Scenario:

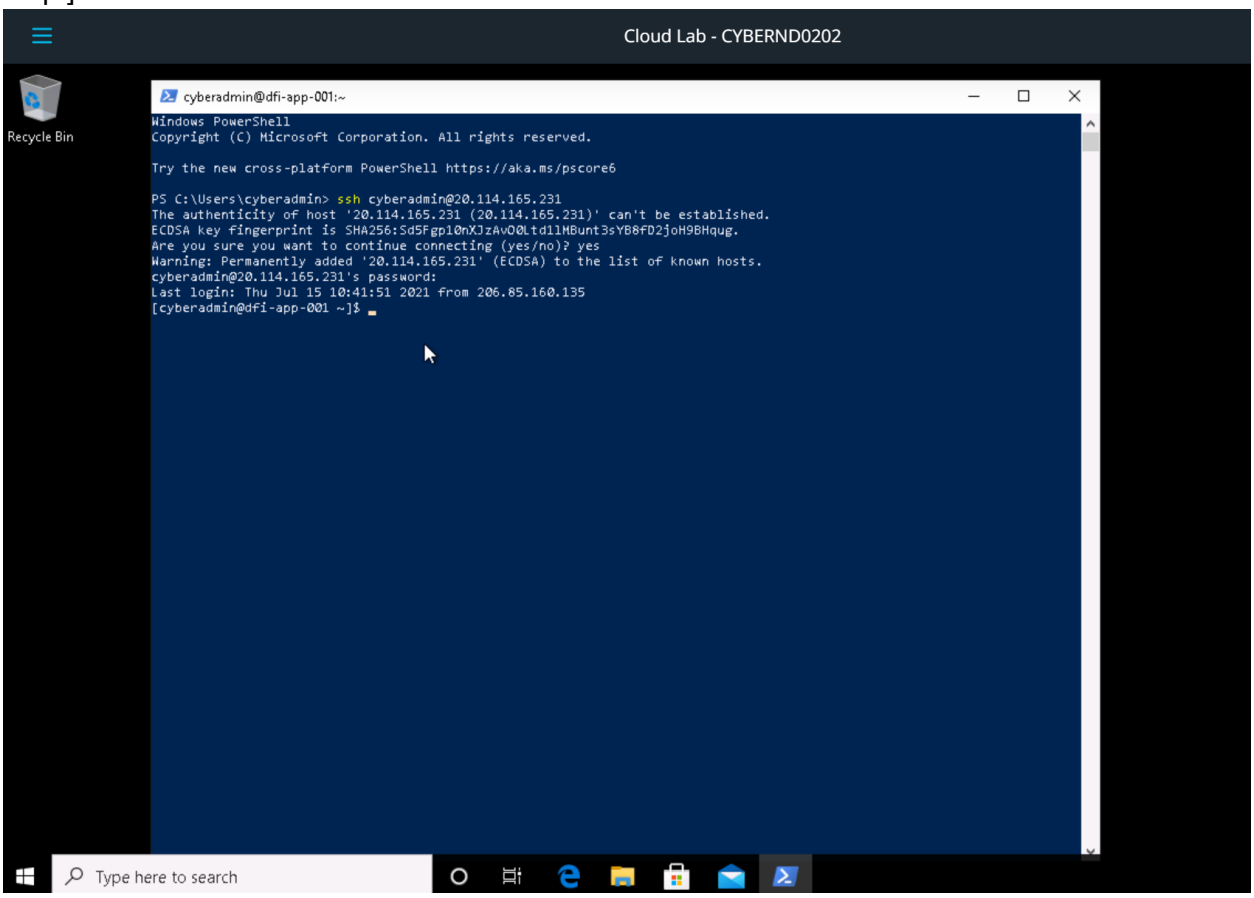
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

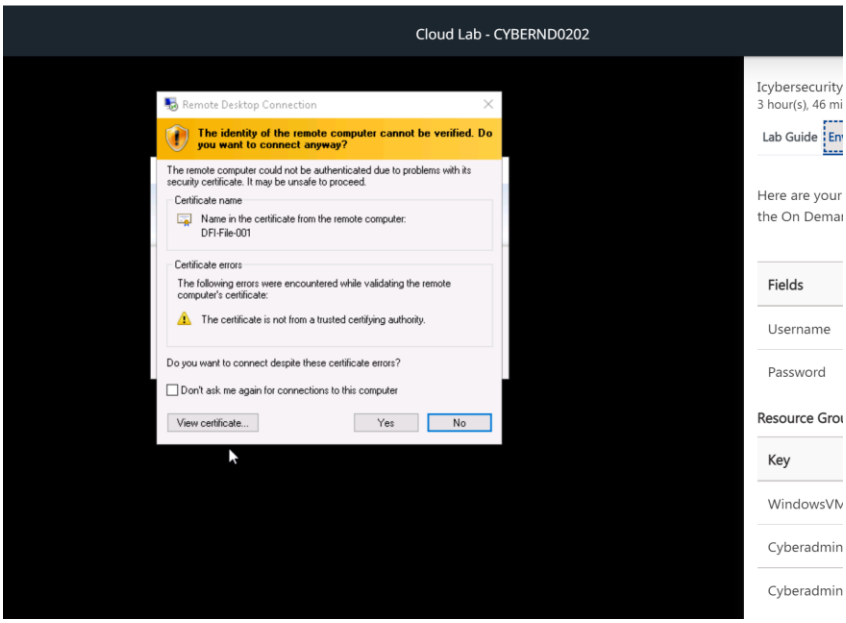
Week One:

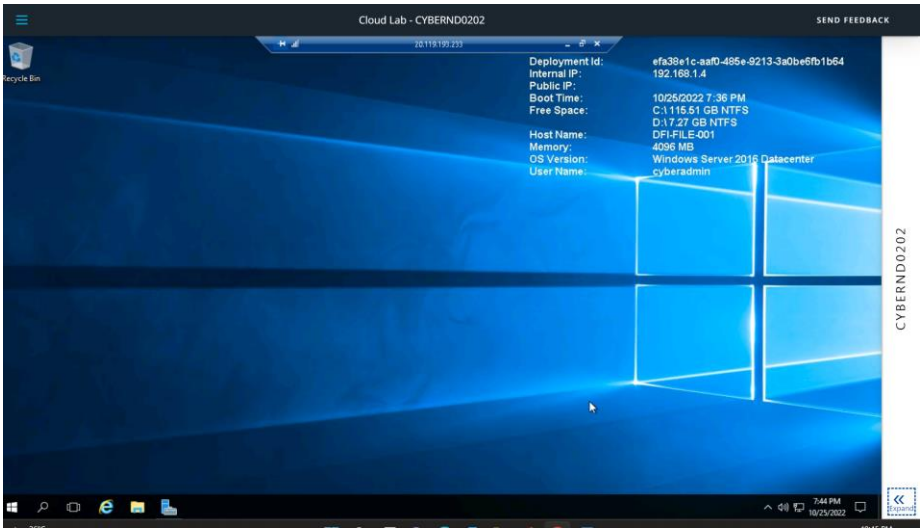
1. **Connect:**

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.]







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.

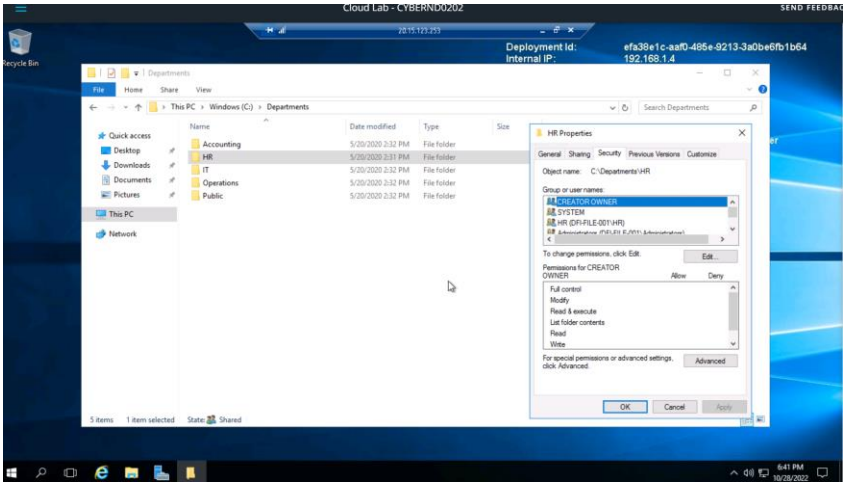
Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI compliant organization and will likely be Sarbanes-Oxley in the near future.

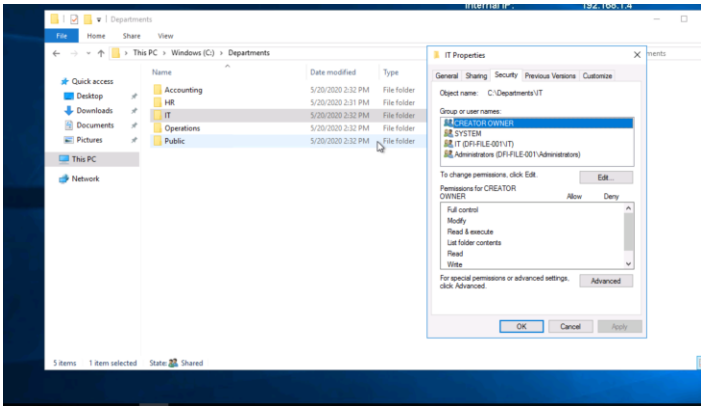
Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add/remove/change**

services, permissions and other settings.Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

