

דו"ח תרחיש - DNS Amplification

1. לוגיסטיקה:
 - A. שם מלא: אליהו פרידמן
 - B. תעודת זהות: 211691159
 - C. שם התרחיש: DNS Amplification

2. תהליך זיהוי התקיפה:

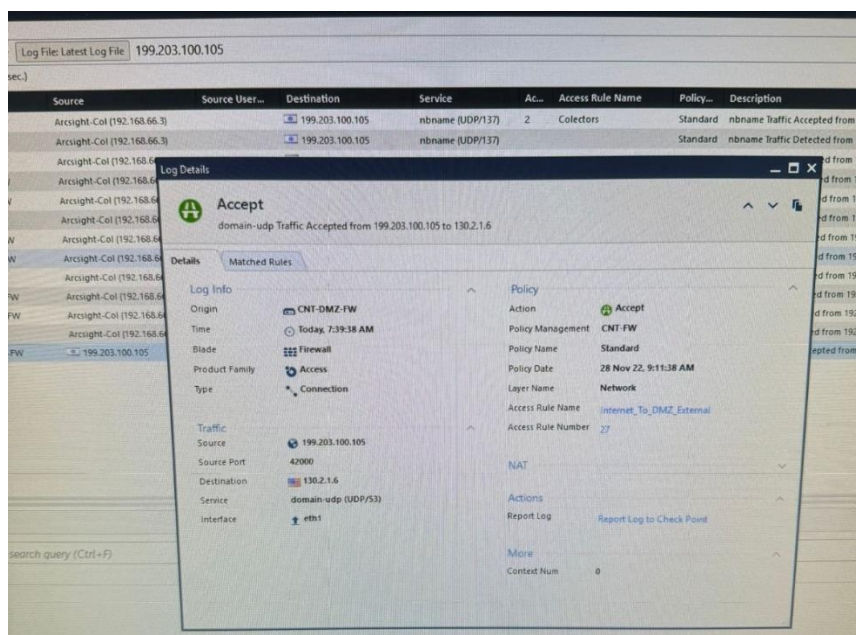
התקיפה זוהתה בעקבות דיווח מחברה אחרת שטענה שאנו תוקפים אותם. החברה ציינה כי כתובת ה-IP 199.203.100.105 הינה כתובת שמותקפת על ידינו. התחלנו בחקירה לברר מה קרה.

התחלנו בבדיקה במערכת ה- ArcSight ללא ממצאים חריגים. בנוסף ביצענו בדיקת Zenoss ללא ממצאים חריגים.

ב-Firewall ניתן לראות שבשעה 39:07 ישנה תעבורת UDP מכתובת 105.100.203.199 (כתובת הנתקף לכאורה) לכתובת 6.100.172.130 (שהיא כתובת בארגון שלנו) שהיא הכתובת 6.100.172.130 מאחורי ה-NAT. זוהי המכונה DNS-DMZ-CNT.

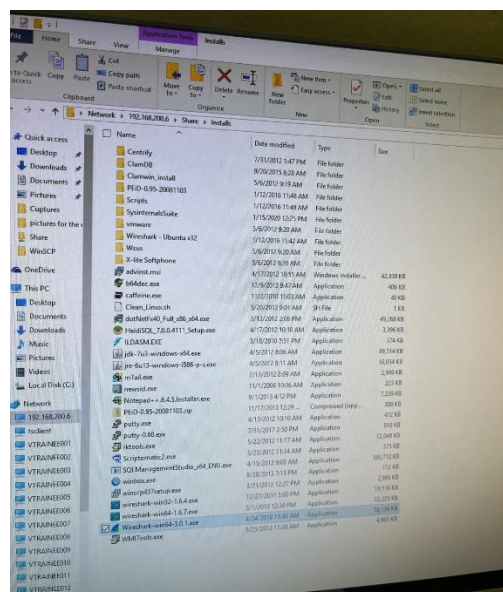
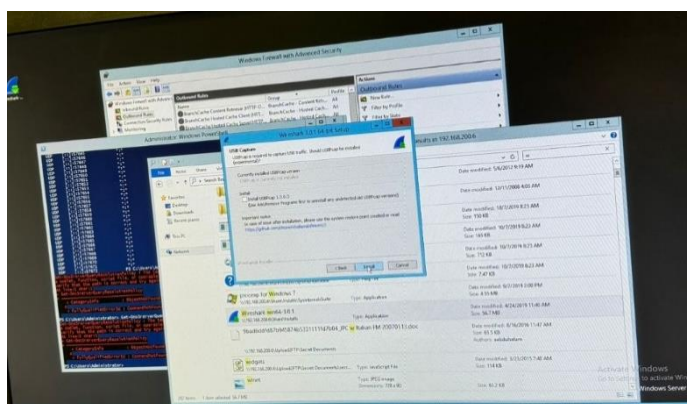
בתמונות נוכל לראות צילום מסך מה-Firewall;

