Cybersecurity Nishama -Technical

The Capstone Project

January 15, 2023

Introduction

The overall goal of this capstone project is to apply as many technical skills as possible that I acquired during the course. To achieve this goal, the following steps will be taken:[1]

Part [1] System Design, Architecture, & Administration In this part, you will simulate the job of a system architect, you will set up the environment securely and design the architecture for it. Then, you will simulate the job of a system administrator, where you will set up the servers, install the operating systems, install different applications, and run them on the server.

Part [2] Offensive Cybersecurity

In this part, you will simulate the job of an offensive cybersecurity specialist, where you will initiate a red team engagement aiming to find the vulnerabilities in the system and exploit them to gain access.

Part [3] Defensive Cybersecurity

In this part, you will simulate the job of a defensive cybersecurity specialist, where you will show the traces of the attack and it can be detected, then apply the right fixes and needed controls to fix the vulnerabilities and protect the system.

Statement of Confidentiality

Statement of Confidentiality The contents of this document have been developed by Oruba Abu-Eisa. Considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner, or contractor without prior written consent from Engineer Mohanad Yousef. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of Engineer Mohanad Yousef.

Engagement Contacts

Assessor Name	Title	Assessor Contact Email
Oruba Abu-Eisa	Cyber Security Student	orubamabueisa@outlook.com

System Design, Architecture & Administration

When building the environment for this project, one of the most popular options is to use a virtualization product, such as VirtualBox and VMware which is what I chose to build the environment.

VMware is a leading provider of multi-cloud services for all apps, enabling digital innovation with enterprise control.[2]

List of All Components

There are 2 servers:

- SERVER-A
- SERVER-B

In addition to 4 machines:

- EMPLOYEE
- CEO
- ADMIN
- ATTACKER (of course it will not be included in the Environment architecture)

Of course, don't forget that we have one router

IP Address Plan

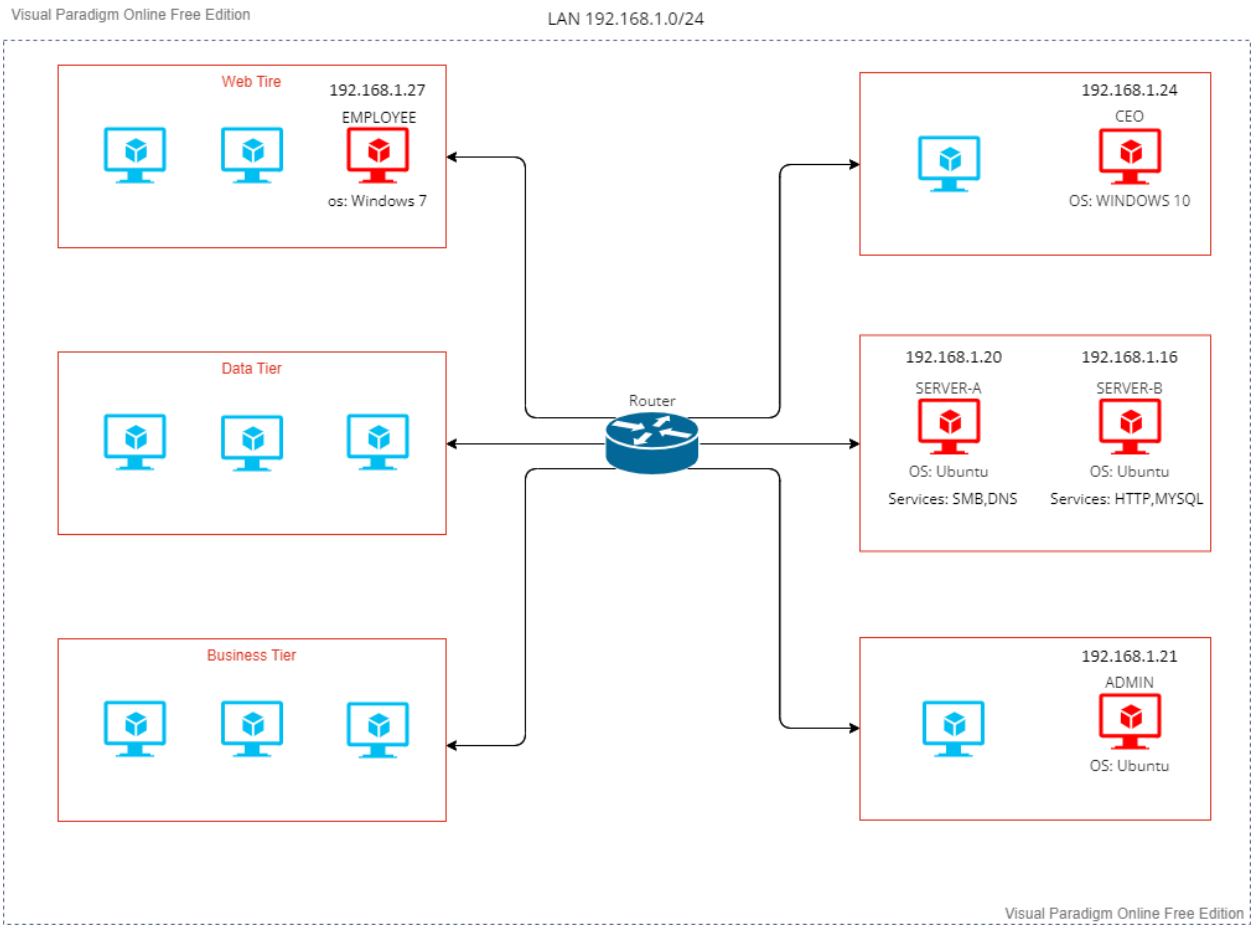
A VMware bridge is a feature that allows virtual machines (VMs) to communicate with the host computer's network interface and with other VMs on the same network.[3]

Lan ➔ 192.168.1.0/24

These are the machines and their Private IP, noting that there is no Public IP for any of these machines

- **SERVER-A** 192.168.1.20
- **SERVER-B** 192.168.1.16
- **EMPLOYEE** 192.168.1.27
- **CEO** 192.168.1.24
- **ATTACKER** 192.168.1.26
- **ADMIN** 192.168.1.21

Environment architecture



All the Running Services

SERVER-A:

- **SMB Service ➔** Version 4.15.9-Ubuntu

  Server Message Block (SMB) is a protocol used for file sharing and other network services between computers.[4]

  The purpose of the SMB service is to provide a way for computers on a network to access and share resources, such as files, printers, and other devices, with each other.[4]

- **DNS Service ➔**

  DNS (Domain Name System) is a service that translates human-friendly domain names (such as www.example.com) into machine-friendly IP addresses (such as 192.0.2.1).[5]

  The purpose of the DNS service is to provide a decentralized, hierarchical system for resolving domain names to IP addresses. This allows users to access web sites, email

servers, and other internet resources using easy-to-remember domain names instead of the IP addresses.[5]

SERVER-B:

- **MYSQL Service ➔** MySQL Ver 8.0.31-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))

  MySQL is a popular open-source relational database management system (RDBMS) that is widely used for managing and storing data in web-based applications, online platforms, and other software systems.[6]

  The purpose of MySQL is to provide a reliable, efficient, and flexible way to store, manage, and retrieve large amounts of data.[6]

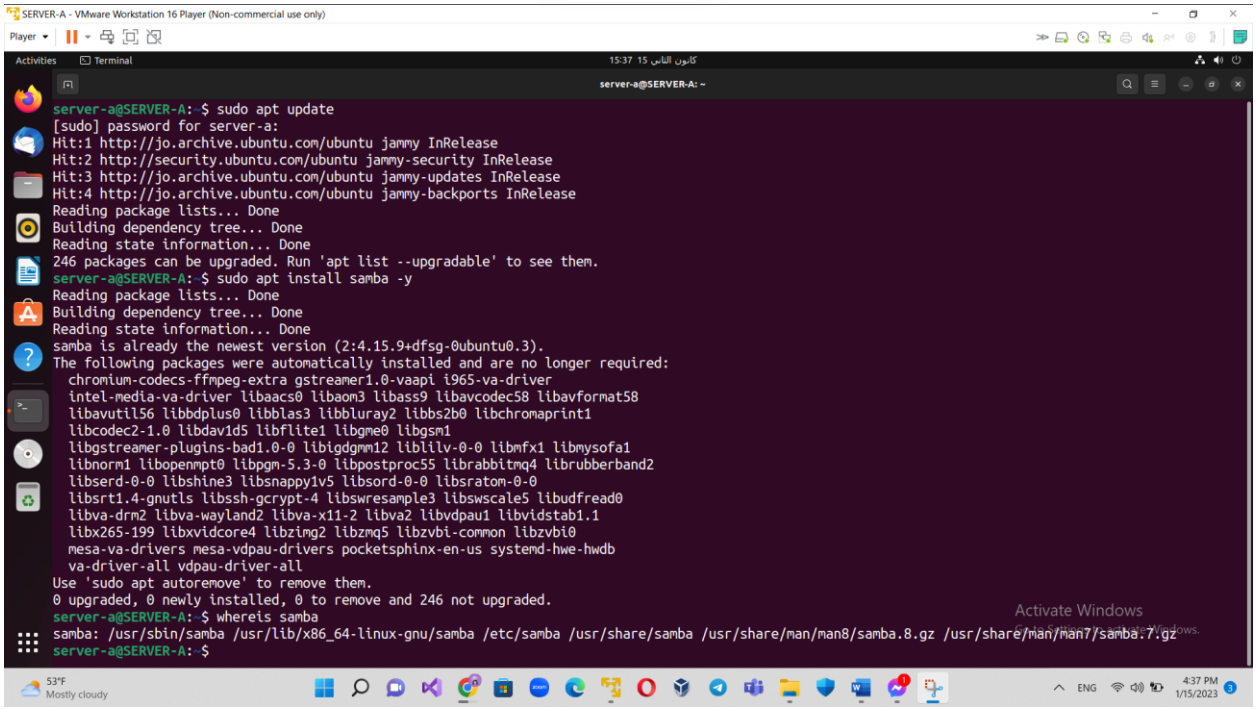
- **HTTP Service ➔** nginx 1.18.0 (Ubuntu)

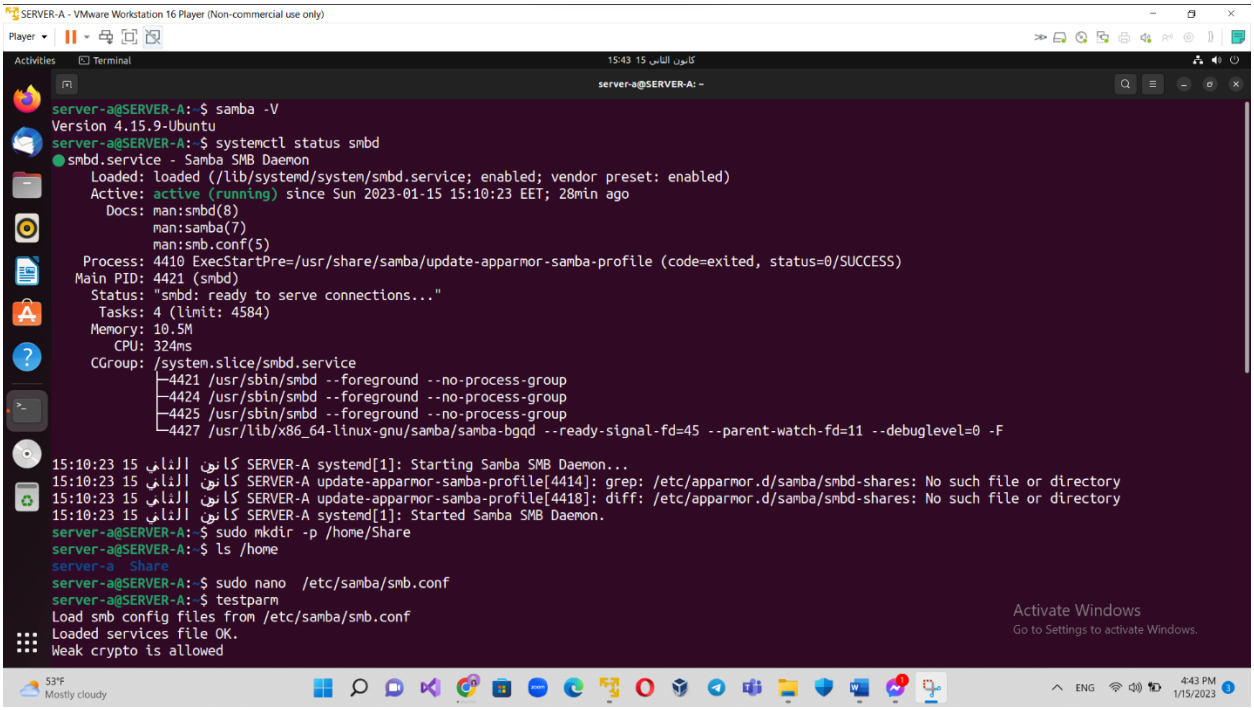
  HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet. It is the foundation of the World Wide Web and is used by web browsers, servers, and other applications to communicate with each other.[7]

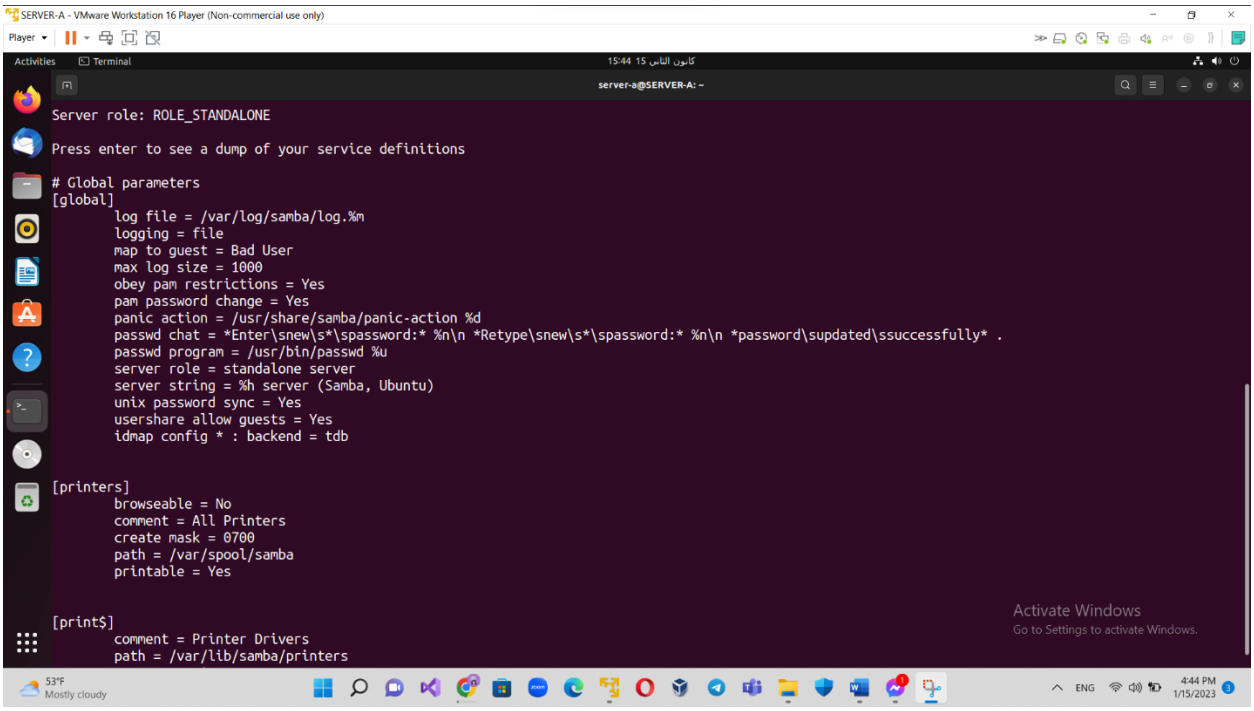
  The purpose of the HTTP service is to transfer data between a client (such as a web browser) and a server.[7]

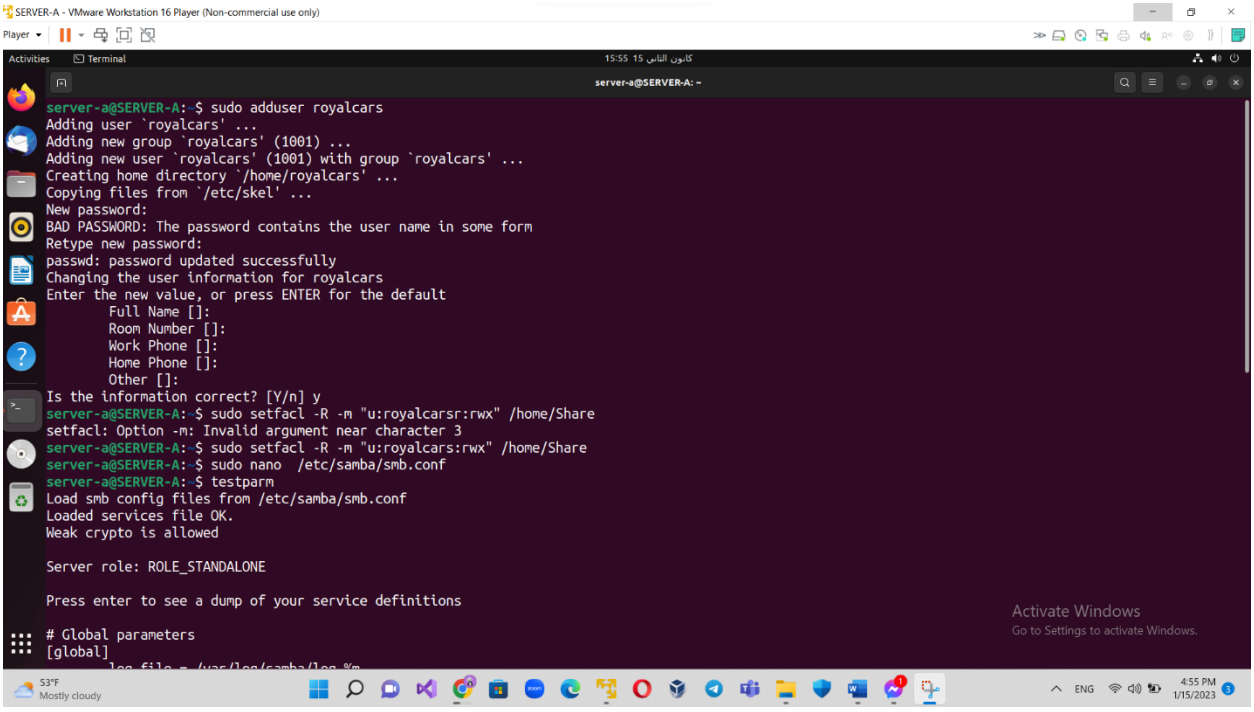
Installation Steps of Services & showing that are running

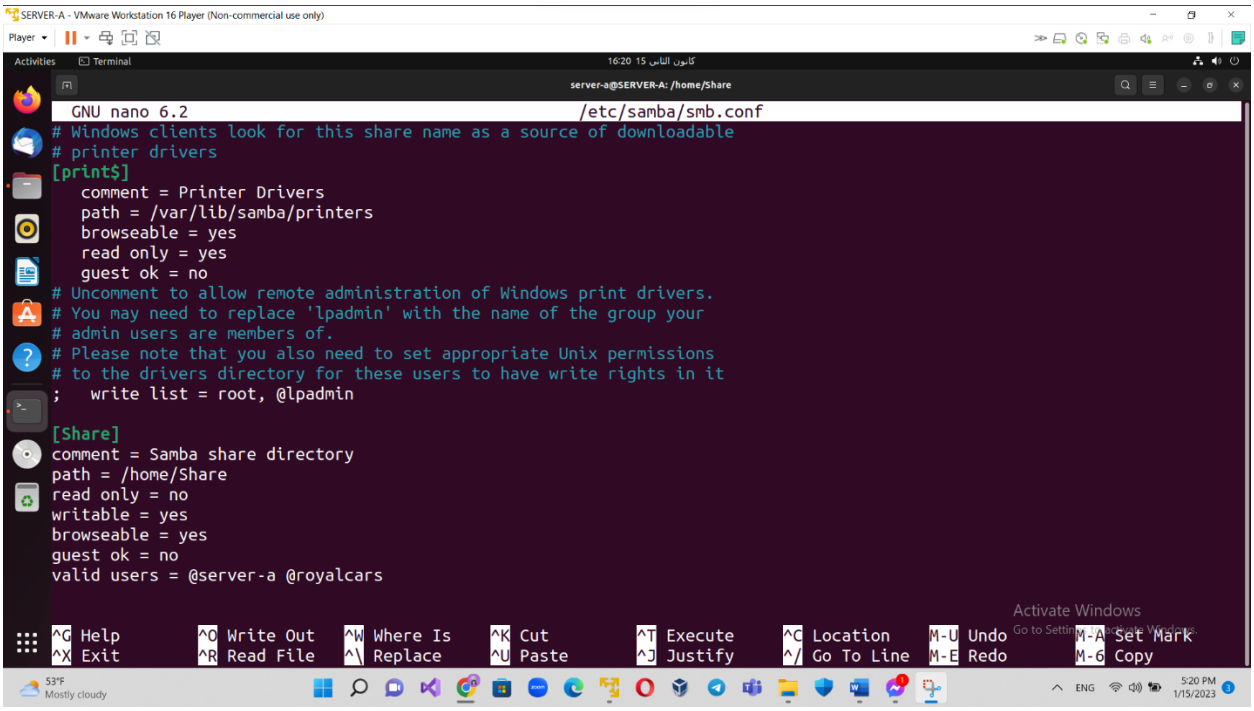
- **SMB Service [8]**

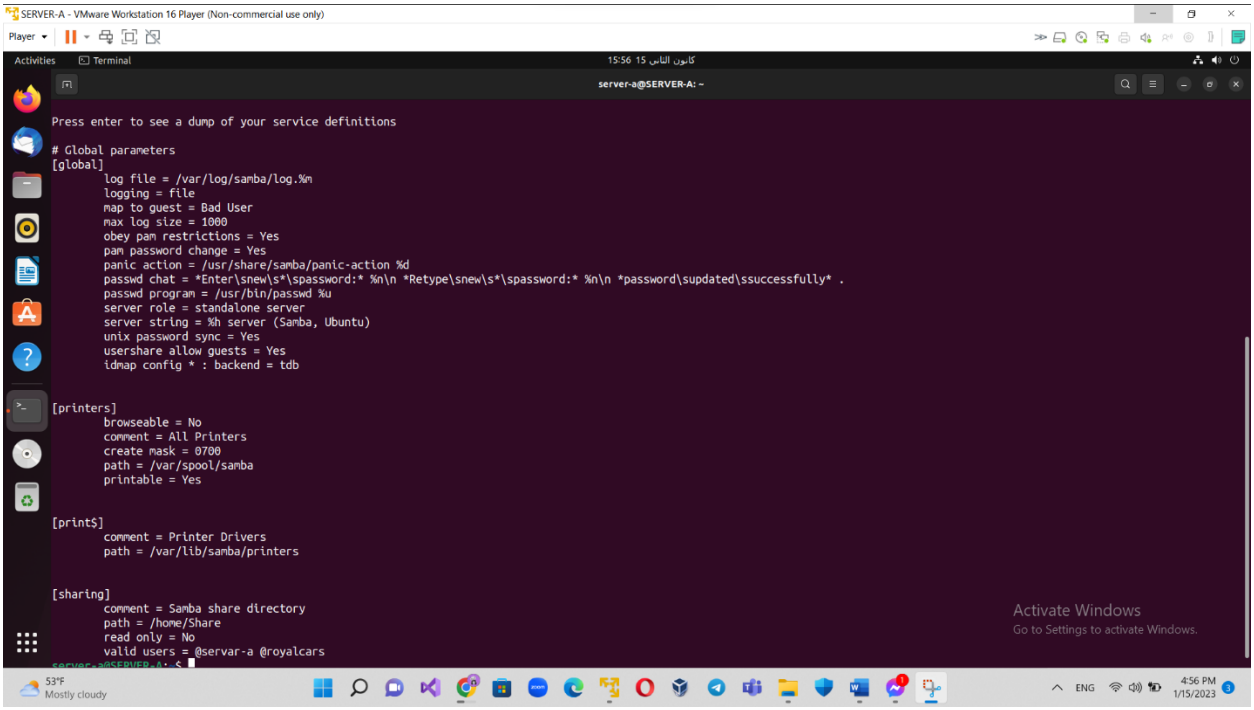


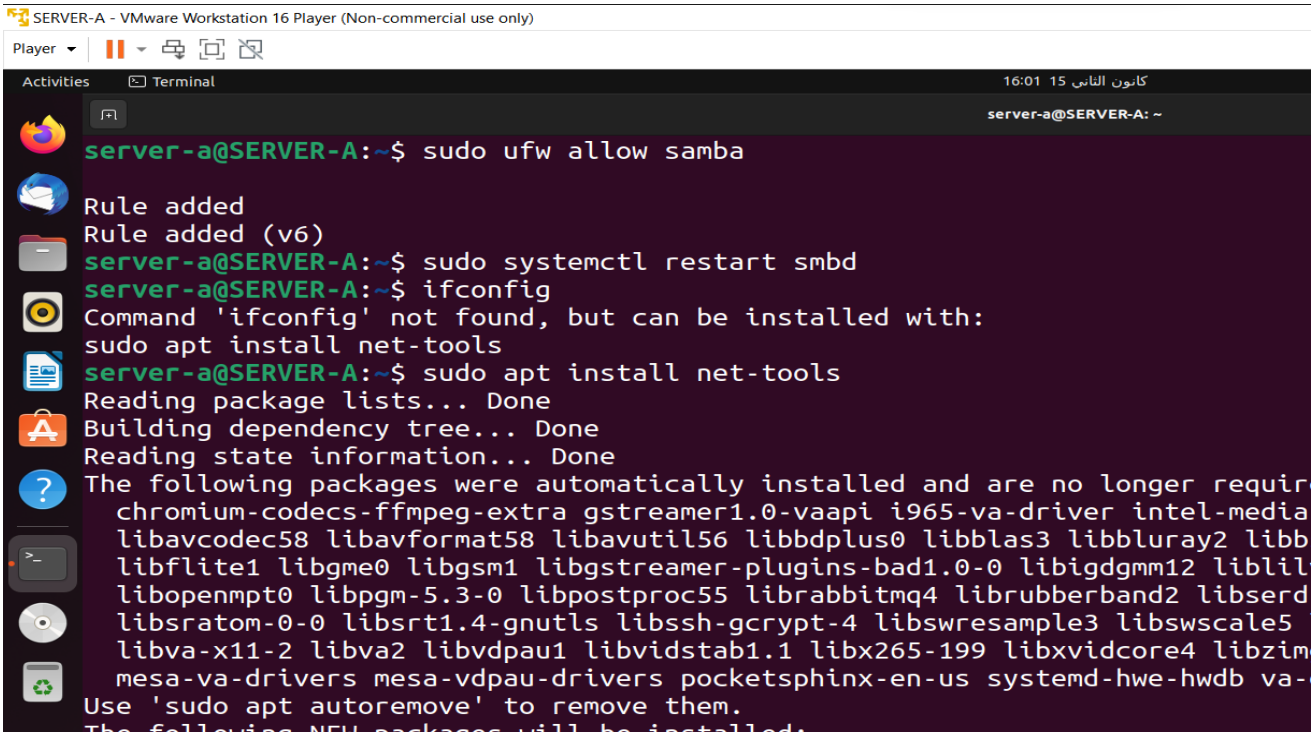

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
server-a@SERVER-A:~$ samba -V
Version 4.15.9-Ubuntu
server-a@SERVER-A:~$ systemctl status smbd
smbd.service - Samba SMB Daemon
Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
Active: active (running) since Sun 2023-01-15 15:10:23 EET; 28min ago
Docs: man:smbd(8)
man:samba(7)
man:smb.conf(5)
Process: 4410 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
Main PID: 4421 (smbd)
Status: "smbd: ready to serve connections..."
Tasks: 4 (limit: 4584)
Memory: 10.5M
CPU: 324ms
CGroup: /system.slice/smbd.service
├─4421 /usr/sbin/smbd --foreground --no-process-group
├─4424 /usr/sbin/smbd --foreground --no-process-group
├─4425 /usr/sbin/smbd --foreground --no-process-group
└─4427 /usr/lib/x86_64-linux-gnu/samba/samba-bgqd --ready-signal-fd=45 --parent-watch-fd=11 --debuglevel=0 -F
15:10:23 15 كانون الثاني SERVER-A systemd[1]: Starting Samba SMB Daemon...
15:10:23 15 كانون الثاني SERVER-A update-apparmor-samba-profile[4414]: grep: /etc/apparmor.d/samba/smbd-shares: No such file or directory
15:10:23 15 كانون الثاني SERVER-A update-apparmor-samba-profile[4418]: diff: /etc/apparmor.d/samba/smbd-shares: No such file or directory
15:10:23 15 كانون الثاني SERVER-A systemd[1]: Started Samba SMB Daemon.
server-a@SERVER-A:~$ sudo mkdir -p /home/Share
server-a@SERVER-A:~$ ls /home
server-a Share
server-a@SERVER-A:~$ sudo nano /etc/samba/smb.conf
server-a@SERVER-A:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed
Activate Windows
Go to Settings to activate Windows.
53°F
Mostly cloudy
ENG
4:43 PM
1/15/2023

