

עבודת גמר – sniffing and spoofing

מגשים: אריאל יפעי ומוטי דהרי.

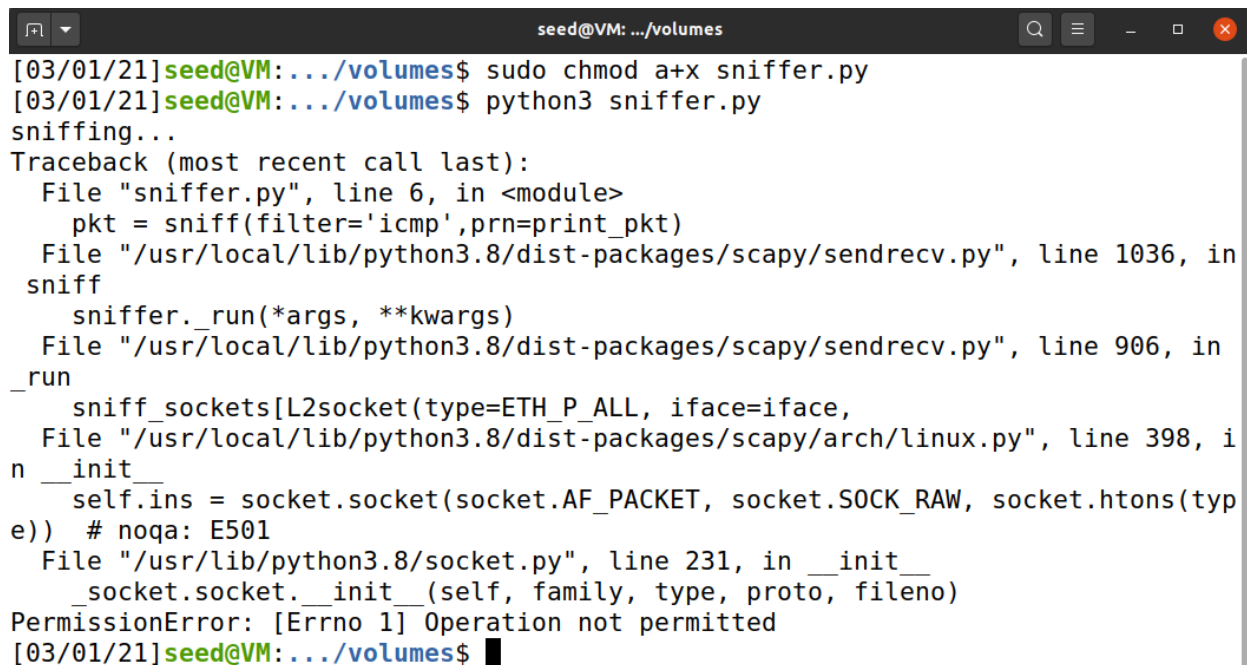
התקנו את SEEDvm בvirtualbox עדכנו את כל התוספים שהיה צריך ולאחר מכן בנינו סניפר בפיתון.

A1.1: התבקשנו להריץ את הסניפר בלי הרשאות אדמין ועם הרשאות אדמין ולראות מה קורה, הרצנו בטרמינל אחד את הסניפר שלנו ובשני את הפקודת ping לאתר של גוגל.

הסניפר:

```
1#!/usr/bin/python3
2from scapy.all import *
3print("sniffing...")
4def print_pkt(pkt):
5    pkt.show()
6pkt = sniff(filter='icmp',prn=print_pkt)
7|
```

הרצה בלי הרשאות אדמין, לא נותן לנו להריץ כי אין לנו הרשאה - Operation not permitted:



```
seed@VM: .../volumes
[03/01/21]seed@VM:.../volumes$ sudo chmod a+x sniffer.py
[03/01/21]seed@VM:.../volumes$ python3 sniffer.py
sniffing...
Traceback (most recent call last):
  File "sniffer.py", line 6, in <module>
    pkt = sniff(filter='icmp',prn=print_pkt)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 1036, in sniff
    sniffer._run(*args, **kwargs)
  File "/usr/local/lib/python3.8/dist-packages/scapy/sendrecv.py", line 906, in _run
    sniff_sockets[L2socket(type=ETH_P_ALL, iface=iface,
  File "/usr/local/lib/python3.8/dist-packages/scapy/arch/linux.py", line 398, in __init__
    self.ins = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.htons(type)) # noqa: E501
  File "/usr/lib/python3.8/socket.py", line 231, in __init__
    _socket.socket.__init__(self, family, type, proto, fileno)
PermissionError: [Errno 1] Operation not permitted
[03/01/21]seed@VM:.../volumes$
```

