

# Scenario:

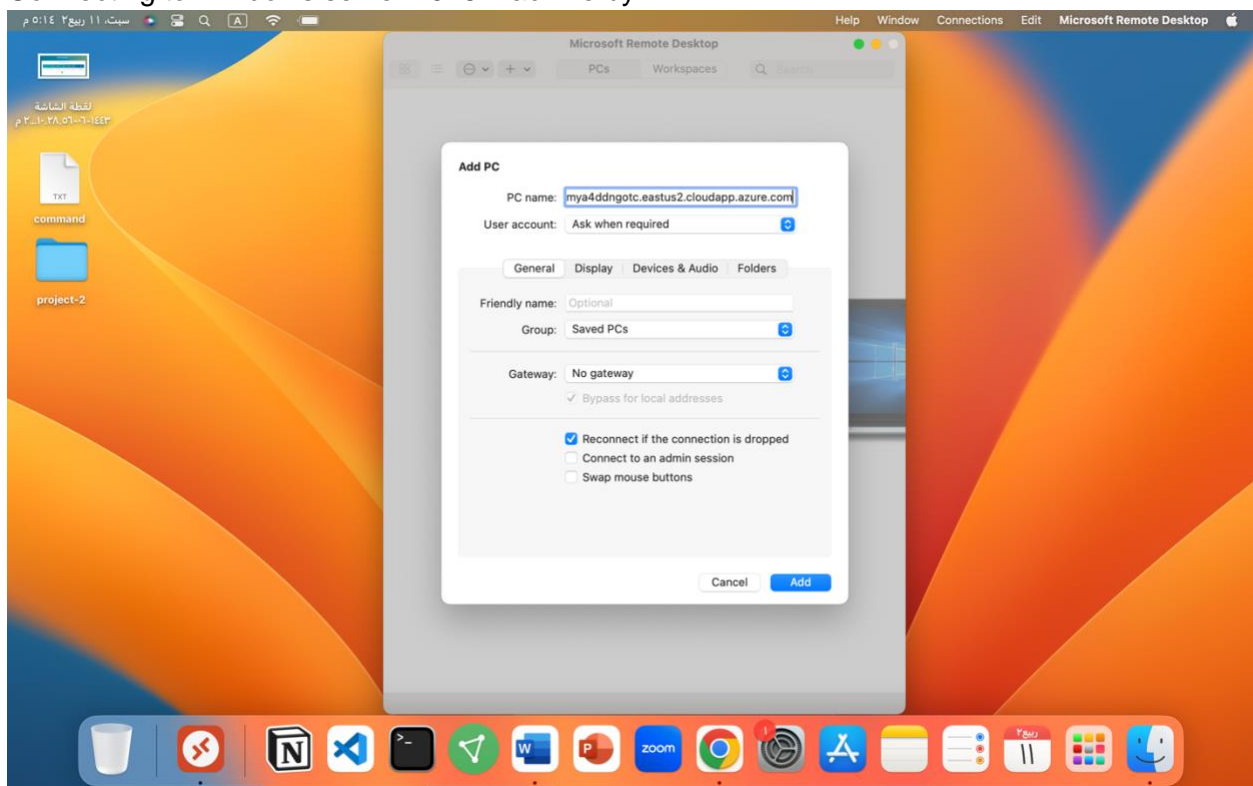
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