[illegible]



ביצענו חיבור למכונה CNT-DNS-DMZ על מנת להמשיך לחקור. מערכת ההפעלה של המכונה היא Windows ולכן נתחבר למכונה דרך .RDF נתקין Wireshark על המכונה כדי להסניף את התעבורה. התקנו Wireshark ע"י גישה לשרת ה-FTP ומשיכת קובץ ההתקנה מתיקית 'shared' ב-CNT-FILES (192.168.200.6).

בתמונות חיבור למכונה CNT-FILES והתקנת Wireshark



ראינו ב-Wireshark כי שרת ה-DNS שלנו מקבל בקשות DNS רבות מהכתובת המתחזה לכתובת ה-IP המדווחת (199.203.100.105). אנו מניחים שנעשה כאן IP Spoofing - התחזות לכתובת IP. כמו כן, הסקנו שאנחנו לא מתקיפים את החברה המתלוננת, אלא עונים לבקשות לגיטימיות, ולכן התוקף מתחזה לשרתי החברה המותקפת.

נבדוק את תוכן הבקשות. הבקשות מכילות שאילות לאתרי אינטרנט כמו twitter.com, וכתוצאה מכך השרת שלנו מחזיר תשובות גדולות (גדולות יחסית לגודל הבקשה) אשר מעמיסות על שרת היעד. בתמונות צילום מסך של Wireshark בו ניתן לראות את הבקשות;

