

## 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:

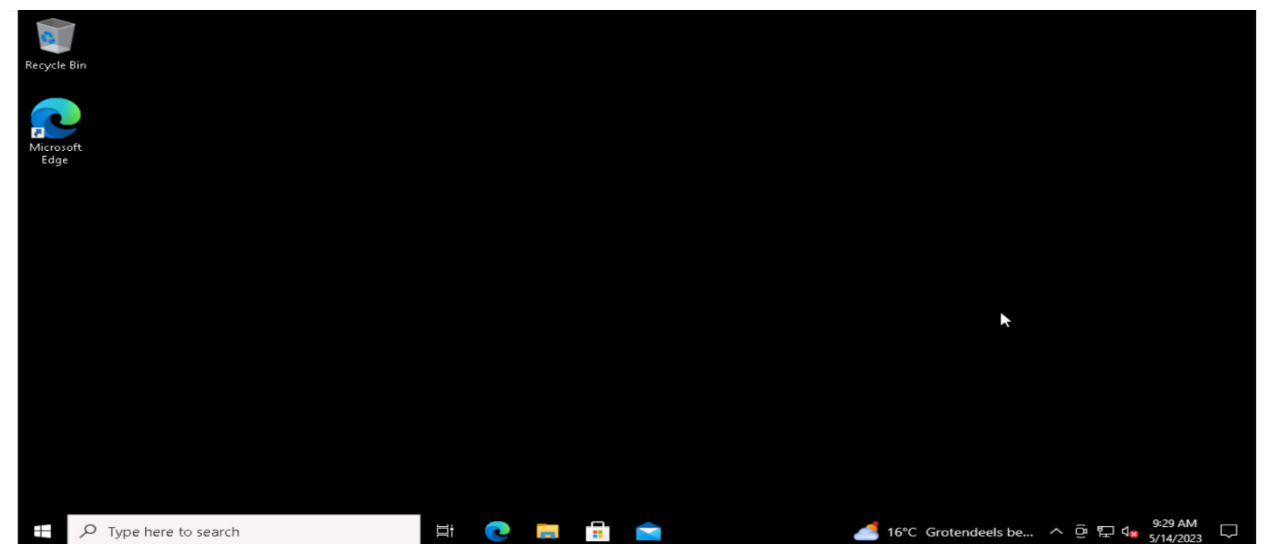
### 1. Connect to the servers:

All of the subsequent steps will take place in the DFI environment. To get started, connect to the Windows server 2016 and Linux (CentOS) machines.

