

WriteUp Jeopardy Nasional
LKS Nasional 2024
Provinsi Jawa Timur



SMKS TELKOM MALANG

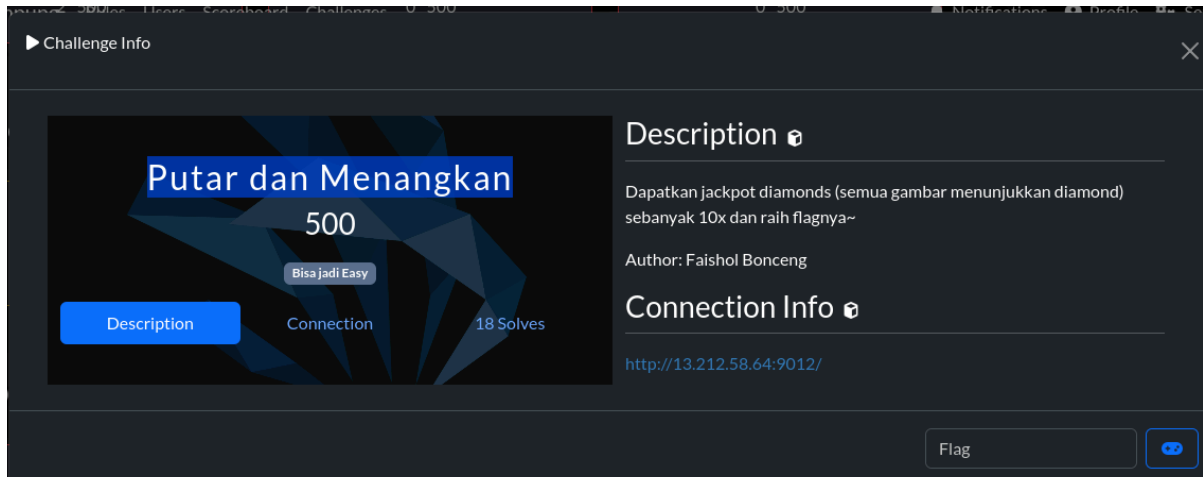
DANIEL DHANISWARA
FARHAN DIWAN ANANTA

Daftar Isi

Daftar Isi.....	1
[Web Exploitation].....	2
Putar dan Menangkan.....	2
Flag:	
LKSN{jangan_ya_dek_ya__jangan_buka_web_semacam_ini_ya_dek_ya}	3
[Cryptography].....	4
Modifikasi.....	4
Flag:	
LKSN{bb61f6f3aacf84db45ee046bbf4edd55b0c11f52367f46fdb11b792833dece11}	6
[Reverse].....	7
Jurassic Pwner.....	7
Flag:	
LKSN{you_reached_the_super_duper_high_score_you_dirty_ch34t3rrrrRrrrrawr!}	9
[Forensic].....	10
Tales of LKSN Crimes #3 - APT-41 Devil's Curriculum.....	10
Flag:	
LKSN{y0u_h4ve_overcome_the_b3ginner_Linux_Memf0ren_such_daredevils5s5s5!}	14

