Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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:

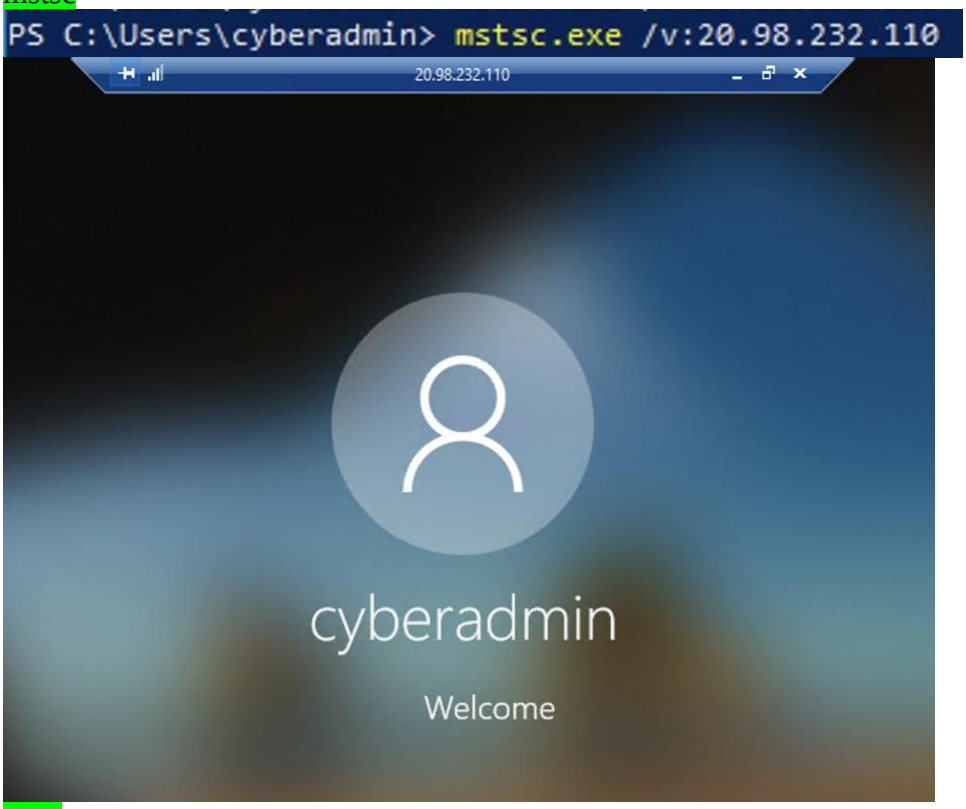
Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

1. **Connect:**

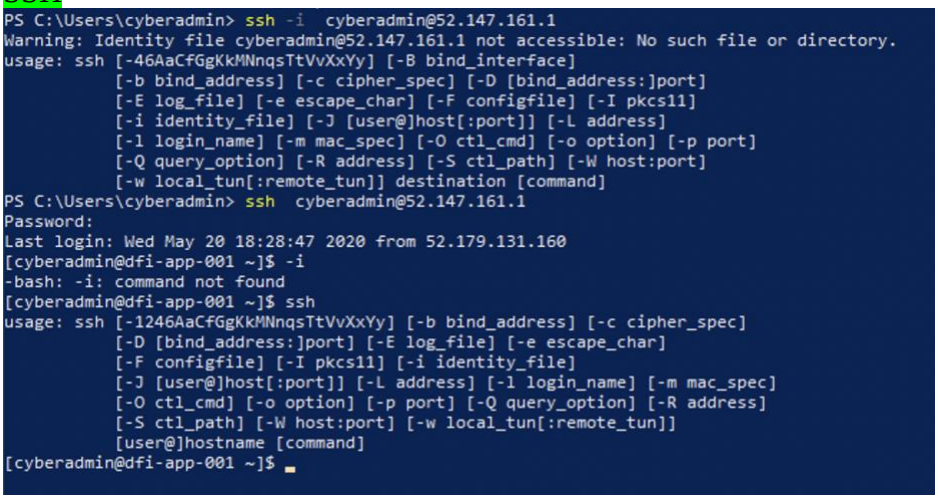
All of the subsequent steps will take place in the DFI environment. You will need to RDP (Remote) into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

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

mstsc



SSH



Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

2. **Security Analysis:**

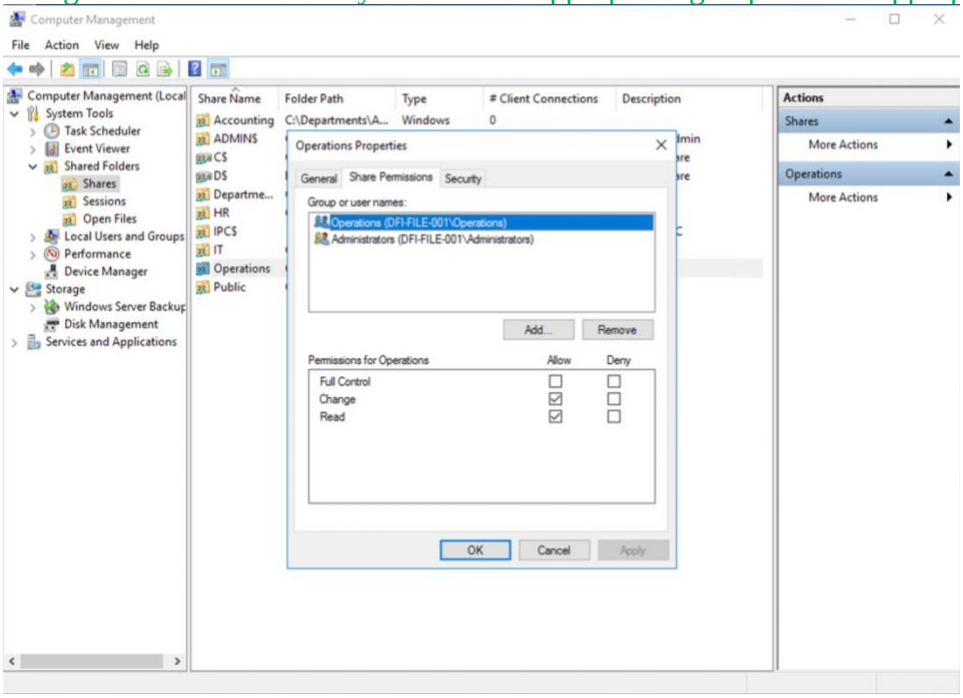
DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

