KEVIN C MEJIAS

Scenario:

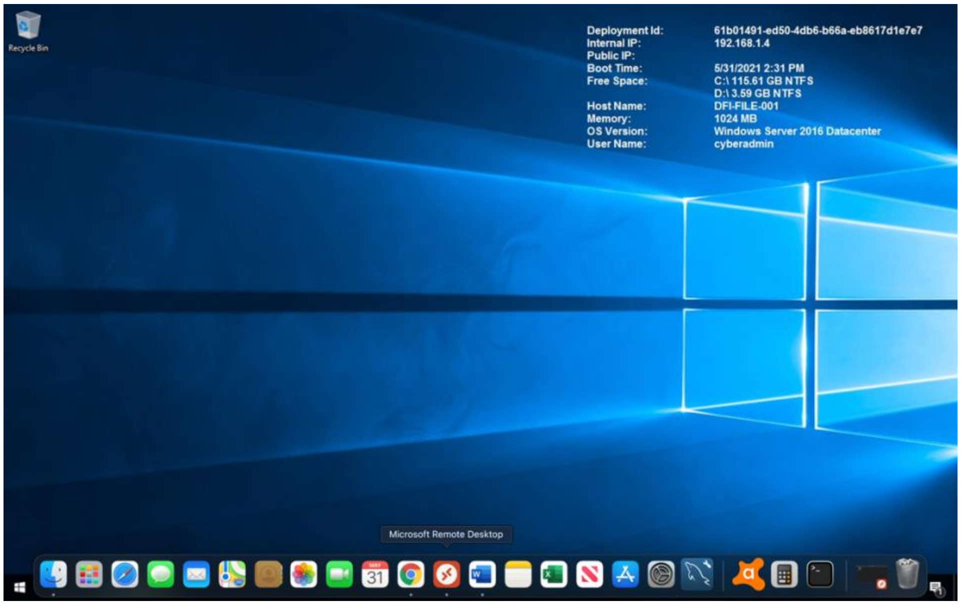
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI we are happy to bring you on as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

Week One:

1. **Connect:**

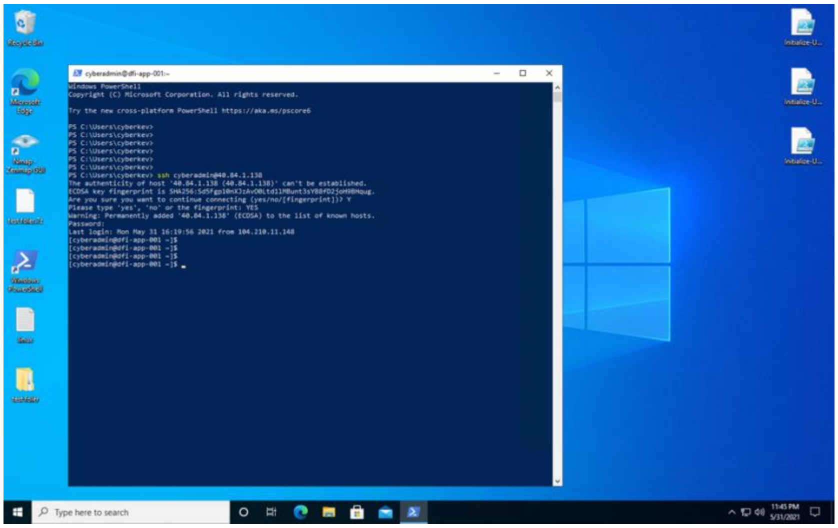
All of the subsequent steps will take place in the DFI environment. You will need to RDP into the Windows 10 workstation and use it to connect with the Windows and Linux servers provided using RDP and SSH (via PowerShell) respectively.

