

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.

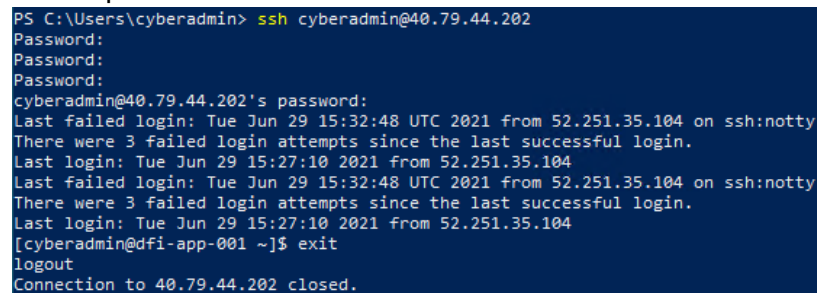
Week One:

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.

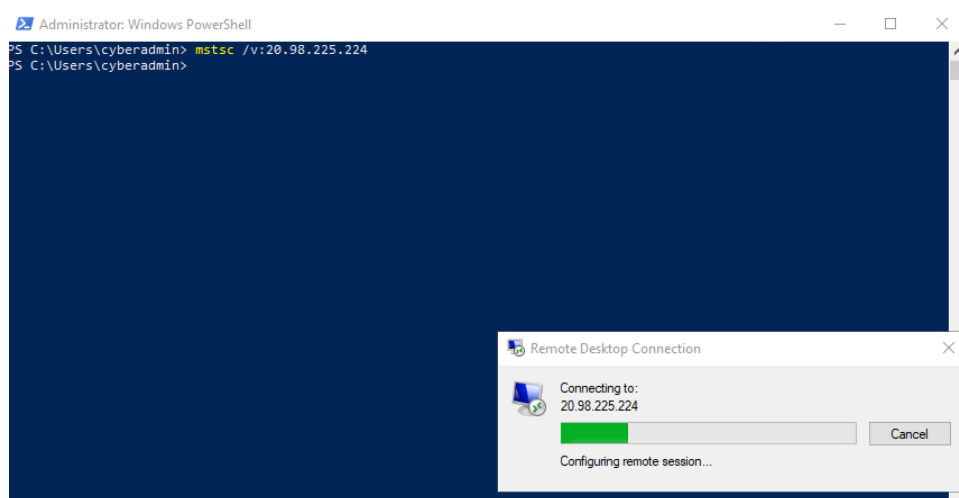
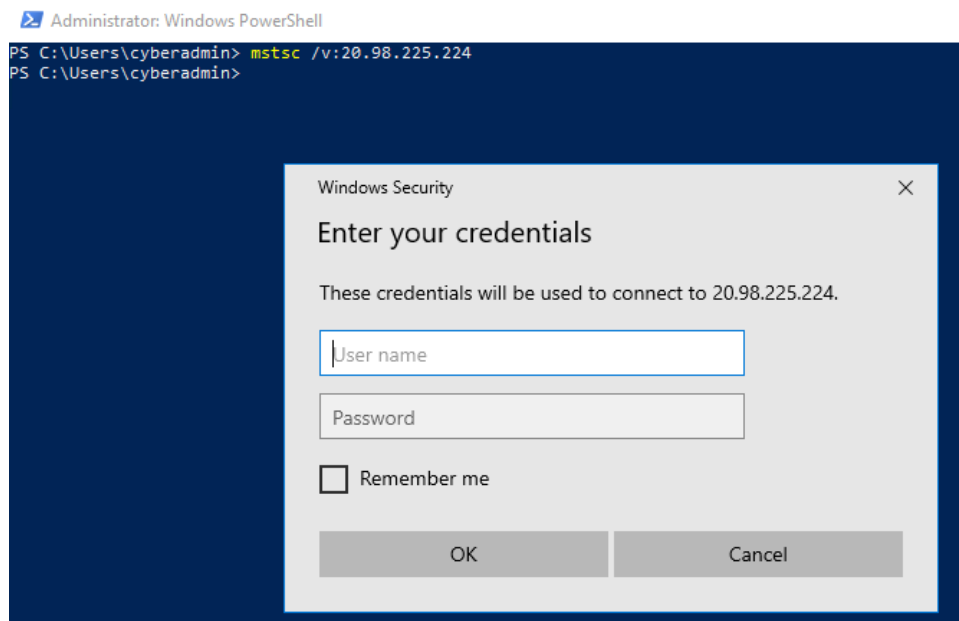
[Please Provide Screenshots of the RDP and SSH here as evidence that you completed this step.]

