מטלה 6

Network programming

צוות הנדסת חסינות מידע

תאריך הגשה: 31.08.2023

יש לקמפל עם דגלים מקסימליים, לקבלת כל האזהרות: -Wall -ansi -pedantic . יש להגיש את קבצי המקור (.h, .c), קבצי ההרצה (את קבצי o. אין צורך לצרף), קבצי הסביבה המתאימים (כולל קבצי makefile), וכן קבצי קלט ותדפיסי מסך או קבצי פלט (לפי ההנחיות במטלה/במפגש/באתר). הקבצים של כל תוכנית יהיו בתיקיה נפרדת. נדרש ששם התיקיה ושם הקובץ לריצה יהיו כשם הקובץ המכיל את הפונקציה main, ללא הסיומת c.

יש להגיש תכניות מלאות (בין השאר מכילות main), הניתנות להידור והרצה, ומאפשרות בדיקה של כל התוצאות המגוונות של הריצה ללא צורך בשינויים כלשהם בקוד המקור של התוכנית.

שאלה 1 (תוכנית ראשית בקובץ my_sniffer.c)

עליכם לכתוב תוכנת סניפר אשר מטרתה תהיה להאזין לכל התעבורה שעוברת בכרטיס הרשת בו המחשב שלכם משתמש. התוכנה תהיה חיקוי מינימלי של wireshark

מבנה התוכנה

התוכנה תהיה בנויה סביב raw socket, שזהו socket מיוחד אשר בשונה משאר הסוקטים, אשר יושבים בשכבה 5-7, יושב על כרטיס הרשת בשכבה 2 ו"מעתיק" אליו כל חבילה אשר מגיעה לכרטיס הרשת, מבלי להפריע לתעבורה עצמה.

התוכנה תספק אפשרות התחלת האזנה, עצירת האזנה, ופירוט על כל חבילה שנתפסה

בעת התחלת האזנה:

- התוכנה תאזין לכל חבילה שהיא מסוג tcp udp או icmp ותציג סיכום שלה למסך על פי הפורמט
[id] (TCP/UDP/ICMP) packet from (sIP: sPORT) to (dIP: dPORT).

כאשר

- ID הוא מספר יחודי עולה הממספר את החבילה
- TCP/UDP/ICMP יהיה סוג ההודעה
- sIP: sPORT יהיה כתובת המקור של החבילה
- dIP: dPORT יהיה כתובת היעד של החבילה

בעת עצירת ההאזנה:

- התוכנה תעצור את ההדפסות למסך ותעצור את הsocket ותאפשר למשתמש להתחיל האזנה מחדש או להזין מספר חבילה לפירוט.

בעת הזנת מספר חבילה לפירוט:

- יופיע פירוט החבילה בהתאם לפורמט הבא:
  - חבילות UDP יוצגו כך:

```
*************************UDP Packet******************************
Ethernet Header
        |-Source Address        : 9C-2A-70-D8-50-ED
        |-Destination Address   : D0-67-E5-12-6F-8F
        |-Protocol              : 8

IP Header
        |-Version              : 4
        |-Internet Header Length  : 5 DWORDS or 20 Bytes
        |-Type Of Service   : 16
        |-Total Length      : 33  Bytes
        |-Identification    : 10201
        |-Time To Live      : 64
        |-Protocol          : 17
        |-Header Checksum   : 19134
        |-Source IP         : 10.240.253.53
        |-Destination IP    : 255.255.255.255

UDP Header
        |-Source Port           : 23451
        |-Destination Port      : 23452
        |-UDP Length            : 13
        |-UDP Checksum          : 0

Data
 AA  BB  CC  DD  EE  00  00  00  00  00  00  00  00  00  00  00
 00  00  00  00  00  00
*****************************************************************
```

- חבילות TCP יוצגו כך:

```
*************************TCP Packet******************************
Ethernet Header
        |-Source Address        : 9C-2A-70-D8-50-ED
        |-Destination Address   : 20-4E-7F-AD-BE-38
        |-Protocol              : 8

IP Header
        |-Version               : 4
        |-Inter Header Length   : 5 DWORDS or 20 Bytes
        |-Type Of Service    : 0
        |-Total Length       : 60  Bytes
        |-Identification     : 21505
        |-Time To Live       : 64
        |-Protocol           : 6
        |-Header Checksum    : 29540
        |-Source IP          : 10.240.253.53
        |-Destination IP     : 208.80.154.224

TCP Header
        |-Source Port           : 38555
        |-Destination Port      : 80
        |-Sequence Number       : 4210678548
        |-Acknowledge Number    : 0
        |-Header Length         : 10 DWORDS or 40 BYTES
        |----------Flags-----------
                |-Urgent Flag          : 0
                |-Acknowledgement Flag : 0
                |-Push Flag            : 0
                |-Reset Flag           : 0
                |-Synchronise Flag     : 1
                |-Finish Flag          : 0
        |-Window size           : 14600
        |-Checksum              : 29573
        |-Urgent Pointer        : 0

Data
 00  00  00  00  A0  02  39  08  73  85  00  00  02  04  05  B4
 04  02  08  0A  00  60  8F  15  00  00  00  00  01  03  03  06
*******************************************************************
```

אופן העבודה אל מול המשתמש יעשה באופן מיידי, כלומר:

- על מנת להתחיל להאזין הלקוח ילחץ על s (start)
- על מנת לעצור האזנה הלקוח ילחץ על k (kill)
- על מנת לפתוח חבילה לפירוט הלקוח ילחץ על i (inspect) ולאחר מכן תודפס לו הודעה ויאופשר לו להקליד מספר חבילה ו enter , בלחיצה על ESC הלקוח ייצא ממצב i ויוכל שוב ללחוץ על s ו k על מנת להתחיל ולעצור האזנה

בונוס: ניתן להוסיף שבעת לחיצה על d (dump) התוכנה תיצור קובץ שכותרתו "my_sniffer_(date)_(hour).txt" ותשמור אליו את כל החבילות שהקליטה, בצורה המפורטת שלהן.
ובעת לחיצה על e (erase) התוכנה תנקה את המסך ותמחק את החבילות שהקליטה עד כה.

בהצלחה!