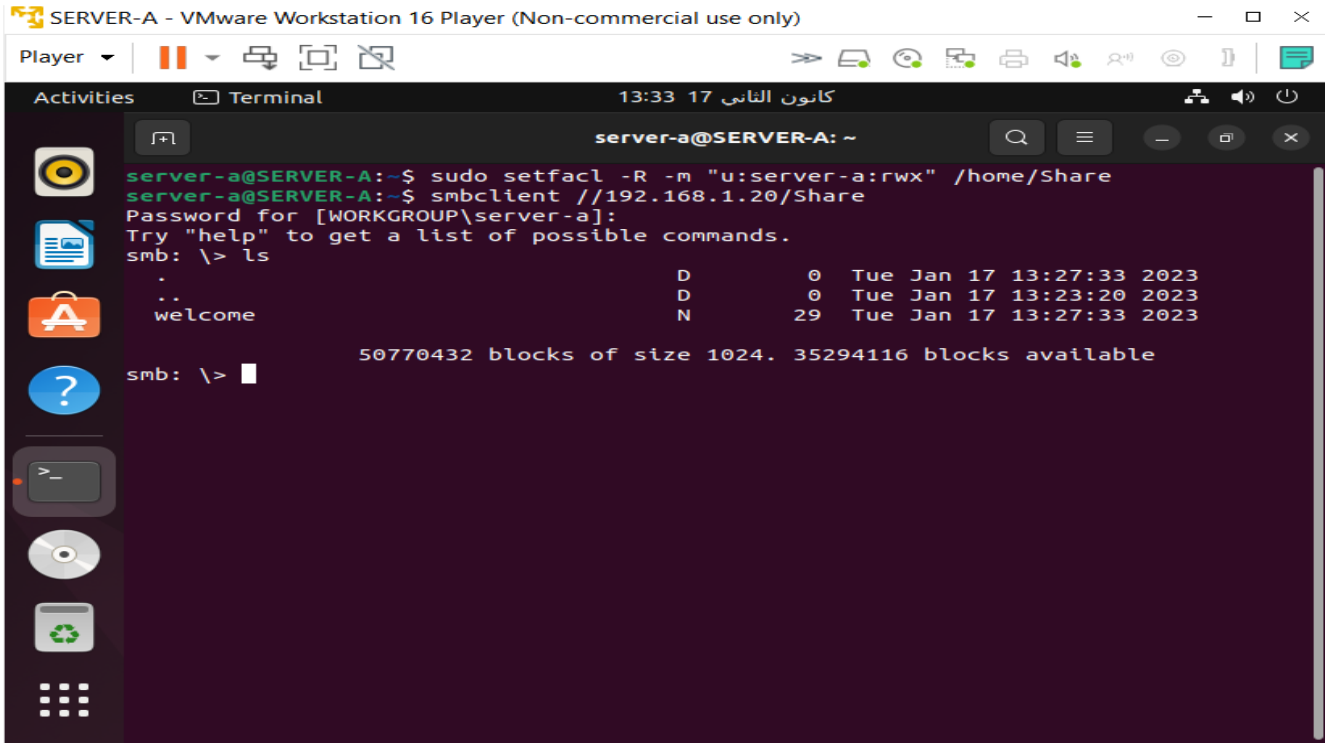

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
15:44 15 كانون الثاني
server-a@SERVER-A: ~
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
Global parameters
[global]
log file = /var/log/samba/log.%m
logging = file
map to guest = Bad User
max log size = 1000
obey pam restrictions = Yes
pam password change = Yes
panic action = /usr/share/samba/panic-action %d
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
passwd program = /usr/bin/passwd %u
server role = standalone server
server string = %h server (Samba, Ubuntu)
unix password sync = Yes
usershare allow guests = Yes
idmap config * : backend = tdb
[printers]
browseable = No
comment = All Printers
create mask = 0700
path = /var/spool/samba
printable = Yes
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
Activate Windows
Go to Settings to activate Windows.
53°F
Mostly cloudy
ENG
4:44 PM
1/15/2023


SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
15:55 15 كانون الثاني
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo adduser royalcars
Adding user `royalcars' ...
Adding new group `royalcars' (1001) ...
Adding new user `royalcars' (1001) with group `royalcars' ...
Creating home directory `/home/royalcars' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: password updated successfully
Changing the user information for royalcars
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
server-a@SERVER-A:~$ sudo setfacl -R -m "u:royalcarsr:rwx" /home/Share
setfacl: Option -m: Invalid argument near character 3
server-a@SERVER-A:~$ sudo setfacl -R -m "u:royalcars:rwx" /home/Share
server-a@SERVER-A:~$ sudo nano /etc/samba/smb.conf
server-a@SERVER-A:~$ testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions
Global parameters
[global]
Activate Windows
Go to Settings to activate Windows.
53°F
Mostly cloudy
ENG
4:55 PM
1/15/2023

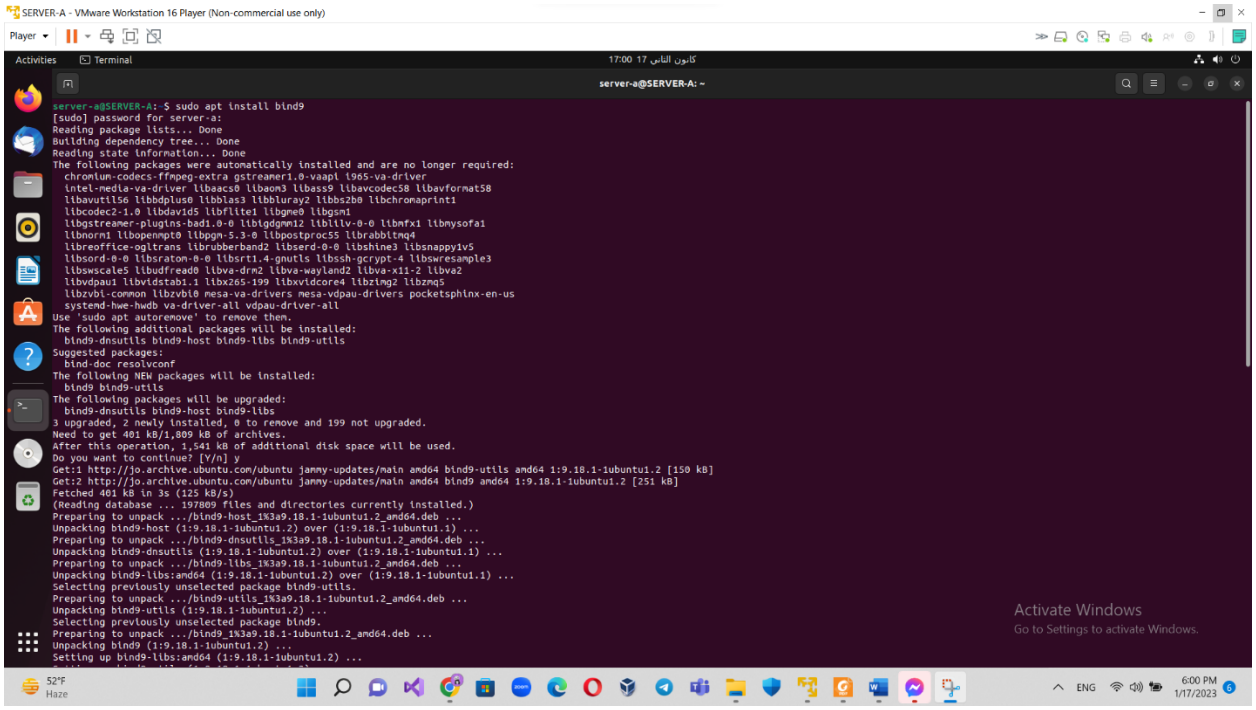

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: /home/Share
GNU nano 6.2 /etc/samba/smb.conf
Windows clients look for this share name as a source of downloadable
printer drivers
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
Uncomment to allow remote administration of Windows print drivers.
You may need to replace 'lpadmin' with the name of the group your
admin users are members of.
Please note that you also need to set appropriate Unix permissions
to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin
[Share]
comment = Samba share directory
path = /home/Share
read only = no
writable = yes
browseable = yes
guest ok = no
valid users = @server-a @royalcars
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy
Activate Windows
53°F
Mostly cloudy
ENG
5:20 PM
1/15/2023

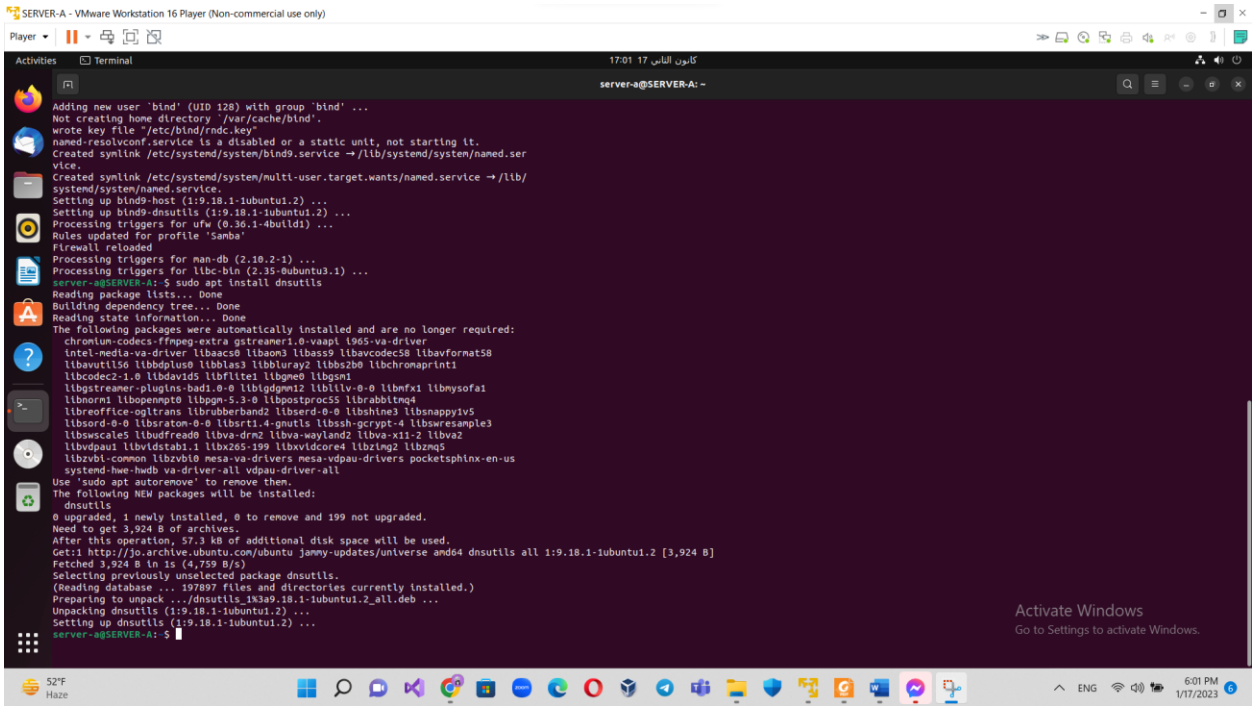

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
Press enter to see a dump of your service definitions
Global parameters
[global]
log file = /var/log/samba/log.%m
logging = file
map to guest = Bad User
max log size = 1000
obey pam restrictions = Yes
pam password change = Yes
panic action = /usr/share/samba/panic-action %d
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
passwd program = /usr/bin/passwd %u
server role = standalone server
server string = %h server (Samba, Ubuntu)
unix password sync = Yes
usershare allow guests = Yes
idmap config * : backend = tdb
[printers]
browseable = No
comment = All Printers
create mask = 0700
path = /var/spool/samba
printable = Yes
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
[sharing]
comment = Samba share directory
path = /home/Share
read only = No
valid users = @servar-a @royalcars
Activate Windows
Go to Settings to activate Windows.
53°F
Mostly cloudy
ENG
4:56 PM
1/15/2023

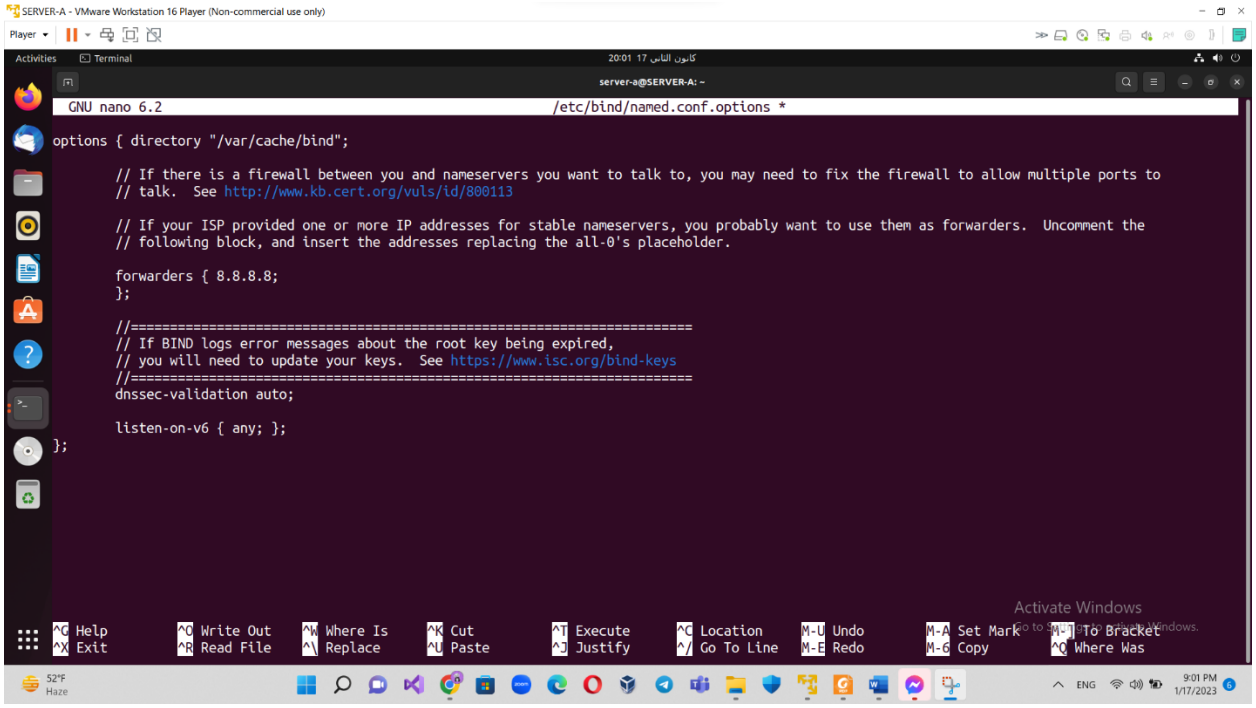

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 15 16:01
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo ufw allow samba
Rule added
Rule added (v6)
server-a@SERVER-A:~$ sudo systemctl restart smbd
server-a@SERVER-A:~$ ifconfig
Command 'ifconfig' not found, but can be installed with:
sudo apt install net-tools
server-a@SERVER-A:~$ sudo apt install net-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer requir
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media
libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2 libb
libflite1 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblil
libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2 libserd
libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5
libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199 libxvidcore4 libzim
mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us systemd-hwe-hwdb va-
Use 'sudo apt autoremove' to remove them.

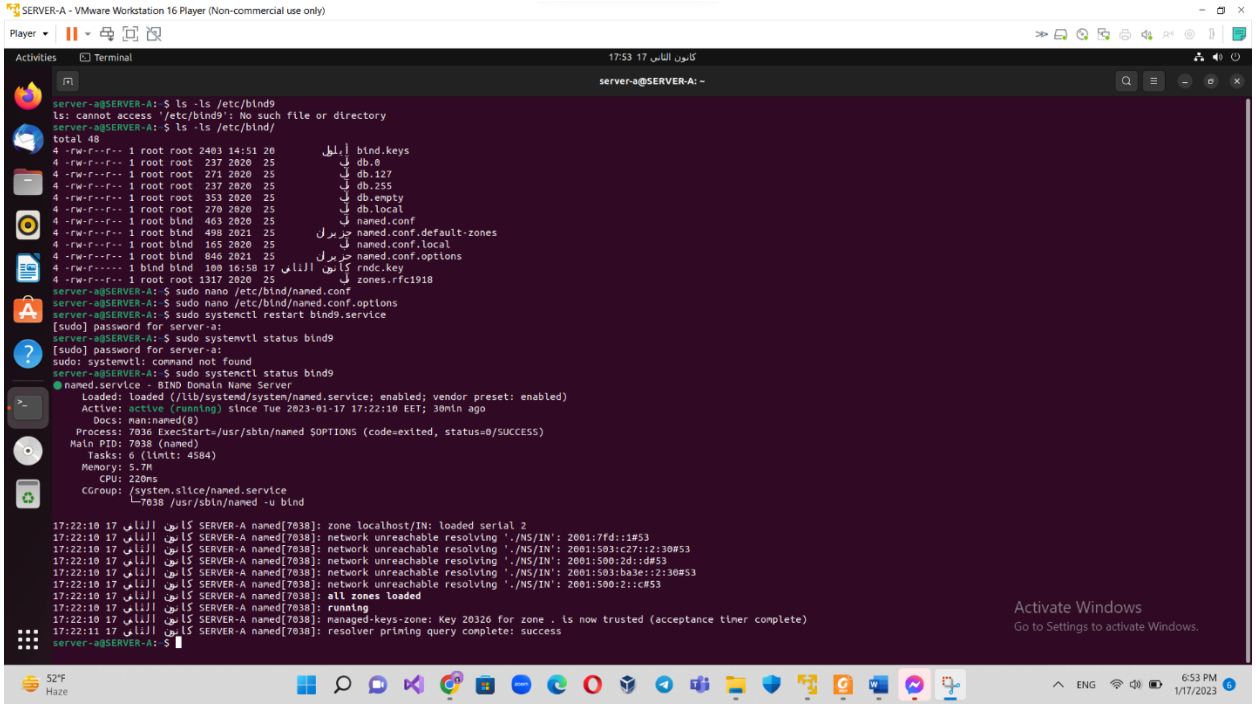

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 13:33
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo setfacl -R -m "u:server-a:rwx" /home/Share
server-a@SERVER-A:~$ smbclient //192.168.1.20/Share
Password for [WORKGROUP\server-a]:
Try "help" to get a list of possible commands.
smb: \> ls
. D 0 Tue Jan 17 13:27:33 2023
.. D 0 Tue Jan 17 13:23:20 2023
welcome N 29 Tue Jan 17 13:27:33 2023
50770432 blocks of size 1024. 35294116 blocks available
smb: \>

