# Scenario:

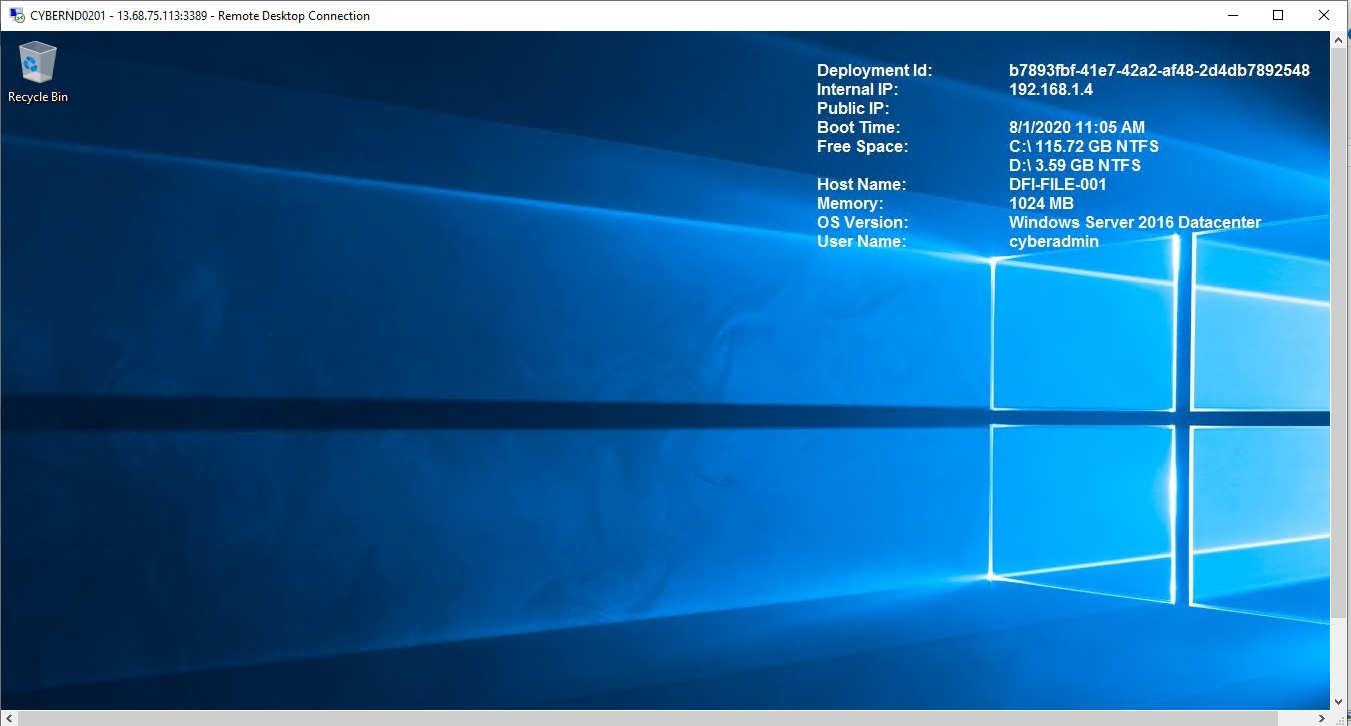
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

