

דו ספרתית, ולכן נשים את הנקודה לאחר הספרה השנייה. נזין את נקודות הציון בגוגל מפות ונקבל את המיקום המבוקש.



נזין אותו בכתובת, ונקבל <http://deceptionisland.xyz>, הגענו ליעד.

Challenge #1

Welcome back Agent C!

Once again we require your skills for an urgent mission.
Our intelligence officers have intercepted a message between notorious terrorists discussing an imminent attack on targets world-wide.
Intel points to a popular chat website used by these terrorists to coordinate and select rendezvous locations.
Your mission is to track the team online and ascertain their physical location.

The following [link](#) leads to the web site of the online chat service.

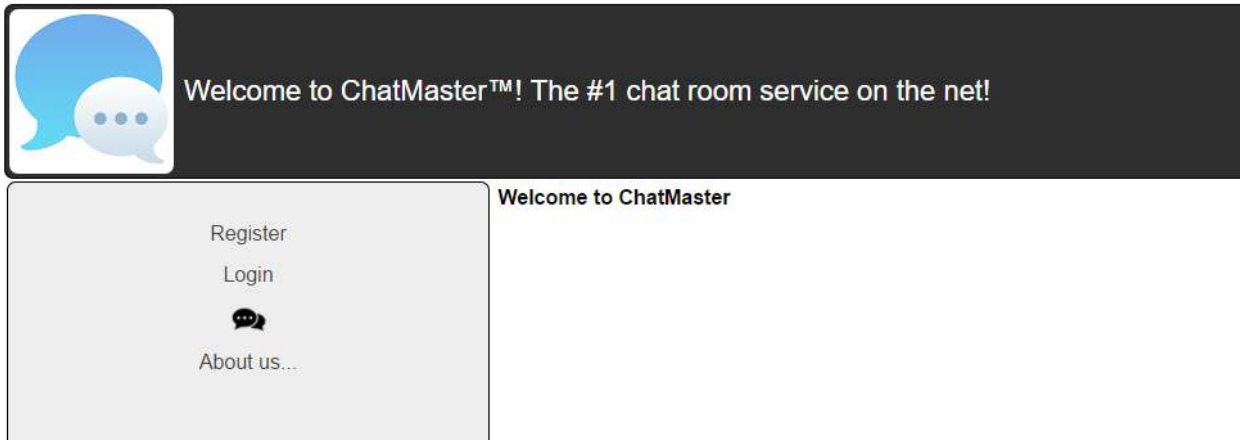
Good luck!,
M.

השלב שלכם באתגר מבוסס על Cookies ששמורים לכם בדפדפן. אם תסגרו את הדפדפן, תאלצו להתחיל מחדש את האתגרים. לכן, מומלץ מאוד לגבות את הקוקית **challengeState** בכל שלב.

האתגר מתחיל בכתובת <http://deceptionisland.xyz/challenge1>.

האתר הוא אתר הצאט "המפורסם" ChatMaster, שהוא, כמובן, מספר אחד באינטרנט ☺. התפריט מורכב מהאפשרויות הבאות:


- הרשמה - מוביל אותנו לטופס הרשמה לשירות הצאט.
- התחברות – מאפשר לנו להתחבר לשירות הצאט
- אודות – פרטים על אודותיה של חברת הצאט ועל מנהליה.



דף ה-HTML הראשי לא טומן בחובו שום דבר מעניין, לכן פשוט נרשם לשירות הצאט בתקווה למצוא את הסטוריסטים.

Welcome to ChatMaster

Please enter your registration information below:



SUBMIT !


לאחר ההרשמה אנו מקבלים הודעה שיש עומסים כבדים לשירות, ולכן יש רשימת המתנה ☹️. האתר מוגבל להוספת משתמש אחד ביום. לתפריט בצד שמאל נוסף לנו גם מצב ההרשמה שלנו.

Register

De-register

Registration Status

Login

 About us...

Welcome to ChatMaster

Thank you for registering with ChatMaster
Due to high demand we are unable to add you to the site's member list at the moment.
You have been placed on our waiting queue and will receive a message when your account is activated. We are currently limited to adding a single user per day.
We are working diligently on upgrading our storage and promise to increase our user capacity very soon.
Please stay tuned.

The **ChatMaster**™ team

נכנס למצב ההרשמה.

אתגר 1 – מצב ההרשמה

Welcome to ChatMaster

ChatMaster Registration Status

There are 36 users before you in the registration queue.
You will get notified when your account is active.

Users on the waiting queue
AgentC
Mr.Li B0b
Dr. Drek
may_o_nez
tom_HW

אבוי, ברשימת ההמתנה יש 36 משתמשים לפנינו. בקצה הזה רק עוד 36 ימים נוכל להתחבר. אם כן, אין ברירה. יש לנו מחבלים לתפוס. הגיע הזמן שנעשה קצת סייבר סייבר.

אף אחד מהדפים באתר לא מריץ קוד JS מלבד אנלטיקיס. מכאן, שהכל קורה בצד שרת. נוסף על כך, הדף De-register עושה את מה שהוא מתיימר לעשות, הוא מוחק את המשתמש שלנו. יש לנו כמה אפשרויות למשחק:

- לנסות להתחבר בתור המשתמש הראשון ברשימה או משתמש אחר. במסך של ההתחברות יש כפתור של שכח סיסמה, והוא מבקש שם משתמש. למשתמש הראשון ברשימת ההמתנה, johndow, אין רמז לסיסמה ולכן לא נוכל לגנוב את סיסמתו.
- לנסות לגרום לכך שאנחנו נהיה ראשונים ברשימת ההמתנה. אבל כיצד?

