

CMMC 2.0 LEVEL 1 ASSESSMENT

Table of Contents

1. Access Control (AC)	3
AC.L1-3.1.1 – Authorized Access Control	3
AC.L1-3.1.2 – Transaction and Function Control.....	4
AC.L1-3.1.20 – External Connections	6
AC.L1-3.1.22 – Control Public Information	7
2. Identification and Authentication (IA)	9
IA.L1-3.5.1 – Identification	9
IA.L1-3.5.2 – Authentication.....	14
3. Media Protection(MP)	18
MP.L1-3.8.3 – Media Disposal.....	18
4. Physical Protection (PE)	18
PE.L1-3.10.1 – Limit Physical Access	18
PE.L1-3.10.3 – Escort Visitors	19
PE.L1-3.10.4 – Physical Access Logs	19
PE.L1-3.10.5 – Manage Physical Access.....	19
5. System and Communications Protection (SC)	20
SC.L1-3.13.1 – Boundary Protection	20
SC.L1-3.13.5 – Public Access System Separation	20
6. System and Information Integrity (SI)	21
SI.L1-3.14.1 – Flaw Remediation	21
SI.L1-3.14.2 – Malicious Code Protection	22
SI.L1-3.14.4 – Update Malicious Code Protection	22
SI.L1-3.14.5 – System and File Scanning.....	23

1. 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.

```
Mar 3 05:17:01 mspc CRON[53297]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 05:17:01 mspc CRON[53297]: pam_unix(cron:session): session closed for user root
Mar 3 05:39:01 mspc CRON[53983]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 05:39:01 mspc CRON[53983]: pam_unix(cron:session): session closed for user root
Mar 3 06:09:01 mspc CRON[54678]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 06:09:01 mspc CRON[54678]: pam_unix(cron:session): session closed for user root
Mar 3 06:17:01 mspc CRON[54942]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 06:17:01 mspc CRON[54942]: pam_unix(cron:session): session closed for user root
Mar 3 06:25:01 mspc CRON[55184]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 06:25:02 mspc CRON[55184]: pam_unix(cron:session): session closed for user root
Mar 3 06:39:01 mspc CRON[55627]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 06:39:01 mspc CRON[55627]: pam_unix(cron:session): session closed for user root
Mar 3 06:47:01 mspc CRON[55860]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 06:47:01 mspc CRON[55860]: pam_unix(cron:session): session closed for user root
Mar 3 07:39:01 mspc CRON[56404]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 07:39:01 mspc CRON[56404]: pam_unix(cron:session): session closed for user root
Mar 3 08:10:16 mspc CRON[57683]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 08:10:16 mspc CRON[57683]: pam_unix(cron:session): session closed for user root
Mar 3 08:17:01 mspc CRON[57982]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 08:17:01 mspc CRON[57982]: pam_unix(cron:session): session closed for user root
Mar 3 08:39:01 mspc CRON[58440]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 08:39:02 mspc CRON[58440]: pam_unix(cron:session): session closed for user root
Mar 3 16:09:01 mspc CRON[59547]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 16:09:01 mspc CRON[59547]: pam_unix(cron:session): session closed for user root
Mar 3 16:17:01 mspc CRON[59809]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 16:17:01 mspc CRON[59809]: pam_unix(cron:session): session closed for user root
Mar 3 18:09:08 mspc CRON[60169]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 3 18:09:08 mspc CRON[60169]: pam_unix(cron:session): session closed for user root
Mar 3 18:27:31 mspc login[878]: pam_unix(login:auth): check pass; user unknown
Mar 3 18:27:31 mspc login[878]: authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty1 ruser= rhost=
Mar 3 18:27:34 mspc login[878]: FAILED LOGIN (1) on '/dev/tty1' FOR 'UNKNOWN', Authentication failure
Mar 3 18:27:48 mspc login[878]: pam_unix(login:session): session opened for user enpm685 by LOGIN(uid=0)
Mar 3 18:27:48 mspc systemd-logind[850]: New session 17 of user enpm685.
Mar 3 18:27:49 mspc systemd: pam_unix(systemd-user:session): session opened for user enpm685 by (uid=0)
Mar 3 18:29:35 mspc sshd[60456]: Accepted password for enpm685 from 192.168.72.1 port 53899 ssh2
Mar 3 18:29:35 mspc sshd[60456]: pam_unix(sshd:session): session opened for user enpm685 by (uid=0)
Mar 3 18:29:35 mspc systemd-logind[850]: New session 19 of user enpm685.
enpm685@mspc:~$
```

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.

```

enpm685@mspc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/:run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:/:run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
enpm685:x:1000:1000:enpm685:/home/enpm685:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:/nonexistent:/bin/false
clamav:x:115:120:/:var/lib/clamav:/bin/false
mscott:x:5002:5002:Michael Scott,,,:/home/mscott:/bin/bash
pbeasley:x:5003:5003:Pam Beasley,,,:/home/pbeasley:/bin/bash
rhoward:x:5004:5004:Ryan Howard,,,:/home/pbeasley:/bin/bash
enpm685@mspc:~$

