ETHICAL HACKING

Session - 2025

SUBMITTED BY: Huzaifa Bin Munir

SUBMITTED BY: 20L-1082

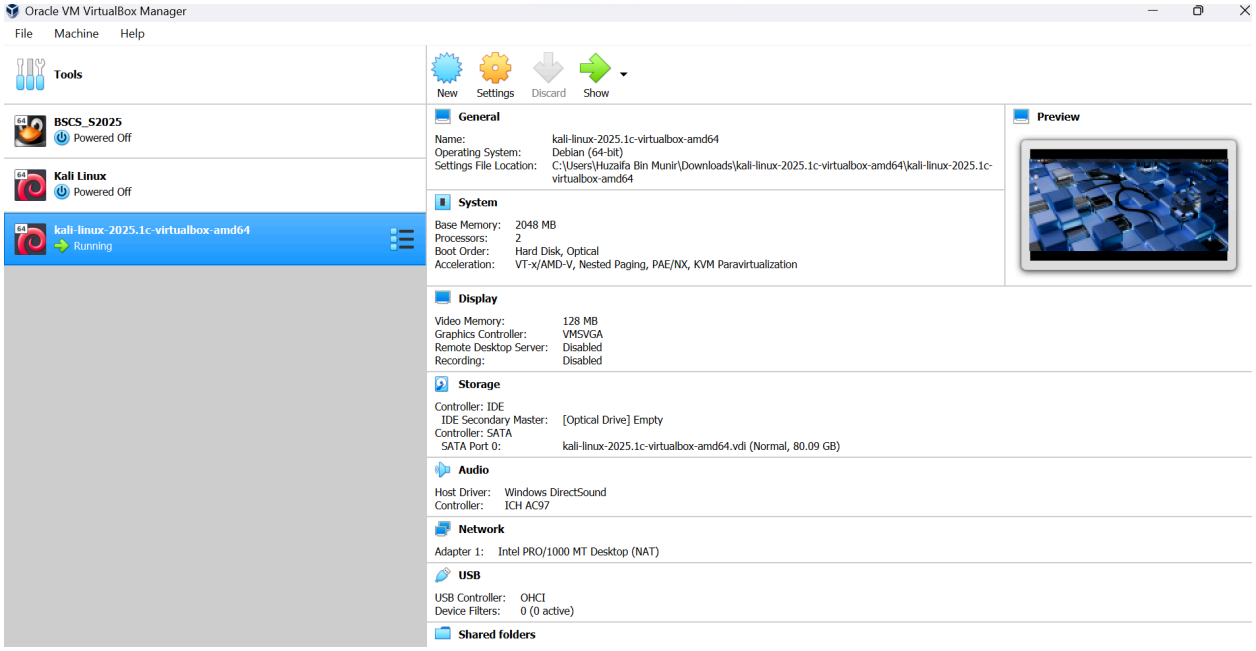
SUBMITTED TO: Ahmad Ali Shah

ASSIGNMENT NO: 3

Table of Contents:

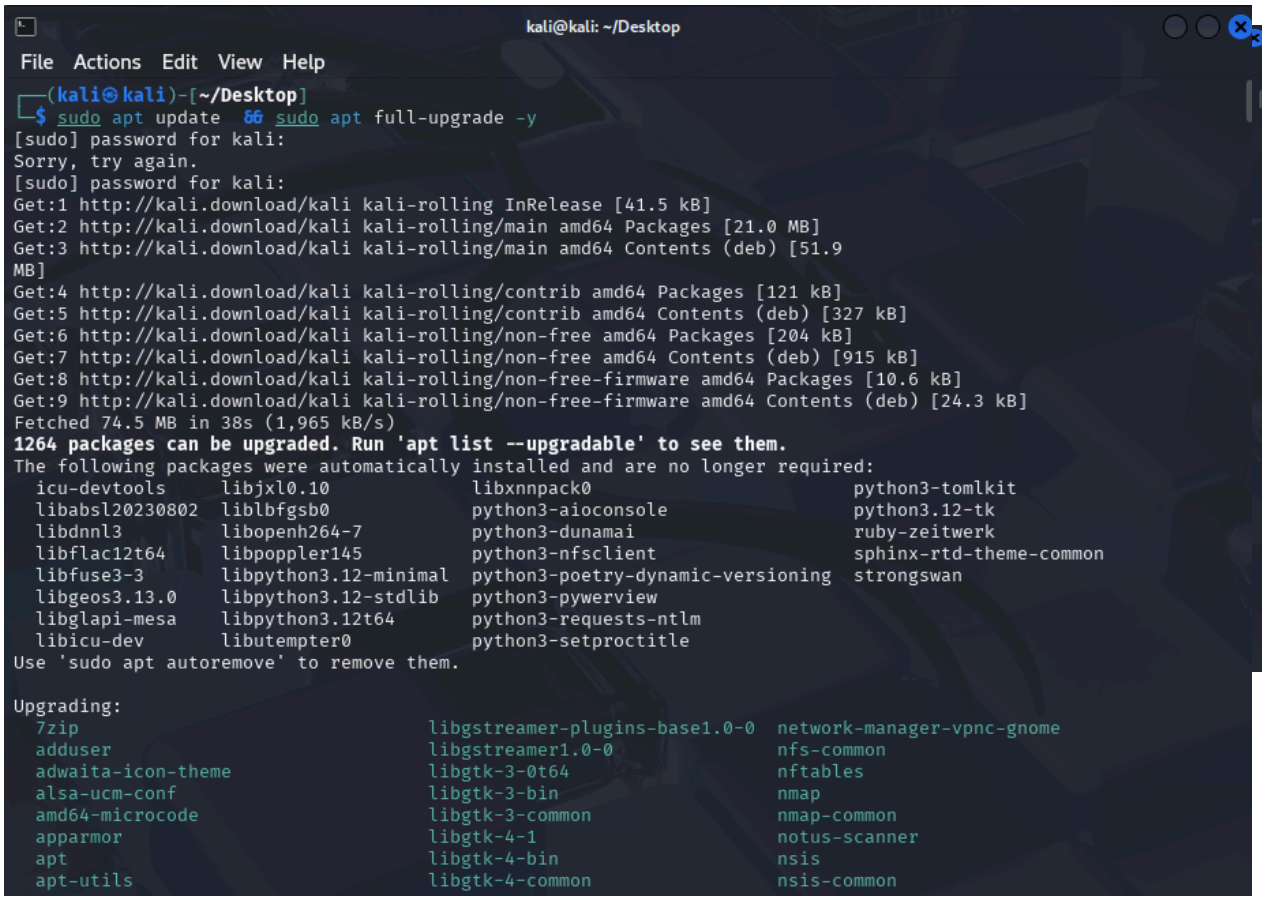
Task1: Setup

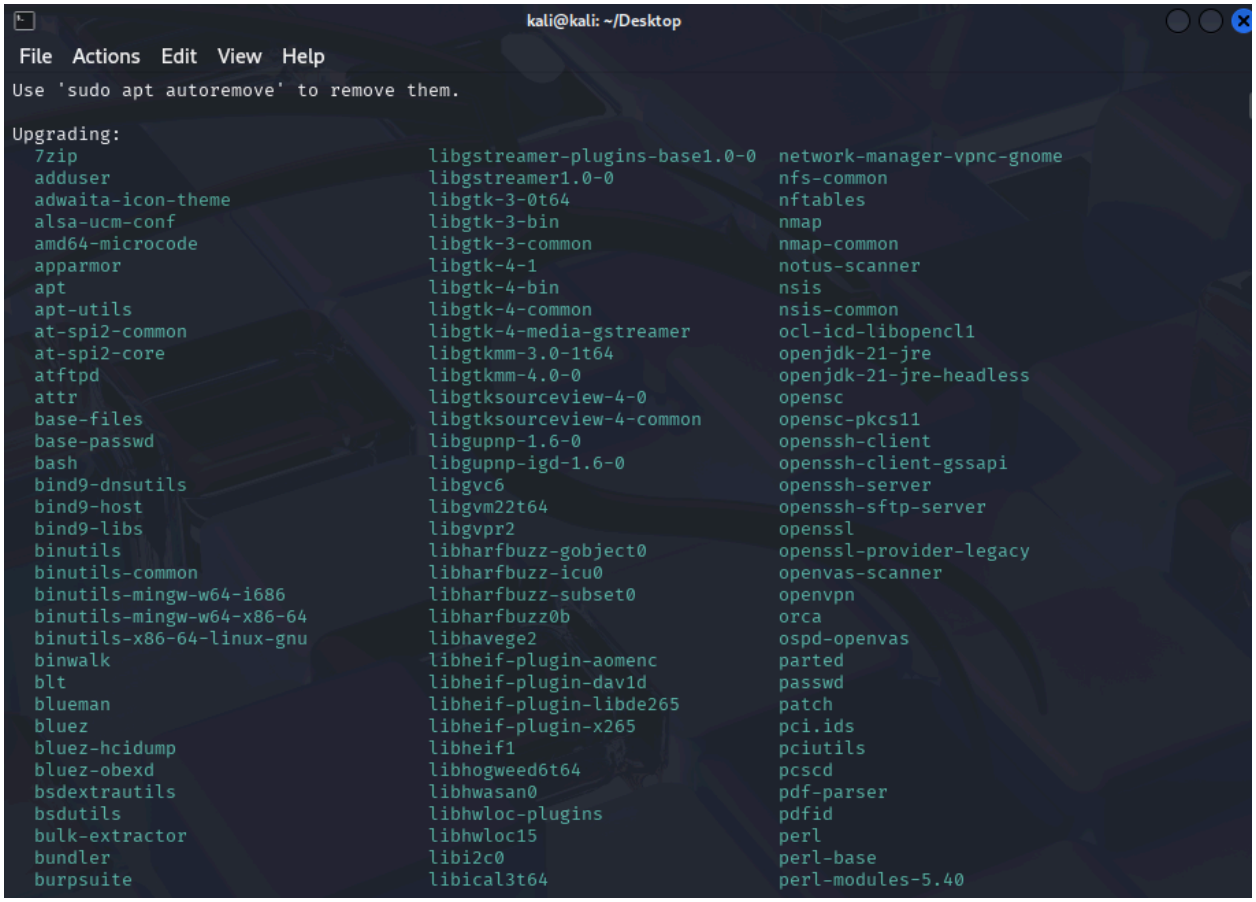
Importing the Pre Built VM and the provided Target Machine.

