

Scenario:

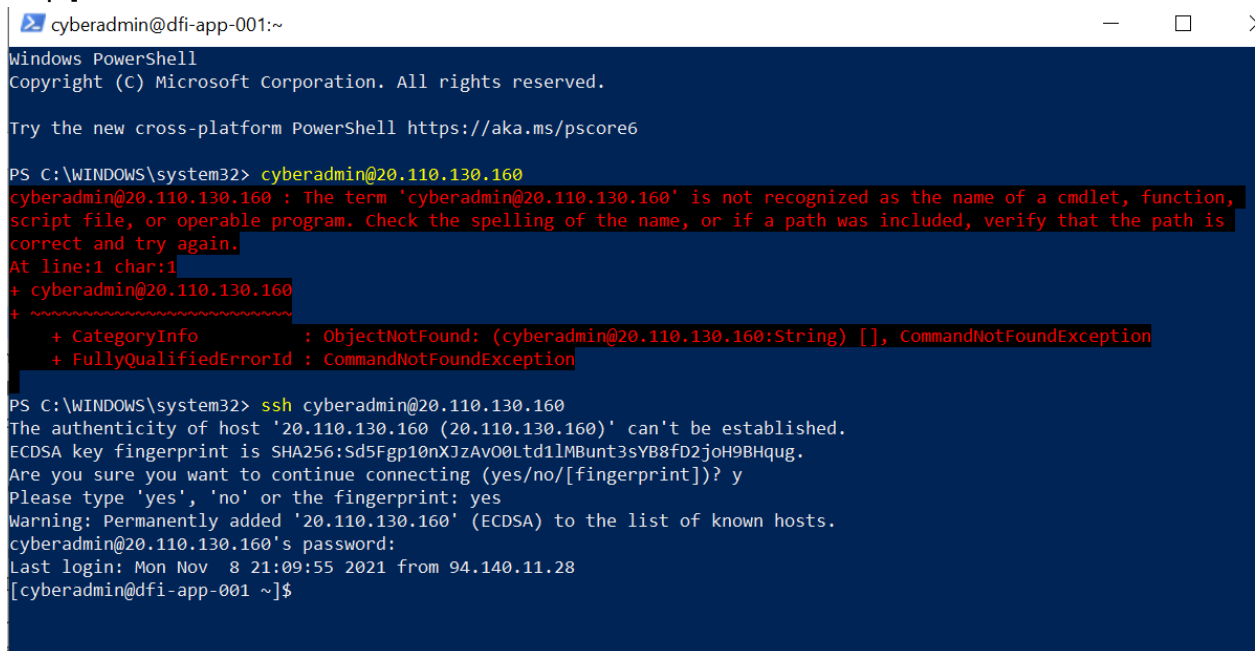
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as 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.]



```
cyberadmin@dfi-app-001:~  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\WINDOWS\system32> cyberadmin@20.110.130.160  
cyberadmin@20.110.130.160 : The term 'cyberadmin@20.110.130.160' is not recognized as the name of a cmdlet, function,  
script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is  
correct and try again.  
At line:1 char:1  
+ cyberadmin@20.110.130.160  
+ ~~~~~  
+ CategoryInfo          : ObjectNotFound: (cyberadmin@20.110.130.160:String) [], CommandNotFoundException  
+ FullyQualifiedErrorId : CommandNotFoundException  
  