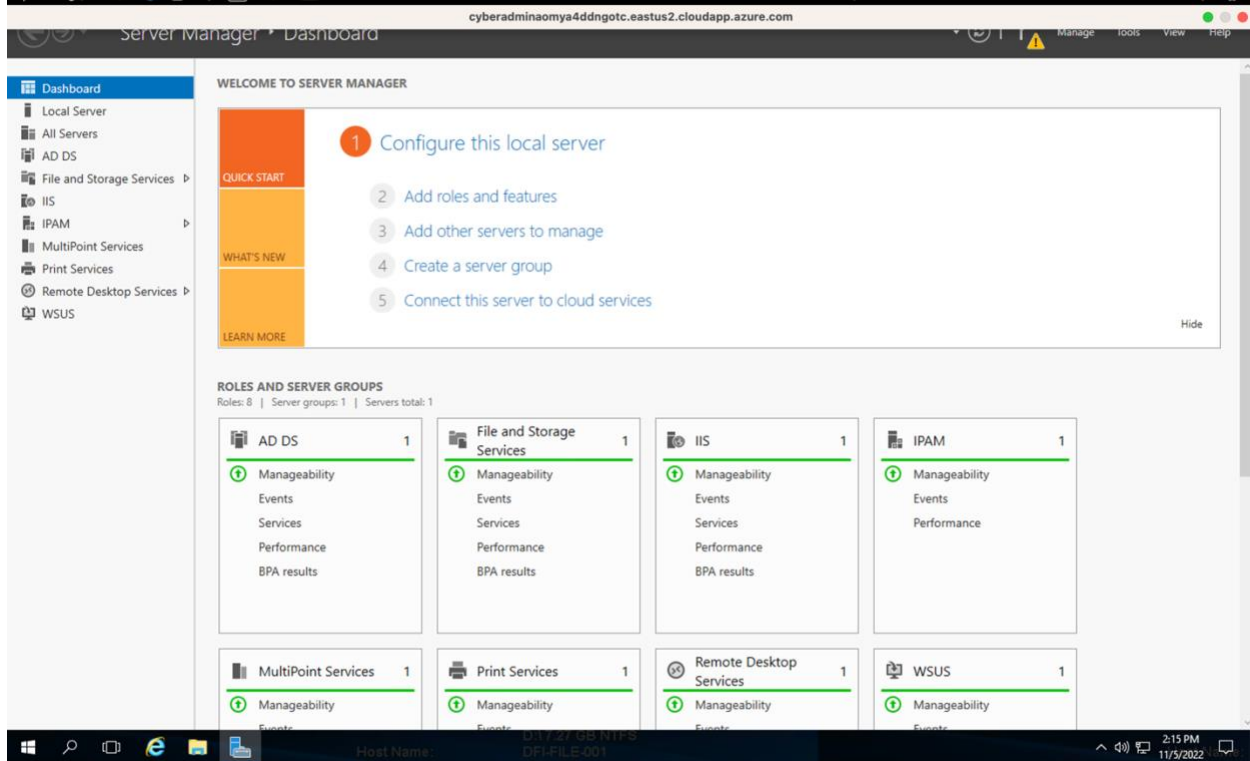
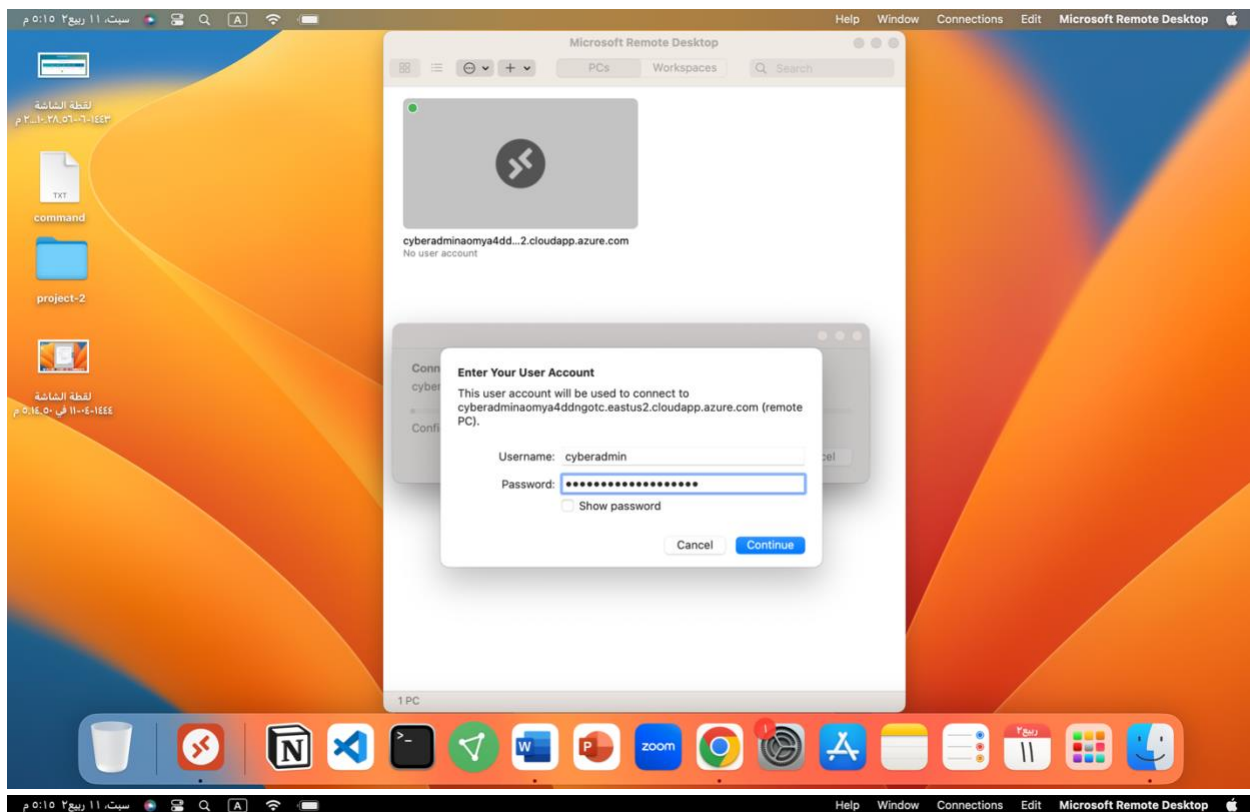
## Week One:

### 1. Connect:

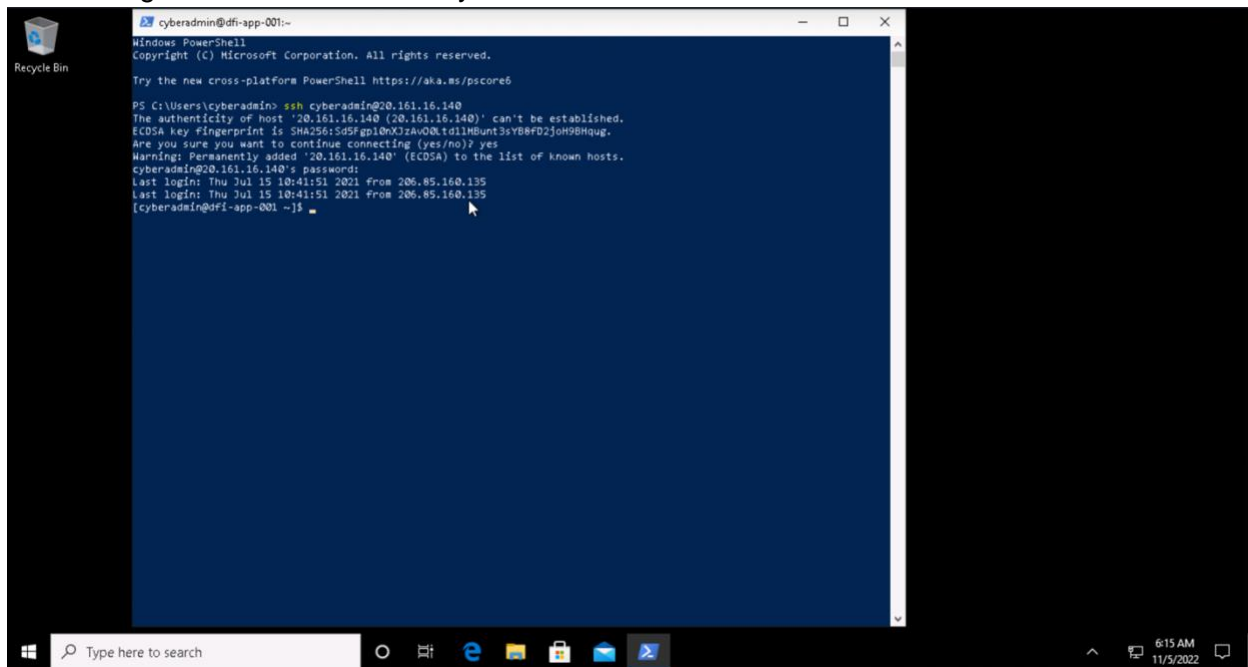
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

Connecting to Windows server 2016 machine by RDP:





Connecting to Centos 7 machine by SSH:



```
cyberadmin@dfi-app-001:~$ ssh cyberadmin@20.161.16.140
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\cyberadmin> ssh cyberadmin@20.161.16.140
The authenticity of host '20.161.16.140 (20.161.16.140)' can't be established.
ECDSA key fingerprint is SHA256:5d5Fgpl0nXJ2AVOQtd1lHBunt3sYB8FD2joh9BHQug.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '20.161.16.140' (ECDSA) to the list of known hosts.
cyberadmin@20.161.16.140's password:
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$
```

