Lama Alhaza

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.

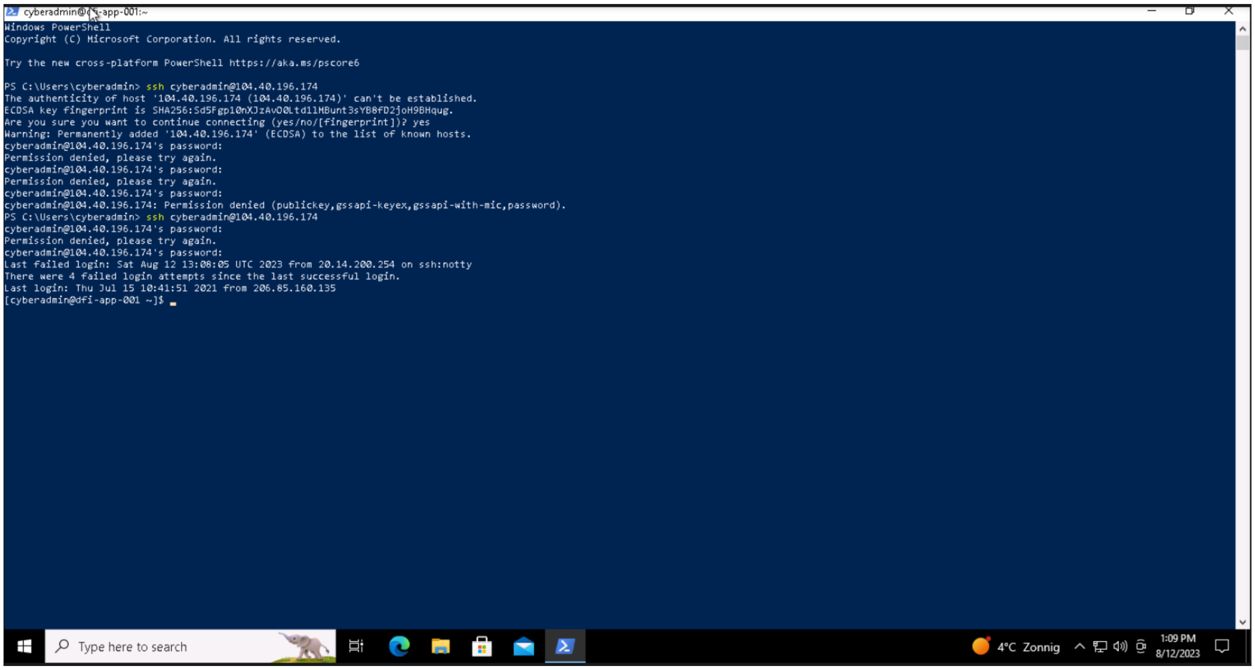
Week One:

1. **Connect:**

All of 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.]

To login to the linux machine
$ ssh cyberadmin@104.40.196.174 then writing the password udacitylearning.1!!

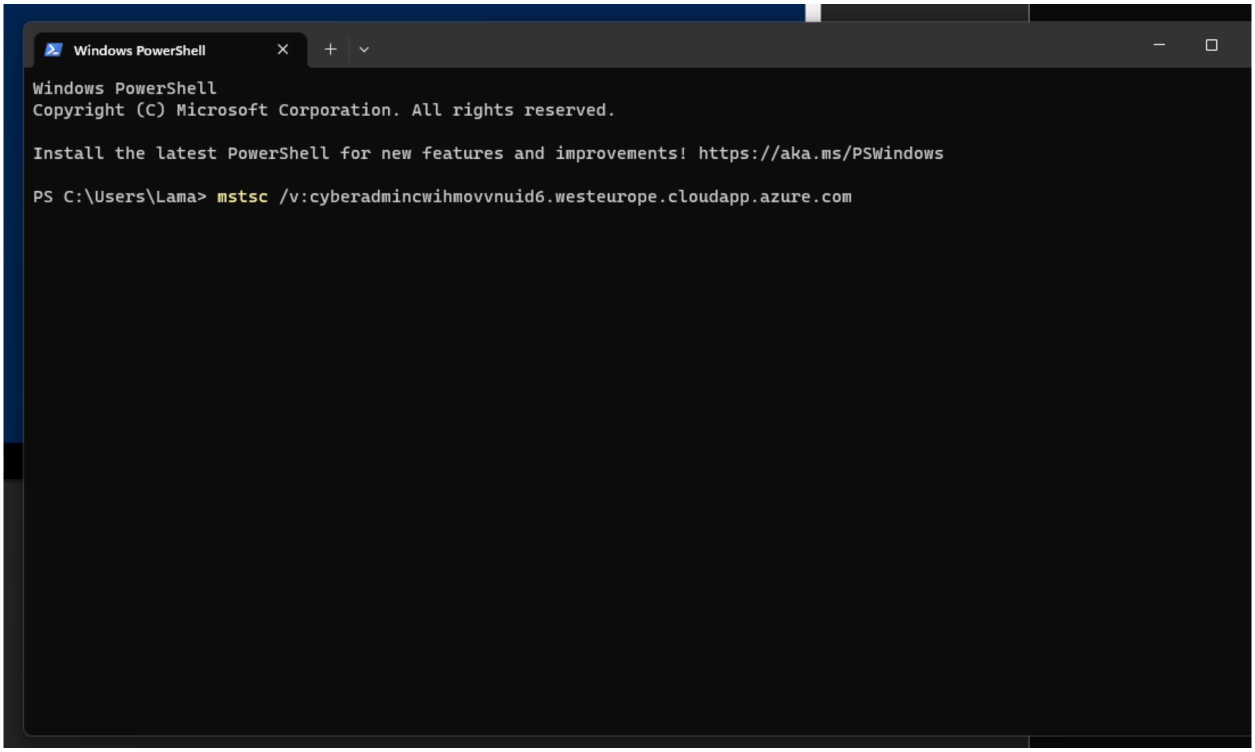


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\cyberadmin> ssh cyberadmin@104.40.196.174
The authenticity of host '104.40.196.174 (104.40.196.174)' can't be established.
ECDSA key fingerprint is SHA256:Sd5Fgp10nXJzAvO0Ltd1lMBunt3sYB8fD2joH9BHqug.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '104.40.196.174' (ECDSA) to the list of known hosts.
cyberadmin@104.40.196.174's password:
Permission denied, please try again.
cyberadmin@104.40.196.174's password:
Permission denied, please try again.
cyberadmin@104.40.196.174's password:
cyberadmin@104.40.196.174: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
PS C:\Users\cyberadmin> ssh cyberadmin@104.40.196.174
cyberadmin@104.40.196.174's password:
Permission denied, please try again.
cyberadmin@104.40.196.174's password:
Last failed login: Sat Aug 12 13:08:05 UTC 2023 from 20.14.200.254 on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$ 
```

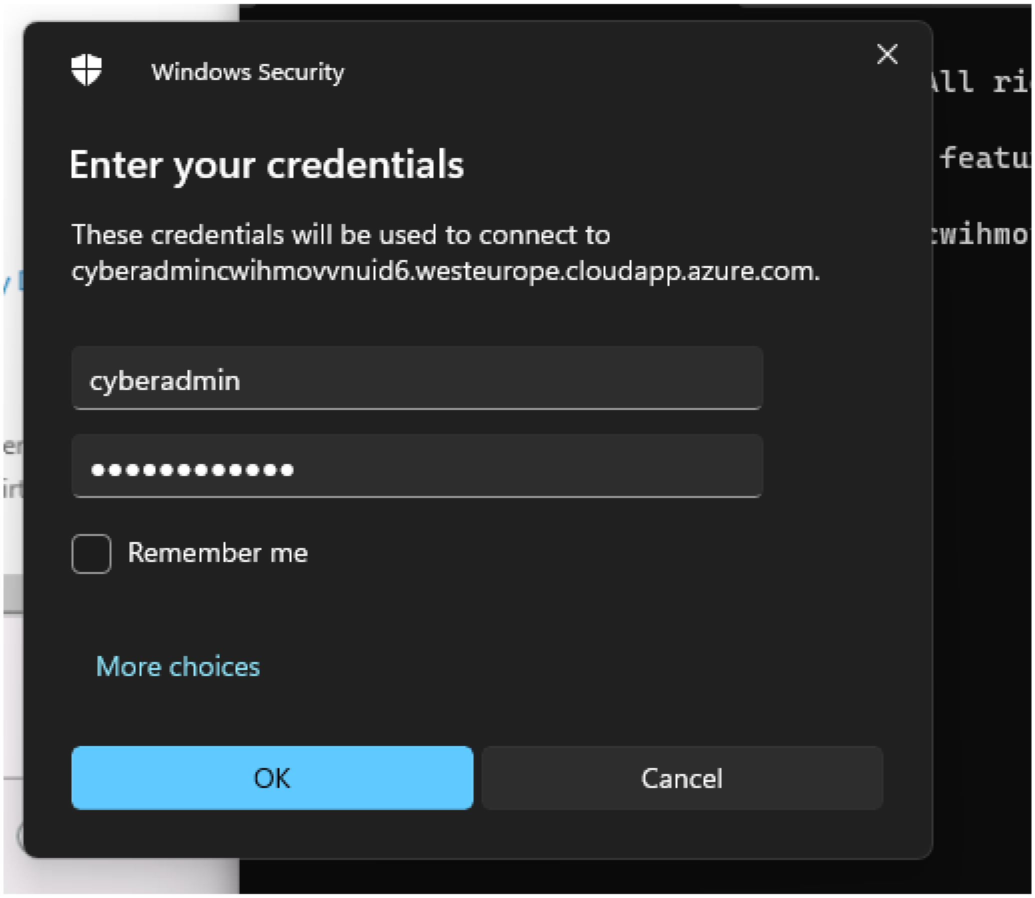
To login to the windows server machine
$ mstsc /v:cyberadmincwihmovvnuid6.westeurope.cloudapp.azure.com



