# Scenario:

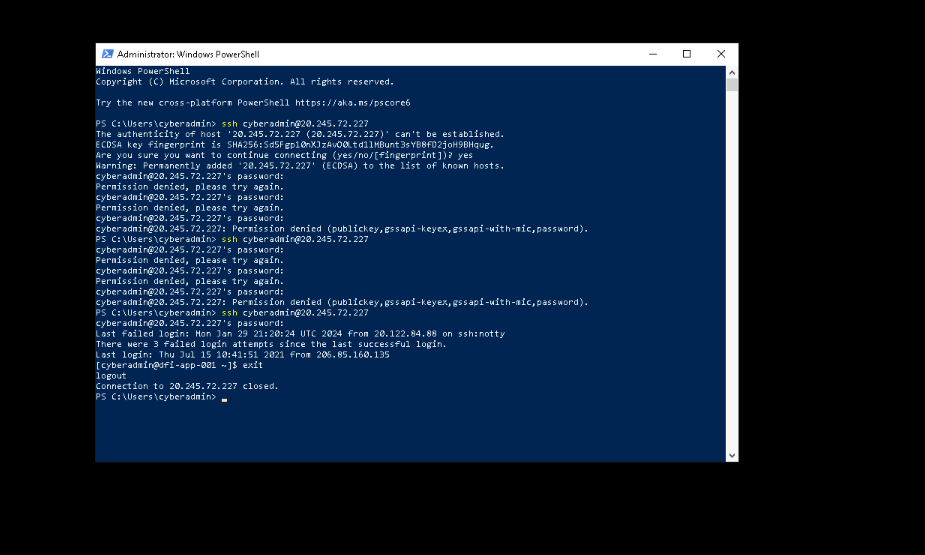
Douglas Financials Inc (DFI from here forward) has experienced successful growth and as a result, is ready to add a Security Analyst position. Previously Information Security responsibilities fell on our System Administration team. Due to compliance and the growth of DFI, we are happy to bring you on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

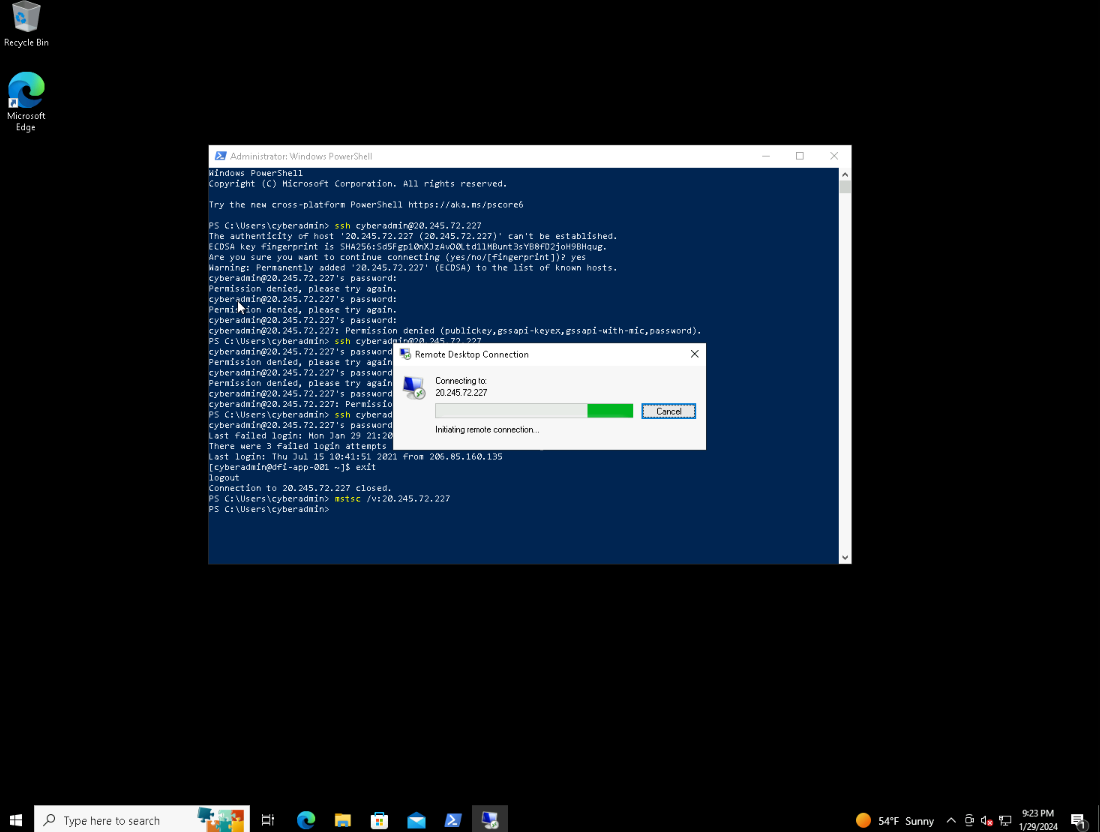
## Week One:

### 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.





### 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.](http://iieng.org/images/proceedings_pdf/8285E0914047.pdf) [NIST 800-123](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf) (other NIST documents could also apply.)

1. Windows SmartScreen:

The PC does not have Windows SmartScreen enabled. Windows SmartScreen plays a crucial role in ensuring the safety of the PC by issuing a warning before running any unfamiliar applications or files downloaded from the internet.

Enabling Windows SmartScreen is essential. Disabling it may lead to potential risks such as background downloads conducted by applications and the possibility of downloading malicious or corrupted files.

2. User Access Control Settings:

The current setting on the PC is set to "Notify me only when apps try to make changes to my computer."

This setting needs to be modified to "Always notify me when: Apps try to install software or make changes to the computer, and I make changes to Windows settings."

The previous settings may result in unintentional changes made by the user going unnoticed. However, by changing the setting to always notify, the user will receive notifications regarding any changes made, allowing them to confirm whether the changes should be implemented or not.

3. BitLocker:

BitLocker is not enabled for Windows (C:).

Enabling BitLocker is crucial as it provides data protection through encryption. It primarily utilizes AES encryption to safeguard the data. By enabling BitLocker, we can ensure that only authorized users can access the data stored on the PC.

4. Permissions on the HR folder:

Full access to the HR folder should be limited to the owner and the administrator. Only trusted and necessary users should be granted access. It is necessary to modify the permissions on the HR folder so that only the admin, owner, and system have full control over the folder.

### 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.

[Place your firewall rules and explanation here.

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

The access-list command is used to create a rule for managing traffic. In this case, the access list is named DFI-Ingress. The extended permit keyword is used to grant permission to a specific host. The first host IP address represents the source, while the second host IP address represents the destination (which is the company's IP address). The eq 9082 specifies the port number through which the data can be accessed. Essentially, this syntax allows the source to access the destination using port 9082.

\*access-list DFI-Ingress extended permit host 21.19.241.63 host 172.21.30.44 eq 9082\*

### 4. **VPN Encryption Recommendation:**

DFI is creating a payroll processing partnership with Payroll-USA; this will involve creating a VPN connection between the two. Research, recommend, and justify an encryption solution for the connection that is using the latest available encryption for Cisco. Use the Cisco [documentation](https://tools.cisco.com/security/center/resources/next_generation_cryptography) as a guide.

[Place your VPN Encryption Recommendation here]

I suggest utilizing Symmetric encryption as the most suitable option. This encryption method employs a single key for both encryption and decryption processes. There are three notable types of symmetric encryption, namely AES, Twofish, and RC4. AES is a mandatory standard set by the PCI-DSS, requiring all stored and transmitted data to be encrypted using AES. RC4 is known for its simplicity and speed. Twofish, on the other hand, is frequently employed in e-commerce websites to ensure secure and safe payment transactions. Considering these factors, I believe that symmetric encryption is the optimal choice for our current situation

### 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.

[Place your System Admin rule and explanation here]

alert icmp any any -> 172.21.30.44 [69] (msg: “ICMP traffic detected”; sid:1000006; rev:1;)

The rule notifies us whenever there is a detection of ICMP traffic. The alert serves as the initial component of the regulation, indicating its purpose of alerting us. Subsequently, the protocol being utilized is specified, which in this case is ICMP. Following that, the source IP address and port are provided. In this scenario, I have used the term "any" to signify that it can originate from any IP and any port. The destination (our company) is identified as 172.21.30.44, with "any" being applicable to any port. Lastly, the message to be displayed, "ICMP traffic detected," is included along with the SID and REV.