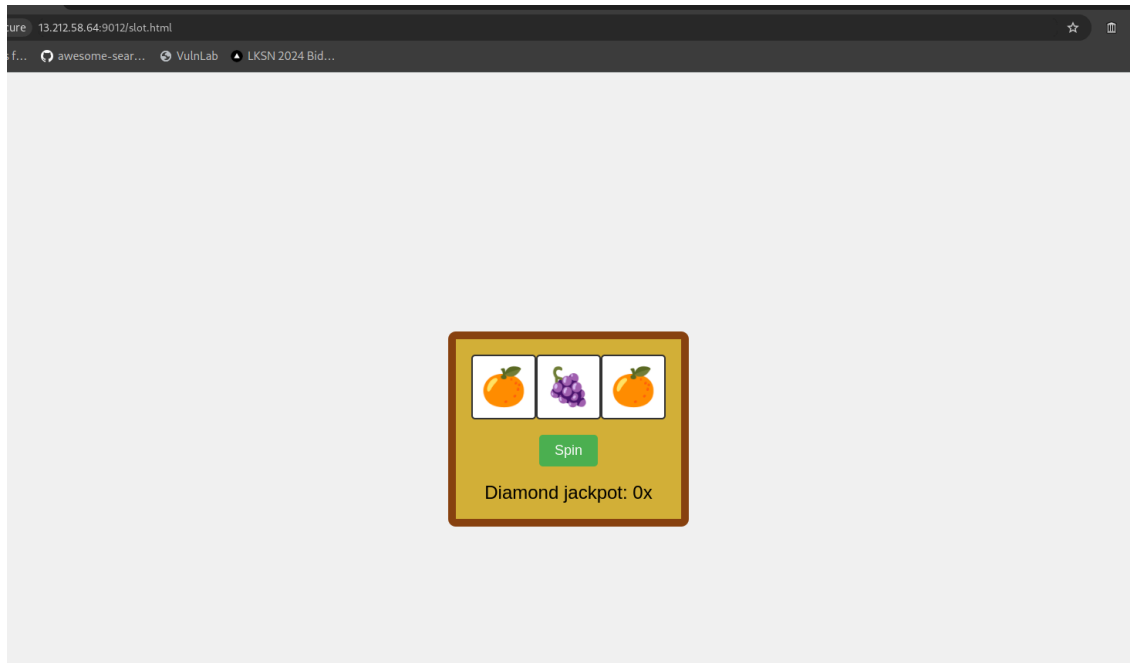
[Web Exploitation]

Putar dan Menangkan



Overview

Berikut adalah tampilan dari webnya.



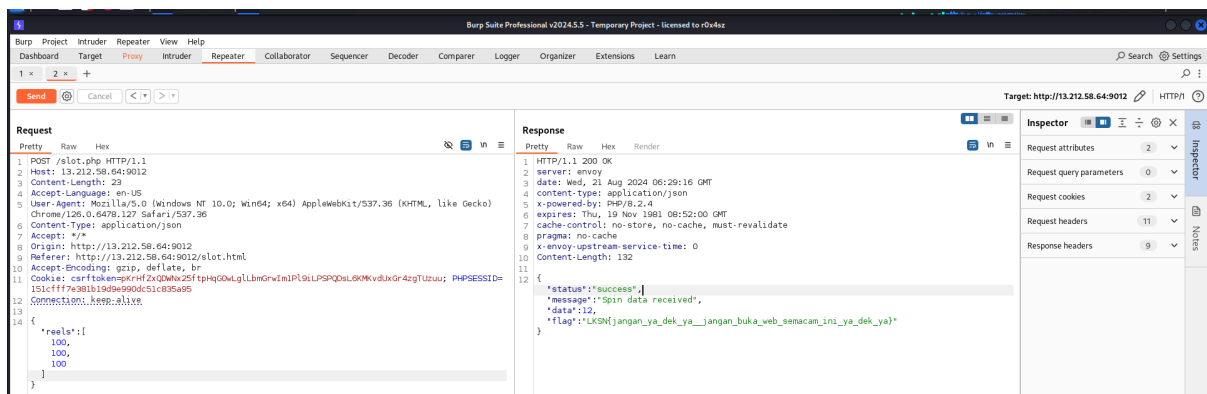
dan setelah saya tekan spin, webnya mengirimkan post request seperti ini

```
POST /slot.php HTTP/1.1
```

```
Host: 13.212.58.64:9012
Content-Length: 20
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127
Safari/537.36
Content-Type: application/json
Accept: */*
Origin: http://13.212.58.64:9012
Referer: http://13.212.58.64:9012/slot.html
Accept-Encoding: gzip, deflate, br
Cookie:
csrftoken=pKrHfZxQDWNx25ftpHqG0wLgLLbmGrwIm1Pl9iLPSPQDsL6KMKv
dUxGr4zgTUzUU; PHPSESSID=151cfff7e381b19d9e990dc51c835a95
Connection: keep-alive

{"reels": [50, 10, 10]}
```

ya sudah tinggal kita samakan saja semuanya jadi reels 100 dan send berulang kali dan yey

