

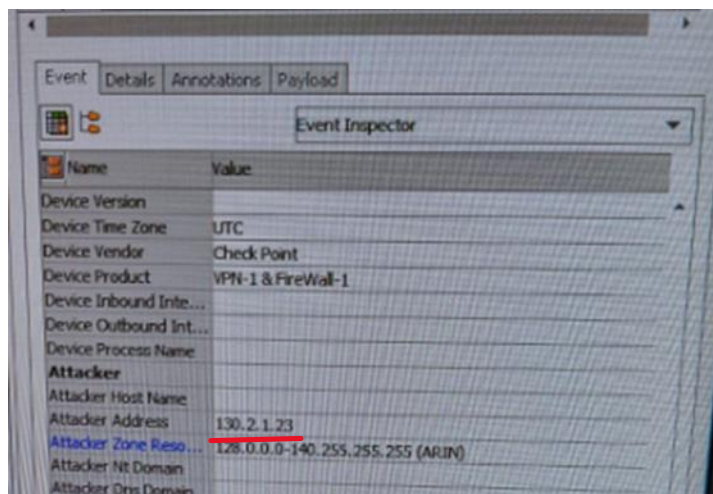
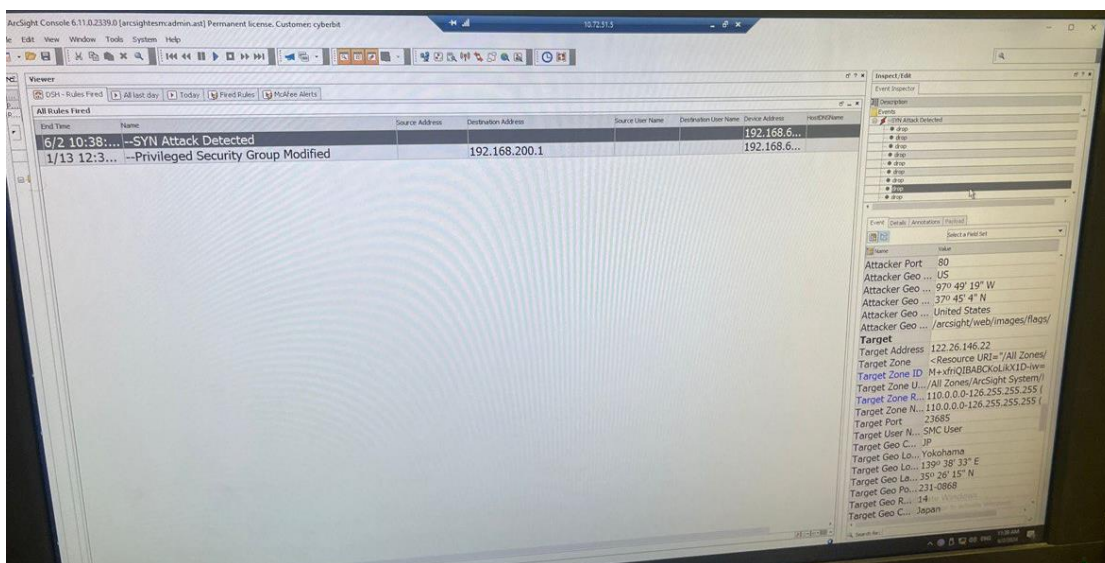
דו"ח תרחיש- SYN Flood

1. לוגיסטיקה:

- A. שם מלא: אליהו פרידמן
- B. תעודת זהות: 211691159
- C. שם התרחיש: SYN Flood

2. תהליך זיהוי התקיפה:

בשעה 10:38 התקבלה התראה במערכת ArcSight על SYN Attack Detected. לאחר בדיקה השרת הנתקף הוא Apache3 (מכונה 130.2.1.23 שהיא 172.16.100.23 מאחורי ה-NAT).



בתמונה ניתן לראות את המכונה שנתקפה 130.2.1.23 שהיא 172.16.100.23 מאחורי ה-NAT. ב-Zenoss לא היה שום דבר חריג.

