

פס

6 אג

318765856 און 321
318636693 - 575 אג

1.1A

ה IP של Host A, Host B ושל
10.9.0.5, 10.9.0.6 ואיפה הם?

אכן בכל השם והטבלה אלו נראה את הקד
מבצע ממנו כל אחרים.

כא שטפסר ליאור בתענה מאוני
2 הודעות פנים ויקראו 2 הודעות
פונ (עלוקה) לכן בולטת אפס
למאת 4 הודעות.

ואצלי בקוד השלישי ספר.

אפס ליאור שואל וינה את SRC
- ו- dest של הפיפ.
א- זה בולט הודעות סמ מלמחמח.
Sub.

בפס השנה שמינו ליפסל גס
הרשאות פה אי נק או ליפסל
כ- אחרת מלמחמח פה
ה- שלח וכו' שאלו יקדו
מחמח קודמות פה קלסר
למחמח הפסל וכן חייב
הרשאות מוח.

```
seed@VM: ~/Labsetup
[01/04/22]seed@VM:~/Labsetup$ dcup
Starting hostA-10.9.0.5 ... done
Starting seed-attacker ... done
Starting hostB-10.9.0.6 ... done
Attaching to seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
hostA-10.9.0.5 | * Starting internet superserver inetd [ OK ]
hostB-10.9.0.6 | * Starting internet superserver inetd [ OK ]
^CGracefully stopping... (press Ctrl+C again to force)
Stopping hostA-10.9.0.5 ... done
Stopping hostB-10.9.0.6 ... done
Stopping seed-attacker ... done
[01/04/22]seed@VM:~/Labsetup$ dcup
Starting hostB-10.9.0.6 ... done
Starting hostA-10.9.0.5 ... done
Starting seed-attacker ... done
Attaching to seed-attacker, hostA-10.9.0.5, hostB-10.9.0.6
hostA-10.9.0.5 | * Starting internet superserver inetd [ OK ]
hostB-10.9.0.6 | * Starting internet superserver inetd [ OK ]
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-04 15:13:10.100	10.9.0.5	10.9.0.6	ICMP	64	80 Echo (ping) 0.066 ms
2	2022-01-04 15:13:10.100	10.9.0.6	10.9.0.5	ICMP	64	80 Echo (ping) 0.117 ms
3	2022-01-04 15:13:10.100	10.9.0.5	10.9.0.6	ICMP	64	80 Echo (ping) 0.025 ms

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5): 56(84) bytes of data:
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.066 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.117 ms
^C
--- 10.9.0.5 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.066/0.091/0.117/0.025 ms
[01/04/22]seed@VM:~/volumes$
```

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ sudo python3 shiffer1.1A.py
sniffing packets
###[ Ethernet ]###
dst      = 02:42:0a:09:00:05
src      = 02:42:97:b3:2e:71
type     = IPv4
###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 84
id       = 39544
flags    = DF
frag     = 0
ttl      = 64
proto    = icmp
chksum   = 0x8c19
src      = 10.9.0.1
dst      = 10.9.0.5
\options
###[ ICMP ]###
type     = echo-request
code     = 0
chksum   = 0x2979
id       = 0x3
seq      = 0x1
###[ Raw ]###
```

```
seed@VM: ~/volumes
[01/04/22]seed@VM:~/volumes$ python3 sniffer1.1A.py
sniffing packets
Traceback (most recent call last):
  File "sniffer1.1A.py", line 8, in <module>
    packet = sniff(iface = "br-ae32e9ad3ed5", 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
[01/04/22]seed@VM:~/volumes$
```

1.1B:

```
seed@VM: ~/./volumes
[01/04/22] seed@VM:~/./volumes$ sudo python3 shiffer1.1A.py
sniffing packets
###[ Ethernet ]###
  dst      = 02:42:0a:09:00:05
  src      = 02:42:97:b3:2e:71
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 39544
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0x8c19
  src      = 10.9.0.1
  dst      = 10.9.0.5
  options  \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x2979
  id       = 0x3
  seq      = 0x1
###[ Raw ]###
```

אנדרסא ק פקטור קמא נבנו כה
ב-111 הינו צינע ק אפאר אפקטור מוא
ב.