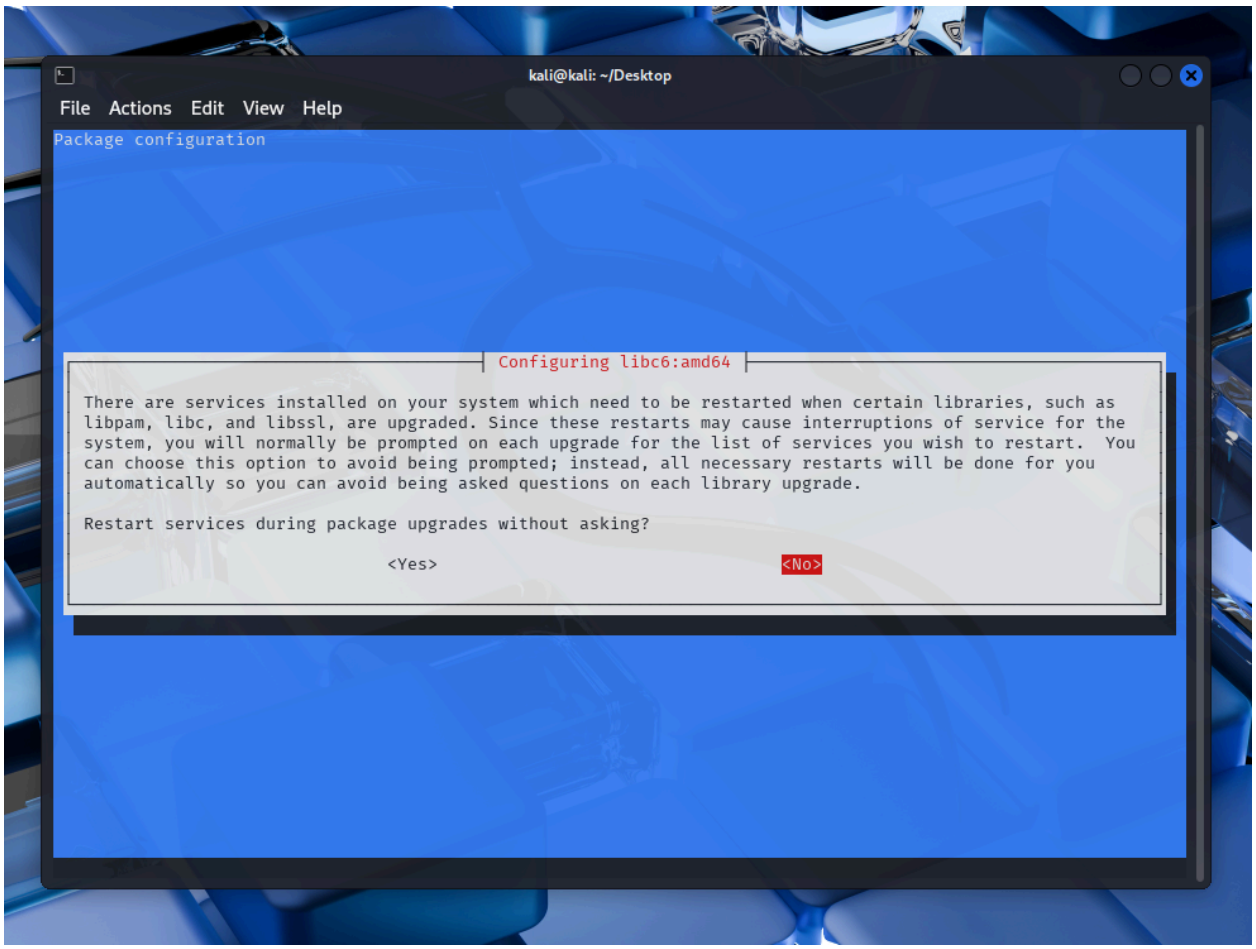


Task2: Run update & upgrade commands

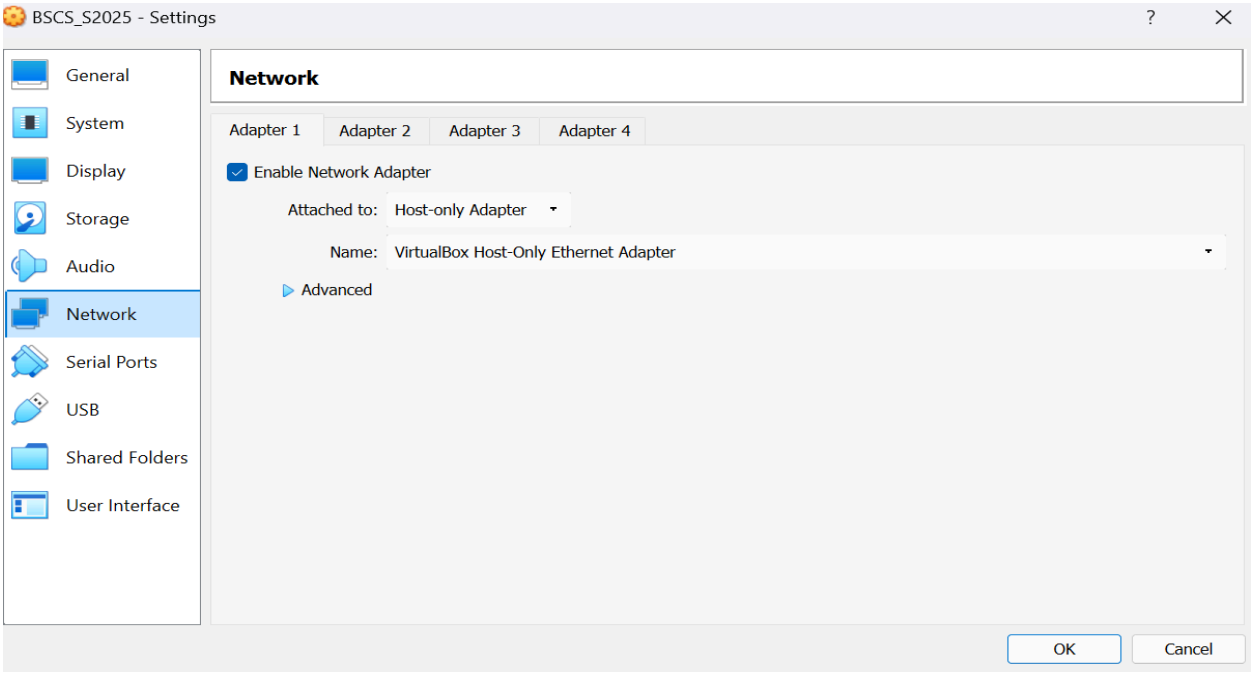
Run Update and Upgrade in Kali Linux VM



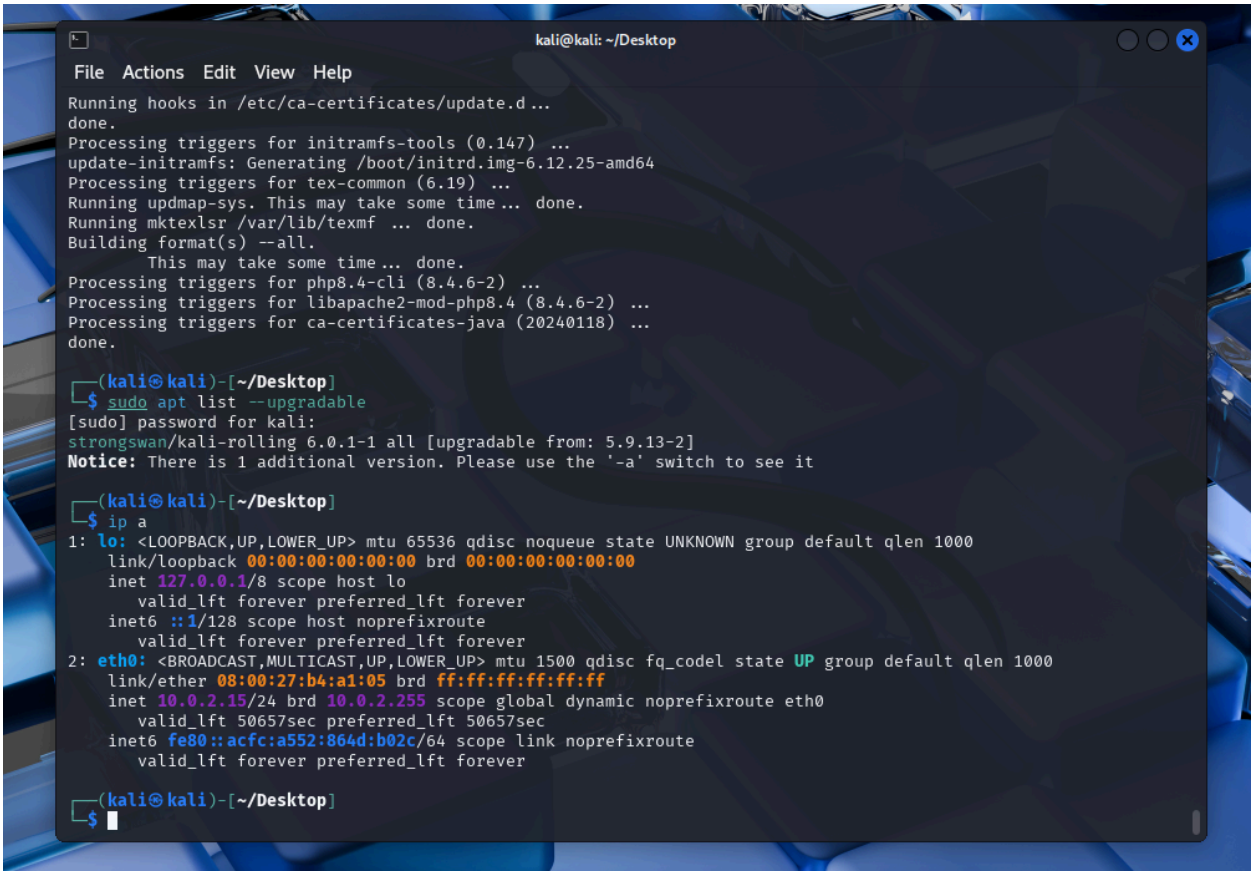

kali@kali: ~/Desktop
File Actions Edit View Help
Use 'sudo apt autoremove' to remove them.
Upgrading:
7zip
adduser
adwaita-icon-theme
alsa-ucm-conf
amd64-microcode
apparmor
apt
apt-utils
at-spi2-common
at-spi2-core
atftpd
attr
base-files
base-passwd
bash
bind9-dnsutils
bind9-host
bind9-libs
binutils
binutils-common
binutils-mingw-w64-i686
binutils-mingw-w64-x86-64
binutils-x86-64-linux-gnu
binwalk
blt
blueman
bluez
bluez-hcidump
bluez-obexd
bsdextrautils
bsdutils
bulk-extractor
bundler
burpsuite
libgstreamer-plugins-base1.0-0
libgstreamer1.0-0
libgtk-3-0t64
libgtk-3-bin
libgtk-3-common
libgtk-4-1
libgtk-4-bin
libgtk-4-common
libgtk-4-media-gstreamer
libgtkmm-3.0-1t64
libgtkmm-4.0-0
libgtksourceview-4-0
libgtksourceview-4-common
libgupnp-1.6-0
libgupnp-igd-1.6-0
libgvc6
libgvm22t64
libgvpr2
libharfbuzz-gobject0
libharfbuzz-icu0
libharfbuzz-subset0
libharfbuzz0b
libhavege2
libheif-plugin-aomenc
libheif-plugin-dav1d
libheif-plugin-libde265
libheif-plugin-x265
libheif1
libhogweed6t64
libhwasan0
libhwloc-plugins
libhwloc15
libi2c0
libical3t64
network-manager-vpnc-gnome
nfs-common
nftables
nmap
nmap-common
notus-scanner
nsis
nsis-common
ocl-icd-libopencl1
openjdk-21-jre
openjdk-21-jre-headless
opensc
opensc-pkcs11
openssh-client
openssh-client-gssapi
openssh-server
openssh-sftp-server
openssl
openssl-provider-legacy
openvas-scanner
openvpn
orca
ospd-openvas
parted
passwd
patch
pci.ids
pciutils
pcscd
pdf-parser
pdfid
perl
perl-base
perl-modules-5.40


kali@kali: ~/Desktop
File Actions Edit View Help
Package configuration
Configuring libc6:amd64
There are services installed on your system which need to be restarted when certain libraries, such as libpam, libc, and libssl, are upgraded. Since these restarts may cause interruptions of service for the system, you will normally be prompted on each upgrade for the list of services you wish to restart. You can choose this option to avoid being prompted; instead, all necessary restarts will be done for you automatically so you can avoid being asked questions on each library upgrade.
Restart services during package upgrades without asking?
<Yes>
<No>

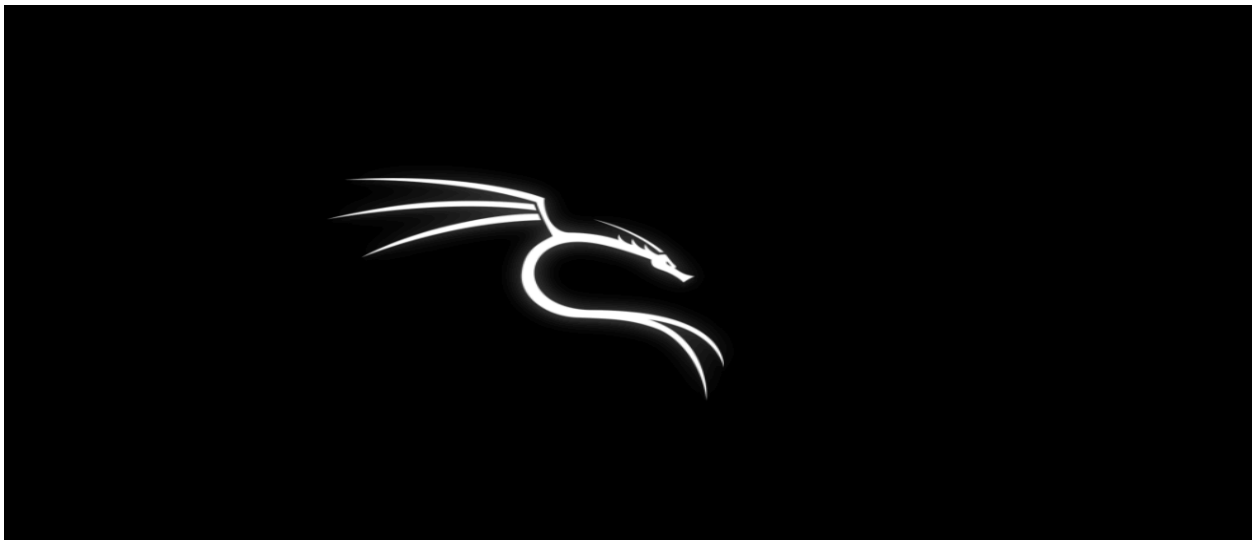
Checking the network settings whether both the target and host machine are working on the same adapter and is attached to: Host-only Adapter and the name is set to VirtualBox Host Only Ethernet Adapter.



