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.

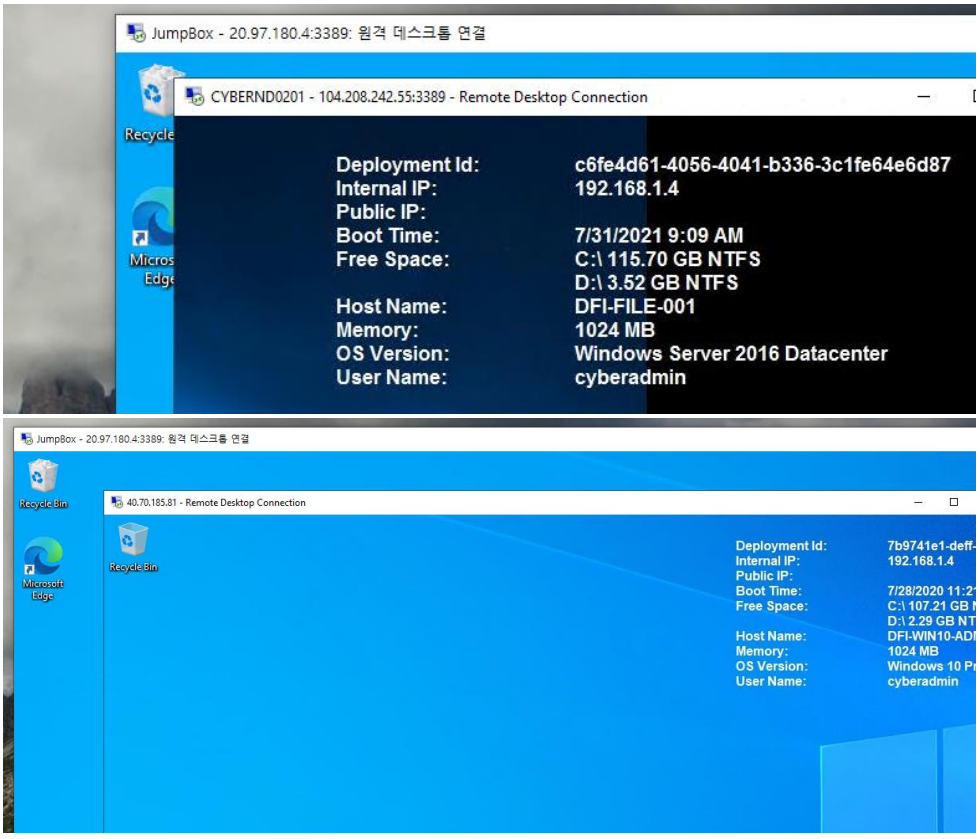
Week One:

1. **Connect:**

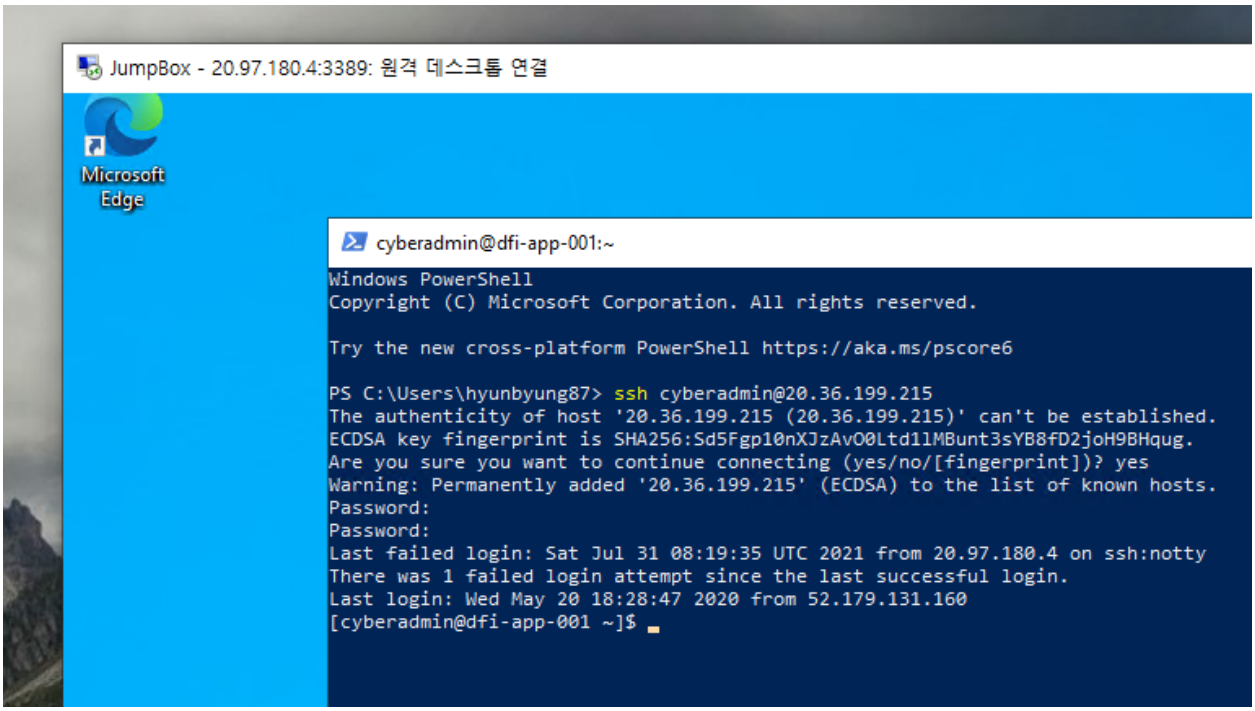
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

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

- **Window 2016 Datacenter and Window**



- Linux



2. **Security Analysis:**

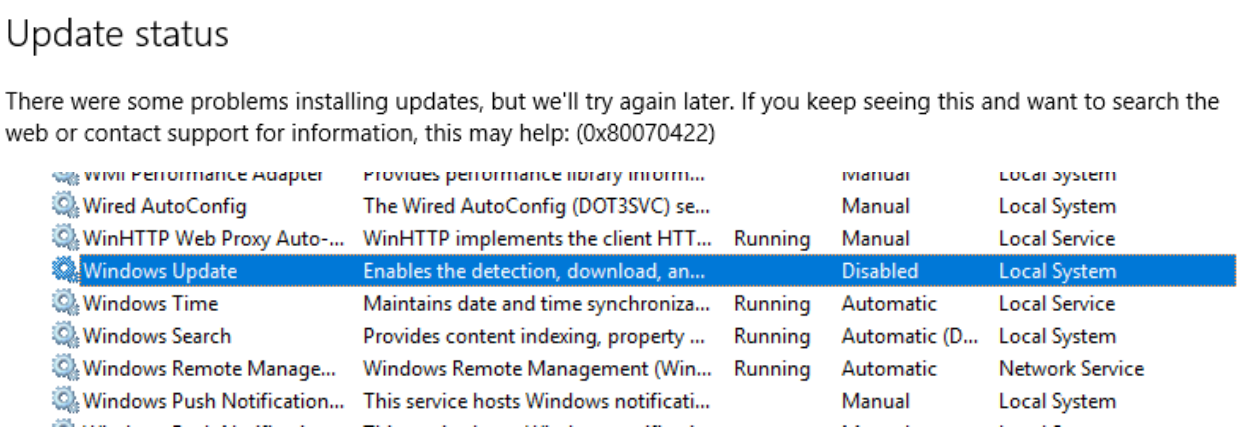
DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

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.

