Cybersecurity (Security+) and P4 Programmable Switches

Overview Cybersecurity Labs

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

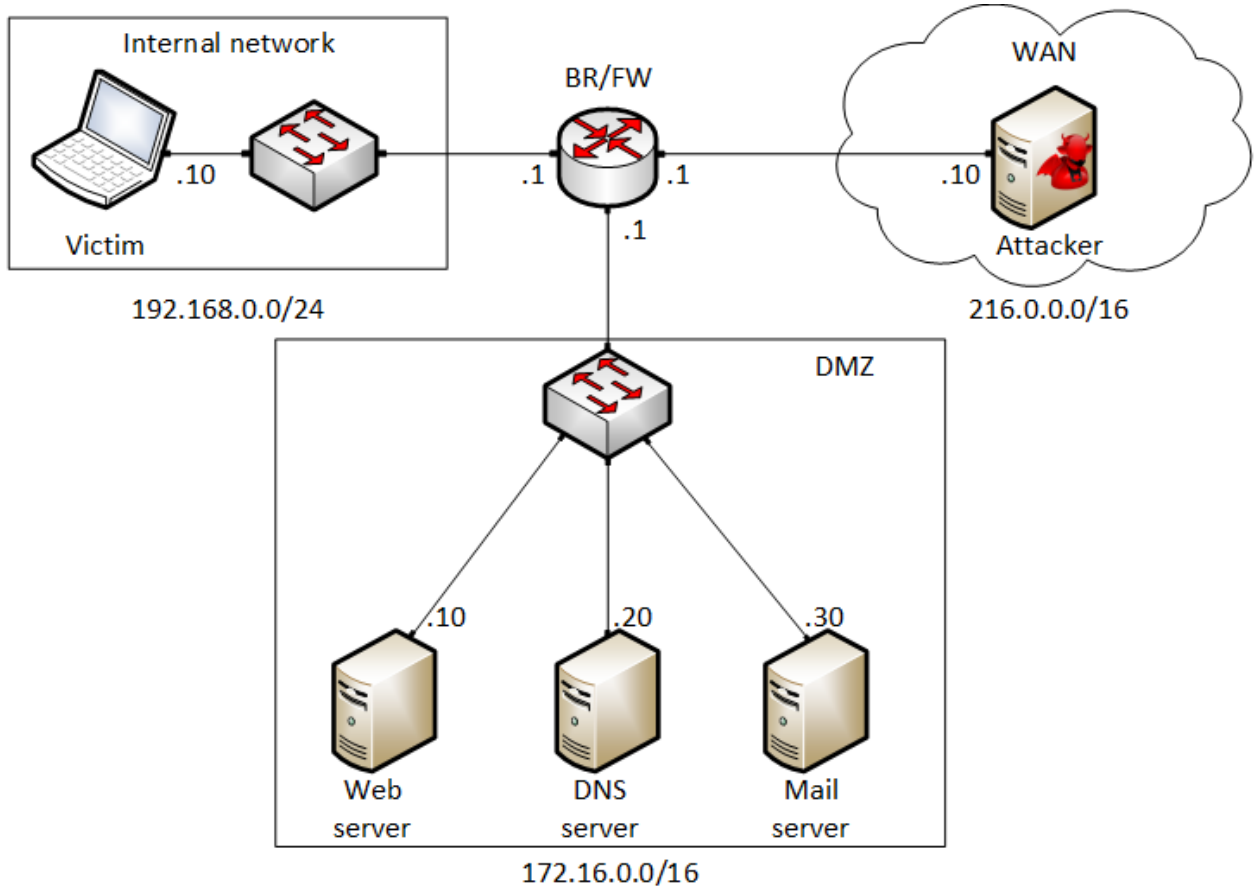
June 20th, 2023

Lab 8: Denial of Service (DoS) Attacks: SYN/FIN/RST Flood, Smurf attack, and SlowLoris

Attack Scenario

Transport layer DoS:

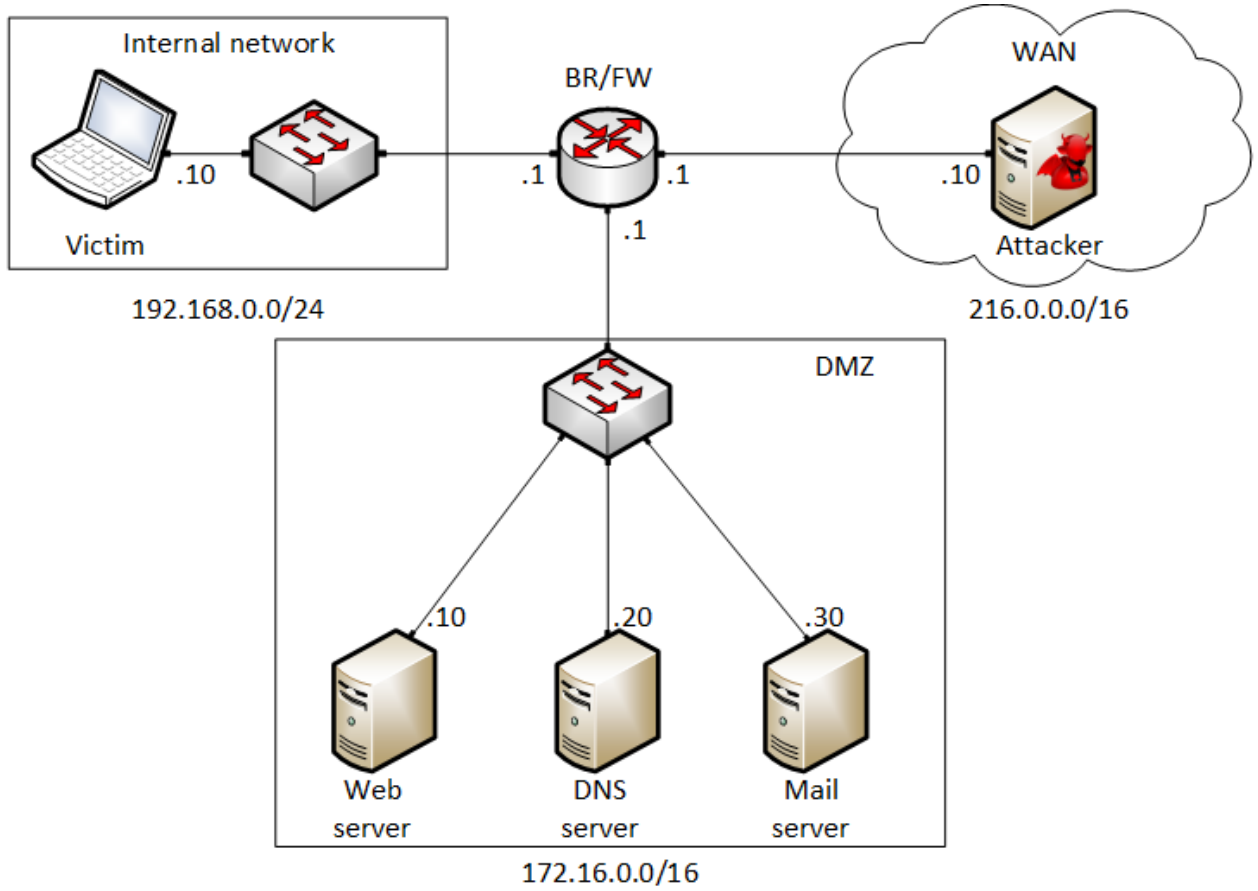
- SYN/FIN/RST flood: the attacker uses the *hping3* tool to perform a SYN/FIN/RST flood against the web server
  - During the attack, the web server will fail to accept new sessions from legitimate users
- UDP flood: the attacker uses the *hping3* tool to perform a UDP flood against the web server



Attack Scenario

Network layer DoS:

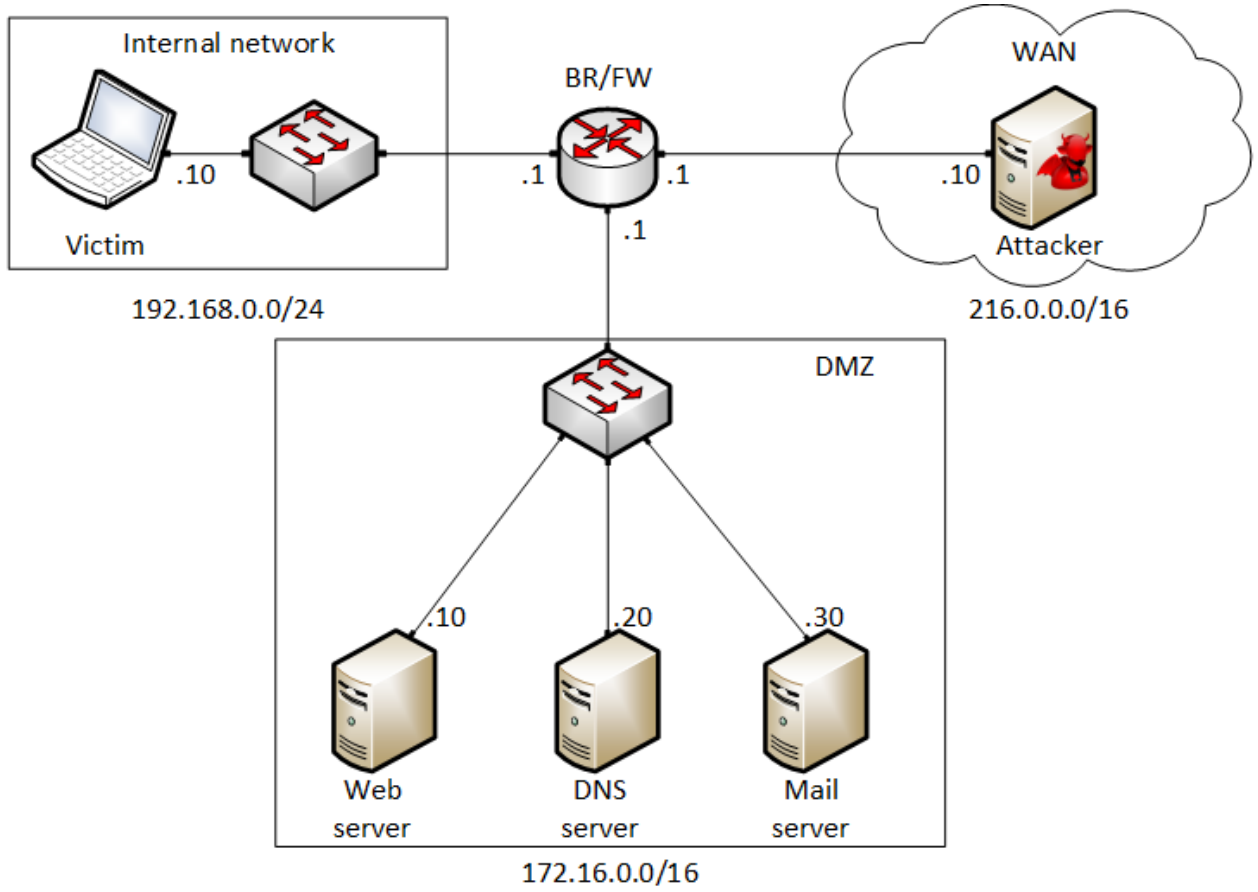
- ICMP flood: the attacker uses the *hping3* tool to perform an ICMP flood against the web server
- Smurf attack: the attacker uses the *hping3* tool to launch a Smurf attack against the victim
  - The attack will use the web server in the DMZ zone as the reflector



Attack Scenario

Application layer DoS:

- *SlowLoris*: the attacker will use a custom script to perform a *SlowLoris* attack against the web server



Disable Linux DoS Attack Defenses

Disabling reverse path forwarding on BR/FW

```
[root@BR-FW ~]# sysctl -w net.ipv4.conf.ens33.rp_filter=0
net.ipv4.conf.ens33.rp_filter = 0
[root@BR-FW ~]# sysctl -w net.ipv4.conf.all.rp_filter=0
net.ipv4.conf.all.rp_filter = 0
[root@BR-FW ~]# _
```