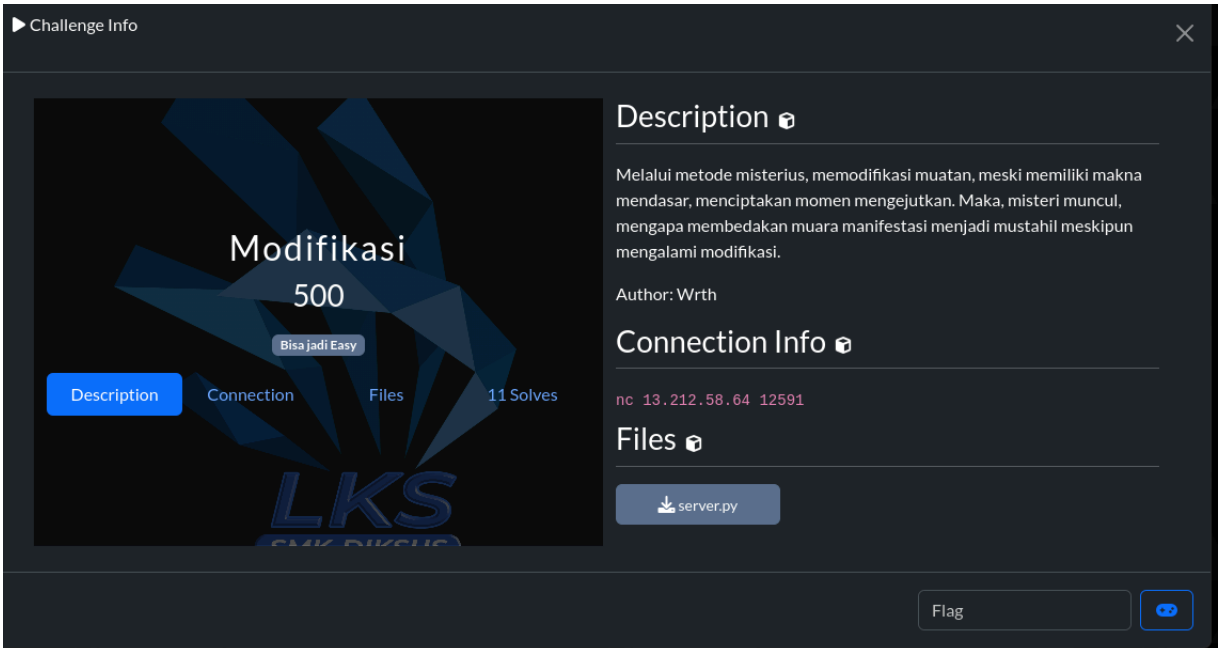


Flag:

LKSN{jangan_ya_dek_ya__jangan_buka_web_semacam_ini_ya_dek_ya}

[Cryptography]

Modifikasi



The screenshot shows a challenge interface for 'Modifikasi' with a score of 500 and 11 solves. The interface includes a description, connection info, and a file named 'server.py'. The description is in Indonesian and discusses modifying content. The connection info shows 'nc 13.212.58.64 12591'. The file 'server.py' is available for download. The interface also has a 'Flag' input field and a 'Bisa jadi Easy' badge.

Challenge Info

Modifikasi
500
Bisa jadi Easy

Description | Connection | Files | 11 Solves

Description

Melalui metode misterius, memodifikasi muatan, meski memiliki makna mendasar, menciptakan momen mengejutkan. Maka, misteri muncul, mengapa membedakan muara manifestasi menjadi mustahil meskipun mengalami modifikasi.

