Scenario:

Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as our first InfoSec employee! Once you are settled in and finished orientation, we have your first 2-Weeks assignments ready.

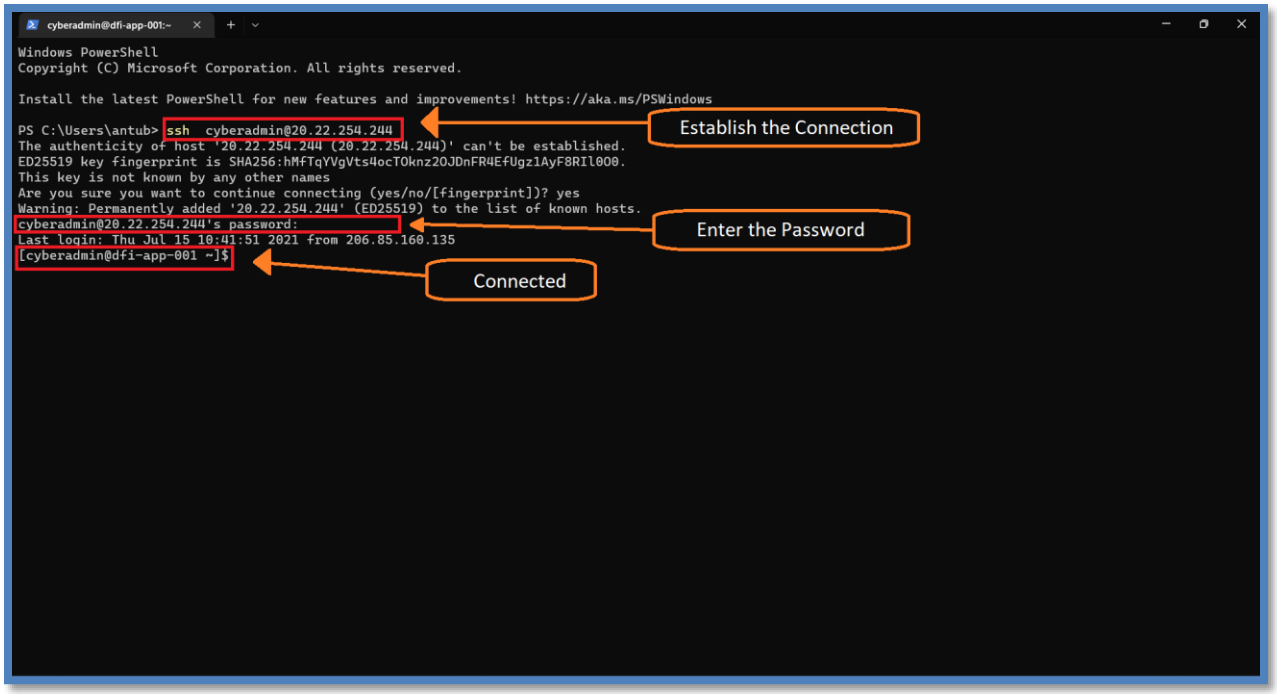
Week One:

1. **Connect:**

All the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

[Please Provide Screenshots of the RDP and SSH here as evidence that you completed this step.]

SSH:

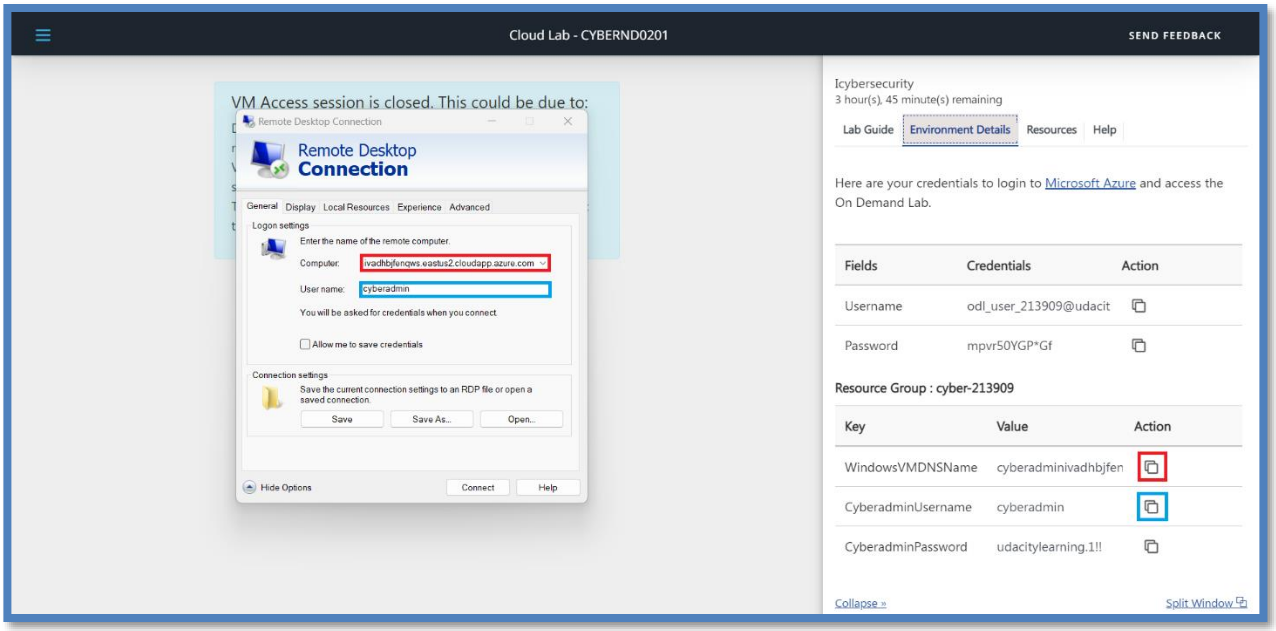


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\antub> ssh  cyberadmin@20.22.254.244
The authenticity of host '20.22.254.244 (20.22.254.244)' can't be established.
ED25519 key fingerprint is SHA256:hMfTqYVgVts4ocTOknz2OJDnFR4EfUgz1AyF8RIl0O0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.22.254.244' (ED25519) to the list of known hosts.
cyberadmin@20.22.254.244's password:
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$
```

RDP:



Cloud Lab - CYBERND0201

SEND FEEDBACK

VM Access session is closed. This could be due to:

Remote Desktop Connection

Remote Desktop Connection

General | Display | Local Resources | Experience | Advanced

Logon settings

Enter the name of the remote computer.

Computer: ivadhbjfenqws.eastus2.cloudapp.azure.com

User name: cyberadmin

You will be asked for credentials when you connect

□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Save | Save As... | Open...

Hide Options | Connect | Help

Icybersecurity

3 hour(s), 45 minute(s) remaining

Lab Guide | Environment Details | Resources | Help

Here are your credentials to login to Microsoft Azure and access the On Demand Lab.

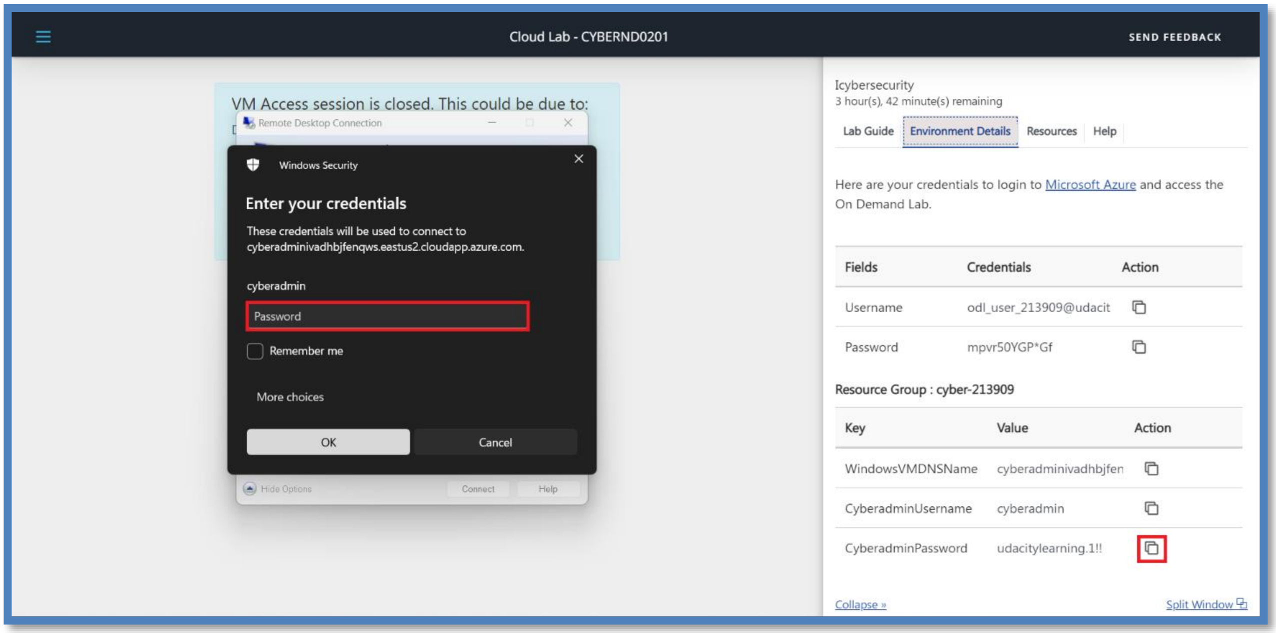
Fields	Credentials	Action
Username	odl_user_213909@udacit	⧉
Password	mpvr50YGP*Gf	⧉

Resource Group : cyber-213909

Key	Value	Action
WindowsVMDNSName	cyberadminivadhbjfen	⧉
CyberadminUsername	cyberadmin	⧉
CyberadminPassword	udacitylearning.1!!	⧉

Collapse »

Split Window



Cloud Lab - CYBERND0201

SEND FEEDBACK

VM Access session is closed. This could be due to:

Remote Desktop Connection

Windows Security

Enter your credentials

These credentials will be used to connect to cyberadminivadhbjfenqws.eastus2.cloudapp.azure.com.

cyberadmin

Password

