Scenario:

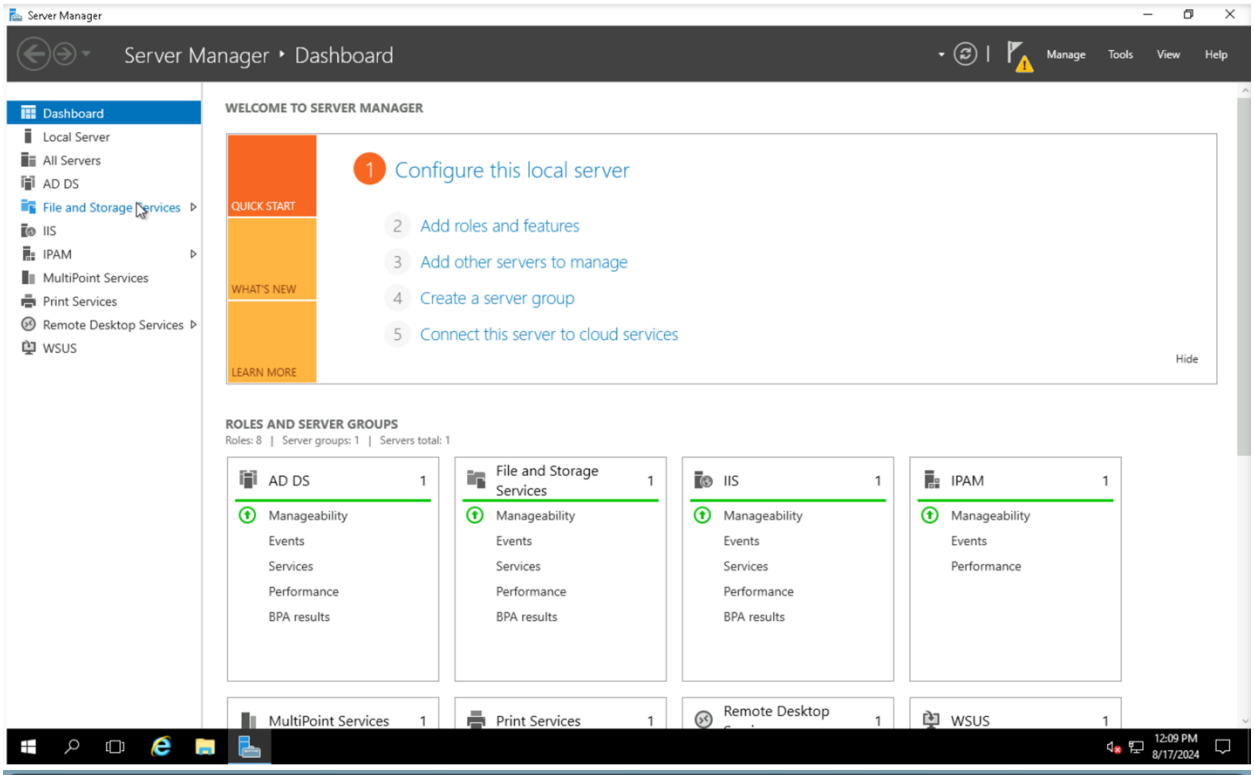
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result, is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI, we are happy to bring you on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

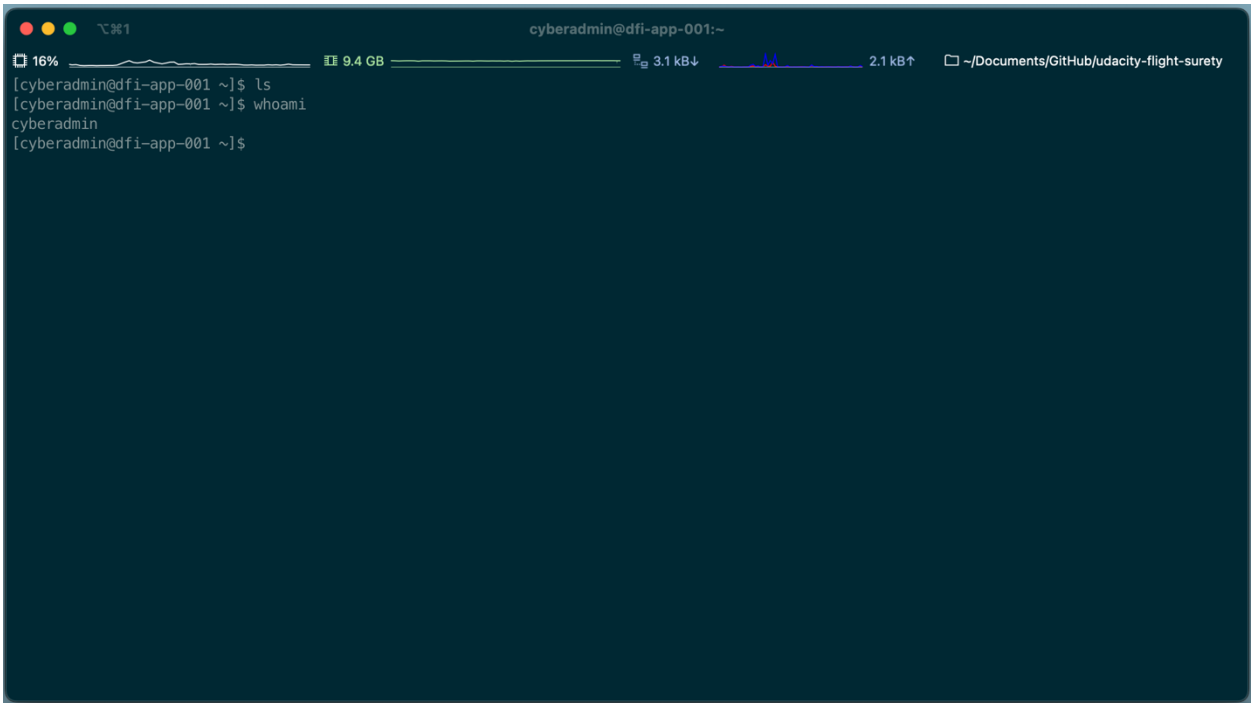
Week One:

1. **Connect to the servers:**

All of the subsequent steps will take place in the DFI environment. To get started, connect to the Windows server 2016 and Linux (CentOS) machines.

- **Windows server 2016** - If you are using Udacity cloud lab, you can directly log into the machine in the classroom. If you have set up the Windows server 2016 VM in your personal Azure account, you will have to use the RDP to connect.
- **Linux (CentOS) server** - If you are using Udacity cloud lab, you can log in using via SSH using Terminal/Gitbash/OpenSSH/Bastion. If you have set up the Linux server in your personal Azure account, you will have to use SSH to connect.
- Alternatively, you can use the **Windows 10** machine as a JumpVM for the other two VMs. Meaning, that you can use the Windows 10 VM to:
    - log into the Windows server 2016 via RDP
    - log into the Linux server via SSH using PuTTy, Gitbash, or OpenSSH.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
IIS
IPAM
MultiPoint Services
Print Services
Remote Desktop Services
WSUS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 8 | Server groups: 1 | Servers total: 1
AD DS 1
File and Storage Services 1
IIS 1
IPAM 1
Manageability
Events
Services
Performance
BPA results
MultiPoint Services 1
Print Services 1
Remote Desktop 1
WSUS 1
12:09 PM
8/17/2024


cyberadmin@dfi-app-001:~
16%
9.4 GB
3.1 kB↓
2.1 kB↑
~/Documents/GitHub/udacity-flight-surety
[cyberadmin@dfi-app-001 ~]$ ls
[cyberadmin@dfi-app-001 ~]$ whoami
cyberadmin
[cyberadmin@dfi-app-001 ~]$

