

1.

در این آزمایش به پیاده سازی syn flooding پرداختم
در مرحله با استفاده از کتابخانه scapy یک اسکریپت نوشتم که پکت های syn را به ادرس مورد نظر ارسال کرده و syn/ack را دریافت میکند.

```

mohammad@mohammad-X556UQ: ~/Documents/amnat/az/hws/q1
$ sudo python3 tcp_flooding.py
Destination IP: 185.50.45.41
Destination Port: 80
Number of Packets: 1000
1 Packet Sent
2 Packet Sent
3 Packet Sent
4 Packet Sent
5 Packet Sent
6 Packet Sent
7 Packet Sent
8 Packet Sent
9 Packet Sent
10 Packet Sent
11 Packet Sent
12 Packet Sent
13 Packet Sent
14 Packet Sent
15 Packet Sent
16 Packet Sent
17 Packet Sent
18 Packet Sent
19 Packet Sent
20 Packet Sent
21 Packet Sent
22 Packet Sent
23 Packet Sent
24 Packet Sent
25 Packet Sent
26 Packet Sent
27 Packet Sent
28 Packet Sent
29 Packet Sent
30 Packet Sent
31 Packet Sent
32 Packet Sent
33 Packet Sent
34 Packet Sent
35 Packet Sent
36 Packet Sent
37 Packet Sent
38 Packet Sent
39 Packet Sent
40 Packet Sent
41 Packet Sent
42 Packet Sent
43 Packet Sent
44 Packet Sent
45 Packet Sent
46 Packet Sent
47 Packet Sent
48 Packet Sent
49 Packet Sent

```

پس از اجرای کد بر روی آیپی 185.50.45.41 و پورت 80 سیستم مورد نظر نتایج زیر را گرفتیم که نشان میدهد کد به درستی کار میکند.

2	0.000964070	192.168.43.119	185.50.45.41	TCP	54	48272 → 80 [SYN] Seq=0 Win=8192 Len=0
3	0.049074949	192.168.43.119	185.50.45.41	TCP	54	30604 → 80 [SYN] Seq=0 Win=8192 Len=0
4	0.056185929	185.50.45.41	192.168.43.119	TCP	58	80 → 13990 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
5	0.076414549	185.50.45.41	192.168.43.119	TCP	58	80 → 1120 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400
6	0.076513328	185.50.45.41	192.168.43.119	TCP	58	80 → 42891 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1400

2.

برای پیاده سازی این حمله با ایجاد تغییر در کد قبل اگر در هر مرحله ایپی سورس را برابر مقداری تصادفی قرار دهیم میتوانیم حمله ip spoofing را پیاده سازی کنیم.
در مرحله بعد هم به پیاده سازی کرنل مازول پرداختم برای این منظور با استفاده از کدهای قبلی که در درس سیستم عامل یاد گرفته بودم سیستم کلی را پیاده سازی کردم و برای اجرا لازمه که در فایل config.txt ادرس ip مدنظر که قراره بلاک بشه رو توی بلک لیست اضافه کنید. به عنوان مثال من کد رو متناسب با ip سیستمم خودم تغییر دادم و روی ماشین مجازی اجرا کردم و سیستمم توانایی اجرای کد syn flooding را علیه ماشین مجازی نداشت.

3.

این حمله برای جعل یک tcp triple handshake میباشد و به طور کلی شامل 5 مرحله میباشد:

در مرحله اول مهاجم سعی میکند که به جمع اوری اطلاعات بپردازد به این صورت که رفتار sequence number generator مربوط به tcp را مدل کند تا بتواند یک رابطه امن را با کامپیوتر مورد هجوم ایجاد کند. همچنین سعی میکند تا ایپی سرورهایی که قبلا با کامپیوتر ارتباط داشته اند را پیدا کند.

پس در این مرحله تعداد زیادی ریکوست به سمت کامپیوتر مورد حمله ارسال میکند و تلاش میکند تا sequence number درست را کشف کند و یک رابطه نیمه باز را ایجاد کند. هنگامی کشف شد رد مرحله بعد بسته syn/ack از طرف کامپیوتر به سمت سرور قبلا متصل شده ارسال میشود پس در مرحله بعد لازم است جلوی سرور را بگیرد چرا که از انجایی که سرور بسته syn را نفرستاده پس از دریافت syn/ack بسته reset را ارسال کرده و همه چیز را خراب میکند پس در با استفاده از ip flooding سرور را مشغول میکنیم تا نتواند به بسته syn/ack ارسالی از کامپیوتر مورد حمله پاسخ دهد. پس با ایپی spoof شده و مقدار sequence number کشف شده میتوانیم تا حمله را ادامه داده و خود را به جای سرور مورد اعتماد به کامپیوتر مورد حمله متصل کنیم.