RDP TO WINDOWS SERVER FROM MCBOOK



```
Deployment Id:      61b01491-ed50-4db6-b66a-eb8617d1e7e7
Internal IP:        192.168.1.4
Public IP:
Boot Time:          5/31/2021 2:31 PM
Free Space:         C:\ 115.61 GB NTFS
                    D:\ 3.59 GB NTFS
Host Name:          DFI-FILE-001
Memory:             1024 MB
OS Version:         Windows Server 2016 Datacenter
User Name:          cyberadmin
```

SSH TO LINUX SERVER



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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\cyberkev>
PS C:\Users\cyberkev>
PS C:\Users\cyberkev>
PS C:\Users\cyberkev>
PS C:\Users\cyberkev>
PS C:\Users\cyberkev>
PS C:\Users\cyberkev> ssh cyberadmin@40.84.1.138
The authenticity of host '40.84.1.138 (40.84.1.138)' can't be established.
ECDSA key fingerprint is SHA256:Sd5Fgp10nXJzAvO0Ltd1lMBunt3sY88fD2joH9BHqug.
Are you sure you want to continue connecting (yes/no/[fingerprint])? Y
Please type 'yes', 'no' or the fingerprint: YES
Warning: Permanently added '40.84.1.138' (ECDSA) to the list of known hosts.
Password:
Last login: Mon May 31 16:19:56 2021 from 104.210.11.148
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
```

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.)

A:

After performing an analysis of DFI Windows server, I was able to spot some configurations that could change and would like to give a couple of advices to improve its security.

-File Permissions:

At the documents folder Departments, there are 5 subfolders for the departments. Some settings prevent a department to be able to do their work properly and some other settings give departments more permissions than they need.

- Accounting should have read, write and execute permission instead of full control, the IT group should have full control
- The administrator should have full control instead of just special control.

-HR:

- HR folder there is a group ‘Users’ that shouldn’t be there

-Users group should have modifications in its permissions.

-Services

- Xbox Live auth manager services should be disable
- Xbox Live game save services should be disable

-Other services that can be disable if not used.

- AllJoyn router service
- Bluetooth service
- Phone service
- Quality windows audio video experience
- Windows push notifications.

-Services that should be running:

- Active directory web services
- Windows update

-Apps and Update

- System is not update and it’s not possible to install update
- Microsoft Visual C++ 2013 is not up to date

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.
A:
Name 21.19.241.63 partner-001
Name 172.21.30.44 DFI-File-001

