

Cloud Computing

Lab 5: Applying Security on Cloud Application

Due Date: Tuesday, March 17, 2021 (11:59pm).

St: Mohammed AL zhrani

Student ID: 2041606 Objective

Applying security on applications through deploying access controls onto virtual machines on VMware platform. Access control are deployed using local firewalls on virtual machines.

Equipment, Tools, Hardware, and Software Needed

1. Desktop PC, Laptop with internet connection.
2. VMware Workstation software - free downloadable
3. Ubuntu (live image) - free downloadable. You may download other Operating Systems image.
4. UFW service.

Theorem

The deployment of an Enterprise Application one of the important practice in cloud computing. Implementing a multitier application on cloud is a vital job.

In this Lab, we will prepare and deploy a firewall to our VMware platform to each virtual machine to limit the access to specific application ports and service

Procedure

***** Note: Use your previous Lab VMs**

Experiment 1 – Check DB server access from none authorized host (VM or Client).

From the **VM 3**, Try the following command:

Install MySQL client:

```
sudo apt install mysql-client
```

Test connecting to DB server

```
sudo
```

```
mysql -h VM_2_IP_Address_or_DB_Server -u example_user -p
```

(**Password:** password)

Report if you were able to connect to DB server or not? **Yes , its enable to connect with DB**

MySQL> ← means you were able to connect

Experiment 2 – Lock down the access of DB server using Firewall.

To do the deployment we have to do the procedure based on the services in sequence:

Database Server – VM 2

Do the following installation and implementation steps.

sudo apt install ufw
sudo ufw app list
sudo ufw status
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow ssh
sudo ufw allow from <i>VM_1_IP_Address_or_Web/PHP_server_Address</i> to any port 3306
sudo ufw enable

Test 1: Client User – VM 3 (or your host machine or desktop)

Re-do Experiment 1 (if not installed), and report your observation

Test 2: Web/PHP server – VM 1

Re-do Experiment 1 (if not installed), and report your observation

Lab Task

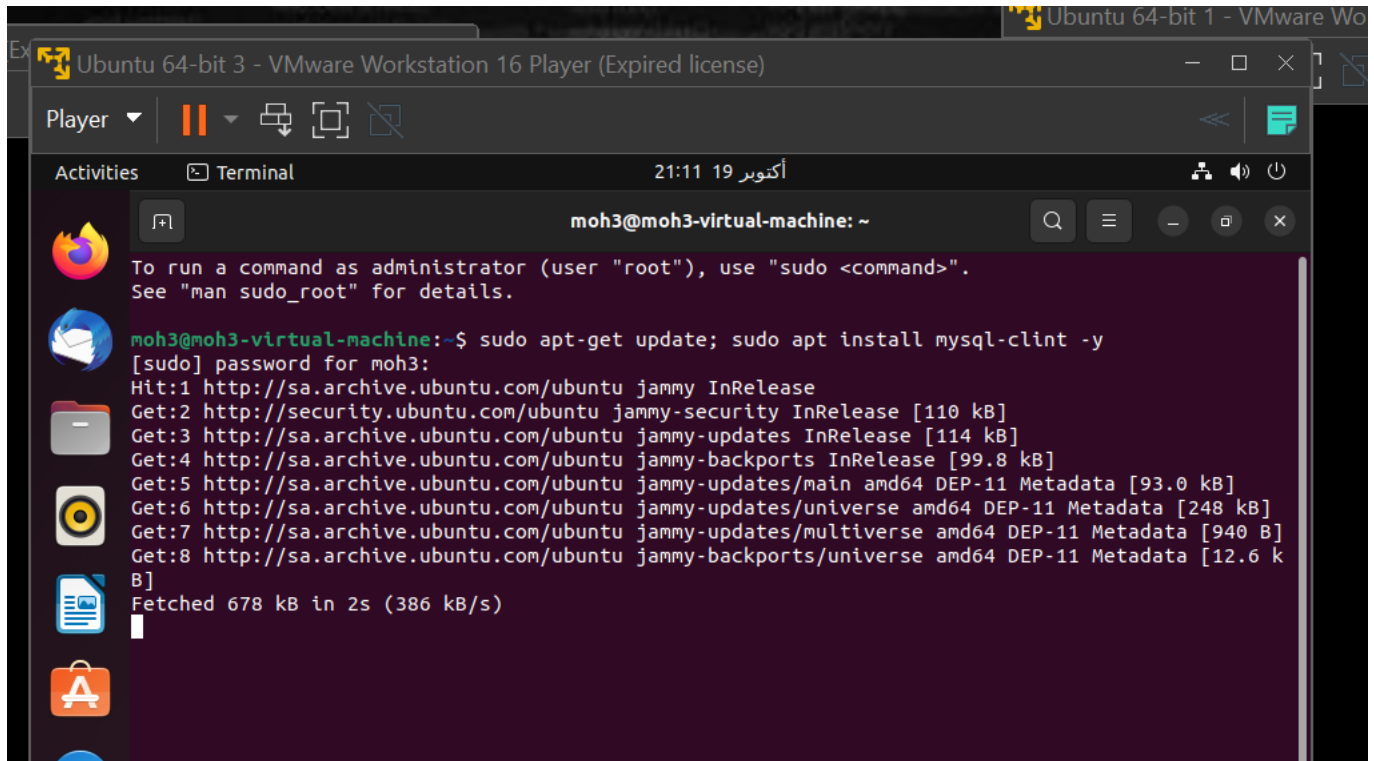
1. Report all outputs of all commands on the procedure above.
2. Answer the following question:
 - What is the use of Firewall on front of data base server?? **ufw**

