UDACITY

Defending and Securing Systems

Monitoring and Securing the DFI Environment

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!

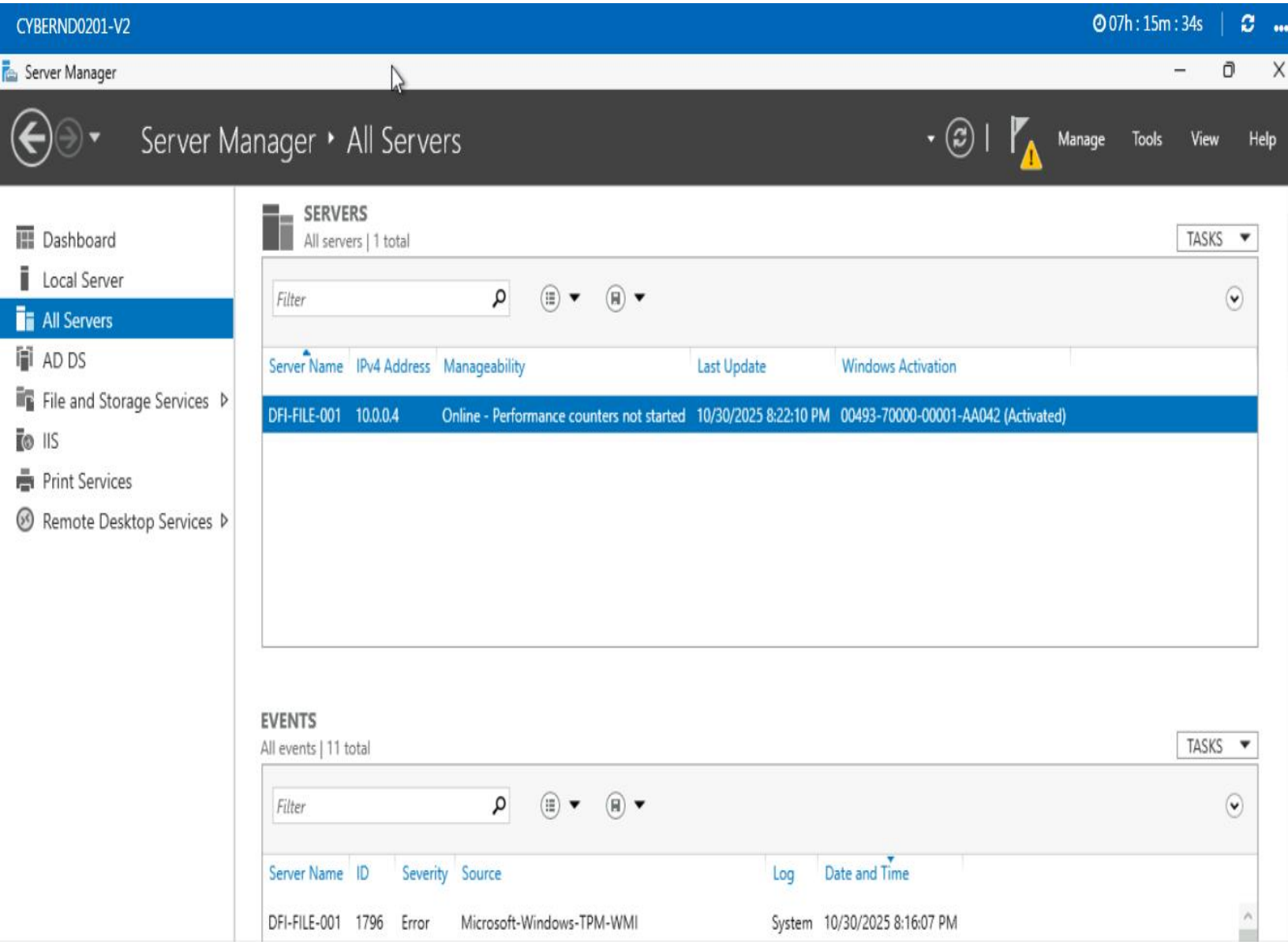
Once you are settled in and finished orientation, we have your first 2-Weeks assignments ready.

Week 1:

Name : LUNA DAHAL

1. Connect - Evidence Windows

All of the subsequent steps will take place in the DFI environment. Use the Cloud Lab CYBERND0201 to connect with the Windows server provided.
Provide a screenshot of a successful connection below.



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.)
Looking at the following requirements, specifically:

- C:\Departments\HR Folder Permissions (that are incorrectly granted)
- Roles Changes (disabled/enabled)
- Services changes (disabled/enabled)

2. Security Analysis: HR and Roles

C:\Departments\HR Folder Permissions	
Permission Problem:	HR has been given Full Control. It violates principle of least privilege , risk of data leakage and breach of regulatory compliance.
Recommendation:	HR should be assigned “modify” permission only to create , add ,delete any employees job records.
Why it helps:	It strengthens organization security by meeting regulatory compliance and limiting the potential attacks by enforcing the proper role-based access.

2. Security Analysis: HR and Roles

Servers Role Evaluation

1. Role: Active Directory Domain Services (AD DS)
Recommendation: ENABLE
How it helps: Centralizes authentication, enforces security policies with Group Policy, and enables least privilege HR folder access.