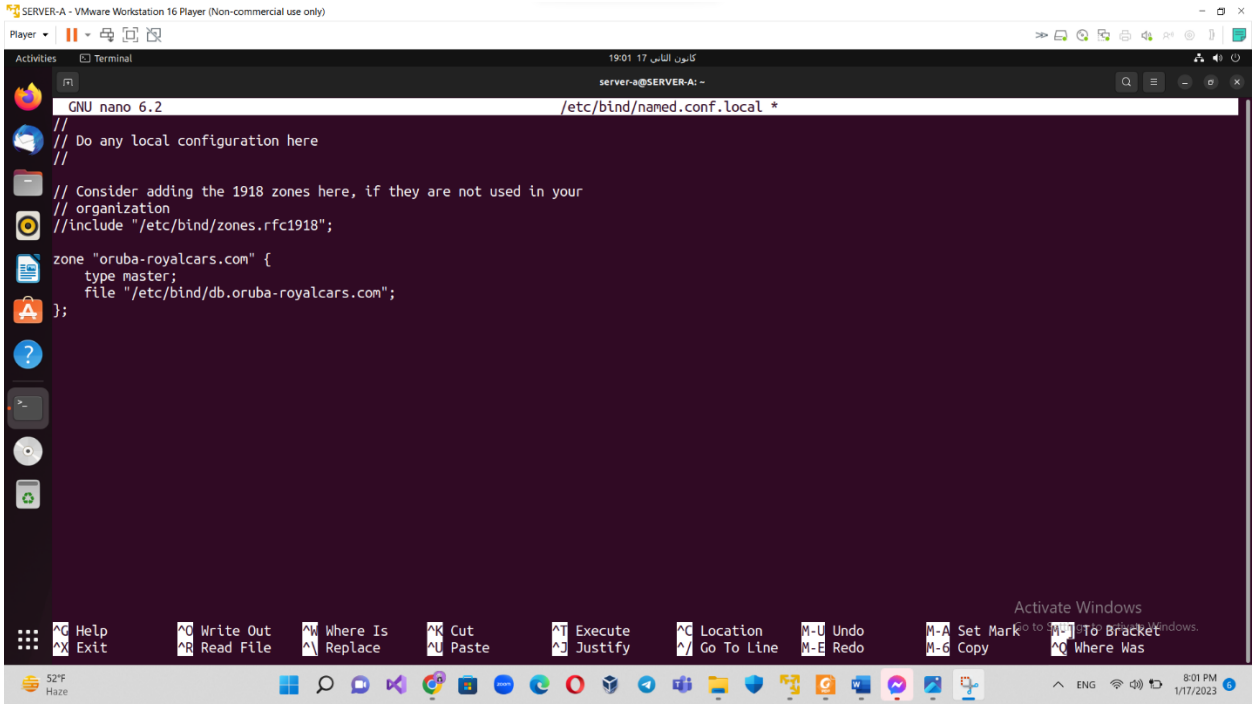
- **DNS Service[9]**

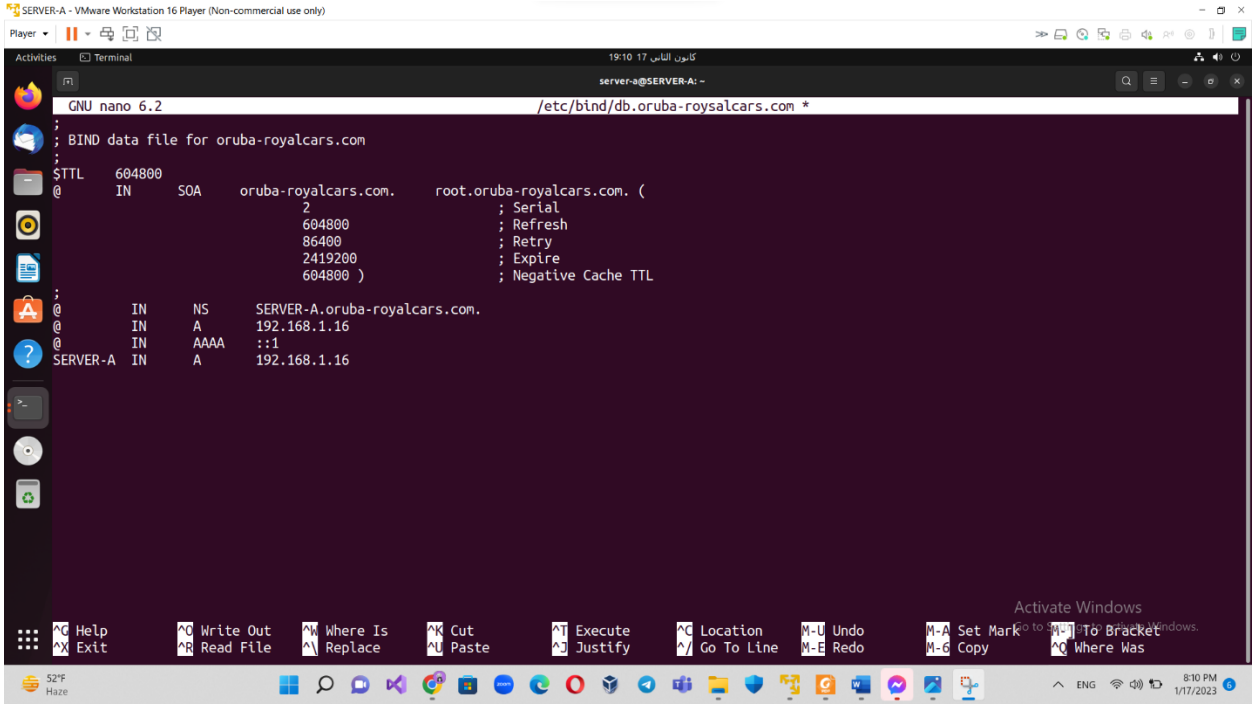


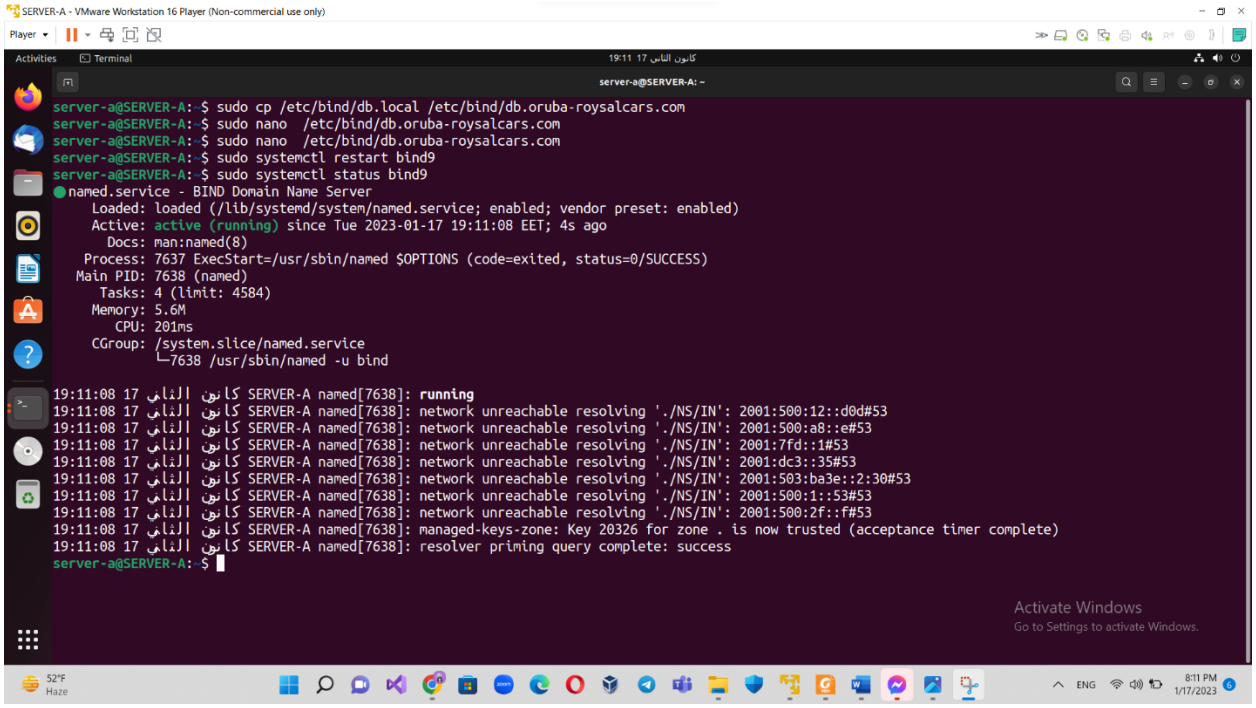


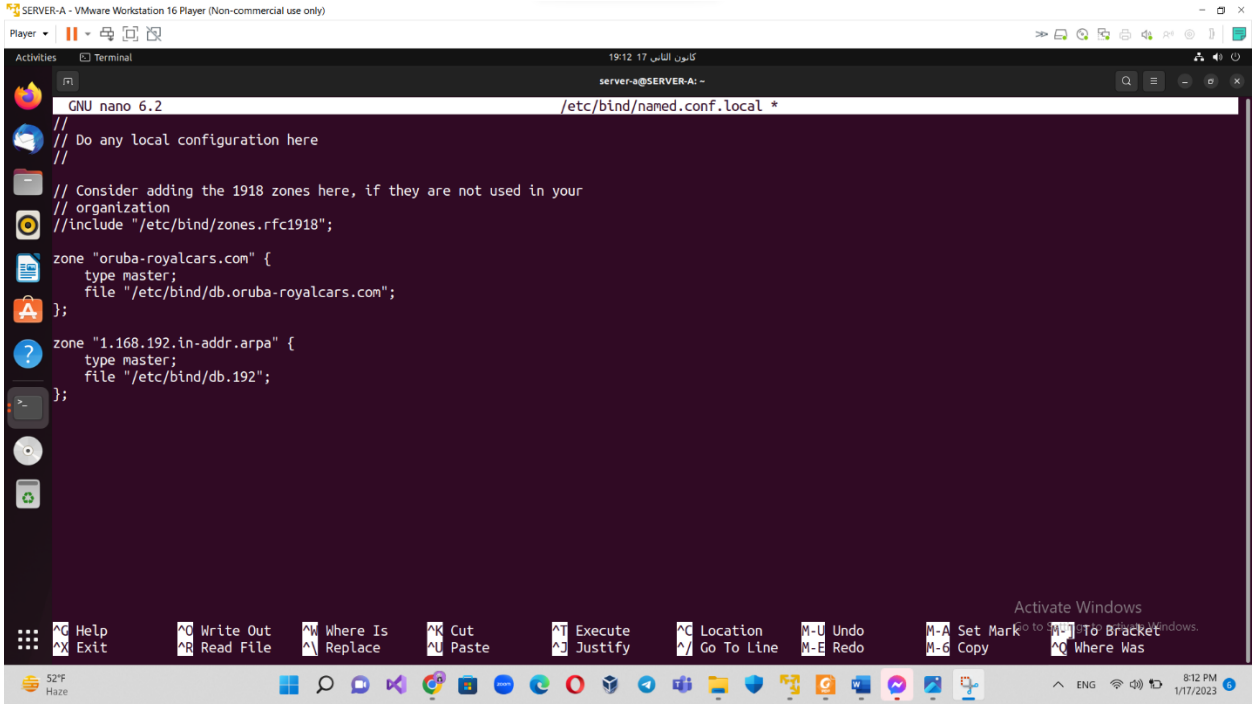

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
GNU nano 6.2 /etc/bind/named.conf.options *
options { directory "/var/cache/bind";
// If there is a firewall between you and nameservers you want to talk to, you may need to fix the firewall to allow multiple ports to
// talk. See http://www.kb.cert.org/vuls/id/800113
// If your ISP provided one or more IP addresses for stable nameservers, you probably want to use them as forwarders. Uncomment the
// following block, and insert the addresses replacing the all-0's placeholder.
forwarders { 8.8.8.8;
};
//==
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
//==
dnssec-validation auto;
listen-on-v6 { any; };
};
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was
Activate Windows
Go to Settings to activate Windows.
52°F Haze
ENG 9:01 PM 1/17/2023

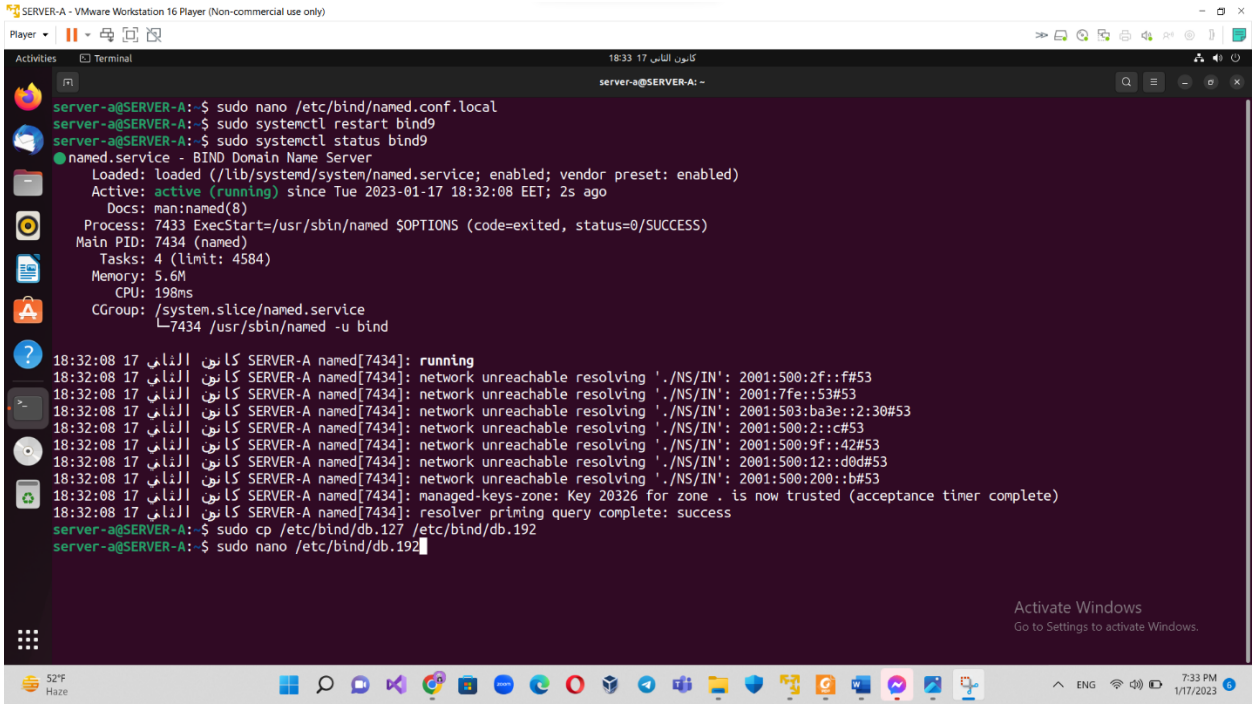

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
server-a@SERVER-A:~$ ls -ls /etc/blnd9
ls: cannot access '/etc/bind9': No such file or directory
server-a@SERVER-A:~$ ls -ls /etc/bind/
total 48
4 -rw-r--r-- 1 root root 2403 14:51 20 bind.keys
4 -rw-r--r-- 1 root root 237 2020 25 db.0
4 -rw-r--r-- 1 root root 271 2020 25 db.127
4 -rw-r--r-- 1 root root 237 2020 25 db.255
4 -rw-r--r-- 1 root root 353 2020 25 db.empty
4 -rw-r--r-- 1 root root 270 2020 25 db.local
4 -rw-r--r-- 1 root bind 463 2020 25 named.conf
4 -rw-r--r-- 1 root bind 498 2021 25 named.conf.default-zones
4 -rw-r--r-- 1 root bind 165 2020 25 named.conf.local
4 -rw-r--r-- 1 root bind 846 2021 25 named.conf.options
4 -rw-r----- 1 bind bind 109 16:58 17 rndc.key
4 -rw-r--r-- 1 root root 1317 2020 25 zones.rfc1918
server-a@SERVER-A:~$ sudo nano /etc/bind/named.conf
server-a@SERVER-A:~$ sudo nano /etc/bind/named.conf.options
server-a@SERVER-A:~$ sudo systemctl restart bind9.service
[sudo] password for server-a:
server-a@SERVER-A:~$ sudo systemvtl status bind9
[sudo] password for server-a:
sudo: systemvtl: command not found
server-a@SERVER-A:~$ sudo systemctl status bind9
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 17:22:10 EET; 30min ago
Docs: man:named(8)
Process: 7036 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7038 (named)
Tasks: 6 (limit: 4584)
Memory: 5.7M
CPU: 220ms
CGroup: /system.slice/named.service
└─7038 /usr/sbin/named -u bind
17:22:10 17 كانون الثاني SERVER-A named[7038]: zone localhost/IN: loaded serial 2
17:22:10 17 كانون الثاني SERVER-A named[7038]: network unreachable resolving './NS/IN': 2001:7fd::1#53
17:22:10 17 كانون الثاني SERVER-A named[7038]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
17:22:10 17 كانون الثاني SERVER-A named[7038]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
17:22:10 17 كانون الثاني SERVER-A named[7038]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
17:22:10 17 كانون الثاني SERVER-A named[7038]: network unreachable resolving './NS/IN': 2001:500:2::c#53
17:22:10 17 كانون الثاني SERVER-A named[7038]: all zones loaded
17:22:10 17 كانون الثاني SERVER-A named[7038]: running
17:22:10 17 كانون الثاني SERVER-A named[7038]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
17:22:11 17 كانون الثاني SERVER-A named[7038]: resolver priming query complete: success
server-a@SERVER-A:~$
Activate Windows
Go to Settings to activate Windows.
52°F Haze
ENG 6:53 PM 1/17/2023

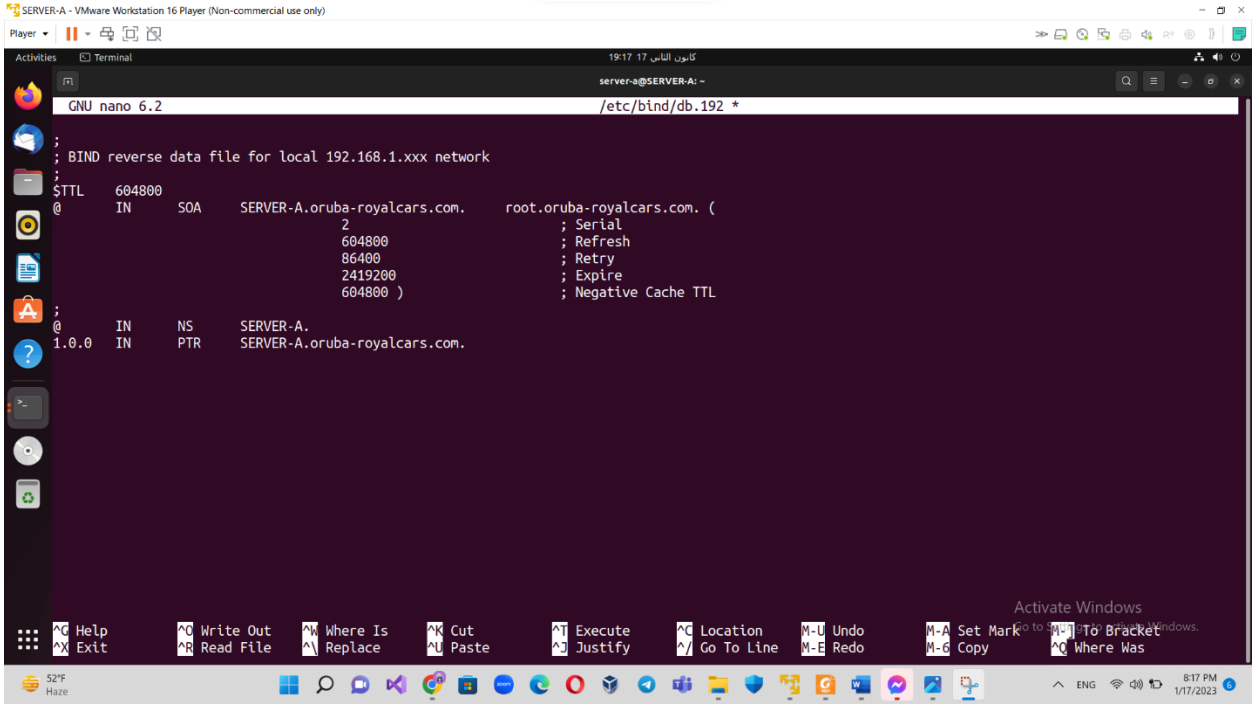

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:01
server-a@SERVER-A: ~
GNU nano 6.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "oruba-royalcars.com" {
type master;
file "/etc/bind/db.oruba-royalcars.com";
};
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-G Copy ^Q Where Was
Activate Windows
52°F Haze
ENG 8:01 PM 1/17/2023

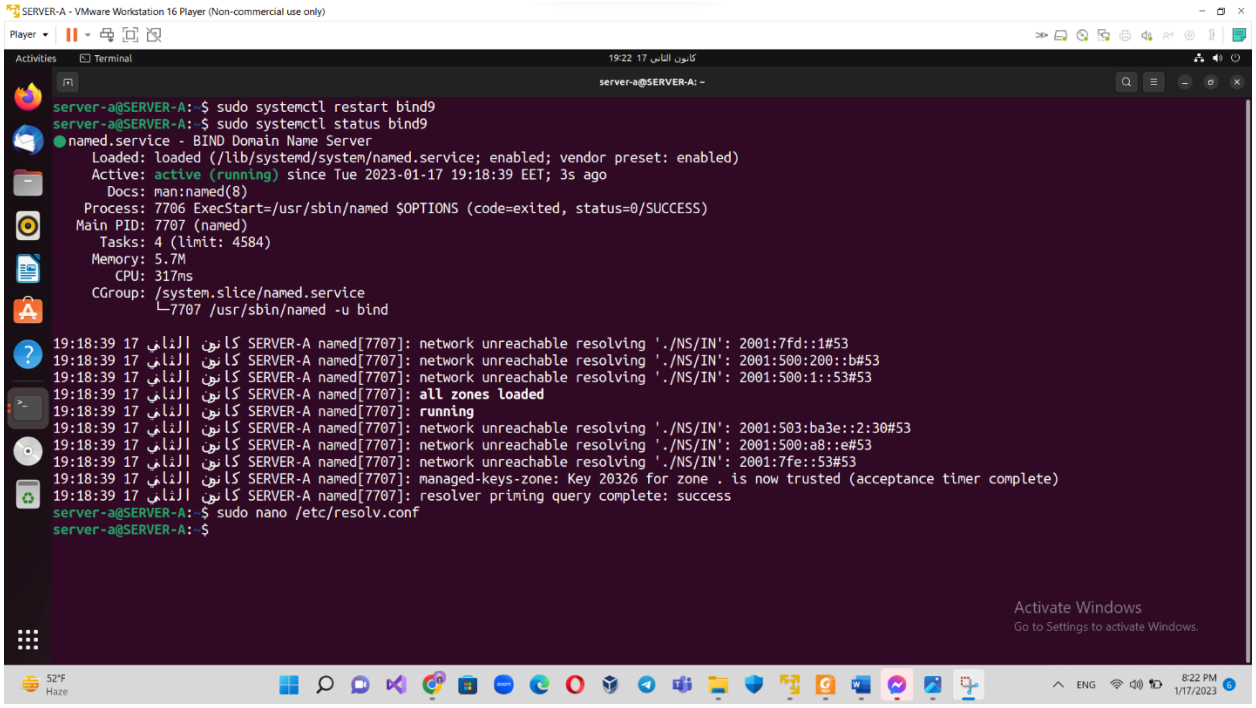

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:10
server-a@SERVER-A: ~
GNU nano 6.2 /etc/bind/db.oruba-roysalcars.com *
;
; BIND data file for oruba-royalcars.com
;
$TTL 604800
@ IN SOA oruba-royalcars.com. root.oruba-royalcars.com. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
@ IN NS SERVER-A.oruba-royalcars.com.
@ IN A 192.168.1.16
@ IN AAAA ::1
SERVER-A IN A 192.168.1.16
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-G Copy ^Q Where Was
Activate Windows
52°F Haze
ENG 8:10 PM 1/17/2023

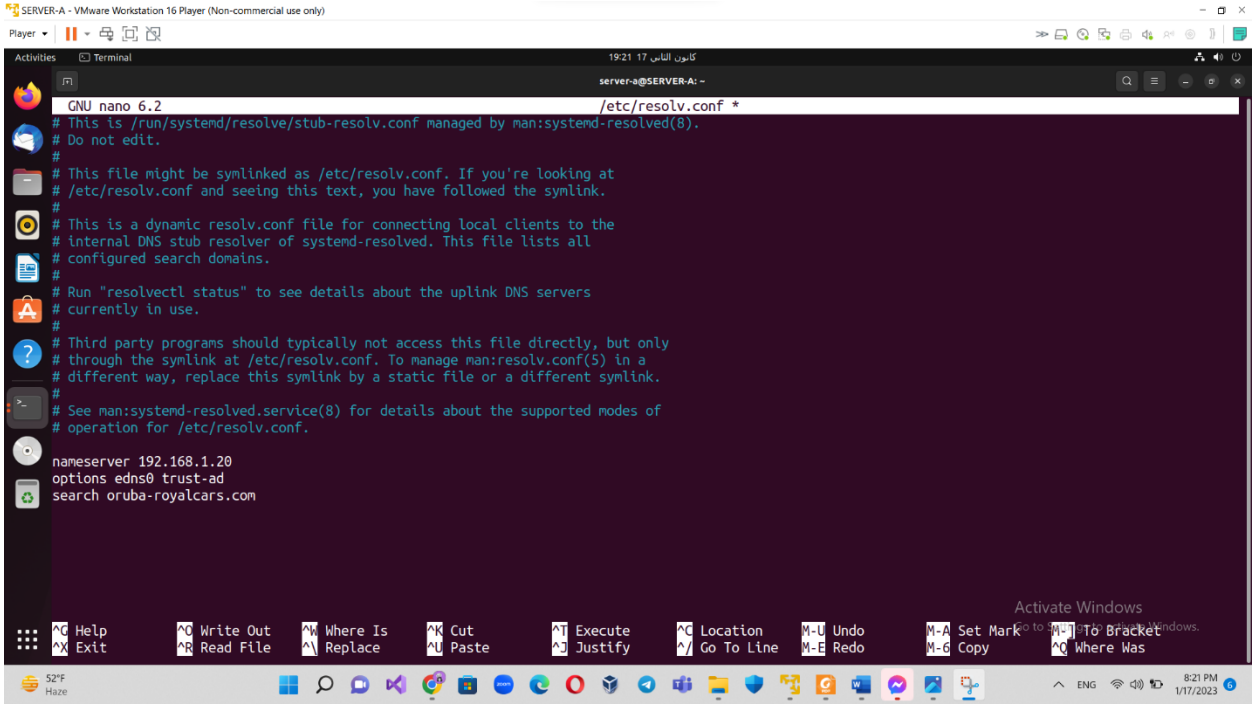

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo cp /etc/bind/db.local /etc/bind/db.oruba-roysalcars.com
server-a@SERVER-A:~$ sudo nano /etc/bind/db.oruba-roysalcars.com
server-a@SERVER-A:~$ sudo nano /etc/bind/db.oruba-roysalcars.com
server-a@SERVER-A:~$ sudo systemctl restart bind9
server-a@SERVER-A:~$ sudo systemctl status bind9
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 19:11:08 EET; 4s ago
Docs: man:named(8)
Process: 7637 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7638 (named)
Tasks: 4 (limit: 4584)
Memory: 5.6M
CPU: 201ms
CGroup: /system.slice/named.service
└7638 /usr/sbin/named -u bind
19:11:08 17 كانون الثاني SERVER-A named[7638]: running
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:7fd::1#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:dc3::35#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:500:1::53#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
19:11:08 17 كانون الثاني SERVER-A named[7638]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:11:08 17 كانون الثاني SERVER-A named[7638]: resolver priming query complete: success
server-a@SERVER-A:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
8:11 PM
1/17/2023