[Place your VoIP Admin rule and explanation here]

alert udp any any -> 172.21.30.55 [69] (msg:” Connection attempted via TFTP”; sid:1000008; rev:1;)

The rule notifies us whenever a connection is being attempted through TFTP. The alert serves as the initial component of the regulation, indicating its purpose of alerting us. Following that, the protocol being utilized is mentioned, which in this case is UDP. Subsequently, the source IP address and port are specified. In this particular scenario, I have used the term "any" to denote that it can originate from any IP and any port. The destination (our company) is identified as 172.21.30.55, with "any" being applicable to any port. Lastly, the message to be displayed, which is "Connection attempted via TFTP," is included along with the SID and REV.

6. **File**

**Hash verification:**

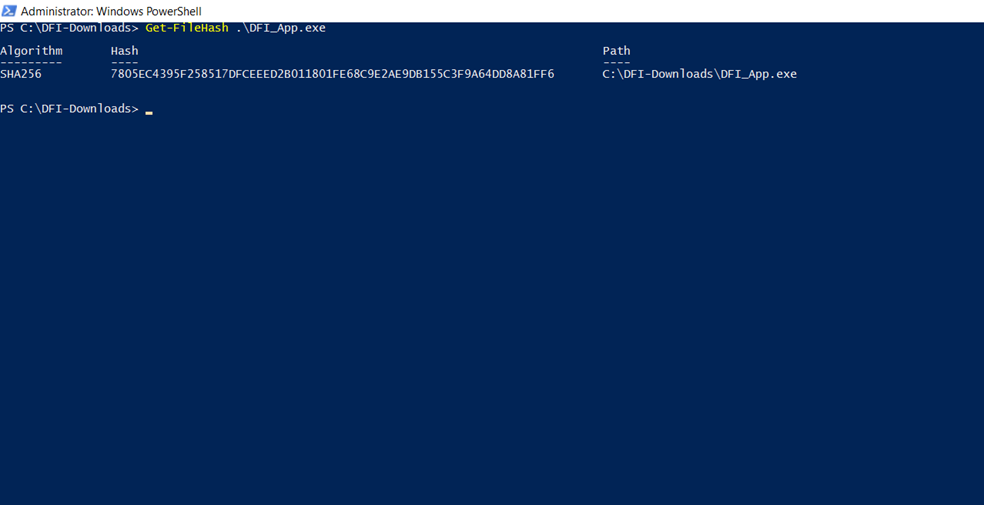
A software vendor has supplied DFI with a custom application. They have provided the file on their public FTP site and e-mailed you directly a file hash to verify the integrity and authenticity. The hash provided is a SHA256.

**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.

[Place your screenshot that displays the command that was run as well as the file hash.]



## 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. Example:

* Area: Active Directory.
* Solution: The item for automation - Automatic account lockout if login from 2 geographically distant IPs
* Justification: Provide a brief explanation for your choices.

|  |  |  |
| --- | --- | --- |
| **DFI Area/Technology** | **Solution** | **Justification for Recommendation** |
| Logging attempts | limit to the number of logins | Upon reviewing the security logs, I discovered a significant number of login attempts. The presence of a limit on login attempts guarantees that only authorized users can access the system, thereby safeguarding confidentiality and integrity. |
|  |  |  |
| Application Monitoring | Real-time application monitoring | By monitoring the applications, one can ensure that there are no other processes or tasks occurring in the background that could potentially pose problems to the system or company in the future. |
|  |  |  |
| Incident Response | Using cyber fusion solutions | Cyber fusion is a technique of combining many solutions into one. I comprise of full incident analysis and response. This protects the system against malware, vulnerabilities and threat actors in real-time. |