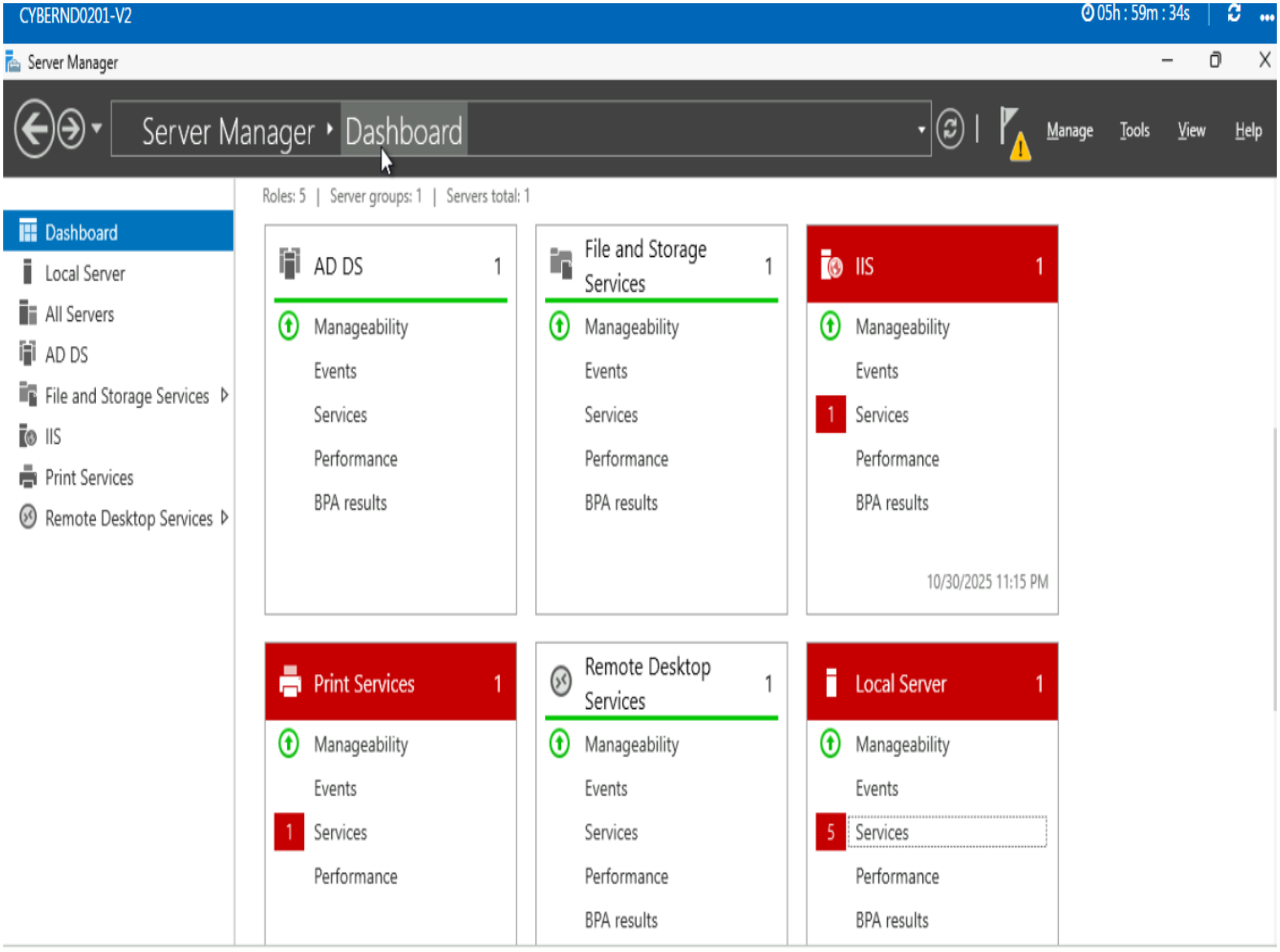
2. Role: File and Storage Services
Recommendation: ENABLE
How it helps: Secures HR data with NTFS permissions, allows encryption and auditing, and ensures only authorized access.

3. Role: Internet Information Services (IIS)
Recommendation: DISABLE
How it helps: Eliminates unnecessary web vulnerabilities, reduces attack surface, and aligns with least privilege principles.

4. Role: Print Services
Recommendation: ENABLE IF NEEDED / DISABLE IF NOT
How it helps: Centralizes printer management and audit if enabled; otherwise, disables an unnecessary service for security.

5. Role: Remote Desktop Services (RDS)
Recommendation: DISABLE unless required for administration
How it helps: Reduces attack surface unless remote management is necessary, otherwise must be tightly secured.

2. Security Analysis: HR and Roles



2. Security Analysis: Services

Click the Start button, type services.msc, and press Enter. Review the list of services and identify any that are disabled but should be running.

Services that should run	
Service name	Reason
Ipsec Policy Agent	To improve the network connectivity issues . And to enable windows defender firewall
Application Information	Allows application to run as administrator
System Guard Run Time Monitor Broker	The service is important for monitoring the platform's integrity and is enabled by default in older versions

2. Security Analysis: Services

Click the Start button, type services.msc, and press Enter. Review the list of services and identify any that are enabled but should not be running.

