

ENPM685 Group Project 1

Group 5

~ Akshay Gangadhar Kanamarlapudi (120388309)
Santhosh Annadurai (120394355)
Shikha Mehta (120222382)
Srikanth Paida (120333507)

Access Control

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:

To facilitate identification, each user is assigned a unique login, and services are executed under individual accounts. The Cybersecurity Authentication Policy establishes recommendations for user verification, including the use of multi-factor authentication and strong password practices, which help restrict system access to only those who are allowed.

User ID (UID): A unique numerical identifier issued to each user. The system uses this ID to internally identify users. The root user normally has a UID of zero. UIDs less than 1000 (or another criterion, depending on the distribution) are often reserved for system accounts.

```
root:x:0:0: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
1xd:x:998:100::/var/snap/1xd/common/1xd:/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
(END)
```

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:

root and admin group have all the privileges. If any authorized users (**mscott**, **pbeasley** and **rhoward**) are added to the admin group, then they can have all the privileges.

```
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
1xd:x:998:100::/var/snap/1xd/common/1xd:/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
(END)
```

```

enpm685@mspc:~$ sudo cat /etc/sudoers
[sudo] password for enpm685:
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include /etc/sudoers.d

```

```

enpm685@mspc:~$ id mscott
uid=5002(mscott) gid=5002(mscott) groups=5002(mscott),4(adm),27(sudo)
enpm685@mspc:~$ id rhoward
uid=5004(rhoward) gid=5004(rhoward) groups=5004(rhoward)
enpm685@mspc:~$ id pbeasley
uid=5003(pbeasley) gid=5003(pbeasley) groups=5003(pbeasley)
enpm685@mspc:~$ id enpm685
uid=1000(enpm685) gid=1000(enpm685) groups=1000(enpm685),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),117(lxd)

```

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:

There are two open ports (HTTP and SSH). HTTP is a default open port, while in SSH we have to check for the configuration. After reviewing the SSH configuration, we find that the SSH is secured with password authentication and rules. So SSH is securely handled. Input connections and the firewall's status must be considered while assessing external connections. Unfortunately, the firewall is still turned off and all default incoming connections are allowed by the IP tables, leaving open the possibility of attacks.

```
enpm685@mspc:~$ nmap -P 192.168.9.133
Warning: You are not root -- using TCP pingscan rather than ICMP
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-07 00:44 UTC
Nmap scan report for mspc (192.168.9.133)
Host is up (0.000036s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

```
enpm685@mspc:~$ cat /etc/ssh/sshd_config
#      $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO
```

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

```
enpm685@mspc:~$ sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source                   destination
          prot opt source                   destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                   destination
          prot opt source                   destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                   destination
enpm685@mspc:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
enpm685@mspc:~$ |
```

Suggestion:

Set up rules about input connections and turn on the firewall to protect against possible instructions from outside connections.

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:

Restricting access to authorized users only and establishing certain methods for accessing web server content are crucial for maintaining compliance. But in this case, there aren't any official rules about what kinds of files are allowed to be uploaded to the web application. In a test run with the Weevely tool, we uploaded a "a.php" file and were able to acquire access by taking advantage of the lack of file type limitations.

**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:

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

```
(kali㉿kali)-[~]
$ weevely http://192.168.9.133/uploads/exploit.php password
The file has been uploaded.
[+] weevely 4.0.1
Back to the Michael Scott Paper Company
[+] Target:      www-data@mspc:/var/www/html/uploads
[+] Session:     /home/kali/.weevely/sessions/192.168.9.133/exploit_0.session
[+] Shell:       System shell

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
exploit.php
www-data@mspc:/var/www/html/uploads $ echo "See !! I got in" > Test.txt
www-data@mspc:/var/www/html/uploads $ ls
Test.txt
exploit.php
www-data@mspc:/var/www/html/uploads $ █
```

```
enpm685@mspc:~$ cd /var/www/html/uploads/
enpm685@mspc:/var/www/html/uploads$ ls
exploit.php Test.txt
enpm685@mspc:/var/www/html/uploads$ cat Test.txt
See!! I got in
```

Suggestion:

Implement strict input validation on the website so that users can only upload approved file types. This means confirming the content type as well as the file extension. To further block public access, secure the upload directory (e.g., 192.168.9.133/uploads). Set filesystem permissions so that only authorized users can access them.

Identification and Authentication

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:

All users have unique usernames through which they can be identified. The processes can be identified as service accounts that run separately. The following screenshot shows the details of the user accounts in the `/etc/passwd` file in the system.

```
enpm685@mspc:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/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:/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
ircx: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:system 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
uidd:x:107:112:/:/run/uidd:/usr/sbin/nologin
tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
polinate:x:110:11:/:/var/cache/polinate:/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:system 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
```

In the above screenshot, we can see that there are a total of 3 users (excluding `enpm685`) and those are the same users as mentioned in the web application. Please refer the screenshot below from the Michael Scott Paper Company website:

Contacts

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

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 authentication policy for the Michael Scott Paper Company includes requirements for strong and unique passwords. However, on an attempt to verify the password hashes in the system, the password for the user **mscott** (Michael Scott) did not follow the policy and the details can be seen in the screenshot below.