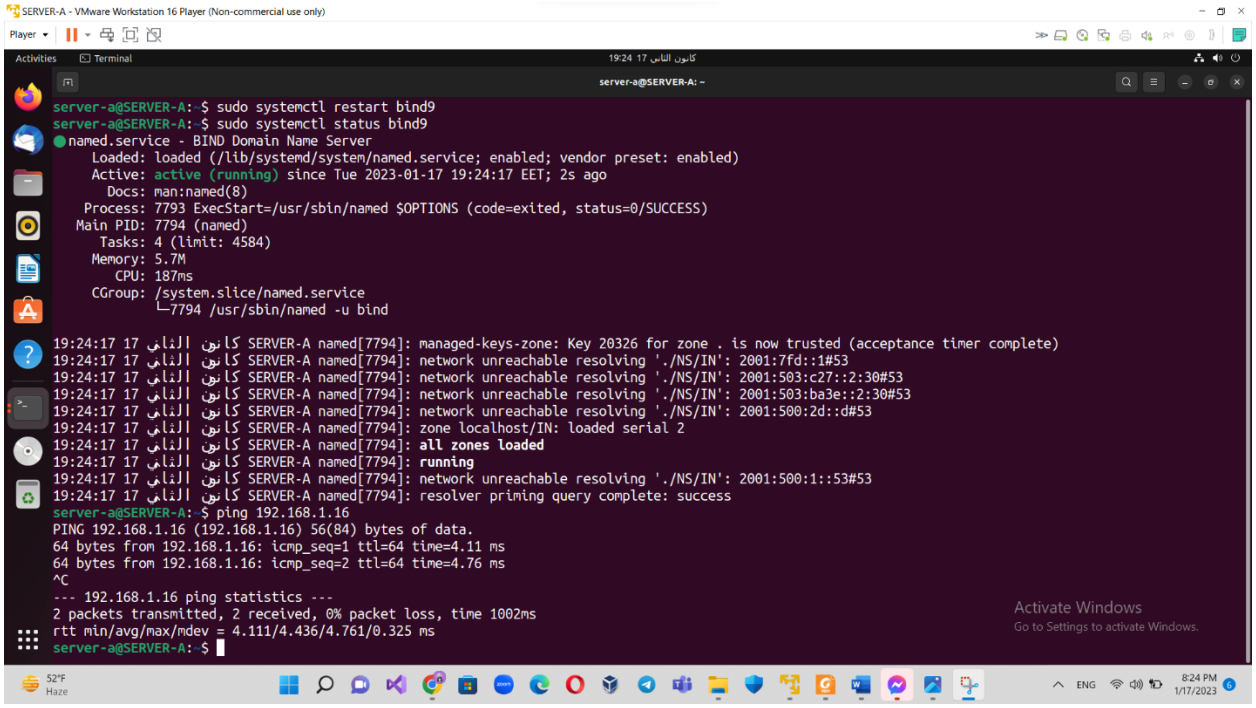

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-a@SERVER-A: ~
GNU nano 6.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "oruba-royalcars.com" {
type master;
file "/etc/bind/db.oruba-roysalcars.com";
};
zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.192";
};
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was
Activate Windows
52°F
Haze
ENG
8:12 PM
1/17/2023

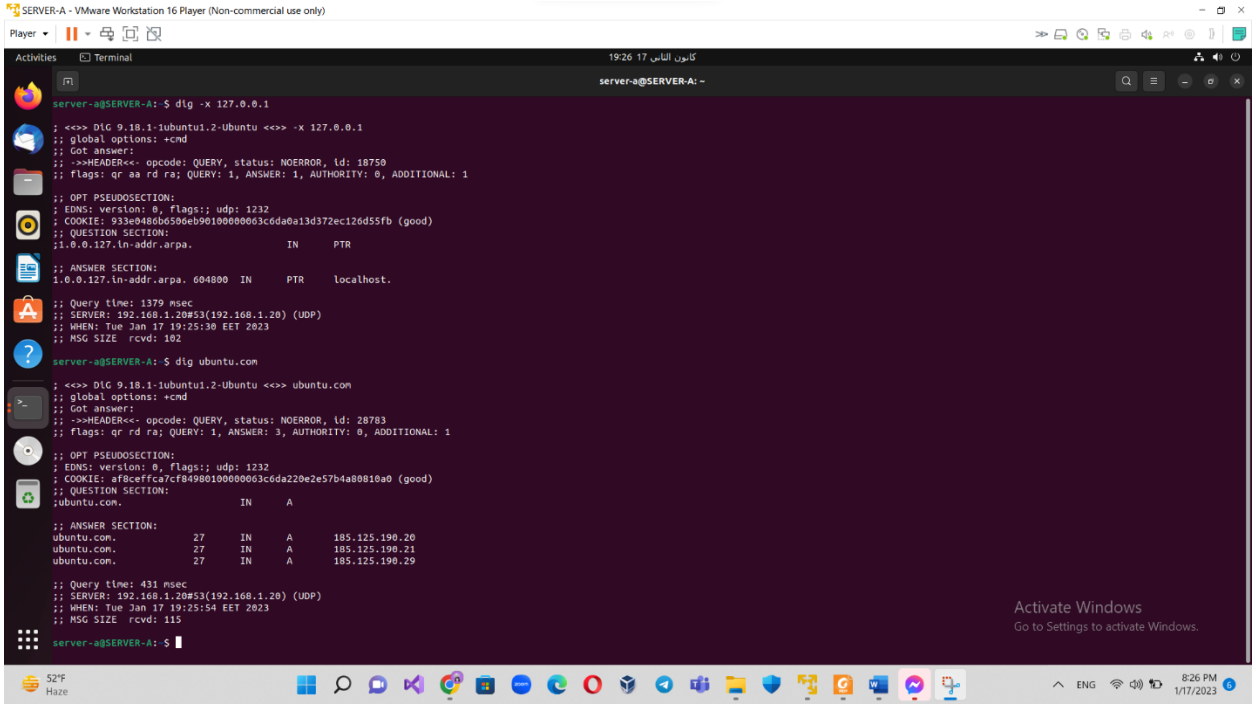

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 18:33
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo nano /etc/bind/named.conf.local
server-a@SERVER-A:~$ sudo systemctl restart bind9
server-a@SERVER-A:~$ sudo systemctl status bind9
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 18:32:08 EET; 2s ago
Docs: man:named(8)
Process: 7433 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7434 (named)
Tasks: 4 (limit: 4584)
Memory: 5.6M
CPU: 198ms
CGroup: /system.slice/named.service
└7434 /usr/sbin/named -u bind
18:32:08 17 كانون الثاني SERVER-A named[7434]: running
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:7fe::53#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:500:2::c#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: network unreachable resolving './NS/IN': 2001:500:200::b#53
18:32:08 17 كانون الثاني SERVER-A named[7434]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
18:32:08 17 كانون الثاني SERVER-A named[7434]: resolver priming query complete: success
server-a@SERVER-A:~$ sudo cp /etc/bind/db.127 /etc/bind/db.192
server-a@SERVER-A:~$ sudo nano /etc/bind/db.192
Activate Windows
Go to Settings to activate Windows.
52°F Haze
ENG 7:33 PM 1/17/2023


SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:17
server-a@SERVER-A: ~
GNU nano 6.2 /etc/bind/db.192 *
;
; BIND reverse data file for local 192.168.1.xxx network
;
$TTL 604800
@ IN SOA SERVER-A.oruba-royalcars.com. root.oruba-royalcars.com. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
@ IN NS SERVER-A.
1.0.0 IN PTR SERVER-A.oruba-royalcars.com.
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was
Activate Windows
52°F Haze
ENG 8:17 PM 1/17/2023

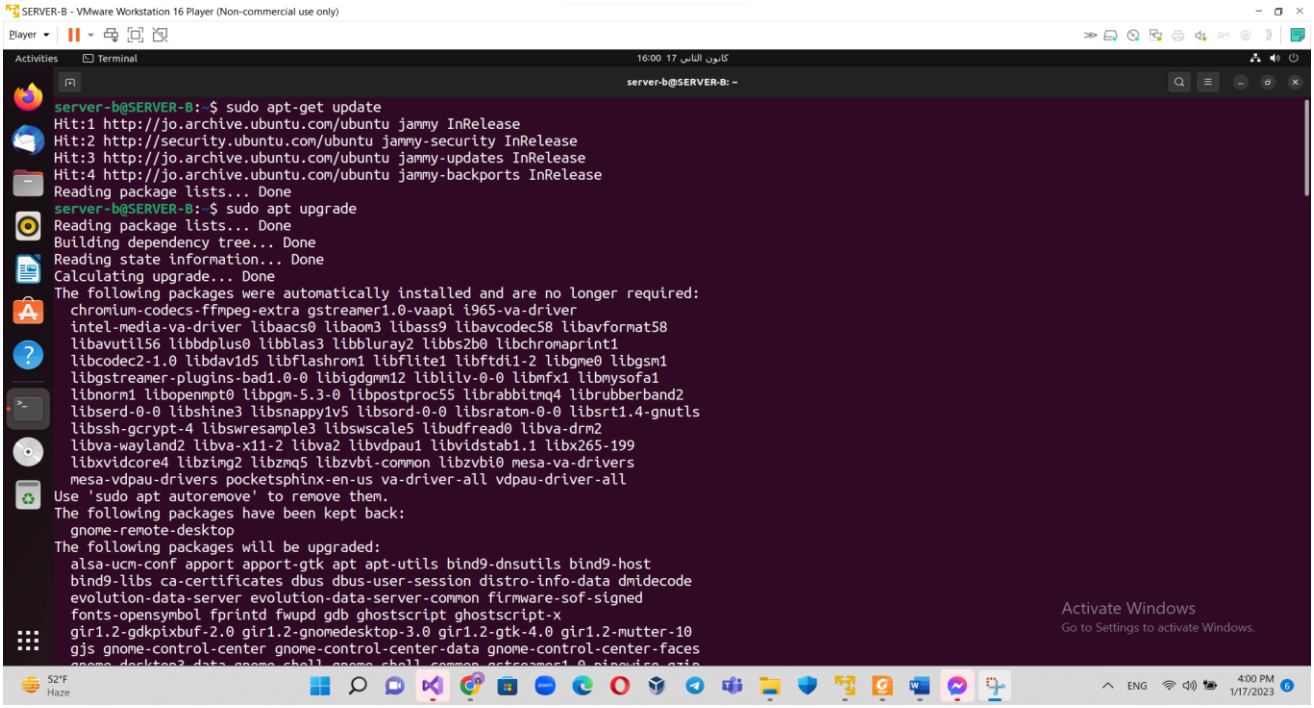

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:22
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo systemctl restart bind9
server-a@SERVER-A:~$ sudo systemctl status bind9
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 19:18:39 EET; 3s ago
Docs: man:named(8)
Process: 7706 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7707 (named)
Tasks: 4 (limit: 4584)
Memory: 5.7M
CPU: 317ms
CGroup: /system.slice/named.service
└─7707 /usr/sbin/named -u bind
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:7fd::1#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:500:200::b#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:500:1::53#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: all zones loaded
19:18:39 17 كانون الثاني SERVER-A named[7707]: running
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: network unreachable resolving './NS/IN': 2001:7fe::53#53
19:18:39 17 كانون الثاني SERVER-A named[7707]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:18:39 17 كانون الثاني SERVER-A named[7707]: resolver priming query complete: success
server-a@SERVER-A:~$ sudo nano /etc/resolv.conf
server-a@SERVER-A:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
8:22 PM
1/17/2023

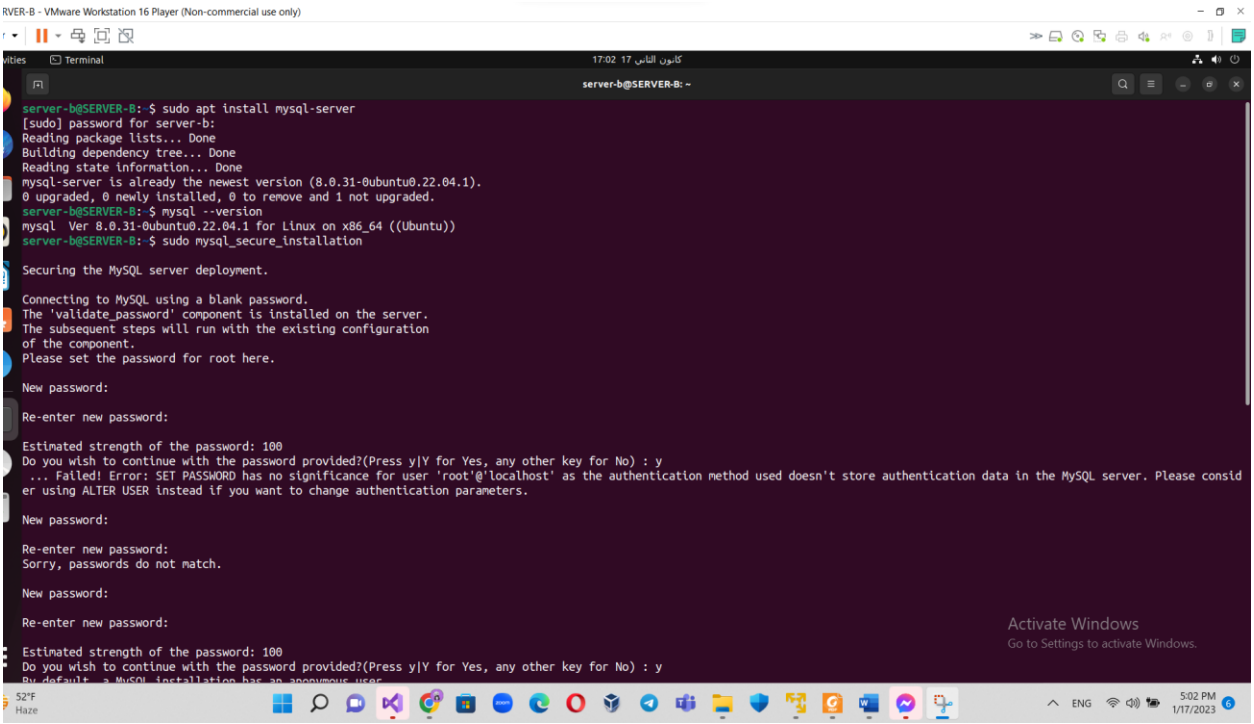

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:21
server-a@SERVER-A: ~
GNU nano 6.2 /etc/resolv.conf *
This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).
Do not edit.
#
This file might be symlinked as /etc/resolv.conf. If you're looking at
/etc/resolv.conf and seeing this text, you have followed the symlink.
#
This is a dynamic resolv.conf file for connecting local clients to the
internal DNS stub resolver of systemd-resolved. This file lists all
configured search domains.
#
Run "resolvectl status" to see details about the uplink DNS servers
currently in use.
#
Third party programs should typically not access this file directly, but only
through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
different way, replace this symlink by a static file or a different symlink.
#
See man:systemd-resolved.service(8) for details about the supported modes of
operation for /etc/resolv.conf.
nameserver 192.168.1.20
options edns0 trust-ad
search oruba-royalcars.com
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was
Activate Windows
52°F
Haze
ENG
8:21 PM
1/17/2023

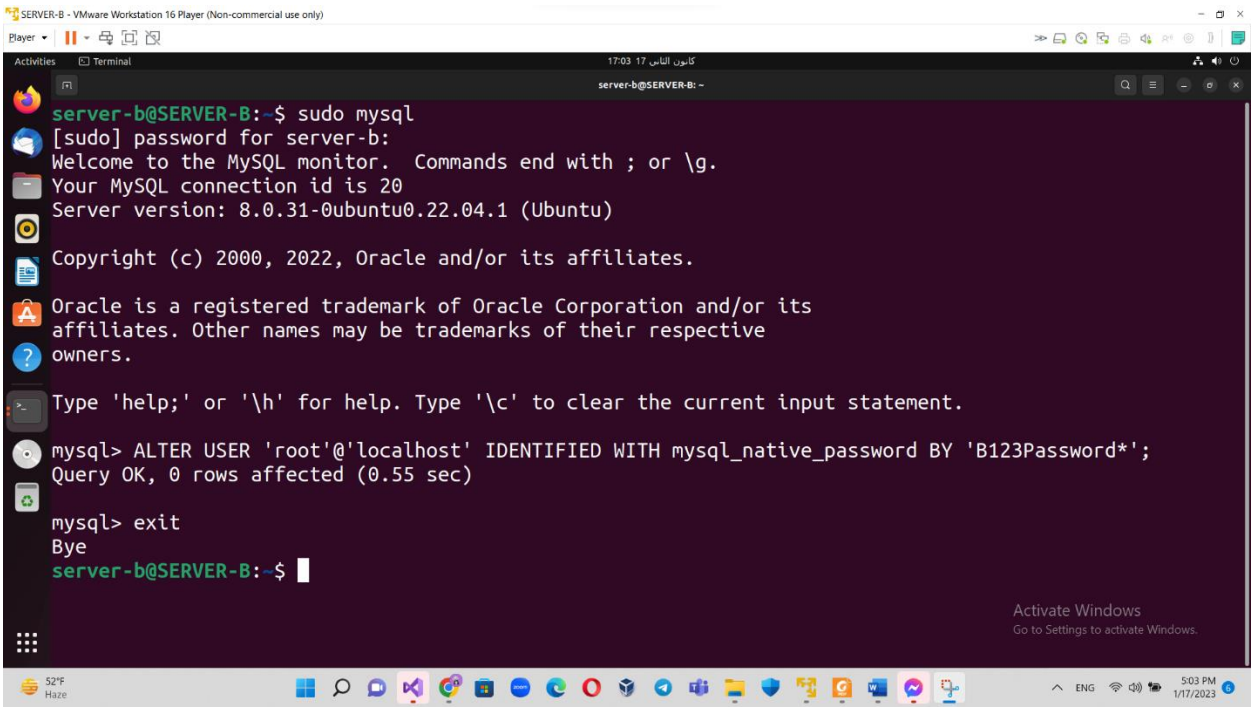

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:24
server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo systemctl restart bind9
server-a@SERVER-A:~$ sudo systemctl status bind9
named.service - BIND Domain Name Server
Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 19:24:17 EET; 2s ago
Docs: man:named(8)
Process: 7793 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
Main PID: 7794 (named)
Tasks: 4 (limit: 4584)
Memory: 5.7M
CPU: 187ms
CGroup: /system.slice/named.service
└─7794 /usr/sbin/named -u bind
19:24:17 17 كانون الثاني SERVER-A named[7794]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:24:17 17 كانون الثاني SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:7fd::1#53
19:24:17 17 كانون الثاني SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
19:24:17 17 كانون الثاني SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
19:24:17 17 كانون الثاني SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
19:24:17 17 كانون الثاني SERVER-A named[7794]: zone localhost/IN: loaded serial 2
19:24:17 17 كانون الثاني SERVER-A named[7794]: all zones loaded
19:24:17 17 كانون الثاني SERVER-A named[7794]: running
19:24:17 17 كانون الثاني SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:500:1::53#53
19:24:17 17 كانون الثاني SERVER-A named[7794]: resolver priming query complete: success
server-a@SERVER-A:~$ ping 192.168.1.16
PING 192.168.1.16 (192.168.1.16) 56(84) bytes of data.
64 bytes from 192.168.1.16: icmp_seq=1 ttl=64 time=4.11 ms
64 bytes from 192.168.1.16: icmp_seq=2 ttl=64 time=4.76 ms
^C
--- 192.168.1.16 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.111/4.436/4.761/0.325 ms
server-a@SERVER-A:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
8:24 PM
1/17/2023

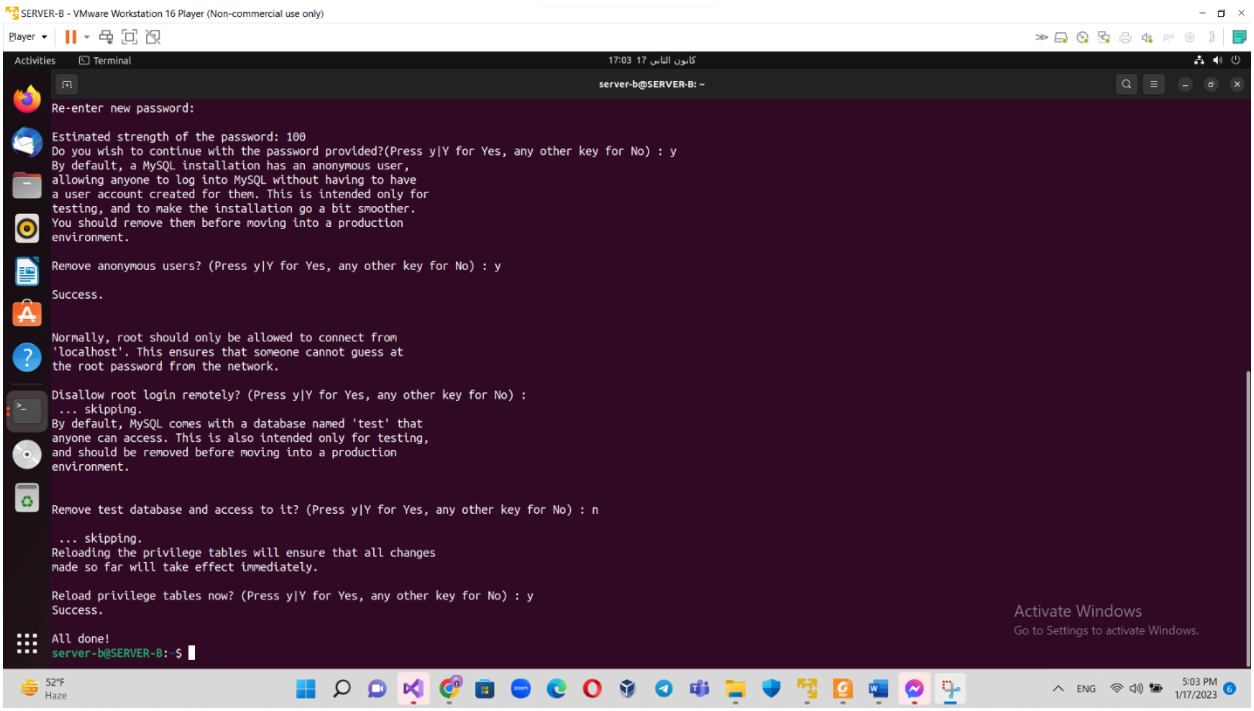

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
كانون الثاني 17 19:26
server-a@SERVER-A: ~
server-a@SERVER-A:~$ dig -x 127.0.0.1
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> -x 127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18750
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 933e0486b6506eb90100000063c6da0a13d372ec126d55fb (good)
;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa. IN PTR
;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 604800 IN PTR localhost.
;; Query time: 1379 msec
;; SERVER: 192.168.1.20#53(192.168.1.20) (UDP)
;; WHEN: Tue Jan 17 19:25:30 EET 2023
;; MSG SIZE rcvd: 102
server-a@SERVER-A:~$ dig ubuntu.com
; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> ubuntu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28783
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: af8ceffca7cf84980100000063c6da220e2e57b4a80810a0 (good)
;; QUESTION SECTION:
;ubuntu.com. IN A
;; ANSWER SECTION:
ubuntu.com. 27 IN A 185.125.190.20
ubuntu.com. 27 IN A 185.125.190.21
ubuntu.com. 27 IN A 185.125.190.29
;; Query time: 431 msec
;; SERVER: 192.168.1.20#53(192.168.1.20) (UDP)
;; WHEN: Tue Jan 17 19:25:54 EET 2023
;; MSG SIZE rcvd: 115
server-a@SERVER-A:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
8:26 PM
1/17/2023