```
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\Lama> mstsc /v:cyberadmincwihmovvnuid6.westeurope.cloudapp.azure.com
```



Windows Security

Enter your credentials

These credentials will be used to connect to cyberadmincwihmovvnuid6.westeurope.cloudapp.azure.com.

cyberadmin

●●●●●●●●●●●●●

□ Remember me

Using the below credentials
Cyberadmin
xxvn09FKL*Dz

2. **Security Analysis:**

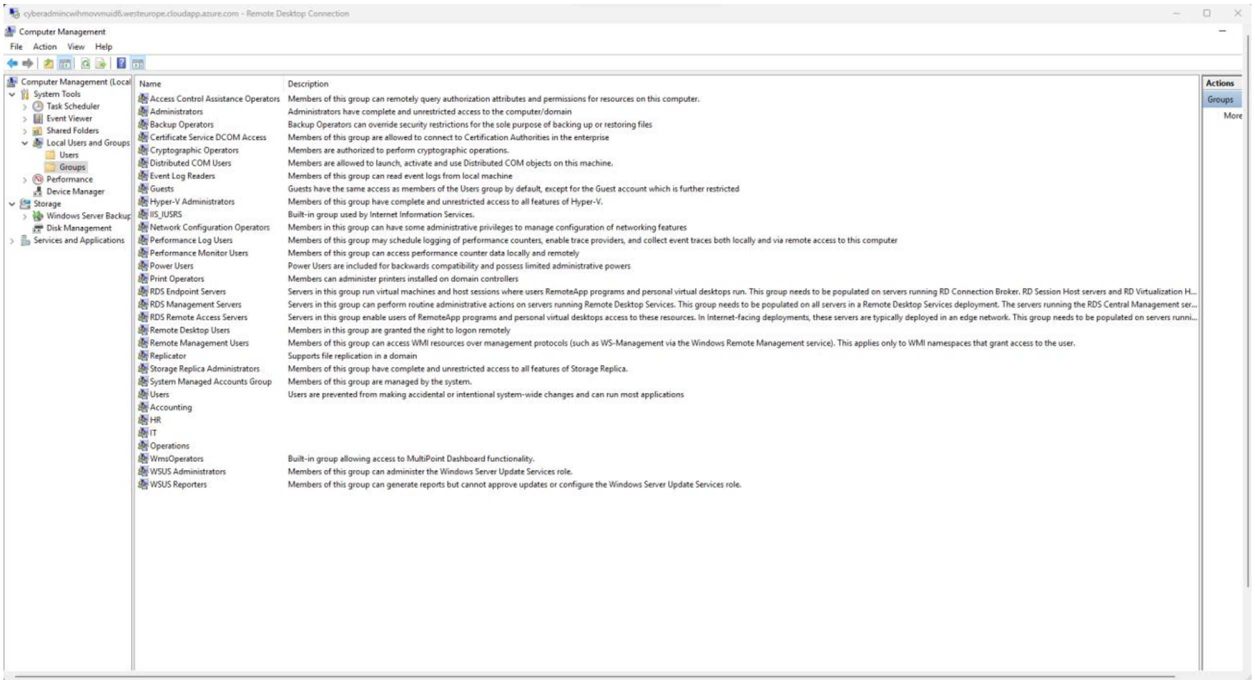
DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

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.

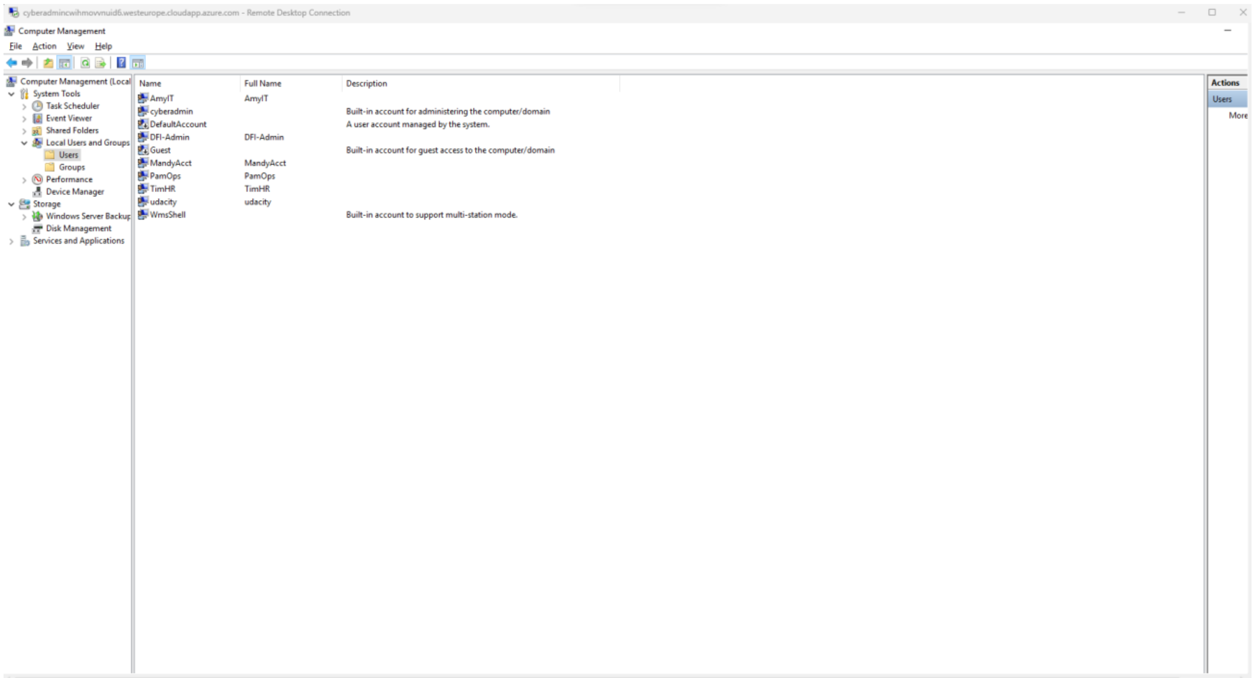
Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions and other settings. Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

[Place your security analysis here]

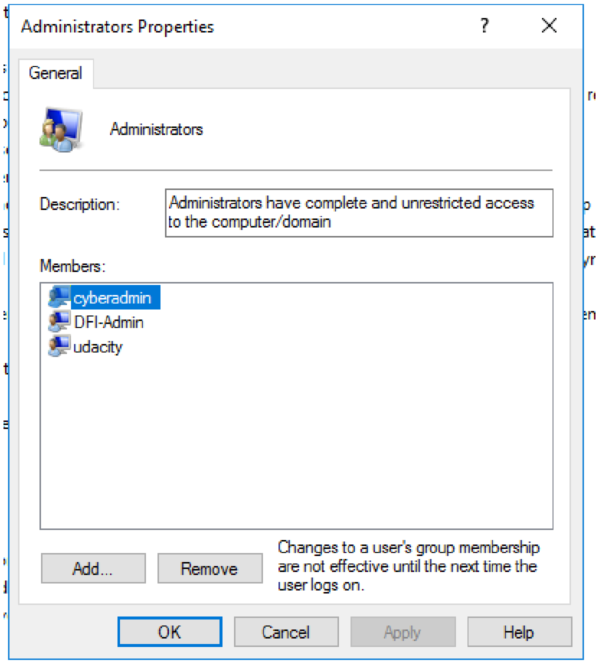
Principle of lease privilege



Name	Description
Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
Certificate Service DCOM Access	Members of this group are allowed to connect to Certification Authorities in the enterprise
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine.
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of Hyper-V.
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and via remote access to this computer
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Power Users	Power Users are included for backwards compatibility and possess limited administrative powers
Print Operators	Members can administer printers installed on domain controllers
RDS Endpoint Servers	Servers in this group run virtual machines and host sessions where users RemoteApp programs and personal virtual desktops run. This group needs to be populated on servers running RD Connection Broker. RD Session Host servers and RD Virtualization H...
RDS Management Servers	Servers in this group can perform routine administrative actions on servers running Remote Desktop Services. This group needs to be populated on all servers in a Remote Desktop Services deployment. The servers running the RDS Central Management ser...
RDS Remote Access Servers	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. In Internet-facing deployments, these servers are typically deployed in an edge network. This group needs to be populated on servers runni...
Remote Desktop Users	Members in this group are granted the right to logon remotely
Remote Management Users	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Replicator	Supports file replication in a domain
Storage Replica Administrators	Members of this group have complete and unrestricted access to all features of Storage Replica.
System Managed Accounts Group	Members of this group are managed by the system.
Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications
Accounting	
HR	
IT	
Operations	
WmsOperators	Built-in group allowing access to MultiPoint Dashboard functionality.
WSUS Administrators	Members of this group can administer the Windows Server Update Services role.
WSUS Reporters	Members of this group can generate reports but cannot approve updates or configure the Windows Server Update Services role.



Name	Full Name	Description
AmyIT	AmyIT	
cyberadmin		Built-in account for administering the computer/domain
DefaultAccount		A user account managed by the system.
DFI-Admin	DFI-Admin	
Guest		Built-in account for guest access to the computer/domain
MandyAcct	MandyAcct	
PamOps	PamOps	
TimHR	TimHR	
udacity	udacity	
WmsShell		Built-in account to support multi-station mode.



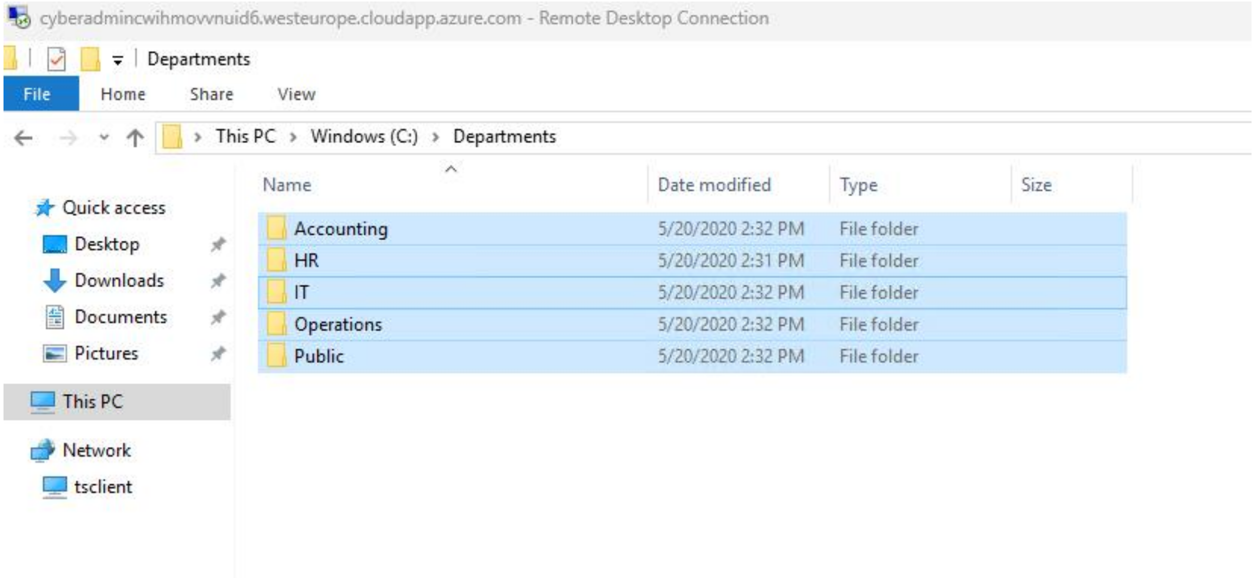
Administrators Properties

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:
- cyberadmin
- DFI-Admin
- udacity

Changes to a user's group membership are not effective until the next time the user logs on.

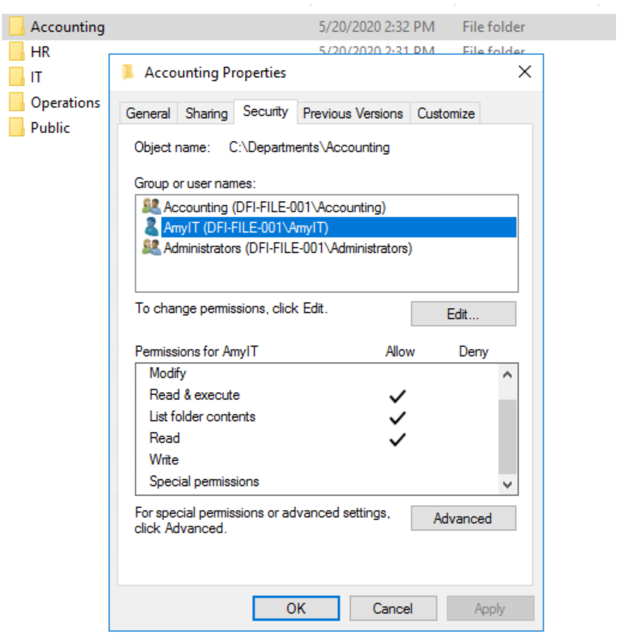


cyberadmincwihmovvnuid6.westeurope.cloudapp.azure.com - Remote Desktop Connection

Departments

This PC › Windows (C:) › Departments

Name	Date modified	Type	Size