□ Remember me

More choices

OK | Cancel

Hide Options | Connect | Help

Icybersecurity

3 hour(s), 42 minute(s) remaining

Lab Guide | Environment Details | Resources | Help

Here are your credentials to login to Microsoft Azure and access the On Demand Lab.

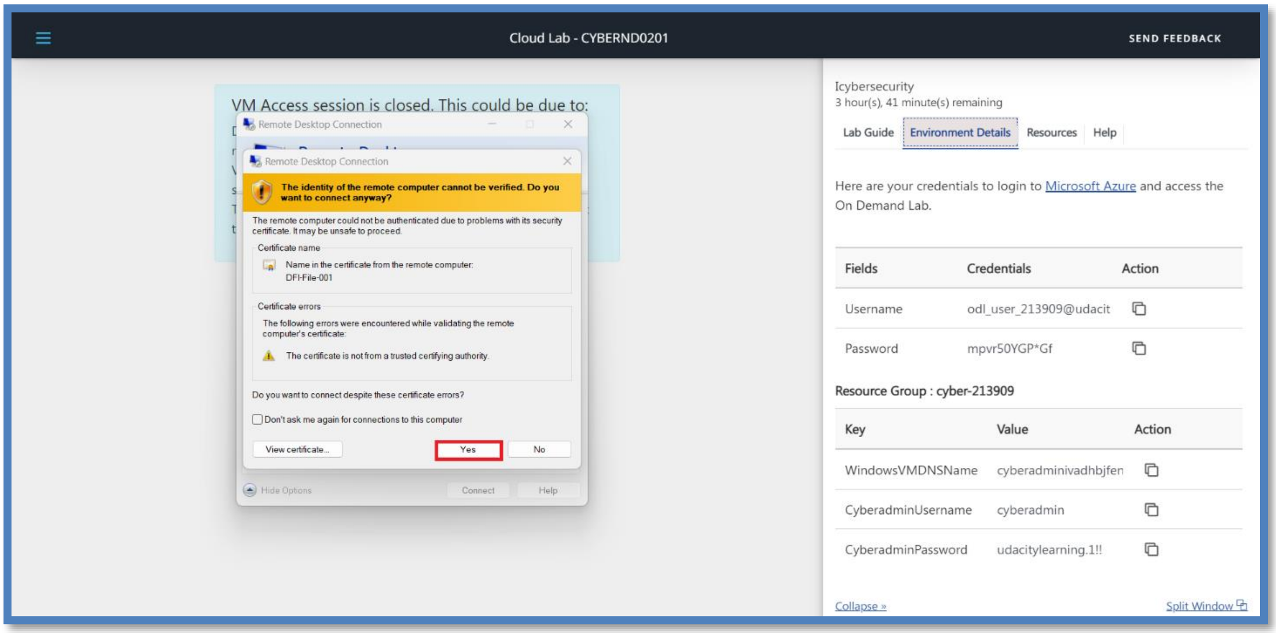
Fields	Credentials	Action
Username	odl_user_213909@udacit	⧉
Password	mpvr50YGP*Gf	⧉

Resource Group : cyber-213909

Key	Value	Action
WindowsVMDNSName	cyberadminivadhbjfen	⧉
CyberadminUsername	cyberadmin	⧉
CyberadminPassword	udacitylearning.1!!	⧉

Collapse »

Split Window



VM Access session is closed. This could be due to:

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
DFI-File-001

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

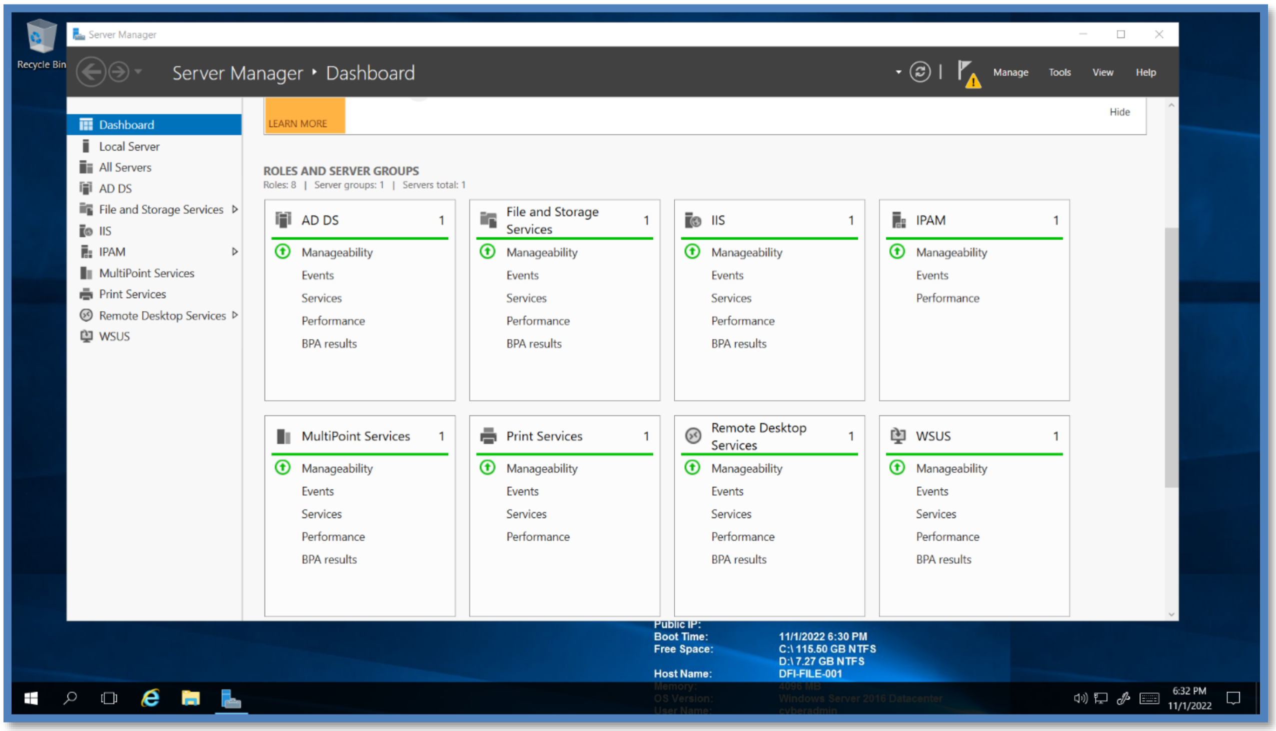
Icybersecurity
3 hour(s), 41 minute(s) remaining

Here are your credentials to login to Microsoft Azure and access the On Demand Lab.

Fields	Credentials	Action
Username	odl_user_213909@udacit	⧉
Password	mpvr50YGP*Gf	⧉

Resource Group : cyber-213909

Key	Value	Action
WindowsVMDNSName	cyberadminivadhbjfen	⧉
CyberadminUsername	cyberadmin	⧉
CyberadminPassword	udacitylearning.1!!	⧉



ROLES AND SERVER GROUPS
Roles: 8 | Server groups: 1 | Servers total: 1

Role	Count	Items
AD DS	1	Manageability Events Services Performance BPA results
File and Storage Services	1	Manageability Events Services Performance BPA results
IIS	1	Manageability Events Services Performance BPA results
IPAM	1	Manageability Events Performance
MultiPoint Services	1	Manageability Events Services Performance BPA results
Print Services	1	Manageability Events Services Performance
Remote Desktop Services	1	Manageability Events Services Performance BPA results
WSUS	1	Manageability Events Services Performance BPA results