אם לדף אין JS, ניתן לומר שהוא מתבסס על הנתונים שנשלחים לו באופן אוטומטי מהבקשות של הדפדפן. אחד מהנתונים הללו הוא ה-Cookies. נראה אילו עוגיות נשמרו במהלך ההרשמה:

Name	Value	Domain	Path	Expires / Max-Age	Size
_ga	GA1.2.2098231819.1493983980	.deceptionisland.xyz	/	2019-05-05T12:06:24.000Z	30
_gid	GA1.2.2102578082.1493985984	.deceptionisland.xyz	/	2017-05-06T12:06:24.000Z	31
challengeState	VS9DTzFTajBycFVYUTRpMm8vVVU...	deceptionisland.xyz	/	Session	814
eu	QWdIbnRD	deceptionisland.xyz	/	Session	10

2 העוגיות הראשונות הן של Google Analytics. השלישית היא מצב האתגר. התוכן ארוך מאוד ולא ברור איך הוא בנוי ולכן נעזב אותו לבנתיים. העוגיה הרביעית נקראת eu והיא קצרה. יש בה גם אותיות קטנות וגם אותיות גדולות. הואיל וכמספר ימים לפני האתגר של המוסד לשב"כ היה אתגר שהשלב הראשון בו הוא base64, נבדוק האם תוכן העוגיה הוא base64 של משהו. ואכן כן. מדובר ב-base64 encode של AgentC, שם המשתמש שלנו. ומה אם ננסה להתחכם? בוא ננסה להתחזות להבא אחרינו ברשימה, Mr.Li B0b. נשים בערך העוגיה את הערך ב-base64 של שם המשתמש ההוא, ונרענו.

חשוב להדגיש שכותב הפתרון הזה לא תומך בהתחזות לאנשים אחרים בשום צורה או דרך. סעיפים 441 עד 446 לחוק העונשין, תשל"ז-1977, אוסרים על פעולות הכרוכות בהתחזות. הסעיף העיקרי הוא סעיף 441 האוסר על "התחזות כאדם אחר". עיקרו של הסעיף הוא כי "המתייצג בכזב כאדם אחר, חי או מת, בכוונה להונות - דינו מאסר שלוש שנים"

האתר עדיין מציג שאנחנו AgentC. חבל. אבל מה אם ננסה למחוק את החשבון? האתר לא ניתק אותנו, והוא הוריד את Mr.Li B0b מרשימת ההמתנה. מצטערים חבר, אבל בטחון המדינה קודם לכל. כנראה שזאת הדרך, יש להתחזות לכל אחד מהמשתמשים שלפנינו ברשימה, ולמחוק את חשבונם. מכיוון שמדובר ב-35 משתמשים, נכתוב סקריפט ל-Developer Console (קורדיט לניר חסן על גרסתו העדכנית של הסקריפט) שמשנה את העוגיה לשם המשתמש של החשבון האחרון ברשימה:

```

1. let usernames = [];
2. $('table[name="waiting list"] td').each((_, o) => usernames.push(o.innerText));
3. usernames.shift();
4.
5. deregisterUsers(usernames);
6.
7. function deregisterUsers(usernames) {
8.   if (usernames.length > 0) {
9.     const user = usernames.shift();
10.    document.cookie=`eu=${btoa(user)}; path=/`;
11.    $.get('http://deceptionisland.xyz/challenge1/deregister', () => {
12.      deregisterUsers(usernames);
13.    });
14.   } else {
15.     location.reload();
16.   }
17. }

```

הסקריפט רץ עד שאני מקום ראשון ברשימה

Welcome to ChatMaster


ChatMaster Registration Status

There are 0 users before you in the registration queue.
You will get notified when your account is active.

Users on the waiting queue
AgentC

עכשיו, ננסה להתחבר. אנחנו בפנים!

Welcome to ChatMaster




Welcome AgentC!

Chatroom membership

View all chatrooms

Active users

Logout



About us...

Chatroom membership מאפשר לנו לבחור לאיזה צאט אנחנו רוצים להיכנס. אולם, הוא מגביל אותנו לצאט אחד בלבד.

Welcome to ChatMaster

Chat room selection

Available Rooms

- 50+
- art
- dating
- news
- politics
- sports

SELECT

REMOVE

Selected Rooms

-

REFRESH!

JOIN ROOMS NOW!

YOAV STERNBERG

YOAVST.COM

View All chatrooms אומר לנו שהפיצ'ר הזה חסום לנו, והוא מיועד רק למשתמשי בפלטינום. כנראה שנצטרך להגיע אליו.
Active Users מציג לנו את רשימת המשתמשים הפעילים באתר.

Welcome to ChatMaster
Recent active users on ChatMaster!

User name	Type
cheetah	PLATINUM
ILove2*ack	PLATINUM
H@ck3rU	PLATINUM
chatW1z	Admin
Justin There	Regular
AgentC	Regular

אם ננסה להתחבר לצאט, ונלחץ על Chat Now נקבל את ההודעה שאדמין צריך לאשר לנו את החברות בצאט. אך אין לנו זמן לחכות. נאלץ לנסות להתחבר בעצמנו כאדמין ולאשר לעצמנו את הבקשה.
זוכרים שבמסך של ההתחברות יש כפתור של "שכחתי סיסמה"? נתנתק מהחשבון, נלך להתחברות, נלחץ על שכחתי סיסמה ונזין את שם המשתמש של האדמין.

Welcome to ChatMaster
Forgot Your Password?



Please enter your username below:

SUBMIT !

The admin password for "chatW1z" was successfully reset. hint: /challenge1/password_hint

אם נכנס לקישור נגלה שירד לנו למחשב קובץ שנקרא password_hint. הגיע הזמן לעבודה.

אתגר 1 – ניתוח ה-DLL

איננו יודעים מה סוג הקובץ. נפתח את ה-Hex Editor ונגלה כי הקובץ מתחיל ב-PK. זהו קובץ Zip.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 50 4E 03 04 14 00 01 00 08 00 17 AC 75 4A 59 74 PK.....-uJYt
```


בתוך ה-zip יש קובץ dll בשם PassMasterExtension. כנראה שבתוכו יש את הסיסמה.

Name	Size	Packed Size	Modified	Created	Accessed
PassMasterExtension3_1.dll	21 504	9 762	2017-03-21 22:32	2017-03-21 22:26	2017-03-21 22:26

ננסה לחלץ אותו, אך לא נוכל, כי יש ל-zip סיסמה.

נשתמש ב-John the ripper לפי המדריך [הבא](#). הסיסמה היא doc1. נזין אותה ונקבל את ה-dll.

