

```
noatzur@noatzur:~/Desktop/Labsetup$ telnet 10.0.6.24
Trying 10.0.6.24...
```

כמו כן ניתן לראות שהחוקה של פורט 23
 :10-100

```
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./sniffer
[sudo] password for noatzur:
From: 10.0.2.15
To: 10.0.6.24
im an TCP packet !!!

From: 10.0.2.15
To: 10.0.6.24
im an TCP packet !!!

From: 10.0.2.15
To: 10.0.6.24
im an TCP packet !!!

From: 10.0.2.15
To: 34.107.221.82
im an TCP packet !!!

From: 10.0.2.15
To: 34.107.221.82
im an TCP packet !!!

From: 10.0.2.15
To: 34.107.221.82
im an TCP packet !!!
```

① ניתן לראות
 כי פורט 23
 נמצא פתוח

② ניתן לראות כי פורט 80
 נמצא פתוח
 לשרת המטרה

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.6.24	TCP	74	54366 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
2	1.023832068	10.0.2.15	10.0.6.24	TCP	74	[TCP Retransmission] 54366 → 23 [SYN] Seq=0 Win=64240 Len=0 M...
3	3.037376559	10.0.2.15	10.0.6.24	TCP	74	[TCP Retransmission] 54366 → 23 [SYN] Seq=0 Win=64240 Len=0 M...
4	7.229806345	10.0.2.15	10.0.6.24	TCP	74	[TCP Retransmission] 54366 → 23 [SYN] Seq=0 Win=64240 Len=0 M...
5	12.709779056	10.0.2.15	8.8.4.4	DNS	95	Standard query 0xe012 A detectportal.firefox.com OPT
6	12.710085976	10.0.2.15	8.8.4.4	DNS	95	Standard query 0x34c6 AAAA detectportal.firefox.com OPT
7	12.777545515	8.8.4.4	10.0.2.15	DNS	206	Standard query response 0xe012 A detectportal.firefox.com CNA...
8	12.790234250	8.8.4.4	10.0.2.15	DNS	218	Standard query response 0x34c6 AAAA detectportal.firefox.com ...
9	12.799050000	10.0.2.15	34.107.221.82	TCP	74	33300 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
10	12.864246944	34.107.221.82	10.0.2.15	TCP	60	80 → 33300 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
11	12.864356038	10.0.2.15	34.107.221.82	TCP	54	33300 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12	12.864549563	10.0.2.15	34.107.221.82	HTTP	350	GET /success.txt HTTP/1.1
13	12.865268073	34.107.221.82	10.0.2.15	TCP	60	80 → 33300 [ACK] Seq=1 Ack=297 Win=65535 Len=0
14	12.932918025	34.107.221.82	10.0.2.15	HTTP	274	HTTP/1.1 200 OK (text/plain)
15	12.932994138	10.0.2.15	34.107.221.82	TCP	54	33300 → 80 [ACK] Seq=297 Ack=221 Win=64020 Len=0
16	12.908538915	10.0.2.15	8.8.4.4	DNS	82	Standard query 0xa412 A example.org OPT
17	13.012384684	10.0.2.15	8.8.4.4	DNS	82	Standard query 0xefd0 AAAA example.org OPT
18	13.012968541	10.0.2.15	8.8.4.4	DNS	84	Standard query 0x2bd4 A ipv4only.arpa OPT
19	13.013694636	10.0.2.15	8.8.4.4	DNS	84	Standard query 0x7ba6 AAAA ipv4only.arpa OPT
20	13.018650942	10.0.2.15	8.8.4.4	DNS	106	Standard query 0xaed6 A content-signature-2.cdn.mozilla.net 0...
21	13.018906963	10.0.2.15	8.8.4.4	DNS	106	Standard query 0xc1cf AAAA content-signature-2.cdn.mozilla.net...
22	13.024058936	10.0.2.15	34.107.221.82	TCP	74	33302 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...