2. **Security Analysis:**

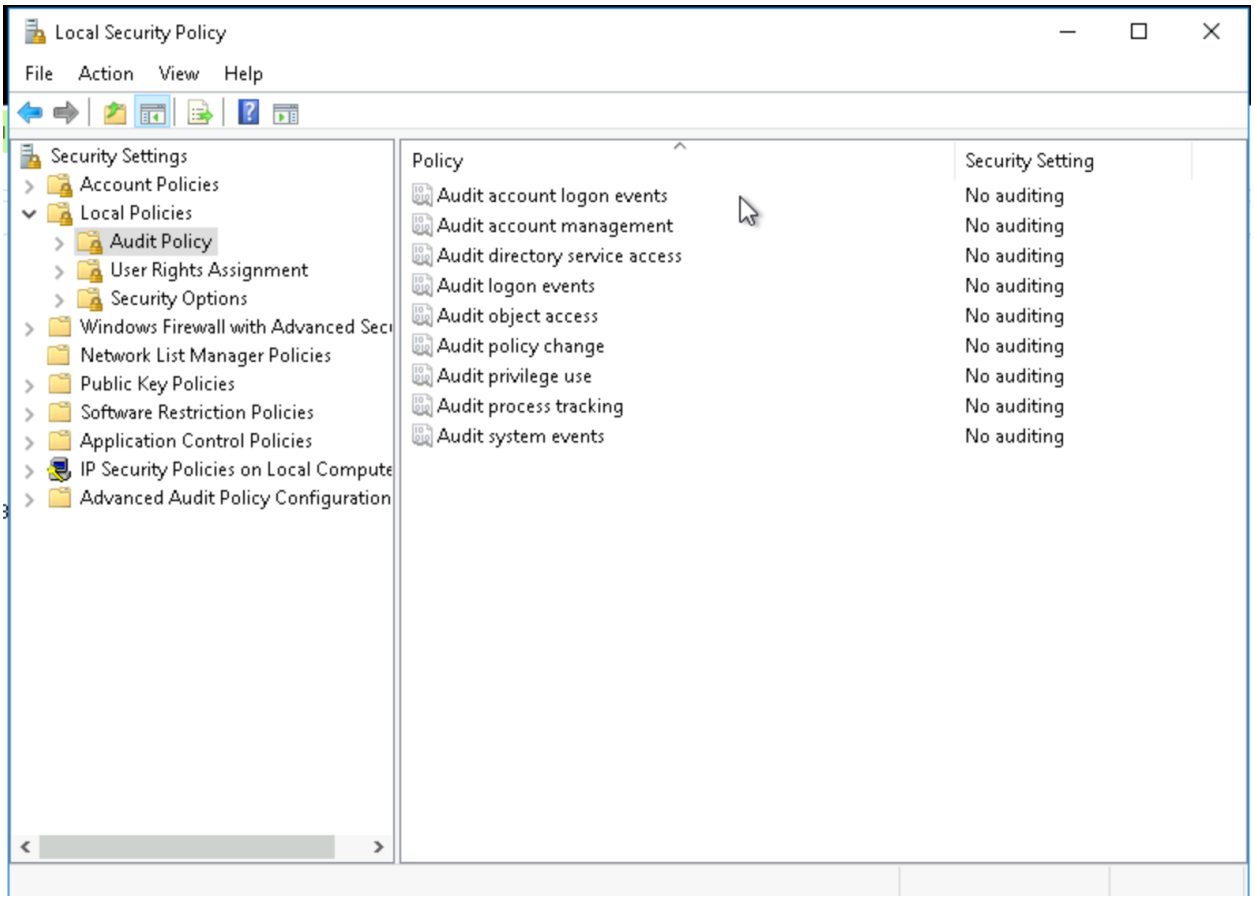
DFI has an excellent SysAdmin team, but they have been focused on system reliability and scaling to meet our growing needs and as a result, security may not be as tight as we'd like. Your first assignment is to familiarize yourself with our file and application servers.

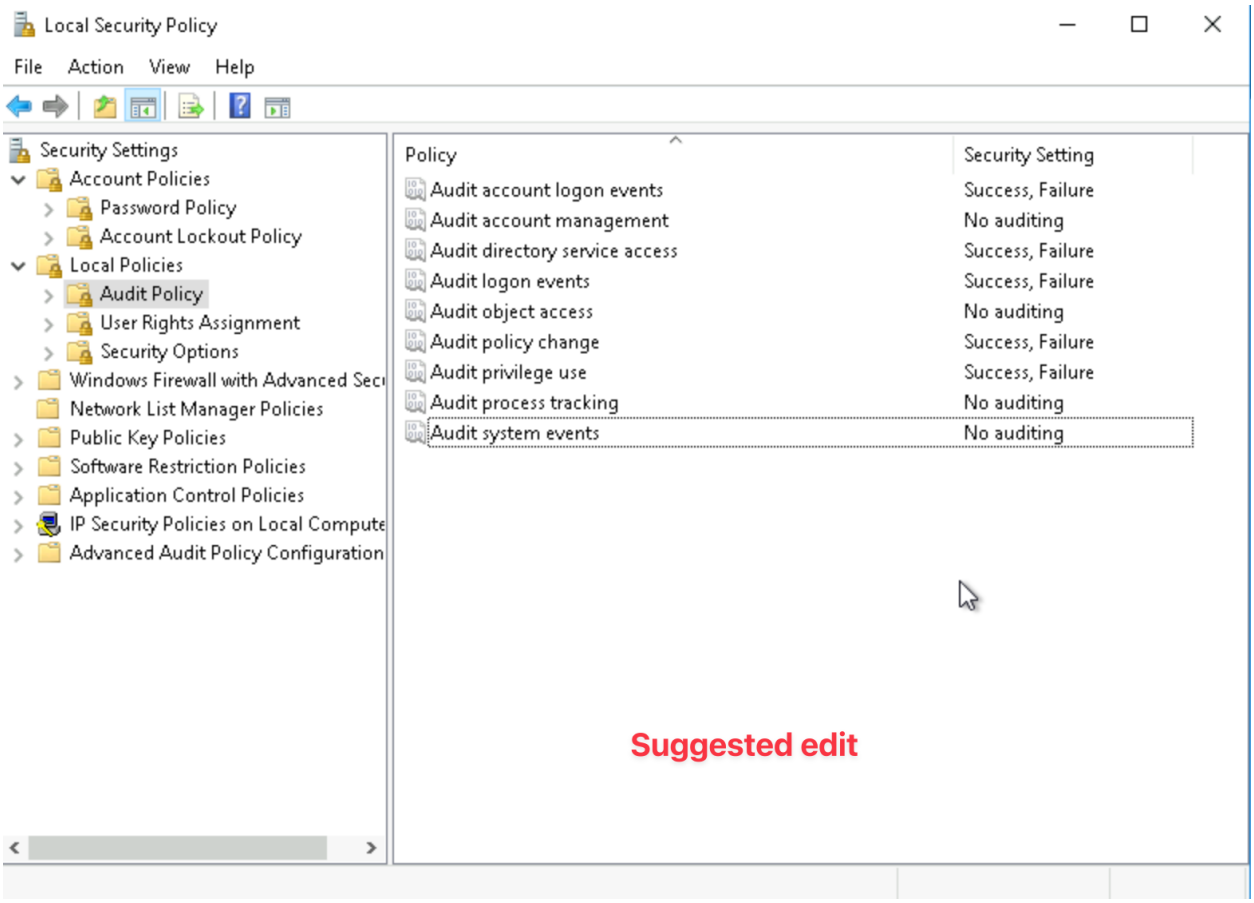
Please perform an analysis of the Windows server and provide a written report detailing any security configuration issues found and a brief explanation and justification of the changes you recommend. DFI is a PCI-compliant organization and will likely be Sarbanes-Oxley in the near future.

