أشبال مصر الرقمية

DECI Cybersecurity Level 3

Term 2 – Project Template

Securing a Computer System

Scenario:

Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position.

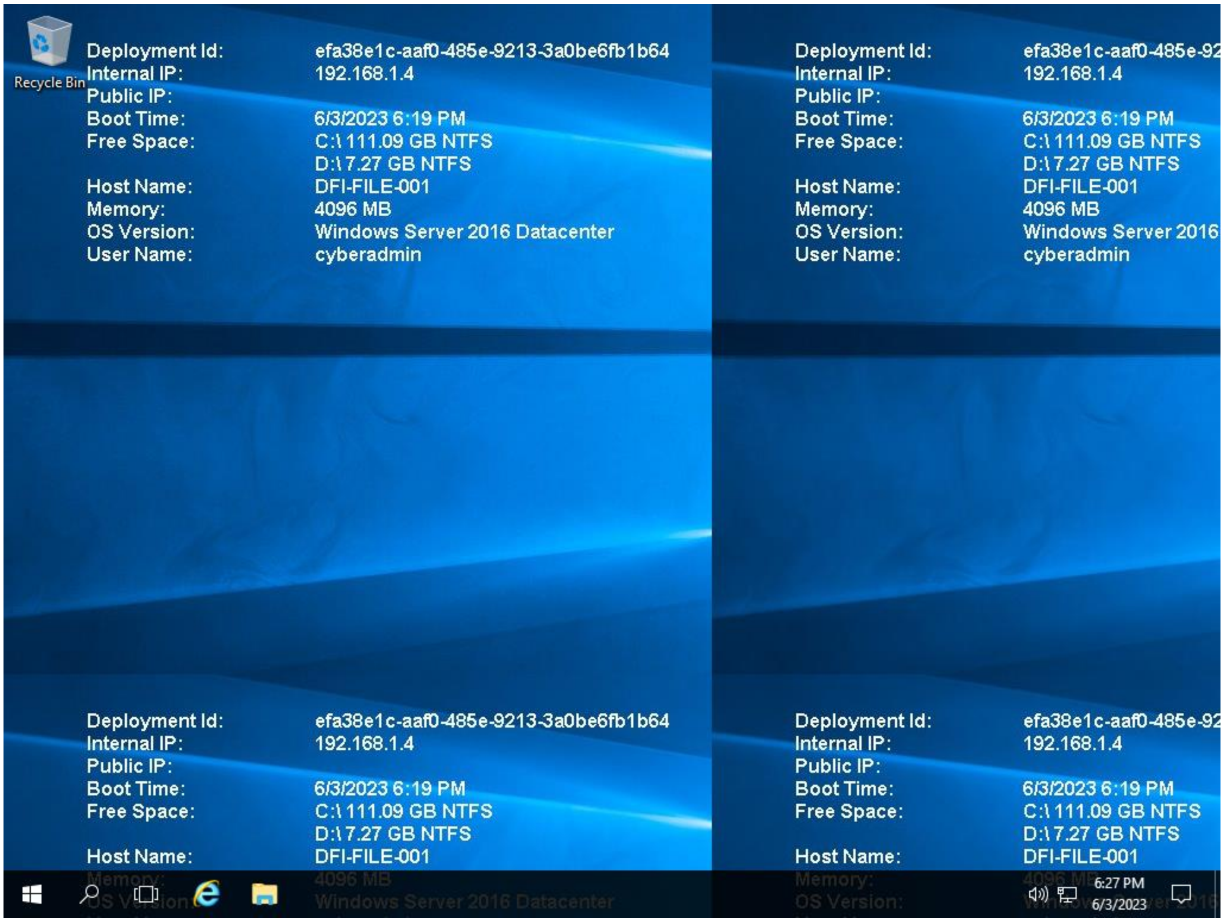
Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as our first InfoSec employee!

Once you are settled in and finished orientation we have your first 2-Weeks assignments ready.

1. Connect – Instructions

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 servers provided using RDP and SSH (via PowerShell) respectively.

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

RDP to Windows Server


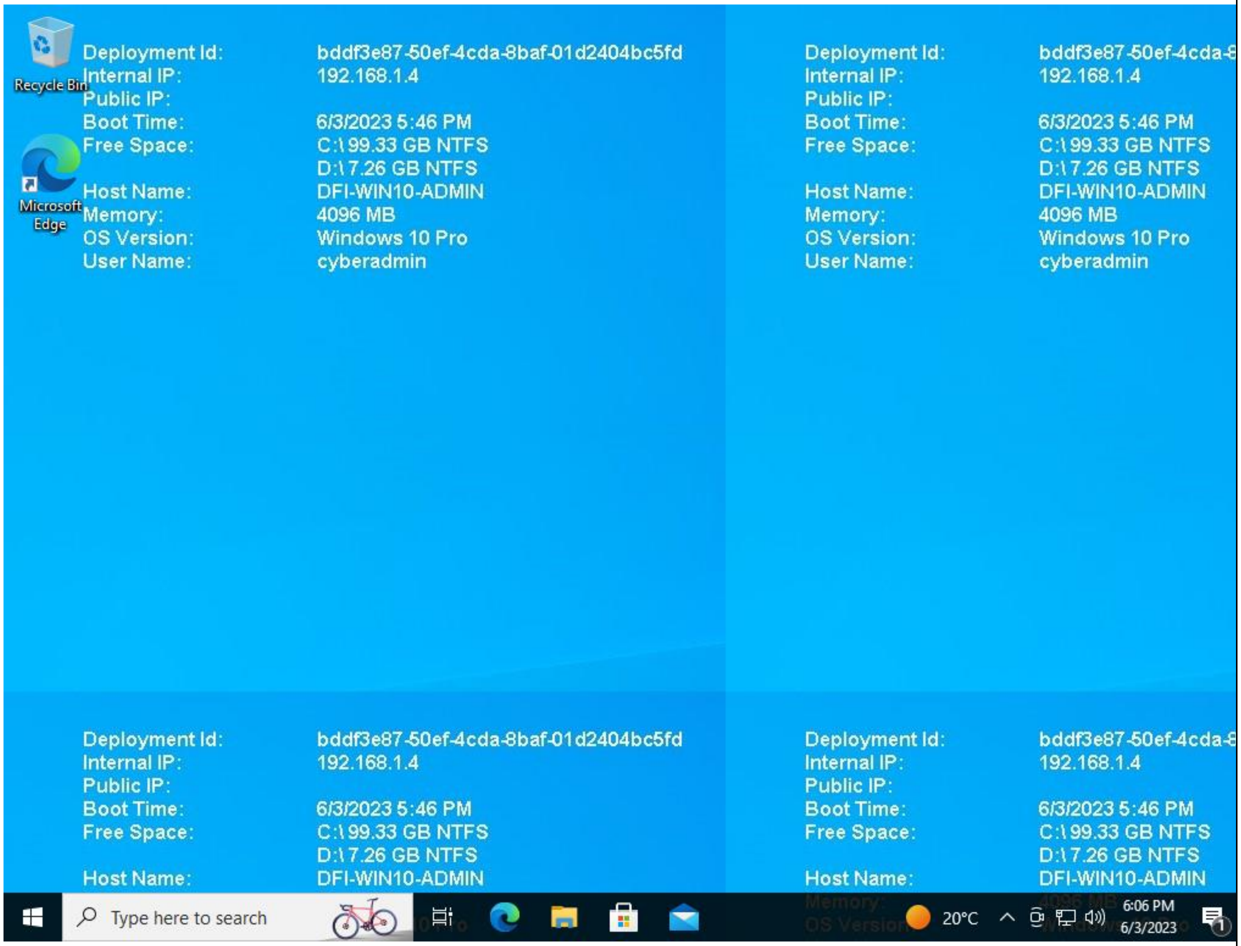
```
Deployment Id:     efa38e1c-aaf0-485e-9213-3a0be6fb1b64
Internal IP:       192.168.1.4
Public IP:
Boot Time:         6/3/2023 6:19 PM
Free Space:        C:\ 111.09 GB NTFS
                   D:\ 7.27 GB NTFS
Host Name:         DFI-FILE-001
Memory:            4096 MB
OS Version:        Windows Server 2016 Datacenter
User Name:         cyberadmin
```

```
Deployment Id:     efa38e1c-aaf0-485e-92
Internal IP:       192.168.1.4
Public IP:
Boot Time:         6/3/2023 6:19 PM
Free Space:        C:\ 111.09 GB NTFS
                   D:\ 7.27 GB NTFS
Host Name:         DFI-FILE-001
Memory:            4096 MB
OS Version:        Windows Server 2016
User Name:         cyberadmin
```

```
Deployment Id:     efa38e1c-aaf0-485e-9213-3a0be6fb1b64
Internal IP:       192.168.1.4
Public IP:
Boot Time:         6/3/2023 6:19 PM
Free Space:        C:\ 111.09 GB NTFS
                   D:\ 7.27 GB NTFS
Host Name:         DFI-FILE-001
Memory:            4096 MB
OS Version:        Windows Server 2016 Datacenter
```

```
Deployment Id:     efa38e1c-aaf0-485e-92
Internal IP:       192.168.1.4
Public IP:
Boot Time:         6/3/2023 6:19 PM
Free Space:        C:\ 111.09 GB NTFS
                   D:\ 7.27 GB NTFS
Host Name:         DFI-FILE-001
Memory:            4096 MB
OS Version:        Windows Server 2016
```