Disabling SYN cookies on the web server

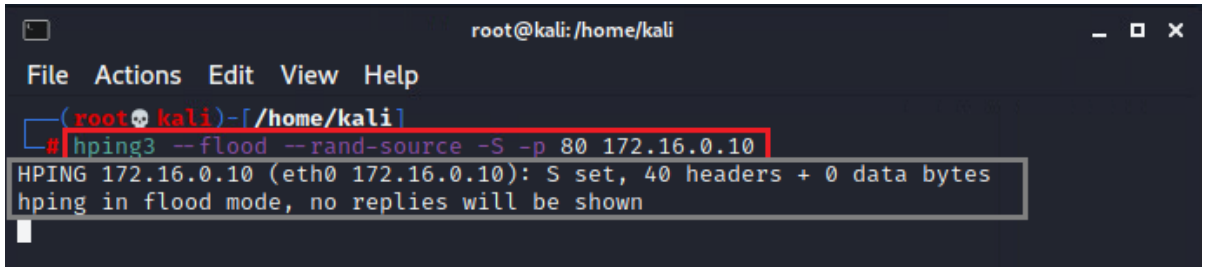
```
[root@Web-server ~]# docker exec -it c1aaf24acdd9 sysctl net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[root@Web-server ~]#
```

Disabling TCP session caching on the web server

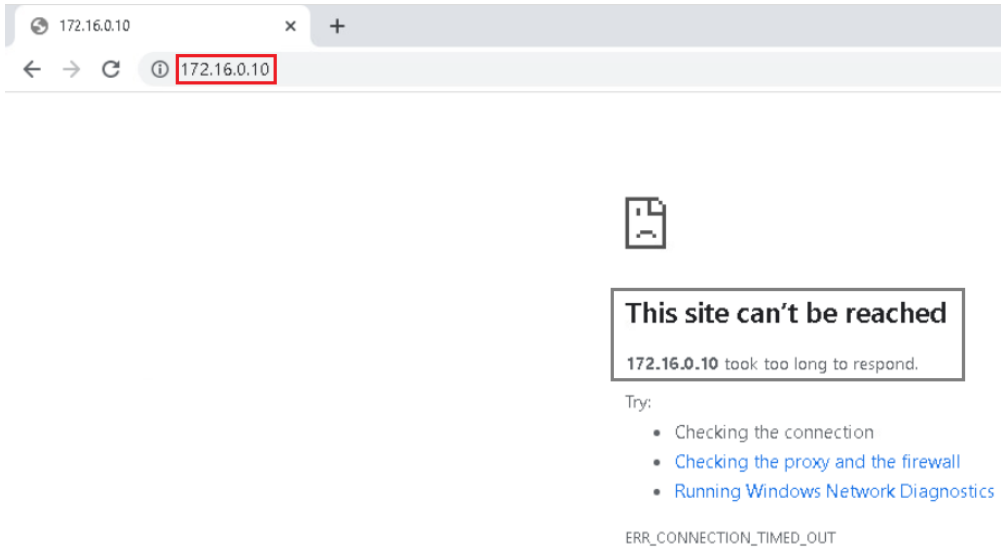
```
[root@Web-server ~]# docker exec -it c1aaf24acdd9 sysctl net.ipv4.tcp_no_metrics_save=1
net.ipv4.tcp_no_metrics_save = 1
[root@Web-server ~]# _
```