Services that should NOT run	
Service name	Reason (Disable when NOT, in Use)
Windows Print Spooler	Disabling reduces the attacks surface, and it aligns with Defense in Depth.
OpenSSH SSH Server	Disabling reduces the exposure to remote attacks.
World Wide Web Publishing Service (W3SVC)	Disabling limits the Entry point for attackers.

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 & DFI-File-002 access via port tcp-9082.

The first partner's IP is 21.19.241.63 and DFI-File-001's IP is 172.21.30.44.
The second partner's IP is 21.19.241.64 and DFI-File-002's IP is 172.21.30.45.

For this exercise assume the two IP objects **have not** been created in the firewall. 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 rule and explanation on the next slide.

3. Firewall Rules - Evidence

Firewall Rule
RULE 1: access-list *DFI-Ingress* extended permit tcp host 21.19.241.63 host 172.21.30.44 eq 9082 **RULE 2:** access-list *DFI-Ingress* extended permit tcp host 21.19.241.64 host 172.21.30.45 eq 9082
Explanation
Access-list : Firewall Rule *DFI Ingress* : Name of the firewall interface receiving incoming traffic. extended permit tcp : specifies that TCP traffic is allowed and not denied from source to destination. host 21.19.241.63 / 64 : source IP host 172.21.30.44 / 45 : destination IP eq 9082 : Traffic is allowed only on port 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 in 3 to 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

AES – GCM-256	
I recommend **AES-GCM-256** to DFI for creating a payroll processing partnership which will involve a VPN connection because it is currently Cisco's recommended strong encryption for site-to-site VPNs, ensuring confidentiality and integrity of sensitive payroll data.	

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. Write your answers on the next slide.

5. IDS Rule

System Admin Rule #1	
Rule 1:	alert icmp any any -> 172.21.30.44 any (msg: “icmp ddos attack attempt” sid 1000005 ; rev 1;)
Explanation:	**alert icmp** → Watch ICMP traffic **any any** → From source IP and port **-> :** operator denotes going to **172.21.30.44 any** → IP and ICMP doesn’t have ports, so used any. **msg: "ICMP DDoS attack attempt"** → The message shown when this alert triggers. **sid:1000005** → Unique ID for this rule. **rev:1** → Version number of the rule.

5. IDS Rule

System Admin Rule #2	
Rule 2:	alert udp any any -> 172.21.30.55 69 (msg:"Attempt to connect VoIP TFTP server"; sid:1000006; rev:1;)
Explanation:	**alert udp** → Watch UDP traffic (TFTP uses UDP). **udp** → TFTP uses the UDP protocol **any any** → From any computer or port. **-> 172.21.30.55 69** → Going to the VoIP server on TFTP (port 69 is the default port for TFTP,) **msg** → What the alert will say **sid** → Unique ID for this rule **Rev 1** → Version of 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.

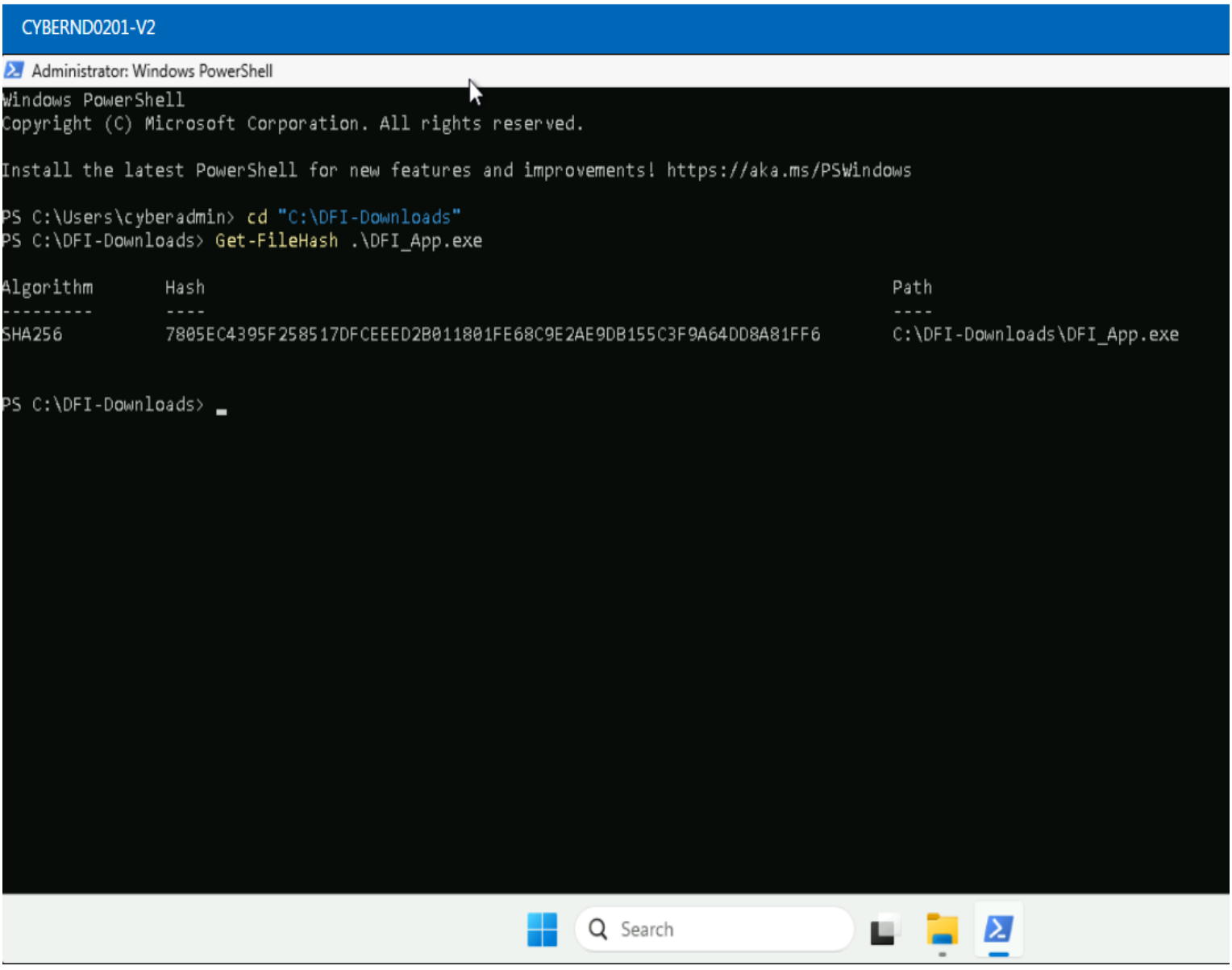
Hash:
7805EC4395F258517DFCEEED2B011801FE68C9E2AE9DB155C3F9A64DD8A81FF6