## 2. Security Analysis:

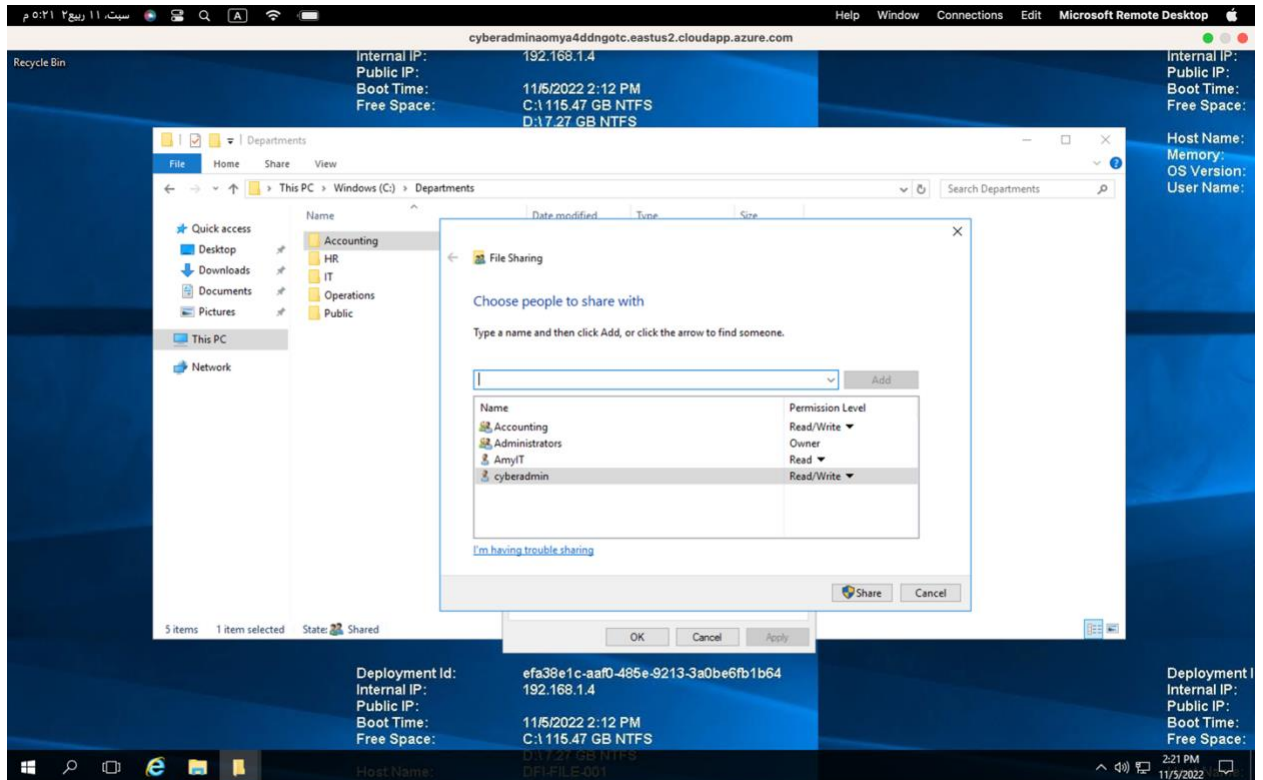
DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

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 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.)