```
access-list DFI-Ingress extended permit tcp host partner-001 host DFI-File eq 9082
```

- access-list: rule that controls traffic
- DFI-Ingress: name of our internal interface
- Extended permit: flexibility in matching traffic and the ability to match based on protocol, source and destination address
- TCP using the TCP protocol
- Partner-001: source
- DFI-File: destination
- Eq 9082: port.

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.

A: I would recommend the Transport Layer Security and suites cipher method:
transport Layer Security (TLS) is used to encrypt communications. TLS is the successor of SSL and provides encryption, authentication, and integrity for web communications. TLS 1.2 is the current version. Where possible, TLS 1.2 is preferred over SSL 3.0, TLS 1.0, and TLS 1.1. TLS is also used in various Cisco products to provide VPN services.
Cipher suites are combinations of security algorithms that are used in TLS. When configuring products that support TLS, administrators are advised to use secure algorithms in the cipher suites of the TLS negotiation when possible.

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.

A:

1) alert tcp any any -> 172.21.30.44 (msg:"ICMP traffic detected"; sid: 10000101;)

2) Alert udp any any -> 172.21.30.55 69 (msg:"TFTP connection attempt"; sid: 10000102)

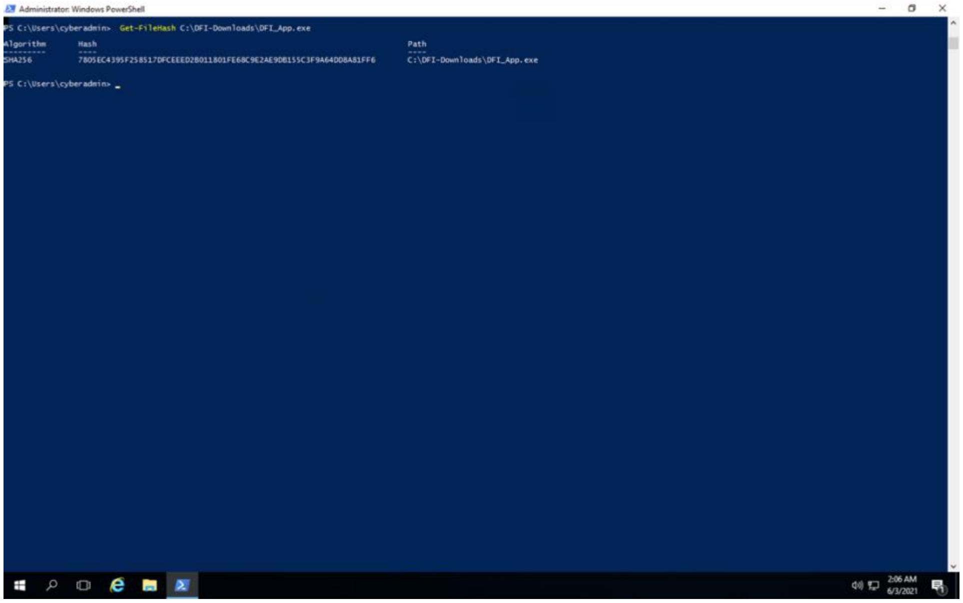
- The word "alert" shows that this rule will generate an alert message when the criteria are met for a captured packet. The criteria are defined by the words that follow.
- The "tcp" part shows that this rule will be applied on all *tcp* packets.
- The first "any" is used for source *IP* address and shows that the rule will be applied to all packets.
- The second "any" is used for destination *IP* address and shows that the rule will be applied to all packets irrespective of destination *IP* address.
-
- The third "any" is used for the port number. Since port numbers are irrelevant at the *IP* layer, the rule will be applied to all packets.
- The -> sign shows the direction of the packet.
- The last part is the rule options and contains a message that will be logged along with the alert.

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.
A:



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

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

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

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
Firewall optimization	SecureTrack from tufin	SecureTrack automatically identifies unused rules, rules for a server or needed to access a server, and automatically removes those from firewalls.
Automated Incident Response	IBM Security QRadar	IBM Security QRadar ingests asset, cloud, network, endpoint, and user data, correlates it against vulnerability information and threat intelligence, and applies advanced analytics to identify and track the most serious threats as they progress through the kill chain
Extended Detection & Response	Cynet	Cynet is an Autonomous Breach Protection platform that delivers native integration of NGAV, EDR, UEBA, Network Traffic Analysis, and Deception to discover and eliminate threats, together with a wide range of automated remediation capabilities using Sensor Fusion technology to continuously collect and analyze endpoint, user and network activities across the entire environment: • Cynet 360 can detect and prevent attacks that include compromised user accounts.

		• It follows the deception method to reveal the presence of attackers by planting fake passwords, data files, configurations, and network connections. • It has functionalities to prevent & detect network-based attacks. • For monitoring and control, it offers features like asset management and vulnerability assessment.

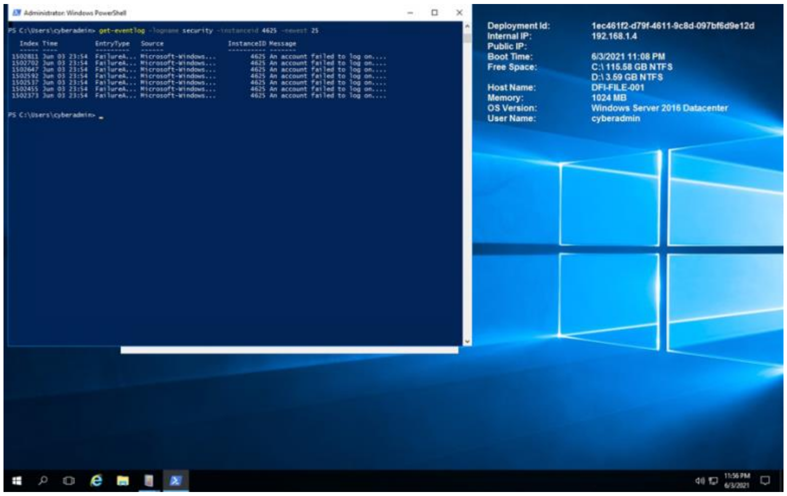
8. Logging RDP Attempts:

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.

A:



```
PS C:\Users\cyberadmin> get-eventlog -logname security -instanceid 4625 -newest 25

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
 1502811 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502702 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502647 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502592 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502537 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502455 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....
 1502373 Jun 03 23:54  FailureA... Microsoft-Windows...         4625 An account failed to log on....