Author: Wrth

Connection Info

nc 13.212.58.64 12591

Files

server.py

Flag

Overview

Diberikan sebuah file server.py yang dimana vulnnya di md5 collision

```

from hashlib import md5

print("Anda sedang menjual tiket konser taylor swift")
print("Terdapat 2 pembeli yang ingin membeli tiket, Alice dan Bob. Sayangnya tiket hanya tersisa 1")
print("Tiket tersebut diverifikasi menggunakan md5")
print("Dapatkah anda membuat tiket palsu untuk dijual ke Bob?")

alice = bytes.fromhex(input("Masukkan kode tiket untuk dijual ke Alice: "))
md5alice = md5(alice).digest()
print("md5 dari tiket Alice:", md5alice.hex())

bob = bytes.fromhex(input("Masukkan kode tiket buatan untuk dijual ke Bob: "))
md5bob = md5(bob).digest()
if alice == bob:
    print("Bob: Hey apa apaan ini, ini sama persis dengan tiket Alice!")
    exit()

print("md5 dari tiket Bob:", md5bob.hex())
if alice != bob and md5bob == md5alice:
    print("Bob: Terima kasih! Ini bayarannya")
    print(open("flag.txt").read())
else:
    print("Bob: Hey apa apaan ini, ini bukan tiket asli!")

```

referensi : [stackoverflow](#)

input 1

```
4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3d
c0783e7b9518afbfa200a8284bf36e8e4b55b35f427593d84967
6da0d1555d8360fb5f07fea2
```

input 2

```
4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3d
c0783e7b9518afbfa202a8284bf36e8e4b55b35f427593d84967
6da0d1d55d8360fb5f07fea2
```

→ Modifikasi nc 13.212.58.64 12591

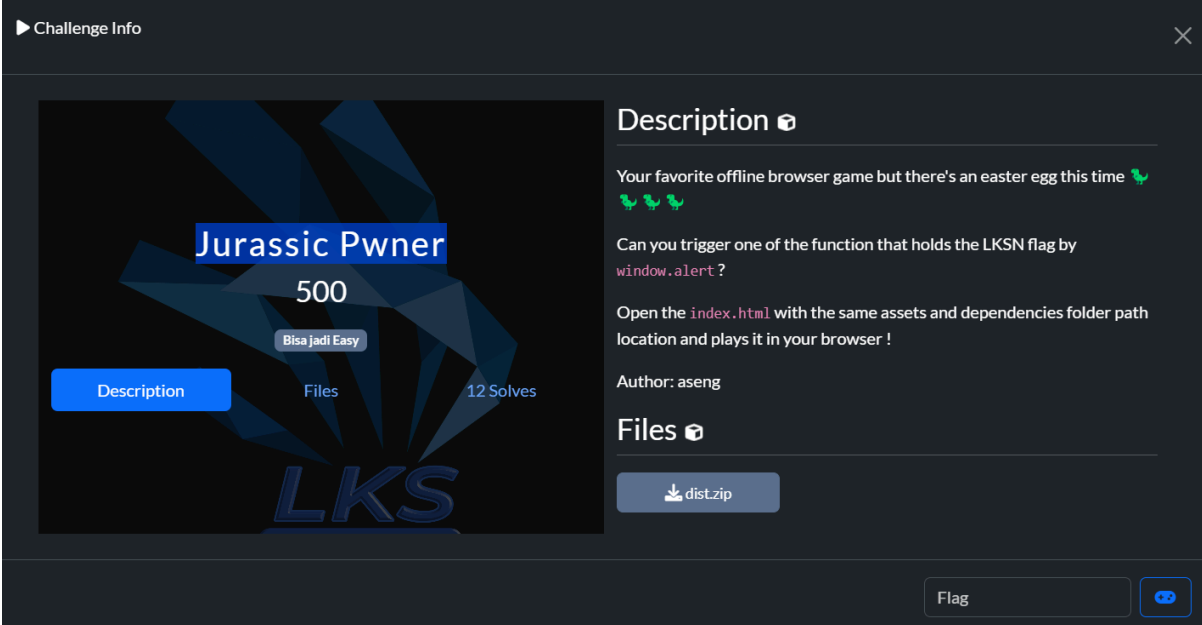
```
Anda sedang menjual tiket konser taylor swift
Terdapat 2 pembeli yang ingin membeli tiket, Alice dan Bob. Sayangnya tiket hanya tersisa 1
Tiket tersebut diverifikasi menggunakan md5
Dapatkah anda membuat tiket palsu untuk dijual ke Bob?
Masukkan kode tiket untuk dijual ke Alice: 4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783e7b95
fea2
md5 dari tiket Alice: @08ee33a9d58b51cfb425b0959121c9
Masukkan kode tiket buatan untuk dijual ke Bob: 4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783
b5f07fea2
md5 dari tiket Bob: @08ee33a9d58b51cfb425b0959121c9
Bob: Terima kasih! Ini bayarannya
LKSN{bb61f6f3aacf84db45ee046bbf4edd55b0c11f52367f46fdb11b792833dece11}
```

