**מסמך תרגיל ניתוח פרוטוקול למתרגל**

**מטרת התרגיל**

איתגור יכולת ניתוח הפרוטוקולים הרשתיים, היכרות עם דיסקציה של פקטות רשת, העמקה בשכבת הרשת הרביעית בדגש על UDP, היכרות עם חבילת הפייתון השימושית ביותר לעבודה עם פקטות רשת - Scapy.

**מבנה התרגיל**

בתרגיל החניכות מקבלות קבצי הסנפה בין שני צדדים, אשר מכילים התקשרות UDP בין שני הצדדים, אשר תחתיו עובר הפרוטוקול הייעודי אותו צריכות לזהות, לאבחן, ולפענח בתרגיל.

**הכנה לתרגיל למתרגל:**

* התקנה של scapy
* כתיבה של קבצי טקסט שרוצים שהחניכות בעצם ישחזרו בתרגיל (פה אפשר לתת את ה"צבע" לתרגיל לפי הצורך של הקורס).
* הרצה של 3 הסקריפטים, שמייצרים את 3 שלבי התרגיל.

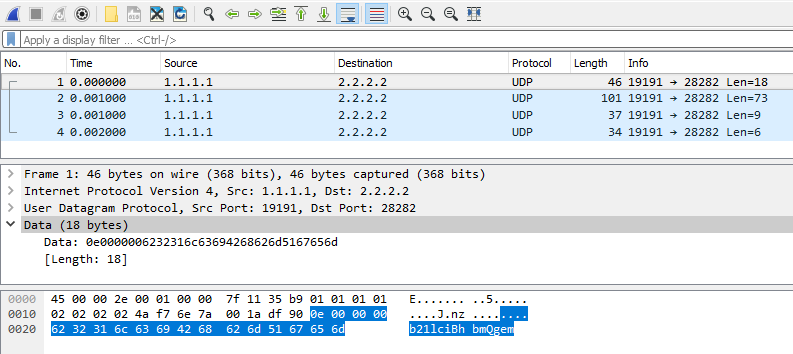
**הכנה לתרגיל לחניכות:**

* התקנה של scapy

התרגיל בנוי משלושה שלבים, ברמת קושי מתגברת:

**שלב ראשון**

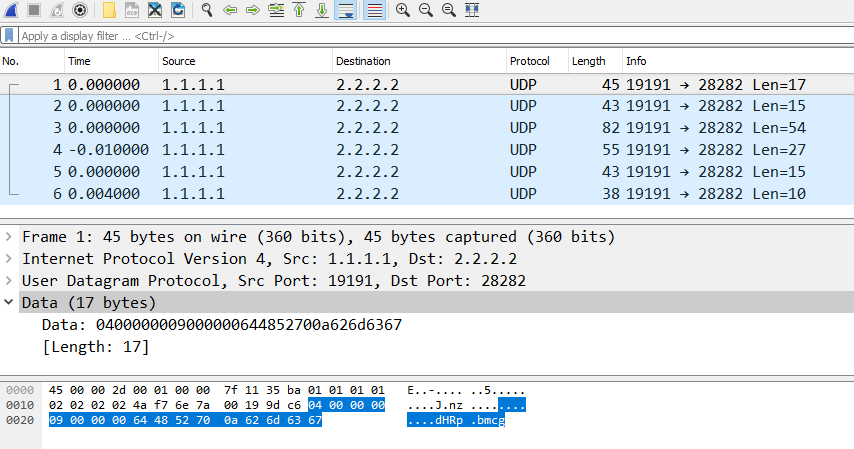
החניכות מקבלות הסנפה עם תקשורת חד צדדית, אשר בה פקטות UDP והפרוטוקול שעובר תחתיו הוא ייעודי בצורתו הפשוטה יותר - כל פקטה מורכבת משלושה חלקים - כל נתוני הפקטה המרכיבים אותה מעל לשכבת הUDP, ושכבת הפרוטוקול הייעודי, שמורכבת מבית המציג את מהגודל של הDATA בהודעה, והDATA עצמו, שהוא בצורת base64 של ההודעה העוברת בין הצדדים בתקשורת.



**שלב שני**

החניכות מקבלות הסנפה עם תקשורת חד צדדית, אשר בה פקטות UDP והפרוטוקול שעובר תחתיו הוא ייעודי בצורתו הפשוטה יותר - כל פקטה מורכבת מארבעה חלקים - כל נתוני הפקטה המרכיבים אותה מעל לשכבת הUDP, ושכבת הפרוטוקול הייעודי, שמורכב בית המציג את המספר הסידורי של הפקטה בתקשורת (מתחיל מ-1 ולא מ-0), מהגודל של הDATA בהודעה, והDATA עצמו, שהוא בצורת base64 של ההודעה העוברת בין הצדדים בתקשורת.

הקושי בשלב השני הוא שסדר הפקטות רנדומלי, ולכן החניכות צריכות לסדר מחדש את המידע בפקטות ולחבר את התוכן של הודעות הפרוטוקול (קטעי הDATA) בסדר הנכון כדי לקבל את ההודעה המקורית כאשר יעשו decode("base64").