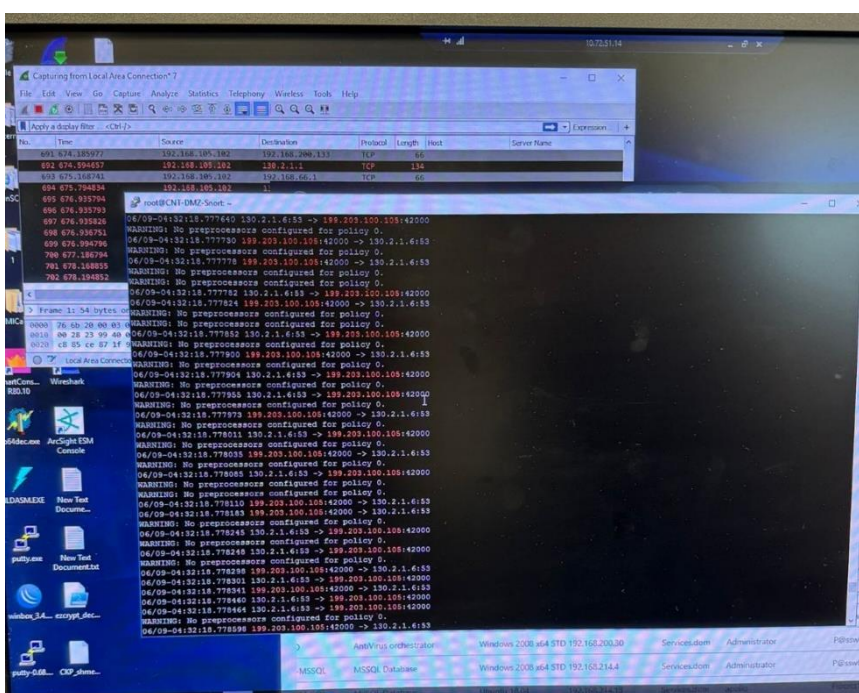
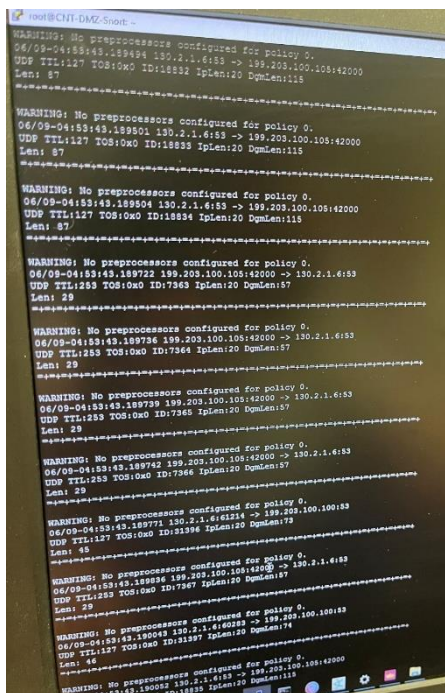
The screenshot displays the Wireshark interface with a packet list on the left and a packet details pane on the right. The packet list shows a series of DNS queries and responses. The selected packet is a standard query response from the Twitter server to the client.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
2	0.000015	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
3	0.000038	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
4	0.000063	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
5	0.000087	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
6	0.000073	199.203.180.105	172.16.100.6	DNS	71	Standard query response #4242 to twitter.com
7	0.000084	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
8	0.000106	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
9	0.000102	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
10	0.000118	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
11	0.000122	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
12	0.000139	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
13	0.000139	172.16.100.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns
14	0.000147	172.16.100.6	199.203.180.105	DNS	129	Standard query request #4242 to twitter.com SOA internet-dns
15	0.000151	199.203.180.105	172.16.100.6	DNS	71	Standard query response #4242 to twitter.com SOA internet-dns
16	0.000162	172.16.100.6	199.203.180.105	DNS	71	Standard query #4242 to twitter.com
17	0.000166	199.203.180.6	199.203.180.105	DNS	129	Standard query response #4242 to twitter.com SOA internet-dns

Packet 17 details: Frame 17: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on Interface 0
 Internet Protocol Version 4, Src: VMware, 192.168.0.107, Dst: VMware, 94.77.06
 User Datagram Protocol, Src Port: 53, Dst Port: 42400
 Domain Name System (Response)