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.)

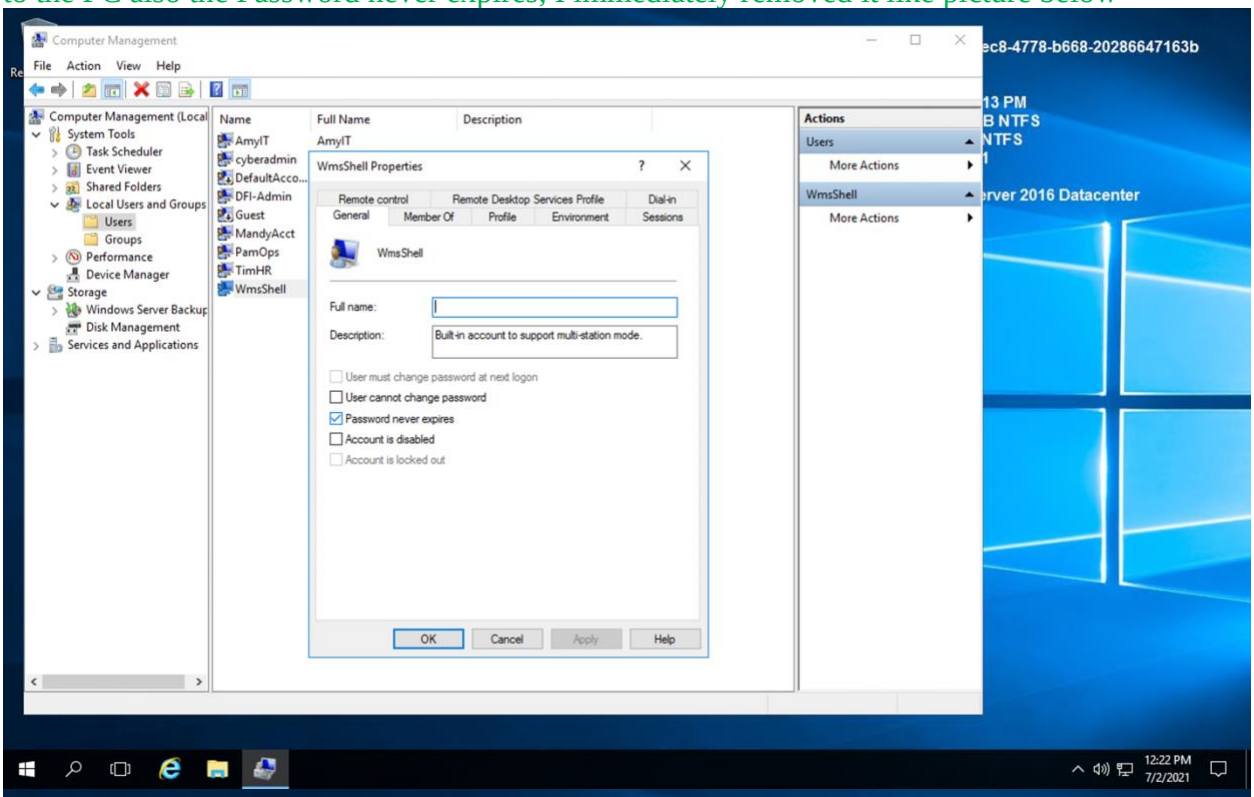
[Place your security analysis here]

