בס"ד

# מטלה 5

ת"ז מגישים: 209326776, 322998287

## **Task A**:

```
---------------got packet 5---------
source_ip: 127.0.0.1
dest_ip: 127.0.0.1
source_port: 9999
dest_port: 32824
timestamp: 1674131869
total_length: 564
cache_flag: 1
steps_flag: 1
type_flag: 0
status_code: 200
cache_control: 65535
00
00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 02
68 6c 16 40 00 40 06 ce 77 7f 00 00 01 7f 00 00
01 27 0f 80 38 1a 95 d6 95 ea ca e1 ab 80 18 02
00 00 5d 00 00 01 01 08 0a 1a 85 a3 61 1a 85 a3
5f 63 c9 39 9d 02 34 c8 18 ff ff 00 00 80 04 95
1d 02 00 00 00 00 00 00 47 bf d8 cc 84 91 13 d5
9f 5d 94 28 8c 43 28 73 69 6e 28 6d 61 78 28 32
2c 20 28 33 20 2a 20 34 29 2c 20 35 2c 20 28 36
20 2a 20 28 28 37 20 2a 20 38 29 20 2f 20 39 29
29 2c 20 28 31 30 20 2f 20 31 31 29 29 29 20 2f
20 31 32 29 20 2a 20 31 33 94 8c 3e 28 73 69 6e
28 6d 61 78 28 32 2c 20 31 32 2c 20 35 2c 20 28
36 20 2a 20 28 28 37 20 2a 20 38 29 20 2f 20 39
29 29 2c 20 28 31 30 20 2f 20 31 31 29 29 29 20
2f 20 31 32 29 20 2a 20 31 33 94 8c 39 28 73 69
6e 28 6d 61 78 28 32 2c 20 31 32 2c 20 35 2c 20
28 36 20 2a 20 28 35 36 20 2f 20 39 29 29 2c 20
28 31 30 20 2f 20 31 31 29 29 29 20 2f 20 31 32
29 20 2a 20 31 33 94 8c 42 28 73 69 6e 28 6d 61
78 28 32 2c 20 31 32 2c 20 35 2c 20 28 36 20 2a
20 36 2e 32 32 32 32 32 32 32 32 32 32 32 32 32
32 32 29 2c 20 28 31 30 20 2f 20 31 31 29 29 29
20 2f 20 31 32 29 20 2a 20 31 33 94 8c 3d 28 73
69 6e 28 6d 61 78 28 32 2c 20 31 32 2c 20 35 2c
20 33 37 2e 33 33 33 33 33 33 33 33 33 33 33 33
33 33 36 2c 20 28 31 30 20 2f 20 31 31 29 29 29
2f 20 31 32 29 20 2a 20 31 33 94 8c 46 28 73
6e 28 6d 61 78 28 32 2c 20 31 32 2c 20 35 2c
20 33 37 2e 33 33 33 33 33 33 33 33 33 33 33 33
33 33 36 2c 20 30 2e 39 30 39 30 39 30 39 30 39
30 39 30 39 30 39 31 29 29 20 2f 20 31 32 29 20
2a 20 31 33 94 8c 23 28 73 69 6e 28 33 37 2e 33
33 33 33 33 33 33 33 33 33 33 33 33 33 36 29 20
2f 20 31 32 29 20 2a 20 31 33 94 8c 20 28 2d 30
```

הסברים על הקוד נמצאים בתוך הקוד.
הרצנו את הקבצי python ממטלה 2 שעובדות על tcp

ולכן בקובץ שלנו הסנפנו פקאטות TCP . והדפסנו את השדות המבוקשים .

```
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 9999, Dst Port: 32824, Seq: 1, Ack: 688, Len: 564
  Source Port: 9999
  Destination Port: 32824
```

```
TCP payload (564 bytes)
TCP segment data (564 bytes)
```

נתונים אלה הם מתוך פאקטה 6 (אנו התחלנו את הספירה מ0 לכן זו אותה פאקטה) וניתן לראות כי נתונים אלה תואמים להדפסה.