```
D:\Downloads\john180j1w\run>zip2john.exe password_hint.zip > zip.hashes
0 [main] zip2john 3348 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
ver 14 password_hint.zip->PassMasterExtension3_1.dll PKZIP Encr: cmplen=9762, decmplen=21504, crc=6C327459

D:\Downloads\john180j1w\run>john.exe zip.hashes
0 [main] john 11004 find_fast_cwd: WARNING: Couldn't compute FAST_CWD pointer. Please report this problem to
the public mailing list cygwin@cygwin.com
Loaded 1 password hash (PKZIP [32/32])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
doc1 (password_hint.zip)
1g 0:00:00:00 DONE 2/3 (2017-05-05 16:11) 1.626g/s 89528p/s 89528c/s 89528C/s 123456..skyline!
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

נשתמש בתוכנה PE-Bear כדי לראות מה יש בתוך ה-DLL. כידוע, DLL הוא קובץ PE (כמו EXE) המכיל בתוכו קוד מקומפל.

The screenshot shows the PE-Bear v0.3.7 interface. On the left, the file structure is expanded to show the 'Exports' section. The main window displays a hex dump of the file's content. Below the hex dump, there is a table of exports with the following data:

Offset	Name	Value	Meaning
4340	Characteristics	0	
4344	TimeDateStamp	58D1739F	
4348	MajorVersion	0	
434A	MinorVersion	0	
434C	Name	559A	PassMasterExtension3_1.dll
4350	Base	1	
4354	NumberOfFunc...	5	
4358	NumberOfNames	5	
435C	AddressOfFunc	5568	

Below this table, there is another table showing the export entries:

Offset	Ordinal	Function RVA	Name RVA	Name	Forwarder
4368	1	2B90	55B5	Decrypt	
436C	2	2BC0	55BD	Decrypt2	
4370	3	2B00	55C6	Encrypt	
4374	4	2B30	55CE	Encrypt2	
4378	5	2C20	55D7	Run	

The 'Run' entry is highlighted with a red box in the original image.

ניתן לראות שהקובץ מייצא פונקציה שנקראת Run. עלינו להריץ אותה. DLL אינו קובץ הרצה, ולכן יש לנו מספר אפשרויות. אני השתמשתי בספריית ctypes של פיטון על מנת להריץ את ה-DLL:

1. `import ctypes`
2. `dll = ctypes.WinDLL("PassMasterExtension3_1.dll")`
3. `dll.Run()`

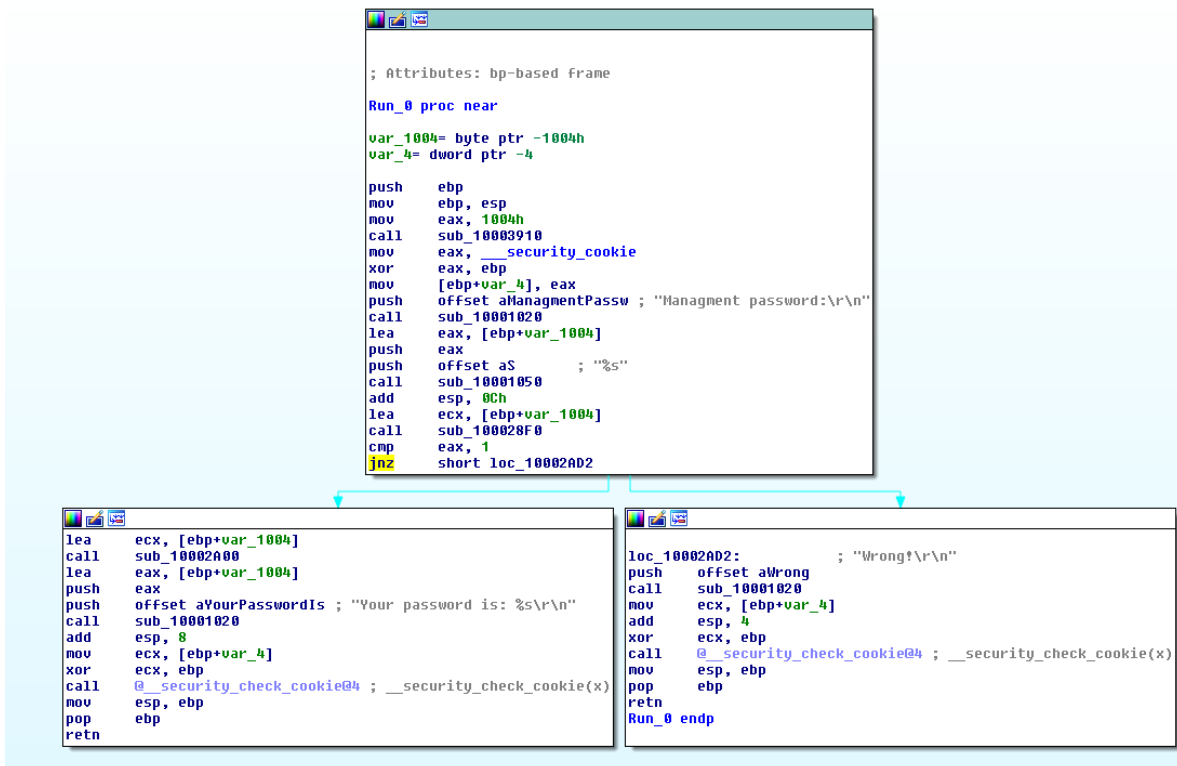
כשמריצים את הפונקציה, מגלים כי היא מבקשת את סיסמת הניהול. לכן, עלינו למצוא את סיסמת הניהול.

```
>>> import ctypes
>>> ctypes.WinDLL("PassMasterExtension3_1.dll").Run()
Managment password:
123456
Wrong!
8
```

אם נריץ את strings על הקובץ, נקבל מספר סיסמות:

- Pass1234567890ssaP
- AdminP@ssW0rd
- C2906BC87254
- SSecretP@sS

אולם אף אחת מהן היא לא סיסמת הניהול, ולא הסיימה של משתמש אדמין. נאלץ להשתמש ב-decompiler כדי להבין איך הוא בודק את סיסמת הניהול, והאם אפשר לדלג על הבדיקה. נפתח ב-IDA את ה-DLL, בפונקציה Run.

