**CMMC 2.0 LEVEL 1 ASSESSMENT**

**Table of Contents**

1. [Access Control (AC) 3](#_TOC_250020)

[AC.L1-3.1.1 – Authorized Access Control 3](#_TOC_250019)

AC.L1-3.1.2 – Transaction and Function Control 4

[AC.L1-3.1.20 – External Connections 6](#_TOC_250018)

[AC.L1-3.1.22 – Control Public Information 7](#_TOC_250017)

1. [Identification and Authentication (IA) 9](#_TOC_250016)

[IA.L1-3.5.1 – Identification 9](#_TOC_250015)

[IA.L1-3.5.2 – Authentication 14](#_TOC_250014)

1. [Media Protection(MP) 18](#_TOC_250013)

[MP.L1-3.8.3 – Media Disposal 18](#_TOC_250012)

1. [Physical Protection (PE) 18](#_TOC_250011)

[PE.L1-3.10.1 – Limit Physical Access 18](#_TOC_250010)

[PE.L1-3.10.3 – Escort Visitors 19](#_TOC_250009)

[PE.L1-3.10.4 – Physical Access Logs 19](#_TOC_250008)

[PE.L1-3.10.5 – Manage Physical Access 19](#_TOC_250007)

1. [System and Communications Protection (SC) 20](#_TOC_250006)

[SC.L1-3.13.1 – Boundary Protection 20](#_TOC_250005)

[SC.L1-3.13.5 – Public Access System Separation 20](#_TOC_250004)

1. [System and Information Integrity (SI) 21](#_TOC_250003)

[SI.L1-3.14.1 – Flaw Remediation 21](#_TOC_250002)

[SI.L1-3.14.2 – Malicious Code Protection 22](#_TOC_250001)

[SI.L1-3.14.4 – Update Malicious Code Protection 22](#_TOC_250000)

SI.L1-3.14.5 – System and File Scanning 23

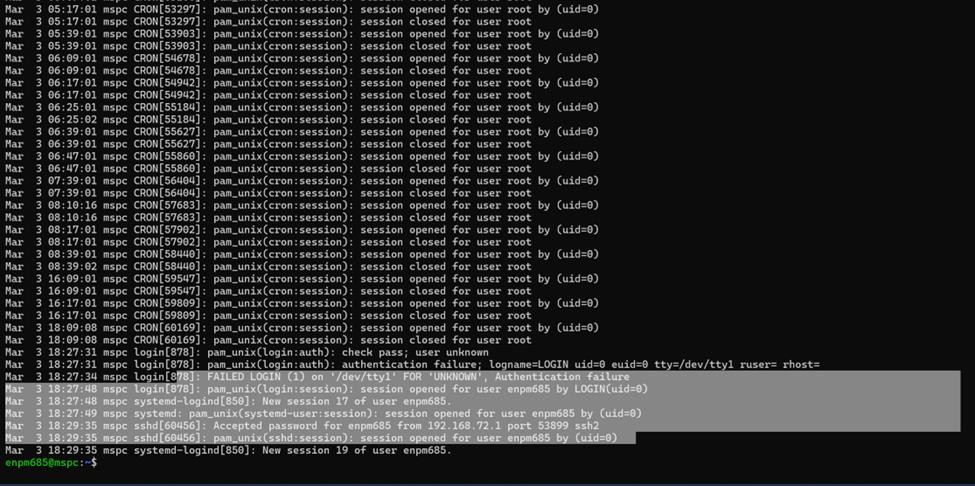
# Access Control (AC)

## AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

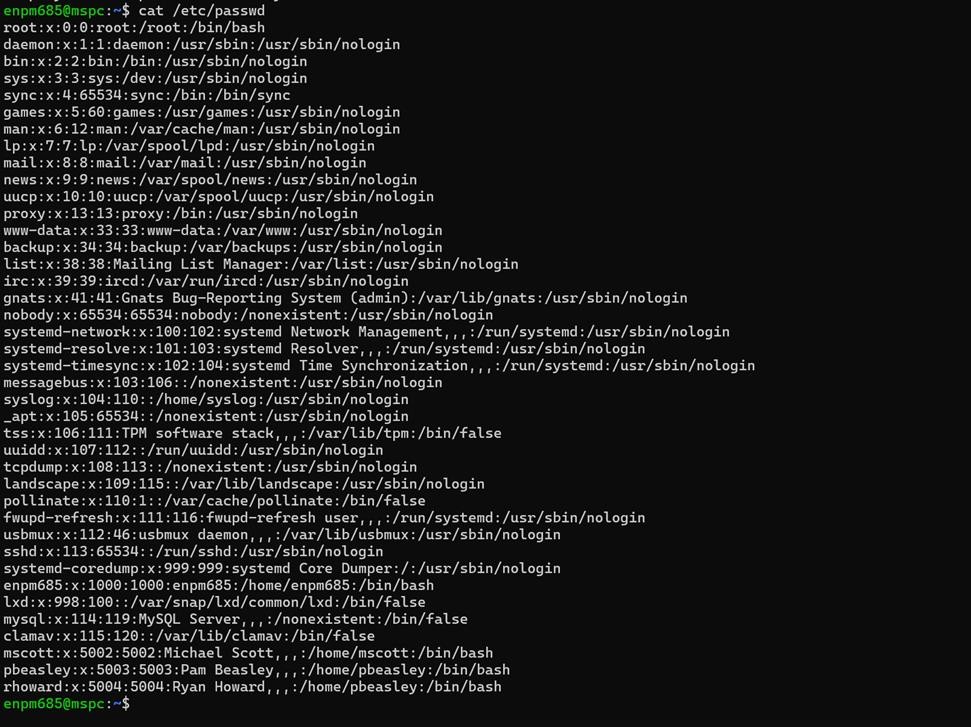
#### Limit information system access to authorized users, and processes acting on behalf of authorized users, or devices (including other information systems).

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** The command "cat /var/log/auth.log" is used to display the contents of the authentication log file on Unix-like systems, such as Linux. The `auth.log` file specifically contains information related to authentication events, such as login attempts, password changes, and authentication failures. The highlighted logs show a failed and a successful login attempt proving that there is authorized control in place.



The following screenshot shows the login credentials of users using “cat /etc/passwd”, further proving that the information system is accessible only to authorized users.