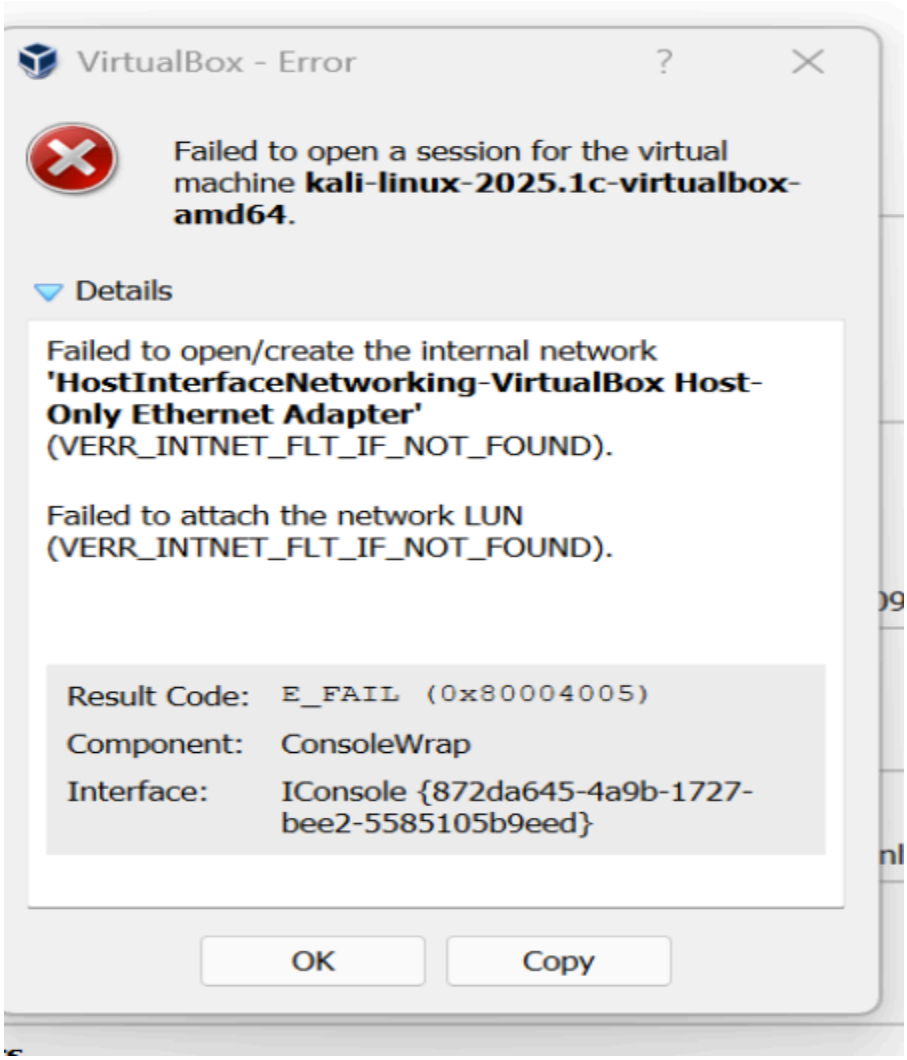
Task3: Getting the target machine IP address -> Host:



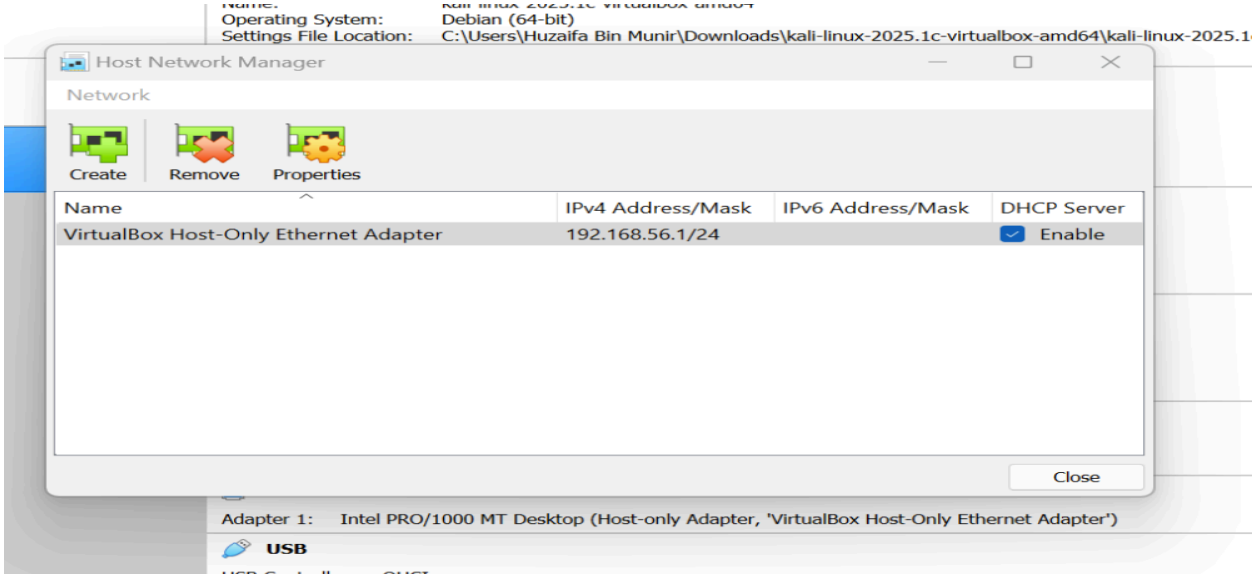
But this was NAT not **Host-Only.** So using sudo poweroff poweroff the machine and set the network settings of each VM to host only.



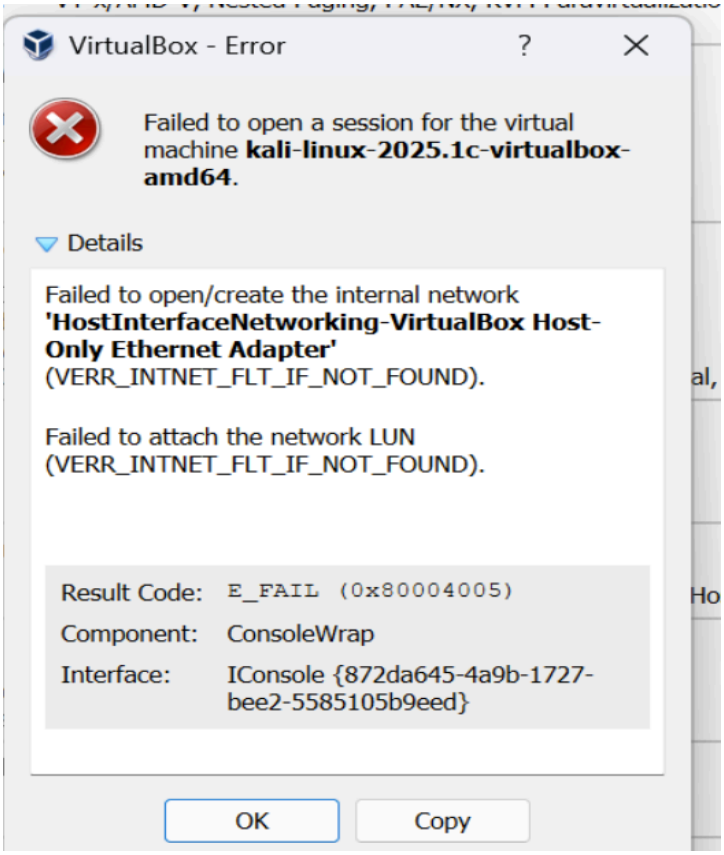
The screen froze so waiting for it to shut down. After shutting down finally, it showed me this screen.



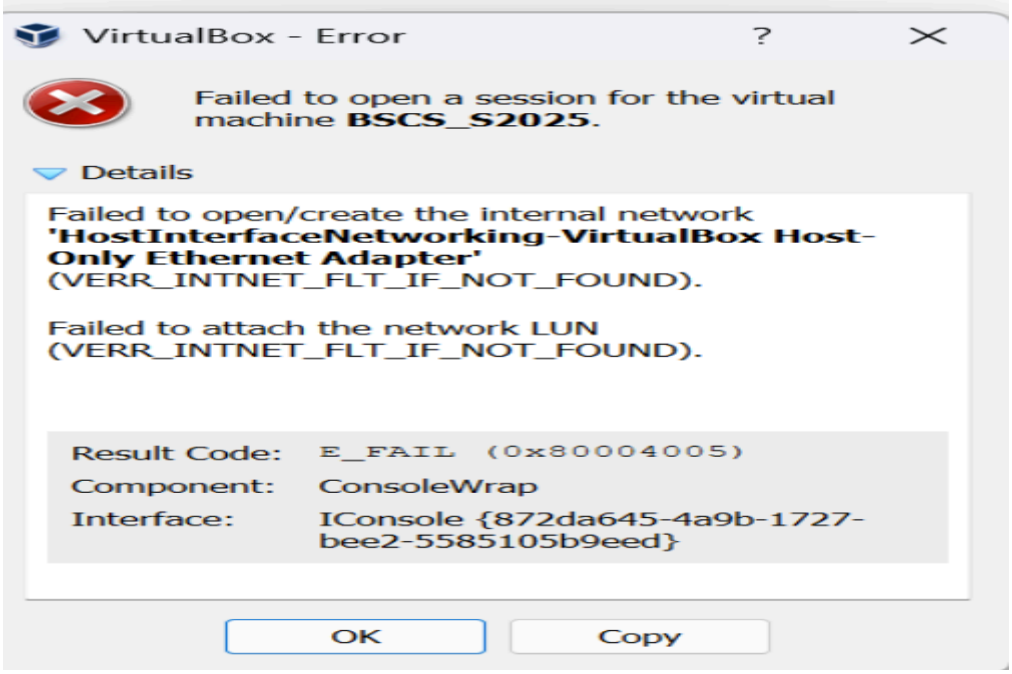
So, it means that the **Host-Only Adapter** VirtualBox is trying to use **doesn't exist anymore or is broken**. Let's fix that. Go toFile-> Host Network Manager and enable this option.



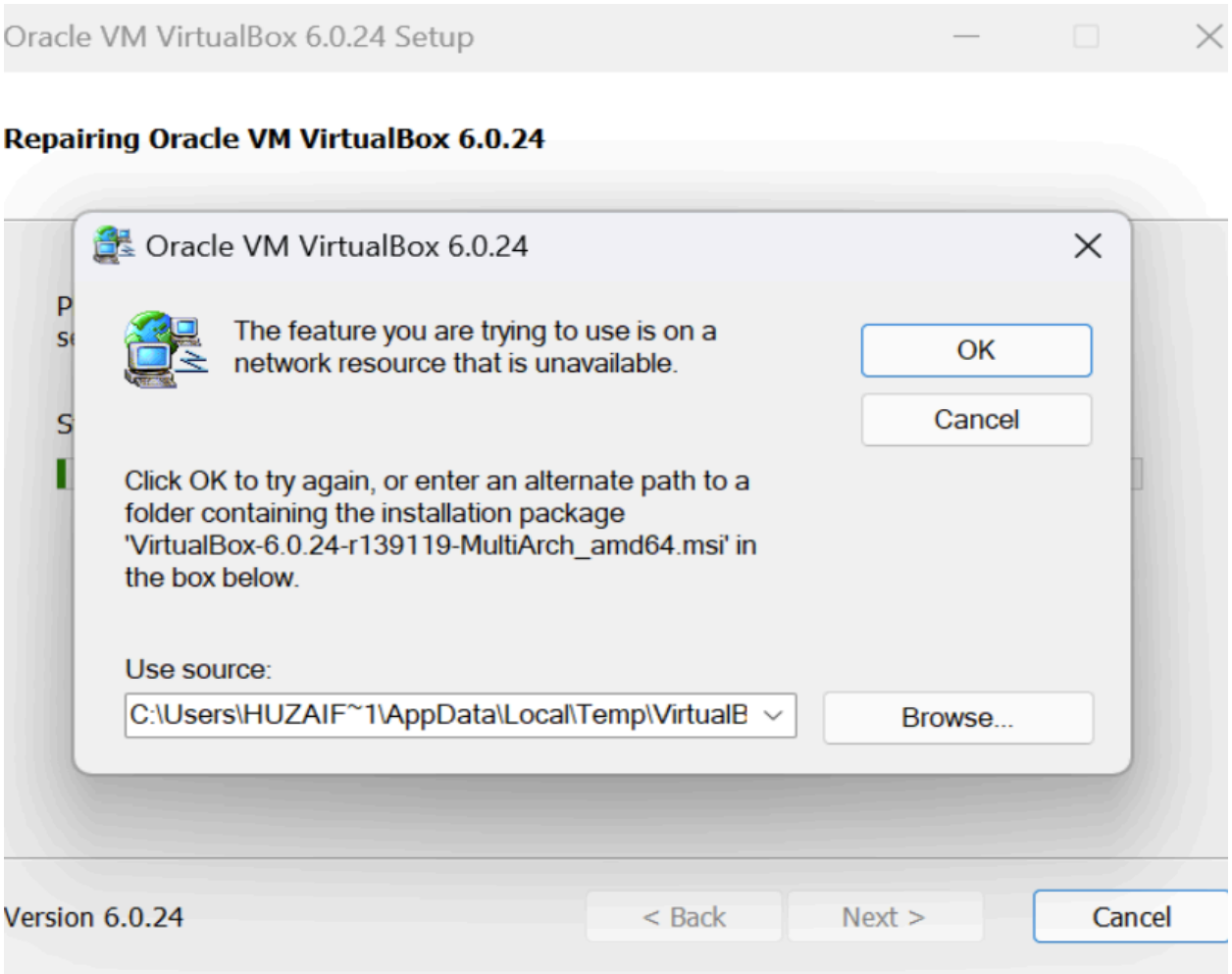
Reassign the adapter to the VMs and start again. Now I got this error again.

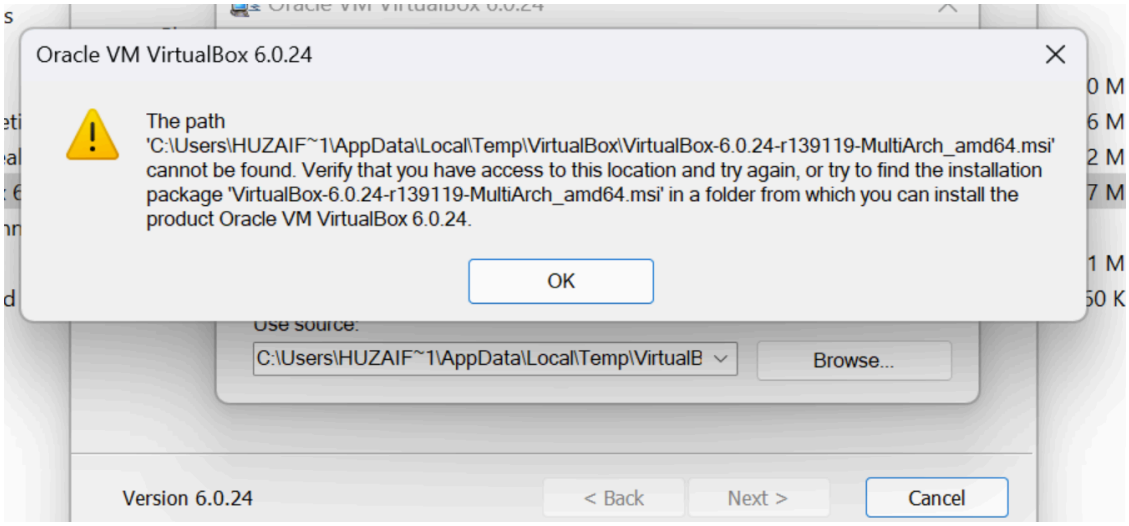


I ran the bscs ova file VM and it also failed to run.

