

## 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:

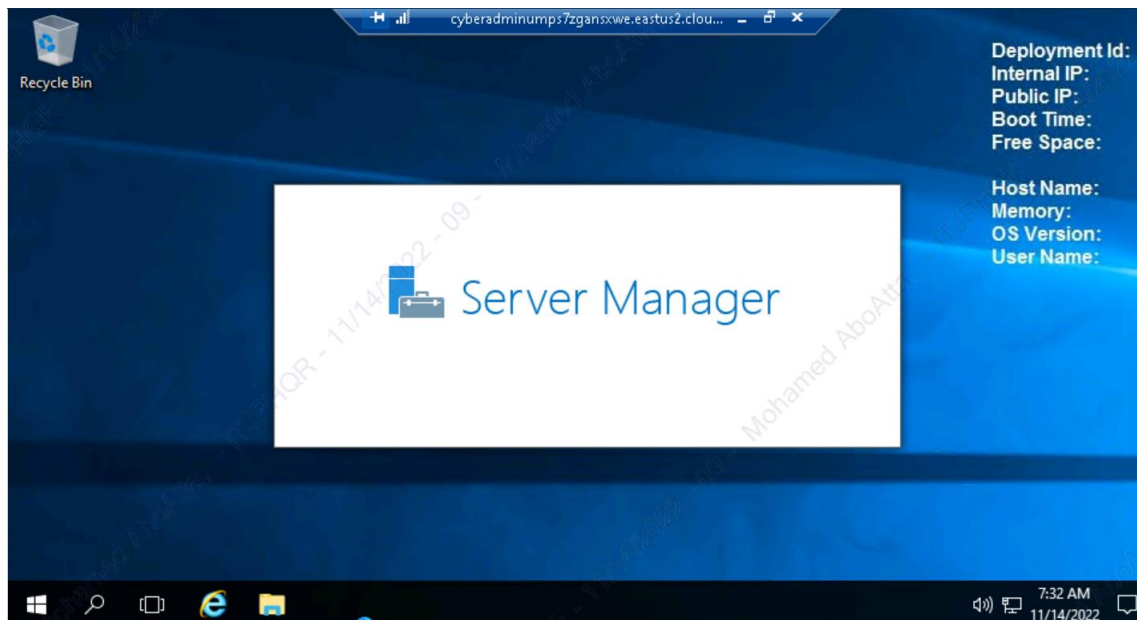
### 1. Connect to the servers:

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

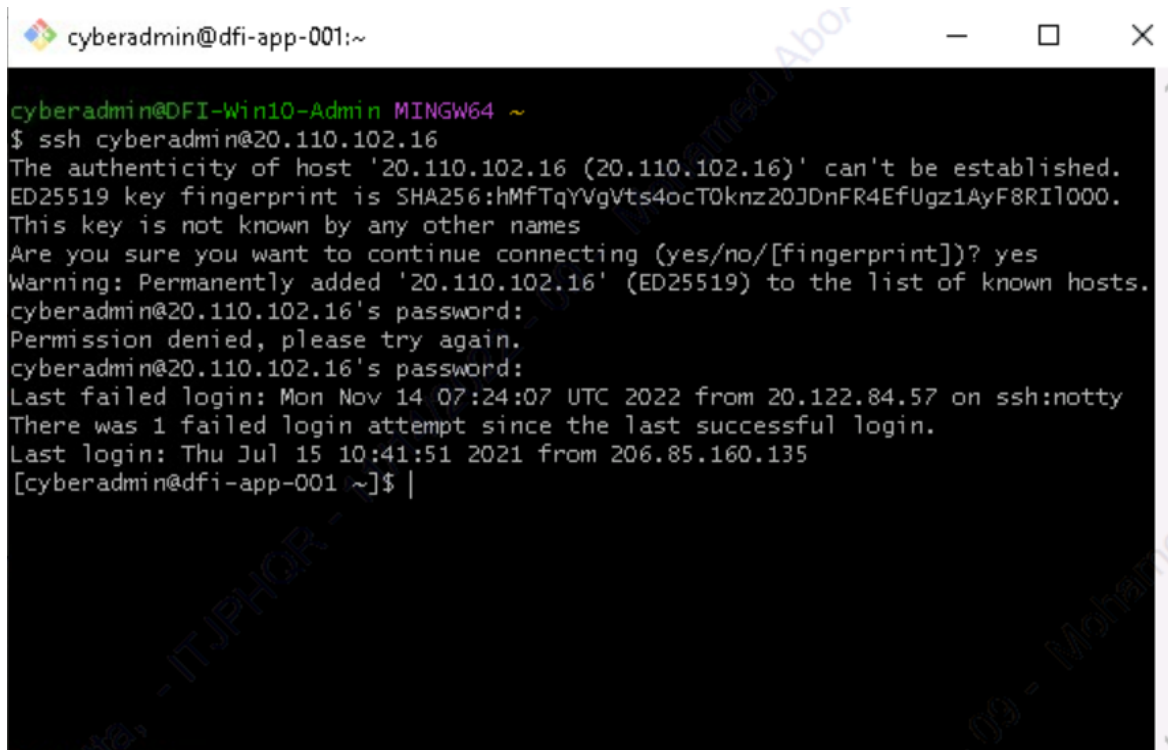
- **Windows server 2016** - If you are using Udacity cloud lab, you can directly log into the machine in the classroom. If you have set up the Windows server 2016 VM in your personal Azure account, you will have to use the RDP to connect.
