# Scenario:

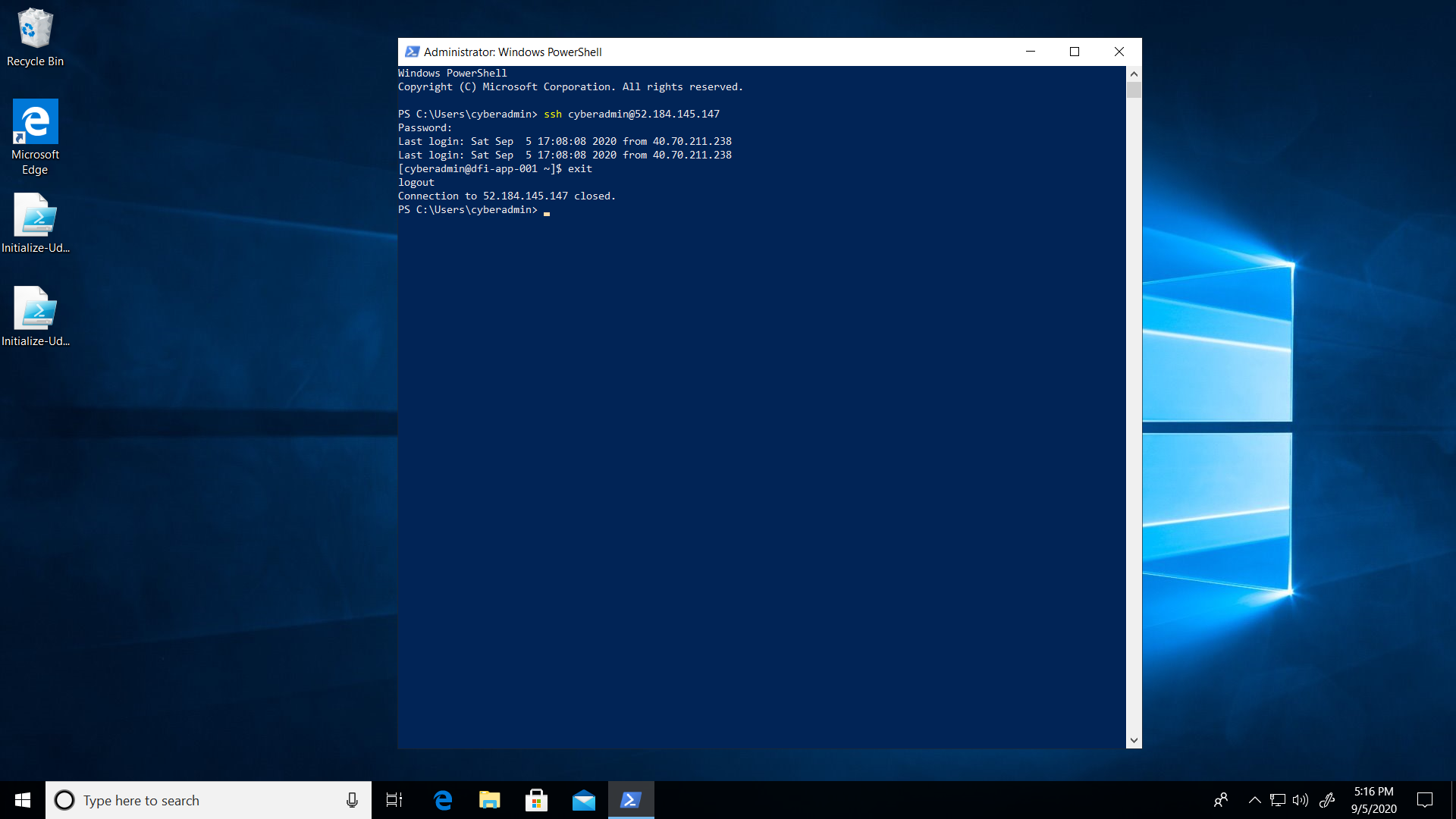
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