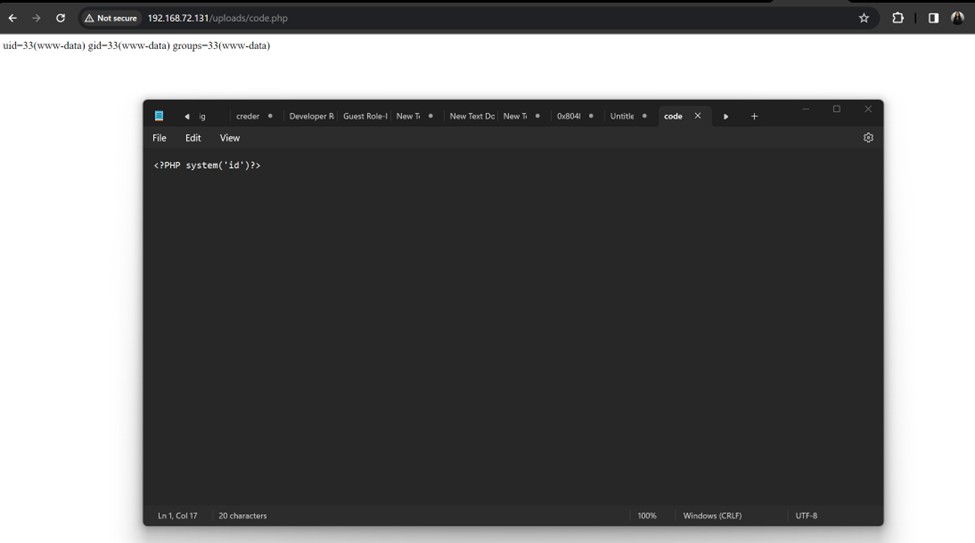
## AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

***Limit information system access to the types of transactions and functions that authorized users are permitted to execute.***

### Is this requirement being met? MET NOT MET N/A

**Evaluation/Evidence:** The website requests user input without incorporating validation, authentication, or authorization measures. Consequently, users possess the ability to upload PHP files for injection, enabling them to manipulate the system to their advantage. We confirmed this by uploading a PHP file.





### Recommendations for Improvement:

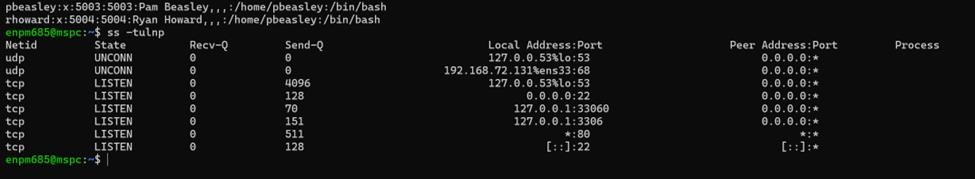
* Implement Input Validation: Implementing input validation contributes to auditing and accountability by reducing the risk of unauthorized access and data manipulation.
* Implement Authentication and Authorization: Authentication and authorization form the core of access control. The implementation of these measures ensures that the system is interacted with solely by users who have been duly authorized.
* Secure File Uploads: Enabling users to upload files to a web application can introduce security risks, especially if proper measures are not in place. Secure file uploads involve implementing controls to mitigate potential vulnerabilities and ensure that the uploaded files do not pose a threat to the system. Verify and restrict the types of files that users can upload. This prevents malicious users from uploading files with executable code, such as PHP or other scripts. Implement server-side validation to check the file's extension and MIME type against an approved list. Reject any files that do not match the allowed types.

## AC.L1-3.1.20 – EXTERNAL CONNECTIONS

#### Verify and control/limit connections to and use of external information systems.

**Is this requirement being met? MET** NOT MET N/A

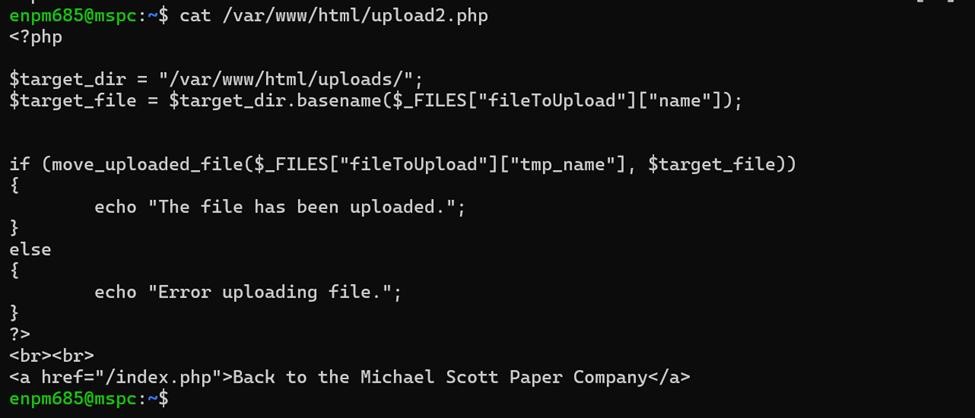
**Evaluation/Evidence:** The presence of "127.0.0.1:3306" in the table indicates that the MySQL database service is listening only on the local loopback interface, meaning it is accessible only from the local system and not externally. This restricted access helps to ensure that external entities cannot directly connect to the MySQL service, thereby enhancing security by limiting potential attack surfaces. This configuration aligns with the requirement to verify and control/limit connections to external information systems, as it effectively restricts access to the MySQL service to only local connections. Additionally, the presence of other listening ports, such as port 80 for web services, further demonstrates control over external connections by specifying which services are accessible from external sources.



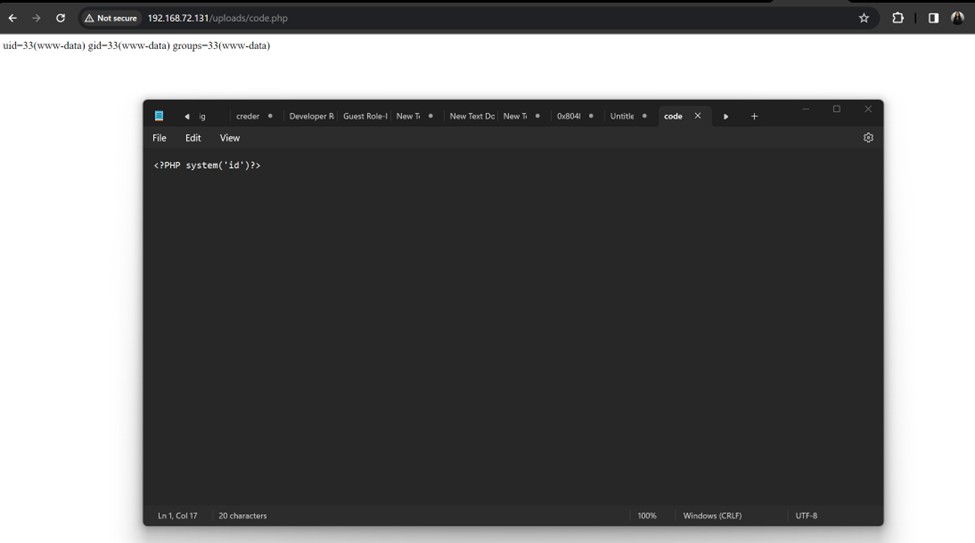
## AC.L1-3.1.22 – CONTROL PUBLIC INFORMATION

***Control information posted or processed on publicly accessible information systems*. Is this requirement being met? MET NOT MET** N/A

**Evaluation/Evidence:** There is a lack of control over the information posted or processed on publicly accessible information systems, as evident from the screenshots provided. There is no presence of any filtering mechanism during the data processing stage. During file uploads, there is a notable absence of file validation, potentially leading to injection vulnerabilities as seen in AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL. This unrestricted upload capability opens the door for anyone to upload any type of file, with the data subsequently being processed without scrutiny.