| | | | | | |
|---|---|---|---|---|---|
| 0.000039097 | 127.0.0.1 | 127.0.0.1 | TCP | 66 | 32824 → 9999 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=444965727 TSecr=444965727 |
| 0.000594959 | 127.0.0.1 | 127.0.0.1 | TCP | 753 | 32824 → 9999 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=687 TSval=444965727 TSecr=444965727 [TCP segment of a reassembled PDU] |
| 0.000615497 | 127.0.0.1 | 127.0.0.1 | TCP | 66 | 9999 → 32824 [ACK] Seq=1 Ack=688 Win=64896 Len=0 TSval=444965727 TSecr=444965727 |
| 0.001950652 | 127.0.0.1 | 127.0.0.1 | TCP | 630 | 9999 → 32824 [PSH, ACK] Seq=1 Ack=688 Win=65536 Len=564 TSval=444965729 TSecr=444965727 [TCP segment of a reassembled PDU] |
| 0.001967183 | 127.0.0.1 | 127.0.0.1 | TCP | 66 | 32824 → 9999 [ACK] Seq=688 Ack=565 Win=65024 Len=0 TSval=444965729 TSecr=444965729 |

מתבצעת השליחה ממטלה 2.

<u>תשובה לשאלה:</u> אנו צריכים הרשאת מנהל כל פעם שאנו רוצים לגשת לממשק ברשת, כיוון שרק promiscuous mode אנו יכולים להאזין promiscuous mode ורק במצב של מנהל יכול לגשת ל לפאקטות שלא מיועדות לנו ברשת.
המערכת תכשל בשורה:

```
handle = pcap_open_live("lo", BUFSIZ, 1, 1000, errbuf);
```

<u>היכולות והמגבלות של ה:sniffer</u>

הסניפר לוכד ומנתח פאקטות, בקוד שלנו אנו מסניפים TCP מנתח אותם ואז הוא צורב את הניתוח לתוך קובץ טקסט עם התז שלנו.
הסניפר יכול לנתח רק מה שנשלח בברטיס רשת שהוא מחובר אליו (אצלנו lo)
בנוסף הוא לא יכול לנתח תעבורה שהיא מוצפנת . (הסיבה היא שההצפנה נועדה למנוע גישה)

בס"ד

## Task B:

בחלק זה כתבנו את ה-spoofer.c בו זייפנו פאקטות ICMP.

<u>אופן ההרצה של Spoofer:</u>

נפתח טרמינל בתקייה בה נמצא הקוד ונריץ את הפקודות הבאות:

```
renana@renana: ~/Desktop/Ex5
renana@renana:~/Desktop/Ex5$ gcc Spoofer.c -o spoofer
renana@renana:~/Desktop/Ex5$ sudo ./spoofer
ICMP sended
renana@renana:~/Desktop/Ex5$
```

<u>הסבר על הקוד:</u>

בפונקציית הmain שלנו יש קריאה לפונקציה Icmp()

```c
int main() {

 icmp();
 printf("ICMP sended\n");

// udp();
// printf("UDP sended\n");

//  tcp();
//  printf("TCP sended\n");
return 0;
}
```

מטרתנו בקוד היא לזייף פאקטת ICMP ולכן נרצה לבנות ICMP header ולשנות בו את הip source

בתוך הפונקציה בשלב ראשון נמלא את הheader:

```c
/*********************************************************
    Step 1: Fill in the ICMP header.
*********************************************************/
struct icmpheader *icmp = (struct icmpheader *) (buffer + sizeof(struct ipheader));
icmp->icmp_type = 8; //ICMP Type: 8 is request, 0 is reply.

 // Calculate the checksum for integrity
icmp->icmp_chksum = 0;
icmp->icmp_chksum = in_cksum((unsigned short *)icmp,sizeof(struct icmpheader));
```

בשלב שני נמלא את IP header :