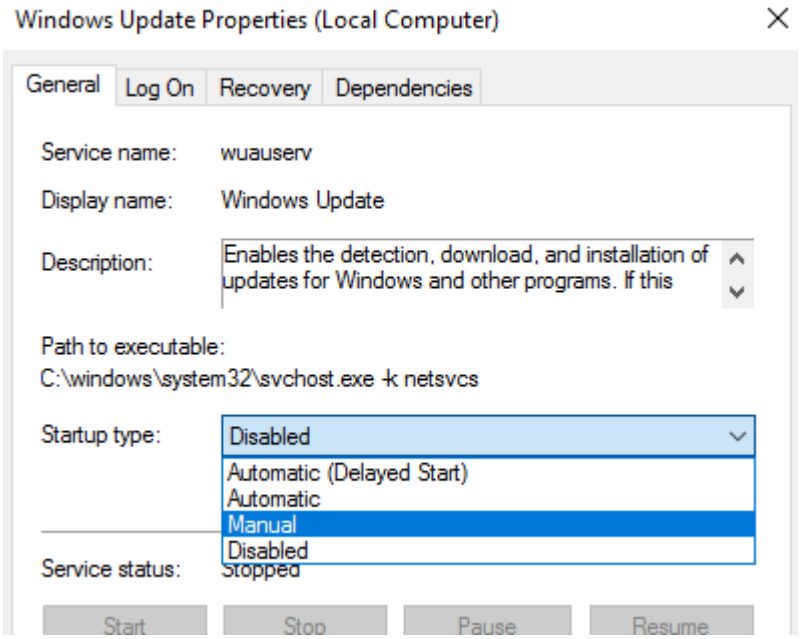
Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions and other settings. Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

[Place your security analysis here]

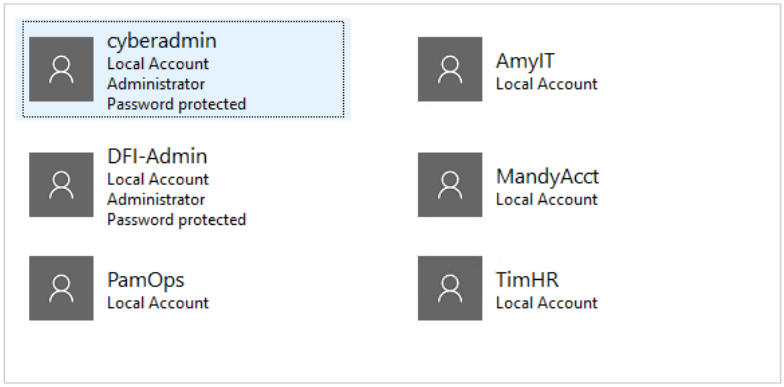
- **[OS update] – NIST 800-123 4.1 Patch and Upgrade Operating System**
  Current OS window system is unable to update the OS because the current window update service is disabled.



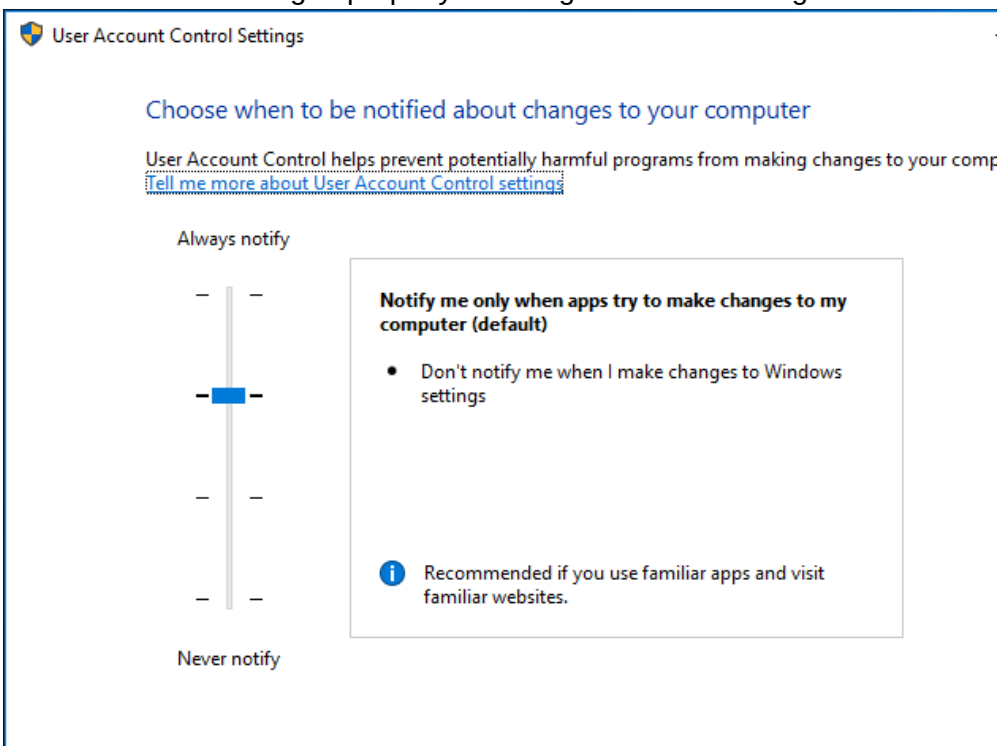
If the windows update is not done then there might be vulnerability for hackers to break through so it's recommended to turn on the windows update service.



- **[User Configuration] – NIST 800-123 4.2 Hardening and Securely Configuring the OS**

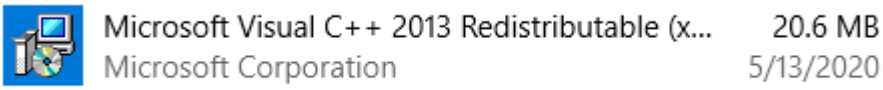


User Account is managed properly following the Least Privilege.



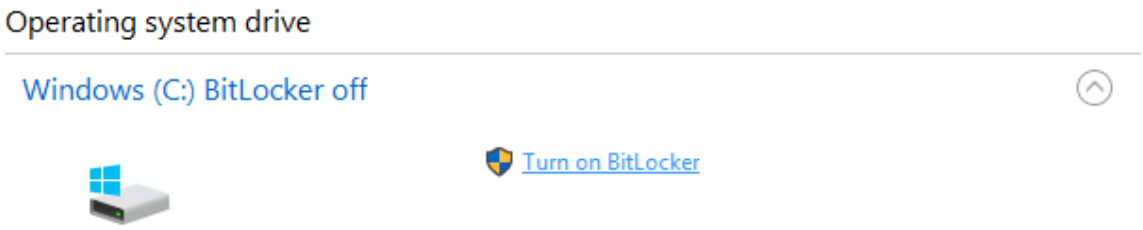
But User Account Control Setting should be set to Always notify. Because this setting doesn't notify anything when administrator change setting. We might make a setting change by mistake and even not notice it. To prevent for potential mistake this notification level should be at the highest level.

- **[Application Install Management] – NIST 800-123 4.2.1 Remove or Disable Unnecessary Services, Applications, and Network Protocols**



Only one program is installed and looks very secure!