```

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.

```
pbeasley:x:5003:5003:Pam Beasley,,,:/home/pbeasley:/bin/bash
rhoward:x:5004:5004:Ryan Howard,,,:/home/pbeasley:/bin/bash
enpm685@mspc:~$ ss -tulnp
Netid      State      Recv-Q     Send-Q      Local Address:Port      Peer Address:Port      Process
udp        UNCONN    0           0            127.0.0.53%lo:53        0.0.0.0:*
udp        UNCONN    0           0            192.168.72.131%ens33:68 0.0.0.0:*
tcp        LISTEN    0           4096         127.0.0.53%lo:53        0.0.0.0:*
tcp        LISTEN    0           128         0.0.0.0:22              0.0.0.0:*
tcp        LISTEN    0           70          127.0.0.1:33060         0.0.0.0:*
tcp        LISTEN    0           151         127.0.0.1:3306         0.0.0.0:*
tcp        LISTEN    0           511         *:80                   *:80
tcp        LISTEN    0           128         [::]:22                [::]:*
```

AC.L1-3.1.22 – CONTROL PUBLIC INFORMATION

Control information posted or processed on publicly accessible information systems.

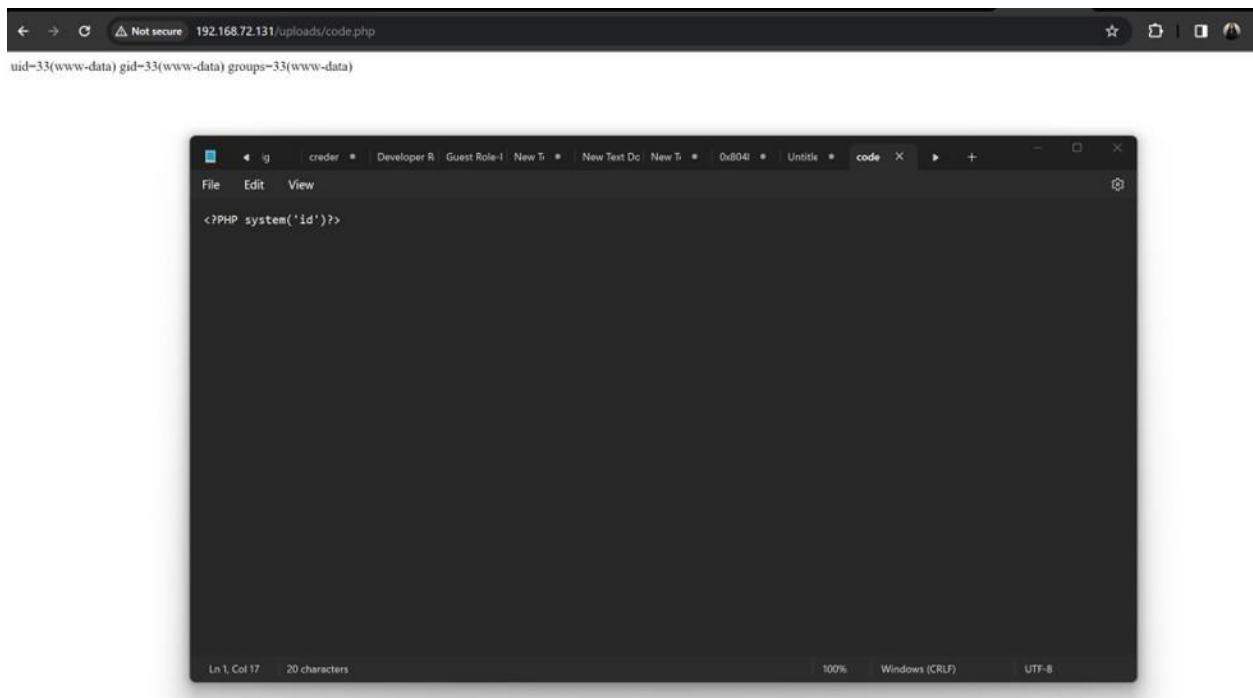
Is this requirement being met? MET NOT MET N/A

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.

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



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.