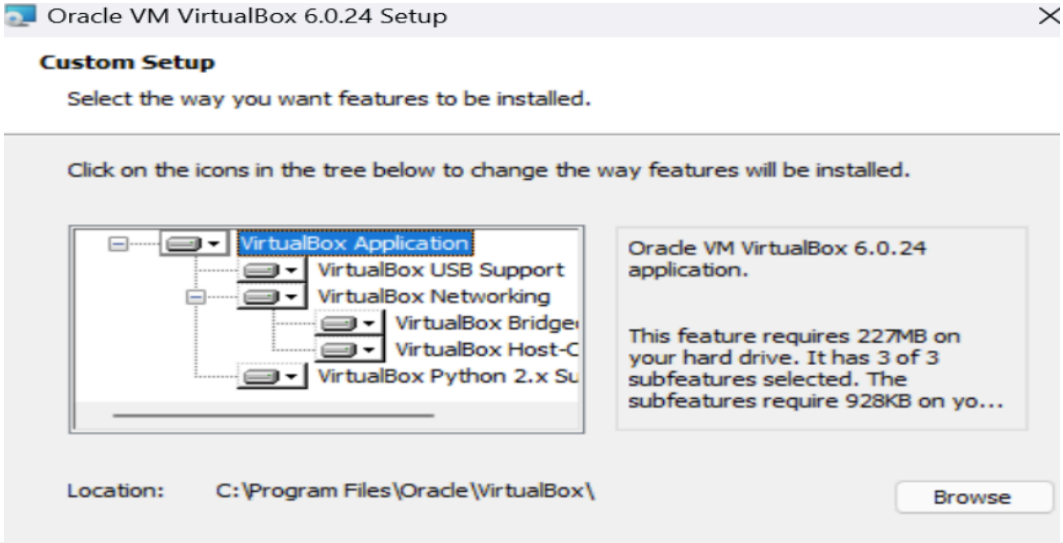


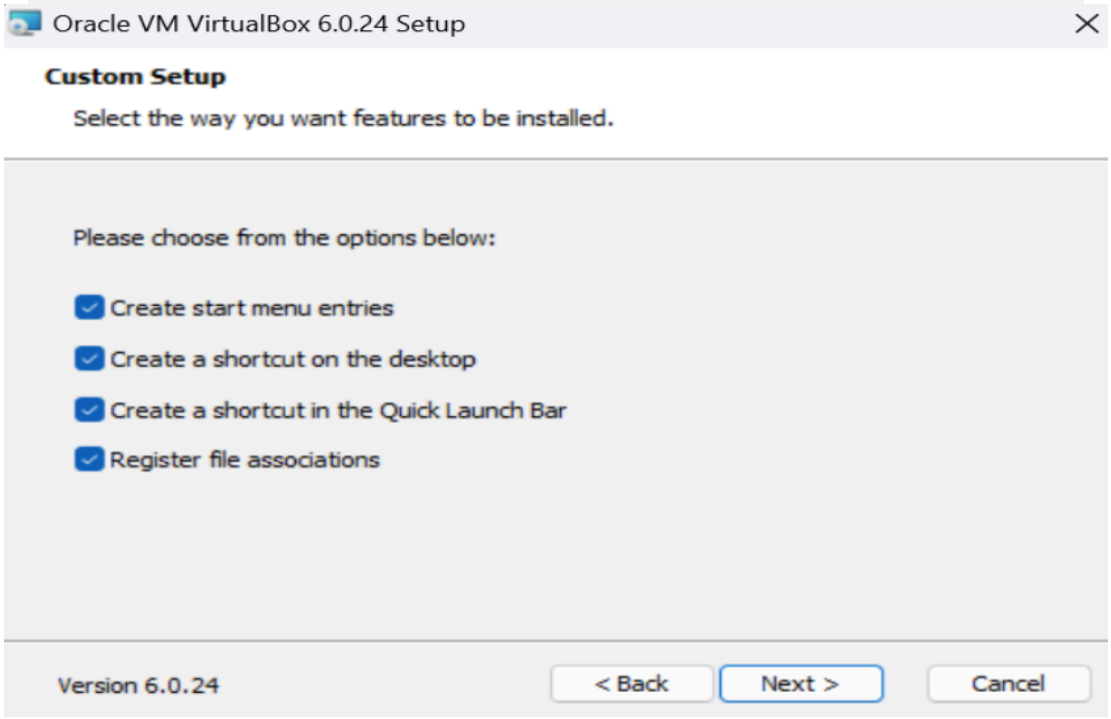
I tried repairing the VirtualBox through the Control Panel but it failed to do so. **because it couldn't find the original installer (`.msi`) file** it used when version 6.0.24 was first installed.

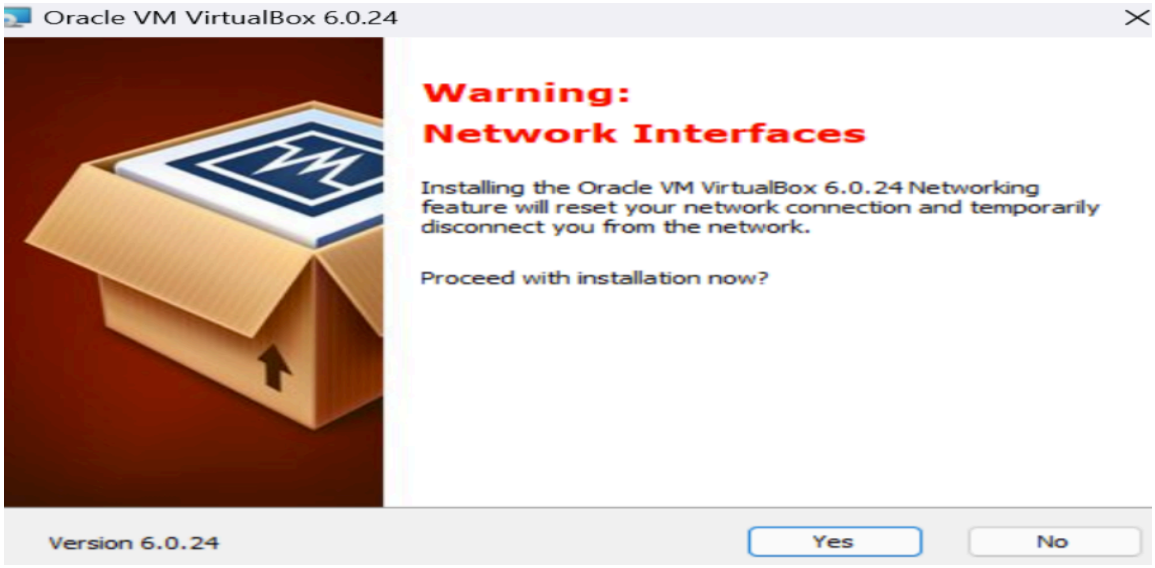


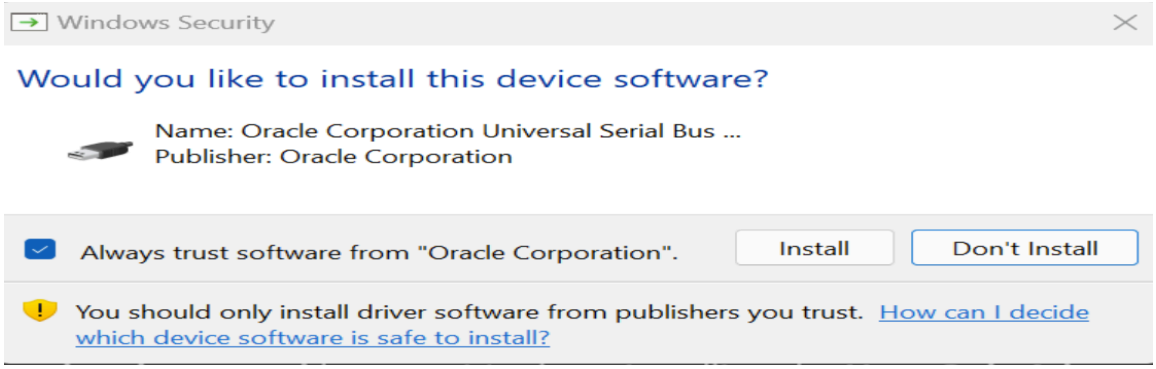


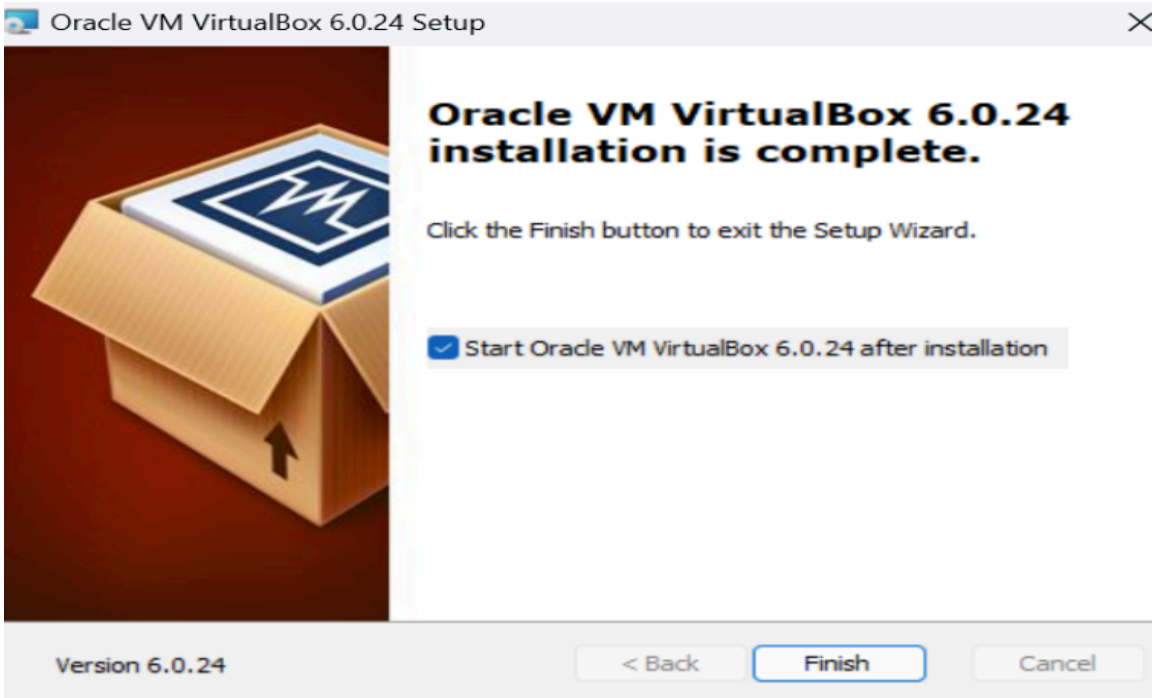
I uninstalled and then reinstalled the VirtualBox.



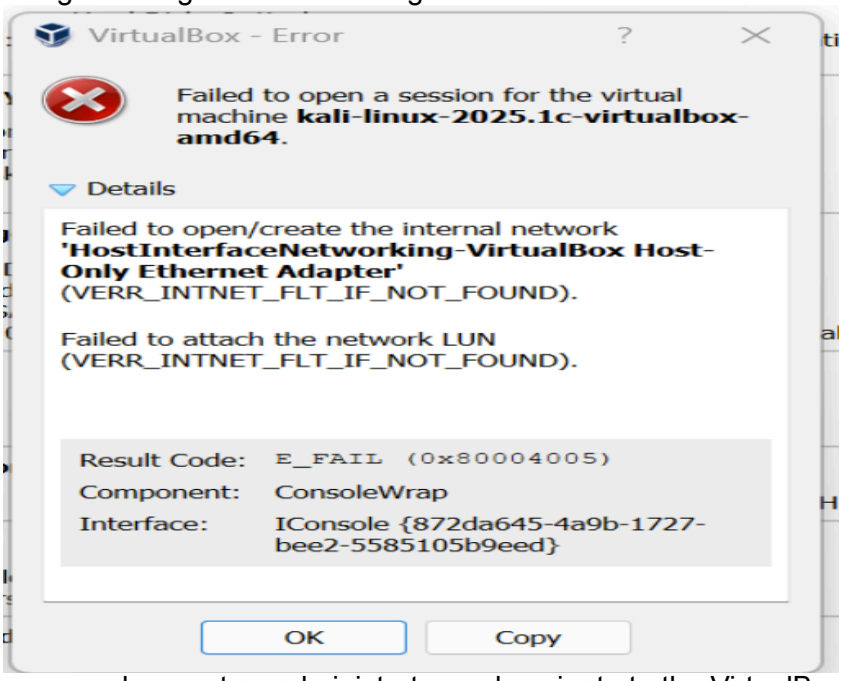



Oracle VM VirtualBox 6.0.24
Warning:
Network Interfaces
Installing the Oracle VM VirtualBox 6.0.24 Networking feature will reset your network connection and temporarily disconnect you from the network.
Proceed with installation now?
Version 6.0.24
Yes
No


Windows Security
Would you like to install this device software?
Name: Oracle Corporation Universal Serial Bus ...
Publisher: Oracle Corporation
Always trust software from "Oracle Corporation".
Install
Don't Install
You should only install driver software from publishers you trust. How can I decide which device software is safe to install?


Oracle VM VirtualBox 6.0.24 Setup
Oracle VM VirtualBox 6.0.24 installation is complete.
Click the Finish button to exit the Setup Wizard.
Start Oracle VM VirtualBox 6.0.24 after installation
Version 6.0.24
< Back
Finish
Cancel

I started the VMs again and got these errors again.



