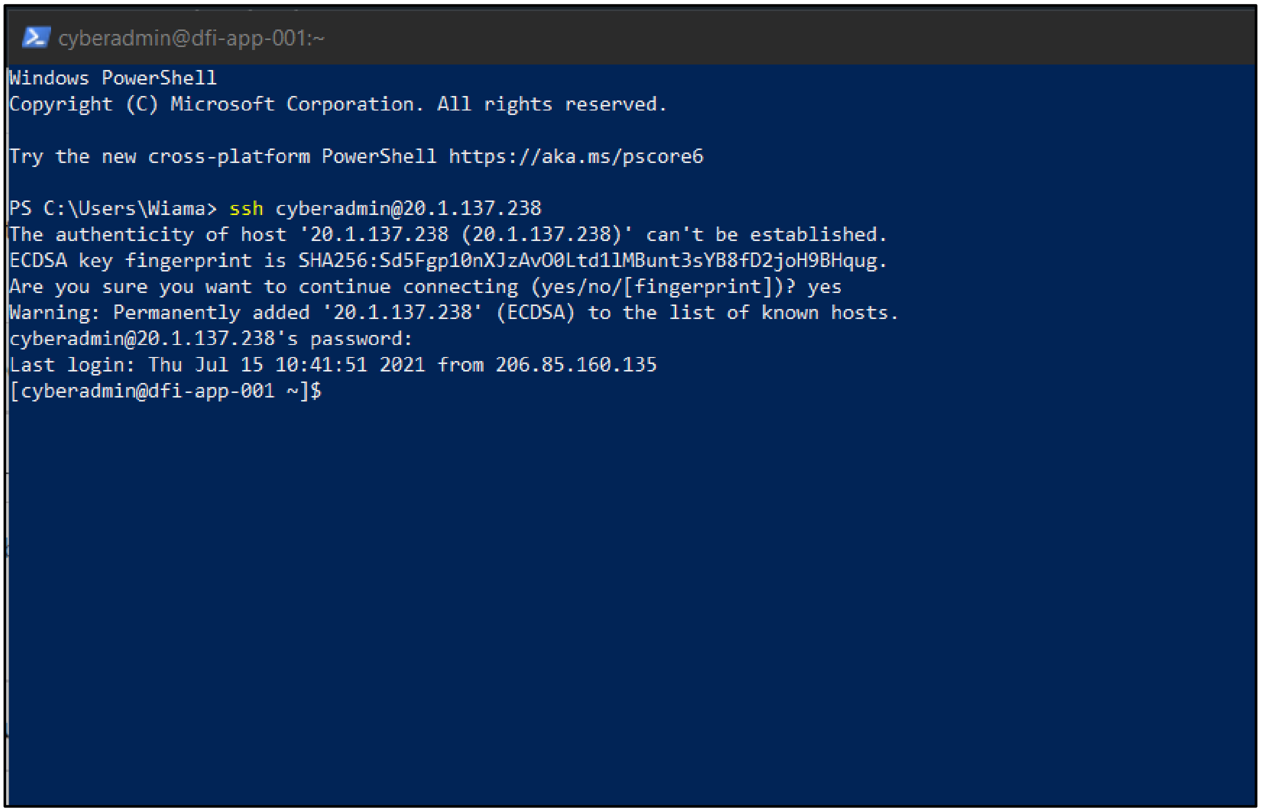
Scenario:

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:**

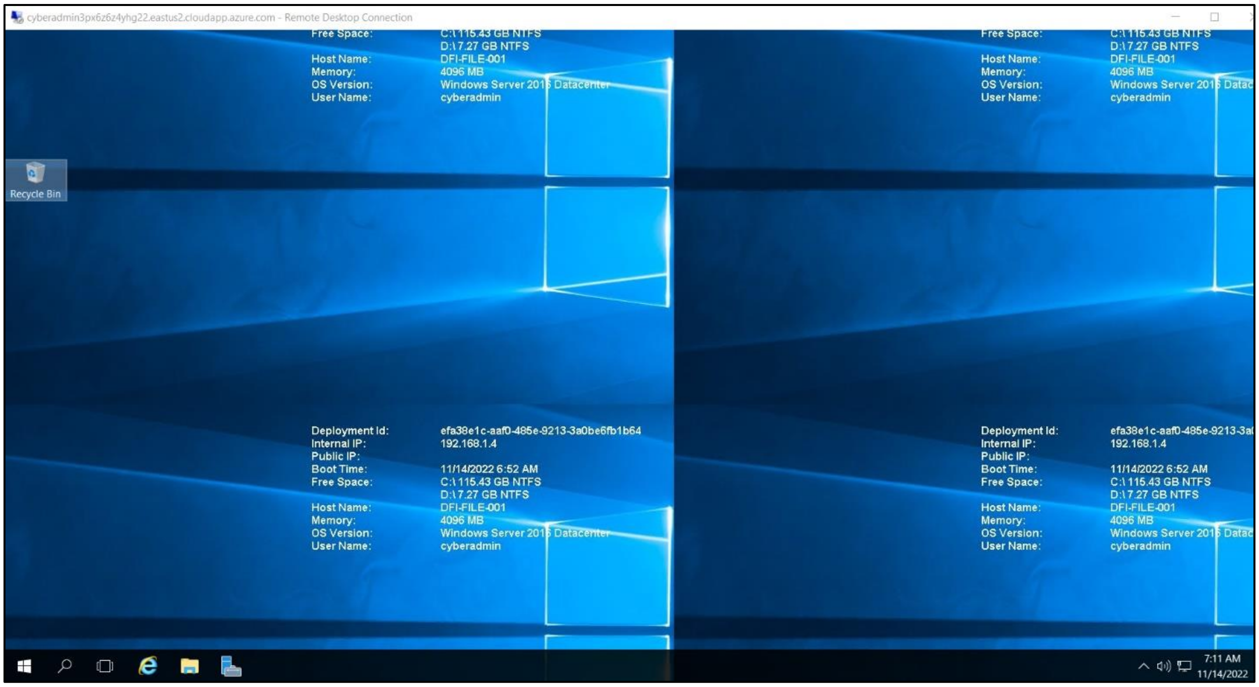
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.
[Please Provide Screenshots of the RDP and SSH here as evidence that you completed this step.]



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

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

PS C:\Users\Wiama> ssh cyberadmin@20.1.137.238
The authenticity of host '20.1.137.238 (20.1.137.238)' 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 '20.1.137.238' (ECDSA) to the list of known hosts.
cyberadmin@20.1.137.238's password:
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$
```



cyberadmin3px6z6z4yhg22.eastus2.cloudapp.azure.com - Remote Desktop Connection

```
Free Space:         C:\ 115.43 GB NTFS
                    D:\ 7.27 GB NTFS
Host Name:          DFI-FILE-001
Memory:             4096 MB
OS Version:         Windows Server 2016 Datacenter
User Name:          cyberadmin
```

```
Free Space:         C:\ 115.43 GB NTFS
                    D:\ 7.27 GB NTFS
Host Name:          DFI-FILE-001
Memory:             4096 MB
OS Version:         Windows Server 2016 Datac
User Name:          cyberadmin
```