Lab Report

For the lab report, take a screenshots of your VMware Workstation configuration and include Command Line logs for the Virtual Machines as requested in the Lab Task.

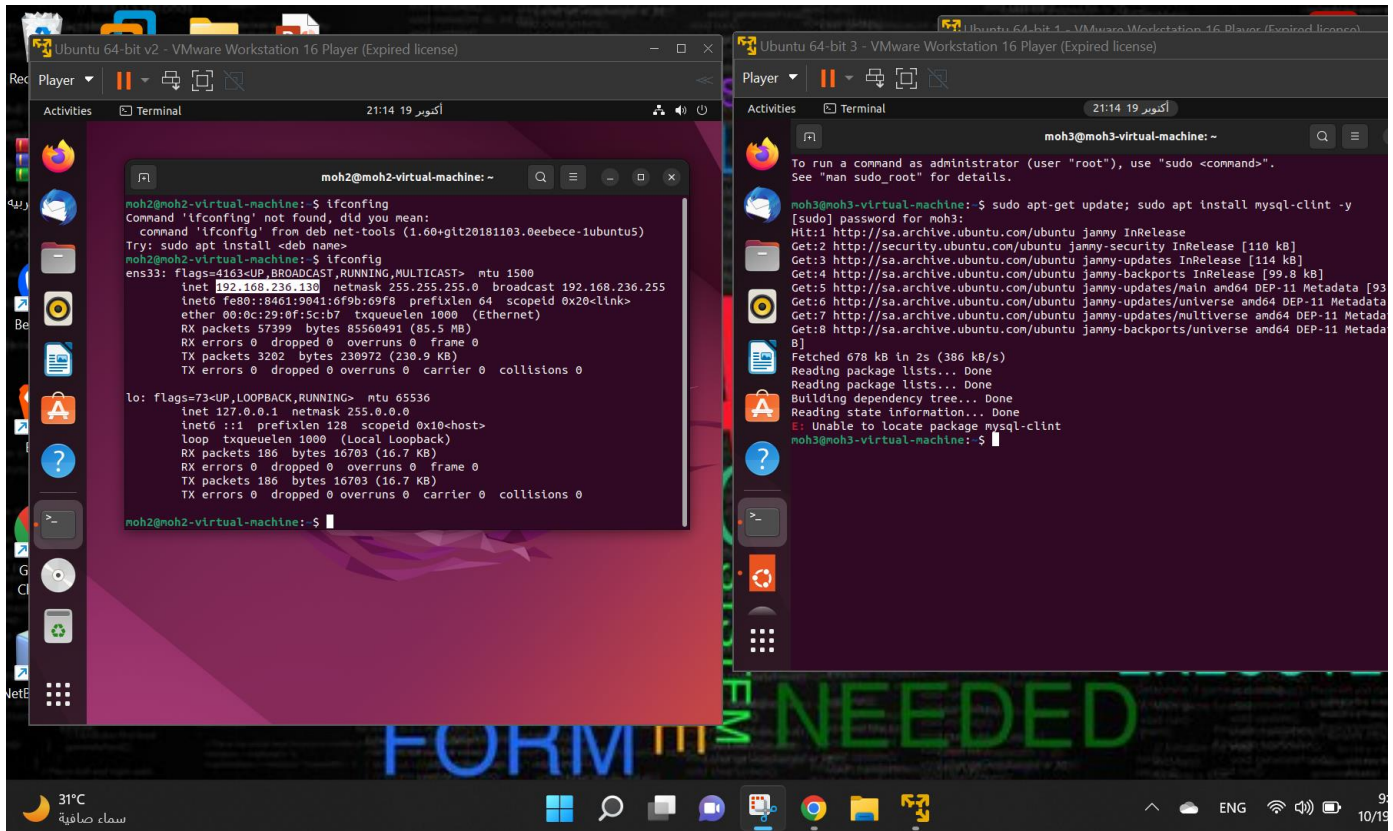
Check DB server access from none authorized host (VM or Client)

