Name: Vianka Lopez
Date: 9/28/25

Module 4 Project: Operating Systems and Network Security

1. Executive Summary:

Techsecure Corp faced multiple security issues in its IT Infrastructure, including weak user account policies, overly permissive shared folder access, default firewall configurations, and a flat network lacking segmentation.
To strengthen security, I:

- Implemented strong password policies and account lockout rules.
- Restricted shared folder permissions based on roles.
- Configured Windows Defender Firewall to only allow HTTPS (443) and RDP (3389)
- Applied pending Windows updates to patch vulnerabilities
- (Optional) Hardened the Ubuntu server by disabling root SSH login, enforcing key-based authentication, and correcting file permissions.
- Segmented the network into VLANs for Admin, HR, IT, and Guest users and applied Access Control Lists (ACLs) to enforce company access policies.
- Verified configurations using PowerShell, ping, and Cisco CLI commands.

These steps significantly improved system and network security, reduced risks of unauthorized access, and optimized network performance.

2. System Hardening Report

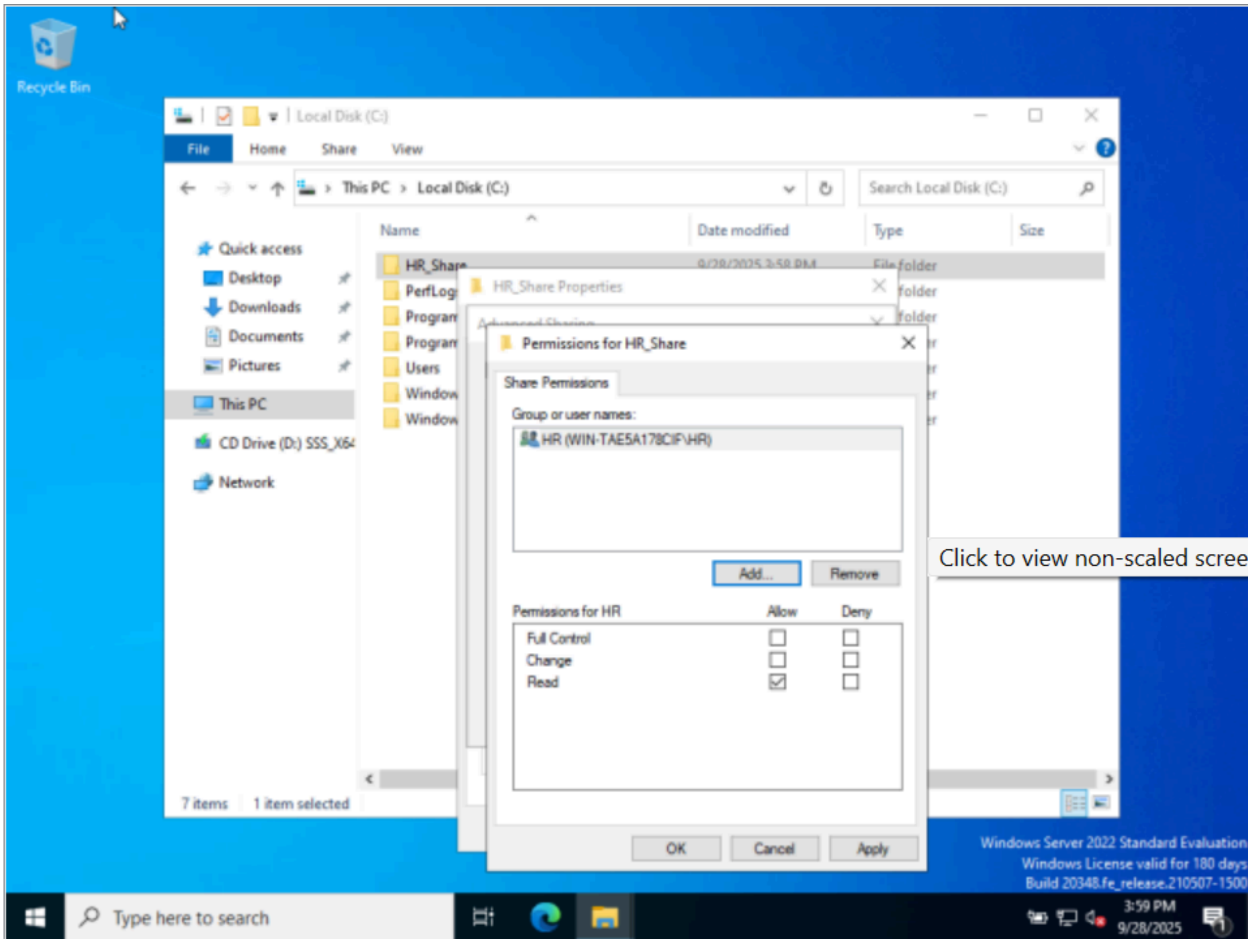
2.1 Windows Server Hardening

a. User Account Security
    - Password Policies Implemented:
        - Minimum Length: 8 Characters
        - Password complexity: Enabled
        - Maximum age: 60 days
        - Account lockout after 3 failed attempts

b. Shared Folder Security
    - Before: All folders accessible to “Everyone”
    - After” Folders restricted based on role (HR→HR folder only, Admin→Admin folder, etc.)

Table of Permissions

Folder	**Before**	**After**
HR	Everyone	HR Group Only
IT	Everyone	IT Group Only
Admin	Everyone	Admin Group Only