Perform a file hash verification and submit a screenshot of your command and output. The File is stored on the Windows Server in C Drive under DFI-Download.

Place your screenshot verification on the next slide.

6. File Hash Verification

Screenshot:



Week 2:

LUNA DAHAL

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 table 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.

7. Automation - Evidence

DFI Area/Technology	Solution	Justification for Recommendation
Incident Response / Soar Integration	Implement a SOAR platform to automatically handle alerts, run playbooks, and coordinate between IDS, firewall, and email systems.	Reduces response time by automating repetitive security tasks
IDS and Firewall Alert	Configure automation scripts or SOAR playbooks to auto-block malicious IPs and quarantine affected hosts when certain IDS signatures trigger.	Prevents further damage by instantly containing threats without waiting for manual review.
User Access Management	Automate account provisioning and deprovisioning with Active Directory scripts or identity management tools.	Reduces insider threat risks by ensuring users get only necessary access.
Patch Management	Implement automated Windows Server Update Services (WSUS).	Keeps systems updated and eliminates vulnerabilities due to delayed patches.

8. Logging RDP Attempts - Instructions

The IT Manager suspects that someone has been attempting to login to the windows server via RDP.

Prepare a report that lists unsuccessful connection attempts. Using the Event Viewer, filter the Windows Security Logs for Event 4625.

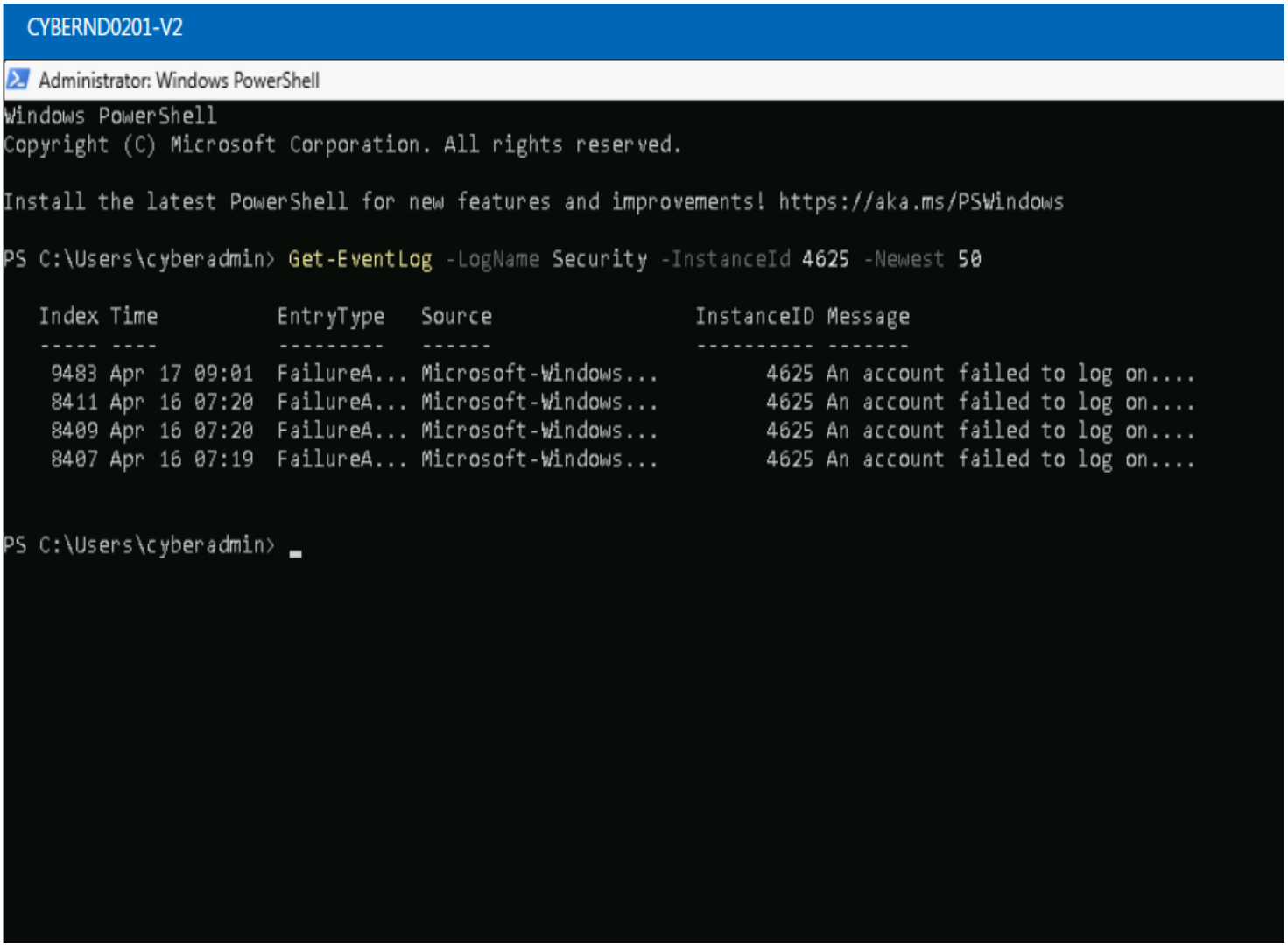
For your deliverable, take a screenshot of the Event Viewer window. Then in 3-5 sentences, explain your findings, recommendations and justifications to the IT Manager.