בשלב הבא, עברנו לבדוק את ה-Firewall שם זיהינו כי אחוזי ה-CPU גבוהים מאוד. ראינו המון חבילות SYN שנשלחות לכיוון השרת Apache3-CNT-DMZ בכתובת 172.16.100.23 (NAT)

Status	Name	IP	Vers...	Active Blades	Hardware	CPU Usage	Recommended Updates	Comments
✓	CNT-QM2-FW	192.168.254.242	R80.10	🔧	Open server	84%	N/A	
✓	CNT-FW	192.168.110.254	R80.10	🔧	Open server	93%	N/A	

כאשר בדקנו את הכתובת www.cnn.com (הכתובת של האתר) וגם עם כתובת ה-IP בעזרת פקודת 'nslookup' ניתן לראות כי ה-DNS לא פועל כראוי (קיבלנו time out)

```
Administrator: Command Prompt
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\trainee005>nslookup www.cnn.com
Server: UnKnown
Address: 10.72.53.10

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out

C:\Users\trainee005>nslookup 172.16.100.23
Server: UnKnown
Address: 10.72.53.10

DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
```

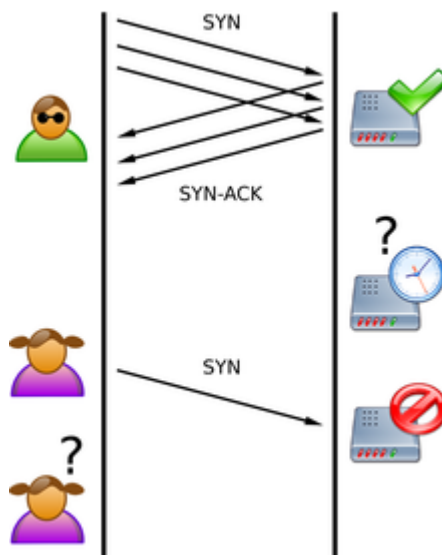
בכדי לוודא את המידע, התחברנו למכונה של Apache3 באמצעות SSH Client עם PuTTY, זאת מכיוון ששרתים אלו מבוססי Linux/GNU.

כאשר ביצענו את הפקודה netstat -tunap, זיהינו שהשרת מופץ בבקשות TCP-SYN רבות מכתובות רבות ושונות. כל אחת מהבקשות האלה הייתה תקועה במצב SYN_RECV, כלומר השרת חיכה להשלמת החיבור אך התשובה לא הגיעה מה שגורם להאטה משמעותית. בתמונה ניתן לראות את הרצאת פקודת netstat -tunap.

tcp	0	0	172.16.100.23:80	209.24.46.60:21661	SYN_RECV
tcp	0	0	172.16.100.23:80	209.24.46.60:14598	SYN_RECV
tcp	0	0	172.16.100.23:80	22.99.16.226:51446	SYN_RECV
tcp	0	0	172.16.100.23:80	22.99.16.226:13024	SYN_RECV
tcp	0	0	172.16.100.23:80	148.253.92.179:53761	SYN_RECV
tcp	0	0	172.16.100.23:80	122.26.146.22:35143	SYN_RECV
tcp	0	0	172.16.100.23:80	200.194.57.145:22395	SYN_RECV
tcp	0	0	172.16.100.23:80	122.26.146.22:23865	SYN_RECV
tcp	0	0	172.16.100.23:80	122.26.146.22:16094	SYN_RECV
tcp	0	0	172.16.100.23:80	49.189.122.94:14133	SYN_RECV
tcp	0	0	172.16.100.23:80	4.124.35.80:28596	SYN_RECV
tcp	0	0	172.16.100.23:80	162.79.214.195:19013	SYN_RECV
tcp	0	0	172.16.100.23:80	94.145.179.142:32015	SYN_RECV
tcp	0	0	172.16.100.23:80	158.201.199.31:34957	SYN_RECV
tcp	0	0	172.16.100.23:80	209.24.46.60:13007	SYN_RECV
tcp	0	0	172.16.100.23:80	97.19.100.125:28298	SYN_RECV
tcp	0	0	172.16.100.23:80	170.22.165.161:21902	SYN_RECV
tcp	0	0	172.16.100.23:80	231.20.86.160:27917	SYN_RECV
tcp	0	0	172.16.100.23:80	40.32.153.186:54130	SYN_RECV
tcp	0	0	172.16.100.23:80	200.194.57.145:30815	SYN_RECV
tcp	0	0	172.16.100.23:80	34.68.100.131:12769	SYN_RECV
tcp	0	0	172.16.100.23:80	200.104.176.117:28013	SYN_RECV
tcp	0	0	172.16.100.23:80	159.64.37.54:18200	SYN_RECV
tcp	0	0	172.16.100.23:80	155.17.92.99:30131	SYN_RECV
tcp	0	0	172.16.100.23:80	125.117.153.166:15896	SYN_RECV
tcp	0	0	172.16.100.23:80	132.31.223.156:22861	SYN_RECV
tcp	0	0	172.16.100.23:80	158.201.199.31:23123	SYN_RECV
tcp	0	0	172.16.100.23:80	223.122.178.223:21945	SYN_RECV
tcp	0	0	172.16.100.23:80	122.26.146.22:25089	SYN_RECV
tcp	0	0	172.16.100.23:80	190.25.156.97:15924	SYN_RECV
tcp	0	0	172.16.100.23:80	217.79.188.238:15141	SYN_RECV