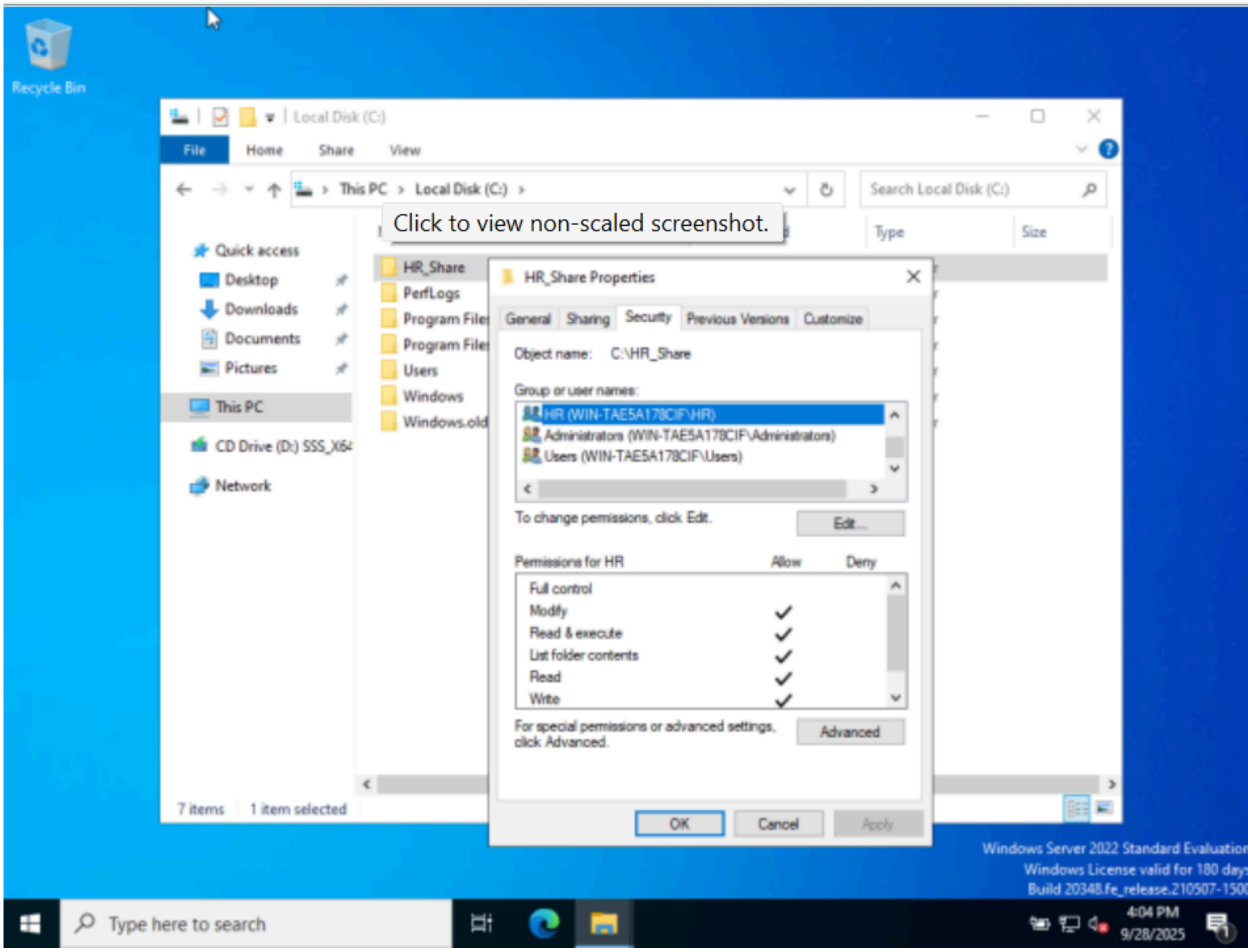
Permissions for HR_Share

Share Permissions

Group or user names:

HR (WIN-TAE5A178CIF\HR)

Permissions for HR	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□



HR_Share Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\HR_Share

Group or user names:

- HR (WIN-TAE5A178CIF\HR)
- Administrators (WIN-TAE5A178CIF\Administrators)
- Users (WIN-TAE5A178CIF\Users)

To change permissions, click Edit. [Edit...]

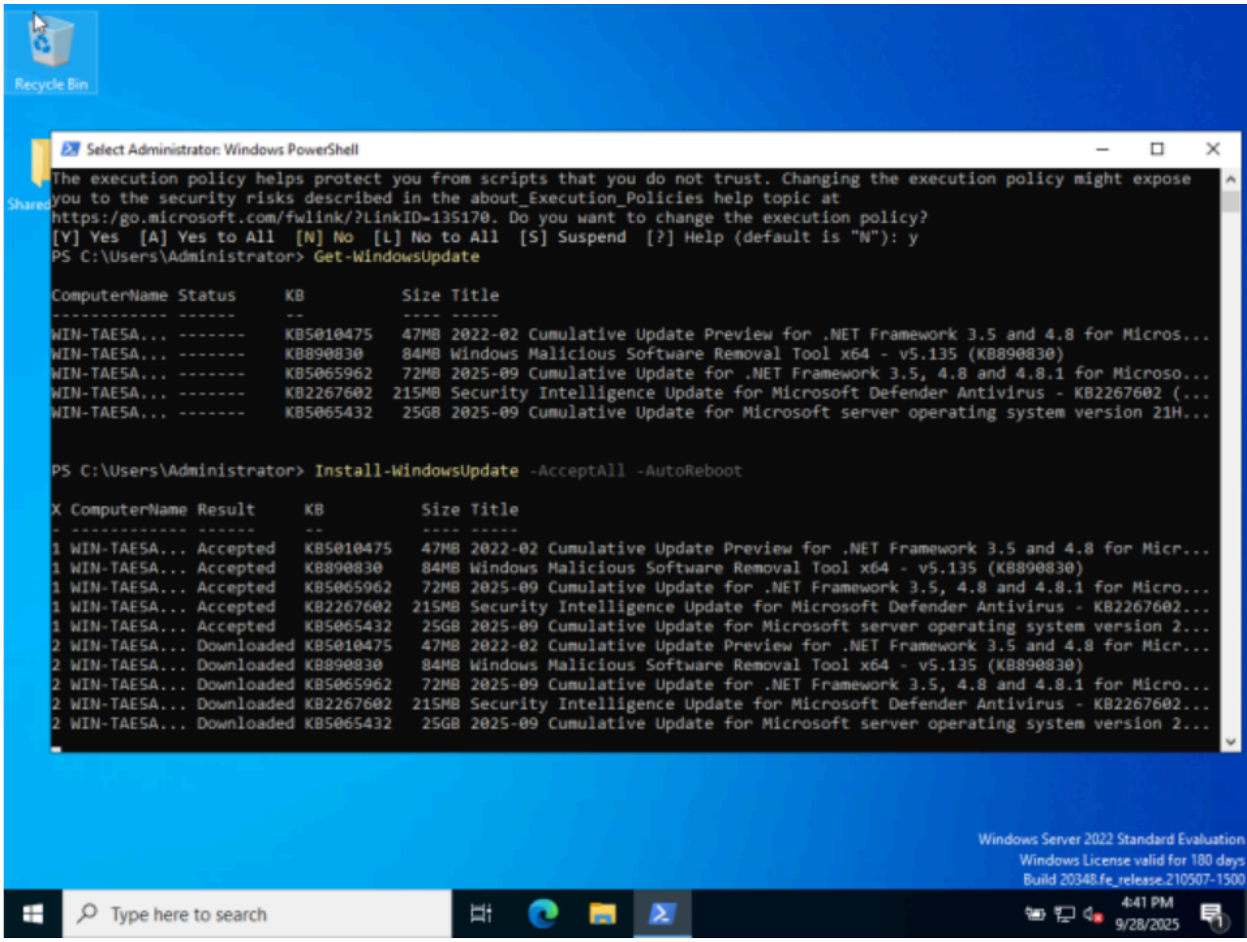
Permissions for HR	Allow	Deny
Full control		
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. [Advanced]