```
Deployment Id:      efa38e1c-aaf0-485e-9213-3a0be6fb1b64
Internal IP:        192.168.1.4
Public IP:
Boot Time:          11/14/2022 6:52 AM
Free Space:         C:\ 115.43 GB NTFS
                    D:\ 7.27 GB NTFS
Host Name:          DFI-FILE-001
Memory:             4096 MB
OS Version:         Windows Server 2016 Datacenter
User Name:          cyberadmin
```

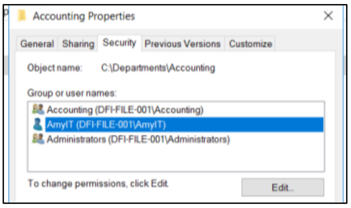
```
Deployment Id:      efa38e1c-aaf0-485e-9213-3a
Internal IP:        192.168.1.4
Public IP:
Boot Time:          11/14/2022 6:52 AM
Free Space:         C:\ 115.43 GB NTFS
                    D:\ 7.27 GB NTFS
Host Name:          DFI-FILE-001
Memory:             4096 MB
OS Version:         Windows Server 2016 Datac
User Name:          cyberadmin
```

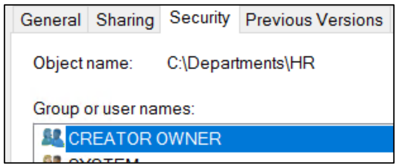
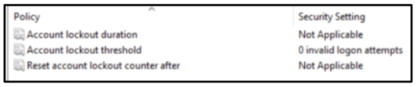
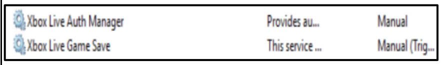
2. **Security Analysis:**

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.)

Issue	Explanation	Recommendation
Permissions: User AmyIT has access to Accounting file.  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...	AmyIT has read/execute privileges on Accounting file. She is from IT department and should not be permitted to access this file.	Apply least privilege by removing AmyIT's access from Accounting folder.

Permissions: CREATOR OWNER group has special permission on HR, IT, and Operations folders  Object name: C:\Departments\HR Group or user names: CREATOR OWNER	The name CREATOR OWNER doesn't specify the role of this group (admin, employee in a department). Also, it doesn't justify why they have special permissions on all the folders.	If CREATOR OWNER are admins, they should be placed under admin group and be given the same privileges If they are employees from a department, least privilege principle should be applied on their access rights.
policies: No account lockout policy applied  Policy — Security Setting Account lockout duration — Not Applicable Account lockout threshold — 0 invalid logon attempts Reset account lockout counter after — Not Applicable	This can increase the risk of unauthorized access to different accounts especially that there aren't any policies that force passwords to be strong	Set a proper password policy and lockout policy
Services: Xbox service startup type is "manual"  Xbox Live Auth Manager — Provides au... — Manual Xbox Live Game Save — This service ... — Manual (Trig...	This service should not be needed in a working environment. It may consume resources	Change startup type to "Disable"

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.

The Rule

```
name 172.21.30.44 DFI_IP
name 21.19.241 WBC_IP
access-list DFI-Ingress extended permit tcp host DFI_IP host WBC_IP eq 9082
```

The explanation:

1- **DFI-Ingress:** the interface being used
2- **Extended permit:** allowing the access
3- **Tcp:** protocol used

4- **DFI_IP, WBC_IP:** IP addresses used for communication, host and destination, respectively
5- **Eq 9082:** name of the port being used

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.

After going through Cisco recommendations, I believe the symmetric encryption AES-256 should be used along with hashing function because it fits the sensitive nature of payrolls.

A key of length 256-bit provides high security. The hash function SHA-256 will add more layer of security by ensuring authentication and integrity

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.

```
alert ICMP any any -> 172.21.30.44 any (msg: “Abnormal ICMP traffic detected”; sid:10000001;)
```

alert ICMP: alerting for ICMP protocol
any any: the traffic coud be coming from any source on any port number
172.21.30.44: company’s IP address
Msg: the message that will be displayed