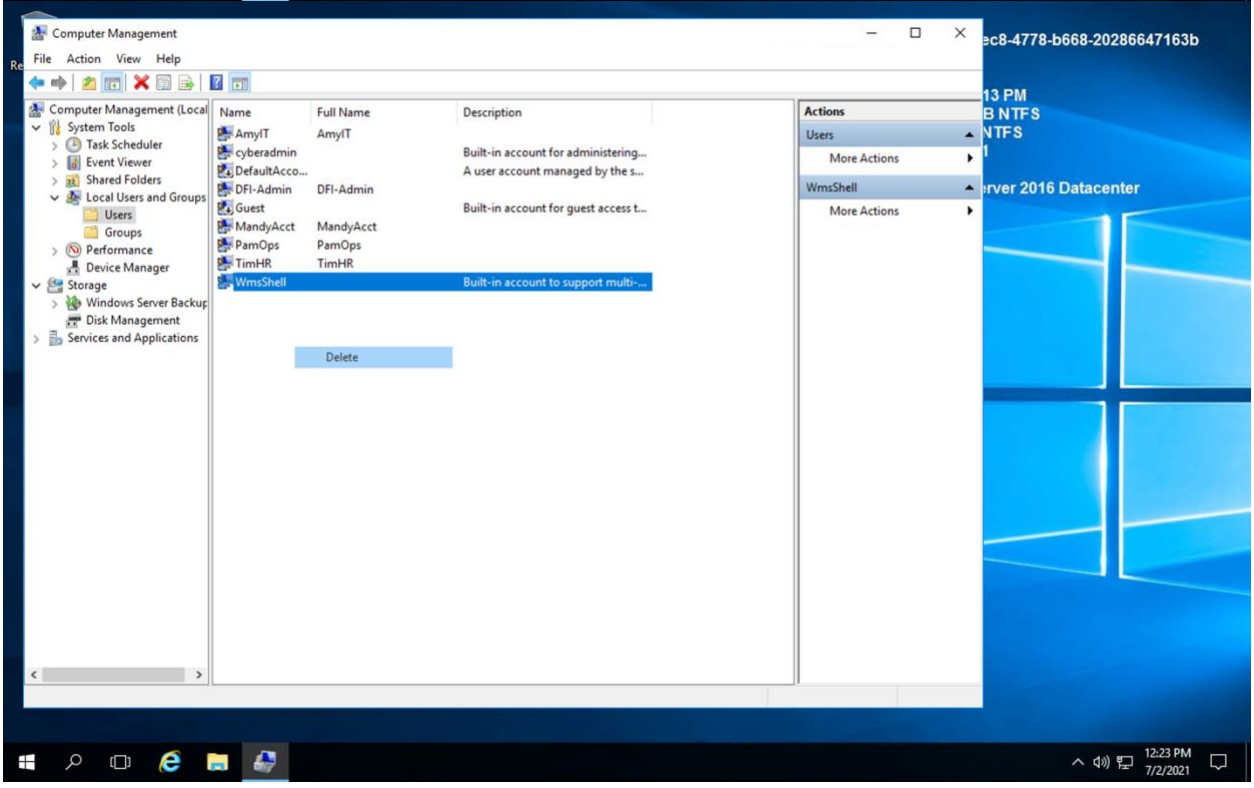
I noticed that some files like HR, Accounting, IT, Operations has access to everyone groups, I changed this and made every file with its appropriate groups and its appropriate access like this



Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

Also, I noticed some big thing that there is a user who is not in any group but has Remote access to the PC also the Password never expires, I immediately removed it like picture below



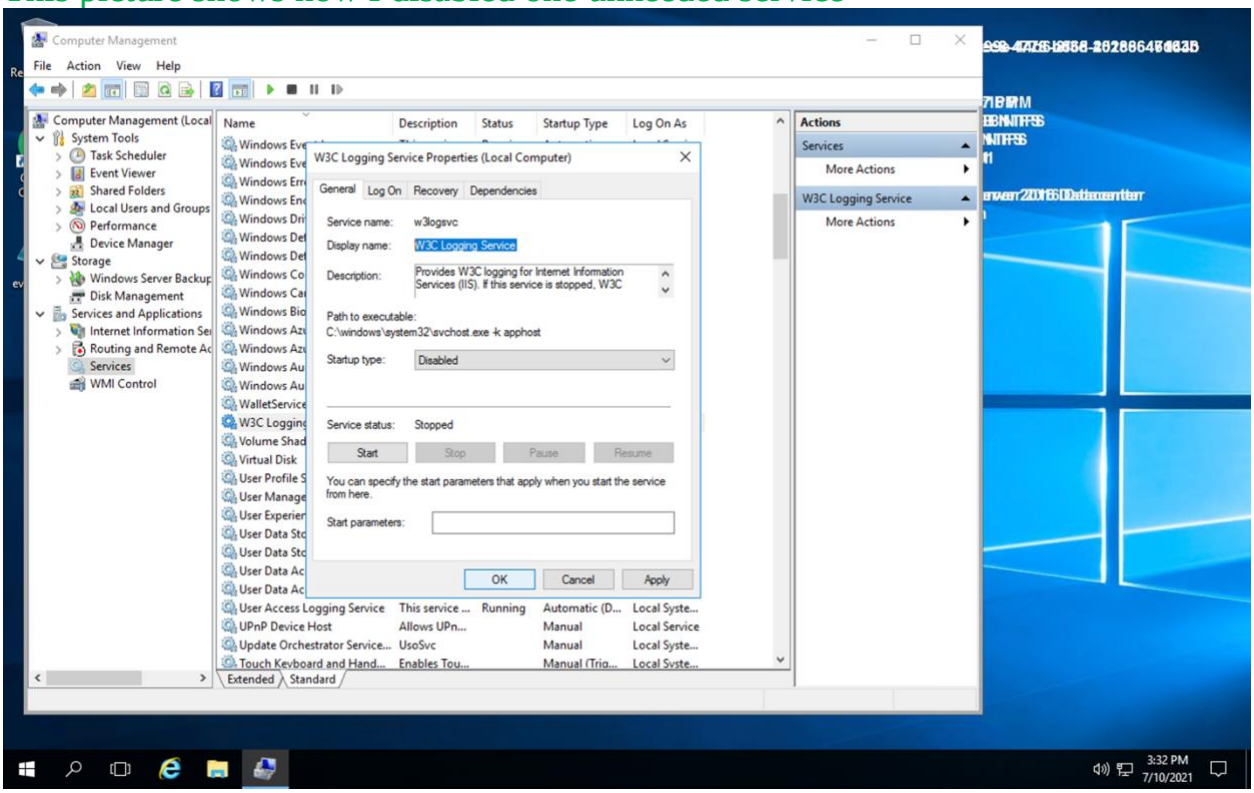


Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

Here I have disabled some services he didn't need like:

- Xbox Live Game Save
- Xbox Live Auth Manager
- Bluetooth Support Service
- ActiveX Installer (AxInstSV)
- IIS Admin Service
- W3C Logging Service
- MultiPoint Repair Service
- MultiPoint Service

This picture shows how I disabled one unneeded service



Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

3. **Firewall Rules:**

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

The partner's IP is 21.19.241.63 and DFI-File-001's IP is 172.21.30.44.