[OK] [Cancel] [Apply]

Verification: test results showing only authorized users could access folders

c. Windows Firewall Configuration
   - ○ Allowed services: HTTPS (443), RDP (3389)
   - ○ Blocked services: FTP (21), HTTP (80), others not in use


Recycle Bin
Shared
Select Administrator: Windows PowerShell
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500
Type here to search
4:41 PM
9/28/2025

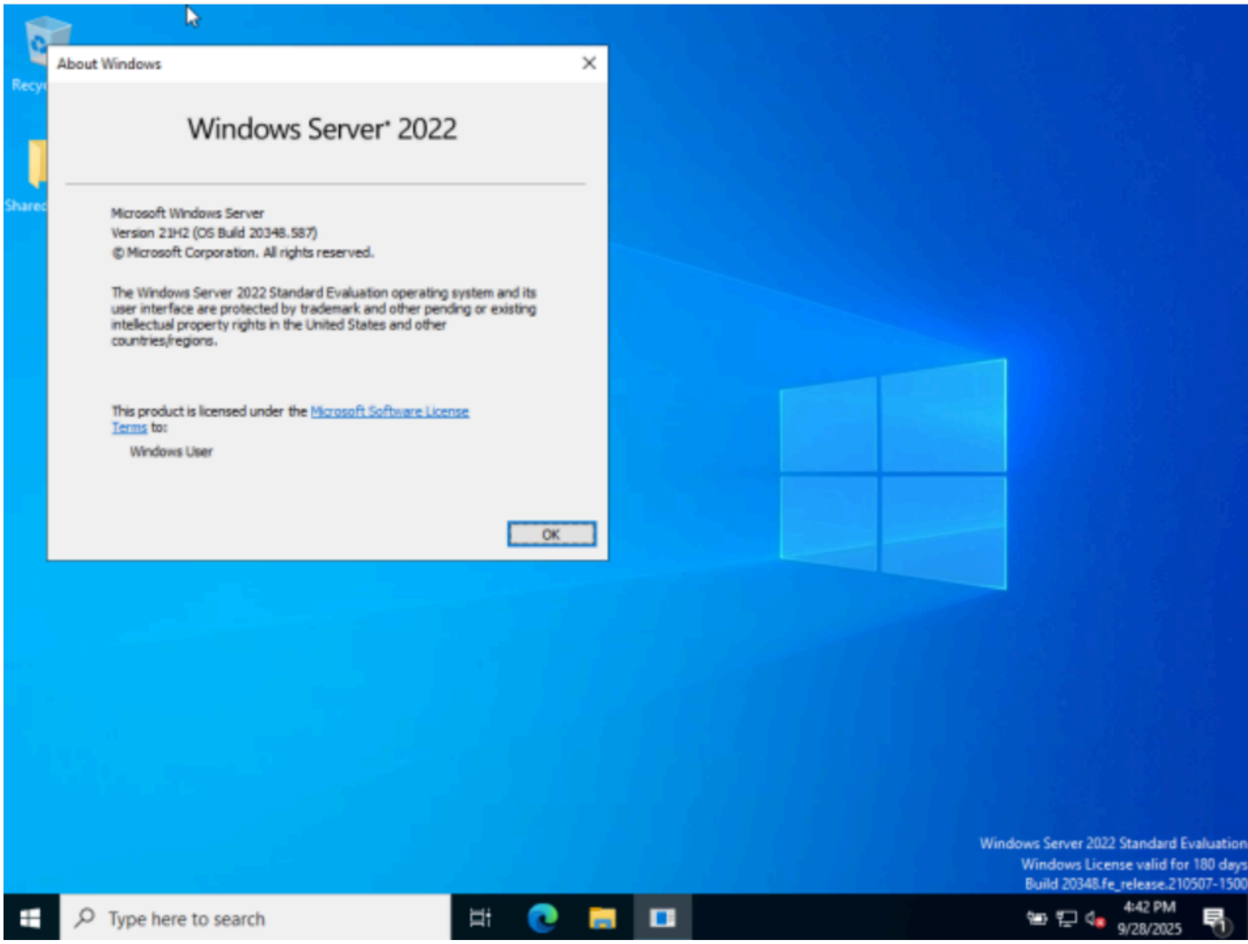
```
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https:/go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\Users\Administrator> Get-WindowsUpdate

ComputerName Status     KB          Size Title
------------ ------     --          ---- -----
WIN-TAE5A... -------    KB5010475   47MB 2022-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Micros...
WIN-TAE5A... -------    KB890830    84MB Windows Malicious Software Removal Tool x64 - v5.135 (KB890830)
WIN-TAE5A... -------    KB5065962   72MB 2025-09 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Microso...
WIN-TAE5A... -------    KB2267602  215MB Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (...
WIN-TAE5A... -------    KB5065432   25GB 2025-09 Cumulative Update for Microsoft server operating system version 21H...


PS C:\Users\Administrator> Install-WindowsUpdate -AcceptAll -AutoReboot

X ComputerName Result     KB          Size Title
- ------------ ------     --          ---- -----
1 WIN-TAE5A... Accepted   KB5010475   47MB 2022-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Micr...
