

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:

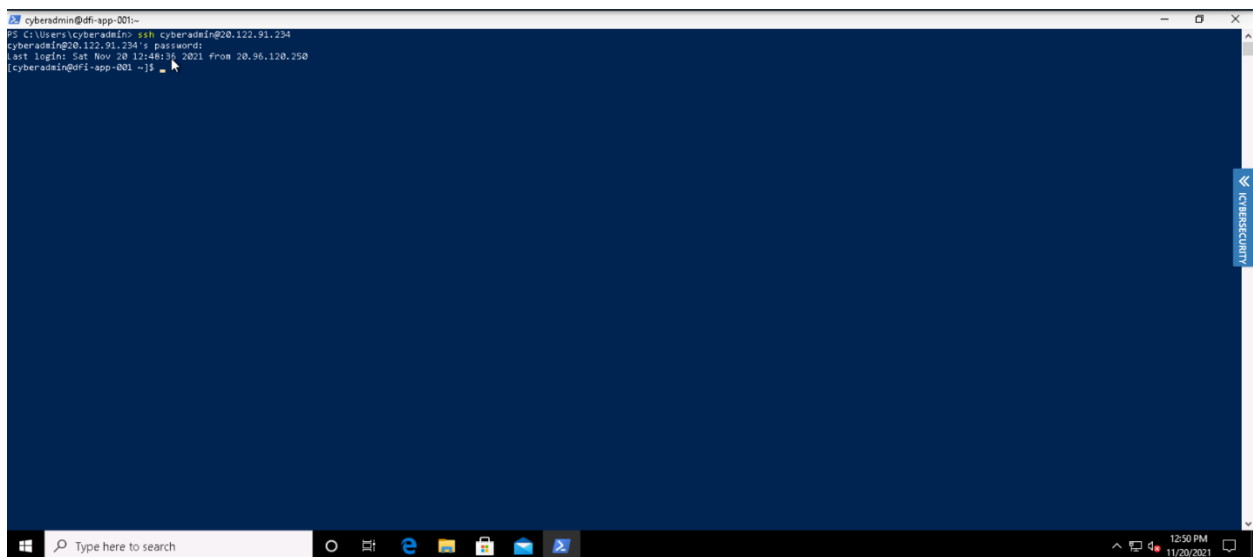
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

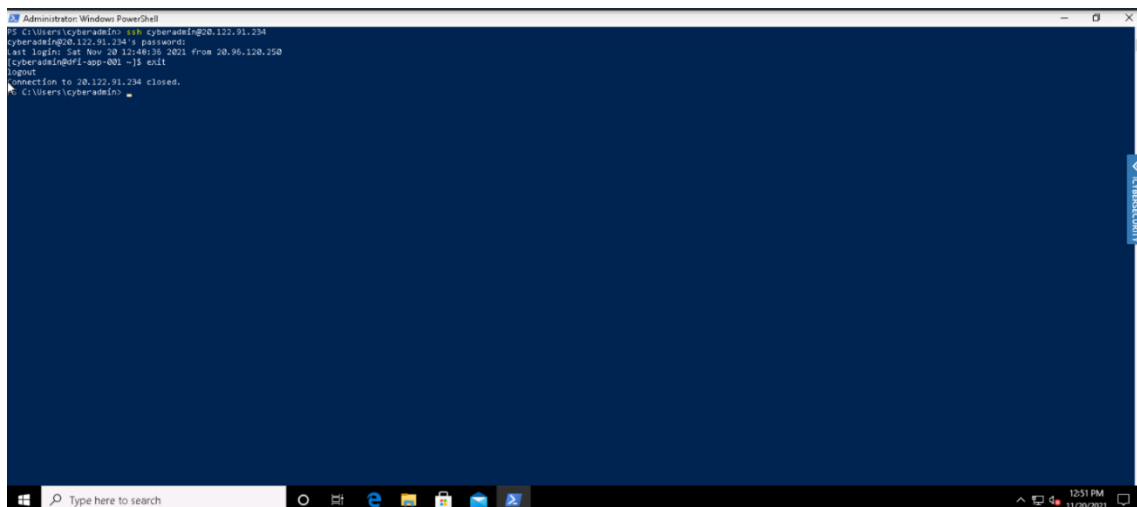
[Please Provide Screenshots of the RDP and SSH here as evidence that you completed this step.]