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

[Place your firewall rules and explanation here]

Access-list DFI-Ingress extended permit tcp host 21.19.241.63 host 172.21.30.44 eq 9082

- Access-list: rule controls the traffic.
- DFI-Ingress is our interface.
- Extended permit: gives additional fixability in matching the traffic more granularly.
- tcp: is the type of traffic.
- First host: is the source “the partner”.
- Second host: is the destination “us”.
- Eq: equal to the port > “in my case is **9082**”.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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]

- Try to Hash *SHA-512* all your files or information that you afraid for its *integrity*.
- Try to use *AES-256* for encrypt the information.
- Try to use Elliptic Curve encryption *(ECDH, ECDSA-521)* for data in transit.
- Do not use NULL encryption (esp-null).
- Use both an authentication algorithm (esp-sha256-hmac is recommended) and an encryption algorithm (esp-aes is recommended).
- Avoid IKE Groups 1, 2, and 5.
- Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively.
- When possible, use IKE Group 19 or 20. They are the 256-bit and 384-bit ECDH groups, respectively.
- Use AES for encryption.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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 Attempt Attack”; sid:1000001)

- I mean by putting ***Alert*** is alerting administrator of the event.
- ***ICMP*** is the type of traffic.
- First ***any*** means any source IP.
- Second ***any*** means ay source port.
- **->** means the traffic is inbound
- Third ***any*** means any ICMP port.
- And the ***msg*** is the massage that will be appear to administrator.
- Then ***sid*** is the identifier.

[Place your VoIP Admin rule and explanation here]

Alert UDP any any -> 172.21.30.55 69 (msg: “TFTP Attempt Attack”; sid:1000002)

// as same as above //
But by putting 69 I mean TFTP port number.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

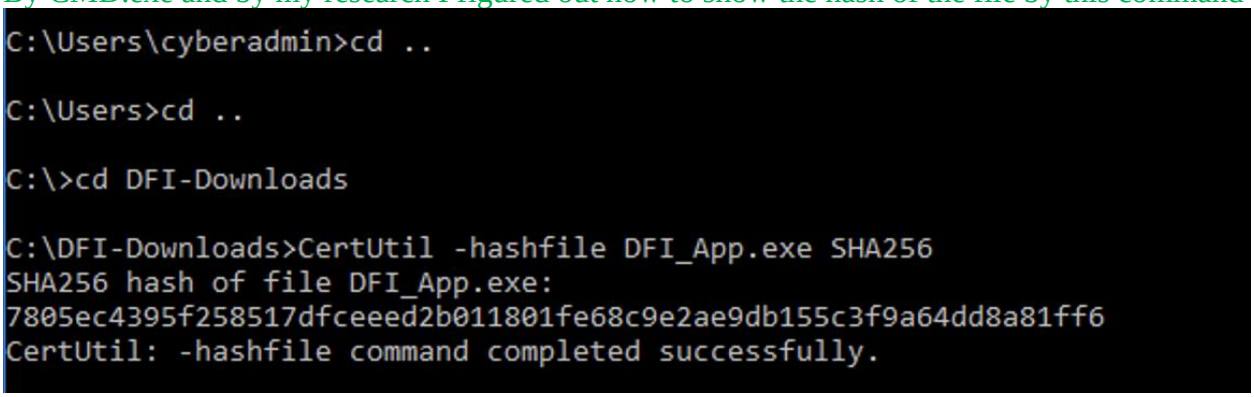
6. File Hash verification:

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]
By CMD.exe and by my research I figured out how to show the hash of the file by this command



Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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
Firewall alert	We added before an IDS rule alerting for ICMP, TFTP attacks.	It helps administers for some sort of unwanted actions in some files and Ips.
Passwords unlock and change	We can customize it from: Local Security Policy > Account Polices > Password Policy and Account Lockout Policy	It reduces the risks and the cost for changing the passwords, you can customize a Policy for your future passwords.
Collect RDP Attempts on a file	We can do it by snort syntax in the PowerShell by adding: **Get-EventLog -logname Security**	This can reveal either successful or unsuccessful attempts on the file and give you a visualization of who access the file and who is trying to access the file.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

