שמות: אנטוני אסייה / אנא פינצוק **ת"ז**: 206431082 / 209971258

תקשורת ומחשוב - מטלה חמישית

חלק א' – myping :

בתקיה מצורף הקובץ **myping.c**, ההרצה של הקובץ בוצעה על ידי קימפול של של התוכנה עם קומפילר **GCC** והרצת הפקודה **Sudo**

```
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX4$ gcc icmp.c -o test3
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX4$ sudo ./test3
>> Reply ping from 129.134.31.12  with RTT: 44.000 millis.  / 44468.000 micros.
```

ניתן לראות בווירשארק את הפקטות **ICMP** הודעת **Echo (Ping) Request** והודעת **Echo (Ping) Reply**. בנוסף ב-**Header** של הודעת **ICMP Reply** ניתן לראות שהזמן שקיבלנו במילי שניות תואם עם הזמן של **RTT** שקיבלנו בטרמינל.

כפי שניתן לראות הסטטוס של ה- **Checksum** מחזיר **Correct**

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	129.134.31.12	ICMP	65	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 2)
2	0.044368197	129.134.31.12	10.0.2.15	ICMP	65	Echo (ping) reply id=0x1200, seq=0/0, ttl=54 (request in 1)

```
▸ Frame 2: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 129.134.31.12, Dst: 10.0.2.15
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xdce2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 4608 (0x1200)
    Identifier (LE): 18 (0x0012)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 1]
    [Response time: 44.368 ms]
  ▸ Data (21 bytes)
```

בצעינו כמה שינויים מהקוד המקורי:

- החלפת IPPROTO_RAW ב- **IPPROTO_ICMP**: socket (AF_INET, SOCK_RAW, IPPROTO_ICMP); , שורה 85
- מחיקה של ה- IP Header ובהתאם את הכתובת יעד עם כתובת של ה DNS של Facebook
- הוספת פונקציות **Sendto** ו- **recvfrom** שבעצם מאפשרות שליחה וקבלה הודעה ICMP על ידי הסוקט לכתובת היעד.
- פונקציה Checksum ללא שינויים, מלבד הורדה IP4_HDRLEN (מכיוון שמחקנו את 4IP)
- מדידת זמן של ה**RTT** בננו ומילי שניות.
-

חלק ב' – **Sniffing**

בתקיה מצורף הקובץ **sniffing.c**, השתמשתי בספרייה **PCAP**, הקובץ במאפשר לשימוש בספרייה זו **pcap.h** נמצא בתקיה **WpdPack**. ההרצה של הקובץ בוצעה על ידי קימפול של התוכנה עם קומפילר **GCC** והרצת הפקודה **sudo**

אתר שהשתמשנו בו: https://www.binarytides.com/packet-sniffer-code-c-libpcap-linux-sockets/

```
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ gcc sniffing.c -lpcap -o test3
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test3
 *************** PACKET SNIFFING ****************
   >> PROTOCOL: ICMP
  >> PACKET #0
  >> SRC_IP: 10.0.2.15
  >> DST_IP: 8.8.8.8
  >> TYPE: Request
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #1
  >> SRC_IP: 8.8.8.8
  >> DST_IP: 10.0.2.15
  >> TYPE: Reply
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #2
  >> SRC_IP: 10.0.2.15
  >> DST_IP: 8.8.8.8
  >> TYPE: Request
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #3
  >> SRC_IP: 8.8.8.8
  >> DST_IP: 10.0.2.15
  >> TYPE: Reply
  >> CODE: 0
```

הסניפר נותן הצגה של חלק מרכיבי ICMP Header :

1) הפרוטוקול שתמיד יהיה ICMP כי אנחנו מסננים רק פקטות של ICMP.
2) מספר הפקטה שהוא בעצם counter שמעלים ב1 .
3) כתובת IP מקור של ההודעה
4) כתובת IP יעד של ההודעה
5) סוג ההודעה: REPLY/REQUEST
6) קוד שהוא יהיה תמיד 0 אין שגעיות