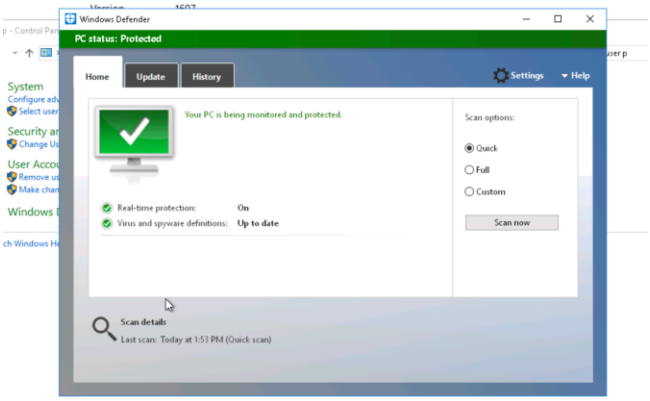
[Place your security analysis here],

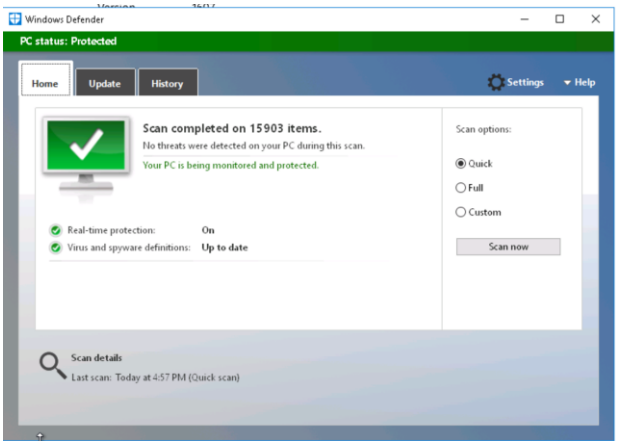
1- I noticed that these files could be access by more than one user (include who should not have the exact right to access), I recommended to apply Principle of Least Privilege that states a given user account should have the exact access rights necessary to execute their role's responsibilities—no more, no less.



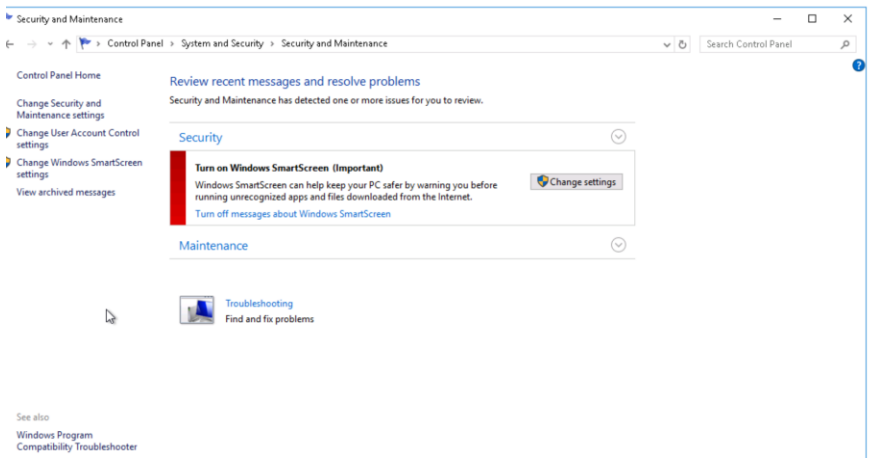


2- I make sure that windows defender is ON, and I also to recommend use scan for malware and other potentially unwanted software



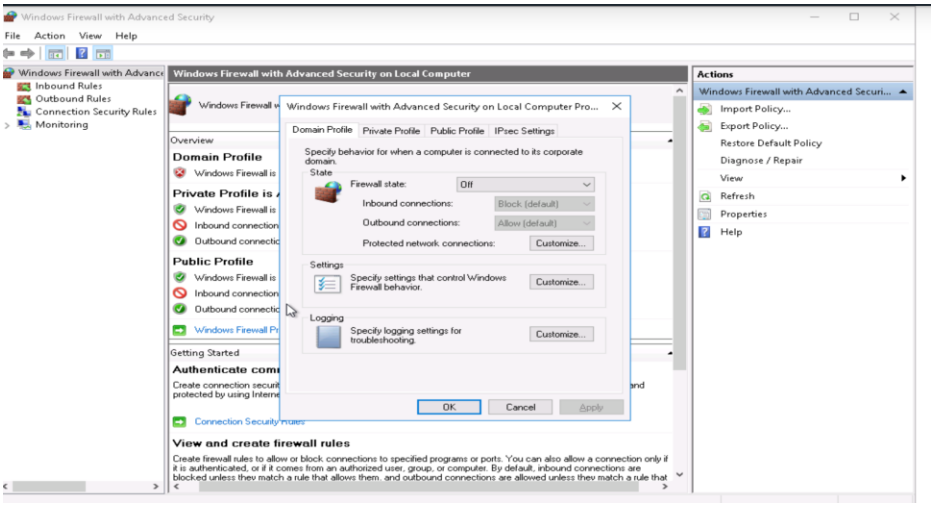


3- I recommend turning on windows smart screen, because Microsoft Defender SmartScreen is part of the Windows Security solution. It helps you protect against common threats by warning against downloading or installing potentially malicious files from other computers.

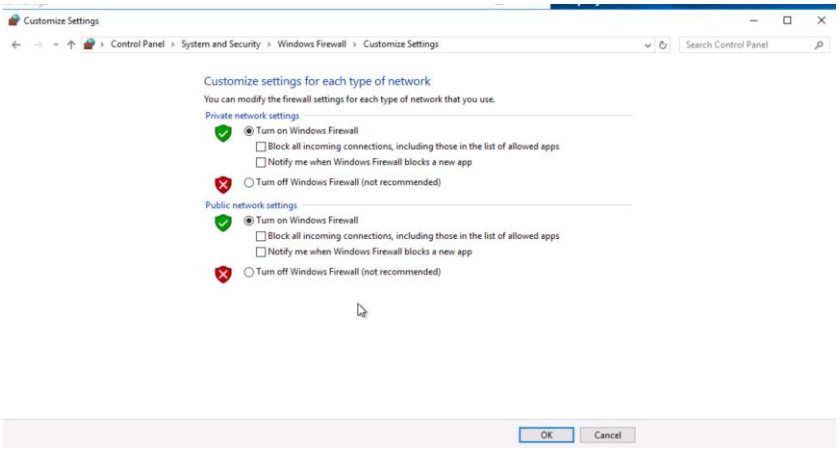


4- Firewall state was off, I recommend to turned ON because it's helps protect your computer by preventing unauthorized users from gaining access to your computer