Connect to the Linux server using SSH
user@ipaddress

A screenshot of a terminal window with a dark blue background and white text. The text shows a PowerShell prompt at C:\Users\cyberadmin> where the command 'ssh cyberadmin@40.79.44.202' is entered. It prompts for a password three times. After the third attempt, it shows a successful login for 'cyberadmin@40.79.44.202's password:'. It then displays system messages about failed login attempts and the last successful login. Finally, the user enters 'exit' and the connection to 40.79.44.202 is closed.

```
PS C:\Users\cyberadmin> ssh cyberadmin@40.79.44.202
Password:
Password:
Password:
cyberadmin@40.79.44.202's password:
Last failed login: Tue Jun 29 15:32:48 UTC 2021 from 52.251.35.104 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Jun 29 15:27:10 2021 from 52.251.35.104
Last failed login: Tue Jun 29 15:32:48 UTC 2021 from 52.251.35.104 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Jun 29 15:27:10 2021 from 52.251.35.104
[cyberadmin@dfi-app-001 ~]$ exit
logout
Connection to 40.79.44.202 closed.
```

Connect to Windows Workstation using RDP
Using mstsc command for remote desktop



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.

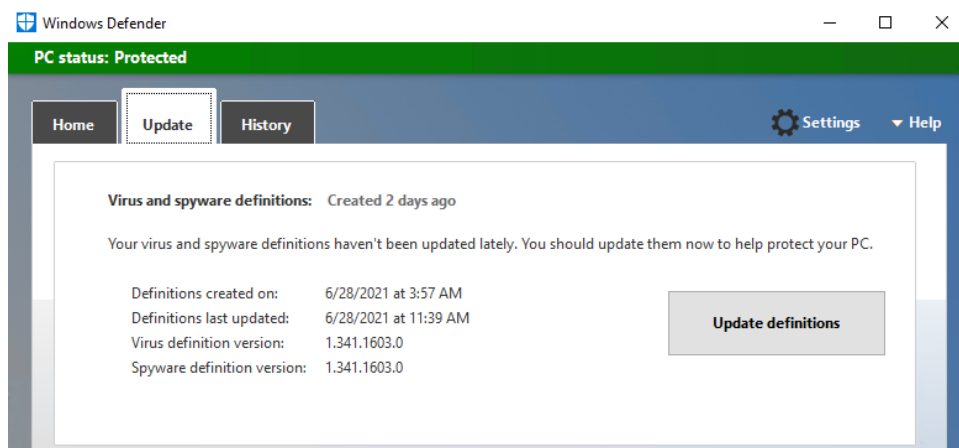
Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI compliant organization and will likely be Sarbanes-Oxley in the near future.

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]

- Patch and upgrade the server application and services

We need to upgrade all the application to prevent from having an attack and to reduce the risk. For example, we need to upgrade the Windows Defenders, because it indicates that virus and spyware definitions haven't been updated in a while.



- Change to be notified about the changes

It is important to always be notified when any changes occur, this will prevent harmful programs from making changes.

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

[Tell me more about User Account Control settings](#)

Always notify



Never notify

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

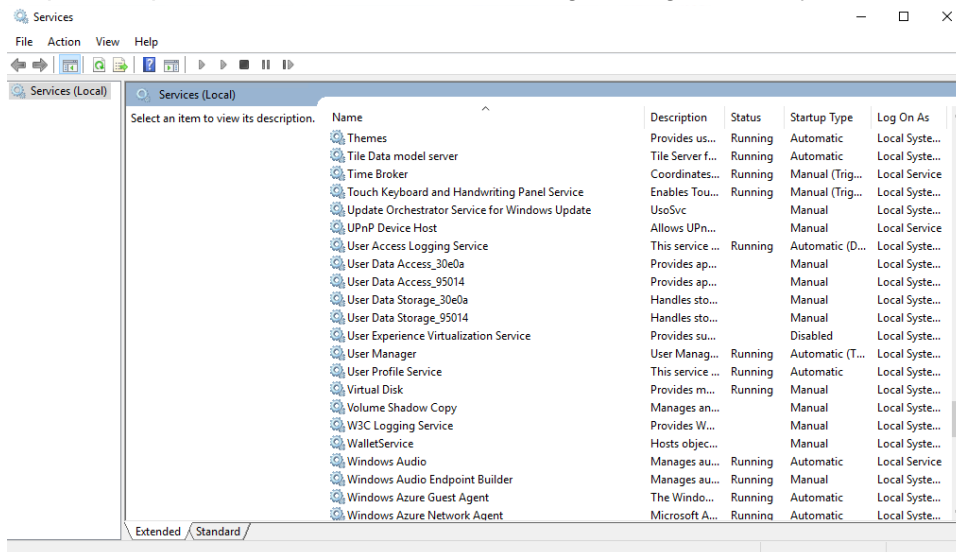
i Recommended if you use familiar apps and visit familiar websites.