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

```
Deployment Id:     1ec461f2-d79f-4611-9c8d-097bf6d9e12d
Internal IP:       192.168.1.4
Public IP:
Boot Time:         6/3/2021 11:08 PM
Free Space:        C:\ 115.58 GB NTFS
                   D:\ 3.59 GB NTFS
Host Name:         DFI-FILE-001
Memory:            1024 MB
OS Version:        Windows Server 2016 Datacenter
User Name:         cyberadmin
```

After analyzing security logs, I could find some logging attempts, which mean somebody else Is trying to gain access to the server, my recommendations are:

Strong passwords on any accounts with access to Remote Desktop should be considered a required step before enabling Remote Desktop.

2. Use Two-factor authentication

Departments should consider using a two-factor authentication approach. This topic is beyond the scope of this article, but RD Gateways can be configured to integrate with the Campus instance of DUO. Other unsupported by campus options available would be a simple mechanism for controlling authentication via two-factor certificate based smartcards. This approach utilizes the Remote Desktop host itself, in conjunction with YubiKey and RSA as examples.

3. Update your software

One advantage of using Remote Desktop rather than 3rd party remote admin tools is that components are updated automatically with the latest security fixes in the standard Microsoft patch cycle. Make sure you are running the latest versions of both the client and server software by enabling and auditing automatic Microsoft Updates. If you are using Remote Desktop clients on other platforms, make sure they are still supported and that you have the latest versions. Older versions may not support high encryption and may have other security flaws.

4. Restrict access using firewalls

Use firewalls (both software and hardware where available) to restrict access to remote desktop listening ports (default is TCP 3389). Using an RDP Gateway is highly recommended for restricting RDP access to desktops and servers (see discussion below). As an alternative to support off-campus connectivity, you can use the campus VPN software to get a campus IP address and add the campus VPN network address pool to your RDP firewall exception rule

5. Enable Network Level Authentication

Windows 10, Windows Server 2012 R2/2016/2019 also provide Network Level Authentication (NLA) by default. It is best to leave this in place, as NLA provides an extra level of authentication before a connection is established. You should only configure Remote Desktop servers to allow connections without NLA if you use Remote Desktop clients on other platforms that don't support it.

- NLA should be enabled by default on Windows 10, Windows Server 2012 R2/2016/2019.
- To check you may look at Group Policy setting Require user authentication for remote connections by using Network Level Authentication found at Computer\Policies\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security. This Group Policy setting must be enabled on the server running the Remote Desktop Session Host role.

6. Limit users who can log in using Remote Desktop

By default, all Administrators can log in to Remote Desktop. If you have multiple Administrator accounts on your computer, you should limit remote access only to those accounts that need it. If Remote Desktop is not used for system administration, remove all administrative access via RDP, and only allow user accounts requiring RDP service. For Departments that manage many machines remotely remove the local Administrator account from RDP access at and add a technical group instead.

7. Set an account lockout policy

By setting your computer to lock an account for a set number of incorrect guesses, you will help prevent hackers from using automated password guessing tools from gaining access to your system (this is known as a "brute-force" attack). To set an account lockout policy:

1. Go to Start-->Programs--> Administrative Tools--> Local Security Policy
2. Under Account Policies--> Account Lockout Policies, set values for all three options. Three invalid attempts with 3-minute lockout durations are reasonable choices.

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-2021-28476	UPDATE	Updates an issue in Task Scheduler that causes monthly tasks and tasks scheduled for 0 UTC to occur at the wrong time. Updates to improve Windows OLE (compound documents).
CVE-2021-26862	UPDATE	Updates the security of the Windows user interface. Updates to improve security when Windows performs basic operations. Updates to improve security when using Microsoft Office products.
CVE-2021-1693	UPDATE	-Adds the ability to set a group policy to show only the domain and username when a user logs in. - Addresses an issue that delays authentication traffic due to Netlogon scalability issues. - Addresses an issue where a principal in a trusted MIT domain does not obtain a Kerberos service ticket from Active Directory domain controllers (DCs).
CVE-2021-27095	IGNORE	improve security when using input devices such as a mouse, keyboard, or pen.
CVE-2021-27089	IGNORE	Update the default values of Internet Explorer registry keys(we do not use internet explorer)