```
Public IP:
Boot Time:     11/1/2022 6:30 PM
Free Space:    C:\ 115.50 GB NTFS
               D:\ 7.27 GB NTFS
Host Name:     DFI-FILE-001
Memory:        4096 MB
OS Version:    Windows Server 2016 Datacenter
User Name:     cyberadmin
```

2. **Security Analysis:**

DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI compliant organization and will likely be Sarbanes-Oxley in the near future.

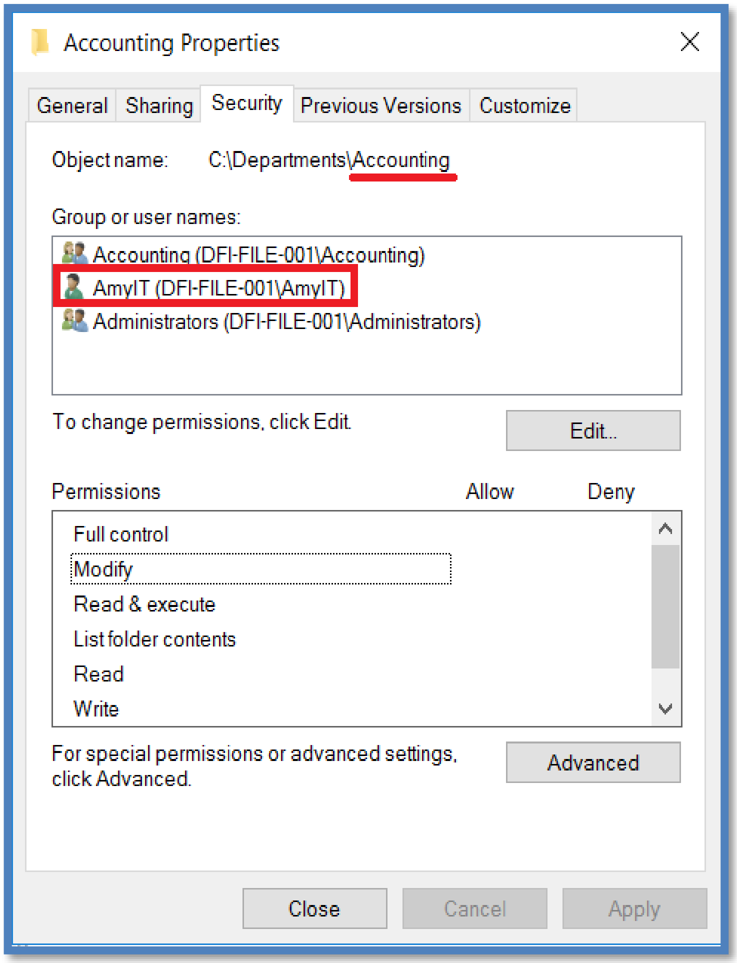
Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions and other settings.Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

[Place your security analysis here]

File Permissions that need modified

Accounting Folder:

The user "AmyIT" shouldn't has a access permission.



Accounting Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Departments\Accounting

Group or user names:

- Accounting (DFI-FILE-001\Accounting)
- AmyIT (DFI-FILE-001\AmyIT)
- Administrators (DFI-FILE-001\Administrators)

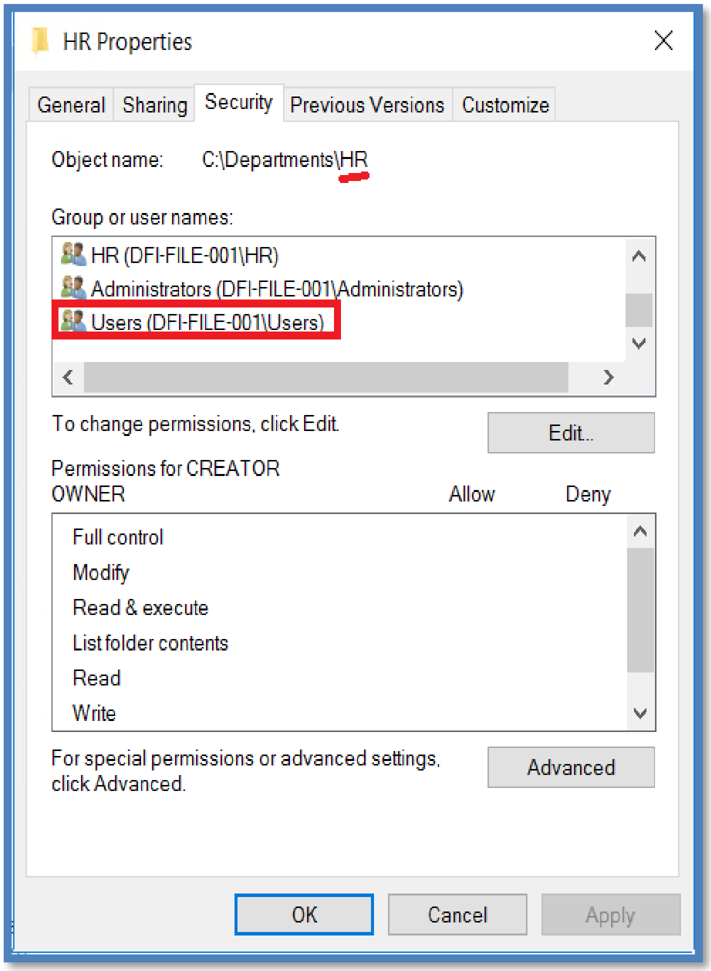
To change permissions, click Edit. [Edit...]

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

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

HR Folder:

Shouldn't have a general access.



HR Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Departments\HR

Group or user names:

- HR (DFI-FILE-001\HR)
- Administrators (DFI-FILE-001\Administrators)
- Users (DFI-FILE-001\Users)

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

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		

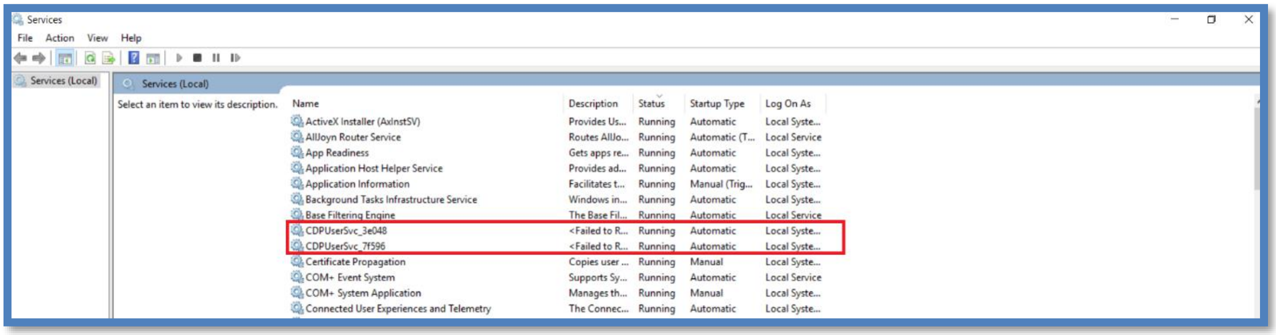
For special permissions or advanced settings, click Advanced. [Advanced]

Services:

Services should be on the server:

1. **Active Directory Domain Services (AD DS)**: acts as the core directory service for an organization, managing hierarchical relationships between network objects (users, systems, servers, applications etc.).
2. **Active Directory Web Services**: is a Windows service that provides a Web service interface to Active Directory domains.
3. **Domain Name System (DNS) Server**: DNS Server associates the domain names people use to access web pages with their respective Internet Protocol (IP) addresses.
4. **Dynamic Host Configuration Protocol (DHCP) Server:** DHCP Server assigns IP addresses and other network configurations to systems and servers so that they may communicate with other IP networks.

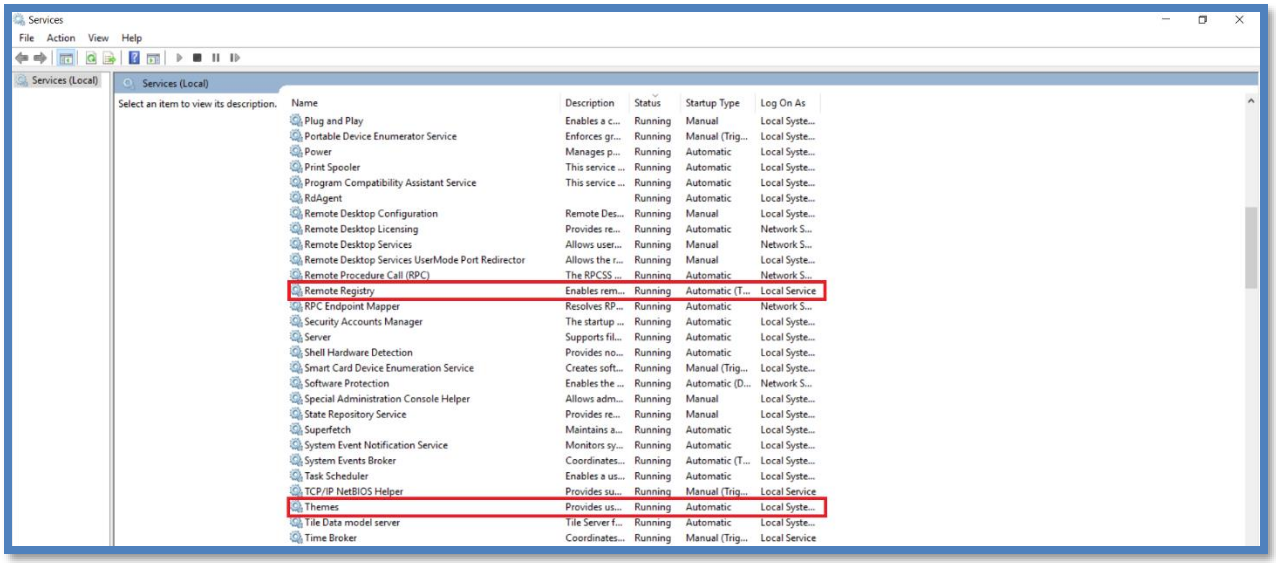
Services shouldn't be in the server:



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...	Running	Automatic	Local Syste...
AllJoyn Router Service	Routes AllJo...	Running	Automatic (T...	Local Service
App Readiness	Gets apps re...	Running	Automatic	Local Syste...
Application Host Helper Service	Provides ad...	Running	Automatic	Local Syste...
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Background Tasks Infrastructure Service	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
CDPUserSvc_3e048	<Failed to R...	Running	Automatic	Local Syste...
CDPUserSvc_7f596	<Failed to R...	Running	Automatic	Local Syste...
Certificate Propagation	Copies user ...	Running	Manual	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...	Running	Manual	Local Syste...
Connected User Experiences and Telemetry	The Connec...	Running	Automatic	Local Syste...

"CDPUserSvc_3e048" and "CDPUserScv_7f596" The function of these services is to make the connection with Bluetooth devices easier. We should disable it.



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Plug and Play	Enables a c...	Running	Manual	Local Syste...
Portable Device Enumerator Service	Enforces gr...	Running	Manual (Trig...	Local Syste...
Power	Manages p...	Running	Automatic	Local Syste...
Print Spooler	This service ...	Running	Automatic	Local Syste...
Program Compatibility Assistant Service	This service ...	Running	Automatic	Local Syste...
RdAgent		Running	Automatic	Local Syste...
Remote Desktop Configuration	Remote Des...	Running	Manual	Local Syste...
Remote Desktop Licensing	Provides re...	Running	Automatic	Network S...
Remote Desktop Services	Allows user...	Running	Manual	Network S...
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local Syste...
Remote Procedure Call (RPC)	The RPCSS ...	Running	Automatic	Network S...
Remote Registry	Enables rem...	Running	Automatic (T...	Local Service
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Network S...
Security Accounts Manager	The startup ...	Running	Automatic	Local Syste...
Server	Supports fil...	Running	Automatic	Local Syste...
Shell Hardware Detection	Provides no...	Running	Automatic	Local Syste...
Smart Card Device Enumeration Service	Creates soft...	Running	Manual (Trig...	Local Syste...
Software Protection	Enables the ...	Running	Automatic (D...	Network S...
Special Administration Console Helper	Allows adm...	Running	Manual	Local Syste...
State Repository Service	Provides re...	Running	Manual	Local Syste...
Superfetch	Maintains a...	Running	Automatic	Local Syste...
System Event Notification Service	Monitors sy...	Running	Automatic	Local Syste...
System Events Broker	Coordinates...	Running	Automatic (T...	Local Syste...
Task Scheduler	Enables a us...	Running	Automatic	Local Syste...
TCP/IP NetBIOS Helper	Provides su...	Running	Manual (Trig...	Local Service
Themes	Provides us...	Running	Automatic	Local Syste...
Tile Data model server	Tile Server f...	Running	Automatic	Local Syste...
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service

"Remote Registry" is a feature that enables remote access the server for viewing and modifying the Windows registry entries. It must be disabled.

"Themes" is a Windows Server service that provides user experience theme management. We might disable it to improve system performance and security.

3. **Firewall Rules:**
DFI does not have a dedicated networking department just yet, once again these tasks normally fall under the SysAdmin group. Now that we have you as a security professional, you'll take over the creation of our firewall rules. We recently entered into a new partnership and require new IP connections.
Using Cisco syntax, create the text of a firewall rule allowing a new DFI partner WBC International, access to DFI-File-001 access via port tcp-9082.
The partner's IP is 21.19.241.63 and DFI-File-001's IP is 172.21.30.44.

For this exercise assume the two IP objects **have not** been created in the firewall. **Note*** Use *DFI-Ingress* as the interface for the rule. For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Place your firewall rules and explanation here]