### Recommendations for Improvement:

* Implement Input Validation and Sanitization: Implement server-side input validation to check user inputs for conformity to expected formats. Sanitize input data to remove or neutralize potentially harmful characters, preventing injection attacks. Utilize input validation libraries or frameworks to automate and standardize the validation process.
* Implement File Upload Controls: Introduce server-side validation mechanisms for uploaded files, checking file types, sizes, and content. Implement restrictions on the types of files that can be uploaded to mitigate the risk of injection vulnerabilities. Utilize file upload libraries or components with built-in security features.
* Enforce Access Controls: Implement role-based access control (RBAC) to restrict user permissions based on their roles. Define and enforce proper access permissions for different functionalities and data resources. Regularly review and update access control policies to adapt to changing security requirements.

# Identification and Authentication (IA)

## IA.L1-3.5.1 - IDENTIFICATION

***Identify information system users, processes acting on behalf of users, or devices.***

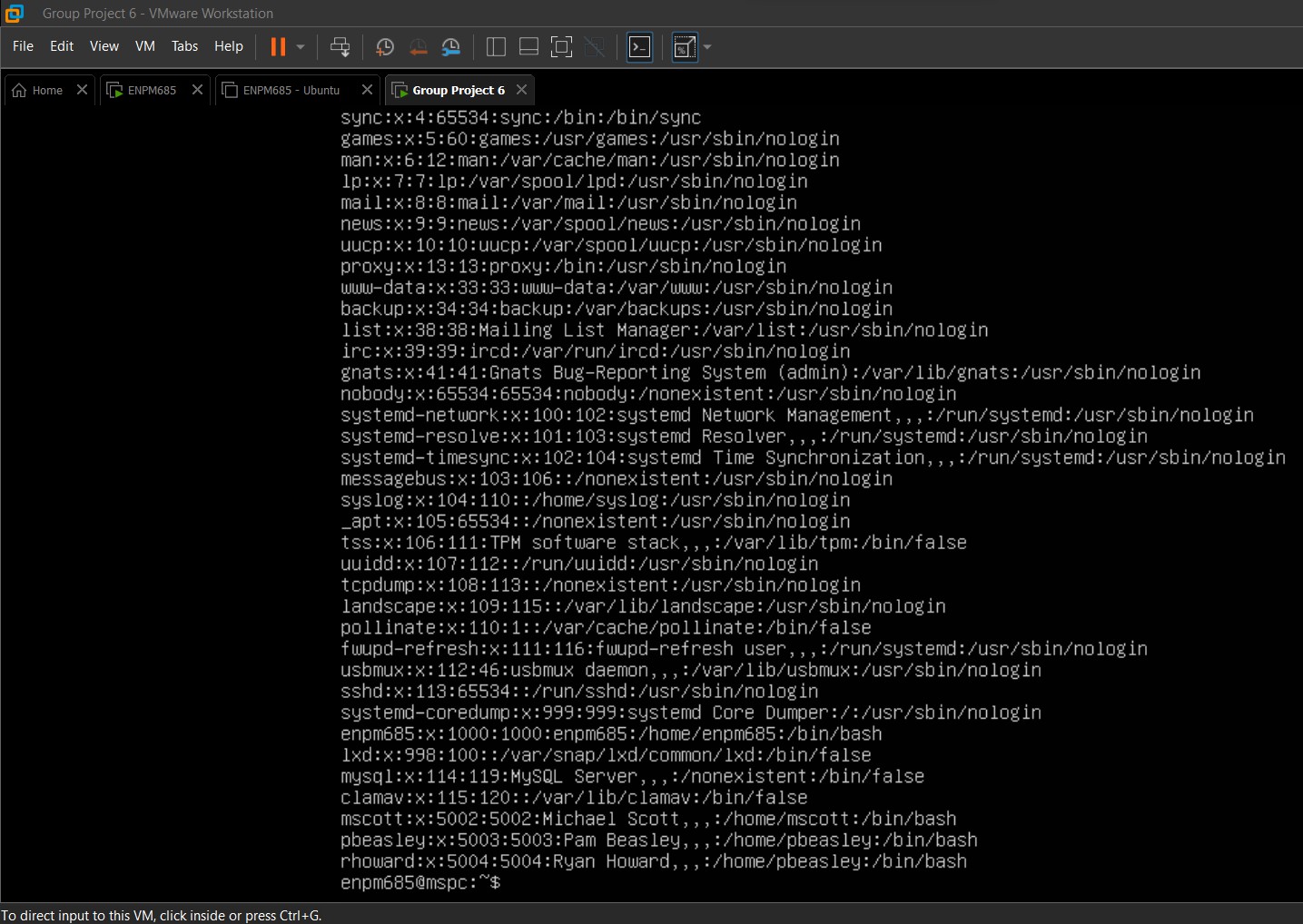
### Is this requirement being met? MET NOT MET N/A