1	0.0.0.0.0.0.0.0	10.0.2.15	10.0.6.24	TCP	74 54366 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS
2	1.023032068	10.0.2.15	10.0.6.24	TCP	74 [TCP Retransmission] 54366 - 23 [SYN] Seq=
Total Length: 60 Identification: 0xe448 (58440) Flags: 0x4000, Don't fragment Fragment offset: 0 Time to live: 64 Protocol: TCP (6) Header checksum: 0x3a3d [validation disabled] [Header checksum status: Unverified] Source: 10.0.2.15 Destination: 10.0.6.24					
Transmission Control Protocol, Src Port: 54366, Dst Port: 23, Seq: 0, Len: 0					
Source Port: 54366					
Destination Port: 23					
[Stream index: 0]					
[TCP Segment Len: 0]					
Sequence number: 0 (relative sequence number)					
Sequence number (raw): 551855110					
[Next sequence number: 1 (relative sequence number)]					
Acknowledgment number: 0					
Acknowledgment number (raw): 0					
1010 = Header Length: 40 bytes (10)					
Flags: 0x002 (SYN)					
Window size value: 64240					
[Calculated window size: 64240]					
Checksum: 0x1c55 [unverified]					
[Checksum Status: Unverified]					
Urgent pointer: 0					
0. Time Source Destination Protocol Length Info 7 12.777545515 8.8.4.4 10.0.2.15 DNS 206 Standard query response 8 12.790234250 8.8.4.4 10.0.2.15 DNS 218 Standard query response 9 12.799050004 10.0.2.15 34.107.221.82 TCP 74 33300 - 80 [SYN] Seq=0					
Total Length: 60					
Identification: 0x7275 (29301)					
Flags: 0x4000, Don't fragment					
Fragment offset: 0					
Time to live: 64					
Protocol: TCP (6)					
Header checksum: 0xbc7a [validation disabled]					
[Header checksum status: Unverified]					
Source: 10.0.2.15					
Destination: 34.107.221.82					
Transmission Control Protocol, Src Port: 33300, Dst Port: 80, Seq: 0, Len: 0					
Source Port: 33300					
Destination Port: 80					
[Stream index: 1]					
[TCP Segment Len: 0]					
Sequence number: 0 (relative sequence number)					
Sequence number (raw): 934879220					
[Next sequence number: 1 (relative sequence number)]					
Acknowledgment number: 0					
Acknowledgment number (raw): 0					
1010 = Header Length: 40 bytes (10)					
Flags: 0x002 (SYN)					
Window size value: 64240					
[Calculated window size: 64240]					
Checksum: 0xbfb [unverified]					
[Checksum Status: Unverified]					

: 2.1c

בסוף זה התקבלו מהצבים ס'מא של user וכל
 שלבי הפחיתוק telnet, פחיתוק של שלבי port 23
 ואינו מאולץ וכן נכנס ס'מא א-ה data שלשל פס.
 במחנה מטה הצבים פחיתוק א-ה data להתקבל
 והס'מא UNION במחנה צ'ג'ג.
 הנוסף צ'ג'גו גם מחנה של WS שלל (פ'ן ס'מא א-
 ה data. פ'ן מ'ן פחיתוק א-ה telnet

```

noatzur@noatzur: ~/Desktop/Labset
From: 10.9.0.5
To: 10.0.2.15
nek!0+
From: 10.9.0.5
To: 10.0.2.15
nek!0+ my password is: sawd564
From: 10.0.2.15
To: 10.9.0.5
0+nek!
From: 10.0.2.15
To: 10.9.0.5
0+nek!0+ my password is: sawd564
From: 10.9.0.5
To: 10.0.2.15
noatzur@noatzur: ~/Desktop/Labsetup/volumes
root@cc85463f989b:/# echo my password is: sawd564 | nc 10.0.2.15 23
**** *#*#*^Z
[3]+ Stopped echo my password is: sawd564 | nc 10.0.2.15 23
root@cc85463f989b:/#