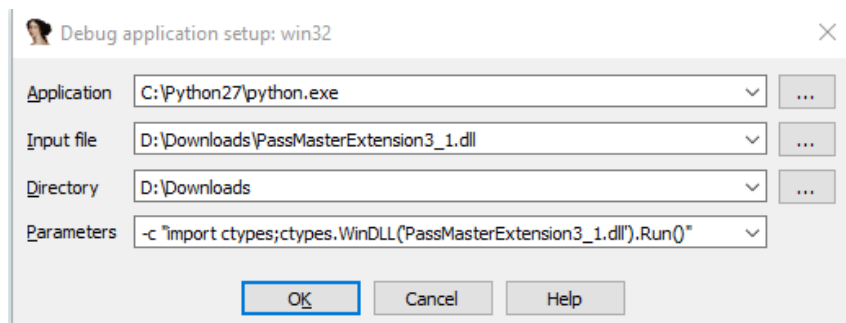


כפי שניתן לראות, יש jnz, כלומר jump not zero, שמבדיל בין סיסמה שגויה לסיסמה נכונה. בוא ננסה את הדרך הנאיבית ונקווה שמנגון יצור הסיסמה לא תלוי בסיסמה שאנחנו רושמים.

את הסקריפט שכתבנו מקודם ניתן להריץ ישירות דרך IDA, ובכך לדלג על הבדיקה בעצמו. נשנה את הגדרות Process options להגדרות הבאות:

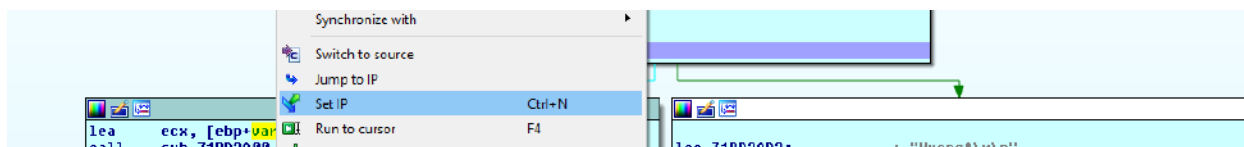
למה לא rundll32

הישום rundll32.exe מאפשר להריץ entry point מ-dll והוא מובנה בווינדוס. אולם, הוא לא console application ולכן איננו יכולים להזין לו stdin ולראות את ה-stdout שלו, שזאת בעיה.

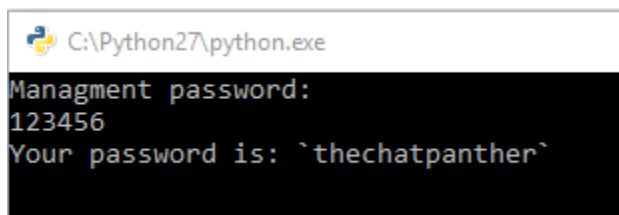


ניתן לראות שאני פשוט מריץ את הסקריפט ממקודם ישירות מ-IDA

נשים את ה-breakpoint בשורה של ה-jnz ונריץ במצב דיבאג. כשנגיע לשורה, פשוט נקבע את IP למקום שאליו אנו רוצים שיקפוץ:




נשים breakpoint נוסף בפקודת ה-retn שבסוף הבלוק, ונלחץ F9 על מנת לראות את הקלט:



קיבלנו את הסיסמה לאדמין. (שימו לב: הסיסמה משתנה בכל DLL שמורד).

ניתן גם לשנות את ה-JNZ ל-JZ ולשמור את השינוי ב-DLL. ההבדל בין 2 הפקודות הוא ביט יחיד. יש לשנות את הבית הראשון מ-74 ל-75


נתחבר ל-chatW1z עם הסיסמה:



--- chatW1z ---

Pending chatroom requests

Logout



About us...

Welcome to ChatMaster

Recent chatroom membership approval:

Request	Action
User 'cheetah' would like to access '50+'	<i>Approved</i>
User 'cheetah' would like to access 'art'	<i>Approved</i>
User 'cheetah' would like to access 'dating'	<i>Approved</i>
User 'cheetah' would like to access 'news'	<i>Approved</i>
User 'cheetah' would like to access 'politics'	<i>Approved</i>
User 'cheetah' would like to access 'sports'	<i>Approved</i>
User 'AgentC' would like to access 'sports'	Approve!

נאשר לעצמנו את הבקשה, ונכנס לחדר הצאט, כדי לבדוק מה cheetah שלנו כתב שמה.


AgentC
Welcome to the *sports* chatroom! (You are the only one in the room)

cheetah:
Hello!...Anyone here?
20:17

- user **cheetah** has left the room...

אם נעבור על כל חדר צאט ברשימה, נגלה שהתוכן זהה. המשתמש שאל אם יש כאן משהו, ועזב שכראה שאין אף אחד. משהו פה חשוד. יכול להיות שזה קשור לתפריט View all chatrooms שחסום לנו? אולי כן יש דרך לראות את הכל מבלי העמוד הזה?

אם נסתכל בקוד של רשימת הצאטים הזמינים שלנו, נגלה שהוא משתמש ב-REST כדי לקבל את רשימת הצאטים:

1. `$(document).ready(function(){`
2. `$.getJSON ('chatroomList', { u: 'apiuser', p: 'apipassword', utype: '1', rand: '62189305-cab1-4b5d-a607-f09847e1d2a7', a: '0', s: '1', g: '5', lat: '32.07973', long: '34.78369'}, populate)`