Accounting	5/20/2020 2:32 PM	File folder	
HR	5/20/2020 2:31 PM	File folder	
IT	5/20/2020 2:32 PM	File folder	
Operations	5/20/2020 2:32 PM	File folder	
Public	5/20/2020 2:32 PM	File folder	



Object name: C:\Departments\Accounting

Group or user names:

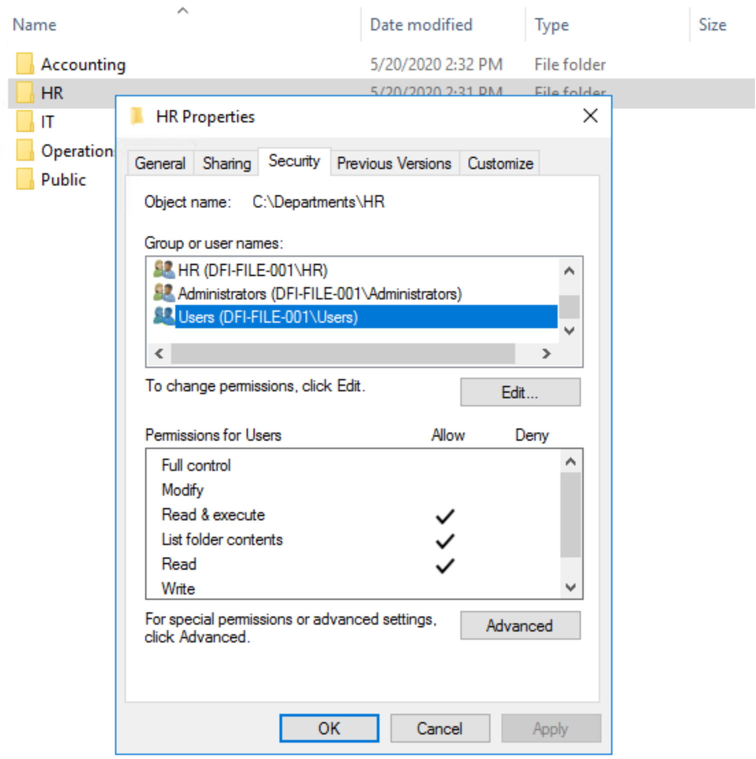
- Accounting (DFI-FILE-001\Accounting)
- AmyIT (DFI-FILE-001\AmyIT)
- Administrators (DFI-FILE-001\Administrators)

To change permissions, click Edit.

Permissions for AmyIT	Allow	Deny
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

After analyzing all groups and users I tried to figure out which members are in accounting group, and I figured out AmyIT should not have access to the accounting folder.



Object name: C:\Departments\HR

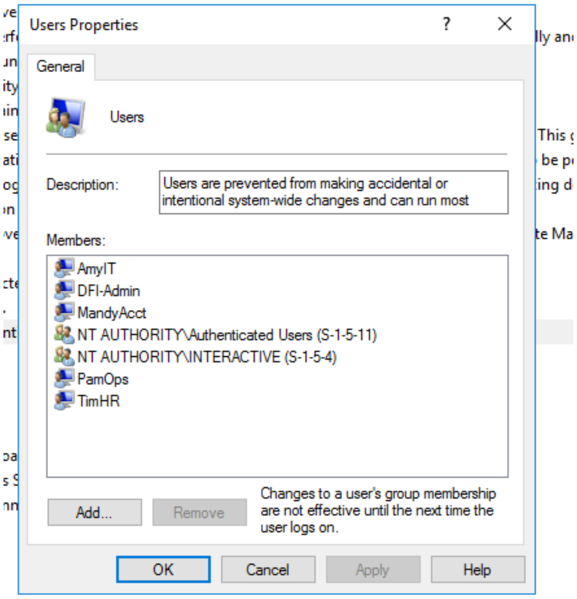
Group or user names:

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

To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.



Users Properties

General

Users

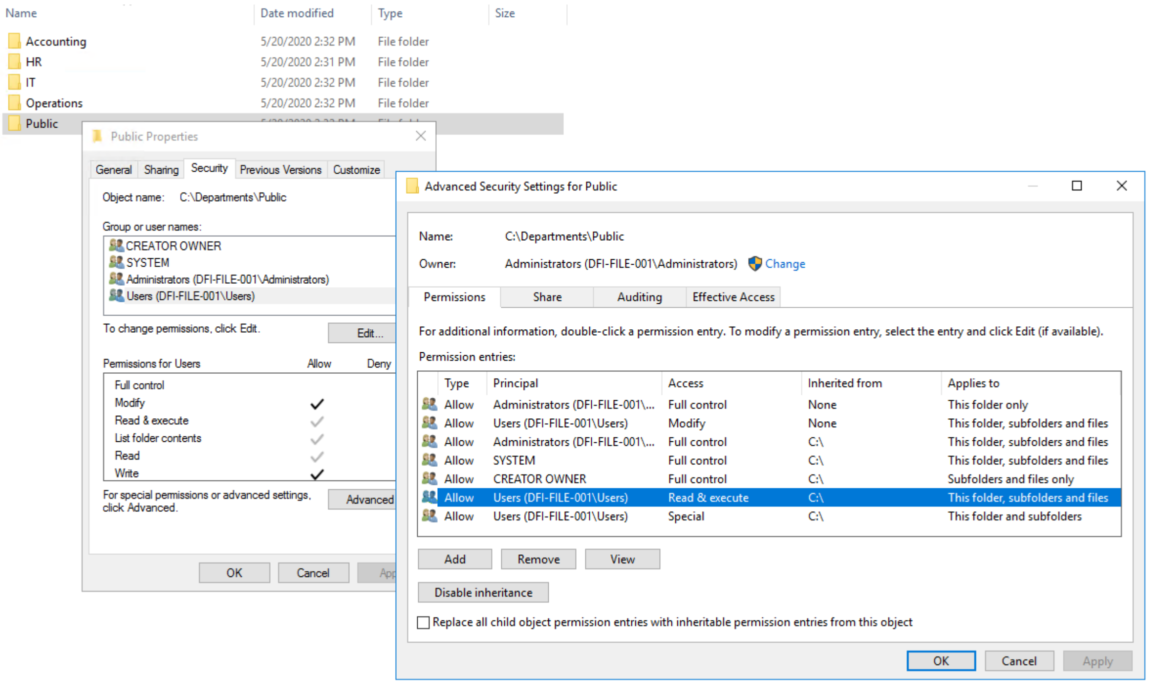
Description: Users are prevented from making accidental or intentional system-wide changes and can run most

Members:

- AmyIT
- DFI-Admin
- MandyAcct
- NT AUTHORITY\Authenticated Users (S-1-5-11)
- NT AUTHORITY\INTERACTIVE (S-1-5-4)
- PamOps
- TimHR

Changes to a user's group membership are not effective until the next time the user logs on.

Users group is also having several accounts such as (AmyIT, MandyAcct, PamOps) that should not have access to the HR folder.



Name	Date modified	Type	Size
Accounting	5/20/2020 2:32 PM	File folder	
HR	5/20/2020 2:31 PM	File folder	
IT	5/20/2020 2:32 PM	File folder	
Operations	5/20/2020 2:32 PM	File folder	
Public			

Public Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Departments\Public

Group or user names:

- CREATOR OWNER
- SYSTEM
- Administrators (DFI-FILE-001\Administrators)
- Users (DFI-FILE-001\Users)

To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.

Advanced Security Settings for Public

Name: C:\Departments\Public

Owner: Administrators (DFI-FILE-001\Administrators) Change

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

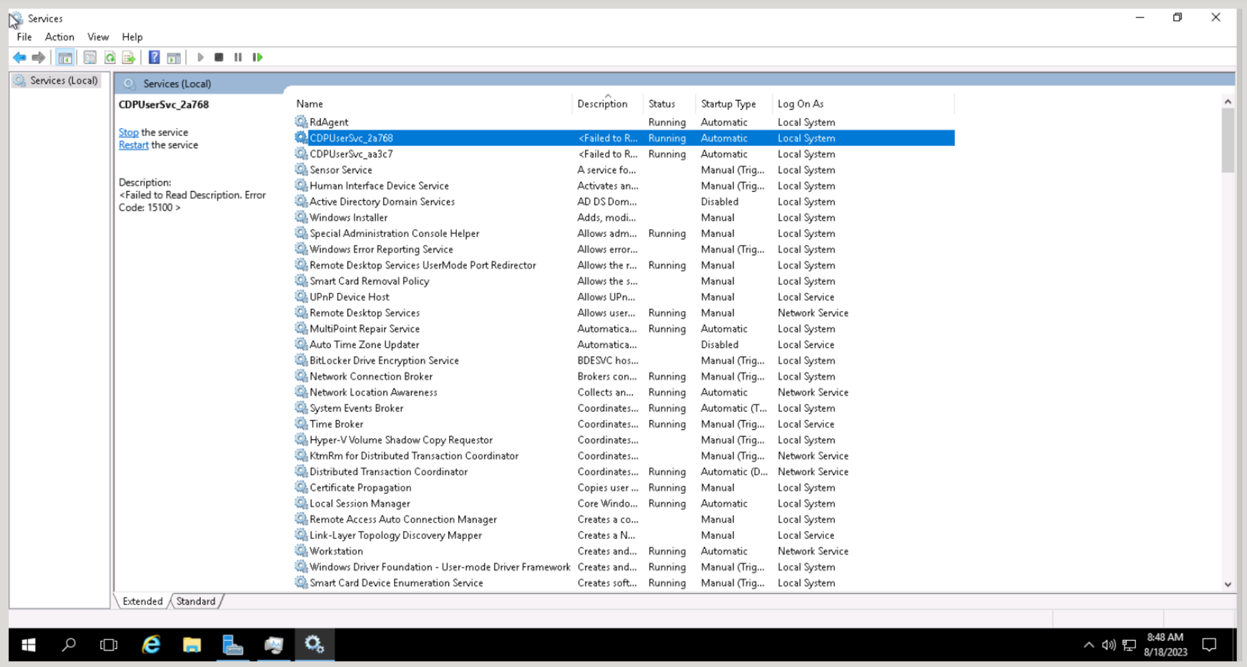
Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (DFI-FILE-001\...	Full control	None	This folder only
Allow	Users (DFI-FILE-001\Users)	Modify	None	This folder, subfolders and files
Allow	Administrators (DFI-FILE-001\...	Full control	C:\	This folder, subfolders and files
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only
Allow	Users (DFI-FILE-001\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (DFI-FILE-001\Users)	Special	C:\	This folder and subfolders

☐ Replace all child object permission entries with inheritable permission entries from this object

Moreover, Users group should not get a Modify and Special privileges in the public folder and should only get a read access if there was no sensitive data will be shared in that folder.

Finally, I have found that administrator group have access to all folders with full control, and even though they are an administrator they should not have access to all folders that belongs to different departments.

Defense-in-Depth



CDPUserSvc_2a768

Stop the service
Restart the service

Description:
<Failed to Read Description. Error Code: 15100 >

Name	Description	Status	Startup Type	Log On As
RdAgent		Running	Automatic	Local System
CDPUserSvc_2a768	<Failed to R...	Running	Automatic	Local System
CDPUserSvc_aa3c7	<Failed to R...	Running	Automatic	Local System
Sensor Service	A service fo...		Manual (Trig...	Local System
Human Interface Device Service	Activates an...		Manual (Trig...	Local System
Active Directory Domain Services	AD DS Dom...		Disabled	Local System
Windows Installer	Adds, modi...		Manual	Local System
Special Administration Console Helper	Allows adm...	Running	Manual	Local System
Windows Error Reporting Service	Allows error...		Manual (Trig...	Local System