2. Identification and Authentication (IA)

IA.L1-3.5.1 - IDENTIFICATION

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

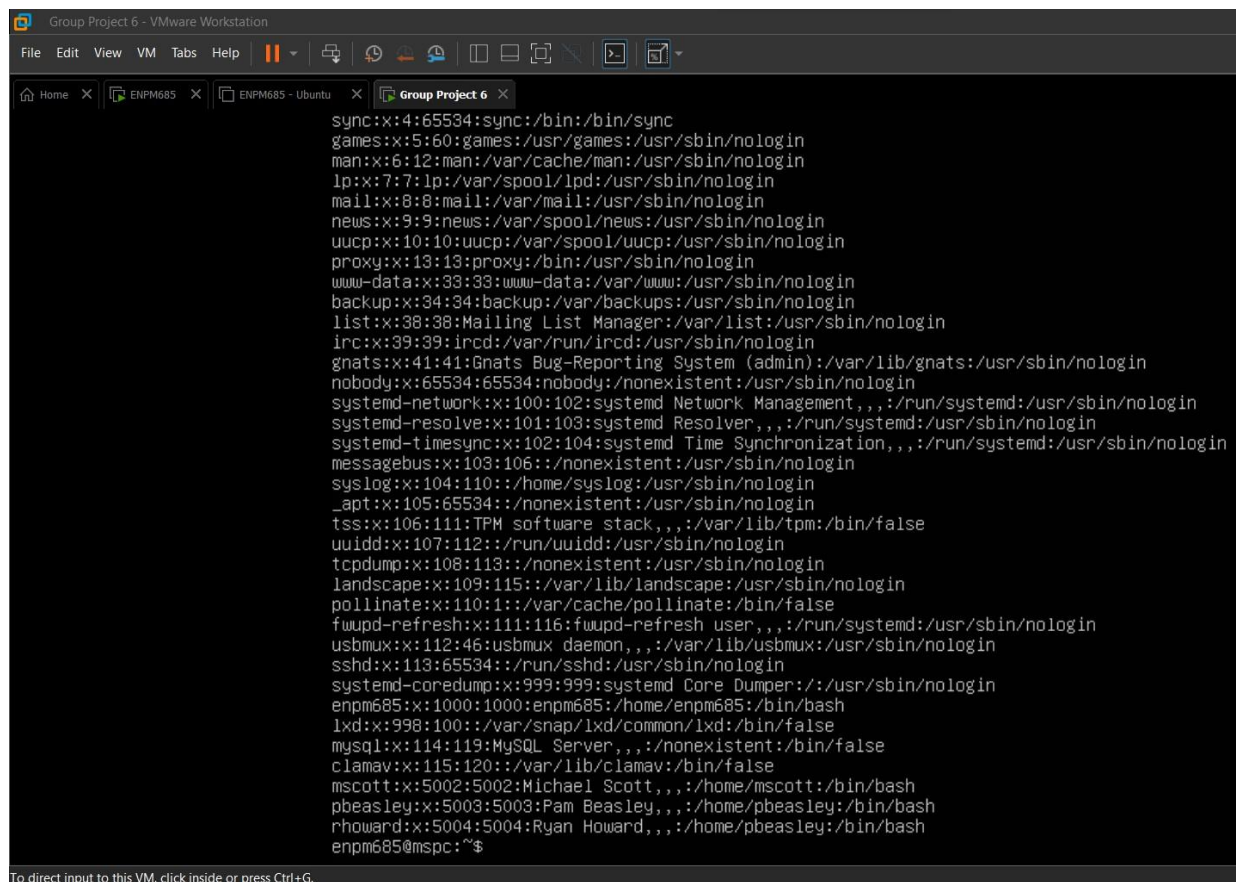
Is this requirement being met? MET NOT MET N/A

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.



```
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106:/:nonexistent:/usr/sbin/nologin
syslog:x:104:110:/:home/syslog:/usr/sbin/nologin
_apt:x:105:65534:/:nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112:/:run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113:/:nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1:/:var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534:/:run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:usr/sbin/nologin
enpm685:x:1000:1000:enpm685:/home/enpm685:/bin/bash
lxd:x:998:100:/:var/snap/lxd/common/lxd:/bin/false
mysql:x:114:119:MySQL Server,,,:nonexistent:/bin/false
clamav:x:115:120:/:var/lib/clamav:/bin/false
mscott:x:5002:5002:Michael Scott,,,:/home/mscott:/bin/bash
pbeasley:x:5003:5003:Pam Beasley,,,:/home/pbeasley:/bin/bash
rhoward:x:5004:5004:Ryan Howard,,,:/home/pbeasley:/bin/bash
enpm685@mspc:~$
```