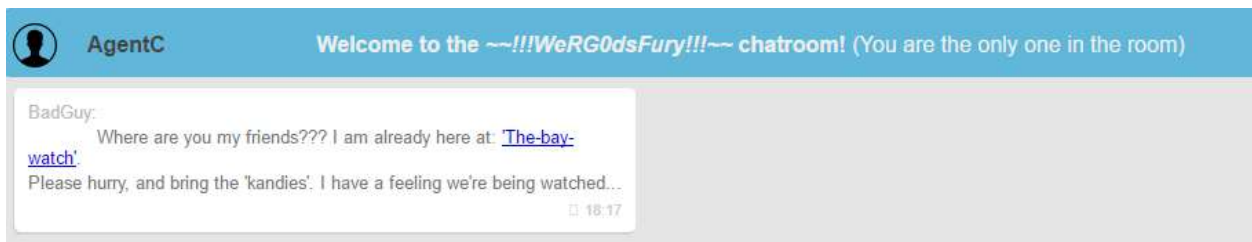
נכנס לדרך של הבקשה, ונקבל את רשימת הצאטים הזמינים לנו:

```
{
  - chatrooms: [
    "50+",
    "art",
    "dating",
    "news",
    "politics",
    "sports"
  ]
}
```

לאחר משחק עם הפרמטרים של הבקשה: שינוי utype מ-1 ל-0, ואת a מ-0 ל-1, נקבל את הרשימה המלאה:

```
{
  - chatrooms: [
    "*just chat*",
    "-Mossad challenge solutions-",
    "50+",
    "Mobile & gadgets",
    "Platinum dancing club",
    "__chat2go__",
    "art",
    "computing",
    "dating",
    "news",
    "politics",
    "sports",
    "~!!WeRG0dsFury!!~"
  ]
}
```

נערוך באתר את הסקריפט שיתן לנו את הרשימה המלאה, ונססה להתחבר לכל אחד מהצאנלים החדשים. האחרון כולל את הפתרון לאתגר:



נכנס לקישור, וסיימנו את האתגר הראשון.

Success!

Well Done!

You have successfully finished your 1st mission.
This is your success token:

You may now send your token and contact info to the following [email](#)

You can also collect and submit additional tokens by completing more challenges.

Take the

Next Challenge

TL;DR

- מצאנו פרצת אבטחה שמאפשרת לנו לנתק משתמשים אחרים לפי ערך הקוקית "eu". כתבנו סקריפט JS לקונסול שעובר על כל המשתמשים ומנתק אותם.
- מצאנו שמשמש האדמין הגדיר קובץ מסויים כרמז לסיסמה.
- חילצנו את קובץ ה-ZIP המוצפן באמצעות John the Ripper, יצא לנו קובץ DLL.
- הרצנו את ה-DLL באמצעות שימוש ב-ctypes של python ודיבגנו אותנו דרך הדיבאגר IDA. הצלחנו לחלץ את הסיסמה למשתמש האדמין ובכך השגנו את היכולת להצטרף לכל חדר צאט שיש לנו את השם שלו.
- מצאנו את רשימת הצאטים המלאה באמצעות שינוי הפרמטרים בפקודת ה-GET.
- התחברנו לצאנל האחרון ברשימה וסיימנו את האתגר.

Challenge #2

Well done Agent!

The location you recovered was correct and we dispatched our tactical team. However, the terrorist group was already gone by the time they arrived. We gathered enough intel to determine that the terrorists have planted a bomb on an airplane somewhere in the world, but we do not know the flight number and/or its destination.

We did however recover a [picture](#) of the bomb from the terrorist meeting.

Our *steganography* expert insists that the picture contains a hidden message, but she was unsuccessful in uncovering it before she left on her honeymoon. We require your assistance in locating and defusing the bomb before it detonates. There isn't much time...

Good luck!,
M.

נוריד את התמונה. נקבל תמונה של פצצה. ההומור של המוסד פשוט פצצה...



נשתמש בכלי אוטומטי שנקרא zsteg כדי לבדוק האם משהו מקודד בתמונה באחת מהדרכים המוכרות.

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
root@kali:~/Downloads# zsteg 0945c38c19f34dc780f37ccf3d520366.png
imagedata      .. text: "\nKSV$-'\n"
b1,b,lsb,xy    .. text: "\t{VyX_^0"
b1,bgr,lsb,xy  .. text: "L2NoYWxsZW5nZTIvYm9tYg=="
b2,r,lsb,xy    .. file: 5View capture file
b2,r,msb,xy    .. file: VISX image file
b2,g,lsb,xy    .. file: 5View capture file
b2,g,msb,xy    .. file: VISX image file
b2,b,lsb,xy    .. file: 5View capture file
b2,b,msb,xy    .. file: VISX image file
b2,rgb,lsb,xy  .. file: 5View capture file
b2,rgb,msb,xy  .. file: VISX image file
b2,bgr,lsb,xy  .. file: 5View capture file
b2,bgr,msb,xy  .. file: VISX image file
b4,r,msb,xy    .. text: ["w" repeated 9 times]
b4,g,msb,xy    .. text: ["w" repeated 14 times]
b4,b,msb,xy    .. text: ["w" repeated 10 times]
b4,rgb,msb,xy  .. text: ["w" repeated 28 times]
b4,bgr,msb,xy  .. text: ["w" repeated 29 times]
root@kali:~/Downloads#
```

קל לזהות שאחד מהפריטים Base64 decoded string. תוכנו הוא challenge2/bomb/. הגענו למרכז השליטה של הפצצה, ואין כמו ספירה לאחור בשביל להלחץ אותנו.

אתגר 2 – ניתוח FIRMWARE



כמו כל אדם שרואה כפתור אדום גדול, חשתי חובה מוסרית ללחוץ על Explode now, למרות הידיעה שאין ספק שזה יפגע פגיעה אנושה בסיכוי שלי להתקבל למוסד.

Explode Now!!

Oops... We are sorry!
It seems that you have purchased the *evaluation version*.
The option is supported only in the *Express* versions (or above).
Please contact support.

כמובן.

Disarm bomb מספק לנו יכולת לבטל את הפעלת הפצצה בהינתן ואנו יודעים את הסיסמה:

Disarm Bomb

Please enter your admin password below to disarm the bomb

<input type="text" value="Admin Password"/>	DEFUSE!
---	----------------

תפריט ניטרול הפצצה הידני נותן לנו עצה מעולה לנטרול הפצצה, אך לא עוזר:

Manual Defuse

Very Gently: cut the **RED** wire...

הפריט האחרון בתפריט כולל את המידע על הפצצה:

Item	Value
Model Number	#BMB123%UKFG%22311 C-4 edition
Serial Number	00000000000000000001
Status	Armed
Firmware Version	iExplode™ 5.4 Beta edition
License	None (Evaluation version)
Plastic (standard) Plugin	Installed
Anthrax Plugin	Not installed
Extra Damage Plugin	Not installed
Mass Destruction Plugin	Not supported

נלחץ על הקישור ל-firmware, וירד לנו קובץ ה-firmware. זהו קובץ zip שמכיל בתוכו קובץ נוסף. 7-zip מסכים לפתוח גם אותו, אז אין צורך לגלות מהו הסוג שלו. בתוכו, יש הפצה של לינוקס, לפחות לפי הקבצים:

```
yoavst@DESKTOP-TCDTCLB:/mnt/d/Downloads/os$ ls
bin  dev  etc  lib  lost+found  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var
```

אנחנו מחפשים את הסיסמה לפצצה שאותה צריך להזין בדף האינטרנט של הפצצה. לכן, ניגש לתקייה `/var/www` ששמה בדרך כלל מצוי סרבר ה-HTTP. ואכן כך.

```
yoavst@DESKTOP-TCDTCLB:/mnt/d/Downloads/os$ cd var/www
yoavst@DESKTOP-TCDTCLB:/mnt/d/Downloads/os/var/www$ ls
iexceptions.py  iexplode.py  iexplode.wsgi  Pmgmt.pyc
```

יש בתקייה 2 קבצי פייטון, הגדרת סרבר, וקובץ פייטון מקומפל. ננסה ראשון את `iexplode.py`.

מיד עם הכניסה נראה את הקוד הבא:

```
def do_login(environ, start_response):
    try:
        if environ["REQUEST_METHOD"] != "POST":
            raise NotLoggedIn()

        login_data = environ["wsgi.input"].read(100)

        data = parse_qs(login_data)

        if data["pass"][0] != "M@ster":
            raise NotLoggedIn()

        cookie_str = str(uuid4())

        write_new_session(cookie_str)

        cookie = SimpleCookie()
        cookie["SessionId"] = cookie_str

        raise RedirectPage("/", [{"Set-Cookie", cookie["SessionId"].OutputString()}])
    except RedirectPage:
        raise
    except Exception:
        raise NotLoggedIn()
```

טוב, אז `M@ster` זאת הסיסמה? לא! ואפילו יותר גרוע, נשאר לנו רק 2 ניסיונות לנטרל את הפצצה. נגלול למטה ונראה את הקוד של דף נטרול הפצצה:

```
def defuse_page(environ, start_response):
    try:
        if environ["REQUEST_METHOD"] != "POST":
            raise ErrorPage("500 Internal Server Error", "")

        defuse_data = environ["wsgi.input"].read(100)
        defuse_data = parse_qs(defuse_data)

        if Pmgmt.CheckPassword(defuse_data["defusecode"][0]):
            start_response("200 OK", [{"Content-Type", "text/html"}])
```

הקוד שבדק את הסיסמה נמצא בקובץ `Pmgmt.pyc`.

נפעיל פייטון, ונריץ dir על ה-module כדי לראות את כל הפונקציות שלו:

```
>>> import Pmgmt
>>> dir(Pmgmt)
['CheckPassword', 'GetManagmentVersion', 'GetMasterPassword', 'GetPassword', 'GetRandomPassword', 'MakePassword',
 '__PASS__', '__builtins__', '__doc__', '__file__', '__name__', '__package__', 'random']
```

ננסה את הפונקציות שמחזירות את הסיסמה:

```
>>> Pmgmt.GetMasterPassword()
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
  File "Pmgmt.py", line 80, in GetMasterPassword
Exception: Not implemented for this iExplode version
>>> Pmgmt.GetPassword()
Problem reading index from /etc/iexprun
```

הפונקציה קוראת את האינדקס מהקובץ /etc/iexprun. נעתיק את הקובץ מהבוקש מה-framework ל-etc שלנו, ונריץ שוב. נקבל שהסיסמה שלנו היא implosion-bomb (הערה: לכל קובץ יש סיסמה אחרת). נזין את הסיסמה וננטרל את הפצצה.

Success!

Well Done!

You have successfully finished your 2nd mission.
This is your success token:

You may now send your token and contact info to the following [email](#)

You can also collect the last token by completing the final challenge!

Take the [Next Challenge](#)

בנוס

אם נריץ Uncompyle6 על הקובץ Pmgmt, נקבל שהוא מכיל מערך של 50 סיסמאות שנקרא PASS. הפעולה GetPassword קוראת את המספר שנמצא בקובץ /etc/iexprun, ומחזירה את האיבר שנמצא במקום ההוא במערך.

Challenge #3

You did it again!

The bomb you defused was discovered soon after the airplane landed (seems that someone posted an anonymous tip to local authorities...).
 Additionally, we have been able to recruit an agent within the terrorist cell.
 We are unable to maintain constant contact with him as the agent is deep undercover.
 However, he did manage to post a [message](#) to our secure servers. We require your skills once again in order to follow the communication trail and reveal the message.

Thanks, and good luck!,
 M.

נוריד את ההודעה ונקבל קובץ pcap (הקובץ כולל את המילים Dumpcap ולכן היה זה ניחוש סביר). נפתח אותו באמצעות Wireshark ונקבל הסנפה של שיחה בין הכתובת 192.168.200.134 ל 192.168.200.136. השיחה מתבצעת ב-2 פרוטוקולים, ICMP ו-TCP.

אם נעשה Follow TCP stream נקבל את ההתחלה הבאה

