

Praktikum \x003

IF1230 - Organisasi dan Arsitektur Komputer

"Binary Civilization"

Binary Exploitation

Dipersiapkan oleh:
Asisten Lab Sistem Terdistribusi

Didukung Oleh:



Waktu Mulai:
Minggu, 22 Desember 2024, 01.30.00 WIB

Waktu Akhir:
Senin, 30 Desember 2024, 23.59.59 WIB

Daftar Isi

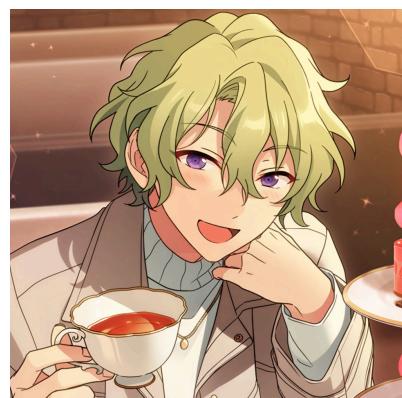
| | |
|--|-----------|
| Daftar Isi | 2 |
| Daftar Revisi | 3 |
| I. Latar Belakang | 1 |
| II. Deskripsi Tugas | 7 |
| III. Teknis dan Penilaian | 10 |
| IV. Langkah Umum Penggerjaan | 11 |
| V. Pengumpulan dan Deliverables | 15 |
| VI. Troubleshooting | 16 |
| nc: command not found | 16 |
| 7z: command not found | 16 |
| No such file or directory | 16 |
| Di GDB program hang saat dijalankan (run) | 16 |
| Address buffer berubah-ubah di local machine | 17 |
| VII. Referensi | 18 |

Daftar Revisi

- 22/12/2024 11:58, penambahan klarifikasi dan revisi soal

I. Latar Belakang

Beberapa bulan telah berlalu sejak kamu berhasil kabur dari ASM Civilization, dunia aneh yang penuh ranjau. Selama beberapa bulan tersebut, kamu masih terpikirkan tentang segala kejadian yang kamu lewati, dan tentang ornamen aneh yang tiba-tiba muncul di tasmu saat kamu kembali ke dunia nyata. Setelah berkali-kali menginspeksi ornamen itu, kamu menyadari bahwa ornamen tersebut berupa sebuah palu. Suatu hari, kamu berjalan-jalan mengitari Labtek V tanpa tujuan, pikiranmu terpenuhi oleh palu itu. Siapa pemilik aslinya? Kenapa sekarang palu itu bisa berada di tanganmu? Tiba-tiba, kamu bertemu dosen Matematika Diskrit bernama Hitori Yomoe.



Hitori Yomoe

Beliau tampak khawatir setelah melihat mukamu. "Hei, kamu baik-baik saja? Kenapa tampangmu suram begitu?" Kamu memutuskan untuk bertanya kepada Hitori tentang palu tersebut. "Ah, Hm-hm. Aku pernah lihat palu itu di *game* temanku. Itu... milik Sprokle!" OH wow, kamu tidak pernah terpikirkan bahwa ternyata dosenmu sendiri tahu tentang palu itu. Semestinya dari awal kamu bertanya saja... Katanya, Sprokle adalah seorang karakter yang hobi melakukan berbagai keisengan mulai dari melepaskan tali sepatu orang lain **hingga terorisme**.



Sprokle

Setelah bertanya-tanya tentang Sprokle, kamu akhirnya memberi tahu Hitori tentang pengalaman anehmu, mulai dari bertemu dengan Furina hingga mendapatkan palu milik Sprokle itu. Hitori sangat terkejut. Ternyata, dia juga mengalami hal yang sama

bertahun-tahun lalu. Dia memberitahu kamu kalau beberapa saat lagi, Sprokle akan datang menculik kamu, karena palu itu adalah penandanya. "Tetapi tenang saja, aku pasti akan melindungimu dari Sprokle!" ucap Hitori.