Flag:

```
LKSN{bb61f6f3aacf84db45ee046bbf4edd55b0c11f52367f46fd
b11b792833dece11}
```

[Reverse]

Jurassic Pwner



Challenge Info

Jurassic Pwner
500
Bisa jadi Easy
Description Files 12 Solves
LKSN

Description

Your favorite offline browser game but there's an easter egg this time 🐲🐲🐲

Can you trigger one of the function that holds the LKSN flag by `window.alert?`

Open the `index.html` with the same assets and dependencies folder path location and plays it in your browser !

Author: aseng

Files

dist.zip

Flag

Attachment

[chall.zip](#)

Overview

Pada challenge kali ini diberikan sebuah web yang bisa kita jalankan secara local dan nampak sama seperti game dino ketika tidak terkoneksi internet di chrome.

Solve

Kita menemukan function `get_LKSN_Flag` yang dimana itu adalah function untuk decrypt dengan cara xor flag dengan `hr` dan menampilkan flag sebagai popup allert.


```

get_LKSN_Flag: function() {
    var hr = this.run();
    const flag = 4830690556514140397518897252109979335664677923435018942901273242454015697691068037340554551586759138432178879438287937684165299693520135533018994309974094302098369656069901396834;
    const p1 = 294704857459121458995842604700946850751n;
    const p2 = 314052721216923470597325825556277950411n;
    const res = 54846125195579777053464962994274277267744411269096779149171289487630586305476n;
    if ((hr ** 65537n) % (p1 * p2) == res) {
        window.alert(transform(hr ^ flag));
    } else {
        window.alert("You need to reach a super high score!");
    }
},

```

Yang perlu kita lakukan yaitu mencari nilai hr yang didapat dari encrypt rsa. Karena kita sudah mengetahui beberapa hal yang dibutuhkan, kita tinggal membuat solver dari chall ini.

```

from Crypto.Util.number import *

flag =
4830690556514140397518897252109979335664677923435018
9429012732424540156976910680373405545515867591384321
7887943828793768416529969352013553301899430997409430
2098369656069901396834
p1 = 294704857459121458995842604700946850751
p2 = 314052721216923470597325825556277950411
e = 65537
res =
5484612519557977705346496299427427726774441126909677
9149171289487630586305476

n = p1*p2
phi = (p1-1) * (p2-1)
d = inverse(e, phi)
HR = pow(res, d, n)

print("HR = ", HR)
print("Flag = ",long_to_bytes(flag^HR))

print("Flag = ",long_to_bytes(flag^key))