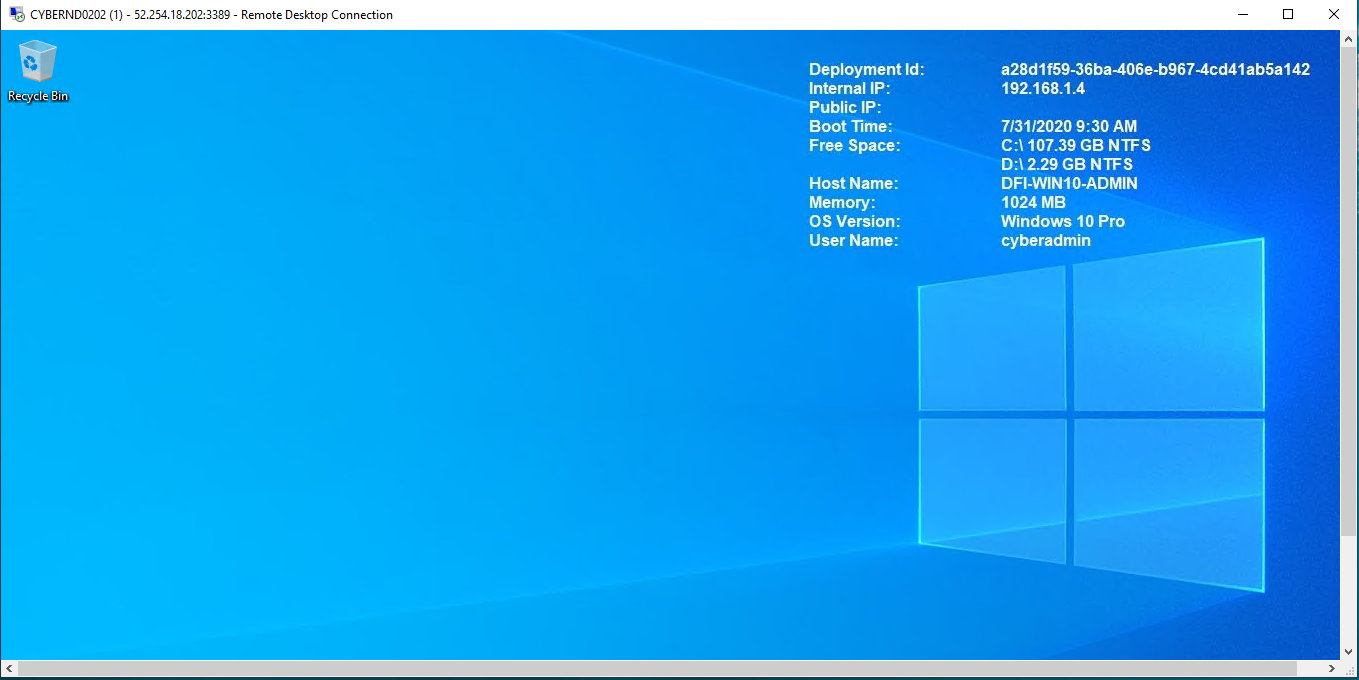
## Week One:

### 1. **Connect:**

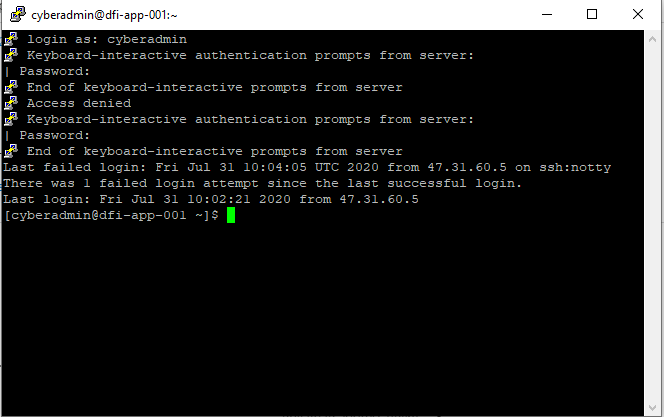
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

**RDP connections**





**SSH Connection**



### 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.](http://iieng.org/images/proceedings_pdf/8285E0914047.pdf) [NIST 800-123](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf) (other NIST documents could also apply.)

**Permissions and User Accounts-** It’s important to follow the principle of least privilege while providing permissions to certain groups in organization.

* Remove or Disable Unneeded Default Accounts
* Disable Non-Interactive Accounts
* Create user groups and user accounts
* For administrator group we can provide Full control, so that they can have access to the full server. This also help them to maintain the server.
* IT group are very similar to administration group and these can be even nested to single group. However, we can create a separate group for IT admin and they can have can access the full control only when required.
* For other groups, principle of least privilege should be provided. Departments should be isolated, and shouldn’t have permission to modify (read, write, change, delete) any document of other department.
* Departments which have dependency can be provided Read and Execute permission. Write permission should be disabled.

Services- Ideally, a server should be on a dedicated, single-purpose host.

* When configuring the OS, remove all services, applications, and network protocols (e.g., IPv4, IPv6) that are not required.
* Disable any such unnecessary components that cannot be removed.
* Don’t install unnecessary services.

Examples of few services that can be removed or disabled are

* File and printer sharing services
* Remote control and remote access programs like Telnet.
* ­ Wireless networking services
* Email services like SMTP
* Language compilers and libraries
* Directory services like Lightweight Directory Access Protocol [LDAP]

**Updates**

* Create, document, and implement a patching process.
* Identify vulnerabilities and applicable patches.
* Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed)
* Install permanent fixes (patches, upgrades, etc.)
* ­ Keep the servers disconnected from networks or connect them only to an isolated “build” network until all patches have been transferred to the servers.
* Place the servers on a virtual local area network (VLAN) or other network segment that severely restricts what actions the hosts on it can perform and what communications can reach the hosts—only allowing those events that are necessary for patching and configuring the hosts.