Seketika kemudian, kamu melihat sebuah boneka kecil yang ber-vibing mengikuti lantunan suatu [lagu](#). Di saat itu juga, kamu menyadari bahwa kamu akan diculik. Tiba-tiba, ada cahaya terang yang membutakan matamu.

Saat kamu kembali membuka mata, kamu berada di tempat yang asing. Untungnya, kamu tidak sendirian, Hitori masih ada di sebelahmu.

"Ah, kelihatannya kita ada di tempat yang sama dengan ketika aku dulu diculik Sprokle" kata Hitori. Hitori menjelaskan bahwa lokasi kalian sekarang adalah dunia lain yang bernama Binary Civilization. Untuk pergi dari tempat tersebut, kalian harus melakukan **buffer overflow** (dan beberapa trik lainnya) ke file binary yang ada di sekitarmu dan "**escape the matrix**".

Binary Civilization... sepertinya tidak terlalu jauh berbeda dengan dua *civilization* yang sudah pernah kamu lalui. Seketika, kamu teringat tentang Furina dan semua hal yang telah kalian hadapi bersama. Kamu tersesat dalam lamunan hingga Hitori membangunkanmu dengan menggoyang-goyangkan badanmu. "Hei lihat, sepertinya aku melihat seseorang yang familiar". Hitori menunjuk ke seorang wanita dengan rambut pirang dan kaca pembesar.

'Itu bukannya dosen logkom yang sempat hilang di tengah semester ya? Ternyata dia di isekai kesini??'



Wamelia Atson

Benar, dia adalah dosen bernama Wamelia Atson. Beliau sempat mengajar salah satu kelas Logkom, sebelum menghilang tanpa jejak. Dia menjelaskan bahwa dia juga tiba-tiba di-isekai ke dunia ini. Saat ini, dia sedang menyelidiki kelemahan dari binary yang

ada agar dapat di-exploit. Kalian bertiga memutuskan untuk bekerja sama. Konon katanya, kalian perlu men-exploit 10 binary untuk mendapatkan kunci ke dunia nyata

Karena kamu ahli orkom, kamu dengan mudah mengalahkan berbagai binary, seperti zamuza, freak out hr., dan living millennium. Namun, saat kamu menghadapi 3 soal terakhir, kamu, Wamelia, dan Hitori kesulitan dan tidak bisa menyelesaikannya. "Ah coba saja ada Furina disini, dia pasti bisa membantu".

Beberapa hari berlalu dan kalian akhirnya bisa menyelesaikan soal kedelapan namun sekarang kalian kesulitan di soal kesembilan. Saat kamu berjalan untuk refreshing, tiba-tiba ada yang terjatuh dari saku kamu. Hal yang terjatuh adalah palu Sprokle. Saat kamu ambil, tiba-tiba palu tersebut menyala. Kamu menanyakan hal itu kepada Hitori dan dia menjawab "Oh aku lupa kita punya benda itu, benda itu dapat memanggil seseorang sebagai bala bantuan, dulu aku memanggil dosen orkom ku". Lalu tanpa keraguan, kamu memanggil Furina. Ketika kamu melihat Furina di belakangmu, kamu mengatakan "Furina aku kangen bangettt".



Furina de Fountain

Setelah Furina kembali kamu memeluk dia seerat yang kamu bisa, kamu memberi tahu kesulitanmu terhadap masalah yang diberikan oleh Sprokle. "Wah kasihan sekali kamu, untung ada aku, aku siap membantu" ucap Furina. Tiba-tiba Sprokle muncul dihadapan kalian dan berkata "Wow, ramai sekali, apakah kalian ingat aku?". Kamu bingung terhadap ucapan Sprokle. "Yap, aku dulu menyamar menjadi Rimothy Tonald, aku ingin mengamatimu dulu sebelum membawamu kesini".

"Tapi kenapa kamu melakukan semua ini??". "Entertainment... Apalagi.. Hehe". Disaat itu kamu sadar bahwa Sprokle adalah seseorang yang sangat berbahaya. "Baiklah, aku akan tinggalkan kalian, selamat bersenang-senang". Setelah Sprokle pergi kalian kemudian melanjutkan menyelesaikan soal kesembilan. Berkat Furina kalian akhirnya bisa menyelesaikan soal kesembilan.