PS C:\WINDOWS\system32> ssh cyberadmin@20.110.130.160  
The authenticity of host '20.110.130.160 (20.110.130.160)' can't be established.  
ECDSA key fingerprint is SHA256:Sd5Fgp10nXJzAv00Ltd1lMBunt3sYB8fD2joH9BHqug.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '20.110.130.160' (ECDSA) to the list of known hosts.  
cyberadmin@20.110.130.160's password:  
Last login: Mon Nov  8 21:09:55 2021 from 94.140.11.28  
[cyberadmin@dfi-app-001 ~]$
```

Figure 1 SSH

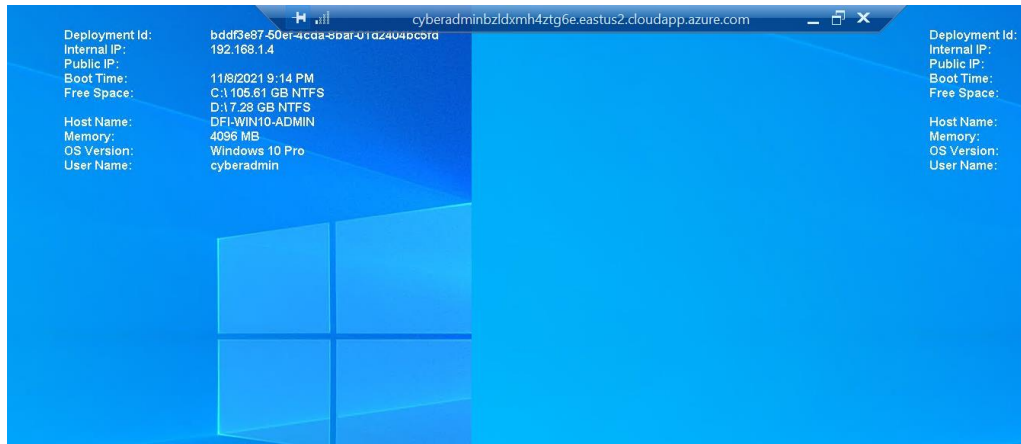


Figure 2 RDP

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]

With the Windows 2016 Server in the following folders:

Windows 2016 Server	Issue	Justification
Accounting Folder	<ul style="list-style-type: none"> ○ AmyIT should not have access to the Accounting group folder ○ Not all accounting employees should have full control. They should have Read, Write, List 	<p>She works for the IT department.</p> <p>Give least privilege</p>

	<p>folder contents, and Execute</p> <ul style="list-style-type: none"> ○ Administrators should have access to the Folder, Subfolders, and File 	
HR Folder	<ul style="list-style-type: none"> ○ Users should not have Special Permissions. Give them only Read and Execute. ○ Place the Owner under the Administrators to give full control ○ HR group give only Read, Write, List Folder Content, and Execute 	Give least privilege
IT Folder	<ul style="list-style-type: none"> ○ Creator Owner should be under the Administrator to have full control ○ IT group should have only Read, Write, List of Folder Content, and Execute ○ Add AmyIT to the IT group 	Give least privilege
Operation Folder	<ul style="list-style-type: none"> ○ Creator Owner should have put under the Administrator for full control 	Give least privilege

	<ul style="list-style-type: none"> ○ Operation group should have Read, Write, List of File Content, and Execute 	
Public Folder	<ul style="list-style-type: none"> ○ Place Creator Owner under Administrator to give full control. ○ Users group should not have modify privileges 	Give least privilege
Sync Host_6307e	Disable	Synchronization of user data is not needed
Sync Host_c2a8b	Disable	Synchronization of user data is not needed
Xbox Live Auth manager	disable	Remove or disable unnecessary services
Xbox Live Game Save	Disable	Remove or disable unnecessary service
Minimum Password length	Change to 8 characters	To aid in password guessing
Enforce Password History	Change to 2 passwords remembered	To aid in password guessing
Account Lockout Threshold	Change to 3 invalid logon attempts	To aid in password guessing
Account lockout duration	Changed to 30 minutes	To aid in password guessing
Reset Account Lockout Counter After	Changed to 30 minutes	To aid in password guessing

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.

Firewalls do not know what is allowed or not allowed to access the network or system. Therefore, a firewall syntax/rule must be created either giving access or denying access to a network or system. In order to create a firewall rule, we need the following parts:

1. An **interface** which allows a person or program to interact with the computer.
2. Whether a traffic/person/program **allowed or denied**
3. The **source Internet Protocol (IP) Address** meaning where the traffic is coming from.
4. The **destination Internet Protocol (IP) Address** meaning where the traffic is going to.

Since we have all the parts for our firewall rule

1. Interface: DFI-Ingress
2. Allowed Access
3. Source IP Address: WBC International with IP Address: 21.19.241.63 Assigned Name: Toledo
4. Destination IP Address: DFI-File-001 with IP Address: 172.21.30.44 Assigned Name: Bubba

We can now create the firewall rule using the template:
access-list **name of our internal interface** extended permit **protocol used** host **source IP address** host **destination IP address** eq **port required**

Using the above template and the information our firewall rule looks like this:

access-list DFI-Ingress extended permit tcp host Toledo host Bubba eq 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](#) as a guide.

I would recommend using the Internet Protocol Security (IPsec) Virtual Private Network (VPN). The reasons are as follows:

- IPsec is within the network layer; it protects the traffic that is traveling to the network
- It monitors the traffic that passes in and out of the network.
- It is invisible in its operations; users do not have to interact with it.
- There is no application dependency
- The privacy of the data is safeguarded using a public key. The data that is being exchanged between DFI and Payroll-USA will use public keys to ensure safety. By using the safety of the keys, you are assuring the data is coming from the right host not from a fake site/source.
- IPsec can be implemented to any network from all the sizes.

- Suggest using Advanced Encryption Standard (AES) 256 to secure your data. AES 256 is unbreakable against brute force attacks and it is the strongest encryption standard.
- It provides authentication by placing digital signatures on each data packet. Any interference from a third party is protected. Any content inside the packet header cannot be modified without detection. It does identify verification for 2 ends of a connection.

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.

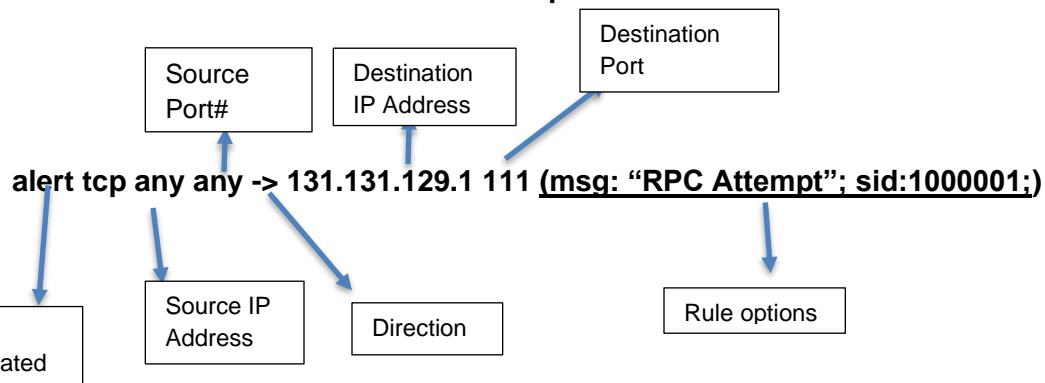
The VoIP Administrator is also concerned that an attacker is attempting to connect to her primary VoIP server which resides at 172.21.30.55 via TFTP. She has requested an IDS rule for this traffic.

For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.

Intrusion Detection System (IDS) is a passive tool that only monitors for the network for possible malicious and dangerous activity. It alerts but does not take any action. It can be hardware or software based.

The anatomy of an IDS rule is using the below example:

Alert on TCP traffic to IP address and port 111:



To create the IDS rule, we have the following:

- Create Rule Alert on ICMP Traffic
- Source IP address: Any
- Source Port#: Any
- Direction: →
- Destination IP Address: DFI-File-001 172.21.30.44
- ICMP Traffic Port: 1

Using the above template and information provided, our IDS rule is

Alert ICMP any any ->172.21.30.44 any (msg: "ICMP Connection Attempt"; sid:1000001;)

For the VoIP Server, the anatomy of an IDS rule still applies. We have the following information:

- Create Rule Alert on TFTP
- Source IP address: Any
- Source Port#: Any
- Direction: ->
- Destination IP Address: VoIP Server 172.21.30.55
- TFTP Traffic Port: 69

Using the same example above and the information provide, our IDS rule is

alert TFTP any any ->172.21.30.55 69 (msg: "TFTP Attempt"; sid:1000002;)

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.

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

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

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
Incident Response Management Network Monitoring and Defense Network Intrusion Detection System	SOAR product such as Splunk Phantom	Security, Orchestration, Automation, and Response (SOAR) product is used to collect security data, identify, analyze, and address potential threats and vulnerabilities coming from different sources. They allow organization to be able to respond quickly and consistently. This will lessen the dwell time an attacker is in an organizations network/system. Refer to CIS Control 17: Incident Response Management; CIS Control 13: Network Monitoring and Defense;
Security Logging and Monitoring	Splunk	You want help to detect, escalate, and respond to active breaches. Without logging and monitoring, vulnerabilities can go detected. Refer to https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/

Audit Logging	Splunk	An audit log is a document that records an event in a system. It documents what was accessed. The audit log entries usually included the destination and source addresses, a timestamp and user login information. Refer to CIS Controls 6: Maintenance, Monitoring, and Analysis of Audit Logs
Continuous Vulnerability Management	Tenable	Implementing a vulnerability management tool can help you detect any areas in your system that could potentially be exploited by an attacker before a breach occurs. Refer to CIS Control 3: Continuous Vulnerability Management

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 Event viewer, 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.