Cancel

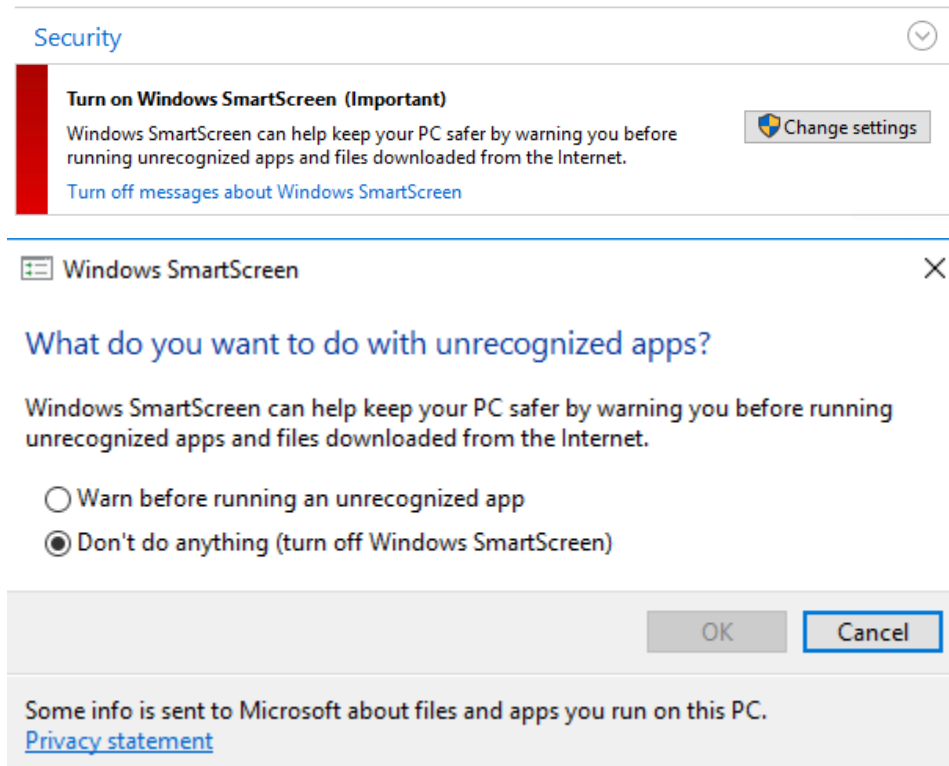
- Turn off the background applications and software

Shutdown the software and applications that running automatically in the background, This will help to keep insecure software from causing damage to the system or running malicious code.



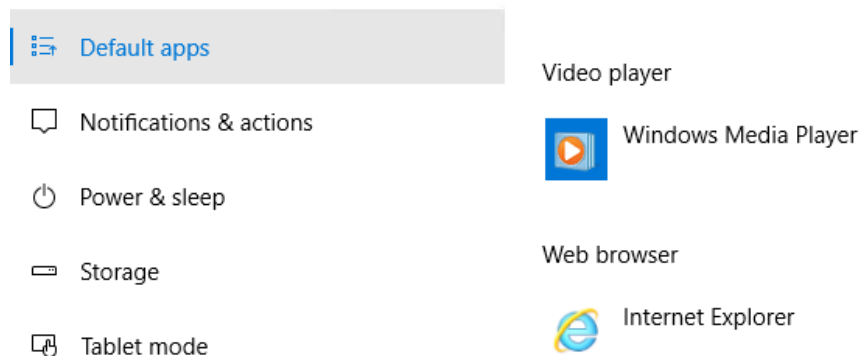
- Windows SmartScreen

Windows SmartScreen should be turned on, because it will send warnings before running unrecognized applications and download files from the internet. If we don't enable it, it won't be able to block the risky content which may contain malicious files that will harm the system.



- Change the default browser

It is important to change the default web browser and avoid using Internet Explorer, because unsafe, vulnerable, and lacks support.




- Ability to granularly control access to data on the server

Controlling data access is a useful security strategy for limiting who or what can see or use a given resource, this will ensure that each user only has access to the information he needs. This also will defend against unwanted visitors and allow you to keep track of who has accessed your information in order to prevent data breaches.

As shown below, it is required to modify the permission for some of the departments such as Accounting and HR department, we should give each department the least privilege. For instance, the HR directory should only allow the administrator to have full control of the

resources as well as the HR team. Which means they could read, write and execute. If there are others who require access to the resource, the access level should be restricted to read-only.





×

←  File Sharing

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.