```
[01/06/22] seed@VM:~/./volumes$ sudo python3 sniffer1.1B.py
sniffing packets
###[ Ethernet ]###
  dst      = 52:54:00:12:35:02
  src      = 08:00:27:04:01:83
  type     = IPv4
###[ IP ]###
  version  = 4
  ihl      = 5
  tos      = 0x0
  len      = 84
  id       = 28243
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = icmp
  chksum   = 0xb037
  src      = 10.9.0.5
  dst      = 8.8.8.8
  options  \
###[ ICMP ]###
  type     = echo-request
  code     = 0
  chksum   = 0x9bc3
  id       = 0x5
  seq      = 0x1
###[ Raw ]###
  load     = 'G\x98\xd6a\x00\x00\x00\x00s1\x0c\x00\x00\x00\x00\x00\x00\x10\x11\x12\x13\x14\x15\
!#$%&'()*+,-./01234567'
###[ Ethernet ]###
```

אז העקר א אפס א קו
מסיים נא אלא ק בקי
אין כאן אפא אלא מרסני
אצור מרסני אפס ק 8.8.8.8

```
1 from scapy.all import *
2 print("sniffing packets")
3
4 def print_pkt(pkt):
5     pkt.show()
6
7 # (filter = "icmp", prn= print_pkt)# part 1
8 packet = sniff(iface = "br-ae32e9ad3ed5", filter = "tcp", prn=
9     print_pkt) #part 2
9 # packet = sniff(filter = "icmp and host 8.8.8.8", prn= print_pkt)
10 # part 3
```

```
seed@VM: ~/./volumes
seed@VM:~/./volumes
  flags    = DF
  frag     = 0
  ttl      = 64
  proto    = tcp
  chksum   = 0x3d85
  src      = 10.9.0.5
  dst      = 10.9.0.1
  options  \
###[ TCP ]###
  sport     = telnet
  dport     = 41514
  seq       = 1784407128
  ack       = 1309346890
  dataofs   = 8
  reserved  = 0
  flags     = PA
  window    = 509
  chksum    = 0x1453
  urgptr    = 0
  options   = [('NOP', None), ('NOP', None)]
53302453]]
###[ Raw ]###
  load     = 'seed@153b7cbbd2e:-$ '
```

כין אפא אלא
מרסני א
הפקטור מוא
קצ. אלא בנאיה
Telnet מין
מין יוקסא מנה עובד
מ קצ.

Task 1.2

כדי שאנחנו נאפשר לוואר בתוכנית
אנחנו נחזיקים את אدرس
מכיוון שאנחנו צריכים 10.9.0.1
ולשנינו 10.9.0.0-10.9.0.1.
אנחנו נאפשר לוואר בולטאין
שלא יתקבל תשובה בחזרה
שבואת פה 4 ק"מ.
ואז לא נאפשר לוואר.
לחלוקה האחרונה אנחנו נאפשר
באופן שינוע האدرس
שאינו השתנה. מכיוון ששאר
10.9.0.1 hostA. איננו צריכים
לחזקת loopback.

```
seed@VM: ~/volumes
[01/06/22]seed@VM:~/volumes$ sudo python3
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>> a=IP()
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'IP' is not defined
>>> s.src = '10.9.0.0'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 's' is not defined
>>> a.src = '10.9.0.0'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'a' is not defined
>>> a.dest = '10.9.0.6'
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
NameError: name 'a' is not defined
>>> from scapy.all import *
>>> a = IP('10.9.0.0')
>>> a.src = '10.9.0.0'
>>> a.dest = '10.9.0.6'
>>> b = ICMP()
>>> p = a/b
>>> send(p)
Sent 1 packets.
>>> send(p)
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 04:12	10.9.0.0	127.0.0.1	ICMP	42	Echo (ping) request 10.9.0.0, seq=0/0, ttl=64 (no response ...)


```
Sent 1 packets.
>>> ls(a)
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 (>) (0)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 0 (0)
chksum : XShortField = None (None)
src : SourceIPField = '10.9.0.0' (None)
dst : DestIPField = '127.0.0.1' (None)
options : PacketListField = [] ([])
>>> ls(a)
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 (>) (0)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 0 (0)
chksum : XShortField = None (None)
src : SourceIPField = '10.9.0.0' (None)
dst : DestIPField = '127.0.0.1' (None)
options : PacketListField = [] ([])
>>> send(p)
```

