Securing the Network Infrastructure

(CompTIA Security + SY – 601)

Objectives:

- To analyze potential indicators associated with network attacks
- To implement secure protocols
- To implement host or application solutions
- To implement secure network designs

Resources:

- Windows Virtual Machine (DC1 & MS1)
- Centos LX1 VM
- PT1-Kali VM
- VPN
- SSH server

Instructions:

Configure secure SSH connectivity

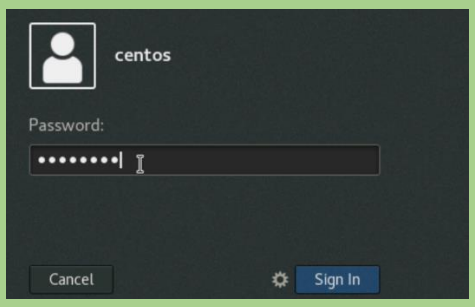
- On the **PT1-Kali** VM
- Run nmap scan to display the VM's own open ports: **nmap 10.1.0.10 -p 22**

```
root@KALI:~# nmap 10.1.0.10 -p 22
Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-06 08:53 PDT
Warning: File ./nmap.xsl exists, but Nmap is using /usr/bin/../share/nmap/nmap.xsl f
or security and consistency reasons.  set NMAPDIR=. to give priority to files in you
r local directory (may affect the other data files too).
Nmap scan report for 10.1.0.10
Host is up (0.00061s latency).
```

- Open a terminal and then establish an SSH connection as the **centos** user to **10.1.0.10**

```
root@KALI:~# ssh centos@10.1.0.10
The authenticity of host '10.1.0.10 (10.1.0.10)' can't be established.
ECDSA key fingerprint is SHA256:wiVs+DWxrxmIJtODINs4M1bj2eLHvupbmZ2oKqpaAqM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.1.0.10' (ECDSA) to the list of known hosts.
centos@10.1.0.10's password:
Last login: Tue Jun 18 09:49:59 2019
```

- Disconnect from the LX1 SSH server
- Switch to the **LX1 SSH** server sign-in with the preconfigured **centos** account and a password of **Pa$$w0rd**



- Open a terminal and then elevate your credentials to root **su – root**

```
[centos@lx1 ~]$ su - root
Password:
Last login: Thu Dec 13 08:03:11 PST 2018 on pts/0
[root@lx1 ~]#
```

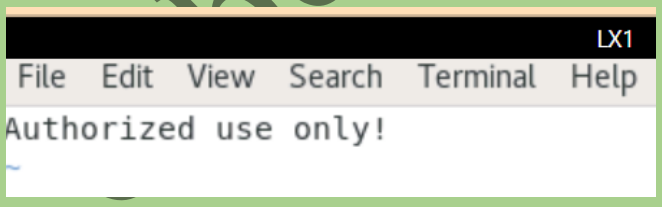
- Type **Pa$$w0rd** when prompted
- Use Vim text editor to edit the **/etc/ssh/sshd_config** SSH configuration file

```
[root@lx1 ~]# vim /etc/ssh/sshd_config
```

- Edit the SSH configuration file to implement the following SSH configurations defined by your company's written security policy:

  - Empty passwords are not allowed for SSH authentication. **Disable the empty password** option.
  - Uncomment the **Banner** line and type **/etc/issue.net** as the banner file path.