בס"ד

```
/*********************************************************
  Step 2: Fill in the IP header.
 *********************************************************/
struct ipheader *ip = (struct ipheader *) buffer;
ip->iph_ver = 4;
ip->iph_ihl = 5;
ip->iph_ttl = 20;
ip->iph_sourceip.s_addr = inet_addr("1.2.3.4");
ip->iph_destip.s_addr = inet_addr("10.0.2.15");
ip->iph_protocol = IPPROTO_ICMP;
ip->iph_len = htons(sizeof(struct ipheader) + sizeof(struct icmpheader));
```

לבסוף נשלח את הפאקטה המזויפת:

```
send_raw_ip_packet (ip);
```

הפונקציה in_cksum מחשבת Checksum עבור ICMP.
הפונקציה send_raw_ip_packet פותחת raw socket ושולחת את הפאקטה המזויפת.

<u>הקלטות wireshark:</u>

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 1.2.3.4 | 10.0.2.15 | ICMP | 44 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (reply in 2) |
| 2 | 0.000010070 | 10.0.2.15 | 1.2.3.4 | ICMP | 44 | Echo (ping) reply id=0x0000, seq=0/0, ttl=64 (request in 1) |

```
Checksum: 0xf7ff [correct]
[Checksum Status: Good]
```

<u>-> נשלח באופן תקין</u>

ניתן לראות כי הsource address הוא 1.2.3.4 המזוייף שאותו אנחנו הכנסנו.
כדי לראות שקיבלנו תגובה וולידית שמנו את הip של המחשב שלי 10.0.2.15, ניתן לראות כי נשלח ping בחזרה.

#ענינו על הדרישה שהקוד יעשה spoof לפאקטות אחרות עם שינויים קטנים, בכך שעשינו שתי פונקציות נוספות(udp(); tcp

<u>תשובה לשאלה 1:</u> כן אנחנו יכולים לשנות את הגודל של פאקטת הip לערך שרירותי כיוון שאורך פקאטת ה-IP משתנה לגודלו המקורי, ללא קשר לגודל שאנחנו קובעים.

<u>תשובה לשאלה 2:</u>
לא, אנו יוצרים socket ומבצעים bind , ואז השדות של הip header_לא משנים לנו, העיקר שאנו יכולים לתקשר עם השרת._ומערכת ההפעלה בונה את הפאקטה כולל הchecksum עם הנתונים שלנו.

<u>היכולות וההגבלות של הspoofer:</u>
המטרה של התוכנית היא לזייף את הפאקטות וה ip שלהם ברשת.
ה spoofer שלנו יכול לזייף פאקטות מסוג TCP UDP ICMP. הספופר מזייף אץ ה ip כך שזה יראה תגובה חוקית.
הספופר מוגבל בכך שהוא לא יוכל לעקוף אמצעי אבטחה , ואפשר לזהות אותו ברשת.

בס"ד

## Task C:

לחלק כזה כתבנו את הקוד Snooper שעושה sniff&spoof לICMP

<u>אופן ההרצה של Spoofer:</u>

פתחנו שלושה containerים בdocker attacker hostB hostA

```
Container hostA-10.9.0.5  Created
Container hostB-10.9.0.6  Created
Container seed-attacker   Created
```

בעוד שתי טרמינילים שונים הרצנו את hostA ואת attacker.
בחלק זה עשינו sniffing וברגע שהוא קיבל gotpacet נכנסנו לפונקציה בה עשינו הדפסות של src dst בשביל מעקב שלנו ובאותה פונקציה עשינו שליחה חוזרת לsrc ששלח את ההודעה(כלומר שליחה חוזרת למי ששלח את ההודעה, החלפנו בין ה srcל dst בשליחה).

