Principle 1: Before performing any kind of operation, one should always obtain consent and acceptance from the receiving end of the operation. This would result in less legal complications (Johansen, 2017).

Principle 2: Always protect the defenseless. An ethical hacker's intention and actions should always reflect the best towards business costumers and should ensure for a more secure world (Ideas, 2018).

Principle 3: Communication and transparency is very important when dealing with clients. One should make sure to disclose ALL information and findings during and after the ethical hacking (Johansen, 2017).

Principle 4: Stay within the boundaries set by your client. Having access or gaining access to more than the target area set by client does not permit one to exploit. This is to avoid access of sensitive information that one is not allowed to see (Johansen, 2017).

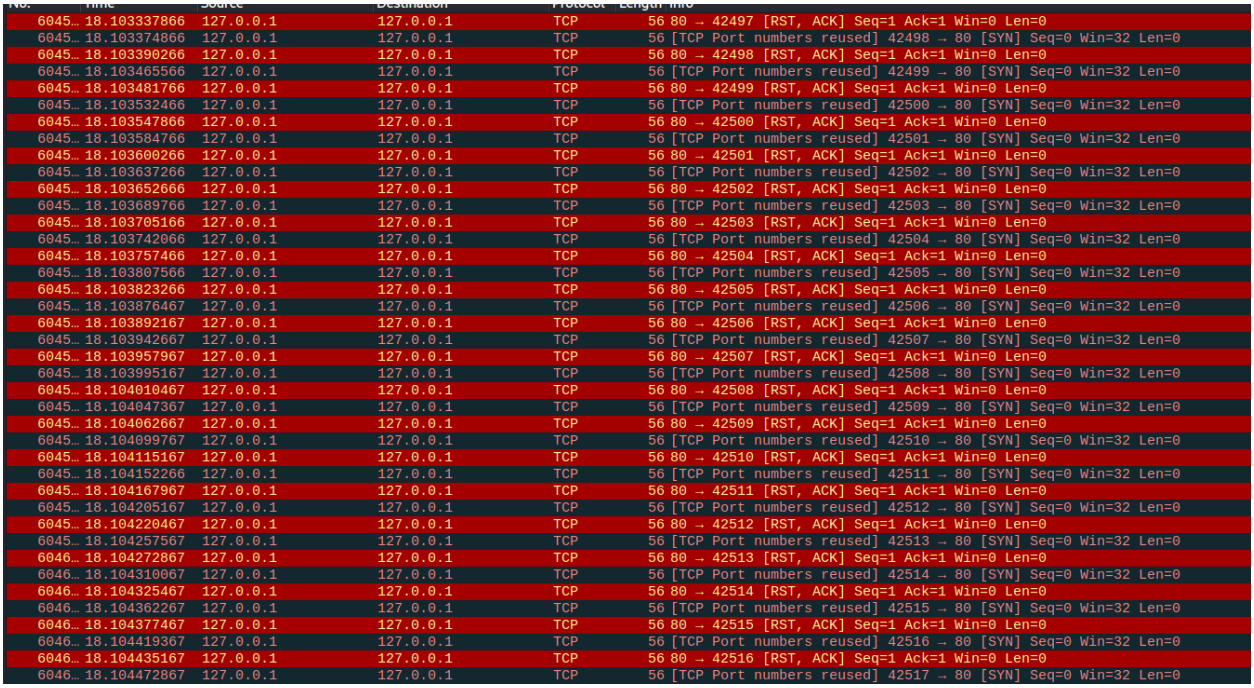
Principle 5: One should always keep records of their operations. Whether those operations were successful or not, specific dates, data and logs should be recorded and stored safely (Jaskolj, 2009).

Principle 6: One should never disclose any client information or findings to anyone but the client. Any disclosure of the client's information disregards the purpose of the ethical hacker which is to help ensure a client's environment safer and secure (Johansen, 2017).