ע"י הרצה בו זמנית של **myping.c** ששולח פינג ו-**sniffing.c** ניתן לראות בווירשארק את התעבורה של הפקטות שמתאום עם הכתובות **IP** של המקור ויעד, וגם עם הפרוטוקול.

icmp

No.	Time	Source	Destination	Protocol	Length	Info
5	5.977556108	10.0.2.15	129.134.31.12	ICMP	63	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 6)
6	6.021092672	129.134.31.12	10.0.2.15	ICMP	63	Echo (ping) reply id=0x1200, seq=0/0, ttl=54 (request in 5)
7	13.227906770	10.0.2.15	129.134.31.12	ICMP	63	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 8)
8	13.271690744	129.134.31.12	10.0.2.15	ICMP	63	Echo (ping) reply id=0x1200, seq=0/0, ttl=54 (request in 7)
9	15.391469351	10.0.2.15	129.134.31.12	ICMP	63	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 10)
10	15.435302733	129.134.31.12	10.0.2.15	ICMP	63	Echo (ping) reply id=0x1200, seq=0/0, ttl=54 (request in 9)
11	19.306088647	10.0.2.15	129.134.31.12	ICMP	63	Echo (ping) request id=0x1200, seq=0/0, ttl=64 (reply in 12)

```
▸ Frame 8: 63 bytes on wire (504 bits), 63 bytes captured (504 bits) on interface enp0s3, id 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_a7:77:d1 (08:00:27:a7:77:d1)
▾ Internet Protocol Version 4, Src: 129.134.31.12, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 49
    Identification: 0x340e (13326)
  ▸ Flags: 0x0000
    Fragment offset: 0
    Time to live: 54
    Protocol: ICMP (1)
    Header checksum: 0xa41d [validation disabled]
    [Header checksum status: Unverified]
    Source: 129.134.31.12
    Destination: 10.0.2.15
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xdce2 [correct]
    [Checksum Status: Good]
    Identifier (BE): 4608 (0x1200)
    Identifier (LE): 18 (0x0012)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Request frame: 7]
    [Response time: 43.784 ms]
  ▸ Data (21 bytes)
```

```
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ gcc sniffing.c -lpcap -o test3
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test3
 *************** PACKET SNIFFING ***************
   >> PROTOCOL: ICMP
  >> PACKET #0
  >> SRC_IP: 10.0.2.15
  >> DST_IP: 129.134.31.12
  >> TYPE: Request
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #1
  >> SRC_IP: 129.134.31.12
  >> DST_IP: 10.0.2.15
  >> TYPE: Reply
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #2
  >> SRC_IP: 10.0.2.15
  >> DST_IP: 129.134.31.12
  >> TYPE: Request
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #3
  >> SRC_IP: 129.134.31.12
  >> DST_IP: 10.0.2.15
  >> TYPE: Reply
  >> CODE: 0

  >> PROTOCOL: ICMP
  >> PACKET #4
  >> SRC_IP: 10.0.2.15
  >> DST_IP: 129.134.31.12
  >> TYPE: Request
  >> CODE: 0
```

```
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ gcc myping.c -o test2
anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test2
129.134.31.12
 >> Reply ping from 129.134.31.12  with RTT: 43.000 millis.  / 43620.000 micros.
 anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test2
129.134.31.12
 >> Reply ping from 129.134.31.12  with RTT: 43.000 millis.  / 43861.000 micros.
 anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test2
129.134.31.12
 >> Reply ping from 129.134.31.12  with RTT: 43.000 millis.  / 43998.000 micros.
 anthonyassayah@anthonyassayah-VirtualBox:~/Desktop/EX5$ sudo ./test2
129.134.31.12
 >> Reply ping from 129.134.31.12  with RTT: 43.000 millis.  / 43787.000 micros.
```