```

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.9.0.5	10.0.2.15	TCP	76	59904 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F...
2	0.000000000	10.9.0.5	10.0.2.15	TCP	76	[TCP Out-Of-Order] 59904 → 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_F...
3	0.000043562	10.0.2.15	10.9.0.5	TCP	76	23 → 59904 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_F...
4	0.000048282	10.0.2.15	10.9.0.5	TCP	76	[TCP Out-Of-Order] 23 → 59904 [SYN, ACK] Seq=0 Ack=1 Win=65160 SACK_F...
5	0.000064200	10.9.0.5	10.0.2.15	TCP	68	59904 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=185 TSecr=0
6	0.000064200	10.9.0.5	10.0.2.15	TCP	68	[TCP Dup ACK 5#1] 59904 → 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0
7	0.000230690	10.9.0.5	10.0.2.15	TELNET	92	Telnet Data ...
8	0.000230690	10.9.0.5	10.0.2.15	TCP	92	[TCP Retransmission] 59904 → 23 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0
9	0.000248148	10.0.2.15	10.9.0.5	TCP	68	23 → 59904 [ACK] Seq=1 Ack=25 Win=65152 Len=0 TSval=13 TSecr=0
10	0.000251112	10.0.2.15	10.9.0.5	TCP	68	[TCP Dup ACK 9#1] 23 → 59904 [ACK] Seq=1 Ack=25 Win=65152 Len=0
11	0.004430679	127.0.0.1	127.0.0.53	DNS	94	Standard query 0x2ac9 PTR 5.0.9.10.in-addr.arpa OPT
12	0.005472205	10.0.2.15	8.8.4.4	DNS	94	Standard query 0x4750 PTR 5.0.9.10.in-addr.arpa OPT
13	0.070025501	8.8.4.4	10.0.2.15	DNS	94	Standard query response 0x4750 No such name PTR 5.0.9.10.in-addr.arpa
14	0.071658924	10.0.2.15	8.8.4.4	DNS	83	Standard query 0x4750 PTR 5.0.9.10.in-addr.arpa
15	0.131252000	8.8.4.4	10.0.2.15	DNS	83	Standard query response 0x4750 No such name PTR 5.0.9.10.in-addr.arpa
16	0.132611220	127.0.0.53	127.0.0.1	DNS	94	Standard query response 0x2ac9 No such name PTR 5.0.9.10.in-addr.arpa
17	0.133268345	10.0.2.15	10.9.0.5	TELNET	80	Telnet Data ...

Frame 7: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface any, id 0

```

0000 00 03 00 01 00 06 02 42 0a 09 00 05 00 00 08 00 .....B.....
0010 45 00 00 4c 30 b0 40 00 40 06 f3 df 0a 09 00 05 E..L.O.....
0020 0a 00 02 0f ea 00 00 17 1d 12 05 13 cd 57 ca 3f .....W.?
0030 80 18 01 f6 16 5b 00 00 01 01 08 0a 6e a1 6b 21 .....a.k!
0040 4f 02 a9 a5 6d 79 20 70 61 73 73 77 6f 72 64 20 0...my p assword
0050 69 73 3a 20 73 61 77 64 35 36 34 0a             is: sawd 564

```

2.2A

spooof.c קובץ Spooof

בסוף זה הפקלטם כטוב את חנני ה Spooof שלנו
 כבנו חנני לעזרה פאקטה מסונן TCP, לה'3 שמה הוא
 88.88 וה IP source שמה 1.1.1.1 (קטן שלא קיים בסדר...)

במחנה המצורפה (ג'ן דראג א הפאקטה לעזרנו ואם פט'יה
 וב S W ג'ן דראג לאק, ולמה הפאקטה ה'51.

The image shows a Wireshark packet capture of a spoofed TCP packet. The packet list shows a packet from 1.1.1.2 to 8.8.8.8 on port 80. The packet details pane shows the following information:

- Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface
- Linux cooked capture
- Packet type: Sent by us (4)
- Link-layer address type: 1
- Link-layer address length: 6
- Source: PcsCompu_88:fa:f0 (08:00:27:88:fa:f0)
- Unused: 0000
- Protocol: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 1.1.1.2, Dst: 8.8.8.8
- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 46
- Identification: 0xcf37 (53047)
- Flags: 0x0000
- Fragment offset: 0
- Time to live: 255
- Protocol: TCP (6)
- Header checksum: 0xda7f [correct]
- [Header checksum status: Good]
- [Calculated Checksum: 0xda7f]
- Source: 1.1.1.2

The packet bytes pane shows the raw data of the packet, including the header and payload.