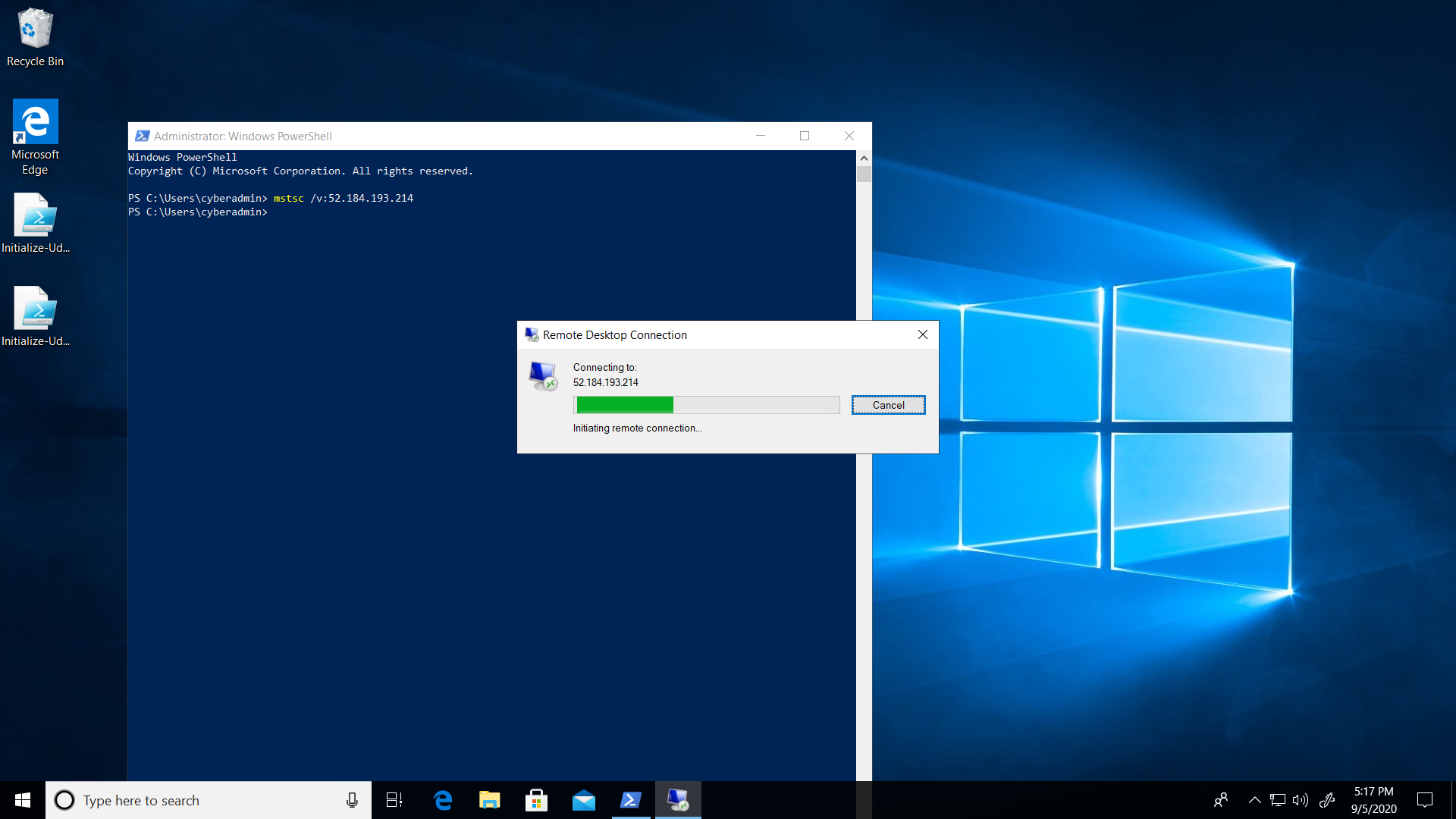
## Week One:

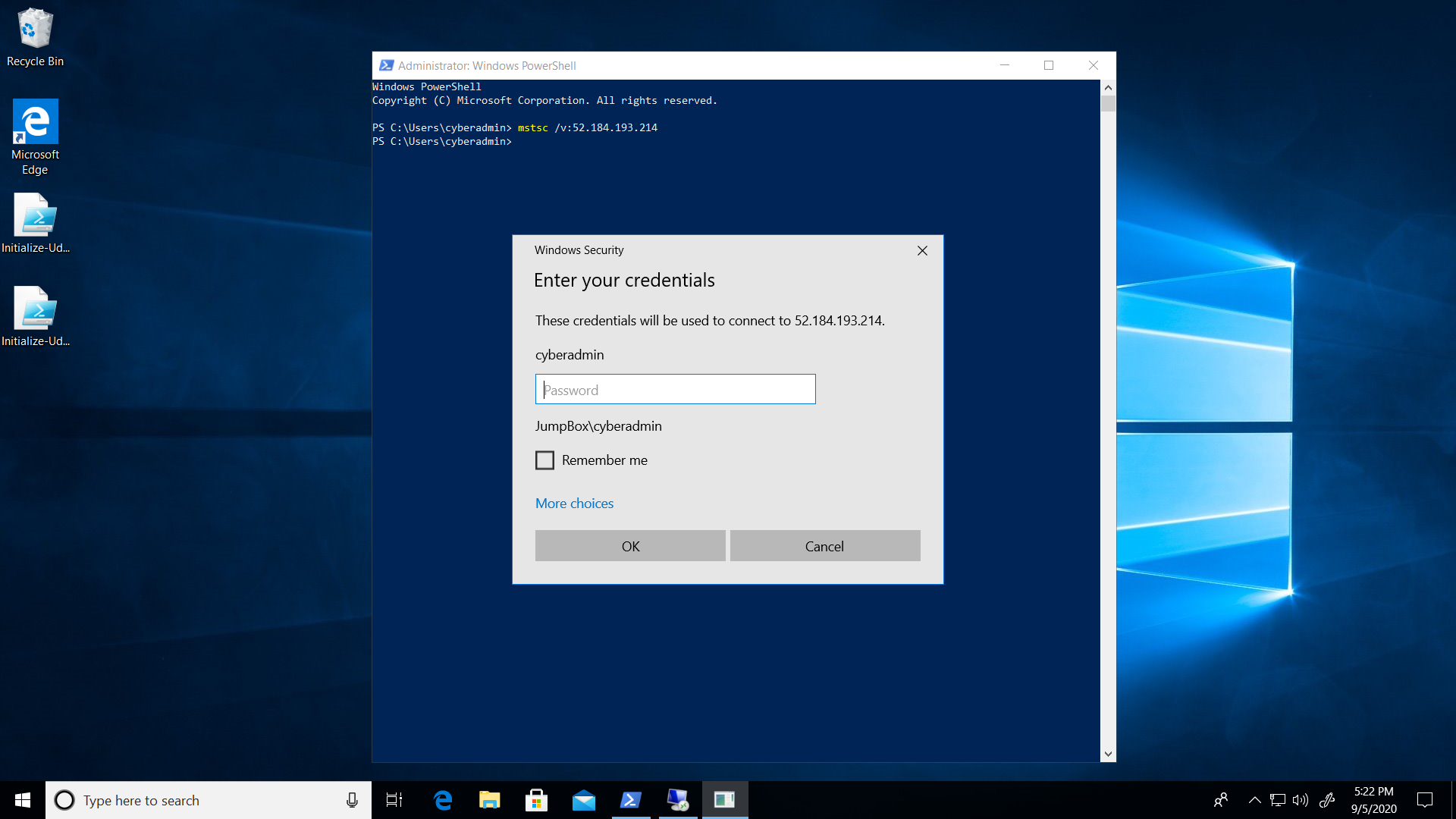
### 1. **Connect:**

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.]







### 2. **Security Analysis:**

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

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

Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege and other resources to determine the changes that should be made. Note changes can be to **add**/**remove/change** services, permissions and other settings.[Defense-in-Depth documentation.](http://iieng.org/images/proceedings_pdf/8285E0914047.pdf) [NIST 800-123](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf) (other NIST documents could also apply.)

[Place your security analysis here]

1. ***Windows SmartScreen:***

***Windows SmartScreen is not enabled in the PC. SmartScreen makes sure that the PC is safe by displaying a warning before running any unrecognized applications and files downloaded from the internet.***

***Windows SmartScreen must be enabled. Disabling Windows SmartScreen may result in:***

* ***Background downloads being conducted by applications***
* ***Downloading malicious/corrupted files***

1. ***User Access Control Settings:***

***Current setting on the PC is to “Notify me only when apps try to make changes to my computer”***

***This setting must be changed to “Always notify me when: Apps try to install software or make changes to the computer and I make changes to windows settings”***

***The previous settings can lead to unintentional changes made by the user go undetected. But if the setting is changed to always notify me, then even if the user makes any changes then there will be a notification about it. Which can help the user confirm if the changes are to be done or not.***

1. ***Bit Locker:***

***Windows (C:) Bit Locker is not enabled.***

***Bit locker must be enabled as it protects the data by providing encryption. It mostly uses AES encryption to safeguard the data. By enabling BitLocker, we can make sure that only authorized users can access the data present in the PC.***

1. ***Permissions on the HR folder:***

***Full access to a folder should be with the owner and the administrator. Other than them only the trusted and necessary user must be given access. The HR folder permissions must be changed so that only the admin, owner and system have full control on the folder.***

### 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 host 21.19.241.63 host 172.21.30.44 eq 9082***

***The syntax starts with the access list which is just a rule that manages traffic. DFI-Ingress which is the next part of the syntax is the interface being used. We are giving permission to the host to access the files, so we use extended permit. The first host ip address is of the source and the second host ip address is the destination (company’s ip address). Eq 9082 is the port number through which the data can be accessed. Basically, the syntax represents that the source can access the destination via port 9082.***

### 4. **VPN Encryption Recommendation:**

DFI is creating a payroll processing partnership with Payroll-USA, this will involve creating a VPN connection between the two. Research, recommend and justify an encryption solution for the connection that is using the latest available encryption for Cisco. Use the Cisco [documentation](https://tools.cisco.com/security/center/resources/next_generation_cryptography) as a guide.