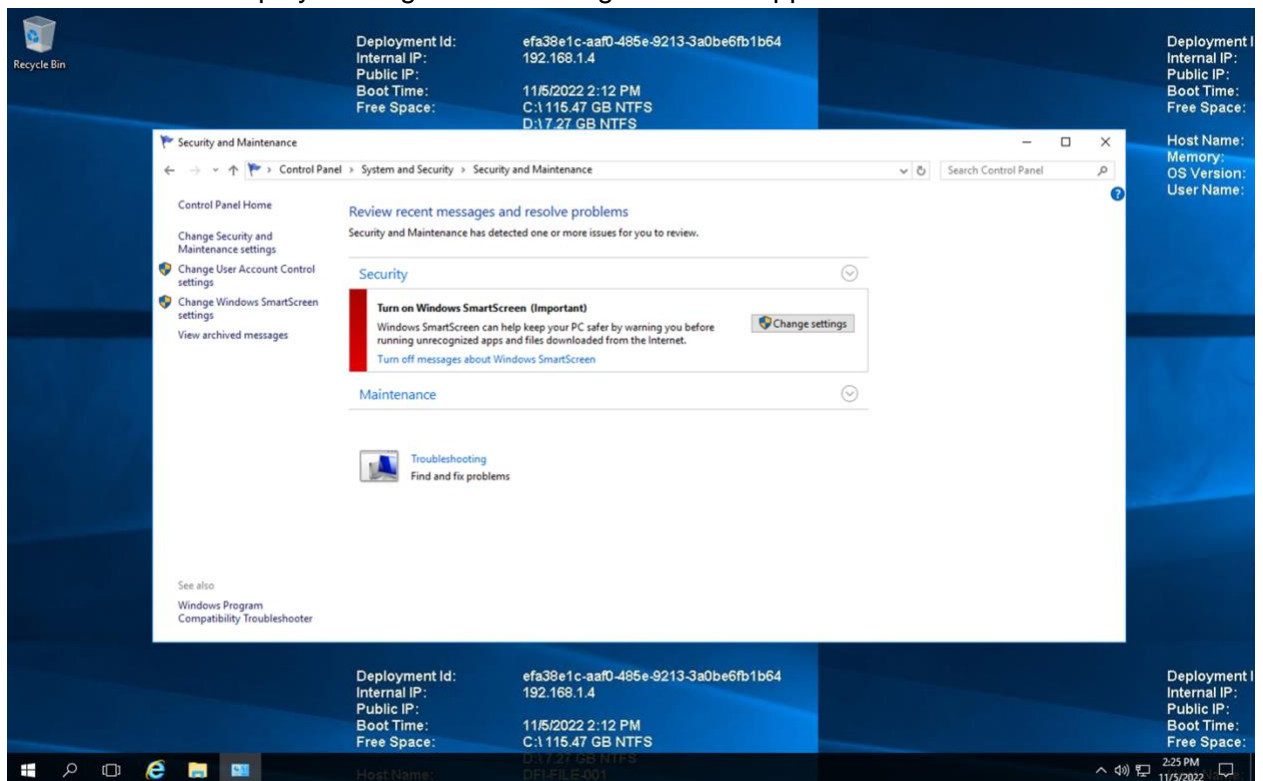
### 1. Principle of Least Privilege

Permission for Accounting folder must be changed.  
AmyIT shouldn't have access to the folder.