הרצה עם הרשאות נותן לנו להריץ כי יש לנו הרשאה :

```
seed@VM: .../volumes
[03/01/21]seed@VM:.../volumes$ sudo python3 sniffer.py
sniffing...
###[ Ethernet ]###
  dst      = 52:54:00:12:35:02
  src      = 08:00:27:82:84:fc
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 5170
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xc4aa
  src      = 10.0.2.15
  dst      = 172.217.168.228
  \options \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x9ab9
```

הצלחנו לתפוס פקאטות!

B1.1: התבקשנו להוסיף עוד פילטרים לסניפר שלנו.

```
1#!/usr/bin/python
2from scapy.all import *
3print("sniffing...")
4def print_pkt(pkt):
5    pkt.show()
6
7pkt = sniff(filter='icmp',prn=print_pkt)
8pkt = sniff(filter='tcp and src host 10.0.2.15 and dst port 23', prn=print_pkt)
9pkt = sniff(filter="dst net 128.230.0.0/16",prn=print_pkt)
10
```

תפיסת פקטת TCP:

```

seed@VM: ~/volumes
[03/01/21]seed@VM:~/volumes$ sudo chmod a+x 1.1B.py
[03/01/21]seed@VM:~/volumes$ sudo python3 1.1B.py
sniffing...
###[ Ethernet ]###
dst      = 52:54:00:12:35:02
src      = 08:00:27:82:84:fc
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x10
len      = 60
id       = 24880
flags    = DF
frag     = 0
ttl      = 64
proto    = tcp
chksum   = 0x84e4
src      = 10.0.2.15
dst      = 142.250.185.142
\options \
###[ TCP ]###
sport    = 50994
dport    = telnet
seq      = 2742102954
ack      = 0
dataofs  = 10
reserved = 0
flags    = S
window   = 64240
chksum   = 0x54c6
urgptr   = 0
options  = [('MSS', 1460), ('SAckOK', b''), ('Timestamp', (1642524737,

```

```

seed@VM: ~
[03/01/21]seed@VM:~$ telnet 142.250.185.142
Trying 142.250.185.142...
^C
[03/01/21]seed@VM:~$

```

תפיסת פקטה מ subnet:

```

seed@VM: ~/volumes
[03/01/21]seed@VM:~/volumes$ sudo chmod a+x 1.1B.py
[03/01/21]seed@VM:~/volumes$ sudo python3 1.1B.py
sniffing...
###[ Ethernet ]###
dst      = 52:54:00:12:35:02
src      = 08:00:27:82:84:fc
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 58693
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0xc869
src      = 10.0.2.15
dst      = 128.230.0.5
\options \
###[ ICMP ]###
type     = echo-request
code     = 0
chksum   = 0x9b7b
id       = 0x6
seq      = 0x1
###[ Raw ]###
load     = '\x1a=\x00\x00\x00\x00\xfd\x06\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f !"#%&\`()*+,-./01234567'
###[ Ethernet ]###

```

```

seed@VM: ~
[03/01/21]seed@VM:~$ ping 128.230.0.5
PING 128.230.0.5 (128.230.0.5) 56(84) bytes of data.
^C
--- 128.230.0.5 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1010ms

```

1.2:

אנחנו צריכים לעשות spoofing לפקטת icmp לכן אנו נשלח באמצעות scapy פקטת ping מקו שהוא לא של האינטרפייס שאנחנו משתמשים לאינטרפייס אחר ברשת שלנו ואנו נבדוק בwireshark שאכן האינטרפייס השני לא רואה שהפקטה נשלחה מהאינטרפייס השני.

הקוד:

```
seed@VM: .../volumes
from scapy.all import *

a = IP()
a.dst = '10.0.2.15' #another machine in our network. we will run wireshark on this machine
to capture the spoofed packet.
a.src = '105.105.105.105' #fake ip
b = ICMP()
p = a/b
send(p)
```

התהליך:

The screenshot displays two windows. The top window is Wireshark, showing a packet capture on the 'icmp' interface. It contains two packets: a request and a reply, both from 105.105.105.105 to 10.0.2.15. The bottom window is a terminal showing the execution of the script 1.2.py with sudo, resulting in 'Sent 1 packets.'