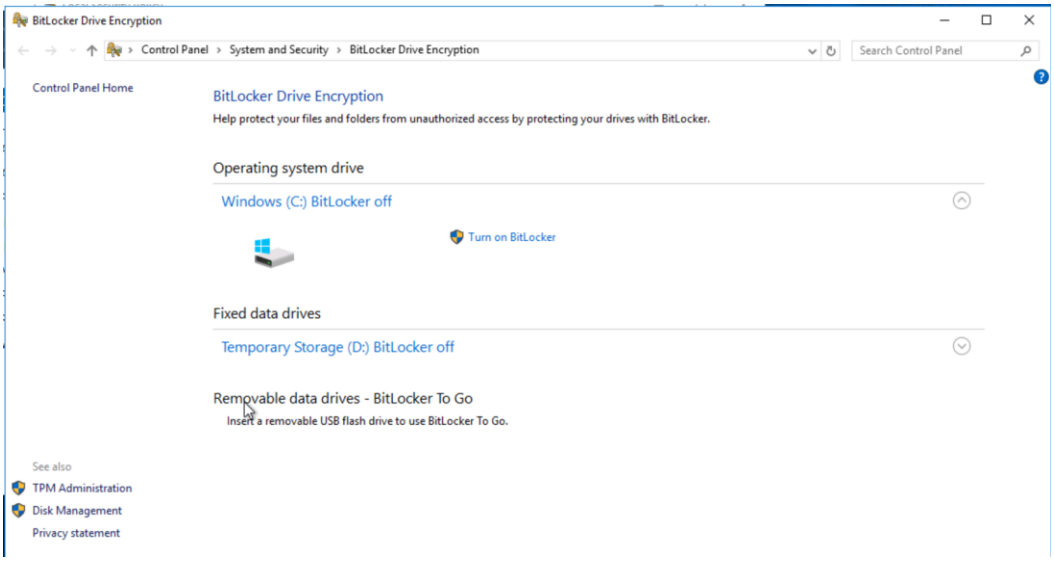
through the Internet or a network. If the firewall is turned off, traffic on all ports will be able to access the system and an attacker may be more able to exploit a weakness in a network service



I suggest that to check (right) in front of the option [Notify me when windows Firewall blocks a new app] in both public and private, then you will be notified when windows firewall blocks a program.



5- Bit locker was off, I recommend to turned it ON because BitLocker is a data protection feature that encrypts the hard drives on your machine to provide enhanced protection against data theft or exposure on computers and removable drives that are lost or stolen. (Defense-in-Depth)



.

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]

To name source IP address & destination
Name 21.19.241.63 WBC
Name 172.21.30.44 DFI-File-001

access-list *DFI-Ingress* extended permit tcp host WBC 21.19.241.63 host DFI-File-001 172.21.30.44 eq 9082
explaining the syntax:

1- The rule begins with (acsess-list) which is a rule that controls traffic.
2- Next is the name of the internal interface being used .

3- Here we use an extended permit that gives additional flexibility in matching the traffic more granularly.
4- Then we identify that TCP is the protocol being used
5- Source is listed before destination, we identify the IP address that will be allowed to access our database server
6- The destination is the IP address of our database server
7- Eq means equal to
8- 9082 is the port required in the request above.

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]

Both of symmetric and asymmetric encryption.

symmetric and asymmetric encryption are combined to take advantage of each method's strengths:
1- Symmetric encryption is used to convert the plaintext to ciphertext. This takes advantage of the symmetric encryption speed.
2- Asymmetric encryption is used to exchange the symmetric key used for encryption. This takes advantage of the security of asymmetric encryption, ensuring that only the intended recipient can decrypt the symmetric key.

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 tcp any any -> 172.21.30.44 9082 (content “icmp”; msg “Ddos Attack” sid:1000011;)
[Place your VoIP Admin rule and explanation here]

[alert tcp any any -> 172.21.30.55 69 (content “VOIP”; msg “TFTP Trafic” sid:1000012;)]