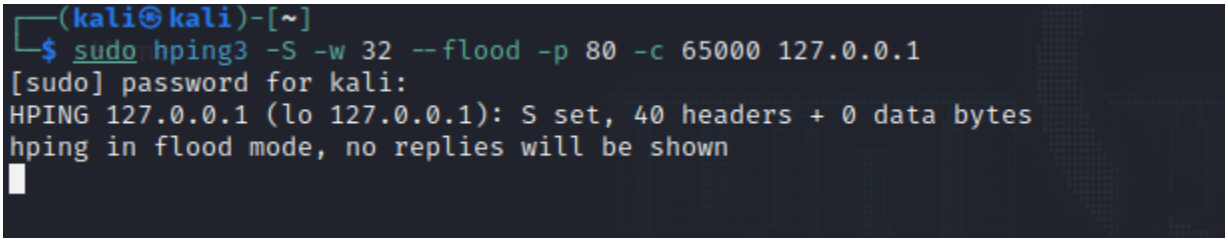
Principle 7: One should never harm a client in any sort or manner (Jaskolj, 2009). The client's environment and business should not be affected by the operation of the ethical hacker and should never result in any loss in any matter or form.

Part 1:

Wireshark:

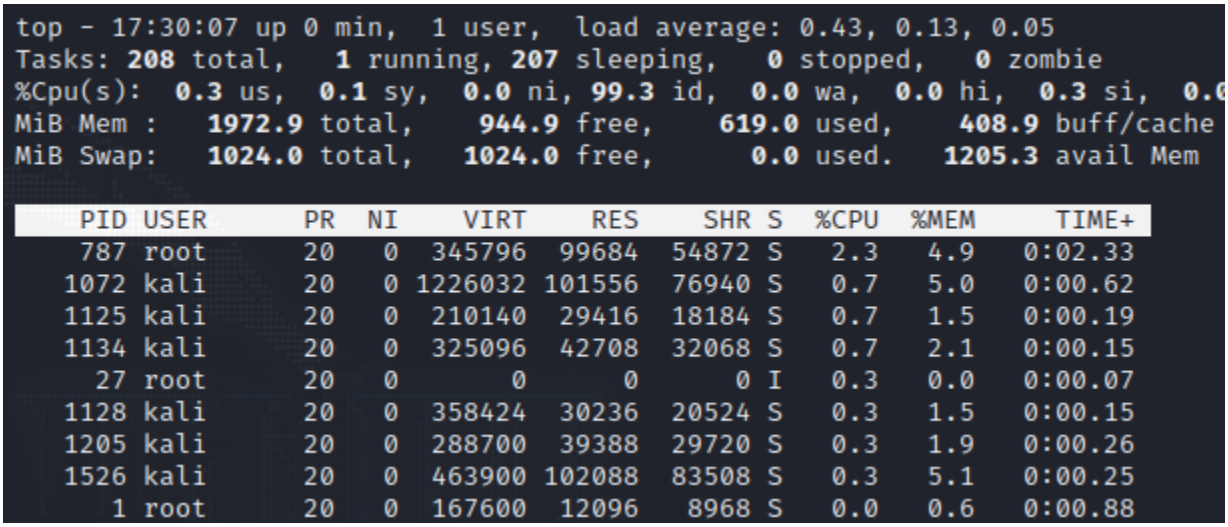


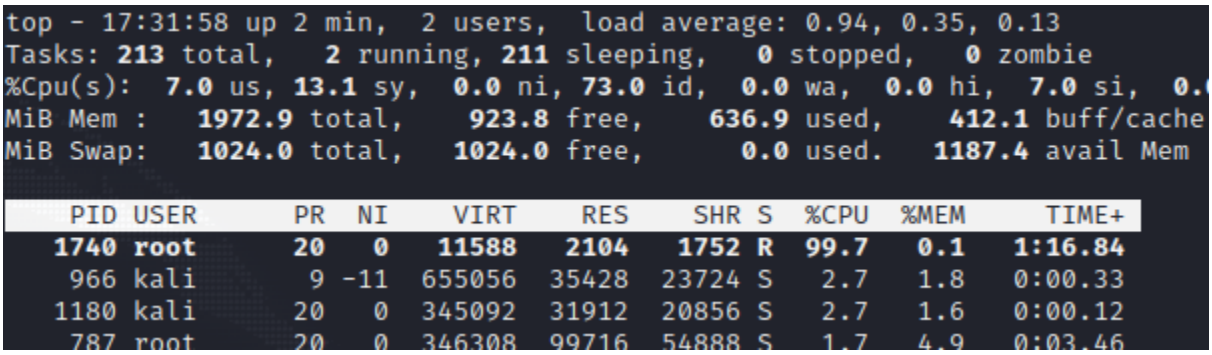
No.	Time	Source	Destination	Protocol	Length	Info
6045…	18.103337866	127.0.0.1	127.0.0.1	TCP	56	80 → 42497 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103374866	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42498 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103390266	127.0.0.1	127.0.0.1	TCP	56	80 → 42498 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103465566	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42499 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103481766	127.0.0.1	127.0.0.1	TCP	56	80 → 42499 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103532466	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42500 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103547866	127.0.0.1	127.0.0.1	TCP	56	80 → 42500 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103584766	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42501 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103600266	127.0.0.1	127.0.0.1	TCP	56	80 → 42501 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103637266	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42502 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103652666	127.0.0.1	127.0.0.1	TCP	56	80 → 42502 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103689766	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42503 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103705166	127.0.0.1	127.0.0.1	TCP	56	80 → 42503 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103742066	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42504 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103757466	127.0.0.1	127.0.0.1	TCP	56	80 → 42504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103807566	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42505 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103823266	127.0.0.1	127.0.0.1	TCP	56	80 → 42505 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103876467	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42506 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103892167	127.0.0.1	127.0.0.1	TCP	56	80 → 42506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103942667	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42507 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.103957967	127.0.0.1	127.0.0.1	TCP	56	80 → 42507 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.103995167	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42508 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.104010467	127.0.0.1	127.0.0.1	TCP	56	80 → 42508 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.104047367	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42509 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.104062667	127.0.0.1	127.0.0.1	TCP	56	80 → 42509 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.104099767	