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------|-----------------|-----------------|----------|--------|--|
| 1 | 2021-03-01 13:0... | 105.105.105.105 | 10.0.2.15 | ICMP | 44 | Echo (ping) request id=0x0000, seq=0/0, ttl=64 |
| 2 | 2021-03-01 13:0... | 10.0.2.15 | 105.105.105.105 | ICMP | 44 | Echo (ping) reply id=0x0000, seq=0/0, ttl=64 |

```
[03/01/21]seed@VM: .../volumes$ sudo chmod a+x 1.2.py
[03/01/21]seed@VM: .../volumes$ sudo python3 1.2.py
Sent 1 packets.
[03/01/21]seed@VM: .../volumes$
```

ואכן זה נשלח מהקו של המזוייף ונשלח response למזוייף.

:1.3

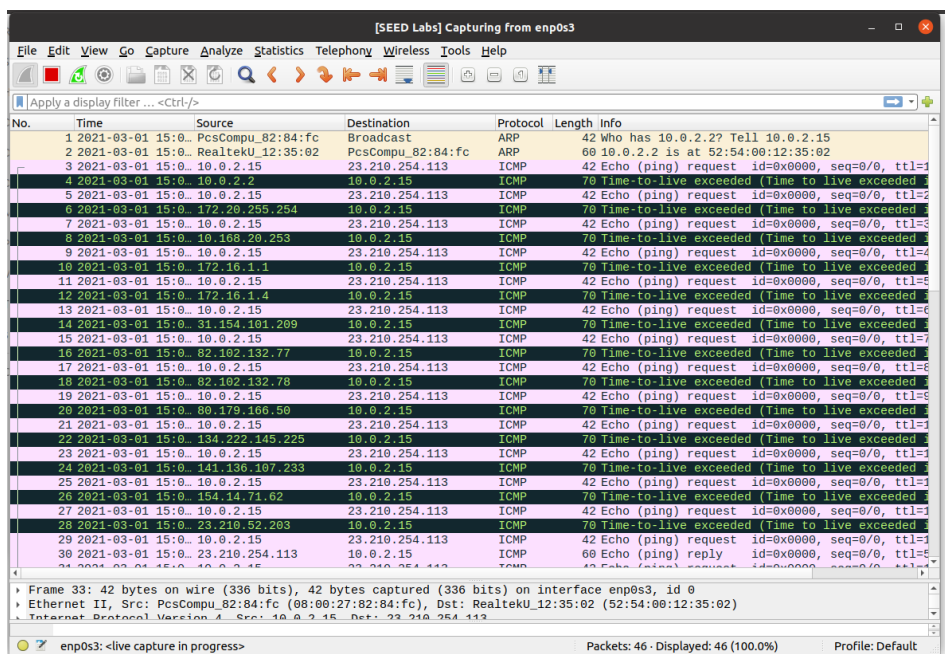
התבקשנו לבדוק כמה ראטרים אנו עוברים עד שאנו מגיעים ליעד, ע"פ ההדרכה עלינו להגביל את זמן החיים של הפקטה ולראות בכל פעם שיש לה error מסוג time-to-live has exceeded (הזמן שלה נגמר אך ללא השלמת המשימה) נבדוק באיזה ip של ראטר היא עצרה, נרוץ בלולאה וכל פעם נעלה את את הttl באחד ונספור כמה ip שונים אנו עוברים עד שאנחנו כבר לא מקבלים שגיאה.

```
from scapy.all import *
import time

for i in range(1,300):
    a= IP()
    a.dst = '23.210.254.113'# ip of ynet.co.il
    print("ttl = ",i)
    a.ttl = i
    b = ICMP()
    send(a/b)
    time.sleep(1)

~
~
~
~
```