<u>הרצה ראשונה: שליחת ping מHost A לHost B:</u>
נבחין בתמונה מעל כי הip של hostB הוא 10.9.0.6.

```
root@37ce81cad40a:/volumes# ./ping 10.9.0.6
ping 10.9.0.6: 19 data bytes
47 bytes from 10.9.0.6 icmp_seq= 0.ttl=64 RTT: 0.115000 milliseconds
28 bytes from 10.9.0.6 icmp_seq= 1.ttl=20 RTT: 0.111000 milliseconds
47 bytes from 10.9.0.6 icmp_seq= 2.ttl=64 RTT: 0.154000 milliseconds
28 bytes from 10.9.0.6 icmp_seq= 3.ttl=20 RTT: 0.173000 milliseconds
47 bytes from 10.9.0.6 icmp_seq= 4.ttl=64 RTT: 0.209000 milliseconds
28 bytes from 10.9.0.6 icmp_seq= 5.ttl=20 RTT: 0.096000 milliseconds
```

```
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 10.9.0.6
```

הרצנו את ה attacker ולאחר מכן הרצנו את hostA B והרצנו פינג מA לB
(הדפסנו את הip src dest של הפאקטה)

ran1hostb.pcapng

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

pply a display filter … <Ctrl-/>

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.000022386 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 1) |
| 3 | 1.000313052 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 4) |
| 4 | 1.000336395 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 3) |
| 5 | 2.002173170 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 6) |
| 6 | 2.002198700 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 5) |
| 7 | 3.007884208 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 3.007940217 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 7) |
| 9 | 4.008529772 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 10) |
| 10 | 4.008574082 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 9) |
| 11 | 5.009696285 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 12) |
| 12 | 5.009717069 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 11) |

רואים שהוא מקבל בקשה ומחזיר תגובה

בס"ד

run1hosta.pcapng

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ply a display filter … <Ctrl-/>

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| | 00000 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| | 56027 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 1) |
| 3 | 0.676494730 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 1.000312597 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 5) |
| 5 | 1.000365408 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 4) |
| 6 | 1.699976482 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 7 | 2.002160299 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 2.002227648 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 7) |
| 9 | 2.723922885 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 3.007849744 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11) |
| 11 | 3.007969224 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 10) |
| 12 | 3.747753874 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 13 | 4.008503790 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 14) |
| 14 | 4.008612873 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 13) |
| 15 | 4.772549139 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 16 | 5.009699413 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 17) |
| 17 | 5.009748445 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 16) |
| 18 | 5.796639714 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

כמו שציפנו אנו רואים כאן שהוא שולח בקשה ומקבל 2 תגובות אחת נ host B ואחת מattacker.

run1attacker.pcapng

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ply a display filter … <Ctrl-/>

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.000046791 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 1) |
| 3 | 0.676482221 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 1.000312597 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 5) |
| 5 | 1.000360800 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 4) |
| 6 | 1.699965263 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 7 | 2.002160299 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 2.002223105 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 7) |
| 9 | 2.723911215 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 3.007849744 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11) |
| 11 | 3.007964622 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 10) |
| 12 | 3.747738661 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 13 | 4.008503790 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 14) |
| 14 | 4.008598487 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 13) |
| 15 | 4.772536135 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 16 | 5.009699413 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 17) |
| 17 | 5.009741474 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 16) |
| 18 | 5.796626371 | 10.9.0.6 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

תוך כדי ההרצה פתחנו 3 ווירשארק כאשר אחד על ממשק של הattacker אחד של הhostA ואחד על hostB

ניתן לראות שיש שני reply זה נובע מכך שה attacker מתערב בשליחה של הפינגים .

<u>הרצה 2: מ hostA אל 8.8.8.8:</u>

נציין שבהרצה2 בממשק של hostB לא הוסנפו שום פאקטות כפי שציפנו .

```
root@37ce81cad40a:/volumes# ./ping 8.8.8.8
ping 8.8.8.8: 19 data bytes
47 bytes from 8.8.8.8 icmp_seq= 0.ttl=112 RTT: 18.240000 milliseconds
28 bytes from 8.8.8.8 icmp_seq= 1.ttl=20 RTT: 0.122000 milliseconds
47 bytes from 8.8.8.8 icmp_seq= 2.ttl=112 RTT: 0.164000 milliseconds
28 bytes from 8.8.8.8 icmp_seq= 3.ttl=20 RTT: 0.104000 milliseconds
```

run2attacker.pcapng

Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ly a display filter … <Ctrl-/>