8. **Logging RDP Attempts:**

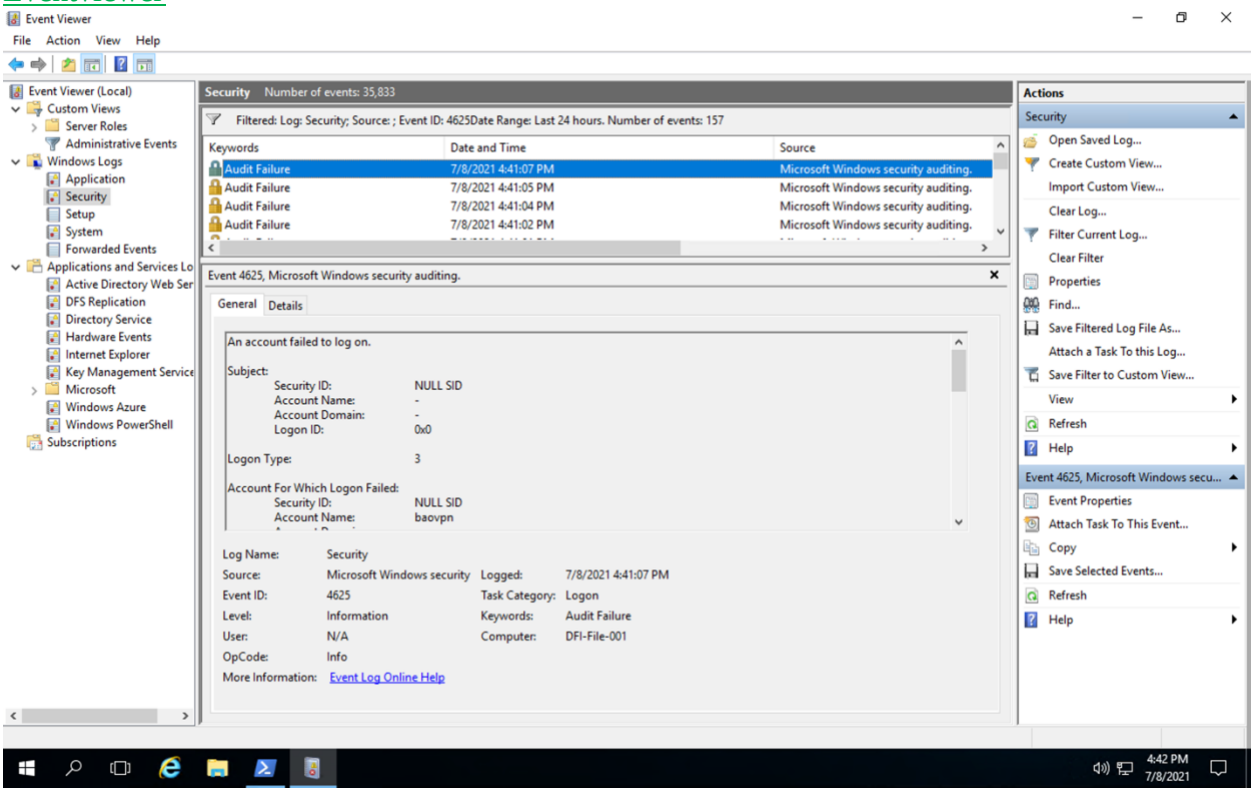
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

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.

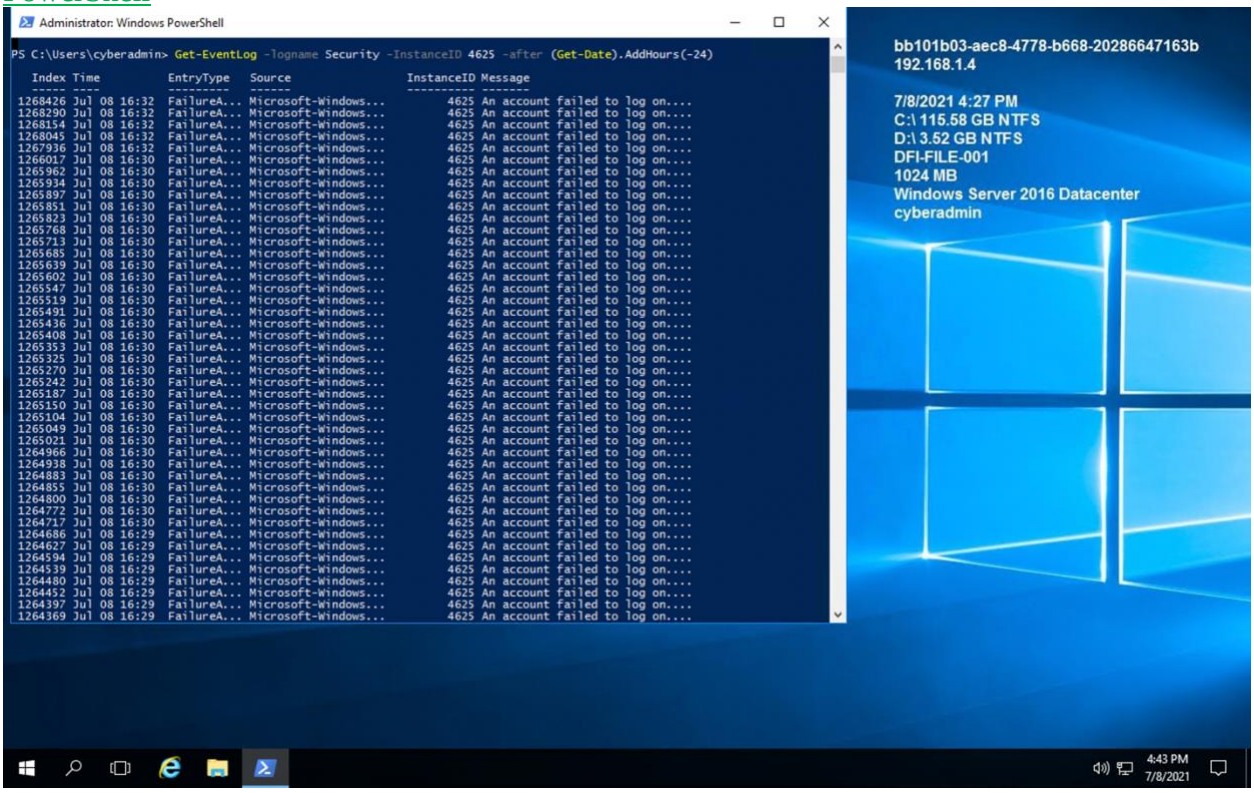
[Place IT Manager Report Here]