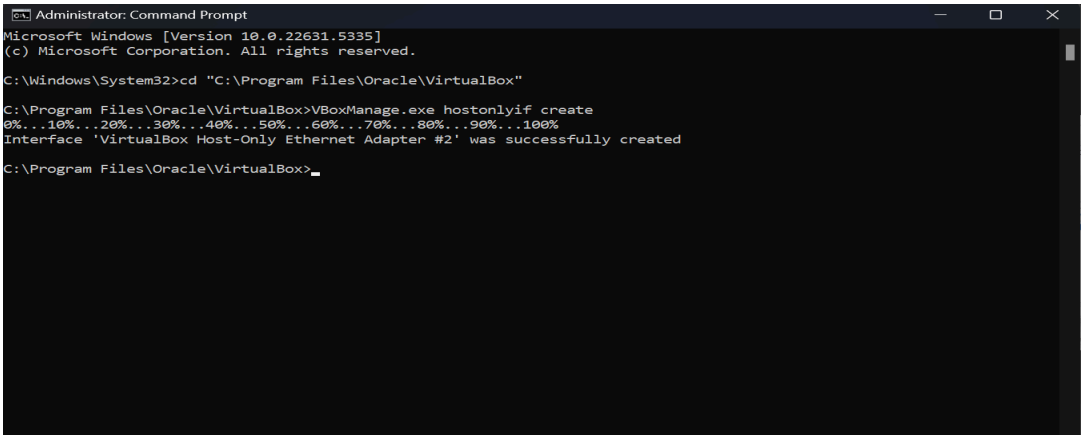
Now open the command prompt as administrator and navigate to the VirtualBox directory.

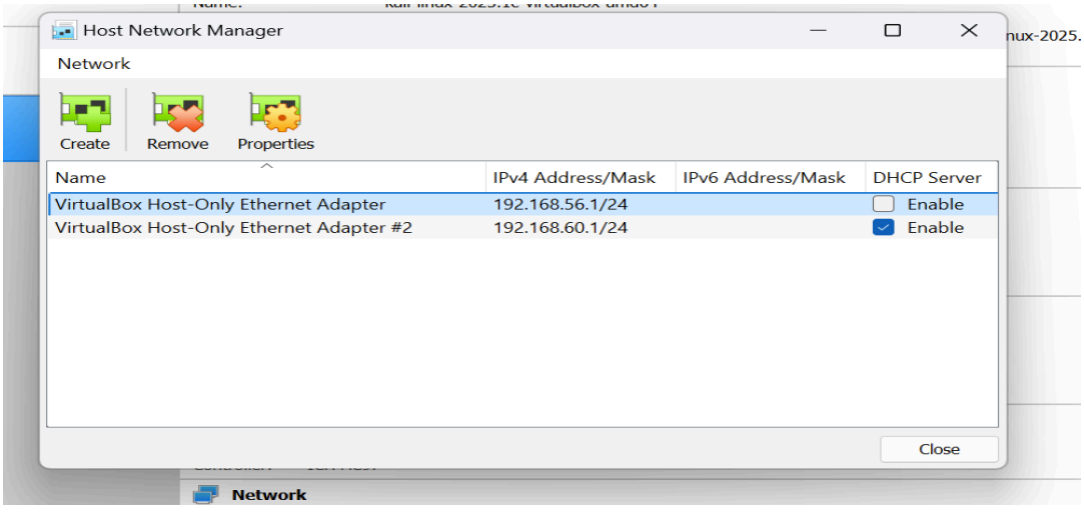
cd "C:\Program Files\Oracle\VirtualBox"

Then force create host-only adapter

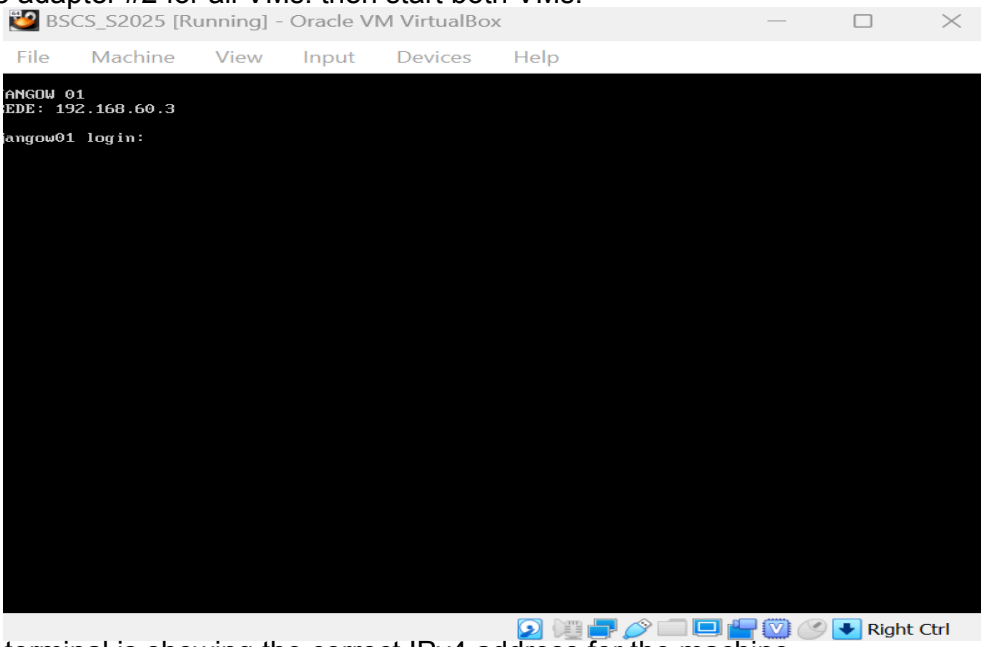
VBoxManage.exe hostonlyif create

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





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



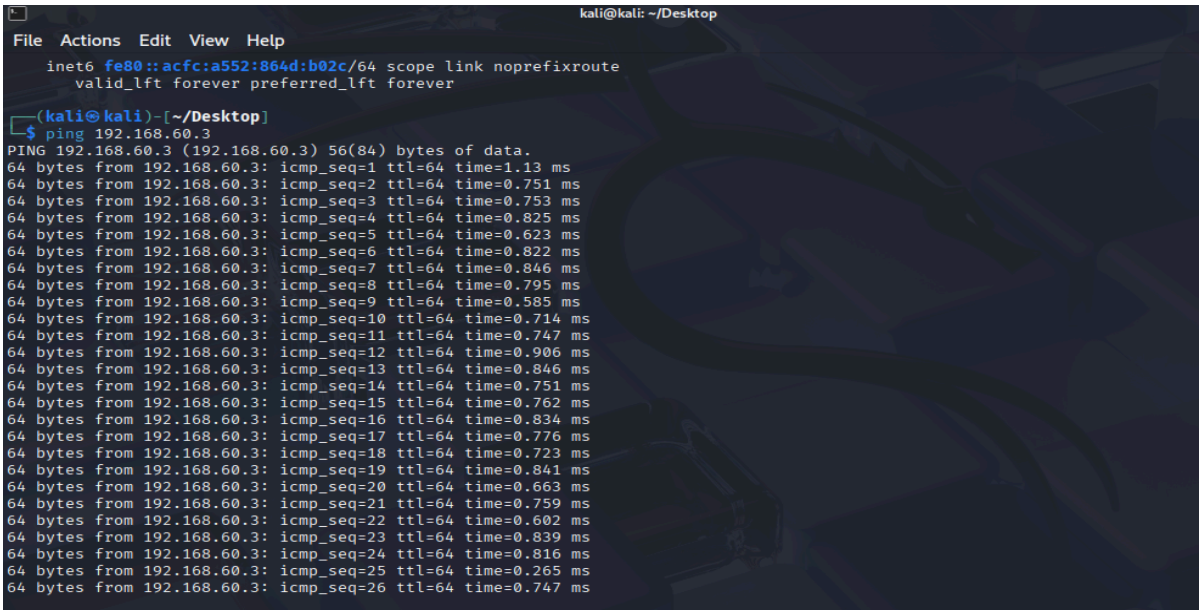
Now the terminal is showing the correct IPv4 address for the machine.

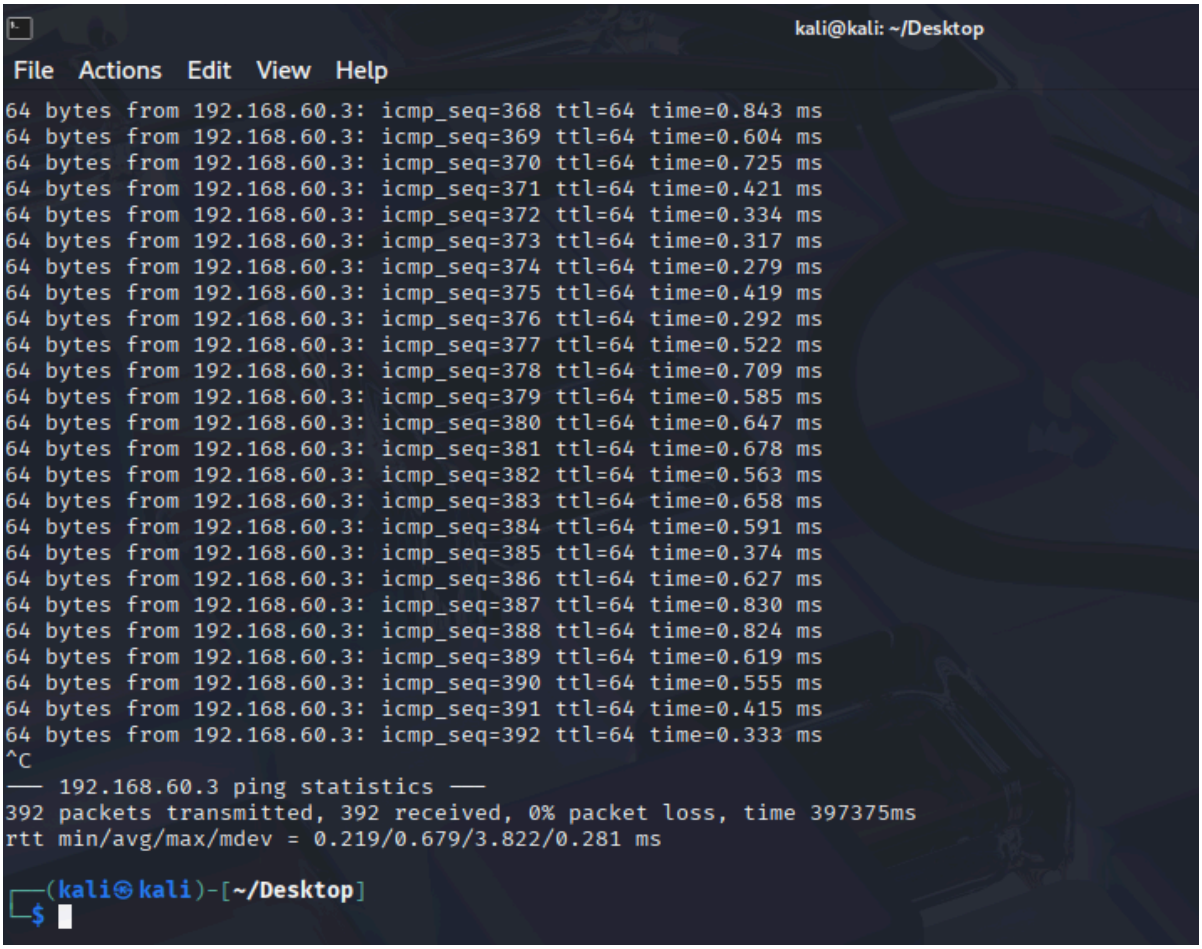
My Kali VM has:
eth0: inet 192.168.60.4
My target VM BSCS_S2025 has:
inet 192.168.60.3
Both machines are on the same subnet (`192.168.60.0/24`) and ready to talk.