Transport Layer DoS

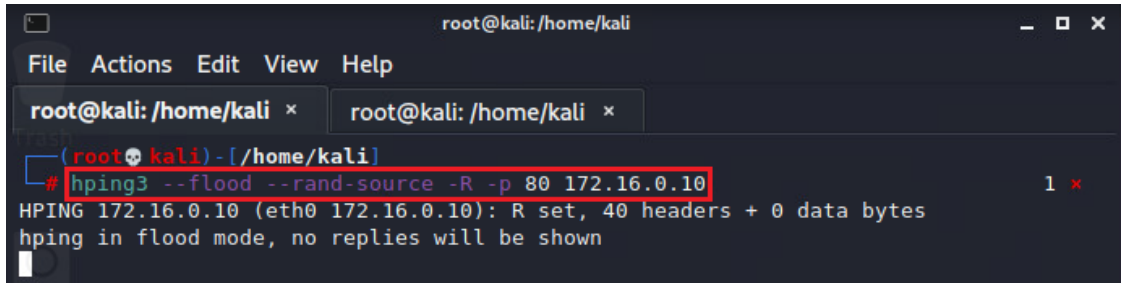
Performing TCP SYN flood on the web server



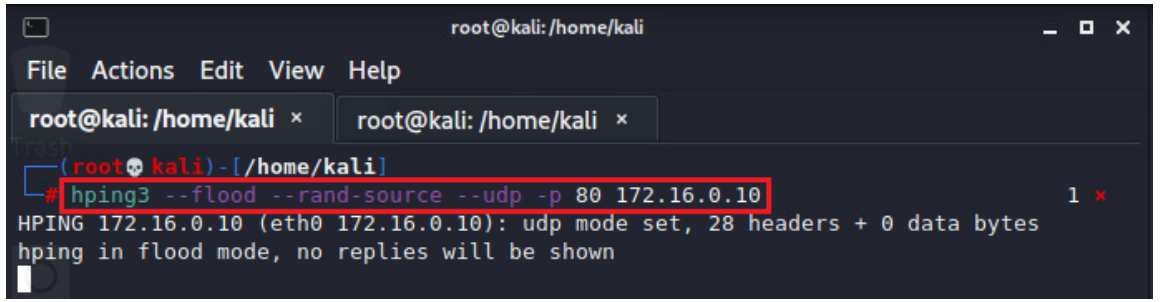
Web server becomes unavailable for legitimate users