To direct input to this VM, click inside or press Ctrl+G.

```
Group Project 6 - VMware Workstation
File Edit View VM Tabs Help
Group Project 6
Home ENPM685 ENPM685 - Ubuntu Group Project 6
root 703 0.0 0.0 0 0 ? S< 18:28 0:00 [loop3]
root 704 0.0 0.0 0 0 ? S< 18:28 0:00 [loop4]
root 706 0.0 0.0 0 0 ? S 18:28 0:00 [jbd2/sda2-8]
root 707 0.0 0.0 0 0 ? I< 18:28 0:00 [ext4-rsv-conver]
systemd+ 720 0.0 0.1 90880 3888 ? Ssl 18:28 0:00 /lib/systemd/systemd-timesyncd
root 732 0.0 0.0 47548 1956 ? Ss 18:28 0:00 /usr/bin/VGAuthService
root 733 0.1 0.2 236848 4720 ? Ssl 18:28 0:00 /usr/bin/vmtoolsd
systemd+ 811 0.0 0.1 27264 3452 ? Ss 18:28 0:00 /lib/systemd/systemd-networkd
systemd+ 813 0.0 0.2 24408 4464 ? Ss 18:28 0:00 /lib/systemd/systemd-resolved
root 825 0.0 0.2 235568 5660 ? Ssl 18:28 0:00 /usr/lib/accounts-service/accounts
clamav 830 0.5 0.1 135236 3596 ? Ss 18:28 0:01 /usr/bin/freshclam -d --foreground
root 831 0.0 0.1 6816 2084 ? Ss 18:28 0:00 /usr/sbin/cron -f
message+ 832 0.0 0.2 7568 4112 ? Ss 18:28 0:00 /usr/bin/dbus-daemon --system --a
root 838 0.0 0.1 29640 3344 ? Ss 18:28 0:00 /usr/bin/python3 /usr/bin/network
root 841 0.0 0.2 232728 4576 ? Ssl 18:28 0:00 /usr/lib/policykit-1/polkitd --no
syslog 842 0.0 0.1 224344 2960 ? Ssl 18:28 0:00 /usr/sbin/rsyslogd -n -iNONE
root 844 0.4 0.6 1171876 12608 ? Ssl 18:28 0:01 /usr/lib/snapd/snapd
root 846 0.0 0.2 17304 5576 ? Ss 18:28 0:00 /lib/systemd/systemd-logind
root 848 0.0 0.2 393208 5928 ? Ssl 18:28 0:00 /usr/lib/udisks2/udisksd
daemon 853 0.0 0.0 3796 1872 ? Ss 18:28 0:00 /usr/sbin/atd -f
root 857 0.0 0.1 5992 3948 tty1 Ss 18:28 0:00 /bin/login -p --
clamav 862 4.2 67.1 1513664 1333940 ? Ssl 18:28 0:12 /usr/sbin/clamd --foreground=true
root 911 0.0 0.2 315096 5332 ? Ssl 18:28 0:00 /usr/sbin/ModemManager
root 915 0.0 0.1 12188 2428 ? Ss 18:28 0:00 sshd: /usr/sbin/sshd -D [listener
929 0.0 0.1 107896 3004 ? Ssl 18:28 0:00 /usr/bin/python3 /usr/share/unatt
root 982 0.0 0.1 228392 2624 ? Ss 18:28 0:00 /usr/sbin/apache2 -k start
mysql 983 1.4 2.6 1332252 56792 ? Ssl 18:28 0:04 /usr/sbin/mysqld
www-data 984 0.0 0.0 228832 872 ? S 18:28 0:00 /usr/sbin/apache2 -k start
www-data 985 0.0 0.0 228832 872 ? S 18:28 0:00 /usr/sbin/apache2 -k start
www-data 986 0.0 0.0 228832 872 ? S 18:28 0:00 /usr/sbin/apache2 -k start
www-data 987 0.0 0.0 228832 872 ? S 18:28 0:00 /usr/sbin/apache2 -k start
www-data 988 0.0 0.0 228832 872 ? S 18:28 0:00 /usr/sbin/apache2 -k start
enpm685 1307 0.0 0.4 19084 9616 ? Ss 18:29 0:00 /lib/systemd/systemd --user
enpm685 1308 0.0 0.1 103888 2660 ? S 18:29 0:00 (sd-pam)
enpm685 1313 0.0 0.2 8264 5284 tty1 S 18:29 0:00 -bash
enpm685 1444 0.0 0.1 8888 3240 tty1 R+ 18:33 0:00 ps aux
enpm685@mspc:~$ _

To direct input to this VM, click inside or press Ctrl+G
Group Project 6 - VMware Workstation
File Edit View VM Tabs Help
Group Project 6
Home ENPM685 ENPM685 - Ubuntu Group Project 6
enpm685@mspc:~$ cat /var/log/auth.log
Mar 7 00:06:44 mspc login[882]: pam_unix(login:session): session opened for user enpm685 by LOGIN(u
id=0)
Mar 7 00:06:44 mspc systemd-logind[852]: New session 1 of user enpm685.
Mar 7 00:06:44 mspc systemd: pam_unix(systemd-user:session): session opened for user enpm685 by (ui
d=0)
Mar 7 00:09:01 mspc CRON[1423]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 7 00:09:01 mspc CRON[1423]: pam_unix(cron:session): session closed for user root
Mar 7 00:13:02 mspc sshd[910]: Server listening on 0.0.0.0 port 22.
Mar 7 00:13:02 mspc sshd[910]: Server listening on :: port 22.
Mar 7 00:13:02 mspc systemd-logind[849]: New seat seat0.
Mar 7 00:13:02 mspc systemd-logind[849]: Watching system buttons on /dev/input/event0 (Power Button
)
Mar 7 00:13:02 mspc systemd-logind[849]: Watching system buttons on /dev/input/event1 (AT Translate
d Set 2 keyboard)
Mar 7 00:14:14 mspc sshd[905]: Server listening on 0.0.0.0 port 22.
Mar 7 00:14:14 mspc sshd[905]: Server listening on :: port 22.
Mar 7 00:14:14 mspc systemd-logind[851]: New seat seat0.
Mar 7 00:14:14 mspc systemd-logind[851]: Watching system buttons on /dev/input/event0 (Power Button
)
Mar 7 00:14:14 mspc systemd-logind[851]: Watching system buttons on /dev/input/event1 (AT Translate
d Set 2 keyboard)
Mar 7 00:14:40 mspc login[865]: pam_unix(login:session): session opened for user enpm685 by LOGIN(u
id=0)
Mar 7 00:14:40 mspc systemd-logind[851]: New session 1 of user enpm685.
Mar 7 00:14:40 mspc systemd: pam_unix(systemd-user:session): session opened for user enpm685 by (ui
d=0)
enpm685@mspc:~$ _
```

