CTF של ברק גונן

שלב 1:

קיבלנו קובץ PDF בשם Fiona's Apple בכתובת:

https://data.cyber.org.il/networks/lev-tal/LevTalCTF.pdf

הקובץ הכיל קישור לקובץ בשם Fiona.pcapng מסוג Wireshark בכתובת:
https://data.cyber.org.il/networks/lev-tal/Fiona.pcapng

פתחתי את הקובץ ב Wireshark. במעבר עליו, הבחנתי בבקשת HTTP לתמונה:

GET /poison_apple.jpg HTTP/1.1	524	HTTP	192.168.1.221	192.168.1.102	3.690930 267

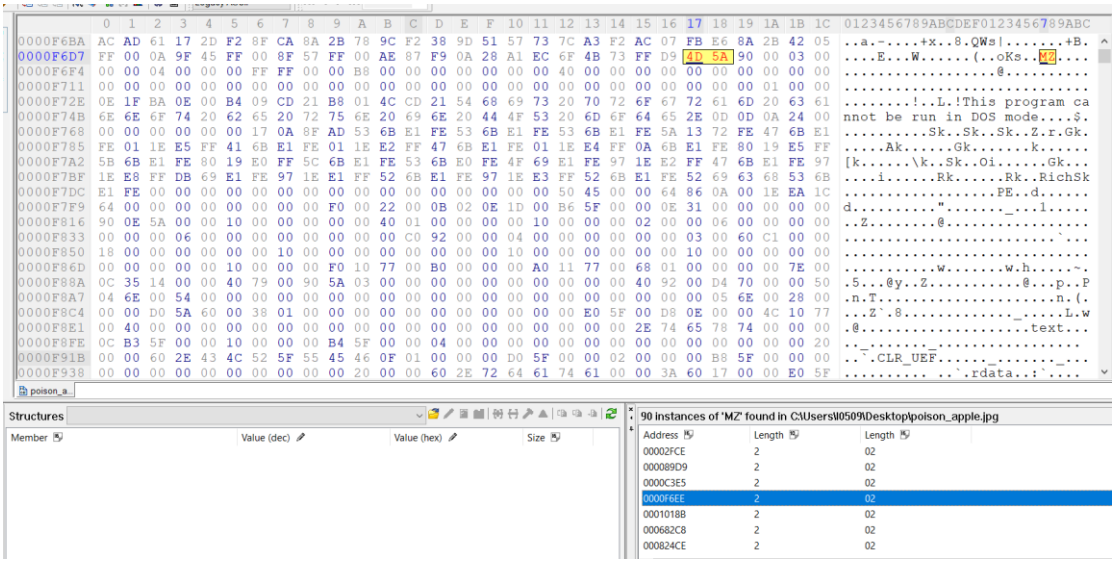
כדי לחלץ את התמונה מתוך התוכנה, בחרתי בפילטר: File > Export Objects > HTTP

ונשמרה התמונה: poison_apple.jpg

שלב 2:

במבט ראשוני, נראה שקובץ התמונה הוא כ – 11 MB, שזה המון, לכן חשדתי שיש בו קובץ ניתן להרצה exe.

בכל הנראה זה קובץ מסוג Portable Executable = PE, ועל מנת למצוא אותו, פתחתי את התמונה ב Hex Editor, וחיפשתי את ה header של הקובץ שהוא MZ.



זה הוא ה MZ הראשון שלאחריו מופיע הערות של תוכנית.

מחקתי את כל השורות שלפני הכתובת הנ"ל, ושמרתי את הקובץ כ exe, כך יצא הקובץ poison_apple.exe.

שלב 3:

הרצתי את הקובץ ב CMD, והוא הוציא את הפלט הבא:

```
C:\Users\l0509>C:\Users\l0509\Desktop\poison_apple.exe
Error connecting to the server WakeUpFiona.co.il. on port 8200: No such host is known.
```

```
C:\Users\l0509\Downloads>C:\Users\l0509\Downloads\poison_apple.exe

Error connecting to the server WakeUpFiona.co.il. on port 8200: No such host is known.
```

נראה שהוא מנסה לגשת לאתר כלשהו בפורט 8200 (:

כדי להבין יותר מה הולך מאחורי הקלעים, פתחתי Wireshark להסניף את התעבורה:

Info	Length	Protocol	Destination	Source	Time	No.
Standard query 0xacf8 A WakeUpFiona.co.il	77	DNS	8.8.8.8	10.0.0.17	1.518242	91
Standard query response 0xacf8 No such name A WakeUpFiona.co.il SOA nsa.ns.il	140	DNS	10.0.0.17	8.8.8.8	1.748215	97

הוא מבצע שאילתת DNS לאתר הנ"ל. (במקרה שלי, שרת ה DNS הוא של Google בכתובת 8.8.8.8)

כדי למנוע ממנו מלבקש את הכתובת מהשרת החיצוני, שיניתי את טבלת הקינפוג של DNS במחשב שלי, כך שכתובת ה IP של האתר WakeUpFiona.co.il תהיה 127.0.0.1

עשיתי זאת ע"י שינוי קובץ ה hosts שנמצא ב `C:\Windows\System32\drivers\etc`

והוספת השורה: `127.0.0.1 WakeUpFiona.co.il`

התקבל הפלט הבא:

```
C:\Users\l0509>C:\Users\l0509\Desktop\poison_apple.exe
Error connecting to the server WakeUpFiona.co.il. on port 8200: No connection could be made because the target machine a
ctively refused it. 127.0.0.1:8200
```

```
C:\Users\l0509\Downloads>C:\Users\l0509\Downloads\poison_apple.exe

Error connecting to the server WakeUpFiona.co.il. on port 8200: No connection could be made because the target machine actively refused it. 127.0.0.1:8200
```

כדי להשלים את ההתחזות, נדרש לכתוב שרת אפליקציה HTTP מקומי, שיתפוס את הבקשה הנ"ל.

שלב 4:

ביקשתי מ GPT שיכתוב לי שרת HTTP פשוט, בכתובת 127.0.0.1, ובפורט 8200:

```
from http.server import SimpleHTTPRequestHandler, HTTPServer
import json


class MyHTTPRequestHandler(SimpleHTTPRequestHandler):
    def do_GET(self):
        # Print request path
        print(f"Received GET request for path: {self.path}")

        # Create a JSON response
        response_data = {
            "message": "Hello, World!",
            "description": "This is a custom JSON response from the
server.",
            "path": self.path
        }
        response_json = json.dumps(response_data)

        # Send a response
        self.send_response(200)
        self.send_header('Content-Type', 'application/json')
        self.end_headers()
        self.wfile.write(response_json.encode('utf-8'))
        print(f"Sent response: {response_json}")


def start_http_server(hostname, port):
    # Define the server address
    server_address = (hostname, port)

    # Create the HTTP server
    httpd = HTTPServer(server_address, MyHTTPRequestHandler)

    print(f"HTTP server started on {hostname} at port {port}")

    # Start the server
    httpd.serve_forever()


# Usage
hostname = "127.0.0.1"  # Listen on localhost
port = 8200
start_http_server(hostname, port)
```

אז הרצתי אותו, ולאחר מכן את הלקוח (poison_apple.exe), והתקבל הפלט הבא:

```
C:\Users\l0509>C:\Users\l0509\Desktop\poison_apple.exe
Request was successful, but 'Success' field is not 'True' or not present.
```

C:\Users\l0509>C:\Users\l0509\Desktop\poison_apple.exe

Request was successful, but 'Success' field is not 'True' or not present.

ז"א שחסר לו ב DATA שהוא מקבל שדה בשם Success, והערך שבו צריך להיות True.

לכן, שיניתי את ה response_data כך שיכיל את השדה הנ"ל:

```
response_data = {
    "Success": True,
    "message": "Hello, World!",
    "description": "This is a custom JSON response from the server.",
    "path": self.path
}
```