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42510 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.104115167	127.0.0.1	127.0.0.1	TCP	56	80 → 42510 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.104152266	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42511 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.104167967	127.0.0.1	127.0.0.1	TCP	56	80 → 42511 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.104205167	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42512 → 80 [SYN] Seq=0 Win=32 Len=0
6045…	18.104220467	127.0.0.1	127.0.0.1	TCP	56	80 → 42512 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6045…	18.104257567	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42513 → 80 [SYN] Seq=0 Win=32 Len=0
6046…	18.104272867	127.0.0.1	127.0.0.1	TCP	56	80 → 42513 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6046…	18.104310067	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42514 → 80 [SYN] Seq=0 Win=32 Len=0
6046…	18.104325467	127.0.0.1	127.0.0.1	TCP	56	80 → 42514 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6046…	18.104362267	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42515 → 80 [SYN] Seq=0 Win=32 Len=0
6046…	18.104377467	127.0.0.1	127.0.0.1	TCP	56	80 → 42515 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6046…	18.104419367	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42516 → 80 [SYN] Seq=0 Win=32 Len=0
6046…	18.104435167	127.0.0.1	127.0.0.1	TCP	56	80 → 42516 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6046…	18.104472867	127.0.0.1	127.0.0.1	TCP	56	[TCP Port numbers reused] 42517 → 80 [SYN] Seq=0 Win=32 Len=0



```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S -w 32 --flood -p 80 -c 65000 127.0.0.1
[sudo] password for kali:
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
```

Top command before attack





a. Source IP: 127.0.0.1 Destination: 127.0.0.1. size: 56 bytes. Protocol: IPv4. Header checksum: 0xda26 [validation disabled]
b. Source port: 1893 destination port: 80, flags: 0x002 (SYN), window size: 32
c. The cpu and memory utilization jumped very high due to processing the packets

Part 2:

Top command before and during attack

```
top - 17:36:21 up 6 min,  1 user,  load average: 0.23, 0.27, 0.16
Tasks: 200 total,   1 running, 198 sleeping,   1 stopped,   0 zombie
%Cpu(s):  0.1 us,  0.2 sy,  0.0 ni, 99.7 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0
MiB Mem :   1972.9 total,    607.0 free,    818.7 used,    547.1 buff/cache
MiB Swap:   1024.0 total,   1024.0 free,      0.0 used.   1001.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
    787 root      20   0  376892 130396  58480 S   2.7   6.5   0:12.13
   1526 kali      20   0  463900 102380  83768 S   1.0   5.1   0:01.88
   1072 kali      20   0 1242504 120200  76940 S   0.7   5.9   0:02.70
     27 root      20   0       0      0      0 I   0.3   0.0   0:00.40
   1121 kali      20   0  400860  49704  36372 S   0.3   2.5   0:00.53
   1125 kali      20   0  210140  29416  18184 S   0.3   1.5   0:02.35
   1129 kali      20   0  665908  45388  34200 S   0.3   2.2   0:00.45
   2301 kali      20   0  464264 102616  83900 S   0.3   5.1   0:00.60
```