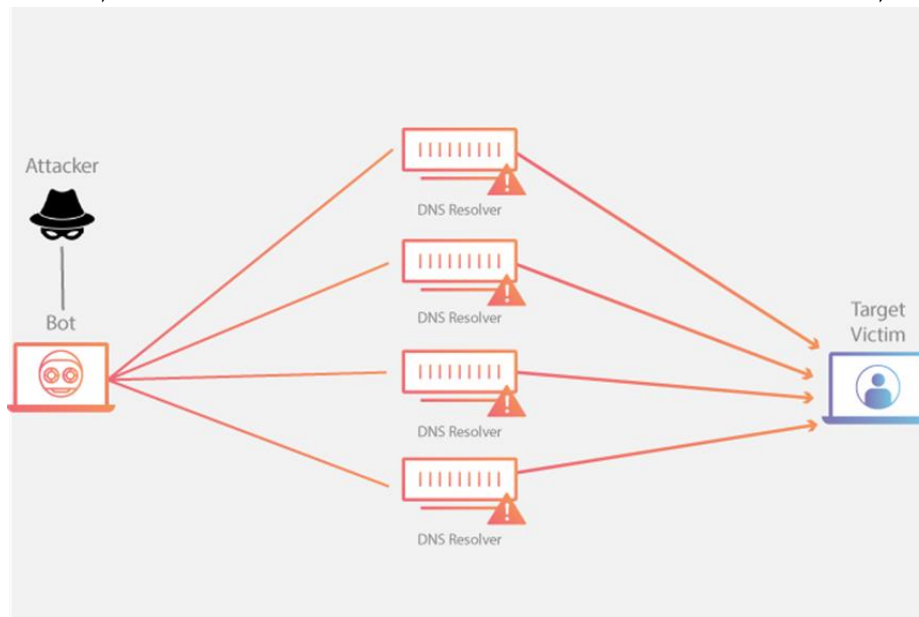
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Nmap - Display filter: <CH>						
No.	Time	Source	Destination	Protocol	Length	Info
65331..	23.705830	199.203.100.195	172.16.100.6	DNS	75	Standard query 00a242 a.twitter.com
65332..	23.705872	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65333..	23.705897	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65334..	23.705944	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65335..	23.705975	172.16.100.6	199.203.100.195	DNS	71	Standard query 00a242 a.twitter.com
65336..	23.706022	199.203.100.195	172.16.100.6	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65337..	23.706036	172.16.100.6	199.203.100.195	DNS	71	Standard query 00a242 a.twitter.com
65338..	23.706080	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65339..	23.706126	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65340..	23.706173	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65341..	23.706198	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65342..	23.706224	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65343..	23.706275	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65344..	23.706325	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65345..	23.706352	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65346..	23.706381	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65347..	23.706392	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65348..	23.706428	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65349..	23.706479	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65350..	23.706504	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65351..	23.706559	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65352..	23.706583	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65353..	23.706609	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65354..	23.706632	172.16.100.6	199.203.100.195	DNS	129	Standard query response 00a242 a.twitter.com SOA Internet-dns
65355..	23.707942	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com
65356..	23.707942	199.203.100.195	172.16.100.6	DNS	71	Standard query 00a242 a.twitter.com

התחברנו ל-SNORT, ה-IDS שלנו, שדרכו עוברת התעבורה אל הרשת שלנו והחוצה. נתחבר למכונת ה-SNORT ע"י SSH Client באמצעות Putty, זאת מכיוון שהמכונה רצה על לינוקס. בבדיקה זיהינו כמות גדולה של בקשות ותגובות DNS שמועברות משרת ה-DNS שלנו לכתובת ה-IP המדווחת, וכן אזהרות.



הבנו שהתקיפה היא מסוג DNS Amplification, תקיפה שבה התוקף שולח בקשות DNS מזויפות (spoofed) לשרת שלנו (כאשר כתובת IP של המקור מזויפת), כך שהשרת שלנו ישלח תשובות גדולות יותר לכתובת IP של החברה המדווחת(התשובה גדולה יותר בגלל שהיא מכילה את השאלה, ולעיתים בגלל שהתשובה כבדה יותר-למשל במקרה שיש כמה כתובות לאתר. בכך התוקף מעמיס על שרת היעד.

מצרף איור שמצאתי באתר www.cloudflare.com המדגים את סוג התקיפה:



3. פירוק ווקטור התקיפה לשלבים לפי [MITRE](#):

- כאן נבצע פירוק של ווקטור התקיפה לתבנית MITRE ATT&CK.
- A. [Reconnaissance](#): התוקף זיהה את כתובת ה-IP של שרת ה-DNS.
 - B. [Resource Development](#): התוקף לא יצר כלים או משאבים מיוחדים. ייתכן שהוא השתמש בבוט או סקריפט כדי להציף בבקשות DNS.
 - C. [Initial Access](#): אין, התוקף לא נכנס לרשת שלנו באופן ישיר אלא שלח בקשות DNS מזויפות מרשת חיצונית.
 - D. [Execution](#): התוקף הריץ את ההתקפה על ידי שליחת בקשות DNS מזויפות מכתובת IP מזויפת, וכתוצאה מכך השרת שלנו שלח תשובות גדולות יותר.
 - E. [Persistence](#): התוקף לא שמר על גישה מתמשכת לרשת שלנו, מכיוון שלא נכנס אליה, אלא התקיפה התבססה על תעבורה חיצונית בלבד.
 - F. [Privilege Escalation](#): אין, התוקף לא ניסה להשיג הרשאות גבוהות ברשת שלנו מכיוון שההתקפה התבצעה מבחוץ.
 - G. [Defense Evasion](#): אין. התוקף השתמש ב-IP Spoofing - בכדי להסתיר את זהותו האמיתית. אך חוץ מכך, לא ביצע שום דבר בכדי להסתיר את פעילותו.
 - H. [Credential Access](#): אין, התוקף לא ניסה לגנוב שמות משתמשים וסיסמאות אלא התמקד בהצפת השרתים.
 - I. [Discovery](#): אין, התוקף לא ניסה להבין את המערכת והרשת הפנימית שלנו. ההתקפה הייתה ממוקדת בשימוש בשרת ה-DNS שלנו כווקטור התקפה.
 - J. [Lateral Movement](#): אין, התוקף לא נע בסביבה כי לא נכנס לרשת שלנו.