- Save your changes by pressing ESC in vim, and then typing **:wq**
- Use Vim to edit the **/etc/issue.net** file. Remove all of the existing content in the file, and then add the following warning: **Authorized use only!**



- Press **ESC** in vim, and then type **:wq** to save your changes to the **/etc/issue.net** file and then exit vim
- In the terminal, run the **systemctl restart sshd** command to restart the SSH service
- Switch to the **PT1-Kali SSH** client VM

```
[root@lx1 ~]# systemctl restart sshd
```

- Attempt the SSH connection by using the centos credentials. Use **Pa$$w0rd** as the password ssh centos@10.1.0.10

```
root@KALI:~# ssh centos@10.1.0.10
Authorized use only!
centos@10.1.0.10's password:
Last login: Tue Aug  6 08:59:49 2024
[centos@lx1 ~]$
```

- Type **exit** to disconnect from the remote LX1 SSH server
- Switch to the **LX1**. If the VM's privacy screen is enabled, press ENTER and sign-in
- If a Terminal window is not already open, right-click on the desktop, and select Open Terminal
- To test log file functionality, run the following command to generate an entry in the **/var/log/messages** log files: **logger "test message"**

```
[root@lx1 ~]# logger "test message"
You have new mail in /var/spool/mail/root
```

- Run the following command to view the lines at the bottom of the **/var/log/messages** log file: **tail /var/log/messages**

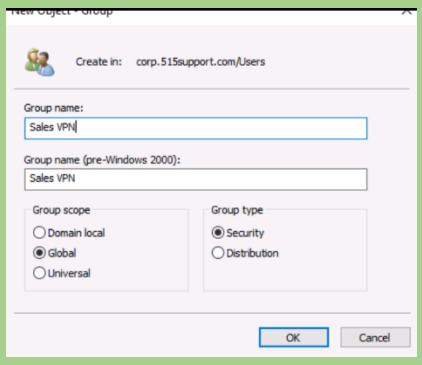
```
[root@lx1 ~]# tail /var/log/messages
Aug  6 09:13:27 lx1 dbus[2405]: [system] Activating service name='org.fedoraproj
ect.Setroubleshootd' (using servicehelper)
Aug  6 09:13:27 lx1 systemd: Started Session 9 of user centos.
Aug  6 09:13:27 lx1 systemd-logind: New session 9 of user centos.
Aug  6 09:13:27 lx1 dbus[2405]: [system] Activating service name='org.freedeskto
p.problems' (using servicehelper)
Aug  6 09:13:27 lx1 dbus[2405]: [system] Successfully activated service 'org.fre
edesktop.problems'
```

- Run the following command to display the lines at the bottom of the **/var/log/secure** log file: **tail /var/log/secure | grep -i ssh**

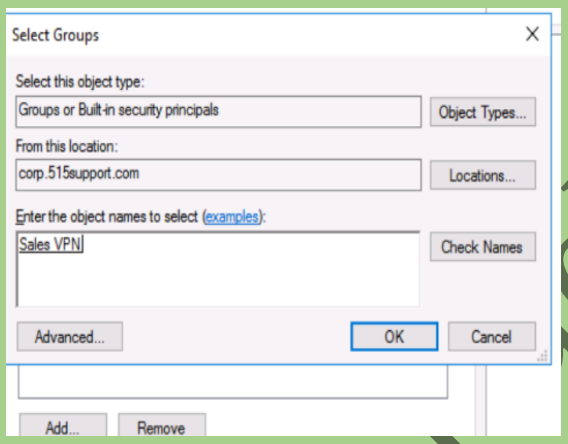
```
[root@lx1 ~]# tail /var/log/secure | grep -i ssh
Aug  6 09:13:27 lx1 sshd[5836]: Accepted password for centos from 10.1.0.192 por
t 59172 ssh2
Aug  6 09:13:27 lx1 sshd[5836]: pam_unix(sshd:session): session opened for user
centos by (uid=0)
Aug  6 09:14:35 lx1 sshd[5850]: Received disconnect from 10.1.0.192 port 59172:1
1: disconnected by user
Aug  6 09:14:35 lx1 sshd[5850]: Disconnected from 10.1.0.192 port 59172
Aug  6 09:14:35 lx1 sshd[5836]: pam_unix(sshd:session): session closed for user
centos
```