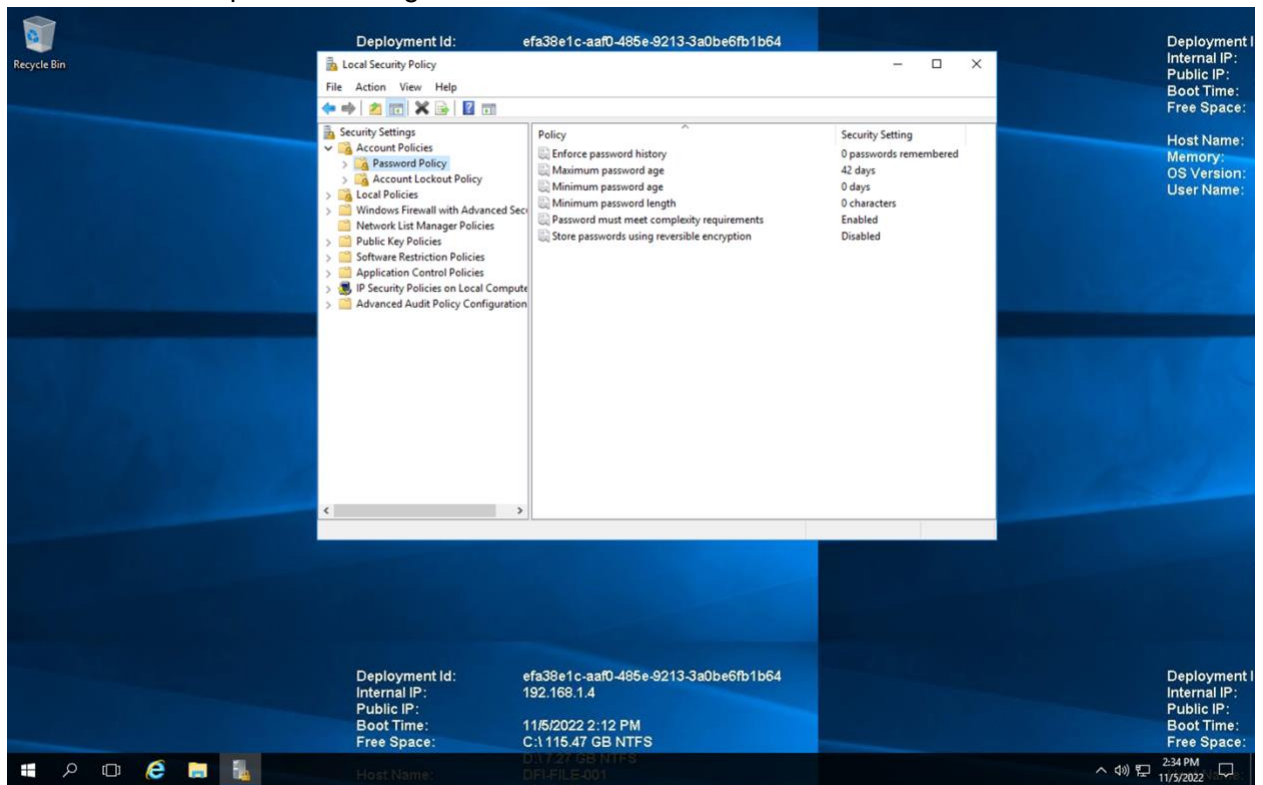
## 2. Windows Smart Screen

Should be on to display warning before running unwanted apps and files

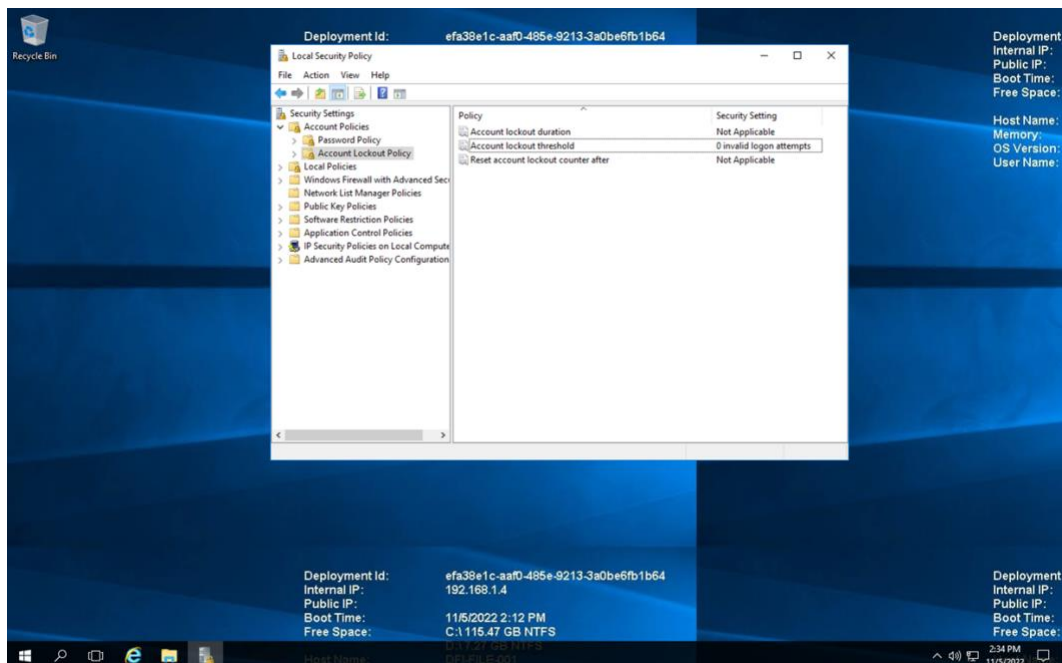


### 3. Local Security Policy

- Change password policy:  
Minimum password length to 12 characters to make it harder to crack



- Change Account lockout policy:  
Change Account lockout threshold to 5 invalid attempts to Prevent random guessing





#### 4. Outdated application

internet explorer is no longer supported, and attacker can benefit for this by using it as initial access point to the system.

#### 5. Securing Removable Media

A security best practice is to not allow the use of removable hard drives

### 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.

name 21.19.241.63 The-partner

name 172.21.30.44 DFI-File-001

access-list *DFI-Ingress* extended permit tcp host The-partner host DFI-File-001 eq 9082

This will allow the partner to access the DFI-File-001 through 9082 port which you can think as channel to connect to the system.

### 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.

We can go with Twofish or AES as an encryption solution.