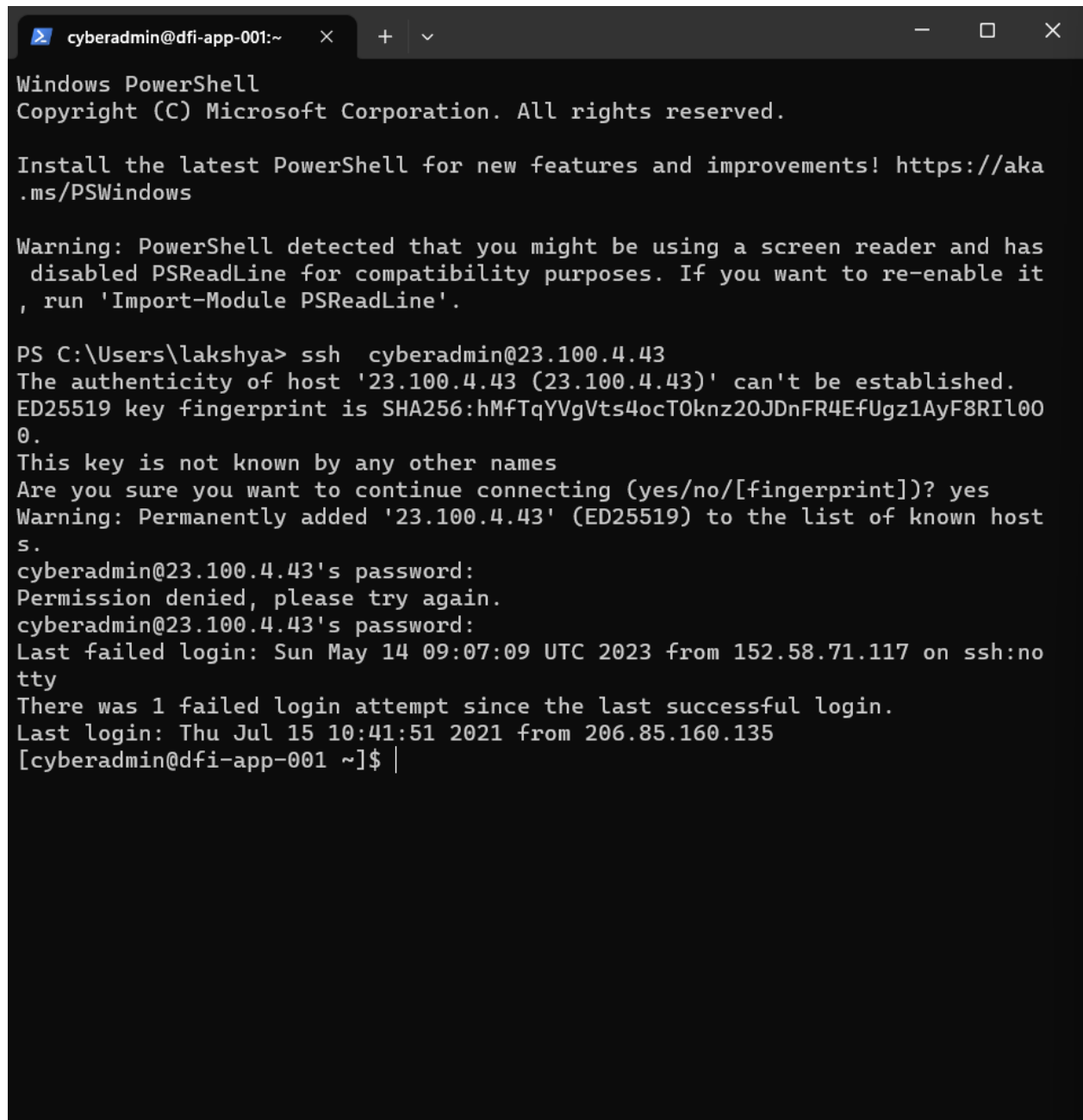
- **Windows server 2016** - If you are using Udacity cloud lab, you can directly log into the machine in the classroom. If you have set up the Windows server 2016 VM in your personal Azure account, you will have to use the RDP to connect.
- **Linux (CentOS) server** - If you are using Udacity cloud lab, you can log in using via SSH using Terminal/Gitbash/OpenSSH/Bastion. If you have set up the Linux server in your personal Azure account, you will have to use SSH to connect.
- Alternatively, you can use the **Windows 10** machine as a JumpVM for the other two VMs. Meaning, that you can use the Windows 10 VM to:
  - log into the Windows server 2016 via RDP
  - log into the Linux server via SSH using PuTTY, Gitbash, or OpenSSH.

[Please provide screenshots to show:]

- a connection to Windows server 2016.



- a connection to the Linux server using SSH.



```
cyberadmin@dfi-app-001:~ x + v
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

Warning: PowerShell detected that you might be using a screen reader and has disabled PSReadLine for compatibility purposes. If you want to re-enable it, run 'Import-Module PSReadLine'.

PS C:\Users\lakshya> ssh cyberadmin@23.100.4.43
The authenticity of host '23.100.4.43 (23.100.4.43)' can't be established.
ED25519 key fingerprint is SHA256:hMfTqYVgVts4ocT0knz20JDnFR4EfUgz1AyF8RIl000.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '23.100.4.43' (ED25519) to the list of known hosts.
cyberadmin@23.100.4.43's password:
Permission denied, please try again.
cyberadmin@23.100.4.43's password:
Last failed login: Sun May 14 09:07:09 UTC 2023 from 152.58.71.117 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$ |
```