Type (windows powershell) on the search bar

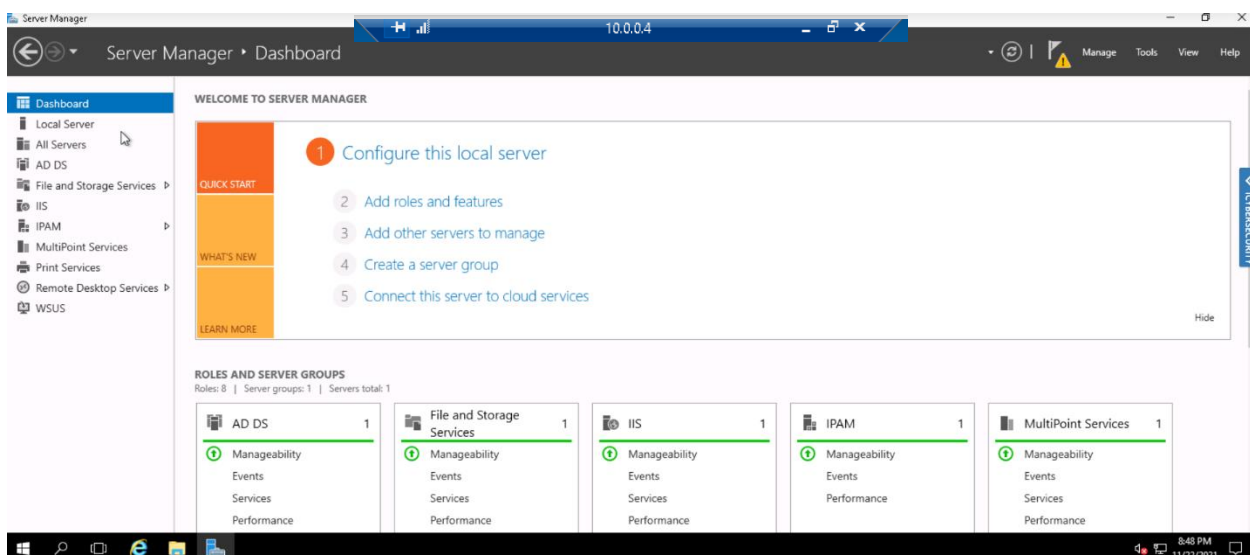
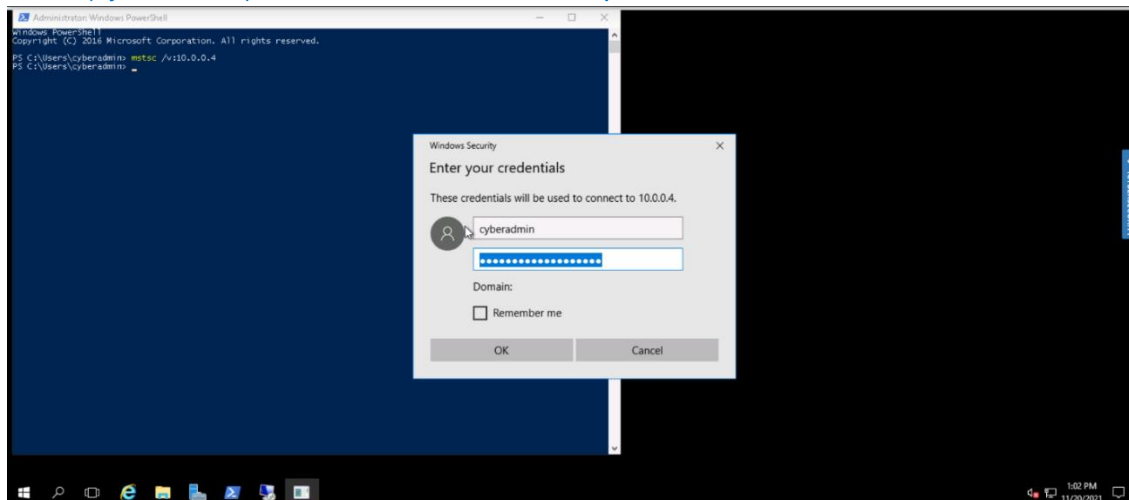
Right click on (windows powershell) and select (run as administrator)

Type “ssh [cyberadmin@20.122.91.234](#)”





For the remote desktop connection
Type "mstsc /v:10.0.0.4" in the windows powershell
Write (cyberadmin) as username and add the password



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]