Home x ENPM685 x ENPM685 - Ubuntu x Group Project 6 x

Kali Linux x Michael Scott Paper Compan x +

192.168.211.140

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

MICHAEL SCOTT PAPER COMPANY INC.

Serving Scranton's Paper Needs Since 2009

Welcome to the Michael Scott Paper Company!

Upload your files to be printed on demand! For now enter name and upload the file and we will process it on our end. (Unique login/user creation feature coming soon!)

Upload file to be printed on demand: No file selected.

Contacts

- Michael Scott - mscott@mspc.com (CEO)
- Pam Beasley - pbeasley@mspc.com (Sales)
- Ryan Howard - rhoward@mspc.com (Sales/IT)

General Contact: enpm685@gmail.com

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Home x ENPM685 x ENPM685 - Ubuntu x Group Project 6 x

Kali Linux x 192.168.211.140/upload2.php x Group Project #1 - CMMC x Sample Assessment - Go x Sample Assessment - Sampl x +

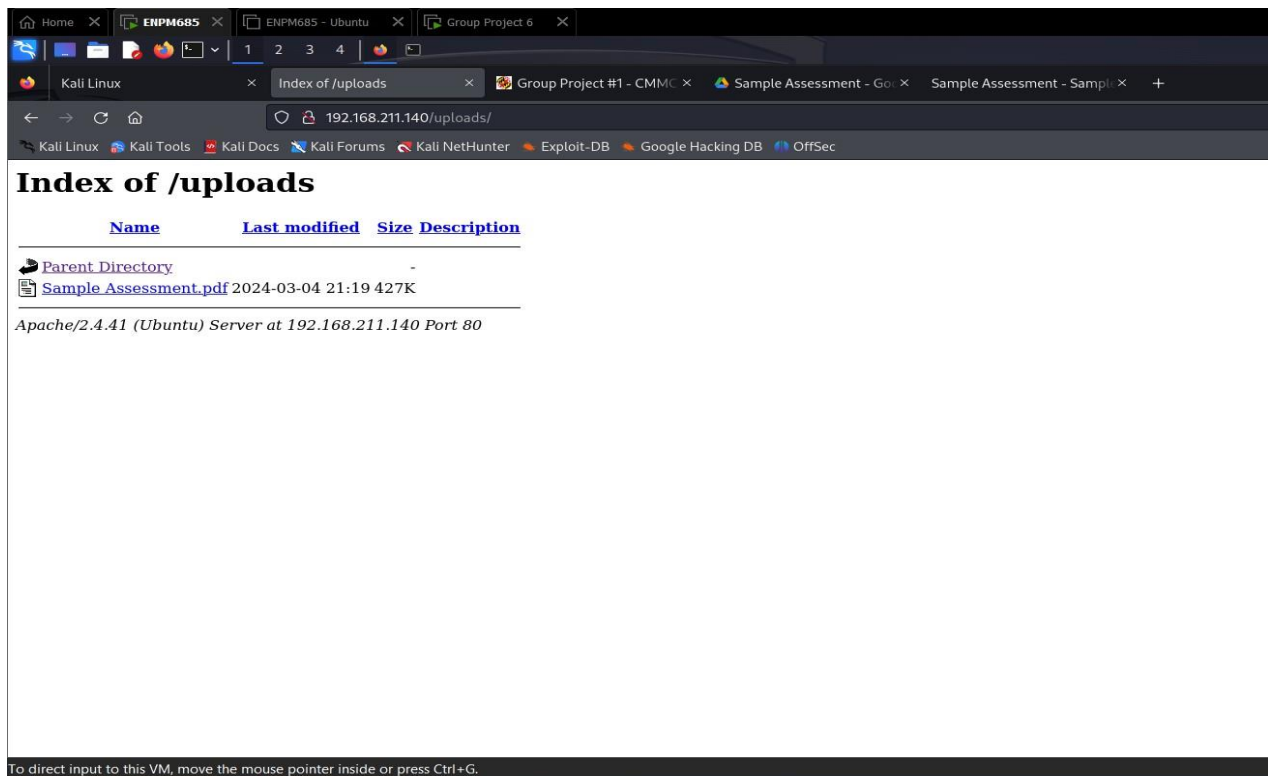
192.168.211.140/upload2.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The file has been uploaded.