### 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.

**Rule**

**name 21.19.241.63 WBC-International**

**name 172.21.30.44 DFI-File-001**

**access-list DFI-Ingress extended permit tcp host WBC-International host DFI-File-001 eq 9082**

**Reason Explanation**

Our partner WBC International wants to connect to our database and we need to provide them access to connect to our network. We used Cisco Firewall rule to allow them to connect them with our network to a specific IP and port number. We have created a rule which allow only authorized traffic to access our database by following principle of least privilege.

**Rule Explanation**

We have named the client IP **21.19.241.63** as **WBC-International**, and our host IP as **172.21.30.44** as **DFI-File-001**.

In our command we start with **access-list** which controls the traffic on network next,

we have used **DFI-Ingress** which is the name of the interface which suggests that traffic will be coming to our internal interface to reach our database server next,

we have used **extended permit** which gives flexibility to matching traffic and protocols next,

we have specified **tcp** is the protocol used next,

we have named the source **WBC-International** which is our client having IP **21.19.241.63** next,

we have named our host name **DFI-FILE-001** with ip **172.21.30.44** and port number 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](https://tools.cisco.com/security/center/resources/next_generation_cryptography) as a guide.

## Since we are dealing with data with transit, I will recommend **IPsec VPN Encryption with Encapsulating Security Payload (ESP).** Here are some recommendations to follow when using the encryption techniques-

* Don’t use null Encryption (esp-null)
* Use both authentication algorithm (esp-sha256-hmac is recommended) and encryption algorithm (esp-aes is recommended).

Cisco Adaptive Security Appliance (ASA) uses 256-bit AES encryption and HMAC-SHA-256 authentication for ESP IPsec in tunnel mode.

### 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.

**System Admin Rule**

**alert tcp any any -> 172.21.30.44 any (msg: “ICMP traffic”; sid: 1000001;)**

**VoIP Admin Rule**

**alert tcp any any -> 172.21.30.55 any (msg: “TFTP traffic”; sid: 1000002;)**

**Rule Explanation**

We have requirement by system admin that we are receiving high volume ICMP traffic and there is a possibility of DDoS attack. Similarly, VoIP administrator is also concerned that attacker is attempting to connect to her primary VoIP server.

We have written snort alert syntax for both.

**System Admin Rule** – Syntax start with **alert**  and is **tcp** protocol, we are expecting traffic from **any** Ip and **any** port number. **->** represents that it’s an inbound traffic to IP **172.21.30.44** on **any** port. The **msg** we will receive when the traffic comes will be **“ICMP traffic”** and we have given an **sid** number **1000001.**

**VoIP admin Rule-** Syntax start with **alert**  and is **tcp** protocol, we are expecting traffic from **any** Ip and **any** port number. **->** represents that it’s an inbound traffic to IP **172.21.30.55** on **any** port. The **msg** we will receive when the traffic comes will be **“TFTP traffic”** and we have given an **sid** number **1000002.**