```
PS C:\Users\cyberadmin> Get-Eventlog -Logname Security -InstanceID 4625 -Newest 15 | Export-Csv -Path .\WmiData.csv
PS C:\Users\cyberadmin>
```

```
Subject:
  Security ID:      S-1-0-0
  Account Name:     -
  Account Domain:   -
  Logon ID:         0x0

Logon Type:        3

Account For Which Logon Failed:
  Security ID:      S-1-0-0
  Account Name:     Administrator
  Account Domain:

Failure Information:
  Failure Reason:    %%2313
  Status:           0xc000006d
  Sub Status:       0xc0000064

Process Information:
  Caller Process ID: 0x0
  Caller Process Name: -

Network Information:
```

Findings:

- This event was generated due to a logon failure.
- The subject field is the account on the local system that requested the logon.
- The logon type indicates the kind of logon that was requested. This was a network logon type.
- The process information indicates the account and process on the system that requested the logon
- The failure reason %%2313 is **Unknown username or bad password**
- Network Information fields indicates where a remote logon request originated.

This may be someone who is not an administrator but an attacker trying to gain access remotely to sensitive data.

Recommendations and Justifications:

- Use multi-factor authentication (MFA) for all privilege and administrator accounts. MFA can help in protecting data. Some users' activities may pose a great risk to an organization's data if they are using an untrusted network, or conducting administrator functions that allow them to add, change, or remove other accounts, or make changes to an operating system or applications making them less secure. This is another reason to give lesser privileges as necessary for a user's role. **CIS Control 6: Access Control Management**
- Use MFA for remote network access. The justification is the same as above. **CIS Control 6: Access Control Management**
- Manage access control for remote access: up-to-date anti-malware is installed, up-to-date operating system and applications. This will help in preventing malicious attacks. **CIS Control 13: Network Monitoring and Defense**
- Use security logging and monitoring software. This will help with detecting, escalating, and responding to active breaches. This type of software will detect and investigate threats across your entire system by automatically scanning your logs.
- Tune security event alerts monthly or more frequently
- Use a network intrusion detection system: This will assist in detecting anomalies with the aim of catching hackers before they do real damage to a network. **CIS Control 13: Network Monitoring and Defense**
- Implement a security awareness program for employees. This program should be done annually for all employees. The purpose of this program is to educate employees on the importance of cybersecurity in the workplace. To let them be able of the policies and procedures related to approved IT devices to use, phishing, web browsing, MFA, passwords, etc. **CIS Control 14: Security Awareness and Skills Training**

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
Windows Feedback Hub Elevation of Privilege Vulnerability	Ignore	Feedback Hub is a feature that DFI does not use or need.
Windows Desktop Bridge Elevation of Privilege Vulnerability CVE-2021-36957	Update	Updates security for Windows Operating System. <ul style="list-style-type: none">▪ Addresses an issue in which certain apps might have unexpected results when rendering some user interface elements or when drawing within the app. You might encounter this issue with apps that use GDI+ and set a zero (0) width pen object on displays with high dots per inch (DPI) or resolution, or if the app is using scaling.▪ Addresses an issue that prevents Failover Clustering from updating Domain Name Server (DNS) records
Windows Denial of Service Vulnerability CVE-2021-41356	Update	Denial of Service can affect the availability of the server.
Windows Hyper-V Denial of Service Vulnerability	Ignore	This is needed only if DFI uses virtual machines but no documentation of DFI using VMs.
Chakra Scripting Engine Memory Corruption Vulnerability CVE-2021-42279	Update	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge (HTML-based). The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary

		code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. If the current user is logged on with administrative user rights, an attacker who successfully exploited the vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit the vulnerability through Microsoft Edge (HTML-based) and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit the vulnerability.
March 18, 2021-KB5001633 Version: OS Build 14393.4288	Ignore	This relates to non-security update that includes quality improvements. Addresses an issue that fails to print the graphical content in a document. Graphical content refers to content that is realistic images or languages such are bad language, violence, drugs, or sex.

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.