## 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.]

Write a report detailing 3 primary areas

- File Permissions that need to be modified

- Hr folder hold the lot of confidiatial data of the company so it can't access by any one but I notice that HR folder can be access by anyone not only access also change by anyone its violating the principal of least previlage . so I suggest modify the permission of HR folder and only hr team access these file.
- IT folder hold the lot of confidiatial data of the company so it can't access by any one but I notice that IT folder can be access by anyone not only access also change by anyone its violating the principal of least previlage . so I suggest modify the permission of IT folder and only IT team access these file.
- Operation folder hold the lot of confidiatial data of the company so it can't access by any one but I notice that Operation folder can be access by anyone not only access also change by anyone its violating the principal of least previlage . so I suggest modify the permission of Operation folder and only Operation team access these file.

- Roles that are not needed on the Windows server

Only file and storage services are running and other Active directory domain servise , multipoint service print and document service should not be running because multiple service open the door of attack. Only one service running at a time

- Any services that should or should not be running

Only file services should be running and other services like Print spooler, SSDP discovery, shell hardware detection and smart card device enumeration service should not be running in the server.

Tip: Do not miss the security permissions on the HR Directory.

### 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.]

Name the IP objects and provide the commands necessary to complete the firewall rule.]

Tip: The rule must be exact.

- Access-list DFI-ingress extended permit tcp host 21.19.241.63 host 172.21.30.44 eq 9082
- Access-list is the rule will be applied in firewall to allow system traffic. I want to allow certain traffic to come certain server of organizations I have to write access-list and apply to the firewall . the firewall take this access-list in the traffic and allow certain traffic to reach my server on certain port number 9082
- name 21.19.241.63 WBC
- name 172.21.30.44 DFI-File-001
- access-list DFI-Ingress extended permit tcp host WBC host DFI-File-001 eq 9082

### 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]

Choose one of the appropriate encryption methods from the documentation provided. Provide justification for the method you chose.

Tip: Do not use those encryption methods whose status is marked either as "Avoid" or "Legacy" in the Cisco documentation.

- Encryption : AES-256-GCM mode
- Authentication : RSA-3072

- Key exchange: DH group 15
- Integrity: SHA-256
- AES-256 encryption is extremely secure. The encryption has a key size of 256 bits, which is considered virtually uncrackable—even with the most advanced computing power and algorithms.

## 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:"DDOS attack";sid=1000001;)
- We used to icmp syntax to indicate that the alert will focus on icmp traffic of any port number from any source address targeting a specific destination address and any destination port

[Place your VoIP Admin rule and explanation here]

- Alert UDP any any -> 172.21.30.55 69 (msg:"attacker is attempting to connect to her primary VoIP server";sid=1000002;)
- We used to UDP syntax to indicate that the alert will focus on UDP traffic of any port number from any source address targeting a specific destination address and any destination port

For documentation purposes, provide and explain your commands to non-technical management.

- Alert use for action.
- Icmp and udp is a protocol.
- Then we write the source address and then source port.

-> its use to direction.

- Then destination address and destination port then we write a message.

Tip: Both the rules should be exact including the parenthesis and classtype. Also, the sid number needs to be 1000000 or higher and can't be the same for both rules.

## 6. File Hash verification:

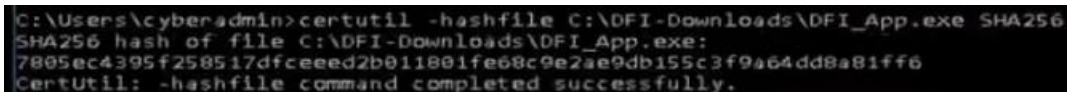
A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

**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 that displays the command that was run as well as the file hash.]



```
C:\Users\cyberadmin>certutil -hashfile C:\DFI-Downloads\DFI_App.exe SHA256
SHA256 hash of file C:\DFI-Downloads\DFI_App.exe:
7805ec4395f258517dfceeed2b011801fe68c9e2ae9db155c3f9a64dd8a81ff6
CertUtil: -hashfile command completed successfully.
```

## 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. Example:

- Area: Active Directory.