### 6. **File Hash verification:**

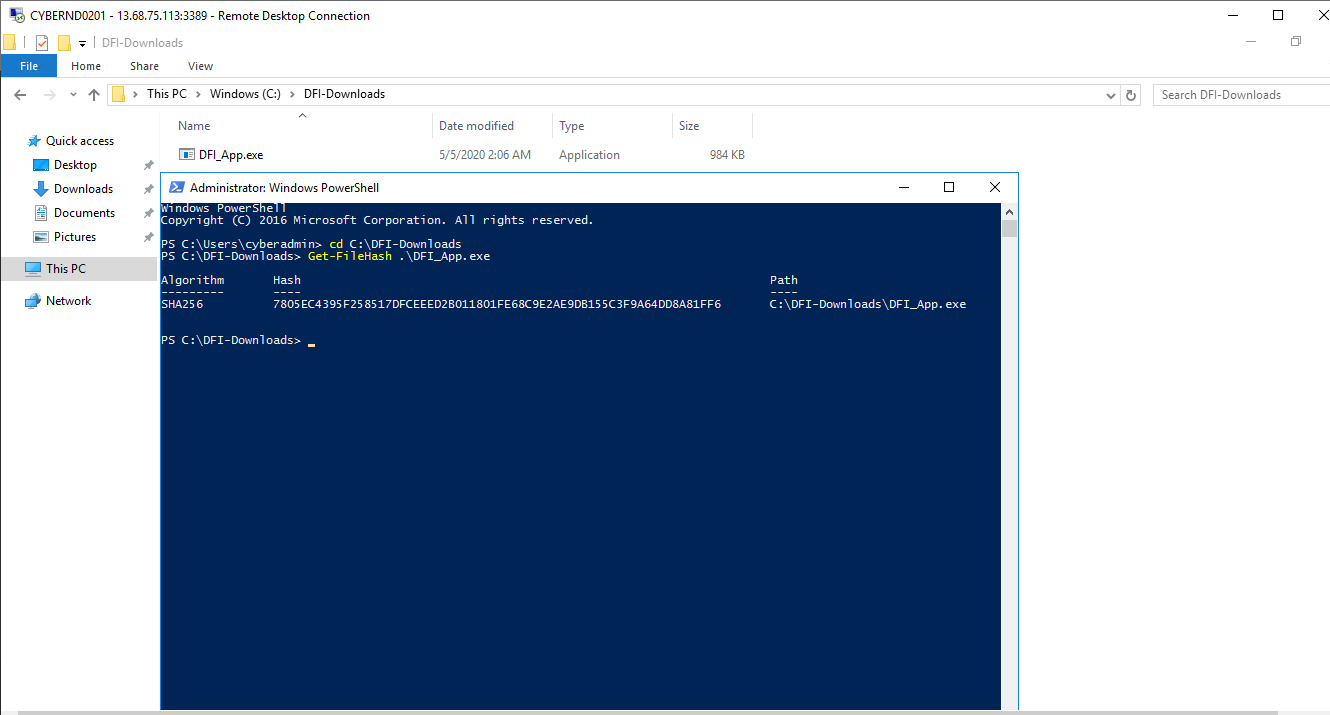
A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

**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.

**Screenshot**



**Conclusion:** The file hash matches.

## 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** |
| 1. AI Firewall | Use Automated Threat Intelligence, to block malicious IP address | Blocking web endpoints manually is a very tough job. With growing end-points it has become almost impossible in terms of time and resource to block these IP addresses. With increase of Artificial Intelligence, most industries are now moving towards a new direction and are implementing AI in their systems to protect them from malicious attacks. |
| 2. Automate IDS rules | We can automate the IDS and Cisco firewall rules that we have written. | These rules are for all traffic and when any unwanted traffic comes, that should be blocked and should only be allowed after authorized admin permission. |
| 3. AWS or Google Cloud Storage | Moving data to cloud for better security and availability. | Its hard to store data as it grows. We can use cloud services provided by Google, Amazon or Azure to store our data for high availability and security. Its also easy to implement the principle of Least privilege in these cloud platforms. In case of any natural disaster or failure chances are less that all our data will be wiped out as they are stored in different location in world. |
| 4. AlienVault: Unified Security Management (USM) | Commercial SIEM tool for data collection and logging. | It’s a universal commercial tool which provides good support. Can be used for event data collection and logging purposes and can be integrated easily with virtual, hardware and cloud platforms. This can help identify many malicious traffic and unauthorized activities on our network. |
|  |  |  |