- **Linux (CentOS) server** - If you are using Udacity cloud lab, 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.**
  - Connected using RDP connection



- a connection to the Linux server using SSH.
  - Connected using SSH remote connection.



The screenshot shows a terminal window titled 'cyberadmin@dfi-app-001:~'. The user is in a MINGW64 environment. They run the command `$ ssh cyberadmin@20.110.102.16`. The terminal output shows a warning about the host's authenticity, a confirmation to continue, and the addition of the host to the known hosts list. The user then enters their password, but the connection is denied. The terminal also shows the last failed login and the last successful login details.

```
cyberadmin@DFI-Win10-Admin MINGW64 ~  
$ ssh cyberadmin@20.110.102.16  
The authenticity of host '20.110.102.16 (20.110.102.16)' can't be established.  
ED25519 key fingerprint is SHA256:hMfTqYVgVts4ocT0knz20JDnFR4EfUgz1AyF8RI1000.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '20.110.102.16' (ED25519) to the list of known hosts.  
cyberadmin@20.110.102.16's password:  
Permission denied, please try again.  
cyberadmin@20.110.102.16's password:  
Last failed login: Mon Nov 14 07:24:07 UTC 2022 from 20.122.84.57 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.

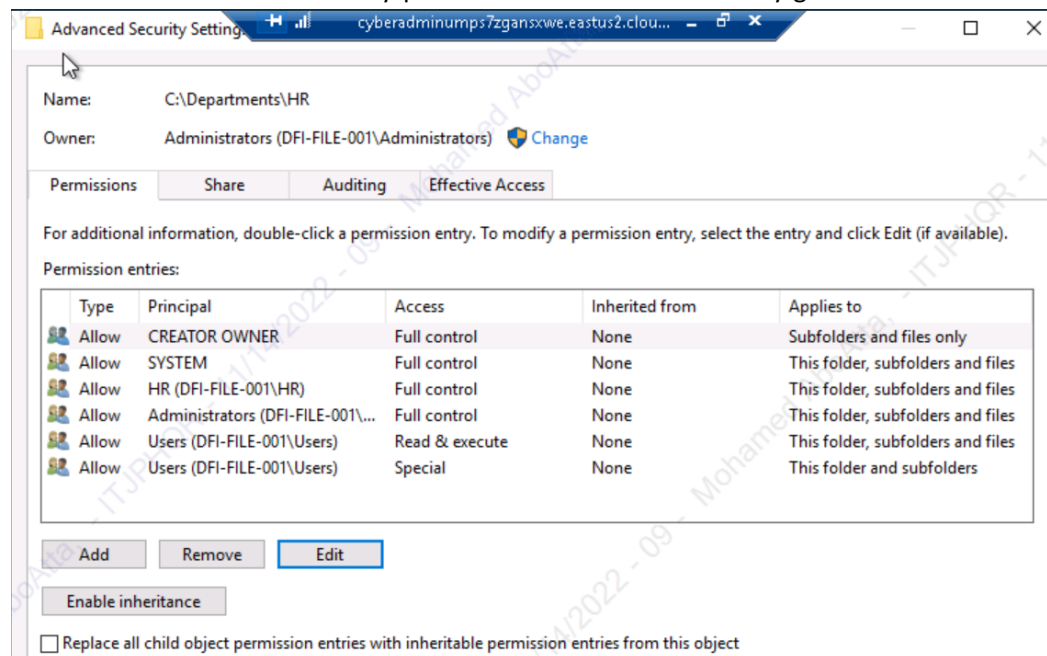
Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI-compliant organization and will likely be Sarbanes-Oxley soon.

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.)

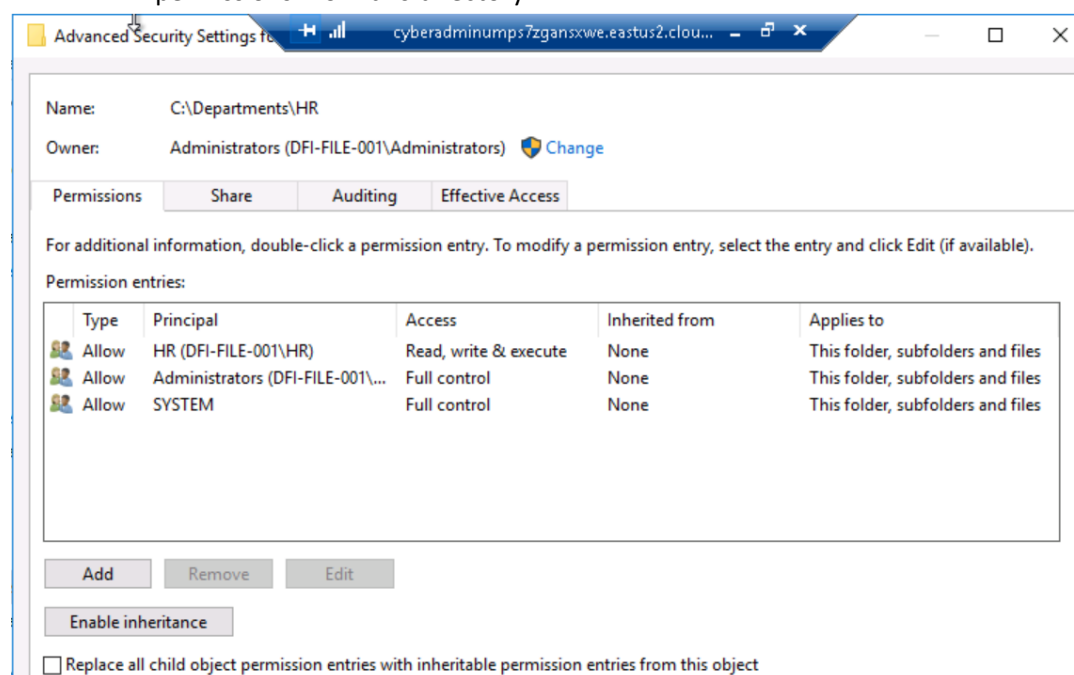
[Place your security analysis here.]

