Group Project #1

CMMC 2.0 Level 1 Assessment

Group 12

Name	Reuben Thomas	Aravindha Hariharan M	Bhavin Panchal	Pranay Venkata Bhamidipati
UID Number	119610626	119449875	120278907	120235726
Course and Section	ENPM685 0201	ENPM685 0301	ENPM685 0301	ENPM685 0201
Email ID	reuben10@umd.edu	aravindh@umd.edu	bhavin22@umd.edu	pbhamid1@umd.edu

Honor Pledge:
"I pledge on my honor that I have not given or received any unauthorized assistance on this exam/assignment."

Table of Contents

Executive Summary

Our team's objective was to audit the security posture of ‘Michael Scott Paper Company’ and do an assessment using the self-assessment document, based on the CMMC policy created by the Department of Defense (DOD). Access control, external connections, public information control, identity and authentication, media disposal, physical protection, boundary protection, and system and communications protection were among the many areas of concern that the assessment found to be concerning. Important discoveries were made when examining the security posture of the company. Vulnerabilities in directory permissions and system entry are exposed by access control. Although Transaction & Function Control works well, there is a need for firewall and VPN deployment because External Connections are not properly verified. Access policies for Public Information Control need to be improved. Strong identification and authentication are hampered by password regulation. There isn't any proof that Media Protection is causing destruction. Physical protection adheres to access restrictions, although device management and logging may be strengthened. Network border identification and improved firewall configurations are necessary for system and communications protection. Flaws in remediation and code protection are exposed by system and information integrity, necessitating enhanced measures and specified timelines. To ensure compliance with CMMC 2.0 Level 1 requirements and improve the organization's overall cybersecurity resilience, recommendations have been made to address these issues.

Reference:

CMMC Self-Assessment Guide

Access Control (AC)

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

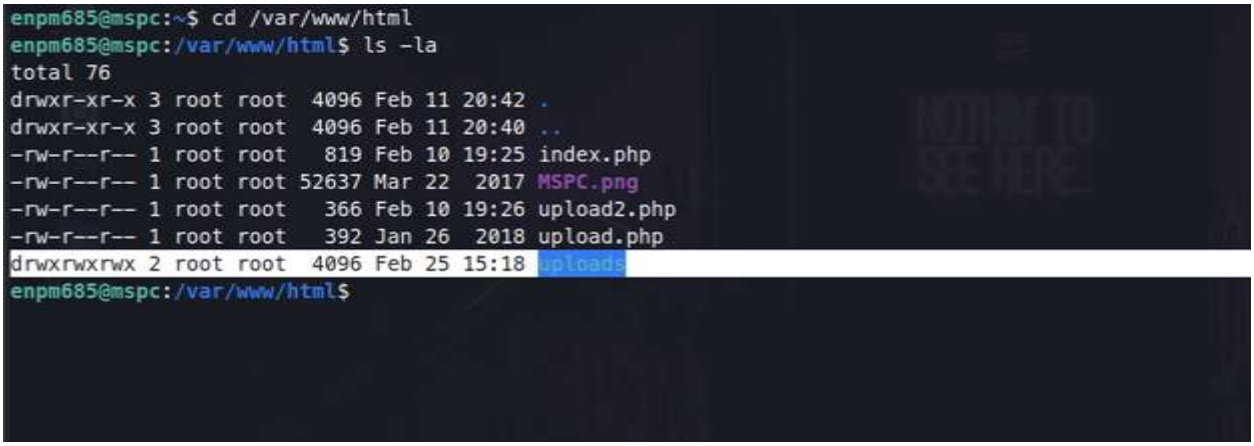
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

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

Evaluation/Evidence:

The system effectively authorized users, processes, and devices requesting access. Each user within the system is assigned with appropriate privileges and group access, coupled with sudo privileges for elevated permissions when necessary. However, the "/var/www/html/uploads" directory which stores sensitive information from users has overly permissive access, allowing read, write, and execute permissions for all users on the system. This configuration contradicts the requirement to limit information system access to authorized users, processes acting on behalf of authorized users, or devices.

System users are identified with unique User ID and Group ID



/var/www/html/uploads directory is configured with improper access controls, resulting in unauthorized and unrestricted access to the directory

Recommendations:
It is advisable to apply the least privilege approach and limit access permissions for the specified directory to authorized users only. Enhancing authentication protocols is crucial to secure access controls and address unauthorized entry points. Increasing the effectiveness of these safeguards will improve system security overall and reduce the possibility of unwanted access. Provide user training to increase understanding of access control rules, evaluate and update access controls on a regular basis, and set up logging and monitoring systems to track unauthorized access attempts.

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:

All users possess unique usernames and are grouped with restricted access to their respective home directories, enhancing user-level security. Additionally, access to the MySQL database, which may contain sensitive information, is limited to a select group of high-privileged users. This segmentation ensures that only authorized individuals with the necessary privileges can execute specific transactions and functions within the system, aligning with the control requirements and fostering a secure access control environment. Furthermore, the Apache web server, responsible for hosting the web application, operates under the restricted user account "www-data." This account is intentionally limited and lacks access to any folder or file data without appropriate permissions.

MySQL user accounts where only the root user has access and privileges to connect to the database.