קיבלנו 13 הודעות שגיאה מ13 ראטרים שונים כלומר עברנו 13 ראטרים עד היעד.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------------------------|-------------------|-------------------|----------|--------|--|
| 1 | 2021-03-01 15:00:00.000000 | PcsCompu_82:84:fc | Broadcast | ARP | 42 | Who has 10.0.2.2? Tell 10.0.2.15 |
| 2 | 2021-03-01 15:00:00.000000 | RealtekU_12:35:02 | PcsCompu_82:84:fc | ARP | 60 | 10.0.2.2 is at 52:54:00:12:35:02 |
| 3 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=1 |
| 4 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 5 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=2 |
| 6 | 2021-03-01 15:00:00.000000 | 172.20.255.254 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 7 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=3 |
| 8 | 2021-03-01 15:00:00.000000 | 10.168.20.253 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 9 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=4 |
| 10 | 2021-03-01 15:00:00.000000 | 172.16.1.1 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 11 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=5 |
| 12 | 2021-03-01 15:00:00.000000 | 172.16.1.4 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 13 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=6 |
| 14 | 2021-03-01 15:00:00.000000 | 31.151.101.209 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 15 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=7 |
| 16 | 2021-03-01 15:00:00.000000 | 82.102.132.77 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 17 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=8 |
| 18 | 2021-03-01 15:00:00.000000 | 82.102.132.78 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 19 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=9 |
| 20 | 2021-03-01 15:00:00.000000 | 80.179.166.50 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 21 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=10 |
| 22 | 2021-03-01 15:00:00.000000 | 134.222.145.225 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 23 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=11 |
| 24 | 2021-03-01 15:00:00.000000 | 141.159.107.233 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 25 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=12 |
| 26 | 2021-03-01 15:00:00.000000 | 154.14.71.62 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 27 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=13 |
| 28 | 2021-03-01 15:00:00.000000 | 23.210.52.203 | 10.0.2.15 | ICMP | 70 | Time-to-live exceeded (Time to live exceeded) |
| 29 | 2021-03-01 15:00:00.000000 | 10.0.2.15 | 23.210.254.113 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=14 |
| 30 | 2021-03-01 15:00:00.000000 | 23.210.254.113 | 10.0.2.15 | ICMP | 60 | Echo (ping) reply id=0x0000, seq=0/0, ttl=14 |

:1.4

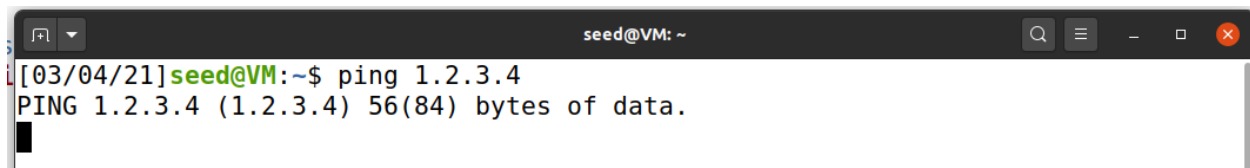
התבקשנו למצוא IP שלא קיים ולאחר מכן לכתוב קוד אשר מקבל בקשה מIP ושולח חזרה reply למי ששלח גם אם היעד לא קיים. כלומר מכונה אחת שולחת בקשת פינג לIP שלא קיים המכונה השנייה עושה sniffing לפקטה שנשלחה ואז עושה spoofing של הודעת reply למכונה הראשונה וככה כביכול אני מצליח לעשות במכונה הראשונה הודעת פינג ולקבל תשובה.

הקוד:

```
1 from scapy.all import *
2
3
4 def spoof(pkt):
5     if ICMP in pkt and pkt[ICMP].type == 8:
6         print("Got Packet!")
7         print("Source: ", pkt[IP].src)
8         print("Destination:", pkt[IP].dst)
9         a = IP()
10        a.src = pkt[IP].dst
11        a.dst=pkt[IP].src
12        a.ihl=pkt[IP].ihl
13        b = ICMP()
14        b.type=0
15        b.seq=pkt[ICMP].seq
16        b.id=pkt[ICMP].id
17        if pkt.haslayer(Raw):
18            data = pkt[Raw].load
19            packet = a/b/data
20        else:
21            packet = a/b
22        print("Spoof reply")
23        send(packet, verbose=0)
24
25 print("Sniffing...")
26 pkt = sniff(iface=['lo', 'enp0s3', 'docker0', 'br-6fdd0758cf02'], filter='icmp or arp', prn=spoof)
```

מנתרים פקטה ושולחים חזרה reply בלי קשר אם השרת הזה קיים או לא.