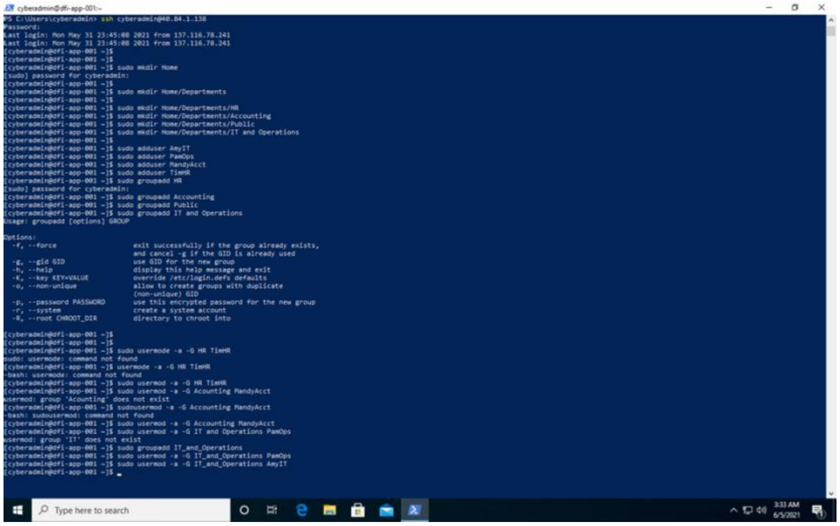
CVE-2021-28435	IGNORE	Addresses an issue with a heap leak that could cause explorer.exe to consume large amounts of memory. Updates the time zone for Volgograd, Russia from UTC + 4 to UTC + 3. Add a new time zone, UTC + 2: 00 Juba, for the Republic of South Sudan.

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.

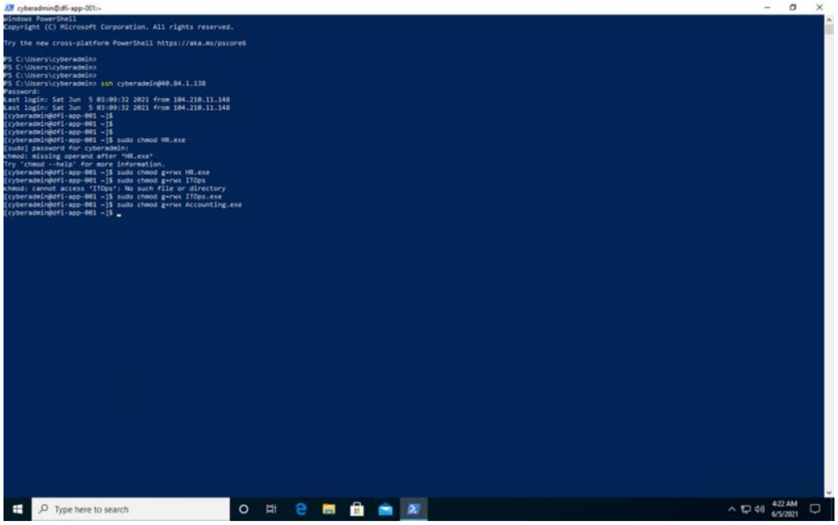
For documentation purposes, please explain the syntax for non-technical management on the change control board that meets weekly.



```
PS C:\Users\cyberadmin> ssh cyberadmin@40.84.1.138
Password:
Last login: Mon May 31 23:45:08 2021 from 137.116.78.241
Last login: Mon May 31 23:45:08 2021 from 137.116.78.241
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home/Departments
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home/Departments/HR
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home/Departments/Accounting
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home/Departments/Public
[cyberadmin@dfi-app-001 ~]$ sudo mkdir Home/Departments/IT and Operations
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo adduser AmyIT
[cyberadmin@dfi-app-001 ~]$ sudo adduser PamOps
[cyberadmin@dfi-app-001 ~]$ sudo adduser MandyAcct
[cyberadmin@dfi-app-001 ~]$ sudo adduser TimHR
[cyberadmin@dfi-app-001 ~]$ sudo groupadd HR
[sudo] password for cyberadmin:
[cyberadmin@dfi-app-001 ~]$ sudo groupadd Accounting
[cyberadmin@dfi-app-001 ~]$ sudo groupadd Public
[cyberadmin@dfi-app-001 ~]$ sudo groupadd IT and Operations
Usage: groupadd [options] GROUP

Options:
  -f, --force                   exit successfully if the group already exists,
                                and cancel -g if the GID is already used
  -g, --gid GID                 use GID for the new group
  -h, --help                    display this help message and exit
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -o, --non-unique              allow to create groups with duplicate
                                (non-unique) GID
  -p, --password PASSWORD       use this encrypted password for the new group
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into

[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo usermode -a -G HR TimHR
sudo: usermode: command not found
[cyberadmin@dfi-app-001 ~]$ usermode -a -G HR TimHR
-bash: usermode: command not found
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G HR TimHR
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G Acounting MandyAcct
usermod: group 'Acounting' does not exist
[cyberadmin@dfi-app-001 ~]$ sudousermod -a -G Accounting MandyAcct
-bash: sudousermod: command not found
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G Accounting MandyAcct
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G IT and Operations PamOps
usermod: group 'IT' does not exist
[cyberadmin@dfi-app-001 ~]$ sudo groupadd IT_and_Operations
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G IT_and_Operations PamOps
[cyberadmin@dfi-app-001 ~]$ sudo usermod -a -G IT_and_Operations AmyIT
[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:\Users\cyberadmin>
PS C:\Users\cyberadmin>
PS C:\Users\cyberadmin>
PS C:\Users\cyberadmin> ssh cyberadmin@40.84.1.138
Password:
Last login: Sat Jun  5 03:09:32 2021 from 104.210.11.148
Last login: Sat Jun  5 03:09:32 2021 from 104.210.11.148
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$
[cyberadmin@dfi-app-001 ~]$ sudo chmod HR.exe
[sudo] password for cyberadmin:
chmod: missing operand after 'HR.exe'
Try 'chmod --help' for more information.
[cyberadmin@dfi-app-001 ~]$ sudo chmod g+rwx HR.exe
[cyberadmin@dfi-app-001 ~]$ sudo chmod g+rwx ITOps
chmod: cannot access 'ITOps': No such file or directory
[cyberadmin@dfi-app-001 ~]$ sudo chmod g+rwx ITOps.exe
[cyberadmin@dfi-app-001 ~]$ sudo chmod g+rwx Accounting.exe
[cyberadmin@dfi-app-001 ~]$
```