לאחר מכן, ניסינו לזהות את מקור החבילות.
ביצענו ping לכמה כתובות IP אך לא קיבלנו תשובה. מכאן הסקנו שהכתובות מזויפות.
בזכות כל הצעדים האלה, הצלחנו לזהות בבירור שמדובר בהתקפת SYN Flood ושמכונת ה-Apache3 הייתה היעד להתקפה זו.

מצ"ב איור שמדמה את התקיפה.



3. פירוק ווקטור התקיפה לשלבים לפי [MITRE](#):
 - A. [Reconnaissance](#): אין. התוקף לא אסף מידע על המכונה לפני התקיפה. לא זוהתה שום פעילות מקדימה שמצביעה על סיור או איסוף מידע.
 - B. [Resource Development](#): התוקף השתמש בכתובות IP מזויפות ובכלים או סקריפטים ייעודיים ליצירת עומס על השרת באמצעות שליחת בקשות SYN רבות. אך לא יצר משאבים בשביל התקיפה.
 - C. [Initial Access](#): אין. התוקף לא נכנס לשרת.
 - D. [Execution](#): התוקף שלח מספר רב של בקשות TCP-SYN לשרת המותקף (Apache3), על מנת לגרום לעומס על השרת. על ידי שליחת מספר רב של בקשות הוא מונע גישה לשירותי המכונה. אך לא הייתה הרצת קוד זדוני במכונה.
 - E. [Persistence](#): התוקף לא שמר על גישה מתמשכת למכונה כיוון שלא הייתה חדירה מלכתחילה.
 - F. [Privilege Escalation](#): התוקף לא ניסה להשיג הרשאות גבוהות יותר, הוא לא נכנס למכונה כלל.
 - G. [Defense Evasion](#): ישנה אפשרות שהתוקף השתמש בכתובות IP שונות (כנראה מזויפות) כדי להקשות על זיהוי המקור האמיתי של התקיפה.
 - H. [Credential Access](#): התוקף לא ניסה לגנוב שמות משתמשים וסיסמאות.
 - I. [Discovery](#): התוקף לא ניסה לגלות מידע נוסף על השרת הפנימית של הארגון.
 - J. [Lateral Movement](#): התוקף לא נע ברשת הארגונית כיוון שלא הייתה חדירה ראשונית למכונה.
 - K. [Collection](#): התוקף לא ניסה לאסוף מידע רלוונטי מהמכונה.
 - L. [Command and Control](#): התוקף לא תקשר עם מערכות שנפגעו. כל הפעולות בוצעו מרחוק.
 - M. [Exfiltration](#): התוקף לא ניסה להוציא מידע מחוץ לשרת.
 - N. [Impact](#): התקפת ה-SYN Flood גרמה לעומס על השרת, מה שהאט את פעולתו ומנע גישה למשתמשים לגיטימיים.