Task 3

```
1 from scapy.all import *
2
3 a = IP(dst = '172.217.171.206', ttl = 1)
4 b = ICMP()
5 p = a/b
6 ls(a)
7 send(p)
```

```
1 from scapy.all import *
2
3 a = IP(dst = '172.217.171.206', ttl = 16)
4 b = ICMP()
5 p = a/b
6 ls(a)
7 send(p)
```

אפשר לראות בקוד כי אנו צורעים ממשלוח
 מה-1 אל-2 ואל-2 אל-3
 על 2 עז שנקרא תשובה.
 אחרי שקיבלנו תשובה ודברנו אל-2
 בדבר אל-3 אנו יודעים (הוספנו אף
 שיש לנו 1-2)

אנו יודעים עליו שיש אולי.

אפשר לראות בואישר
 שבאנו בהתחלה אל קיבלנו
 תשובה כי אל-2 הינו
 קצר מדי. ואחרי מכן אנו
 מקבלים תשובה.

הספנו לשם התחלת ודברים
 את הפקודה שלפניה
 מה שאנו רואים
 בהתחלה.

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
2	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
3	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response f...
4	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
5	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
6	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response f...
7	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
8	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
9	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response f...
10	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
11	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
12	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response f...
13	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
14	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
15	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=16 (no response f...
16	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
17	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
18	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=32 (no response f...
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface enp3s3, id 0						
Ethernet II, Src: PcsCompu_04:01:03 (08:00:27:04:01:03), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (Request)						
19	2022-01-06 04:4:10.000000	208.67.220.220	10.0.2.15	DNS	161	Standard query response 0x581 AAAA connectivity-check.ubuntu.
20	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
21	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
22	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
23	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=12 (reply in 30)
24	2022-01-06 04:4:10.000000	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in ...)
25	2022-01-06 04:4:10.000000	208.67.220.220	10.0.2.15	DNS	161	Standard query response 0x453 AAAA connectivity-check.ubuntu.
26	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
27	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
28	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 30)
29	2022-01-06 04:4:10.000000	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in ...)
30	2022-01-06 04:4:10.000000	PcsCompu_04:01:03	Broadcast	ARP	42	Who has 10.0.2.27 Tell 10.0.2.15
31	2022-01-06 04:4:10.000000	RealtekU_12:35:02	PcsCompu_04:01:03	ARP	60	10.0.2.2 is at 52:54:00:12:35:02
32	2022-01-06 04:4:10.000000	10.0.2.15	172.217.171.206	ICMP	42	Echo (ping) request id=0x0000, seq=0/0, ttl=8 (reply in 40)
33	2022-01-06 04:4:10.000000	172.217.171.206	10.0.2.15	ICMP	60	Echo (ping) reply id=0x0000, seq=0/0, ttl=115 (request in ...)

```
seed@VM: ~/volumes
proto      : ByteEnumField      = 0      (0)
chksum     : XShortField       = None   (None)
src        : SourceIPField     = '10.0.2.15' (None)
dst        : DestIPField      = '172.217.171.206' (None)
options    : PacketListField   = []     ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/../volumes$ sudo python3 Task1.3.py
version    : BitField (4 bits) = 4      (4)
ihl        : BitField (4 bits) = None   (None)
tos        : XByteField       = 0      (0)
len        : ShortField       = None   (None)
id         : ShortField       = 1      (1)
flags      : FlagsField (3 bits) = <Flag 0 ()> (<Flag 0 ()>)
frag       : BitField (13 bits) = 0      (0)
ttl        : ByteField        = 9      (64)
proto      : ByteEnumField     = 0      (0)
chksum     : XShortField       = None   (None)
src        : SourceIPField     = '10.0.2.15' (None)
dst        : DestIPField      = '172.217.171.206' (None)
options    : PacketListField   = []     ([])
.
Sent 1 packets.
[01/06/22]seed@VM:~/../volumes$
```