[Back to the Michael Scott Paper Company](#)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



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

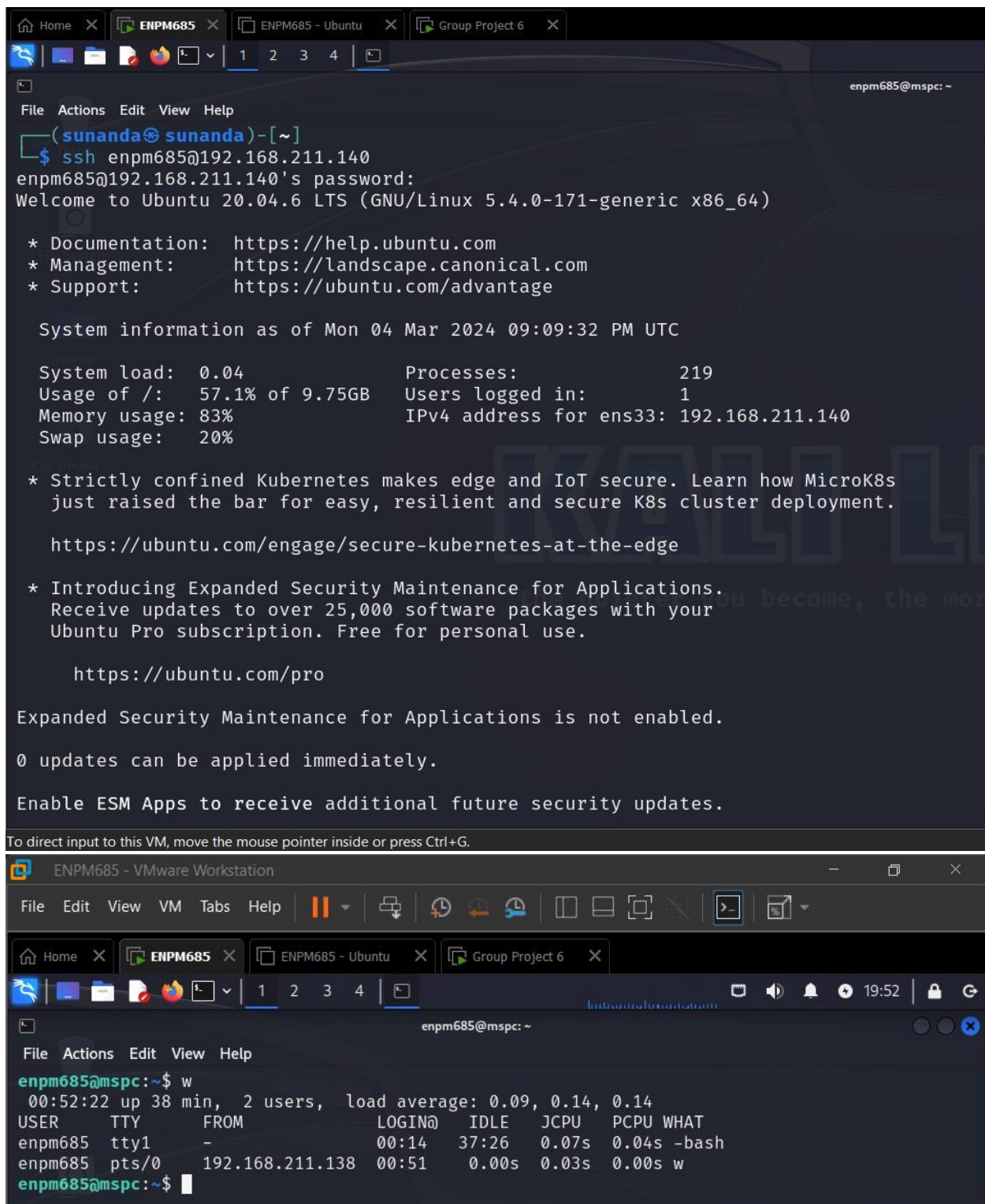
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