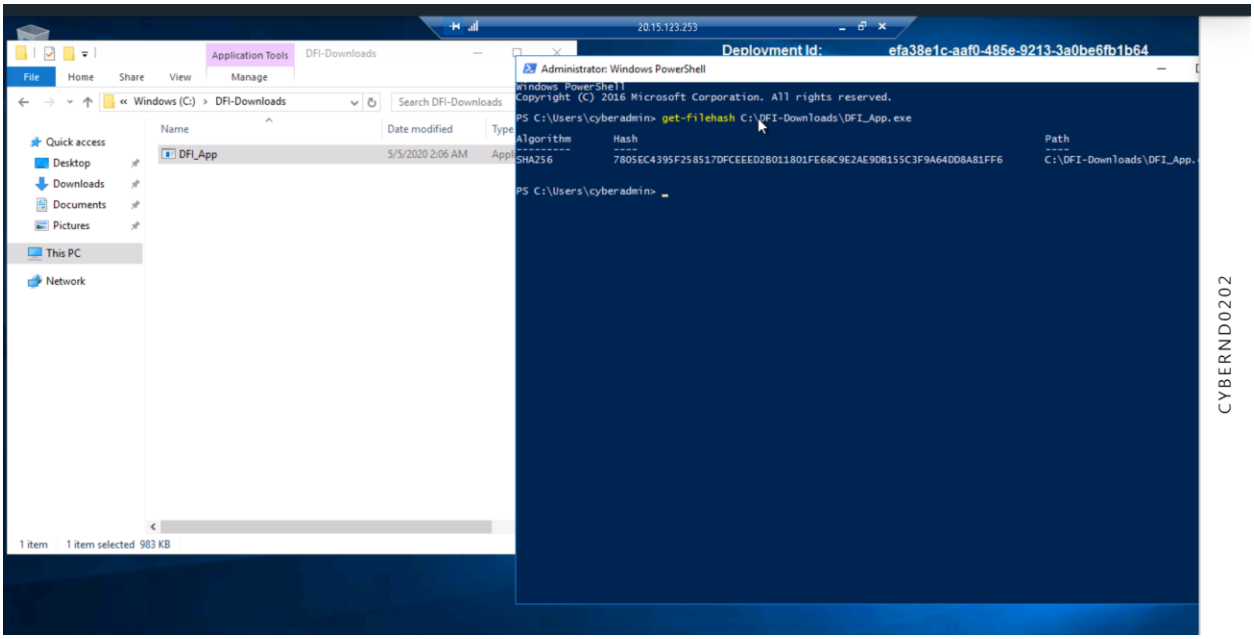
6. **File Hash verification:**

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]



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
Access control	Logging attempt	Logging attempt
firewall	Block any suspicious connection from unknown ip to critical port	reduce the potential for human error
IDS	alerts for potential attacks	providing extra coverage for sensitive workstations.

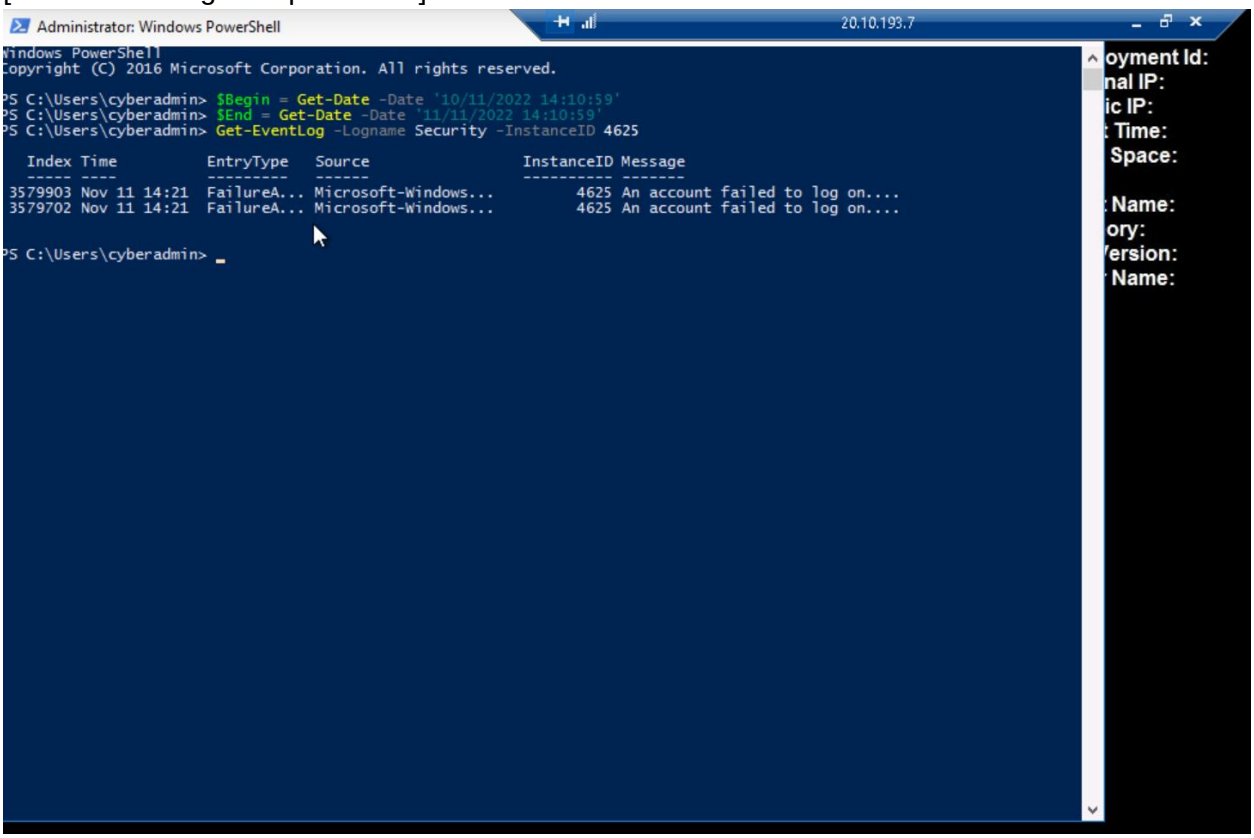
8. **Logging RDP Attempts:**

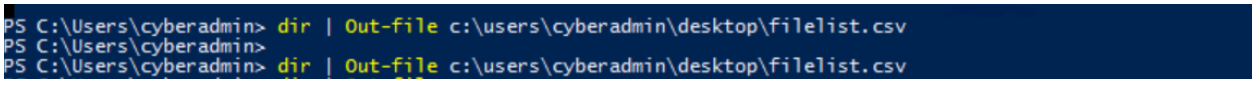
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