"Yey 1 soal lagi" ucap Furina dengan wajahnya yang terlihat sangat bahagia. Sayangnya soal kesepuluh sangatlah sulit dan kelihatannya Sprokle memperhatikan kalian dari jauh. Kalian berusaha berjam-jam untuk menyelesaikannya namun kalian tetap tidak

mendapatkan hasil. Namun kamu tiba-tiba teringat beberapa kode assembly yang kamu pelajari di civilization sebelumnya. Ternyata ada pola yang sangat mirip sekali dengan soal kesepuluh. Kamu akhirnya menggunakan pengetahuanmu itu untuk menyelesaikan soal kesepuluh.

Setelah soal kesepuluh kamu selesaikan, Sprokle akhirnya membuka pintu untuk kembali ke dunia nyata. Saat kamu, Wamelia, Hitori, dan Furina akhirnya berdiri di depan pintu yang akan membawa kalian kembali ke dunia nyata, semuanya terasa begitu surreal. Pintu itu bersinar terang, seolah menyembunyikan sesuatu yang lebih besar di baliknya. Namun, meskipun ada kelegaan di wajah kalian, kecemasan masih menggelayuti pikiranmu. Sprokle, dengan senyum nakalnya, mengamati kalian dari kejauhan.

“Jangan lupa, hadiah kalian belum selesai,” kata Sprokle dengan nada yang penuh teka-teki. “Kamu bisa membawa Furina ke dunia nyata, tapi...,” ia mendekat dengan tatapan tajam, “apakah kalian yakin ingin meninggalkan dunia ini begitu saja?”

Wamelia, yang semula terlihat tenang, tiba-tiba merasakan kegelisahan di hatinya. “Apa maksudmu, Sprokle?” tanya Wamelia dengan suara sedikit gemetar.

Sprokle tertawa lebar. “Karena setiap perjalanan ada harganya, dan dunia nyata tidak akan pernah sama lagi setelah ini. Siapa yang tahu apa yang bisa terjadi jika kalian membawa Furina, atau jika kalian tetap berada di sini? Dunia ini, ‘Binary Civilization,’ dapat memberikan kekuatan yang tak terbatas bagi yang menguasainya,” Sprokle berkata dengan nada penuh godaan.

Kamu merasa bingung dan terombang-ambing antara pilihan untuk pulang dan keinginan untuk berjuang lebih lama di dunia ini demi menyelamatkan Furina. Sprokle menambah ketegangan dengan mengangkat palu kecil di tangannya. “Apakah kalian siap untuk mempertaruhkan segalanya? Dunia ini... akan selalu bisa menarik kalian kembali.”

Tiba-tiba, sebuah suara mengejutkan dari belakangmu: “Aku tidak akan membiarkanmu menguasai dunia ini dengan cara yang tidak benar.”

Kamu terbelalak. Itu suara Furina. Tapi bukan Furina yang kamu kenal. Seorang sosok dengan mata yang penuh tekad dan aura penuh kekuatan muncul dari bayangan, mengenakan pakaian yang lebih misterius, memegang pedang digital yang berkilau.

“Ini bukan hanya soal kembali ke dunia nyata. Ini adalah soal memilih apa yang benar!” kata Furina, suaranya lebih dalam dan serius dari sebelumnya.

Sprokle tertawa lepas, menatap Furina dengan ekspresi penasaran. “Ah, aku tahu akan ada kejutan! Kalian benar-benar tidak mudah, ya?”

Pertarungan yang luar biasa pun dimulai, dengan Sprokle melancarkan serangan cepat menggunakan palu digitalnya, sementara Furina dengan cekatan menghindari dan membalas dengan serangan pedangnya yang bersinar. Hitori dan Wamelia, yang terkejut oleh perubahan Furina, tidak bisa tinggal diam. Mereka segera mempersiapkan diri untuk

memberikan dukungan dengan memanfaatkan keahlian mereka dalam memanipulasi kode dan sistem binary.