[Place your VPN Encryption Recommendation here]

***I would recommend Symmetric encryption. In this type of encryption there is only one key for both encryption and decryption. There are 3 types of symmetric encryption, AES, Twofish, RC4. AES is a mandatory standard given by the PCI-DSS that all the all the data stored as well as in-transit forms must be encrypted using AES. RC4 is simple and quick. Twofish is commonly used in e-commerce websites because it makes payment safe and secure. For these reasons I think symmetric encryption is the best to use in our situation.***

### 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;)***

***The above rule alerts us when there is an ICMP traffic detected. Alert is first part of the rule which tells us that the rule is for alerting us. Next comes the protocol that is used, here it is ICMP. Then the source ip address and port are written. In this case I have written any which represents that it can be from any ip and any port. 172.21.30.44 is the destination (our company) and any is on any port. Then the message that needs to be displayed in this case “ICMP traffic detected” is written and the sid and rev.***

[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;)***

***The above rule alerts us when there is a connection attempted via TFTP. Alert is first part of the rule which tells us that the rule is for alerting us. Next comes the protocol that is used, here it is UDP. Then the source ip address and port are written. In this case I have written any which represents that it can be from any ip and any port. 172.21.30.55 is the destination (our company) and any is on any port. Then the message that needs to be displayed in this case “Connection attempted via TFTP” is written and the sid and rev***

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

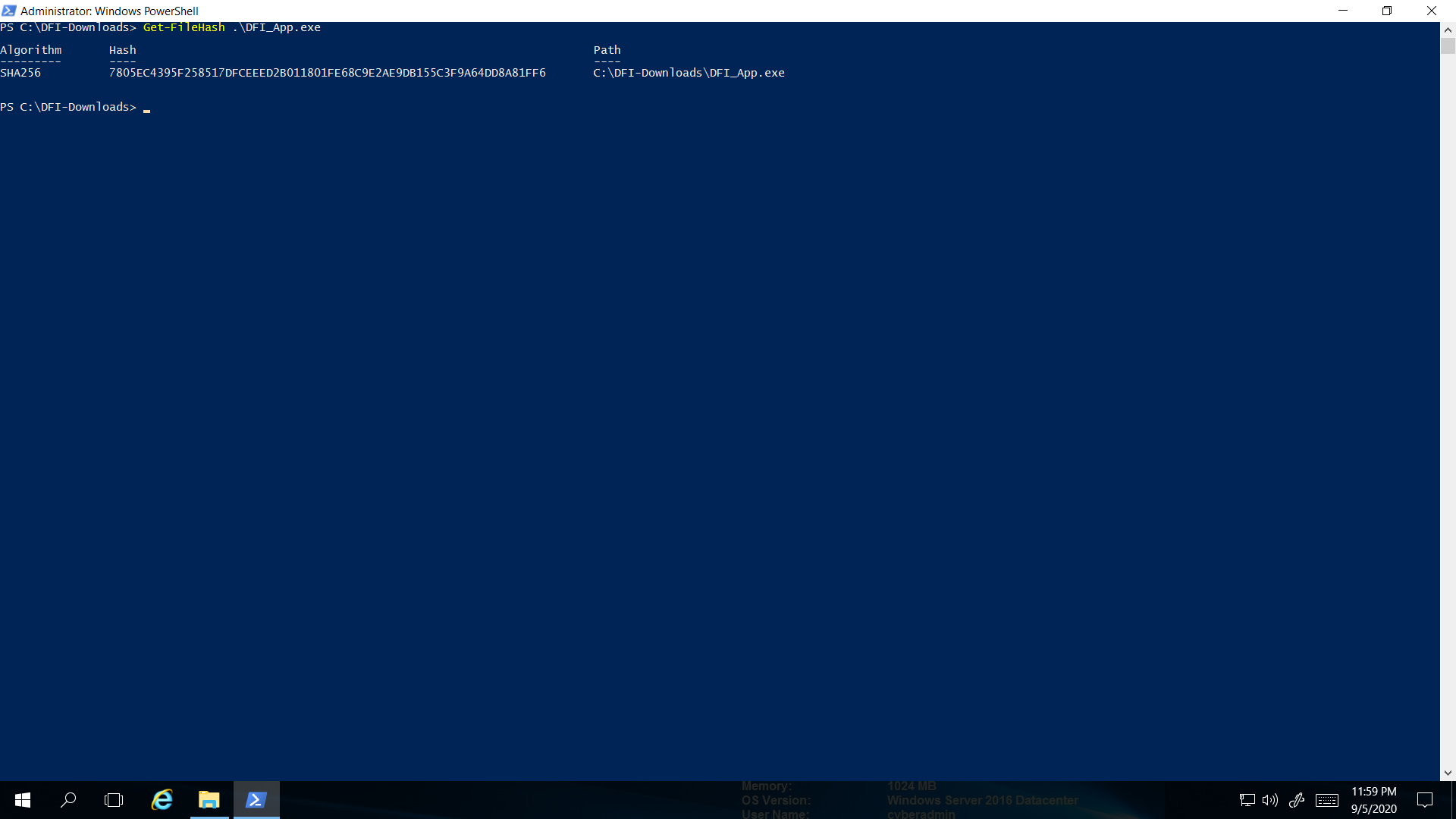
A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