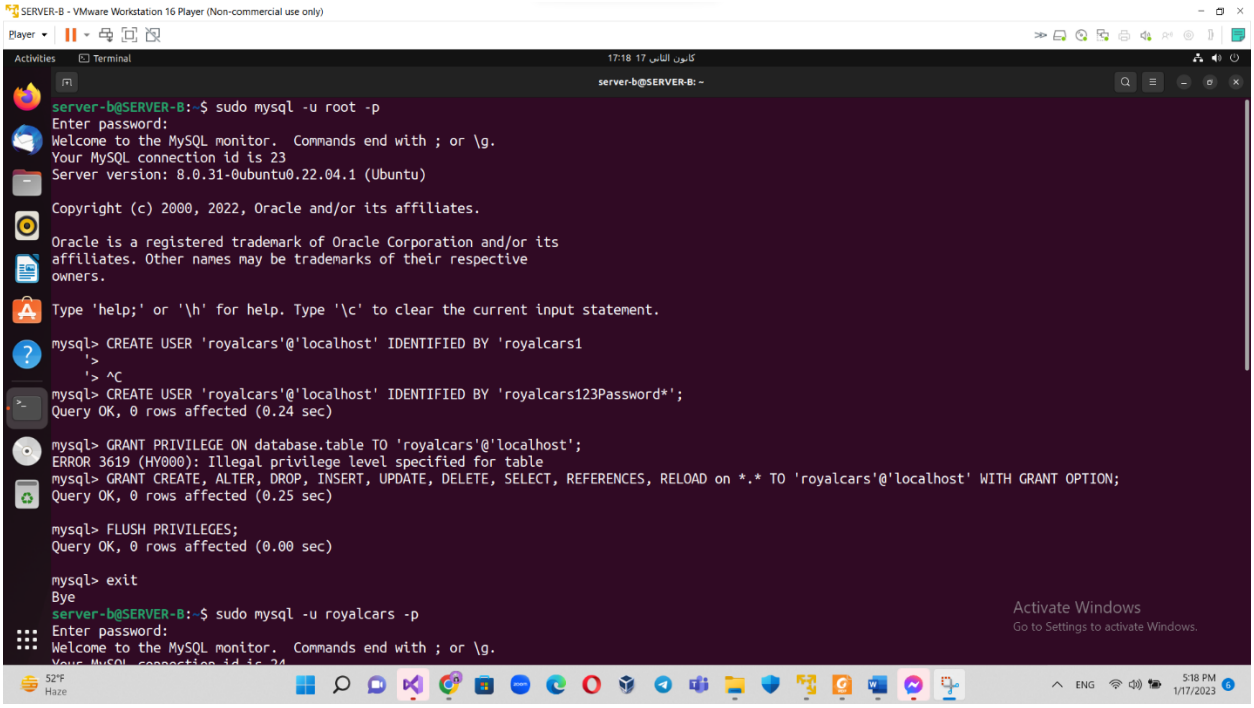
- **MYSQL Service [10][11]**

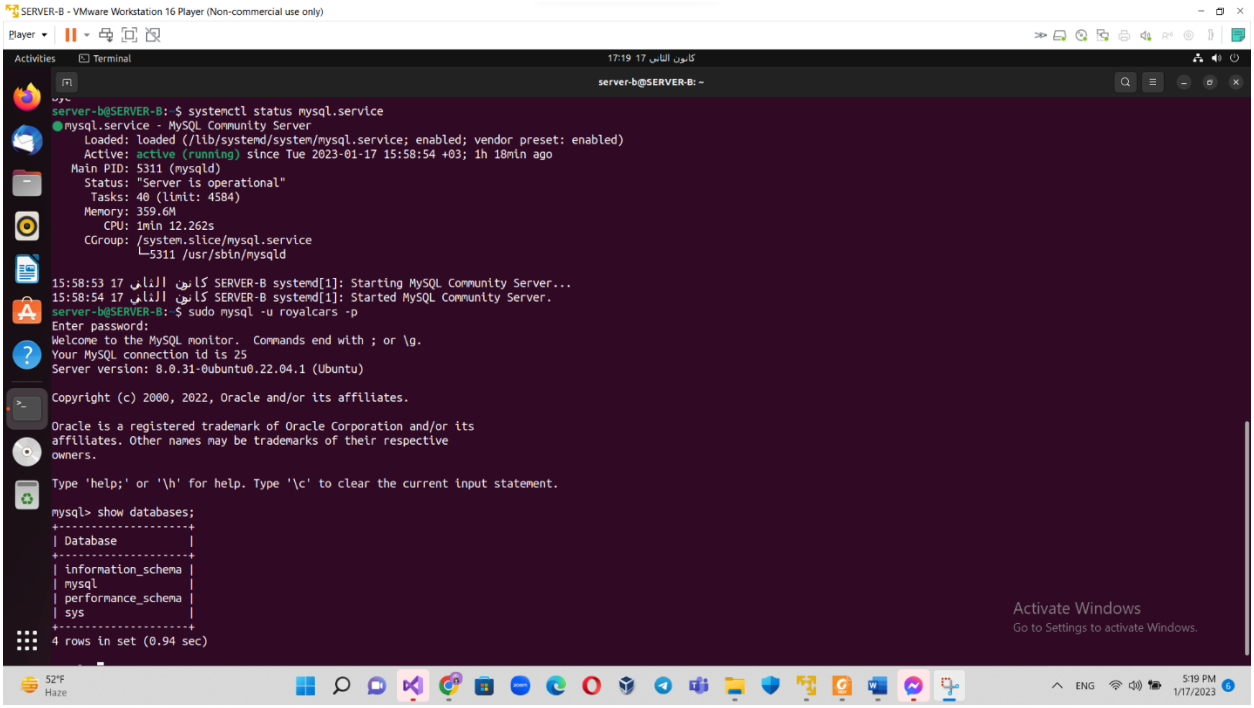




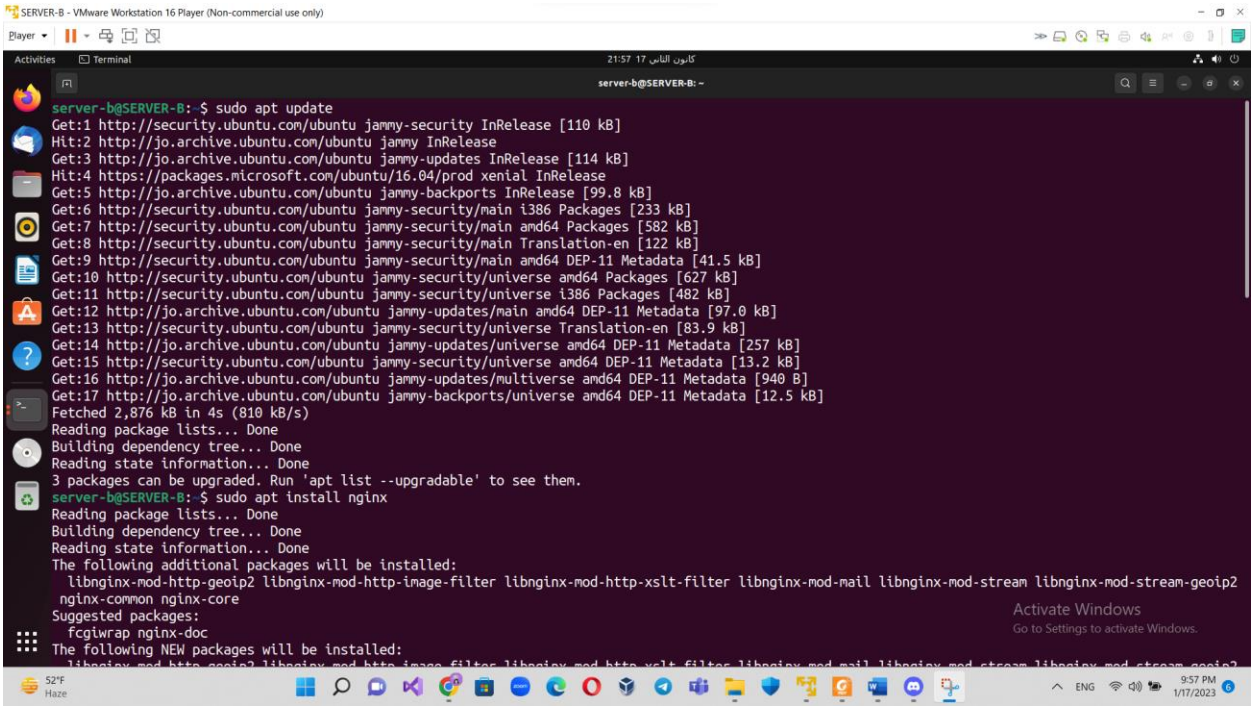

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
17:03 17 كانون الثاني
server-b@SERVER-B: ~
server-b@SERVER-B:~$ sudo mysql
[sudo] password for server-b:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 8.0.31-0ubuntu0.22.04.1 (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> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'B123Password*';
Query OK, 0 rows affected (0.55 sec)
mysql> exit
Bye
server-b@SERVER-B:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
5:03 PM
1/17/2023

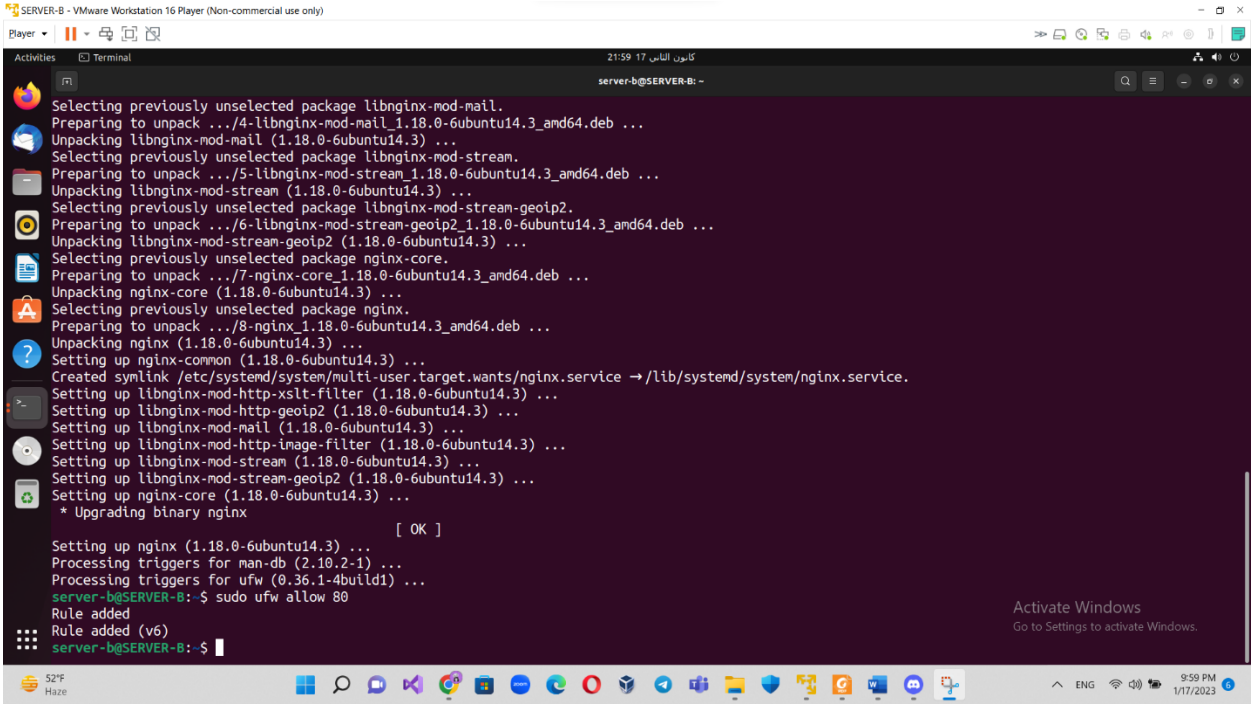

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
17:03 17 كانون الثاني
server-b@SERVER-B: ~
Re-enter new password:
Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.
Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.
Disallow root login remotely? (Press y|Y for Yes, any other key for No) :
... skipping.
By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.
Remove test database and access to it? (Press y|Y for Yes, any other key for No) : n
... skipping.
Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.
Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.
All done!
server-b@SERVER-B:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
5:03 PM
1/17/2023

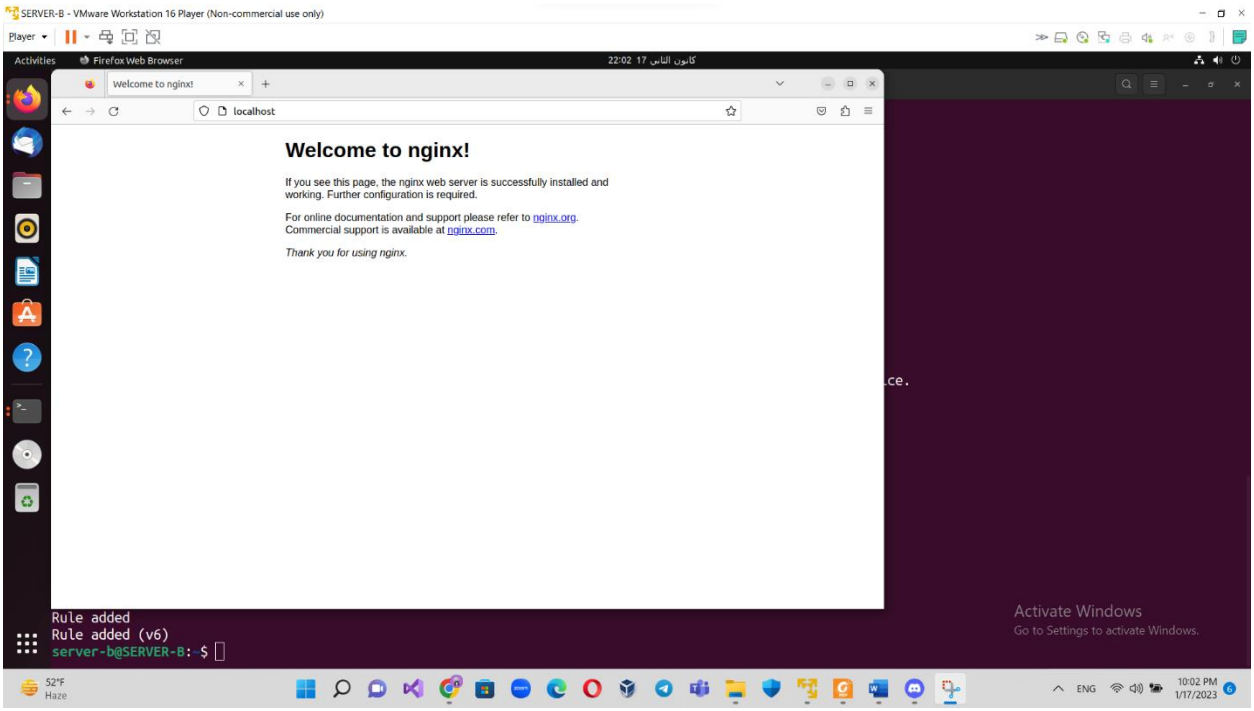

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
17:18 17 كانون الثاني
server-b@SERVER-B: ~
server-b@SERVER-B:~$ sudo mysql -u root -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 23
Server version: 8.0.31-0ubuntu0.22.04.1 (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> CREATE USER 'royalcars'@'localhost' IDENTIFIED BY 'royalcars1
'>
'> ^C
mysql> CREATE USER 'royalcars'@'localhost' IDENTIFIED BY 'royalcars123Password*';
Query OK, 0 rows affected (0.24 sec)
mysql> GRANT PRIVILEGE ON database.table TO 'royalcars'@'localhost';
ERROR 3619 (HY000): Illegal privilege level specified for table
mysql> GRANT CREATE, ALTER, DROP, INSERT, UPDATE, DELETE, SELECT, REFERENCES, RELOAD on *.* TO 'royalcars'@'localhost' WITH GRANT OPTION;
Query OK, 0 rows affected (0.25 sec)
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> exit
Bye
server-b@SERVER-B:~$ sudo mysql -u royalcars -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
5:18 PM
1/17/2023

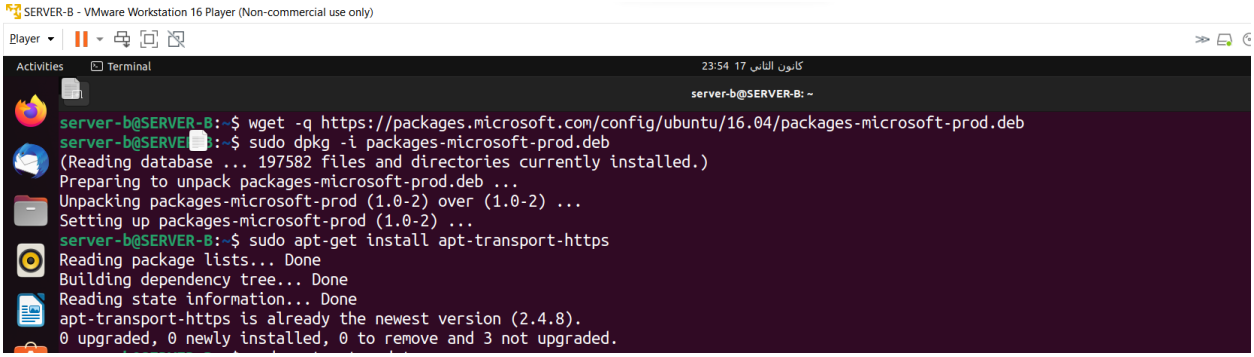

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
17:19 17 كانون الثاني
server-b@SERVER-B: ~
server-b@SERVER-B:~$ systemctl status mysql.service
mysql.service - MySQL Community Server
Loaded: loaded (/lib/systemd/system/mysql.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 15:58:54 +03; 1h 18min ago
Main PID: 5311 (mysqld)
Status: "Server is operational"
Tasks: 40 (limit: 4584)
Memory: 359.6M
CPU: 1min 12.262s
CGroup: /system.slice/mysql.service
└─5311 /usr/sbin/mysqld
15:58:53 17 كانون الثاني SERVER-B systemd[1]: Starting MySQL Community Server...
15:58:54 17 كانون الثاني SERVER-B systemd[1]: Started MySQL Community Server.
server-b@SERVER-B:~$ sudo mysql -u royalcars -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 25
Server version: 8.0.31-0ubuntu0.22.04.1 (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> show databases;
+--------------------+
| Database |
+--------------------+
| information_schema |
| mysql |
| performance_schema |
| sys |
+--------------------+
4 rows in set (0.94 sec)
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
5:19 PM
1/17/2023

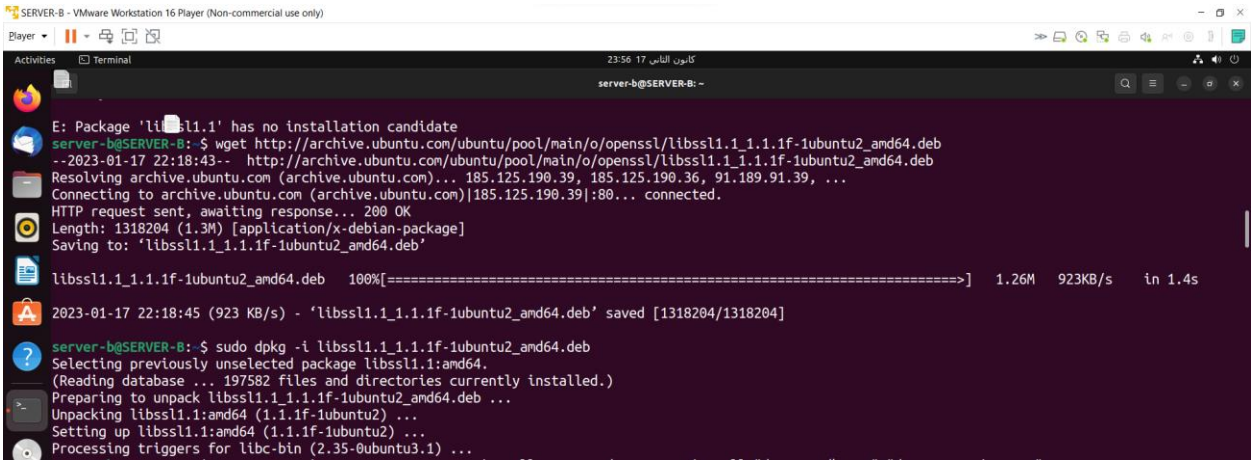
- **HTTP Service [12]**

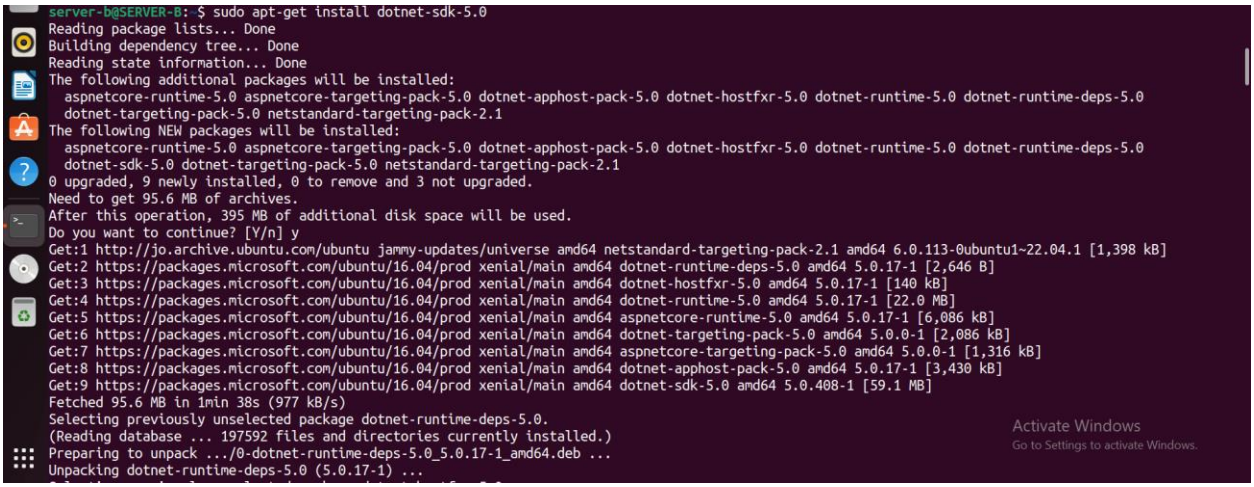




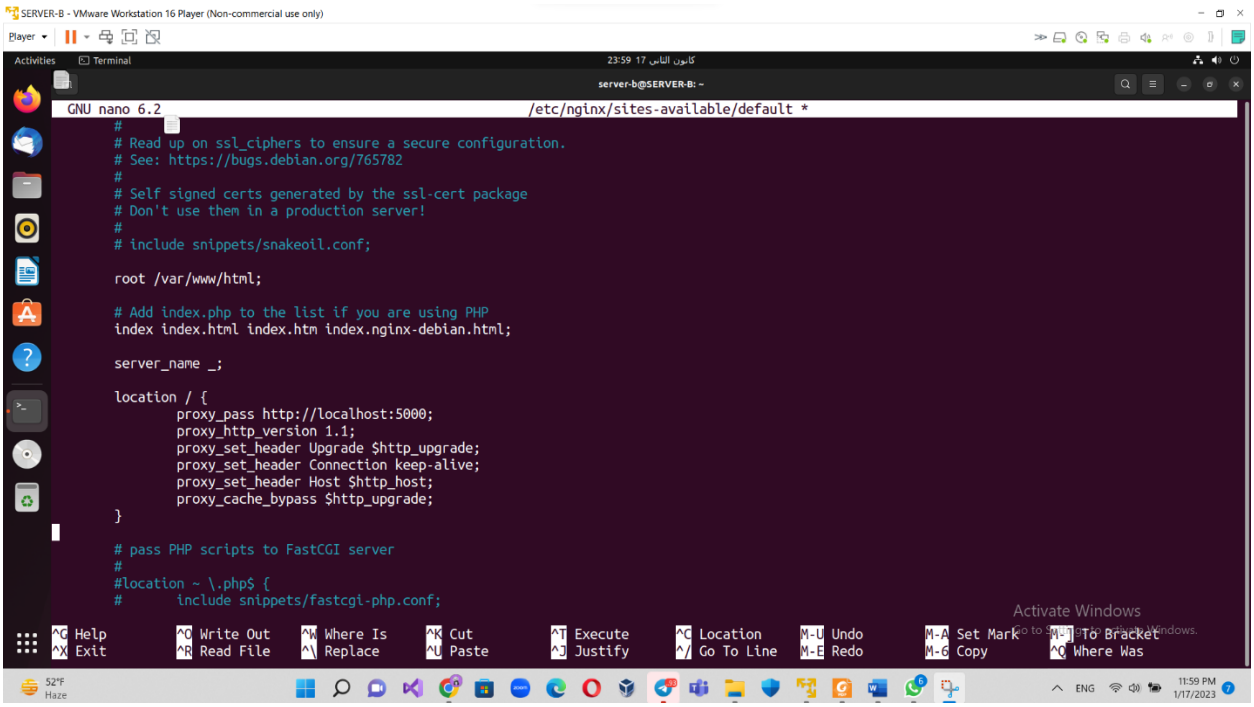

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
22:02 17 كانون الثاني
Welcome to nginx!
localhost
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.
Rule added
Rule added (v6)
server-b@SERVER-B:~$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
10:02 PM
1/17/2023

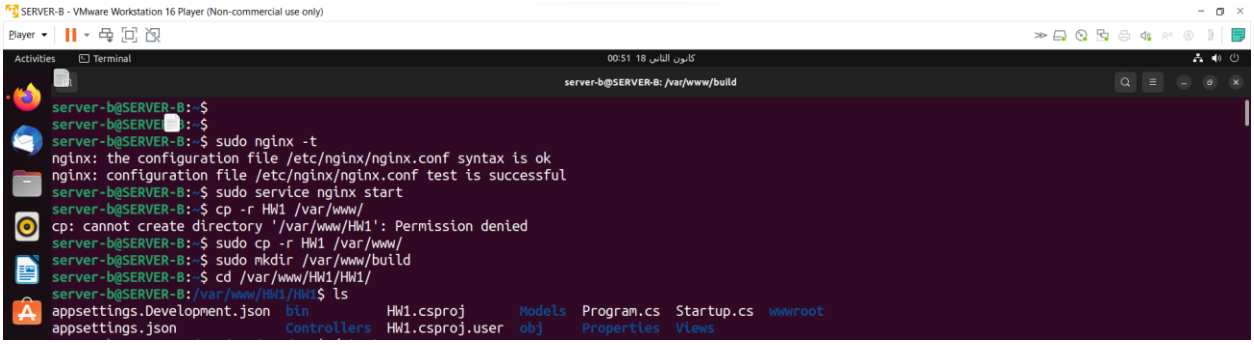

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
23:54 17 كانون الثاني
server-b@SERVER-B: ~
server-b@SERVER-B:~$ wget -q https://packages.microsoft.com/config/ubuntu/16.04/packages-microsoft-prod.deb
server-b@SERVER-B:~$ sudo dpkg -i packages-microsoft-prod.deb
(Reading database ... 197582 files and directories currently installed.)
Preparing to unpack packages-microsoft-prod.deb ...
Unpacking packages-microsoft-prod (1.0-2) over (1.0-2) ...
Setting up packages-microsoft-prod (1.0-2) ...
server-b@SERVER-B:~$ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apt-transport-https is already the newest version (2.4.8).
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.

