שיעור 07 – הסנפה בסקאפי

Magshimshark

לאחר שבשבוע שעבר כתבנו את כלי ה-CMD מחדש, היום נכתוב את הגרסה שלנו לתוכנה האהובה (עמוק בתוכו אנחנו יודעים שאתם אוהבים אותה...) הלא היא Wireshark! במסגרת התרגיל נכתוב תוכנה שיודעת להסניף בכמה "מצבים" כאשר בכל אחד היא מדפיסה מידע אחר המעניין את המשתמש.

הסבר על הסניפר

לסניפר שלנו יש מספר מצבים שהוא פועל בהם. עבור כל מצב יש לכתוב פונקציית סינון ופונקציית עיבוד משלו. בפתיחת התוכנה יוצג בפני המשתמש תפריט עם הסוגים השונים של המצבים והוא יבחר את המצב שהוא רוצה לעבוד בו. לאחר מכן תתחיל הסנפה אינסופית, שבמהלכה יוצגו התוצאות למסך.

שימו לב:

- הדרך היחידה לעצור הסנפה אינסופית הוא באמצעות Ctrl+C. בכל פעם שהמשתמש ילחץ Ctrl+C, המשתמש יחזור לתפריט ההתחלה.
- בחירת אופציה 0 (אפס) תסיים את ריצת התוכנית (סעיף זה הינו סעיף רשות).
- חשבו איך אפשר להפעיל את המצב הנבחר מבלי ליצור if שיגדל עם כל הוספה של מצב (בצורה דומה לפתרון של פינק פלויד...).

מצב 1: הדפסת כתובות שחזרו משרת ה-DNS

1. הריצו הסנפה בעלת פילטר של תשובות DNS בלבד.
2. עבור כל חבילה יש להדפיס את 2 כתובות האתר (דומיין ו-IP) שחזרו בתשובה.
3. בדקו שהמצב עובד ע"י כניסה לאתרים חדשים שלא נכנסתם אליהם לאחרונה.

מצב 2: הדפסת תשובה משרת מזג האוויר

כתבו מצב בו התוכנה מזהה **תשובות שחזרו משרת מזג האוויר** ומדפיסה אותן. כדי לבדוק שמצב זה עובד, הפעילו את קליינט מזג האוויר. שימו לב, יש להדפיס רק תשובות בהן השרת שלח מידע על מזג אוויר, ולא את הודעת ה-Welcome שלו.

מצב 3: הדפסת כתובות GET

כתבו מצב בו התוכנה מזהה חבילות HTTP, ומדפיסה את כל כתובות ה-GET שהמחשב ניגש אליהן. כלומר החלק שבאדום: **GET /home/index/new.jpg HTTP/1.1**. בדקו שהמצב עובד ע"י גלישה באינטרנט (שימו לב שאתם לא גולשים ב-HTTPS).

בונוסים:

מצב 4: סריקת כתובות אימייל

כתבו מצב בו התוכנה מזהה חבילות HTTP, ומדפיסה כל כתובות אימייל שהתגלו בתוך הודעת ה-HTTP. ניתן לבדוק שמצב זה עובד ע"י ביצוע לוגאין (לחשבון שלא קיים) באתר groopy.co.il. מומלץ לעבוד עם חבילת re (Regular Expressions, שיעור בנושא תמצאו בחומרי ההעשרה של הקורס) כדי לגלות כתובות אימייל.

נספח – דוגמת הרצה

```
Welcome to Magshishark!
Please select sniffing state:
1. DNS
2. Forecast
3. HTTP
4. E-mails
Or select 0 to Exit: 1

cyber.org.il ===> 1.1.1.1
8200.org.il ===> 2.2.2.2

Please select sniffing state:
1. DNS
2. Forecast
3. HTTP
4. E-mails
Or select 0 to Exit: 2

200:ANSWER:date=28/05/2022&city=Eilat&temp=34.59&text=sky is clear
200:ANSWER:date=31/05/2022&city=London&temp=16.96&text=light rain

Please select sniffing state:
1. DNS
2. Forecast
3. HTTP
4. E-mails
Or select 0 to Exit: 3

/about.html
/
/check.png?1653667588542_10
/home/index/new.jpg

Please select sniffing state:
1. DNS
2. Forecast
3. HTTP
4. E-mails
Or select 0 to Exit: 4

ori@example.com
admin@nsa.gov.il

Please select sniffing state:
1. DNS
2. Forecast
3. HTTP
4. E-mails
Or select 0 to Exit: 0
```