Install my sql clint

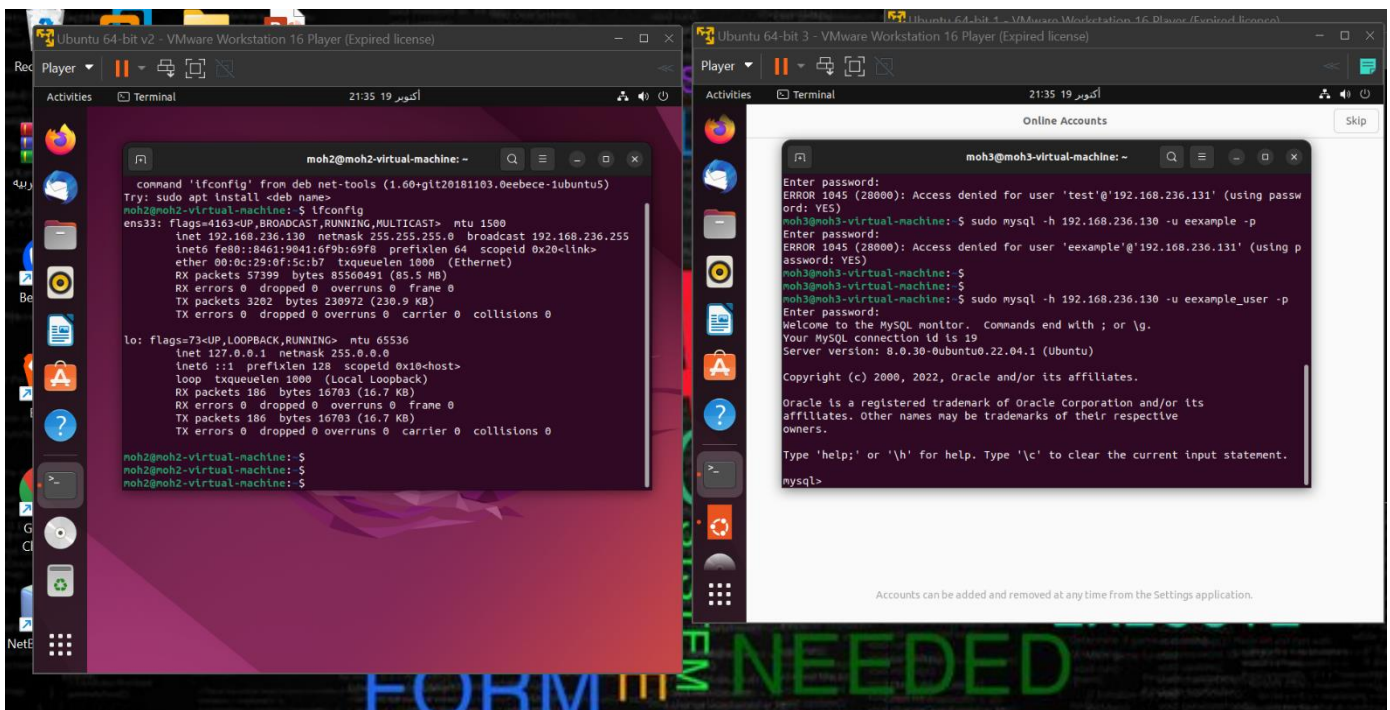


```
moh3@moh3-virtual-machine: ~  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
moh3@moh3-virtual-machine:~$ sudo apt-get update; sudo apt install mysql-clint -y  
[sudo] password for moh3:  
Hit:1 http://sa.archive.ubuntu.com/ubuntu jammy InRelease  
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]  
Get:3 http://sa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]  
Get:4 http://sa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]  
Get:5 http://sa.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [93.0 kB]  
Get:6 http://sa.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [248 kB]  
Get:7 http://sa.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]  
Get:8 http://sa.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [12.6 k  
B]  
Fetched 678 kB in 2s (386 kB/s)
```