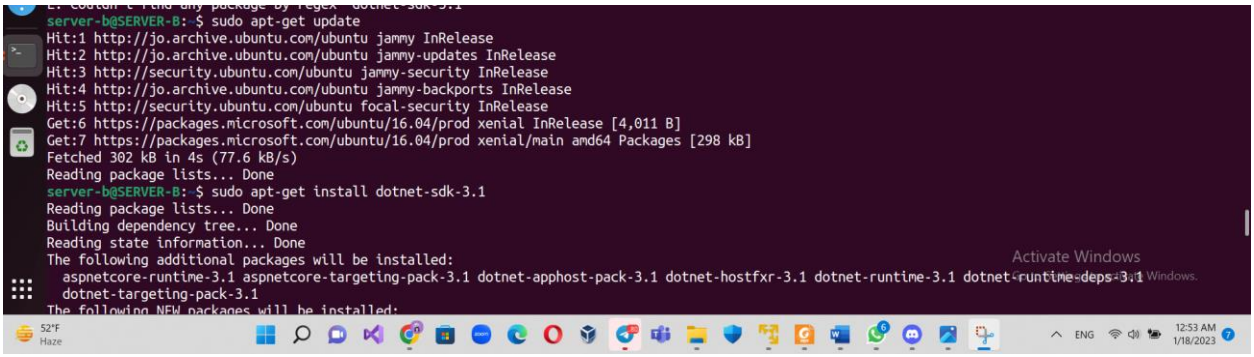

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
23:56 17 كانون الثاني
server-b@SERVER-B: ~
E: Package 'libssl1.1' has no installation candidate
server-b@SERVER-B:~$ wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2_amd64.deb
--2023-01-17 22:18:43-- http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.1_1.1.1f-1ubuntu2_amd64.deb
Resolving archive.ubuntu.com (archive.ubuntu.com)... 185.125.190.39, 185.125.190.36, 91.189.91.39, ...
Connecting to archive.ubuntu.com (archive.ubuntu.com)|185.125.190.39|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1318204 (1.3M) [application/x-debian-package]
Saving to: 'libssl1.1_1.1.1f-1ubuntu2_amd64.deb'
libssl1.1_1.1.1f-1ubuntu2_amd64.deb 100%[==========>] 1.26M 923KB/s in 1.4s
2023-01-17 22:18:45 (923 KB/s) - 'libssl1.1_1.1.1f-1ubuntu2_amd64.deb' saved [1318204/1318204]
server-b@SERVER-B:~$ sudo dpkg -i libssl1.1_1.1.1f-1ubuntu2_amd64.deb
Selecting previously unselected package libssl1.1:amd64.
(Reading database ... 197582 files and directories currently installed.)
Preparing to unpack libssl1.1_1.1.1f-1ubuntu2_amd64.deb ...
Unpacking libssl1.1:amd64 (1.1.1f-1ubuntu2) ...
Setting up libssl1.1:amd64 (1.1.1f-1ubuntu2) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...


server-b@SERVER-B:~$ sudo apt-get install dotnet-sdk-5.0
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
aspnetcore-runtime-5.0 aspnetcore-targeting-pack-5.0 dotnet-apphost-pack-5.0 dotnet-hostfxr-5.0 dotnet-runtime-5.0 dotnet-runtime-deps-5.0
dotnet-targeting-pack-5.0 netstandard-targeting-pack-2.1
The following NEW packages will be installed:
aspnetcore-runtime-5.0 aspnetcore-targeting-pack-5.0 dotnet-apphost-pack-5.0 dotnet-hostfxr-5.0 dotnet-runtime-5.0 dotnet-runtime-deps-5.0
dotnet-sdk-5.0 dotnet-targeting-pack-5.0 netstandard-targeting-pack-2.1
0 upgraded, 9 newly installed, 0 to remove and 3 not upgraded.
Need to get 95.6 MB of archives.
After this operation, 395 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://jo.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 netstandard-targeting-pack-2.1 amd64 6.0.113-0ubuntu1~22.04.1 [1,398 kB]
Get:2 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-runtime-deps-5.0 amd64 5.0.17-1 [2,646 B]
Get:3 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-hostfxr-5.0 amd64 5.0.17-1 [140 kB]
Get:4 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-runtime-5.0 amd64 5.0.17-1 [22.0 MB]
Get:5 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 aspnetcore-runtime-5.0 amd64 5.0.17-1 [6,086 kB]
Get:6 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-targeting-pack-5.0 amd64 5.0.0-1 [2,086 kB]
Get:7 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 aspnetcore-targeting-pack-5.0 amd64 5.0.0-1 [1,316 kB]
Get:8 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-apphost-pack-5.0 amd64 5.0.17-1 [3,430 kB]
Get:9 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-sdk-5.0 amd64 5.0.408-1 [59.1 MB]
Fetched 95.6 MB in 1min 38s (977 kB/s)
Selecting previously unselected package dotnet-runtime-deps-5.0.
(Reading database ... 197592 files and directories currently installed.)
Preparing to unpack .../0-dotnet-runtime-deps-5.0_5.0.17-1_amd64.deb ...
Unpacking dotnet-runtime-deps-5.0 (5.0.17-1) ...
Activate Windows
Go to Settings to activate Windows.

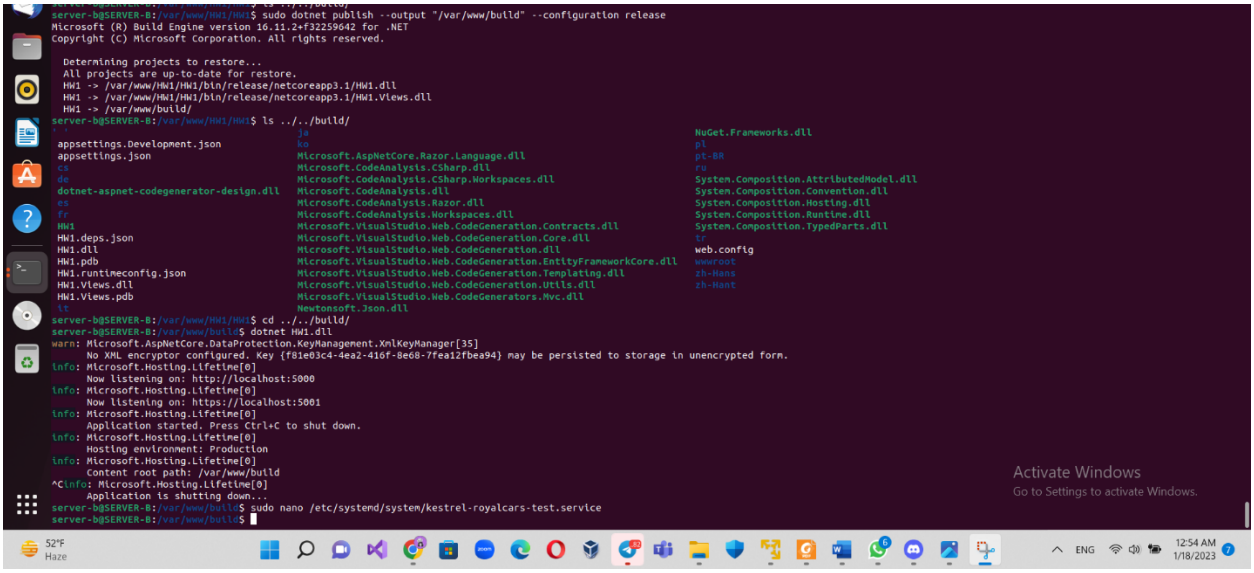

server-b@SERVER-B:~$ ls
Desktop Documents Downloads HW1 libssl1.1_1.1.1f-1ubuntu2_amd64.deb Music packages-microsoft-prod.deb Pictures Public snap Templates Videos
server-b@SERVER-B:~$ sudo service nginx status
[sudo] password for server-b:
nginx.service - A high performance web server and a reverse proxy server
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
Active: active (running) since Tue 2023-01-17 21:56:25 +03; 1h 55min ago
Docs: man:nginx(8)
Process: 39060 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
Process: 39062 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCESS)
Main PID: 39158 (nginx)
Tasks: 3 (limit: 4584)
Memory: 3.8M
CPU: 284ms
CGroup: /system.slice/nginx.service
├─39158 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
├─39160 "nginx: worker process"
└─39161 "nginx: worker process"
21:56:25 17 كانون الثاني SERVER-B systemd[1]: Starting A high performance web server and a reverse proxy server...
21:56:25 17 كانون الثاني SERVER-B systemd[1]: Started A high performance web server and a reverse proxy server.
server-b@SERVER-B:~$ nano /etc/nginx/sites-available/default
server-b@SERVER-B:~$ sudo nano /etc/nginx/sites-available/default
server-b@SERVER-B:~$
Activate Windows
Go to Settings to activate Windows.

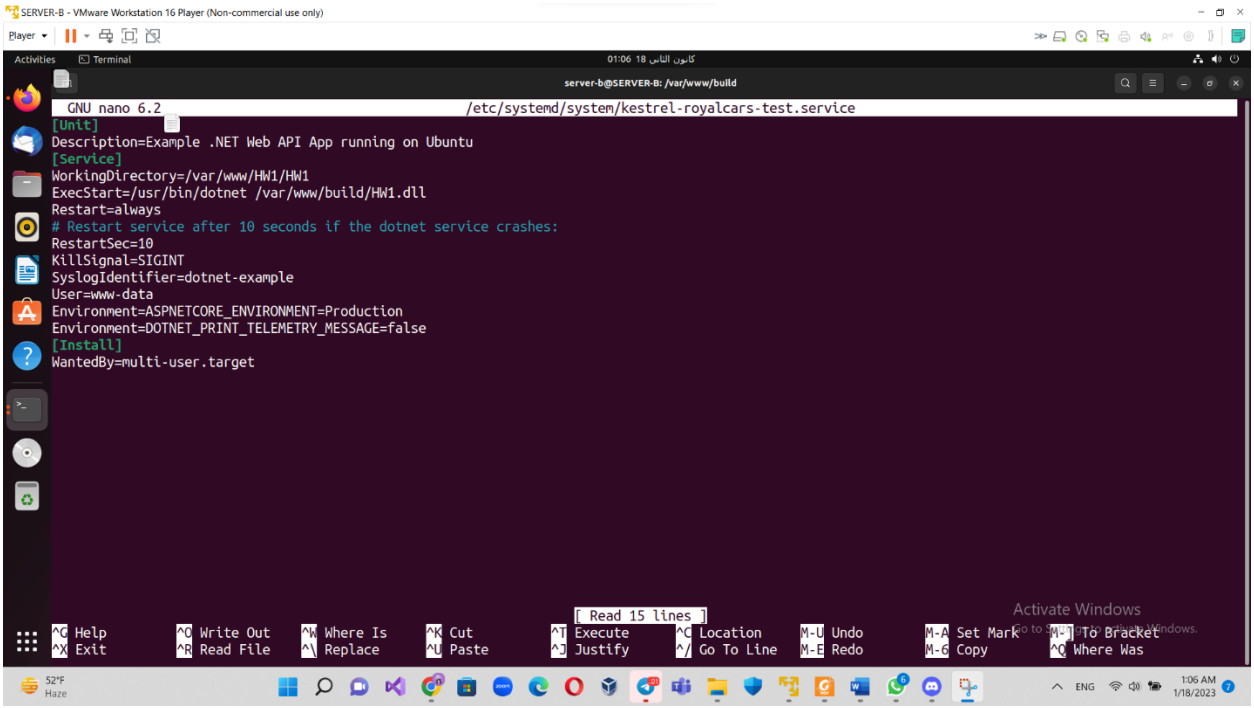

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-b@SERVER-B: ~
GNU nano 6.2 /etc/nginx/sites-available/default *
Read up on ssl_ciphers to ensure a secure configuration.
See: https://bugs.debian.org/765782
Self signed certs generated by the ssl-cert package
Don't use them in a production server!
include snippets/snakeoil.conf;
root /var/www/html;
Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;
server_name _;
location / {
proxy_pass http://localhost:5000;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection keep-alive;
proxy_set_header Host $http_host;
proxy_cache_bypass $http_upgrade;
}
# pass PHP scripts to FastCGI server
#location ~ \.php$ {
include snippets/fastcgi-php.conf;
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was
Activate Windows
52°F Haze
ENG 11:59 PM 1/17/2023

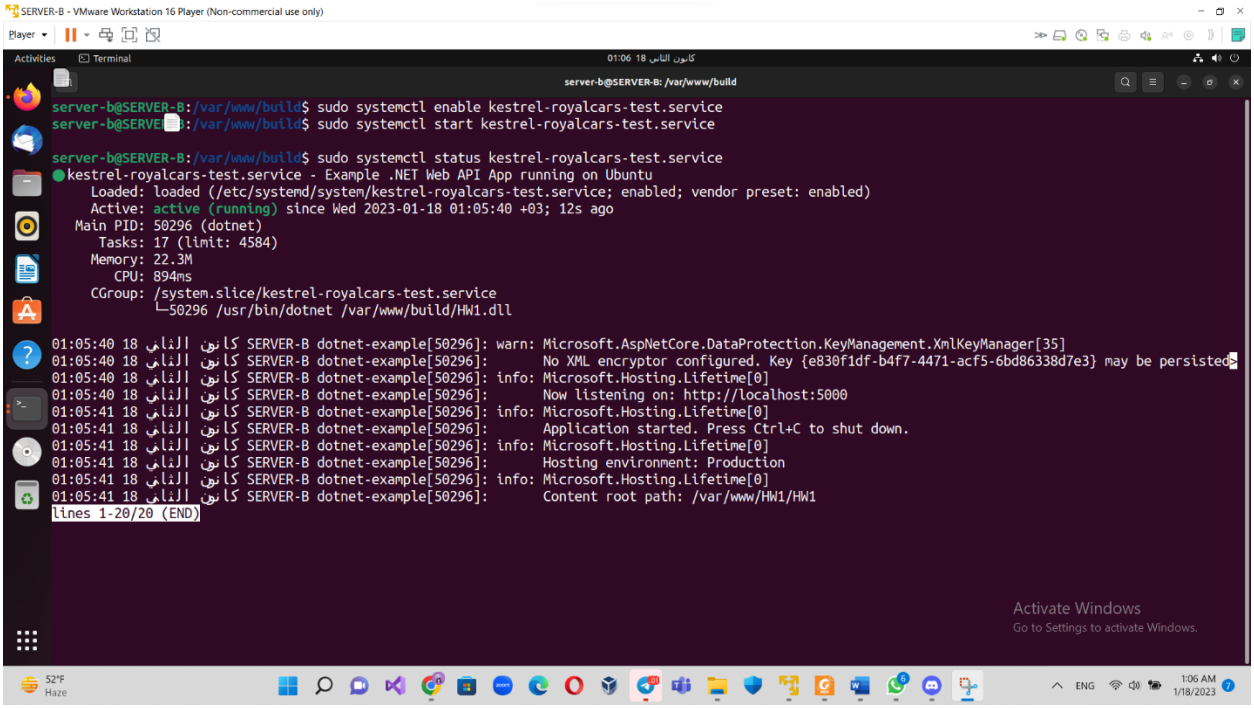

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-b@SERVER-B: /var/www/build
server-b@SERVER-B:~$
server-b@SERVER-B:~$
server-b@SERVER-B:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
server-b@SERVER-B:~$ sudo service nginx start
server-b@SERVER-B:~$ cp -r HW1 /var/www/
cp: cannot create directory '/var/www/HW1': Permission denied
server-b@SERVER-B:~$ sudo cp -r HW1 /var/www/
server-b@SERVER-B:~$ sudo mkdir /var/www/build
server-b@SERVER-B:~$ cd /var/www/HW1/HW1/
server-b@SERVER-B:/var/www/HW1/HW1$ ls
appsettings.Development.json bin HW1.csproj Models Program.cs Startup.cs wwwroot
appsettings.json Controllers HW1.csproj.user obj Properties Views

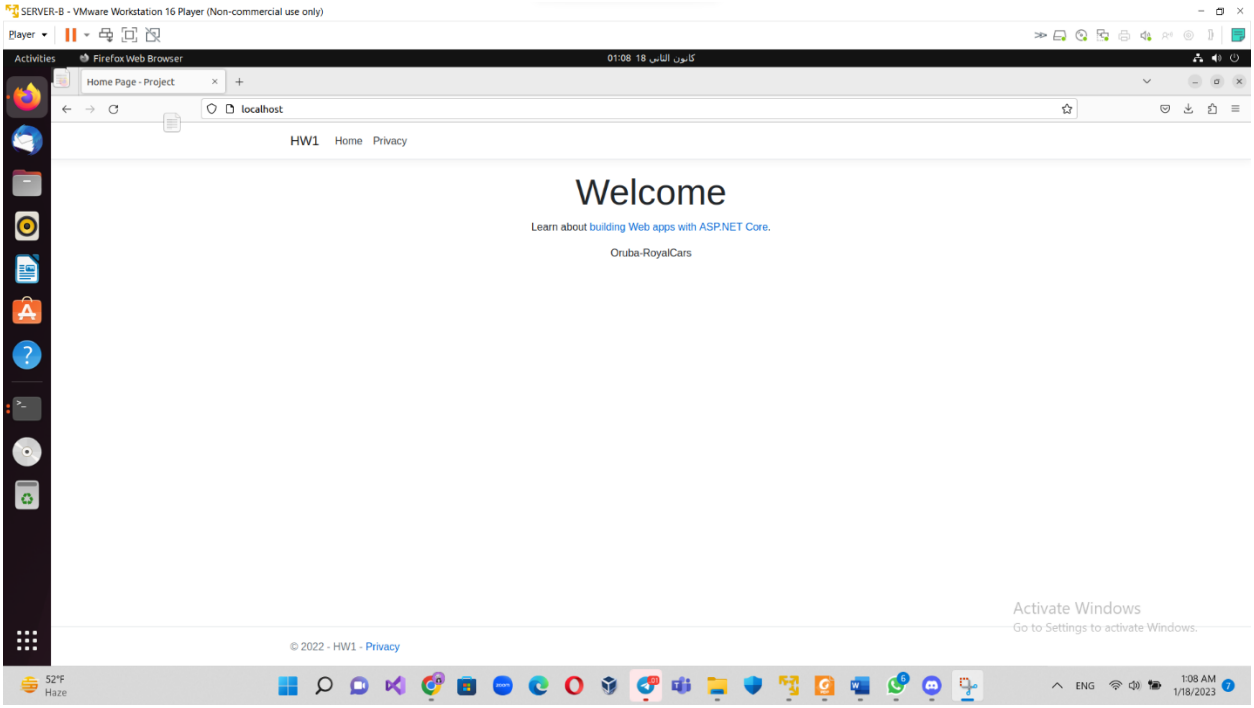

server-b@SERVER-B:~$ sudo apt-get update
Hit:1 http://jo.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://jo.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:4 http://jo.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:5 http://security.ubuntu.com/ubuntu focal-security InRelease
Get:6 https://packages.microsoft.com/ubuntu/16.04/prod xenial InRelease [4,011 B]
Get:7 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 Packages [298 kB]
Fetched 302 kB in 4s (77.6 kB/s)
Reading package lists... Done
server-b@SERVER-B:~$ sudo apt-get install dotnet-sdk-3.1
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
aspnetcore-runtime-3.1 aspnetcore-targeting-pack-3.1 dotnet-apphost-pack-3.1 dotnet-hostfxr-3.1 dotnet-runtime-3.1 dotnet-runtime-deps-3.1
dotnet-targeting-pack-3.1
Activate Windows
52°F Haze
ENG 12:53 AM 1/18/2023


server-b@SERVER-B:~$ cd /var/www/HW1/HW1/
server-b@SERVER-B:/var/www/HW1/HW1$ sudo dotnet run
warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
No XML encryptor configured. Key {1074b11d-f0e8-4cd8-a0aa-64a92c964d7a} may be persisted to storage in unencrypted form.
info: Microsoft.Hosting.Lifetime[0]
Now listening on: https://localhost:5001
info: Microsoft.Hosting.Lifetime[0]
Now listening on: http://localhost:5000
info: Microsoft.Hosting.Lifetime[0]
Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
Hosting environment: Development
info: Microsoft.Hosting.Lifetime[0]
Content root path: /var/www/HW1/HW1
^Cinfo: Microsoft.Hosting.Lifetime[0]
Application is shutting down...


server-b@SERVER-B:/var/www/HW1/HW1$ sudo dotnet publish --output "/var/www/build" --configuration release
Microsoft (R) Build Engine version 16.11.2+f32259642 for .NET
Copyright (C) Microsoft Corporation. All rights reserved.
Determining projects to restore...
All projects are up-to-date for restore.
HW1 -> /var/www/HW1/HW1/bin/release/netcoreapp3.1/HW1.dll
HW1 -> /var/www/HW1/HW1/bin/release/netcoreapp3.1/HW1.Views.dll
HW1 -> /var/www/build/
server-b@SERVER-B:/var/www/HW1/HW1$ ls ../../build/
appsettings.Development.json
appsettings.json
cs
de
dotnet-aspnet-codegenerator-design.dll
es
fr
HW1
HW1.deps.json
HW1.dll
HW1.pdb
HW1.runtimeconfig.json
HW1.Views.dll
HW1.Views.pdb
it
ja
ko
Microsoft.AspNetCore.Razor.Language.dll
Microsoft.CodeAnalysis.CSharp.dll
Microsoft.CodeAnalysis.CSharp.Workspaces.dll
Microsoft.CodeAnalysis.dll
Microsoft.CodeAnalysis.Razor.dll
Microsoft.CodeAnalysis.Workspaces.dll
Microsoft.VisualStudio.Web.CodeGeneration.Contracts.dll
Microsoft.VisualStudio.Web.CodeGeneration.Core.dll
Microsoft.VisualStudio.Web.CodeGeneration.dll
Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore.dll
Microsoft.VisualStudio.Web.CodeGeneration.Templating.dll
Microsoft.VisualStudio.Web.CodeGeneration.Utils.dll
Microsoft.VisualStudio.Web.CodeGenerators.Mvc.dll
Newtonsoft.Json.dll
NuGet.Frameworks.dll
pl
pt-BR
ru
System.Composition.AttributedModel.dll
System.Composition.Convention.dll
System.Composition.Hosting.dll
System.Composition.Runtime.dll
System.Composition.TypedParts.dll
tr
web.config
wwwroot
zh-Hans
zh-Hant
server-b@SERVER-B:/var/www/HW1/HW1$ cd ../../build/
server-b@SERVER-B:/var/www/build$ dotnet HW1.dll
warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
No XML encryptor configured. Key {f81e03c4-4ea2-416f-8e68-7fea12fbea94} may be persisted to storage in unencrypted form.
info: Microsoft.Hosting.Lifetime[0]
Now listening on: http://localhost:5000
info: Microsoft.Hosting.Lifetime[0]
Now listening on: https://localhost:5001
info: Microsoft.Hosting.Lifetime[0]
Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
Hosting environment: Production
info: Microsoft.Hosting.Lifetime[0]
Content root path: /var/www/build
^Cinfo: Microsoft.Hosting.Lifetime[0]
Application is shutting down...
server-b@SERVER-B:/var/www/build$ sudo nano /etc/systemd/system/kestrel-royalcars-test.service
server-b@SERVER-B:/var/www/build$
Activate Windows
Go to Settings to activate Windows.
52°F
Haze
ENG
12:54 AM
1/18/2023


SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-b@SERVER-B: /var/www/build
GNU nano 6.2
/etc/systemd/system/kestrel-royalcars-test.service
[Unit]
Description=Example .NET Web API App running on Ubuntu
[Service]
WorkingDirectory=/var/www/HW1/HW1
ExecStart=/usr/bin/dotnet /var/www/build/HW1.dll
Restart=always
# Restart service after 10 seconds if the dotnet service crashes:
RestartSec=10
KillSignal=SIGINT
SyslogIdentifier=dotnet-example
User=www-data
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=DOTNET_PRINT_TELEMETRY_MESSAGE=false
[Install]
WantedBy=multi-user.target
[Read 15 lines]
^G Help
^X Exit
^O Write Out
^R Read File
^W Where Is
^\ Replace
^K Cut
^U Paste
^T Execute
^J Justify
^C Location
^/ Go To Line
M-U Undo
M-E Redo
M-A Set Mark
M-6 Copy
M-] To Bracket
^Q Where Was
Activate Windows
52°F
Haze
ENG
1:06 AM
1/18/2023


SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Terminal
server-b@SERVER-B: /var/www/build
server-b@SERVER-B:/var/www/build$ sudo systemctl enable kestrel-royalcars-test.service
server-b@SERVER-B:/var/www/build$ sudo systemctl start kestrel-royalcars-test.service
server-b@SERVER-B:/var/www/build$ sudo systemctl status kestrel-royalcars-test.service
kestrel-royalcars-test.service - Example .NET Web API App running on Ubuntu
Loaded: loaded (/etc/systemd/system/kestrel-royalcars-test.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2023-01-18 01:05:40 +03; 12s ago
Main PID: 50296 (dotnet)
Tasks: 17 (limit: 4584)
Memory: 22.3M
CPU: 894ms
CGroup: /system.slice/kestrel-royalcars-test.service
└─50296 /usr/bin/dotnet /var/www/build/HW1.dll
01:05:40 18 كانون الثاني SERVER-B dotnet-example[50296]: warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
01:05:40 18 كانون الثاني SERVER-B dotnet-example[50296]: No XML encryptor configured. Key {e830f1df-b4f7-4471-acf5-6bd86338d7e3} may be persisted
01:05:40 18 كانون الثاني SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:40 18 كانون الثاني SERVER-B dotnet-example[50296]: Now listening on: http://localhost:5000
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: Application started. Press Ctrl+C to shut down.
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: Hosting environment: Production
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كانون الثاني SERVER-B dotnet-example[50296]: Content root path: /var/www/HW1/HW1
lines 1-20/20 (END)
Activate Windows
Go to Settings to activate Windows.
52°F Haze
ENG
1:06 AM 1/18/2023


SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Home Page - Project
localhost
HW1 Home Privacy
Welcome
Learn about building Web apps with ASP.NET Core.
Oruba-RoyalCars
© 2022 - HW1 - Privacy
Activate Windows
Go to Settings to activate Windows.
52°F Haze
ENG
1:08 AM 1/18/2023

An explanation of the vulnerabilities and the attack used to take advantage of the vulnerability

They are arranged so that the circle symbolizes the vulnerabilities, and the square symbolizes the used attacks as you can see:

- ○ **Password pattern vulnerability**, this type of vulnerability can occur when a website or application has a password policy that requires users to follow a specific pattern when creating their passwords, such as including a certain number of special characters or numbers. Because these patterns are often predictable, they can make it easier for attackers to crack passwords using brute-force or dictionary-based attacks.[13]

- ○ **The DNS (Domain Name System) Tunneling vulnerability** that provides a means of encapsulating malicious payloads is known as "DNS Tunneling." It is a technique used to bypass network security restrictions by using the DNS protocol to transmit data in an encrypted format, which can be used to exfiltrate data from a network, establish a command-and-control channel, or deliver malware payloads. This type of vulnerability is often used in advanced persistent threat (APT) attacks, where attackers use DNS Tunneling to evade detection and maintain access to a compromised system.[14]

- ○ **Windows Shell Remote Code Execution Vulnerability (MS10-046)** is a security vulnerability that exists in the way that the Windows Shell, which is the interface that provides access to the files and folders on a computer, handles shortcut files (LNK files) in Windows.[15]

- ☐ **A brute-force attack** is a trial-and-error method used by application programs to decode login information and encryption keys to use them to gain unauthorized access to systems. Using brute force is an exhaustive effort rather than employing intellectual strategies.[16]

- ☐ **A malicious shortcut file attack** is a type of cyber-attack that exploits a vulnerability in the way that the Windows Shell handles shortcut files (LNK files) in Windows. The vulnerability allows an attacker to remotely execute arbitrary code on an affected system by tricking a user into clicking on a malicious shortcut file. The code would then run with the privileges of the user who clicked on the file.[17]

- ☐ **A spyware attack** is a type of cyber-attack in which malicious software is installed on a victim's device without their knowledge or consent. The software is designed to gather sensitive information, such as login credentials, financial data, and browsing history, and send it back to the attacker. Spyware can also be used to control the victim's device, allowing the attacker to perform actions such as disabling security software, downloading other malware, or displaying unwanted ads. Spyware is often spread through phishing emails, infected websites, or malicious software downloads.[18]

Offensive Cybersecurity

Executive Summery

The attacker entered the company's network in some way and hacked the admin's device using a brute-force attack based on information collected through social engineering and made his device a reliable source to access the company's website and took advantage of this by entering an employee's device and manipulating a project on it by adding spyware code. The project file has been accessed by the CEO device to view it, which caused the hacker to be able to spy on the CEO and obtain passwords for the database and many sensitive information from the employee and CEO devices.