Task 1.4

```
Task1.4.py
1 from scapy.all import *
2
3 def spoof(pkt):
4     if ICMP in pkt and pkt[ICMP].type == 8:
5         print('start sniff')
6         print('original source:', pkt[IP].src)
7         print('original dest:', pkt[IP].dst)
8
9         ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
10        icmp = ICMP(type=8, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
11        data = pkt[Raw].load
12        newpkt = ip/icmp/data
13
14        print('spoof')
15        print('spoof source:', newpkt[IP].src)
16        print('spoof dest:', newpkt[IP].dst)
17        send(newpkt, verbose=0)
18
19 packet = sniff(filter='br-a3226a3d3e05', filter='icmp', promiscuous=True)
20
21 [1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

```
64 bytes from 10.9.0.5: icmp_seq=13 ttl=64 time=0.117 ms
64 bytes from 10.9.0.5: icmp_seq=14 ttl=64 time=0.126 ms
64 bytes from 10.9.0.5: icmp_seq=15 ttl=64 time=0.120 ms
64 bytes from 10.9.0.5: icmp_seq=16 ttl=64 time=0.098 ms
64 bytes from 10.9.0.5: icmp_seq=17 ttl=64 time=0.098 ms
^C
--- 10.9.0.5 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 1634
rtt min/avg/max/mdev = 0.090/0.126/0.260/0.037 ms
[01/06/22]seed@VM:~/../volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.100 ms
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=24.2 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.139 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=13.2 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=12.6 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=0.131 ms
64 bytes from 10.9.0.5: icmp_seq=4 ttl=64 time=6.23 ms (DUP!)
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=0.127 ms
64 bytes from 10.9.0.5: icmp_seq=5 ttl=64 time=12.8 ms (DUP!)
^Z
[1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

No.	Time	Source	Destination	Protocol	Length	Info
1	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=8/2848, ttl=64 (reply in ...)
2	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=8/2848, ttl=64 (reply in ...)
3	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=9/2904, ttl=64 (request i...
4	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=9/2904, ttl=64 (reply in ...)
5	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=10/2960, ttl=64 (request i...
6	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=10/2960, ttl=64 (reply in ...)
7	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=11/3016, ttl=64 (request i...
8	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=11/3016, ttl=64 (reply in ...)
9	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=12/3072, ttl=64 (request i...
10	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=12/3072, ttl=64 (reply in ...)
11	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=13/3128, ttl=64 (request i...
12	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=13/3128, ttl=64 (reply in ...)
13	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=14/3184, ttl=64 (request i...
14	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=14/3184, ttl=64 (reply in ...)
15	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=15/3240, ttl=64 (request i...
16	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=15/3240, ttl=64 (reply in ...)
17	2022-01-06 08:41:10.9.0.1	10.9.0.1	10.9.0.5	ICMP	80	Echo (ping) request 10.9.0.0.0.0. seq=16/3296, ttl=64 (request i...
18	2022-01-06 08:41:10.9.0.5	10.9.0.5	10.9.0.1	ICMP	80	Echo (ping) reply 10.9.0.0.0.0. seq=16/3296, ttl=64 (reply in ...)

```
Frame 1: 80 bytes on wire (784 bits), 80 bytes captured (784 bits) on interface br-a3226a3d3e05, id 0
Ethernet II, Src: 02:42:ad:bd:f2:0f (02:42:ad:bd:f2:0f), Dst: 02:42:8a:99:00:05 (02:42:8a:99:00:05)
Internet Protocol Version 4, Src: 10.9.0.1, Dst: 10.9.0.5
.
Task1.4.py
1 from scapy.all import *
2
3 def spoof(pkt):
4     if ICMP in pkt and pkt[ICMP].type == 8:
5         print('start sniff')
6         print('original source:', pkt[IP].src)
7         print('original dest:', pkt[IP].dst)
8
9         ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl)
10        icmp = ICMP(type=8, id=pkt[ICMP].id, seq=pkt[ICMP].seq)
11        data = pkt[Raw].load
12        newpkt = ip/icmp/data
13
14        print('spoof')
15        print('spoof source:', newpkt[IP].src)
16        print('spoof dest:', newpkt[IP].dst)
17        send(newpkt, verbose=0)
18
19 packet = sniff(filter='br-a3226a3d3e05', filter='icmp', promiscuous=True)
20
21 [1]+  Stopped                  ping 10.9.0.5
[01/06/22]seed@VM:~/../volumes$
```

```
[01/06/22]seed@VM:~/../volumes$ ^C
[01/06/22]seed@VM:~/../volumes$ sudo python3 Task1.4.py
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
spoof source: 10.9.0.5
spoof dest: 10.9.0.1
start sniff
original source: 10.9.0.1
original dest: 10.9.0.5
spoof
```