```
[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]$ ls
cyberadmin  Departments  dfi-admin  JoePublic
[cyberadmin@dfi-app-001 home]$ cd /Departments
-bash: cd: /Departments: No such file or directory
[cyberadmin@dfi-app-001 home]$ cd Departments
[cyberadmin@dfi-app-001 Departments]$ mkdir HR
mkdir: cannot create directory 'HR': Permission denied
[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
```

Figure 3 Creating the directories

```
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
d-----, 2 root root 6 Nov 29 18:58 Accounting
d-----, 2 root root 6 Nov 29 18:58 HR
d-----, 2 root root 6 Nov 29 18:58 IT
d-----, 2 root root 6 Nov 29 18:58 Operations
d-----, 2 root root 6 Nov 29 18:58 Public
[cyberadmin@dfi-app-001 Departments]$ sudo chmod +rwxr Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chmod +rwxr HR
[cyberadmin@dfi-app-001 Departments]$ sudo chmod +rwxr IT
[cyberadmin@dfi-app-001 Departments]$ sudo chmod +rwxr Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chmod +rwxr Public
[cyberadmin@dfi-app-001 Departments]$ ls -l
total 0
drwxr-xr-x, 2 root root 6 Nov 29 18:58 Accounting
drwxr-xr-x, 2 root root 6 Nov 29 18:58 HR
drwxr-xr-x, 2 root root 6 Nov 29 18:58 IT
drwxr-xr-x, 2 root root 6 Nov 29 18:58 Operations
drwxr-xr-x, 2 root root 6 Nov 29 18:58 Public
[cyberadmin@dfi-app-001 Departments]$
```

Figure 4 Setting Owner Permissions

```
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -m TimeHR
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -m MandyAcct
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -m PamOps
[cyberadmin@dfi-app-001 Departments]$ sudo useradd -m AmyIt
[cyberadmin@dfi-app-001 Departments]$
```

Figure 5 Creating Users

```

cyberadmin@dfi-app-001 Departments]$ sudo groupadd HR
cyberadmin@dfi-app-001 Departments]$ sudo groupadd Accounting
cyberadmin@dfi-app-001 Departments]$ sudo groupadd Operations
cyberadmin@dfi-app-001 Departments]$ sudo groupadd IT
cyberadmin@dfi-app-001 Departments]$ sudo groupadd Public
cyberadmin@dfi-app-001 Departments]$

```

Figure 6 Creating Groups