Performing TCP FIN flood on the web server

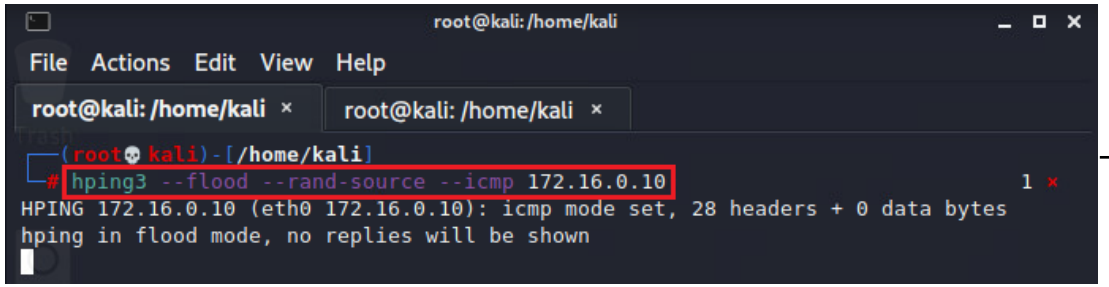


Performing UDP flood on the web server

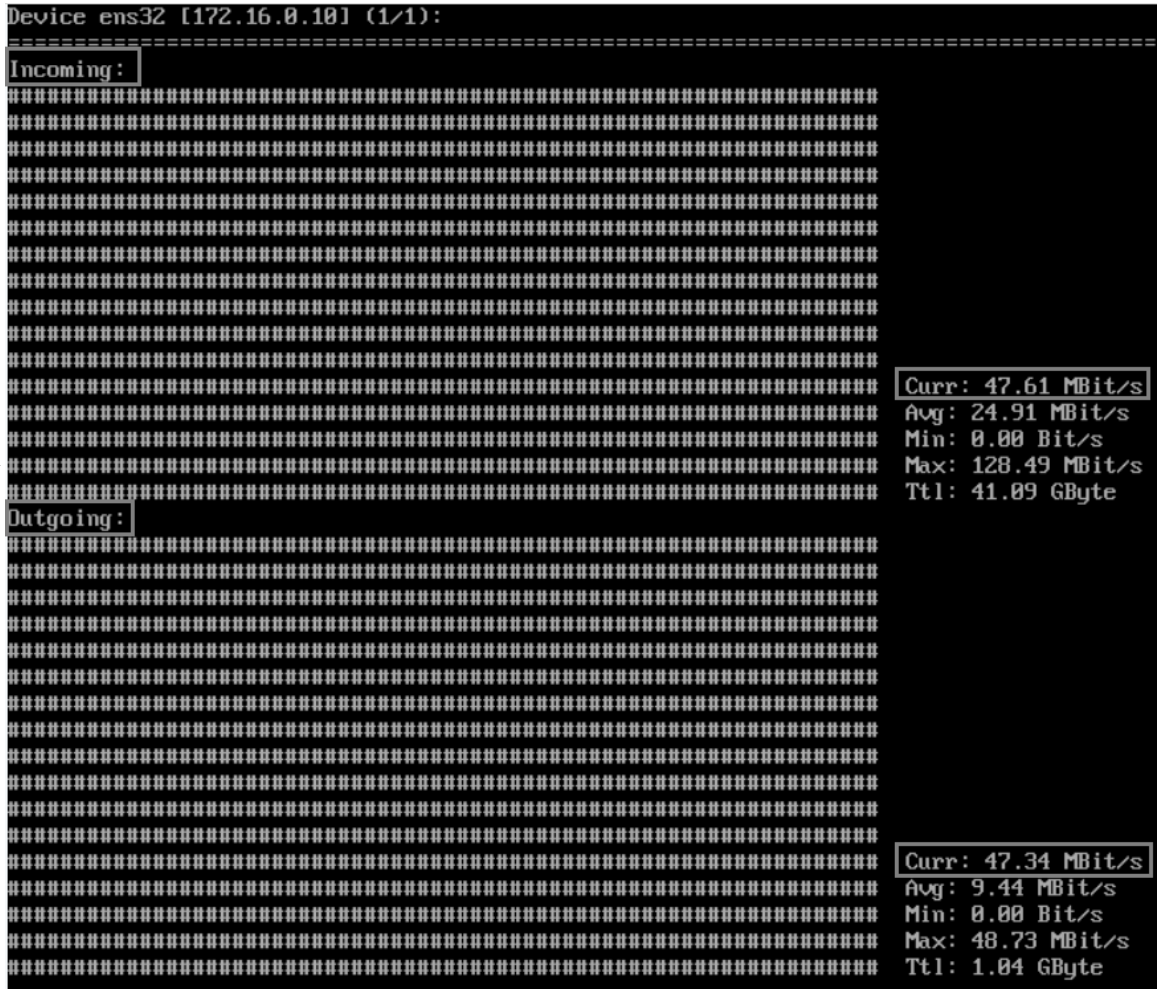


Network Layer DoS

Performing ICMP flood on the web server

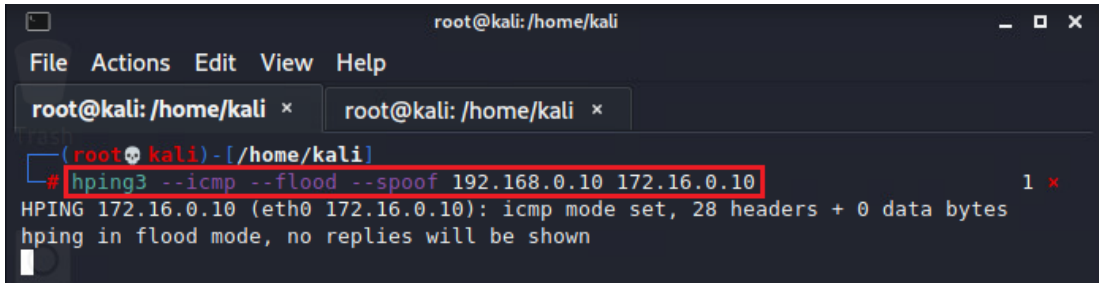


Inspecting the incoming and outgoing throughput rates on the web server

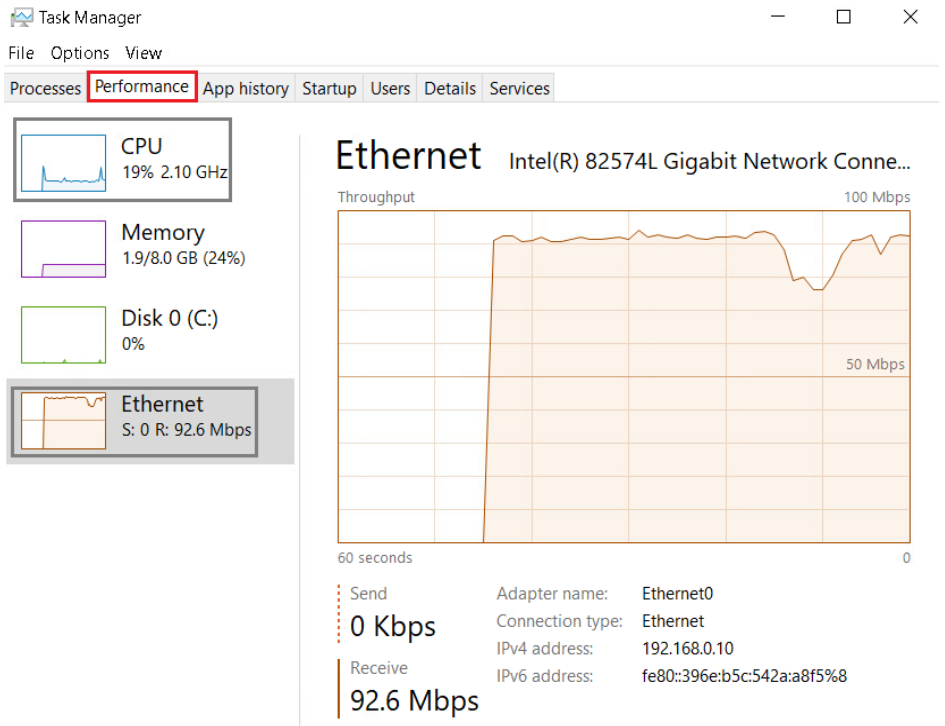


