

Scenario:

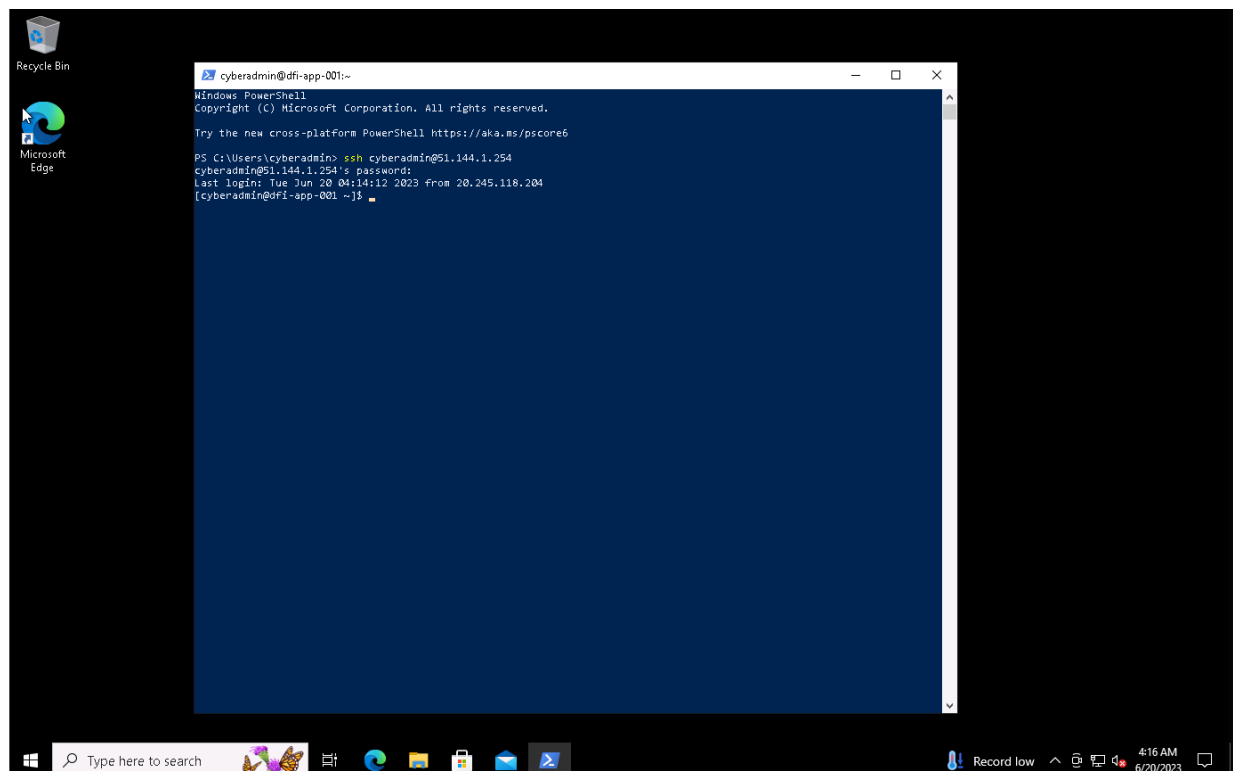
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