Namun, Sprokle terus mengontrol medan dengan manipulasi dunia ini, menciptakan jebakan-jebakan tak terduga yang menantang kalian. Setiap langkah kalian menuju kemenangan tampak lebih berat dan penuh risiko. Setiap detik berlalu, dunia ini semakin mengungkapkan rahasia gelapnya.

Akhirnya, dengan semua kekuatan yang tersisa, kamu menggunakan pengetahuan yang kamu dapatkan dari berbagai pertempuran sebelumnya. Dengan serangan yang bersinergi antara kamu, Furina, Hitori, dan Wamelia, kalian berhasil menembus pertahanan Sprokle. Palu milik Sprokle terbang dari tangannya, hancur menjadi serpihan data yang tak terpakai.

Sprokle, yang tampak kaget dan kehilangan kontrol, berkata dengan nada yang lebih tenang, “Kalian benar-benar luar biasa... Tapi ingat, dunia ini tidak akan pernah bisa dilupakan begitu saja.”

Dengan kekuatan terakhir yang kalian miliki, pintu menuju dunia nyata terbuka lebar. Tanpa ragu, kamu menarik tangan Furina dan melangkah menuju pintu itu. Sesaat sebelum melangkah masuk, kamu menolehkan kepala dan melihat Sprokle yang tersenyum samar, tapi kali ini dengan sedikit kekalahan di matanya. “Kalian berhasil kali ini, tapi aku akan menunggu di tempat lain... Untuk permainan selanjutnya.”

Begitu kalian melangkah melewati pintu, cahaya itu menyelimuti tubuh kalian. Dunia nyata yang familiar menyambutmu, namun ada sesuatu yang berbeda. Kamu merasakan kehadiran Furina di sisimu, nyata dan hidup, bukan lagi karakter 2D. Dunia yang baru ini ternyata penuh dengan kemungkinan tak terhingga.

“Selamat datang kembali,” ucap Furina, tersenyum dengan penuh kebahagiaan. “Ini baru permulaan, kan?”

II. Deskripsi Tugas

Pada praktikum ini, kalian akan mengeksplorasi cara eksploitasi program dengan **buffer overflow** dan metode lainnya. Tugas kalian adalah untuk memasukkan input sedemikian rupa sehingga terjadi *buffer overflow* dan memanipulasi eksekusi program untuk mendapatkan *flag*.

Seperti praktikum sebelumnya, dengan bantuan **gdb** atau tools sejenis kalian dapat memasang *breakpoint*, melihat perintah yang sedang dijalankan, disassembly suatu fungsi, isi memory (terutama stack), serta informasi lain yang dapat membantu keberjalanannya praktikum ini.

Apa itu *buffer overflow*? *Buffer overflow* adalah kondisi ketika program menulis data yang ukurannya lebih besar dibandingkan ukuran buffer yang disediakan, sehingga menimpa data yang bersebelahan. Kondisi ini dapat terjadi pada penggunaan fungsi input yang tidak memperhatikan ukuran input seperti **gets()**. Sebagai contoh, perhatikan kode C berikut.

```
#include <stdio.h>

void vuln() {
    int val = 0;

    volatile int local = 0x12345678;
    char buff[4];

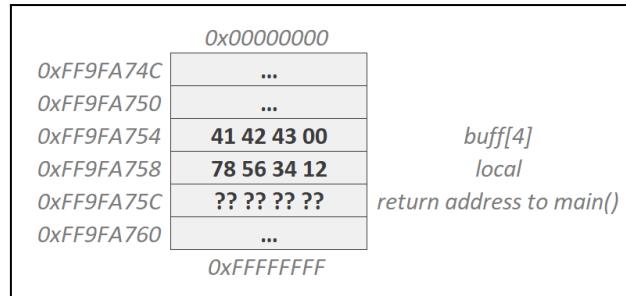
    printf("Local variable address %p\n", &local);
    printf("Buffer address %p\n", buff);
    printf("Your input : ");
    gets(buff);
    printf("Local variable value 0x%x\n", local);
}

int main() {
    vuln();
    return 0;
}
```