1 WIN-TAE5A... Accepted   KB890830    84MB Windows Malicious Software Removal Tool x64 - v5.135 (KB890830)
1 WIN-TAE5A... Accepted   KB5065962   72MB 2025-09 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Micro...
1 WIN-TAE5A... Accepted   KB2267602  215MB Security Intelligence Update for Microsoft Defender Antivirus - KB2267602...
1 WIN-TAE5A... Accepted   KB5065432   25GB 2025-09 Cumulative Update for Microsoft server operating system version 2...
2 WIN-TAE5A... Downloaded KB5010475   47MB 2022-02 Cumulative Update Preview for .NET Framework 3.5 and 4.8 for Micr...
2 WIN-TAE5A... Downloaded KB890830    84MB Windows Malicious Software Removal Tool x64 - v5.135 (KB890830)
2 WIN-TAE5A... Downloaded KB5065962   72MB 2025-09 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Micro...
2 WIN-TAE5A... Downloaded KB2267602  215MB Security Intelligence Update for Microsoft Defender Antivirus - KB2267602...
2 WIN-TAE5A... Downloaded KB5065432   25GB 2025-09 Cumulative Update for Microsoft server operating system version 2...
```

d. System Updates and Patching
   - Applied all critical updates



About Windows

Windows Server® 2022

Microsoft Windows Server
Version 21H2 (OS Build 20348.587)
© Microsoft Corporation. All rights reserved.

The Windows Server 2022 Standard Evaluation operating system and its user interface are protected by trademark and other pending or existing intellectual property rights in the United States and other countries/regions.