4. מידע תקשורתי:
התקיפה הכילה תעבורת רשת רבה כמו שניתן לראות בהקלטת הוירשארק.
התקיפה כללה שימוש בפרוטוקול TCP.
ניתן לראות שליחת בקשה לפתיחת קשר (SYN) ותשובה חזרה של המכונה (SYN ACK), כמו כן
ניתן לראות שאין "לחיצת ידיים משולשת".
בכך מנסה התוקף לגרום להצפת המכונה בבקשות ובאמצעות זאת למנוע גישה לאתר.

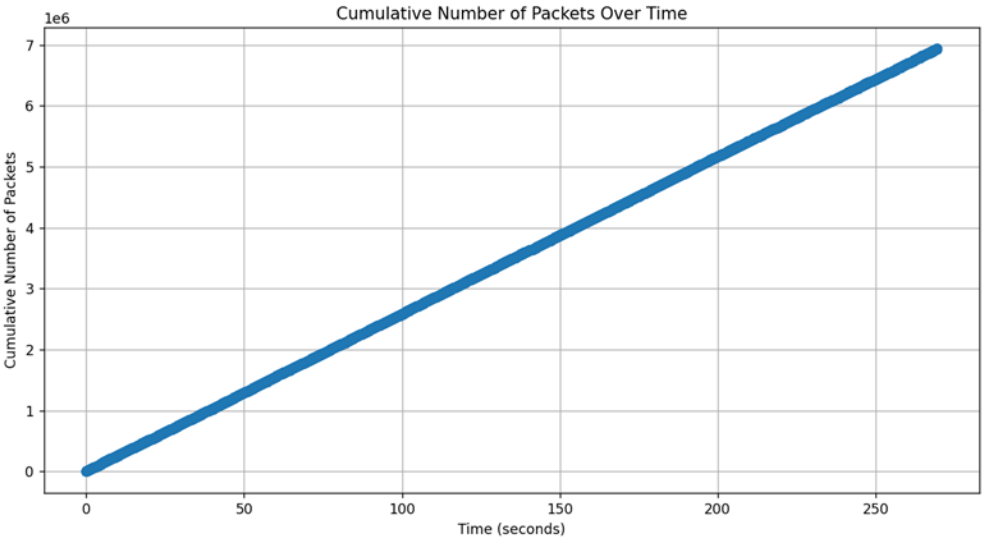
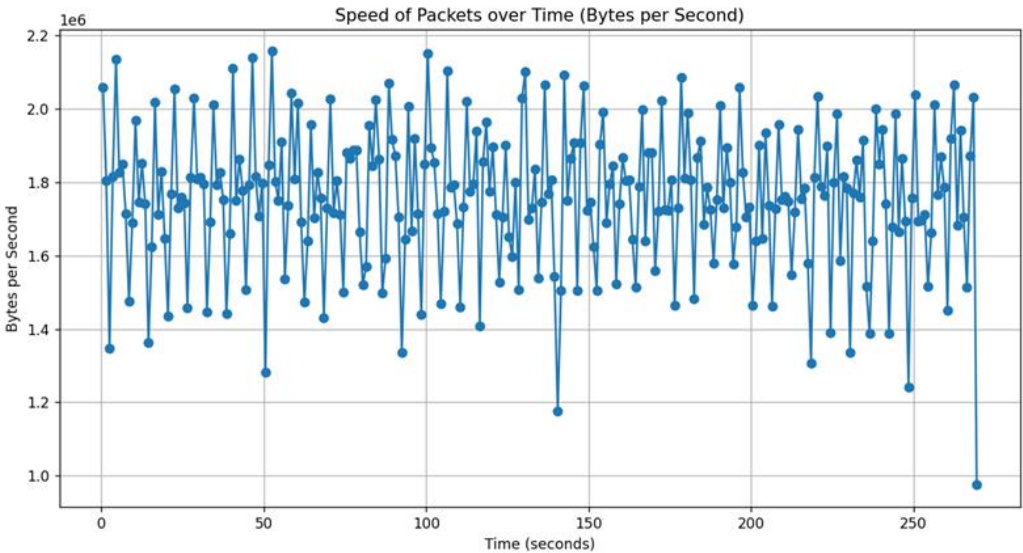
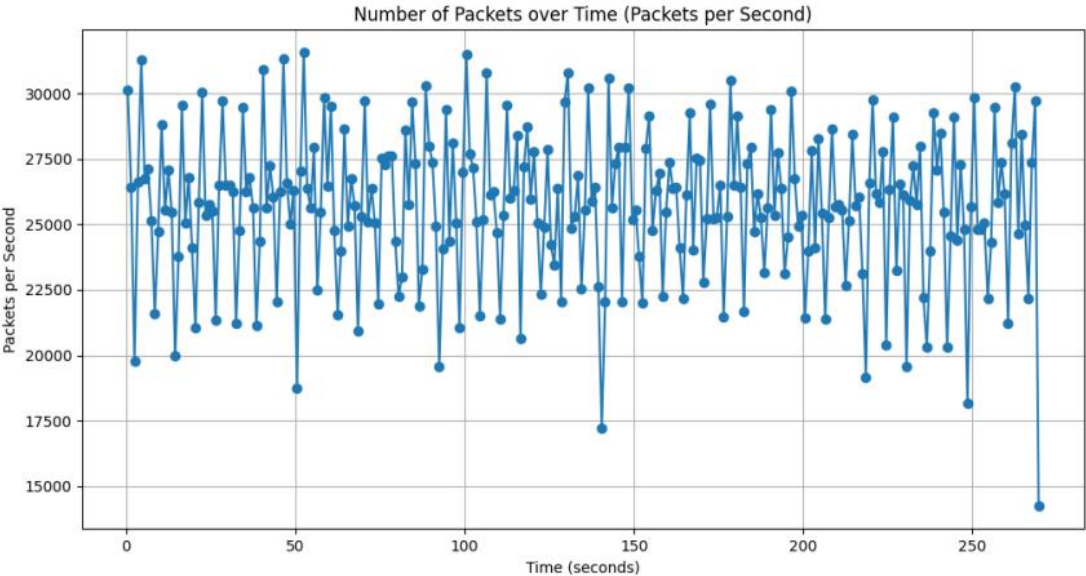
A. פרטי חבילות:

No	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.134.57.145	172.16.100.23	TCP	80	Seq=0 Win=4096 Len=0 MSS=1430 SACK_PERM TSval=1840537518 TSecr=0 WS=1 [SYN] 80 → 20204 74
2	0.000007	172.16.100.23	200.134.57.145	TCP	80	20204 → 80 74 [SYN, ACK] 20204 → 80 74
3	0.000009	49.159.122.54	172.16.100.23	TCP	80	Seq=0 Win=4096 Len=0 MSS=1460 WS=1 TSval=7670306 TSecr=0 [SYN] 80 → 19668 74
4	0.000011	172.16.100.23	49.159.122.54	TCP	80	19668 → 80 74 [SYN, ACK] 19668 → 80 74
5	0.000012	70.165.135.67	172.16.100.23	TCP	80	Seq=0 Win=4096 Len=0 MSS=1460 WS=4 SACK_PERM [SYN] 80 → 23930 66
6	0.000014	172.16.100.23	70.165.135.67	TCP	80	23930 → 80 58 [SYN, ACK] 23930 → 80 58

B. מהירות שליחת החבילות: 6,941,940 חבילות במשך 269.469 שניות, כלומר במוצע 25761.55 חבילות בשנייה.

Wireshark - Capture File Properties - syn_flood_filtered.pcap				
Details				
File				
Name:	C:\Users\innbj\OneDrive\סייבר\עבודה\לימודים\מעבדת סייבר\SYN Flood\pcap\syn_flood_filtered.pcap			
Length:	585 MB			
Hash (SHA256):	ef4e5a9ff0cc74d37b270d21a3e2322b474cb54bae765f288f9eb32b3704ac9a			
Hash (SHA1):	c1d49e088f1f901dffa277345d1b279c328ad70			
Format:	Wireshark/tcpdump/... - pcap			
Encapsulation:	Ethernet			
Snapshot length:	96			
Time				
First packet:	2024-06-14 20:12:01			
Last packet:	2024-06-14 20:16:30			
Elapsed:	00:04:29			
Capture				
Hardware:	Unknown			
OS:	Unknown			
Application:	Unknown			
Interfaces				
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	96 bytes
Statistics				
Measurement	Captured	Displayed	Marked	
Packets	6941940	6941940 (100.0%)	—	
Time span, s	269.469	269.469	—	
Average pps	25761.6	25761.6	—	
Average packet size, B	68	68	—	
Bytes	474230882	474230882 (100.0%)	0	
Average bytes/s	1759 k	1759 k	—	
Average bits/s	14 M	14 M	—	