- **[Bitlocker] NIST 800-123 5.4 Selecting and Implementing Authentication and Encryption Technologies**

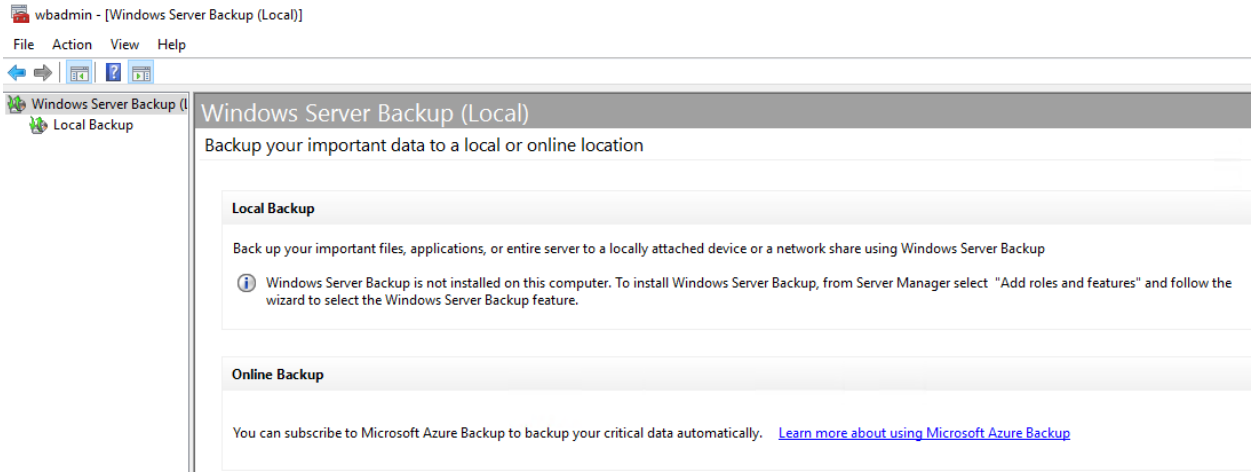


- Bitlocker should be enabled. Or every information in hardware is opened to anyone logged into the computer. Encrypting the hardware will add one more layer to the Security layer and make the computer more secure.

  But recently the Bitlocker was broken down by soldering technique to the TMP. So should be aware of this. Read the following link for more information about this vulnerability.
  https://dolosgroup.io/blog/2021/7/9/from-stolen-laptop-to-inside-the-company-network

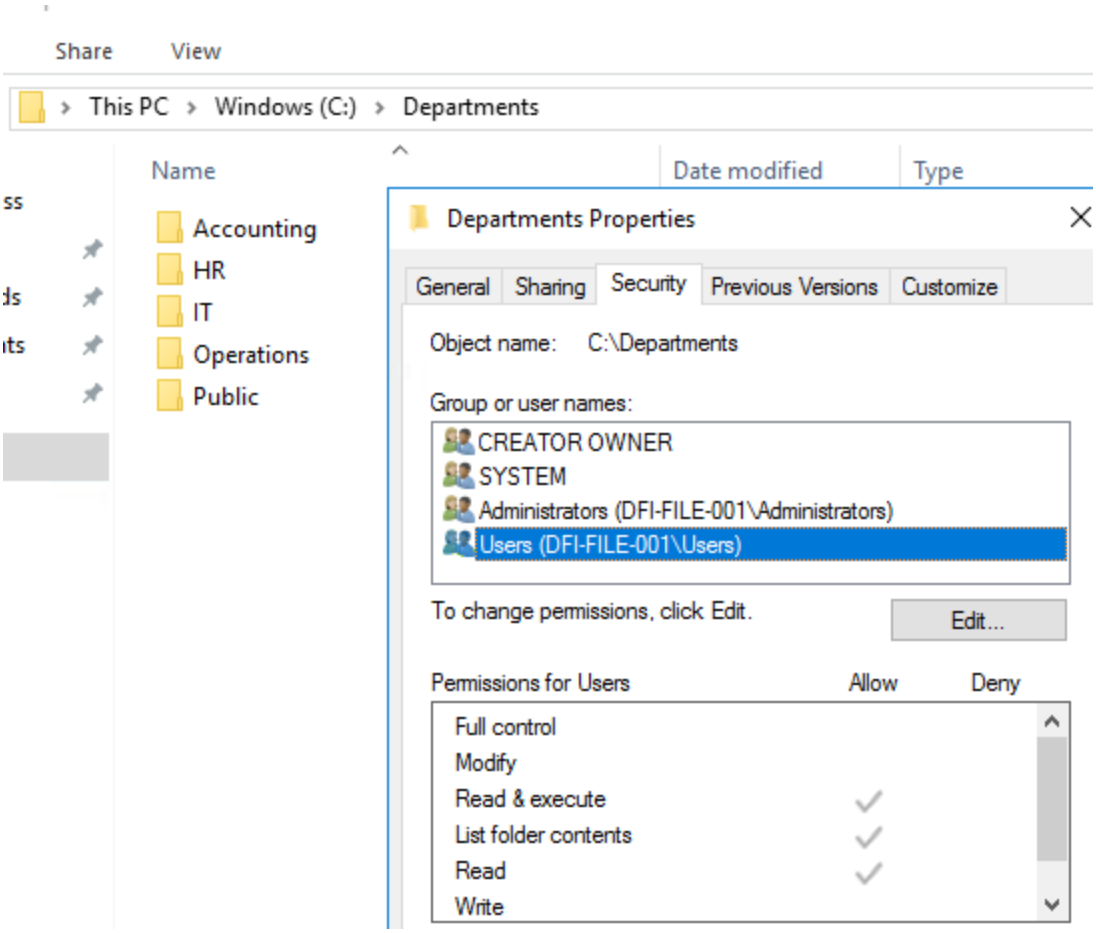
- **[Log] NIST 800-123 6.1 Logging**
  Use SIEM (System Information and Event Management) to collect and manage the logs. If the business scale is very small this might not be needed but when we expect it will Scale then we should consider using SIEM. It will help us manage the logs conveniently even for a large

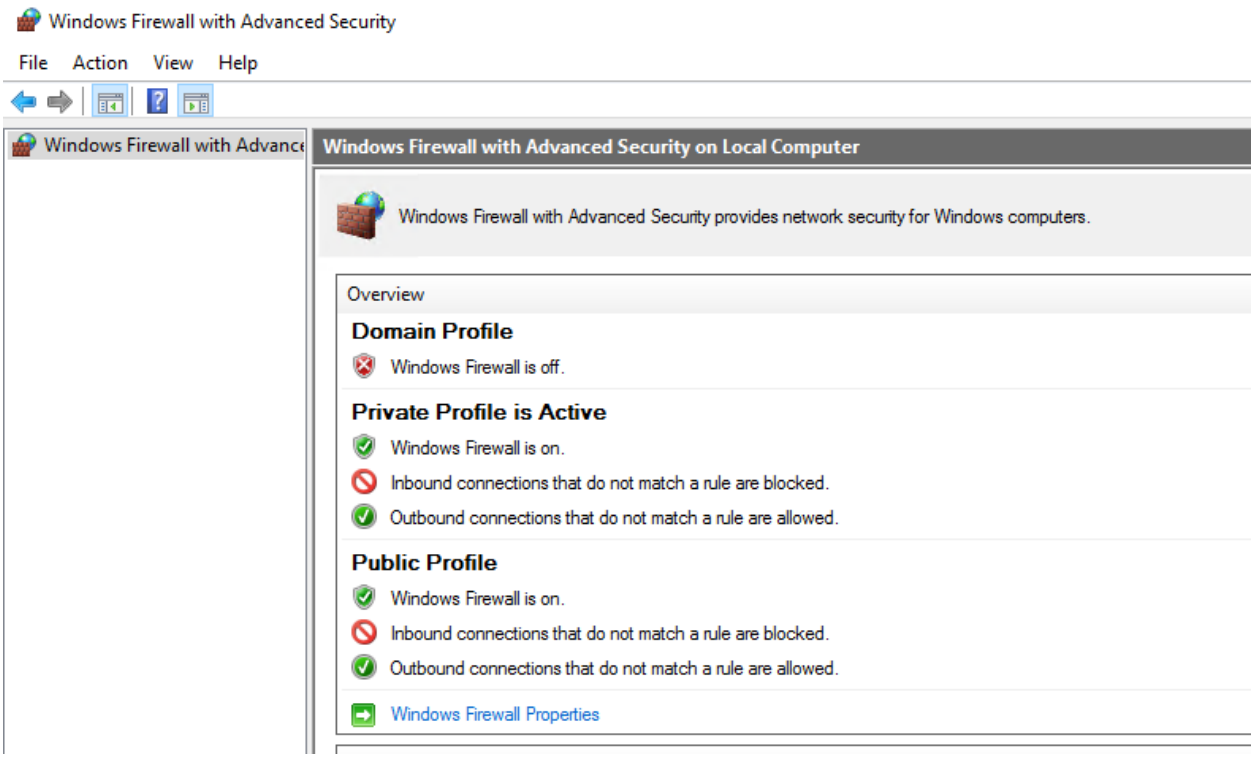
- **[Backup] NIST 800-123 6.2 Server Backup Procedures**
  The data stored to this server should be backup properly preventing from disaster and ransom ware. Windows Server Backup Role should be turned up! Or Online Backup.