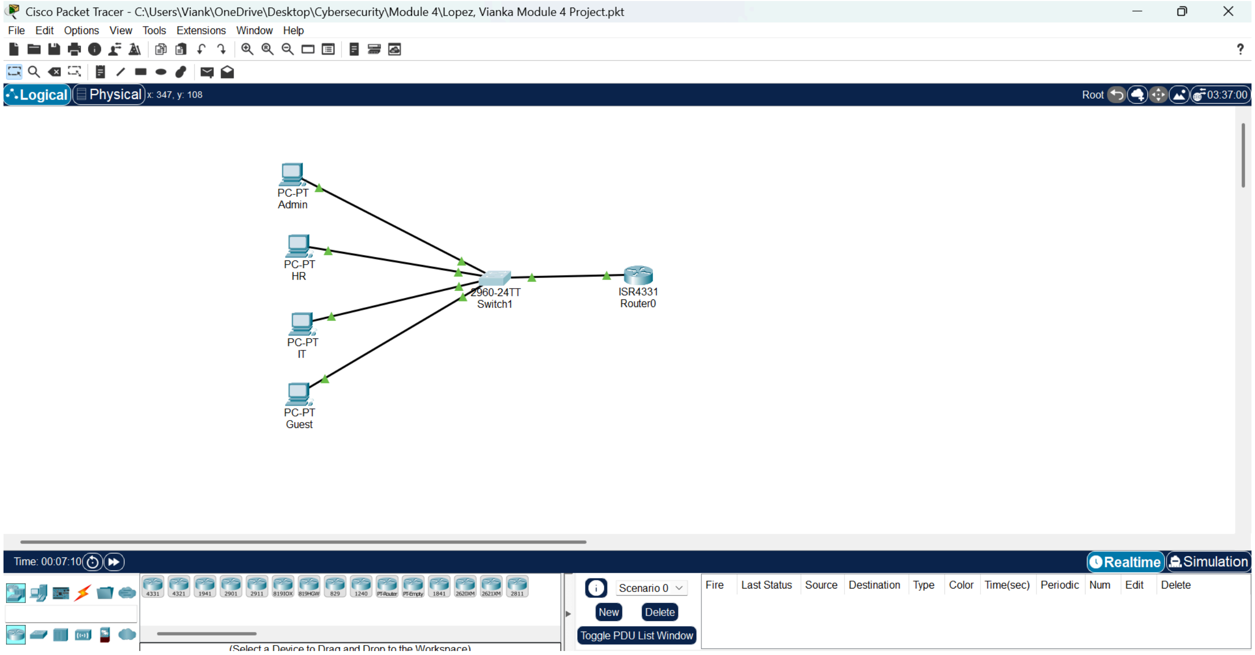
This product is licensed under the Microsoft Software License Terms to:
Windows User

OK

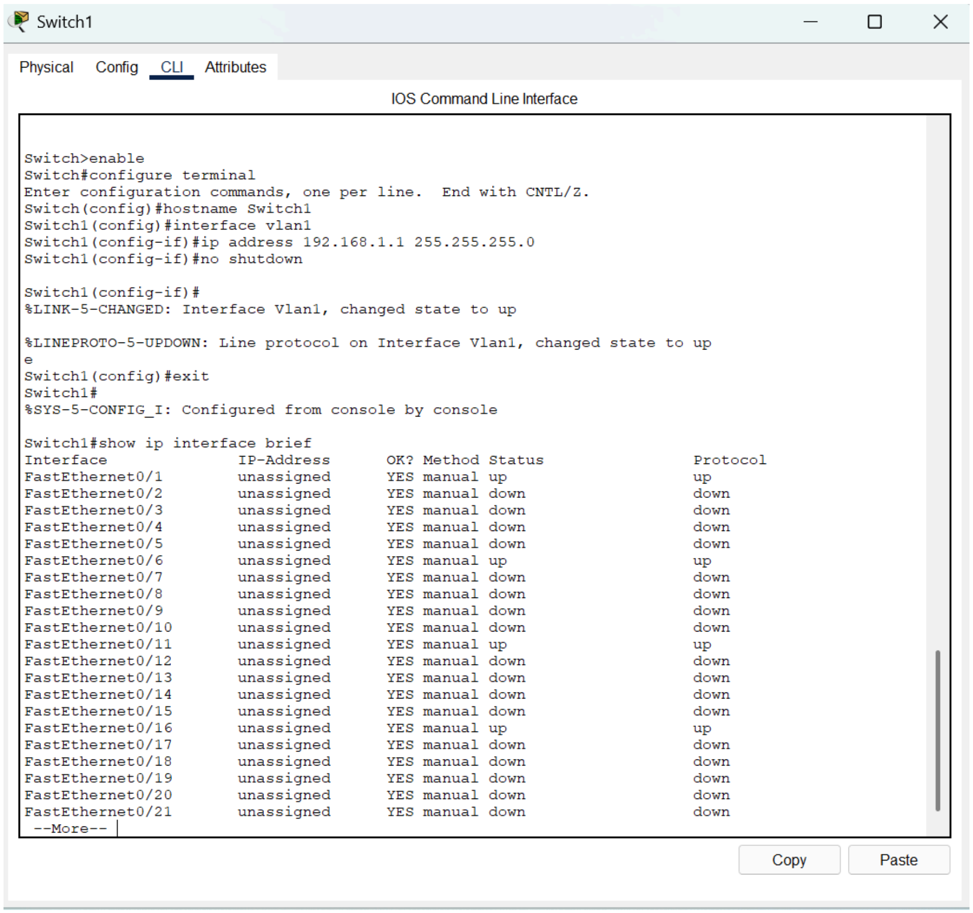
Windows Server 2022 Standard Evaluation
Windows License valid for 180 days
Build 20348.fe_release.210507-1500