IP שלא קיים:



The screenshot shows a terminal window titled 'seed@VM: ~'. The user has entered the command 'ping 1.2.3.4'. The output shows the first ping attempt: 'PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.' followed by a black square, indicating the ping failed.

נפעיל את הקוד שלנו בטרמינל שונה וננסה שוב לשלוח PING מאותו IP:

```
seed@VM: ~$ sudo chmod a+x 1.4.py
[03/04/21] seed@VM: ~/volumes$ sudo python3 1.4.py
Sniffing....
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 1.2.3.4
Spoof reply
Got Packet!
```

```
[03/04/21] seed@VM: ~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
^C
--- 1.2.3.4 ping statistics ---
103 packets transmitted, 0 received, 100% packet loss, time 105073ms
```

```
[03/04/21] seed@VM: ~$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=64 time=22.5 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=33.5 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=33.1 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=31.5 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=64 time=30.7 ms
^C
--- 1.2.3.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4038ms
rtt min/avg/max/mdev = 22.509/30.251/33.526/4.005 ms
[03/04/21] seed@VM: ~$
```

ואכן הצלחנו לקבל את reply כאשר שלחנו את הבקשת ping למרות שהשרת הזה בכלל לא קיים, בטרמינל אחד שלחנו את הבקשת ping ובשני ניתרנו את הפקטה ועשינו לה spoofing ששלח reply מזוייף לטרמינל הראשון.

ip קיים:

```
[03/04/21] seed@VM: ~/volumes$ sudo chmod +x 1.4.py
[03/04/21] seed@VM: ~/volumes$ sudo python3 1.4.py
Sniffing....
Got Packet!
Source: 10.0.2.15
Destination: 8.8.8.8
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 8.8.8.8
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 8.8.8.8
Spoof reply
Got Packet!
Source: 10.0.2.15
Destination: 8.8.8.8
Spoof reply
Got Packet!
```

```
[03/04/21] seed@VM: ~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=64 time=27.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=81.3 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=2 ttl=64 time=28.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=79.3 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=3 ttl=64 time=30.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=82.4 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=4 ttl=64 time=39.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=82.1 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=5 ttl=64 time=28.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=108 time=79.4 ms (DUP!)
64 bytes from 8.8.8.8: icmp_seq=6 ttl=64 time=34.0 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, +5 duplicates, 0% packet loss, time 5056ms
rtt min/avg/max/mdev = 26.982/53.827/82.356/24.934 ms
[03/04/21] seed@VM: ~$
```

אנו רואים שנשלח reply פעמיים על כל request.

:2.1A

התבקשנו לעשות סניפר לפקטות מסוג icmp ולרשום את הקו מקור וקו יעד:

```
seed@VM: ~/C
[03/07/21]seed@VM:~/C$ gcc 2.1A.c -lpcap -o sniff
[03/07/21]seed@VM:~/C$ gcc 2.1A.c -lpcap -o sniff
[03/07/21]seed@VM:~/C$ sudo ./sniff
packet:
  src: 10.0.2.15
  dest: 8.8.8.8
packet:
  src: 8.8.8.8
  dest: 10.0.2.15
packet:
  src: 10.0.2.15
  dest: 10.0.0.138
packet:
  src: 10.0.2.15
  dest: 10.0.0.138
packet:
  src: 10.0.2.15
  dest: 8.8.8.8
packet:
  src: 10.0.0.138
  dest: 10.0.2.15
packet:
  src: 10.0.0.138
  dest: 10.0.2.15

seed@VM: ~/C
[03/07/21]seed@VM:~/C$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=108 time=80.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=108 time=78.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=108 time=79.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=108 time=78.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 78.702/79.283/80.295/0.638 ms
[03/07/21]seed@VM:~/C$
```

שאלה 1:

רצף הקריאות בספריה pcap שנחוצות בכדי להסניף פקטות:

1. נקרא לפונקציה pcap_open_live שתאזין לאינטרפייס מסוים שנגדיר (המשתנה הראשון בפונקציה).
המשתנה השני - מקסימום בתים שיתפסו על ידי pcap.
המשתנה השלישי - הוא האם להפעיל במוד של promiscuous או לא (אם הוא מוגדר ל-0 זה אפשרי במקרים ספציפיים).
המשתנה הרביעי - הוא זמן לקריאה עד שהפקטה תמות.
המשתנה החמישי - ebuf הוא מצביע מסוג סטרינג שבמידה ויש שגיאה כלשהי אז ירשום לשם את השגיאה ונוכל לצורך העניין לפלוט את זה בקובץ שגיאות שניצור.
הפונקציה מחזירה *pcap_t אם הצליח או NULL אם נכשל ואם הוחזר NULL אז השגיאה תיכנס לתוך המשתנה errorMsg.