- **[Firewall] Depth in Depth – Network Security**
  Domain Profile Firewall is off. It should be enabled. Different from private and public its inside network traffic but it should be blocked properly because hacker could break other part of inside network traffic and penetrate to the current server.

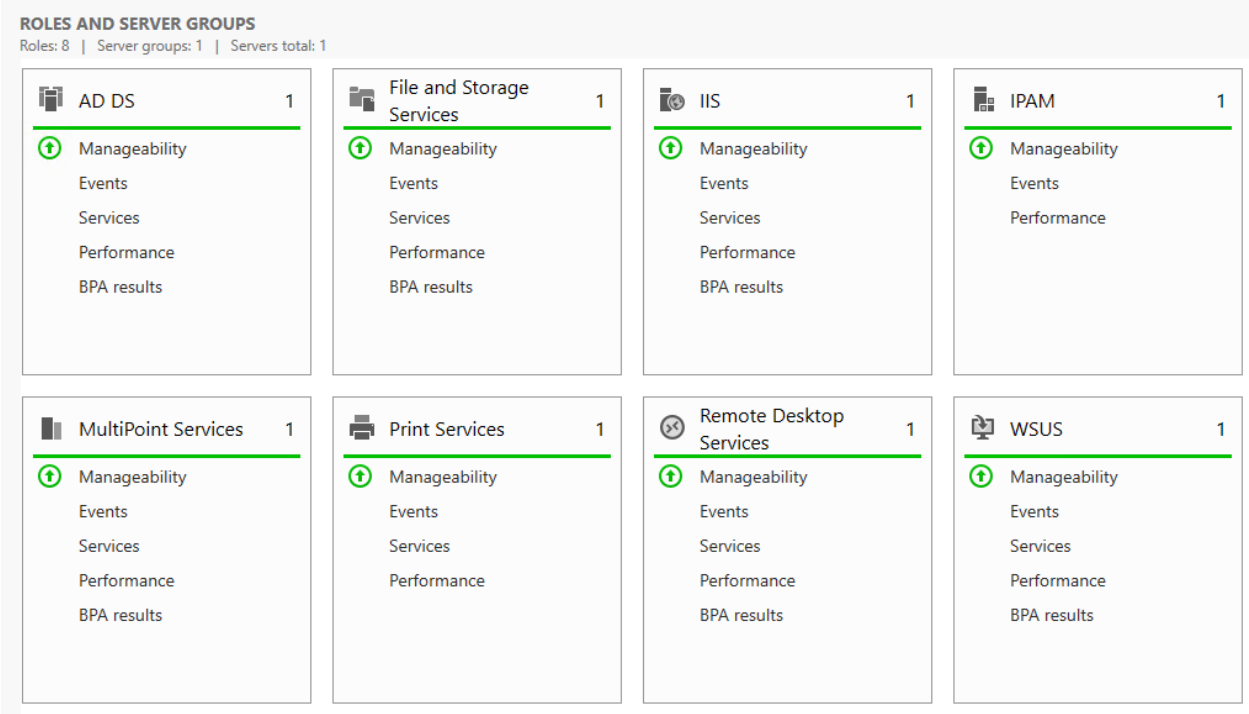
- **[File Permission] Least Privilege**
  There are 4 important folder at C:/Departments. Accounting, HR, IT, Operations. This folder could only be accessed by the stake-holder who is related to. So Users should be removed from the permission and only Administrator and the related Account should have permission to access to the folder. Or otherwise important information could be exposed to the other departments.


Share
View
This PC
Windows (C:)
Departments
Name
Date modified
Type
Accounting
HR
IT
Operations
Public
Departments Properties
General
Sharing
Security
Previous Versions
Customize
Object name: C:\Departments
Group or user names:
CREATOR OWNER
SYSTEM
Administrators (DFI-FILE-001\Administrators)
Users (DFI-FILE-001\Users)
To change permissions, click Edit.
Edit...
Permissions for Users
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write


Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advanc
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is off.
Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties

- **[Unnecessary Roles]**

Currently there are 8 Server Roles

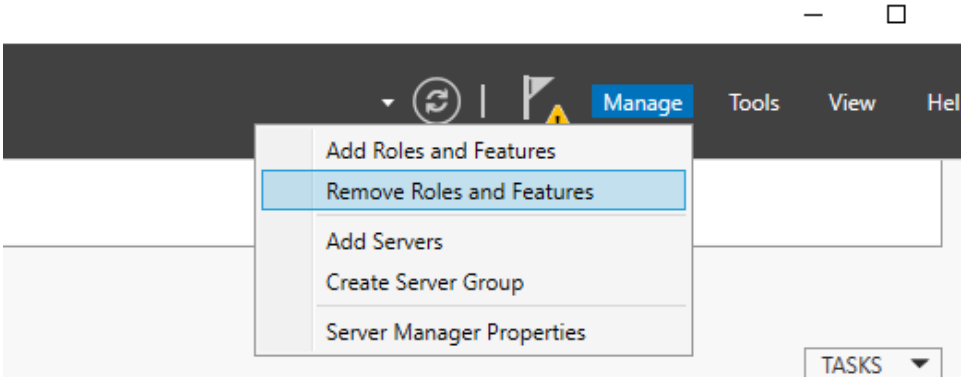


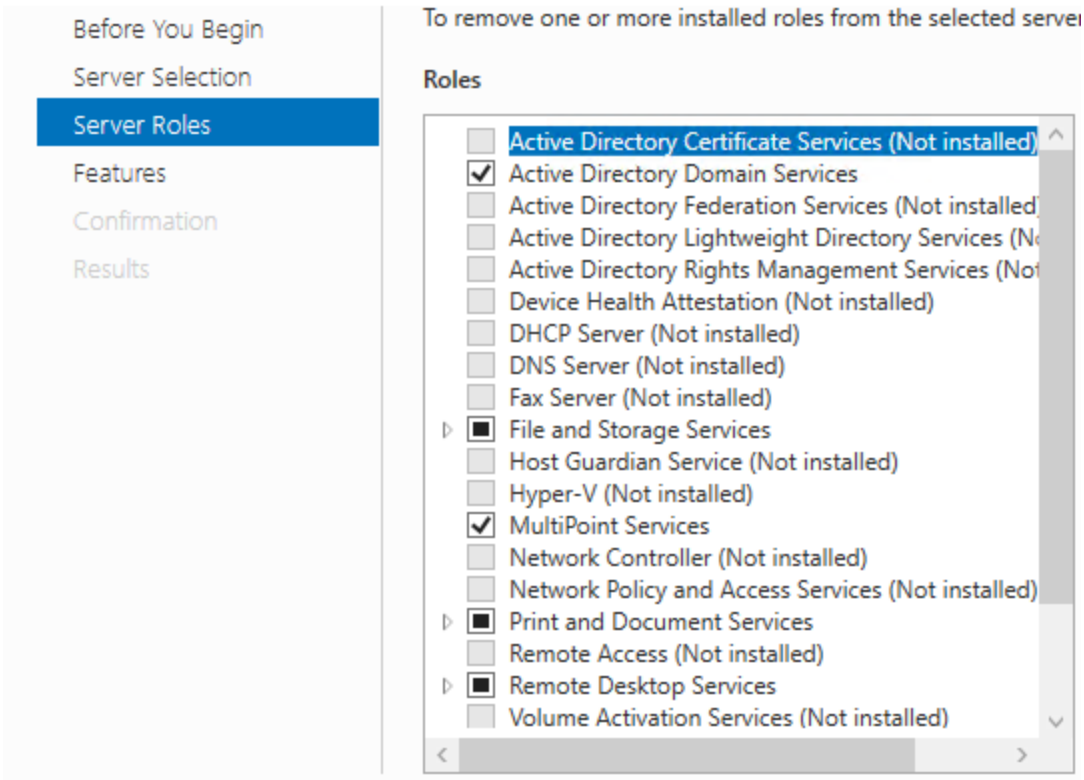
The DFI-File-001 server is purposed for file and application.

We need to remove unnecessary role from the server that doesn't match the purpose.

- **AD DS (Active Directory Domain Services)** – this is for Directory as a Service being a major role at the organization network. But this is not needed for file server purpose. This server is not for managing the directories spread around the organization
- **IIS (Internet Information Services)** – This is for Web Server and no needed.
- **IPAM (IP Address Management)** – This server is not for IP Address management among the servers inside the organization
- **MultiPoint Services** – This role is for multiuser shared windows. No need.
- **Print Services** – No match for purpose

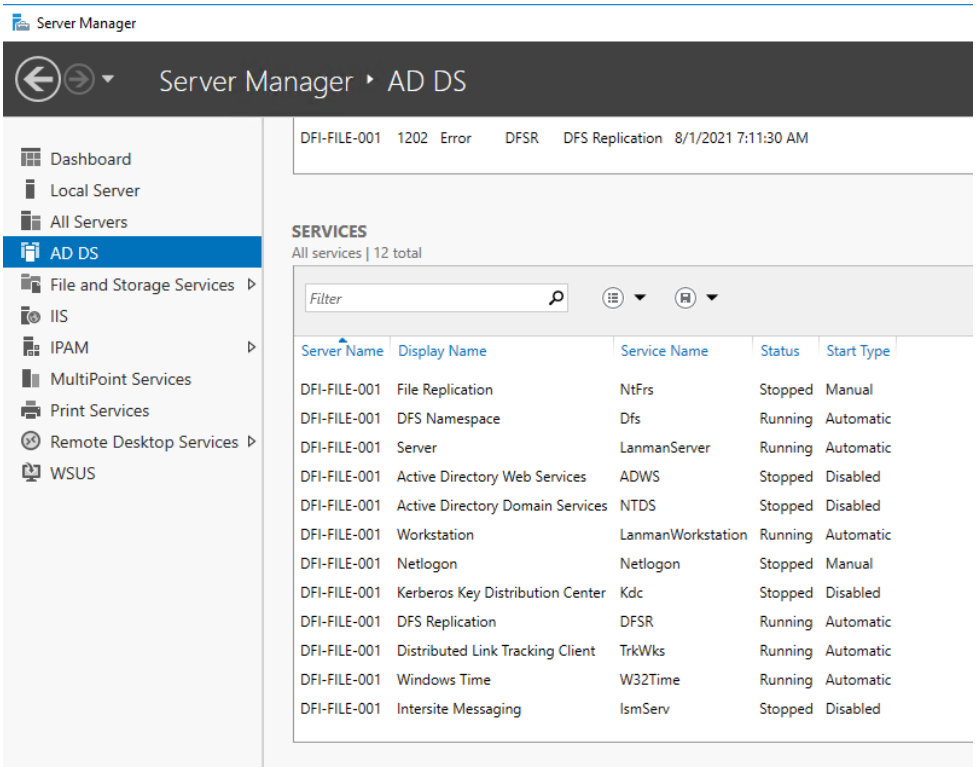
This follows **NIST 800-123 4.2.1 Remove or Disable Unnecessary Services, Applications, and Network Protocols.** Roles could be removed by following





- **[Unnecessary Services]**

For each role there are services allocated. We could simply disable the services that belongs to the roles we need to remove



For example, for AD DS

- File Replication
- DFS Namespace

For IIS

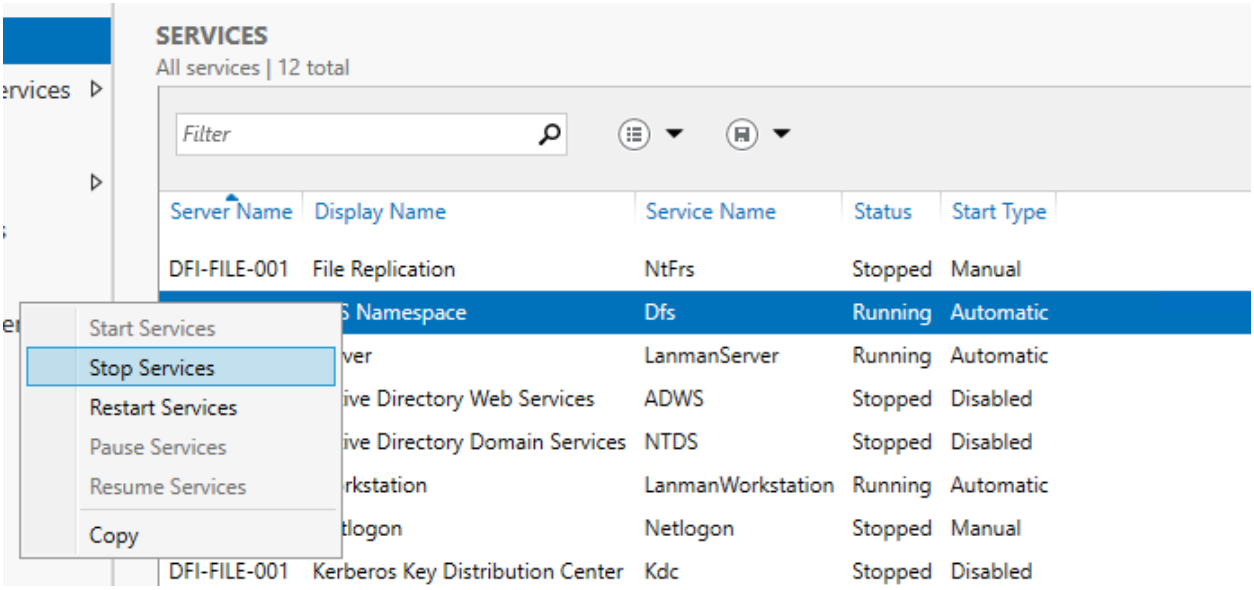
- Application Host Helper Service
- IIS Admin Service

For Print Services,

- Spooler

And more! This follows **NIST 800-123 4.2.1 Remove or Disable Unnecessary Services, Applications, and Network Protocols.** We should only leave services that exactly matches our purpose to make the vulnerabilities as small as possible.