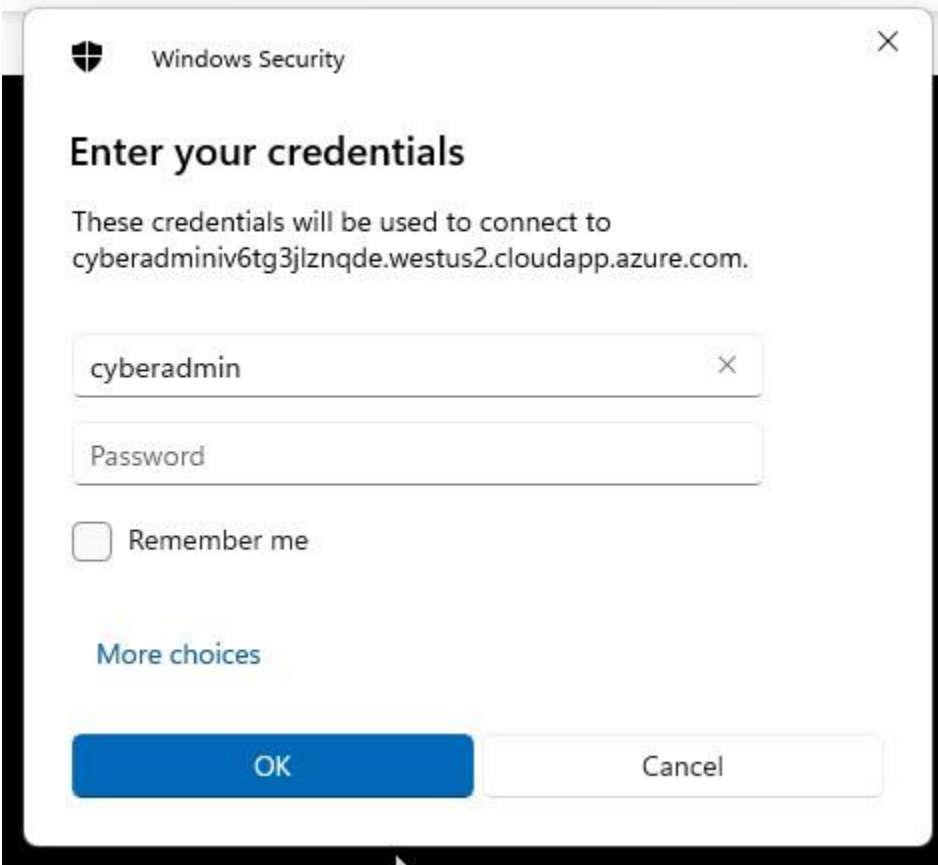
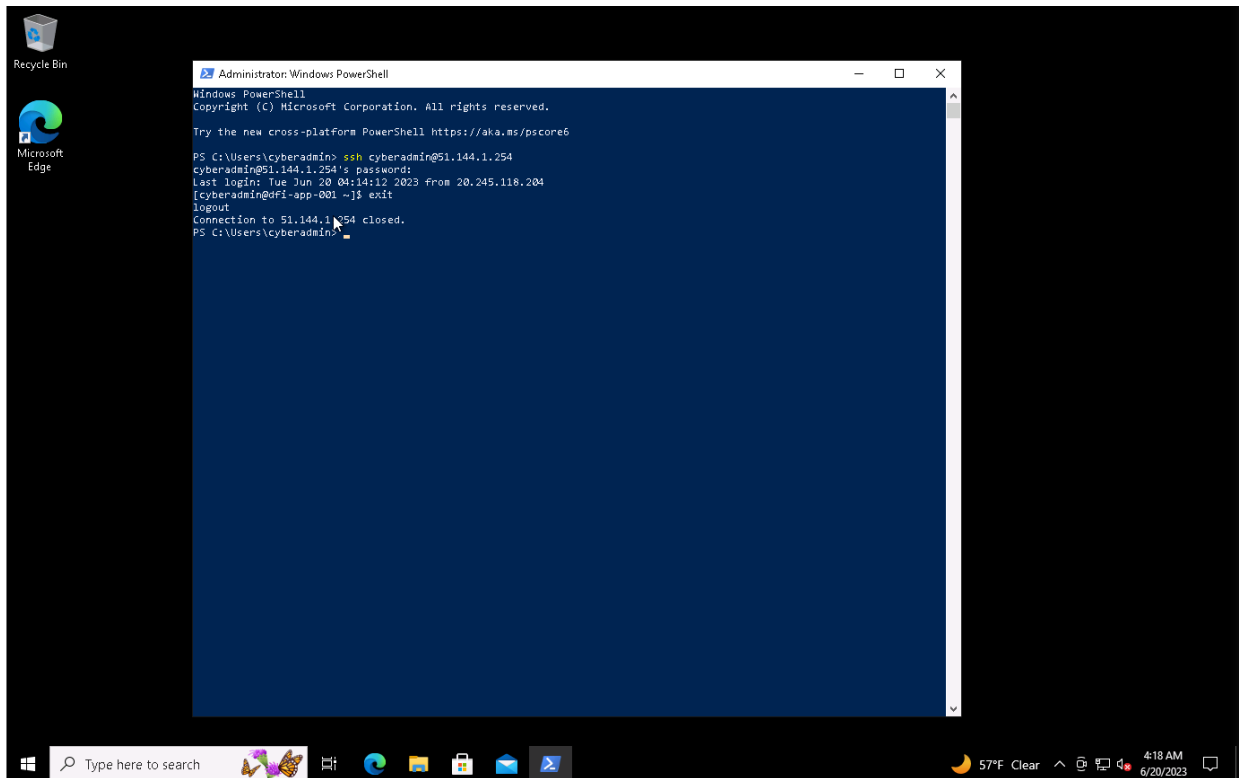
Week One:

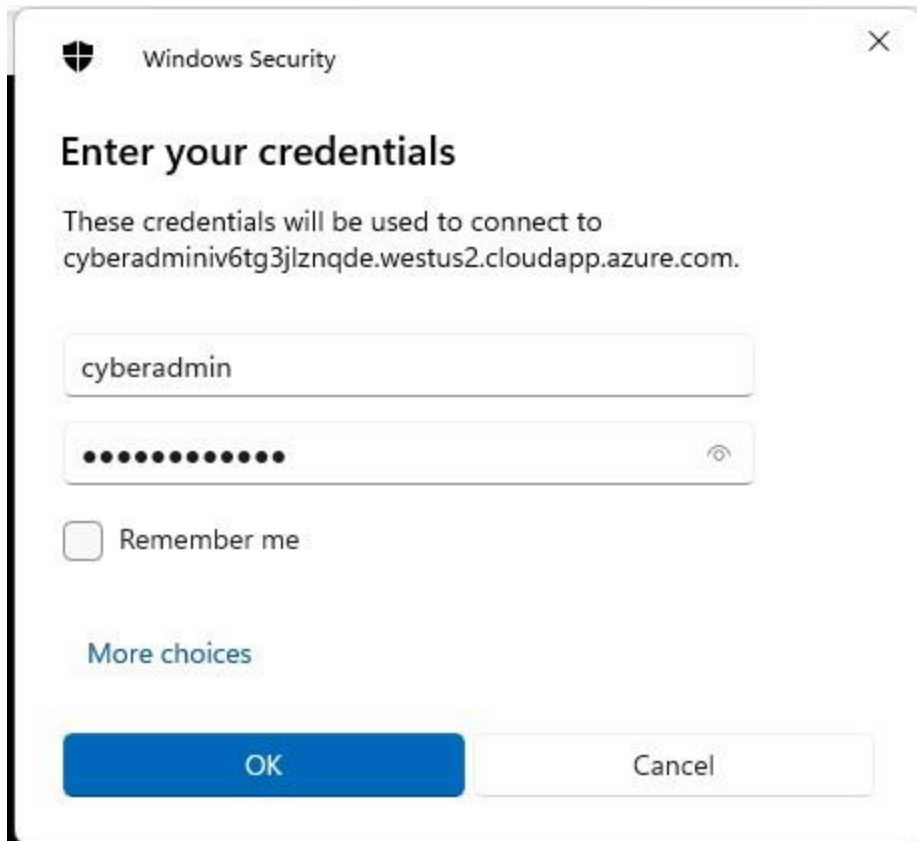
1. Connect:

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](#). [NIST 800-123](#) (other NIST documents could also apply.)

[Place your security analysis here]

- The windows have not been updated, this means that certain patches wouldn't have been fixed. It could also lead to open ports and possibly be vulnerable to any recent threats that can be handled only by the updated version.
- Virus and Threat protection was turned off which leads to the system being more vulnerable and being unprotected the system might have also been affected by virus already
- The user account control settings were placed in the mode "never notify" for making any changes to windows and any installation of apps, I changed it to "always notify" especially since hackers might take advantage of the previous mode and install malicious apps which would act as a backdoor
- Through backdoors hackers would have easy access to the resources within the computer
- To see various users and their privileges on the computer, we can use computer management app on windows to manage the users who can access the computer along with their permissions
- The folders present in the computer might contain some important information for the organization hence those folders permission must be changed
- When changing permissions of the folder, we are controlling who has the ability to access such folder and so we must make sure that all these folder's permissions must be changed so that only HR and IT admins would have access and normal users in the system won't have the authority to access (in other words they would need to know the password when they try to open the folders)

Settings

Home

Find a setting

Update & Security

Windows Update

Delivery Optimization

Windows Security

Backup

Troubleshoot

Recovery

Activation


Find my device

For developers

Windows Insider Program

Windows Update

***Some settings are managed by your organization**
[View configured update policies](#)

**Updates available**
Last checked: Today, 4:06 AM

Your device is missing important security and quality fixes.