Place your screenshot and the explanation on the following slide.

8. Logging RDP Attempts

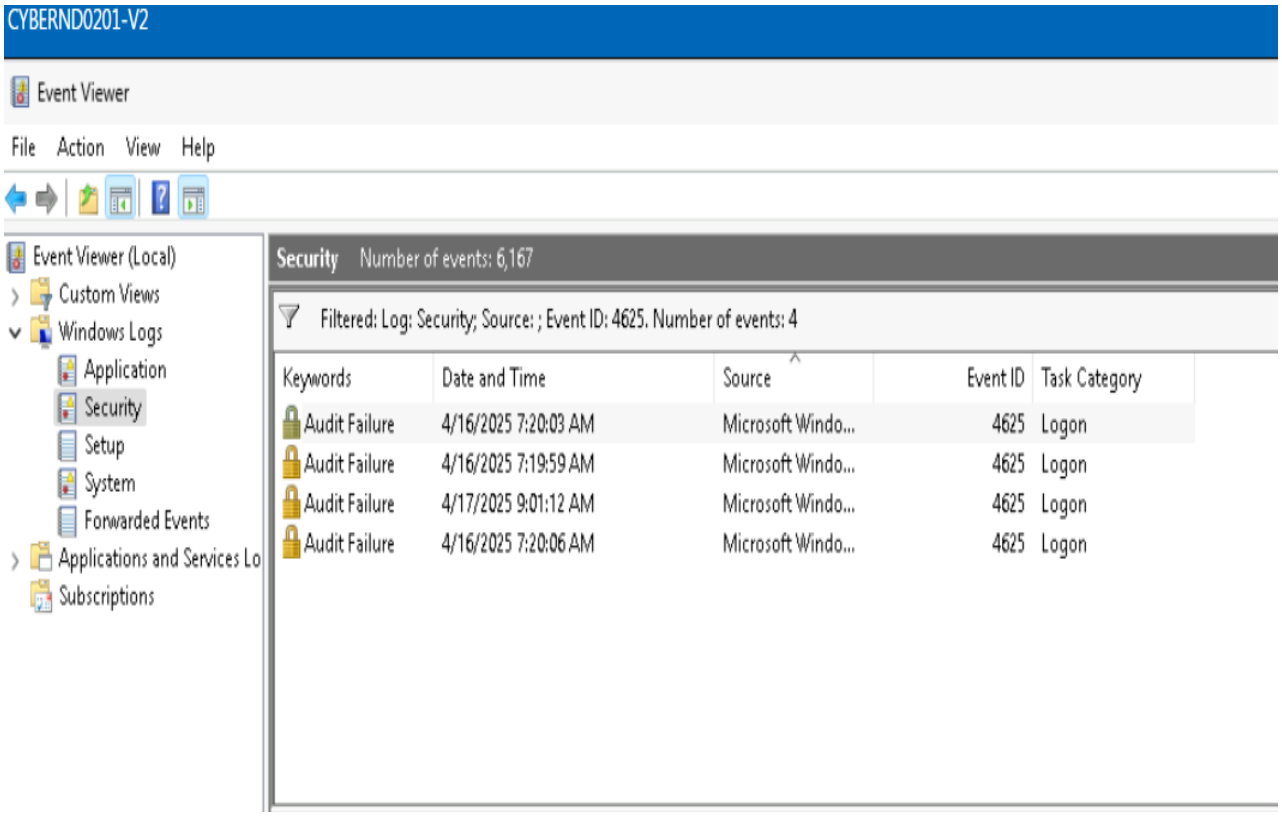
Screenshot of PowerShell after excexuting command

Get-EventLog -Logname Security -InstanceID 4625 -Newest 25



8. Logging RDP Attempts

Screenshot of Event Viewer



I found 4 audit failures in the Security log, which appears to be a normal number and does not indicate a significant security concern.