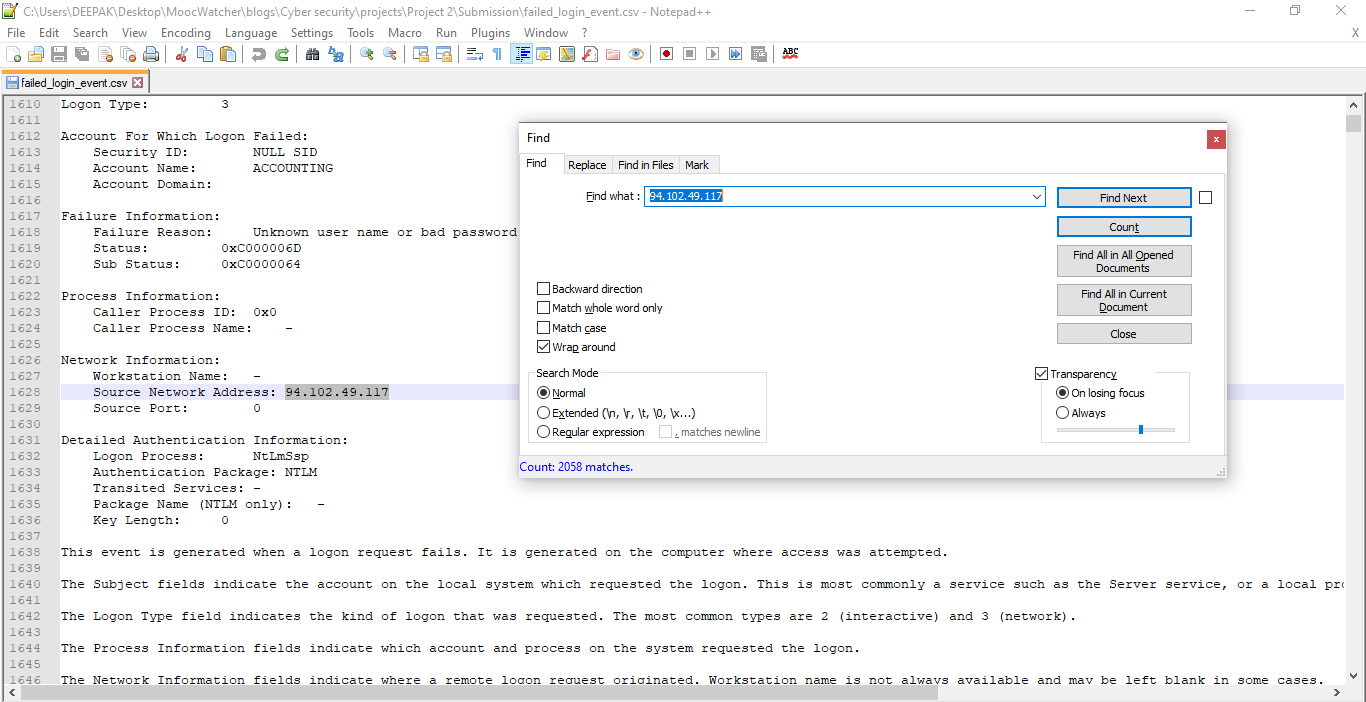
### 8. **Logging RDP Attempts:**

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

Prepare a report that lists unsuccessful attempts. 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.

**Screenshot (File attached in submission “*failed\_login\_event.csv*”)**



**Finding, justification and Recommendations**

In my finding I found that IP **94.102.49.117** had made **2058** attempts on our server, attacker have used different account names to login into the system and have failed to do so. With the attempt we can see that the DDOS attack may be imminent. My suggestions will be to upgrade our firewall rule to block this IP immediately.

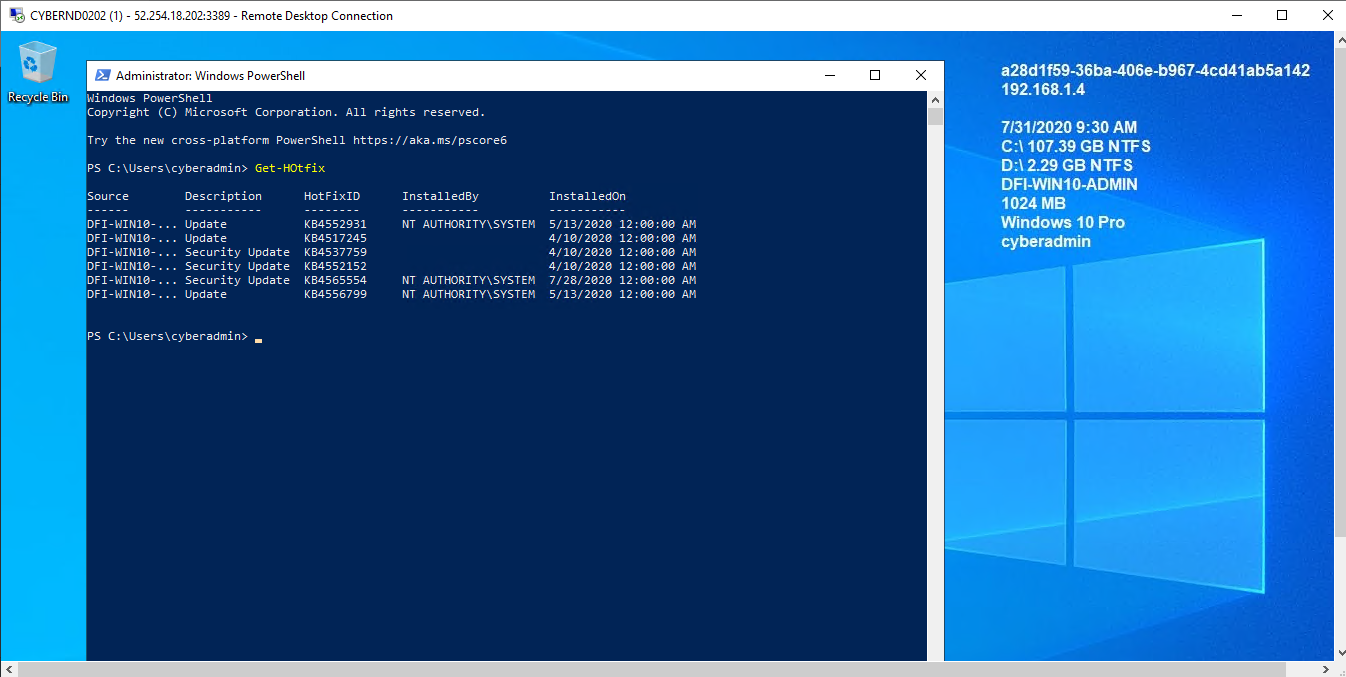
Other than that, there were several one-time failed attempts with different IP addresses. I recommend we should avoid principle of least privilege and block all unwanted traffic, and a new Firewall rule to be created to allow only authorized IP on our internal network.