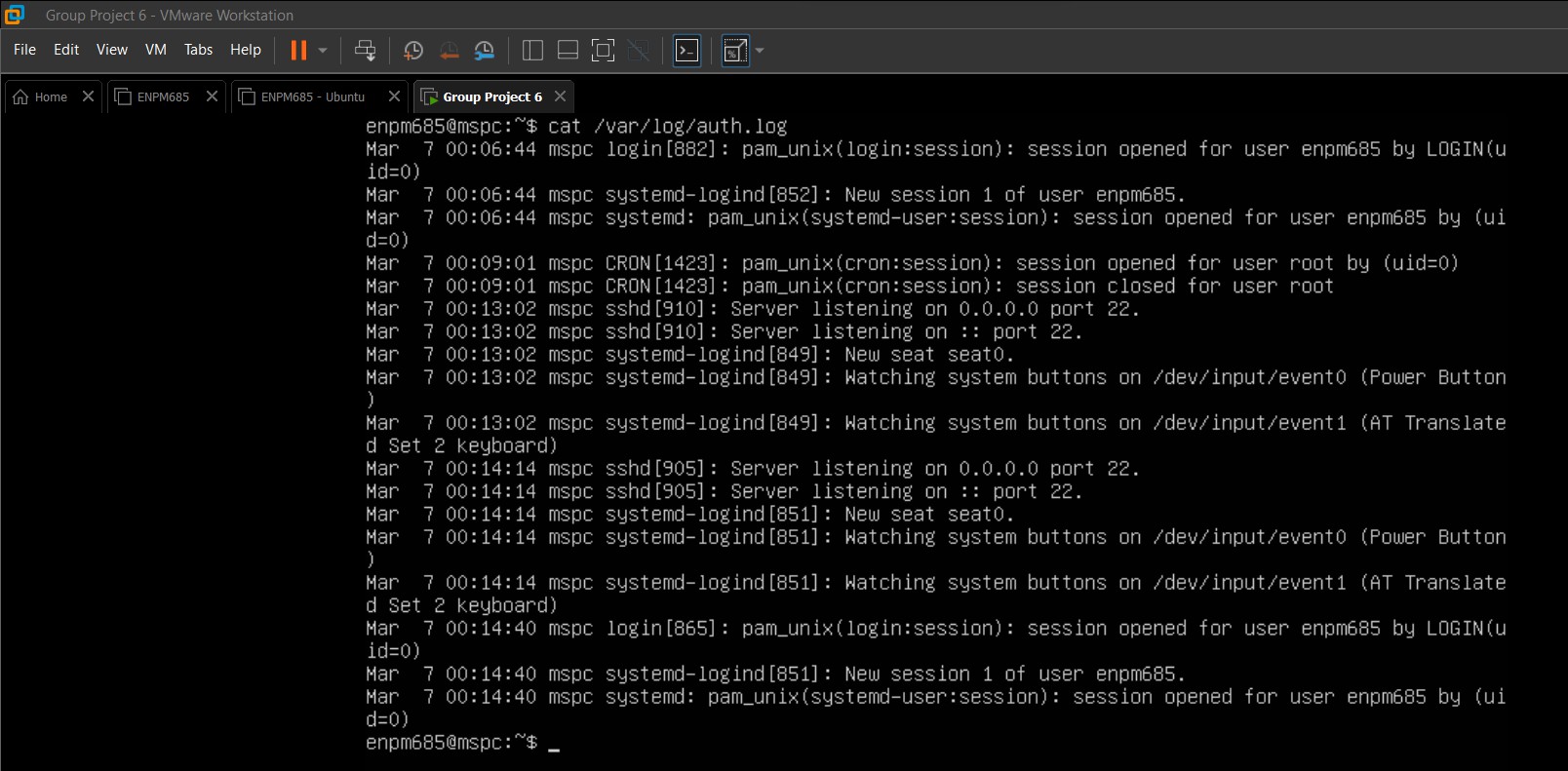
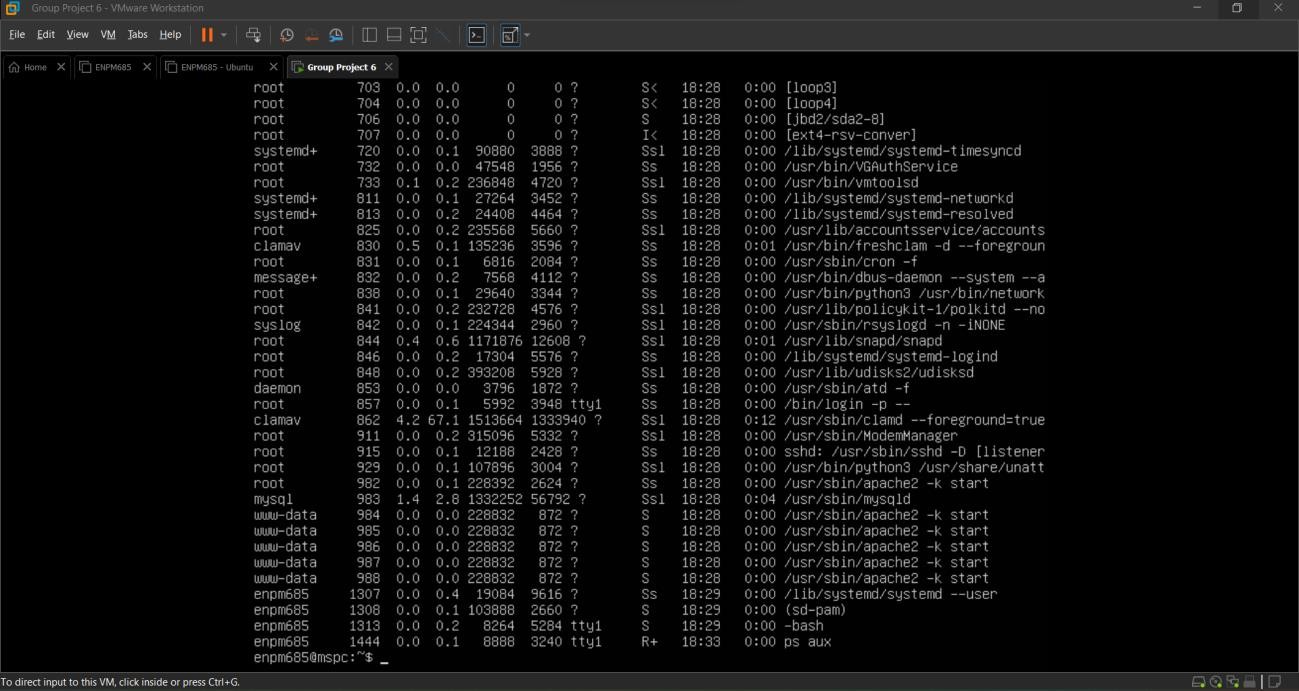
**Evaluation/Evidence:** Executing the **cat /etc/passwd** command on Ubuntu provides users with the ability to examine the content of the **/etc/passwd** file. This file acts as a centralized database containing information about user accounts configured on the system. It organizes user details into specific fields such as usernames, home directories, default shells, unique numerical identifiers (UIDs), and primary group identifiers (GIDs).

The **ps aux** command on Ubuntu indicated in the second screenshot is used for presenting information about the currently active processes on the system. It furnishes a comprehensive list of all processes, encompassing those initiated by various users. Each process entry typically contains details such as the user responsible for initiating the process, the Process ID (PID), CPU and memory consumption, command name, and other relevant information.

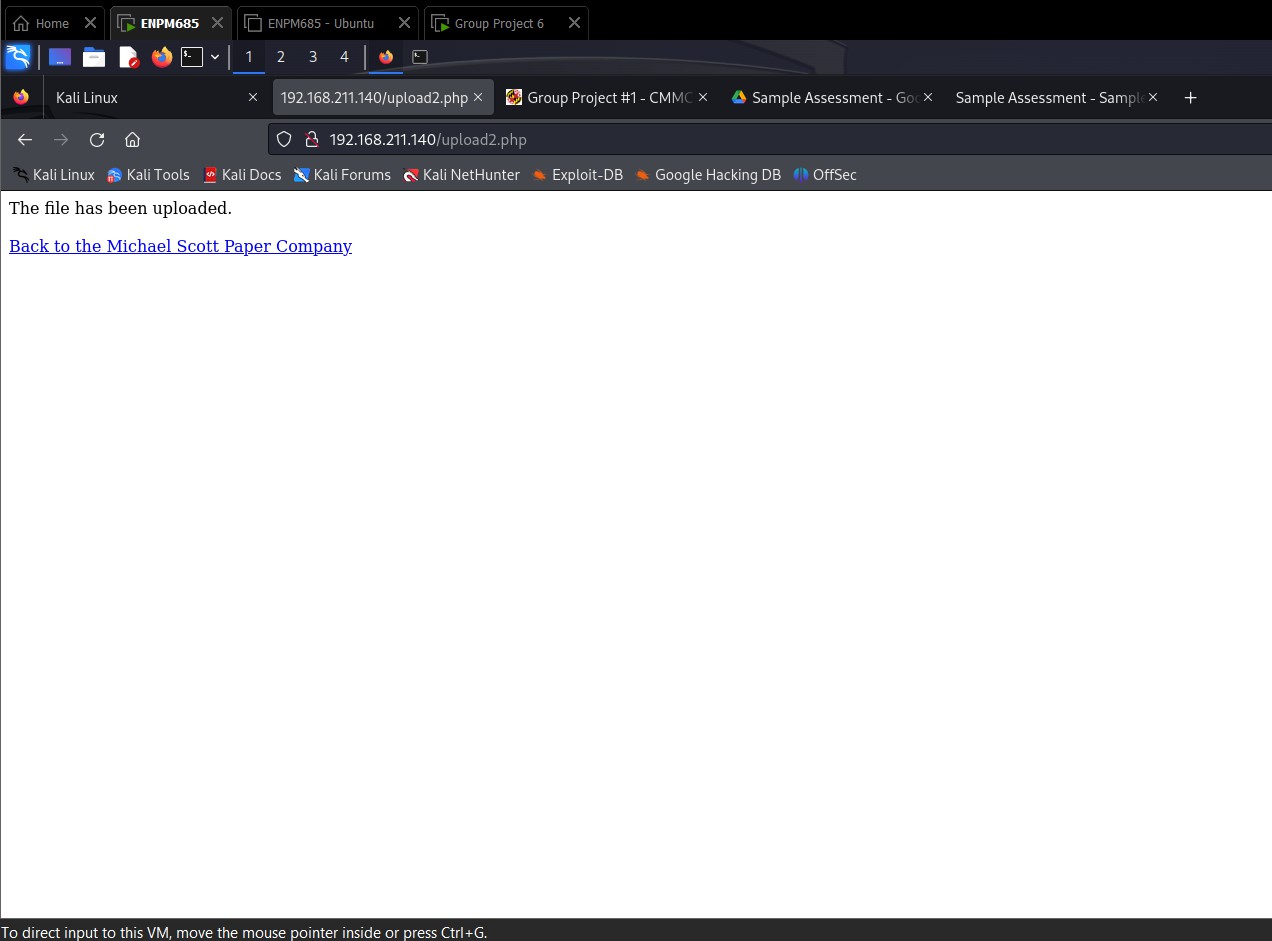
In the third screenshot, we can see details related to user logins, which can be useful while trying to monitor any user access to the system.