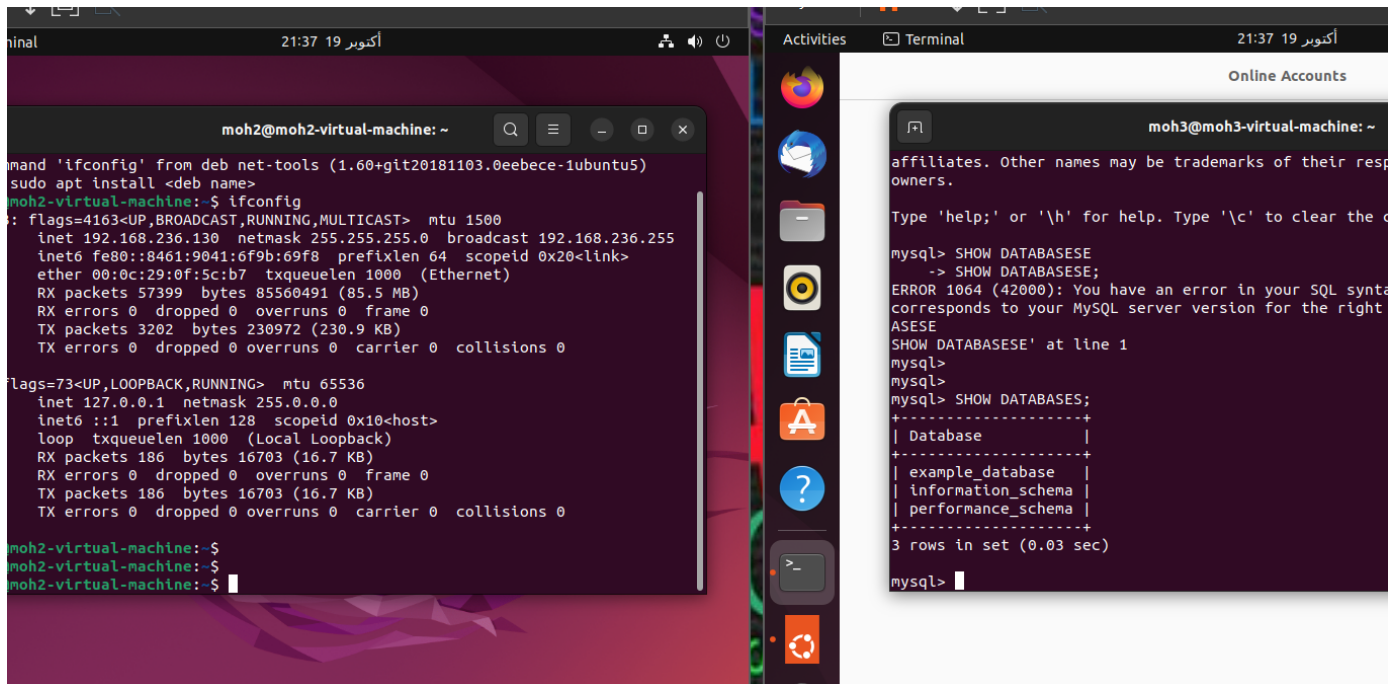
We should know the ip of vm2 to try connect to DB



We have connected to DB



Check ..



Now we will go to vm2 and do the task

```
sudo apt install ufw
```

```
sudo ufw app list
```

```
sudo ufw status
```

```
sudo ufw default deny incoming
```

```
sudo ufw default allow outgoing
```

```
sudo ufw allow ssh
```

```
sudo ufw allow from VM_1_IP_Address_or_Web/PHP_server_Address to any port 3306
```

```
sudo ufw enable
```

S

```
TX packets 186 bytes 16703 (16.7 KB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 186 bytes 16703 (16.7 KB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

moh2@moh2-virtual-machine:~$
moh2@moh2-virtual-machine:~$
moh2@moh2-virtual-machine:~$
moh2@moh2-virtual-machine:~$ sudo apt-get update; sudo apt install ufw -y
[sudo] password for moh2:
Hit:1 http://sa.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://sa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
```