Remote Desktop Services UserMode Port Redirector	Allows the r...	Running	Manual	Local System
Smart Card Removal Policy	Allows the s...		Manual	Local System
UPnP Device Host	Allows UPn...		Manual	Local Service
Remote Desktop Services	Allows user...	Running	Manual	Network Service
MultiPoint Repair Service	Automatica...	Running	Automatic	Local System
Auto Time Zone Updater	Automatica...		Disabled	Local Service
BitLocker Drive Encryption Service	BDESVC hos...		Manual (Trig...	Local System
Network Connection Broker	Brokers con...	Running	Manual (Trig...	Local System
Network Location Awareness	Collects an...	Running	Automatic	Network Service
System Events Broker	Coordinates...	Running	Automatic (T...	Local System
Time Broker	Coordinates...	Running	Manual (Trig...	Local Service
Hyper-V Volume Shadow Copy Requestor	Coordinates...		Manual (Trig...	Local System
KtmRm for Distributed Transaction Coordinator	Coordinates...		Manual (Trig...	Network Service
Distributed Transaction Coordinator	Coordinates...	Running	Automatic (D...	Network Service
Certificate Propagation	Copies user ...	Running	Manual	Local System
Local Session Manager	Core Windo...	Running	Automatic	Local System
Remote Access Auto Connection Manager	Creates a co...		Manual	Local System
Link-Layer Topology Discovery Mapper	Creates a N...		Manual	Local Service
Workstation	Creates and...	Running	Automatic	Network Service
Windows Driver Foundation - User-mode Driver Framework	Creates and...	Running	Manual (Trig...	Local System
Smart Card Device Enumeration Service	Creates soft...	Running	Manual (Trig...	Local System

Any unnecessary services should be disabled.

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]

Partner IP: 21.19.241.63 → source ip
Partner Host: WBC-International → the name that we want to call the source ip
DFI IP: 172.21.30.44 → destination ip
DFI Host: DFI-File-001→ the name that we want to call the destination ip
Interface: DFI-Ingress
Port: tcp 9082 → the port where the source will connect to the destination

After gathering all needed information, the firewall rule syntax should be: -
Name 21.19.241.63 WBC-International Name 172.21.30.44 DFI-File-001 Access-list DFI-Ingress extended permit tcp host WBC-International host DFI-File-001 eq 9082

This firewall rule will allow the partner to connect to the system.

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]

According to Cisco guidelines, I recommend using the following recommendations: -

- For an authentication algorithm, I recommend using HMAC-SHA-256 because it provides a high level of security due to the strength of the SHA-256 hash function and is also resistant to various cryptographic attacks, including collision and preimage attacks.
- For an encryption algorithm, I suggest using AES-256 bit because it performs 14 rounds of encryption, making it resistant to brute-force attacks. Moreover, it protects sensitive, unclassified, and classified information.

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 found"; sid:1000000;)
Explanations: -
Alert: alert generating
ICMP: a port that generates error messages, it is commonly used for network devices.
Any: used for the source IP address
Any: used for the source port number
->: a direction
172.21.30.44: destination IP
Any: since ICMP doesn't use a specific port I put any so it will monitor all ports.

[Place your VoIP Admin rule and explanation here]
Alert UDP any any -> 172.21.30.55 69 (msg:"UDP traffic found"; sid:1000001;)
Explanations: -
Alert: alert generating
UDP: I chose UDP rather than TCP because it is commonly used for VoIP (voice over internet protocol).
Any: used for the source IP address
Any: used for the source port number
->: a direction
172.21.30.55: destination IP
69: the port number for TFTP

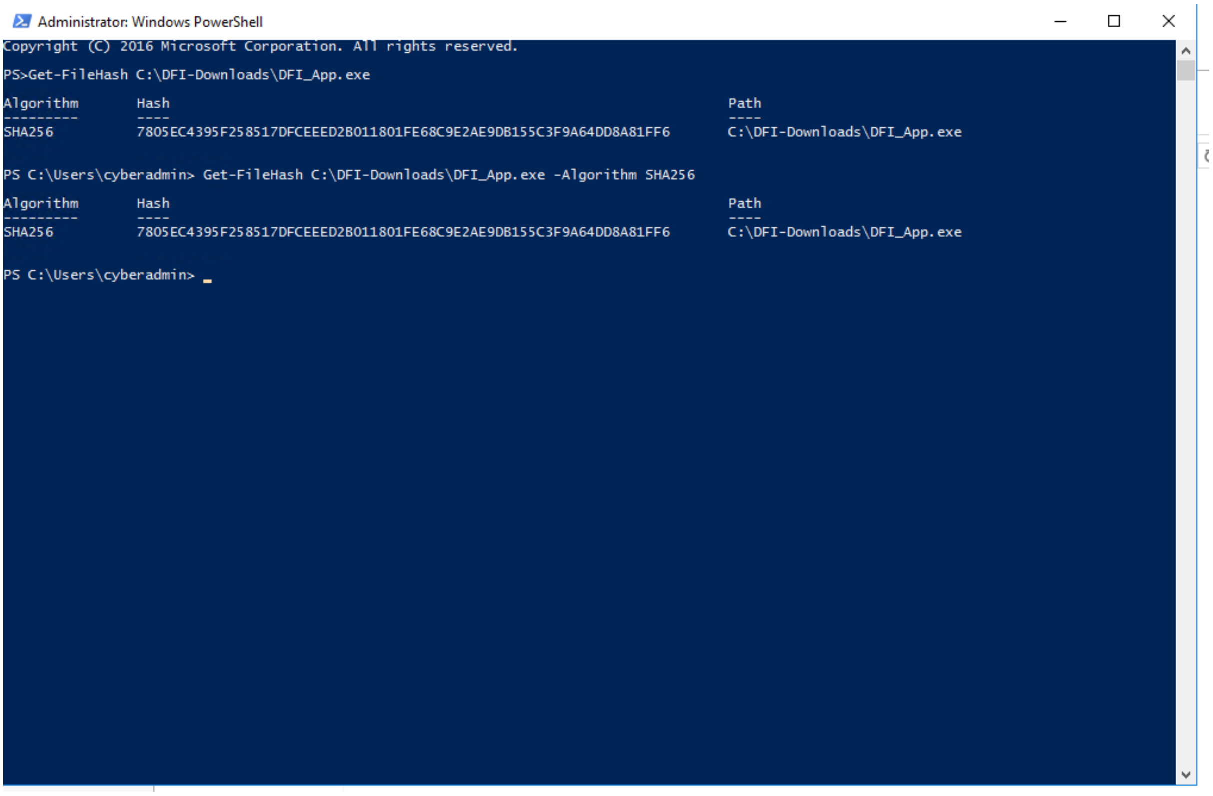
6. **File Hash verification:**

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]