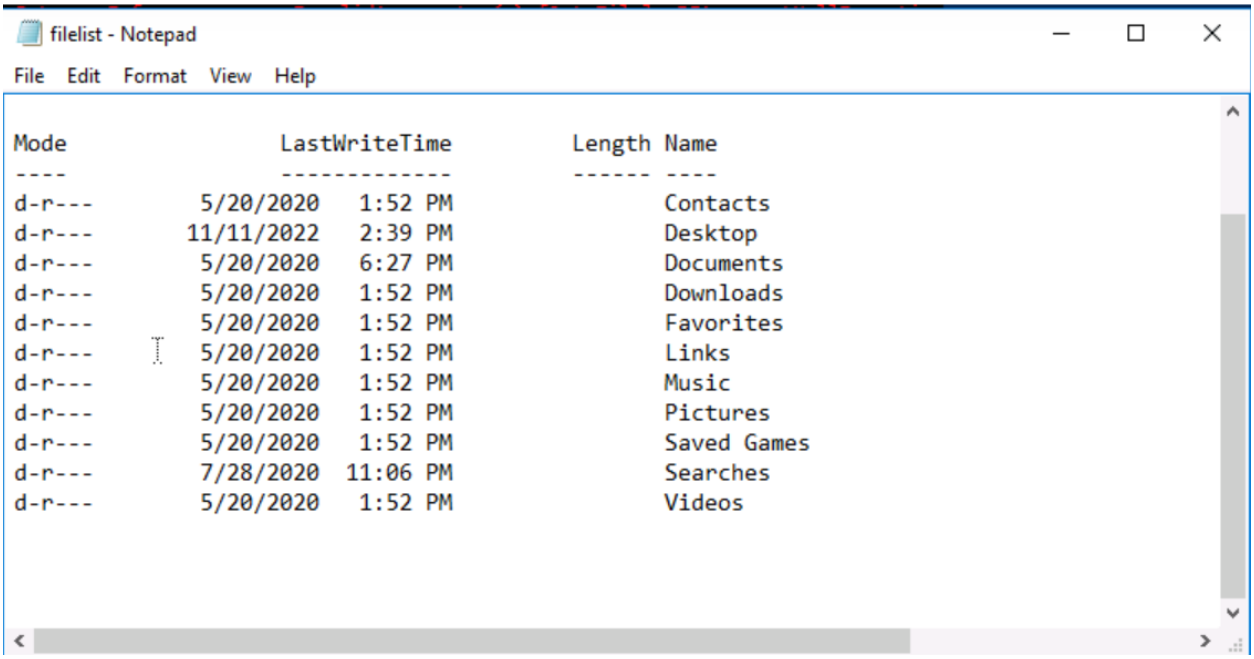
Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

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]



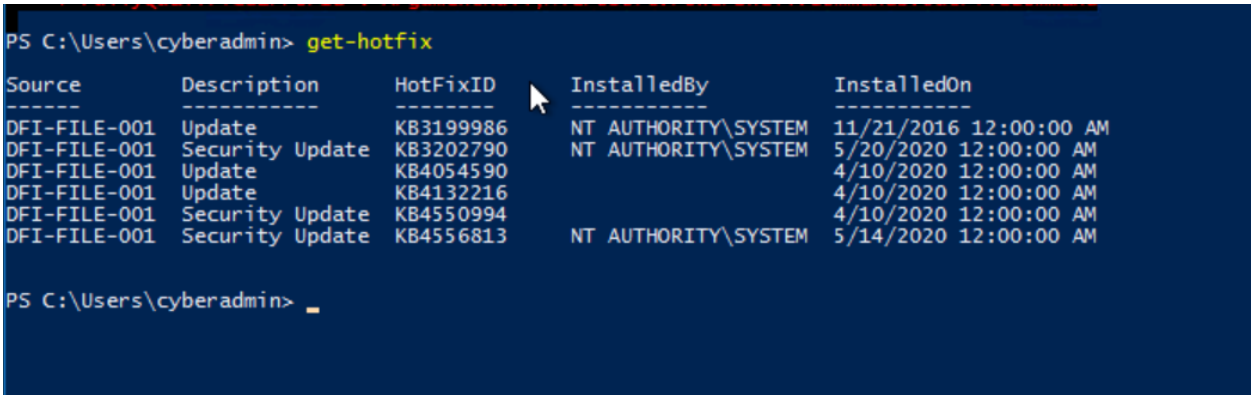




9. **Windows Updates:**

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
Security Update for Adobe Flash Player (3202790)	Update	Because This update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash libraries
KB4550994	update	This update makes quality improvements to the servicing stack, which is the component that installs Windows updates. Servicing stack updates (SSU) makes sure that you have a robust and reliable servicing stack so that your devices can receive and install Microsoft updates.
KB4556813	Update	The Microsoft Security Response Center (MSRC) investigates all reports of security vulnerabilities affecting Microsoft products and services, and provides the information here as part of the ongoing effort to help you manage security risks and help keep your systems protected