Write a report detailing 3 primary areas

- File Permissions that need to be modified (Tip: Do not miss the security permissions on the HR Directory.)
- The security permissions on the HR Directory gives full access to many users:

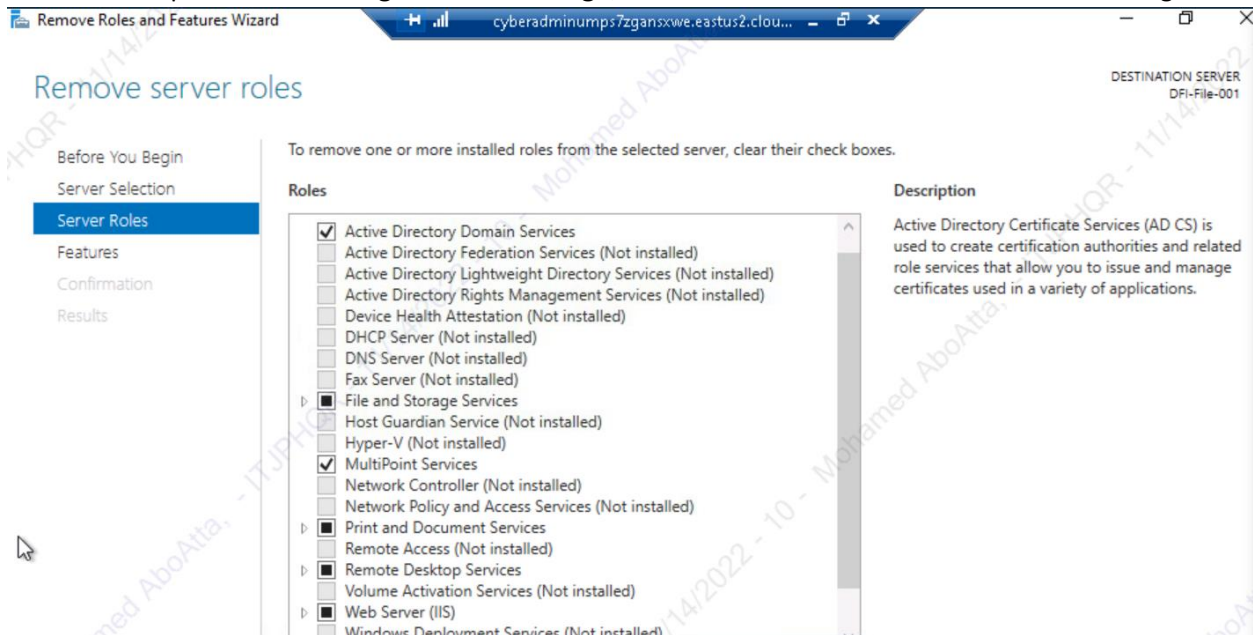


- We should limit the full control to the Administrators and SYSTEM groups only. Also, we should give the right permissions to the HR group and remove all other users/groups permissions from this directory.