על מנת להבין את הבעיה
Host B - ping
ואם נשאל את השרת
שמידת בין השרת לשרת
אשר הוא נמצא
בהצפנה וזה בקוד,
הוא יחזיר לנו את
המקור והיעד של
Host B - src

Task 2.1A

```
seed@VM: ~/Volumes
[01/06/22]seed@VM:~/.../Volumes$ ping 10.9.0.5
PING 10.9.0.5 (10.9.0.5) 56(84) bytes of data.
64 bytes from 10.9.0.5: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 10.9.0.5: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 10.9.0.5: icmp_seq=3 ttl=64 time=0.058 ms
^C
[!]+ Stopped ping 10.9.0.5
[01/06/22]seed@VM:~/.../Volumes$
```

```
seed@VM: ~/Volumes
[01/06/22]seed@VM:~/../Volumes$ sudo ./sniffer
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
Got a packet
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.5
Got a packet
Source IP is: 10.9.0.5
Destination IP is: 10.9.0.1
```

(א) חב' מלך נק' אר
 src ip dest קו אר צר' אר
 אר אר מלך אר אר אר
 אר src ip dest קו אר

2. אף רחמים הרגאת מנהל נ-2 סדר
ל. כפי זהות בטרם יסוס קיז (נצב ויזל) אכילס.

Raw sock -> לוקח את הנתונים
 ומוסיף את הנתונים.

Q3) מה אני מצפה את מצב
בחסמים אחד. אני יקבל יק את החבילות שאחזור להוציא אלי
ישרות ולא אל הפקטור הסבירות הכפלים וגם שלי.

```

c
h
e
/
=
***** ICMP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

***** ICMP Packet *****
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0 Echo Reply
ICMP Echo code is: 0
Got a packet

d
h
***** ICMP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
ICMP Echo type is: Type 8 Echo Request
ICMP Echo code is: 0
Got a packet

e
e
***** ICMP Packet *****
Source IP is: 10.9.0.6
Destination IP is: 10.9.0.1
ICMP Echo type is: Type 0 Echo Reply
ICMP Echo code is: 0

[2]+ Stopped ping 10.9.0.6
[01/06/22] seed@VM:~/.../volumes$

```

Task 2.1B

שטער אראפ כי הספנו יך פקטור
מסל קמא' בין 01.09.01
לין 06.09.01, ואלאני היזער פליג
דב' אראפ איר פא

```

seed@VM: ~/volumes
***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59580
Destination Port is: 23
Got a packet

```

```

seed@VM: ~/volumes
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan 6 18:46:44 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7elf08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/volumes$ telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^'.
Ubuntu 20.04.1 LTS
61faa7elf08a 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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Thu Jan 6 18:51:19 UTC 2022 from 10.9.0.1 on pts/2
seed@61faa7elf08a:~$ exit
logout
Connection closed by foreign host.
[01/06/22]seed@VM:~/volumes$

```

```

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
D?000d
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
C?000e
Got a packet

***** TCP Packet *****
Source IP is: 10.9.0.1
Destination IP is: 10.9.0.6
Source Port is: 59596
Destination Port is: 23
Data:
?000s
Got a packet