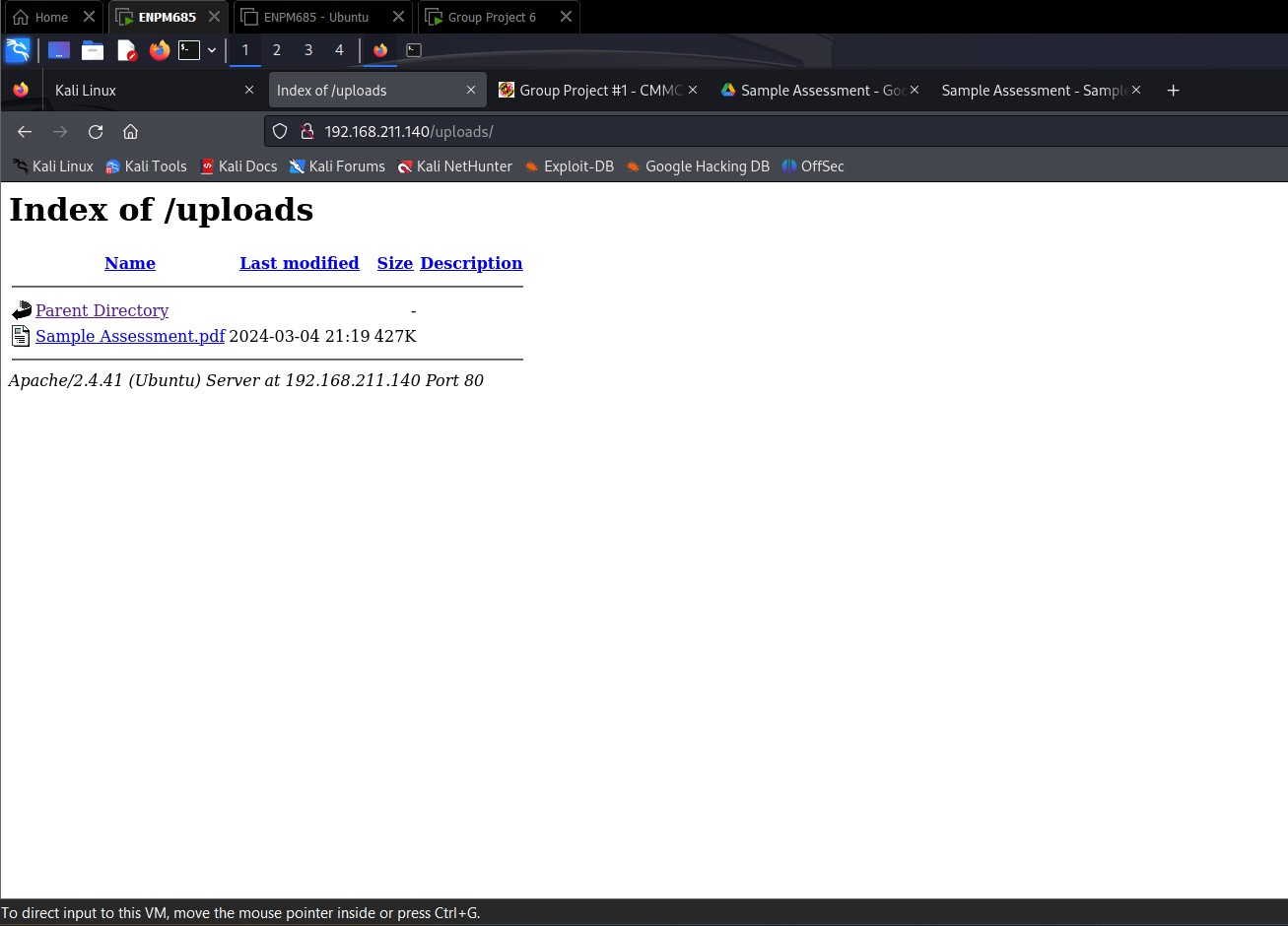
Michael Scott Paper Company’s web application homepage suggests that a distinct user login feature is in the pipeline for implementation. Currently, the application lacks user identification, leading to unregulated uploading and downloading of files.











### Recommendations for Improvement:

* Enhance the security of user accounts by implementing strong password policies and enforcing multi-factor authentication (MFA). Additionally, conduct a thorough review of user access permissions, ensuring that individuals have access only to the resources necessary for their roles. Implement stringent controls for file uploads, including restrictions on file types and sizes, to prevent potential security threats.
* Implement malware scanning on uploaded files to mitigate the risk of malicious content. Additionally, establish secure file download mechanisms, ensuring that only authorized users can access and download files.
* Strengthen logging mechanisms to capture relevant security events, such as user logins, failed login attempts, and critical system activities. Regularly review and monitor logs for any suspicious activities or unauthorized access attempts. Set up alerts to promptly identify abnormal or potentially malicious behavior.