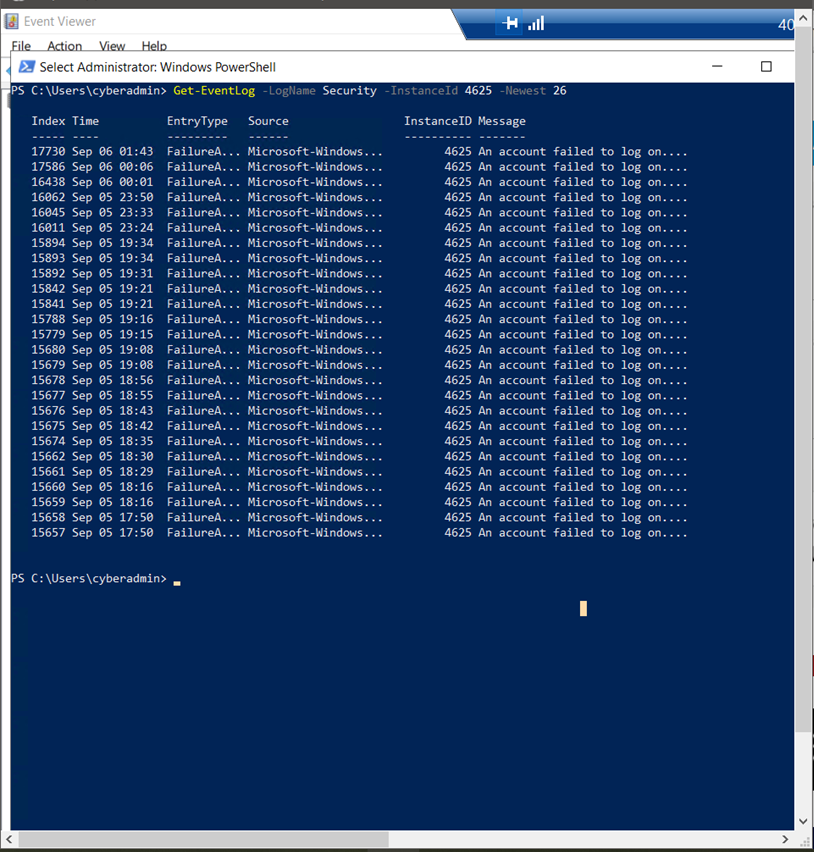
### 8. **Logging RDP Attempts:**

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.

[Place IT Manager Report Here ]



Based on the analysis conducted on the Security log, it appears that there is a significant number of unsuccessful login attempts. To mitigate such events and safeguard the system, it is imperative to implement a restriction on the number of failed login attempts. This measure ensures that brute force attacks, aimed at gaining unauthorized access to the system, are prevented. By limiting the occurrences of failed logins, the overall vulnerability to hacking is reduced. To further enhance security, it is recommended to include trusted IP addresses while removing blocked or untrusted IP addresses from the firewall configuration. This approach will only permit access from trusted sources, effectively blocking any attempts from untrusted IP addresses.

### 9. **Windows Updates:**

Using [NIST 800-40r3](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf) and [Microsoft Security Update Guide](https://portal.msrc.microsoft.com/en-us/security-guidance), 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.

Provide a table that lists at least 3 updates that should be installed and 3 updates that are not necessary.

Justify your recommendations as to why you are making your choices.

Tip: The severity of the updates can also help you decide the updates you’d like to install or ignore.

Add as many rows or additional columns as you need to the table.

|  |  |  |
| --- | --- | --- |
| Available Updates | Update/Ignore | Justification |
| KB4569751 | Update | It observes application runtime failures or unexpected behaviors. |
| KB4561600 | Update | Security updates are very critical in all the situations. Security cannot be compromised even if it is a small problem. Later this small problem can cause fatal destruction. |
| KB2267602 | Update | Microsoft Windows Defender Antivirus protects the system from being affected. It uses cloud-delivered protection and downloads security intelligence updates to provide protection to the system. |
| KB4565351 | Ignore | These are the optional, improvement features provided by Microsoft. These updates can be added to the end of the update list. It is not an urgent update that needs to be done |
| 21.90.1.1 – Driver Update | Ignore | Bluetooth driver updates are of relatively low significance and can be performed as needed. Once the essential updates have been completed, the Bluetooth driver update can be executed. |
| KB4565483 | Ignore | These updates are mainly optional, but they make many improvements. But these can be done once the other important aspects or updates are done. |