**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.

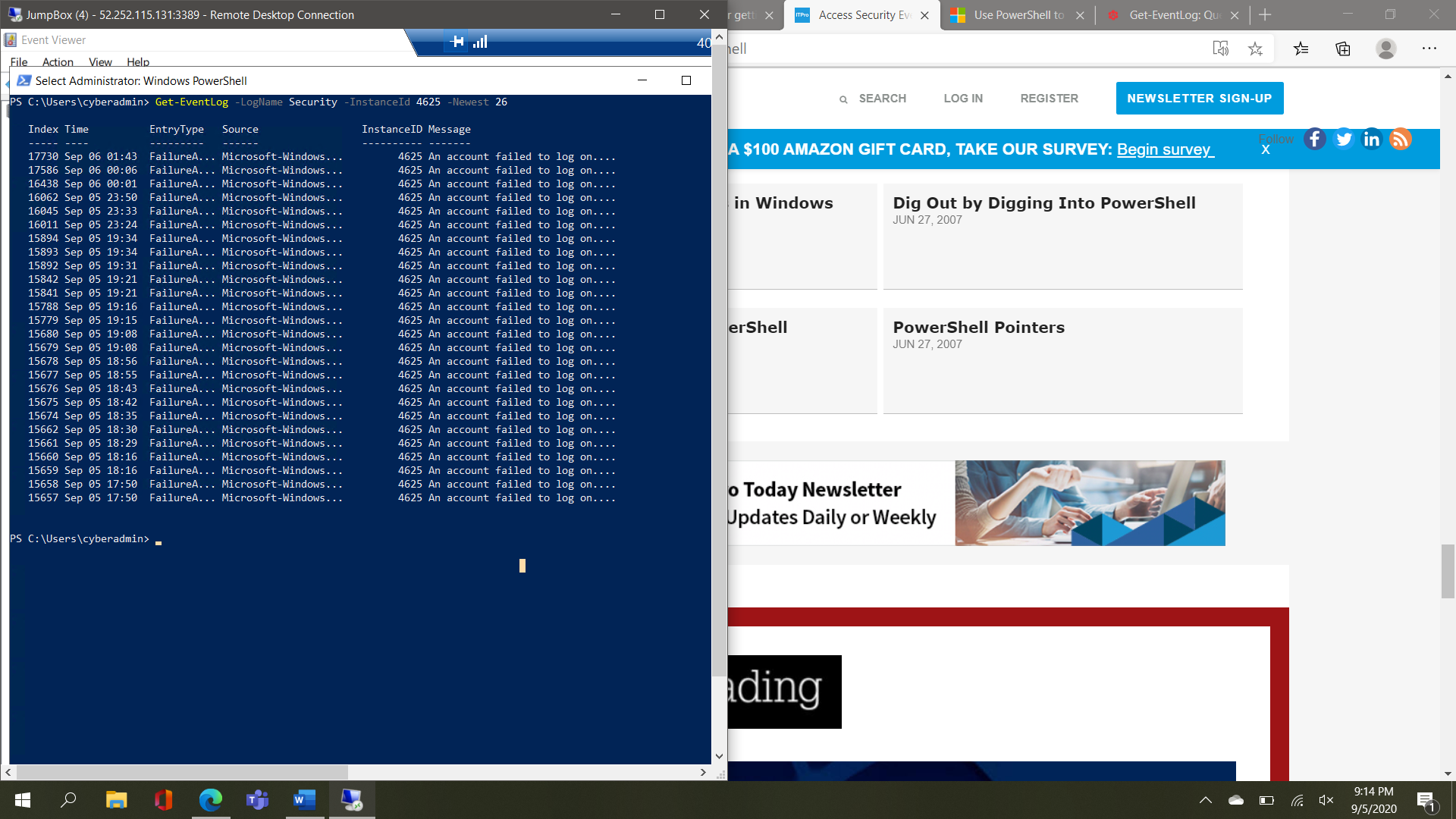
Complete the chart below including the area/technology within DFI and a proposed solution, with a minimum of 3 areas. Provide a brief explanation for your choices.