## IA.L1-3.5.2 - AUTHENTICATION

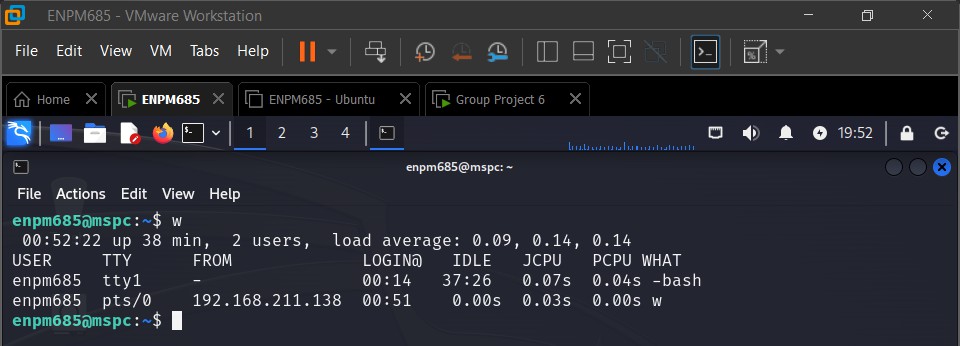
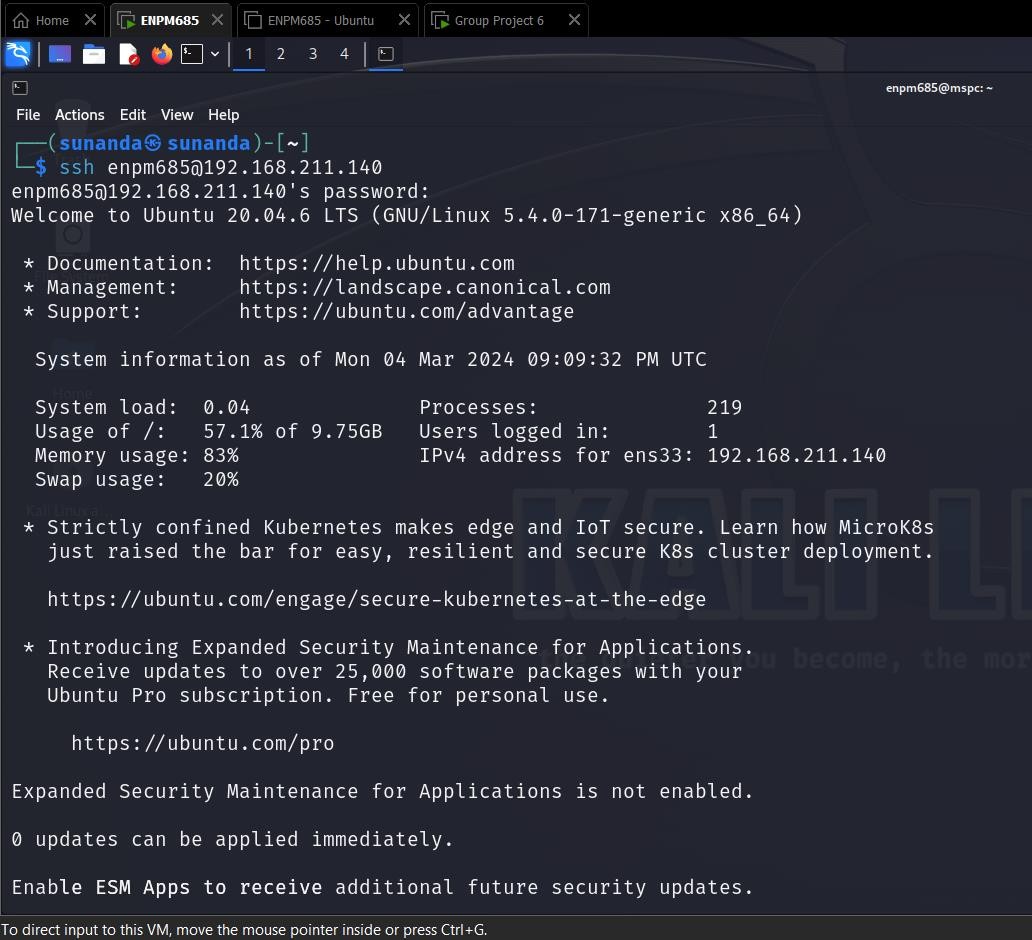
#### Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

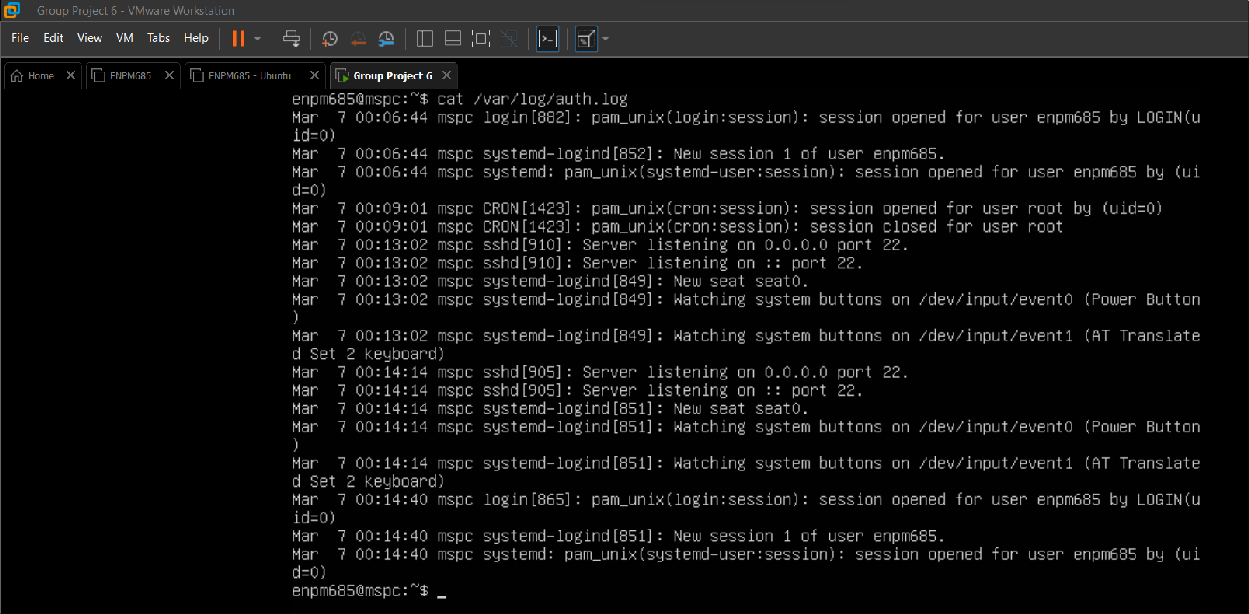
**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** Upon SSH access to the Ubuntu user enpm685 via its IP address, the system requests the password for the Ubuntu user, signaling that the web server employs user authentication before permitting entry. Furthermore, scrutiny of the auth.log file unveils entries documenting authentication and logging activities for users, each identified by their respective user IDs.