3. Network Security with VLANs and ACLs

a. VLANs Created:
   - VLAN 10→ Admin
   - VLAN 20→ HR
   - VLAN 30→ IT
   - VLAN 40→ Guest



b. ACL Rules:
  - Admin VLAN can reach HR and IT VLANs
  - HR VLAN connot reach Admin or IT VLANs
  - Guest VLAN only allowed internet access

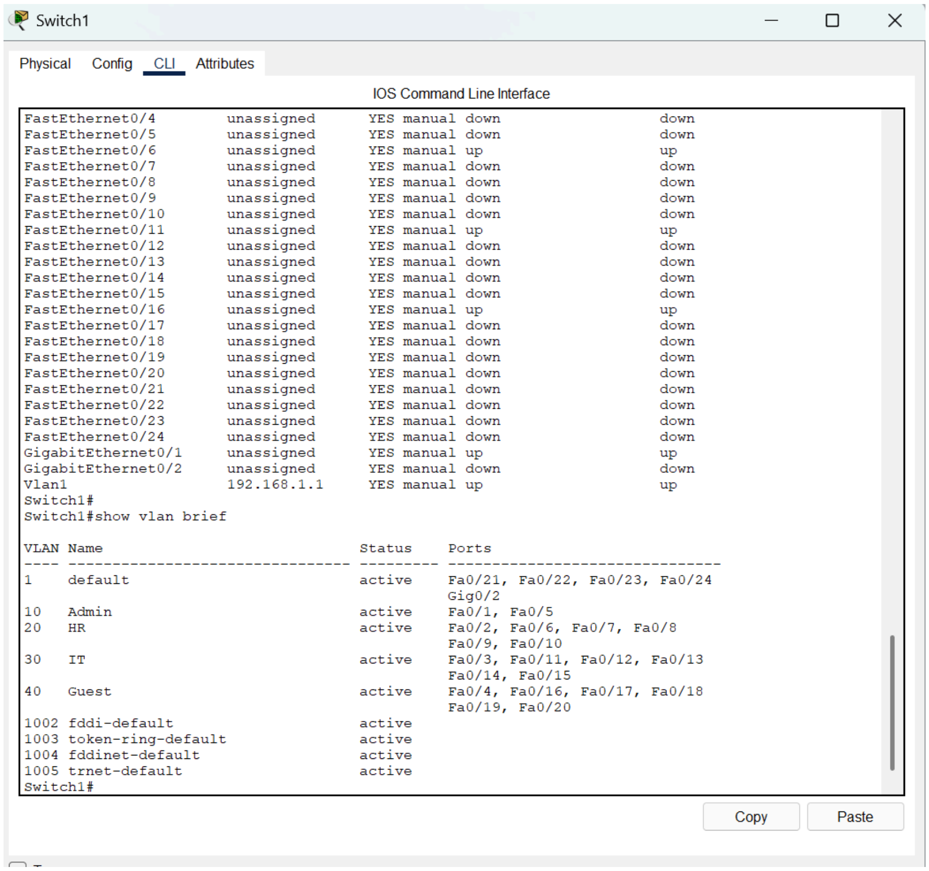


```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Switch1
Switch1(config)#interface vlan1
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown

Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
e
Switch1(config)#exit
Switch1#
%SYS-5-CONFIG_I: Configured from console by console

Switch1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual down                  down
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual up                    up
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
 --More--
```