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.



```
(sunanda@sunanda)-[~]
$ ssh enpm685@192.168.211.140
enpm685@192.168.211.140's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-171-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Mon 04 Mar 2024 09:09:32 PM UTC

System load:  0.04          Processes:           219
Usage of /:   57.1% of 9.75GB Users logged in:          1
Memory usage: 83%          IPv4 address for ens33: 192.168.211.140
Swap usage:   20%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

  https://ubuntu.com/engage/secure-kubernetes-at-the-edge

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

ENPM685 - VMware Workstation
File Edit View VM Tabs Help
enpm685@mspc: ~$ w
00:52:22 up 38 min, 2 users, load average: 0.09, 0.14, 0.14
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
enpm685   tty1     -             00:14    37:26  0.07s  0.04s -bash
enpm685   pts/0    192.168.211.138 00:51    0.00s  0.03s  0.00s w
enpm685@mspc: ~$
```



```
Group Project 1.6 - VMware Workstation
File Edit View VM Tabs Help
enpm685@mspc:~$ cat /var/log/auth.log
Mar 7 00:06:44 mspc login[882]: pam_unix(login:session): session opened for user enpm685 by LOGIN(uid=0)
Mar 7 00:06:44 mspc systemd-logind[852]: New session 1 of user enpm685.
Mar 7 00:06:44 mspc systemd: pam_unix(systemd-user:session): session opened for user enpm685 by (uid=0)
Mar 7 00:09:01 mspc CRON[1423]: pam_unix(cron:session): session opened for user root by (uid=0)
Mar 7 00:09:01 mspc CRON[1423]: pam_unix(cron:session): session closed for user root
Mar 7 00:13:02 mspc sshd[910]: Server listening on 0.0.0.0 port 22.
Mar 7 00:13:02 mspc sshd[910]: Server listening on :: port 22.
Mar 7 00:13:02 mspc systemd-logind[849]: New seat seat0.
Mar 7 00:13:02 mspc systemd-logind[849]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 7 00:13:02 mspc systemd-logind[849]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Mar 7 00:14:14 mspc sshd[905]: Server listening on 0.0.0.0 port 22.
Mar 7 00:14:14 mspc sshd[905]: Server listening on :: port 22.
Mar 7 00:14:14 mspc systemd-logind[851]: New seat seat0.
Mar 7 00:14:14 mspc systemd-logind[851]: Watching system buttons on /dev/input/event0 (Power Button)
Mar 7 00:14:14 mspc systemd-logind[851]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard)
Mar 7 00:14:40 mspc login[865]: pam_unix(login:session): session opened for user enpm685 by LOGIN(uid=0)
Mar 7 00:14:40 mspc systemd-logind[851]: New session 1 of user enpm685.
Mar 7 00:14:40 mspc systemd: pam_unix(systemd-user:session): session opened for user enpm685 by (uid=0)
enpm685@mspc:~$
```

Home

ENPM685

ENPM685 - Ubuntu

Group Project 6

Kali Linux

Michael Scott Paper Company

192.168.211.140

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

MICHAEL SCOTT PAPER COMPANY INC.

Serving Scranton's Paper Needs Since 2009

Welcome to the Michael Scott Paper Company!

Upload your files to be printed on demand! For now enter name and upload the file and we will process it on our end. (Unique login/user creation feature coming soon!)

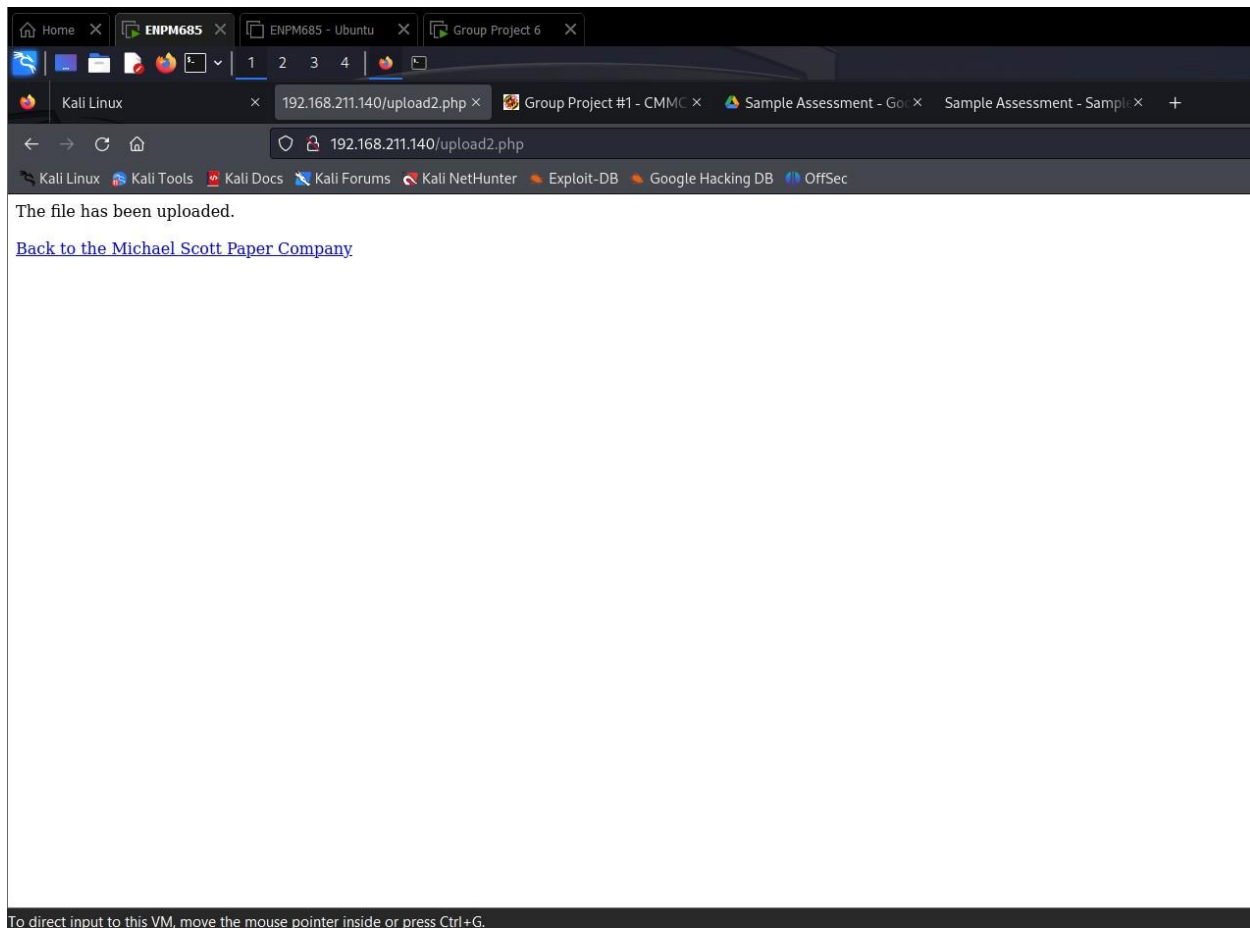
Upload file to be printed on demand: No file selected.