```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 5fa96f985c514a27a96e0823ffb64460
220 (vsFTPd 3.0.2)
AUTH SSL
234 Proceed with negotiation.
  
```

מדובר כאן בפרוטוקול FTPS שהוא FTP מעל SSL, אשר פועל בפורט 990. עלינו למצוא את המפתח הפרטי שאיתו התבצעה השיחה. נבדוק את המידע שמכילות פקטות ה-ICMP באמצעות scapy:

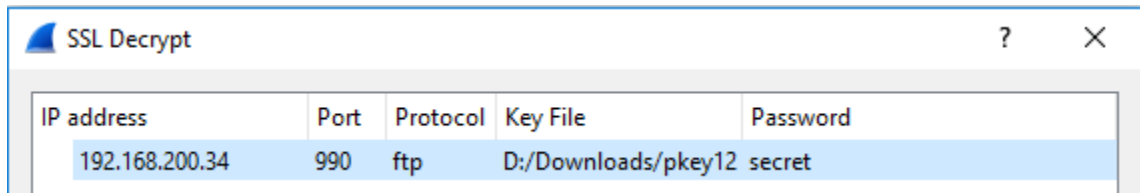
```

>>> p = rdpcap("5fa96f985c514a27a96e0823ffb64460.pcap")
>>> icmps = filter(lambda packet: ICMP in packet, p)
>>> messages = set(map(lambda packet: packet[Raw].load, icmps))
>>> for message in messages:
...     print message
...
τ%0X      X
@          @@@@@@@@@@@@@@@@@@1234567
r%0X      °@          @@@@@@@@@@@@@@@@@@1234567
β%0X      è|@          @@@@@@@@@@@@@@@@@@1234567
÷%0X      ú@@          @@@@@@@@@@@@@@@@@@1234567
≤%0X      +@@          @@@@@@@@@@@@@@@@@@1234567
r%0X      β|@          /challenge3/pkey/challenge3/pkey/challen
θ%0X      i@@          @@@@@@@@@@@@@@@@@@1234567
f%0X      @          @@@@@@@@@@@@@@@@@@1234567
r%0X      (σ@          /challenge3/abcd/challenge3/abcd/challen
r%0X      5~@          @@@@@@@@@@@@@@@@@@1234567
~%0X      Ü@@          @@@@@@@@@@@@@@@@@@1234567
| %0X      β°@          @@@@@@@@@@@@@@@@@@1234567
±%0X      °@@          @@@@@@@@@@@@@@@@@@1234567
n%0X      ■@@          @@@@@@@@@@@@@@@@@@1234567
r%0X      Å|@          @@@@@@@@@@@@@@@@@@1234567
π%0X      °@          @@@@@@@@@@@@@@@@@@1234567
0%0X      ú@@          @@@@@@@@@@@@@@@@@@1234567
@          @@@@@@@@@@@@@@@@@@1234567
μ%0X      r @          @@@@@@@@@@@@@@@@@@1234567
φ%0X      i @          @@@@@@@@@@@@@@@@@@1234567
ε%0X      |@@          @@@@@@@@@@@@@@@@@@1234567
T%0X      ¿~@          @@@@@@@@@@@@@@@@@@1234567
| %0X      È|@          @@@@@@@@@@@@@@@@@@1234567
| %0X      i@@          @@@@@@@@@@@@@@@@@@1234567
- %0X      T^@          @@@@@@@@@@@@@@@@@@1234567
| %0X      8+@          @@@@@@@@@@@@@@@@@@1234567
| %0X      Lh@          @@@@@@@@@@@@@@@@@@1234567
+ %0X      ]~@          @@@@@@@@@@@@@@@@@@1234567
r%0X      2r@          secret          secret          secret
σ%0X      Γ·@          @@@@@@@@@@@@@@@@@@1234567
Ω%0X      @          @@@@@@@@@@@@@@@@@@1234567
δ%0X      V@@          @@@@@@@@@@@@@@@@@@1234567
L%0X      @@@          @@@@@@@@@@@@@@@@@@1234567
ll%0X      >~@          @@@@@@@@@@@@@@@@@@1234567
T%0X      &%@          @@@@@@@@@@@@@@@@@@1234567
Σ%0X      ÷~@          @@@@@@@@@@@@@@@@@@1234567
α%0X      q·@          @@@@@@@@@@@@@@@@@@1234567
≥%0X      k@@          @@@@@@@@@@@@@@@@@@1234567
≡%0X      @@@          @@@@@@@@@@@@@@@@@@1234567
r%0X      <·@          @@@@@@@@@@@@@@@@@@1234567
[ %0X      ' @          @@@@@@@@@@@@@@@@@@1234567
+ %0X      @~@          @@@@@@@@@@@@@@@@@@1234567
| %0X      V^@          @@@@@@@@@@@@@@@@@@1234567

```

ניתן לראות שיש 2 קישורים, אחד הוא /challenge3/abcd והשני הוא /challenge3/pkey.

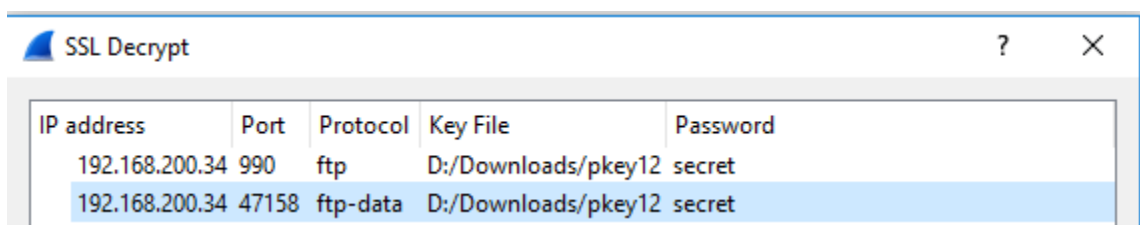
הקובץ abcd הוא קובץ טקסט שנראה זהה לערך של המוסד בויקיפדיה. הקובץ pkey הוא בהחלט private key. אולם אנחנו עדיין צריך את ה-passphrase שלו. גם הוא מופיע ב-CMP, והוא secret. מעולה! נוסף את ה-private key ל-scapy על מנת שיפענח את הבקשות TCP המוצפנות. אולם wireshark מתלונן שהקובץ לא בפורמט האהוב עליו. כמה חבל בשבילו. נמיר אותו: openssl pkcs12 -export -nocerts -inkey pkey -out pkey12. עכשיו wireshark לא מתלונן.