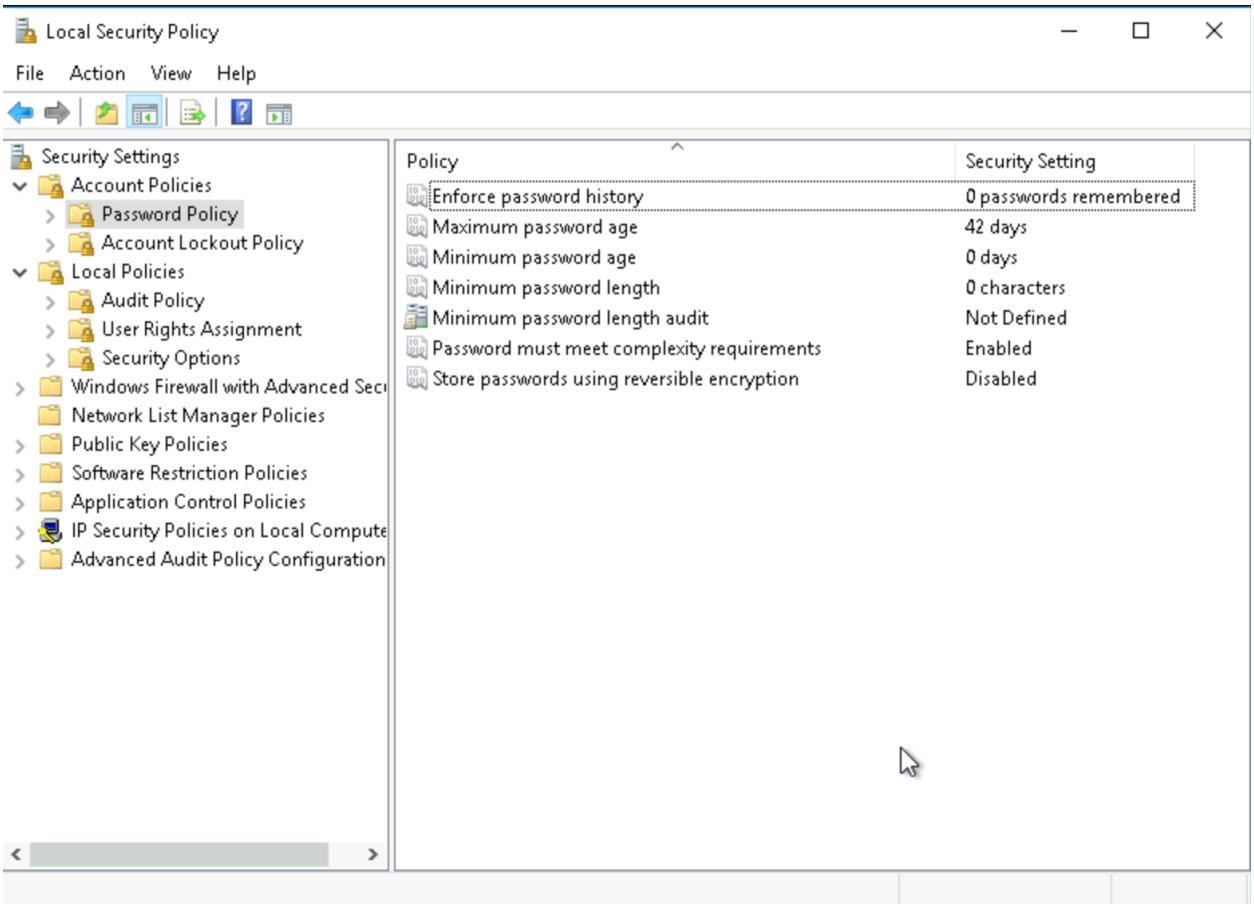
Use NIST, Microsoft, Defense-in-Depth, Principle of Least Privilege, and other resources to determine the changes that should be made. Note changes can be to **add/remove/change** services, permissions, and other settings. Defense-in-Depth documentation. NIST 800-123 (other NIST documents could also apply.)

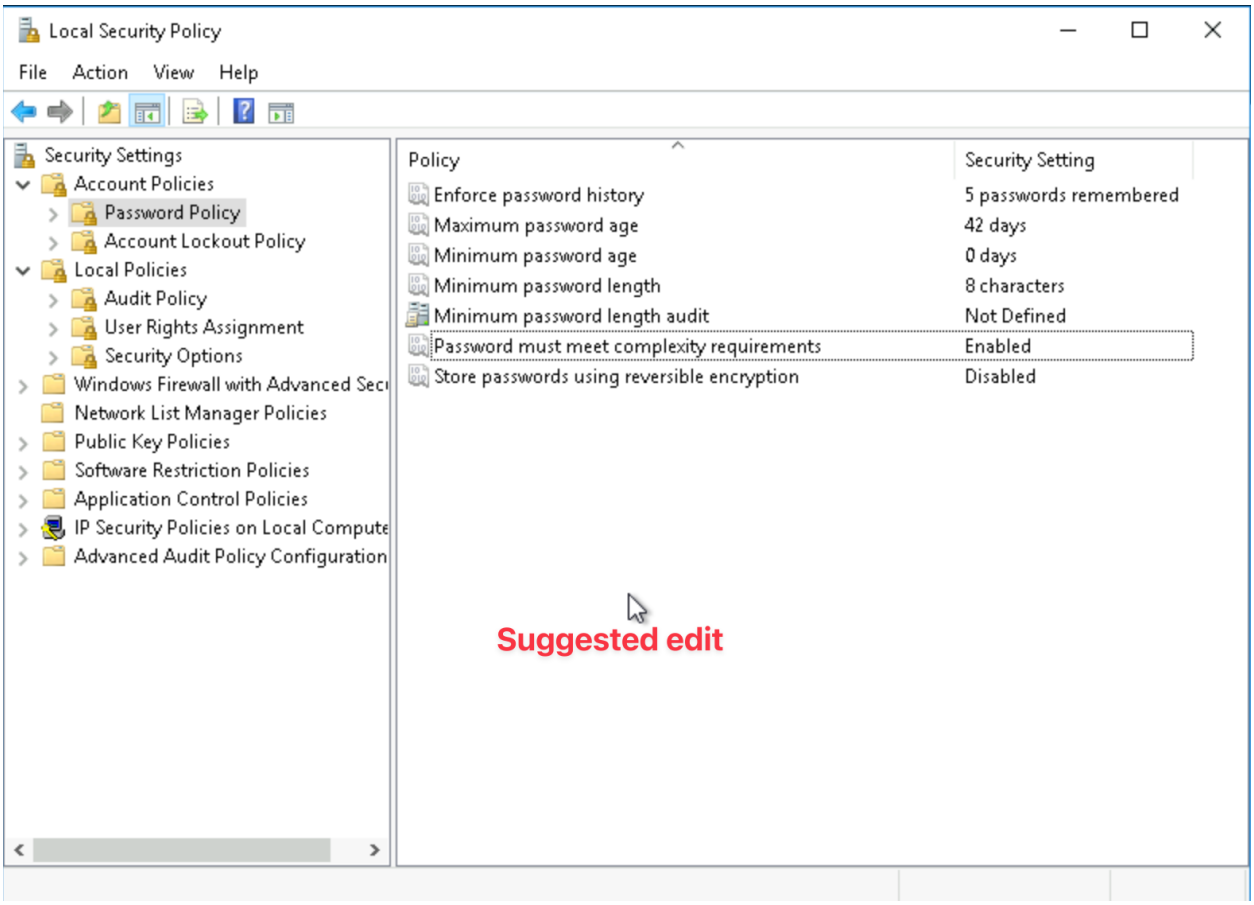
ELEMENT	SUGGESTED ACTIVITY	CONSIDERATION
HR Directory	Remove access to Users group	This folder contains sensitive information and only authorized users should be able to access it.
Rationalize Admin Users	Reconsider the actual Administration structure for the server. Actually, 3 accounts has admin permissions on it (Udacity, Cyberadmin and DFI-Admin)	Having multiple admin accounts leads to decrease security over the server. It is possible that non all of the current three accounts really need admin privilege over the server. If this is the case, I suggest to remove admin permission to them.
Auditing	Implement local auditing for Policy and Accounts	An appropriate auditing for Policies and Accounts will improve
Enforce account security requirements	Implement an appropriate lockout threshold and minimum password strength	In order to protect access from malicious logon attempts, I suggest to implement an adequate lockout threshold to be combined with an appropriate privacy strength policy.
Rationalize Groups	Remove groups that only have 1 user.	IT, HR, Accounting -> Only 1 account related. There is no need for a role wirth a single user on it. 3 groups contains only one user. If this is the case and we don't assume to hire new employers that soon that will fit onto that specifig group, I suggest to

