ניתוק קשר

<u>מבוא</u>

בתרגיל זה ננסה להבין:

1. מה היא התקפת ניתוק קשר?
2. איך לחולל התקפת ניתוק קשר?

<u>תיאור ההתקפה</u>

ניתוק הקשר בTCP מתבצע באמצעות אחד משני אופנים:

1. באופן מסודר, ע"י שליחת 4 הודעות:
    1. שליחת FIN ע"י יוזם הניתוק
    2. שליחת ACK ע"י הצד השני
    3. שליחת FIN ע"י הצד שני
    4. שליחת ACK ע"י הצד היוזם
2. באופן לא מסודר, ע"י שליחת RST ע"י היוזם

<u>ביצוע ההתקפה</u>

לצורך ביצוע ההתקפה, התוקף שולח הודעת RST בלתי צפויה שגורמת לניתוק הקשר בין הלקוח והשרת. על מנת שהשרת "יחשוב" שהודעת הRST 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 הערוץ הTCP
6. דגל RST

כדי לגלות את הערכים שיש לשים בשדות אלו, נשתמש בתוכנת Wireshark כדי להקליט ולנתח את התעבורה בין השרת והלקוח. ספציפית יש להסתכל על השדה Next sequence number (המספר הסידורי הבא) בהודעה האחרונה שנשלחה מהלקוח לשרת. יש לשים לב שהמספר שמוצג ע"י Wireshark הוא מספר יחסי ולא אבסולוטי. על מנת להציג מספר אבסולוטי, יש ללחוץ לחיצה ימנית על ההודעה, לבחור Protocol Preferences ולאחר מכן לוודא שלא מסומן V ב-Relative sequence number. בנוסף לשדה Next sequence number, נתעניין גם בשדה Source Port – שער מקור של הלקוח.

כדי לבצע את ההתקפה יש להתקין מספר תוכנות: sudo apt install hping3 telnetd wireshark
התוכנה telnetd היא שרת telnet שמאפשרת למשתמש מרוחק לבצע פקודות על המכונה.
התוכנה hping3 מאפשר לשלוח הודעות TCP מלאכותיות.
התוכנה wireshark מאפשרת להקליט ולנתח הודעות שעוברות בתקשורת.

ההתקפה תודגם על תקשורת עם שרת telnet. לצורך ההדגמה הרץ "telnet 10.0.0.15" (ללא הגרשיים), כאשר 10.0.0.15 היא כתובת הIP המקומית. הזן שם משתמש וסיסמא. הזן מספר פקודות לינוקס כדי לוודא שהתקשורת עובדת כהלכה. הפעל את wireshark והתחל הקלטה. כדי לצמצם את ההקלטה רק להודעות שנשלחות לשרת telnet הזן בשדה הסינון את המחרוזת "tcp.dstport==23" (ללא הגרשיים). הזן עוד מספר פקודות telnet וודא שמופיעות הודעות חדשות ב-wireshark. כעת בצע את ההתקפה כפי שמפורט להלן. נסה להזין עוד פקודות וודא שהתקשורת מתנתקת.

לביצוע ההתקפה הרץ את התוכנה hping3 באופן הבא:

```
sudo hping3 -c 1 -R -p 23 -s 56866 -M 804895780 10.0.0.15
```

כאשר במקום 10.0.0.5 יש לכתוב את כתובת הIP של המכונה המותקפת.
במקום 56866 יש לכתוב את שער המקור של הלקוח.
במקום 804895780 יש לכתוב את המספר הסידורי הבא.
משמעות הפרמטרים היא כדלקמן:

- הפרמטר c קובע את מספר ההודעות לשידור
- הפרמטר R קובע שיש להדליק את הדגל RST בהודעות
- הפרמטר p קובע את השער אליו נשלחות ההודעות
- הפרמטר s קובע את שער המקור
- הפרומטר M קובע את המספר הסידורי של ההודעה

יש להגיש את שורת ההרצה של hping3 וצילום מסך של wireshark בו נראית ההודעה התקינה האחרונה שנשלחה לשרת telnet והודעת ה-RST.