RDP to Windows 10



```
Deployment Id:    bddf3e87-50ef-4cda-8baf-01d2404bc5fd
Internal IP:      192.168.1.4
Public IP:
Boot Time:        6/3/2023 5:46 PM
Free Space:       C:\ 99.33 GB NTFS
                  D:\ 7.26 GB NTFS
Host Name:        DFI-WIN10-ADMIN
Memory:           4096 MB
OS Version:       Windows 10 Pro
User Name:        cyberadmin
```

```
Deployment Id:    bddf3e87-50ef-4cda-8
Internal IP:      192.168.1.4
Public IP:
Boot Time:        6/3/2023 5:46 PM
Free Space:       C:\ 99.33 GB NTFS
                  D:\ 7.26 GB NTFS
Host Name:        DFI-WIN10-ADMIN
Memory:           4096 MB
OS Version:       Windows 10 Pro
User Name:        cyberadmin
```

```
Deployment Id:    bddf3e87-50ef-4cda-8baf-01d2404bc5fd
Internal IP:      192.168.1.4
Public IP:
Boot Time:        6/3/2023 5:46 PM
Free Space:       C:\ 99.33 GB NTFS
                  D:\ 7.26 GB NTFS
Host Name:        DFI-WIN10-ADMIN
```

```
Deployment Id:    bddf3e87-50ef-4cda-8
Internal IP:      192.168.1.4
Public IP:
Boot Time:        6/3/2023 5:46 PM
Free Space:       C:\ 99.33 GB NTFS
                  D:\ 7.26 GB NTFS
Host Name:        DFI-WIN10-ADMIN
Memory:           4096 MB
OS Version
```

2. Security Analysis Instructions

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 (5 sentences at least) 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.)

Write your analysis here.

After Analyzing the windows machine I found that:

- Most users are administrators, violating the Principle of least privilege PoLP concept
- Passwords are not secure and don't meet the best security practices for password creation
- Some users have shared passwords, where a user has the exact same password as the other
- Passwords file is shared to the network, violating the confidentiality in the CIA

By analyzing the events I found the following security-violating events:

ID	Task Category	Count
0	Login failure	107
1	Inbound SSH failure	98
3	Unauthorized access attempt	98
4	Malicious software detected	97
5	Suspicious network activity detected	95
6	Password policy violation	109
7	Failed audit attempt	109
8	User account locked out	105
9	Privilege escalation attempt	96

3. Firewall Rules – Instructions

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 in 2-3 sentences the syntax for non-technical management on the change control board that meets weekly.

Write the text of your firewall rules

```
name 21.19.241.63 WBC
name 172.21.30.44 DFI-File-001
access-list DFI-Ingress extended permit tcp host WBC host DFI-File-001 eq 9082
```

We could also directly use:

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

Write the text of your firewall rule explanation

To create a firewall rule, I named the two IP objects using the *name* command to be easily referred to using their names instead of retyping the IP addresses again and again (IP address is an address used to identify network devices).

After this, I used the ***access-list*** command to create the rule, I used DFI-Ingress as an interface to and then allowed access using ***extended permit***, then I specified the protocol used to be **tcp** and declared the source and destination after the keyword ***host*** using the objects I created which are WBC and DFI-File-001 and lastly I specified the port used to be 9082

4. VPN Encryption Recommendation Instructions and Evidence

DFI is creating a payroll processing partnership with Payroll-USA, this will involve creating a VPN connection between the two.

Research, and in **not less than 5 sentences**, 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

VPN Encryption Recommendation

VPN is needed to establish secure connections to secure communications and data exchange

I recommend AES-256 as an encryption solution supported by Cisco AnyConnect VPN and uses the latest encryption for Cisco.

Justification:

- AES 256 is resistant to brute-force attacks, side-channel attacks, and cryptanalysis
- AES 256 Uses Symmetric Keys
- AES-256 is also widely supported by hardware and software vendors, making it compatible with various platforms and devices.
- much faster than asymmetric methods
- AES-256 uses 14 rounds of encryption
- it is widely used and trusted by governments, financial institutions, and other organizations around the world
- it has been extensively studied and tested, and no major weaknesses have been found in its design.

Recommended Hash algorithm: SHA256 algorithm

Justification: it is a stronger hash function that is currently considered to be secure against collision attacks

Recommended Key exchange algorithm: RSA algorithm

Justification: RSA is more secure because it provides authentication, widely used, is relatively fast and efficient, making it suitable for use in real-time applications.

5. IDS Rule – Instructions

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 in 3-5 sentences for non-technical management on the change control board that meets weekly

DDOS IDS Rule

```
alert icmp any any -> 172.21.30.44 any (msg:” Possible DDOS attack!”; sid: 10000006;)
```

DDOS IDS Rule explanation for non-technical management

The IDS rule above is used to detect DDoS attacks by alerting on receiving high volume ICMP traffic

- first we have the *alert* keyword and then the protocol used which is *icmp*,
- the next two parameters are the source IP and the source port which I have set to *any* to include any source IP and any source port,
- the *->* sign refers to the direction of the traffic,
- the following two parameters are the destination IP of the server and the destination port, again set to any
- and lastly the message to be included on the alert and a unique ID for the rule

VOIP IDS Rule

```
alert tftp any any -> 172.21.30.55 any (msg:” Connection attempt to the primary VoIP server!”; sid: 10000005;)
```

VOIP IDS Rule explanation for non-technical management

The IDS rule above is used to detect connection attempts to the primary VoIP server

- first we have the *alert* keyword and then the protocol used which is *tftp*,
- the next two parameters are the source IP and the source port which I have set to *any* to include any source IP and any source port,
- the *->* sign refers to the direction of the traffic,
- the following two parameters are the destination IP of the server and the destination port, again set to any
- and lastly the message to be included on the alert and a unique ID for the rule

6. File Hash Verification – Instructions

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.