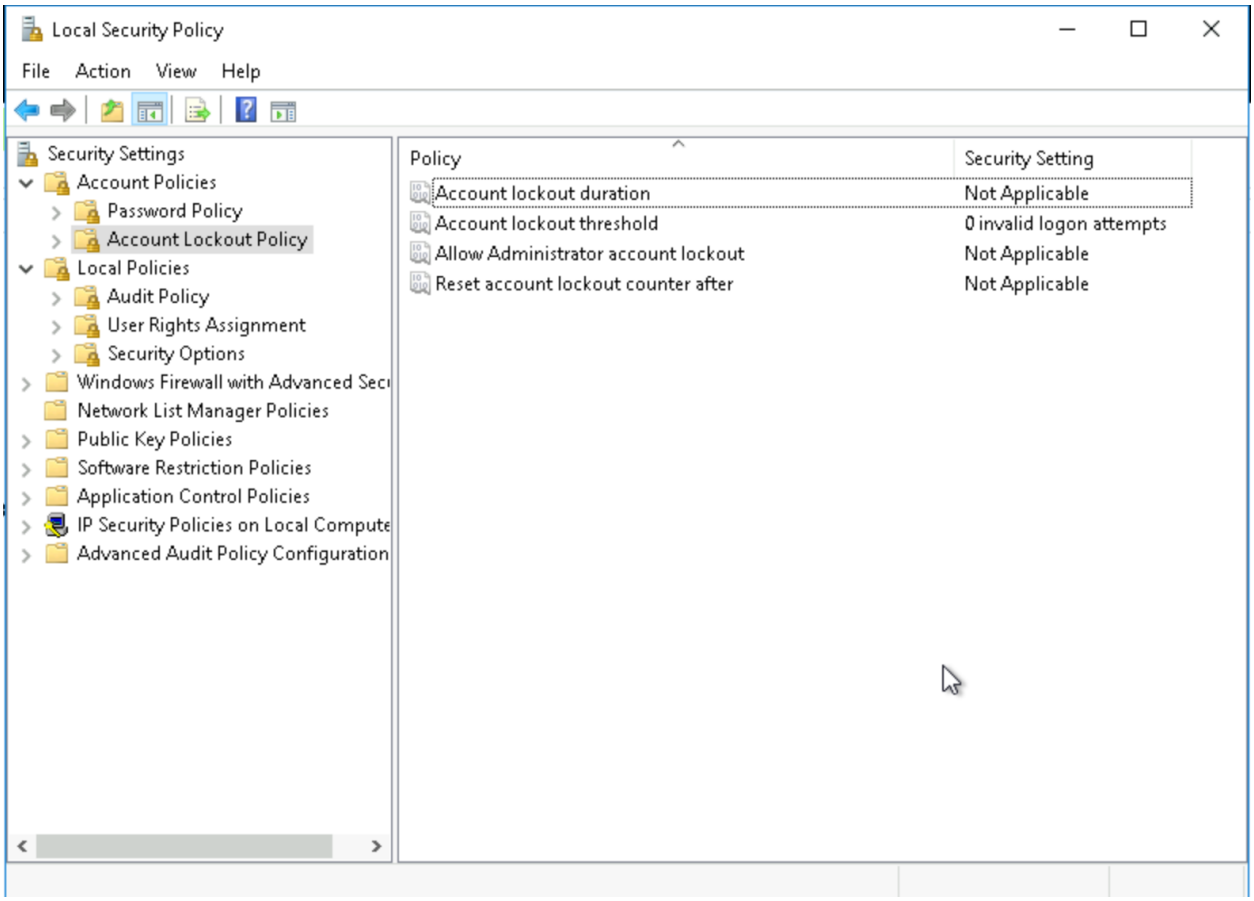
		remove them in order to simplify security procedures and streamline security process.
Elevate User Account Control Settings	Elevate setting to “Always Notify”	We are working on a server that contains sensitive information. The current setting already allows for a good level of logging but in my opinion it is necessary to maintain the maximum level, even in the case of installing applications and changes to the Windows configuration