Eventviewer

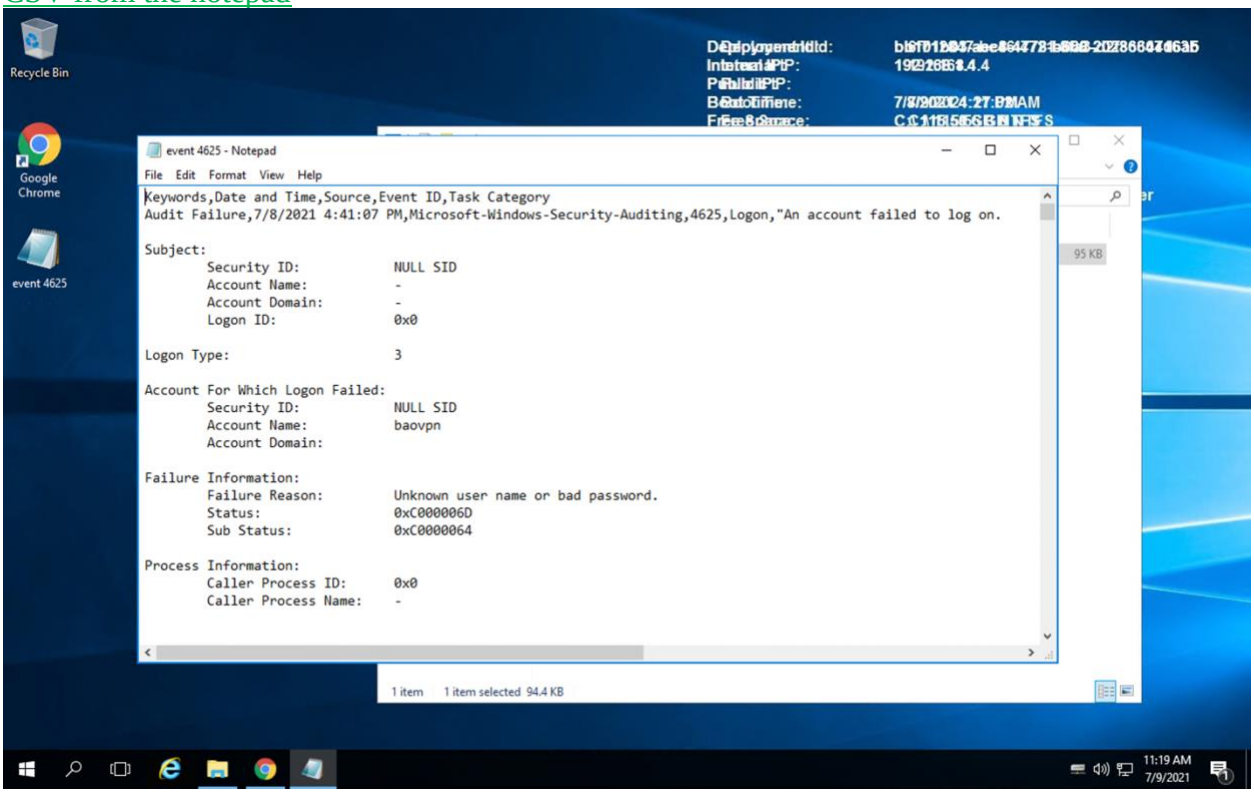


Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

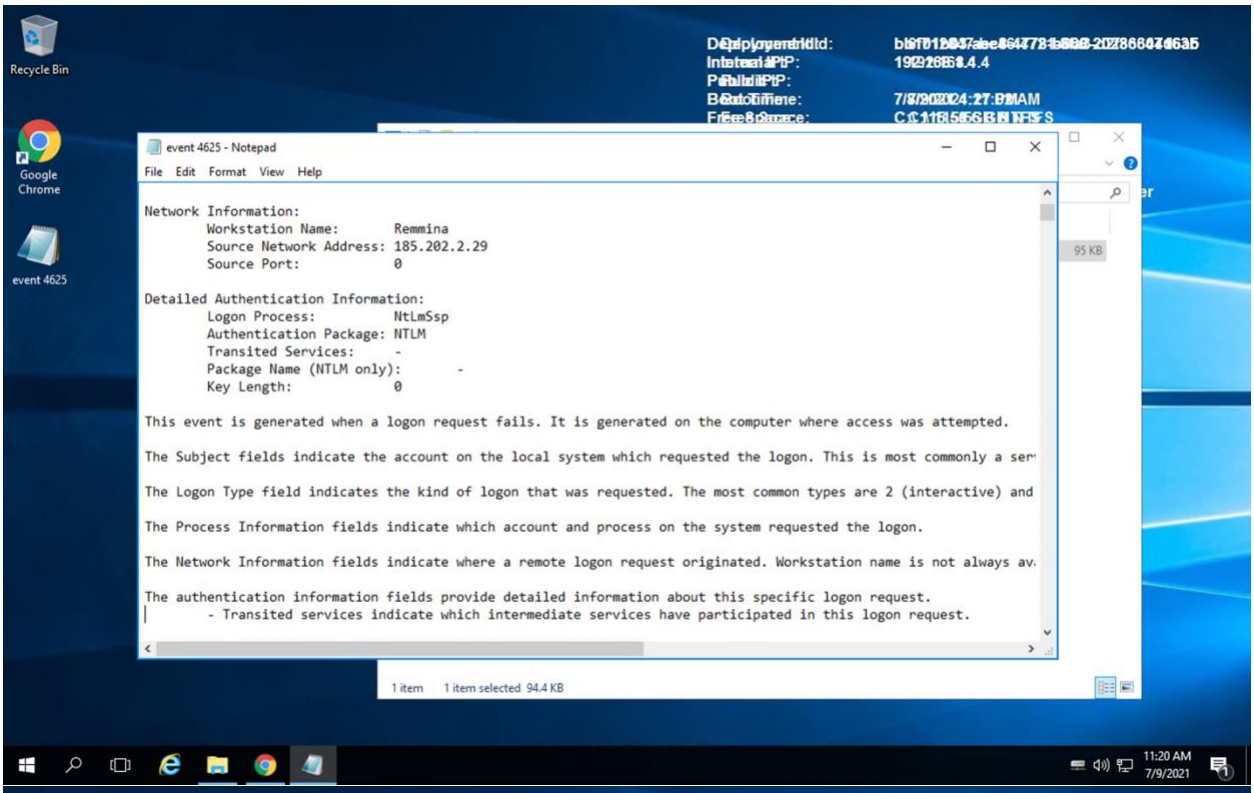
PowerShell

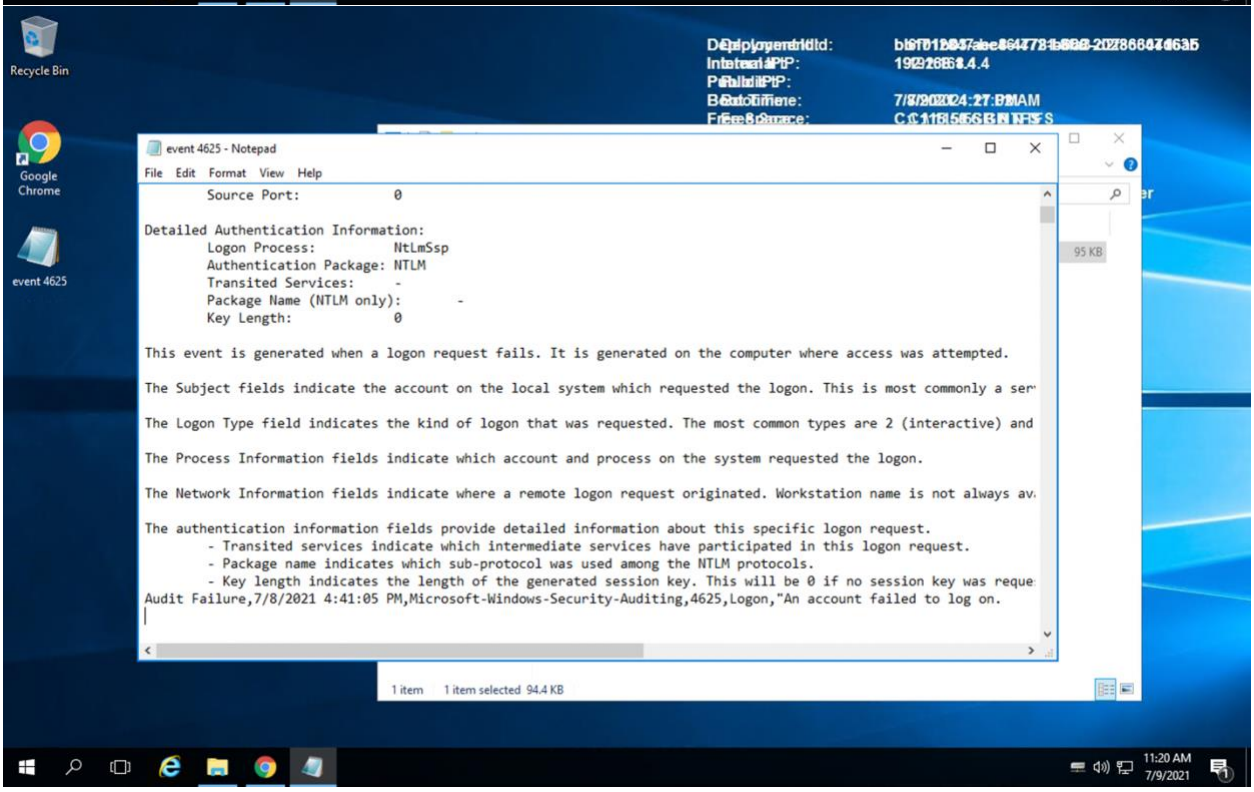


CSV from the notepad



Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com





Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

I find that there are multiple times of attempts using RDP to your PC by your IP
My recommendation that you try to change your IP address, make a powerful password for your PC to prevent yourself from brute force attack “like trying to add symbols, capital and small letters on your password” use this website **here** to chick whether your password is strong or not.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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-2021-34527 5004948	Update	Since it's a critical update, and it impacts Remote Code Execution, it should be considered. Have a high value in all CIA.
CVE-2021-31959 5003638	Update	Since it's a critical update, and it impacts Remote Code Execution, it should be considered. Have a high value in Integrity.
CVE-2021-33742 5003638	Update	Since it's a critical update, and it impacts Remote Code Execution, it should be considered. Have a high value in all CIA.
CVE-2020-24588 5003197	Ignore	Since it's an Important update "not critical", and it only impacts Spoofing, it can be left. Which you don't have an interest about it.
CVE-2021-28357 5001347	Ignore	Since it's an Important update "not critical", and it has a little impact on Remote Code Execution, it can be left.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