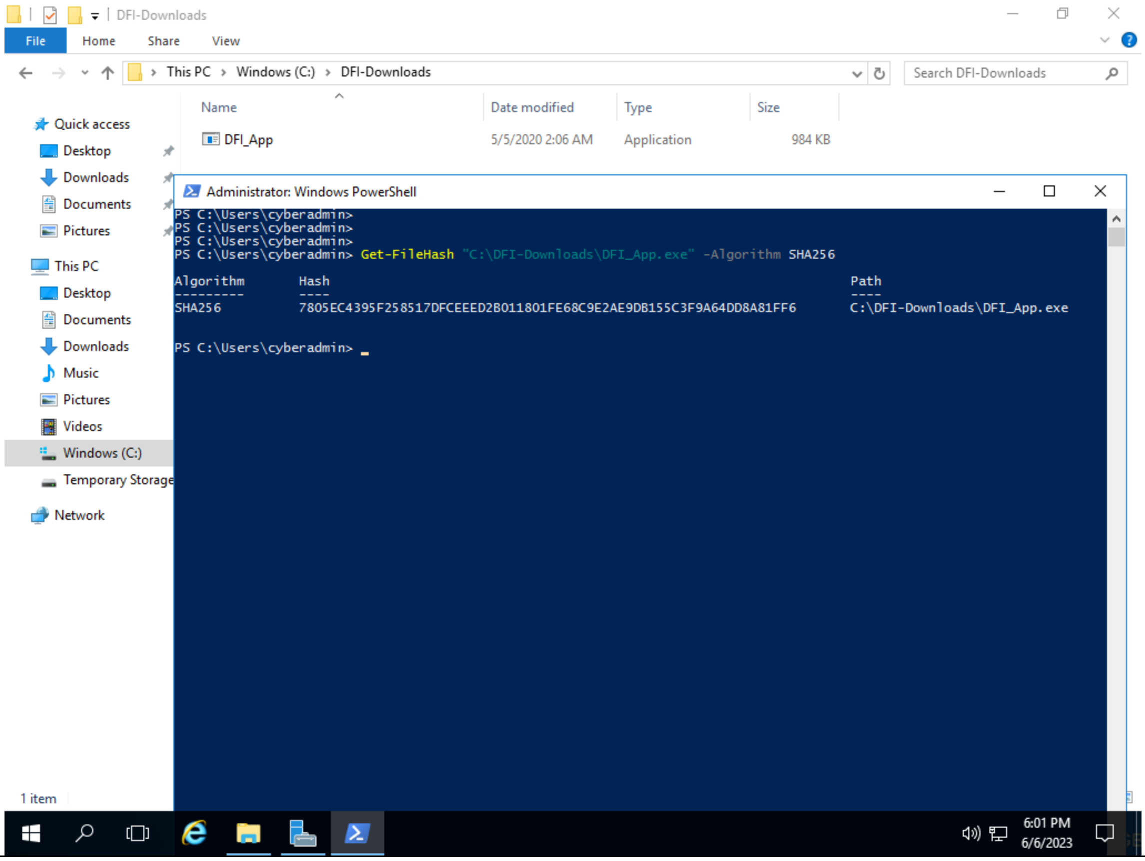
Hash:

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.

Screenshot of the File verification process (Type Date before and after the verification)
Integrity verified! the two hashes match.



Name	Date modified	Type	Size
DFI_App	5/5/2020 2:06 AM	Application	984 KB

```
PS C:\Users\cyberadmin>
PS C:\Users\cyberadmin>
PS C:\Users\cyberadmin>
PS C:\Users\cyberadmin> Get-FileHash "C:\DFI-Downloads\DFI_App.exe" -Algorithm SHA256

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


PS C:\Users\cyberadmin> _
```

7. Automation - Instructions

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.

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 on the next slide including the area/technology within DFI and a proposed solution, with a minimum of 3 areas. Provide a brief explanation (at least one sentence each) for your choices.

DFI Area/Technology	Solution	Justification for Recommendation
Vulnerability scanning	Nessus	✓ Nessus features high-speed asset discovery, configuration auditing, target profiling, malware detection, sensitive data discovery and more.
Simulating attacks	Metasploit	✓ Metasploit makes it easy to automate all phases of a penetration test, from choosing the right exploits to streamlining evidence collection and reporting.
Managing permissions	Chef	✓ Chef manages the infrastructure by writing code rather than using a manual process so that it can be automated, tested and deployed very easily ✓ Chef has Client-server architecture and it supports multiple platforms like Windows, Ubuntu, Centos, and Solaris etc. ✓ It can manage a variety of node types, including servers, cloud virtual machines, network devices and containers

Playbook Creation	Ansible	✓ Ansible is Free and Open Source ✓ It is a simple Automation Software ✓ It models all your infrastructure by describing interrelation of your systems. ✓ It uses SSL to connect the servers.
Incident response	Splunk Phantom	✓ The most valuable feature of Splunk Phantom that stands out is it has a great SOAR. ✓ The automation and orchestration module is highly mature. ✓ A lot of use cases are on user entity and behavioral analytics (UEBA), which is artificial intelligence and machine learning-based (AIML). ✓ Technical support is helpful.

8. Logging RDP Attempts - Instructions

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

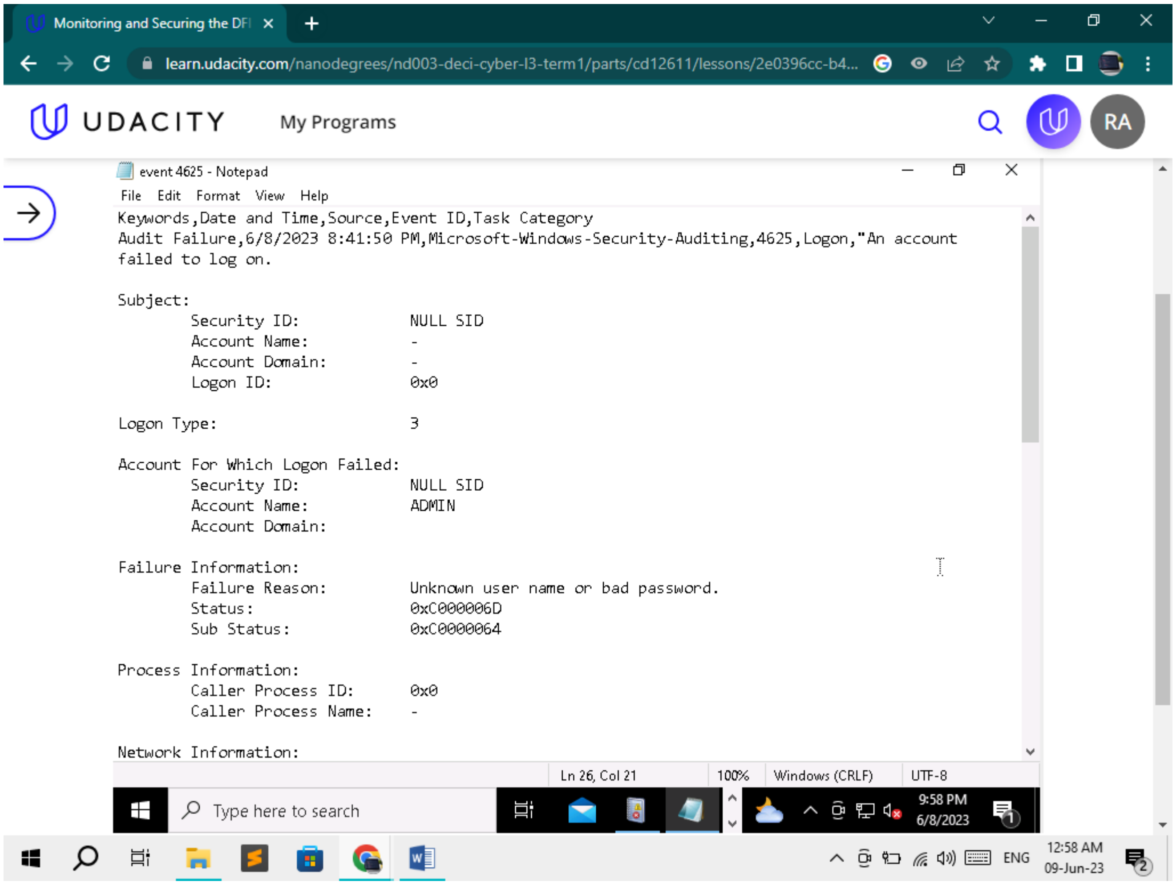
Prepare a report that lists unsuccessful attempts in connecting over the last 24-hours. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

For your deliverable, open the CSV with Notepad and take a screenshot from your personal computer for your explanation.