Add

Name	Permission Level
 Accounting	Read/Write ▼
 Administrators	Owner
 AmyIT	Read ▼
 cyberadmin	Read/Write ▼

[I'm having trouble sharing](#)

Share Cancel




×

←  File Sharing

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Add

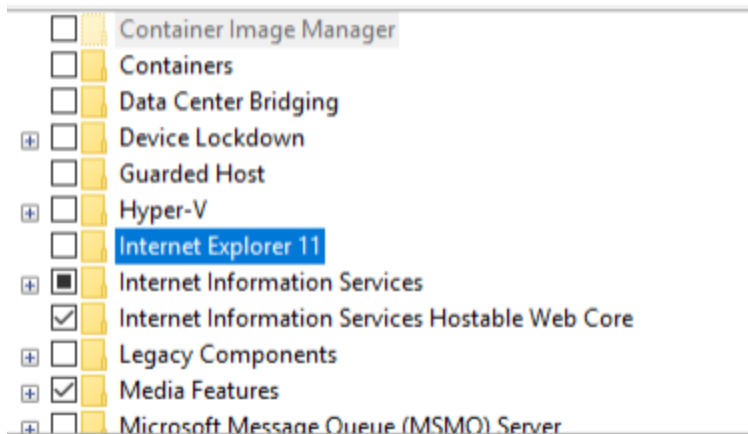
Name	Permission Level
 Administrators	Owner
 cyberadmin	Read/Write ▼
 HR	Read/Write ▼

[I'm having trouble sharing](#)

Share Cancel

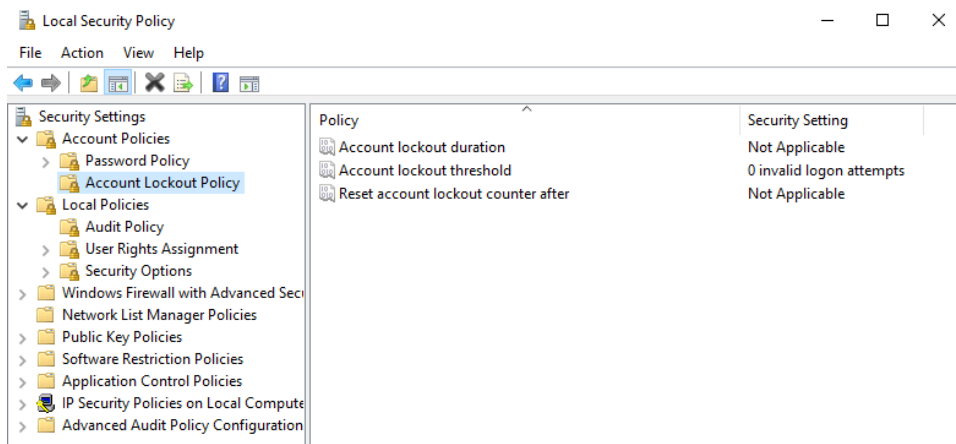
- Turn off unneeded Windows features

We should disable all the unnecessary features that provided by Windows to properly secure the system and avoid any future risks.



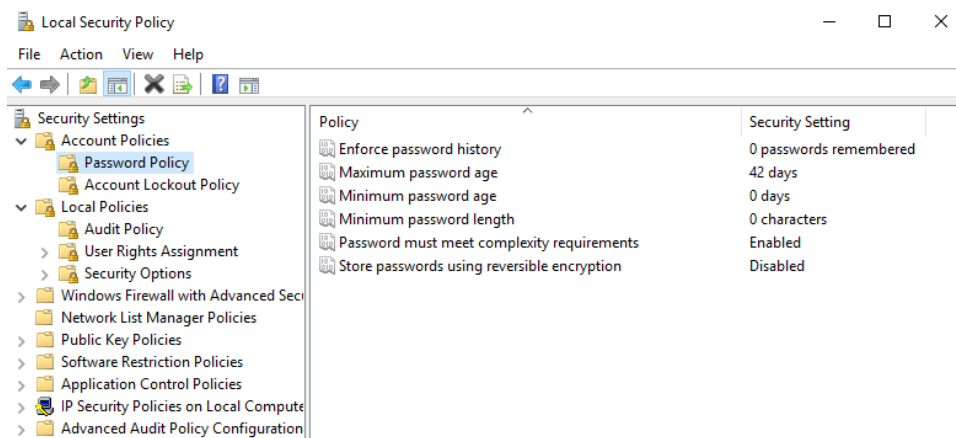
- Change account lockout policy

By managing the lockout polices, the lockout policy will assist limit the danger of attacks.



- Change password policy

It is important to list all the required password polices to strengthen passwords and prevent against attacks, this will protect both users' accounts as well as the system as whole.



- Turn on BitLocker Drive Encryption

It is important to turn it on to protect the drives, as it will aid in the protection of files and folders from unauthorized access.