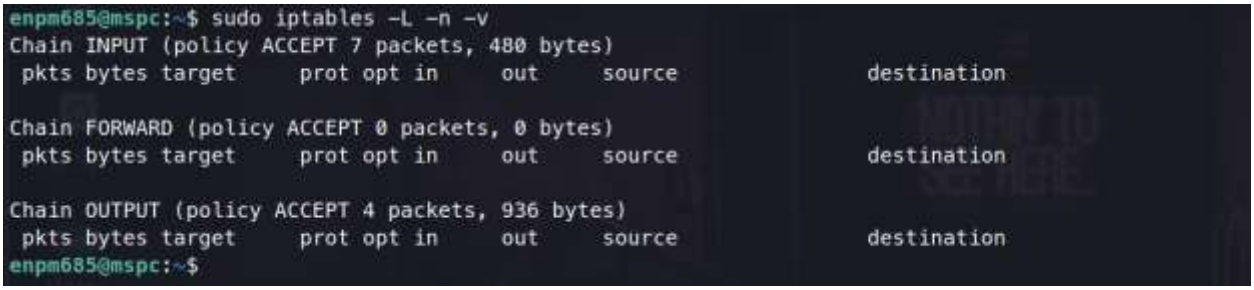
AC.L1-3.1.20 – EXTERNAL CONNECTIONS

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

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

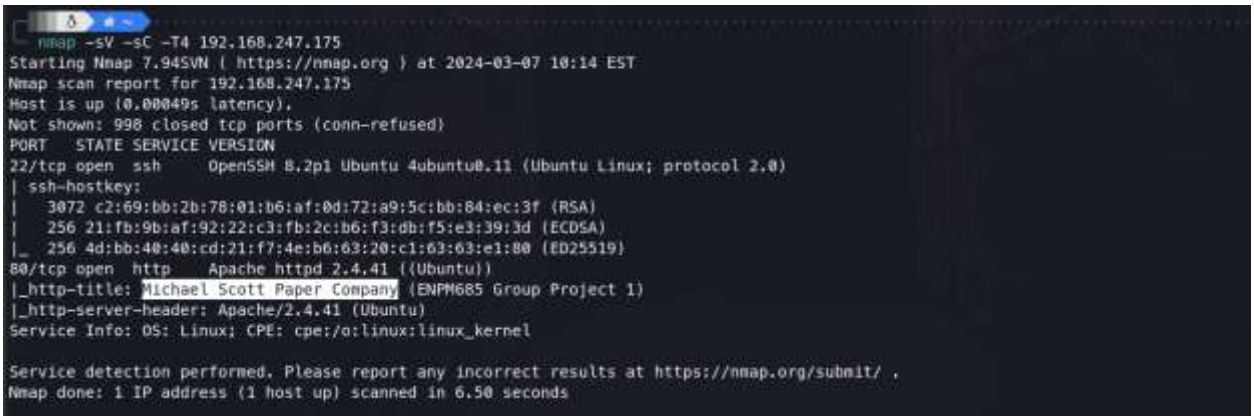
Evaluation/Evidence:

The requirement AC.L1-3.1.20 for verifying and limiting connections to external information systems has not been met. During our review, we found that adequate controls were not in place to verify and restrict communication between the internal network and external systems like employee devices or other public systems on the internet. The external assets connecting to the internal network were not being verified prior to giving them access to the system. Additionally, the current firewall (iptables) configuration of the system allows unrestricted flow of network traffic inbound and outbound to/from the system. The lack of network controls could allow the system on the internal network to connect to malicious websites/systems, which could potentially compromise sensitive Federal Contract Information (FCI) stored on the system. The objectives mandate proper identification and verification of external systems along with appropriate controls to limit such connections, and hence this requirement (AC.L1-3.1.20) has not been met.



Current firewall configuration allows unrestricted access to inbound and outbound communications

Demonstration of lack of outbound firewall rules, which allows the internal system (web server) to communicate with unverified and untrusted external systems.



Port scan of the system reveals the SSH port is open to the internet

Recommendations:

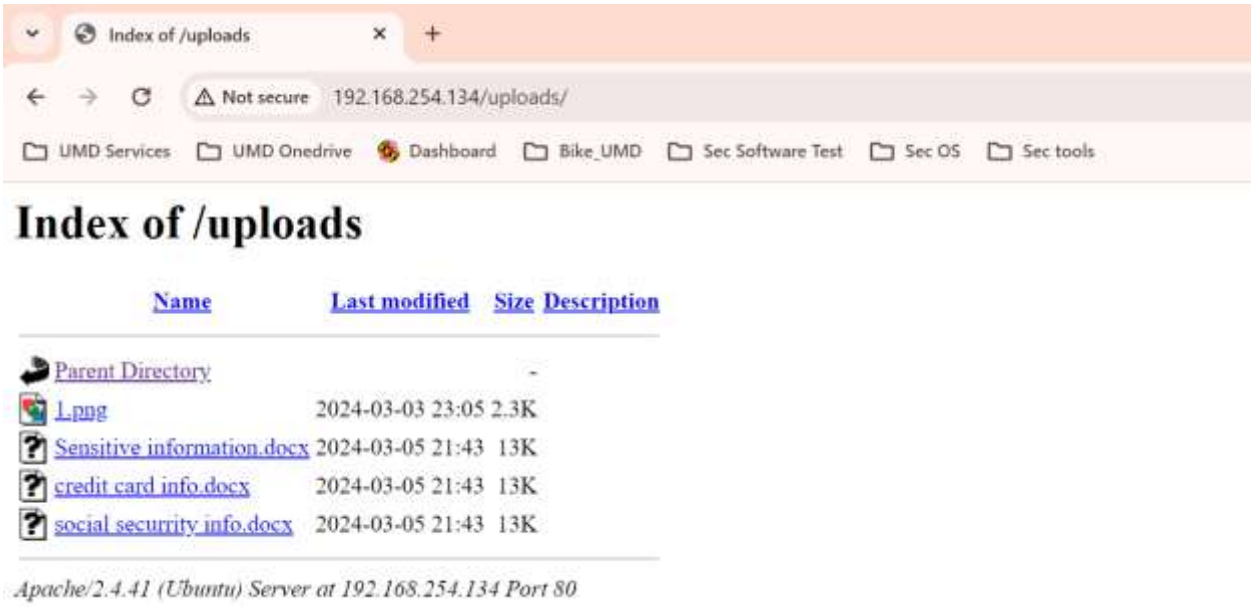
- Implementing firewalls with precise inbound and outbound rules, including Access Control Lists (ACLs), is imperative for ensuring robust network security. Restrict inbound traffic to allow remote access to known management IP addresses only. Block all outbound traffic from the internal network to external systems by default, and any exceptions must be pre-approved and verified by the IT Team. This can also help protect the data stored in the internal network by blocking connection attempts made to malicious systems or websites that could compromise the system.
- The IT team must identify external assets connecting to the internal network like employee devices, verify these systems prior to giving them access to the systems and restrict access to these users/systems only. Implementing a corporate VPN solution can help ensure only trusted and verified users have access to the internal network.
- The above recommendations along with role-based access to limit access to resources based on roles as mentioned in the policy can help meet this requirement by identifying, verifying and limiting connections to external information systems.