|  |  |  |
| --- | --- | --- |
| **DFI Area/Technology** | **Solution** | **Justification for Recommendation** |
| ***Logging attempts*** | ***There should be a limit to the number of logins*** | ***While analyzing the security logs, I came across the fact that there were a lot of login attempts done. If there is a limit to the number of logins attempts, then only the authorized user can login to the system. Which also ensures confidentiality and integrity.*** |
| ***Application Monitoring*** | ***Real-time application monitoring*** | ***My monitoring the applications one can make sure that there are no other process/tasks that are taking place in the background that may cause problems to the system/company in the future.*** |
| ***Incident Response*** | ***Using cyber fusion solutions*** | ***Cyber fusion is a technique of combining many solutions into one. I comprise of full incident analysis and response. This protects the system against malware, vulnerabilities and threat actors in real-time.*** |
|  |  |  |
|  |  |  |

### 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 ] 

***According the analysis on the Security log, it seems that there are a lot of failed logging attempts. In order to reduce this kind of events and protect the system, there should be a limit in the number of failed log-in attempts. This makes sure that there are no brute force attacks that can be done in order to gain access to the system. Limiting the number of failed log-in, it will help reduce the risk of being hacked. In order to avoid untrusted IP address to try to login to the system add trusted IP address and remove Blocked/Untrusted IP address from the firewall configuration. By doing this only the trusted IP addresses will be allowed and the untrusted ones will be stopped.***

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

Using [NIST 800-40r3](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf) and [Microsoft Security Update Guide](https://portal.msrc.microsoft.com/en-us/security-guidance), analyze the windows servers and provide your answers in the table below of available updates (KB and CVE) that should be installed as well as any updates that can be safely ignored for DFI's purpose. To assist, be aware that DFI is concerned with stability and security, any update that is not labeled as a 'critical' or 'security' can be left off.

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

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

|  |  |  |
| --- | --- | --- |
| Available Updates | Update/Ignore | Justification |
| ***KB4569751*** | ***Update*** | ***It observes application runtime failures or unexpected behaviors.*** |
| ***KB4561600*** | ***Update*** | ***Security updates are very critical in all the situations. Security cannot be compromised even if it is a small problem. Later this small problem can cause fatal destruction.*** |
| ***KB2267602*** | ***Update*** | ***Microsoft Windows Defender Antivirus protects the system from being affected. It uses cloud-delivered protection and downloads security intelligence updates to provide protection to the system.*** |
| ***KB4565351*** | ***Ignore*** | ***These are the optional, improvement features provided by Microsoft. These updates can be added to the end of the update list. It is not an urgent update that needs to be done immediately.*** |
| ***21.90.1.1 – Driver Update*** | ***Ignore*** | ***Bluetooth driver updates are not so important. They can be updated when there are in need. Once the important updates are done then the update on the Bluetooth drive can be done.*** |
| ***KB4565483*** | ***Ignore*** | ***These updates are mainly optional, but they make many improvements. But these can be done once the other important aspects or updates are done.*** |