3. Firewall Rules:

DFI does not have a dedicated networking department just yet, once again these tasks normally fall under the SysAdmin group. Now that we have you as a security professional, you'll take over the creation of our firewall rules. We recently entered into a new partnership and require new IP connections.

Using Cisco syntax, create the text of a firewall rule allowing a new DFI partner WBC International, access to DFI-File-001 access via port tcp-9082.

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

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

[Place your firewall rules and explanation here]

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

In the previous step, I used basic Cisco firewall rule which consists of several parts:

access-list – This is the rule that controls the traffic

DFI_Ingress - The name of the internal interface

Extended permit – The action (The traffic will permit). The ability to match traffic based on protocol, source, and destination address.

Tcp: Using TCP protocol

Host: The object involved

21.19.241.63 - The source

172.21.30.44 - The destination

Eq – equal to

9082 – The port required in the request (The port opened)

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]

In this situation, Symmetric encryption is preferable to asymmetric encryption in my opinion. Despite the fact that asymmetric encryption is believed to be more secure, Symmetric encryption will allow them to communicate quickly because just one key is necessary. The AES algorithm is so efficient, and the length of the key utilized determines how long it takes to decrypt. However, the RC4 is more powerful in terms of coding and more easy to implement, it also, requires less memory, and most importantly, is it is faster than the other algorithms and can be used on big data streams.

5. IDS Rule:

The System Administrator gave you a heads up that DFI-File-001 with an IP address of 172.21.30.44 has been receiving a high volume of ICMP traffic and is concerned that a DDoS attack is imminent. She has requested an IDS rule for this specific server.

The VoIP Administrator is also concerned that an attacker is attempting to connect to her primary VoIP server which resides at 172.21.30.55 via TFTP. She has requested an IDS rule for this traffic.

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

[Place your System Admin rule and explanation here]

```
alert icmp any any -> 172.21.30.44 any (msg: "ICMP traffic detected"; sid:1000006; rev:1;)
```

In the previous step, I used IDS rule which consists of several parts:

Alert: Used to notify the administrator when the rule fires.

Icmp: Type of traffic

Any: Used to alerting on any source, IP, and port

172.21.30.44: Ip address (destination)

Msg: Used to display the message that we want

Sid: The sid needs to be one million or higher

Rev1: Let us know that this is the first instance of the rule but isn't required

[Place your VoIP Admin rule and explanation here]

```
alert udp any any -> 172.21.30.55 any (msg:" Connection attempted via TFTP"; sid:1000008; rev:1;)
```

In the previous step, I used IDS rule which consists of several parts:

Alert: Used to notify the administrator when the rule fires.

udp: Type of traffic

Any: Used to alerting on any source, IP, and port

172.21.30.55: Ip address (destination)

Msg: Used to display the message that we want

Sid: The sid needs to be one million or higher

Rev1: Let us know that this is the first instance of the rule but isn't required

6. File Hash verification:

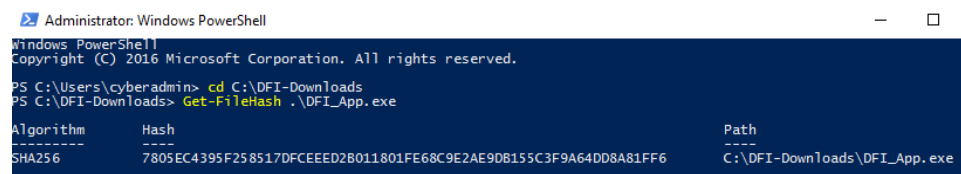
A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

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]

The hash is the same so we could verify the integrity and authenticity.