```

cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G HR TimeHR
cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Accounting MandyAcct
cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G Operations PamOps
cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G IT AmyIT
usermod: user 'AmyIT' does not exist
cyberadmin@dfi-app-001 Departments]$ sudo userdel -m AmyIt
userdel: invalid option -- 'm'
Usage: userdel [options] LOGIN

Options:
  -f, --force          force some actions that would fail otherwise
                        e.g. removal of user still logged in
                        or files, even if not owned by the user
  -h, --help           display this help message and exit
  -r, --remove         remove home directory and mail spool
  -R, --root CHROOT_DIR
                        directory to chroot into
  -Z, --selinux-user   remove any SELinux user mapping for the user

cyberadmin@dfi-app-001 Departments]$ sudo userdel -r AmyIt
cyberadmin@dfi-app-001 Departments]$ sudo useradd -m AmyIT
cyberadmin@dfi-app-001 Departments]$ suod usermod -a -G IT AmyIT
bash: suod: command not found
cyberadmin@dfi-app-001 Departments]$ sudo usermod -a -G IT AmyIT

```

Figure7 Adding Users to Group

```

[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+wx IT
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+wx Operations
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+wx Accounting
[cyberadmin@dfi-app-001 Departments]$ sudo chmod g+wx Public
[cyberadmin@dfi-app-001 Departments]$ cd IT
[cyberadmin@dfi-app-001 IT]$ ls -ld
drwx-wxr-x. 2 root root 6 Nov 29 18:58 .
[cyberadmin@dfi-app-001 IT]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ cd Operations
[cyberadmin@dfi-app-001 Operations]$ ls -ld
drwx-wxr-x. 2 root root 6 Nov 29 18:58 .
[cyberadmin@dfi-app-001 Operations]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ cd Accounting
[cyberadmin@dfi-app-001 Accounting]$ ls -ld
drwx-wxr-x. 2 root root 6 Nov 29 18:58 .
[cyberadmin@dfi-app-001 Accounting]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ cd Public
[cyberadmin@dfi-app-001 Public]$ ls -ld
drwx-wxr-x. 2 root root 6 Nov 29 18:58 .
[cyberadmin@dfi-app-001 Public]$ cd ..
[cyberadmin@dfi-app-001 Departments]$ cd HR
[cyberadmin@dfi-app-001 HR]$ ls -ld
drwx-wxr-x. 2 root root 6 Nov 29 18:58 .
[cyberadmin@dfi-app-001 HR]$

```

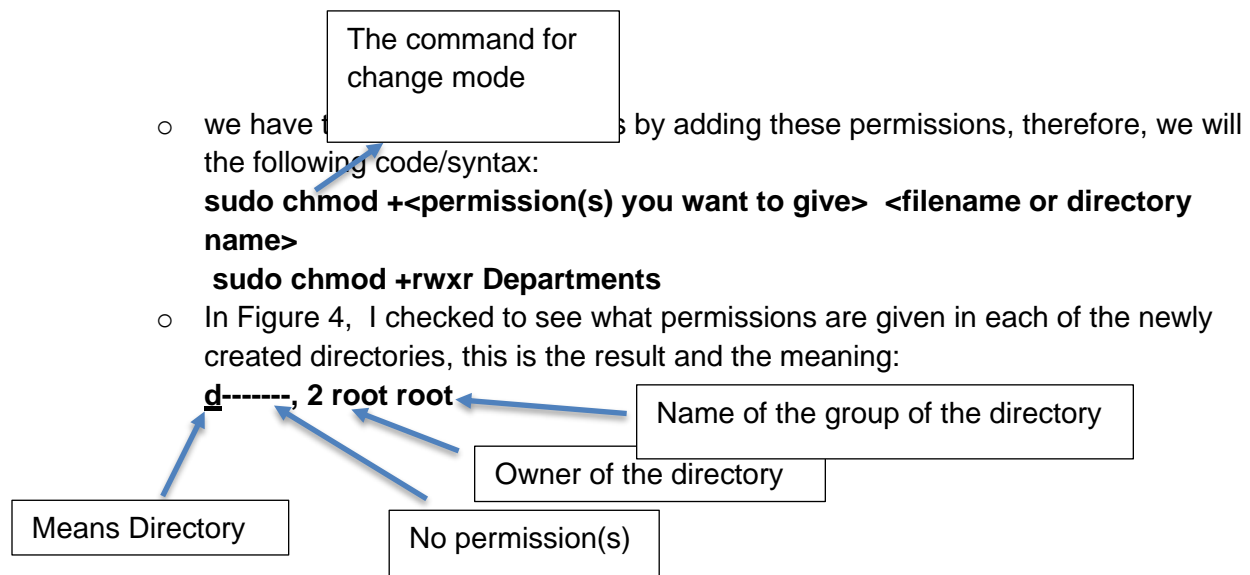
Figure 8 Giving rwx permission to the groups

Explanation:

- **Figure 3:** To create a directory titled “Departments” and the subdirectories HR, IT, Accounting, Operations, and Public, we need to use the following command:

sudo mkdir <name of the directory>

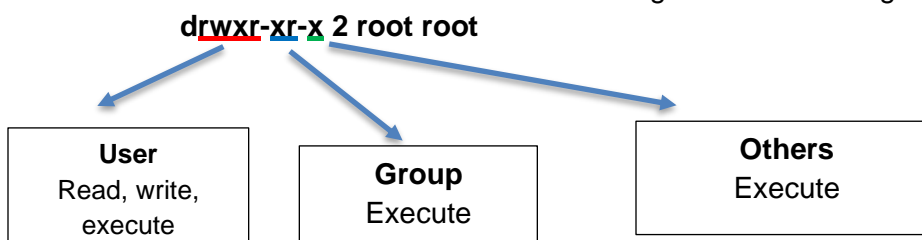
- **Sudo** means super user do, this gives you elevated privileges as a user to all the rights or permissions of a file, directory.
 - **mkdir** = make a directory...this is what we are doing to; create a directory