List

```
0 upgraded, 0 newly installed, 0 to remove and 128 not upgraded.
moh2@moh2-virtual-machine:~$
moh2@moh2-virtual-machine:~$ sudo ufw app list
Available applications:
  CUPS
moh2@moh2-virtual-machine:~$
```

status

```
app info PROFILE          show information on PROFILE
app update PROFILE        update PROFILE
app default ARG           set default application policy

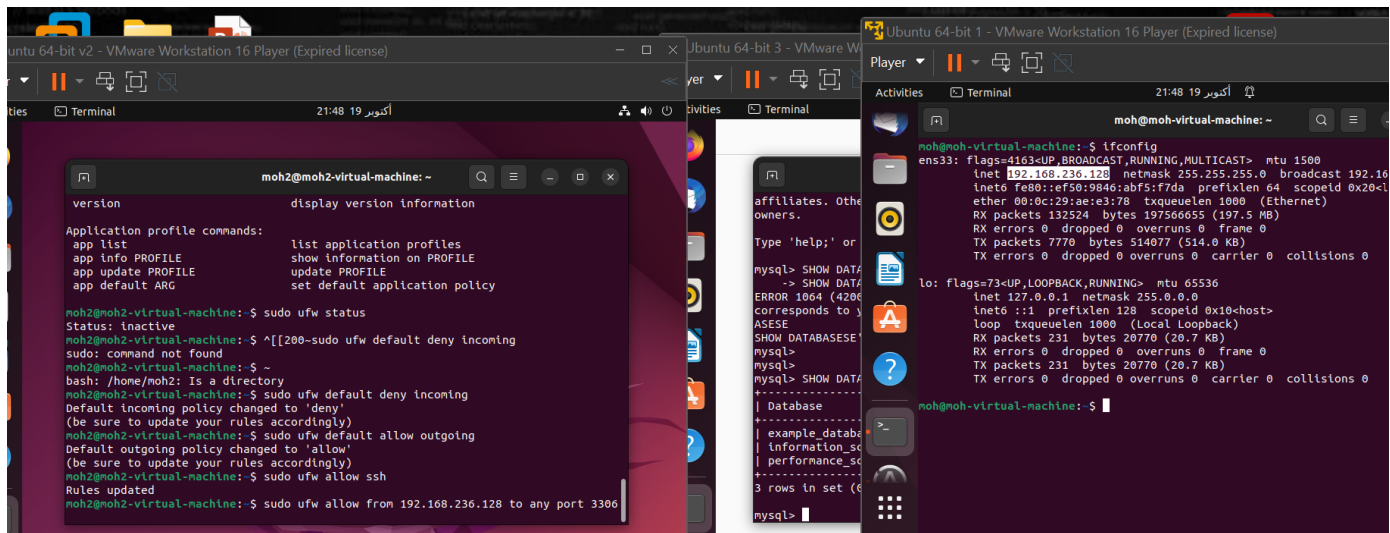
moh2@moh2-virtual-machine:~$ sudo ufw status
Status: inactive
moh2@moh2-virtual-machine:~$
```

sudo ufw default deny incoming

sudo ufw default allow outgoing

```
bash: /home/moh2: Is a directory
moh2@moh2-virtual-machine:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
moh2@moh2-virtual-machine:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
moh2@moh2-virtual-machine:~$
```