```

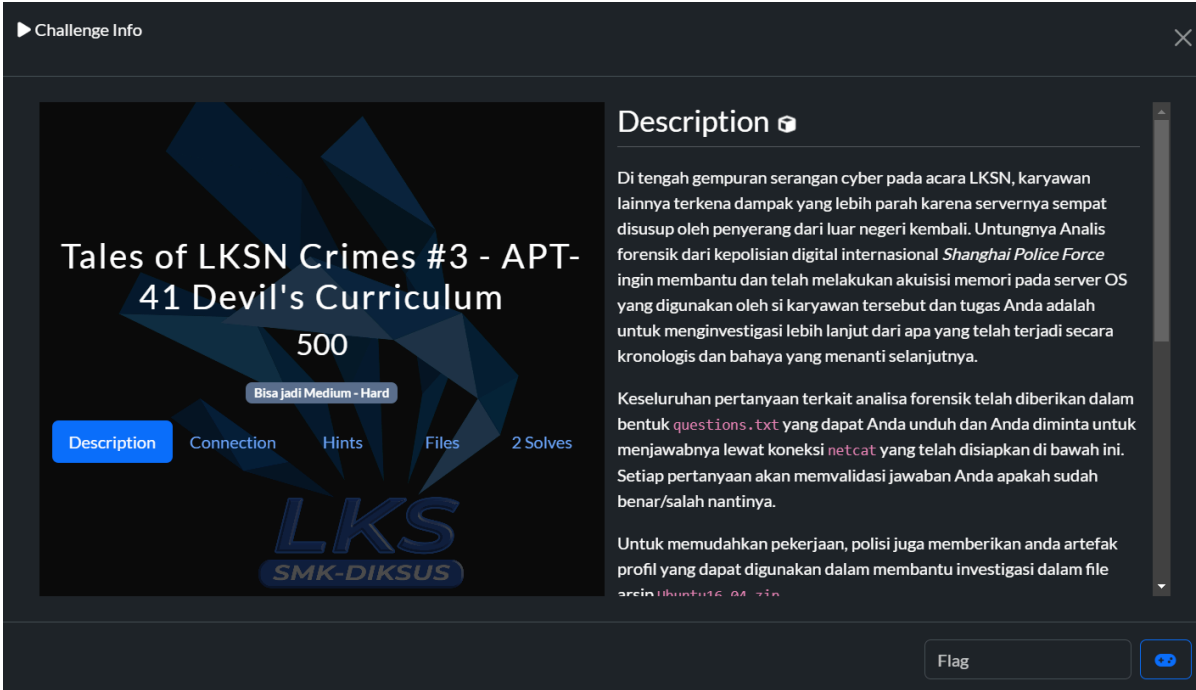
```
b'LKSN{you_reached_the_super_duper_high_score_you_dirty_ch34t3rrrrRrrrrawr!}'  
> python dist/solve.py  
HR = 13377331133773137113377113377311  
Flag = b'LKSN{you_reached_the_super_duper_high_score_you_dirty_ch34t3rrrrRrrrrawr!}'
```

Flag:

LKSN{you_reached_the_super_duper_high_score_you_dirty_ch34t3rrrrRrrrrawr!}

[Forensic]

Tales of LKSN Crimes #3 - APT-41 Devil's Curriculum



The screenshot shows a challenge interface with a dark theme. On the left, a card displays the challenge title 'Tales of LKSN Crimes #3 - APT-41 Devil's Curriculum' with a score of 500 and a difficulty level of 'Bisa jadi Medium - Hard'. Below the title are tabs for 'Description', 'Connection', 'Hints', 'Files', and '2 Solves'. The 'Description' tab is active. On the right, the 'Description' section contains the following text:

Di tengah gempuran serangan cyber pada acara LKSN, karyawan lainnya terkena dampak yang lebih parah karena servernya sempat disusup oleh penyerang dari luar negeri kembali. Untungnya Analis forensik dari kepolisian digital internasional *Shanghai Police Force* ingin membantu dan telah melakukan akuisisi memori pada server OS yang digunakan oleh si karyawan tersebut dan tugas Anda adalah untuk menginvestigasi lebih lanjut dari apa yang telah terjadi secara kronologis dan bahaya yang menanti selanjutnya.