Melakukan compile program kemudian menjalankannya, didapatkan output berikut.

```
Local variable address 0xff9fa758
Buffer address 0xff9fa754
Your input :
```

Perhatikan bahwa **buff[4]** memiliki address yang lebih kecil dibandingkan **local** (**0xFF9FA754 < 0xFF9FA758**). Jika pengguna menuliskan masukan **ABC** dan menekan **enter**, posisi kedua variabel pada stack dapat digambarkan sebagai berikut

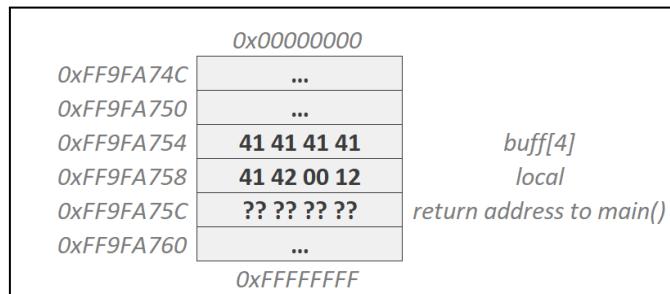


Gambar diatas memperlihatkan kondisi stack setelah input ditulis ke dalam array **buff**. Semua angka yang berada pada dalam *stack* menggunakan hexadecimal (**41** merupakan 0x41 atau 65 dalam desimal).

Sistem berbasis Linux menggunakan ***little-endian*** yang dapat terlihat pada susunan variabel lokal pada gambar. 0x41, 0x42, dan 0x43 merupakan karakter A, B, dan C dengan *encoding ASCII*. Bahasa C menggunakan ***Null Terminated String***, yaitu *array of char* yang akan dianggap serangkaian *string* hingga ditemukan nilai 0x00 (*null terminator*) yang menunjukkan akhir string.

Jika program diberikan input yang ukurannya lebih besar dari 3 karakter (3 byte karakter ditambah dengan 1 byte *null terminator*), maka dapat menimpa data yang telah ada di variabel **local**. Dengan input **AAAAAB**, didapatkan output sebagai berikut

```
Local variable address 0xff9fa758
Buffer address 0xff9fa754
Your input : AAAAAB
Local variable value 0x12004241
```



Dengan menggunakan fakta tersebut, fungsi **gets** dapat di-exploit dengan mengirimkan *payload* tertentu untuk memanipulasi eksekusi program. Variabel lokal dapat diubah dengan **menimpa nilai asli / overwrite** (**0x12345678**) dengan input yang diterima oleh **gets**.

Perhatikan bahwa dengan menggunakan masukkan keyboard, nilai byte dari *payload* akan terbatas oleh karakter yang terdapat pada keyboard. Input menggunakan keyboard tidak dapat memasukkan byte 0x18 misalnya, dikarenakan 0x18 merupakan *unprintable character* pada encoding ASCII. Untuk memasukkan byte yang merupakan *unprintable character* dapat menggunakan *hex2raw.py* yang disediakan pada kit.

III. Teknis dan Penilaian

1. Praktikum ini **tidak lagi** dilakukan pada OS *custom*. Untuk lebih detailnya ada di Langkah Umum Pengerjaan.
2. Terdapat 10 soal yang terdiri dari 7 soal wajib dan 3 soal bonus.
3. Praktikan akan mendapatkan nilai akhir 100 pada praktikum ini jika praktikan telah menjawab 7 soal pertama (1 soal = 14.2~ poin nilai akhir).
4. Nilai akhir maksimal yang bisa didapatkan praktikan adalah 100, dengan perhitungan sebagai berikut:

$$\min(C, 7) * 100 / 7$$

dengan C adalah jumlah soal wajib yang telah berhasil dikerjakan.