Steps:

patch and upgrade the server application

remove or disable unnecessary services and applications

configure server using authentication

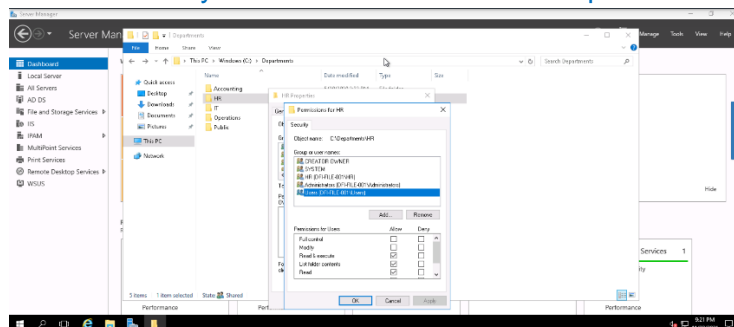
configure server resource controls

perform security testing on the server application

the first improvement that needs to be done to enable windows SmartScreen so that to prevent downloading malwares or malicious files that would run in the background without noticing

the second improvement to be done is to apply least privilege concept on the HR folder by only giving full control (administrative) access on that folder only to the trusted people like the owner and the admin

so users and system must be removed from permission list



the third improvement that needs to be taken in consideration is encryption.

bit locker needs to be enabled so that data would be encrypted by AES to assure that the data will not be accessed by an unauthorized person

the last improvement needs to be done is to change the UAC (which is the user account control setting) to always notify me when apps try to install or make changes to my computer or i make changes to my computer

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]

Code:

```
name 21.19.241.63 new-DFI-partner-WBC-International
```

```
name 172.21.30.44 DFI-File-001
```

```
access-list DFI-Ingress extended permit host new-DFI-partner-WBC-International host DFI-File-001 eq 9082
```

explanation:

first, we name (The partner's IP) "source" which is 21.19.241.63 to new-DFI-partner-WBC-International to enhance the code readability

we also name (DFI-File-001's IP) "destination" which is 172.21.30.44 to DFI-File-001 to be readable for any user

then the last syntax we need to break it down

firstly, access list to manage the traffic

secondly, DFI-Ingress is the interface for the rule

thirdly, we extend the permission to also include the host so that it can access files

fourthly, we add the source and the destination

lastly, we add the port number (9082) so that data can use this port to be accessed

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]

AES encryption is the best to be used. it is a type of symmetric encryption that is mandatory standard. all rest data and data in motion must be encrypted by AES

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]

Code:

```
alert icmp any any -> 172.21.30.44 any (msg: "high volume of ICMP traffic"; sid:1000001; rev:1;)
```

explanation:

alert rule when high volume of icmp traffic occurs

the protocol used is icmp

source ip address and source port are assigned to any
172.21.30.44 (destination)

destination port is assigned to any

when high volume of icmp traffic occurs the displayed message will be "high volume of ICMP traffic"

sid is to assigned any number larger than 1000000

[Place your VoIP Admin rule and explanation here]

Code:

```
alert udp any any -> 172.21.30.55 any (msg:"TFTP Connection attempt";  
sid:1000002; rev:1;)
```

explanation:

alert rule when TFTP Connection attempt is established

the protocol used is UDP

source ip address and source port are assigned to any

172.21.30.55 (destination)

destination port is assigned to any

when TFTP Connection attempt is established the displayed message will be "TFTP Connection attempt"

sid is assigned any number larger than 1000000

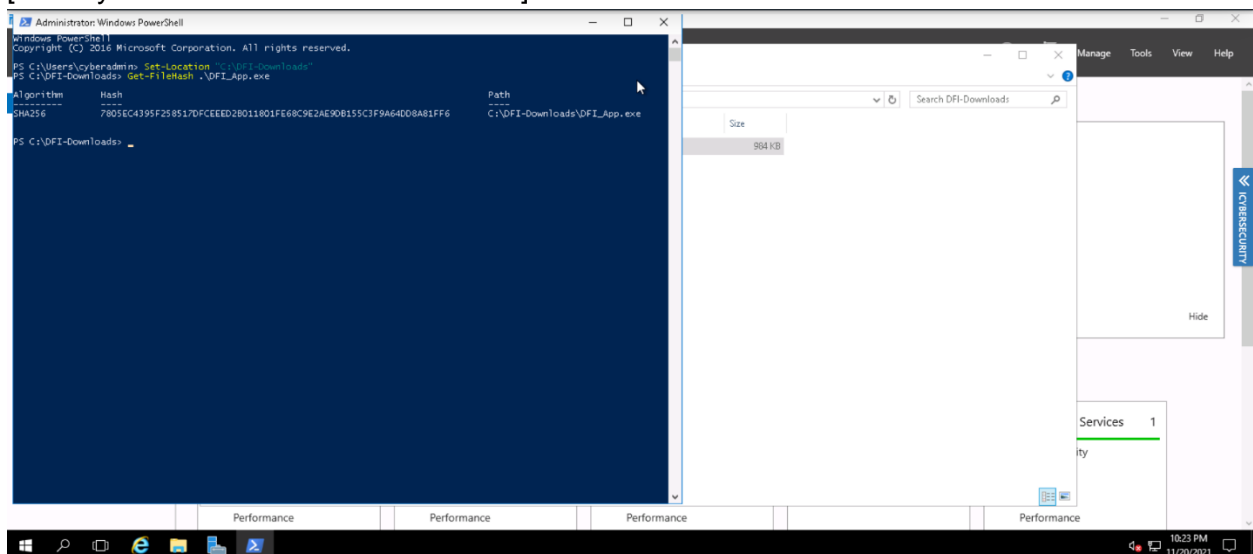
6. File Hash verification:

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:

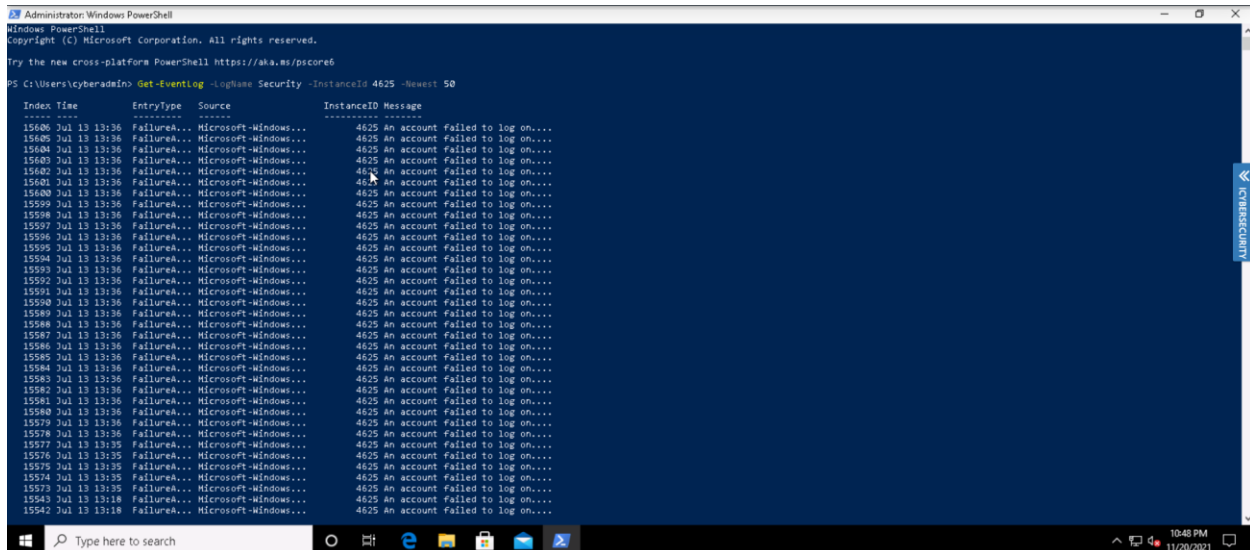
- SOAR products and specifically what could be done with them
- Automation of mitigation actions for IDS and firewall alerts.
- Feel free to elaborate on other areas that could be improved.

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
Security Orchestration, Automation and Response (SOAR)	collect data about security threats and respond to security incidents without human assistance	SOAR platforms are able to orchestrate operations across multiple security tools. They support automated security workflows, policy execution, and report automation, and are commonly used for automated vulnerability management and remediation
Robotic Process Automation (RPA)	automate low-level processes that do not require intelligent analysis	1) Scanning for vulnerabilities 2) Running monitoring tools and saving results 3) Basic threat mitigation for example adding a firewall rule to block a malicious IP
XDR	consolidate data from across the security environment, including endpoints, networks, and cloud systems, allowing it to identify evasive attacks that hide between security layers	1) automatically compile telemetry data into an attack story, giving analysts everything they need to investigate and respond to the incident 2) integrate with security tools to execute automated responses, making it a comprehensive automation platform for incident investigation and response

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]