Keseluruhan pertanyaan terkait analisa forensik telah diberikan dalam bentuk `questions.txt` yang dapat Anda unduh dan Anda diminta untuk menjawabnya lewat koneksi `netcat` yang telah disiapkan di bawah ini. Setiap pertanyaan akan memvalidasi jawaban Anda apakah sudah benar/salah nantinya.

Untuk memudahkan pekerjaan, polisi juga memberikan anda artefak profil yang dapat digunakan dalam membantu investigasi dalam file `arcin@ubuntu16_04.zip`

At the bottom of the interface, there is a 'Flag' input field and a 'Submit' button.

Overview

Dari deskripsi soal ini, kita diminta untuk melakukan memori forensik terhadap memori dump yang telah diberikan. Kita diberi beberapa pertanyaan yang harus di jawab untuk mendapatkan flag.

Attachment

[Ubuntu16_04.zip](#)

[questions.txt](#)

[nuclear.zip](#)

Solve

Hal yang pertama dan paling penting untuk mengerjakan challenge ini adalah import profile yang telah

diberikan di attachment. copy ke path/volatility/volatility/plugins/overlays/linux

```
> pwd
/tools/volatility/volatility/plugins/overlays/linux
> ls
elf.py  elf.pyc  __init__.py  __init__.pyc  linux.py  linux.pyc  Ubuntu16_04.zip
```

setelah itu cek profile dengan command

```
python vol.py --info | grep -i profile
```

```
> vol2 --info | grep -i profile
Volatility Foundation Volatility Framework 2.6.1
Profiles
LinuxUbuntu16_04x64 - A Profile for Linux Ubuntu16_04 x64
VistaSP0x64 - A Profile for Windows Vista SP0 x64
VistaSP0x86 - A Profile for Windows Vista SP0 x86
VistaSP1x64 - A Profile for Windows Vista SP1 x64
VistaSP1x86 - A Profile for Windows Vista SP1 x86
VistaSP2x64 - A Profile for Windows Vista SP2 x64
VistaSP2x86 - A Profile for Windows Vista SP2 x86
Win10x64 - A Profile for Windows 10 x64
Win10x64_10240_17770 - A Profile for Windows 10 x64 (10.0.10240.17770 / 2018-02-10)
Win10x64_10586 - A Profile for Windows 10 x64 (10.0.10586.306 / 2016-04-23)
Win10x64_14393 - A Profile for Windows 10 x64 (10.0.14393.0 / 2016-07-16)
Win10x64_15063 - A Profile for Windows 10 x64 (10.0.15063.0 / 2017-04-04)
```

jika berhasil maka akan ada profile LinuxUbuntu16_04x64 yang dimana itu adalah profile yang kita import.

Pertanyaan 1. The attacker seems to build a custom rootkit-like kernel object to the victim OS. What's the kernel module load address for that rootkit?

Pertama kita menggunakan plugin linux_bash terlebih dahulu untuk mengetahui apa yang penyerang lakukan.

```
vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem
linux_lsmod
```

kita menemukan ada satu modul kernel yang memiliki nama mencurigakan, yaitu evilrootkit.

```
> vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem linux_lsmod
Volatility Foundation Volatility Framework 2.6.1
ffffffffffc0551000 evilrootkit 16384
ffffffffffc0530040 lime 16384
ffffffffffc05371c0 vmw_balloon 20480
ffffffffffc054b900 snd_ens1371 28672
```

kami ambil nilai hex dari evilrootkit dan kemudian kami tambahkan 0x agar sesuai dengan format jawaban. Jawaban: 0xffffffffc0551000

pertanyaan 2. There's a zip file that is created by the user. This file is password-protected and it is cached. In what inode number that this file is cached?