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.018114223 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 1) |
| 3 | 0.759655426 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 1.029925774 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 5) |
| 5 | 1.045917116 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 4) |
| 6 | 1.782871448 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 7 | 2.035243867 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 2.051020049 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 7) |
| 9 | 2.807283963 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 3.036363473 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11) |
| 11 | 3.051654483 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 10) |
| 12 | 3.830582016 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 13 | 4.038018489 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 14) |
| 14 | 4.053219553 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 13) |
| 15 | 4.854788500 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

```
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 8.8.8.8
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 8.8.8.8
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 8.8.8.8
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 8.8.8.8
ash T PACKET
  Version: 4
  From: 10.9.0.5
    To: 8.8.8.8
```

בס"ד

run2hosta.pcapng

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

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.018125769 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 1) |
| 3 | 0.759075239 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 1.029925774 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 5) |
| 5 | 1.045934818 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 4) |
| 6 | 1.782879028 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 7 | 2.035243867 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 2.051036164 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 7) |
| 9 | 2.807292027 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 3.036363473 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 11) |
| 11 | 3.051683500 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 10) |
| 12 | 3.830592486 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 13 | 4.038018489 | 10.9.0.5 | 8.8.8.8 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 14) |
| 14 | 4.053238845 | 8.8.8.8 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=112 (request in 13) |
| 15 | 4.854833596 | 8.8.8.8 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

אפשר לראות שב hostA יש 2 reply כנראה מהתערבות של ה attacker.

הרצה 3: מ host A ל IP מזוייפת:

```
root@37ce81cad40a:/volumes# ./ping 1.2.3.4
ping 1.2.3.4: 19 data bytes
^C
root@37ce81cad40a:/volumes# ./ping 1.2.3.4
ping 1.2.3.4: 19 data bytes
28 bytes from 1.2.3.4 icmp_seq= 0.ttl=20 RTT: 157.419006 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 1.ttl=20 RTT: 29.155001 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 2.ttl=20 RTT: 18.056999 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 3.ttl=20 RTT: 18.761999 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 4.ttl=20 RTT: 18.634001 milliseconds
```

```
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 1.2.3.4
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 1.2.3.4
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 1.2.3.4
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 1.2.3.4
GOT PACKET
  Version: 4
  From: 10.9.0.5
    To: 1.2.3.4
```

run3attacker.pcapng

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

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 2 | 49.473711805 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 3 | 49.630838326 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 50.633139102 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 5 | 50.662139850 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 6 | 51.662531994 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 7 | 51.680306593 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 8 | 52.685258195 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 9 | 52.703833029 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 53.708142794 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 11 | 53.726678524 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

run3hosta.pcapng

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

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 2 | 49.473711805 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 3 | 49.630850950 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 4 | 50.633139102 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 5 | 50.662150656 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 6 | 51.662531994 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 7 | 51.680321581 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 8 | 52.685258195 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 9 | 52.703845568 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |
| 10 | 53.708142794 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 11 | 53.726691164 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) reply id=0x1200, seq=0/0, ttl=20 |

מה שעשינו הוא שהרצנו את hostA מבלי להריץ את ה attacker נשלח רק פינג אחד- ניתן לראות זאת בטרמינל שהוא נתקע עד שעשינו C^ וגם בשורה הראשונה שיש no response found
לאחר מכן הרצנו את ה attacker ושוב הרצנו פינג ואז רואים שהתקבל תשובה שמראה לנו שזה ה attacker שעונה.

בס"ד

## הרחבה לtask C:

כדי להראות שהתהליך שלנו באמת התבצע כראוי שנינו בקוד את ה srcכך:

```
struct ipheader *ip_attac = (struct ipheader *) buffer;
ip_attac->iph_v = 4;
ip_attac->ip_hl = 5;
ip_attac->ip_ttl = 20;
ip_attac->ip_src.s_addr = inet_addr("1.2.3.4");//(ip->ip_dst.s_addr);
ip_attac->ip_dst.s_addr = (ip->ip_src.s_addr);
ip_attac->ip_p = IPPROTO_ICMP;
ip_attac->ip_len = htons(sizeof(struct ipheader) +
                         sizeof(struct icmpheader));
```

