אבטחת נתונים - עבודה 6 להגנה

תיאור ההתקפה

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

ביצוע ההתקפה

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

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, נכתוב את הפקודה:

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

במקום 56866 -> נשים את המספר של שער המקור
במקום 804895780 -> נשים את המספר של המספר הסידורי הבא
הערה: התוכנה hping3 מאפשר לשלוח הודעות TCP מלאכותיות.

8. נעשה אנטר, ואז תקפוץ באדום ב-wireshark הודעת RST -> הודעה זו נשלחת מהתוקף, וגורמת לניתוק הקשר בין הלקוח לשרת.
9. על-מנת לוודא את הניתוק, נסתכל בטרמינל שבו ביצענו telnet localhost ננסה לכתוב הודעה וישר יקפוץ לנו "Connection closed..." מה שמעיד שאכן הודעת ה-RST גרמה לניתוק הקשר בין הלקוח לשרת.

משמעות הפרמטרים:

- 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
- הפרמטר M קובע את המספר הסידורי של ההודעה