Ping the Target Machine:

Now, let's ping the target machine.

ping 192.168.60.3

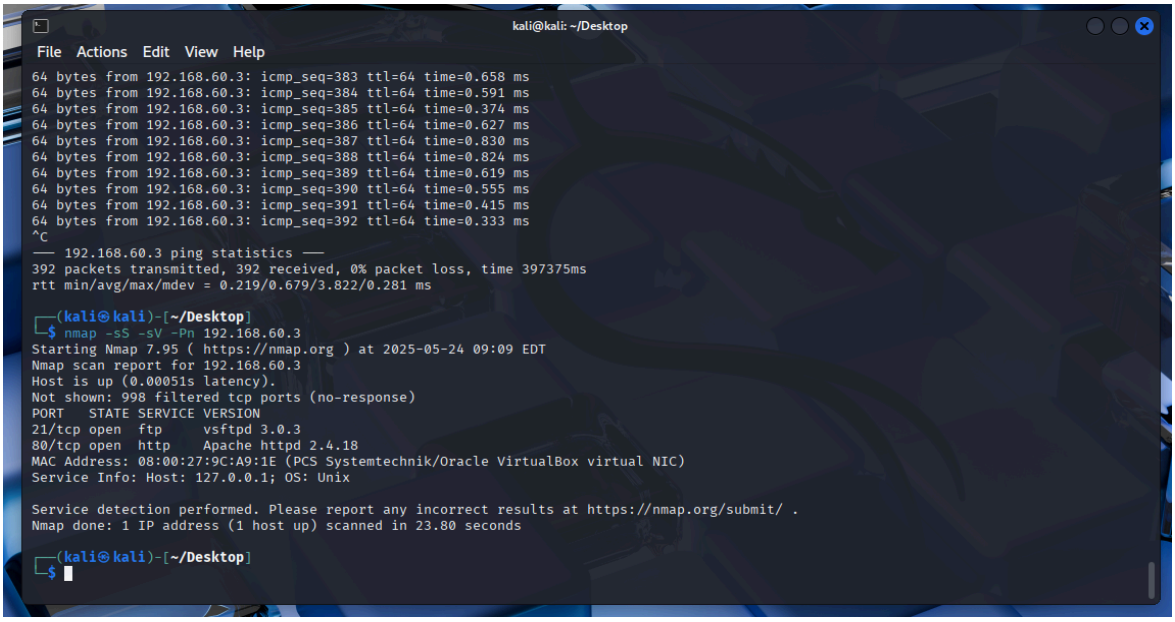




Task4: Starting the Nmap Scan

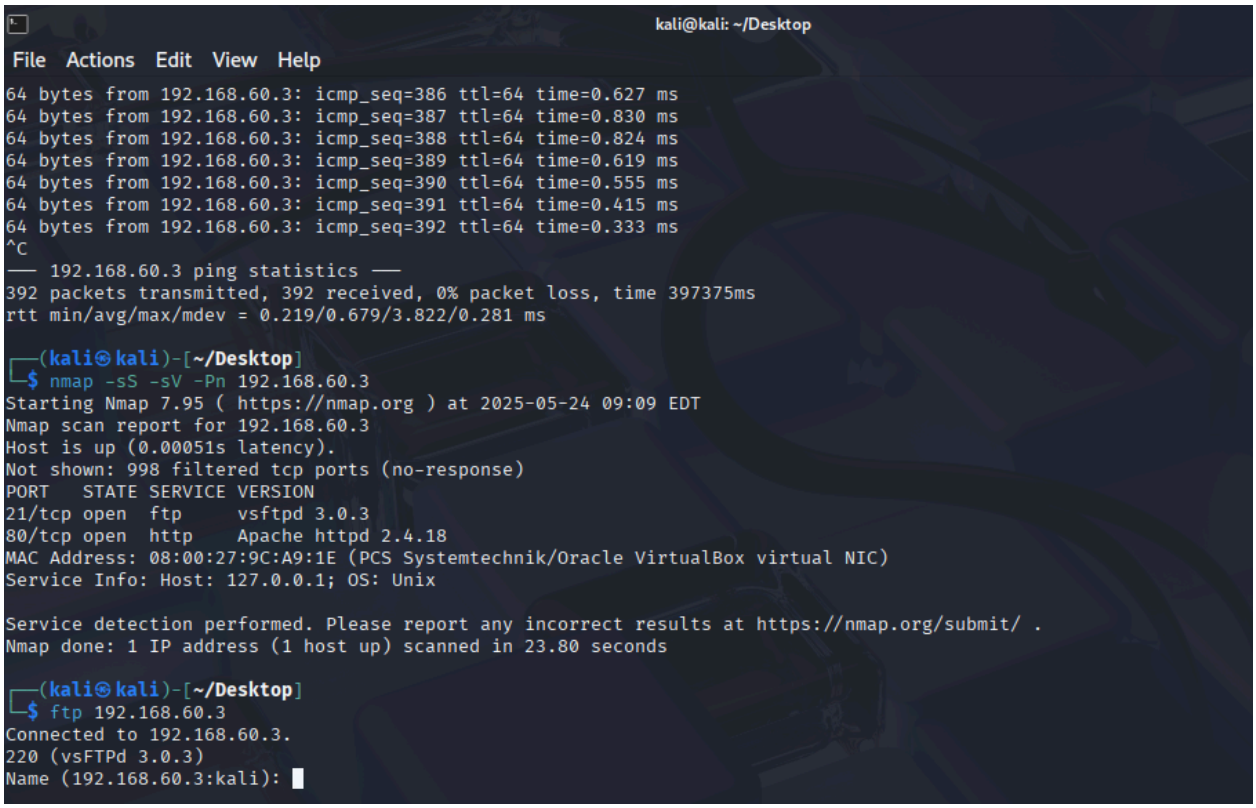
Run the following command:

nmap -sS -sV -Pn 192.168.60.3



Now, test FTP for default/anonymous access.

ftp 192.168.60.3

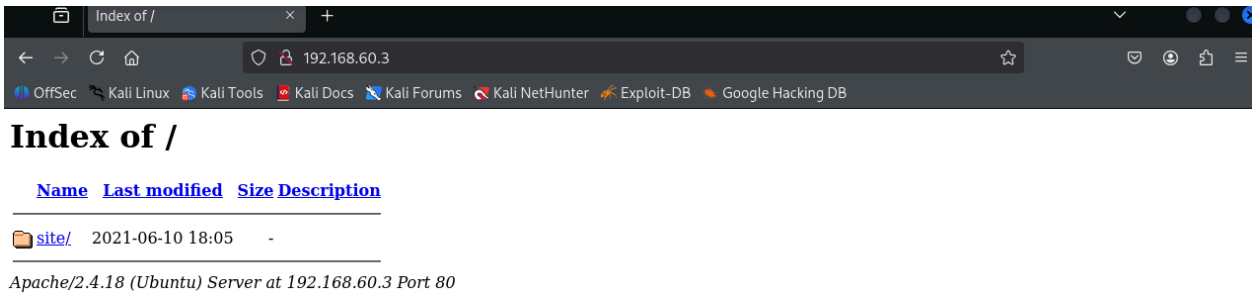


As though the ftp port was unsuccessful, now we try the other http port.

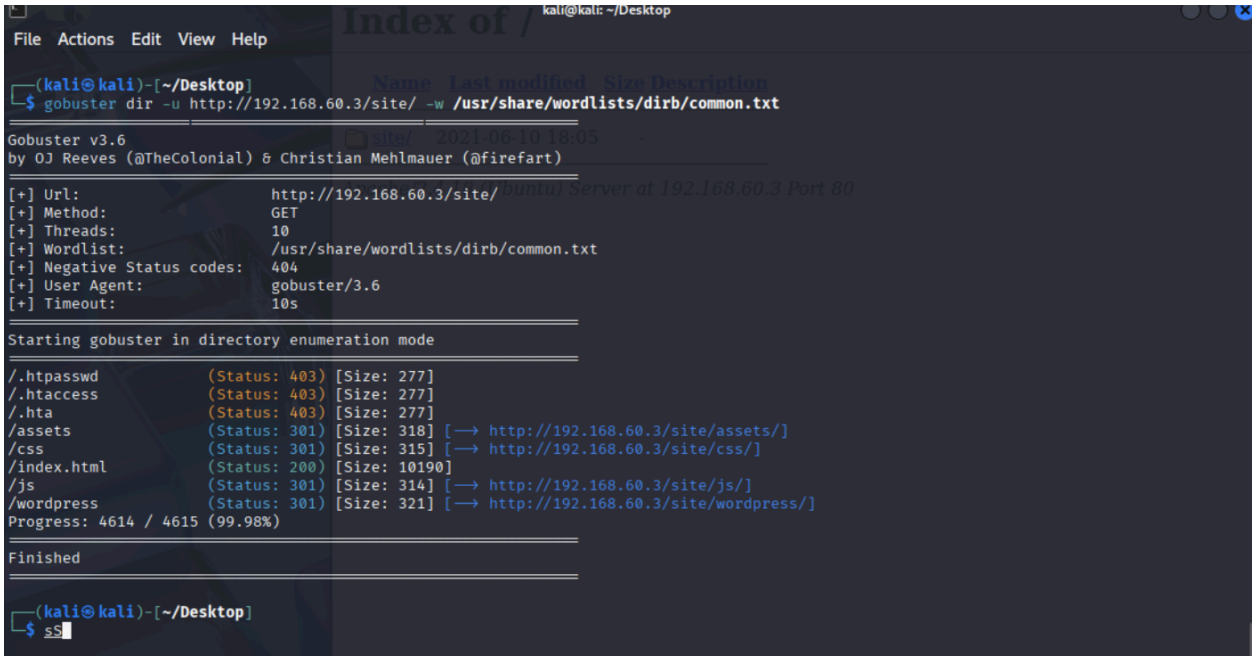
Task6: HTTP Port: Go to the Webpage

Open firefox in kali go to

http://192.168.60.3

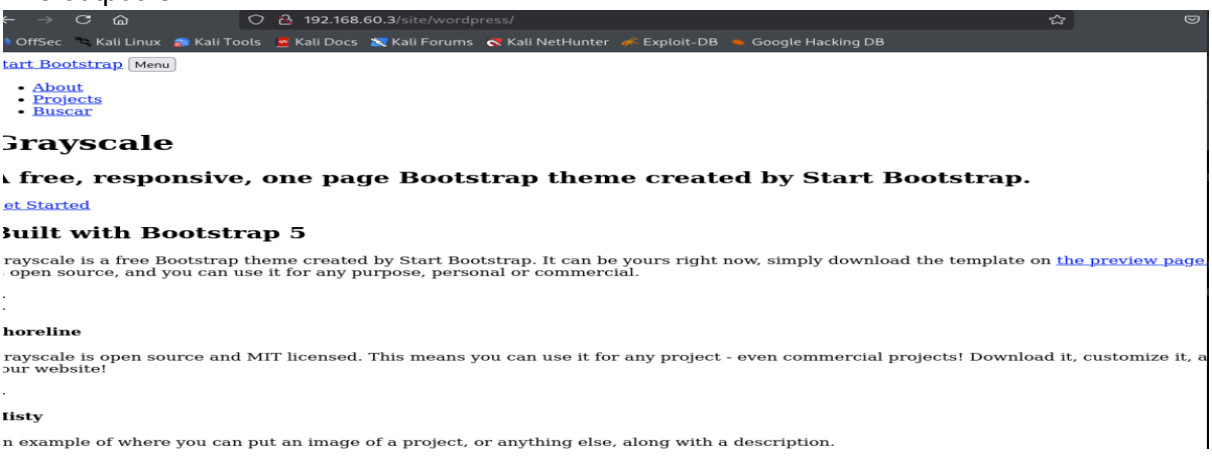


Task7: Directory Bursting

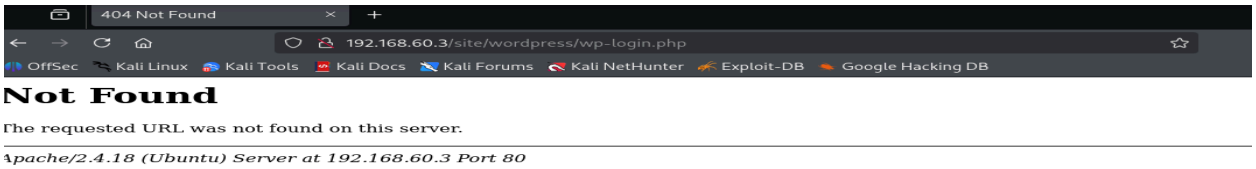


Directory	Statu	Description
`/site/assets/`	301	Static files (CSS/JS/images) — usually not useful
`/site/css/`	301	CSS files
`/site/js/`	301	JavaScript files (may contain hints!)
`/site/wordpress/`	301	**Main target — could lead to login/exploit**
`.htaccess`, `.htpasswd`, `.hta`	403	Forbidden (hidden,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

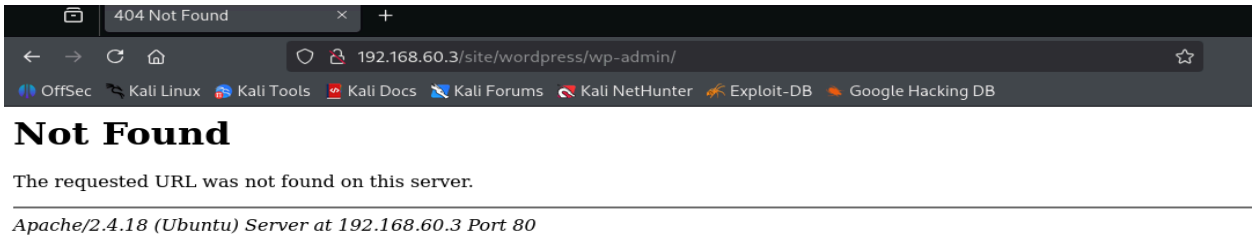
Let's check this out:
http://192.168.60.3/site/wordpress/
The output is:



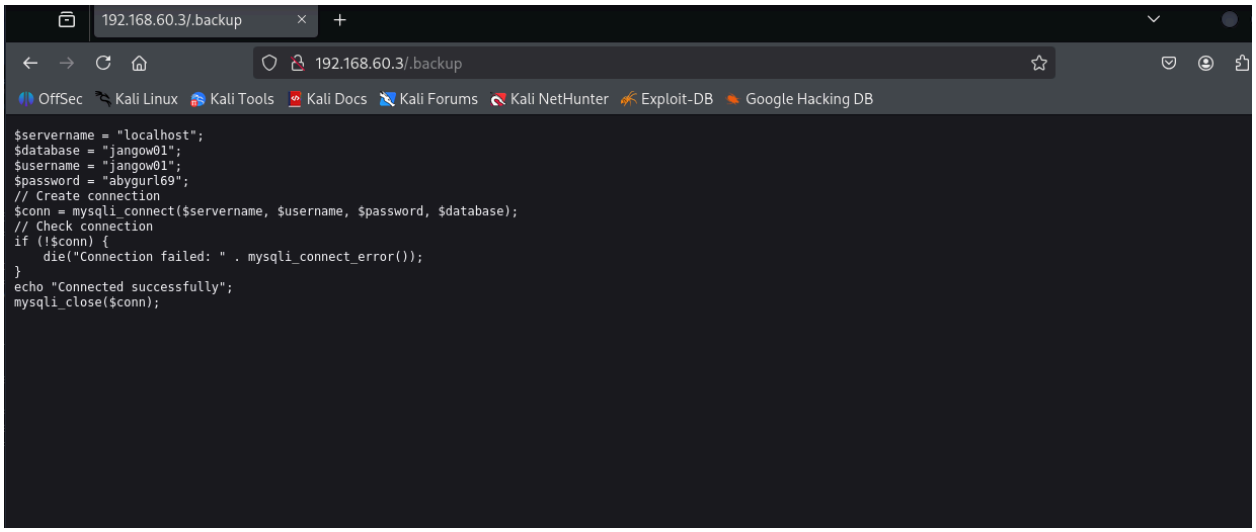
Now, try visiting.
http://192.168.60.3/site/wordpress/wp-login.php