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:
This requirement mandates the control of information posted or processed on publicly accessible information systems. After reviewing, it can be concluded that Michael Scott Paper Company has not met this requirement, since Federal Contract Information (FCI) uploaded by clients are being posted and processed on the publicly accessible web server. The “/uploads” directory is publicly accessible on the internet, and sensitive FCI data could potentially be present on this publicly accessible directory. This can lead to exposure of sensitive upload information by the users and FCI. Furthermore, there are no specific-authorized individuals, policies that explicitly address or mention practices and procedures for controlling public information, particularly in terms of ensuring that sensitive or FCI is not disclosed on the public platform. Thus, these areas leave a potential gap in the company's public information control measures.



The ‘uploads’ directory is publicly accessible and anyone on the internet can access the web application to read client uploaded files like FCI

Recommendations:

- Implement access controls and configure web server settings to restrict unauthorized access to the /uploads directory, using user authentication or IP address filtering.
- Content on publicly accessible website should not contain FCI.
- Draft clear policies, procedures and guidelines for managing and securing FCI.
- Design an approval chain and implement a review process for content before it's posted to public systems.

Identification and Authentication (IA)

IA.L1-3.5.1 – IDENTIFICATION

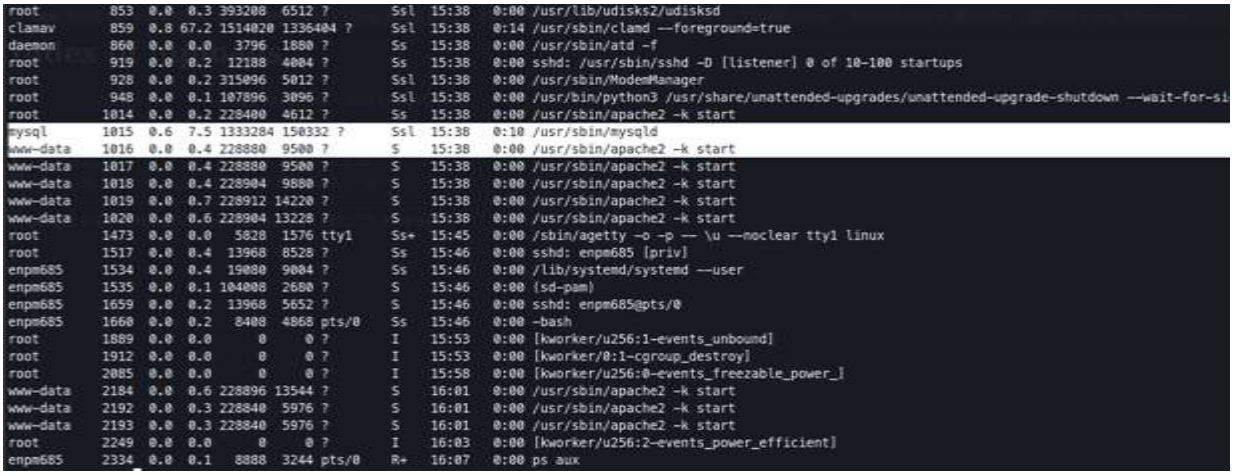
Identify information system users, processes acting on behalf of users, or devices

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

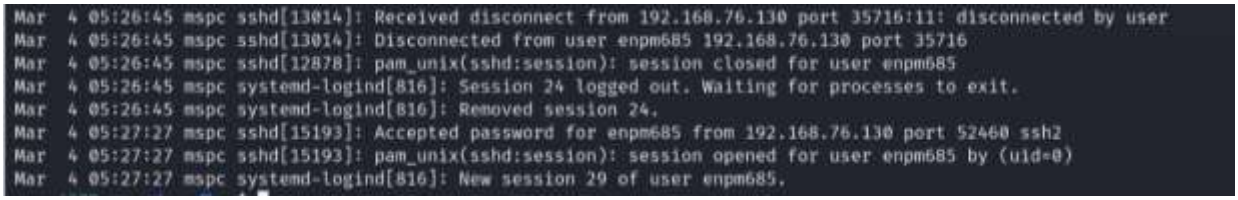
Evaluation/Evidence:

The requirement IA.L1-3.5.1, focusing on the identification of information system users, processes acting on behalf of users, and devices, is effectively met. Each user is assigned a unique identifier within a designated group, enhancing user distinction and accountability. Furthermore, all processes operate under restricted user privileges, ensuring that actions within the system are traceable to specific users. This approach aligns with the control requirements, establishing a robust framework for the clear identification of users, processes, and devices within the information system.