```
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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

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


PS C:\Users\cyberadmin> Get-FileHash C:\DFI-Downloads\DFI_App.exe -Algorithm SHA256

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


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

```
$ Get-FileHash C:\DFI-Downloads\DFI_App.exe -Algorithm SHA256
```

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
SOAR	Devo	The entire threat lifecycle can be automated which will make it easier for the blue team to make a threat case
IDS	Snort	Because it provides opportunities for automation and manual threat hunting and its free to use
Firewall	Vmware NSX	Enables the creation of entire networks in software and embeds them in the hypervisor layer, abstracted from the underlying physical hardware.
SOAR	Fortinet FortiSOAR	Role-based dashboard, reporting capabilities, and incident management. this allows to track metrics, analyze performance, create data models, generate weekly reports
SIEM	Datadog security monitoring	A cloud-native network monitoring and management system that includes real-time security monitoring and log management. Comes with over 600 vendor integrations out-of-the-box.
NDR	Cisco Stealthwatch Enterprise	Because it protects against DDoS attacks, intrusion, malware, and insider threats. It also runs on Cisco's cloud platform.
EDR	Cisco Secure Endpoint	Because it monitors the behavior of each protected device for malicious activities, ensuring that threats are identified quickly. When a

		threat is found, Secure Endpoint isolates the infected endpoint from the rest of the network, allowing security teams to mitigate the issue before it can spread to other machines.
XDR	Heimdal Security XDR	This cloud-based system provides an XDR service by extending protection to each endpoint on a network through on-device agents and coordinating threat intelligence and responses between devices.
Sandbox	FortiSandbox	Is high performance security solution which comes with AI and Machines learning technology, which makes FortiSandbox robust and help organization to identify and isolate the advanced threats in real time.

8. **Logging RDP Attempts:**

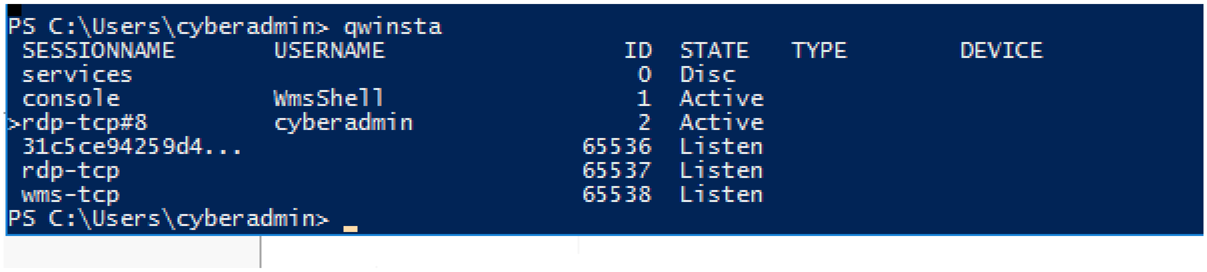
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

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.

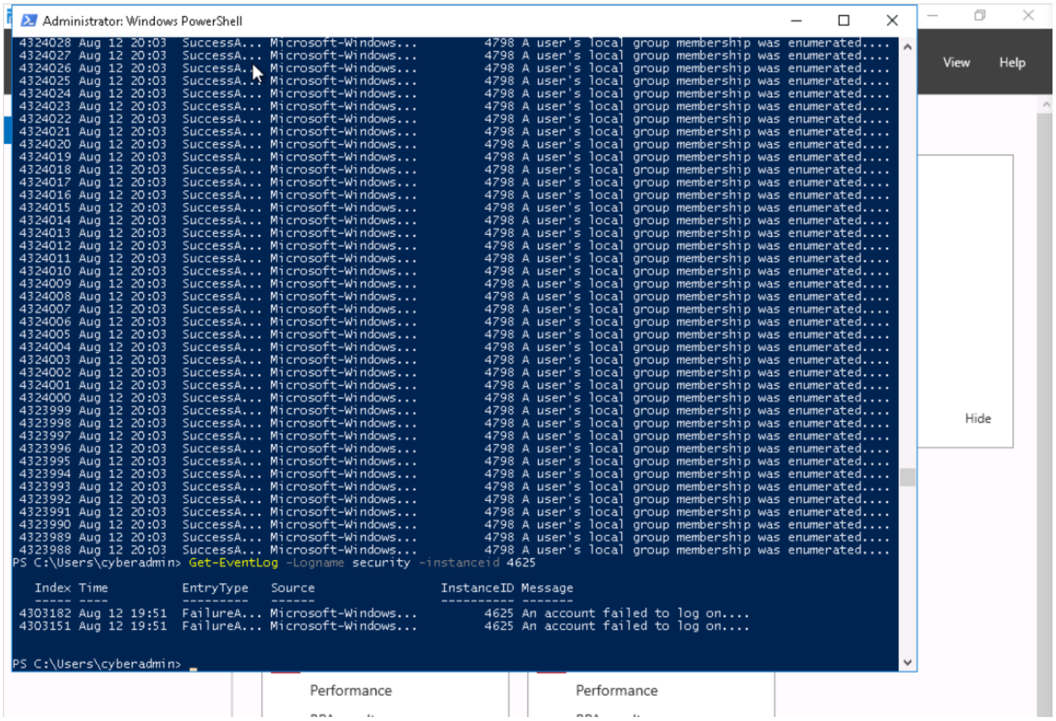
For your deliverable, open the CSV with notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below explain your findings, recommendations and justifications to the IT Manager.