**שלב שלישי**

החניכות מקבלות הסנפה עם תקשורת דו צדדית, אשר בה פקטות UDP והפרוטוקול שעובר תחתיו הוא ייעודי בצורתו הפשוטה יותר - כל פקטה מורכבת מארבעה חלקים - כל נתוני הפקטה המרכיבים אותה מעל לשכבת הUDP, ושכבת הפרוטוקול הייעודי, שמורכב בית המציג את המספר הסידורי של הפקטה בתקשורת (מתחיל מ-1 ולא מ-0), מהגודל של הDATA בהודעה, והDATA עצמו, שהוא בצורת base64 של ההודעה העוברת בין הצדדים בתקשורת.

הקושי בשלב זה הוא ניתוח ההסנפה כולה, והפרדה של התקשורת לשיחה בין שני צדדים, ולא לסטרים אחד של הודעות מצד אחד לאחר.

שימו לב: כרגע הסקריפט לא מייצר את ההודעות בסדר רנדומלי, כי הדגש על השלב הוא בטיפול בצדדי תקשורת, אך בשינוי קל ניתן שכל שליחה של פקטות תהיה בסדר רנדומלי כמו בשלב 2, צריך להחליף את השורה:

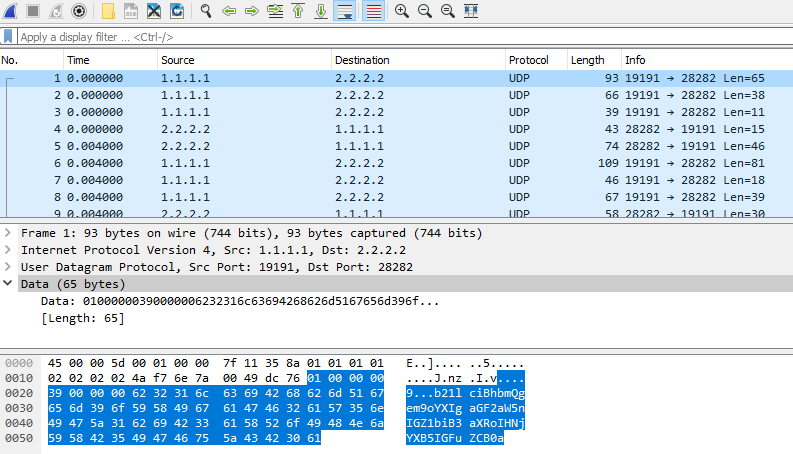
packets += create\_protocol\_data(data.encode("base64"), src\_ip, src\_port, dest\_ip, dest\_port)

בשורות:

message\_packets = create\_protocol\_data(data.encode("base64"), src\_ip, src\_port, dest\_ip, dest\_port)

shuffle(message\_packets)

packets += message\_packets



כדי לייצר כל שלב, רק צריך להכין מראש קובץ "שיחה", הבנוי משורות טקסט מופרדות בשורה חדשה רגילה.

בשלבים 1,2 הקובץ שיחה צריך להכיל רק שורה אחת, המתרגמת לקובץ הסנפה כפי המתואר.

בשלב 3 צריך להכין קובץ שיחה המכיל מספר שורות, כשכל שורה חדשה מחליפה בין הצדדים של התקשורת בקובץ ההסנפה.

את כל הסקריפטים מריצים באותו האופן, וכן ישנה הדפסה של usage אם מכניסים משתנים לא כנכון:

Usage: script.py <pcap\_output\_file> <text\_file>

**פתרון התרגיל:**

ישנן שתי דרכים לפתור את התרגיל לראייתנו, והן תלויות בצורה בה מעבירים אותו ולאן מכוונים את החניכות בו.

בשני הפתרונות מומלץ להשתמש גם במודול של struct בפייתון כדי לפרק את המידע הבינארי של הפקטות.

**שיטה 1 - פיתרון עם scapy**

סקאפי היא החבילה הפייתונית המועדפת לעבודה עם פקטות וניתוח ופיענוח של תעבורת פרוטוקולים, ולכן אנו ממליצים להנחות את החניכות לפתור את התרגיל בעזרתה. יחד עם הסקריפטים של התרגיל ישנו גם פיתרון בשימוש בסקאפי שמדגים למתרגל כיצד ניתן להשתמש בחבילה לניתוח של הקובץ הסנפה.

**שיטה 2 - פיתרון עם wireshark**

ניתן לפתור את התרגיל מבלי להשתמש בסקאפי כלל, אבל הדרך פחות מועדפת ודורשת עבודה עם הGUI של wireshark באופן שבעינינו מפספס את האתגר בתרגיל. בכל אופן אם בוחרים להנחות את החניכות לפתור את התרגיל באופן זה, ניתן לעבור בהסנפה פקטה פקטה, ולהעתיק את התוכן שלה לפייתון, ואז לפרק כל פקטה לפי הפרוטוקול של התרגיל.