### 9. **Windows Updates:**

Using [NIST 800-40r3](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf) and [Microsoft Security Update Guide](https://portal.msrc.microsoft.com/en-us/security-guidance), 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.

These are the updates we found in windows system



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

|  |  |  |
| --- | --- | --- |
| Available Updates | Update/Ignore | Justification |
| KB4537759 | Update (Critical) | Its security update for windows Flash player. |
| KB4552152 | Update (Critical) | Its security update, servicing Stack Update for Windows 10 Version |
| KB4565554 | Update (Critical) | This update addresses an elevation of privilege vulnerability that exists when the Windows Modules Installer improperly handles file operations. |
| KB4552931 | Ignore | Its a .NET framework update. Not critical and can be ignored. |
| KB4556799 | Ignore | Its not critical update and causing bugs in network issues. New update KB4559004 was launched to fix its issues. |
| KB4517245 | Ignore | Its feature updates for functionality like search feature. It’s not critical update can be ignored for now. |

### 10. **Linux Data Directories:**

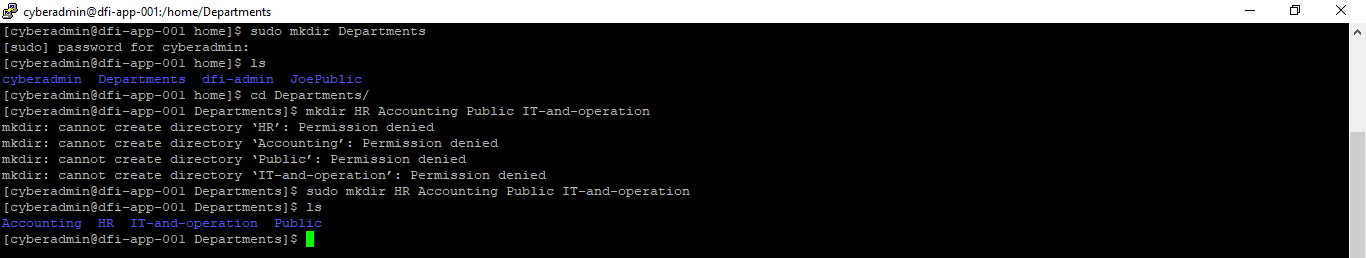
The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

* 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.

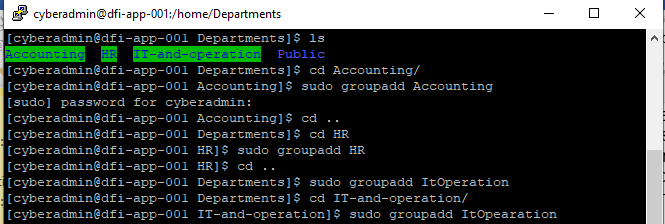
For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

**Screenshots with Details**

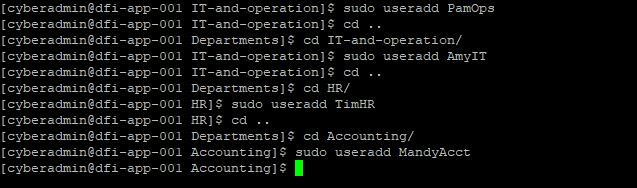
1. **Creating Departments in Home Directory with subdirectories HR, Accounting, Public, IT and Operations**. Here we have requirement to create different departments for our organization, we know we need to create HR, Accounting, HR and IT and Operations departments. We used **mkdir** linux command to create directories



1. **Creating New Groups:** Next we need to create groups for each department so that the user created can access the files of their Department. We created Accounting, ItOperation and HR Groups using **groupadd** commands.