Windows Malicious Software Removal Tool x64 - v5.114 (KB890830)
Status: Pending install

2023-06 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5027538)
Status: Pending install

2023-06 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5027215)
Status: Pending install

2023-04 Update for Windows 10 Version 22H2 for x64-based Systems (KB4023057)
Status: Pending install

Install now

Adjust active hours to reduce disruptions

We noticed you regularly use your device between 11:00 AM and 4:00 AM. Would you like Windows to automatically update your active hours to match your activity? We won't restart for updates during this time.

Turn on

Pause updates for 7 days
Get latest updates to pause again

Install updates as soon as possible

Looking for info on the latest updates?
[Learn more](#)

Related links

[Check Storage](#)

[OS build info](#)

Help from the web

[Installing Windows 11 on eligible devices](#)

[Troubleshooting Windows Update problems](#)

[More about Windows 11](#)

Get help

Give feedback

Windows Security

Home

Virus & threat protection

Account protection

Firewall & network protection

App & browser control

Device security


Device performance & health

Family options

Settings


Security at a glance


See what's happening with the security and health of your device and take any actions needed.


**Virus & threat protection**
Set up OneDrive for file recovery options in case of a ransomware attack.

Set up OneDrive

Dismiss

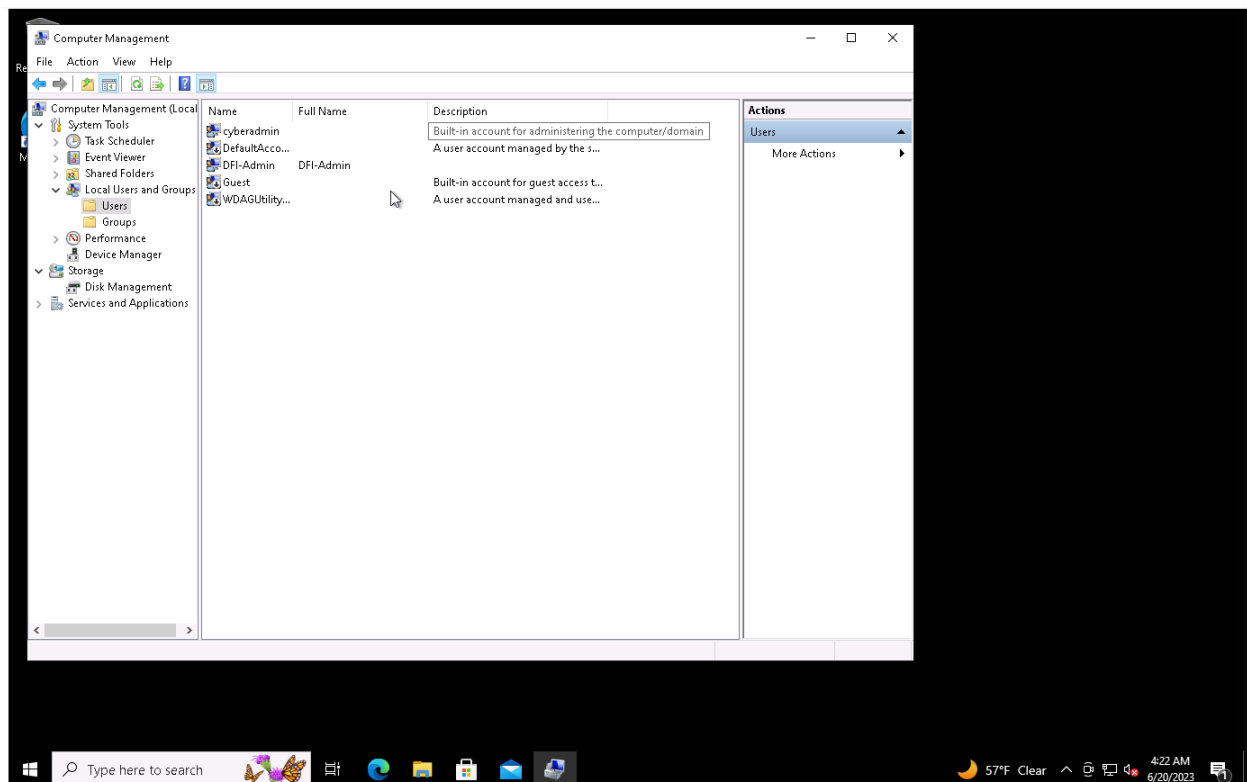
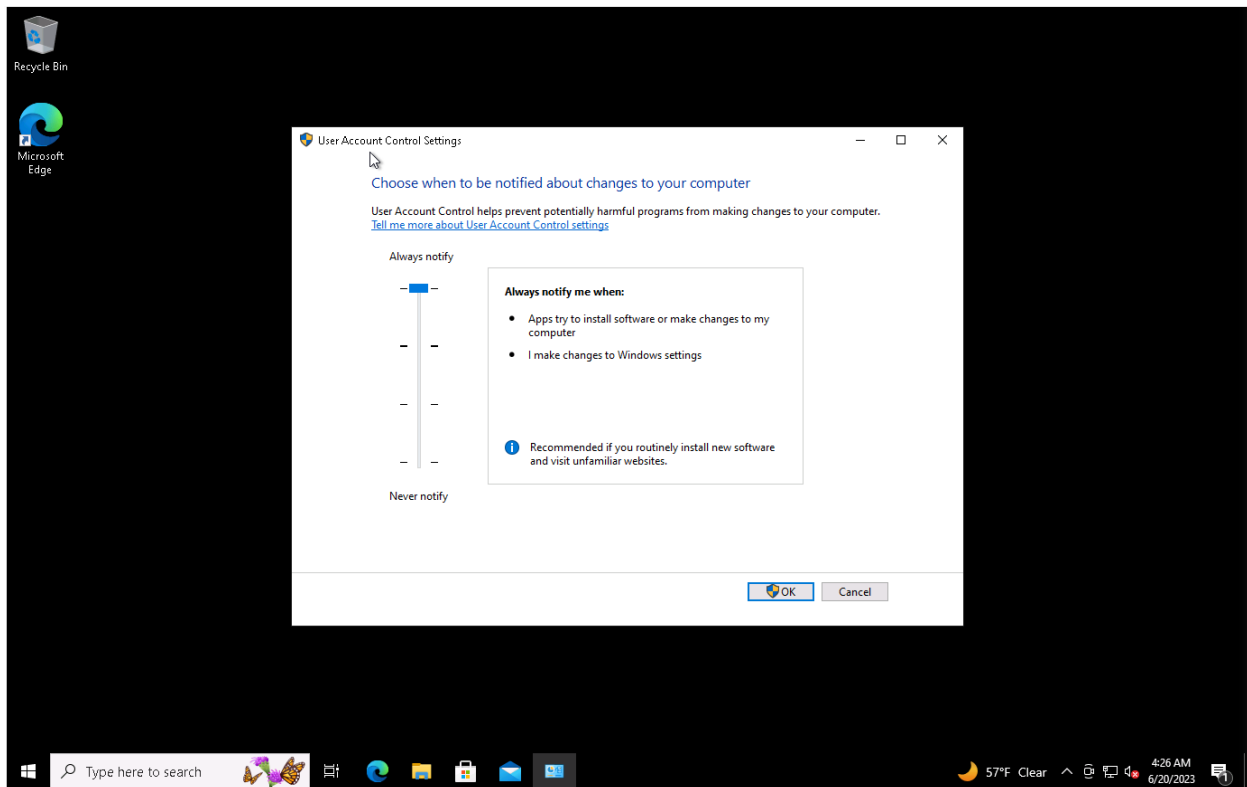
**Account protection**
No action needed.

**Firewall & network protection**
No action needed.

**App & browser control**
The setting to block potentially unwanted apps is turned off. Your device may be vulnerable.

Turn on

Dismiss



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
```

access-list: will control the traffic that occurs in firewall

DFI-Ingress: an internal interface

Extended permit: it has ability to match the traffic (aka source and destination address)

Tcp: we would be following the TCP protocol

host 21.19.241.63: This would be our source IP address

host 172.21.30.44: This would be our destination IP address

eq 9082: "equal to" the tcp port 9082

In simple terms, we are creating a firewall rule where the source IP given above wants to access data from the destination IP and this can be done through the port 9082 by using DFI-Ingress as our internal interface.

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]

I would suggest using a symmetric key because the same key would be used for encryption and decryption. Types of Symmetric Encryption:

- AES Advanced Encryption Standard - it uses blocked algorithm, it also shuffles data around for total of 9 rounds making it complicated and secure
- Twofish - It also uses XOR algorithm but it differs in the way it shuffles data compared to AES and finally it is usually used in e-commerce website to secure all the payments made
- RC4 Rivest Cipher 4 - It combines the random stream with plaintext however its retired

Using the Symmetric key is very fast and that's why i would recommend using this key

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;)
```