- Solution: The item for automation - Automatic account lockout if login from 2 geographically distant IPs
- Justification: Provide a brief explanation for your choices.

DFI Area/Technology	Solution	Justification for Recommendation
SIEM	Implementing a SIEM solution	Collect and correlate logs from various security solutions as IDS and firewall to have more visibility
SOAR	Implementing a SOAR solution	Implement use case to have automated responses from various security solutions as blocking a malicious IP once receiving an IDS alert for it
EDR	Implementing an EDR solution	Continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware.

## 8. Logging RDP Attempts:

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

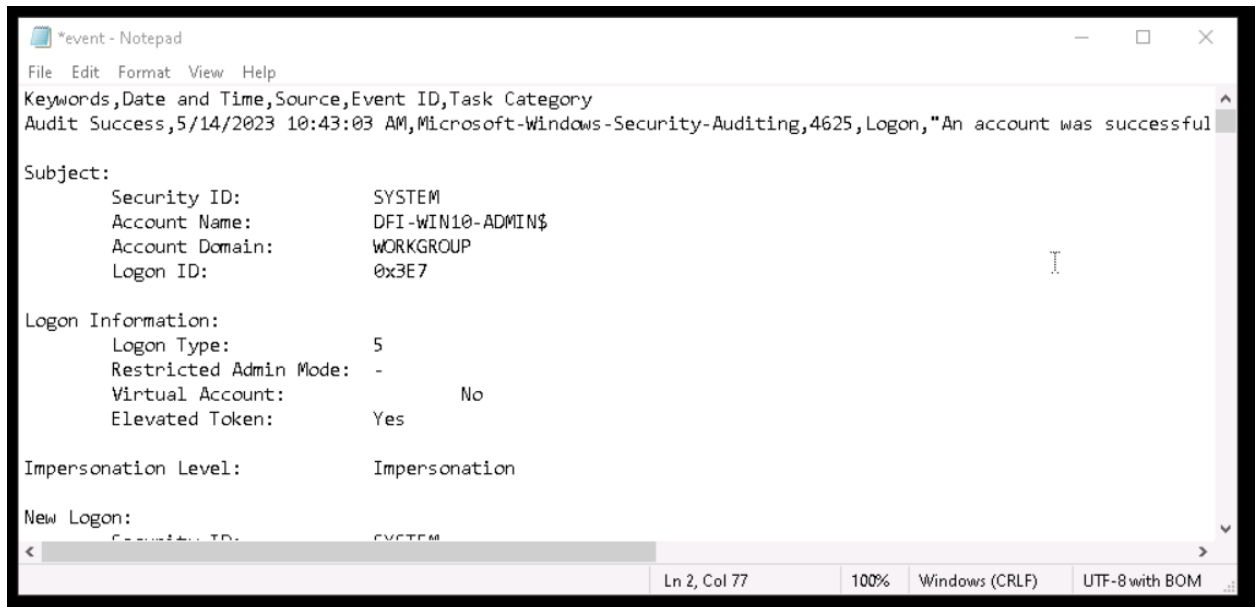
Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

For your deliverable, open the CSV with a 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 ]

- Export the results to CSV on the server provided.
- Open the CSV with notepad. It must have the Event 4625 present.

- Provide a screenshot of the results



## 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 'critical' or 'security' can be left off.

Provide a table that lists at least 3 updates that should be installed and 3 updates that are not necessary. Justify your recommendations as to why you are making your choices.

Tip: The severity of the updates can also help you decide the updates you'd like to install or ignore.