Vulnerability Severity Ratings:[19]

- Windows Shell Remote Code Execution Vulnerability MS10-046 ➔ Critical (9.2)
- The DNS (Domain Name System) Tunneling Vulnerability ➔ High (7.5)
- Password Pattern Vulnerability ➔ Medium (4.9)
- Social Engineering ➔ Low (0.1-3.9)

Recommendations:

- Windows Shell Remote Code Execution Vulnerability MS10-046 ➔Install the security update from Microsoft.[15]
- The DNS (Domain Name System) Tunneling Vulnerability ➔ DNS filtering is a security technique that uses DNS servers to block or allow access to specific websites or internet addresses based on predefined rules.[20]
- Password Pattern Vulnerability ➔ Implement strong password policies and to use password managers.
- Social Engineering ➔ Educate employees on how to recognize and respond to potential social engineering attacks.

Attack narrative and findings

The hacker visited a company for customer service, and during one of the employees opened a device to display the company’s website to view the available cars, he was able to deceive the employee and use social engineering by distracting him and making him enter a device password without hiding it from the customer.

After entering the company's network, a full scan for all environment was done to determine the existing devices

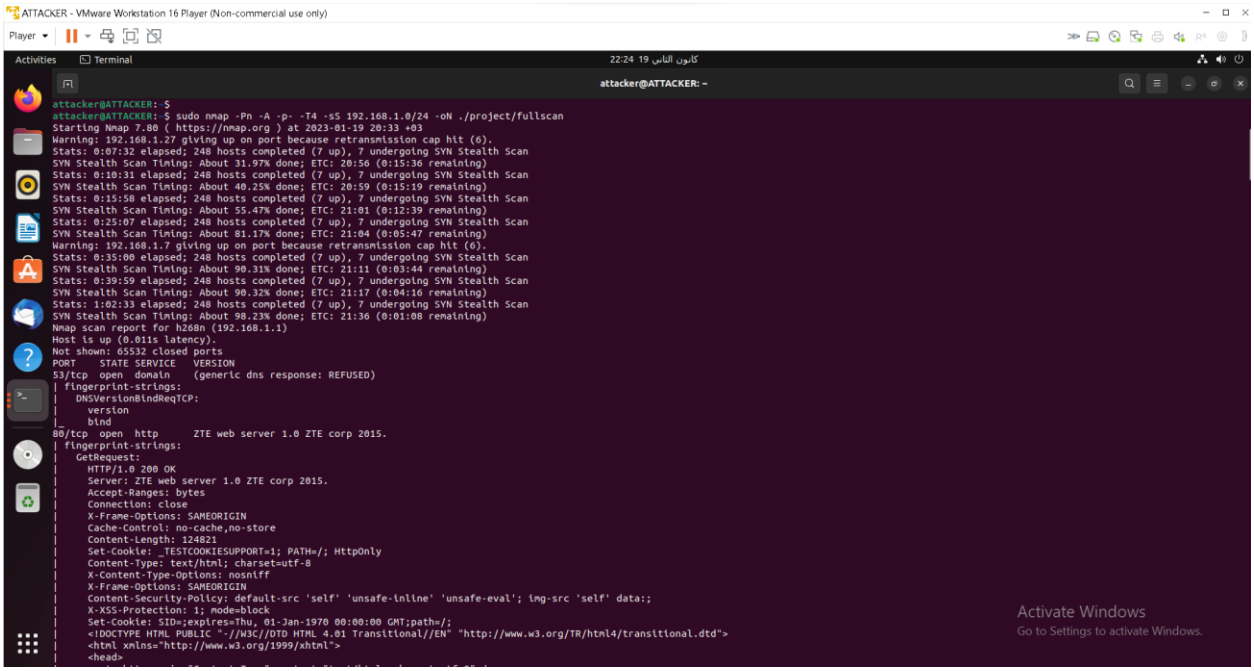
nmap ➔ Network exploration tool and security / port scanner.

-A ➔ used to enable OS detection, version detection, script scanning and traceroute.

-p- ➔ used to scan all ports instead of the default, which is to scan only the top 1000 most common ports.

-T4 ➔ used to set the timing template to "aggressive", which speeds up the scan.

-oN ➔ used to output the results of the scan to a file in normal format. The file name would be specified after this flag.



We found that there is an Ubuntu device on which the ssh service was activated, and based on what was collected through social engineering, it was expected that the password includes the username in addition to 123Password* and of course I used the most famous wordlist for that rockyou.txt

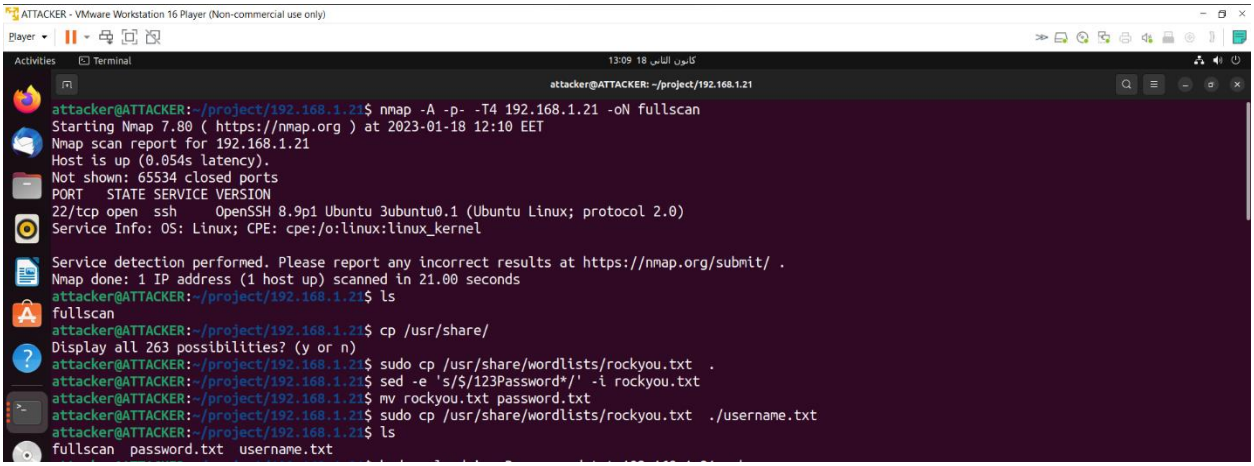
IP Address of the victim machine: 192.168.1.21

We will do scan in this specific Ip Address for double check

sed ➔ is a command-line tool for editing files

-e ➔ used to specify a script or command to be executed

-I ➔ used to edit a file in-place

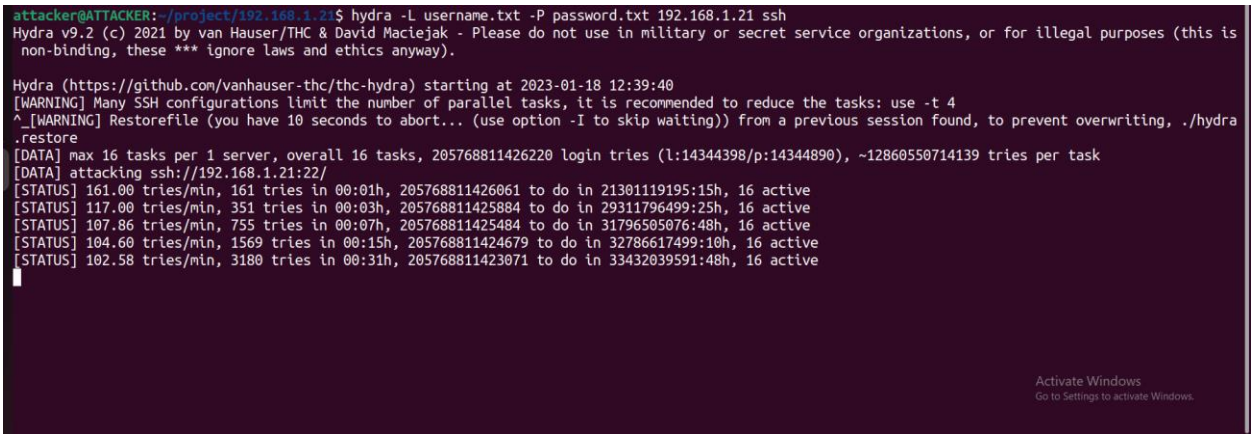


We will use brute force attack to access victim's machine through ssh with hydra

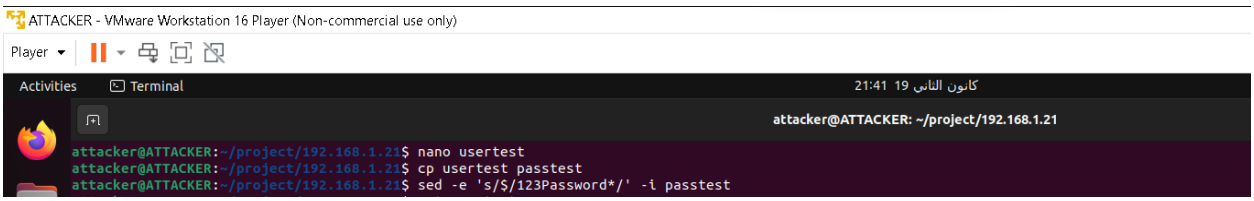
hydra ➔ a very fast network logon cracker which supports many different services

-L ➔ set usernames file

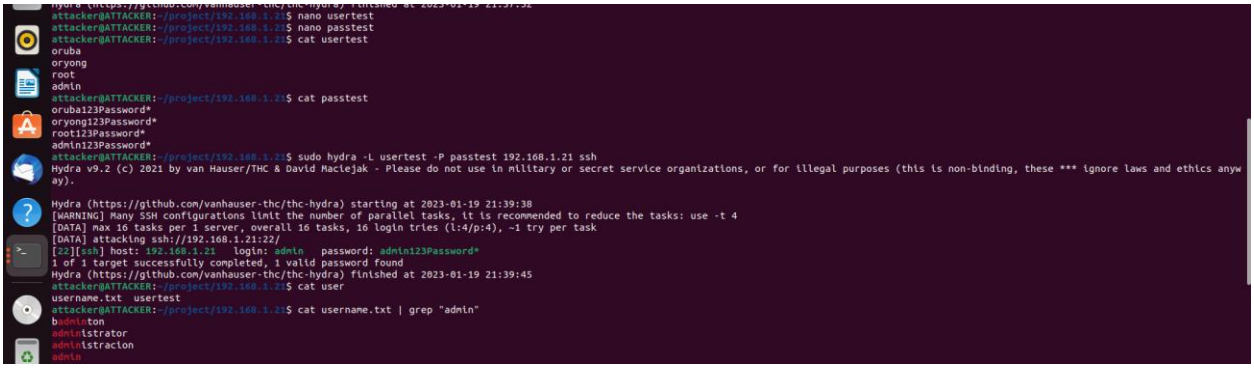
-P ➔ set passwords file

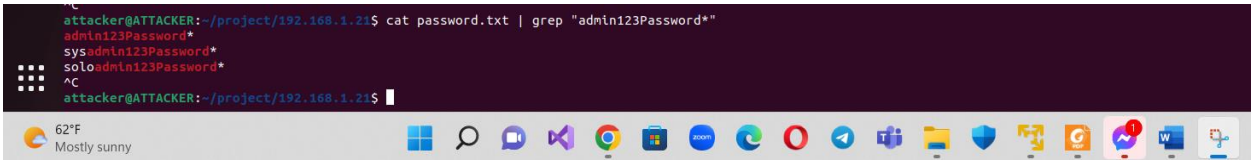


Since we do not have much time, and this process is just a simulation, we will use two smaller files containing the username and password to prove the matter.

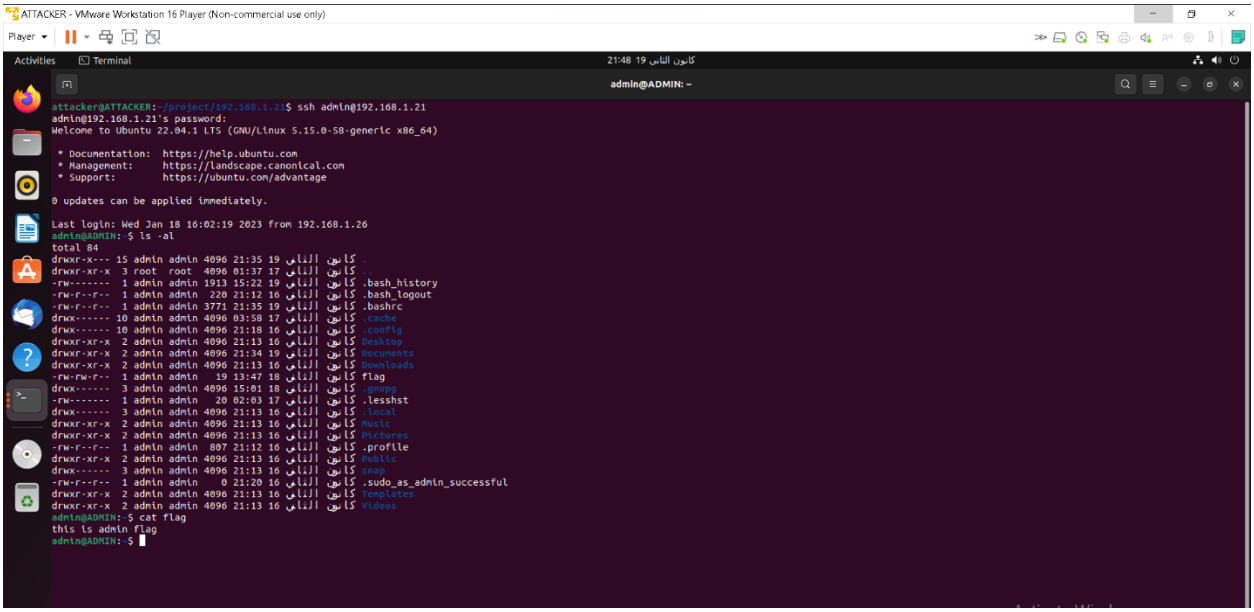


The following image shows proof of brute force success with proof of their presence in the original files, whether it is admin, root, or others. The matter will succeed as long as the name is common.



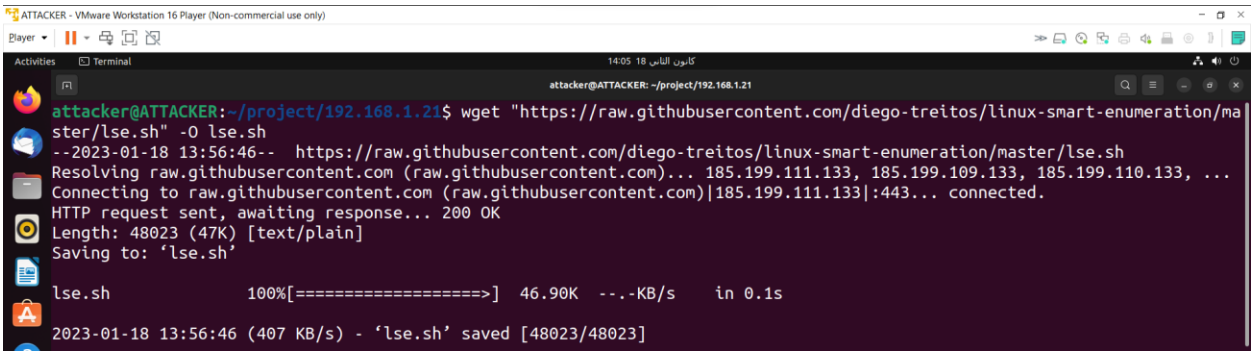


Use username and password to log into the victim's machine



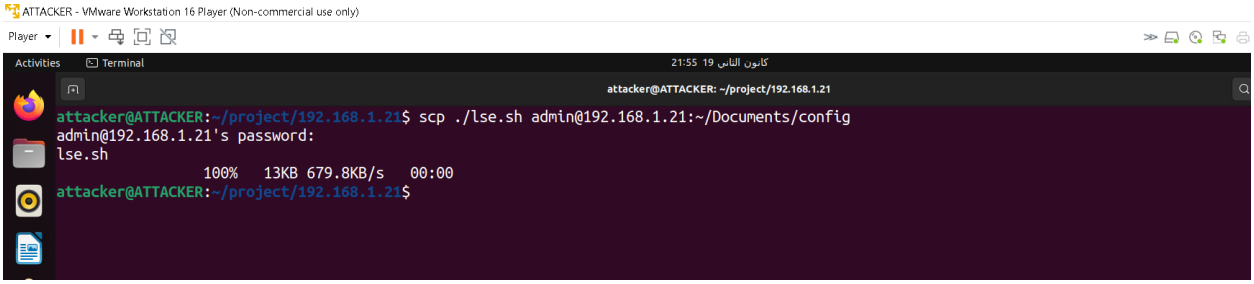
We will try to determine what permissions are given to the user using Linux Smart Enumeration (LSE) which is a script that automates the process of enumeration on a Linux system during a penetration testing or security assessment engagement.

wget ➔ is a command-line utility for downloading files from the Internet.

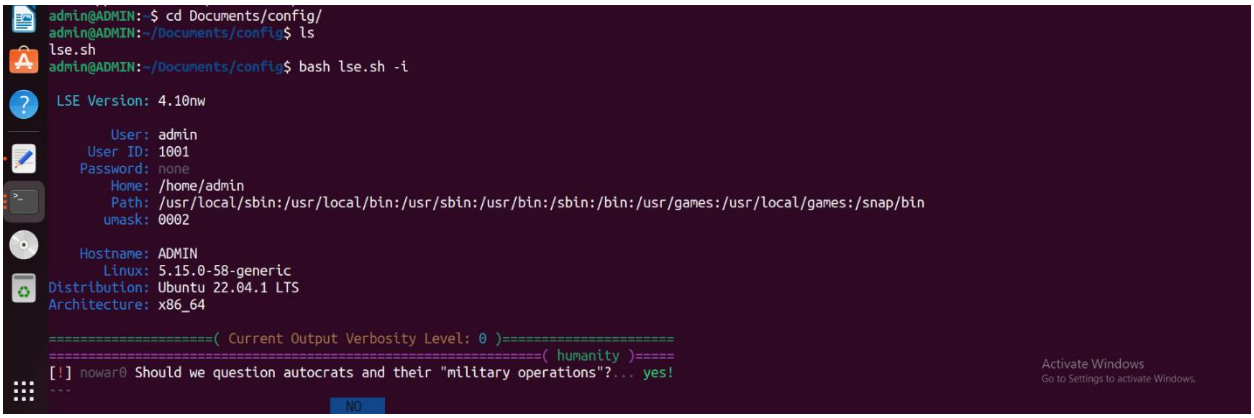


With the script present, I now need to transfer it to the victim's machine via scp

scp ➔ (secure copy) is a command-line utility that allows you to securely copy files between different computers. It uses the SSH (Secure Shell) protocol to encrypt the data transfer and authenticate the user.



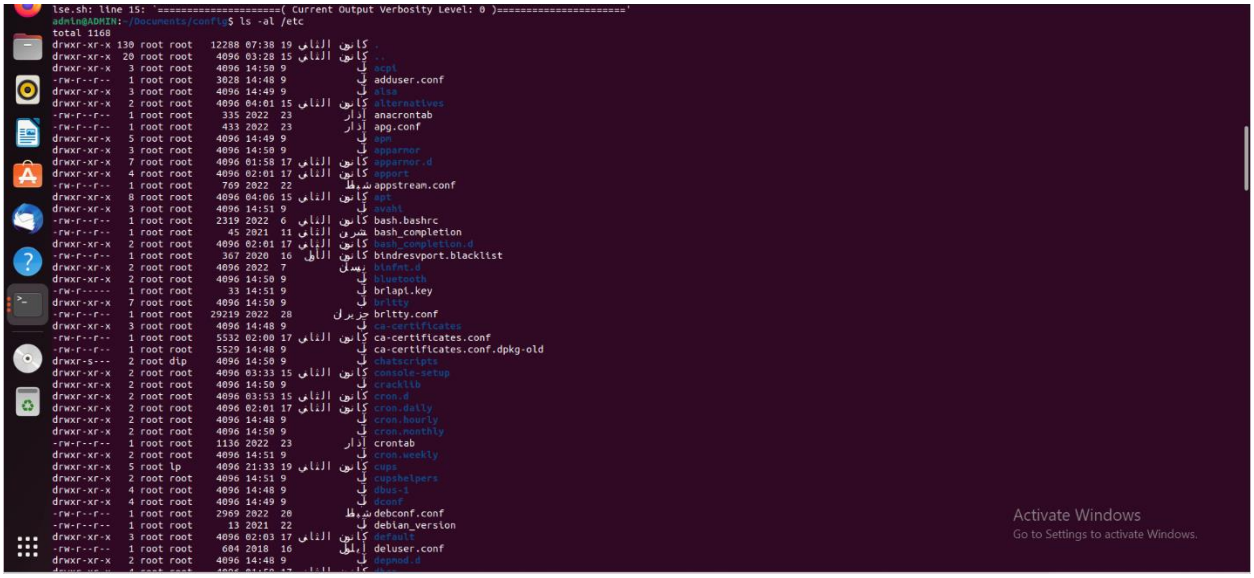
We conclude that the user has sudo privileges in addition to the absence of root being the nologin account as default



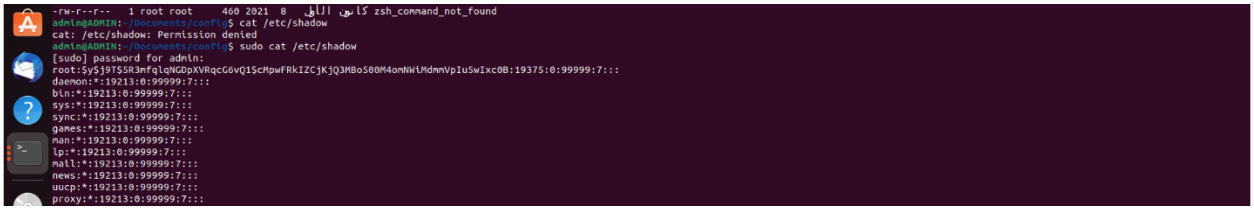
We start a file scan and try to access sensitive files such as shadow

Shadow file ➔is a system file that stores the password information for all user accounts on the system.