K. [Collection](#): אין, התוקף לא אסף מידע. המטרה הייתה לגרום לעומס על השרתים ולא לאסוף מידע.

L. [Command and Control](#): אין, לתוקף אי שרת שליטה ובקרה.

M. [Exfiltration](#): התוקף לא גנב מידע במטרה להזליג אותו החוצה. המטרה הייתה לגרום לעומס ולא לגניבת מידע.

N. [Impact](#): התקיפה כללה הצפת שרתי החברה המותקפת בתשובות DNS גדולות מה שגרם לעומס רב על שרתיהם.

4. מידע תקשורתי:

A. פרטי חבילות:

התוקף השתמש בפרוטוקול UDP כדי לשלוח בקשות DNS לשרת ה-DNS שלנו. השרת שלנו שלח את הודעת תשובה חזרה גדולה יותר מהשאלה, בכך התוקף מעמיס על היעד הנתקף.

Standard query response 0x4242 A twitter.com 129	DNS	172.16.100.6	199.203.100.105	0.000002
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000029
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000038
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000046
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000053
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000063
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000080
Standard query 0x4242 A twitter.com 71	DNS	172.16.100.6	199.203.100.105	0.000133
Standard query 0x4242 A twitter.com 71	DNS	172.16.100.6	199.203.100.105	0.000133
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000157
Standard query response 0x4242 A twitter.com SOA internet-dns 129	DNS	172.16.100.6	199.203.100.105	0.000169

Frame 7: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface \Device\NPF_{A2B8B5C6-1501-4D0F-86B6-29E891C8A4AB}, id 0
Ethernet II, Src: VMware_9a:bd:d7 (00:50:56:9a:bd:d7), Dst: VMware_9a:47:d6 (00:50:56:9a:47:d6)
Internet Protocol Version 4, Src: 172.16.100.6, Dst: 199.203.100.105
User Datagram Protocol, Src Port: 53, Dst Port: 42000
Domain Name System (response)

ניתן לראות את בקשות ה-DNS (query) בגודל של 71 bytes, בפרוטוקול UDP, מ-IP 172.16.100.6 בפורט 42000 ; ל-IP 199.203.100.105 בפורט 53 (DNS). בנוסף ניתן לראות גם את התשובה (query response) בגודל 129 bytes והפוך בכתובות.

B. מהירות שליחת החבילות:

עבור כל פרוטוקול, שהתקיפה כללה נשלחו 10,066,679 חבילות במשך 373.870 שניות. כלומר 26,925.6 חבילות בשנייה בממוצע ו- 1,438,096 לדקה בממוצע.