Alert - alert would be generated

Icmp - the traffic it handles

any - Source IP

any (2) - Source port #

-> - direction

172.21.30.44 - destination IP

any(3) - Destination port
(msg: "ICMP traffic detected"; sid:1000006; rev:1;) - Rule options

[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;)

Alert - alert would be generated

Udp - the type of traffic it handles

any - Source IP

any (2) - Source port #

-> - direction

172.21.30.55 - destination IP

Any (3) - destination port

(msg:" Connection attempted via TFTP"; sid:1000008; rev:1;) - Rule options

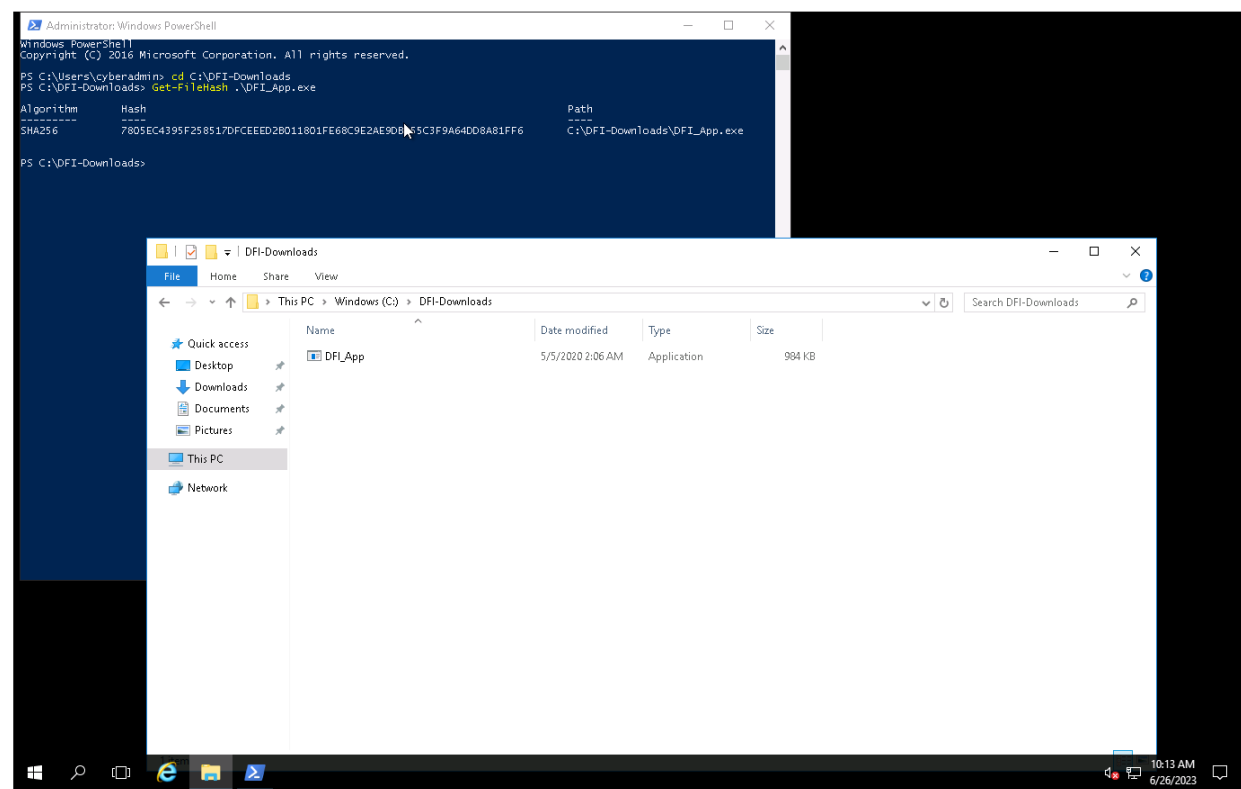
6. File Hash verification:

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 must be a limit to the amount of wrong login attempts(kind of like a lock where after certain attempts it will not allow the user to enter any credentials for a certain period)	If there isn't any limit then the login credentials can easily be compromised by brute-force attacks and it would violate confidentiality and integrity of the system.
Monitoring Firewalls	There could be an application that identify all the traffic that goes in and out of firewall (because firewall can't exactly say if a traffic is good or not)	Similarly to spam finder in emails, we would be able to have some data about past bad traffic and further increase the security of our organization
Detecting infections in the network	We need to automatically detect the threats that is present in the network and give us alerts	It will help us prevent any further spread within the network and allows us to handle with such threats at an early stage

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]

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs: Security

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

Task category:

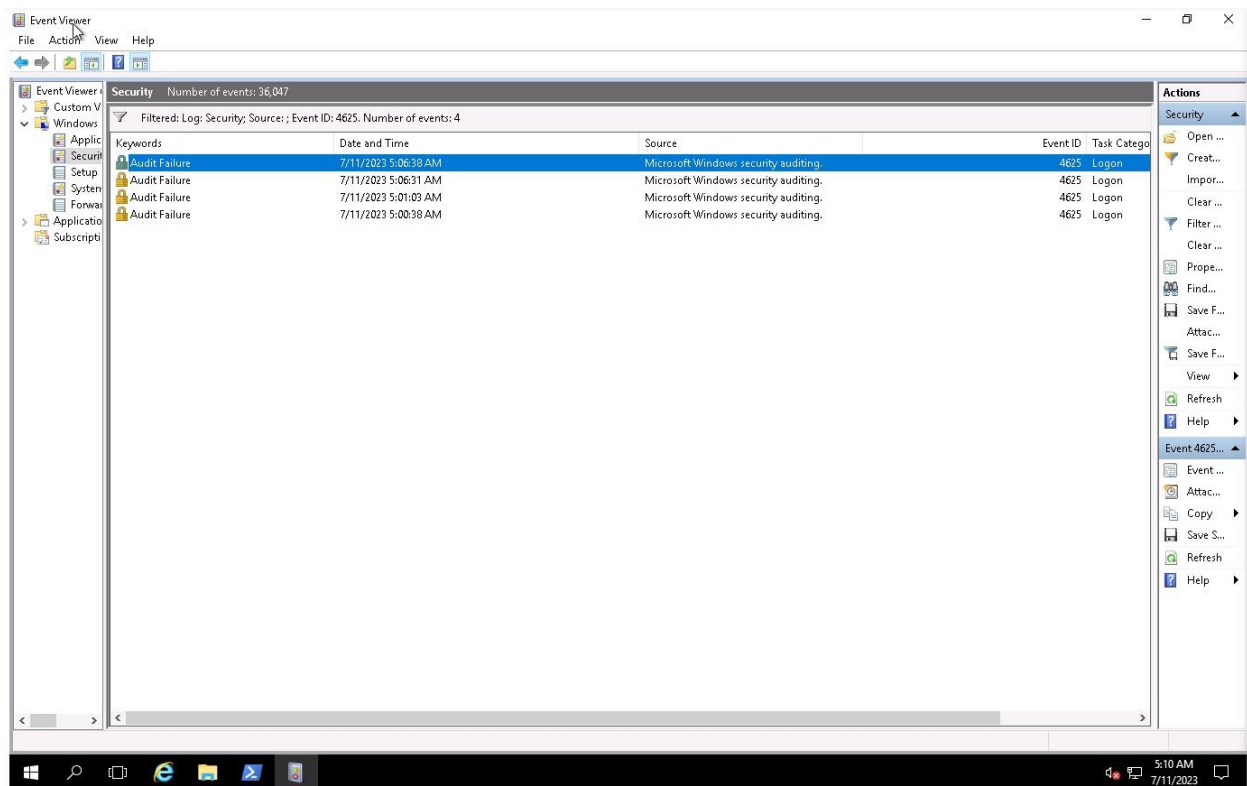
Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel



This is all the audit failure you would be seeing in Event Viewer. It indicates all the failed attempts to log in. It shows that there is no limit to the amount of login attempts and it could possibly be compromised by Brute Force attacks. Therefore, we need some limit to the amount of incorrect login attempts that can be made. We should also be able to identify the IP that is potentially breaching 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-2023-33137	Update	It is a vulnerability in remote code execution. This is a very important update as it helps us to safely access other desktop remotely without having our information compromised
CVE-2023-3217	Ignore	It is not a important severity and it is related to WebXR
CVE-2023-33139	Update	It is a very important severity and it will disclose all the sensitive information of the users and it would violate the confidentiality
CVE-2019-1483	Update	It has a high severity and this vulnerability can be easily exploited if the hackers have an easy way to access the victim computer and change their privileges to an admin to install backdoors and possibly damage all the data present
CVE-2023-2941	Ignore	It has a low severity where the vulnerability is

		present in the extension API in google chrome
CVE-2023-2938	Ignore	Although the severity is medium, it's basically inappropriate implementation in Picture in Picture in google chrome

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
login as: cyberadmin
cyberadmin@172.176.142.229's password:
Last login: Wed Jun 28 06:54:21 2023 from 115.99.52.126
[cyberadmin@dfi-app-001 ~]$ pwd
/home/cyberadmin
[cyberadmin@dfi-app-001 ~]$ cd..
-bash: cd..: command not found
[cyberadmin@dfi-app-001 ~]$ cd ..
[cyberadmin@dfi-app-001 home]$ pwd
/home
[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 HR
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Public
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir IT
[cyberadmin@dfi-app-001 Departments]$ sudo mkdir Operations
[cyberadmin@dfi-app-001 Departments]$ ls
Accounting HR IT Operations Public
[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]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ sudo chown Amy IT
[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
[cyberadmin@dfi-app-001 Departments]$ ls -la
total 0
drwxr-xr-x. 7 root root 76 Jun 28 07:01 .
drwxr-xr-x. 10 root root 123 Jun 28 07:05 ..
drwxr-xr-x. 2 Mandy root 6 Jun 28 07:01 Accounting
drwxr-xr-x. 2 Tim root 6 Jun 28 07:01 HR
drwxr-xr-x. 2 Amy root 6 Jun 28 07:01 IT
drwxr-xr-x. 2 Pam root 6 Jun 28 07:01 Operations
drwxr-xr-x. 2 root root 6 Jun 28 07:01 Public
[cyberadmin@dfi-app-001 Departments]$
```

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

First, we create a root directory called "Home", under "Home" we have "Department" folder. Inside the "Department" we have HR, Accounting, Public, IT and Operations. Then, multiple users with unique permissions are created and the permissions are for accessing certain directories.

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]

- As there is many attempts for Brute Force Attacks, we should have a limit to the amount of times every user have to make incorrect attempts at logging in
- We should be able to make firewall rules to allow only certain IP addresses to the systems and it makes it more secure and prevents any sort of unauthorized connections
- There should be a two way verification factor, in case all the credentials are exploited, the hacker would still need to pass the second verification to prove that they are that person and it would be much more harder to access the computers
- Captchas would be a great way to reduce Brute Force Attacks as it's not always humans performing these Brute Force Attacks, it's the bots that tries to overload the system by spamming multiple request, therefore captchas can act as a layer of protection from these bots
- To further block the IP that could potentially be a threat to our organization, we can add that IP address to the blacklist
- Packet filtering also can be considered as a mitigation strategy by inspecting all the packets and it will block certain packets if they have incorrect source address information.
- Using VPN would also add an extra layer of protection and encrypts data from third party

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, I was able to establish a safe connection between Windows and CentOS. I was running a small security check on the computer such as the notification settings, if the windows were properly updated and i had to turn the windows virus defender on. Certain group permissions have also been modified where I recommended that only Admin group must have access to all the files and groups like HR,IT must have only permission to access their respective files. I also made firewall rules to improve the firewall security by allowing only certain company partners. I was able to recommend the best VPN encryption to improve the confidentiality of the organization. I made some IDS rules in order to monitor the traffic and connections that are made within the organization. File hash verification was done for the file provided by the software vendor. Security Logs were analyzed and recommendations were made. All the windows updates are checked and classified as which ones are necessary to be updated or not. Lastly, the firewall reports were analyzed and mitigation steps were recommended. I would recommend the organization to follow the following security policies: 800-41R1(Firewall) and 800-123(for server handling and monitoring). I would recommend that in order to make the product more secure they must follow the encryption procedures to encrypt the files so it would be accessible to only the authorized people. Second thing I would recommend would be hashing the file whenever received as it helps us see if no information has been modified.

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.