We could easily stop the services by **right click the service name – Stop services**



3. **Firewall Rules:**

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

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

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

[Place your firewall rules and explanation here]
name 21.19.241.63 WBC
name 172.21.30.44 DFI-File-001
access-list DFI-Ingress extended permit tcp host WBC host DFI-File-001 eq 9082

The Cisco syntax is consisted with the following

- **The rule that controls traffic**– access-list
- **The name of our internal interface** – DFI-Ingress
- **Flexibility in matching traffic and the ability to match based on protocol, source and destination address** – extended permit
- **Network protocol** - TCP
- **The source IP** – 21.19.241.63 named with WBC
- **The destination IP** – 172.21.30.44 named with DFI-File-001
- **The port or service being used** – 9082

Access list is a like a book used for identification only for those invited to the party. So, we must add WBC to the access list to let them access to our DFI-File-001 server.

And this access list is named as DFI-Ingress. So, the same server could have several access lists same as we could have different books for each party held in same place.

When the people came to the party, we could ask the person only the name. Or we could check did he get some enough money because the party's purpose is for donation. So which items to check? That is about permit.

Normally, standard permit only checks for source IP.
But extended permit checks source IP, destination IP, protocol, and port number.
This is stricter than standard and more secure. Because the server could let in only for the request that has the correct purpose.

So, we chose extended permit, and provide source, destination, protocol, port number for the checklist!

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]
Cisco supports asymmetric and symmetric encryption. I recommend asymmetric encryption at connection phase because this could help to be able to make connection between 2 points without having keys from each.

After making connection by asymmetric encryption exchange the key for symmetric encryption. And after exchanging the 2 points could make connection by symmetric encryption.

Asymmetric encryption recommended – RSA-2048
Symmetric encryption recommended – AES-CBC mode / RC4

These encryptions status are Acceptable which means this algorithms provide adequate security for data transit in the Cisco standard.

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 any (msg:“ICMP Connection Attempt”; sid:1000001; classtype: attempted-dos;)

From the beginning to the end it means the following

- **alert** – Alert generated
- **tcp** – the network protocol used for connection
- **any** – Source IP Address
- **any** – Source Port
- **172.21.30.44** – Destination IP
- **any** – Destination Port

When all the above condition is met then we are going to do the following.

- **msg** : this option tells the logging and alert engine the message to print along with a packet dump or to an alert. And we are sending the message that the connection attempt has occurred
- **sid** : this tells this specific rule ID is 1000001. Below 1000000 are all reserved so we cannot use.
- **classtype** : this keyword is to use to categorize a rule as detecting an attack that is part of more general type of attack class. We are assuming this is DDoS attack so set as attempt of Dos attack.

ICMP stands for **Internet Control Message Protocol** and use **TCP protocol.**
And there is no specific port number for ICMP so the Destination Port is set to any.

[Place your VoIP Admin rule and explanation here]
alert udp any any -> 172.21.30.55 69 (msg:“TFTP Connection Attempt”; sid:1000002;)

From the beginning to the end, it means the following

- **alert** – Alert generated
- **udp** – the network protocol used for connection
- **any** – Source IP Address
- **any** – Source Port
- **172.21.30.44** – Destination IP
- **69** – Destination Port

When all the above condition is met then we are going to do the following.

- **msg** : same with above explanation.
- **sid** : ID 1000001 is already used above so we choose the next one 1000002

TFTP stands for **Trivial File Transfer Protocol** and use **UDP protocol.**
69 is the specific port number for TFTP so the Destination Port is set to 69.

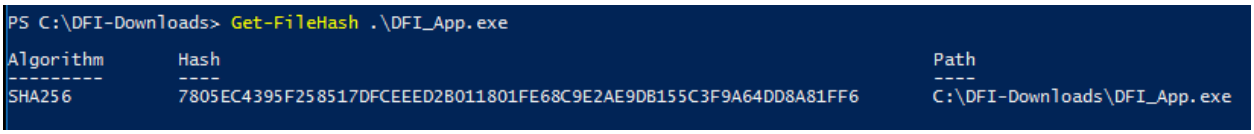
6. **File Hash verification:**

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
Firewall Optimization	Use Stack Storm Automation Tool	Stack Storm analysis the package and find anomaly automatically and block the IP sending them. This is Automated Threat Intelligence and will alleviate potential threats without security analysis involved. Less traffic from hackers means a more pleasant use environment for ordinary users.
Log and Event Management	Use Autointelli	This tool is for Auto Remediation. When specific logs or event happens, we have to response with specific solution. This could be repeatable and when we automate this process the efficiency of managing log and event will be boosted. For example, removing logs and events when it has been piled up enough would be a mundane task. Also, for specific situation like when A event occur notify the B stakeholder is somewhat be able to automate. All kind of process related to log and events could be automated and not just for security analyst, everyone

		within the company can benefit from solving the problem without having to wait for a response from the security team if there is a problem that is recorded to logs and events.
Backup Server	Use OneDrive from Microsoft	Backup is very essential to prevent loss of important assets inside server. This could prevent loss by disaster, or ransomware by hacker. But manual backup is mundane task. Using automatic backup will assure the company assets will be safe and integrity all the time even no one is caring about by mistake and gain more trust from client.

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.

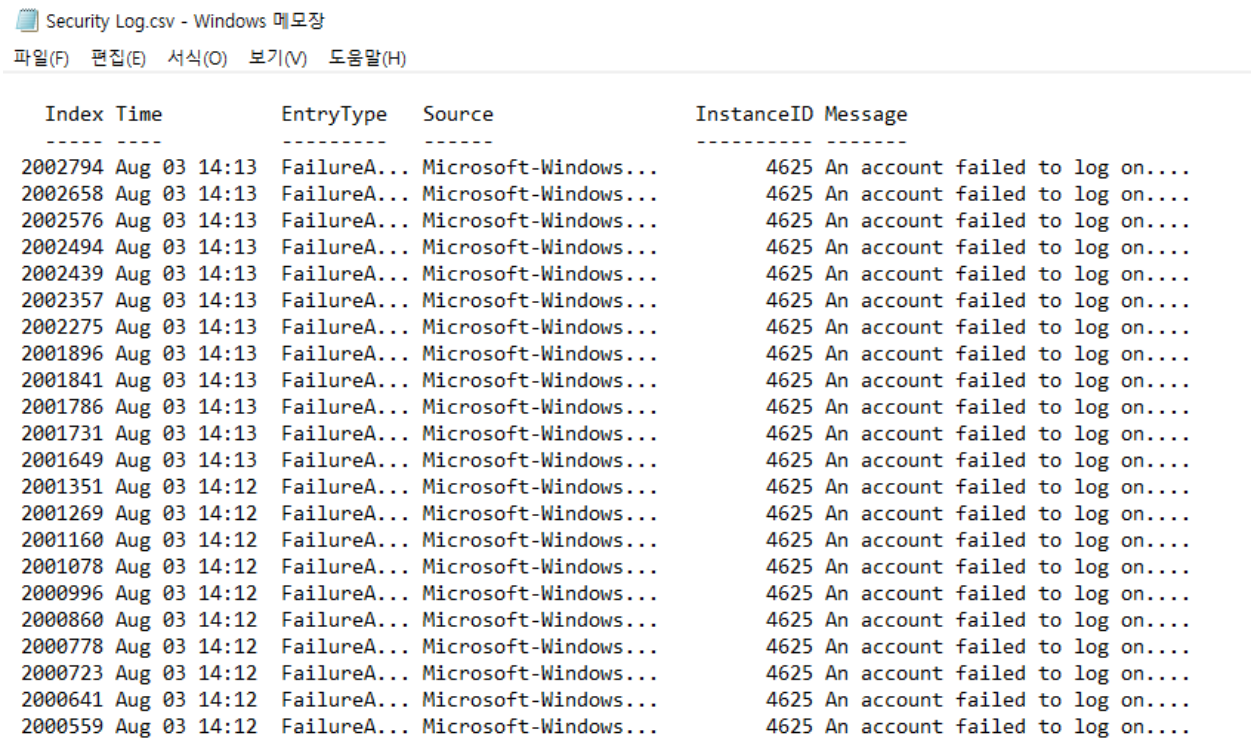
For your deliverable, open the CSV with notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below explain your findings, recommendations, and justifications to the IT Manager.