 - **<name of the directory>** is the name of the directory.
 - **Figure 4:** Now that we have created a new directory Departments, we need to set owner permission. The type of permissions we can give the owner or user are:
 - **Read (r):** ability to open and read a file. With directories, read permissions gives you the ability to list the contents
 - **Write (w):** gives you the ability to change/modify a file. With the created directories in Linux, write permissions gives you the ability to add, remove, and rename files stored in the directories.
 - **Execute (x):** In Linux, this gives you the permission to run a program
- Before you give the owner permission to Departments, you first need to check to see what permissions are assigned if any by using the following command:
- **ls -l**
 - if there are no permission, we want to give the owner of Departments the permission to 'rwx'



Since there are no permissions set, I have to use the same code/syntax above;

sudo chmod +<permission(s) you want to give> <filename or directory name>

To check to make sure the change and permissions are correct, I use the command: **ls -l** and the result is along with the meaning:



The change and permissions are correct for each directory.

Figure 5: In order to create Users: TimeHR, MandyAcct, PamOps, AmyIT; we need to use the following code/syntax:

- sudo useradd -m <user's name>**

The command to add a user

- The code/syntax is this when using the user name "TimeHR":

sudo useradd -m TimeHR

Figure 6: To create the following groups to place the users into: HR, Accounting, IT, Operations, Public, you need to use the following code/syntax:

- sudo groupadd <directory name>**

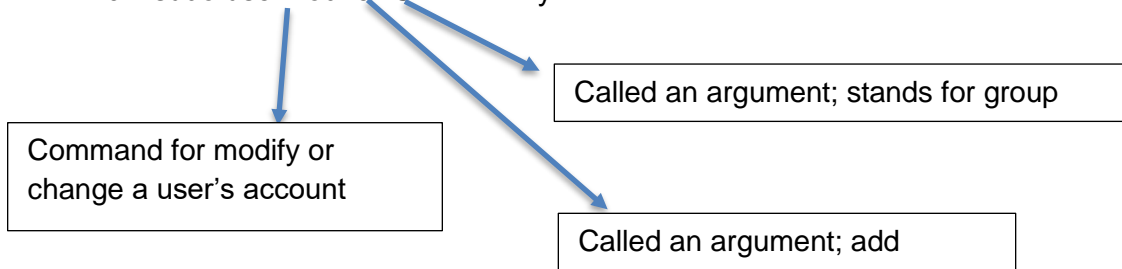
Command for adding a group to a Directory

-
- The result using the above code/syntax is

`sudo groupadd HR`

Figure 7: Now that you have users and groups, you have to add the users to the appropriate group

- `sudo usermod -a -G <directory> <user's name>`



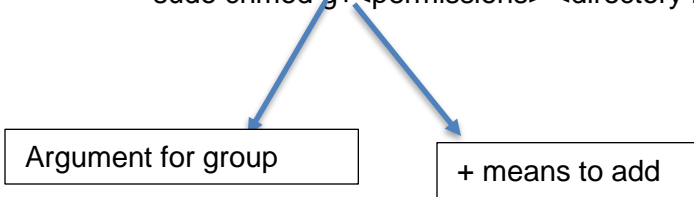
- The result should be when using the above syntax:

`sudo usermod -a -G HR TimeHR`

Figure 8: With the users' name adding to the respective group, we have to assign the permissions of rwx to the groups within HR, IT, Accounting, Operations, Public.

- Prior to assigning the permissions, I checked to see if any group permission has been assigned with `r` (read). Therefore, I need to add the `wx` permissions. Using the code/syntax:

`sudo chmod g+<permissions> <directory name>`




- Using the same code/syntax, the result using HR is:

`sudo chmod g+wx HR`

- To check to see if the permissions were assigned correctly, I used the command

cd HR which means change directory to HR. This has to be done since I am in the Departments directory. Once I am in the HR directory, I use the command: ls -ld to show me the lists of permissions and the following result is:

```
drwx-wxr-x 2 root root
```



Remember this is group. They have the Write, Execute, and Read

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.

- Check to see if there is a configuration problem, sometimes a configuration problem can generate this type of traffic.
- It is unexpected contact the abuse contact of the registrar of the offending IP address
- Lookup the IP address on **abuseIPDB** which is a database that allow users to check the report history of any IP address to see if anyone else has reported any malicious acts. In addition, any user can report any malicious act of an IP address. You want to check to see if these IP addresses are on this report history.
- If they are, you should block them by configuring the firewall.
- If Secure Shell (SSH) is needed and used, consider using a Virtual Private Network (VPN). This will increase the security of the private network.

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.

The goal of my first two weeks was to get a sense of your security posture. In order to accomplish this, I did the following:

- Analyzed your Windows server, file permissions, and password management
- Wrote Firewall and Intrusion Detection System rules with explanations
- Reviewed DFI's desire to establish a VPN connection with Payroll-USA and provide recommendations on which Cisco VPN encryption solution.
- Conducted a File Hash verification from a software vendor of a custom application. This was done to verify integrity and authenticity. The file is downloaded and stored on the Windows 2016 Server in C Drive under DFI-Download.
- Researched areas that could improve thru automation and provided solutions
- Investigated logging attempts of the file DFI-File-001 via Remote Desktop Protocol (RDP), provided solutions
- Using the Microsoft Updates Guide and Common Vulnerabilities and Exposures (CVE) website (www.cve.org), I checked for any necessary Windows Server 2016 security updates.
- Created directories as instructed by the IT manager

My recommendations are as follows:

- Give the least privileges as necessary
- Remove any applications that are not needed in the organization
- Improve your password policy using increase in character length, maximum logon attempts, set a password change date, use multi-factor authentication (MFA)
- Purchase security logging and monitoring software
- Check for any security updates and/or set Windows security updates to update automatically

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.