Configure the VPN server

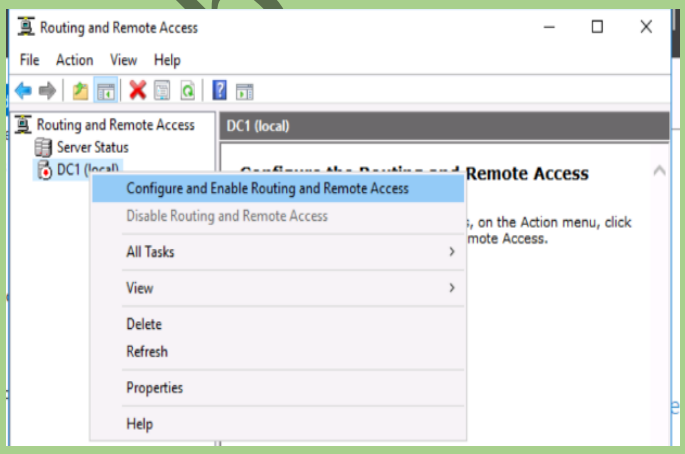
- Sign-in to the DC1 VM
- Use **Active Directory Users and Computers** to create a new global security group in the **Users** container named **Sales VPN**



- Add **Bobby** to the **Sales VPN** group



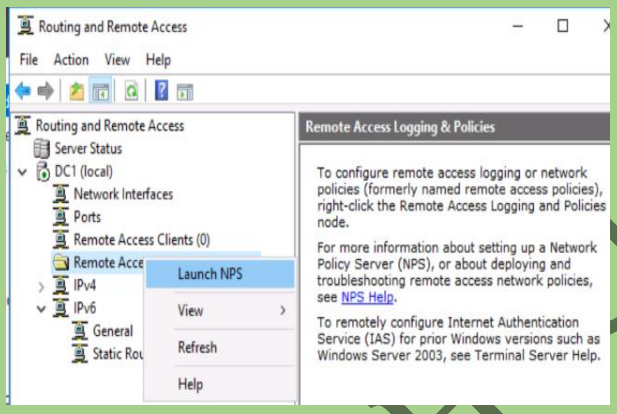
- Close Active Directory Users and Computers after adding Bobby to the Sales group
- In Server Manager, select **Tools > Routing and Remote Access**. Right-click **DC1 (local)** and then select **Configure and Enable Routing and Remote Access**



- Set the following configurations in the wizard

- **Remote access (dial-up or VPN)**
- **VPN**
- Select the **INTERNET** interface as the Internet connection.
- Accept all remaining defaults.
- Acknowledge the policy message and DHCP notification when prompted.

- Select and then right-click **Remote Access Logging & Policies** and then select **Launch NPS**



- Select the **Network Policies** node
- Create a new policy by right-clicking the Network Policies node. Use the following settings (unless otherwise stated, accept the defaults):

- Policy name: T Sales VPN access
- Type of network access server: **Remote Access Server(VPN-Dial up)**
- Conditions: select **User Groups** and then add the T Sales VPN group
- Specify Access Permission: **Access Granted**
- Configure Authentication Methods: check the box for **Encrypted authentication (CHAP)** and leave the MS-CHAP and MS-CHAPv2 boxes at their default (checked)
- Acccept all remaining defaults, and then select **Finish**

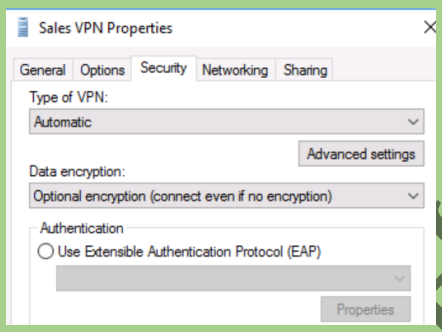
- Observe the new policy in the **Network Policies console**