הרצנו פינג מ host a לhost b

```
root@37ce81cad40a:/volumes# ./ping 10.9.0.6
ping 10.9.0.6: 19 data bytes
47 bytes from 10.9.0.6 icmp_seq= 0.ttl=64 RTT: 0.218000 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 1.ttl=20 RTT: 0.134000 milliseconds
28 bytes from 1.2.3.4 icmp_seq= 2.ttl=20 RTT: 0.194000 milliseconds
```

ניתן לראות בwireshark :

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.000117463 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 1) |
| 3 | 0.338175747 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 4 | 0.338301261 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 5 | 0.338324873 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 6 | 0.338376215 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 7 | 0.338406474 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 8 | 0.338431850 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 9 | 1.006537789 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 10) |
| 10 | 1.006596006 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 9) |
| 11 | 1.359974310 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 12 | 1.360024887 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 13 | 1.360046761 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 14 | 1.360101403 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 15 | 1.360142398 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 16 | 1.360173438 | 1.2.3.4 | 10.9.0.6 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 17 | 2.010225830 | 10.9.0.5 | 1.2.3.4 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (no response found!) |
| 18 | 2.382274883 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 19 | 2.382372545 | 1.2.3.4 | 10.9.0.5 | ICMP | 42 | Echo (ping) request id=0x0000, seq=0/0, ttl=20 (no response found!) |
| 20 | 5.038210391 | 02:42:0a:09:00:06 | 02:42:0a:09:00:05 | ARP | 42 | Who has 10.9.0.5? Tell 10.9.0.6 |
| 21 | 5.038225148 | 02:42:0a:09:00:05 | 02:42:0a:09:00:06 | ARP | 42 | Who has 10.9.0.6? Tell 10.9.0.5 |
| 22 | 5.038296192 | 02:42:0a:09:00:05 | 02:42:0a:09:00:06 | ARP | 42 | 10.9.0.5 is at 02:42:0a:09:00:05 |
| 23 | 5.038301457 | 02:42:0a:09:00:06 | 02:42:0a:09:00:05 | ARP | 42 | 10.9.0.6 is at 02:42:0a:09:00:06 |
| 24 | 5.549201995 | 02:42:8a:3d:78:02 | 02:42:0a:09:00:06 | ARP | 42 | Who has 10.9.0.6? Tell 10.9.0.1 |
| 25 | 5.549235934 | 02:42:8a:3d:78:02 | 02:42:0a:09:00:05 | ARP | 42 | Who has 10.9.0.5? Tell 10.9.0.1 |
| 26 | 5.549562850 | 02:42:0a:09:00:06 | 02:42:8a:3d:78:02 | ARP | 42 | 10.9.0.6 is at 02:42:0a:09:00:06 |
| 27 | 5.549568446 | 02:42:0a:09:00:05 | 02:42:8a:3d:78:02 | ARP | 42 | 10.9.0.5 is at 02:42:0a:09:00:05 |
| 28 | 7.085879328 | 02:42:0a:09:00:05 | 02:42:8a:3d:78:02 | ARP | 42 | Who has 10.9.0.1? Tell 10.9.0.5 |
| 29 | 7.085923197 | 02:42:8a:3d:78:02 | 02:42:0a:09:00:05 | ARP | 42 | 10.9.0.1 is at 02:42:8a:3d:78:02 |

ב1run אנחנו רואים הרבה פעמים שמתקבל no response found , מכוון שהhost a זיהה שהפונגים של attacker לא מתאימים לשלו מבחינה כלשהוא עד שהוא קיבל requestמתאים הגענו למסקנה זו מכוון שאנחנו יודעים ש attackerכן שולח פונגים לhost a ווידאנו זאת ע"י זה ש aatackerשלח פונגים מ1.2.3.4 uואכן רואים שנשלח ההודעות שלו.