در این مرحله لازم است تا یک backdoor در کامپیوتر ایجاد کنیم تا ازین به بعد به راحتی به آن وصل شویم.

در مرحله بعد هم سرور مورد اعتماد بسته reset را ارسال میکند.

4.

در این آزمایش به دنبال پیاده سازی DDOS هستیم. در مرحله اول سیستم ها را آماده به کار کردم. از روی سیستم خودم با ایپی 192.168.43.119 و یک ماشین مجازی با ایپی 192.168.198.129 به ماشین مجازی دیگر با ایپی 192.168.198.128 حمله میکنیم و برای این منظور اسکریپت ضمیمه شده را اجرا کردیم.

قبل از اجرای اسکریپت سیستم مورد حمله در حالت معمولی بوده و ریسورس ها هم به طور معمولی مورد استفاده قرار گرفته بودند و همه چیز مساعد بود.

```

top - 08:21:47 up 1:20, 1 user, load average: 0.21, 0.14, 0.29
Tasks: 264 total, 1 running, 197 sleeping, 0 stopped, 0 zombie
%cpu(s): 0.7 us, 1.4 sy, 0.0 ni, 97.6 id, 0.3 wa, 0.0 hi, 0.0 st, 0.0 sr
Mem: 2017292 total, 77948 free, 1237960 used, 781384 buff/cache
Mem Swap: 1459804 total, 1362524 free, 97280 used, 606696 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

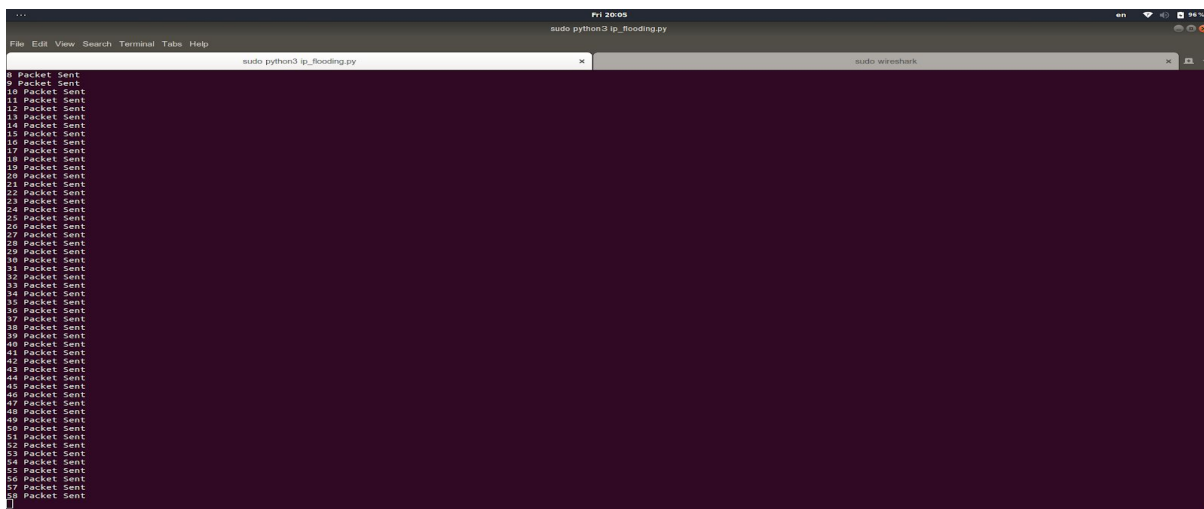
  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324   4120   3372  R  0.7   0.2   0:00.12 cp
 638 root       0  -20 234916  4368   4004  S  0.3   0.2   0:08.54 vntoolsd
   1 root      20   0 160668   7284   5036  S  0.0   0.4   0:09.84 systemd