עכשיו כשהבקשות מופענחות, נשתמש ב-filter של ftp כדי לקבל את הדיאלוג:

No.	Time	Source	Destination	Proto	Lengt	Info
29	6.293292	192.168.200.134	192.168.200...	FTP	107	Request: USER user1
30	6.293481	192.168.200.136	192.168.200...	FTP	129	Response: 331 Please specify the password.
36	8.332458	192.168.200.134	192.168.200...	FTP	106	Request: PASS 1234
37	8.339872	192.168.200.136	192.168.200...	FTP	118	Response: 230 Login successful.
39	8.340002	192.168.200.134	192.168.200...	FTP	101	Request: SYST
40	8.340365	192.168.200.136	192.168.200...	FTP	114	Response: 215 UNIX Type: L8
54	10.492322	192.168.200.134	192.168.200...	FTP	106	Request: CWD files
55	10.493155	192.168.200.136	192.168.200...	FTP	132	Response: 250 Directory successfully changed.
61	12.884246	192.168.200.134	192.168.200...	FTP	103	Request: TYPE I
62	12.884559	192.168.200.136	192.168.200...	FTP	126	Response: 200 Switching to Binary mode.
64	12.884690	192.168.200.134	192.168.200...	FTP	124	Request: PORT 192,168,200,134,184,54
65	12.884857	192.168.200.136	192.168.200...	FTP	146	Response: 200 PORT command successful. Consider using PASV.
66	12.884906	192.168.200.134	192.168.200...	FTP	103	Request: RETR 1
70	12.885393	192.168.200.136	192.168.200...	FTP	157	Response: 150 Opening BINARY mode data connection for 1 (10121 bytes).
82	12.887645	192.168.200.136	192.168.200...	FTP	119	Response: 226 Transfer complete.
92	16.411690	192.168.200.134	192.168.200...	FTP	101	Request: QUIT
93	16.412108	192.168.200.136	192.168.200...	FTP	109	Response: 221 Goodbye.

ניתן לראות שנשלח קובץ בינארי ביניהם. כדי שנוכל לראות אותו, נצטרך לפענח את בקשת השליחה, שהיא בפורט אחר, עם אותו המפתח:



עכשיו נוכל להריץ את הפילטר של ftp-data. יש בקשה אחת

No.	Time	Source	Destination	Proto	Lengt	Info
76	12.886735	192.168.200.136	192.168.200...	FTP...	102...	FTP Data: 10121 bytes

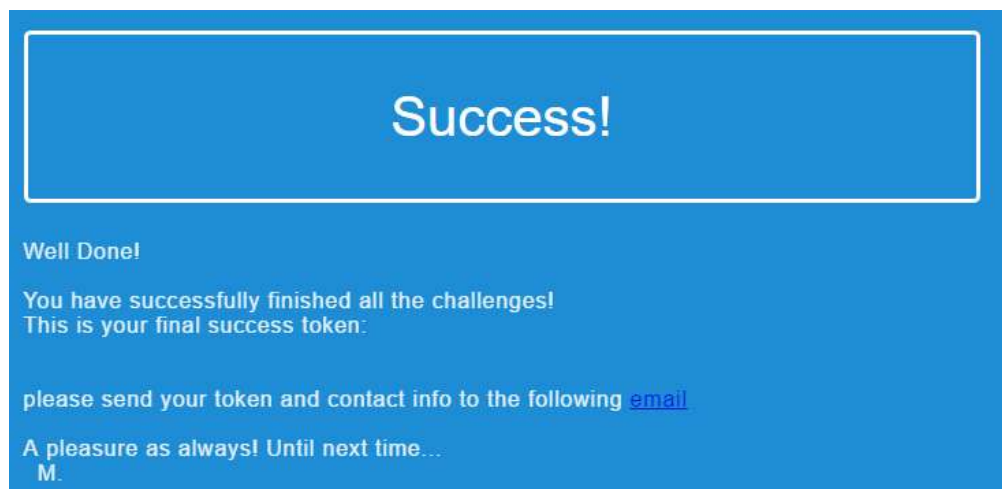
נחלץ את ה-data שלה ונקבל קובץ. הקובץ אומנם מתחיל ב-PK ולכן הוא zip, אבל הוא בעצם xls שהוא פורמט מבוסס zip. נפתח את הקובץ עם אקסל ונקבל את טבלת הקניות של הסוכן הסמוי שלנו:

	item	price
1	Milk	12894
2	Bread	6665
3	Honey	1738
4	Butter	23193
5	Eggs	24671
6	Tomatoes	7066
7	Ice cream	11652
8	Broccoli	10160
9	Asparagus	15725
10	Yogurt	21028
11	Apples	15793
12	Cheese	1032
13	Pita Bread	1160
14	Sugar	6941
15	Flour	28133
16	Cookies	20504
17		

טוב, יש לנו מספרים, ויש לנו את קובץ הטקסט ממקודם. אינדקסים אולי? ננסה:

```
1. with open("411310ed0d6c43eb8db50ddd20202421", 'r') as f:
2.     text = f.read()
3.
4.     arr = [12894, 6665, 1738, 23193, 24671, 7066, 11652, 10160, 15725, 21028, 15793, 1032, 1160, 6941, 281
5.           33, 20504]
6.
7.     result = ""
8.     for i in arr:
9.         result += text[i]
10.    print result
```

הסקריפט מדפיס " /challenge3/b3f5", ניגש לכתובת, וסיימנו את האתגר!



Success!

Well Done!

You have successfully finished all the challenges!
This is your final success token:

please send your token and contact info to the following [email](#)

A pleasure as always! Until next time...
M.

קרדיטים

פתרון האתגר וכתובת מדריך זה לא היו מתאפשרים ללא עזרתם של האנשים הבאים:

- ההורים שלי, שהביאוני עד הלום.
- ניר חסן – שכתב את הסקריפט של רשימת ההמתנה לשימוש ב-ES6 במקום במאקרו של ווינדוס, השתמש ב-ZSTEG, והכי חשוב, שעבר על כל הפרמטרים של פקודת ה-GET של רשימת הצאטים עד אמצע הלילה.
- תומר טלגם – שהכריח אותי לכתוב את המדריך הזה