All users are identified by unique User ID and have their own respective home directories



System processes with restricted access as process user



External devices are identified and logged when attempting to access the system

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:

The criteria listed in IA.L1-3.5.2, which emphasizes authentication as a requirement for access to organizational information systems, are not met by the existing implementation. Weak password criteria provide a serious risk, even though the system uses strong authentication techniques to verify users and safely saves passwords with salt and high encryption standards. Although unprivileged tasks carried out by system processes are assigned distinct verified user accounts, a significant security vulnerability remains because some user accounts have passwords that do not adhere to the password policy as defined by the company in the authentication policy, leaving them open to dictionary-based attacks. It is critical to resolve this problem in order to reduce the related security threats and guarantee that authentication regulations are followed. Furthermore, the current state of the web application lacks authentication measures to verify whether a user possesses the necessary permissions for specific actions. This absence of user validation introduces a potential security vulnerability, emphasizing the need for implementing robust authentication mechanisms to ensure authorized access.

We found weak user credentials not following the company's password policy, making them susceptible to dictionary attacks

The web application lacks proper mechanisms to allow access to only authenticated users.

Recommendations:

Enforcing strict adherence to the organization's password policy is necessary to address this. In order to comply with industry best practices, this means enforcing a combination of complexity requirements for passwords, including length, alphanumeric composition, and the use of special characters. The implementation of proactive monitoring and regular audits can guarantee sustained adherence to the strengthened password policy, strengthening the authentication system's defense against possible security breaches. Ensure comprehensive authentication implementation across all systems and applications to accurately identify users and verify their authorized actions, establishing a secure environment by validating permissible actions for each user.

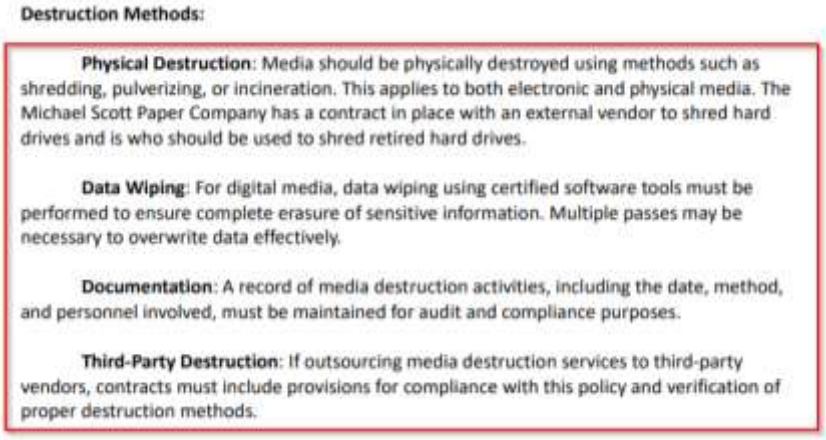
Media Protection (MP)

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 organization policy shows evidence of the appropriate steps and mechanisms that must be carried out in order to dispose or reuse the media containing FCI, however during our review we did not find any evidence or documentation of media destruction activities such as a certificate of destruction or media sanitation records that could indicate that these procedures were being followed correctly. Hence, this requirement (MP.L1-3.8.3) has been marked as not met.



Destruction Methods:

Physical Destruction: Media should be physically destroyed using methods such as shredding, pulverizing, or incineration. This applies to both electronic and physical media. The Michael Scott Paper Company has a contract in place with an external vendor to shred hard drives and is who should be used to shred retired hard drives.

Data Wiping: For digital media, data wiping using certified software tools must be performed to ensure complete erasure of sensitive information. Multiple passes may be necessary to overwrite data effectively.

Documentation: A record of media destruction activities, including the date, method, and personnel involved, must be maintained for audit and compliance purposes.

Third-Party Destruction: If outsourcing media destruction services to third-party vendors, contracts must include provisions for compliance with this policy and verification of proper destruction methods.

Source: Media-Destruction-Policy Page

Recommendations:

- Detailed records of all the media destruction activities must be maintained for audit purposes and to ensure adherence to compliance requirements.
- Certificates of destruction and other information of retired hard drives must be obtained as evidence from Third-Party vendors at the time of destruction.

The organization policy follows proper media sanitization guidelines by identifying and classifying data, performing appropriate media destruction steps such as physical destruction (shredding, pulverizing or incineration) of media containing FCI data. Additionally, for reusing a hard drive, the company has a policy of wiping/erasing the data multiple times with certified tools to ensure FCI/sensitive data is completely erased. The company also has a contract with an external vendor to shred all unused hard drives and to provide verification of the destruction methods. All these methods can ensure that FCI data on physical or digital media can no longer be read or retrieved. By maintaining a detailed record of all the media destruction activities, the requirement MP.L1-3.8.3 can be met.

Physical Protection (PE)

PE.L1-3.10.1 – LIMIT PHYSICAL ACCESS

Limit physical access to organization’s 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's Data Center Policy Document, revised in January 2024, outlines guidelines and procedures for limiting physical access to the data center facility. It mentions access controls, approval controls, and access level policies. However, our review found no evidence of how authentication is implemented. There was no data center design plan indicating restricted areas, nor were there physical logs for authenticated and authorized personnel. Given these gaps, it cannot be confirmed that the policy fully adheres to the requirement to limit physical access to authorized individuals.

Recommendations:

- Develop and maintain a detailed data center design plan highlighting restricted areas.
- Create a list of authorized members for the restricted or sensitive zones.
- Keep physical logs for all authenticated and authorized personnel entering/leaving the data center and other restricted zones.