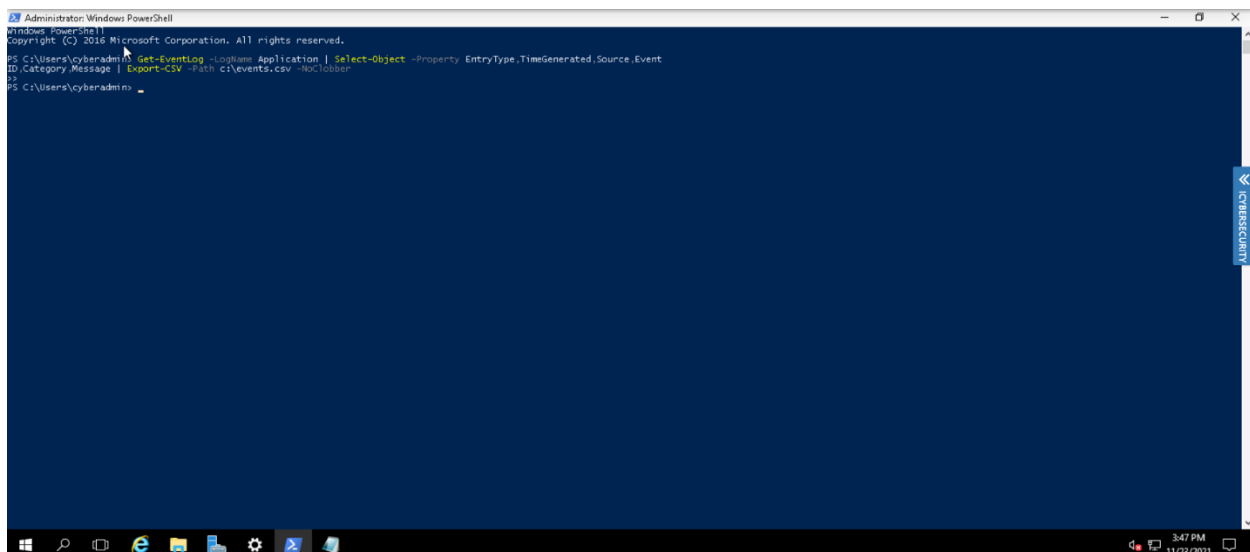
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\cyberadmin> Get-EventLog -LogName Security -InstanceId 4625 -Newest 50