Details

File

Name:

C:\Users\nnbbj\OneDrive\סייבר\תעודת סייבר\העבודה\לימודים\סייבר\Syn Flood\pcap\dns_amplification_filtered.pcapng

Length:

1348 MB

Hash (SHA256):

b6f3eb2aedf92c3085c6df49e0da8aba7f328a9c635a351f8e4d099f365691fe

Hash (SHA1):

9ae25700374bcb42de95bc1d5a9153f9e48a34d

Format:

Wireshark/... - pcapng

Encapsulation:

Ethernet

Time

First packet:

2024-06-14 20:39:47

Last packet:

2024-06-14 20:46:01

Elapsed:

00:06:13

Capture

Hardware:

Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz (with SSE4.2)

OS:

64-bit Windows Server 2012 R2, build 9600

Application:

Dumpcap (Wireshark) 3.0.1 (v3.0.1-0-gea351cd8)

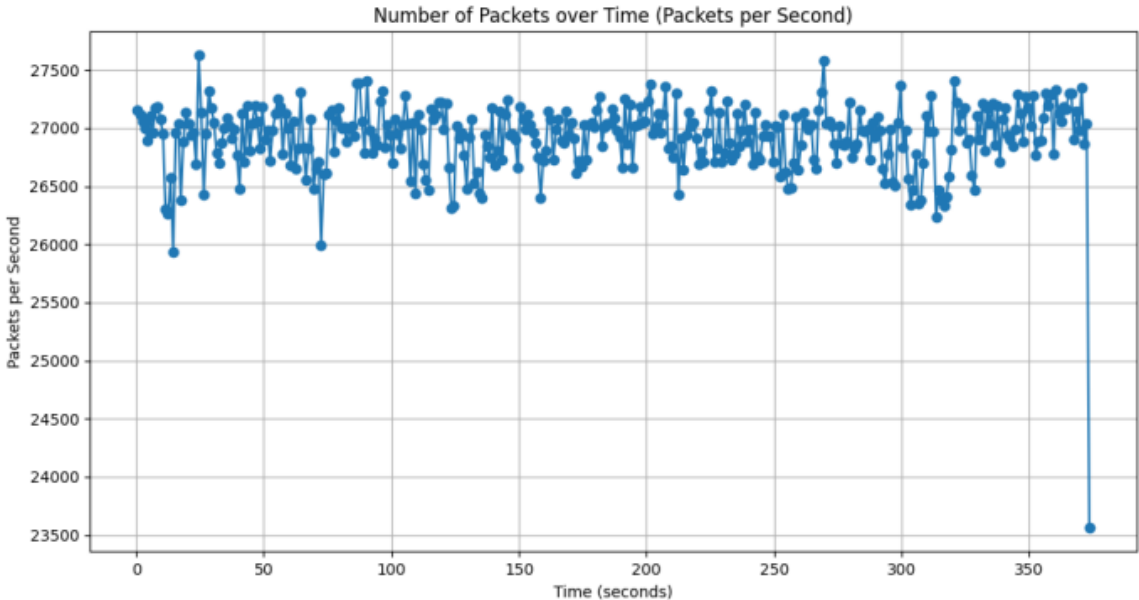
Interfaces

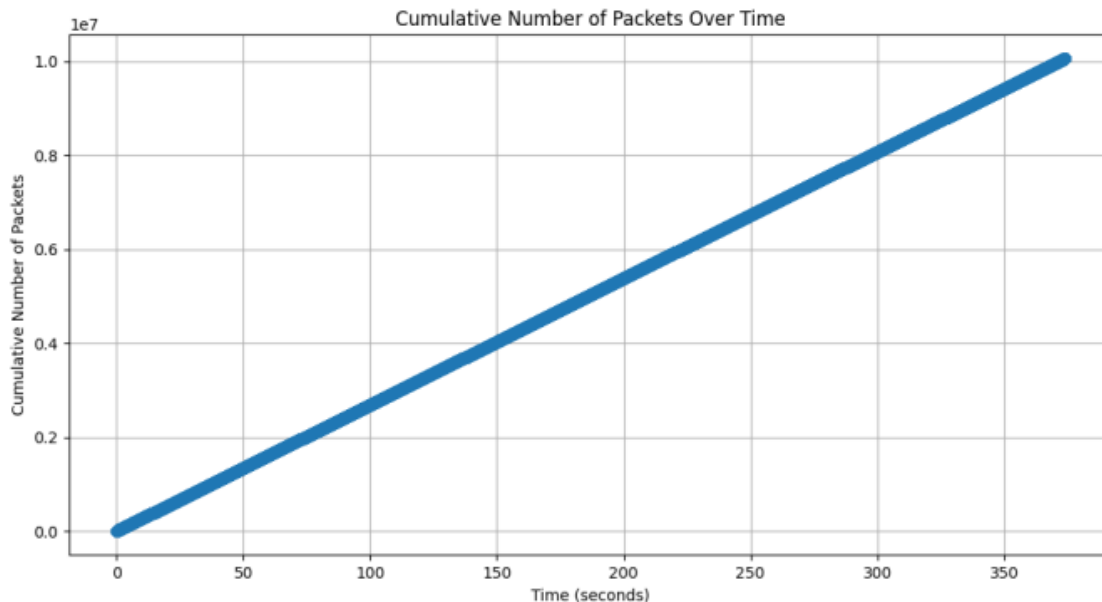
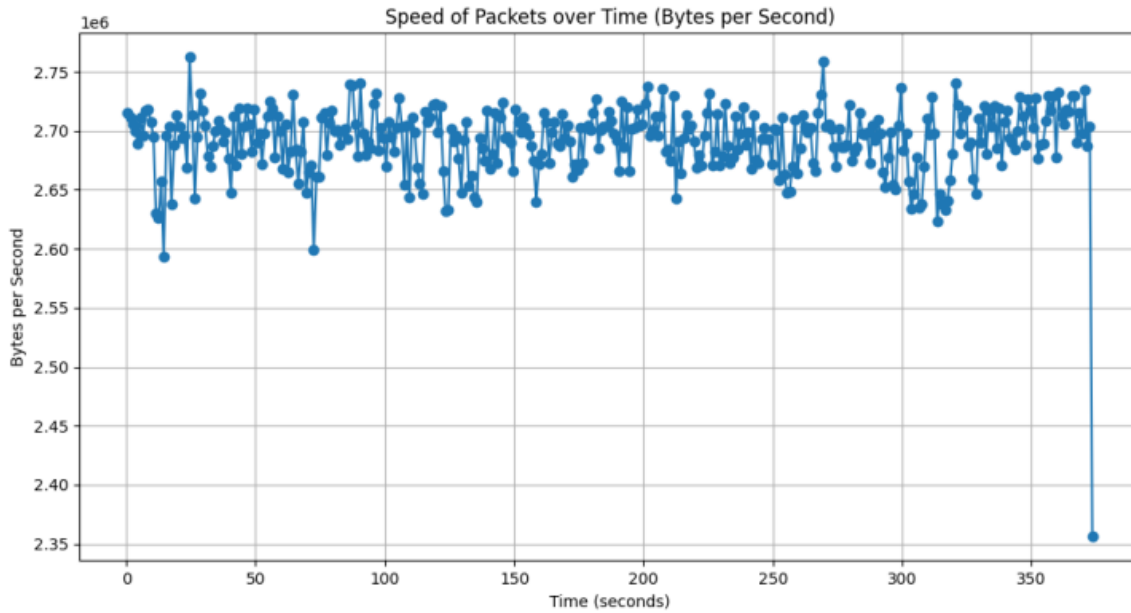
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Ethernet0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	10066679	10066679 (100.0%)	—
Time span, s	373.870	373.870	—
Average pps	26925.6	26925.6	—
Average packet size, B	100	100	—
Bytes	1006689075	1006689075 (100.0%)	0
Average bytes/s	2692 k	2692 k	—
Average bits/s	21 M	21 M	—

C. גרפים לתיאור התקשורת:





D. סטטיסטיקות נוספות :
זמן הממוצע בין חבילות : 0.000037 microseconds.
גודל חבילה ממוצעת : 100 bytes.

5. פעולות לוקאליות :
אין חדירה של התוקף למכונות או לקבצים בתוך הארגון.

