אבטחת נתונים – עבודה 5

מגישות:

צליל לוי – 206796088

לינוי אסלן – 313279036

שאלות הבנה:

1. האם ניתן להתחבר באמצעות telnet בזמן ביצוע ההתקפה? למה?

לא. לא ניתן להתחבר באמצעות telnet בזמן ביצוע ההתקפה:

```
user@infosec:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection timed out
```

וזאת מהסיבה, שבמסגרת ההתקפה, התוקף שולח ללא הרף הודעות SYN לשרת. השרת מגיב ב-SYN+ACK, אך התוקף לא שולח את ה ACK שאמור להישלח. בשביל החיבור צריך להקצות מבני נתונים אצל השרת, וישנה כמות מוגבלת של מבנים כאלו שניתן לפתוח, כתוצאה מההתקפה מצטברים בשרת מבני נתונים עד אשר לא ניתן עוד להקצות מבני נתונים חדשים. בשלב זה, לא ניתן להתחבר לשרת בתקשורת TCP, כלומר אצלנו לא ניתן להתחבר באמצעות telnet המדמה תקשורת של שרת ולקוח כשעושים חיבור TCP, כי לא ניתן להקצות מבנה נתונים להתחברות שלו.

2. האם ניתן להשתמש בחיבור telnet שנפתח לפני תחילת ההתקפה? למה?

כן. ניתן להשתמש בחיבור telnet שנפתח לפני תחילת ההתקפה:

```
user@infosec:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
infosec login:
```

מהסיבה, שניתן להקצות מבנה נתונים להתחברות שלו, שהרי אין הצפת SYN.

3. וידוא שההתקפה לא יעילה כאשר מנגנון ההגנה של LINUX מופעל:

```
user@infosec:~$ sudo sysctl -w net.ipv4.tcp_syncookies=1
[sudo] password for user:
net.ipv4.tcp_syncookies = 1
```

```
user@infosec:~$ sudo hping3 -c 15000 -S -p 23 --flood --rand-source localhost
HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
user@infosec:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Ubuntu 18.04.4 LTS
infosec login:
```

ניתן לראות שכאשר מנגנון ההגנה פועל, ואנחנו מבצעים הצפת SYN, אז כן ניתן לבצע חיבור telnet, כלומר, ניתן להקצות מבנה נתונים על-מנת לבצע חיבור מה שמעיד על כך שההתקפה לא יעילה כאשר מנגנון ההגנה מופעל.