Administrator: Windows PowerShell

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

PS C:\Users\cyberadmin> cd C:\DFI-Downloads
PS C:\DFI-Downloads> Get-FileHash .\DFI_App.exe
```

Algorithm	Hash	Path
SHA256	7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6	C:\DFI-Downloads\DFI_App.exe

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
Insightconnect	A security automation and response system	Provides real-time visibility and ability to respond faster to security incidences including, detecting, blocking, email phishing, malicious programs, compromised URLs and domains, suspicious activities, compromised user accounts, vulnerable network ports.
RespondX	Real-time threat detection	Automatically suspend risky or compromised user accounts, processes, network access, and ports.
ServiceNow	Managing incidents and vulnerabilitie	Provides a summary of vulnerabilities, hence allowing teams to quickly discover and address the weaknesses and prevent attacks before they happen.

8. Logging RDP Attempts:

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

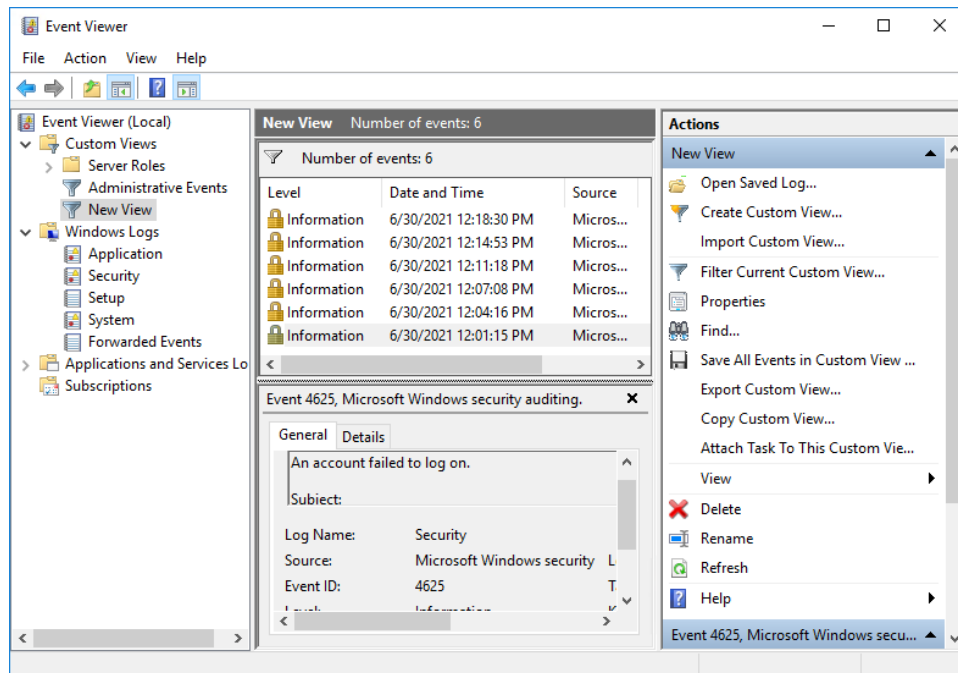
Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

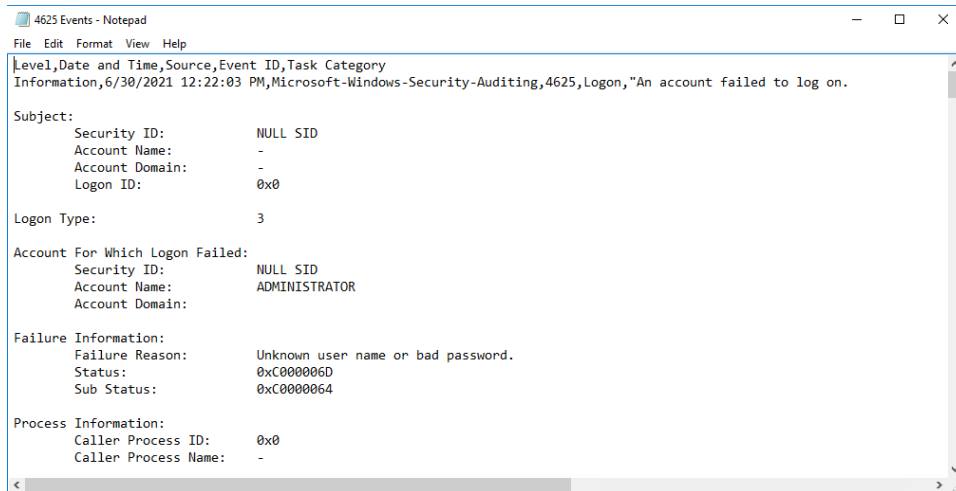
For your deliverable, open the CSV with notepad and take a screenshot from your personal computer for your explanation. Please also include this file in your submission. Then in your report below explain your findings, recommendations and justifications to the IT Manager.

[Place IT Manager Report Here]

```
PS C:\Users\cyberadmin> Get-EventLog -LogName Security -after (get-date).AddHours(-24) -InstanceId 4625
```

Index	Time	EntryType	Source	InstanceId	Message
2740053	Jun 30 12:43	FailureA...	Microsoft-Windows...	4625	An account failed to log on....
2734355	Jun 30 12:39	FailureA...	Microsoft-Windows...	4625	An account failed to log on....
2728711	Jun 30 12:36	FailureA...	Microsoft-Windows...	4625	An account failed to log on....
2723013	Jun 30 12:32	FailureA...	Microsoft-Windows...	4625	An account failed to log on....
2717180	Jun 30 12:29	FailureA...	Microsoft-Windows...	4625	An account failed to log on....
2711185	Jun 30 12:25	FailureA...	Microsoft-Windows...	4625	An account failed to log on....





```
4625 Events - Notepad
File Edit Format View Help
Level, Date and Time, Source, Event ID, Task Category
Information, 6/30/2021 12:22:03 PM, Microsoft-Windows-Security-Auditing, 4625, Logon, "An account failed to log on."