Configure the VPN client

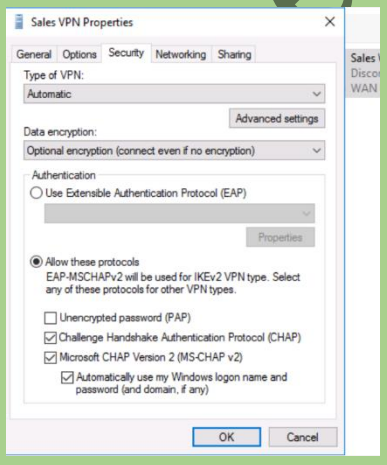
- Switch to the **MS1** Virtual Machine
- Sign-in as **Bobby** using **Pa$$w0rd** as the password
- Open **Network settings** and from the **Settings** page, select **VPN** and then select Add a VPN **connection**. Configure the following values:

  - VPN provider: **Windows (built-in)**
  - Connection name: Sales VPN
  - Server name or address: 10.1.0.1
  - VPN type: **Automatic**
  - Type of sign-in info: **User name and password**
  - User name (optional): 515support\bobby
  - Password (optonal): Pa$$w0rd
  - When all values are configured, select **Save**.

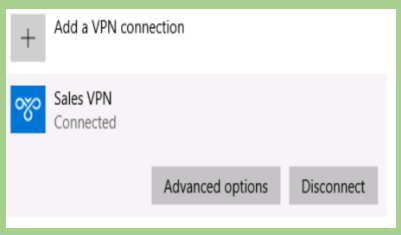
- In the Settings window, select the link for **change adapter options**
- Right-click the **Sales VPN**, select **Properties** and then select **Security** tab



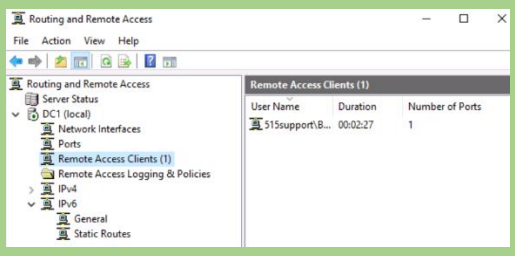
- Select the radio button for **Allow these protocols**, and then check the boxes for the following protocols



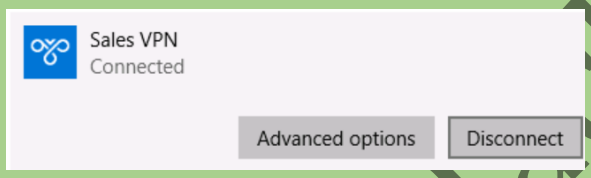
- Select OK to close the **Sales VPN** adapter properties. When prompted, confirm the changes
- On the network Settings page, select the Sales VPN icon, and then select connect



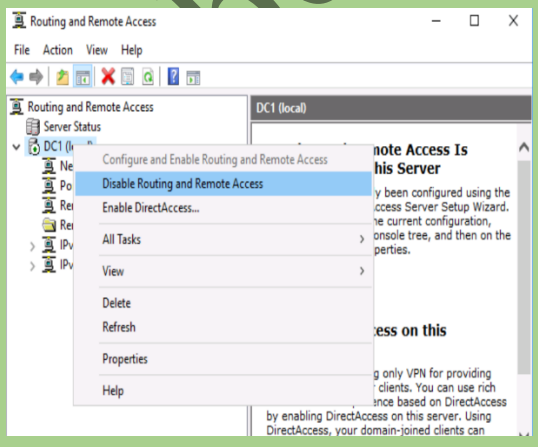
- Switch to DC1, select the **Routing and Remote Access** console
- View the active connections in the **Remote Access Clients** page