Both are similar in terms of:

- 128 Bit Block
- 128, 192 and 256 Key size
- Both are well secure

I will go with Two-fish for two reasons:

- Shuffled using Feistel network

- 16 round of shuffle

## 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.

1. alert icmp any any -> 172.21.30.44 any (msg:"DDoS attack";sid:1000001;)
2. alert udp any any -> 172.21.30.55 69 (msg:" VoIP attempt";sid:1000002;)

basically, what we do is monitor the traffic for:

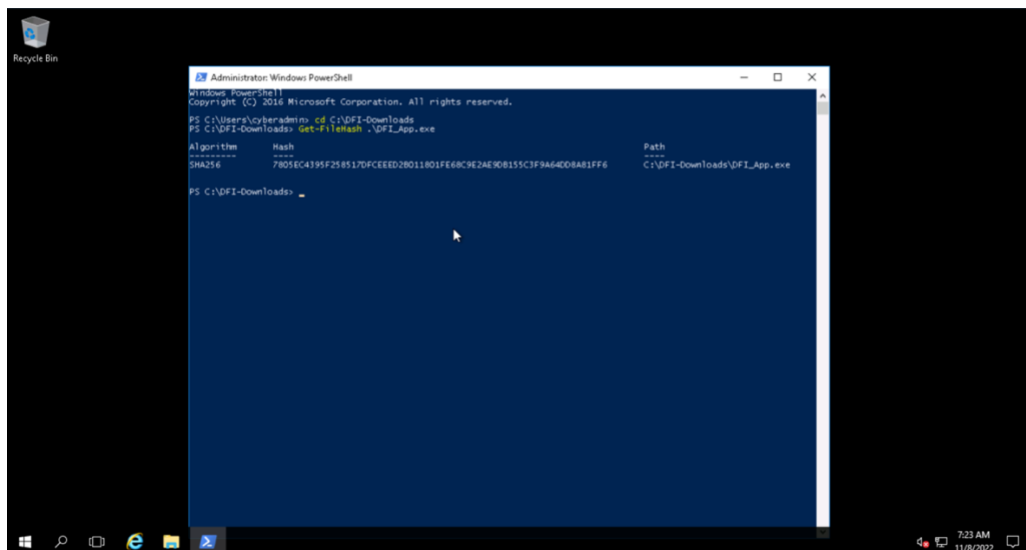
- icmp traffic coming to 172.21.30.44
- udp traffic coming to 172.21.30.55 through port (like a specific channel on the computer) 69

## 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.



## 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	Make whitelist of all employees and partners need to connect the system remotely	Speed the process of granting access via the firewall



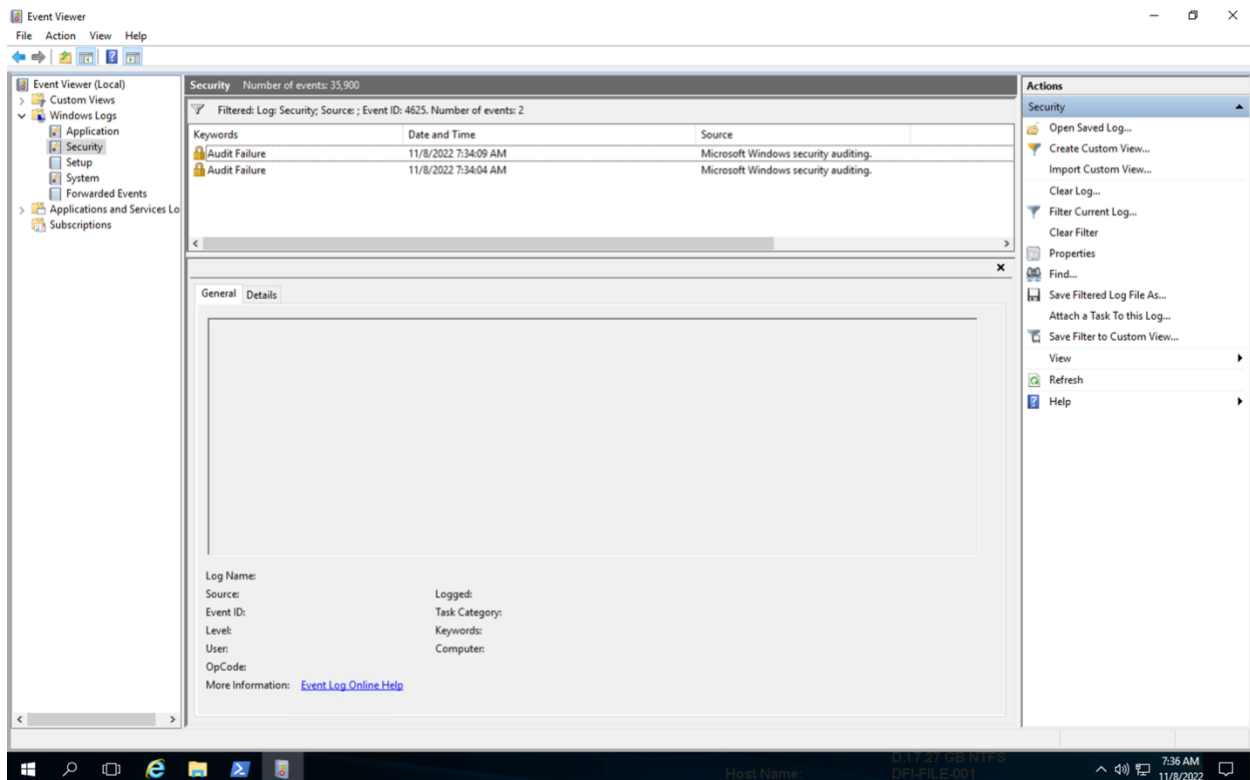
Windows OS	preimage of windows with default security settings	Install new pc easily and ensuring secure setting for them.
RDP Login attempts	Ban IP address based on a number of unsuccessful login attempts?	This will prevent bad actors from enter by brute-force. <a href="#">suggested solution</a>