We need to let vm1 have an access to DB Not: its just for this ip in this port



The image shows three terminal windows from a VMware Workstation 16 Player. The left window shows the output of 'ufw status' and 'ufw default deny incoming', followed by 'ufw default allow outgoing' and 'ufw allow from 192.168.236.128 to any port 3306'. The middle window shows the output of 'ifconfig' for the 'ens33' interface, displaying the IP address 192.168.236.128. The right window shows the output of 'mysql> SHOW DATABASES;' and 'mysql> exit;', followed by the command 'sudo mysql -h 192.168.236.130 -u eexample_user -p'.

```
moh2@moh2-virtual-machine: ~  
version display version information  
Application profile commands:  
app list list application profiles  
app info PROFILE show information on PROFILE  
app update PROFILE update PROFILE  
app default ARG set default application policy  
  
moh2@moh2-virtual-machine:~$ sudo ufw status  
Status: inactive  
moh2@moh2-virtual-machine:~$ sudo ufw default deny incoming  
sudo: command not found  
moh2@moh2-virtual-machine:~$ sudo ufw default deny incoming  
bash: /home/moh2: Is a directory  
moh2@moh2-virtual-machine:~$ sudo ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
moh2@moh2-virtual-machine:~$ sudo ufw default allow outgoing  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
moh2@moh2-virtual-machine:~$ sudo ufw allow ssh  
Rules updated  
moh2@moh2-virtual-machine:~$ sudo ufw allow from 192.168.236.128 to any port 3306
```

```
moh@moh-virtual-machine:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.236.128 netmask 255.255.255.0 broadcast 192.168.236.255  
    inet6 fe80::ef50:9846:abf5:f7da prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:ae:e3:78 txqueuelen 1000 (Ethernet)  
    RX packets 132524 bytes 197566655 (197.5 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 7770 bytes 514077 (514.0 KB)  
    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 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 231 bytes 20770 (20.7 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 231 bytes 20770 (20.7 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
moh@moh-virtual-machine:~$
```

```
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| example_database |  
| information_schema |  
| performance_schema |  
+-----+  
3 rows in set (0.03 sec)  
  
mysql>  
mysql> exit;  
Bye  
moh3@moh3-virtual-machine:~$ sudo mysql -h 192.168.236.130 -u eexample_user -p  
[sudo] password for moh3:  
Sorry, try again.  
[sudo] password for moh3:  
Enter password:
```

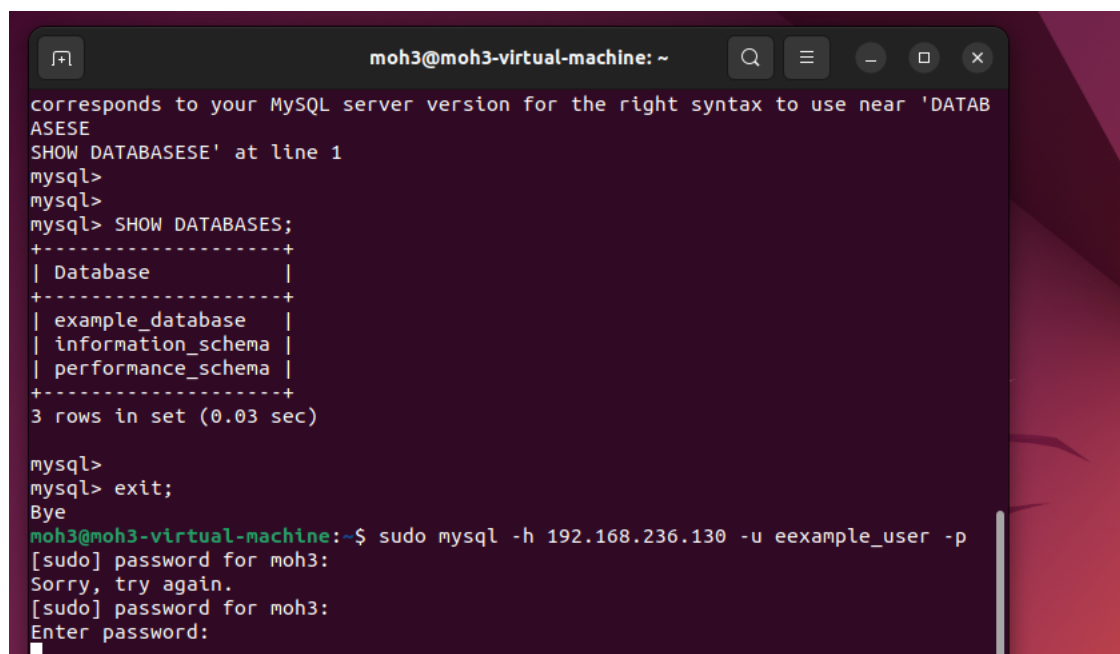
And last thing is enable



The image shows a terminal window with the command 'sudo ufw enable' and its output 'Firewall is active and enabled on system startup'.

```
moh2@moh2-virtual-machine:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
moh2@moh2-virtual-machine:~$
```