5. Nilai yang didapat pada soal bonus akan digunakan untuk menutup nilai yang kurang pada praktikum lainnya.
6. 3 NIM yang pertama kali berhasil menyelesaikan semua soal setelah praktikum dimulai, atau jika tidak ada, 3 NIM dengan jumlah soal terselesaikan paling banyak di akhir praktikum, akan mendapatkan apresiasi khusus dari Sister '22. Bagi praktikan yang berhasil memenuhi ini, silahkan hubungi Wiswis (Line: tiny.cc/wiswis Discord: wiswis) dan berikan tangkapan layar/foto yang mendukung.

IV. Langkah Umum Pengerajan

1. Lakukan instalasi Operating System berbasis **Linux**. Anda dapat melakukan instalasi pada *Virtual Machine* ataupun *Native Installation*. Untuk WSL, gunakan **WSL 2** karena WSL 1 tidak support program 32 bit.
2. Install pwntools melalui pip atau repositori yang ada sesuai dengan distribusi linux yang digunakan <https://docs.pwntools.com/en/dev/install.html>.
3. Unduh zip *binary* melalui [tautan ini](#). Unduh zip sesuai NIM.
4. Lakukan unzip pada file *zip binary* yang telah diunduh. Gunakan perintah berikut.

```
$ 7z x <filename>
...
Enter password (will not be echoed): <password>
```

Bagian <filename> diisi dengan nama file zip binary yang telah diunduh. Bagian <password> diisi dengan kata sandi yang diperoleh melalui surel.

5. Lakukan uji coba koneksi terhadap server. Gunakan perintah **nc** (netcat) dengan ketentuan sebagai berikut.

```
$ nc 52.184.85.16 <PORT>
NIM: <NIM>
Challenge: <CHALLENGE_ID>
...
```

*Berikut adalah ketentuan terkait **CHALLENGE_ID**:*

- a. **X**, yaitu nomor challenge (1-10).
- b. “**welcome**”, yaitu untuk mengakses dokumen **welcome.md**.

Contoh perintah yang digunakan untuk berkoneksi dengan server adalah sebagai berikut.

```
$ nc 52.184.85.16 12345
NIM: 13522420
Challenge: 2
...
```

```
$ nc 52.184.85.16 12345
NIM: 13522420
Challenge: welcome
...
```

6. Jalankan perintah **chmod +x <CHALLENGE-BINARY>** pada terminal Anda di directory tempat Anda mengekstrak file hasil download. Hal ini dilakukan agar program dapat dijalankan.

7. Anda tidak disarankan untuk melakukan eksekusi file biner secara langsung untuk menebak karakter untuk buffer overflow. Anda dapat menggunakan **gdb** pada terminal (disarankan menggunakan plugin gdb). Untuk memberikan input yang tidak termasuk dalam *printable character* (A-Z, a-z, 1-9 dan simbol), akan diberikan guidebook penggunaan library `pwn`: <https://docs.pwntools.com/en/stable/>

```
from pwn import *

def conn():
    if args.GDB:
        return gdb.debug(args.BINARY,
                        gdbscript="""\n        continue\n        """ # Add necessary gdb commands here
    elif args.REMOTE:
        return remote('52.184.85.16', 12345)
    else:
        return process(args.BINARY)

def solve():
    p = conn()
    padding = b'A' * <jumlah_agar_buffer_overflow>
    payload = padding

    # write your payload here

    p.sendline(payload) # meng-inject payload ke dalam binary
    p.interactive() # flush to stdout

solve()
```

```
$ python3 solver.py <ARGS: GDB | REMOTE>
```

Untuk sekaligus menjalankan GDB
\$ python3 solver.py GDB

Untuk menjalankan di remote untuk mendapatkan flag
\$ python3 solver.py REMOTE

Untuk menjalankan tanpa GDB
\$ python3 solver.py

8. Setelah input anda benar, anda akan mendapatkan jawaban pada komputer anda berupa string sebagai berikut (iya, stringnya memang ini, bukan lupa diganti):

```
I love furina so much fr fr - local flag X
```