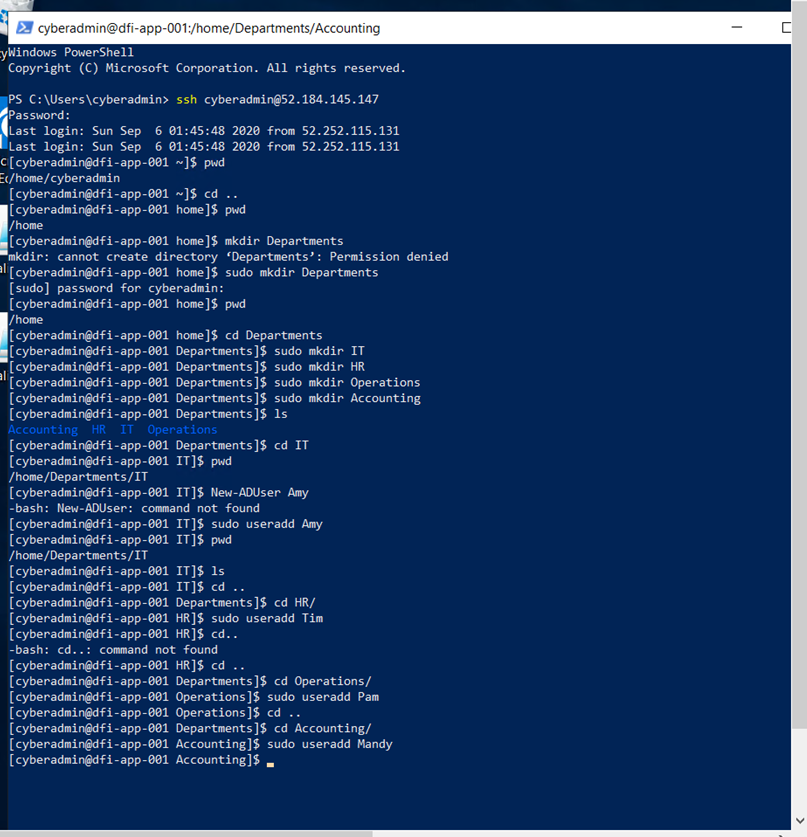
### 10. **Linux Data Directories:**

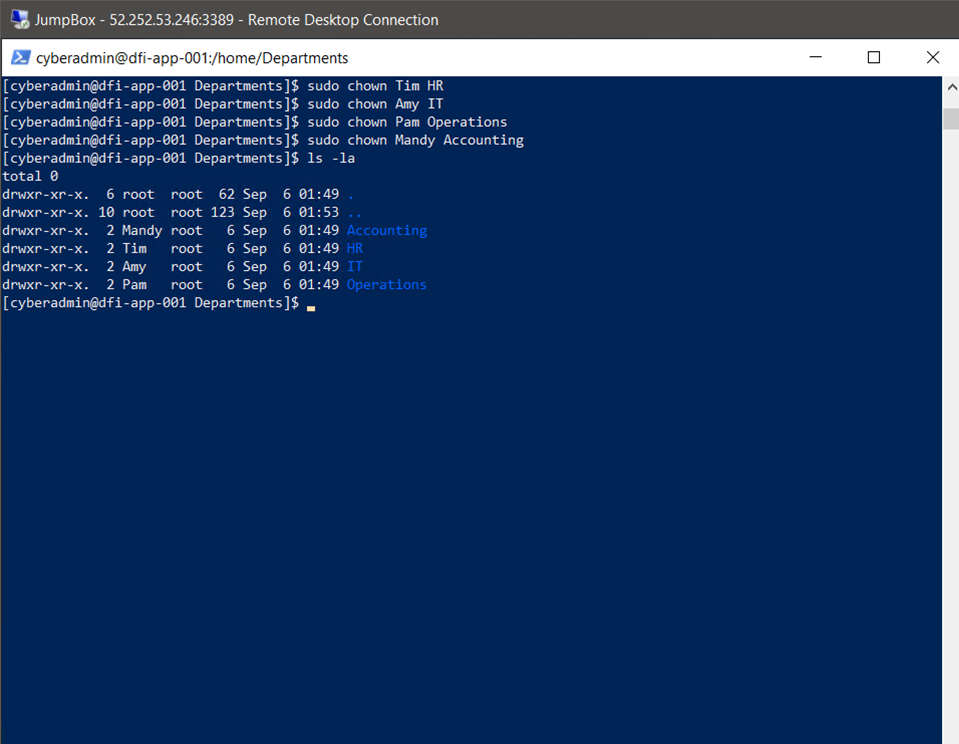
The IT Manager has requested your help with creating directories on the CentOS server DFI-App-001 (reachable by ssh from the Windows 10 machine. in the DFI subnet.)

* 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.

[Provide a screenshot(s) of completed tasks and the correctly set permissions here]





[Provide your non-technical syntax explanation for management here]

We are currently establishing a directory called "Department" within the Home directory. Within the Departments directory, we are creating four separate directories: IT, HR, Operations, and Accounting. In each of these directories, we have created user accounts and assigned them to their respective groups.

### 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.

[Firewall mitigation response and justification goes here]

### There are several methods to mitigate the situation:

### 1. Implementing a restriction on the number of failed login attempts ensures that a large number of attempts cannot be made to gain access to the system. This significantly decreases the likelihood of an unauthorized user successfully logging in.