הרצתי שוב את השרת, והתקבל הפלט הבא:

```
C:\Users\l0509>C:\Users\l0509\Desktop\poison_apple.exe
QVRL YGQV P AMDG BWLVV YIH H TIKVRLWJ. VPTYI NCA PSWF C LDUOVA ICK E GQTXJI FHNXJII, DCI MVFO I IVXRNTN KMWHMGLRK OWKPI...
XQWS DSIM. GDB HZF I GLEC HQCL AFTS RYETMQCN XYKA GPHUNM. NVY JJWLLH JMQASW ZP XNALFP, VTAAFTSH, VTVTIIPRX UGHAIDU ICK ME VPT ZG
ZGVRL SW UMRYITA.
GDBV IKLSSI ZU LDUI YGZT: KEKC LDA GPDMG KSK QZV KSK KT HSEJJ VTAAFTSH ZPRUP RAJ JNIHO WLEKTZW UQB YWK
RNT HTECN TTAXVTA
```

```
C:\Users\l0509\Downloads>C:\Users\l0509\Downloads\poison_apple.exe

QVRL YGQV P AMDG BWLVV YIH H TIKVRLWJ. VPTYI NCA PSWF C LDUOVA ICK E GQTXJI
FHNXJII, DCI MVFO I IVXRNTN KMWHMGLRK OWKPI…

XQWS DSIM. GDB HZF I GLEC HQCL AFTS RYETMQCN XYKA GPHUNM. NVY JJWLLH JMQASW
ZP XNALFP, VTAAFTSH, VTVTIIPRX UGHAIDU ICK ME VPT ZGZGVRL SW UMRYITA.

GDBV IKLSSI ZU LDUI YGZT: KEKC LDA GPDMG KSK QZV KSK KT HSEJJ VTAAFTSH ZPRUP
RAJ JNIHO WLEKTZW UQB YWK

RNT HTECN TTAXVTA
```

התקבל פלט מוצפן, ויש לפענח אותו.

שלב 5:

הפלט מוצפן ככל הנראה בהצפנה א-סימטרית, הדבר הראשון שעלה לי לראש הוא צופן קיסר.

ביקשתי מ GPT שיכתוב קוד מפענח, ולאחר שעברתי על 26 האופציות ראיתי שאף אחת מהתוצאות לא הייתה הגיונית.

פיענוח צופן קיסר (shift):

```
def caesar_decrypt(ciphertext, shift):
    decrypted_text = ''
    for char in ciphertext:
        if char.isalpha():
            shift_amount = shift % 26
            start = ord('A') if char.isupper() else ord('a')
            new_char = chr(start + (ord(char) - start - shift_amount)
% 26)
            decrypted_text += new_char
        else:
            decrypted_text += char
    return decrypted_text

# Example usage
ciphertext = "QVRL YGQV P AMDG BWLVV YIH H TIKVRLWJ. VPTYI NCA PSWF C
LDUOVA ICK E GQTXJI FHNXJII, DCI MVFO I IVXRNTN KMWHMGLRK OWKPI..."

# Try all shifts from 1 to 26
for shift in range(1, 27):
    print(f"Shift {shift}: {caesar_decrypt(ciphertext, shift)}")
```

משום שהניסיון לא צלח, חשבתי על דרכים אחרות.

צופן סימטרי נוסף שנלמד הוא צופן ויז'נר, כפי שנלמד מהסרטון בערוץ היוטיוב של ברק:

https://www.youtube.com/watch?v=dRl8O2u8az8&list=PLEj7E6n4N83Gv1SgpY5d_keOjCEcC6YH7&index=19

השתמשתי באתר https://www.dcode.fr/vigenere-cipher על מנת לפענח את הטקסט, והתקבלה ההודעה:

```
ONCE UPON A TIME THERE WAS A PRINCESS. THERE WAS ALSO A DONKEY AND A POLICE
OFFICER, BUT FROM A TOTALLY DIFFERENT MOVIE...
GOOD WORK. YOU DID A REAL FINE WORK CRACKING THIS RIDDLE. YOU SHOWED SKILLS
IN PYTHON, NETWORKS, OPERATING SYSTEMS AND IN THE SCIENCE OF SECRECY.
YOUR RIDDLE IS DONE HERE: DATA DOT CYBER DOT ORG DOT IL SLASH NETWORKS SLASH
CTF SLASH SUCCESS DOT JPG
ALL SMALL LETTERS
```

ובגלל שלא היה לי כוח להמיר את הכתובת, כתבתי קוד פייתון שיעשה את זה:

```
text = "DATA DOT CYBER DOT ORG DOT IL SLASH NETWORKS SLASH CTF SLASH
SUCCESS DOT JPG"
text = text.lower().replace('dot', '.').replace('slash',
'/').replace(' ', '')

print(text)  # Output: data.cyber.org.il/networks/ctf/success.jpg
```

ויצאה הכתובת: https://data.cyber.org.il/networks/ctf/success.jpg

שהכילה את התמונה: success.jpg

סיימתי :)

תודה רבה לברק גונן על CTF מעשיר ומלמד!