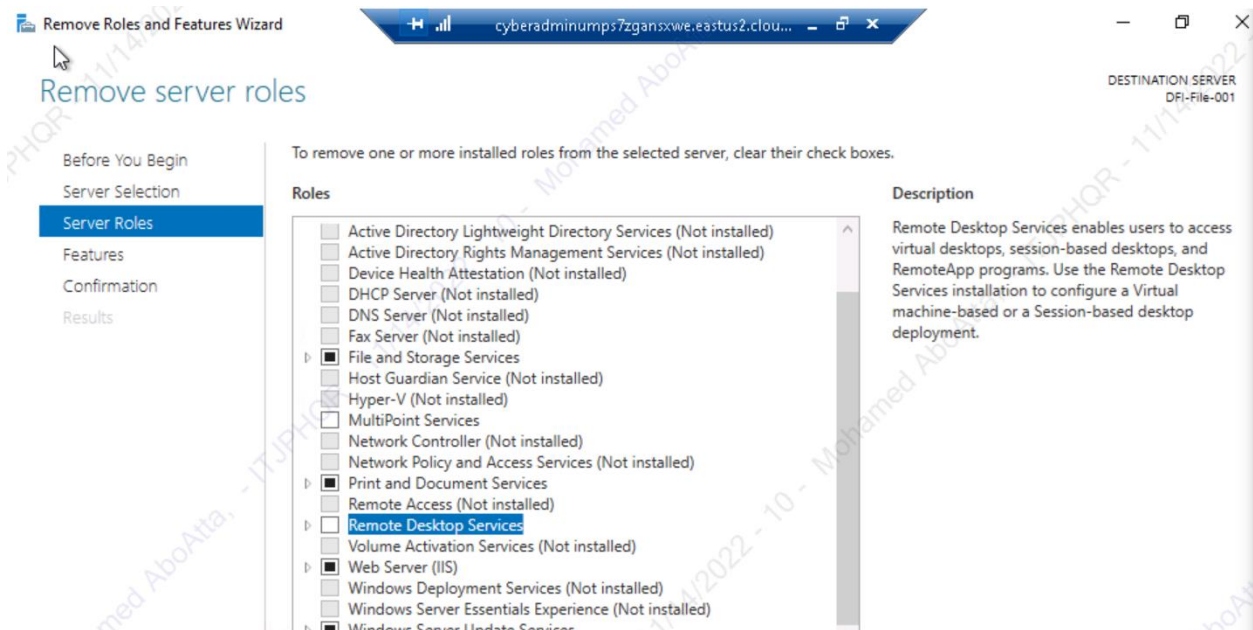


- **Roles that are not needed on the Windows server**

➤ Open **Server Manager**. Under **Manage**, click **Remove Roles**. We will find the following roles:

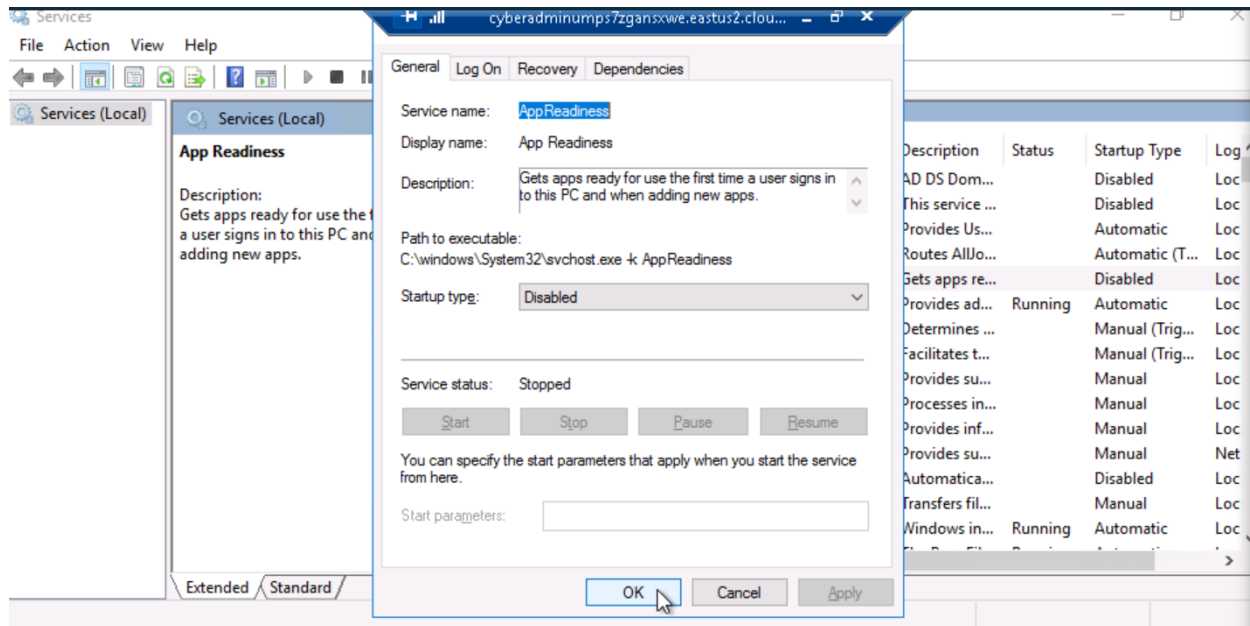


➤ Some the following roles should be removed: Active Directory DS, Remote Desktop Services, IIS, and MultiPoint Services. On the other hand, any other essential services like File and Storage Services should be kept:



- **Any services that should or should not be running**

- Search for **Services**. stop the services that are not necessary/or maybe to exposed to vulnerabilities such as
  - W3SVC
  - App Readiness
  - MapsBroker
  - OneSyncSvc
  - AxInstSV



### 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 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.**

- Granting Access to Vendor:
  - Vendor IP: 21.19.241.63
  - Our IP: 172.21.30.44
  - Port: TCP-9082
- To name the source IP, we type **name**, the IP address, and the name we want to call it.
  - **name 21.19.241.63 WBC-001**
- Similarly, we name the destination IP:
  - **name 172.21.30.44 DFI-File-001**
- Now, that those are in place, let's create the rule. A basic rule begins with **access-list**. Since this traffic is coming inbound, we'll use our internal interface of **DFI-Ingress**. The interface is named when the firewall is initially configured. Next, we'll use **extended permit**. We're also using the TCP protocol. For the source, we use our named object **WBC-001**. For our destination, we use the named object for that as well **DFI-File-001**. Finally, the port we're opening is **9082**.
- Template command:
  - **access-list [interface] extended permit tcp host [source] host [dest] eq [port]**
- Final command:
  - **access-list DFI-Ingress extended permit tcp host WBC-001 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.**

- The acceptable encryption solutions as per Cisco documentation are:
  - AES-CBC mode
  - RSA-2048
  - RSA-3072
- I will choose the AES-CBC encryption solution.