### 2. Restricting logins to specific IP addresses ensures that only authorized individuals with access can attempt to log into the system. No other IP address will be able to be used for login purposes.

### 3. Utilizing two-factor authentication adds an extra layer of security and reduces the chances of unauthorized access. Even if an unauthorized user obtains the password, they will still require the second factor to successfully log in.

### 4. Disabling SSH access for the root user can greatly enhance security measures.

### 5. Implementing Captchas can effectively reduce the risk of automated bots attempting to log in.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.

To accomplish any task, it is essential to establish connections between machines in order to complete our work. Initially, I established connections between the servers. Subsequently, an analysis was conducted to identify necessary changes and the reasons behind them. A firewall rule was then created to grant access to a specific file for our company partner. We determined the most secure VPN encryption to be used for the payment payroll partnership.

Monitoring the systems and networks is imperative. Therefore, we implemented IDS rules to monitor incoming traffic and attempted connections. Additionally, we performed file hash verification on software provided by a vendor. We accessed security logs containing specific events, analyzed them, and made recommendations based on our findings.

We checked for Windows updates and determined whether they were necessary at that time or could be disregarded. Furthermore, we thoroughly analyzed a firewall report and determined mitigation steps or recommendations that can be utilized in the future.

Throughout these two weeks, we covered various skills and topics including analysis, monitoring, logging, alert response, IDS, firewall rules, and alert response.

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.**

This submission error persists when I submit the encrypted zip, below I provide how I encrypted the folder as well as the contents of the csv file.

A screenshot of a computer

Description automatically generated

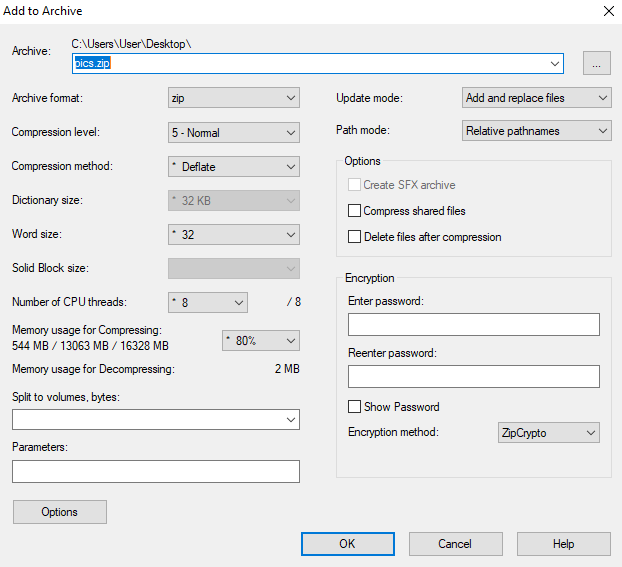
How to encrypt a file with 7 Zip:

-Right click folder > 7 Zip > Send to archive.

-Save it as zip rather than 7Zip’s archive format.

-Enter a long complex master password in the enter password space on the bottom left section.

(RqHg8Ayxep`KBu&?m;~\*<bWT8]5/b;Vad=M<Cct^vfNy)



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CSV FILE:  Keywords | Date and Time | Source | Event ID | Task Category | |
|  |  |  |  |  | |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMIN Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 40.118.133.149 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 103.133.105.133 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 40.118.133.149 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMIN Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 65.166.246.37 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 185.53.141.120 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 65.166.246.37 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 65.166.246.37 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 185.53.141.120 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 185.53.141.120 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 103.133.105.133 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |
| Audit Failure | ######## | Microsoft-Windows-Security-Auditing | 4625 | Logon | An account failed to log on.  Subject: Security ID: NULL SID Account Name: - Account Domain: - Logon ID: 0x0  Logon Type: 3  Account For Which Logon Failed: Security ID: NULL SID Account Name: ADMINISTRATOR Account Domain:   Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064  Process Information: Caller Process ID: 0x0 Caller Process Name: -  Network Information: Workstation Name: - Source Network Address: 199.96.246.226 Source Port: 0  Detailed Authentication Information: Logon Process: NtLmSsp  Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0  This event is generated when a logon request fails. It is generated on the computer where access was attempted.  The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.  The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).  The Process Information fields indicate which account and process on the system requested the logon.  The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.  The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested. |