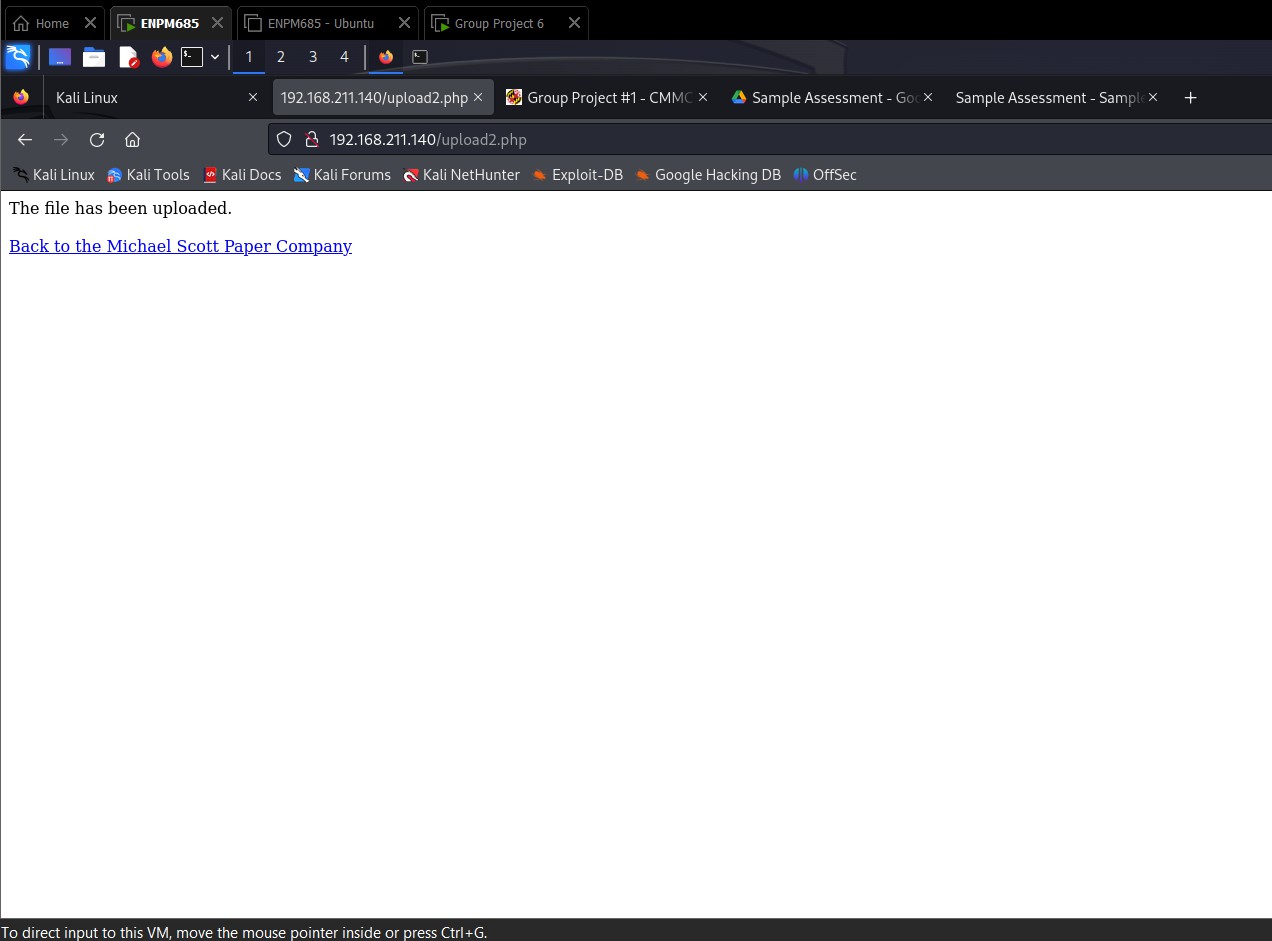
The present state of the web application does not incorporate any user authentication mechanisms, as the implementation of the unique user login feature is pending. Consequently, individuals can access the system and upload content without encountering any restrictions.

Even though the web server carries out user authentication, which is being validated while accessing Ubuntu via SSH, the web application lacks any user login feature functionality, leaving it vulnerable to potential security threats. Hence, it is imperative to prioritize the implementation of user authentication within the web application.









### Recommendations for Improvement:

* Develop a mechanism to allow users to create individual accounts within the web application. This typically involves a registration process where users provide necessary information such as username, email, and password. Create a secure login page where users can enter their credentials to access the web application. Establish a clear authentication workflow that validates user credentials against the stored data during the login process. Successful authentication should grant users access to the application, while unsuccessful attempts trigger appropriate error messages or account lockout policies.
* Implement logging and monitoring functionalities within the web application to capture relevant security events, including authentication activities. This will aid in identifying and responding to potential security incidents.

# Media Protection (MP)

## MP.L1-3.8.3 – MEDIA DISPOSAL

#### Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** The Michael Scott Paper Company has a media destruction policy that applies to all employees and consists of identifying and classifying physical media based on media sensitivity. The policy creates proper definitions of what classifies as PII or sensitive information and enforces rules on media destruction. This includes contracting with an external vendor for hardware destruction and using authorized software to digitally wipe software drives. All destroyed media must be documented including date, method and personnel involved to ensure proper handling. This policy is documented within the MSPC-Media-Destruction-Policy.

# Physical Protection (PE)

## PE.L1-3.10.1 – LIMIT PHYSICAL ACCESS

#### Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** The Michael Scott Paper Company has a policy for the IT department to control access to the data center facility, including all physical access points and areas containing sensitive information or critical infrastructure. This access is based on the principle of least privilege. Access to the Michael Scott Paper Company’s data center is only given to authorized personnel with legitimate business needs who additionally have the proper job role and responsibilities. Access must be requested through official channels and is based on the requestor’s job role. This policy is documented within the MSPC-Data-Center-Policy.

## PE.L1-3.10.3 – ESCORT VISITORS

#### Escort visitors and monitor visitor activity

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** Any visitors must be pre-authorized by the MSPC IT department/facility management and must be accompanied by an authorized and trained employee or contractor while visiting the data center. The accompanying authorized employee is responsible for monitoring the visitor and ensuring the visitor adheres to any relevant data center access policies. This policy is documented within the MSPC-Data-Center-Policy.

## PE.L1-3.10.4 – PHYSICAL ACCESS LOGS

#### Maintain audit logs of physical access.

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** As documented within the Michael Scott Paper Company’s Data Center Policy, all visitors must sign in and out when visiting the data center and provide appropriate ID when doing so. The policy does not state whether current employees are also required to sign in/out when physically accessing the data center. This could be implemented using badges or other forms of identification for employees and temporary badges or a sign-in sheet for visitors. This policy is documented within the MSPC-Data-Center-Policy.

## PE.L1-3.10.5 – MANAGE PHYSICAL ACCESS

#### Control and manage physical access devices

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** Included within the policy is the management of all areas containing any critical infrastructure. The MSPC is responsible for identifying and managing any physical access devices and storing them in controllable locations. The policy does not explicitly manage exactly

how the physical devices are being logged within the asset inventory. It is recommended that the Michael Scott Paper Company implement a robust asset management system which includes information on each physical access device, what the device is used for, the sensitivity of information stored on the device, and the location of the device which should be periodically inventoried. This policy is documented within the MSPC-Data-Center-Policy.

# System and Communications Protection (SC)

## SC.L1-3.13.1 – BOUNDARY PROTECTION

***Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.***

### Is this requirement being met? MET NOT MET N/A

**Evaluation/Evidence:** Network configurations were reviewed, and it was found that external activities are denied by default. Only authorized ports, protocols, and services are allowed. However, there are no firewalls, gateways, routers, or encrypted tunnels that were implemented to protect the information.