- AES (Advanced Encryption Standard) has become the encryption algorithm of choice for governments, financial institutions, and security-conscious enterprises around the world. The U.S. National Security Agency (NSA) uses it to protect the country’s “top secret” information, as per [this article](#).
- Symmetric Strengths and Weaknesses (**AES Advanced Encryption Standard**):
  - Very Fast.
  - Each party already has the key so the data can be transmitted in any manner.
  - Key transport is difficult. The only true secure way is to hand it from person to person.
  - Once key is exchanged there is no identity verification as to who has the key.
- Asymmetric Strengths and Weaknesses (RSA Rivest Shamir Adleman):
  - Authentication allows you to verify the identity of the sender/recipient.
  - Private Key never needs to be shared.
  - Slower than Symmetric.
  - By requiring a Certificate Authority, it creates the need to trust a 3rd party.

## 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]**

**[Place your VoIP Admin rule and explanation here]**

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

**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.**

- An IDS is an intrusion detection system.
- Intrusion Detection is a critical layer in an organization's security program.
- It can be a hardware appliance or a virtual machine.
- It can reside at the edge of the network for incoming traffic, or it can reside inside the network to monitor internal traffic.
- An IDS is generally passive; it reports alerts to the Sysadmin.
- An IPS operates the same but adds active response to the alert.
- IDS uses behavior or heuristic monitoring and fires signatures or rules in reaction.
- Snort Rule Template:

alert [protocol: tcp, udp, or icmp] [Source IP address] [Source port#] [Direction -> or <-] [Destination IP] [Destination Port] [Rule options: (msg:"RPC Attempt"; sid:1000001;)]

- System Admin rule:
  - alert icmp any any -> 172.21.30.44 any (msg:"DFI-File-001 Access Attempt"; sid:1000001;)
- VoIP Admin rule:
  - alert udp any any -> 172.21.30.55 8099 (msg:"VoIP server Access Attempt"; sid: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**.

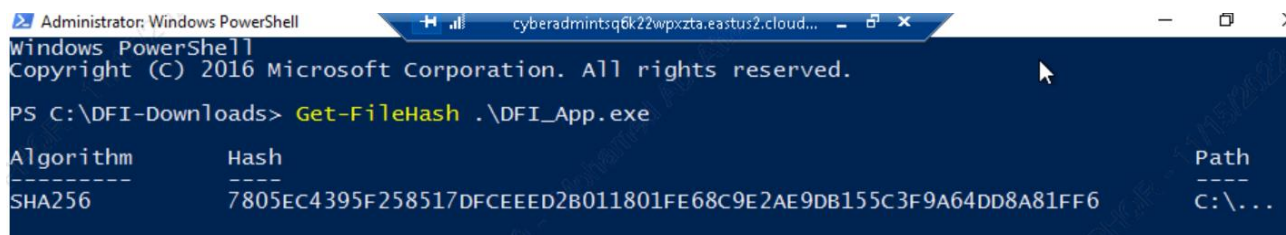
**Hash:** 7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6

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.**

**[Place your screenshot that displays the command that was run as well as the file hash.]**

- File Hashing transforms blocks of data into a far shorter length to represent the original string.
- It is not encryption. Hashing is a one-way function.
- Common Types of Hashes:
  - MD5 Message Digest 5 - mainly retired due to collisions which are the risk of a duplicate hash.
  - SHA2 Secure Hashing Algorithm 2. When you think SHA256, this is it.
- Key Terms
  - File Hash: is the process of using an algorithm for verifying the integrity of a computer file.
  - Collision: is a situation that occurs when two distinct pieces of data have the same hash value.
- We use the Powershell file hash feature to compare the digital fingerprint of the file.
- We navigate to the path of the file.
- Then, we type **powershell** in the address bar to open the PowerShell in the current directory.
- Finally, we use the command:
  - **Get-FileHash filename**



```
Administrator: Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

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

Algorithm      Hash
-----
SHA256         7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6
Path
-----
C:\...
```

## 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
Active Directory	Automatic account lockout if login from 2 geographically distant Ips.	It's the Superman theory. No one could exist in two geographically distant locations in the same time frame.
Wireless	I recommend a Controller-Based Wireless Solution. Choose the strongest authentication available, for instance, WPA2-Enterprise with 802.1x Encryption.	This will allow management of the wireless network to be controlled only by DFI and will be accessible locally even in the event of an internet outage.
Incoming Traffic	Snort IDS / IPS	We can use IDS/IPS to set rules that alerts us if we receive a huge traffic volume that could be a DDoS attack.