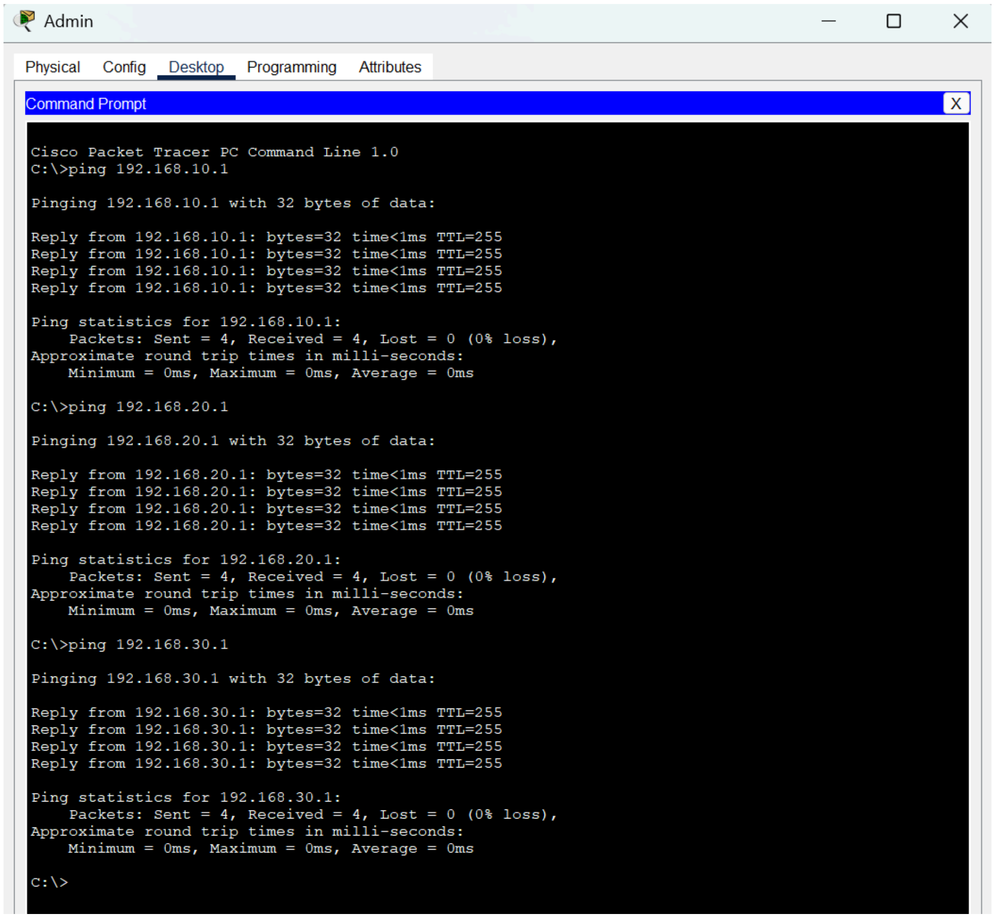


```
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual up                    up
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual up                    up
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual up                    up
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual up                    up
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.1     YES manual up                    up
Switch1#
Switch1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/2
10   Admin                            active    Fa0/1, Fa0/5
20   HR                               active    Fa0/2, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10
30   IT                               active    Fa0/3, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15
40   Guest                            active    Fa0/4, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch1#
```

c. VLAN Isolation Testing

- Ping results:
  - Admin→ HR Allowed
  - HR→Admin Blocked
  - Guest→Internal Blocked
  - Guest → internet Allowed



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:

Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255
Reply from 192.168.20.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.30.1

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

4. Lessons Learned

- Learned how to configure password policies and enforce role-based access.
- Practiced securing Windows Firewall with PowerShell and GUI tools
- Understood how to secure SSH access on Linux and apply least-privilege file permissions
- Gained hands-on experience configuring VLANs and ACLs in Cisco Packet Tracer
- Saw how testing with tools like ping and Nmap validates security controls

5. References:

- Microsoft Docs -Windows Server Group Policy
- Cisco CLI Configuration Guide- VLANs and ACLs
- Coding Temple Module 4 Learning Resources