Subject:
  Security ID:      NULL SID
  Account Name:     -
  Account Domain:   -
  Logon ID:         0x0

Logon Type:        3

Account For Which Logon Failed:
  Security ID:      NULL SID
  Account Name:     ADMINISTRATOR
  Account Domain:   -

Failure Information:
  Failure Reason:   Unknown user name or bad password.
  Status:           0xC000006D
  Sub Status:       0xC0000064

Process Information:
  Caller Process ID: 0x0
  Caller Process Name: -
```

I used the following command line in PowerShell

```
Get-EventLog -LogName Security -after (get-date).AddHours(-24) -InstanceId 4625
```

To display all the events for the unsuccessful attempts in connecting that occurred within the last 24 hours. Also, I used the Event Viewer and filter technique to display the events that meets the requirements. From the results, I have six failed connecting attempts occurred the last 24 hours with 4625 event ID. In order to secure the system, we could limit the number of failed login attempts, which could help to lowering the danger of being hacked. We might employ the whitelisting technique, which allows us to compile a list of secure IP addresses that have permission to access the system.

9. Windows Updates:

Using [NIST 800-40r3](#) and [Microsoft Security Update Guide](#), analyze the windows servers and provide your answers in the table below of available updates (KB and CVE) that should be installed as well as any updates that can be safely ignored for DFI's purpose. To assist, be aware that DFI is concerned with stability and security, any update that is not labeled as a 'critical' or 'security' can be left off.

Justify your recommendations as to why you are making your choices.

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

Available Updates	Update/Ignore	Justification
CVE-2021-31985	Update	The vulnerability allows a remote attacker to execute arbitrary code on the victim system.
KB4565351	Ignore	It's an optional upgrade of the features which doesn't have to be completed right

		away.
CVE-2021-31978	Update	The vulnerability allows a remote attacker to perform a denial of service (DoS) attack.
CVE-2021-31971	Update	The vulnerability allows a remote attacker to bypass implemented security restrictions.
CVE-2021-31945	Ignore	They can be updated as needed.
CVE-2021-31943	Ignore	This is a minor feature that can be changed as needed.
CVE-2021-31970	Update	The vulnerability allows a local user to perform a denial of service (DoS) attack.

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.

I used some commands to create directories on the CentOS server DFI-App-001, such as cd which used to change directory, mkdir to create a new directory, pwd to show current directory, useradd to create a new user, and chown to set owner permission.

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

Connect to the Linux server using SSH

```

PS C:\Users\cyberadmin> ssh 40.79.44.202
Password:
Password:
Password:
cyberadmin@40.79.44.202's password:
Last failed login: Tue Jun 29 20:24:08 UTC 2021 from 52.251.35.104 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Jun 29 15:33:00 2021 from 52.251.35.104
Last failed login: Tue Jun 29 20:24:08 UTC 2021 from 52.251.35.104 on ssh:notty
There were 3 failed login attempts since the last successful login.
Last login: Tue Jun 29 15:33:00 2021 from 52.251.35.104
[cyberadmin@dfi-app-001 ~]$

```

- The root directory should be 'Home'

```

[cyberadmin@dfi-app-001 ~]$ pwd
/home/cyberadmin
[cyberadmin@dfi-app-001 ~]$ cd ..
[cyberadmin@dfi-app-001 home]$ pwd
/home
[cyberadmin@dfi-app-001 home]$

```

- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.

```

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

```

- Set owner permissions for the groups IT, HR, Operations and Accounting

```

[cyberadmin@dfi-app-001 Departments]$ sudo chown Amy IT
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ sudo chown Tim HR
[cyberadmin@dfi-app-001 Departments]$ sudo chown Pam Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chown Mandy 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.

```

[cyberadmin@dfi-app-001 Departments]$ cd IT
[cyberadmin@dfi-app-001 IT]$ pwd
/home/Departments/IT
[cyberadmin@dfi-app-001 IT]$ sudo useradd Amy
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ cd HR
[cyberadmin@dfi-app-001 HR]$ pwd
/home/Departments/HR
[cyberadmin@dfi-app-001 HR]$ sudo useradd Tim
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 HR]$ cd ..