[Place IT Manager Report Here]

```
Get-EventLog Security | Where-Object {$_.EventID -eq "4625"} | Export-CSV "C:\Users\cyberadmin\Desktop\SystemEvents8.CSV"
```



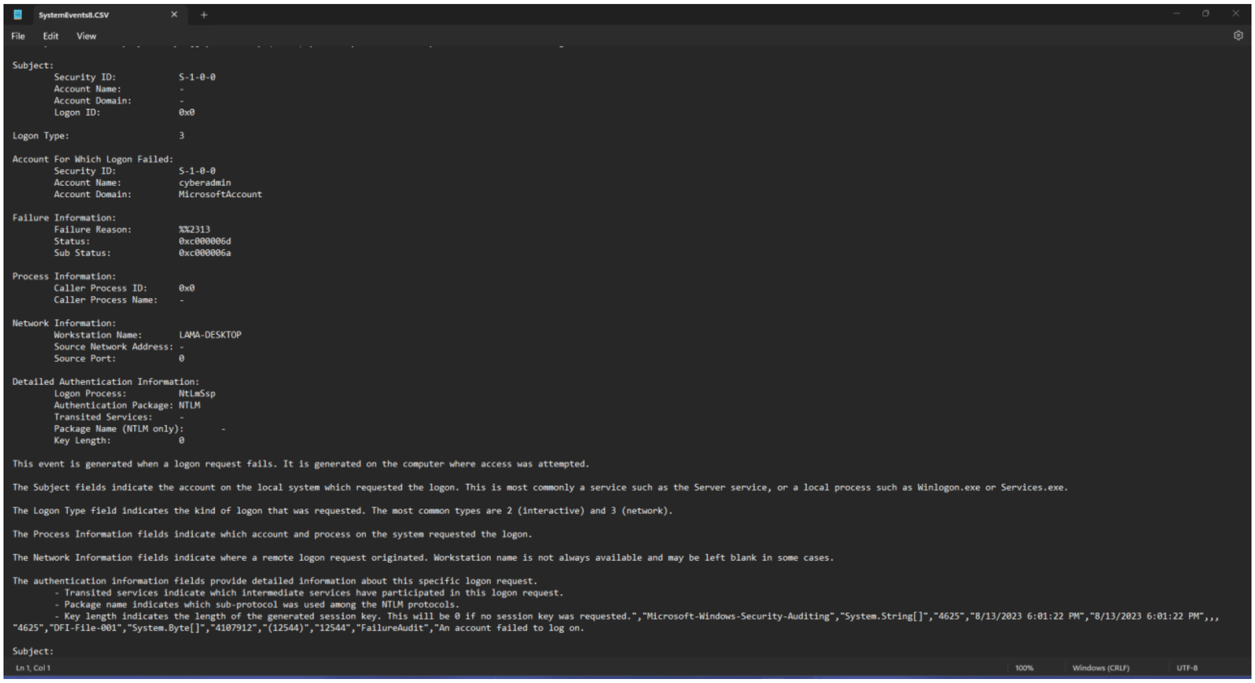
```
PS C:\Users\cyberadmin> qwinsta
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 console           WmsShell                  1  Active
>rdp-tcp#8         cyberadmin                2  Active
 31c5ce94259d4...                        65536  Listen
 rdp-tcp                                 65537  Listen
 wms-tcp                                 65538  Listen
PS C:\Users\cyberadmin> _
```



```
 4324028 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324027 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324026 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324025 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324024 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324023 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324022 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324021 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324020 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324019 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324018 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324017 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324016 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324015 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324014 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324013 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324012 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324011 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324010 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324009 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324008 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324007 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324006 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324005 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324004 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324003 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324002 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324001 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4324000 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323999 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323998 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323997 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323996 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323995 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323994 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323993 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323992 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323991 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323990 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323989 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
 4323988 Aug 12 20:03  SuccessA... Microsoft-Windows...          4798 A user's local group membership was enumerated....
PS C:\Users\cyberadmin> Get-EventLog -Logname security -instanceid 4625

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
 4303182 Aug 12 19:51  FailureA... Microsoft-Windows...          4625 An account failed to log on....
 4303151 Aug 12 19:51  FailureA... Microsoft-Windows...          4625 An account failed to log on....


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



```
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:		cyberadmin
	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:	LAMA-DESKTOP
	Source Network Address:	-
	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","8/13/2023 6:01:22 PM","8/13/2023 6:01:22 PM",,,
"4625","DFI-File-001","System.Byte[]","4107912","(12544)","12544","FailureAudit","An account failed to log on.