```
alert TFTP any any -> 172.21.30.55 any (msg: “ connection via TFTP is detected”; sid:10000002;)
```

alert TFTP: alerting for TFTP protocol
any any: the traffic coud be coming from any source on any port number
172.21.30.55: server’s IP address
Msg: the message that will be displayed

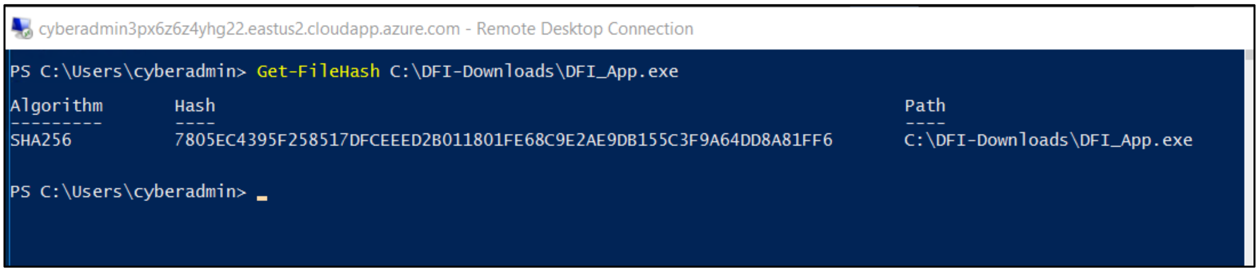
6. **File Hash verification:**

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.

The hashes are identical, that means the program is authentic and integrity was preserved in transporting the file


cyberadmin3px6z6z4yhg22.eastus2.cloudapp.azure.com - Remote Desktop Connection

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

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


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

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.

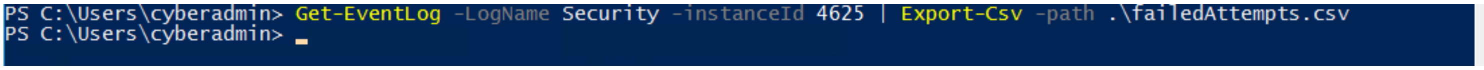
DFI Area/Technology	Solution (product)	Justification for Recommendation
Audit logging	Datadog	Datadog provides: - complete audit logging records. - Logs can be filtered and listed based on different criteria which enhances the speed when looking for specific information - Shared access for team and alerting critical events for fast action
Incident Response	IBM Resilient	- It addresses threats fast and uses machine learning to automate responses to threats - It keeps records for everything it does and allows team access to records
Vulnerability/ incident management	SIRP	- Collects data from different business resources - It categorizes the data to incident or vulnerability - It gives a score to each incident and vulnerability and generate alerts accordingly

8. **Logging RDP Attempts:**

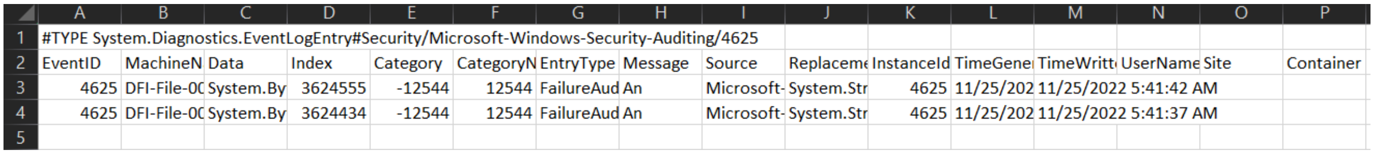
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

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.



```
PS C:\Users\cyberadmin> Get-EventLog -LogName Security -instanceId 4625 | Export-Csv -path .\failedAttempts.csv
PS C:\Users\cyberadmin> _
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	#TYPE System.Diagnostics.EventLogEntry#Security/Microsoft-Windows-Security-Auditing/4625															
2	EventID	MachineN	Data	Index	Category	CategoryN	EntryType	Message	Source	Replaceme	InstanceId	TimeGene	TimeWritt	UserName	Site	Container
3	4625	DFI-File-0(	System.By	3624555	-12544	12544	FailureAud	An	Microsoft-	System.Str	4625	11/25/202	11/25/2022 5:41:42 AM			
4	4625	DFI-File-0(	System.By	3624434	-12544	12544	FailureAud	An	Microsoft-	System.Str	4625	11/25/202	11/25/2022 5:41:37 AM			
5																

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
CVE-2022-41064. Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Microsoft server operating system version	Update	- This update fixes a vulnerability that causes the system to return inaccurate data. - Also, it fixes Information Disclosure Vulnerability
KB5020000	Update	- It raises authentication level. This is marked

		as a critical update and it's associated with security
KB5019961 CVE-2022-41045	Update	- It addresses security issues for Windows operating system. - security improvements to internal OS functionality
CVE-2022-3890 Microsoft Edge (Chromium-based)	Ignore	- No serious security impact

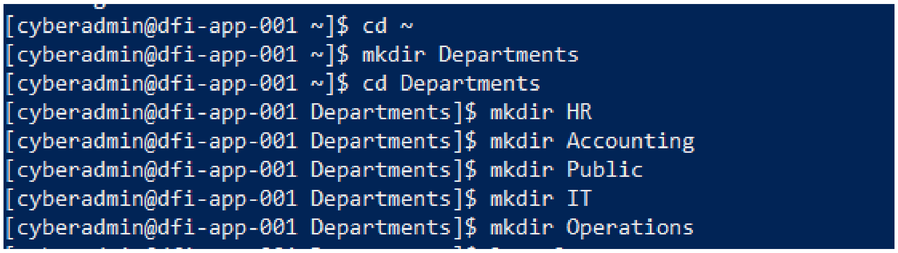
10. **Linux Data Directories:**

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.