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

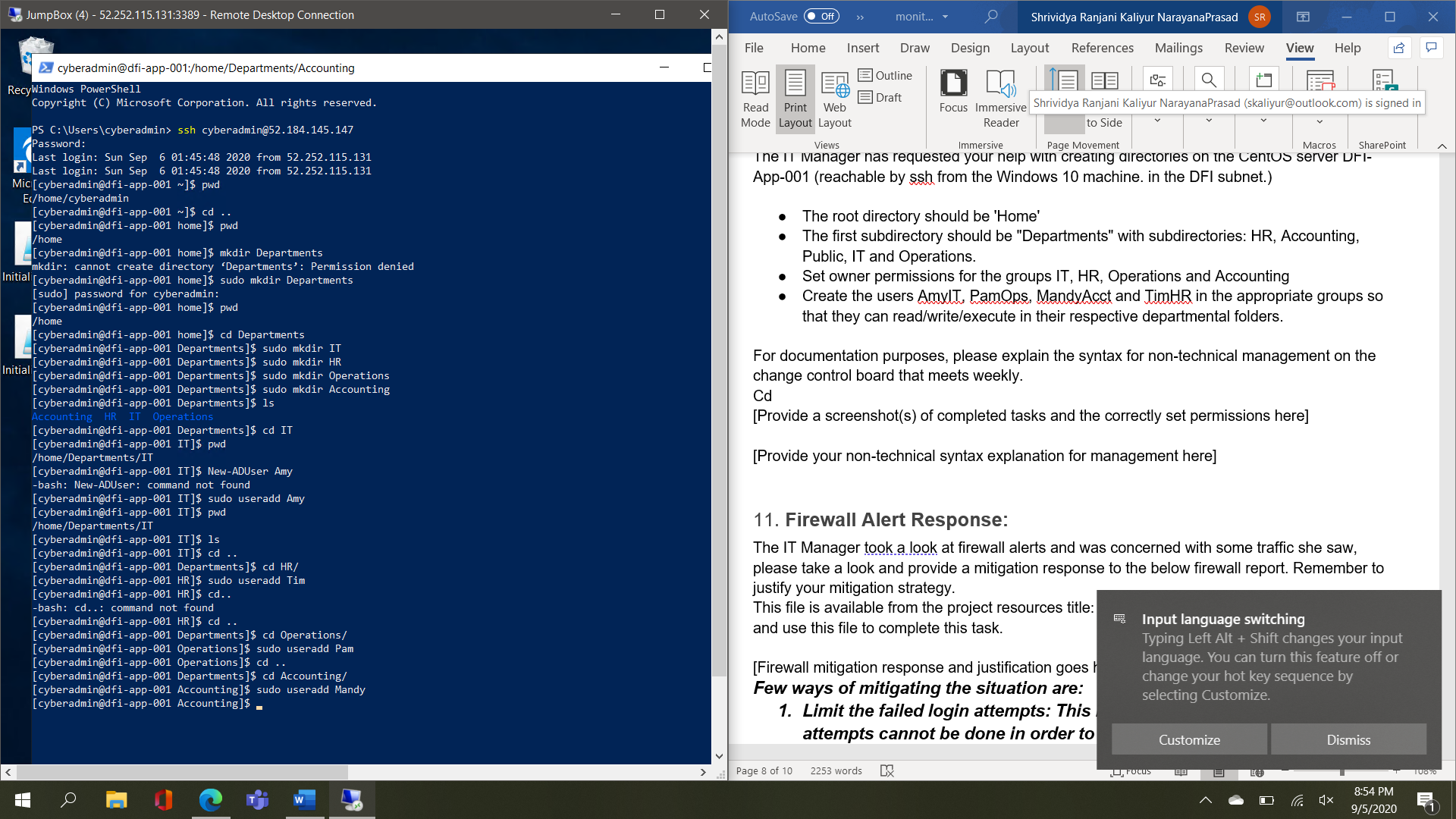
The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