```

```

[cyberadmin@dfi-app-001 Departments]$ cd Operations
[cyberadmin@dfi-app-001 Operations]$ pwd
/home/Departments/Operations
[cyberadmin@dfi-app-001 Operations]$ sudo useradd Pam
[cyberadmin@dfi-app-001 Operations]$ cd ..

[cyberadmin@dfi-app-001 Departments]$ cd Accounting
[cyberadmin@dfi-app-001 Accounting]$ pwd
/home/Departments/Accounting
[cyberadmin@dfi-app-001 Accounting]$ sudo useradd Mandy
[cyberadmin@dfi-app-001 Accounting]$ cd ..

[cyberadmin@dfi-app-001 Departments]$ ls -la
total 0
drwxr-xr-x.  6 root  root  62 Jun 29 20:32 .
drwxr-xr-x. 10 root  root 123 Jun 29 20:53 ..
drwxr-xr-x.  2 Mandy root   6 Jun 29 20:32 Accounting
drwxr-xr-x.  2 Tim  root   6 Jun 29 20:32 HR
drwxr-xr-x.  2 Amy  root   6 Jun 29 20:31 IT
drwxr-xr-x.  2 Pam  root   6 Jun 29 20:32 Operations

```

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

I created a Departments directory inside the home directory. Then, within Departments, I constructed four directories to represent IT, HR, Accounting, and Operations. Inside each of the departments I created the user who in charge of the department.

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]

The mitigation strategy include:

- Use the whitelisting technique, which allows us to compile a list of secure IP addresses that have permission to access the system.
- Limit the number of failed login attempts, this will stop the attacker from attempting to log into the system.
- TCP wrappers can be used to sort and filter who is able to access to the SSH server.
- Disable root login.
- Set a custom SSH port.
- Disable the port.

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]

I began scanning the entire system for vulnerabilities and determining what we needed to do to secure the system and avoid future attacks. We needed to upgrade the application and software, such as upgrading the Windows Defenders, especially the virus and spyware definitions because they haven't been updated in a while. In addition, I disabled the unnecessary background application that was running in the background. This will help to keep insecure software from causing damage to the system or running malicious code. I also turned on Windows SmartScreen, because it will help to send warnings before running unrecognized applications and download files from the internet. Moreover, I turned on BitLocker Drive Encryption, which will the files and folders from the unauthorized accesses. I changed the default browser and stop using Internet Explorer, because it is unsafe, vulnerable, and lacks support. After that, I changed the notifications settings to always notified when any changes occurs this will prevent harmful programs from making changes. I turned off the the Windows features that we don't need. Also, I controlled the data access to limit who can access or use the resources. After that, I changed the password and account lockout policy to protect both users' accounts as well as the system as whole. After I done, I created a firewall rules by using Cisco syntax. Also, I made an IDS rule for the server. Then, I tried to check the integrity and authenticity for a file by checking the hash. In addition, I did a research to recommend products, technologies, and areas within DFI such as, Insightconnect, RespondX, and ServiceNow. After that, I checked the unsuccessful attempts that occurred within the last 24-hours. I also, I checked for the important Windows updates. I also Created a directory that include the departments and the users with their permissions. Lastly, I found multiple ways that will help us to reduce the dangerous traffics such as, using the whitelisting technique, limit the number of failed login attempts, use TCP wrappers, and set custom SSH port. For future changes, we could use more of SOAR products such as, Splunk Phantom and IBM Resilient. Also, we could use whitelisting technique and update the system and programs automatically.

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.

The screenshot shows the 'Add to Archive' dialog box in 7-Zip. The 'Archive' field is set to 'C:\Users\maria\OneDrive\Documents\11111111111111\Monitoring and Securing the DFI Environment-Mariam Alabkari.7z'. The 'Archive format' is '7z', 'Compression level' is 'Normal', 'Compression method' is 'LZMA2', 'Dictionary size' is '16 MB', 'Word size' is '32', 'Solid Block size' is '4 GB', and 'Number of CPU threads' is '4 / 4'. The 'Update mode' is 'Add and replace files' and 'Path mode' is 'Relative pathnames'. The 'Options' section has three unchecked checkboxes: 'Create SFX archive', 'Compress shared files', and 'Delete files after compression'. The 'Encryption' section has 'Enter password:' and 'Reenter password:' fields, both containing masked text. There are also checkboxes for 'Show Password' and 'Encrypt file names', both unchecked. The 'Encryption method' is set to 'AES-256'. The 'Split to volumes, bytes' field is empty. The 'Parameters' field is also empty. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Archive: C:\Users\maria\OneDrive\Documents\11111111111111\Monitoring and Securing the DFI Environment-Mariam Alabkari.7z

Archive format: 7z Update mode: Add and replace files

Compression level: Normal Path mode: Relative pathnames

Compression method: LZMA2

Dictionary size: 16 MB

Word size: 32

Solid Block size: 4 GB

Number of CPU threads: 4 / 4

Memory usage for Compressing: 720 MB

Memory usage for Decompressing: 18 MB

Split to volumes, bytes:

Parameters:

Options

- ☐ Create SFX archive
- ☐ Compress shared files
- ☐ Delete files after compression

Encryption

Enter password: *****

Reenter password: *****

☐ Show Password

Encryption method: AES-256

☐ Encrypt file names

OK Cancel Help