Then in 3-5 sentences, explain your findings, recommendations and justifications to the IT Manager.

Place your screenshot on the following slide and the explanation on the slide after your screenshot.

Place your screenshot below


Monitoring and Securing the DFI
learn.udacity.com/nanodegrees/nd003-deci-cyber-l3-term1/parts/cd12611/lessons/2e0396cc-b4...
UDACITY
My Programs
RA
event 4625 - Notepad
File Edit Format View Help
Ln 26, Col 21
100%
Windows (CRLF)
UTF-8
Type here to search
9:58 PM
6/8/2023
ENG
12:58 AM
09-Jun-23

```
Keywords,Date and Time,Source,Event ID,Task Category
Audit Failure,6/8/2023 8:41:50 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:		ADMIN
	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:	-

Network Information:
```

Write your 3-5 sentence explanation of your findings, recommendations, and justifications to the IT manager below.

After analyzing the Event logs through filtering and exporting, I found only one event with the ID 4625.

So having only one failed RDP logon attempt isn’t considered a problem but in case of more attempts it’s better to follow the next recommendations (justifications are provided with each recommendation):

- Change your passwords regularly, make them complex to be hard to be guessed
- Use multifactor authentication, to make it harder for the system to be compromised
- Limit logon attempts to avoid brute force attacks, where a user is locked out after a certain number of failed logon attempts
- Use the firewall to block unauthorized access

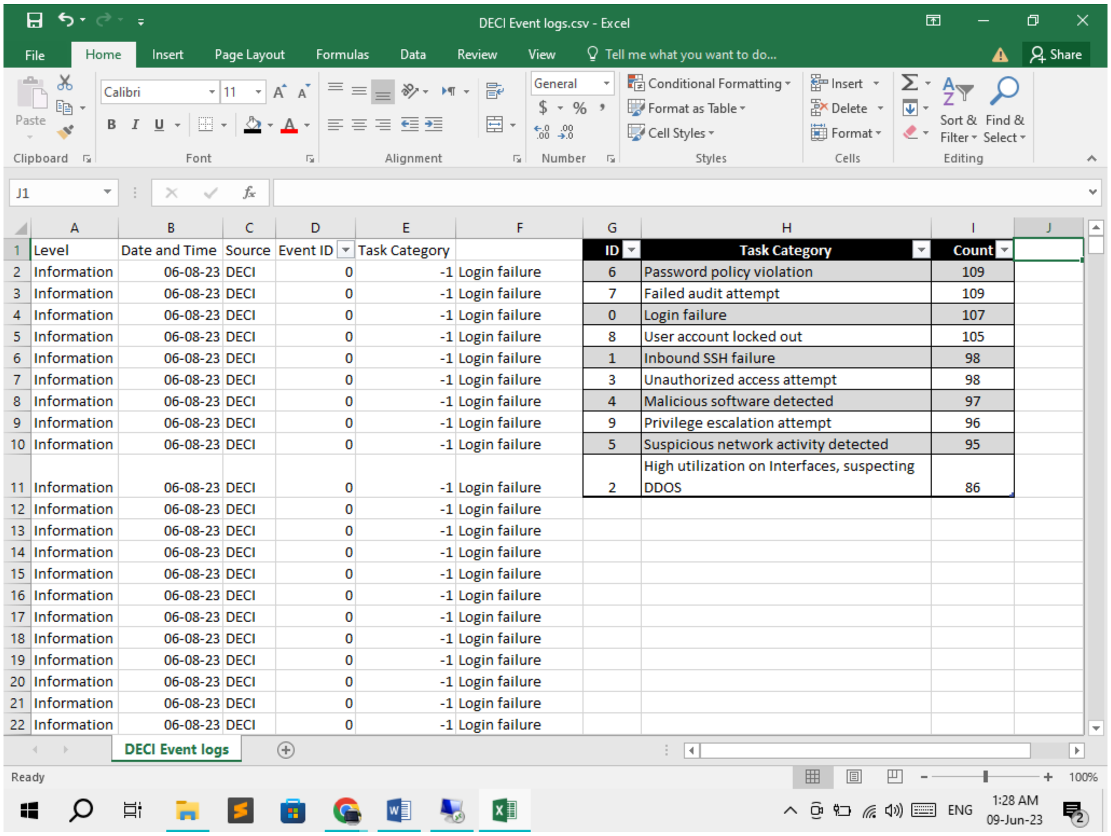
Prepare a report that lists security attacks detected in windows 10 application logs. Using Powershell or Eventviewer, search the Windows Security Log for Event 4625. Export to CSV.

For your deliverable, open the CSV with Notepad and take a screenshot from your personal computer for your explanation.

Then in 3-5 sentences, explain your findings, recommendations and justifications to the IT Manager.

Place your screenshot on the following slide and the explanation on the slide after your screenshot.

Place your screenshot below



	A	B	C	D	E	F
1	Level	Date and Time	Source	Event ID	Task Category	
2	Information	06-08-23	DECI	0	-1	Login failure
3	Information	06-08-23	DECI	0	-1	Login failure
4	Information	06-08-23	DECI	0	-1	Login failure
5	Information	06-08-23	DECI	0	-1	Login failure
6	Information	06-08-23	DECI	0	-1	Login failure
7	Information	06-08-23	DECI	0	-1	Login failure
8	Information	06-08-23	DECI	0	-1	Login failure
9	Information	06-08-23	DECI	0	-1	Login failure
10	Information	06-08-23	DECI	0	-1	Login failure
11	Information	06-08-23	DECI	0	-1	Login failure
12	Information	06-08-23	DECI	0	-1	Login failure
13	Information	06-08-23	DECI	0	-1	Login failure
14	Information	06-08-23	DECI	0	-1	Login failure
15	Information	06-08-23	DECI	0	-1	Login failure
16	Information	06-08-23	DECI	0	-1	Login failure
17	Information	06-08-23	DECI	0	-1	Login failure
18	Information	06-08-23	DECI	0	-1	Login failure
19	Information	06-08-23	DECI	0	-1	Login failure
20	Information	06-08-23	DECI	0	-1	Login failure
21	Information	06-08-23	DECI	0	-1	Login failure
22	Information	06-08-23	DECI	0	-1	Login failure

ID	Task Category	Count
6	Password policy violation	109
7	Failed audit attempt	109
0	Login failure	107
8	User account locked out	105
1	Inbound SSH failure	98
3	Unauthorized access attempt	98
4	Malicious software detected	97
9	Privilege escalation attempt	96
5	Suspicious network activity detected	95
2	High utilization on Interfaces, suspecting DDOS	86

Write your 3-5 sentence explanation of your findings, recommendations, and justifications to the IT manager below.

After exporting the events from the source DECI I found that the highest 3 DECI events are:

- Event ID: 6, Password policy violation
- Event ID: 7, Failed audit attempt
- Event ID: 0, Login failure

In addition to the recommendations in the previous task (about failed logon attempts), I would also recommend keeping the system up-to-date and making awareness notes or sessions for the users on how to create secure and strong passwords

9. Windows Update - Instructions and Evidence

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.