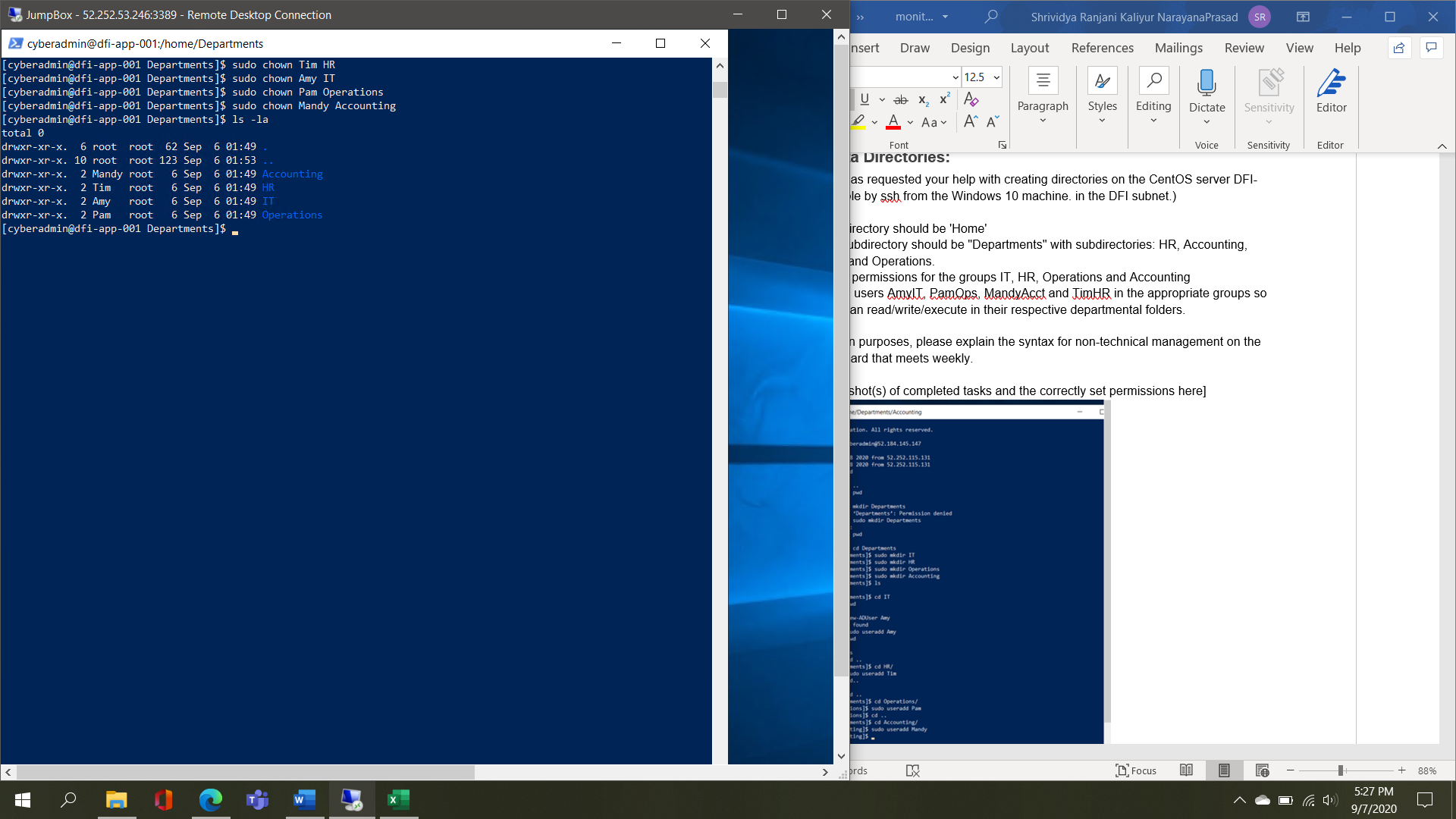
* The root directory should be 'Home'
* The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.
* Set owner permissions for the groups IT, HR, Operations and Accounting
* Create the users AmyIT, PamOps, MandyAcct and TimHR in the appropriate groups 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.

Cd

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





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

***Here we are creating a directory named Department under the Home directory. Inside Departments directory we are creating 4 directories named IT, HR, Operations, Accounting. Inside each of the directories we created a user account in appropriate groups.***

### 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]

***Few ways of mitigating the situation are:***

1. ***Limit the failed login attempts: This makes sure that a greater number of attempts cannot be done in order to login. This reduces the chance of an authorized user to log into the system.***
2. ***Limit logins to a specified IP address name: This makes sure that only those who are given access can try and log into the system. No other IP address can be used to log in***
3. ***Two factor authentications: Two factor authentication can reduce the probability of someone else to log into the system. Even if the other user gets access to the password, he/she will not have the second factor needed to log in***
4. ***Making the root user inaccessible via SSH can be very beneficial***
5. ***Using Captcha’s can help in reducing the risk of bots trying to login***

### 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 doing anything we need the connection between the machines to get our work done. So, first I established the connection between the servers. Then an analysis was conducted to find out what changes were needed to make and why do we need those changes. Firewall rule was created to give access to a file to the company partner. The best VPN encryption that is to be used for the payment payroll partnership was determined.***

***Monitoring the systems and the networks are mandatory. So, IDS rules were created in order to keep an eye on the incoming traffic and connections attempted. File hash verification was done on a vendor supplied software.***

***Security logs with specific events were accessed, analyzed and recommendations were determined.***

***Windows updates were checked and determined if they were necessary at that moment or they can be ignored.***

***A firewall report was thoroughly analyzed, and mitigation steps or recommendations were determined so that they can be used in the future.***

***The skills and topics that were covered in these two weeks were: Analysis, Monitoring, Logging, Alert Response, IDS, Firewall Rules and Alert Response.***

### 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.**