Index Time          EntryType Source                                InstanceID Message
-----
15606 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15605 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15604 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15603 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15602 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15601 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15600 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15599 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15598 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15597 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15596 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15595 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15594 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15593 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15592 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15591 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15590 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15589 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15588 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15587 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15586 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15585 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15584 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15583 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15582 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15581 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15580 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15579 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15578 Jul 13 13:36 Failure... Microsoft-Windows... 4625 An account failed to log on...
15577 Jul 13 13:35 Failure... Microsoft-Windows... 4625 An account failed to log on...
15576 Jul 13 13:35 Failure... Microsoft-Windows... 4625 An account failed to log on...
15575 Jul 13 13:35 Failure... Microsoft-Windows... 4625 An account failed to log on...
15574 Jul 13 13:35 Failure... Microsoft-Windows... 4625 An account failed to log on...
15573 Jul 13 13:35 Failure... Microsoft-Windows... 4625 An account failed to log on...
15543 Jul 13 13:18 Failure... Microsoft-Windows... 4625 An account failed to log on...
15542 Jul 13 13:18 Failure... Microsoft-Windows... 4625 An account failed to log on...
```

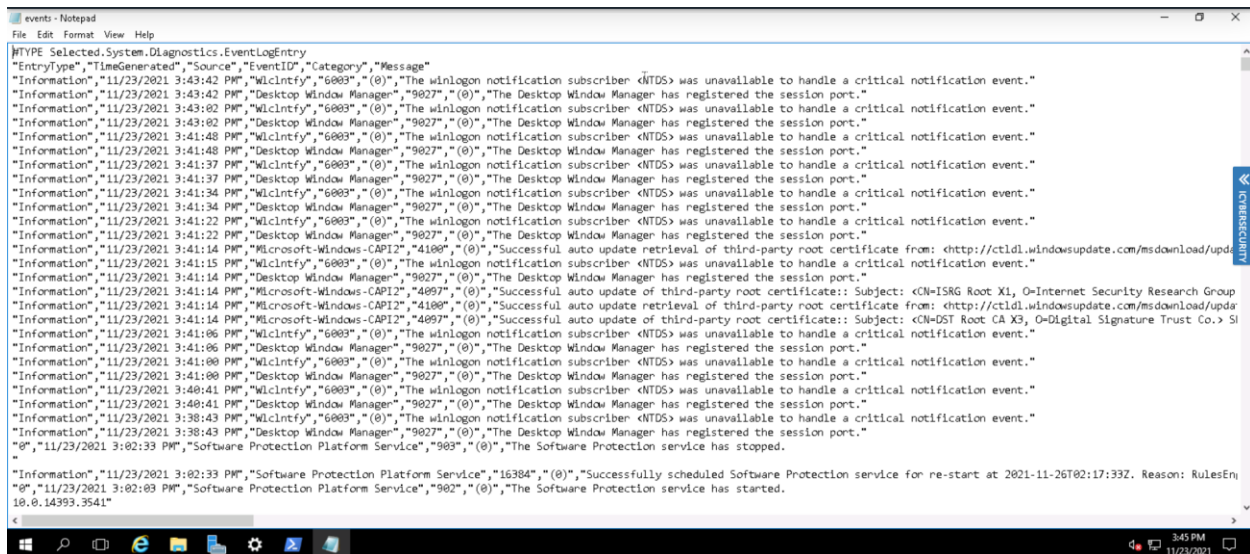
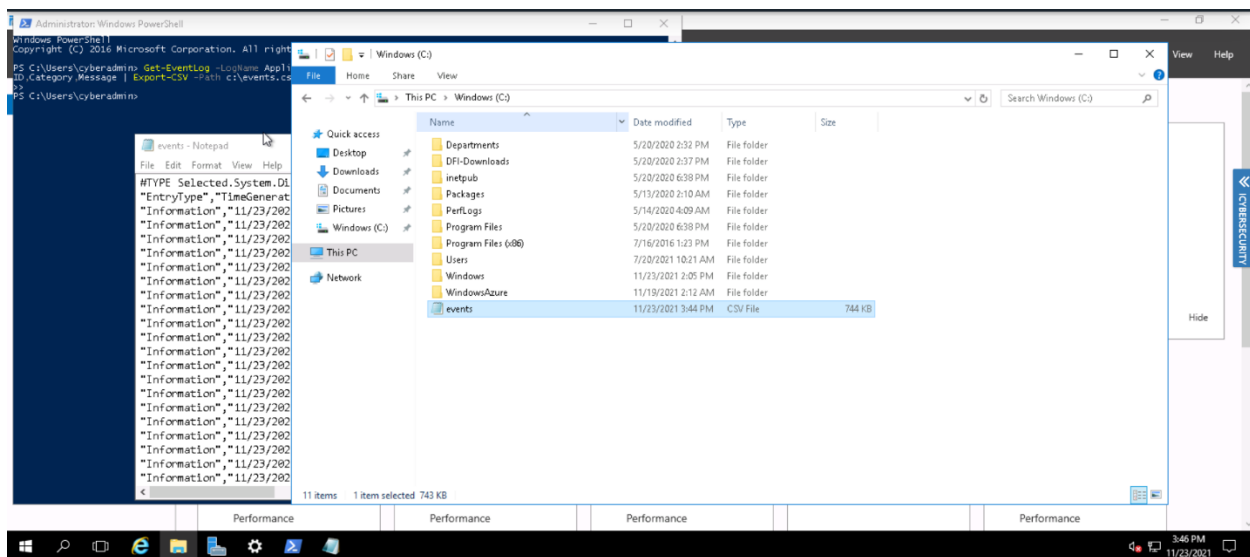
brute force attack is done to gain access to the system
to defend our system from such attack we should limit the failed login attempts
we can also remove the untrusted IP addresses from the firewall configuration



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

PS C:\Users\cyberadmin> Get-EventLog -LogName Application | Select-Object -Property EntryType,TimeGenerated,Source,EventID,Category,Message | Export-Csv -Path c:\events.csv -NoTypeInformation

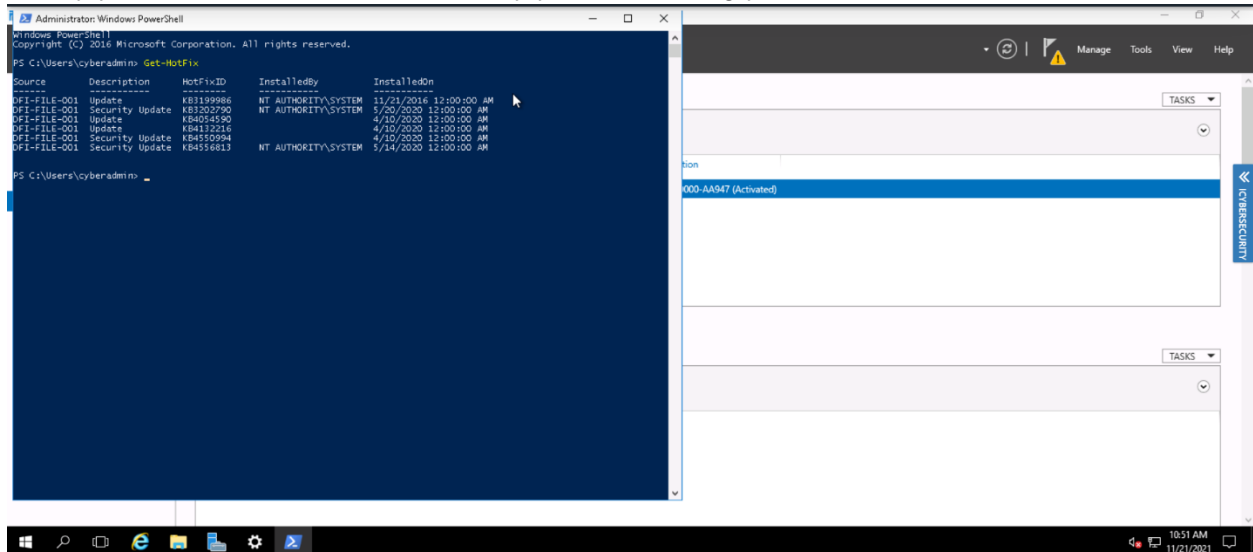
PS C:\Users\cyberadmin>
```