## 8. Logging RDP Attempts:

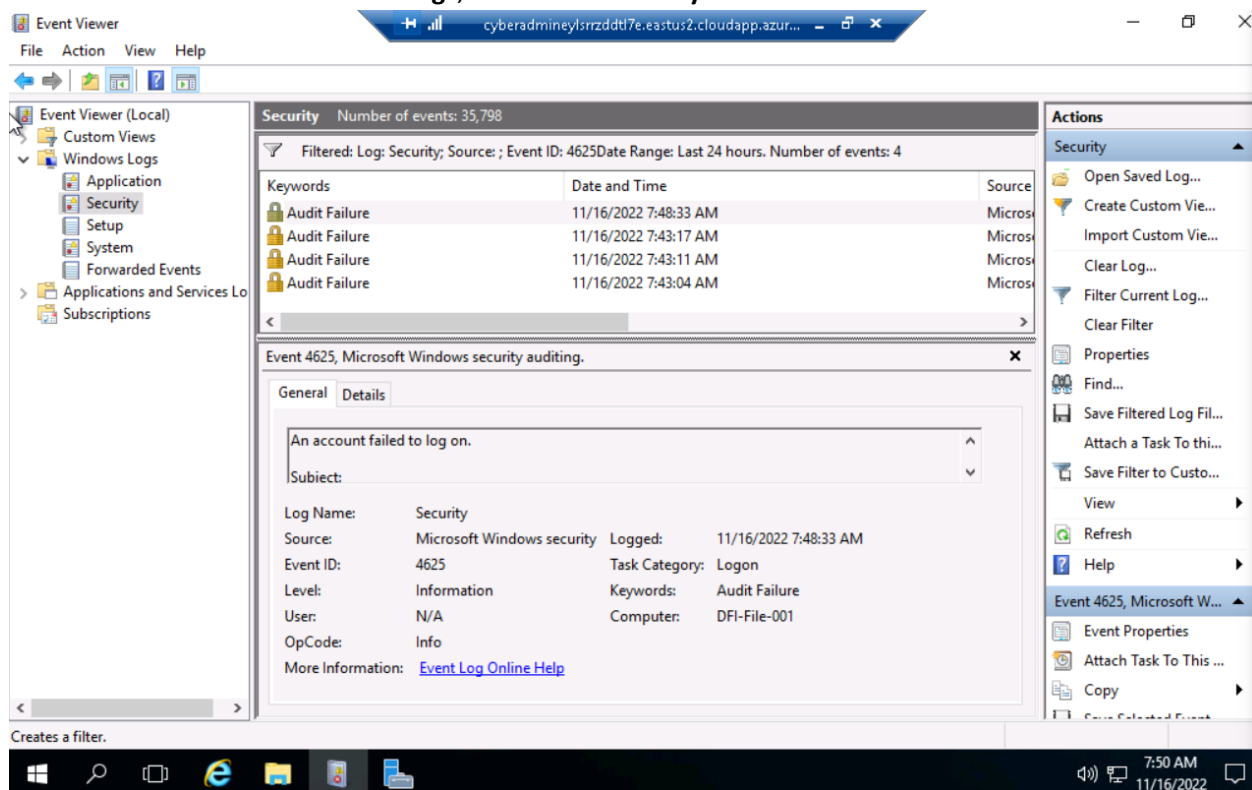
The IT Manager suspects that someone has been attempting to login to DFI-File-001 via RDP.

Prepare a **report** that lists **unsuccessful attempts** in connecting over the **last 24-hours**. Using **PowerShell or Event viewer**, 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.

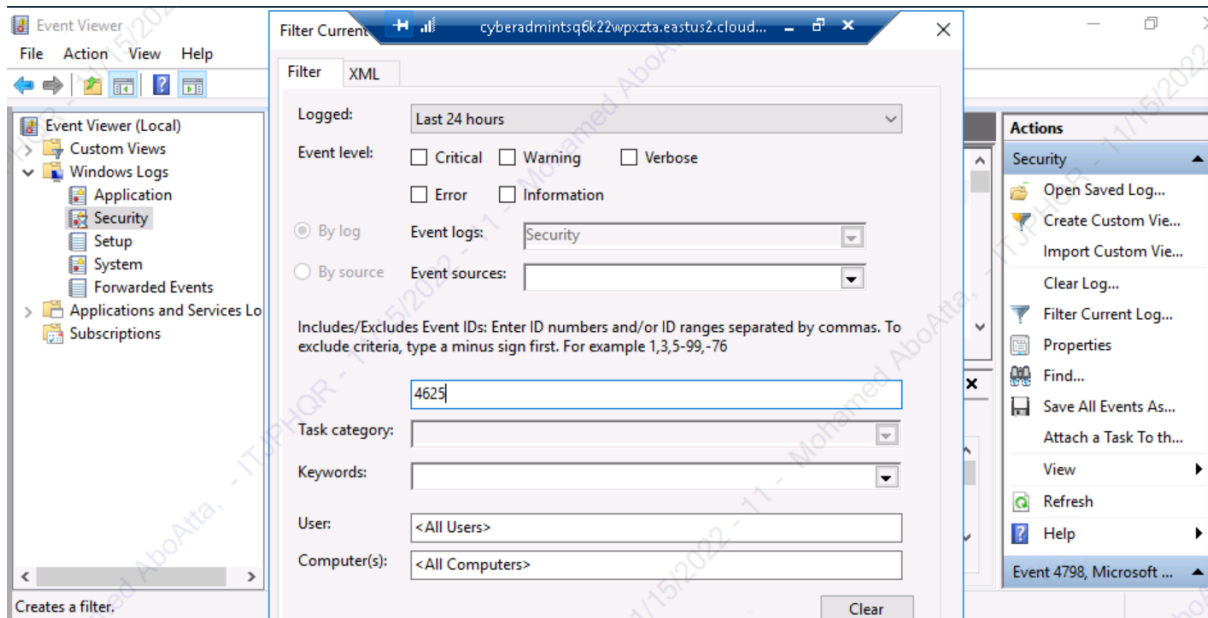
[Place IT Manager Report Here]

- **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**
  - First, we open the **Event Viewer** by searching on it.