```
access-list DFI-Ingress extended permit host 21.19.241.63 host 172.21.30.44 eq 9082
```

1. **access-list:** This is the rule that controls the traffic.
2. **DFI-Ingress:** This is the name of an interface.
3. **Extended:** To set an access-list type to extended.
4. **Permit:** To allow the traffic.
5. **host 21.19.241.63:** This is the source IP address which is "WBC International".
6. **host 172.21.30.44:** This is the destination IP address which is "DFI-FILE-001".
7. **eq 9082:** eq means 'equal to' and 9082 is the port number in which the data can be accessed.

4. VPN Encryption Recommendation:

DFI is creating a payroll processing partnership with Payroll-USA, this will involve creating a VPN connection between the two. Research, recommend and justify an encryption solution for the connection that is using the latest available encryption for Cisco. Use the Cisco documentation as a guide.
[Place your VPN Encryption Recommendation here]

I recommend using **Symmetric Encryption** Because It is faster and more efficient than asymmetric encryption, For the algorithm, since the original DES is not used anymore as it is considered too weak. I recommend using the widely used symmetric algorithm which is **Advanced Encryption Standard (AES)** AES-256, which has a key length of 256 bits, supports the largest bit size and is practically unbreakable by brute force based on current computing power, making it the strongest encryption standard.

5. **IDS Rule:**

The System Administrator gave you a heads up that DFI-File-001 with an IP address of 172.21.30.44 has been receiving a high volume of ICMP traffic and is concerned that a DDoS attack is imminent. She has requested an IDS rule for this specific server.

The VoIP Administrator is also concerned that an attacker is attempting to connect to her primary VoIP server which resides at 172.21.30.55 via TFTP. She has requested an IDS rule for this traffic.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Place your System Admin rule and explanation here]

alert icmp any any -> 172.21.30.44 any (msg: “ICMP traffic detected”;)

1. **Alert:** This is a rule action that tells Snort what to do when it finds a packet that matches the rule criteria.
2. **ICMP:** This is the protocol that Snort currently analyzes for suspicious behavior.
3. **Any:** The source IP address, the keyword 'any' may be used to define any address.
4. **Any:** This is the source port, The keyword 'any' may be used to define any port.
5. **->:** indicates the direction of the traffic that the rule applies to.
6. **172.21.30.44:** The destination IP address, which is "DFI-File-001" in this example.
7. **Any:** This is the destination port, The keyword 'any' may be used to define any port.
8. **(msg: "ICMP traffic detected";):** This message will display in case the ICMP traffic detected.

[Place your VoIP Admin rule and explanation here]

alert udp any any -> 172.21.30.55 69 (msg:” Connection attempted via TFTP”;)

1. **Alert:** This is a rule action that tells Snort what to do when it finds a packet that matches the rule criteria.
2. **UDP:** This is the protocol that Snort currently analyzes for suspicious behavior.
3. **Any:** The source IP address, The keyword 'any' may be used to define any address.
4. **Any:** This is the source port, The keyword 'any' may be used to define any port.
5. **->:** indicates the direction of the traffic that the rule applies to.
6. **172.21.30.55:** The destination IP address, which is "VoIP server" in this example.

7. **69:** This is the destination port, TFTP is a simple protocol for transferring files, implemented on top of the UDP/IP protocols using well-known port number 69.
8. **(msg: "Connection via TFTP";):** This message will display in case the connection detected.

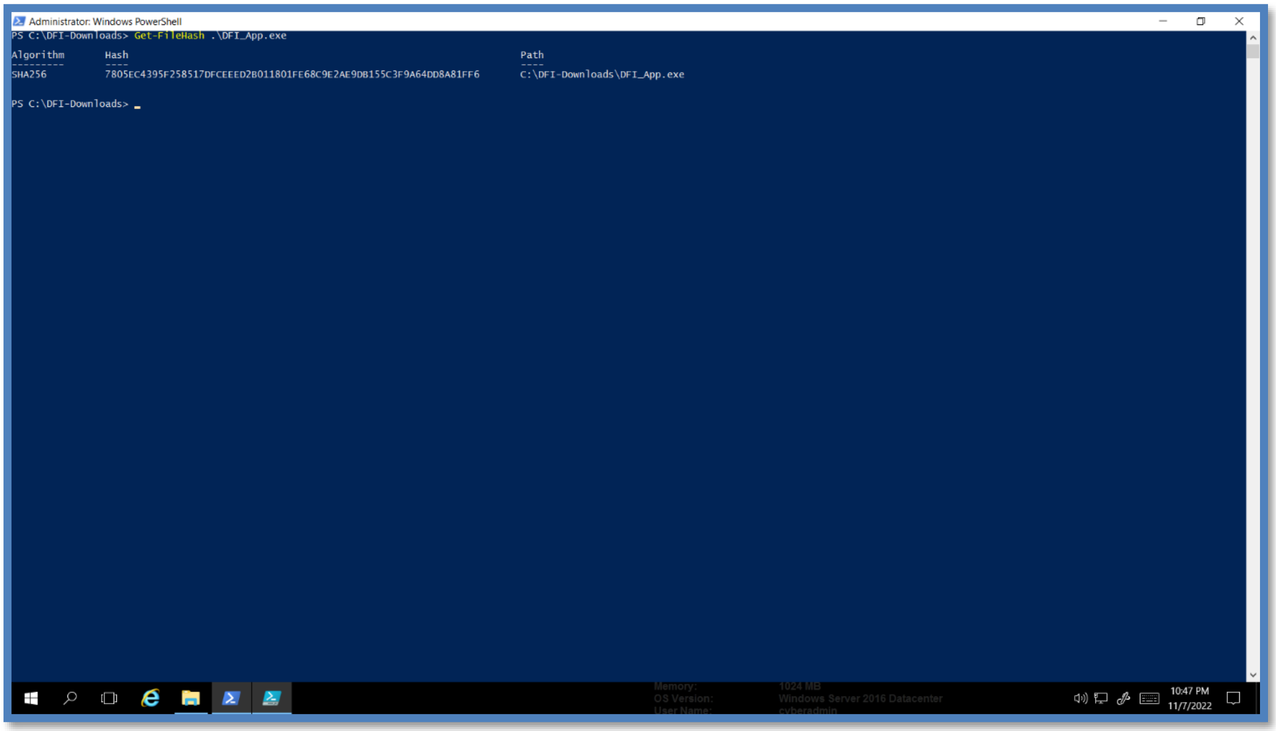
6. **File Hash verification:**

A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

Hash: 7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6

Perform a file hash verification and submit a screenshot of your command and output.
The File is stored on the Windows 2016 Server in C Drive under DFI-Download.

[Place your screenshot verification here]


Administrator: Windows PowerShell