## 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.



As we see there was two unsuccessful attempts to logon to the computer.

We to activate Account Lockout policy to prevent breaking to system by try and error technique.

## 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
KB5019964 (OS Build 14393.5501)	Update	It solves a remote code execution vulnerability (CVE-2022-41039)
KB5018411 (OS Build 14393.5427)	Update	Address a vulnerability where attacker can gain domain administrator privileges on the system (CVE-2022-37976)
KB5016622 (OS Build 14393.5291)	Update	Attacker can spoof their identity by manipulate an existing public certificate.
KB5017396	Ignore	It updates the service pack which is not critical for the system.
KB5004237	Ignore	Solve some difficulty user face when using certain printers.
KB4586781	Ignore	It address issue regarding input devices such as a mouse, keyboard, or pen.

## 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.

start by creating the directories using command **mkdir**

```
[root@dfi-app-001 ~]# mkdir Home
[root@dfi-app-001 ~]# cd Home/
[root@dfi-app-001 Home]# mkdir Departments
[root@dfi-app-001 Home]# cd Departments/
[root@dfi-app-001 Departments]# mkdir HR Accounting Public IT Operations
[root@dfi-app-001 Departments]# ls
Accounting HR IT Operations Public
```

Add the groups using command **groupadd**

```
[root@dfi-app-001 ~]# groupadd Accounting
[root@dfi-app-001 ~]# groupadd HR
[root@dfi-app-001 ~]# groupadd IT
[root@dfi-app-001 ~]# groupadd Operations
```

Change the ownership for the directories to their respective groups using command **chown**

```
[root@dfi-app-001 Departments]# chown :Accounting Accounting/
[root@dfi-app-001 Departments]# chown :HR HR/
[root@dfi-app-001 Departments]# chown :IT IT/
[root@dfi-app-001 Departments]# chown :Operations Operations/
```

Add new users using command **useradd**

```
[root@dfi-app-001 Departments]# useradd AmyIT
[root@dfi-app-001 Departments]# useradd PamOps
[root@dfi-app-001 Departments]# useradd MandyAcct
[root@dfi-app-001 Departments]# useradd TimHR
```

Add each user to the respective group using command **usermod**

```
[root@dfi-app-001 Departments]# usermod -g Accounting MandyAcct
[root@dfi-app-001 Departments]# usermod -g HR TimHR
[root@dfi-app-001 Departments]# usermod -g IT AmyIT
[root@dfi-app-001 Departments]# usermod -g Operations PamOps
```

## 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.

As we observe for the firewall alerts the system is under brute-force attack.  
mitigation :

- **Limit the number of authentication attempts**
- **Implement brute-force protection:** It works by going over the system log, searching for field login or suspicious activities, and then taking action like banning the IP address.

[reference](#)

## 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.

After analyzing the system and following the best security practices we apply these changes:

- Give each user the minimum permissions for doing their job
- Change the policy regarding the age for passwords and the permitted tries before the system lock

- Activate monitoring of any change concerning system configuration
- Update any outdated software
- Securing the system by denying any use of removable hard drives
- Protecting remote access by applying encryption channels and denying malicious connections.
- Using new technologies to automate redundant work.

### **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.**