חטיפת קשר

מבוא

בתרגיל זה ננסה להבין:

1. מה היא התקפת חטיפת קשר?
2. איך לחולל התקפת חויפת קשר?

תיאור ההתקפה

בתקשורת TCP כל חבילה מכילה, בין השאר, מספר סידורי ומספר אישור. כל חבילה שתישלח עם מספר תקינים בשדות אלו, תטופל כאילו הגיעה מהלקוח האמיתי.

ביצוע ההתקפה

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

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 ובשדה Acknowledgement Number.

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 צור קובץ בשם 1 עם סיומת txt והזן בו את הפקודה הבאה

```
cp 1.txt 2.txt
```

לחץ על enter ושמור. התו מעבר שורה הוא זה שיגיד ל-telnet להריץ אותה.
לביצוע ההתקפה הרץ את התוכנה hping3 באופן הבא:

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

כאשר במקום 10.0.0.5 יש לכתוב את כתובת הIP של המכונה המותקפת.
במקום 45270 יש לכתוב את שער המקור של הלקוח.
במקום 761998920 יש לכתוב את המספר הסידורי הבא.
במקום 3109912034 יש לכתוב את מספר האישור.
משמעות הפרמטרים היא כדלקמן:

- 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
- הפרומטר 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

יש להגיש את שורת ההרצה של hping3 וצילום מסך של wireshark בו נראית ההודעה התקינה האחרונה שנשלחה לשרת telnet, ההודעה שנשלחה ע"י hping3 ותיקיה בה מופיע הקובץ 2 עם סיומת txt.