Subject:
```

SystemEvents8.CSV

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
Windows Server 2022/ Remote Code Execution / CVE-2023-36910	update	This update is important because the attack complexity is low and doesn't require any privilege or user interaction which makes it easy for the threat actor to exploit this vulnerability and attacks the confidentiality, availability and integrity of the

		system.
Windows 10 Version 1809 for 32-bit Systems / Remote Code Execution / CVE-2023-36910	update	This vulnerability is associated with the network, and it doesn't require any privileges or user interaction and has a low complexity, which makes it an easy exploit for the threat actor to attack the confidentiality, availability and the integrity of the system.
Windows Remote Desktop / Security Feature Bypass / CVE-2023-35352	update	Since this attack has a low complexity and doesn't require any privileges or user interaction it will be easy for the attacker to exploit it and attack the integrity of the system.
Windows Server 2019 (Server Core installation) / Remote Code Execution / CVE-2023-36910	update	This vulnerability attacks the network and has a low attack complexity that doesn't require any user interaction and privileges, which will make it an easy for the threat actor to attack the confidentiality, integrity, and the availability of the system.
Memory Integrity System Readiness Scan Tool Defense in Depth Update / ADV230004	Ignore	This update is used to check for compatibility issues with memory integrity and is not related to security.
Microsoft Edge (Chromium-based) Spoofing Vulnerability / Spoofing / CVE-2023-35392	Ignore	This vulnerability is a network-based attack that involves user interaction and has low severity. So, I don't think it needs much attention if the organization has a strong security defense system and employees that are knowledgeable about certain attacks.

Windows Server 2019 / Defense in Depth / ADV230001	Ignore	There is no need for an update because the server is using Windows Server 2016, and this update is related to Windows Server 2019.

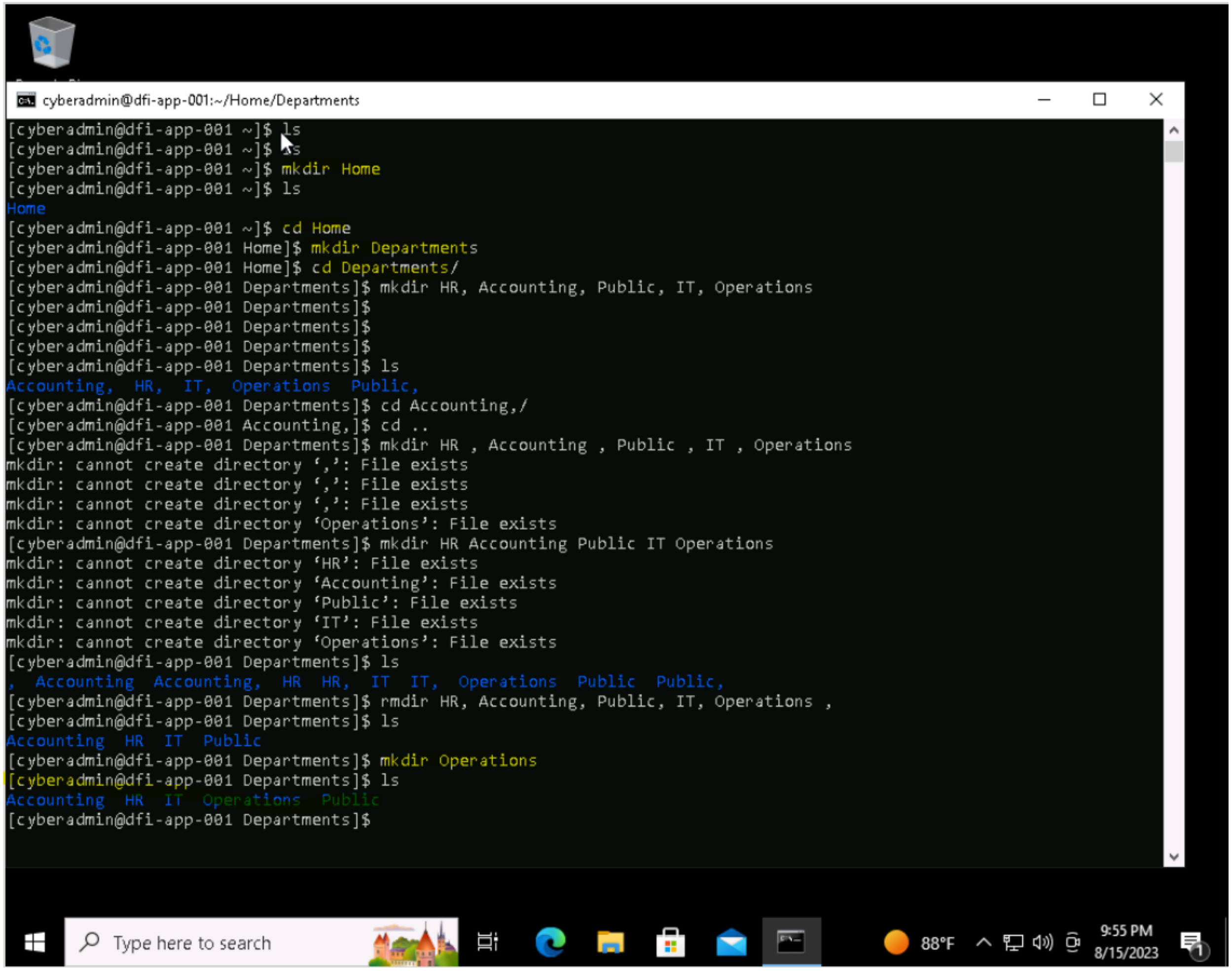
10. **Linux Data Directories:**

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.

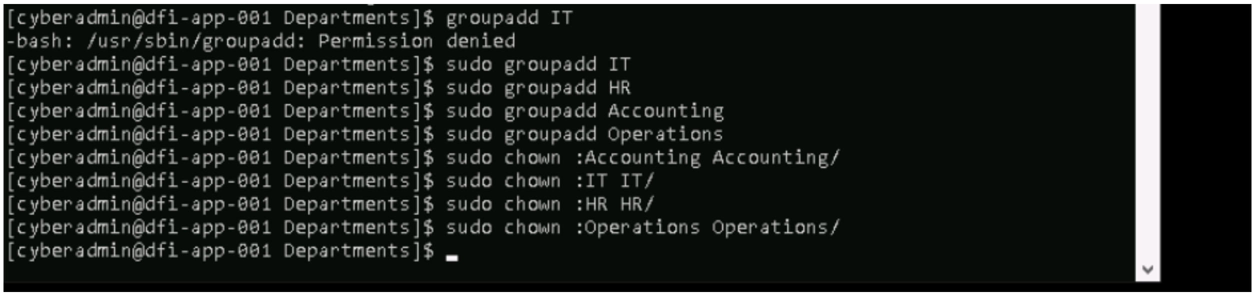
For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

[Provide a screenshot(s) of completed tasks and the correctly set permissions here]
[Provide your non-technical syntax explanation for management here]



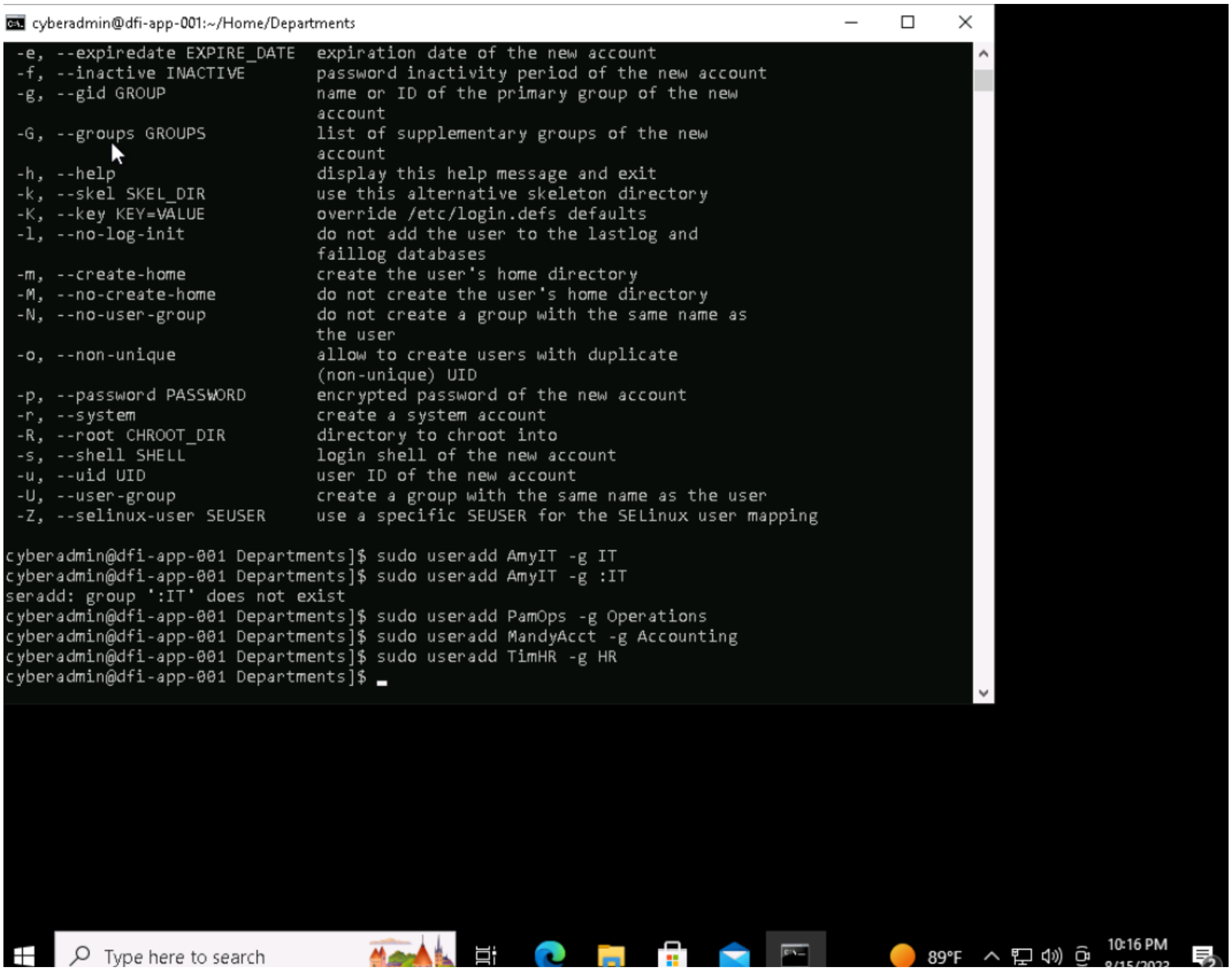
```
[cyberadmin@dfi-app-001 ~]$ ls
[cyberadmin@dfi-app-001 ~]$ ls
[cyberadmin@dfi-app-001 ~]$ mkdir Home
[cyberadmin@dfi-app-001 ~]$ ls
Home
[cyberadmin@dfi-app-001 ~]$ cd Home
[cyberadmin@dfi-app-001 Home]$ mkdir Departments
[cyberadmin@dfi-app-001 Home]$ cd Departments/
[cyberadmin@dfi-app-001 Departments]$ mkdir HR, Accounting, Public, IT, Operations
[cyberadmin@dfi-app-001 Departments]$
[cyberadmin@dfi-app-001 Departments]$
[cyberadmin@dfi-app-001 Departments]$
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting,  HR,  IT,  Operations  Public,
[cyberadmin@dfi-app-001 Departments]$ cd Accounting,/
[cyberadmin@dfi-app-001 Accounting,]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ mkdir HR , Accounting , Public , IT , Operations
mkdir: cannot create directory ‘,’: File exists
mkdir: cannot create directory ‘,’: File exists
mkdir: cannot create directory ‘,’: File exists
mkdir: cannot create directory ‘Operations’: File exists
[cyberadmin@dfi-app-001 Departments]$ mkdir HR Accounting Public IT Operations
mkdir: cannot create directory ‘HR’: File exists
mkdir: cannot create directory ‘Accounting’: File exists
mkdir: cannot create directory ‘Public’: File exists
mkdir: cannot create directory ‘IT’: File exists
mkdir: cannot create directory ‘Operations’: File exists
[cyberadmin@dfi-app-001 Departments]$ ls
,  Accounting  Accounting,  HR  HR,  IT  IT,  Operations  Public  Public,
[cyberadmin@dfi-app-001 Departments]$ rmdir HR, Accounting, Public, IT, Operations ,
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting  HR  IT  Public
[cyberadmin@dfi-app-001 Departments]$ mkdir Operations
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting  HR  IT  Operations  Public
[cyberadmin@dfi-app-001 Departments]$
```

At first I made a directory in root file and called it Home, then changed the directory to Home and made a sub folder and called it Departments. After that I made 4 subdirectories in the Departments folder and I tagged them with HR, Accounting, Public, IT, Operations. All of that just by using mkdir command for making the directory and cd command to move from one directory to another.