```
PS C:\DFI-Downloads> Get-FileHash .\DFI_App.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6       C:\DFI-Downloads\DFI_App.exe

PS C:\DFI-Downloads> _
```

Memory: 1024 MB
OS Version: Windows Server 2016 Datacenter
User Name: cyberadmin
10:47 PM
11/7/2022

Week Two:

Now that you've performed a light audit and crafted Firewall and IDS Signatures we're ready for you to make some additional recommendations to tighten up our security.

7. **Automation:**

The IT Manager has tasked you with some introductory research on areas that could be improved via automation.

Research and recommend products, technologies and areas within DFI that could be improved via automation.

Recommended areas are:

- SOAR products and specifically what could be done with them
- Automation of mitigation actions for IDS and firewall alerts.
- Feel free to elaborate on other areas that could be improved.

Complete the chart below including the area/technology within DFI and a proposed solution, with a minimum of 3 areas. Provide a brief explanation for your choices.

DFI Area/Technology	Solution	Justification for Recommendation
Security	Azure Security Center	It provides advanced threat protection across hybrid cloud workloads. It suites for a small business.
Configuration management	Puppet	configuration management ensures that misconfigurations don't go unnoticed and prevents them from creating problems across the environment.
Incident Response	Heimdal Endpoint Detection and Response.	It Filters DNS, HTTP and HTTPs traffic, predicting future threats and Spot malicious URLs, processes, and backtrack the attacker's origins. The software is provided on Windows and Linux.

8. **Logging RDP Attempts:**

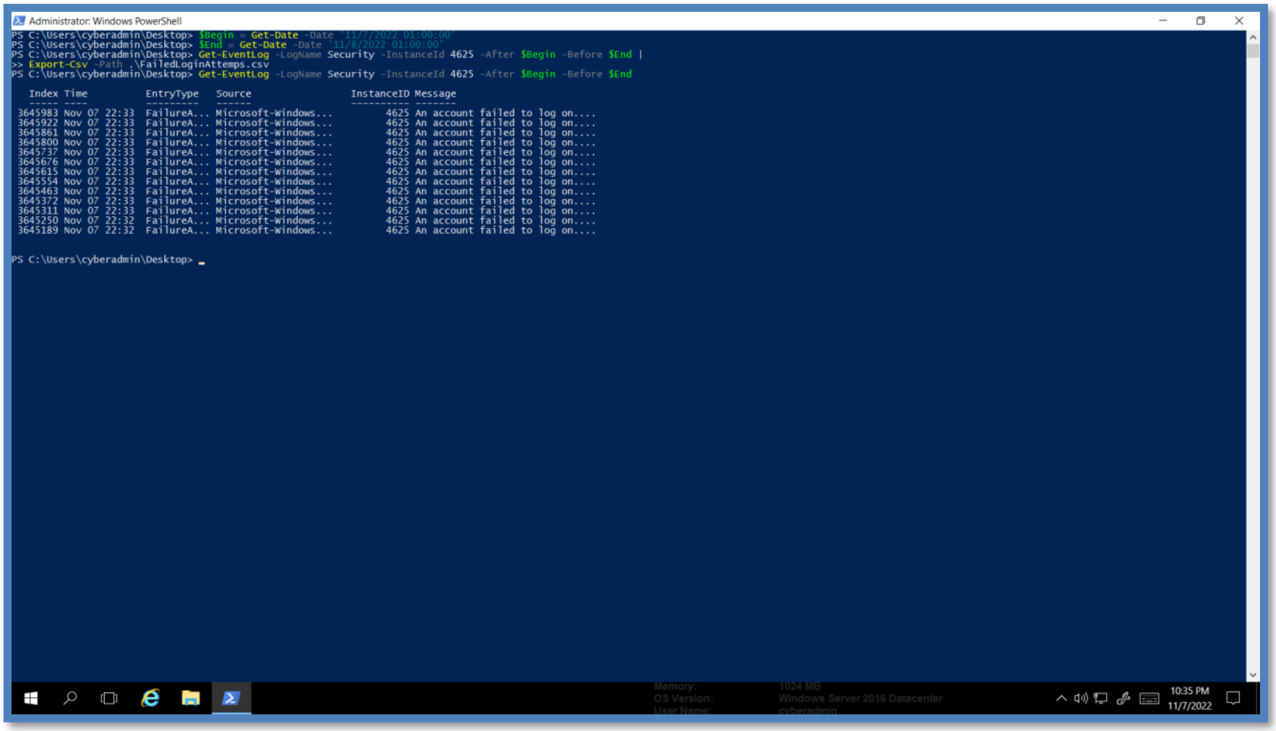
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

For your deliverable, open the CSV with notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below explain your findings, recommendations and justifications to the IT Manager.

[Place IT Manager Report Here]

The result on PowerShell at DFI-File-001:



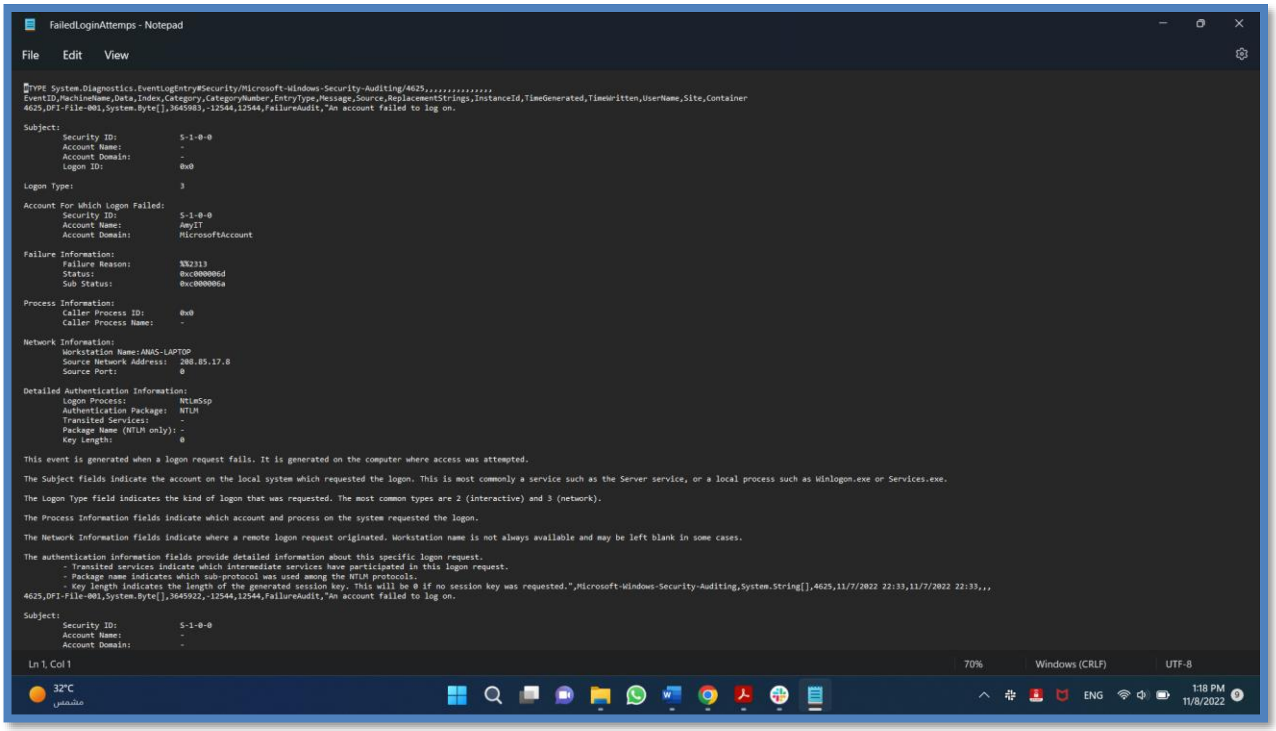
Administrator: Windows PowerShell
Memory: 1024 MB
OS Version: Windows Server 2016 Datacenter
User Name: cyberadmin
10:35 PM
11/7/2022

```
PS C:\Users\cyberadmin\Desktop> $Begin = Get-Date -Date '11/7/2022 01:00:00'
PS C:\Users\cyberadmin\Desktop> $End = Get-Date -Date '11/8/2022 01:00:00'
PS C:\Users\cyberadmin\Desktop> Get-EventLog -LogName Security -InstanceId 4625 -After $Begin -Before $End |
>> Export-Csv -Path .\FailedLoginAttemps.csv
PS C:\Users\cyberadmin\Desktop> Get-EventLog -LogName Security -InstanceId 4625 -After $Begin -Before $End

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
 3645983 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645922 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645861 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645800 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645737 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645676 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645615 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645554 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645463 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645372 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645311 Nov 07 22:33  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645250 Nov 07 22:32  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 3645189 Nov 07 22:32  FailureA... Microsoft-Windows...         4625 An account failed to log on....