Contacts

- Michael Scott - mscott@mspc.com (CEO)
- Pam Beasley - pbeasley@mspc.com (Sales)
- Ryan Howard - rhoward@mspc.com (Sales/IT)

General Contact: enpm685@gmail.com

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



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.

3. 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.

4. 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.

5. 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.

6. 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.

```
enpm685@mspc:~$ clamscan --version
ClamAV 0.103.11/27196/Sun Feb 25 09:29:27 2024
enpm685@mspc:~$
```

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.

```

enpm685@mspc:/var/log/clamav$ cat /etc/clamav/freshclam.conf
# Automatically created by the clamav-freshclam postinst
# Comments will get lost when you reconfigure the clamav-freshclam package

DatabaseOwner clamav
UpdateLogFile /var/log/clamav/freshclam.log
LogVerbose false
LogSyslog false
LogFacility LOG_LOCAL6
LogFileMaxSize 0
LogRotate true
LogTime true
Foreground false
Debug false
MaxAttempts 5
DatabaseDirectory /var/lib/clamav
DNSDatabaseInfo current.cvd.clamav.net
ConnectTimeout 30
ReceiveTimeout 0
TestDatabases yes
ScriptedUpdates yes
CompressLocalDatabase no
Bytecode true
NotifyClamd /etc/clamav/clamd.conf
# Check for new database 24 times a day
Checks 24
DatabaseMirror db.local.clamav.net
DatabaseMirror database.clamav.net
enpm685@mspc:/var/log/clamav$ _

```

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.

```
enpm685@mspc:~$ ps axf | grep clam
  836 ?        Ss          0:00 /usr/bin/freshclam -d --foreground=true
  893 ?        Ssl         0:22 /usr/sbin/clamd --foreground=true
 1456 tty1     S+          0:00      \_ grep --color=auto clam
enpm685@mspc:~$
```

```
enpm685@mspc:/var/log/clamav$ cat /etc/clamav/clamd.conf | grep OnAccess
OnAccessMaxFileSize 5M
enpm685@mspc:/var/log/clamav$ _
```

```
enpm685@mspc:~$ clamscan .
/home/enpm685/.profile: OK
/home/enpm685/.bash_logout: OK
/home/enpm685/.bash_history: OK
/home/enpm685/.viminfo: OK
/home/enpm685/.bashrc: OK
/home/enpm685/.sudo_as_admin_successful: Empty file
/home/enpm685/install.sh: OK
/home/enpm685/text.txt: Eicar-Signature FOUND

----- SCAN SUMMARY -----
Known viruses: 8685899
Engine version: 0.103.11
Scanned directories: 1
Scanned files: 7
Infected files: 1
Data scanned: 0.01 MB
Data read: 0.00 MB (ratio 2.00:1)
Time: 18.396 sec (0 m 18 s)
Start Date: 2024:03:08 02:03:28
End Date: 2024:03:08 02:03:46
enpm685@mspc:~$
```

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:
 - Set the `ScanOnAccess` option to `yes`
 - Specify the path(s) to recursively watch by setting the `OnAccessIncludePath` option
 - Set `OnAccessPrevention` to `yes`.

The `clamonnacc` 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.