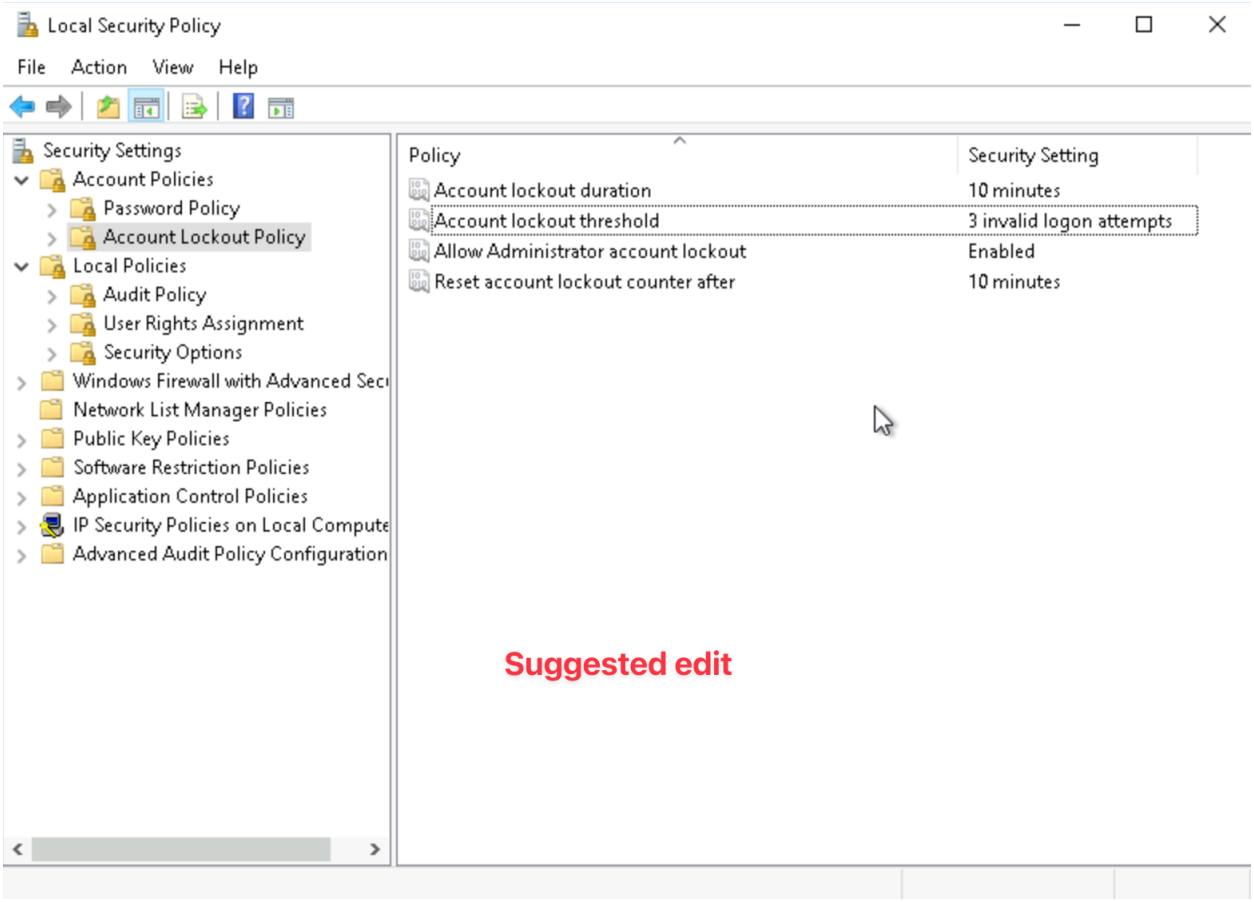



Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Audit account logon events
Success, Failure
Audit account management
No auditing
Audit directory service access
Success, Failure
Audit logon events
Success, Failure
Audit object access
No auditing
Audit policy change
Success, Failure
Audit privilege use
Success, Failure
Audit process tracking
No auditing
Audit system events
No auditing
Suggested edit


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
0 passwords remembered
Maximum password age
42 days
Minimum password age
0 days
Minimum password length
0 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled


Local Security Policy
File Action View Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Enforce password history
5 passwords remembered
Maximum password age
42 days
Minimum password age
0 days
Minimum password length
8 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Suggested edit


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Account lockout duration
Not Applicable
Account lockout threshold
0 invalid logon attempts
Allow Administrator account lockout
Not Applicable
Reset account lockout counter after
Not Applicable



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.

object network WBC-International
host 21.19.241.63

object network DFI-File-001
host 172.21.30.44

access-list DFI-Ingress extended permit tcp object WBC-International object DFI-File-001 eq 9082

Explanation:

- **Define IP Objects**:
    - We created two IP objects to represent the devices involved in this rule:
    - **WBC-International**: Represents the external partner's IP address (21.19.241.63).
    - **DFI-File-001**: Represents our internal server's IP address (172.21.30.44).
    - These objects simplify the rule creation and make it easier to manage in the future.
- **Create the Access Control Rule**:
    - We defined a rule that allows the partner's IP to connect to our server specifically on TCP port 9082.
    - This rule is applied to the **DFI-Ingress** interface, which is the entry point for external traffic coming into our network.
    - The rule permits only the specified type of traffic (TCP on port 9082) from the partner's IP to the server, enhancing security by limiting access to only what is necessary.

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.

For creating a secure VPN connection between DFI and Payroll-USA, I recommend using **IPsec with IKEv2** (Internet Key Exchange version 2) and the **AES-GCM (Galois/Counter Mode)** encryption method. This is currently one of the most secure and efficient encryption options available for VPN connections using Cisco technology.

Justification:

1. **AES-GCM Encryption**: AES-GCM provides both confidentiality (encryption) and integrity (authentication) in one efficient operation, which is critical for ensuring that the data transmitted over the VPN is not only secure but also tamper-proof. Cisco highly recommends AES-GCM for its robust security and performance advantages.
2. **IKEv2 Protocol**: IKEv2 is the latest version of the Internet Key Exchange protocol, which is used to set up a secure tunnel between two parties. IKEv2 is preferred over older versions like IKEv1 due to its improved security, faster connection times, and better support for modern encryption algorithms like AES-GCM.

3. **Cisco's Recommendations**: Cisco's documentation indicates that AES-GCM combined with IKEv2 is a recommended and secure choice for modern VPNs. It is specifically noted for its resilience against various types of cryptographic attacks and is widely supported across Cisco's range of security appliances and software.

By implementing this encryption solution, DFI can ensure that the VPN connection with Payroll-USA is secured to the highest standards, protecting sensitive payroll data from unauthorized access or tampering during transmission.

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.

System Admin Rule for DFI-File-001 (ICMP Traffic)

alert icmp 172.21.30.44 any -> any any (msg:"Potential DDoS - High volume ICMP traffic to DFI-File-001"; sid:1000001; rev:1; classtype:attempted-dos; threshold:type both, track by_dst, count 100, seconds 1;)

Explanation:

ICMP Traffic: The rule specifically monitors ICMP (ping) traffic directed towards DFI-File-001.
Source and Destination: It triggers an alert when any external source sends ICMP traffic to the server at IP 172.21.30.44.
Threshold: This rule is configured to detect if more than 100 ICMP packets are received in 1 second, which could indicate a potential DDoS (Distributed Denial-of-Service) attack.
SID (Signature ID): The sid:1000001 is a unique identifier for this rule, ensuring it is distinct within the IDS system.

VoIP Admin Rule for VoIP Server (TFTP Traffic)

alert udp any any -> 172.21.30.55 69 (msg:"Unauthorized TFTP connection attempt to VoIP Server"; sid:1000002; rev:1; classtype:attempted-recon; content:"|00 01|"; depth:2; offset:0;)

Explanation:

UDP Traffic: The rule monitors UDP traffic, specifically TFTP (Trivial File Transfer Protocol) attempts, directed towards the VoIP server.
Port 69: TFTP operates on port 69, so the rule triggers when a connection is attempted on this port.
Content Match: The content check content:"|00 01|" ensures the rule is targeting legitimate TFTP read request attempts, which are characterized by this specific byte sequence.
SID (Signature ID): The sid:1000002 is a unique identifier for this rule, ensuring it is distinct from other IDS rules.

Non-Technical Management Explanation

Purpose of Rules: These IDS (Intrusion Detection System) rules are designed to monitor and alert on specific suspicious activities:

The **first rule** is to protect the DFI-File-001 server from a potential flood of ICMP requests, which could overwhelm the server and cause a denial-of-service (DoS) attack.

The **second rule** is to detect unauthorized attempts to connect to the VoIP server using TFTP, which could be an attempt to download or modify VoIP configurations maliciously.

SID: The SID (Signature ID) is a unique number assigned to each rule, allowing the system to identify and manage them individually.