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)



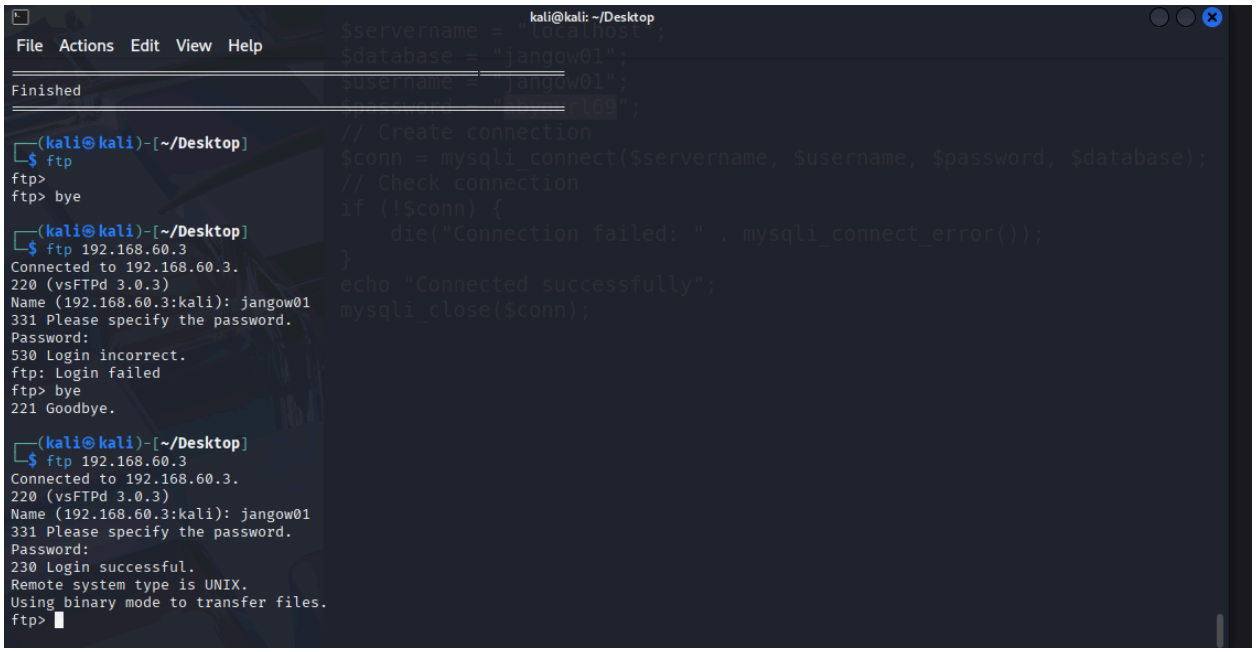
Task9: FTP Port: Inputing the .Backup Credentials

The credentials found in .backup file are:

$username = *"jangow01";*

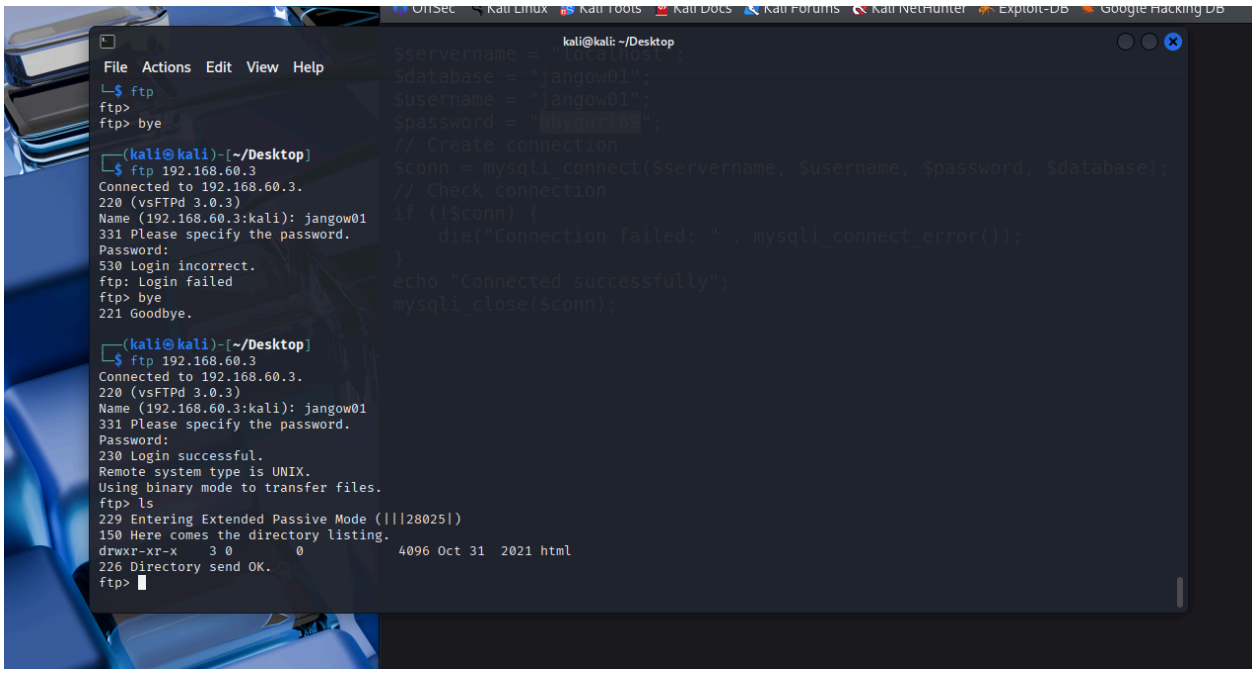
$password = *"abgyur169";*

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



Now, use these commands:

ls # list directory

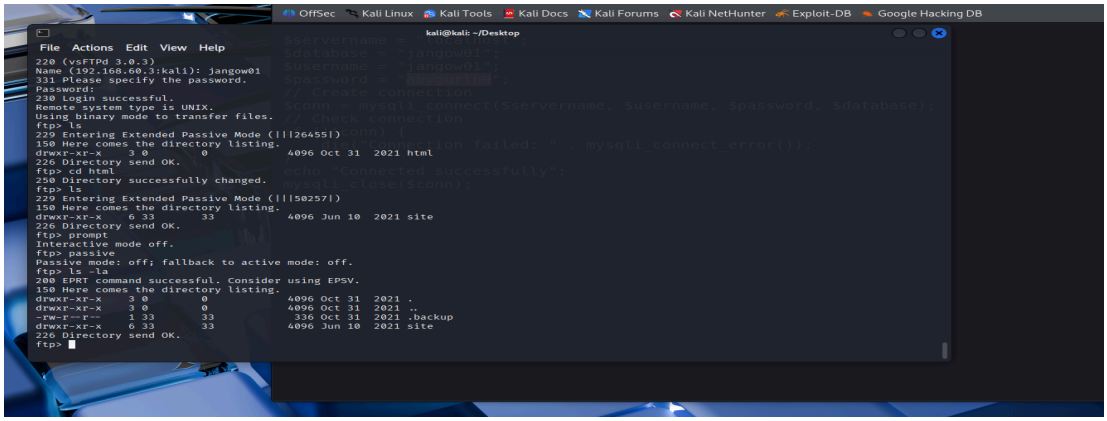


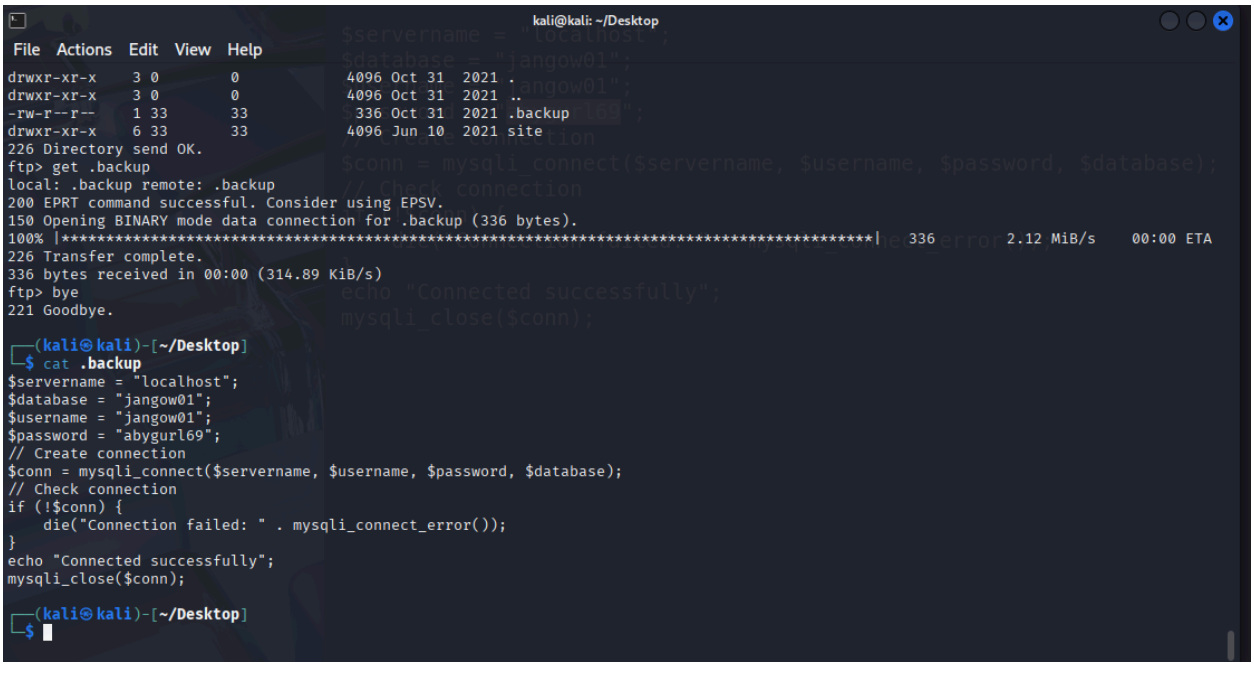
Directory found:

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

cd <dir> # change directory

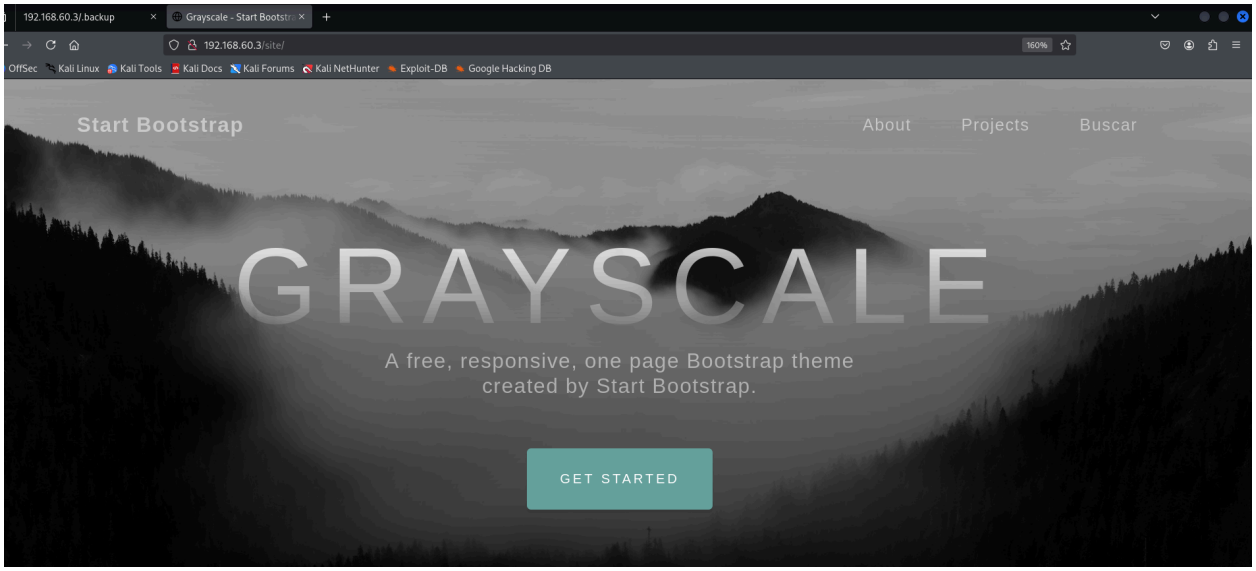
get <file> # download file



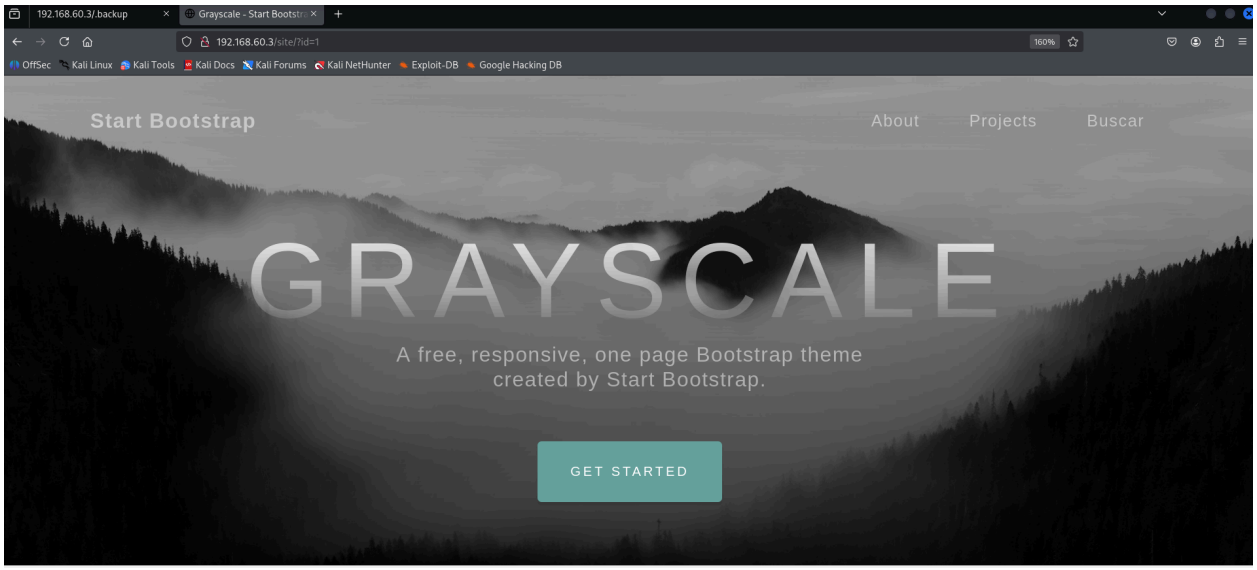


Task8: Command-Line Injection

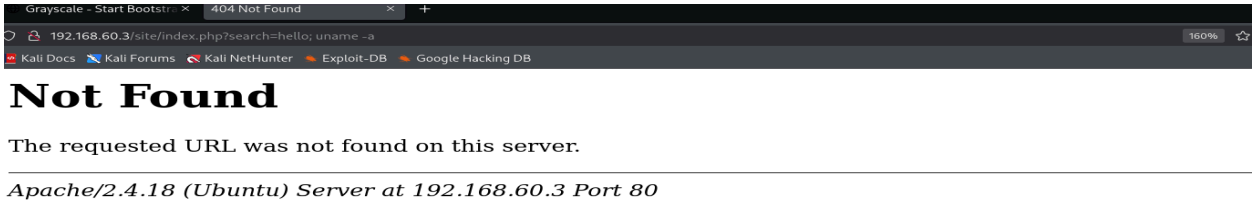
Opened the website again:



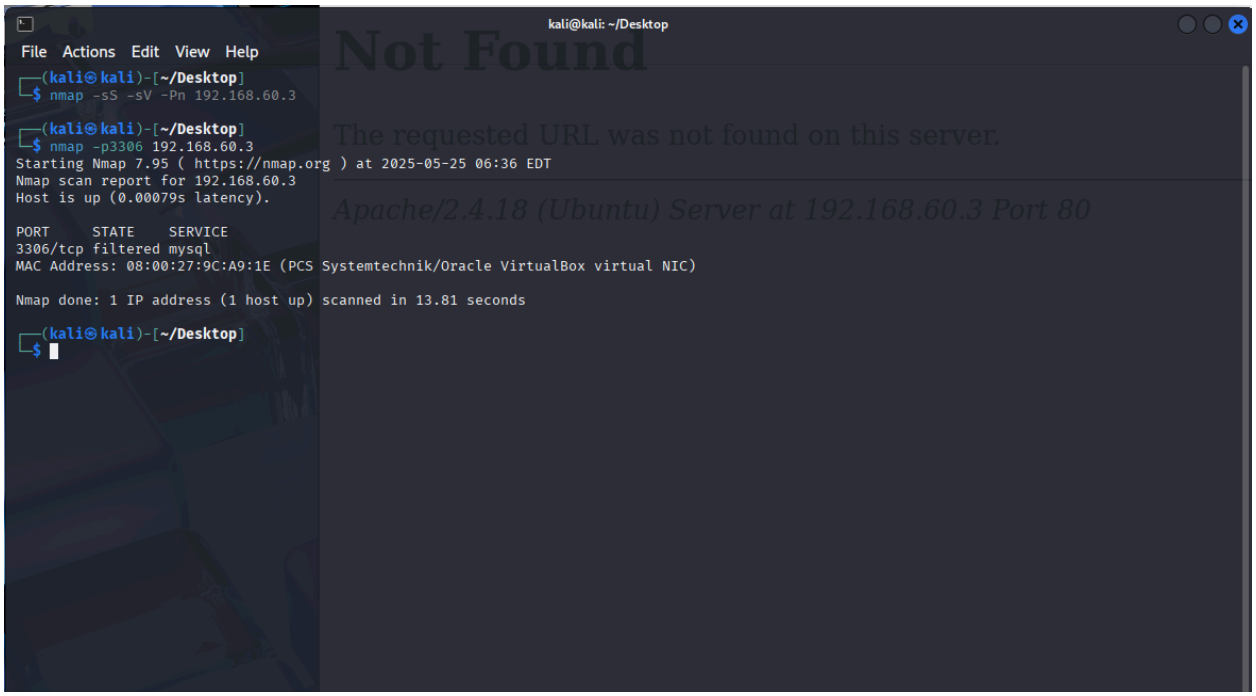
Trying the Url: http://192.168.60.3/site/?id=1 also takes us to the same site.



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.

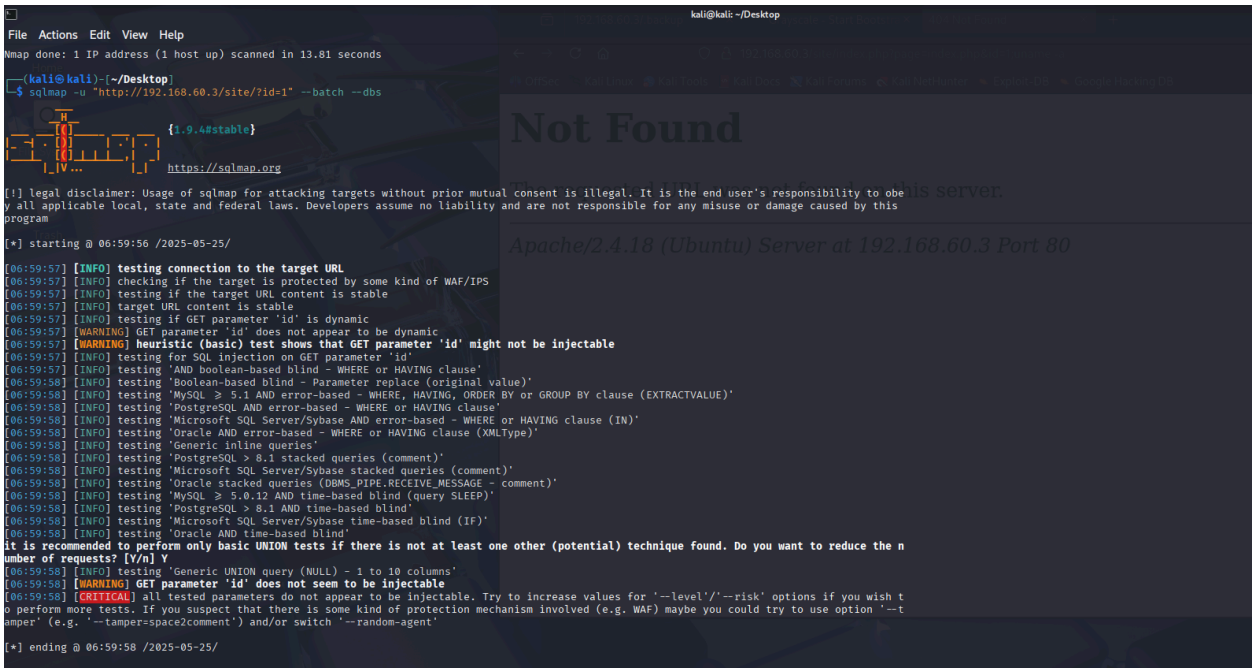


Trying nmap scan to check if mysql port(3306) is open. It is present but **filtered**, likely due to firewall rules or it being only accessible locally.



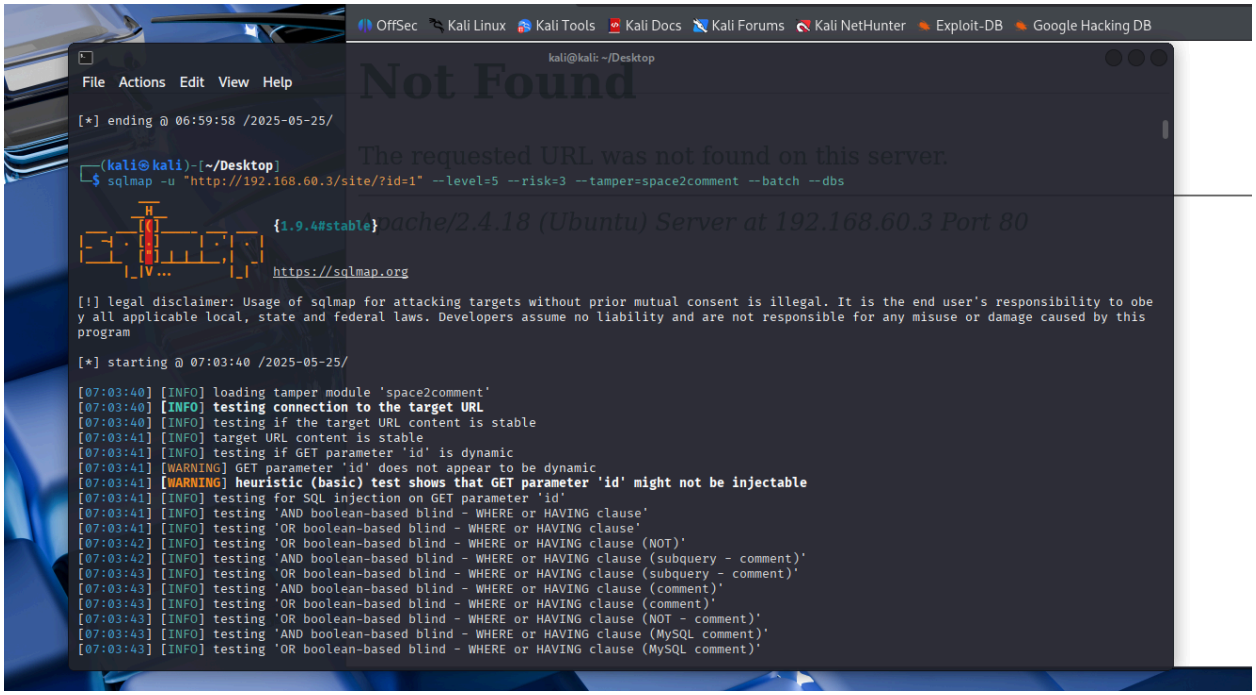
Now let's try **SQL Injection** to work this out. Targeting the following URL.
http://192.168.60.3/site/?id=1

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



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



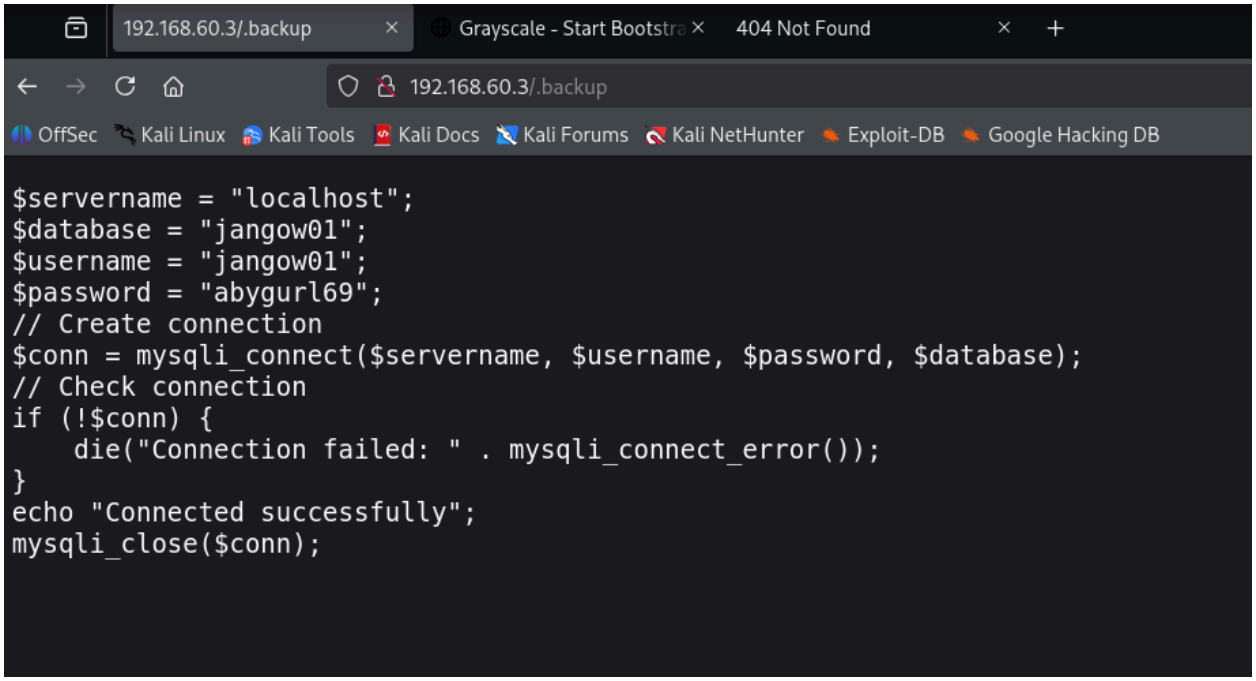
The parameters are not injectable.

```
[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.



Logging in to the machine: Login was successful.