```
enpm685@mspc:~$ sudo john /etc/shadow --show
enpm685:password:19764:0:99999:7:::
mscott:monkey:19008:0:99999:7:::
```

The password needs to be updated as mentioned in the authentication policy of Michael Scott Paper Company as the statements are according to CMMC requirements.

Media Protection

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:

1. Media files present in system

```
enpm685@mspc:~$ sudo apt install lsscsi
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
lsscsi
0 upgraded, 1 newly installed, 0 to remove and 66 not upgraded.
Need to get 43.6 KB of archives.
After this operation, 114 kB of additional disk space will be used.
Get:1 http://ports.ubuntu.com/ubuntu-ports focal/main arm64 lsscsi arm64 0.30-0.1 [43.6 KB]
Fetched 43.6 KB in 0s (113 kB/s)
Selecting previously unselected package lsscsi.
(Reading database ... 77430 files and directories currently installed.)
Preparing to unpack .../lsscsi_0.30-0.1_arm64.deb ...
Unpacking lsscsi (0.30-0.1) ...
Setting up lsscsi (0.30-0.1) ...
Processing triggers for man-db (2.9.1-1) ...
enpm685@mspc:~$ lsscsi
[0:0:0:0]    disk    ATA      ENPM685 Group Pr 7XX0  /dev/sda
[1:0:0:0]    cd/dvd   Virtual DVD-ROM R103  /dev/sr0
```

Block Devices:

```
enpm685@mspc:~$ lsblk
NAME           MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0            7:0    0 57.9M  1 loop /snap/core20/1614
loop1            7:1    0  61M  1 loop /snap/1xd/22761
loop3            7:3    0 35.2M  1 loop /snap/snapd/20674
loop4            7:4    0 59.7M  1 loop /snap/core20/2186
loop5            7:5    0 91.9M  1 loop /snap/1xd/24065
sda              8:0    0   64G  0 disk 
└─sda1           8:1    0   1.1G 0 part /boot/efi
└─sda2           8:2    0    2G  0 part /boot
└─sda3           8:3    0   61G  0 part
  └─ubuntu--vg-ubuntu--lv 253:0  0 30.5G 0 lvm  /
sr0             11:0   1 1024M 0 rom
```

Hard Drives:

```
bus 001 device 001: id 1060:0002 Linux Foundation 2.0 root hub
enpm685@mspc:~$ df -h
Filesystem           Size  Used Avail Use% Mounted on
udev                  426M    0   426M  0% /dev
tmpfs                 98M   1.5M  96M  2% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  30G  5.7G  23G  20% /
tmpfs                486M    0   486M  0% /dev/shm
tmpfs                 5.0M    0   5.0M  0% /run/lock
tmpfs                486M    0   486M  0% /sys/fs/cgroup
/dev/loop0              58M   58M    0 100% /snap/core20/1614
/dev/loop1              62M   62M    0 100% /snap/lxd/22761
/dev/sda2              2.0G  107M  1.7G  6% /boot
/dev/sda1              1.1G  6.4M  1.1G  1% /boot/efi
/dev/loop3              36M   36M    0 100% /snap/snapd/20674
/dev/loop4              60M   60M    0 100% /snap/core20/2186
/dev/loop5              92M   92M    0 100% /snap/lxd/24065
tmpfs                 98M    0   98M  0% /run/user/1000
```

USB Devices:

```
enpm685@mspc:~$ lsusb
Bus 003 Device 011: ID 203a:ffffb Parallels Virtual Keyboard
Bus 003 Device 010: ID 203a:fffc Parallels Virtual Mouse
Bus 003 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