   2 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kthreadd
   3 root      20   0      0      0      0  S  0.0   0.0   0:01.09 kworker/0:0
   4 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 kworker/0:0+
   6 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 mm_percpu+
   7 root      20   0      0      0      0  S  0.0   0.0   0:05.02 ksoftirqd/0
   8 root      20   0      0      0      0  S  0.0   0.0   0:02.46 rcu_sched
   9 root      20   0      0      0      0  S  0.0   0.0   0:00.00 rcu_bh
  10 root      rt    0      0      0      0  S  0.0   0.0   0:00.00 migration/0
  11 root      rt    0      0      0      0  S  0.0   0.0   0:00.02 watchdog/0
  12 root      20   0      0      0      0  S  0.0   0.0   0:00.00 cpuhp/0
  13 root      20   0      0      0      0  S  0.0   0.0   0:00.00 kdevtmpfs
  14 root      0  -20      0      0      0  S  0.0   0.0   0:00.00 netns

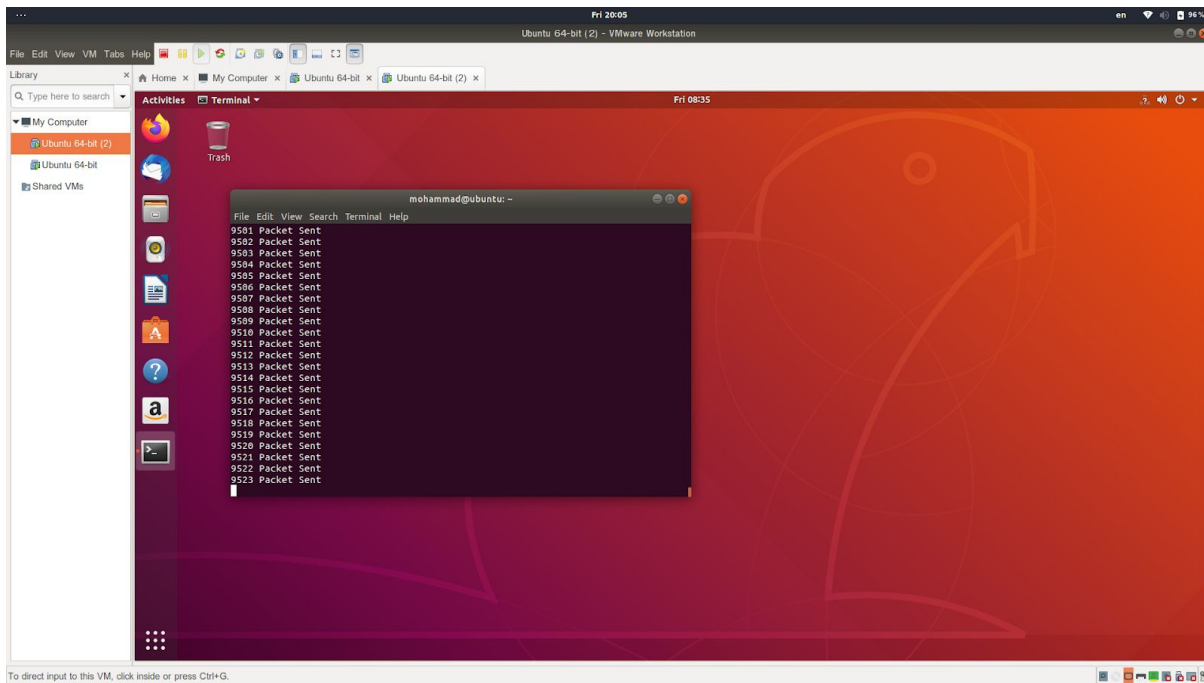
  PID USER      PR  NI    VIRT    RES    SHR   S %CPU  %MEM    TIME+  COMMAND
 1000 gdn        20   0 258432   5716   4616  S  1.0   0.3   0:06.97 kwayland
 1535 mohammad 20   0 489592  14136  7576  S  0.7   0.7   0:09.42 vntoolsd
117545 mohammad 20   0 51324
```