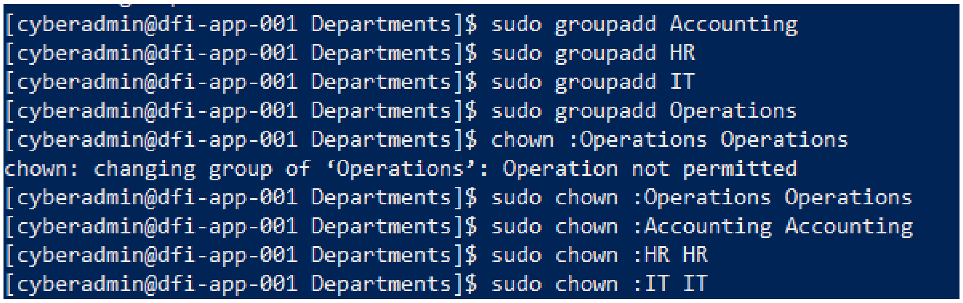
For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.
(each image will have a brief explanation about the command)

Creating the directories using mkdir command



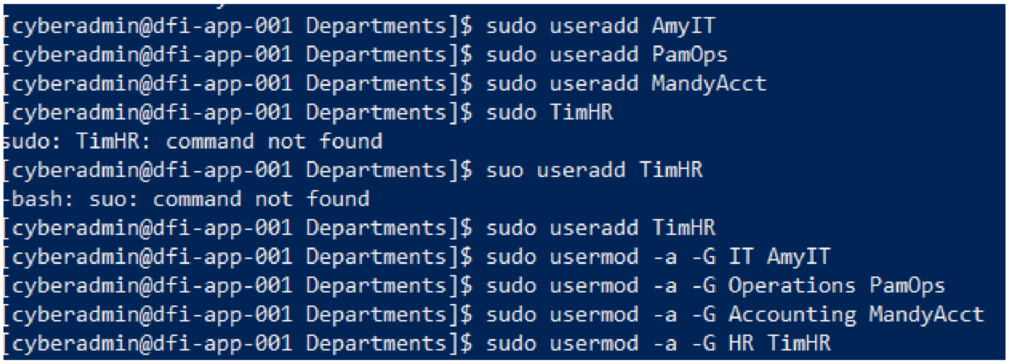
```
[cyberadmin@dfi-app-001 ~]$ cd ~
[cyberadmin@dfi-app-001 ~]$ mkdir Departments
[cyberadmin@dfi-app-001 ~]$ cd Departments
[cyberadmin@dfi-app-001 Departments]$ mkdir HR
[cyberadmin@dfi-app-001 Departments]$ mkdir Accounting
[cyberadmin@dfi-app-001 Departments]$ mkdir Public
[cyberadmin@dfi-app-001 Departments]$ mkdir IT
[cyberadmin@dfi-app-001 Departments]$ mkdir Operations
```

creating groups using groupadd command
making the groups owners using chown command
sudo is used to give elevated priviliges (to execute some commands)



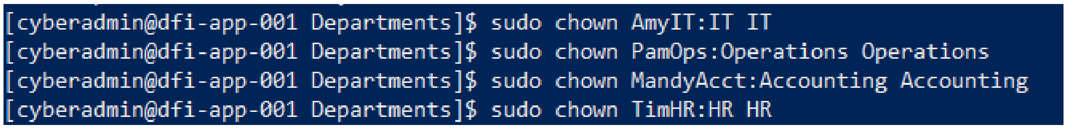
```
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
[cyberadmin@dfi-app-001 Departments]$ chown :Operations Operations
chown: changing group of ‘Operations’: Operation not permitted
[cyberadmin@dfi-app-001 Departments]$ sudo chown :Operations Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chown :Accounting Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chown :HR HR
[cyberadmin@dfi-app-001 Departments]$ sudo chown :IT IT
```

creating users and adding them to the groups
useradd is the command
ex: AmyIT is the user name