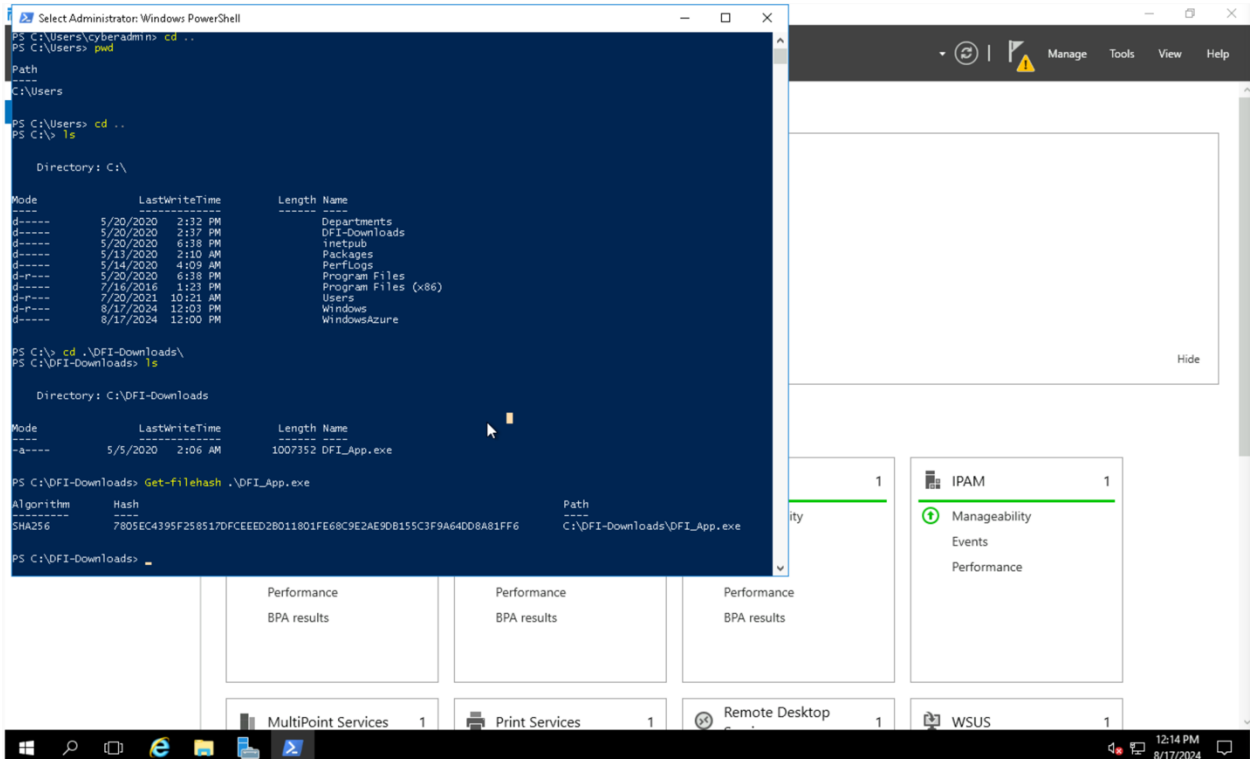
Alert Mechanism: Both rules are configured to alert the security team if the conditions are met, enabling quick responses to potential threats.

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.



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.

DFI Area/Technology	Solution	Justification for Recommendation
1. SOAR (Security Orchestration, Automation, and Response)	Implement SOAR for automated incident response workflows.	**Justification**: SOAR platforms can automate complex incident response procedures, reducing response time and improving consistency in handling security events. This includes automating tasks such as threat intelligence gathering, automated malware analysis, and incident tracking, freeing up valuable human resources for more strategic tasks.
2. IDS/Firewall Alert Automation	Automate the mitigation actions for IDS and firewall alerts using scripts or SOAR integrations.	**Justification**: Automating responses to IDS and firewall alerts, such as blocking IP addresses, adjusting firewall rules, or notifying the security team, can significantly reduce the time between detection and response, lowering the risk of breaches. This ensures that threats are neutralized faster and consistently, reducing the window of exposure.
3. Patch Management	Implement automated patch management using tools like Microsoft SCCM or WSUS.	**Justification**: Automated patch management ensures that all systems are consistently updated with the latest security patches, reducing the risk of vulnerabilities being exploited. This process can include scheduling updates, verifying their successful application, and automatically rolling back patches that cause issues, which is essential for maintaining system security and stability.

4. Active Directory (AD) Management	Automate account lockout policies based on anomalous login behavior, such as login attempts from geographically distant IPs or after-hours access.	**Justification**: Automating these processes enhances security by quickly mitigating potential unauthorized access attempts. It also reduces the manual workload on IT staff, who would otherwise need to monitor and respond to such incidents manually.
5. Backup and Disaster Recovery	Implement automated, scheduled backups with instant alerts for failures using solutions like Veeam or Acronis.	**Justification**: Ensuring consistent and reliable backups is critical for disaster recovery. Automating this process minimizes the risk of data loss due to human error and ensures that backups are completed on time and verified for integrity. Immediate alerts for backup failures enable quick remediation before it affects business continuity.

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 a 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.

Findings:

A search of the Windows Security logs for the last 24 hours has revealed several unsuccessful login attempts to the DFI-File-001 server via Remote Desktop Protocol (RDP).

The Event ID 4625, which logs failed login attempts, indicates repeated attempts from specific IP addresses. These attempts were made using various user accounts, potentially indicating a brute-force attack.

Recommendations:

1. **Implement IP Blocking**: Consider blocking the IP addresses identified in the failed login attempts at the firewall level to prevent further attempts.
2. **Enable Account Lockout Policies**: Implement stricter account lockout policies to mitigate brute-force attempts. This policy will temporarily lock accounts after a specified number of failed attempts.
3. **Multi-Factor Authentication (MFA)**: Enforce MFA for all RDP connections to add an additional layer of security.
4. **Audit and Review**: Regularly review the security logs for similar events and ensure that auditing is enabled to catch such attempts early.

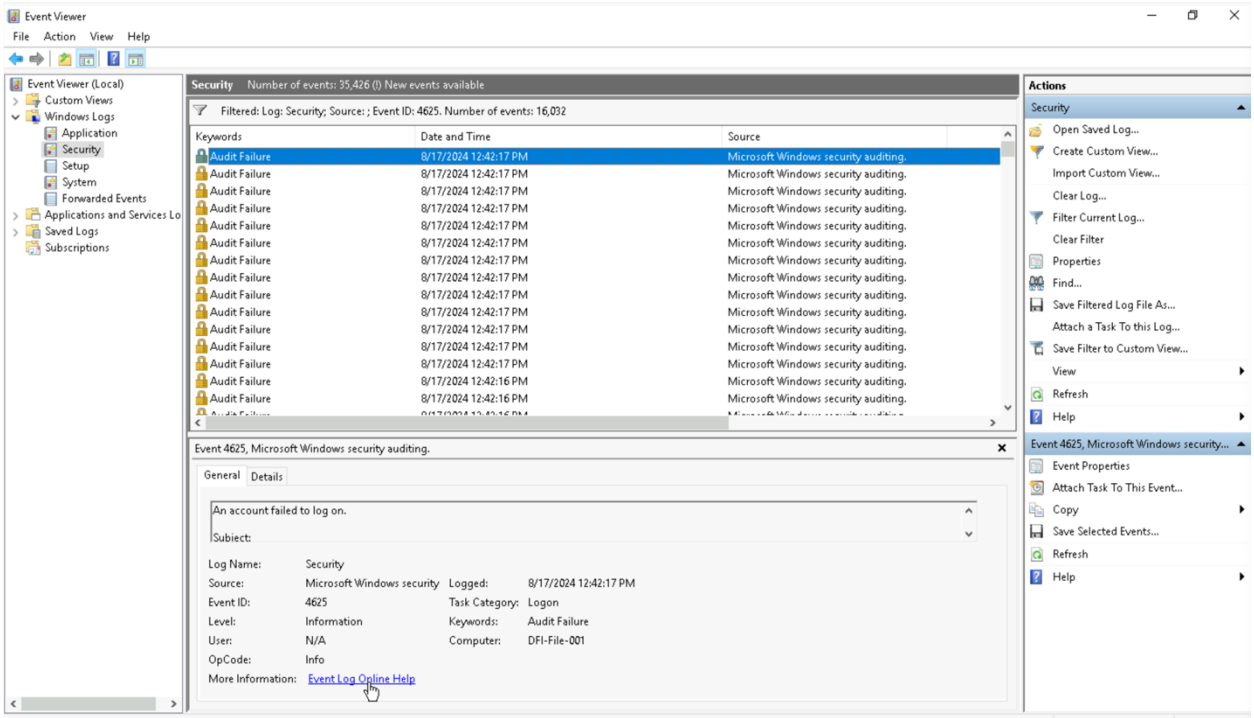
Justifications:

IP Blocking: Blocking the malicious IPs can prevent further access attempts from those sources, reducing the risk of a successful brute-force attack.