The terminal output shows the following commands and results:

```
noatzur@noatzur: ~/Desktop/Labsetup
noatzur@noatzur:~/Desktop/Labsetup$ gcc -o spoof spoof.c
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./spoof
Packet length : 46
Packet source ip : 1.1.1.2
Packet destination ip : 8.8.8.8
Packet ttl : 255
Packet id : 0
noatzur@noatzur:~/Desktop/Labsetup$
```

spoof_ICMP.c קובץ Spoof ICMP request : 2.2.B

בסעיף זה הברקסו דוגמה סכומי spoof
 נוסח ICMP request (id=8), הולשלו בקרו לרבו
 כמילא הקורסמ כזי הוא אופי עם מנאס 18 כזיק.

The image shows a Wireshark packet capture of a spoofed ICMP packet. The packet list shows two packets: a request from 10.0.2.15 to 8.8.8.8 and a reply from 8.8.8.8 to 10.0.2.15. The packet details pane shows the following information:

- Time: 0.000000000
- Source: 10.0.2.15
- Destination: 8.8.8.8
- Protocol: ICMP
- Length: 61
- Info: Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response)

The packet bytes pane shows the raw data of the packet, including the header and payload.

The terminal output shows the following commands and results:

```
noatzur@noatzur: ~/Desktop/Labsetup
noatzur@noatzur:~/Desktop/Labsetup$ gcc -o spood_icmp spoof_ICMP.c
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./spoof_icmp
[sudo] password for noatzur:
sudo: ./spoof_icmp: command not found
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./spood_icmp
packet recieved:
ICMP type 0
ICMP code 0
ICMP chksum 14006
ICMP id 18
ICMP seq 0
noatzur@noatzur:~/Desktop/Labsetup$
```

request נסח
 אלוני '3 רנו,
 אהקבד reply.

כנוסל בסעיף זה הברקסו דוגמה סכומי 3 אלוני:

Question 4

לאחר ניסוי קצר שעשנו בקוד Spoof.c, לבד שניתן את קוד
 ה header ip גילינו כי לא משנה מה הקוד שנזכר לו, כל עוד
 הערך קוד מ-20 כי צה הקוד המינימלי.
 (וכל שלם גם עתים קודים, למשל 100, הפקטה שלם באופן מיון
 ו"מפץ" את ה data ה-אבסים

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	1.1.1.2	8.8.8.8	TCP	60
2	5.250797530	PcsCompu_88:fa:f0	RealtekU_12:35:02	ARP	28
3	5.251586175	RealtekU_12:35:02	PcsCompu_88:fa:f0	ARP	28

.... 0101 = Header Length: 20 bytes (5)

Offset	Time	Source	Destination	Protocol	Length
0000	52 54 00 12 35 02	08 00 27	88 fa f0 08 00 45 00	RT-5	...
0010	00 64 b9 0b 00 00	ff 06 f0 75 01 01	01 02 08 08
0020	00 08 04 d2 00 00	00 00 00 00 00 00	00 00 00 00 50 02
0030	16 d0 50 0a 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0040	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0050	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0060	00 00 00 00 00 00	00 00 00 00 00 00	00 00 00 00 00 00
0070	aa aa				

→ הפוך באבסים
 כאשר הקצתו את הערך
 8-100.