- Return to the **MS1** VM, and then disconnect the VPN connections

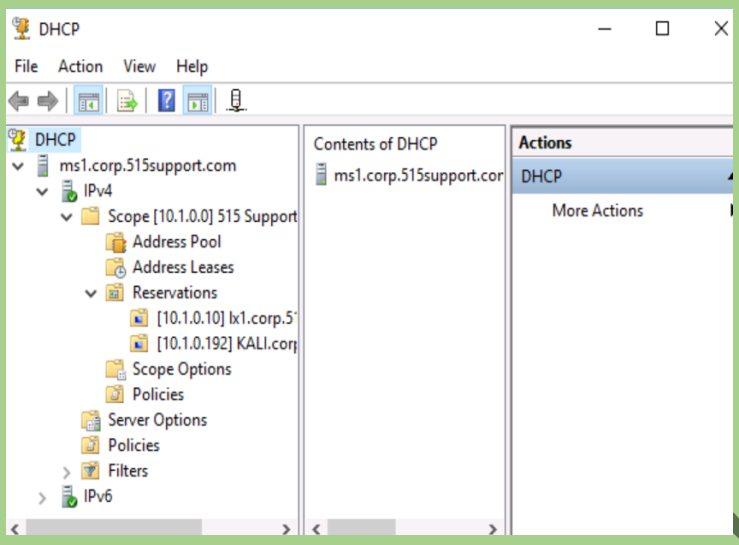


- Sign out of the **MS1** VM. In the next task you will sign-in as the Administrator, instead of Bobby
- Select the DC1 VM
- In the Routing and Remote Access console, right-click the **DC1 (local)** server, and then select **Disable Routing and Remote Access**. When prompted, confirm action

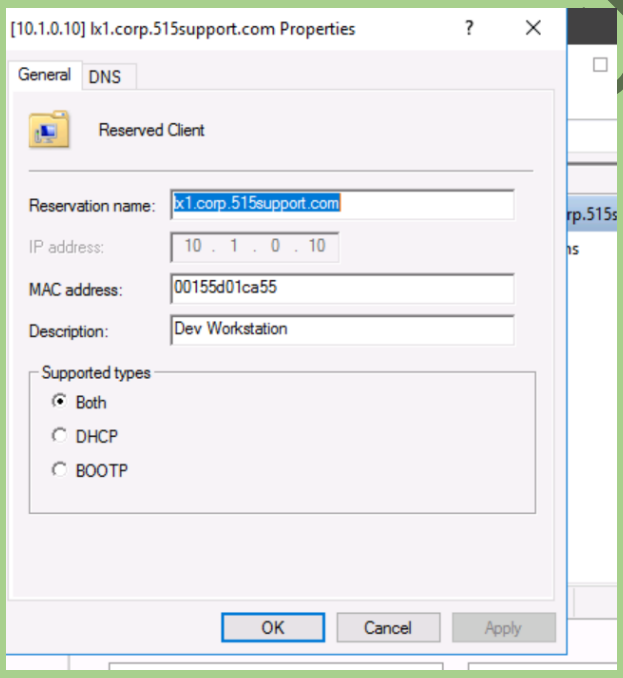


Implement network addressing security configurations

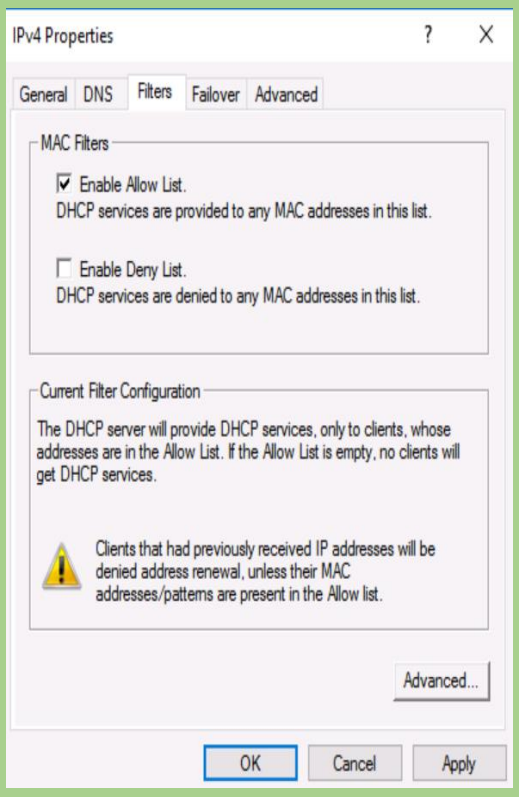
- Select **MS1** VM
- Make sure you are not signed-in as Bobby
- Launch your DHCP console