Account Lockout: This can drastically reduce the effectiveness of brute-force attacks by locking out the account after multiple failed attempts.

MFA: This ensures that even if an attacker manages to guess or obtain a password, they still need a second form of authentication, which is typically much harder to compromise.

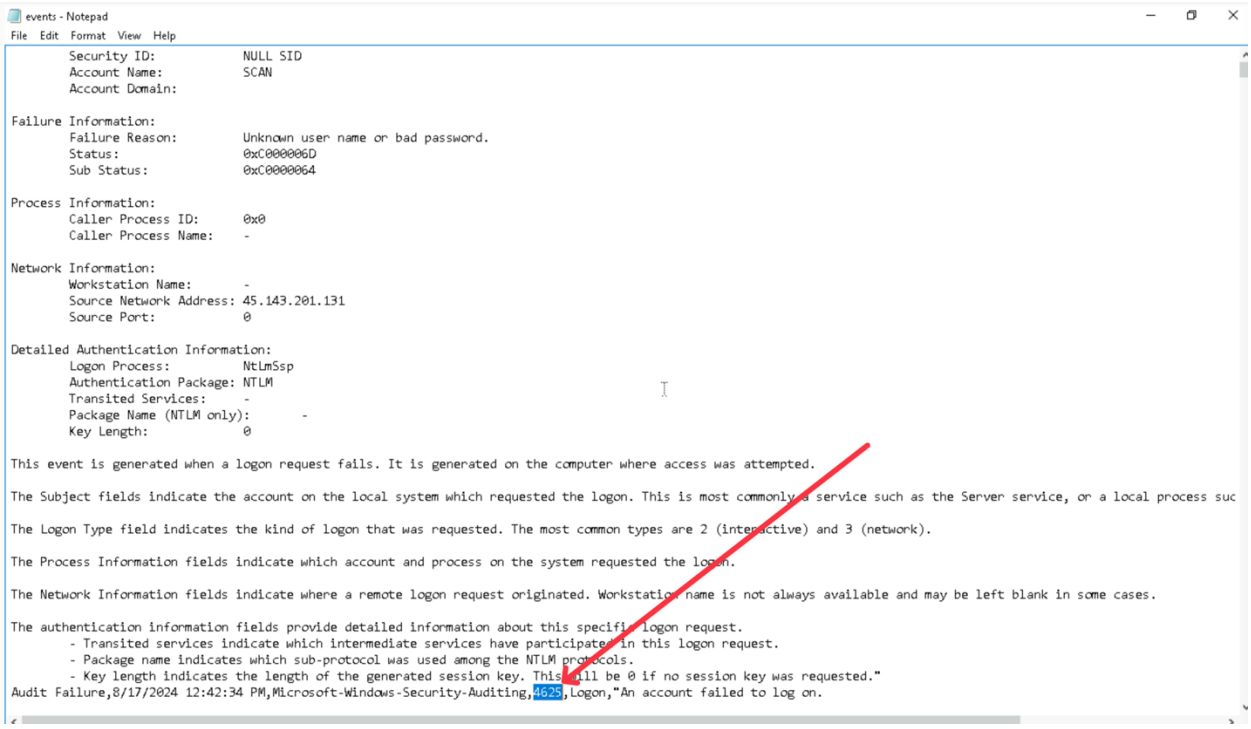
Regular Audits: Keeping a close eye on security logs allows for quick detection and response to potential threats, minimizing the window of opportunity for attackers.


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Saved Logs
Subscriptions
Security Number of events: 35,426 (!) New events available
Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 16,032
Keywords Date and Time Source
Audit Failure 8/17/2024 12:42:17 PM Microsoft Windows security auditing.
Audit Failure 8/17/2024 12:42:16 PM Microsoft Windows security auditing.
Event 4625, Microsoft Windows security auditing.
General Details
An account failed to log on.
Subject:
Log Name: Security
Source: Microsoft Windows security
Logged: 8/17/2024 12:42:17 PM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: DFI-File-001
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Clear Filter
Properties
Find...
Save Filtered Log File As...
Attach a Task To this Log...
Save Filter to Custom View...
View
Refresh
Help
Event 4625, Microsoft Windows security...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help

Untitled - Notepad

File Edit Format View Help

Audit Failure	8/17/2024 12:28:14 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:14 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:13 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:12 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:11 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:10 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:10 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:10 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:10 PM	Microsoft Windows security auditing.	4625	Logon
Audit Failure	8/17/2024 12:28:10 PM	Microsoft Windows security auditing.	4625	Logon



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 'critical' or 'security' can be left off.

Available Updates	Update/Ignore	Justification
KB890830	Update	This is a security-related tool that helps remove malicious software from the server, crucial for security.
KB5041576	Update	This is a Servicing Stack Update (SSU), which is essential for ensuring that future updates can be installed properly.
KB5041773	Update	This is a Cumulative Update, which often includes important security patches and bug fixes that are critical for system stability and security.

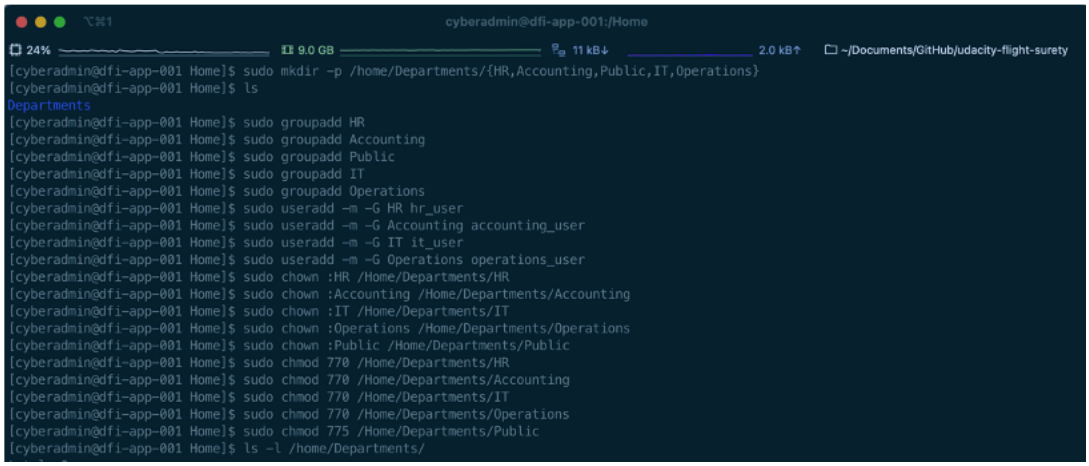
KB4577586	Ignore	**Update for the removal of Adobe Flash Player:** This update is focused on removing Adobe Flash Player, which may not be critical if Flash is not being used or has already been removed from the environment.
KB4033631	Ignore	**Feature Update for Windows Server 2016 (RS3): This update introduces new features and improvements, but does not address critical security vulnerabilities. It can be deferred if the new features are not required immediately.**
KB4487006	Ignore	**Update for Microsoft .NET Framework 4.8 for Windows Server 2016: This update provides quality improvements but is not a security update. It can be deferred if there are no immediate issues or dependencies on this version of .NET.**