PS C:\Users\cyberadmin\Desktop> _
```

The Exported file (FailedLoginAttemps.csv) | Personal Computer:



```
#TYPE System.Diagnostics.EventLogEntry#Security/Microsoft-Windows-Security-Auditing/4625,,,,,,,,,,,,,,,
EventID,MachineName,Data,Index,Category,CategoryNumber,EntryType,Message,Source,ReplacementStrings,InstanceId,TimeGenerated,TimeWritten,UserName,Site,Container
4625,DFI-File-001,System.Byte[],3645983,-12544,12544,FailureAudit,"An account failed to log on.

Subject:
	Security ID:		S-1-0-0
	Account Name:		-
	Account Domain:		-
	Logon ID:		0x0

Logon Type:			3

Account For Which Logon Failed:
	Security ID:		S-1-0-0
	Account Name:		AmyIT
	Account Domain:		MicrosoftAccount

Failure Information:
	Failure Reason:		%%2313
	Status:			0xc000006d
	Sub Status:		0xc000006a

Process Information:
	Caller Process ID:	0x0
	Caller Process Name:	-

Network Information:
	Workstation Name:ANAS-LAPTOP
	Source Network Address:	208.85.17.8
	Source Port:		0

Detailed Authentication Information:
	Logon Process:		NtLmSsp
	Authentication Package:	NTLM
	Transited Services:	-
	Package Name (NTLM only):	-
	Key Length:		0

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.
	- Transited services indicate which intermediate services have participated in this logon request.
	- Package name indicates which sub-protocol was used among the NTLM protocols.
	- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.",Microsoft-Windows-Security-Auditing,System.String[],4625,11/7/2022 22:33,11/7/2022 22:33,,,
4625,DFI-File-001,System.Byte[],3645922,-12544,12544,FailureAudit,"An account failed to log on.

Subject:
	Security ID:		S-1-0-0
	Account Name:		-
	Account Domain:		-
```

According to the result of the security logs. There are many failed logging attempts for the last 24 hours. To reduce this kind of events:

1. We should limit the number of failed log-in attempts.
2. Restrict RDP access using Windows Firewall. By allowing Trusted IP only to connect to the server.
3. Change RDP default port. By navigating the "Registry Editor" and change the listening port from '3389' to any port for example '3390'.

9. **Windows Updates:**

Using NIST 800-40r3 and Microsoft Security Update Guide, analyze the windows servers and provide your answers in the table below of available updates (KB and CVE) that should be installed as well as any updates that can be safely ignored for DFI's purpose. To assist, be aware that DFI is concerned with stability and security, any update that is not labeled as a 'critical' or 'security' can be left off.

Justify your recommendations as to why you are making your choices.

Add as many rows or additional columns as you need to the table.

Available Updates	Update/Ignore	Justification
KB5017396 Windows Server 2016 September 13, 2022	update	This is a security update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft update
KB5014630 Windows Server 2016 June 14, 2022	update	.NET Runtime Addresses several issues that would cause too many garbage collections under high memory load
KB5020439 Windows Server 2016 October 18, 2022	update	It addresses an issue that might affect some types of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) connections. These connections might have handshake failures.
KB5011329 Windows Server 2016 February 7, 2022	ignore	No Security improvements and it will be included in the next cumulative updates.
KB5005393 Windows Server 2016 July 29, 2021	Ignore	This update is related to printers, Scanners and multifunction devices. We don't need to update it.

KB5001633 Windows Server 2016 March 18, 2021	Ignore	Addresses an issue that fails to print the graphical content in a document in a previous update.

10. **Linux Data Directories:**

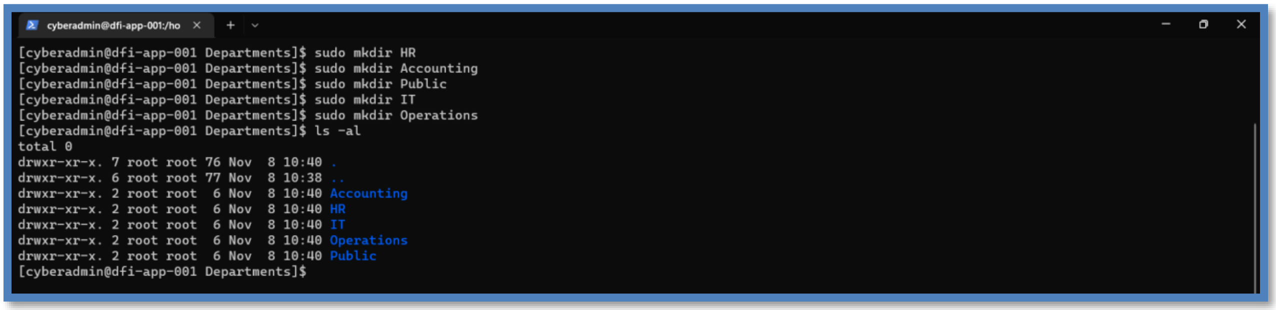
The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

- The root directory should be 'Home'
- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.
- Set owner permissions for the groups IT, HR, Operations and Accounting
- Create the users AmyIT, PamOps, MandyAcct and TimHR in the appropriate groups so that they can read/write/execute in their respective departmental folders.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

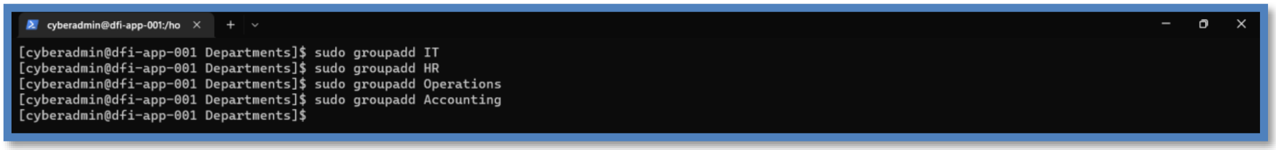
[Provide a screenshot(s) of completed tasks and the correctly set permissions here]

Creating "Departments" directory and sub-directories:



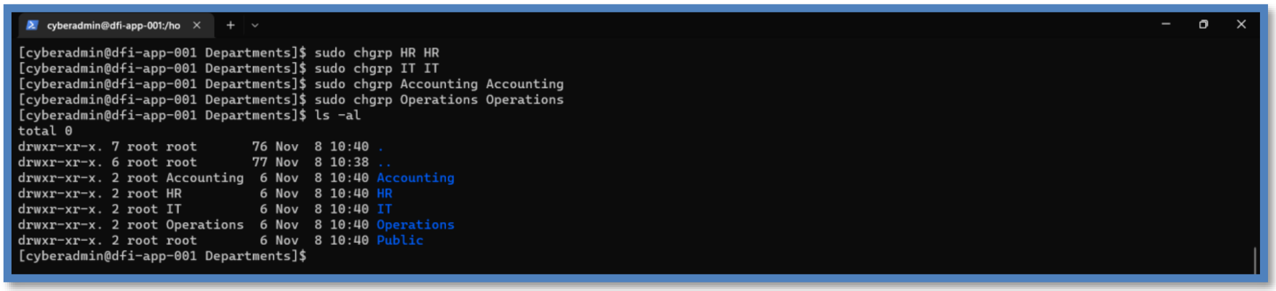
```
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir HR
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Public
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir IT
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Operations
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxr-xr-x. 7 root root 76 Nov  8 10:40 .
drwxr-xr-x. 6 root root 77 Nov  8 10:38 ..
drwxr-xr-x. 2 root root  6 Nov  8 10:40 Accounting
drwxr-xr-x. 2 root root  6 Nov  8 10:40 HR
drwxr-xr-x. 2 root root  6 Nov  8 10:40 IT
drwxr-xr-x. 2 root root  6 Nov  8 10:40 Operations
drwxr-xr-x. 2 root root  6 Nov  8 10:40 Public
[cyberadmin@dfi-app-001 Departments]$
```

Creating groups:



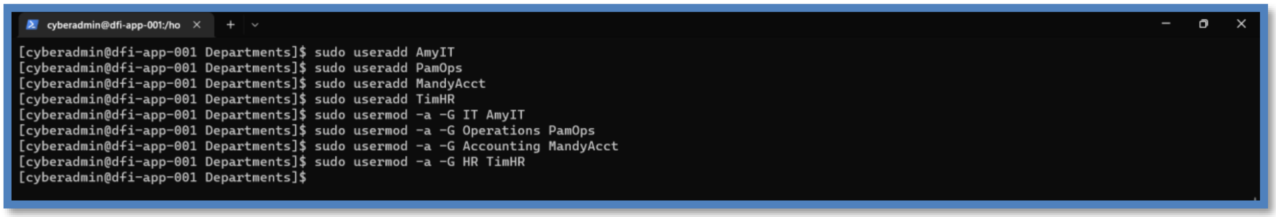
```
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$
```

Set owner permission to groups:



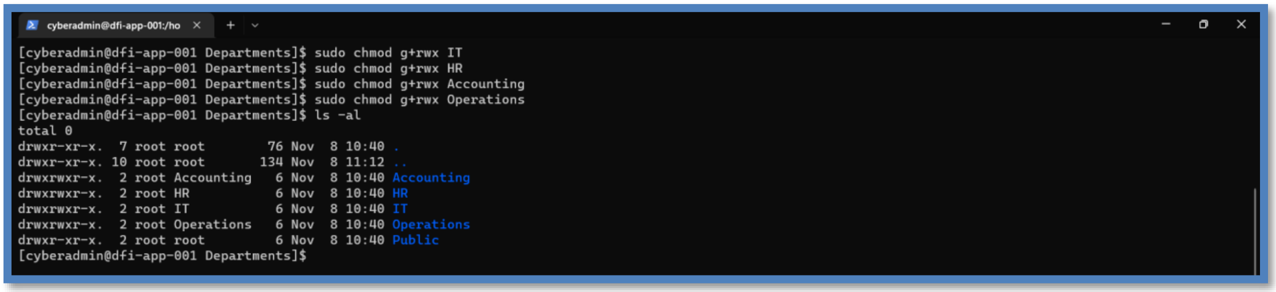
```
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp HR HR
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp IT IT
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp Accounting Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp Operations Operations
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxr-xr-x. 7 root root       76 Nov  8 10:40 .
drwxr-xr-x. 6 root root       77 Nov  8 10:38 ..
drwxr-xr-x. 2 root Accounting  6 Nov  8 10:40 Accounting
drwxr-xr-x. 2 root HR          6 Nov  8 10:40 HR
drwxr-xr-x. 2 root IT          6 Nov  8 10:40 IT
drwxr-xr-x. 2 root Operations  6 Nov  8 10:40 Operations
drwxr-xr-x. 2 root root        6 Nov  8 10:40 Public
[cyberadmin@dfi-app-001 Departments]$
```

Creating users and add them to groups:



```
[cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo useradd PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo useradd MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo useradd TimHR
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G IT AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Operations PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Accounting MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G HR TimHR
[cyberadmin@dfi-app-001 Departments]$
```

Change permissions for groups:



```
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx IT
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx HR
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx Operations
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxr-xr-x.  7 root root        76 Nov  8 10:40 .
drwxr-xr-x. 10 root root       134 Nov  8 11:12 ..
drwxrwxr-x.  2 root Accounting   6 Nov  8 10:40 Accounting
drwxrwxr-x.  2 root HR           6 Nov  8 10:40 HR
drwxrwxr-x.  2 root IT           6 Nov  8 10:40 IT
drwxrwxr-x.  2 root Operations   6 Nov  8 10:40 Operations
drwxr-xr-x.  2 root root         6 Nov  8 10:40 Public
[cyberadmin@dfi-app-001 Departments]$
```

[Provide your non-technical syntax explanation for management here]

- I created "Department" directory using this command **mkdir Departments** then I moved into that directory using this command **cd .\Departments** After that I create sub-directories for each department using this command **mkdir (Department_name).**
- I created a new groups for each department using this command **groupadd (Department_name).**
- After that I set owner permission for each sub-directory to its group by this command **chgrp (Group_name) (Directory_name).**
- I created new users using this commend **useradd (username)** then added them to their groups by this command **usermod -a -G (Group_name) (username).** Where '**-a**' using to Add the user to the supplementary group(s) '**-G**' which is A list of supplementary groups.
- I changed permissions and set it to "Read/Write/Execute" for each sub-directory by using this command **chmod g+rwx (Directory_name).**

11. **Firewall Alert Response:**

The IT Manager took a look at firewall alerts and was concerned with some traffic she saw, please take a look and provide a mitigation response to the below firewall report. Remember to justify your mitigation strategy.
This file is available from the project resources title: **DFI_FW_Report.xlsx**. Please download and use this file to complete this task.

[Firewall mitigation response and justification goes here]

1. **Account Lockouts After Failed Attempts**
   and set the lockout for a set amount of time to avoid DOS attacks.

2. **Make the Root User inaccessible via SSH**.

3. **Limit Logins to a Specified IP Address or Range**
   To make sure only trusted IP have access to the server.

4. **Employ 2-Factor Authentication (2FA)**
   If a password is hacked, guessed, or even phished, that's no longer enough to give an intruder access: without approval at the second factor.

5. **Modify the Default Port**:
   Most automated SSH attacks are attempted on the default port 22. So, running ssh on a different port could prove to be a useful way of dealing with brute force attacks.

12. **Status Report and where to go from here:**

As your first two weeks wind down, the IT Manager, HR Manager as well as other management are interested in your experience. With your position being the first dedicated Information Security role, they would like a 'big picture' view of what you've done as well as the security posture of DFI.

Similar to Defense-in-Depth, an organization has multiple layers of security from the edge of their web presence all the way to permissions on a file.

In your own words explain the work you've done, the recommendations made and how DFI should proceed from a security standpoint. This is your opportunity to provide a thoughtful analysis that shows your understanding of Cyber Security and how all of the tasks you've performed contribute to the security of DFI. As this will be reviewed by non-technical management please keep the technical jargon to a minimum.

[Provide your Status Report Here]

First week: I've tested the connectivity by **establishing the connection** between "Windows 10" client and "Windows 2016" Server. I connected to "Linux" server using PowerShell at Windows client. Then I analysis the Windows server to find what changes should be applied on permissions, Services, Policies. After that I've created a **firewall rule** to partner company and grant them an access to Windows server. I've recommended the **VPN encryption** we should use. I've created **Intrusion detection system (IDS) rule** to detect suspicious activities and generate alerts when they are detected. At last, I used **File hash verification** to make sure that "DFI application" is not modified.

Second Week: I've researched and recommended areas within DFI that could be improved via **automation**. I prepared a list of a **failed RDP logins** and recommended the steps to avoid this kind of events. Then I reviewed some **windows updates** and determined what to update immediately and what to ignore. In **Linux server**, I created a Directory, sub-directories and groups for each Department on the company then I created users for: Amy, Pam, Mandy and Tim and added them to their appropriate group. At last, I reviewed the **firewall report** and provided steps with mitigation strategy.

13. **File Encryption:**

As your final task, assemble all of the deliverables you have created in Steps 1-12 and encrypt them using 7zip with a strong password.

When you submit the file you must also include your password as a note to the reviewer at Udacity or they will not be able to review your project.