[Place IT Manager Report Here]

```
PS C:\Users\cyberadmin> Get-EventLog -LogName Security -InstanceId 4625

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
 2002794 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002658 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002576 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002494 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002439 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002357 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2002275 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001896 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001841 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001786 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001731 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001649 Aug 03 14:13  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001351 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001269 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001160 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2001078 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000996 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000860 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000778 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000723 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000641 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 2000559 Aug 03 14:12  FailureA... Microsoft-Windows...         4625 An account failed to log on....

PS C:\Users\cyberadmin> Get-EventLog -LogName Security -InstanceId 4625 > "Security Log.csv"
```



Window Security event ID 4625 is about **Failed Account Log On.**
There is someone who is trying to log in to the **DFI-File-001** server!

These are recommendations.

- **Set Password Policies**
  [Local Security Policy – Account Policies – Password Policy]
  - Account lockout duration – ex) 15 minutes

    - Account lockout threshold – ex) 5 invalid logon attempts
- **Set automatic IP block**
    - When the log on attempt is ongoing block the IP by firewall.
    - If it was real employee by mistake then security team could unblock it manually
- **Set Alert to email that is often checked**
    - When the message of failed logon is sent to email, we could easily check it by real time and response.

The above recommendation could prevent the hacker's brute force attack. 5 attempts will lead to 15 minutes of account lock on and if that attempt repeated after the unlocked the IP will be blocked. I didn't put account lock so the hacker could change the IP and repeat the attack again but it won't be easy to break in with limited number of attempts. And email will be ringing continuously so the security team and the account owner could response immediately. So the hacker's attack will be shut down in fast time period.

So why just IP block and not an account lock? In case of argent business problem account lock could cause very unpleasant situation so didn't recommend for the first place.

There might be a few employees who could feel uncomfortable with the limited password entry but this will make the server more secure and save the assets inside.

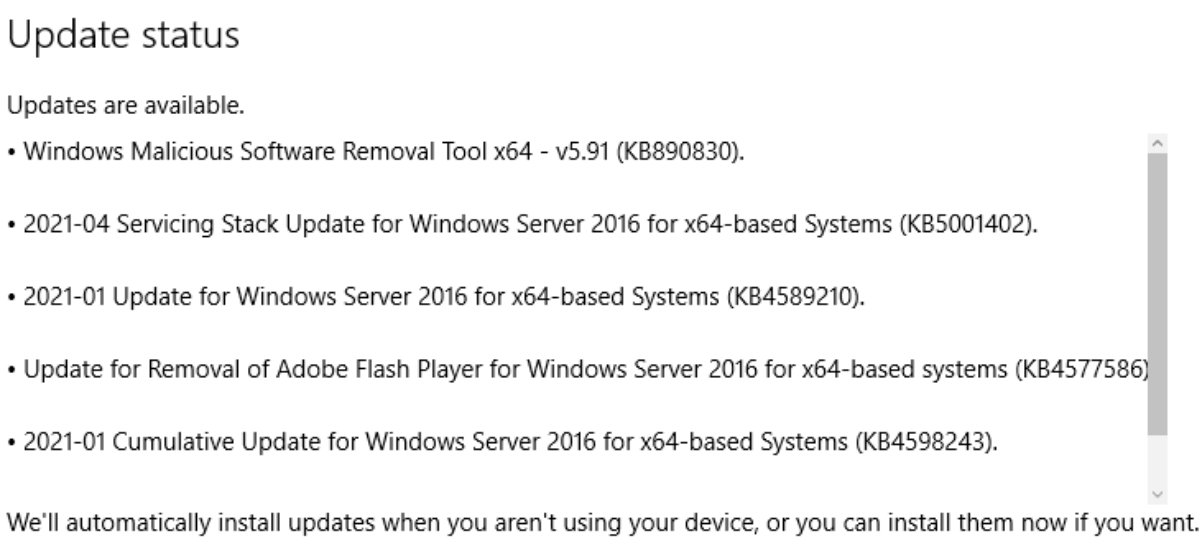
9. **Windows Updates:**

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.

According to NIST 800-40r3 Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems. Installation could have side effects, so organizations should be capable of detecting side effects, such as changes to security configuration settings, caused by patch installation.

DFI is concerned with stability and security so we should be careful choosing what to install and what to not. Updates could break down the system so if it is not fixing serious security problems we could ignore.



Updates could be checked by **Windows Update**.

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

Available Updates	Update/Ignore	Justification
KB890830	**Update**	This is update for Windows Malicious Software Removal Tool that helps remove malicious software from computers. This is essential because as malware evolve time by time the defender should be evolved also to catch up. So, need to be updated.
KB5001402	Ignore	This update makes quality improvements to the serving stack, which is the component that installs Windows updates. This could be beneficial but not security problem. Ignored.
KB4589210	Ignore	This is microcode update but not because of security problem. If this was Spectre(Hardware Vulnerabilities affecting microprocessor) fixing update this should be updated but this is just normal update so ignored.
KB4577586	Ignore	This update is for removal of Adobe Flash Player and not very important! Also, the server doesn't have any Adobe Flash Player so could be ignored.
KB4598243	**Update**	**This is security update!** There are multiple vulnerabilities that could affect the remote Windows host. For example

		- Windows AppX Deployment Extensions Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-1685. (CVE-2021-1642) - Windows DNS Query Information Disclosure Vulnerability (CVE-2021-1637) - Windows Update Stack Elevation of Privilege Vulnerability (CVE-2021-1694) And much more! More than 70 kinds of vulnerabilities are existing in all kind of service inside Windows so this update is very important
KB4535680	**Update**	**This is security update!** It is giving improvements to Secure Boost DBX. There was a vulnerability where the attacker could bypass secure boot and load untrusted software. This could lead to server full of malware and should be updated immediately!

10. **Linux Data Directories:**

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

- The root directory should be 'Home'
- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.
- Set owner permissions for the groups IT, HR, Operations and Accounting
- Create the users AmyIT, PamOps, MandyAcct and TimHR in the appropriate groups so that they can read/write/execute in their respective departmental folders.

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

[Provide a screenshot(s) of completed tasks and the correctly set permissions here]

```
[cyberadmin@dfi-app-001 home]$ pwd
/home
[cyberadmin@dfi-app-001 home]$ ls
AmyIT  cyberadmin  Departments  dfi-admin  JoePublic  MandyAcct  PamOps  TimHR
```

```
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting  HR  IT  Operations
```

- Created Subdirectories
- **Home (ROOT)**

- Departments
  - IT
  - HR
  - Operations
  - Accounting

```
[cyberadmin@dfi-app-001 Departments]$ ls -al
total 0
drwxr-xr-x. 6 root root       62 Aug  4 05:44 .
drwxr-xr-x. 6 root root       77 Aug  4 05:43 ..
drwxrwx---. 2 root Accounting  6 Aug  4 05:44 Accounting
drwxrwx---. 2 root HR          6 Aug  4 05:44 HR
drwxrwx---. 2 root IT          6 Aug  4 05:44 IT
drwxrwx---. 2 root Operations  6 Aug  4 05:44 Operations
```

- Each folder IT, HR, Operations and Accounting has its appropriate groups
- **Only registered user or groups could read / write / execute**
- Other user has no permissions for each folder

```
IT:x:1003:AmyIT
HR:x:1004:TimHR
Operations:x:1005:PamOps
Accounting:x:1006:MandyAcct
```

- **Each group includes each appropriate user**

[Provide your non-technical syntax explanation for management here]
I made folders for IT, HR, Accounting and Operations and add users and groups. And set the permission for each folder and put the user to the right group.