Available Updates	Solution	Justification for recommendation
2023-05 Cumulative Update for Windows 10 Version 22H2 for x64-based Systems (KB5026361)	needed	Max. Severity : Important
2023-02 Cumulative Update for .NET Framework 3.5, 4.8 and 4.8.1 for Windows 10 Version 22H2 for x64 (KB5022729)	needed	Max. Severity : Critical
2023-03 Servicing Stack Update for Windows Server 2016 for x64-based Systems (KB5023788)	needed	Max. Severity : Critical
Windows Malicious Software Removal Tool x64 - v5.113 (KB890830)	Not needed	Max. Severity : Moderate severity

10. Data Directories – Instructions

The IT Manager has requested your help with creating directories (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

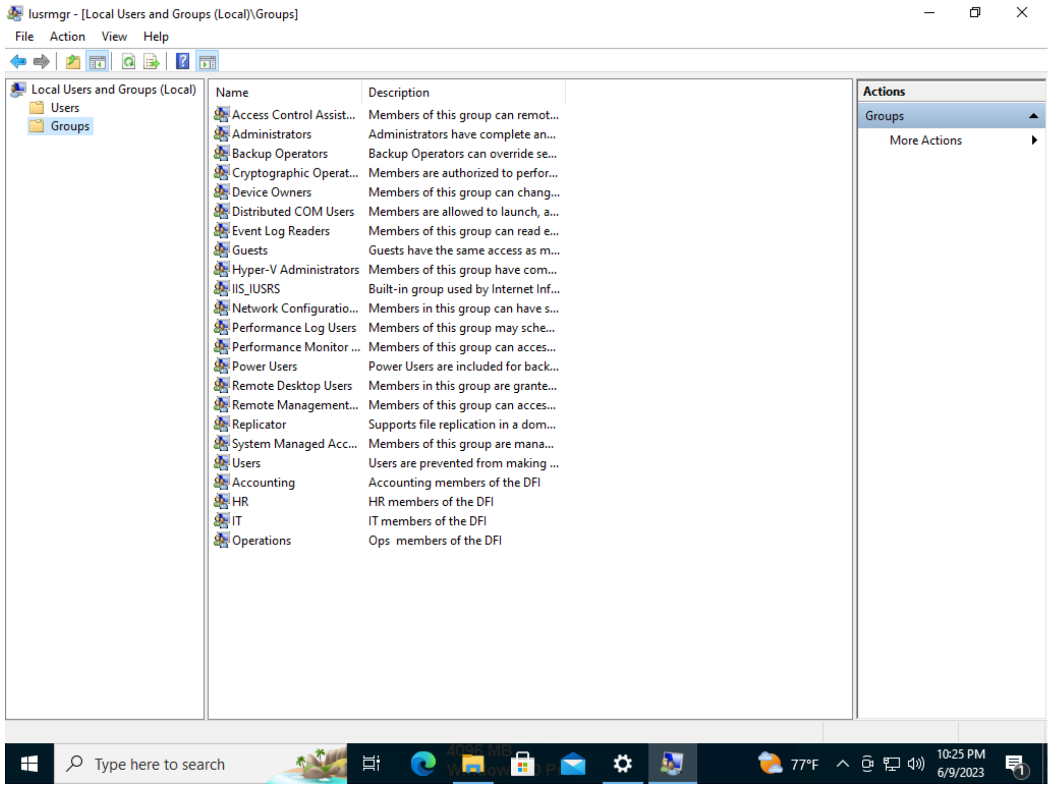
the appropriate groups so that they can read/write/execute in their respective departmental folders.

For documentation purposes, in 3 - 5 sentences, please explain the syntax for non-technical management on the change control board that meets weekly on the next slide.

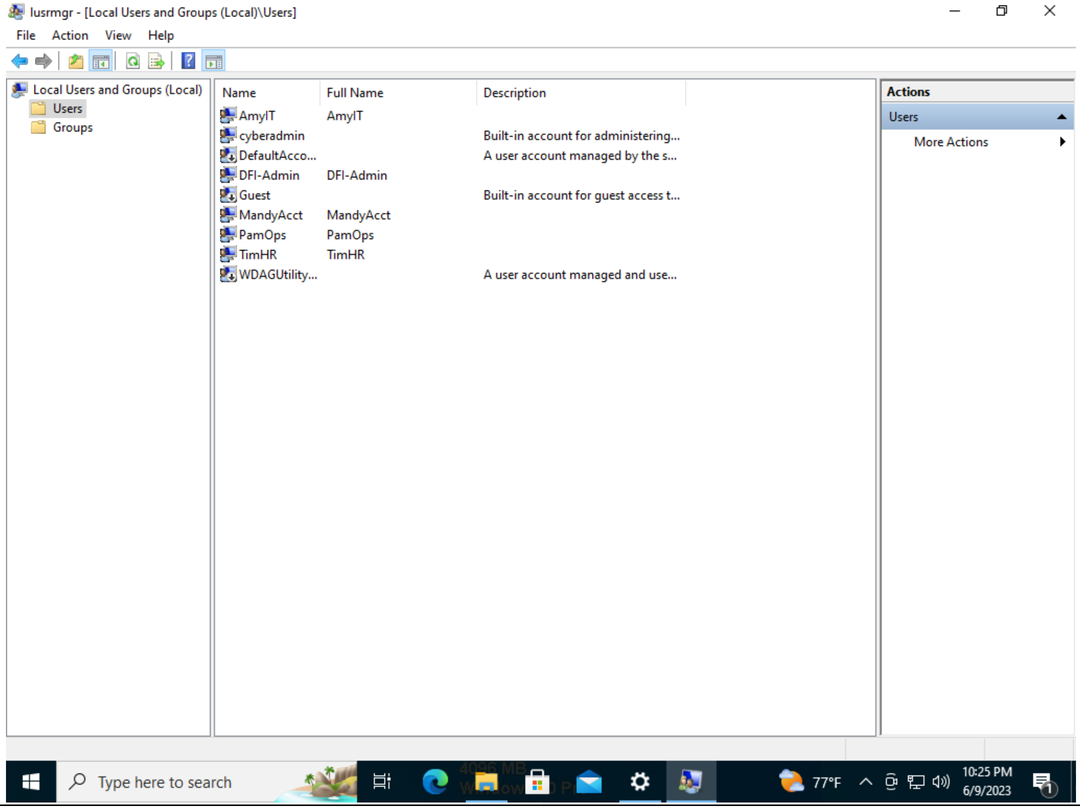
Next, provide a screenshot(s) of completed tasks and the correctly set permissions on the slide after your explanation.

Please write your 3-5 sentence explanation below.
To complete this task, I have made some simple steps and explained them in easy words below: • First, I created the directories. To do this, right-click for the context menu to appear, select new, and then select folder and name it. Repeat the operation for the subdirectories. • Second, I created the groups, to do this search for "users", "Add, edit or remove other users" will appear, select it and look for "Add someone else to this PC", add the four users listed above. • Third, I created the groups, right click the windows start button, select "Computer management", expand "Local users and groups", go to "Groups", from the action menu select the option to add new group, name the group and type a description, add the right members by typing their username, repeat the operation for all the groups and you are finished with creating groups! • Finally, set permissions, right-click the folder, select "Properties" from the context menu, go to security and select "edit", add the right group and click "apply" then "Ok".