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:

The Data Center Policy Document of Michael Scott Paper Company outlines the visitor access policy, stating that visitors must be signed in after identity verification and escorted by authorized personnel within the data center facility. However, during our review we did not find any visitor audit logs, nor was there evidence of how and where visitors are signing in. Furthermore, there is no evidence of proper visitor identification, as there is no mention of visitor tags or ID cards, nor of CCTV surveillance for monitoring their activities in the policy. Given these gaps, it cannot be confirmed that the policy fully adheres to the requirements for escorting visitors and monitoring their activity.

Recommendations:

- Implement a standardized visitor sign-in procedure with documented audit and log trails.
- Introduce visitor badges or ID cards for easy identification and tracking of visitors inside the data center.
- Install CCTV surveillance systems and have security personnel at different zones to monitor visitor movements physically and virtually within the data center.

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:

Based on the Data Center Policy Document of the Michael Scott Paper Company January 2024 Revised Edition and our review, this requirement is not met. The company has policies for physical access, but they are not comprehensively outlined. During our review, we did not find any physical access logs for entry and exit of personnel which can be used for audit purposes. This approach of not having physical access logs for everyone leaves a potential gap in security and may lead to unauthorized access not being detected.

Recommendations:

- Implement a unified access logging system for all individuals entering the data center.
- Use of electronic cards, biometrics at entry and exit points can be set up to ensure physical access security and logging.
- Set up CCTV cameras at entry and exit points.

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:

Based on the Data Center Policy Document of the Michael Scott Paper Company January 2024 Revised Edition and our review, there is no mention of managing physical access devices. The requirement for managing physical access devices involves specific practices and technologies

to control entry to secure areas, such as electronic card readers, biometric scanners, and surveillance systems along with their operation and maintenance. Furthermore, there is no list or inventories of physical access devices maintained by the company. Not managing physical access properly could pose significant security risks by leaving secure areas vulnerable to unauthorized access. Thus, this requirement is not met.

Recommendations:

- Implement existing access control system policies by installing electronic card readers or biometric scanners to secure entry points.
- Create and maintain inventory of physical access devices like keys, badges etc.
- Deploy CCTV cameras at critical access points for monitoring and recording.
- Schedule routine maintenance and functionality checks for all physical access devices.

System and Communications Protection (SC)

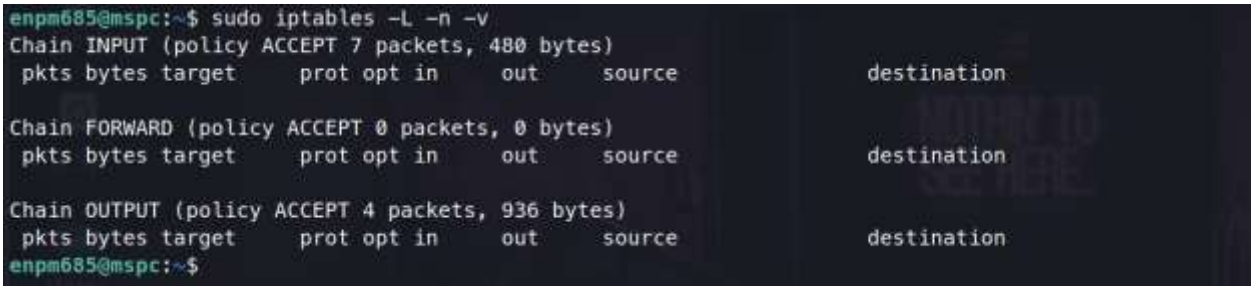
SC.L1-3.13.1 – BOUNDARY PROTECTION

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.

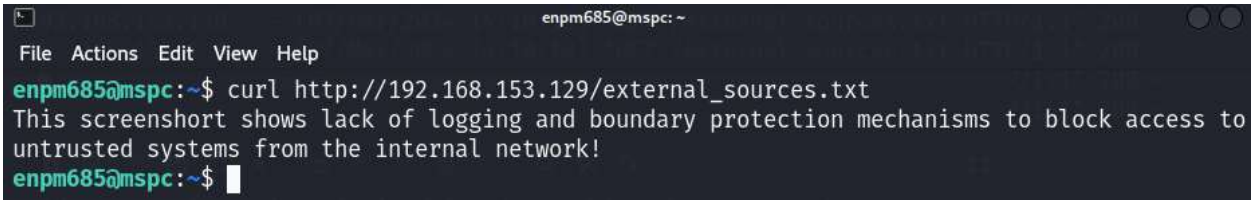
Is this requirement being met? MET **NOT MET** N/A

Evaluation/Evidence:

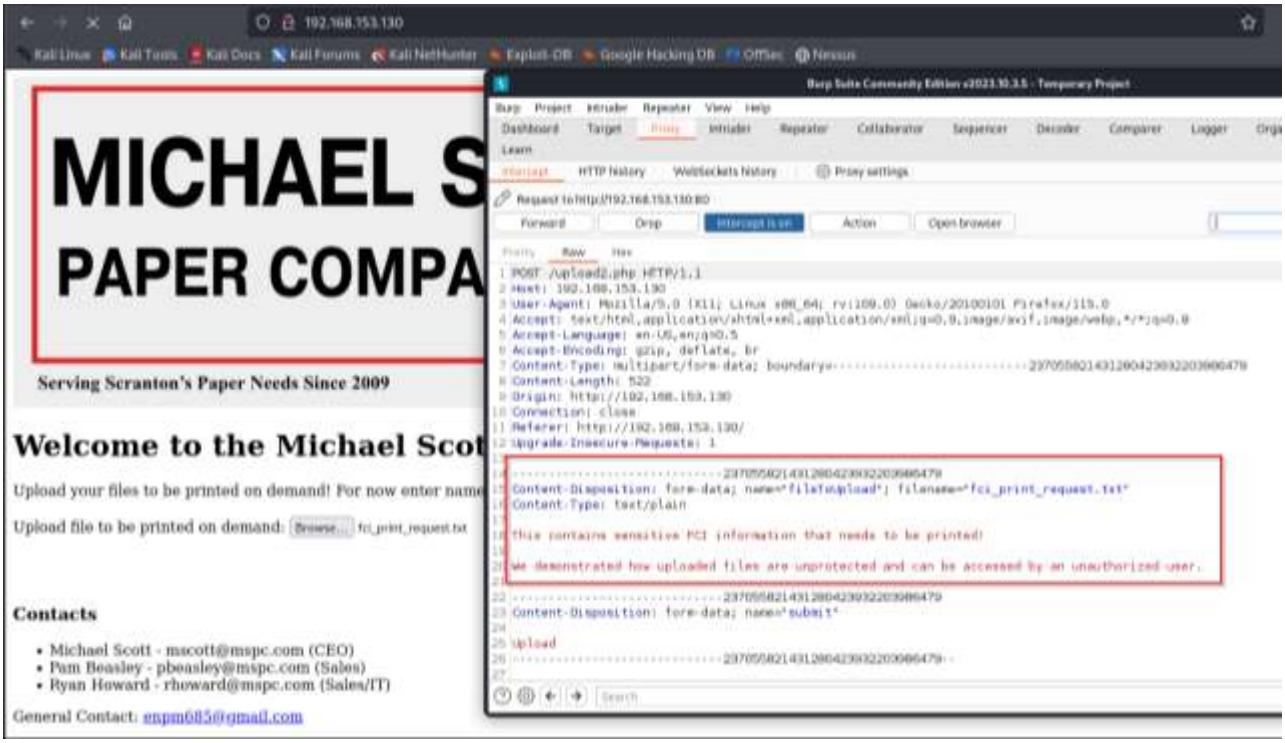
The requirement SC.L1-3.13.1 for monitoring, controlling and protecting the network communications taking place at network boundaries has not been met. During our review, we observed that internal and external system boundaries such as network entry and exit points were not clearly defined and documented. The firewall configuration in the system allows all traffic inbound and outbound of the network, and does not restrict or control the flow of network traffic. Therefore, untrusted connections to and from internal systems are not being verified and controlled. The absence of detailed network flow logs can impact monitoring capabilities of the organization since it is helpful in identifying and detecting malicious activities in the network. Furthermore, the organization also uses insecure HTTP protocol for their web application which could allow FCI data to be transmitted in clear text and thus susceptible to eavesdropping.



Firewalls not implemented with appropriate rules to restrict communication and absence of network logging.



The system allows connection to untrusted sources without any restrictions.



An attacker may be able to intercept network traffic and access confidential information that is transferred in plain text since the client and server are communicating using an unsecured HTTP protocol.

Recommendations:

- Identify and document the internal and external network boundaries to verify if critical resources are protected and all network ingress/egress points are properly defined.
- Implement a VPN solution to restrict access to sensitive resources in the company network to authorized users only. This control along with authentication and role-based access can limit the risk of unauthorized access in the internal network.
- Firewall rules must be configured to block all outbound traffic to untrusted sources by default and any exceptions must be pre-approved by the IT team. This can help protect internal systems from accessing or sending data to untrusted or malicious systems which could result in FCI data being compromised. Inbound traffic to management ports like SSH should be restricted to authorized/management IP addresses only.
- Maintain detailed logs of all network traffic flowing in and out of the network interfaces. The logs can help in achieving network visibility and can also be integrated with a SIEM tool to help identify and respond to malicious activities.
- Encrypt communication between the web application and the client by using TLS connections (Port 443) to ensure sensitive data in-transit is encrypted.

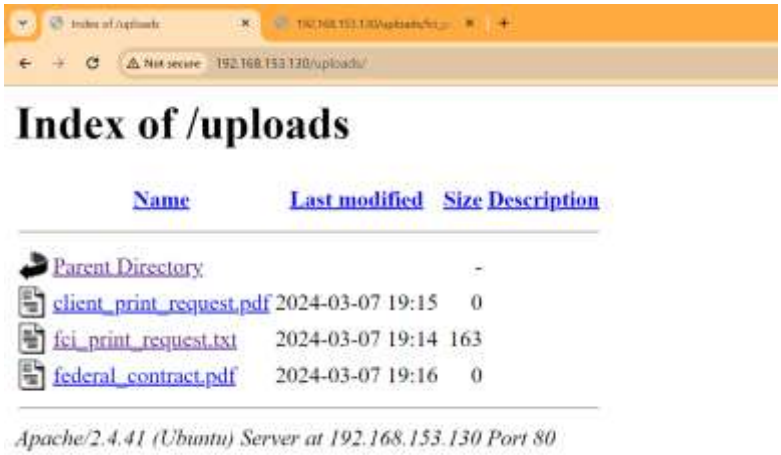
SC.L1-3.13.5 – PUBLIC-ACCESS SYSTEM SEPARATION

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:

We observed that the publicly accessible web server stores data such as sensitive Federal Contract Information (FCI) on the same system. Any such information uploaded by the clients for printing is stored on the web server and can be accessed from the '/uploads' directory of the web application. Sensitive data is at risk of exposure since anyone on the internet can access this directory due to lack of proper separation and security controls. The uploaded files were not stored in a separate internal database, nor did it have any access control measures in place to restrict unauthorized access to the uploads directory. The requirement SC.L1-3.13.5 mandates physical/logical separation of publicly accessible system components from internal resources that may contain FCI data, and hence this requirement could not be met.