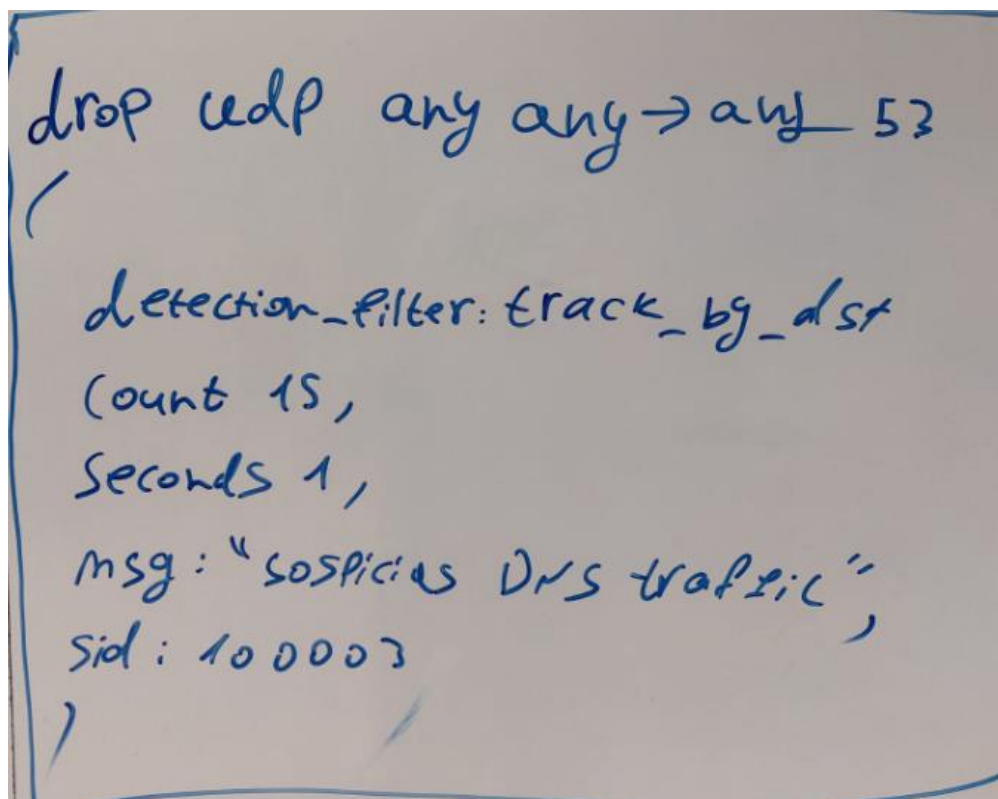
A. המשתמש שדרכו נכנס התוקף : אין
B. קבצים שנפגעו/שונו/הועתקו/הושתלו : אין
C. איזה קבצים התוקף החדיר? באיזה קבצים התוקף פגע? אין

6. הגנה :
A. הגנה ראשונית :
כהגנה ראשונית פנינו לחברה המותקפת בהודעה שלאחר בדיקה מקיפה אנחנו לא אלה שמתקיפים אותה, וכן נחסום את כתובת ה-IP 199.203.100.105 אשר אותרה כ'תוקפת' בידי

החברה.

B. הגנה מניעתית:

על מנת למנוע התקפות כאלו בעתיד נבצע הוספת חוק ל-SNORT להתעלם מבקשות DNS בכמות גדולה מכתובת IP מסוימת בפרק זמן קצר.
נוסיף את החוק הבא ל-Snort:



```
drop udp any any → any 53  
(  
  detection-filter: track_by_dst  
  count 15,  
  seconds 1,  
  msg: "suspicious DNS traffic",  
  sid: 100003  
)
```

הסבר לחוק: תשמיט את חבילות UDP מכל מקום לכל מקום על גבי פורט 53-DNS אם בשנייה אחת יש מעל 15 חבילות.
בנוסף נבצע הוספת חוק ל-Firewall לחסום כתובת IP שמבקשת מספר רב של בקשות DNS בפרק זמן קצר.

7. הערות נוספות:

A. אופן עבודת הצוות: האירוע נוהל בצורה טובה.

B. מגבלות העבודה: לא היו פערים.