We were able to performed this task using the following commands:

$mkdir: create directories
$adduser: create users
$addgroup: create groups
$usermod: adds users to groups
$chmod :change permissions
WRX: write, read, execute

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.

A:

After reviewing the the DFI_FW_Report, I could notice that in fact there is suspected/ unknow traffic. Based on security procedures and policies I would recommend the following:

- Block traffic by default and monitor user access

It is advisable to block all traffic to the network by default. Allow only some specific traffic to certain known services. This helps you to have control over who can access your network and prevents any security breaches from occurring.

The firewall being your first layer of protection against threats, must not allow access to anyone and everyone to alter the configuration. User permission control is necessary to ensure that only authorized administrators have access to change firewall configurations. Apart from this, every time an authorized administrator does change any configuration, it must be recorded in the log for audits and compliance. Any unwarranted configuration changes can thus be detected, and configuration restore may be implemented in such a case.

You can also create separate user profiles to provide various levels of access to the IT staff, only as much as needed for a job. Firewall logs must be monitored regularly to detect any unauthorized break-ins to the firewall, from inside or outside the network.

- Establish a firewall configuration change plan

Your network's firewall will need to be updated from time to time for various reasons. This is necessary to ensure that the firewall remains strong and capable of protecting against new threats. But it is important to have a change management plan so that the process is smooth and secure. Any unplanned configuration change leaves a loophole in your network's security.

A well-defined and robust firewall change management plan must include certain basic features:

1. It must define the changes that are required and their objectives.
2. It should also enlist the risks involved due to the policy changes, their impacts on the network, and a mitigation plan to minimize the risks.
3. A well-defined structure of change management workflow between various network teams.
4. Proper audit trails that record who made the change, why, and when.

- Optimize the firewall rules of your network

The firewall rules must be well-defined and optimized to provide the expected protection. Cleaning up your firewall rule base of any kind of unnecessary clutter can have a positive impact on your network security.

Your firewall rule base may have certain redundant elements, duplicates, or bloated unnecessary rules that make the guidelines complicated and less effective. It is important to get rid of such rules to have a clear set of guidelines that can be followed better.

To clean your firewall rule base, you must:

-Eliminate redundant or duplicate rules that slow down the firewall performance as they require the firewall to process more rules in its sequence than necessary.