But if there were a higher number of failed login attempts, we could have implemented additional measures, such as:

•Enforcing account lockouts after a set number of failed attempts.
•Monitoring and blocking suspicious IP addresses automatically.
•Enabling multi-factor authentication (MFA) for RDP access.

9. Linux Data Management

The IT Manager has requested your help with creating directories, users and groups on the Linux server (reachable by ssh from your machine or the Windows machine).

- The root directory should be '/home'
- The first subdirectory should be "Departments" with subdirectories: HR, Accounting, Public, IT and Operations.
- Create the groups for HR, Accounting, Public, IT and Operations.
- Set owner permissions for their respective folders 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.

You need to document your work after you finished it. In the following slides provide screenshots and explain the syntax of the commands you used for non-technical management on the change control board that meets weekly.

9. Linux Directories

Step 1: Connect to ssh cyberadmin@20.253.221.106

Type yes in the power shell

Enter pwd

sudo su *[switch user to root]*

cd /home [*Go to the root home directory]*

Step 2: #To Create Sub Directory

mkdir -p Departments

9. Linux Groups

Step 3: #To create sub directories inside Departments :

mkdir –p Departments/HR

[i*f Departments doesn't exist, mkdir -p Departments/HR will first create Departments, then create HR inside it and doesnot throw an error if the directory already exists]*