  - Under **Windows Logs**, we choose **Security**.

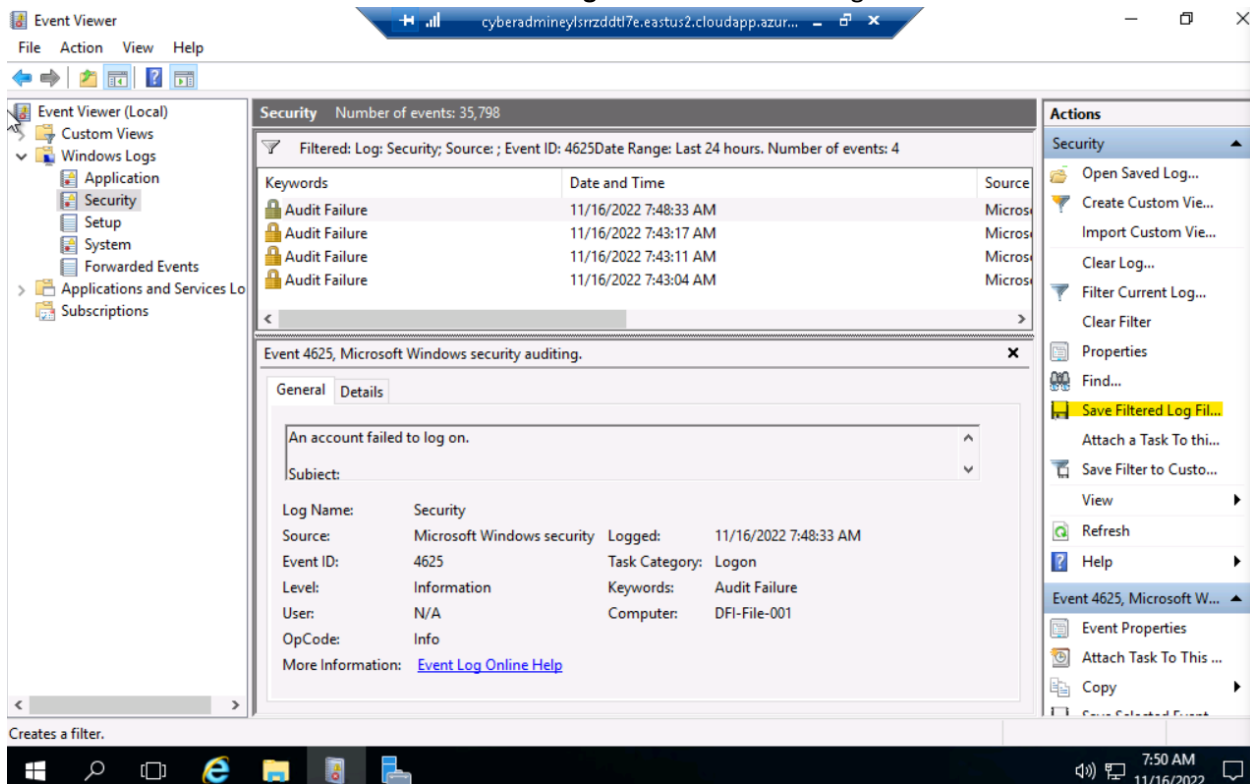


- In the **Actions** side menu, we choose **Filter Current Log**.

- We set the search criteria that we need.



- The events we've searched for will appear.
- We can click on **Save Filtered Log** to save the results logs.



## 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
CVE-2022-41035	Ignore	Max Severity is Moderate
CVE-2022-33636	Ignore	Max Severity is Moderate
CVE-2022-33638	Ignore	Max Severity is Moderate
CVE-2022-35766	Update	Max Severity is Critical
CVE-2022-35794	Update	Max Severity is Critical
CVE-2022-35767	Update	Max Severity is Critical



## 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]

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

- Create the directories listed in the request.

cyberadmin@dfi-app-001:/home/Departments

```
[cyberadmin@dfi-app-001 ~]$ pwd
/home/cyberadmin
[cyberadmin@dfi-app-001 ~]$ cd ..
[cyberadmin@dfi-app-001 home]$ sudo mkdir Departments
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 home]$ cd Departments/
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir IT
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir HR
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Operations
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Public
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting HR IT Operations Public
[cyberadmin@dfi-app-001 Departments]$ |
```

- Create the groups listed in the request.

cyberadmin@dfi-app-001:/home/Departments


```
[cyberadmin@dfi-app-001 Departments]$ clear
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
[cyberadmin@dfi-app-001 Departments]$ cat /etc/group
```

```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:dfi-admin
cdrom:x:11:
```

```
slocate:x:21:
postdrop:x:90:
postfix:x:89:
ntp:x:38:
chrony:x:994:
stapusr:x:156:
stapusr:x:157:
stapdev:x:158:
tcpdump:x:72:
cyberadmin:x:1000:
dfi-admin:x:1001:
JoePublic:x:1002:
IT:x:1003:
HR:x:1004:
Accounting:x:1005:
Operations:x:1006:
[cyberadmin@dfi-app-001 Departments]$ |
```

I

- Create the users listed and place them in the appropriate groups.

 cyberadmin@dfi-app-001:/home/Departments

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

- Set the directory permissions where the groups are the owners of their respective directories.  