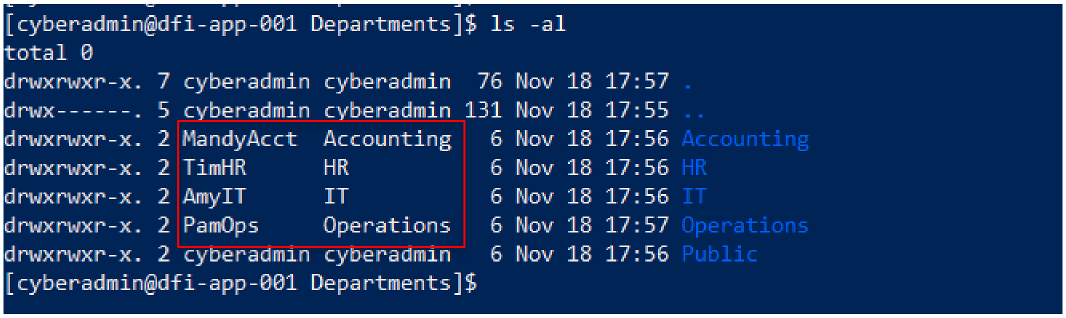
```
[cyberadmin@dfi-app-001 Departments]$ sudo useradd AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo useradd PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo useradd MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo TimHR
sudo: TimHR: command not found
[cyberadmin@dfi-app-001 Departments]$ suo useradd TimHR
-bash: suo: command not found
[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
```

Changing the owner from admin to users so they can read/write/ execute
Chown is the command
Ex:
AmyIT is the user we want to give read,write, execute privileges
IT is the group
Second IT is the name of the folder



```
[cyberadmin@dfi-app-001 Departments]$ sudo chown AmyIT:IT IT
[cyberadmin@dfi-app-001 Departments]$ sudo chown PamOps:Operations Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chown MandyAcct:Accounting Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chown TimHR:HR HR
```

The final result : The owners have now changed



```
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxrwxr-x. 7 cyberadmin cyberadmin  76 Nov 18 17:57 .
drwx------. 5 cyberadmin cyberadmin 131 Nov 18 17:55 ..
drwxrwxr-x. 2 MandyAcct  Accounting   6 Nov 18 17:56 Accounting
drwxrwxr-x. 2 TimHR      HR           6 Nov 18 17:56 HR
drwxrwxr-x. 2 AmyIT      IT           6 Nov 18 17:56 IT
drwxrwxr-x. 2 PamOps     Operations   6 Nov 18 17:57 Operations
drwxrwxr-x. 2 cyberadmin cyberadmin   6 Nov 18 17:56 Public
[cyberadmin@dfi-app-001 Departments]$
```

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.

- Block the IP addresses that attempted the attack from logging into the network to prevent any further malicious attempts.
- Reset the firewall configuration to avoid any problems caused by mistakes in configuration
- Avoid remote connection for root user as it allows many privileges that can be exploited

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.

What I have learned about securing systems

- The first step to securing a system is creating an inventory for all software and hard hardware. That is:

  1- all the programs installed

2- the users of the system along with their privileges
3- hardware devices

- Security must be layered meaning that it should not be limited to one aspect of the system but to all parts including:
  1- program security
  2- network security: policies, firewall rules, access control
  3- operating system security: security policies, services, permissions, and update
  4- data security: encryption
  5- Employee's awareness
- Frameworks like NIST800 and CSF are used as a reference to understand how each part can be secured
- Least privilege is a fundamental concept that should be kept in mind whenever security is applied.
- Different aiding software can be used for auditing, detecting, and preventing and threats. This is better done by software than manually since it's a tedious process

What I've done/ my recommendations

Based on what I have learned I have done the following:

- Analyze file permissions and change them based on least privilege principle
- Check security policies and and change them so that they provide more security features and prevent any unauthorized access
- Write firewall rules that allows/denies specific accesses to the network
- Check for available updates and decide whether to consider them or not based on DFI instructions and how critical the update is.
- Check audit logs to see if there are any failed login attempts
- Recommend software that automatically detect and prevent threats

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.