mkdir –p Departments/Accounting

mkdir –p Departments/Public

mkdir –p Departments/IT

mkdir –p Departments/Operations

#Create the Groups

sudo groupadd HR

sudo groupadd Accounting

sudo groupadd Public

sudo groupadd IT

sudo groupadd Operations

9. Linux Directories & Groups

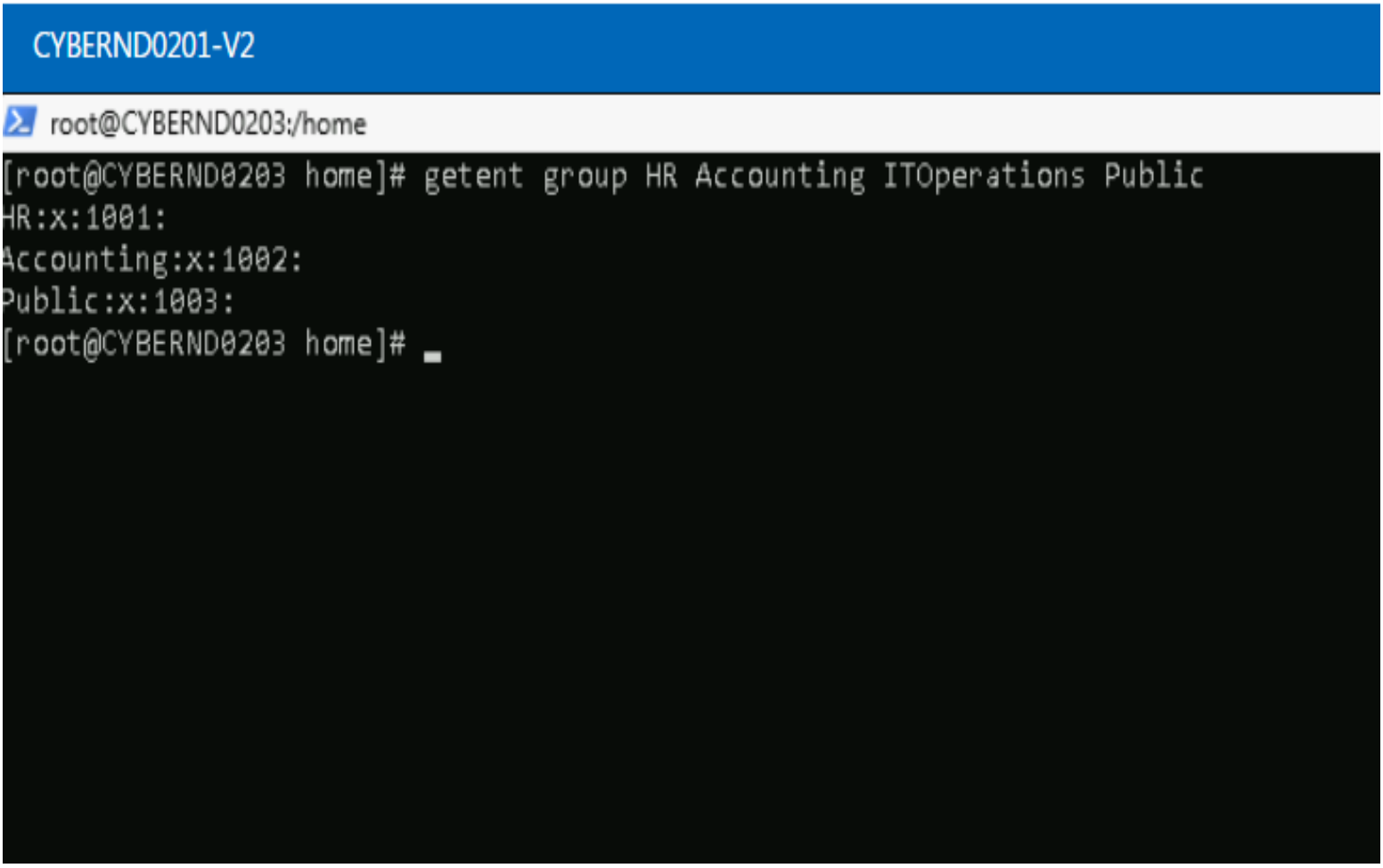
CYBERND0201-V2

root@CYBERND0203:/home

```
[root@CYBERND0203 home]# mkdir -p Departments
[root@CYBERND0203 home]# mkdir -p Departments/HR
[root@CYBERND0203 home]# mkdir -p Departments/Accounting
[root@CYBERND0203 home]# mkdir -p Departments/Public
[root@CYBERND0203 home]# mkdir -p Departments/IT
[root@CYBERND0203 home]# mkdir -p Departments/Operations
[root@CYBERND0203 home]# sudo groupadd HR
[root@CYBERND0203 home]# sudo groupadd Accounting
[root@CYBERND0203 home]# sudo groupadd Public
[root@CYBERND0203 home]# sudo groupadd IT
[root@CYBERND0203 home]# sudo groupadd Operations
[root@CYBERND0203 home]# tree Departments
Departments
├── Accounting
├── HR
├── IT
├── Operations
└── Public

5 directories, 0 files
[root@CYBERND0203 home]#
```