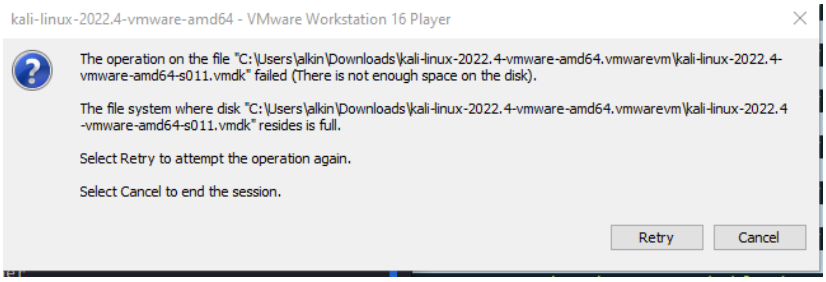
```
top - 17:37:06 up 7 min,  2 users,  load average: 1.15, 0.46, 0.23
Tasks: 203 total,   5 running, 197 sleeping,   1 stopped,   0 zombie
%Cpu(s): 27.9 us, 31.7 sy,  0.0 ni, 24.7 id,  1.6 wa,  0.0 hi, 14.1 si,  0.0
MiB Mem :   1972.9 total,     71.2 free,   1188.5 used,    713.2 buff/cache
MiB Swap:   1024.0 total,    884.2 free,    139.8 used.    619.1 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+
   3432 root      20   0   11588    560    204 R  96.0   0.0   0:14.48
   3107 kali      20   0 1841876 618132  21140 R  89.4  30.6   0:14.63
   3230 kali      20   0   19004   5692   4896 R  59.8   0.3   0:08.94
     35 root      20   0       0      0      0 R  14.0   0.0   0:02.14
    201 root      20   0       0      0      0 I  13.0   0.0   0:00.71
```

```
4955… 41.262100105  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262106393  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262108423  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262114560  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262116678  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262122699  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262124728  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262130801  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262132963  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262139001  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262141025  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262147338  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262149341  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262155361  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262157355  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262163346  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262165366  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262171386  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4955… 41.262173336  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4955… 41.262179321  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4956… 41.262181248  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4956… 41.262188314  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4956… 41.262190320  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4956… 41.262196693  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
4956… 41.262198731  127.0.0.1  127.0.0.1  ICMP   592 Destination unreachable (Port unreachable)
4956… 41.262219154  127.0.0.1  127.0.0.1  TFTP  4044 Unknown (0x5858)
```

```
$ sudo hping3 --udp --flood -p 69 -c 20000 -d 4000 127.0.0.1
[sudo] password for kali:
HPING 127.0.0.1 (lo 127.0.0.1): udp mode set, 28 headers + 4000 data bytes
hping in flood mode, no replies will be shown
```

Vmware crashing



a. Source IP: 127.0.0.1 Destination: 127.0.0.1. Length: 592 bytes. Protocol: ICMP. Header Checksum: 0x87a7 [validation disabled]
b. Source port: 20134. Destination port: 69. Checksum: 0x617e [unverified].
c. The cpu and memory utilization jumped very high due to processing the packets. Compared to the tcp attack we did, this one had much more effect. My Virtual machine crashed a few times while doing this part

References:

Ideas, S. (2018, June 18). *Ethics of ethical hacking*. Security Boulevard. Retrieved February 12, 2023, from https://securityboulevard.com/2018/06/ethics-of-ethical-hacking/

Jaskolj. (2009). *Ethical hacking*. Computing and Software Wiki RSS. Retrieved February 12, 2023, from http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking

Johansen, R. (2017, March 24). *Ethical hacking code of ethics: Security, risk & issues*. Panmore Institute. Retrieved February 12, 2023, from https://panmore.com/ethical-hacking-code-of-ethics-security-risk-issues