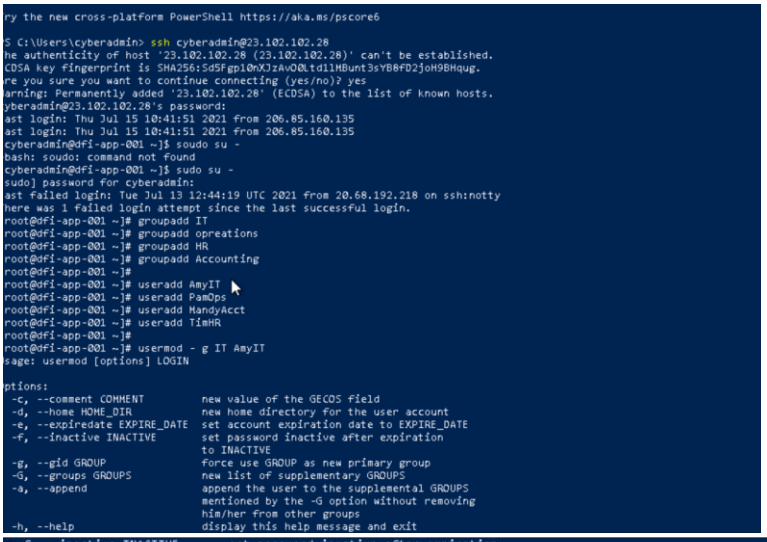
10. **Linux Data Directories:**

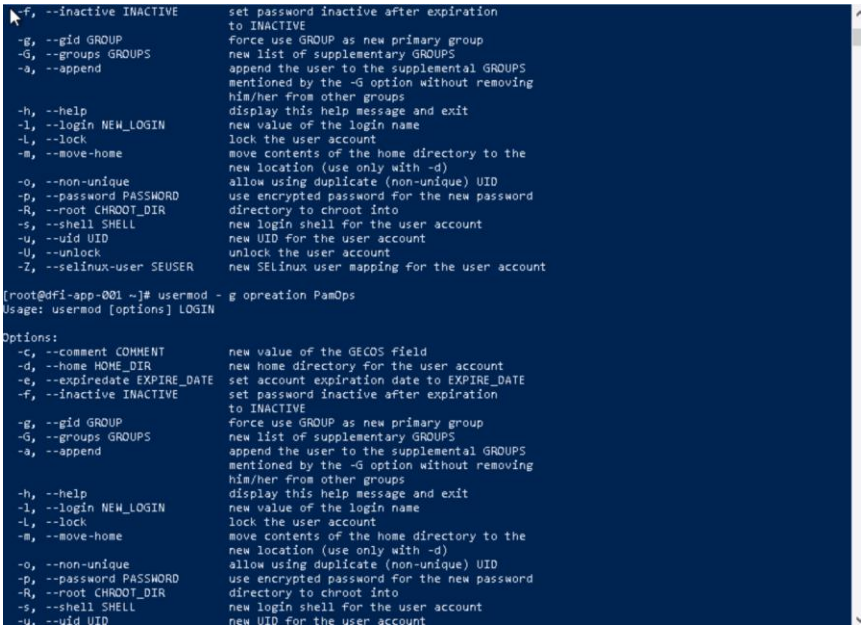
The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

- 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]





```
[root@dfi-app-001 ~]# cd ~
[root@dfi-app-001 ~]# ls -al
total 44
dr-xr-x---. 11 root root 4096 Nov 11 16:23 .
dr-xr-xr-x. 17 root root  236 Jul 28  2020 ..
drwxr-xr-x.  2 root root    6 Nov 11 16:02 Accounting
-rw-------.  1 root root 5270 Aug 15  2018 anaconda-ks.cfg
-rw-------.  1 root root  343 Nov 11 16:09 .bash_history
-rw-r--r--.  1 root root   18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 29  2013 .bashrc
drwxr-xr-x.  3 root root   18 Nov 11 15:42 .cache
drwxr-xr-x.  3 root root   18 Nov 11 15:42 .config
-rw-r--r--.  1 root root  100 Dec 29  2013 .cshrc
drwxr-xr-x.  2 root root    6 Nov 11 16:23 department
drwxr-xr-x.  2 root root    6 Nov 11 16:09 ~department
drwxr-xr-x.  2 root root    6 Nov 11 16:02 HR
drwxr-xr-x.  2 root root    6 Nov 11 16:02 IT
drwxr-xr-x.  2 root root    6 Nov 11 16:06 ls
drwxr-xr-x.  2 root root    6 Nov 11 16:03 opreation
-rw-------.  1 root root 5230 Aug 15  2018 original-ks.cfg
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
```