הפגה שלונזיה
 כאשר הקצתו
 את הקוד
 עתים 10.

```
noatzur@noatzur:~/Desktop/Labsetup$ gcc -o spoof spoof.c
noatzur@noatzur:~/Desktop/Labsetup$ sudo ./spoof
[sudo] password for noatzur:
sendto failed: Invalid argument
noatzur@noatzur:~/Desktop/Labsetup$
```

Question 5

גם בסעיף זה ביצענו ניסוי קטן כפי דמיון שא
 מחקנו את הלוח למחלקת checksum עבור חבירה המכילים ב iph
 ולמנו רק 0. שורה הפקטה עברה באופן מיון, וכל שא נין
 היה מראה שה checksum header הוא correct או status הוא
 good. מכאן הוכח שה Socket raw מחלק עברנו את ה checksum
 ואם לא הכחזי שאנו נעשה את החישוב.

: Question 6

[illegible]

sniff_spoot_new.c Sniff & spoot : 2.3

הפעם זה היבט של "חבר" אחר חברה ה Sniff
למבנה עם חברה ה Spoof.
ה container של השליש הרגיל לפני ping ו IP
שלד ק"מ 1.2.3.4 כאשר במקרים, Containers של ה attacker
הרגילי אחר ה sniff & spoof שלד.
החברה, ע"י פור ה sniff למבנה, צורה אחר ה ping שלד
מהשליש הרגילי (ICMP) ונדרה כאקט של reply משוב
ולאחר לאורו IP ממני היקבל ה ping.
כך בעצם "זרני מנח" שלא שלשליש הרגילי האומר שהוא קיבל
האברה מ IP שלד ק"מ, כאילו היה ק"מ...

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=1/256, ttl=64
2	1.012154608	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=2/512, ttl=64
3	1.438120007	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=1/256, ttl=64
4	2.013259496	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=3/768, ttl=64
5	2.452097962	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=2/512, ttl=64
6	3.013819538	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=4/1024, ttl=64
7	3.477443931	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=3/768, ttl=64
8	4.015282455	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=5/1280, ttl=64
9	4.500789624	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=4/1024, ttl=64
10	5.016529343	10.9.0.5	1.2.3.4	ICMP	98	Echo (ping) request id=0x0011, seq=6/1536, ttl=64
11	5.172609036	02:42:0a:09:00:05	02:42:56:e2:d1:7d	ARP	42	Who has 10.9.0.1? Tell 10.9.0.5
12	5.172716779	02:42:56:e2:d1:7d	02:42:0a:09:00:05	ARP	42	10.9.0.1 is at 02:42:56:e2:d1:7d
13	5.524551384	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=5/1280, ttl=64
14	6.451776770	02:42:56:e2:d1:7d	02:42:0a:09:00:05	ARP	42	Who has 10.9.0.5? Tell 10.9.0.1
15	6.451851468	02:42:0a:09:00:05	02:42:56:e2:d1:7d	ARP	42	10.9.0.5 is at 02:42:0a:09:00:05
16	6.548242951	1.2.3.4	10.9.0.5	ICMP	98	Echo (ping) reply id=0x0011, seq=6/1536, ttl=64

Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on

Ethernet II, Src: 02:42:56:e2:d1:7d (02:42:56:e2:d1:7d), Dst: 02:42:0a:09:00:05

Internet Protocol Version 4, Src: 1.2.3.4, Dst: 10.9.0.5

Internet Control Message Protocol

Type: 0 (Echo (ping) reply)

Code: 0

Checksum: 0x342f [correct]

[Checksum Status: Good]

Identifier (BE): 17 (0x0011)

Identifier (LE): 4352 (0x1100)

Sequence number (BE): 1 (0x0001)

Sequence number (LE): 256 (0x0100)

[Request frame: 1]

[Response time: 1438.120 ms]

Timestamp from icmp data: Feb 23 2021 00:32:50.000000000 IST

```

noatzur@noatzur: ~/Desktop/Labsetu
root@3b7b633b0914:/# 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=1438 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=64 time=1440 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=64 time=1464 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=64 time=1487 ms
^Z
[2]+  Stopped                  ping 1.2.3.4
root@3b7b633b0914:/#

```

0000 02 42 0a 09 00 05 02 42 56 e2 d1 7d 08 00 45 00 .B....B V...E

sniff_...
boof_new
c

red arrow pointing to the 3rd packet in the list

red text: .reply 'סדנ' ק'ס pk 1.2.3.4 (אך)