Network Layer DoS

Performing *Smurf* attack on the victim using the web server as the reflector

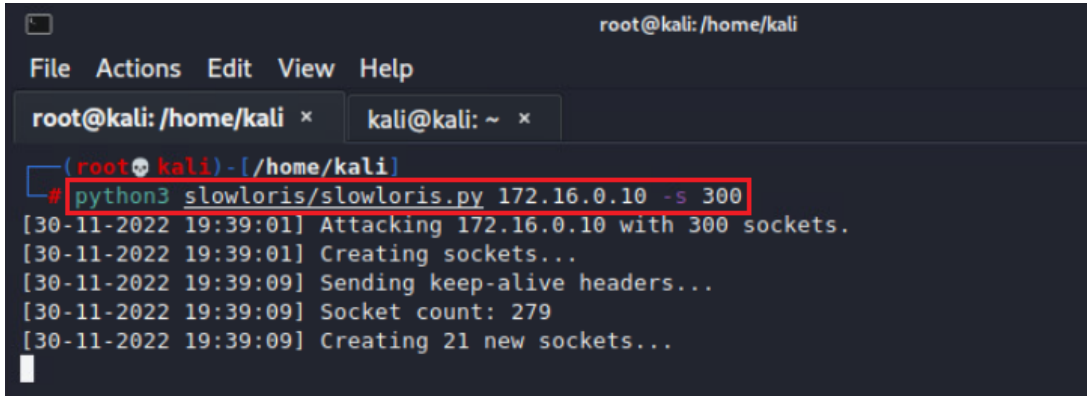


Inspecting the incoming throughput rate and the CPU on the victim's machine



Application Layer DoS

Performing *SlowLoris* attack on the web server



Testing the connectivity time to reach the web server