הגנה עבודה 7 אבטחת נתונים

לצורך ביצוע ההתקפה, התוקף שולח הודעה בלתי צפויה בשם הלקוח.

על מנת שהשרת "יחשוב" שהודעה הגיעה מהלקוח האמיתי צריך ש-6 שדות יוגדרו כהלכה:

1. כתובת מקור – הכתובת של הלקוח
2. כתובת יעד – הכתובת של השרת
3. שער מקור – השער של הלקוח
4. שער יעד – השער של השרת
5. מספר סידורי – מספר הבית הבא שיישלח ע"י הלקוח
6. מספר אישור – מספר אישור על הבית האחרון שנשלח ע"י השרת
7. דגל ACK

שלבים:

1. נפתח טרמינל ונכתוב: Sudo wireshark נרשום סיסמא 1234 ואנטר
הערה: התוכנה wireshark מאפשרת להקליט ולנתח הודעות שעוברות בתקשורת.
2. יפתח ה-wireshark, נלחץ על any
3. נפתח טרמינל נוסף אחר, ונרשום את הפקודה: telnet localhost
הערה: התוכנה telnetd היא שרת telnet שמאפשרת למשתמש מרוחק לבצע פקודות על המכונה.
נרשום שם משתמש user, סיסמא 1234 ואנטר. כדי לבדוק שהחיבור עובד ניתן לכתוב פקודות / אותיות ולראות ב-wireshark שישנם הודעות שמתווספות.
4. נסנן בשורת הסינון באמצעות: tcp.dstport==23 ונלחץ אנטר
5. ניקח את ההודעה האחרונה, נלחץ לחצן ימני => protocol preferences => לוודא שאין V על Relative sequence number, אם יש אז להסיר אותו.
6. נלחץ פעמיים על ההודעה האחרונה, ואז נלחץ על החץ של " Transmission control protocol"
7. נפתח טרמינל נוסף אחר.
נבצע nano 1.txt ושם נכתוב את הפקודה cp 1.txt 2.txt
8. נכתוב את הפקודה:

```
sudo hping3 -c 1 -p 23 -s 45270 -A -L 3109912034 -M 761998920 10.0.0.5 -E 1.txt -d
16
```

במקום 45270-> נשים את המספר של שער המקור
במקום 761998920-> נשים את המספר של המספר הסידורי הבא
במקום 3109912034 -> נשים את ה-Acknowledgement (ACK)

משמעות הפרמטרים:
- הפרמטר c קובע את מספר ההודעות לשידור
- **הפרמטר A קובע שיש להדליק את הדגל ACK בהודעות**
- הפרמטר p קובע את השער אליו נשלחות ההודעות
- הפרמטר s קובע את שער המקור
- הפרמטר M קובע את המספר הסידורי של ההודעה
- הפרמטר L קובע את מספר האישור
- **הפרמטר E מבקש לצרף בגוף ההודעה את תוכן הקובץ**

- הפרמטר d קובע את גודל גוף ההודעה

הערה: התוכנה hping3 מאפשר לשלוח הודעות TCP מלאכותיות.

9. נפתח את ה-wireshark ונראה כי התקבלה הודעה חדשה (ההודעה מהתוקף). אם נלחץ עליה פעמיים נוכל לראות למטה את התוכן של ההודעה (cp 1.txt 2.txt).

<u>למה בעצם פותחים קובץ 1.txt?</u>

באמצעות הפרמטר E- משתמשים בתוכן של הקובץ כדי למלא פקטת מידע שאותה התוקף בעצם ישלח לשרת בשם הלקוח.

ובאופן כללי, בפרוטוקול TCP, פקטות המידע הנשלחות זה בעצם קובץ שפורק לחבילות קטנות שנשלחות מקצה לקצה.

<u>מה ההבדל בין מטלה 6 ל-7?</u>

במטלה 6 אנחנו מנתקים את הקשר בין הלקוח לשרת באמצעות הפקודה hping ושם מוחזרת הודעת RST - הודעה הנשלחת מהתוקף, וגורמת לניתוק הקשר בין הלקוח לשרת.

לעומת זאת, **במטלה 7** אנחנו חוטפים את הקשר בין הלקוח לשרת. ההודעה המוחזרת לאחר הפקודה היא הודעה של התוקף (המתחזה ללקוח ושולח הודעות בשמו), וניתן לראות שתוכן ההודעה היא באמת התוכן של הקובץ טקסט שאותו שלח התוקף, כך ניתן לראות שההתקפה עבדה.