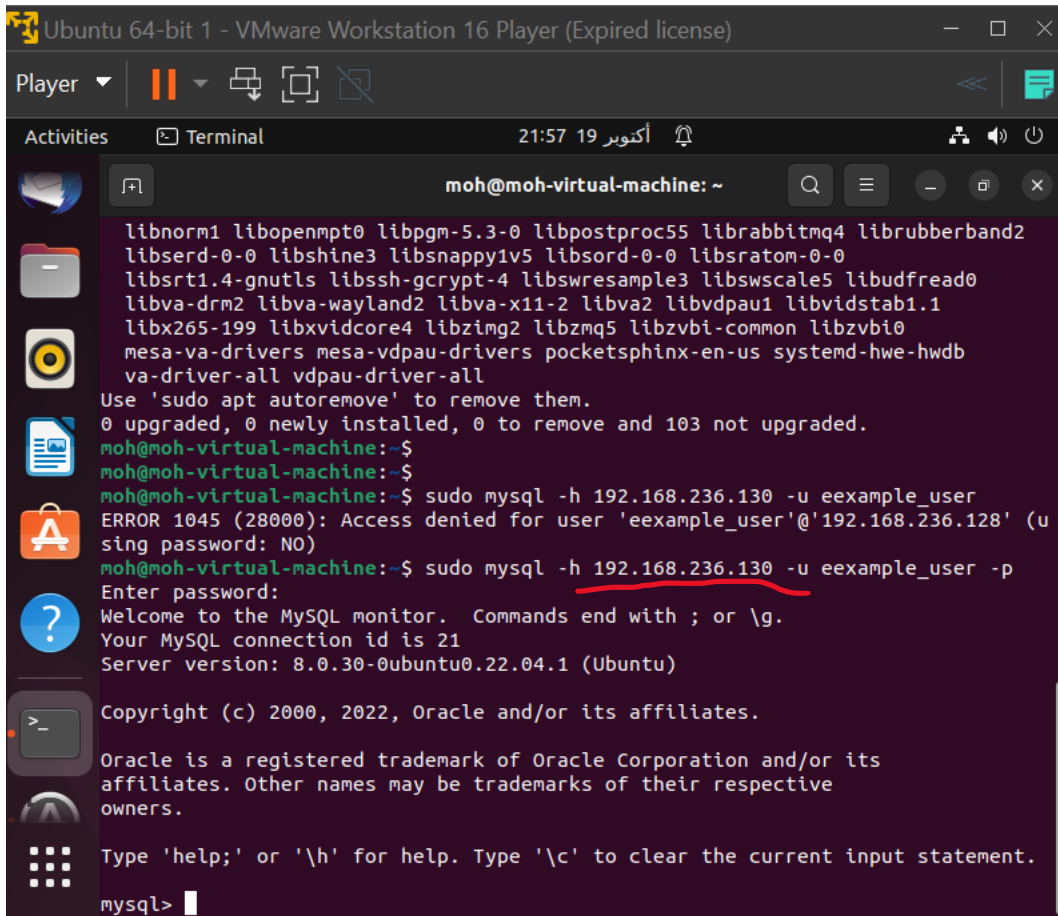
Note : if we try to connect from vm3 , we will not have access



The image shows a terminal window with the command 'mysql> SHOW DATABASES;' and its output. It also shows the command 'mysql> exit;' and the command 'sudo mysql -h 192.168.236.130 -u eexample_user -p' with the password prompt.

```
moh3@moh3-virtual-machine:~  
corresponds to your MySQL server version for the right syntax to use near 'DATAB  
ASESE  
SHOW DATABASESE' at line 1  
mysql>  
mysql>  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| example_database |  
| information_schema |  
| performance_schema |  
+-----+  
3 rows in set (0.03 sec)  
  
mysql>  
mysql> exit;  
Bye  
moh3@moh3-virtual-machine:~$ sudo mysql -h 192.168.236.130 -u eexample_user -p  
[sudo] password for moh3:  
Sorry, try again.  
[sudo] password for moh3:  
Enter password:
```

but if we try to connect from vm1 we will connect !



```
libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2
libserd-0-0 libshine3 libsnappy1v5 libsord-0-0 libsratom-0-0
libstr1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0
libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1
libx265-199 libxvidcore4 libzim2 libzmq5 libzvt-common libzvt0
mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us systemd-hwe-hwdb
va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 103 not upgraded.
moh@moh-virtual-machine:~$
moh@moh-virtual-machine:~$
moh@moh-virtual-machine:~$ sudo mysql -h 192.168.236.130 -u eexample_user
ERROR 1045 (28000): Access denied for user 'eexample_user'@'192.168.236.128' (u
sing password: NO)
moh@moh-virtual-machine:~$ sudo mysql -h 192.168.236.130 -u eexample_user -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 8.0.30-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```