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
KB3199986	update	Brings stability improvements (servicing stack update)
KB3202790	Security update	Security update for adobe flash player
KB4054590	update	Microsoft .NET Framework 4.7.2 (feature packs)
KB4132216	update	Update for windows 10 for x86-based systems
KB4550994	Security update	Servicing stack update
KB4556813	Security update	OS Build 14393.3686
KB5003279	Ignore	Optional
KB4565483	Ignore	Optional improvements
KB4565351	Ignore	Optional Microsoft features

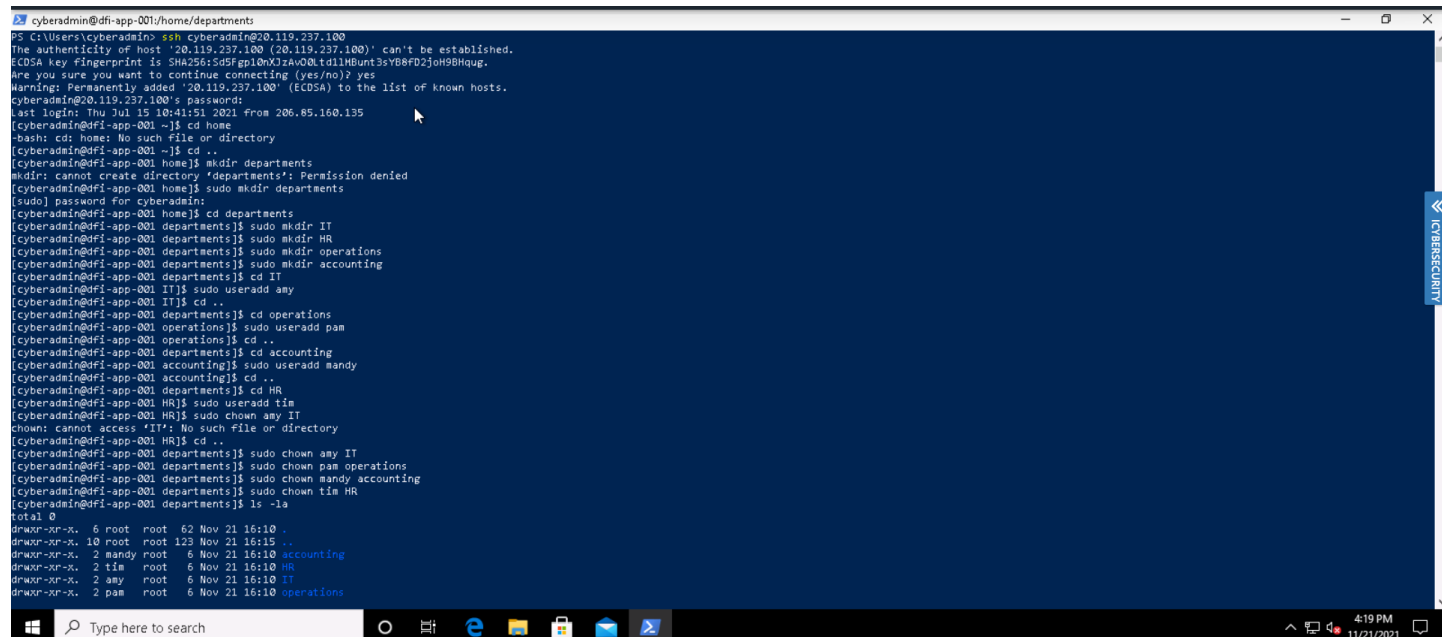
10. Linux Data Directories:

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/departments
PS C:\Users\cyberadmin> ssh cyberadmin@20.119.237.100
The authenticity of host '20.119.237.100 (20.119.237.100)' can't be established.
ECDSA key fingerprint is SHA256:5d5Fgp10xXjzAVQQLtd1lMBunt3yVB8FD2joh9BHqag.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '20.119.237.100' (ECDSA) to the list of known hosts.
cyberadmin@20.119.237.100's password:
Last login: Thu Jul 15 10:41:51 2021 from 206.85.160.135
[cyberadmin@dfi-app-001 ~]$ cd home
-bash: cd: home: No such file or directory
[cyberadmin@dfi-app-001 ~]$ cd ..
[cyberadmin@dfi-app-001 home]$ mkdir departments
mkdir: cannot create directory 'departments': Permission denied
[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]$ cd IT
[cyberadmin@dfi-app-001 IT]$ sudo useradd amy
[cyberadmin@dfi-app-001 IT]$ cd ..
[cyberadmin@dfi-app-001 departments]$ cd 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]$ sudo useradd mandy
[cyberadmin@dfi-app-001 accounting]$ cd ..
[cyberadmin@dfi-app-001 departments]$ cd HR
[cyberadmin@dfi-app-001 HR]$ sudo useradd tim
[cyberadmin@dfi-app-001 HR]$ sudo chown amy IT
chown: cannot access 'IT': No such file or directory
[cyberadmin@dfi-app-001 HR]$ cd ..
[cyberadmin@dfi-app-001 departments]$ sudo chown amy IT
[cyberadmin@dfi-app-001 departments]$ sudo chown pam operations
[cyberadmin@dfi-app-001 departments]$ sudo chown mandy accounting
[cyberadmin@dfi-app-001 departments]$ sudo chown tim HR
[cyberadmin@dfi-app-001 departments]$ ls -la
total 0
drwxr-xr-x. 6 root root 62 Nov 21 16:10 .
drwxr-xr-x. 10 root root 123 Nov 21 16:15 ..
drwxr-xr-x. 2 mandy root 6 Nov 21 16:10 accounting
drwxr-xr-x. 2 tim root 6 Nov 21 16:10 HR
drwxr-xr-x. 2 amy root 6 Nov 21 16:10 IT
drwxr-xr-x. 2 pam root 6 Nov 21 16:10 operations
```

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

First of all we established the connection by "ssh [cyberadmin@20.119.237.100](#)"

Then we used "cd .." to go back to home directory

Then we used "mkdir departments" to create a directory named departments

Then we used "cd departments" to enter the departments directory

Then we used "mkdir" to add four directories (IT, HR, operations, accounting)

Then used "cd IT" to enter the IT directory

Then used "sudo useradd amy" to add amy as a user in the IT directory

Then used "cd .." to go back to departments directory

Then used "cd operations" to enter the operations directory

Then used "sudo useradd pam" to add pam as a user in the operations directory

Then used "cd .." to go back to departments directory

Then used "cd accounting" to enter the accounting directory

Then used "sudo useradd mandy" to add mandy as a user in the accounting directory

Then used "cd .." to go back to departments directory

Then used "cd HR" to enter the HR directory

Then used "sudo useradd tim" to add tim as a user in the HR directory

Then used "cd .." to go back to departments directory

Then "sudo chown amy IT"

Then "sudo chown pam operations"

Then "sudo chown mandy accounting"

Then "sudo chown tim HR"

Finally used "ls -la" to get the feedback about what we done and ensure that each user can read/write/execute in his/her departmental folder

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 first thing to be apply two factor authentications so that to add another layer of security if by any means the password fall in the hand of an unauthorized person

The second improvement to be done is to eliminate bot's login by using captcha

The third and most important improvement is to limit both the number of failed logins attempts and the IP address to only include authorized ones

The last change that can be done is to prevent accessing the root via "ssh"

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]

First week -> First, we started by the connection via "ssh"

then we established a remote desktop connection via mstsc

after that we recommended some security analysis such as: (enabling windows SmartScreen, applying least privilege, data encryption by bit locker, and changing the UAC to always notify me upon any changes done)

moreover, we added firewall rules by accessing list to manage the traffic with the use of DFI-INGRESS interface and extending the permission of accessing files to source and destination hosts through port number 9082

we also recommended the use of AES encryption which is a symmetric encryption type

IDS rules was also added to alert when high volume of icmp traffic occurs and TFTP connection attempt is detected

we have done a file hash verification

Second week -> we added some DFI areas/technologies such as (incident response, number of logins and monitoring apps)

we will use cyber fusion to protect the system against malwares

we will limit number of failed logins to assure to brute force attack is done

and finally, we will monitor the apps to prevent any background unwanted running task

we categorized the updates need to be done on a table with a justification for each update

we created directories to IT, HR, operations and accounting under the departments directory

and gave the right access for each user to his/her specific department

we suggested four improvements for the firewall alert response which are (two factor

authentications, eliminating bots login by using captcha, limiting both number of failed logins

and the IP address to only include the authorized one, prevent accessing the root using "ssh")

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.