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

Available Updates	Update/Ignore	Justification
Security intelligence update for microsoft defender antivirus- KB2267602	Can't be ignored	Important security update
Security update for windows server – KB5012170	Can't be ignored	Classified critical severity by microsoft
Security update for adobe flash player - 3202790	Can't be ignored	Classified critical severity by microsoft



.net framework update- KB4054590	Can be ignored	Not critical as it is a feature pack ass per microsoft classification
Microsoft edge- CVE-2022-38012	Can be ignored	Normal update from microsoft
Update for windows server 2016 – KB4589210	Can be ignored	Normal update from microsoft

## 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]

```
cyberadmin@dfi-app-001:~/C x + - □ x
0.
This key is not known by any
Are you sure you want to cont
Warning: Permanently added '23.100.4.43' (ED25519) to the list of known host
s.
cyberadmin@23.100.4.43's password:
Permission denied, please try again.
cyberadmin@23.100.4.43's password:
Last failed login: Sun May 14 09:07:09 UTC 2023 from 152.58.71.117 on ssh:no
tty
There was 1 failed login attempt since the last successful login.
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[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 OPeration
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operation
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo adduser AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo adduser MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo adduser TimHR
[cyberadmin@dfi-app-001 Departments]$ sudo adduser PamOps
\[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G IT AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G HR TimHR
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Accounting MandyAcc
t
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Operations PamOps
usermod: group 'Operations' does not exist
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G OPerations PamOps
usermod: group 'OPerations' does not exist
[cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Operation PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo chown AmyIT:IT IT
[cyberadmin@dfi-app-001 Departments]$
```

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

- Create the directories listed in the request.
  - -mkdir Departments
  - -cd Departments
  - -mkdir HR
  - -mkdir Accounting
  - -mkdir public
  - -mkdir IT
  - -mkdir Operation
- Create the groups listed in the request.
  - sudo groupadd IT
  - sudo groupadd HR
  - sudo groupadd Operation
  - sudo groupadd Accounting
- Create the users listed and place them in the appropriate groups.
  - -sudo adduser AmyIT
  - -sudo adduser MandyAcct
  - -sudo adduser TimHR
  - -sudo adduser PamOps
- Set the directory permissions where the groups are the owners of their respective directories.
  - -sudo usermod -a -G IT AmyIT

- -sudo usermod -a -G HR TimHR
- -sudo usermod -a -G Accounting MandyAcct
- -sudo usermod -a -G Operation PamOps
- -sudo chown any IT:IT IT
- **Tip: Appropriate groups should be the owners of the respective directories.**
- **Explain the syntax used for setting the permissions.**

-mkdir use for the create the directory  
 -cd use to change the directory.  
 -sudo groupadd use to add a new group.  
 -sudo adduser use to add new user.  
 -sudo usermod use to change the permissions.

## 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]**

**Provide mitigation recommendations based on your analysis of the report with a focus on friend/foe of the source IP as well as an additional layer of protection for the destination IP.**

**Tips: Edge case - Think about what should you do with IPs from non-trusted source.**

- We should allow traffic on SSH for the authorized pool of ips and deny any other traffic.
- Also we should deny any traffic any port that is originating outside of our business country which is the USA in our solution.
- we must initially check the status of the IP if it is from malicious source we must block the IP.
- close the port no 22 and open any other port.

## 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]

- Explain all of the tasks performed in the first two weeks.
  - Explain any recommendations for changes in permissions.
  - Tie all of the work done together in a big picture narrative.
  - Recommend the way forward for DFI in terms of security products (at least 2) and policies (also at least 2.)
- 
- System OS hardening was performed for the window Server 2016 as file services was accessible to all the company
  - Unnecessary services on the window server were removed as it widens our attack surface
  - System updates were installed on the windows server
  - RDP logs were retrieved from the event viewer to have visibility on RDP attempts.
  - Firewall rules were implemented to better protect the company assets
  - VPN encryption was used with latest secure algorithms to protect our communication with our partners.
  - IDS rules were implemented to alert in case of DDOS or VOIP attack is in place.
  - Recommendations were made regarding installing necessary security solution that can automate security work as SIEM , SOAR , EDR , NDR.
  - Users . user groups , directories were created in the linux machine.
  - Permissions were assigned so that each user group can only access it's department directory.
  - We implmented Defense in depth by the above mentioned steps as we protected our network edge through FW , VPN & IDS , then through services and updated on the system and assigning permissions on directories
  - We use the product like as VPN , Firewall and end point security.
  - We use the policies like as **organizational security policy** and **System-specific security policies**.

### 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, 15 or more characters.

**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. See the classroom instructions for the submission.**