מגמת סייבר, רוטברג



# Transport layer – UDP הודעות סודיות

בתרגיל זה עליכם לסייע לשני תלמידים, גיל ומאור, לתקשר בצורה סודית מעל הרשת. מטרת התלמידים היא להצליח להעביר מסרים מאחד לשני, מבלי שאף אדם יוכל לקרוא אותם, גם אם הוא יכול להסניף את התעבורה ביניהם.

התלמידים החליטו על הפיתרון הבא: על מנת להעביר אות ביניהם, הם ישלחו הודעה ריקה למספר פורט שמסמל אותה, כשהסימול הוא לפי קידוד ASCII . לדוגמה ,נאמר שגיל רוצה לשלוח למאור את האות 'a'.

לשם כך, עליו ראשית להבין מה הערך ה-ASCII שלה. בכדי לעשות זאת, הוא יכול להשתמש בפונקציה ord של

פייתון:



כעת כשגיל גילה שערך ה-ASCII של האות 'a' הוא 97, הוא ישלח הודעת UDP ריקה לפורט 97 של מאור. במידה שגיל ירצה להעביר למאור את ההודעה "Hello", עליו יהיה לשלוח הודעה ריקה לפורט 72 (הערך של התו 'e'), שתי הודעות ריקות (הערך של התו 'e'), שתי הודעות ריקות לפורט 101 (הערך של התו 'o').

בתרגיל זה עליכם לממש את הסקריפטים בהם ישתמשו גיל ומאור בכדי להעביר מסרים זה לזה:

- כתבו סקריפט בשם scrt\_udp\_client.py. הסקריפט יבקש מהמשתמש להקליד הודעה, ולאחר מכן ישלח אותה אל השרת באופן סודי, כפי שתואר למעלה. את כתובת ה-IP של השרת אתם יכולים לכלול בקוד שלכם באופן קבוע ולא לבקש אותה מהמשתמש. השתמשו ב-Scapy בכדי לשלוח את החבילות.
- כתבו סקריפט בשם scrt\_udp\_server.py. הסקריפט ידפיס למסך מידע שהוא הבין כתוצאה משליחה. secret\_message\_client.py של הסקריפט של הסקריפט את החבילות.

מגמת סייבר, רוטברג

## הלקוח

- נקלוט מהמשתמש מחרוזת
- נעבור על המחרוזת בלולאה ועבור כל תו:
- ריקה UDP אליו נשלח הודעת port ס נחשב את ערך ה

port = ord(ch) # ch is character in the user input

ס נבנה את ההודעה ⊙

### תזכורת

כדי לבנות הודעה ב scapy נשתמש בבנאים של השכבות השונות ונפריד ביניהם עם האופרטור "/'

packet = IP(dst=DST\_IP) / UDP(sport=SRC\_PORT, dport=port)

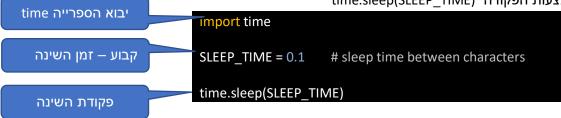
- נשלח את ההודעה

### תזכורת

send מתבצעת בעזרת פקודת scapy שליחת הודעה ב

- נסמן לשרת שסיימנו את השליחה ע"י שליחת תו מוסכם מראש למשל '-'
  - :♥ שימו לב

Scapy אינו עומד בקצב שידור גבוה מדי ועליכם לייבא את ה time module ו "לישון" בין אות לאות באמצעות הפקודה (time.sleep(SLEEP TIME)



# השרת

- שלתוכו נשמור כל אות שתגיע message נגדיר משתנה גלובאלי
- נגדיר פונקציית פילטר המזהה את ההודעות שלנו udp\_filter.

\_\_\_\_\_ איה 8. (packet[UDP].len) UDP בשכבת ה header הוא 8. כלומר גודל השדה len בשכבת ה UDP הוא 8.

נגדיר פונקציית prn כלומר פונקציה המבצעת פעולה על הפקטות שעברו add\_to\_message – סינון

הפונקציה תבדוק את ערך ה port תהפוך אותו ל ascii ותוסיף אותו למחרוזת.

c = packet[UDP].dport
ch = chr(c)
message += ch

- כעת משיש לנו את 2 הפעולות נגדיר לולאה שקוראת לפונקציה sniff עם count=1. כלומר, בכל פעם נסניף תו אחד. הלולאה תעצור כשיגיע התו המוסכם.
  - message לסיום נדפיס את

# בהצלחה