Setelah mendapatkan string di atas pada local, maka kirimkan payload yang sama pada server dengan menggunakan command

```
$ python3 solver.py REMOTE
```

Jika payload berhasil maka akan didapatkan text dengan contoh berikut

```
Orkom3{I'm A Walking Travesty_9a3d1f7b4c8e2a6f0d5b}
```

Sebagai catatan, terdapat lebih dari satu server yang akan dihidupkan, namun hanya satu port yang terbuka karena web server secara otomatis akan melakukan load balancing atas setiap request ke server yang tersedia.

9. Perhatikan bahwa **flag berbeda** untuk tiap orang dan untuk tiap soal. **Flag** inilah yang harus Anda submit pada **platform** yang dapat diakses pada link <http://52.184.85.16:8083/> untuk **mendapatkan nilai** untuk soal yang bersangkutan. Login ke platform dapat dilakukan dengan username NIM dan password yang dikirimkan lewat email anda.
10. Anda bebas menggunakan tools **APAPUN** untuk menyelesaikan praktikum (selama tidak melanggar aturan-aturan).
11. **Tidak ada penalti** untuk mengirim *payload* yang salah ke server. **Tidak ada juga penalti** untuk meng-submit *flag* yang salah ke server. Namun, Anda dibatasi untuk meng-submit *flag* ke web hanya sebanyak 5 kali untuk masing-masing soal.

V. Sistematika dan Peraturan

1. **Waktu Mulai** Minggu, 22 Desember 2024, 01.30.00 WIB waktu server.
Waktu Akhir Senin, 30 Desember 2024, 23.59.59 WIB waktu server.
Pengumpulan jawaban akan ditutup setelah waktu tersebut.
2. Dilarang melakukan serangan *Denial of Service* terhadap server.
3. Anda **diperbolehkan** menggunakan sumber-sumber eksternal, termasuk internet, *large language model* seperti ChatGPT, serta meminta bantuan teman. Namun, "*Percayalah, jika menemukan sendiri jawabannya, Anda akan mendapatkan sense of pride and accomplishment*" – Duke.
4. **Dilarang keras** untuk submit dengan NIM orang lain. Tolong bertanggung jawab atas pekerjaan Anda sendiri.
5. Kami akan menindaklanjuti segala bentuk kecurangan yang terstruktur, masif, dan sistematis.
6. **Dilarang melakukan kecurangan lain yang merugikan peserta mata kuliah IF1230.**
7. Jika ada pertanyaan atau masalah penggeraan harap langsung isi pertanyaan di <https://bit.ly/QNAOrkomArsikom2024>

VI. Troubleshooting

nc: command not found

Jika OS 64 bit dan baru diinstal, lakukan instalasi untuk **netcat**

```
sudo apt update  
sudo apt install netcat-openbsd
```

7z: command not found

Jika OS 64 bit dan baru diinstal, lakukan instalasi untuk **p7zip**

```
sudo apt update  
sudo apt install p7zip-full
```

No such file or directory

Jika OS 32 bit dan baru diinstal

1. Untuk menjalankan kode 64 bit dibutuhkan OS 64 bit, silakan cari perangkat dengan OS 64 bit yang dapat menjalankan *binary linux* (*Linux, WSL on Windows*, dll)

Di GDB program hang saat dijalankan (run)

Jika saat perintah run diberikan program tidak bekerja (*stuck*) dan kadang muncul tulisan error seperti

```
warning: Breakpoint address adjusted from 0xf7fd9be0 to  
0xffffffff7fd9be0.  
warning: Breakpoint address adjusted from 0xf7fda195 to  
0xffffffff7fda195.  
warning: Breakpoint address adjusted from 0xf7fdbd1c to  
0xffffffff7fdbd1c.  
warning: Breakpoint address adjusted from 0xf7fdb924 to  
0xffffffff7fdb924.
```