```

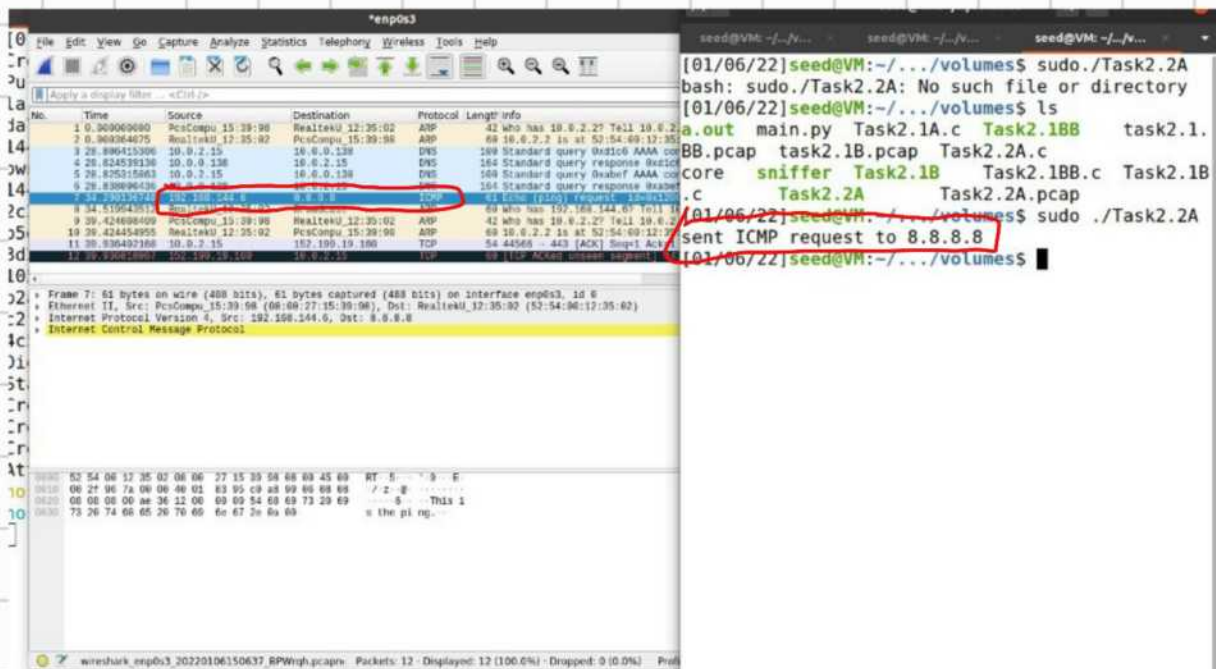
אשלי אדואר טן כי אין התעלה
 מ. החלק השני כולו האזנים
 1-100-100 port כפחוקה
 TCP. אשלי זלזלתי כי אשלי
 שכן הסנדר אשלי מרבים את זה.

Tas/2.1C
 TCP data אשלי אשלי
 אשלי אשלי אשלי אשלי
 אשלי אשלי אשלי אשלי

Task 2.2A

Task 2.2B

ענין ע' ש' והשמות
 ב"בני קו' אברה אברה
 בתחילה שנתנו רחמים
 אברהם ping אב' ה' אב' ש
 לא תואם אברהם ואלו
 נולד לא נשק אב'
 הוא קיבל את היקשרה



Handwritten notes at the bottom of the page:

טעם צו זיין שטח אים תשעה בקצה יתר קטני ה'רצ"ד יתרה באבס"ס
אז מען גייט יהודה באדן הינצ'ס

Q5) שני חידים לחשב את check sum כאשר מן ואתרנט
 ב socket server. כדי בואר לחיזו לנקודת הרצויה של קו
 וסלוג (המחשבו) במקום במסלול (5).

Q6. מניין חילים אימתנים במלחמה? Ethernet, ip, icmp, data שני הסוגים.

מכיוון שאני נכנס לזמן בו העברתי הרבה שנים מחייבי
אני חייב להשתמש במילה Society אבל אני חייב
להגיד את זה.

ping 10.9.0.5

```
sent ICMP reply to 10.9.0.6
sent ICMP reply to 10.9.0.6
```

אבשר לראות כי אלהים
 רשמים נ HostA
 - HostB את א ICMP
 אק ה Atacker נותן
 /רשום את הניסוח אבן
 /רשום את הניסוח בן
 SRC - dst ואלו
 אבשר לראות אם הניסוח
 ע"ן תצורה זכרתי ICMP
 נהנו את הניסוח
 - 10.9.06 - 0.9.05