The path of the shadow is /etc/shadow



Important information has been reached



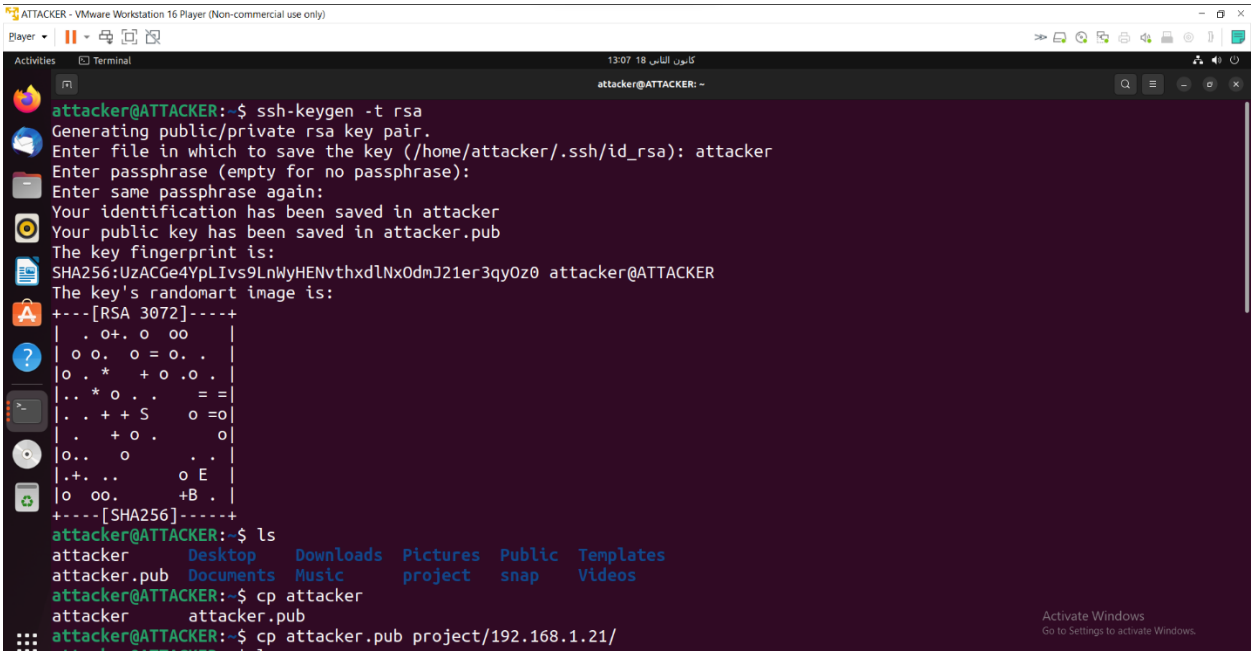
Now you need to do maintain access by creating a backdoor

We will create a private and public key to use it to access the device. In the event of a password change, we will use ssh-keygen to create them.

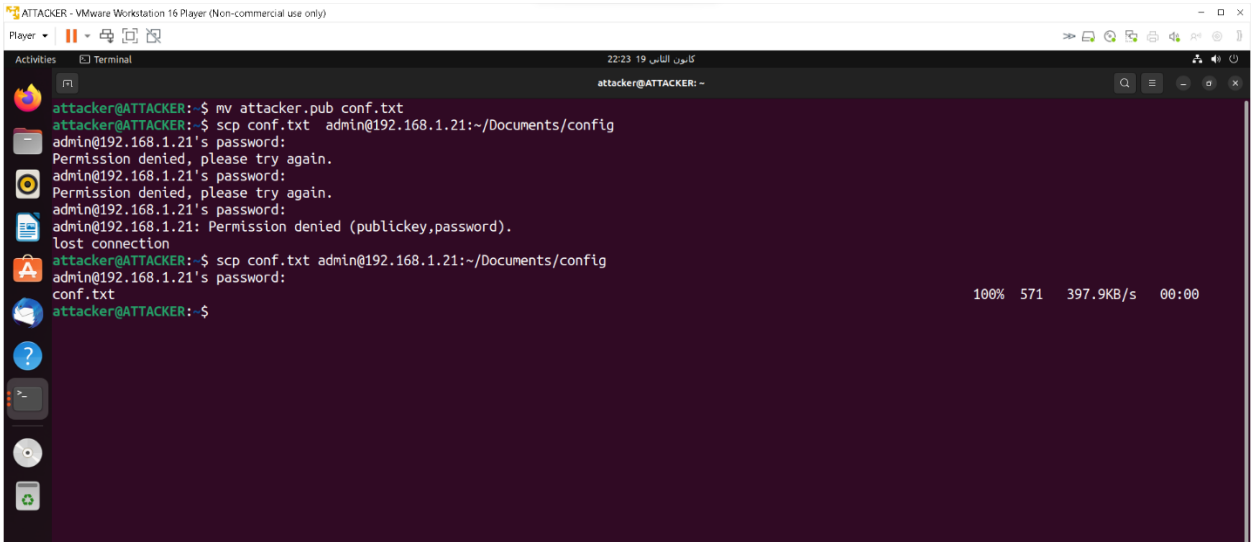
Ssh-keygen ➔ is a command-line utility in Linux and Unix operating systems that is used to generate, manage, and convert authentication keys for SSH (Secure Shell) protocol. It can be used to generate both RSA and DSA keys.

-t ➔ used to specify the type of key to be generated

Here we will generate RSA key



We will transfer it to the victim's device under a different name so as not to raise suspicion. In any case, the files will be deleted from the documents on the victim's device after the completion of the attack.

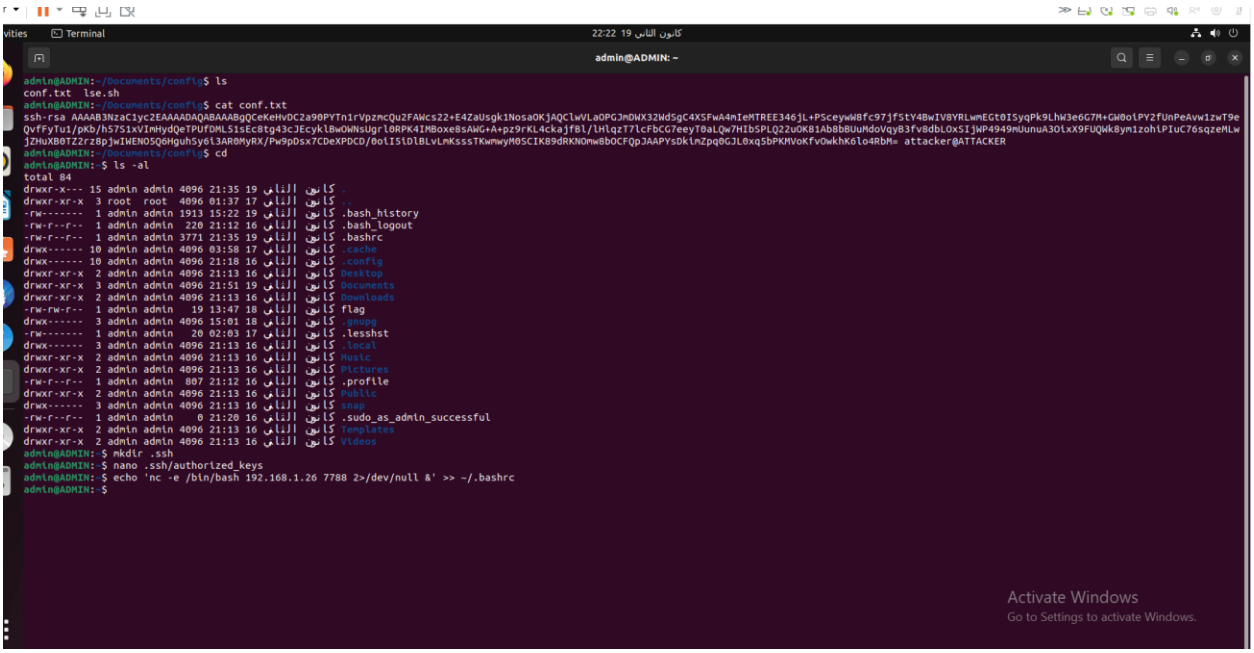


We will create a .ssh directory and an authorized_keys file since they do not exist and add the public key to it so that we can enter ssh using the private key

The ".ssh" directory is typically located in a user's home directory, and it contains the user's private and public SSH keys. The "authorized_keys" file, which is located within the ".ssh" directory, contains a list of public keys that are authorized to access the user's account via SSH.

In addition to adding a script to the. bashrc file to be installed on the hacker's machine in case ssh is closed from a victim's machine

The ".bashrc" file is a script file that is executed whenever a new instance of the Bash shell is started, including when a user logs into the system. It is typically located in the user's home directory, and it contains a list of commands and settings that are executed to configure the user's environment



The Second hack:[21]

The plan was to exploit DNS and make the hacker reliable for the victim to the company's website, and if he tries to enter it, but it doesn’t work to install dnscat2-server

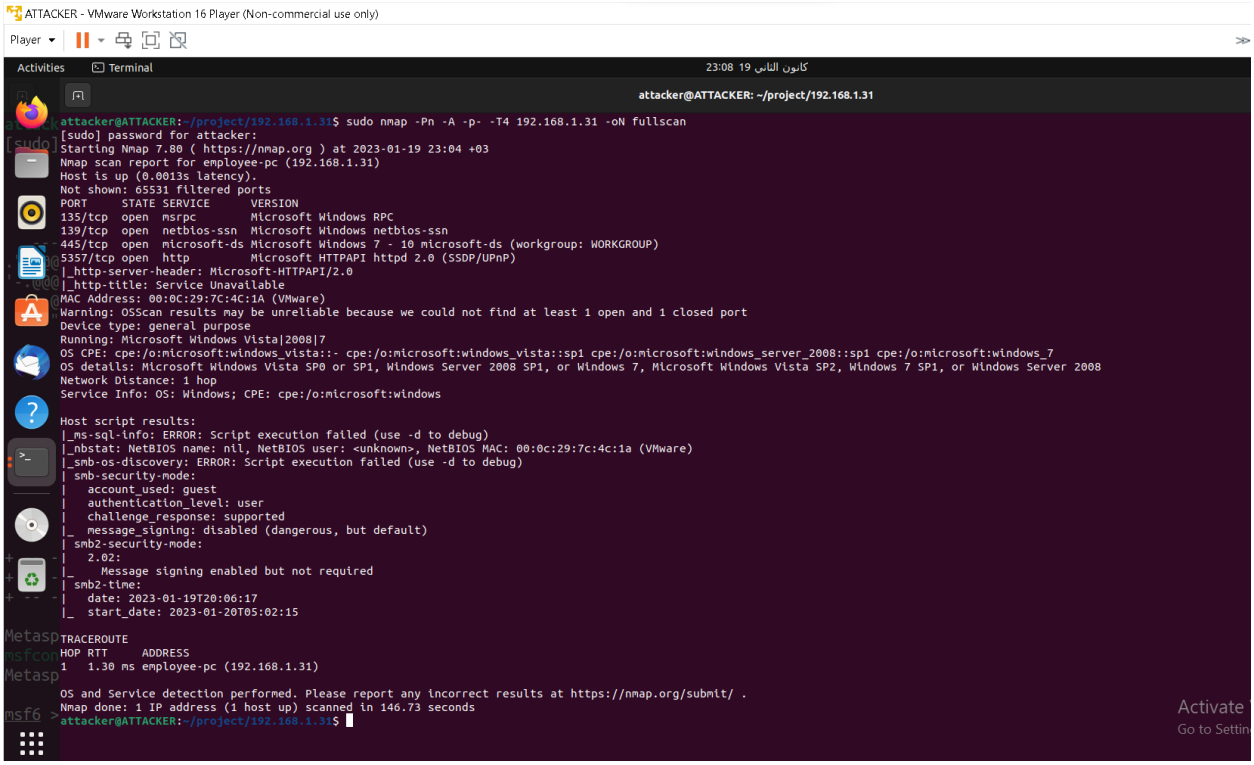
Dnscat2 is a tool used for creating a covert command and control channel using DNS (Domain Name System) as the transport mechanism.

The third hack:[22]

DNS will be directed to the hacker's device to http://attacker-ip//anything.link Because we know that there is a window 7 device through scan

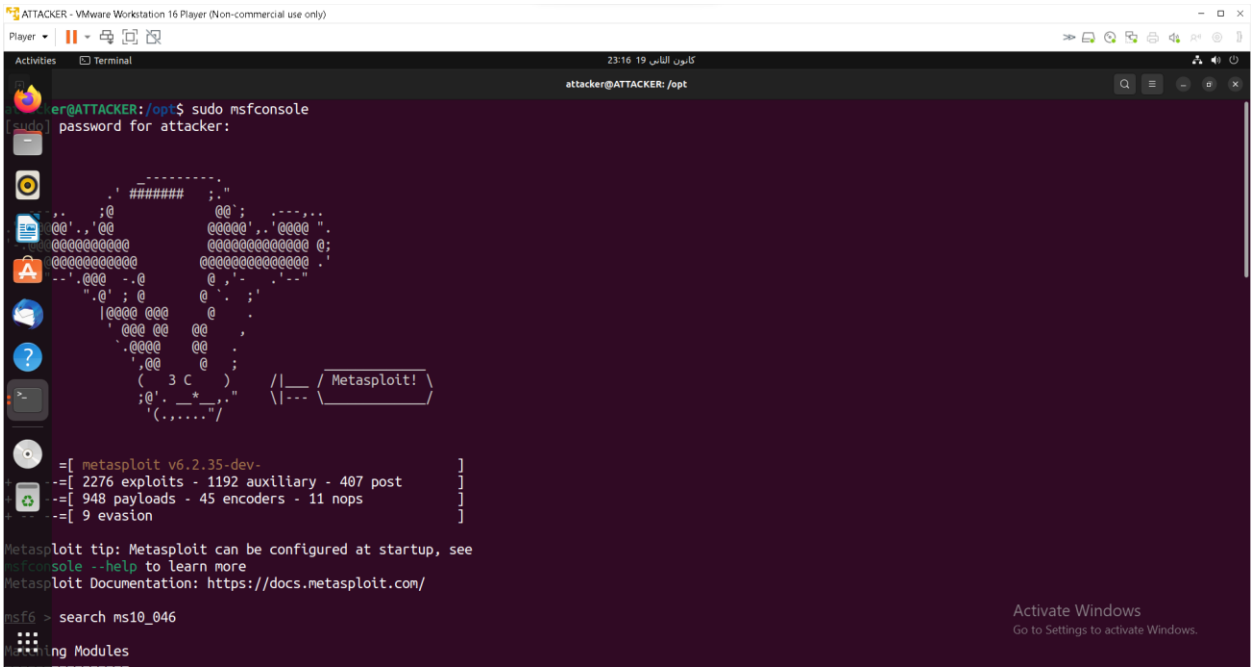
Note that the employee's device has changed its ip because the old ip, machine, was modified during the vulnerability fix, so a copy of the old machine was used to document the vulnerability, and the new ip is 192.168.1.31

We did a scan of the employee ip to increase the confirmation of the presence of vulnerabilities



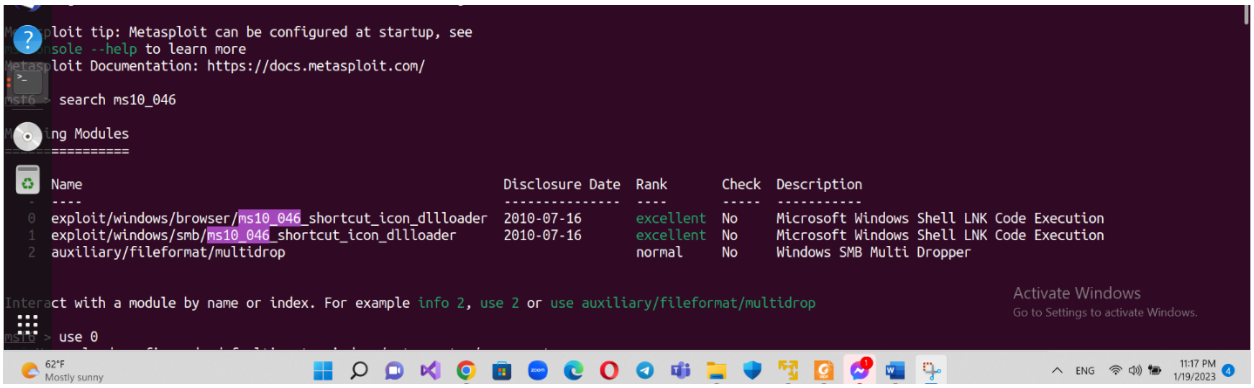
We will be using msfconsole to do this hack

Metasploit Framework Console (msfconsole) is the command-line interface of the Metasploit Framework, an open-source project that provides a platform for developing, testing, and executing exploits.



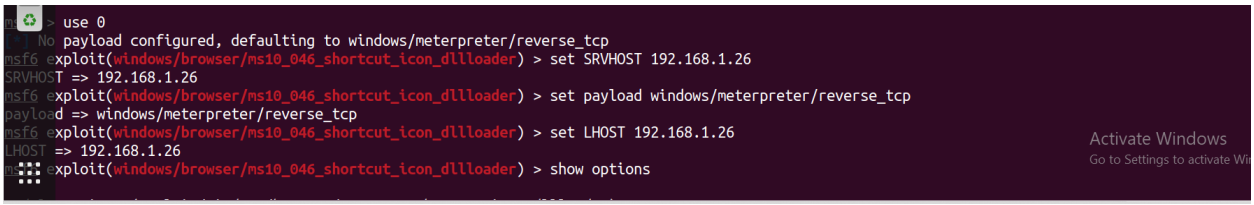
We need to use ms10_046_shortcut_icon_dllloader to exploit the vulnerability

ms10_046_shortcut_icon_dllloader is a known exploit that targets a vulnerability in the Microsoft Windows operating system. The vulnerability exists in the way that Windows handles shortcut files (with the .lnk extension) that have a specially crafted icon.



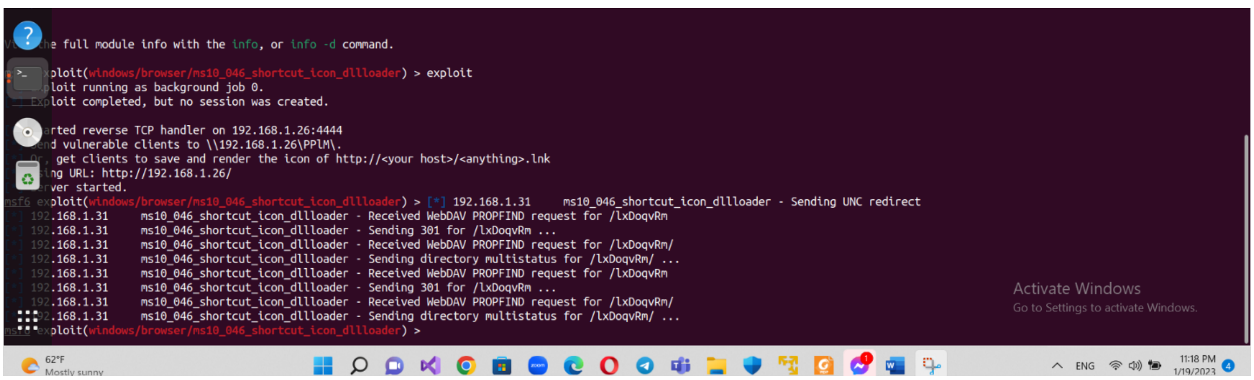
We will set the attacker's IP address as ServerHost and set payload for windows reverse shell. Of course, do not forget to change Lhost for attacker's Ip address also

A payload is the component of a cyber-attack that delivers the malicious code or action intended by the attacker.



Use the command show option to see the settings

To start the attack, we will type exploit or run



We can see that the victim opened the hacker's URL and the hacker was able to get a reverse shell on the victim's machine

To use reverse shell we need to type session then use session number Unfortunately it didn't work here for unknown reasons

The fourth hack:[23]

The completion of the scenario is that the spyware file is uploaded with the project, which will be sent to the CEO, according to what has been known from the calendar on the victim's device, in order to listen to it and take passwords for the database.

Recommendations and mitigations

- ✓ **Windows Shell Remote Code Execution Vulnerability MS10-046[15]**

  Microsoft released a security update (MS10-046) to address a Windows Shell Remote Code Execution Vulnerability.

  To protect against this vulnerability, Microsoft recommends that users apply the security update as soon as possible. The update can be downloaded from the Microsoft Download Center or installed using Windows Update. Additionally, should ensure that antivirus software is up-to-date and scan systems regularly for malicious files.

  Users should also be aware of phishing emails and websites that may contain malicious links or attachments. If an email or website appears suspicious, users should not open any attachments or click on any links contained within it. Finally, should ensure that systems are running the latest version of Windows and all other software applications installed on their systems are up to date with the latest security patches.

- ✓ **The DNS (Domain Name System) Tunneling Vulnerability [21]**

  DNS filtering is a security technique that uses DNS servers to block or allow access to specific websites or internet addresses based on predefined rules. These rules can be based on the URL or IP address of the website, the type of content on the website, or other factors.

  DNS filtering can be used to block access to known malicious websites, such as those hosting malware or phishing scams, as well as to prevent users from accessing non-work-related websites during work hours. Some organizations use DNS filtering to block access to social media, gaming, and other types of sites that are a distraction or a security risk.

  There are different ways to implement DNS filtering, some organizations use a DNS proxy or firewall, others use a specialized software or service that allows to configure the filtering rules, and some others use a combination of both.

  It's important to note that DNS filtering can be bypassed using various methods, such as using a VPN, Proxy, or other similar tools, that's why it's important to use this technique as part of a defense in depth strategy and not to rely just on this mechanism.

- ✓ **Password Pattern Vulnerability[13]**

  1. Use strong passwords: Strong passwords should include a combination of upper and lowercase letters, numbers, and special characters. Avoid using common words or phrases that can be easily guessed.

2. Implement password policies: Establish password policies that require users to change their passwords regularly and use complex passwords with a combination of upper and lowercase letters, numbers, and special characters.

3. Limit access to sensitive data: Limit access to sensitive data by assigning user roles and permissions that are appropriate for each user's job function. This will help ensure that only authorized personnel have access to confidential information.

4. Monitor user activity: Monitor user activity on your network and systems to detect any suspicious behavior or attempts at unauthorized access.

- ✓ **Social Engineering[24]**

1. Educate Employees: The first step in preventing social engineering attacks is to educate employees about the risks and how to recognize them. This can be done through training sessions, emails, or other forms of communication. Employees should be taught how to identify suspicious emails, recognize phishing attempts, and be aware of the potential for social engineering attacks.

2. Implement Security Policies: Establishing and enforcing security policies can help protect against social engineering attacks. Policies should include guidelines for handling sensitive information, such as passwords and financial data, as well as rules for using public Wi-Fi networks and other online services.

Appendices and attachments

All files containing the information found will be attached in a zip file with the report

Defensive Cybersecurity

Complete detailed analysis for the systems

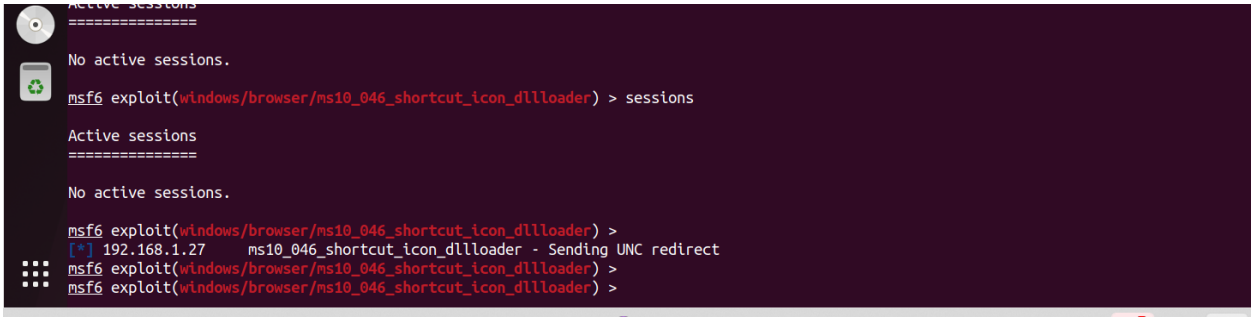
Timeline of the incidents and the attack

Fix problems and the vulnerability

Password pattern vulnerability: the password has been changed in addition to putting the police to create passwords such as complex and not including the username and to be changed every three months in addition to the presence of a password that is used for the first time only to enter the device and is changed after that

Windows Shell Remote Code Execution Vulnerability MS10-046

Microsoft released a security was update



The DNS (Domain Name System) Tunneling Vulnerability: use a DNS proxy

Social Engineering: Educate Employees

References

[1] NCSC Cybersecurity Capstone Project.pdf

[2] https://www.linkedin.com/company/vmware/?trk=public_profile_result-card_subtitle-click&originalSubdomain=jo

[3] https://docs.vmware.com/en/VMware-Workstation-Pro/17/com.vmware.ws.using.doc/GUID-BAFA66C3-81F0-4FCA-84C4-D9F7D258A60A.html

[4] https://en.wikipedia.org/wiki/Server_Message_Block

[5] https://www.cloudflare.com/learning/dns/what-is-dns/

[6] https://dev.mysql.com/doc/refman/8.0/en/what-is-mysql.html

[7] https://help.synatic.com/en/articles/4719865-http-service

[8] https://phoenixnap.com/kb/ubuntu-samba

[9] https://ubuntu.com/server/docs/service-domain-name-service-dns

[10] https://hevodata.com/learn/installing-mysql-on-ubuntu-20-04/

[11] https://devanswers.co/how-to-fix-failed-error-set-password-has-no-significance-for-user-rootlocalhost/

[12] https://faun.pub/ubuntu-servers-and-asp-net-core-project-deployment-using-nginx-d9a3a1f6ac82

[13] https://portswigger.net/web-security/authentication/password-based

[14] https://www.cloudns.net/blog/dns-tunneling-attack-what-is-it-and-how-to-protect-oursel

[15] https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046

[16] https://www.techtarget.com/searchsecurity/definition/brute-force-cracking

[17] https://resecurity.com/blog/article/shortcut-based-lnk-attacks-delivering-malicious-code-on-the-rise

[18] https://www.techtarget.com/searchsecurity/definition/spyware

[19] https://cve.mitre.org/

[20] https://www.youtube.com/watch?v=49F0co_VrTY

[21] https://www.youtube.com/watch?v=49F0co_VrTY&t=309s

[22] https://www.youtube.com/watch?v=cNJU7zAB27M&t=732s

[23] https://www.youtube.com/watch?v=5xFdCdE7TT0&t=1079s

[24] https://www.imperva.com/learn/application-security/social-engineering-attack/