

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 הודעה
- `dst_app` –יעד הודעה
- `message` – תוכן הודעה
- `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 ופומטת.

3. עיבוד הקובץ במחברת Jupyter

3.1 טעינת 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:

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

3.3 יצירת תעבורה

בהמשך המחברת יוצרת מנוט רשות בהתאם להדמיה, כך שניתן לכך 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:

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

5.2 הסבר הממצאים

הנition מדגים כיצד הודעה משכבה היישום נארצת וmoveרת ברשות, וכייז ניתן לצפות בכל שכבה בנפרד באמצעות Wireshark.

6. סיכום

בחלק זה של הפרויקט הוגדרה הבנה מעשית של ארכיטקטורת נתונים בשכבות IP/TCP, עבודה עם קובץ קלט, שימוש במערכות Jupyter וליידת תעבורת בפועל. השילוב בין סימולציה ללכידה אמיתי מאפשר הבנה עמוקה של תהליכי התקשרות ברשות.