

אריזת נתונים ולכידת מנות בעזרת Wireshark

קורס: תקשורת מחשבים
פרויקט גמר – ניתוח תעבורת פרוטוקול IP/TCP

1. מבוא

בחלק זה של הפרויקט הודגמה אריזת נתונים בשכבות IP/TCP, החל משכבה היישום ועד שכבת הרשת, תוך שימוש בקובץ הודעות, מחברת Jupyter ולכידת תעבורת בפועל באמצעות Wireshark

2. ייצרת קובץ CSV (שכבה היישום)

2.1 תיאור הקובץ

הוקן קובץ CSV המכיל הודעות בשכבה היישום של פרוטוקול צ'אט (CHAT).

שם הקובץ:
`groupXX_chat_input.csv`

2.2 שדות הקובץ

הקובץ כולל את השדות הבאים:

- `msg_id` – מזהה הודעה
- `app_protocol` – שם פרוטוקול היישום
- `src_app` – מקור ההודעה
- `dst_app` –יעד ההודעה
- `message` – תוכן ההודעה
- `timestamp` – חותמת זמן יחסית

2.3 אופן יצירת הקובץ

קובץ ההודעות נוצר ידנית על בסיס תרחיש תקשורת של מערכת צ'אט, במטרה ליצג הודעות טיפוסיות בשכבה ה夷ום בצורה מבוקרת ופושאה.

3. עיבוד הקובץ במחברת Jupyter

שם של הקובץ בפורמט ipynb : raw_tcp_ip_notebook_fallback_annotated-v1.ipynb

3.1 טיענת הקובץ

בשלב הראשון נטען קובץ ה-CSV למחברת Jupyter באמצעות Python, והנתונים עובדו למבנה טבלאי.

3.2 הדמיית אריזת נתונים

המחברת מדמה את תהליך אריזת ההודעה בשכבות:

- שכבה יישום – תוכן ההודעה
- שכבה תעבורה – הוספה כוורת TCP
- שכבה רשת – הוספה כוורת IP

3.3 יצירת תעבורה

בהמשך המחברת יוצרת מנוט רשות בהתאם להדמיה, כך שנitinן לילכוד אותן בזמן אמת באמצעות Wireshark.

4. לכידת תעבורה ב-Wireshark

4.1 תהליכי הלכידה

- הופעל Wireshark על ממוקם רשות פעיל
- הוגדר פילטר תעבורה מתאים
- המחברת הוריצה בזמן הלכידה
- קובץ הלכידה נשמר בפורמט .pcap

5. ניתוח המנות

5.1 מבנה המנה

ב-Wireshark ניתן לראות:

- שכבת Ethernet / Loopback
- שכבת IP – כתובות מקור ויעד
- שכבת TCP – פורטים, flags
- שכבת Data – תוכן הודעה

5.2 הסבר הממצאים

הניטוח מדגים כיצד הודעה משכבה היעומן נארצת וmovebraת ברשות, וכייז ניתן לצפות בכל שכבה בנפרד באמצעות Wireshark.

6. סיכום

ב חלק זה של הפרויקט הודגמה הבנה מעשית של אריזת נתונים בשכבות IP/TCP, עבודה עם קובץ קלט, עיבוד באמצעות Jupyter וליקידת תעבורת בפועל. השילוב בין סימולציה לליקידה אמיתי מאפשר הבנה עמוקה של תהליכי התקשרות ברשות.