Tip: Appropriate groups should be the owners of the respective directories.
- Explain the syntax used for setting the permissions.

- The command for setting the permissions of a directory is:
  - `chgrp [group] [directory]`

cyberadmin@dfi-app-001:/home/Departments

```
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting HR IT Operations Public
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp IT IT
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp HR HR
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp Accounting Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chgrp Operations Operations/
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
drwxr-xr-x. 2 root Accounting 6 Nov 16 20:26 Accounting
drwxr-xr-x. 2 root HR        6 Nov 16 20:26 HR
drwxr-xr-x. 2 root IT        6 Nov 16 20:26 IT
drwxr-xr-x. 2 root Operations 6 Nov 16 20:26 Operations
drwxr-xr-x. 2 root root      6 Nov 16 20:26 Public
[cyberadmin@dfi-app-001 Departments]$ |
```

## 11. Firewall Alert Response:

The IT Manager looked at firewall alerts and was concerned with some traffic she saw, please 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 you should do with IPs from non-trusted source.**

- By analyzing the provided report, I've identified a potential danger which is a brute force attack attempts from the following IP address: 45.35.0.252.
- A mitigation strategy could range from blocking the suspected IP address discovered from the analysis to closing most vulnerable ports target on the network, such as 22.
- This way, the traffic will not go through again, increasing the security of the system.
- Another way could be to employ VPN.

1	Type	Threat/Content Type	Source address	Destination address	Application	Repeat Count	Source Port	Destination Port	IP Protocol	Threat/Content Name	Source Country	Destination Country
274	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	1	47164	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
275	THREAT	vulnerability	45.35.0.252	222.51.64.20	ssh	2	56890	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
276	THREAT	vulnerability	45.35.0.252	222.51.64.14	ssh	1	56284	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
277	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	2	45664	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
278	THREAT	vulnerability	45.35.0.252	222.51.64.39	ssh	2	58528	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
279	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	6	43934	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
280	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	4	43934	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
281	THREAT	vulnerability	45.35.0.252	222.51.65.53	ssh	2	59156	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
282	THREAT	vulnerability	45.35.0.252	222.51.64.39	ssh	2	55216	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
283	THREAT	vulnerability	45.35.0.252	222.51.64.10	ssh	2	45652	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
284	THREAT	vulnerability	45.35.0.252	222.51.65.53	ssh	4	59156	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
285	THREAT	vulnerability	45.35.0.252	222.51.64.14	ssh	2	51380	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
286	THREAT	vulnerability	45.35.0.252	222.51.64.39	ssh	4	53616	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
287	THREAT	vulnerability	45.35.0.252	222.51.65.53	ssh	3	57504	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
288	THREAT	vulnerability	45.35.0.252	222.51.64.10	ssh	3	44004	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
289	THREAT	vulnerability	45.35.0.252	222.51.65.53	ssh	2	55870	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
290	THREAT	vulnerability	45.35.0.252	222.51.64.20	ssh	4	50228	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
291	THREAT	vulnerability	45.35.0.252	222.51.64.10	ssh	5	40714	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
292	THREAT	vulnerability	45.35.0.252	222.51.64.10	ssh	4	40714	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
293	THREAT	vulnerability	45.35.0.252	222.51.64.14	ssh	4	48034	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
294	THREAT	vulnerability	45.35.0.252	222.51.64.20	ssh	4	46926	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
295	THREAT	vulnerability	45.35.0.252	222.51.64.39	ssh	2	48604	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
296	THREAT	vulnerability	45.35.0.252	222.51.64.14	ssh	4	46396	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
297	THREAT	vulnerability	45.35.0.252	222.51.64.20	ssh	6	46926	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
298	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	16	33970	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
299	THREAT	vulnerability	45.35.0.252	222.51.64.14	ssh	4	44674	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States
300	THREAT	vulnerability	45.35.0.252	222.51.64.12	ssh	14	60600	22	tcp	SSH User Authentication Brute Force Attempt(40015)	United States	United States

## **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.

Like 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 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 the tasks performed in the first two weeks.**
- **Explain any recommendations for changes in permissions.**
- **Tie all 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).**

I have performed the following tasks:

- Security Analysis
  - In each system provided, analyzed using Defense in Depth, Principles of least privilege, NIST 800, and Microsoft best practices.
- Firewall Rules
  - Recommended firewall rule for new vendor connections.
- VPN Encryption Recommendation
  - Recommended encryption in transit for new vendor connections.
- IDS Rule
  - Created at least one IDS rule based on the intelligence provided.
- File Hash verification
  - Ensured executables received from vendors are legitimate by comparing file hash with known good copy.
- Automation
  - Recommended areas that could be improved using automation.
- Logging RDP Attempts
  - Created a report detailing successful and unsuccessful connection attempts using PowerShell to view event logs.
- Windows Updates
  - Using NIST 800 and Microsoft Best Practices, recommended which updates should be installed and which could be left off.
- Linux Data Directories
  - Created a data directory on CentOS for internal use and set appropriate permissions.
- Firewall Alert Response
  - Provided mitigation response to firewall alert report. (Sample data provided.)
- I recommend using a VPN product and a Controller-Based Wireless Solution.
- I also recommend setting password expiration period and password strength policies.

### 13. File Encryption:

As your final task, assemble all 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.**