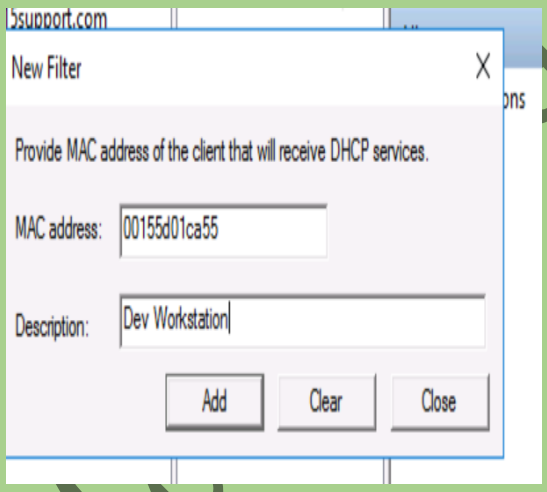
- In the scope [10.1.0.0] 515Support Scope display the properties of the reservation for the LX1 VM. Accomplish the following tasks:



- Select the **Properties** of the IPv4 node. On the Filter tab, check the **Enable Allow List** box. Select **OK**

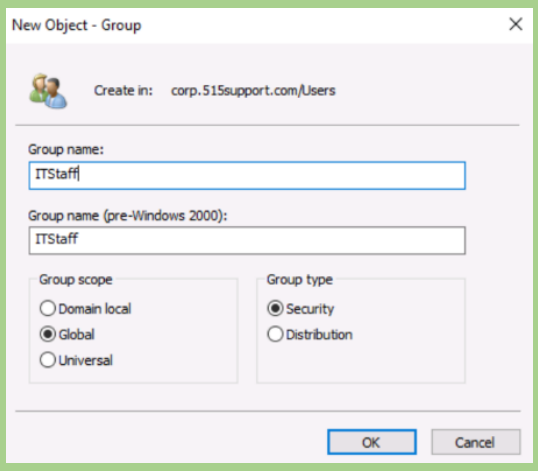


- In the Filter > Allow node, right-click and select **New Filter**. Accomplish the following tasks