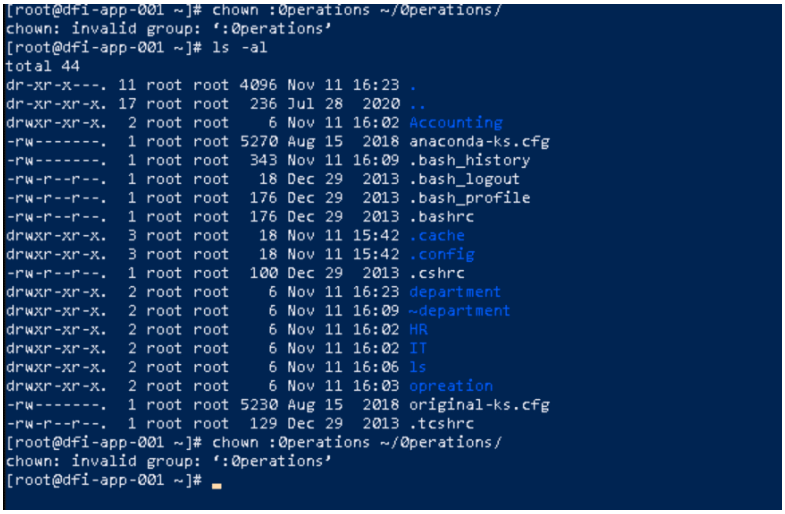
```
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account

[root@dfi-app-001 ~]# usermod - g Accounting MandyAcct
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT         new value of the GECOS field
  -d, --home HOME_DIR           new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP               force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                  append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                him/her from other groups
  -h, --help                    display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                    lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique              allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR         directory to chroot into
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                  unlock the user account
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account

[root@dfi-app-001 ~]# mkdir -p ~/IT
[root@dfi-app-001 ~]# mkdir -p ~/Accounting
[root@dfi-app-001 ~]# mkdir -p ~/HR
[root@dfi-app-001 ~]# mkdir -p ~/opreation
[root@dfi-app-001 ~]# mkdir -p ls
[root@dfi-app-001 ~]#
```

```
[root@dfi-app-001 ~]# chmod g+w  ~/0perations
chmod: cannot access '/root/0perations': No such file or directory
[root@dfi-app-001 ~]# chmod g+w  ~/0perations
chmod: cannot access '/root/0perations': No such file or directory
[root@dfi-app-001 ~]# ls -al
total 44
dr-xr-x---. 11 root root 4096 Nov 11 16:23 .
dr-xr-xr-x. 17 root root  236 Jul 28  2020 ..
drwxr-xr-x.  2 root root    6 Nov 11 16:02 Accounting
-rw-------.  1 root root 5270 Aug 15  2018 anaconda-ks.cfg
-rw-------.  1 root root  343 Nov 11 16:09 .bash_history
-rw-r--r--.  1 root root   18 Dec 29  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 29  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 29  2013 .bashrc
drwxr-xr-x.  3 root root   18 Nov 11 15:42 .cache
drwxr-xr-x.  3 root root   18 Nov 11 15:42 .config
-rw-r--r--.  1 root root  100 Dec 29  2013 .cshrc
drwxr-xr-x.  2 root root    6 Nov 11 16:23 department
drwxr-xr-x.  2 root root    6 Nov 11 16:09 ~department
drwxr-xr-x.  2 root root    6 Nov 11 16:02 HR
drwxr-xr-x.  2 root root    6 Nov 11 16:02 IT
drwxr-xr-x.  2 root root    6 Nov 11 16:06 ls
drwxr-xr-x.  2 root root    6 Nov 11 16:03 opreation
-rw-------.  1 root root 5230 Aug 15  2018 original-ks.cfg
-rw-r--r--.  1 root root  129 Dec 29  2013 .tcshrc
```



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

1. Connect to the VM
2. Switch user to root
3. Add groups
4. Add users
5. Add user to the respective group
6. Create new directories in the Home
7. change your current directory
8. List the current permissions
9. Adding specific permissions
10. Changing group ownership
11. Then The permission will change to

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 noticed there are more than one IP Address have lots of hacking attempts and we have to block them, Also I noticed from **DFI_FW_Report.xlsx** file that all of hacking attempts targeting Port Number 22 that is using for SSH , I recommend to change the number to high port Number to protect DFI server from these attacks that target SSH

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

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

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

In your own words explain the work you've done, the recommendations made and how DFI should proceed from a security standpoint. This is your opportunity to provide a thoughtful analysis that shows your understanding of Cyber Security and how all of the tasks you've performed contribute to the security of DFI. As this will be reviewed by non-technical management please keep the technical jargon to a minimum.
[Provide your Status Report Here]
First I connect windows server 2016 and Linux to windows 2010 via RDP and PowerShell(SSH) respectively, Then I performed a Windows server analysis : make sure that windows defender is ON, firewall state , Bit locker and windows smart screen , recommended to apply Principle of Least Privilege and Defense-in-Depth principles NIST800 I used them and other resources to determine the changes that should be made.
Also I created text of a firewall rule allowing a new DFI partner access to DFI-File-001 access via port tcp. As for VPN Encryption Recommendation , I recommend both of symmetric and asymmetric encryption because complement each other. File Hash verification , hash-based verification ensures that a file has not been corrupted by comparing the file's hash value to a previously calculated value. If these values match, the file is presumed to be unmodified via PowerShell. And checking for Logging RDP Attempts that was helpful by proving the date, the specific time and length name. then I searched for windows update that should be installed as well as any updates that can be safely ignored for DFI's purpose.
I took a look at firewall alerts in DFI_FW_Report.xlsx file I noticed some I noticed there are more than one hacking attempts and we have to block them for the purpose of protection

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.