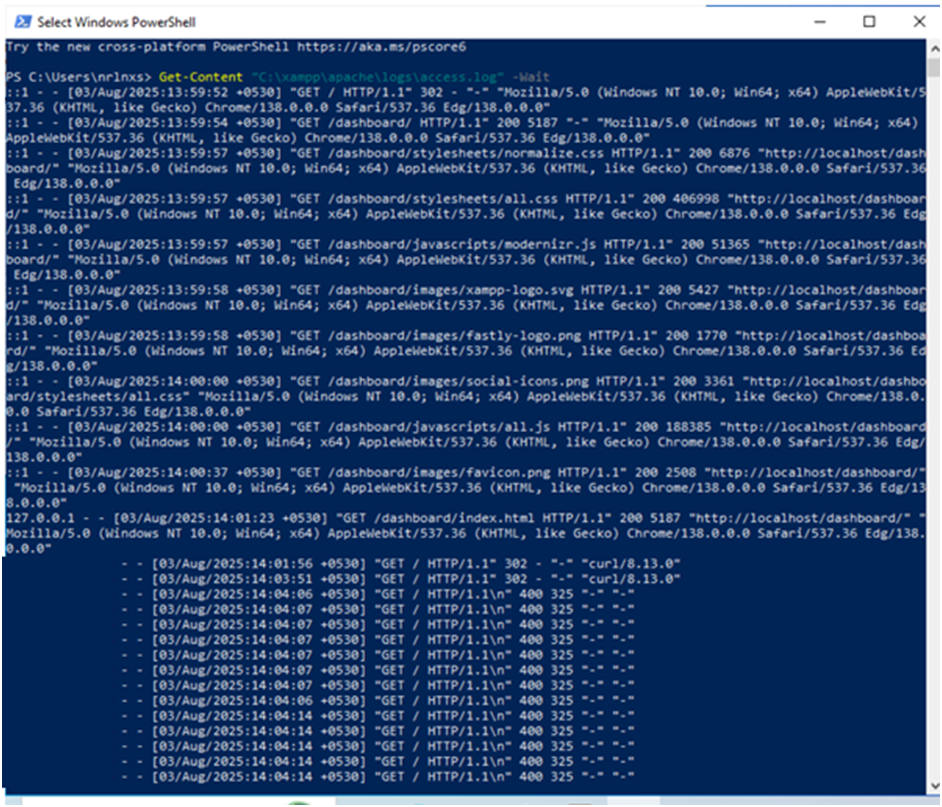


• To check status of victim, in powershell

Type: Get-Content “C:\xampp\apache\logs\access.log\” –Wait



• To count no.of packets: (Get-Content “C:\xampp\apache\logs\access.log\”).Count



• To stop the packet simulation, use ctrl+c in attacker machine.

• After that stop apache.