Pada saat membuat zip penyerang pastinya menjalankan command zip pada bash, maka dari itu kita gunakan plugin linux_bash untuk mengetahui command bash yang dijalankan oleh penyerang

```
vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem
linux_bash
```

Dari sini kita mengetahui bahwa penyerang membuat file zip dengan nama confidential.zip. Kemudian kita menggunakan plugin linux_enumerate_files

```
vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem
linux_enumerate_files
```

dari sini kita bisa mendapatkan inode dari confidential.zip

```
0x0 ----- /tmp/home/victim/0
0xffff880077d5ee98 2095015 /tmp/home/victim/confidential.zip
0x0 ----- /tmp/home/victim/.secret.txt.swp
```

Jawaban: 2095015

pertanyaan 3. It seems the password that is used for the zip file is stored in a linux variable. Can you find its variable name? And what is the value of that? This will indicate its password

pada pertanyaan sebelumnya kita mencari command bash yang di run oleh penyerang dan kita menemukan command dimana penyerang membuat variabel dengan nama FANATIC yang digunakan untuk password file zip tersebut

```
1381 bash 2024-08-12 14:03:50 UTC+0000 openssl passwd -ne110
1381 bash 2024-08-12 14:04:20 UTC+0000 FANATIC=$(openssl passwd "LKSN2024asik")
1381 bash 2024-08-12 14:04:23 UTC+0000 env
1381 bash 2024-08-12 14:04:34 UTC+0000 echo $FANATIC
1381 bash 2024-08-12 14:04:40 UTC+0000 export FANATIC=$FANATIC
1381 bash 2024-08-12 14:04:42 UTC+0000 env
1381 bash 2024-08-12 14:05:04 UTC+0000 echo $FANATIC | zip -P "$FANATIC" confidential.zip secret.txt
```

Maka dari itu kita gunakan plugin linux_bash_env untuk melihat nilai dari variabel tersebut.

```
vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem
linux_bash_env | grep FANATIC
```

```
FANATIC=cZn5xU67st3LI
```

Jawaban: FANATIC_cZn5xU67st3LI

Pertanyaan 4. The uncovered zip content may leaks the APT plan in order to breach their targeted victim company and usually it involves a name of their higher ups.

Can you tell us WHO will likely to be targeted (not an OSINT challenge) ?

Pada pertanyaan sebelumnya, kita mengetahui file yang di compress menjadi zip adalah file secret.txt dan

kita sebelumnya juga telah melakukan enumerate file. Ini bisa kita gunakan untuk mendapatkan file secret.txt dengan menggunakan plugin linux_find_file

```
vol2 --profile LinuxUbuntu16_04x64 -f nuclear.vmem  
linux_find_file -i 0xffff880077d5c030 -o secret.txt
```

0xffff880077d5c030 adalah inode dari file secret.txt dan -o secret.txt adalah nama file outputnya.

ketika kita buka, file tersebut berisi link yang mengarahkan kita pada suatu website yang berisi note dan ada password yang dibutuhkan untuk mengakses note tersebut.

```
Here's our plan to attack one of the Nuclear Plant in Wakanda Country:
```

- a) Hijack the HQ of the Nuclear Plant Institution
- b) Install a zero-day CVE to Armin Bahanang's Laptop (one of the higher ups in the institution)
- c) Initiate a modbus connection to wreck havoc the nuclear
- d) Become a new president


dari sini kita bisa tahu target dari serangan ini adalah Armin Bahanang

Jawaban: Armin_Bahanang

Flag:

```
LKSN{y0u_h4ve_overcome_the_b3ginner_Linux_Memf0ren_su  
ch_daredevils5s5s5!}
```

Terima Kasih :)

**Dibuat dengan penuh perasaan dan cinta 
Love from Telkom Schools**