9. Linux Groups



Checks the system and lists all five groups, showing their GID and member users

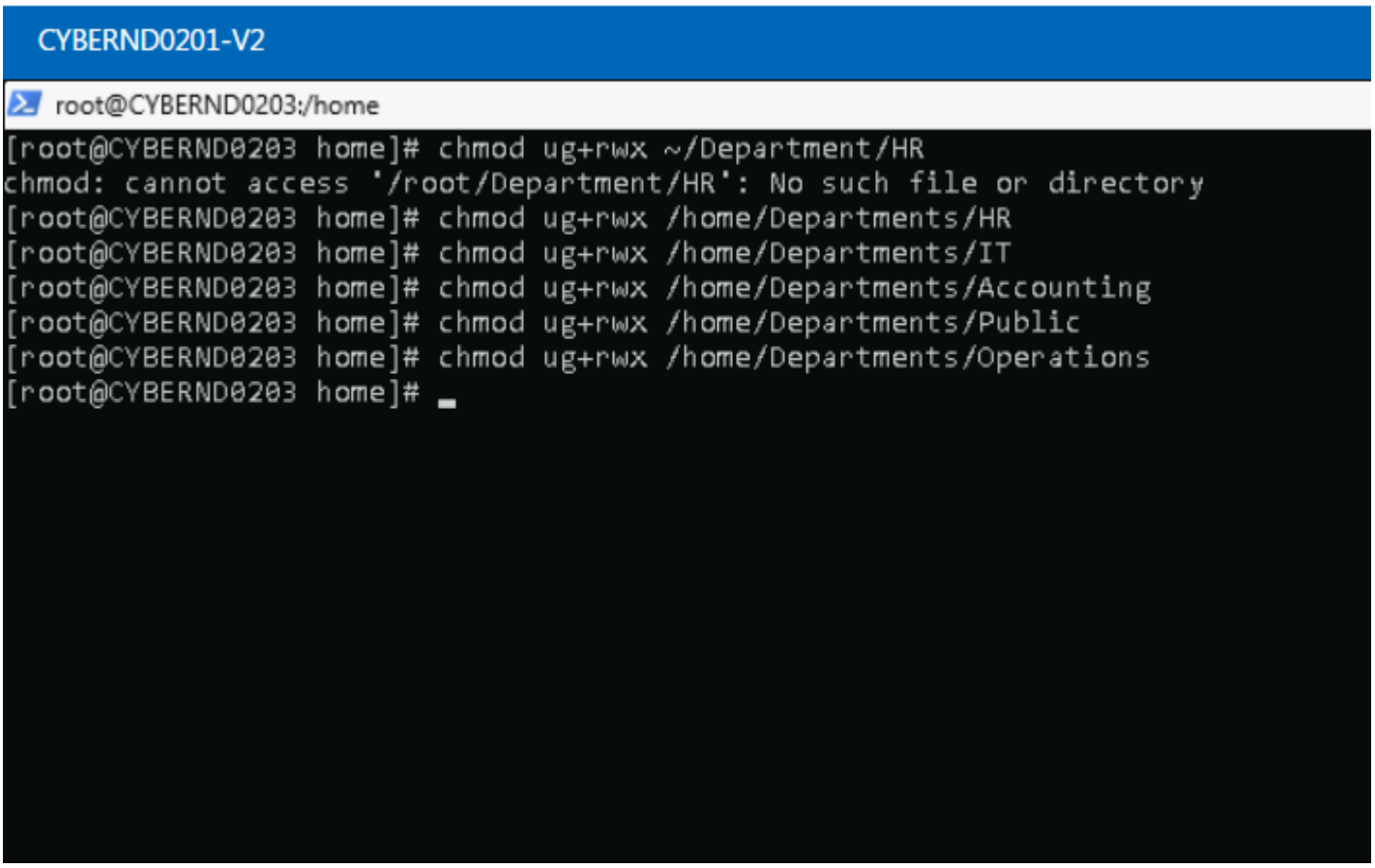
9. Linux Folder Permissions

CYBERND0201-V2

root@CYBERND0203:/home

```
[root@CYBERND0203 home]# sudo chown :HR /home/Departments/HR
[root@CYBERND0203 home]# sudo chown :Accounting /home/Departments/Accounting
[root@CYBERND0203 home]# sudo chown :Public /home/Departments/Public
[root@CYBERND0203 home]# sudo chown :IT /home/Departments/IT
[root@CYBERND0203 home]# sudo chown :Operations /home/Dpartments/Operations
chown: cannot access '/home/Dpartments/Operations': No such file or directory
[root@CYBERND0203 home]# sudo chown :Operations /home/Dpartments/Operations
chown: cannot access '/home/Dpartments/Operations': No such file or directory
[root@CYBERND0203 home]# sudo chown :Operations /home/Departments/Operations
[root@CYBERND0203 home]#
```

9. Linux Folder Permissions



U → user/owner of the file/folder
G → group assigned to the file/folder
+rwx → add read (r) , write (w) , execute (x) permisiion

9. User Add to their group

CYBERND0201-V2

root@CYBERND0203:/home

```
[root@CYBERND0203 home]# useradd -g IT AmyIT
[root@CYBERND0203 home]# useradd -g HR TimHR
[root@CYBERND0203 home]# useradd -g Operations PamOps
[root@CYBERND0203 home]# useradd -g Accounting MandyAcct
[root@CYBERND0203 home]#
```

9. More supporting Screenshots

CYBERND0201-V2

root@CYBERND0203:/home

```
[root@CYBERND0203 home]# tree /home/Departments
/home/Departments
├── Accounting
├── HR
├── IT
├── Operations
└── Public

5 directories, 0 files
[root@CYBERND0203 home]#
```

CYBERND0201-V2

root@CYBERND0203:/home

```
[root@CYBERND0203 home]# tree -pug /home/Departments
/home/Departments
├── [drwxrwxr-x root     Accounting]  Accounting
├── [drwxrwxr-x root     HR        ]  HR
├── [drwxrwxr-x root     IT        ]  IT
├── [drwxrwxr-x root     Operations]  Operations
└── [drwxrwxr-x root     Public    ]  Public

5 directories, 0 files
[root@CYBERND0203 home]# getent group HR Acoounting IT Operations Public
HR:x:1001:
IT:x:1004:
Operations:x:1005:
Public:x:1003:
[root@CYBERND0203 home]# getent group IP
[root@CYBERND0203 home]# getent group HR
HR:x:1001:
[root@CYBERND0203 home]# getent group Operations
Operations:x:1005:
[root@CYBERND0203 home]# getent group Accounting
Accounting:x:1002:
```

10. Firewall Alert Response

The IT Manager took a look at firewall alerts in the **DFI_FW_Report** and was concerned with some traffic she saw. Please take a look and provide a mitigation response to the firewall report in that file.
Remember to justify your mitigation strategy in 3 - 5 sentences.

This file is available from the project resources **DFI_FW_Report as xlsx and Google Sheets**. Please view/download and use this file to complete this task.

The firewall logs show that many computers from different countries are trying to break into our SSH servers by guessing usernames and passwords over port 22.
These are brute-force attacks, meaning hackers are repeatedly trying different login combinations to find weak passwords. It shows that both local and international sources are scanning our network for vulnerable SSH accounts.

10. Firewall Alert Response

The most effective mitigation strategy is to block any unauthorized external SSH access, use strong login methods such as SSH keys or multi-factor authentication (MFA), and monitor for any successful break-ins.
This approach helps protect the system by reducing possible entry points for attackers, preventing password guessing, and detecting compromised accounts early.

11. Status Report and Next Steps

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.

[Provide your Status Report on the next slide.]

11. Status Report

Status Report
In my first two weeks, I improved DFI's security by making several practical updates. I handled Linux data safely, monitored remote desktop (RDP) login attempts to detect unauthorized access, and automated routine security tasks to boost efficiency and catch threats sooner. I verified file hashes to ensure data integrity and prevent tampering. I also set up new IDS rules in Snort and updated Cisco firewall policies to block malicious traffic. Additionally, I implemented VPN encryption to secure remote connections and protect sensitive data in transit. These measures strengthen our defense-in-depth approach, adding multiple layers of protection across the network, systems, and data.

11. Next Steps

Security Product Recommendations:

Next Gen Firewall : This firewall offers advanced intrusion prevention, deep packet inspection, and real-time threat intelligence, which makes it ideal for blocking external attacks and monitoring suspicious traffic.

Intrusion Detection System : It is powerful open-source IDS that detects and alerts on network threats using customizable rules. It is effective for monitoring unauthorized access attempts, including brute-force attacks and known malware patterns.

11. Next Steps

Security Policy Recommendations:

SIEM (Security Information and Event Management) : It is log, aggregator which analyzes the logs to allow alerting, dashboard creation and efficient queries to run.

Logging and Monitoring Policy : Continuous logging of RDP attempts, failed logins, and network traffic provides an audit trail for incident investigation and enables early threat detection.

12. File Encryption

As your final task, encrypt the PDF using 7zip with a strong password. Password complexity: 15 or more characters and a combination of alphanumerics and special characters.

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.