2. נקרא לפונקציה pcap_compile שמשמש לקימפול הסטרינג לפילטר התכנית.

המשתנה הראשון - מחזיק את הsession שלנו
המשתנה השני - מצביע למקום שנאחסן את הגרסה המסודרת של המסנן שלנו.
המשתנה השלישי - הביטוי עצמו, בפורמט מחרוזת רגיל.
המשתנה הרביעי - מספר שלם שמחליט אם הביטוי צריך להיות "optimized" (אופטימיזציה) או לא (0 false, 1 true).
המשתנה החמישי - מסכת הרשת של הרשת שהמסנן חל עליה
מחזירה 0 אם זה הקימפול של המחרוזת הצליח, ו-Pcap_Error אם זה נכשל אם חזר Pcap_Error ניתן לקרוא עם p כארגומנט לאחזור או הצגת טקסט השגיאה שהתקבל.

3. נקרא לפונקציה pcap_setfilter שמשמשת להגדרת המסנן (filter) של התכנית.

fp – הוא פויינטר למבנה bpf_program.
מחזירה 0 אם זה הצליח, ו-Pcap_Error אם זה נכשל אם חזר Pcap_Error ניתן לקרוא עם p כארגומנט לאחזור או הצגת טקסט השגיאה שהתקבל.

:2.1C

התבקשנו לנטר את הסיסמא שמשתמש מזין כאשר משתמש בtelnet:

```
seed@VM: ~/C
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
64
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
```

```
seed@VM: ~
[03/07/21]seed@VM:~/C$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

84 updates can be installed immediately.
84 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Mar  6 09:26:13 EST 2021 from VM on pts/2
[03/07/21]seed@VM:~$
```

```

Data:
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
e
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
e
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
65
e
*****Got Packet!*****
Source IP      : 10.0.2.15
Destination IP : 10.0.2.15
Data:
73
s
*****Got Packet!*****
Source IP      : 10.0.2.15

```

```

[03/07/21]seed@VM:~/C$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
VM login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

84 updates can be installed immediately.
84 of these updates are security updates.
To see these additional updates run: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sat Mar  6 09:26:13 EST 2021 from VM on pts/2
[03/07/21]seed@VM:~$

```

ואכן הצלחנו לנטר את הסיסמה שהיא dees.

:2.2A

התבקשנו לעשות spoofing להודעת reply ולתעד שהיא אכן עובדת (הקוד ארוך לכן הוא לא מצורף כאן אלה רק בתיקיה המצורפת).

```

[03/07/21]seed@VM:~/C$ gcc 2.2A.c -lpcap -o spoof
[03/07/21]seed@VM:~/C$ sudo ./spoof

Send one packet!
[03/07/21]seed@VM:~/C$

```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------|-----------------|-------------|----------|--------|--|
| 1 | 2021-03-07 05:0... | 195.105.195.105 | 10.0.2.15 | ICMP | 63 | Echo (ping) reply id=0x1200, seq=0/0, ttl=12 |

:2.2B

התבקשנו לעשות spoofing להודעת request אז שלחנו בקשה מקו חיצוני אל אחת המכונות שלנו והמכונה שלנו אכן ראתה שהוא שלח לה בקשה (למרות שאנחנו שלחנו ולא הוא) והמכונה שלנו הגיבה לאותו IP בחזרה.

הוכחה:

```

[03/07/21]seed@VM:~/C$ gcc 2.2B.c -lpcap -o spoof
[03/07/21]seed@VM:~/C$ sudo ./spoof

Send one packet!
[03/07/21]seed@VM:~/C$

```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------------|-----------------|-----------------|----------|--------|--|
| 1 | 2021-03-07 05:0... | 195.105.195.105 | 10.0.2.15 | ICMP | 63 | Echo (ping) request id=0x1200, seq=0/0, ttl=12 |
| 2 | 2021-03-07 05:0... | 10.0.2.15 | 195.105.195.105 | ICMP | 63 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 |

שאלה 4:

בעקרון אפשר לשנות את האורך של הפקאטה אך זה לא באמת ישפיע כי הפונקציה sendto תחזיר אותה לגודל המקורי.