נעשה הרצה של הפינג ללא ה:attacker

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0.000000000 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2) |
| 2 | 0.000098578 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 1) |
| 3 | 1.012406496 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 4) |
| 4 | 1.012452726 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 3) |
| 5 | 2.015189597 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 6) |
| 6 | 2.015249069 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 5) |
| 7 | 3.015846167 | 10.9.0.5 | 10.9.0.6 | ICMP | 61 | Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8) |
| 8 | 3.015876952 | 10.9.0.6 | 10.9.0.5 | ICMP | 61 | Echo (ping) reply id=0x1200, seq=0/0, ttl=64 (request in 7) |

ניתן לראות שכך הוא עובד כראוי שולח בקשה ומקבל תשובה , ניתן להבחין בכתובת של ההוסטים.

בס"ד

## Task D:

הסברים על הקוד נמצאים בתוך הקוד.

נציין שאצלנו הוא מאזין ל"0.0.0.0" אז הוא מאזין לכל הכתובות.

ניתן לראות שזה שולח כאשר rand>0.5

וכאשר rand<0.5 לא שולח

אצלנו ניתן לראות שנשלחו 4 פאקטות וזה תואם למה שרואים בווירשארק

```
renana@renana:~/Desktop/Ex5$ gcc Gateway.c -o gateway
renana@renana:~/Desktop/Ex5$ sudo ./gateway 127.0.0.7
in the main
host_ip 127.0.0.7
cerate host sock
cerate sock p
bind host sock
bind p sock
 enter to whileloop
receve
rand 0.840188
*******SEND**********
 enter to whileloop
receve
rand 0.394383
 enter to whileloop
receve
rand 0.783099
*******SEND**********
 enter to whileloop
receve
rand 0.798440
*******SEND**********
 enter to whileloop
receve
rand 0.911647
*******SEND**********
 enter to whileloop
receve
rand 0.197551
```

שלחנו לו פאקטות UDP בצורה הבאה-> אל port 8000 (P)

```
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$ echo -n example | nc -4u -w1 10.9.0.1 8000
renana@renana:~/Desktop/Ex5$
```

| | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 17 | 15.517076570 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 57789 → 8000 Len=7 |
| 18 | 15.517349153 | 127.0.0.7 | 10.0.2.15 | UDP | 51 | 8001 → 57789 Len=7 |
| 20 | 18.405347213 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 58371 → 8000 Len=7 |
| 25 | 28.433202145 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 60659 → 8000 Len=7 |
| 26 | 28.433354467 | 127.0.0.7 | 10.0.2.15 | UDP | 51 | 8001 → 60659 Len=7 |
| 28 | 30.241388777 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 36972 → 8000 Len=7 |
| 29 | 30.241527461 | 127.0.0.7 | 10.0.2.15 | UDP | 51 | 8001 → 36972 Len=7 |
| 51 | 32.225851325 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 53799 → 8000 Len=7 |
| 52 | 32.225951333 | 127.0.0.7 | 10.0.2.15 | UDP | 51 | 8001 → 53799 Len=7 |
| 54 | 34.599003784 | 10.0.2.15 | 10.9.0.1 | UDP | 51 | 44479 → 8000 Len=7 |

שורות -1 הרנדומלי

Dst Port: 8001

2: אנו יודעים לפי ההדפסה שעשינו בטרמינל כי המספר שהוגרל הוא 0.5<0.840188 ע

ל כן אנו נכנסים אל תוך הif ומעבירים את ה datagram לhost_sock שיושב על P+1. אכן:

שורה 3: עפ"י הטרמינל אנו יודעים כי המספר הרנדומלי שיצא הוא 0.5>0.3994383 כלומר לא מתבצעת שליחה ואכן אנו רואים כי בשורה הבאה הוא כבר עובר הלאה ולא שולח.

שורה 4: עפ"י הטרמינל rand=00.783099>0.5 כלומר

בס"ד

https://stackoverflow.com/questions/70449344/if-i-have-populated-all-fields-of-iphdr-then-how-to-calculate-the-tcphdr-doff-a

/https://www.opensourceforu.com/2015/03/a-guide-to-using-raw-sockets

https://stackoverflow.com/questions/11383497/libpcap-payload-offset-66-but-sizeofheaders-doff-62