Sensitive files uploaded by various clients are publicly accessible to unauthorized users without prior authentication.

The screenshot indicates how sensitive FCI data is at risk of unauthorized access due to lack of security controls or separation from the publicly accessible web server.

Recommendations:

- Implement proper access control measures such as authentication and authorization to allow only authorized users to access the uploaded data. Additionally, the client uploaded data must be stored in a separate secured internal database/system and communications to the internal systems must be restricted to minimize the risk of data exposure.
- Implement network segmentation to separate the publicly accessible web application from other internal company resources. Creating network subnets and implementing necessary security controls like firewalls to limit traffic flow can help protect and isolate FCI data.
- The publicly accessible web server can also be deployed on a separate DMZ network and allow access to the internal network to authorized users using a VPN.

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:

The system fails to meet any of the specified criteria for identifying, reporting, and rectifying system flaws. There is an absence of defined timeframes, reports, or documented procedures for addressing vulnerabilities in the system. We found no evidence of a vulnerability management process to identify, report or rectify vulnerabilities present in the operating systems or softwares installed. There is also a lack of proper documentation that defines the remediation timelines to fix various vulnerabilities found in the internal systems based on their criticality.

Recommendations:
To rectify the non-adherence with the specified requirements for identifying, reporting, and fixing system flaws, the following measures are recommended:

- Implement a vulnerability management process to identify and detect vulnerabilities in systems and have a well-defined process to fix the identified issues as per criticality levels and remediation service-level agreements (SLAs).
- Conduct frequent audits of processes and perform periodic vulnerability scans/assessments.
- Use patch management tools to automate fixes to systems based on the findings of the vulnerability scans.
- Documents all the above scanning/remediation activities and ensure specific timeframes required for fixing system flaws based on severity levels are properly defined.

SI.L1-3.14.2 – MALICIOUS CODE PROTECTION

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

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

Evaluation/Evidence:

The requirement SI.L1-3.14.2 for providing protection from malicious code within organizational information systems is not fully met. Despite the presence of ClamAV on the system, there are significant gaps in the protection mechanism. Specifically, the installed ClamAV does not perform scans on uploaded files, and there is an absence of file type validation during the upload process.

This deficiency leaves the system vulnerable to potential threats, as malicious code within files may go undetected and unaddressed.

```
enpm685@mspc:/var/www/html$ cat upload2.php
<?php

$target_dir = "/var/www/html/uploads/";
$target_file = $target_dir.basename($_FILES["fileToUpload"]["name"]);


if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file))
{
        echo "The file has been uploaded.";
}
else
{
        echo "Error uploading file.";
}
?>
<br><br>
<a href="/index.php">Back to the Michael Scott Paper Company</a>
enpm685@mspc:/var/www/html$
```

PHP code doesn't have any input file validation to restrict malicious code uploads

```
enpm685@mspc:~$ clamscan --version
ClamAV 0.103.11/27202/Sat Mar  2 09:23:28 2024
enpm685@mspc:~$
enpm685@mspc:~$ systemctl status clamav-daemon
● clamav-daemon.service - Clam AntiVirus userspace daemon
     Loaded: loaded (/lib/systemd/system/clamav-daemon.service; enabled; vendor preset: enabled)
    Drop-In: /etc/systemd/system/clamav-daemon.service.d
             └─extend.conf
     Active: active (running) since Sat 2024-03-02 15:38:20 UTC; 40min ago
       Docs: man:clamd(8)
             man:clamd.conf(5)
             https://docs.clamav.net/
    Process: 831 ExecStartPre=/bin/mkdir -p /run/clamav (code=exited, status=0/SUCCESS)
    Process: 856 ExecStartPre=/bin/chown clamav /run/clamav (code=exited, status=0/SUCCESS)
   Main PID: 859 (clamd)
      Tasks: 2 (limit: 2218)
     Memory: 1.2G
     CGroup: /system.slice/clamav-daemon.service
             └─859 /usr/sbin/clamd --foreground=true

Mar 02 15:38:52 mspc clamd[859]: Sat Mar  2 15:38:52 2024 -> Portable Executable support enabled.
Mar 02 15:38:52 mspc clamd[859]: Sat Mar  2 15:38:52 2024 -> ELF support enabled.
Mar 02 15:38:52 mspc clamd[859]: Sat Mar  2 15:38:52 2024 -> Mail files support enabled.
Mar 02 15:38:52 mspc clamd[859]: Sat Mar  2 15:38:52 2024 -> OLE2 support enabled.
```

Even though ClamAV is enabled and running, it doesn't scan for malicious code

Recommendations:

Enforcing strong file upload security in the PHP codebase is essential to close this security gap. In order to make sure that only approved file types are allowed, first incorporate file type validation checks into the upload process. Immediately upon upload completion, launch the ClamAV antivirus program and do a full file scan of every uploaded file. Segregate and quarantine any file that ClamAV flags as harmful right away to stop any further damage from occurring. Using ClamAV for real-time scanning and integrating file type validation strengthens the information system's security measures and strengthens the organization's defenses against harmful code.