1. **Creating Users :**  After creating Groups we created Users AmyIt and PamOps for It Operation group, TimHR for HR group, MandyAcct for Accounting group. We used **useradd** linux command to create each user.



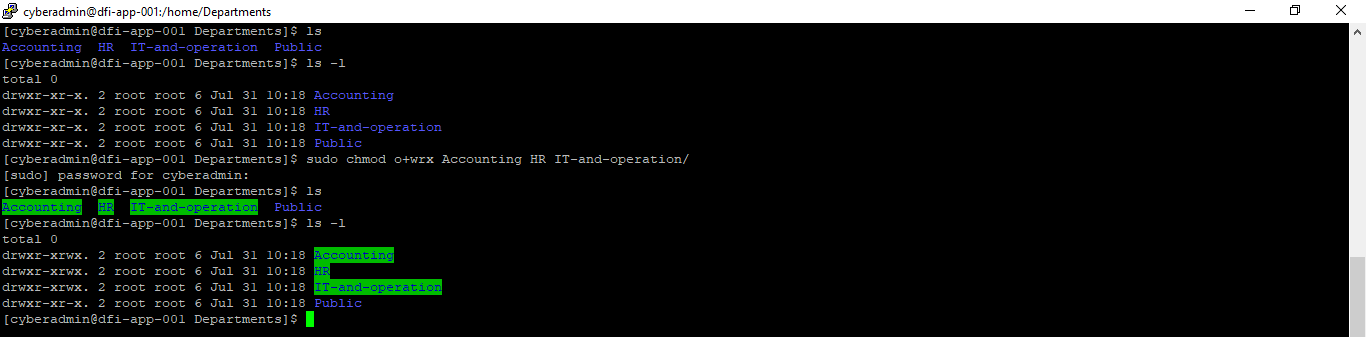
1. **Adding User to group:** After creating users and groups for each department, We need to add these users to their respective departments. We used **usermod -G groupname username** to add user to their respective group



1. **Confirmation of added users:**  We confirmed that our users are added to their respective groups by using the **cat \etc\group command** (Can’t display command here due to lack of space during screenshot capture. Showing only the result)



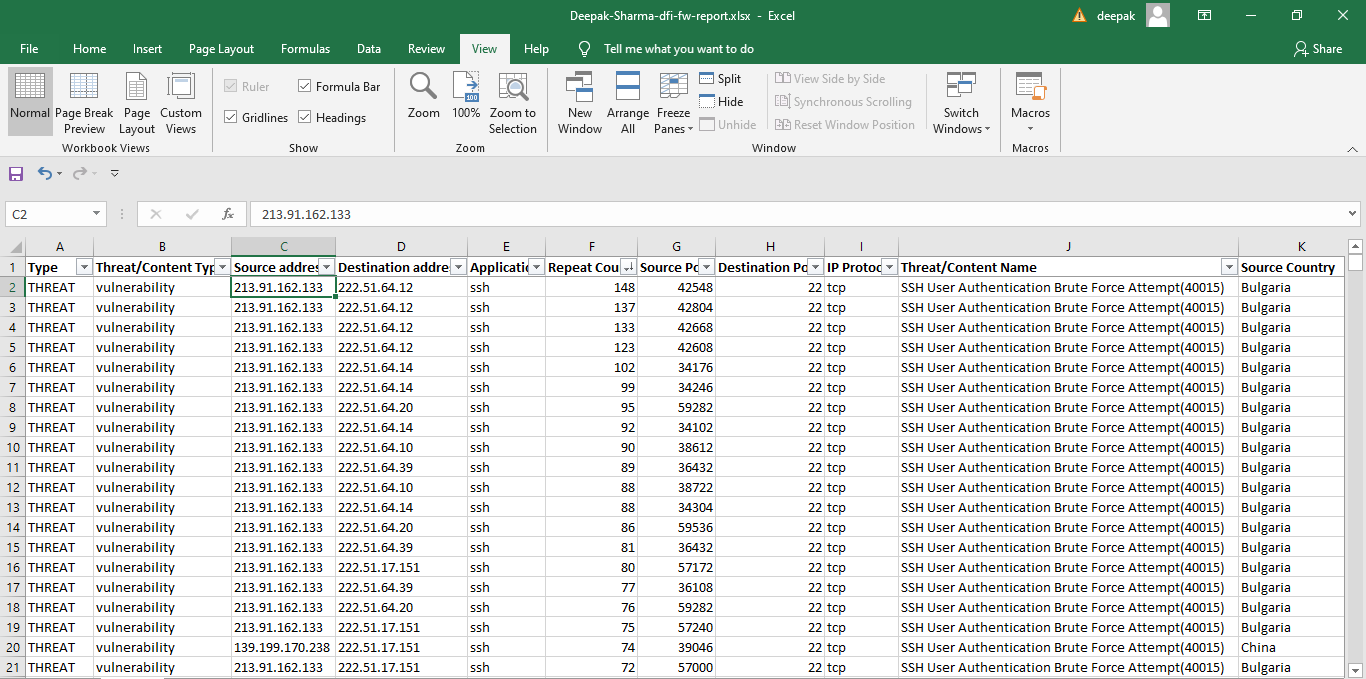
1. **Changing Owner Permission:** Lastly, we provided the owner permission to the directories to be used by their respective users. We used **chmod o+wrx directory name** command, which is confirmed by green color using **ls -l command**