Commands used and syntax explanation

- **Go to root directory**
  - cd ..
- **Make Subdirectory**
  - sudo mkdir Departments
  - sudo mkdir IT HR Operations Accounting
- **Add groups**
  - sudo groupadd IT
  - sudo groupadd HR
  - sudo groupadd Operations
  - sudo groupadd Accounting
- **Set each folder's owner to the related group**
  chgrp [group] [folder]
  - sudo chgrp IT IT

    - sudo chgrp HR HR
    - sudo chgrp Operations Operations
    - sudo chgrp Accounting Accounting
- **Change the permission of each folder**
    - sudo chmod 770 IT
    - sudo chmod 770 HR
    - sudo chmod 770 Operations
    - sudo chmod 770 Accounting
- **Add users**
    - sudo adduser AmyIT
    - sudo adduser PamOps
    - sudo adduser MandyAcct
    - sudo adduser TimHR
- **Set users to related groups**
    - sudo usermod -G IT AmyIT
    - sudo usermod -G HR TimHR
    - sudo usermod -G Operations PamOps
    - sudo usermod -G Accounting MandyAcct

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]

Source Po	Destination Por	IP Protoc	Threat/Content Name
43606	22	tcp	SSH User Authentication Brute Force Attempt(40015)
43606	22	tcp	SSH User Authentication Brute Force Attempt(40015)
52430	22	tcp	SSH User Authentication Brute Force Attempt(40015)
52430	22	tcp	SSH User Authentication Brute Force Attempt(40015)
33408	22	tcp	SSH User Authentication Brute Force Attempt(40015)
33408	22	tcp	SSH User Authentication Brute Force Attempt(40015)
42898	22	tcp	SSH User Authentication Brute Force Attempt(40015)
42898	22	tcp	SSH User Authentication Brute Force Attempt(40015)
55038	22	tcp	SSH User Authentication Brute Force Attempt(40015)
36082	22	tcp	SSH User Authentication Brute Force Attempt(40015)
35904	22	tcp	SSH User Authentication Brute Force Attempt(40015)
56490	22	tcp	SSH User Authentication Brute Force Attempt(40015)
47102	22	tcp	SSH User Authentication Brute Force Attempt(40015)
47102	22	tcp	SSH User Authentication Brute Force Attempt(40015)
40542	22	tcp	SSH User Authentication Brute Force Attempt(40015)
45868	22	tcp	SSH User Authentication Brute Force Attempt(40015)
56736	22	tcp	SSH User Authentication Brute Force Attempt(40015)
51486	22	tcp	SSH User Authentication Brute Force Attempt(40015)
37716	22	tcp	SSH User Authentication Brute Force Attempt(40015)

The attacks are all about SSH User Authentication Brute Force Attempt.

The mitigation strategy for brute force is the following.

1. **In case to block the brute force attack**
   - **A. Lock the account after a fixed number of failed attempts**
     Brute force attack is just putting random password so when there is limited number of password entry it will be hard to maintain the brute force attack. This is very efficient to block most brute force attack because they require lots of chances to enter password to actually get the password.
   - **B. Delaying the response time**
     Most brute force requires huge number of attempts to actually get the password. But when delay happens for each password entry then the total amount of possible attempt reduces and it will be very hard to get the password.
   - **C. IP address lock-out**
     This could help distinguishing the black IPs but as seen at the firewall report the attacker is changing the IP repeatedly so IP blocking could be recommended but might not be efficient.
   - **D. Two factor authentication**
     Adding at least one more authentication process will reduce huge amount of brute force attack. Another authentication factor might be OTP(One-time password) or fingerprint, smartphone verification code etc. Even brute force attack successfully acquires the password there is no way to easily go through the 2nd authentication process

E. **Use Captcha**
   Most brute force attack is by bot. So, when we add Captcha for each password attempt it will be very hard to execute brute force further.

2. **In case if the hacker has successfully achieved the password**
   A. **Location (IP) monitoring**
      If hacker already acquired the password, then he/she is already working under surface. Monitoring unusual login patterns could help to detect the takeover account.

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]

For 2 weeks of work, the task what worked on could be summarized in 2 parts

- Blocking outside attack
- Securing inside computers

What I've first done is to connect to the computers remotely to start the analysis of computers. The very first step is to understand the security status of the computers.

I've looked from account permissions, folders, security configuration like firewall, vaccine etc. While I was looking for security problems, I followed NIST 800-123 which is a standard guide of security field. I've checked what the guide tells me to check very meticulously. And I didn't only used one guide, I've used several guides while checking the computer security status. For example, Defense-in-Depth. Which is about layering security barriers.

After the check I've found several problems.

There was a lot of attack by outside hackers. IT Manager told me her concern and I've found she was right by checking the logs inside computer. But there was no proactive movement to

defend this. This company were getting attacked but there were no people who were defending it.

I wrote down what to do to defend this outsider attack in the report. For example, firewall optimizing to block suspicious attackers, adding IDS rules which gives message when someone attacks etc. To defend the attacks even much better I recommend using VPN. It stands for Virtual Private Network. It will boost the company protection from outsiders!

But there is no perfect protection. Some hackers could break into the system no matter what and we should always be preparing for the moment. That's why we have vaccines like Window Defender.

I've found some problems inside the computer too. The window was outdated, and unnecessary programs were running inside server. We should always keep the computer simple as possible. The more program it runs not only the performance goes low, but there is more door for hackers to come in.

Encrypting all the hardware inside server is one good idea. It causes no problem for the employees but makes hacker hard to look into the important assets company has.

I've talked about in the hacker's perspective but security problem doesn't always happen by hacker. It could be caused by curious staff. The folders and files inside computer could be accessed by any user. But this should not happen. If anyone could look inside the HR team files and know everyone's annual salary amount image how will it go.

That is why all files and folders inside company could be only accessed by the people who needs to. This will prevent further mistake by naïve employee. **We call it the Least Privilege**. The permission of access to files and folders should be set properly and I've worked on Linux server the company has.

Besides, I've checked the custom application sent to the company from the software vendor and I've checked that the software is OK.

And there is another idea to protect the company even much better. Automation is what I strongly recommend. When we have security problems there is a solution. But mostly the solution is done by manpower. What if we can do it automatically even when security team is all in sleep? This will help security team to work less on mundane task and focus on the most important security problems.

My recommended product is Stack Strom. It is used by big names including fortune 500 companies. Alternative could be Autointelli! Not famous but has strong product at this field! It might be a cliché but they are using AI for automated security!

Even the company follows all the security recommendation I've wrote down the employee should be aware of security problems. Because unintended employee mistakes could cause security problem. Most of the security strategy is for hackers not employee. Educating the employee about security must have security policy for the company.

Multi-Factor Authentication is very important for secured log in. This is adding one more step to log in rather than just password. As the company is suffering from attack from outside hacker

this will help to make log in way much harder for hacker. Adding Multi-Factor Authentication to the User Account Policy is recommended.

Thanks for reading the report. Overall the company security was maintained well and with few more steps which I wrote in the report in details the security level will be improved significantly.

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.