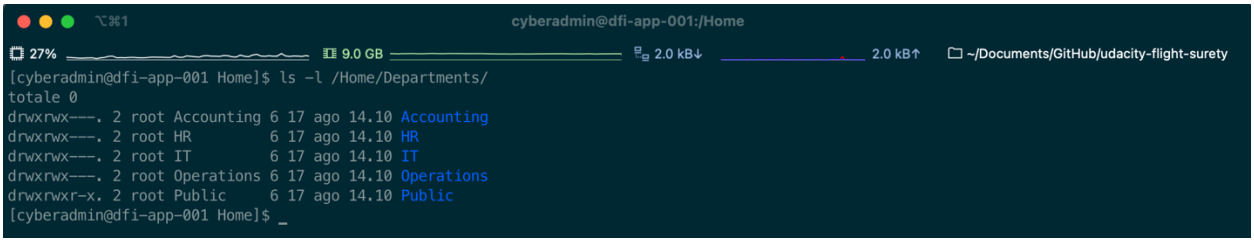
10. **Linux Data Directories:**

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
- Cd ..

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





Commands:

Non-Technical Explanation for the Change Control Board:

Directory Creation: We created a directory structure under /Home/Departments to organize departmental files.

sudo mkdir -p /Home/Departments/{HR,Accounting,Public,IT,Operations}

Group Creation: User groups corresponding to each department were created to manage access control.

sudo groupadd HR
sudo groupadd Accounting
sudo groupadd Public
sudo groupadd IT
sudo groupadd Operations

User Creation and Group Assignment: Users were added to these groups to align their access permissions with departmental needs.

```
sudo useradd -m -G HR hr_user
sudo useradd -m -G Accounting accounting_user
sudo useradd -m -G IT it_user
sudo useradd -m -G Operations operations_user
```

Permissions Set: Directory permissions were configured so that only members of the respective groups have access to their department's files, while public directories are accessible to all.

```
sudo chown :HR /Home/Departments/HR
sudo chown :Accounting /Home/Departments/Accounting
sudo chown :IT /Home/Departments/IT
sudo chown :Operations /Home/Departments/Operations
sudo chown :Public /Home/Departments/Public

sudo chmod 770 /Home/Departments/HR
sudo chmod 770 /Home/Departments/Accounting
sudo chmod 770 /Home/Departments/IT
sudo chmod 770 /Home/Departments/Operations
sudo chmod 775 /Home/Departments/Public
```

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.

Analysis of the Firewall Report:

The firewall report indicates repeated **SSH User Authentication Brute Force Attempts** originating from the IP address 192.34.57.157 targeting multiple destination IP addresses (222.51.64.10, 222.51.64.14, 222.51.65.53). These attempts are recognized as a significant security threat, categorized under "brute-force".

- **Threat/Content Type:** Vulnerability (SSH brute-force attempts)
- **Source Address:** 192.34.57.157 (United States)
- **Destination Addresses:** Multiple, all within the United States.

- **Application:** SSH (Port 22)

Mitigation Strategy:

Block the Source IP Address:

Action: Immediately block the IP address 192.34.57.157 on the firewall to prevent any further brute-force attempts.

Justification: The repeated brute-force attempts from this IP indicate a likely automated attack aimed at compromising SSH services. Blocking the source IP will stop these attempts and protect the targeted servers from unauthorized access.

Implement Geo-blocking (If Applicable):

Action: If the source country of these attacks is not commonly associated with legitimate traffic for your organization, consider geo-blocking or restricting access from that region.

Justification: Geo-blocking is an additional layer of security that can help prevent attacks originating from regions where the organization has no business presence or operations, thus reducing the risk of unwanted traffic.

Enforce Stronger SSH Security Practices:

Action: Review and enforce SSH security settings across all servers. This includes:

Using non-standard ports: Changing the SSH port from the default 22 to another port can reduce the risk of automated attacks.

Implementing Fail2Ban: Deploy Fail2Ban or a similar intrusion prevention system to automatically block IP addresses that demonstrate suspicious behavior, such as multiple failed login attempts.

Enforcing key-based authentication: Disable password-based SSH authentication in favor of key-based authentication, which is less susceptible to brute-force attacks.

Justification: Strengthening the SSH security configuration will provide additional protection against brute-force attacks and unauthorized access attempts, even if the initial firewall rule is bypassed.

Monitor for Further Attempts:

Action: Set up continuous monitoring and alerting for any future SSH brute-force attempts, especially from other IP addresses.

Justification: Continuous monitoring allows for quick detection and response to ongoing or new threats, ensuring that the organization remains proactive in its defense strategy.

Additional Protection for the Destination IP:

Deploy an Intrusion Detection and Prevention System (IDPS):

Action: Implement an IDPS solution that can detect and respond to suspicious activities, such as brute-force attempts, in real-time.

Justification: An IDPS will provide an additional layer of security by detecting threats and automatically responding to them, such as blocking malicious IPs or logging out potential attackers.

Harden SSH Access:

Action: Ensure that the destination servers have SSH access restricted to known IP addresses (e.g., through the use of firewall rules or security groups).

Justification: Limiting SSH access to specific IP ranges minimizes the attack surface and reduces the risk of unauthorized access.

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.

As I complete my first two weeks in the role of Information Security Analyst at DFI, I want to provide an overview of the work I've done, the recommendations made, and the overall security posture of DFI. My focus has been on identifying potential vulnerabilities, implementing security improvements, and establishing a foundation for ongoing cybersecurity efforts. Below is a summary of my work and the path forward for enhancing DFI's security.

Work Performed

1. **Firewall Analysis and Mitigation**
   - **Task**: I reviewed and analyzed the firewall alerts that were raised due to unusual traffic. This included identifying potential threats such as brute-force attempts on our servers.
   - **Action**: I blocked the identified malicious IP addresses and recommended further hardening of our SSH configurations to protect against future attacks.
2. **Server Security and Permissions Review**

- **Task**: I performed a security analysis on DFI's Windows and Linux servers, focusing on file permissions, installed roles, and running services.
- **Action**: I recommended restricting file permissions, particularly on sensitive directories like HR, to ensure that only authorized personnel have access. I also identified unnecessary roles and services that could be removed or disabled to reduce the attack surface.

3. **Automation Opportunities**
   - **Task**: I explored areas where automation could enhance security, particularly in the management of alerts and responses to potential threats.
   - **Action**: I recommended the implementation of SOAR (Security Orchestration, Automation, and Response) tools to automate incident response, streamline patch management, and improve the efficiency of our security operations.
4. **Directory and User Management**
   - **Task**: I established a structured directory hierarchy on the DFI-App-001 server, creating specific directories for departments like HR, IT, and Accounting, and assigned appropriate permissions.
   - **Action**: I ensured that only the relevant departmental groups had access to their respective directories, enforcing the Principle of Least Privilege.
5. **Security Configuration Review**
   - **Task**: I reviewed the current security configurations across systems, including firewall settings, user account controls, and system update policies.
   - **Action**: I made recommendations to disable non-essential services, enforce stricter password policies, and ensure that all systems are updated with the latest security patches.

Recommendations for Changes

- **Permission Enhancements**:
  - **File Access**: Implement strict access controls on sensitive directories, such as those in HR and Accounting, ensuring that only

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, 15 or more 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. See the classroom instructions for the submission.