### 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.



We can see that our network is experiencing SSH User Authentication Brute Force attack from different IP and different countries including Bulgaria, China, USA, Argentina, Poland, Vietnam etc. With Bulgaria been the top, followed by China and USA. **213.91.162.133** is the source of most attacks from Bulgaria.

We can take the following steps-

* Are the IP addresses authorized to access the network? This can be approved by the server admin. We should check if these IP addresses are malicious and are present in any global block list database like AbuseGlobalDb.com.
* If any IP is found malicious, these should be reported to ISP hosting.
* We should add malicious IP addresses to our manual block lists to prevent future attacks.
* We should update all our systems, antivirus and other software’s to prevent from any zero-day attack.
* We can use VPN as an extra security layer to access the SSH traffic.
* We should verify that we are using strong passwords as these attackers have already tried many passwords during their Brute Force attempt. Change if necessary.

### 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.

**Status Report**

It has been very informative weeks for me and company. I have worked in different areas and will like to share my experience as a Security Analyst and findings and improvement that we can follow in our organization.

* I have created Cisco Firewall rules to take new network connection with our new partner **WBC-International.** I have only exposed the specific port and Ip address for incoming traffic which only allows authorized traffic to access our database by following the principle of least privilege.
* Recommended Cisco VPN Encryption algorithm and product to use for our new payroll processing partnership with Payroll-USA
* I have created the new IDS snort rule, to block malicious traffic to prevent our network from a possible DDOS attack. This rule was created after observation from system admin and VoIP admin as they were getting heavy unwanted traffic on our network.
* I have done successful hash verification for the new windows custom application that was provided by software vendor on their public FTP site by email.
* In future, to prepare for future attacks I recommend automation done in some area of our infrastructure. I recommend to use AI powered firewalls to stop malicious traffic and attack, automate the IDS rule to block the malicious rule in future and recommends to move our critical data to cloud infrastructure and use commercial logging tools to better observe our servers.
* I checked the Windows security logs to identify the IP that was trying to log in to our windows RDP, as our IT Manager was having suspicion that someone has been attempting to login to DFI-File-001 via RDP. We observed the login failed attempts for 24 hours.
* I checked the update status in our Windows server and found that we have not updated 3 critical security updates that makes our server vulnerable for attacks. I also verified the non-critical updates that can be ignored for now as they were not that critical.
* I created directories on the CentOS server DFI-App-001. I created different Directories and users accounts for their respective departments. We followed the principle of least privilege, so that the users of each department own authority of their department but can’t modify or access files of other department.
* Finally, I did analysis of **DFI\_FW\_Report.xlsx** file, containing the result of firewall results. We observed unwanted traffic coming to our network and recommended how we can fix the issues and block the malicious traffic.

Finally, I want to thank my managers for providing me the opportunity and taking into consideration my recommendation which I feel can help us company implement to make our network more secure and make our customers and client feel safe on using our products.

### 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.**