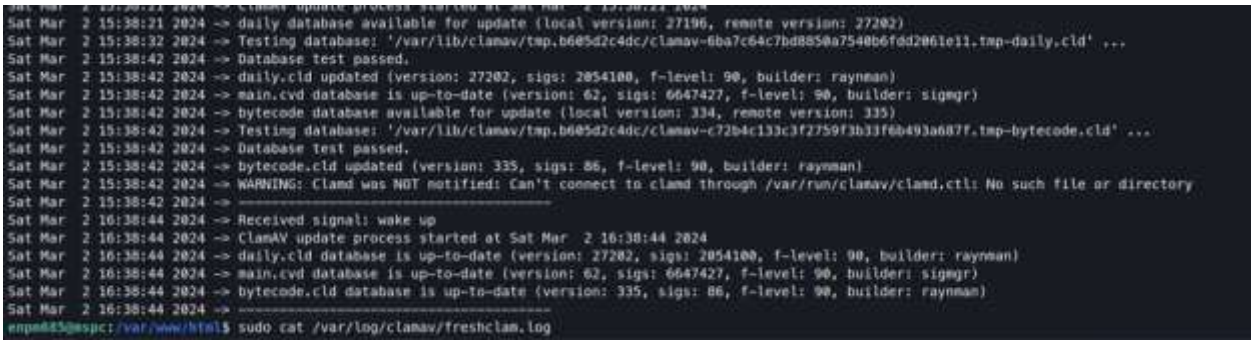
SI.L1-3.14.4 – UPDATE MALICIOUS CODE PROTECTION

Update malicious code protection mechanisms when new releases are available

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

Evaluation/Evidence:

The installed instance of ClamAV is continuously updated, guaranteeing that the most recent features, bug patches, and virus definitions are quickly integrated into the system's defense mechanisms. Using the freshclam tool strengthens the organization's dedication to automatic signature database upgrades and improves its capacity to proactively counter new threats. This proactive method of remaining up to date with releases and signature databases shows how to maintain the robustness of the organizational information systems' harmful code prevention mechanisms in a strong and efficient manner. Assuring the continuous effectiveness of the preventative measures will depend on regular monitoring and validation of the updating procedure.



Freshclam service logs, indicating scheduled and automated updates for malware signature database

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:

During our review, we observed that the organization has installed and configured ClamAV anti-virus on the web server to periodically scan the system for threats. The antivirus software was observed to be in the active running state and was configured to perform scheduled scans of the system at predetermined intervals. However, we noticed that the anti-virus software did not have real-time protection capabilities enabled. Files that were uploaded or downloaded to the system

from external sources by users were not being scanned for threats. Since the objective mandates real-time scanning of files from external sources, this requirement (SI.L1-3.14.5) has not been met.

```
enpm685@mspc:/var/log$ cat /etc/clamav/clamd.conf
#Automatically Generated by clamav-daemon postinst
#To reconfigure clamd run #dpkg-reconfigure clamav-daemon
#Please read /usr/share/doc/clamav-daemon/README.Debian.gz for details
LocalSocket /var/run/clamav/clamd.ctl
FixStaleSocket true
LocalSocketGroup clamav
LocalSocketMode 666
# TemporaryDirectory is not set to its default /tmp here to make overriding
# the default with environment variables TMPDIR/TMP/TEMP possible
User clamav
ScanMail true
ScanArchive true
ArchiveBlockEncrypted false
MaxDirectoryRecursion 15
FollowDirectorySymlinks false
FollowFileSymlinks false
ReadTimeout 180
MaxThreads 12
```

The ClamAV configuration file lacks the real-time scanning configuration.

```
enpm685@mspc:/var/log$ sudo tail -n 50 /var/log/clamav/clamav.log
Tue Mar  5 22:00:15 2024 -> Bytecode: Security mode set to "TrustSigned".
Tue Mar  5 22:01:20 2024 -> Loaded 8685899 signatures.
Tue Mar  5 22:01:24 2024 -> LOCAL: Unix socket file /var/run/clamav/clamd.ctl
Tue Mar  5 22:01:24 2024 -> LOCAL: Setting connection queue length to 15
Tue Mar  5 22:01:24 2024 -> Limits: Global time limit set to 120000 milliseconds.
Tue Mar  5 22:01:24 2024 -> Limits: Global size limit set to 104857600 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: File size limit set to 26214400 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: Recursion level limit set to 16.
Tue Mar  5 22:01:24 2024 -> Limits: Files limit set to 10000.
Tue Mar  5 22:01:24 2024 -> Limits: MaxEmbeddedPE limit set to 10485760 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: MaxHTMLNormalize limit set to 10485760 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: MaxHTMLNoTags limit set to 2097152 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: MaxScriptNormalize limit set to 5242880 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: MaxZipTypeRcg limit set to 1048576 bytes.
Tue Mar  5 22:01:24 2024 -> Limits: MaxPartitions limit set to 50.
Tue Mar  5 22:01:24 2024 -> Limits: MaxIconsPE limit set to 100.
Tue Mar  5 22:01:24 2024 -> Limits: MaxRecHWP3 limit set to 16.
Tue Mar  5 22:01:24 2024 -> Limits: PCREMatchLimit limit set to 10000.
Tue Mar  5 22:01:24 2024 -> Limits: PCRERecMatchLimit limit set to 5000.
Tue Mar  5 22:01:24 2024 -> Limits: PCREMaxFileSize limit set to 26214400.
Tue Mar  5 22:01:24 2024 -> Archive support enabled.
Tue Mar  5 22:01:24 2024 -> AlertExceedsMax heuristic detection disabled.
```

ClamAV log file misses real-time scanning of files when uploaded or downloaded from external sources

Recommendations:

- Anti-malware or antivirus software like ClamAV must be properly configured and installed to help to detect and eliminate potential threats. The frequency of automated periodic scans must be defined in the policy, and systems on the network must be configured accordingly.
- In addition to scheduled periodic scans, real-time scanning must also be enabled to ensure any files downloaded or executed on the system are free from malware.
- Ensure antivirus software is updated regularly to ensure malware signatures are updated. This can help identify and quarantine threats more effectively.
- Behavior and pattern analysis techniques can be used to prevent malicious files from executing on the system.