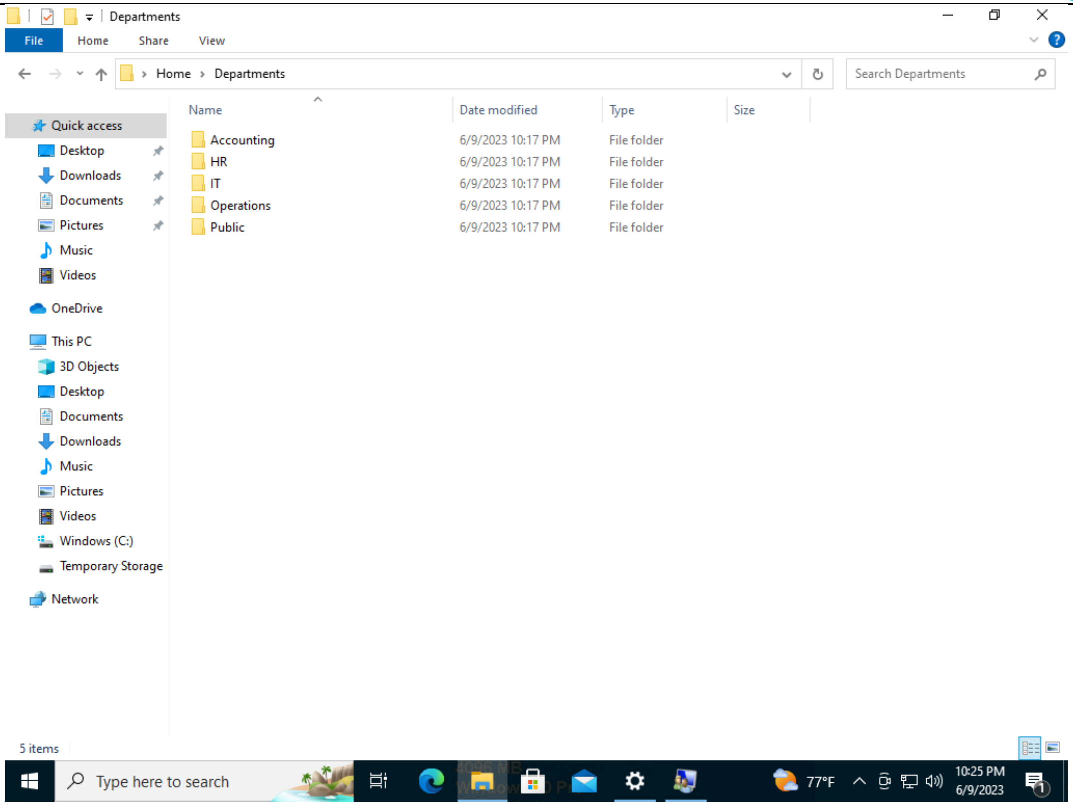
Please include your screenshot below.


lusrmgr - [Local Users and Groups (Local)\Groups]

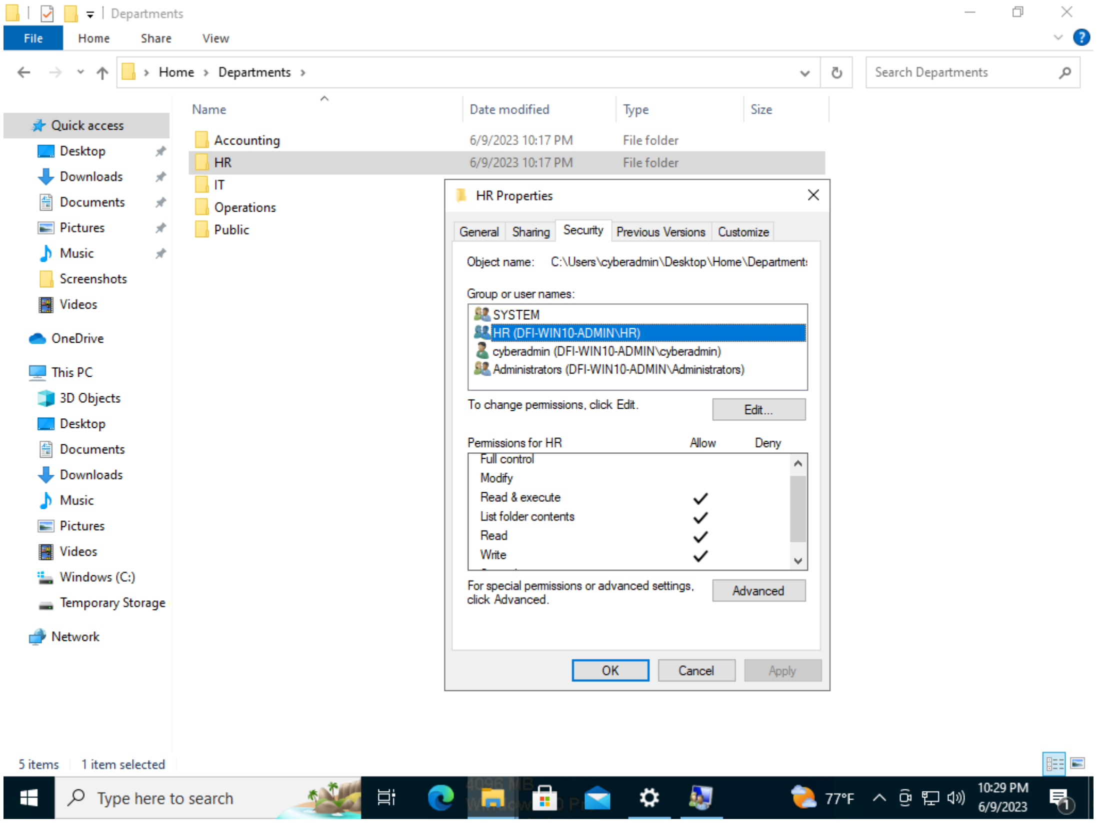
Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...
Accounting	Accounting members of the DFI
HR	HR members of the DFI
IT	IT members of the DFI
Operations	Ops members of the DFI


lusrmgr - [Local Users and Groups (Local)\Users]

Name	Full Name	Description
AmyIT	AmyIT	
cyberadmin		Built-in account for administering...
DefaultAcco...		A user account managed by the s...
DFI-Admin	DFI-Admin	
Guest		Built-in account for guest access t...
MandyAcct	MandyAcct	
PamOps	PamOps	
TimHR	TimHR	
WDAGUtility...		A user account managed and use...



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT	6/9/2023 10:17 PM	File folder	
Operations	6/9/2023 10:17 PM	File folder	
Public	6/9/2023 10:17 PM	File folder	



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT			
Operations			
Public			

HR Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\cyberadmin\Desktop\Home\Department:

Group or user names:

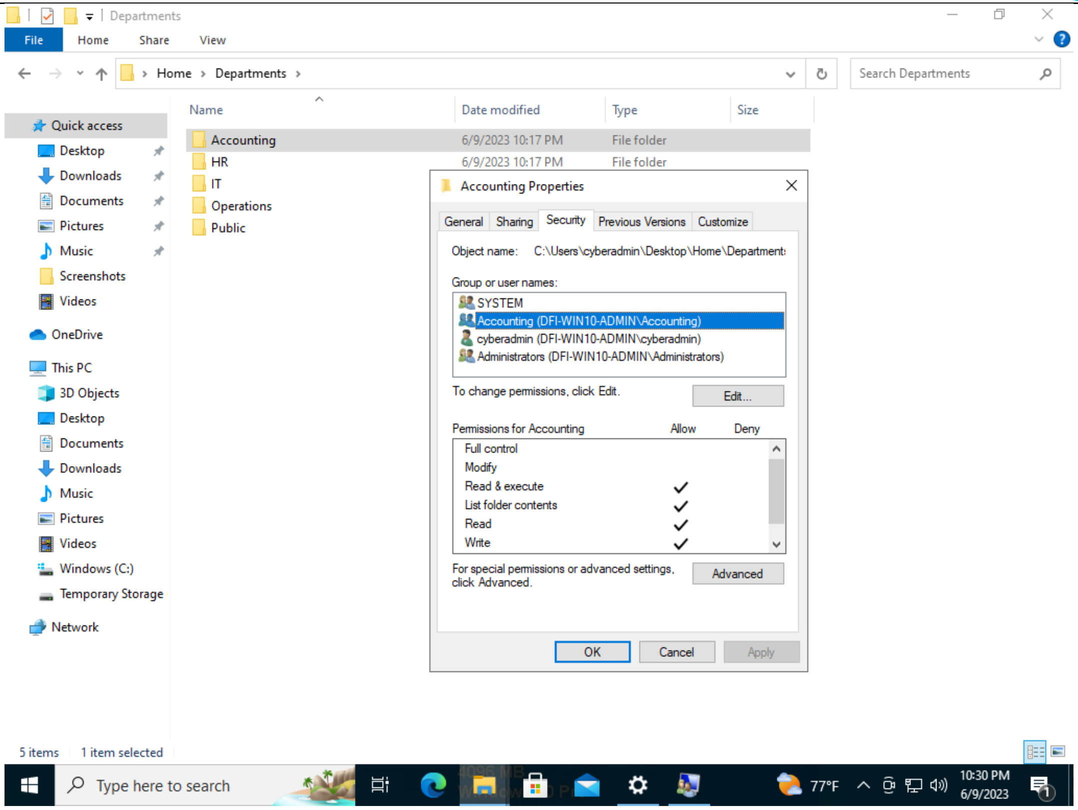
- SYSTEM
- HR (DFI-WIN10-ADMIN\HR)
- cyberadmin (DFI-WIN10-ADMIN\cyberadmin)
- Administrators (DFI-WIN10-ADMIN\Administrators)

To change permissions, click Edit. Edit...

Permissions for HR	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT			
Operations			
Public			

Accounting Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\cyberadmin\Desktop\Home\Department:

Group or user names:

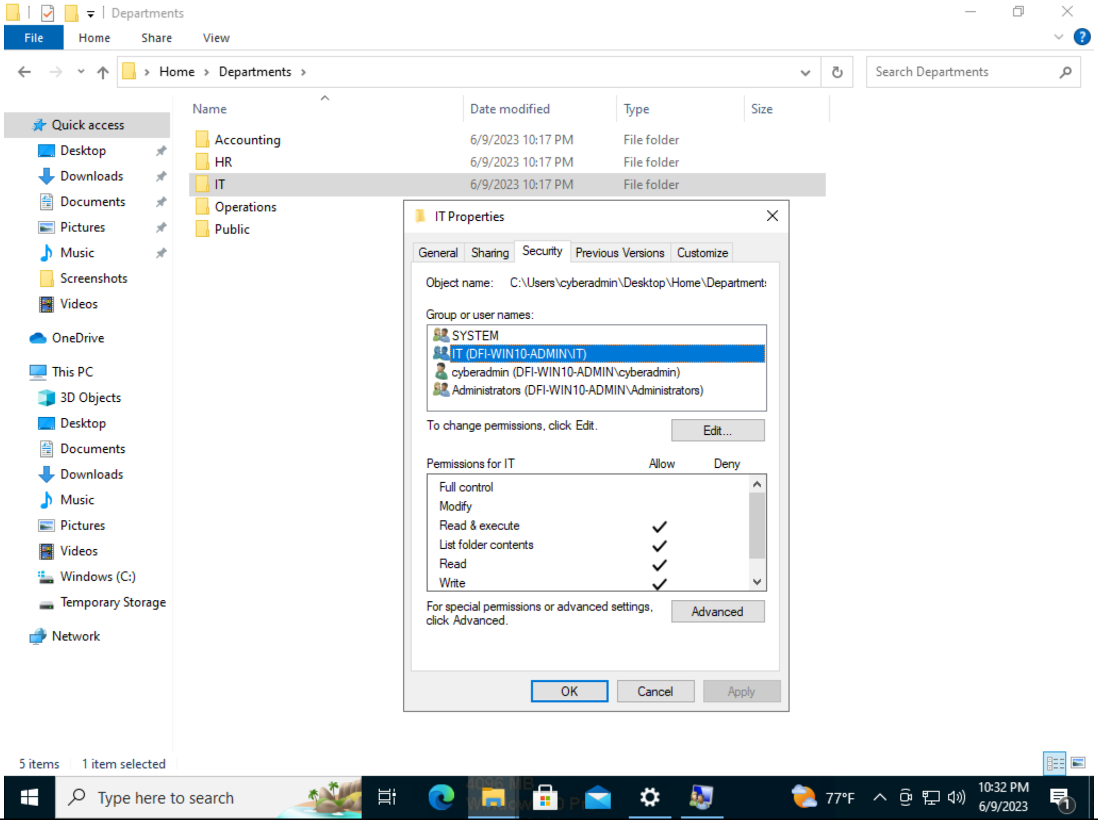
- SYSTEM
- Accounting (DFI-WIN10-ADMIN\Accounting)
- cyberadmin (DFI-WIN10-ADMIN\cyberadmin)
- Administrators (DFI-WIN10-ADMIN\Administrators)

To change permissions, click Edit. Edit...

Permissions for Accounting	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT	6/9/2023 10:17 PM	File folder	
Operations			
Public			

IT Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\cyberadmin\Desktop\Home\Department:

Group or user names:

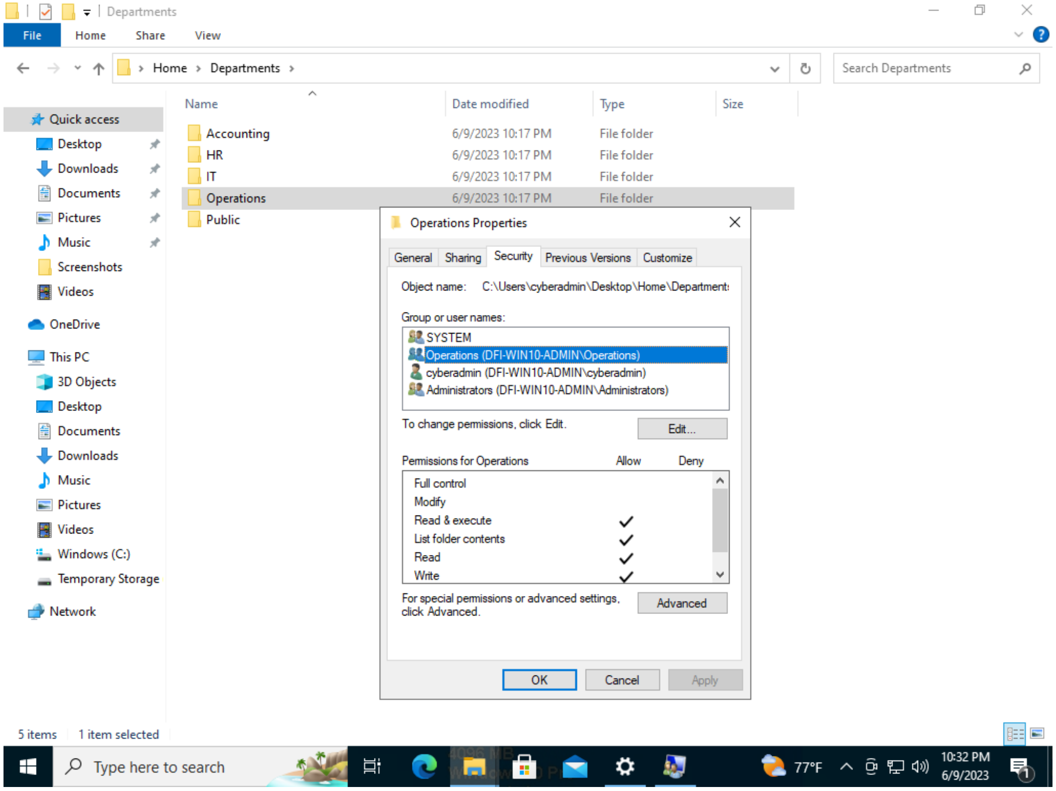
- SYSTEM
- IT (DFI-WIN10-ADMIN\IT)
- cyberadmin (DFI-WIN10-ADMIN\cyberadmin)
- Administrators (DFI-WIN10-ADMIN\Administrators)

To change permissions, click Edit. Edit...