שאלה 5:

לא צריך לחשב את ה checksum המערכת הפעלה קובעת את זה לבד, אפילו אין אפשרות לשנות את ה checksum שמשתמשים ב raw socket .

שאלה 6:

כאשר משתמשים ב raw socket אנו ניהיה חייבים לתת הרשאות אדמין מכון שיש המון אפשריות בתכנות מסוג זה (כמו לשלוח פקאטות מזויפות או לגשת לפורט מתחת ל 1024 וכו'..). שזה דברים שתוכניות רגילות לא צריכות הרשאה אליהם.

אם נריץ ללא הרשאת אדמין זה יפול לנו בשלב הקומפילציה מסיבה : Operation not permitted.

2.3:

התבקשנו לעשות sniffing לכל הודעת icmp request שיוצאת מאיתנו ולשלוח באמצעות spoofing הודעת reply, ככה שלא משנה אם עשינו פינג לקו שלא קיים אנחנו עדיין נראה שהוא כאילו קיים.

שלחנו ping ל ip שלא קיים מבלי להפעיל את הקוד שלנו וזאת התוצאה:

```
seed@VM: ~/C
[03/07/21]seed@VM:~/C$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
^C
--- 1.2.3.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss,
[03/07/21]seed@VM:~/C$
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------------|-----------|-------------|----------|--------|---|
| 1 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0004, seq=1/256, ttl= |
| 2 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0004, seq=2/512, ttl= |
| 3 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0004, seq=3/768, ttl= |
| 4 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0004, seq=4/1024, ttl= |
| 5 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0004, seq=5/1280, ttl= |

עכשיו נפעיל את הקוד שלנו:

```
seed@VM: ~/C
[03/07/21]seed@VM:~/C$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
^C
--- 1.2.3.4 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss,
[03/07/21]seed@VM:~/C$ ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=99 time=156 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=99 time=177 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=99 time=201 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=99 time=230 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=99 time=244 ms
^C
--- 1.2.3.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, t
rtt min/avg/max/mdev = 156.425/201.810/244.291/32.51
[03/07/21]seed@VM:~/C$
```

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------------|-----------|-------------|----------|--------|---|
| 1 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0005, seq=1/256, ttl= |
| 2 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0005, seq=2/512, ttl= |
| 3 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0005, seq=3/768, ttl= |
| 4 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0005, seq=4/1024, ttl= |
| 5 | 2021-03-07 05:11 | 10.0.2.15 | 1.2.3.4 | ICMP | 100 | Echo (ping) request id=0x0005, seq=5/1280, ttl= |
| 6 | 2021-03-07 05:11 | 1.2.3.4 | 10.0.2.15 | ICMP | 100 | Echo (ping) reply id=0x0005, seq=1/256, ttl= |
| 7 | 2021-03-07 05:11 | 1.2.3.4 | 10.0.2.15 | ICMP | 100 | Echo (ping) reply id=0x0005, seq=2/512, ttl= |
| 8 | 2021-03-07 05:11 | 1.2.3.4 | 10.0.2.15 | ICMP | 100 | Echo (ping) reply id=0x0005, seq=3/768, ttl= |
| 9 | 2021-03-07 05:11 | 1.2.3.4 | 10.0.2.15 | ICMP | 100 | Echo (ping) reply id=0x0005, seq=4/1024, ttl= |
| 10 | 2021-03-07 05:11 | 1.2.3.4 | 10.0.2.15 | ICMP | 100 | Echo (ping) reply id=0x0005, seq=5/1280, ttl= |

Frame 1: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 1.2.3.4
Internet Control Message Protocol

```
0000  00 04 00 01 00 06 00 00 27 82 84 fc 00 00 00 00  .....T..@:.....
0010  45 00 00 54 fd 14 40 00 40 01 2d 80 0a 00 02 0f  E..T..@:.....
```

זה נותן לנו תשובה כאילו האתר הזה מחזיר לנו reply למרות שהוא לא קיים.

כל הקודים מצורפים בתיקיות!