### Recommendations for improvement:

* + Implement Firewalls and IPS/IDS at network boundaries to monitor and control inbound and outbound traffic.
  + Implement network segmentation from critical systems from less sensitive networks to reduce attack surface.
  + Implement strong access control and authentication mechanisms to ensure that only authorized users can access sensitive systems.
  + Implement encryption at rest and in transit to protect from unauthorized access.

## SC.L1-3.13.5 – PUBLIC-ACCESS SYSTEM SEPARATION

***Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.***

### Is this requirement being met? MET NOT MET N/A

**Evaluation/Evidence:** Public-access systems are neither physically nor logically segregated from internal systems since there are no firewalls, gateways, or routers. There are no perimeter networks established. There are no specialized VLANs, or DMZs designated for subnetwork isolation.

### Recommendations for improvement:

* + Implement DMZ zone between public internet and private internal systems.
  + Segment public facing systems from internal networks and sensitive critical data.
  + Implement firewalls and IPS/IDS to monitor and filter inbound and outbound traffic.
  + Implement WAF to protect web applications from common web-based attacks.
  + Encrypt traffic between public facing systems and user by using HTTPS/TLS secure protocols.

# System and Information Integrity (SI)

## SI.L1-3.14.1 – FLAW REMEDIATION

***Identify, report, and correct information and information system flaws in a timely manner.***

### Is this requirement being met? MET NOT MET N/A

**Evaluation/Evidence:** There is no formal process for identifying and reporting system flaws in place. There are no policy procedures defined for regular vulnerability scans or configuration scans, thus systems are vulnerable. The web application is potentially vulnerable to clickjacking.

### Recommendations for improvement:

* + Implement a vulnerability management program that includes frequent vulnerability assessments, scanning, and patch management procedures.
  + Implement a systematic patch management strategy to enable the timely distribution of security patches and upgrades for operating systems, applications, and firmware. To remain up to date on newly identified vulnerabilities, follow vendor security advisories on a regular basis.
  + Maintain a current inventory of hardware and software assets and implement configuration management procedures to standardize setups and maintain consistency across systems, making it easier to detect and fix issues.

## SI.L1-3.14.2 – MALICIOUS CODE PROTECTION

#### Provide protection from malicious code at appropriate locations within the organizational information systems.

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** The Michael Scott Paper Company has ClamAV installed on their workstation image. ClamAV is an open-source antivirus product that can conduct on-demand command line-based scanning. ClamAV appears to be properly updated as the program appears to have updated recently which can be seen in the ClamAV logs and by running the version command.

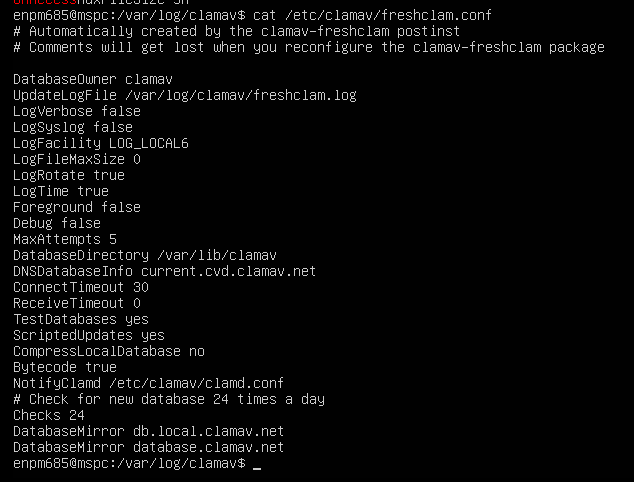


## SI.L1-3.14.4 – UPDATE MALICIOUS CODE PROTECTION

#### Update malicious code protection mechanisms when new releases are available

**Is this requirement being met? MET** NOT MET N/A

**Evaluation/Evidence:** The freshclam conf file (ClamAV update service) contains the ScriptedUpdates flag and is configured to check for updates 24 times a day (approximately once per hour). This should ensure the virus databases are properly updated to detect new threats. Additionally the ClamAV version is one that is still supported for updates.

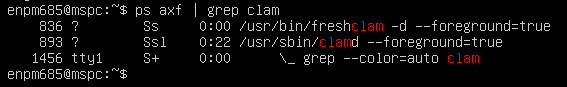


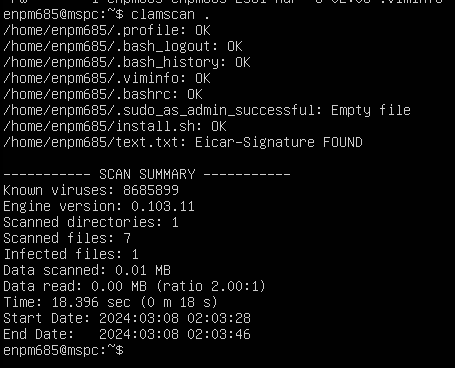
## SI.L1-3.14.5 – SYSTEM & FILE SCANNING

***Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.***

### Is this requirement being met? MET NOT MET N/A

**Evaluation/Evidence:** There does not appear to be a scheduled process such as cron for running periodic file scans despite the presence of ClamAV on the device. Additionally, the ClamAV service does not have the ScanOnAccess setting set within the clamd.conf configuration file set or the clamonacc process running which would allow for real-time scanning of potentially malicious files. This was tested by placing the eicar test file on device and not seeing a real-time response then running a scan to verify the file was found.





### Recommendations for Improvement:

* Establish a recurring system, utilizing tools like cron, to conduct periodic file scans using ClamAV. Schedule these scans during periods of low activity to minimize any potential disruptions. Creating a cron job to periodically run ClamAV scans at fixed intervals and enabling the ScanOnAccess flag would help ensure that threats are being monitored periodically and in real-time. According to the ClamAV website, on-access scanning can be enabled by changing the following in the ClamAV clamd.conf file:
  1. Set the `ScanOnAccess` option to `yes`
  2. Specify the path(s) to recursively watch by setting the `OnAccessIncludePath` option
  3. Set `OnAccessPrevention` to `yes`.

The ‘clamonacc’ daemon (ClamAV’s on-access utility) can then be started.

* Enable ongoing monitoring of ClamAV logs to observe scanning activities and detect any irregularities or issues. Regularly examine these logs to verify that scans are proceeding as intended and that the system is effectively identifying and responding to potential threats.
* Integrate ClamAV scanning activities into the incident response plan. Define procedures for responding to detected threats, including isolating affected systems, removing malicious files, and investigating the root cause.
* Create comprehensive documentation for the ClamAV configuration settings and conduct regular reviews to confirm their alignment with industry best practices and security standards. This documentation serves as a valuable reference for consistently maintaining a secure configuration.
* Activate the ScanOnAccess setting within the clamd.conf configuration file. This configuration enhancement facilitates real-time scanning of files as they are accessed or opened, enabling the system to promptly detect and respond to potential threats. Essentially, with ScanOnAccess enabled, ClamAV continuously monitors file access events, ensuring immediate scrutiny for any malicious content and allowing for swift actions to mitigate security risks. This real-time scanning capability enhances the overall security posture of the system by proactively identifying and addressing potential threats in a timely manner.