		Which you don't have an interest about it.
CVE-2021-26894 5000803	Ignore	Since it's an Important update "not critical", and it has a little impact on Remote Code Execution, it can be left. Which you don't have an interest about it.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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]

Here I added the directory **Departments** and its subdirectories **HR**, **Accounting**, **Public**, **IT** and **Operations**

```
[cyberadmin@dfi-app-001 home]$ sudo mkdir Departments
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ ls
cyberadmin  Departments  dfi-admin  JoePublic
[cyberadmin@dfi-app-001 home]$ cd departments
-bash: cd: departments: No such file or directory
[cyberadmin@dfi-app-001 home]$ cd Departments
[cyberadmin@dfi-app-001 Departments]$ pwd
/home/Departments
[cyberadmin@dfi-app-001 Departments]$ ls
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir HR
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Public
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir IT
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Operations
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting  HR  IT  Operations  Public
[cyberadmin@dfi-app-001 Departments]$ ls -ld HR
drwxr-xr-x. 2 root root 6 Jul  6 08:14 HR
```

Here I gave directory's group the owner permissions

```
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx HR
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ ls -ld HR
drwxrwxr-x. 2 root root 6 Jul  6 08:14 HR
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx IT
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+rwx Operations
```

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

Here I added groups and new users and assign them to their groups

```
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -g IT AmyIT
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -g Operations PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -g Accounting MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -g HR TimHR
[cyberadmin@dfi-app-001 Departments]$
```

Here I linked the groups with its directories

```
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
drwxrwxr-x. 2 root root 6 Jul  6 08:15 Accounting
drwxrwxr-x. 2 root root 6 Jul  6 08:14 HR
drwxrwxr-x. 2 root root 6 Jul  6 08:15 IT
drwxrwxr-x. 2 root root 6 Jul  6 08:15 Operations
drwxr-xr-x. 2 root root 6 Jul  6 08:15 Public
[cyberadmin@dfi-app-001 Departments]$ sudo chown IT IT
[sudo] password for cyberadmin:
chown: invalid user: ‘IT’
[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]$ sudo chown :Accounting Accounting
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
drwxrwxr-x. 2 root Accounting 6 Jul  6 08:15 Accounting
drwxrwxr-x. 2 root HR         6 Jul  6 08:14 HR
drwxrwxr-x. 2 root IT         6 Jul  6 08:15 IT
drwxrwxr-x. 2 root Operations 6 Jul  6 08:15 Operations
drwxr-xr-x. 2 root root       6 Jul  6 08:15 Public
[cyberadmin@dfi-app-001 Departments]$
```

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

- **Sudo** > for more privileges tasks like adding or deleting or modifying…, you need it.
- **Mkdir** > it simply like “make directory”.
- **Ls** > it shows all the files and directories in your path.
- **Cd** > for going deep in the path or “cd ..” for going back in the path.
- **Pwd** > shows you the path you in.
- **Ls -ld “name”** > it shows the information of (file or directory) by its “name”.
- **Chmod g+rwx** > simply chmod used to change the access of a file or directory, g means the scope is the group, +rwx means add read, write and execute permissions to the file or directory.
- **Groupadd** > for adding a group to the PC

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

- **Useradd -g IT AmyIT** > useradd means add new user, -g meens add it to only this group (for my case its IT group), AmyIT it's the name of the new user.
- **Chown :"name1" "name2"** > chown means change owner, :"name1" "name2", name1 is the name of group, name2 is the name of the directory I want to link the group with it.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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]

- I recommend you search for the source IP address in abuseipdb.com or VirusTotal so you can find out if this IP is one of yours or not.
- If NOT please report the IP with the ISP hosting it, by searching for who is information, also add.
- Lastly update the software.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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]

Week One:

- I opened the windows PC and seen the files and what file's share permission and I noticed that some files like HR, Accounting, IT, Operations has access to everyone groups, I changed this and made every file with its appropriate groups and its appropriate access.
- Also, I deleted a user who is not in any group but has Remote access to the PC also the Password never expires.
- I added a firewall rule to accessing the new partner to DFI-File-001 on Windows OS.
- I suggest a VPN encryption method for their data security.
- I recommended an IDS rule for alerting DDoS attack to the IP address who has a lot of ICMP traffic attack and
- I recommended an IDS rule for alerting if someone trying to connect to her VoIP server.
- I did a file's integrity by its Hash from CMD.exe.

Week Two:

- I added 3 deferent areas to automate to reduce cost, time and to make the system more reliable.
- I collected the **unsuccessful** attempts on DFI-File-001 via RDP by *snort* line in **PowerShell** and made my recommendations on the list provided from PowerShell
- I suggested some available updates from Windows website and recommendations and why they should update.
- In Linux I added directory **Departments** and its subdirectories **HR**, **Accounting**, **Public**, **IT** and **Operations**, I gave directory's group the owner permissions, I added groups and new users and assign them to their groups, I linked the groups with its directories then show you what syntax I used and why I put it.
- In firewall alerts I suggested some mitigation responses for the DDoS attack they reserve from different Ips.

Student Name: ABDULLAH ALSHALAN
Email address: ab1alshalan@gmail.com

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.