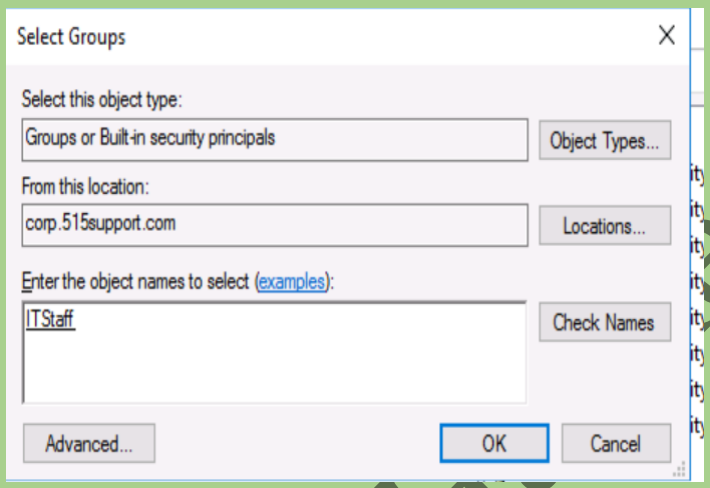


Create a fine-grained password policy for IT staff accounts

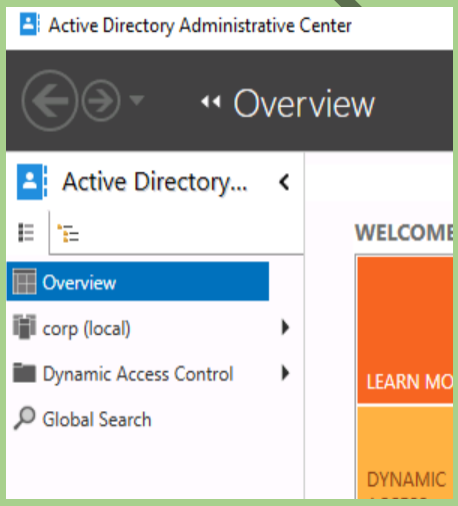
- Switch to the **DC1** VM
- Open the **Active Directory Users and Computers** console, and then create a new ITStaff group



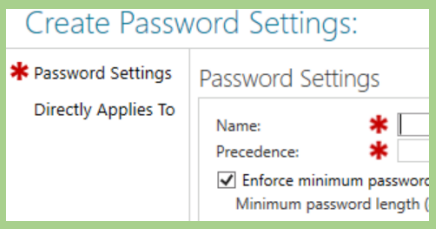
- Add the **Domain Admins** and **Local Admin** objects to the New ITStaff group



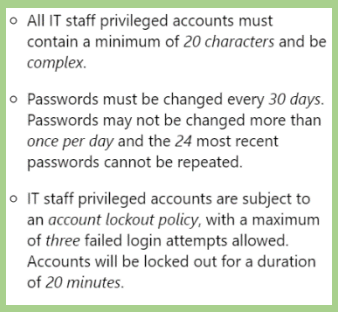
- Close the Active Directory Users and Computers
- Open the **Active Directory Administrative Center** console



- In the left-hand pane, select **corp(local) > System > Password Settings Container**



- Review the following security policy summary for IT staff account password management



- Create a password policy named **IT Account Policy** that meets the requirements listed in the security policy. Set a precedence level of **10** on the policy
- Under Directory Applies To, add the **ITStaff** group

Observations:

- **SSH Configuration**: The SSH configuration file was edited to implement company-defined security policies and to display an "Authorized use only!" warning.
- **Log File Entries**: Commands were executed to generate and view log file entries in /var/log/messages and /var/log/secure.
- **VPN Configuration**: A new global security group named Sales VPN was created, and a VPN connection was configured and tested on the MS1 VM.
- **Network Addressing Security**: DHCP configurations were adjusted to enable an allow list and new filters for enhanced security.
- **Password Policy Implementation**: A fine-grained password policy for IT staff accounts was created and applied in the Active Directory Administrative Center.

Results:

- **Successful SSH Configuration**: SSH service was secured according to the company's policies, including the display of a security warning.
- **Log File Verification**: Log files accurately recorded SSH connection attempts and other activities, verifying logging functionality.
- **VPN Connectivity**: The VPN setup was successful, allowing secure remote access and validating the configurations made in the Sales VPN group.

- **Enhanced DHCP Security**: Network addressing security was improved by implementing filters and enabling the allow list on the DHCP server.
- **Effective Password Policy**: The newly created password policy for IT staff was successfully applied, meeting the security requirements and precedence level.

Conclusion:

The practical exercise successfully demonstrated the implementation and verification of various network security measures, including SSH configuration, log file management, VPN setup, network addressing security, and password policy enforcement. Each step was executed according to the provided instructions, resulting in a more secure network infrastructure.

Future Work:

- **Automate Security Configurations**: Develop scripts to automate the configuration of SSH, VPN, and DHCP settings to reduce manual intervention and potential errors.
- **Regular Security Audits**: Implement routine audits and monitoring to ensure continuous compliance with security policies and to detect any unauthorized changes.
- **Expand Security Policies**: Extend the fine-grained password policies and other security measures to additional user groups and network devices to further enhance overall security.