```
[cyberadmin@dfi-app-001 Departments]$ groupadd IT
-bash: /usr/sbin/groupadd: Permission denied
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chown :Accounting Accounting/
[cyberadmin@dfi-app-001 Departments]$ sudo chown :IT IT/
[cyberadmin@dfi-app-001 Departments]$ sudo chown :HR HR/
[cyberadmin@dfi-app-001 Departments]$ sudo chown :Operations Operations/
[cyberadmin@dfi-app-001 Departments]$ _
```

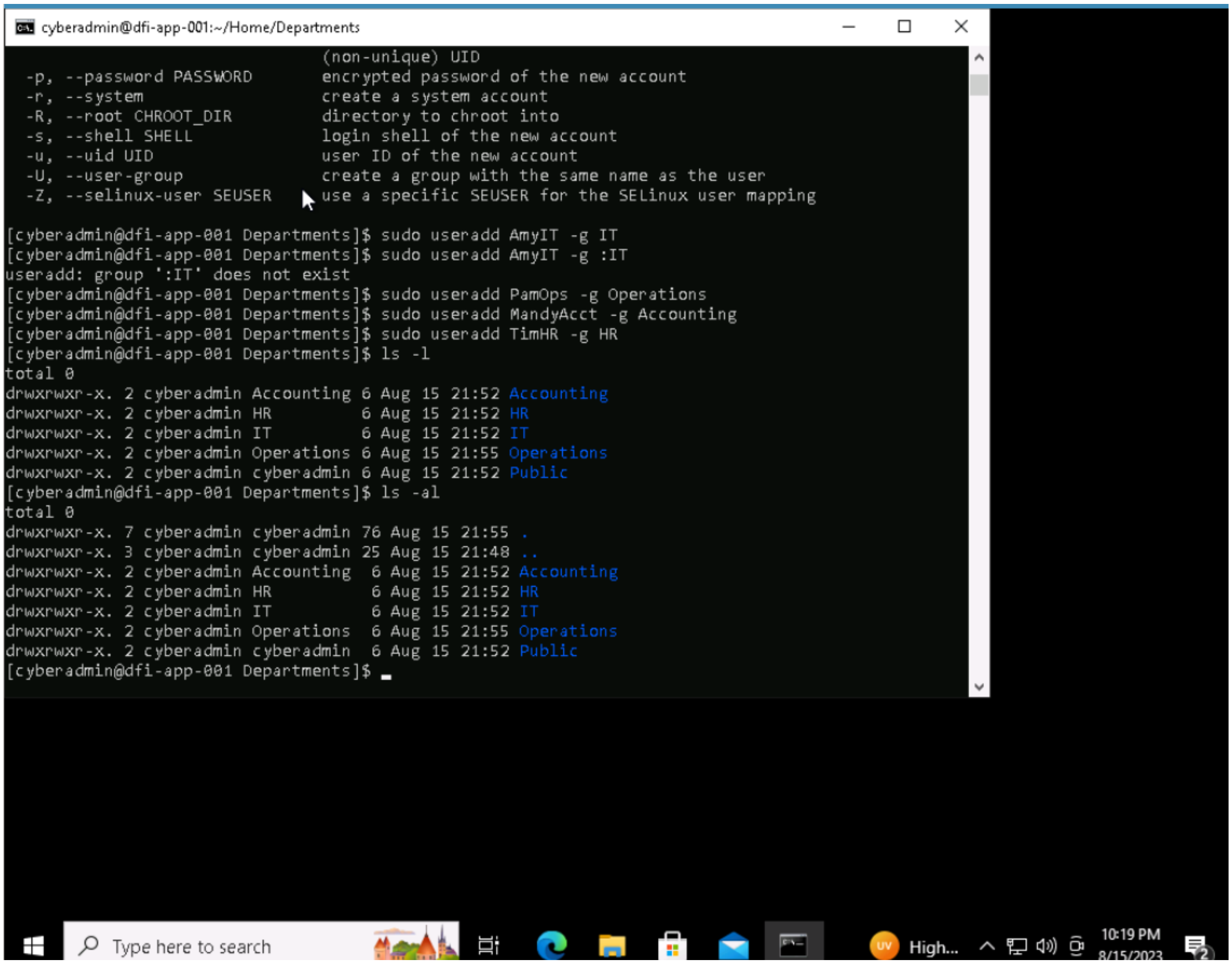
I made multiple groups with a sudo privilege then assigned them to their own folders by using groupadd to create the users and chown for the assigning part.



```
 -e, --expiredate EXPIRE_DATE  expiration date of the new account
 -f, --inactive INACTIVE       password inactivity period of the new account
 -g, --gid GROUP               name or ID of the primary group of the new
                               account
 -G, --groups GROUPS           list of supplementary groups of the new
                               account
 -h, --help                    display this help message and exit
 -k, --skel SKEL_DIR           use this alternative skeleton directory
 -K, --key KEY=VALUE           override /etc/login.defs defaults
 -l, --no-log-init             do not add the user to the lastlog and
                               faillog databases
 -m, --create-home             create the user's home directory
 -M, --no-create-home          do not create the user's home directory
 -N, --no-user-group           do not create a group with the same name as
                               the user
 -o, --non-unique              allow to create users with duplicate
                               (non-unique) UID
 -p, --password PASSWORD       encrypted password of the new account
 -r, --system                  create a system account
 -R, --root CHROOT_DIR         directory to chroot into
 -s, --shell SHELL             login shell of the new account
 -u, --uid UID                 user ID of the new account
 -U, --user-group              create a group with the same name as the user
 -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mapping

cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT -g IT
cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT -g :IT
seradd: group ':IT' does not exist
cyberadmin@dfi-app-001 Departments]$ sudo useradd PamOps -g Operations
cyberadmin@dfi-app-001 Departments]$ sudo useradd MandyAcct -g Accounting
cyberadmin@dfi-app-001 Departments]$ sudo useradd TimHR -g HR
cyberadmin@dfi-app-001 Departments]$ 
```

I created multiple users and assigned them to their own group by using sudo privilege, after that I wrote useradd command to add them then followed the command with the name of the user and -g command to assign the user to their own primary group and followed it by the name of the group.



```
                                (non-unique) UID
  -p, --password PASSWORD       encrypted password of the new account
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             login shell of the new account
  -u, --uid UID                 user ID of the new account
  -U, --user-group              create a group with the same name as the user
  -Z, --selinux-user SEUSER     use a specific SEUSER for the SELinux user mapping

[cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT -g IT
[cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT -g :IT
useradd: group ':IT' does not exist
[cyberadmin@dfi-app-001 Departments]$ sudo useradd PamOps -g Operations
[cyberadmin@dfi-app-001 Departments]$ sudo useradd MandyAcct -g Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo useradd TimHR -g HR
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
drwxrwxr-x. 2 cyberadmin Accounting 6 Aug 15 21:52 Accounting
drwxrwxr-x. 2 cyberadmin HR         6 Aug 15 21:52 HR
drwxrwxr-x. 2 cyberadmin IT         6 Aug 15 21:52 IT
drwxrwxr-x. 2 cyberadmin Operations 6 Aug 15 21:55 Operations
drwxrwxr-x. 2 cyberadmin cyberadmin 6 Aug 15 21:52 Public
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxrwxr-x. 7 cyberadmin cyberadmin 76 Aug 15 21:55 .
drwxrwxr-x. 3 cyberadmin cyberadmin 25 Aug 15 21:48 ..
drwxrwxr-x. 2 cyberadmin Accounting  6 Aug 15 21:52 Accounting
drwxrwxr-x. 2 cyberadmin HR          6 Aug 15 21:52 HR
drwxrwxr-x. 2 cyberadmin IT          6 Aug 15 21:52 IT
drwxrwxr-x. 2 cyberadmin Operations  6 Aug 15 21:55 Operations
drwxrwxr-x. 2 cyberadmin cyberadmin  6 Aug 15 21:52 Public
[cyberadmin@dfi-app-001 Departments]$
```

Used $ ls -al to display the complete list of the directory.

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. The server connection should be open for the required user as well as for a particular source IP address and port.
2. The max login attempt should be limited. Ex: no more than 3 attempts per 30 minutes.
3. Any unusual traffic comes from an inbound IP address or port should get blocked.
4. Organizations should permit the connection of inbound IP address for the ones needed by the organization.

5. User activities while connection should be logged.
6. Root remote login should get disabled.
7. Users should use a strong password to login.
8. Any brute force attempt should get blocked automatically.
9. Since port 22 is vulnerable to unauthorized access, it is recommended to close the port and run the server using another port that is only accessible via an authorized IP and port.
10. A VPN should be used to connect to the server so all traffic will be encrypted to prevent potential MITM attacks.

Note: Unusual IP addresses should get blocked for a long time (ex: not more than 24 hours) and only if it is determined that they are a malicious IP source by looking at their status using several tools such as AbuseIPDB, VirusTotal, IPInfo, etc. Otherwise, it is recommended to block them for a short time only Ex: no more than 30 minutes.

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]

After exploring the system and following standard security procedures, I applied the following changes: -

- Implementing the concept of least privilege by assigning users to their folders and removing any unauthorized access.
- Adopting the principle of defense-in-depth on Windows services.
- Suggested the best option for VPN encryption algorithm using Cisco guidelines.
- Configured several IDS rules.
- Recommended several DFI technologies.
- Recommended several Windows updates.
- Created several directories for Linux system using the principle of least privilege.

- Suggested a firewall mitigation response for unusual attempts from inbound traffic.

In addition, I recommend applying the NIST and ISO 27001 frameworks along with the following products from Cisco to elevate security: -

1. Cisco Security Packet Analyzer
2. Cisco Secure Firewall ASDM

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.