اجرای کد بر روی ماشین اول :



```
File Edit View Search Terminal Tabs Help
sudo python3 ip_flooding.py
9 Packet Sent
10 Packet Sent
11 Packet Sent
12 Packet Sent
13 Packet Sent
14 Packet Sent
15 Packet Sent
16 Packet Sent
17 Packet Sent
18 Packet Sent
19 Packet Sent
20 Packet Sent
21 Packet Sent
22 Packet Sent
23 Packet Sent
24 Packet Sent
25 Packet Sent
26 Packet Sent
27 Packet Sent
28 Packet Sent
29 Packet Sent
30 Packet Sent
31 Packet Sent
32 Packet Sent
33 Packet Sent
34 Packet Sent
35 Packet Sent
36 Packet Sent
37 Packet Sent
38 Packet Sent
39 Packet Sent
40 Packet Sent
41 Packet Sent
42 Packet Sent
43 Packet Sent
44 Packet Sent
45 Packet Sent
46 Packet Sent
47 Packet Sent
48 Packet Sent
49 Packet Sent
50 Packet Sent
51 Packet Sent
52 Packet Sent
53 Packet Sent
54 Packet Sent
55 Packet Sent
56 Packet Sent
57 Packet Sent
58 Packet Sent
]
```

اجرای کد بر روی ماشین دوم:



پکت های دریافتی در ماشین مورد حمله :

Wireshark interface showing a packet capture from vmnet8. The top pane displays a list of 6052 packets, with the bottom pane showing the details of the selected packet (No. 6052).

No.	Time	Source	Destination	Protocol	Length	Info
6033	0.65396428	192.168.1.152	192.168.1.128	TCP	60	17155 → 80 [SYN] Seq=0 Win=6192 Len=0
6034	0.672083854	71.195.158.25	192.168.1.128	TCP	60	10724 → 80 [SYN] Seq=0 Win=6192 Len=0
6035	0.68409391	228.30.144.125	192.168.1.128	TCP	60	29663 → 80 [SYN] Seq=0 Win=6192 Len=0
6036	0.69166150	214.155.101.232	192.168.1.128	TCP	60	62833 → 80 [SYN] Seq=0 Win=6192 Len=0
6037	0.701671069	192.168.1.128	192.168.1.128	TCP	60	58200 → 80 [SYN] Seq=0 Win=6192 Len=0
6038	0.71124371	56.27.46.180	192.168.1.128	TCP	60	65524 → 80 [SYN] Seq=0 Win=6192 Len=0
6039	0.719669568	210.231.111.252	192.168.1.128	TCP	60	17469 → 80 [SYN] Seq=0 Win=6192 Len=0
6040	0.72489482	50.178.177.14	192.168.1.128	TCP	60	63226 → 80 [SYN] Seq=0 Win=6192 Len=0
6041	0.73249441	244.189.22.196	192.168.1.128	TCP	60	29613 → 80 [SYN] Seq=0 Win=6192 Len=0
6042	0.74057294	1.141.240.220	192.168.1.128	TCP	60	15047 → 80 [SYN] Seq=0 Win=6192 Len=0
6043	0.757925192	60.71.62.285	192.168.1.128	TCP	60	41841 → 80 [SYN] Seq=0 Win=6192 Len=0
6044	0.761430923	42.150.107.117	192.168.1.128	TCP	60	51676 → 80 [SYN] Seq=0 Win=6192 Len=0
6045	0.776329730	196.147.31.15	192.168.1.128	TCP	60	9430 → 80 [SYN] Seq=0 Win=6192 Len=0
6046	0.784668659	32.251.135.211	192.168.1.128	TCP	60	14377 → 80 [SYN] Seq=0 Win=6192 Len=0
6047	0.785767672	168.67.26.67	192.168.1.128	TCP	54	32134 → 80 [SYN] Seq=0 Win=6192 Len=0
6048	0.794208091	222.17.251.192	192.168.1.128	TCP	60	7934 → 80 [SYN] Seq=0 Win=6192 Len=0
6049	0.801933636	10.230.173.73	192.168.1.128	TCP	60	21530 → 80 [SYN] Seq=0 Win=6192 Len=0
6050	0.812664859	200.203.241.206	192.168.1.128	TCP	60	11882 → 80 [SYN] Seq=0 Win=6192 Len=0
6051	0.824863499	197.250.25.159	192.168.1.128	TCP	60	13993 → 80 [SYN] Seq=0 Win=6192 Len=0
6052	0.834863305	60.251.180.60	192.168.1.128	TCP	60	8913 → 80 [SYN] Seq=0 Win=6192 Len=0