Permissions for IT	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT	6/9/2023 10:17 PM	File folder	
Operations	6/9/2023 10:17 PM	File folder	
Public	6/9/2023 10:17 PM	File folder	

Operations Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\cyberadmin\Desktop\Home\Department:

Group or user names:

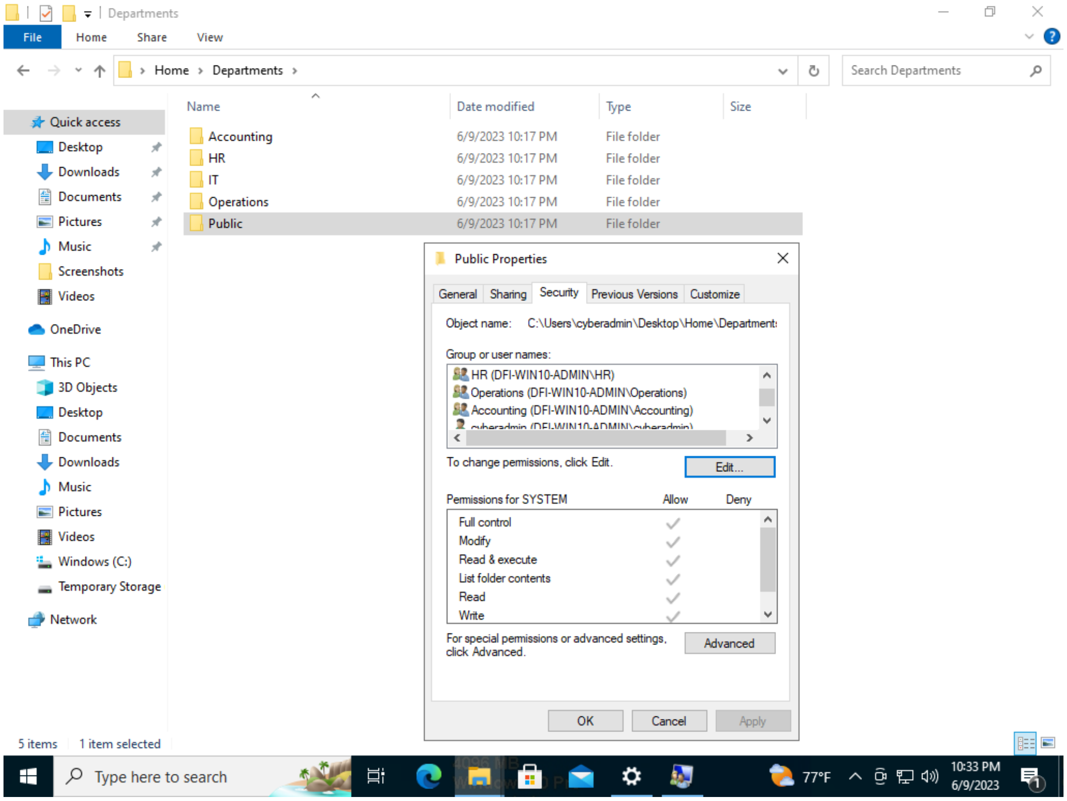
SYSTEM
Operations (DFI-WIN10-ADMIN\Operations)
cyberadmin (DFI-WIN10-ADMIN\cyberadmin)
Administrators (DFI-WIN10-ADMIN\Administrators)

To change permissions, click Edit. Edit...

Permissions for Operations	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply



Name	Date modified	Type	Size
Accounting	6/9/2023 10:17 PM	File folder	
HR	6/9/2023 10:17 PM	File folder	
IT	6/9/2023 10:17 PM	File folder	
Operations	6/9/2023 10:17 PM	File folder	
Public	6/9/2023 10:17 PM	File folder	

Public Properties

General | Sharing | Security | Previous Versions | Customize

Object name: C:\Users\cyberadmin\Desktop\Home\Department:

Group or user names:

HR (DFI-WIN10-ADMIN\HR)
Operations (DFI-WIN10-ADMIN\Operations)
Accounting (DFI-WIN10-ADMIN\Accounting)
cyberadmin (DFI-WIN10-ADMIN\cyberadmin)

To change permissions, click Edit. Edit...

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced. Advanced

OK Cancel Apply

11. Firewall Alert Response - Instructions and Evidence

The IT Manager took a look at firewall alerts and was concerned with some traffic she saw, please take a look and provide 2 different mitigation response to the below firewall report. Remember to justify your mitigation strategy in 3 - 5 sentences.

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

After analyzing the DFI_FW_report.xlsx, I found that the whole alert is about “SSH user authentication brute force attempts. So to mitigate such threat I recommend the following:

- Applying firewall rules to block the following IPs list’s access to the network:

    ✗ 192.34.57.157, 185.244.39.112, 117.131.14.38, 41.50.139.255, 154.8.140.74, 175.6.47.5, 103.79.141.158, 34.201.223.194, 3.132.217.60, 37.110.85.110, 192.109.240.69, 104.50.90.145, 51.79.21.228, 103.125.191.115, 103.133.106.244, 208.113.129.65, 208.113.167.204, 39.116.31.62, 51.15.88.139, 170.210.83.86, 61.161.143.170, 192.210.236.38, 213.91.162.133, 37.49.226.212, 198.12.32.123, 139.199.170.238, 111.200.23.2, 45.35.0.252, 122.141.177.112, 5.182.211.180

    Justification:

    These are the source IPs for the brute force attacks, so initially blocking them is essential until we perform the next mitigation step

- Writing IDS rule to alert on SSH failed authentication attempts, and applying automation using the tools listed in the automation section to be used to respond to the failed attempts to lockout users trying to breach the system’s security

    Justification:

    This will be an effective solution to quickly respond to this type of incidents, by both alerting and making initial and quick response

- Keeping system up-to date
- Making sure of regularly changing passwords, also creating strong passwords and to train users to be aware of the importance of using strong and complex passwords and the risk of sharing their credentials with others.

12. Status Report and Next Steps – Instructions

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 6-8 sentences, 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.

Your report here

Having been a security analyst for the DFI for two weeks I can say that the findings were a lot, we had some security issues from security events to firewall alerts to some attempts to breach the system security. This wide range of threats were managed and I responded to them successfully.

To sum up, the security posture of the DFI is now much better through hardening the system by analyzing it, tuning suitable firewall and IDS rules, integrity checking and VPN recommendation to connect securely with our partner, applying automation and analyzing logs, creating directories, users and user groups and setting suitable permissions, deciding which updates are needed and analyzing firewall reports, but it still needs much more to be implemented!

The next steps will be working on applying defense in depth on these three security perspectives:

- Physical security: by using a set of physical devices and procedures, an example may be using CCTV cameras, using smart cards and tokens, using physical barriers and biometric authentication system etc.

- Logical security: by using logical controls as firewalls and ACLs (Access control lists). We need to apply defense in depth using the firewalls and ACLs together side-by-side so if one control fails to block the malicious action the other will do.

- Administrative security: by applying administrative controls, procedures and guidelines such as enforcing password policies, access control policies, device usage policies, etc. to help in making sure that the human factor is not the weakest point in the system and minimizing the exposure to security risks.

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.