-Remove the rules that are obsolete or no longer in use. These only make the firewall management more complex, and can even be a threat to network security if not updated.

-Remove shadowed rules that are not essential. These may lead to more critical rules being neglected.

-Conflicting rules must be eliminated.

-Any errors or inaccuracies in the rules must be eliminated as these may result in malfunctions.

- Update your firewall software regularly

Firewall vendors usually release software updates regularly. These updates address any new potential security threats by making minor changes to the software. It is important to keep updating your firewall software to ensure that your network is secure, and there are no loopholes in the system that could pose a threat to security. You must check from time to time if your firewall software is updated to the latest version.

- Conduct regular firewall security audits

Security audits are necessary to ensure that the firewall rules comply with the organizational, as well as external security regulations that apply to the network. Unauthorized firewall configuration changes that are a policy violation can cause non-compliance. It is important for administrators and IT security staff to carry out regular security audits to ensure no unauthorized changes have taken place.

This will also keep you updated on the necessary changes made to the firewall and warn you against any potential risks created by these changes. Security audits are most essential when there is a new firewall installed, firewall migration activity happening, or when there are bulk configuration changes made on firewalls.

- Have a centralized management tool for multi-vendor firewalls

Multi-vendor firewalls are quite common in most organizations. Companies prefer firewalls manufactured by different companies installed in the systems to offer additional layers of security. But the challenge here is that the architecture of firewalls from different manufacturers is usually different.

It is important to manage all your firewalls centrally at one place to ensure they are all functioning properly. Using a multi-vendor firewall management tool allows you to have a unified view of firewall policies and rules, enabling you to compare and manage firewall rules easily. You can also perform security auditing and reporting, troubleshoot configuration issues, and provide support with a gap analysis for firewall migration through this centralized management tool.

- Automate the process of firewall updating

With improvements in technology, many processes have become faster and easier. It may not always be possible for firewall administrators to constantly check for updates and perform software updates regularly. This leaves the network at risk of security breaches.

To avoid any lapse in updating your firewall, you can automate the process instead. An automated system can be scheduled to check for available updates and implement the updates when they find one. This reduces the need for human intervention and keeps the firewall secure and robust at all times.

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.

A:

DFI Security report.

DFI has been having an exponential growth over the last years, as the organization grow, responsibilities to protect its assets grow as well, based on the industry I was able to perform different security configurations that will just not improve the security but will make vulnerabilities and risk management easier.
I could perform an analysis to DFI servers where I could find some weak points or configurations that didn't necessarily help to protect its assets and base on that analysis, I made my recommendations.
I was able to set firewall rules to allow secure connection with DFI partners, provide VPN encryption recommendations, set Intrusion detection system rules to better protect DFI servers, provide SOAR products recommendation, review logs and provide security recommendations, review updates and provide advices on whether they need to be installed or ignored, create directories, groups and user and configure permissions for better use and management of information, review login attempts report and provide mitigation response advices.

DFI still needs to work in improving its security, they are on the right path but handling so much sensitive information make them a desired target for malicious activities, been aware of that we could say there are more security configurations that could be done to improve DFI security and performance.
Enterprises like DFI should ensure network infrastructure is fully documented and architecture diagrams are kept up to date. It is important for key infrastructure components to have vendor support for patches and feature upgrades. Upgrade End-of-Life (EOL) components before the date they will be out of support or apply mitigating controls to isolate them. Enterprises need to monitor their infrastructure versions and configurations for vulnerabilities that would require them to upgrade the network devices to the latest secure and stable version that does not impact the infrastructure. CONTROL CIS Controls v8 Control 12: Network Infrastructure Management 39 An up-to-date network architecture diagram, including security architecture diagrams, are an important foundation for infrastructure management. Next is having complete account management for access control, logging, and monitoring. Finally, infrastructure administration should only be performed over secure protocols, with strong authentication (MFA for PAM), and from dedicated administrative devices or out-of band networks. Commercial tools can be helpful to evaluate the rule sets of network filtering devices to determine whether they are consistent or in conflict. This provides an automated sanity check of network filters. These tools search for errors in rule sets or Access Controls Lists (ACLs) that may allow unintended services through the network device. Such tools should be run each time significant changes are made to firewall rule sets, router ACLs, or other filtering technologies.

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.