Frame 1: 60 bytes on wire (480 bits): 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: VMware_82:0c:29:3e:19:c4, Dst: VMware_82:0c:29:3e:19:c4
 Internet Protocol Version 4, Src: 190.168.91.192, Dst: 192.168.1.128
 Transmission Control Protocol, Src Port: 82467, Dst Port: 80, Seq: 8, Len: 0

پس از انجام حمله مشاهده کردم که ماشین مورد حمله بسیار کند شده و حتی top هم به کندی اجرا میشد و ریسورس ها به طور زیادی مصرف شدند و سیستم بسیار کند شد و علاوه بر آن شبکه سیستم مورد تضعیف شده و اگر سیستم هایی بیشتری هم حمله کنند کل ترافیک شبکه سیستم مورد حمله گرفته شده و توانایی ایجاد ارتباط با بقیه سیستم ها را ندارد.

Terminal window showing system status and the output of the 'top' command.

```

top - 08:36:14 up 1:34, 1 user, load average: 0.08, 0.08, 0.14
Tasks: 264 total, 1 running, 197 sleeping, 0 stopped, 0 zombie
%Cpu(s): 7.1 us, 8.1 sy, 0.0 ni, 82.4 id, 1.7 wa, 0.0 hi, 0.7 si, 0.0 st
KiB Mem : 201792 total, 99660 free, 1260028 used, 635596 buff/cache
KiB Swap: 1459804 total, 1362524 free, 97280 used, 578690 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 1332 mohammad 20   0 2962156 139576 37760 S   8.6   6.9   0:39.76 gnome-shell
 1674 mohammad 20   0 803336 25124 14392 S   2.7   1.2   0:03.40 gnome-terminal-
 1188 mohammad 20   0 459392 63432 21160 S   2.3   3.1   0:08.47 xorg
 1006 gdm        20   0 258432 5716 4616 S   1.0   0.3   0:14.92 Xwayland
    20 root       20   0 0 0 0 S   0.7   0.0   0:00.20 kcompactd0
    8 root       20   0 0 0 0 S   0.3   0.0   0:02.79 rcu_sched
 1535 mohammad 20   0 489592 14136 7576 S   0.3   0.7   0:10.67 vmttoolsd
 117545 mohammad 20   0 51324 4120 3372 R   0.3   0.2   0:06.81 top
    1 root       20   0 160068 7284 5836 S   0.0   0.4   0:09.92 systemd
    2 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kthreadd
    3 root       20   0 0 0 0 S   0.0   0.0   0:01.69 kworker/0:0
    4 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 kworker/0:0H
    6 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 mm_percpu_wq
    7 root       20   0 0 0 0 S   0.0   0.0   0:05.71 ksoftirqd/0
    9 root       20   0 0 0 0 S   0.0   0.0   0:00.00 rcu_bh
   10 root       20   0 0 0 0 S   0.0   0.0   0:00.00 migration/0
   11 root       20   0 0 0 0 S   0.0   0.0   0:00.02 watchdog/0
   12 root       20   0 0 0 0 S   0.0   0.0   0:00.00 cpuhp/0
   13 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kdevtmpfs
   14 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 netns
   15 root       20   0 0 0 0 S   0.0   0.0   0:00.00 rcu_tasks_kthre
   16 root       20   0 0 0 0 S   0.0   0.0   0:00.00 kauditd
   17 root       20   0 0 0 0 S   0.0   0.0   0:00.01 khungtaskd
   18 root       20   0 0 0 0 S   0.0   0.0   0:00.00 oom_reaper
   19 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 writeback
   21 root       25   5 0 0 0 S   0.0   0.0   0:00.00 ksm
   22 root       39 19 0 0 0 S   0.0   0.0   0:00.00 khugepaged
   23 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 crypto
   24 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 kintegrityd
   25 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 tblockd
   26 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 ata_sff
   27 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 md
   28 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 edac-poller
   29 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 devfreq_wq
   30 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 watchdogd
   34 root       20   0 0 0 0 S   0.0   0.0   0:04.00 kswapd0
   35 root       20   0 0 0 0 S   0.0   0.0   0:00.00 ecryptfs-kthrea
   77 root       0 -20 0 0 0 S   0.0   0.0   0:00.00 kthrotld

```