Kemungkinan besar disebabkan karena bug

<https://bugs.launchpad.net/ubuntu/+source/gdb/+bug/1848200>

Solusinya adalah menginstall GDB versi lebih lama dengan perintah berikut

```
sudo apt install gdb=8.1-0ubuntu3
```

Address buffer berubah-ubah di local machine

Jika saat kalian menjalankan di komputer kalian dan mendapatkan bahwa address buffer berubah-ubah, hal itu disebabkan karena **ASLR** menyala. Untuk menonaktifkannya:

```
echo 0 | sudo tee /proc/sys/kernel/randomize_va_space
```

Perintah tersebut hanya akan menonaktifkannya sementara. Setelah restart, maka **ASLR** akan aktif kembali.

VII. Klarifikasi dan Revisi Soal

1. Dibutuhkan sebuah file eksternal untuk mengerjakan soal nomor 7, yaitu `libc.so.6` dari server. Unduh file tersebut pada tautan [berikut](#) (perhatikan bahwa ada dua *file*, tetapi *file* `ld-linux-prak.so.2` tidak diperlukan)

Untuk mendapatkan *libc address* server, silakan gunakan hasil eksekusi `ldd` dari server sebagai berikut.

```
linux-vdso.so.1 (0x00007ffff7fc1000)
libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007ffff7d90000)
/lib64/ld-linux-x86-64.so.2 (0x00007ffff7fc3000)
```

VIII. Referensi

1. **GDB** - <https://docs.google.com/document/d/1u-wryLpYS2CyWxOxGI5VQElsYemFzNL12FRb8EB6yy4/edit?usp=sharing>
2. **pwntools** - <https://docs.pwntools.com/en/stable/>
3. **Ironstone pwn notes** - <https://github.com/ir0nstone/pwn-notes>

Pesan Asisten



<< >>

«👉👉 Ano... M-mohon maaf ya mesti ngerjain orkom pas libur natal 😢 😢 😢 ... Kami asisten pada keos semester 5 desu... 😔 😔 😔 jadi release praktikum 2-nya kemarin agak telat nanodesu... 👈👈 »

- Pol



<< >>

- Owen



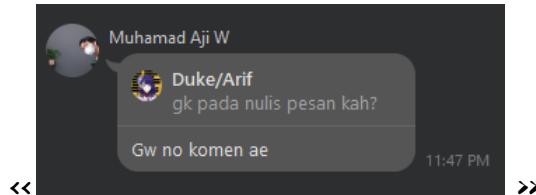
<< >>

«Satu langkah menjadi Hecker»

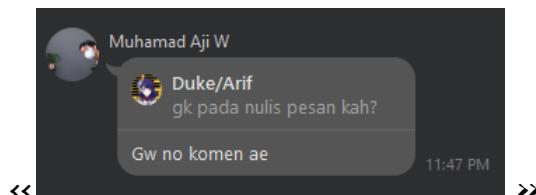
- Albert

<< It's just a simple pwn or baby pwn(?). Yah bisa lah ya, coba aja sendiri kalian kan IF.
Dua hari harusnya selesse kok ini riil no fek. >>

- インドラ



- Flora



- Onta



<< Yang bikin semua soalnya aku hehe~ good luck y'all >>

- Layla

<< 00.00-00.15 >>

- Rafiki

<<

nnnn-

dGGGGMMb

@p~qp~~qMb

M|@||@) M|

@, ----. JM|

JS^_ / qKL
dZP qKRb
dZP qKKb
fZP SMMb
HZM MMMM
FqM MMMM
__| ". | \dS"qML
| ` . | ^ ' \zq
_) _. ___. , | . '
____) MMMMMMP | . '
`- ' `-- '

»
- Ryle

<< Classic Ah [Helper of All Kind](#) >>

- Edbert

<< Biar ngerjain praktikum ini lancar, bunuh tembok daging dulu biar dapet Pwnhammer ;)

(ketik 1 di QnA jika Anda mengerti reference ini)

(just kidding don't do that lmao) »

- Aldy