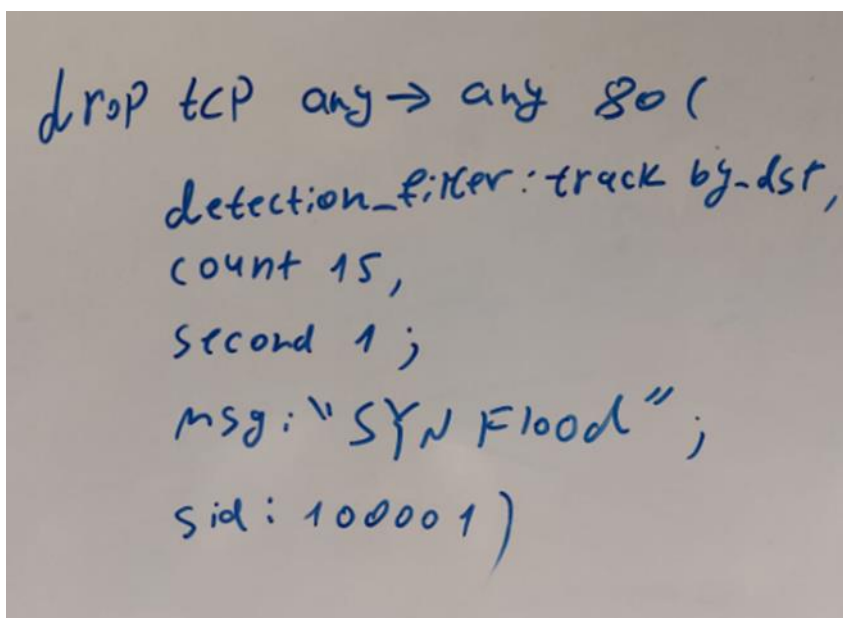
C. גרפים לתיאור התקשורת:



D. סטטיסטיקות נוספות :
גודל חבילה ממוצע : 68 bytes
זמן ממוצע בין כל חבילה : 0.000039 microseconds

5. פעולות לוקאליות :
A. המשתמש שדרכו נכנס התוקף : התוקף לא חדר למכונות או משתמשים בארגון, אלא שלח כמות גדולה של בקשות לפתיחת קשר TCP למכונת Apache3 .
B. קבצים שנפגעו/שונו/הועתקו/הושטלו : אין.

6. הגנה :
A. הגנה ראשונית :
התחברות ל IDS והוספת חוק ל-Snort שיעצור את ההתקפה על ידי זיהוי וזריקת חבילות TCP-SYN שמגיעות בקצב גבוה.
לאחר מכן נתחבר ל-Snort ע"י SSH Client באמצעות PuTTY. נכנס לקובץ locals.rules ונוסיף את הכלל המצורף בתמונה :



```
drop tcp any -> any 80 (
  detection_filter: track by-dst,
  count 15,
  second 1 ;
  msg: "SYN Flood";
  sid: 100001)
```

כלומר, אם מגיעות מעל 15 פקטות TCP לפורט 80 לאותה המכונה בשנייה, תזרוק את החבילות ותרשום הודעת שגיאה SYN Flood. לאחר מכן נאתחל את המכונה.

B. הגנה מניעתית :
בין הפעולות שיש לעשות על מנת למנוע התקפות כאלה בעתיד הן הוספת כלל ל-Snort שמונעת התקפות מסוג זה בעתיד. הוספת חוק זה תמנע את התקפות ה-SYN Flood בעתיד על ידי הגבלת כמות החבילות שמגיעות לפורט מסוים.

7. הערות נוספות :
A. אופן עבודת הצוות : התנהלות הייתה טובה ודינמיקה קבוצתית הייתה מצוינת.
B. מגבלות העבודה : לא היו פערים.