2. Media classified according to the sensitivity of the information it contains.

```
enpm685@mspc:/dev/disk$ ls
by-dname  by-id  by-partuuid  by-path  by-uuid
enpm685@mspc:/dev/disk$ cd by-dname
enpm685@mspc:/dev/disk/by-dname$ ls
ubuntu--vg-ubuntu--lv
enpm685@mspc:/dev/disk/by-dname$ cat ubuntu--vg-ubuntu--lv
cat: ubuntu--vg-ubuntu--lv: Permission denied
enpm685@mspc:/dev/disk/by-dname$ cd -
/dev/disk
enpm685@mspc:/dev/disk$ cd by-id
enpm685@mspc:/dev/disk/by-id$ ls
ata-ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF
ata-ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF-part1
ata-ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF-part2
ata-ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF-part3
ata-Virtual_DVD-ROM_1__-_31415B265
dm-name-ubuntu--vg-ubuntu--lv
dm-uuid-LVM-ISkKnxN1Qleunfu18Z0ipL2d6hVoJFQFCor36CcMLH2i2sv0qv6n0A52uV2Uvcx
1vm-pv-uuid-0uPEcf-xtBR-dz98-vVLB-nu4u-6eVe-Hn40Uh
scsi-0ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF
scsi-0ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part1
scsi-0ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part2
scsi-0ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part3
scsi-0ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part4
scsi-1ATA_ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF
scsi-1ATA_ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF-part1
scsi-1ATA_ENPM685_Group_Project_1-0_SSD_MX5HQK0FR314Q3Q3VHBF-part2
scsi-1ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part3
scsi-1ATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part4
scsi-SATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF
scsi-SATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part1
scsi-SATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part2
scsi-SATA_ENPM685_Group_Pr_MX5HQK0FR314Q3Q3VHBF-part3
enpm685@mspc:/dev/disk/by-id$ cd -
/dev/disk
enpm685@mspc:/dev/disk$ cd by-partuuid
enpm685@mspc:/dev/disk/by-partuuid$ ls
46dec98-c514-4c85-bb61-d1353062e9b  affb737a-98e9-44b2-a538-da2cdec7e7aa  c5d33c58-6356-4aad-9001-8219c3295989
enpm685@mspc:/dev/disk/by-partuuid$ cd -
/dev/disk
enpm685@mspc:/dev/disk$ cd by-path
enpm685@mspc:/dev/disk/by-path$ ls
platform-PRL4010:00-ata-1  platform-PRL4010:00-ata-1-part2  platform-PRL4010:00-ata-2
platform-PRL4010:00-ata-1-part1  platform-PRL4010:00-ata-1-part3
enpm685@mspc:/dev/disk/by-path$ cd -
/dev/disk
enpm685@mspc:/dev/disk$ cd by-uuid
enpm685@mspc:/dev/disk/by-uuid$ ls
08812951-9057-4011-a446-b93338a46685  8906-59E2  c3c5a575-fdf5-477b-9b26-12b18cd4df3d
enpm685@mspc:/dev/disk/by-uuid$
```

3. System media containing FCI is sanitized or destroyed before disposal using sg_sanitize version 1.11 20180628:

Is this requirement met? MET NOT MET NA

Evaluation/Evidence:

Even though sanitization tools are installed, we have no proof whether they are being implemented to dispose of system media since we couldn't find any media destruction certificate for the same.

```
enpm685@mspc:~$ which sg_sanitize
/usr/bin/sg_sanitize
enpm685@mspc:~$ sg_sanitize --version
sg_sanitize: version: 1.11 20180628
enpm685@mspc:~$ sg_sanitize --help
Usage: sg_sanitize [--ause] [--block] [--count=OC] [--crypto] [--dry-run]
                   [--early] [--fail] [--invert] [--ipl=LEN]
                   [--overwrite] [--pattern=PF] [--quick] [--test=TE]
                   [--timeout=SECS] [--verbose] [--version] [--wait]
                   [--zero] [--znr] DEVICE
where:
  --ause|-A      set AUSE bit in cdb
  --block|-B     do BLOCK ERASE sanitize
  --count=OC|-c OC  OC is overwrite count field (from 1 (def) to 31)
  --crypto|-C    do CRYPTOGRAPHIC ERASE sanitize
  --desc|-d      polling request sense sets 'desc' field
                 (def: clear 'desc' field)
  --dry-run|-D   to preparation but bypass SANITIZE command
  --early|-e     exit once sanitize started (IMMED set in cdb)
                 user can monitor progress with REQUEST SENSE
  --fail|-F     do EXIT FAILURE MODE sanitize
  --help|-h      print out usage message
  --invert|-I    set INVERT bit in OVERWRITE parameter list
  --ipl=LEN|-i LEN initialization pattern length (in bytes)
  --overwrite|-o  do OVERWRITE sanitize
  --pattern=PF|-p PF PF is file containing initialization pattern
                 for OVERWRITE
  --quick|-q     start sanitize without pause for user
                 intervention (i.e. no time to reconsider)
  --test=TE|-t TE TE is placed in TEST field of OVERWRITE
                 parameter list (def: 0)
  --timeout=SECS|-t SECS SANITIZE command timeout in seconds
  --verbose|-v    increase verbosity
  --version|-v   print version string then exit
  --wait|-w      wait for command to finish (could take hours)
  --zero|-z      use pattern of zeros for OVERWRITE
  --znr|-Z       set ZNR (zone no reset) bit in cdb

Performs a SCSI SANITIZE command.
<<<WARNING>>>: all data on DEVICE will be lost.
Default action is to give user time to reconsider; then execute SANITIZE
command with IMMED bit set; then use REQUEST SENSE command every 60
seconds to poll for a progress indication; then exit when there is no
more progress indication.
```

Recommendation: The company should have automated sanitization of media and should contain all the appropriate certificates for media destruction policy.

4. Sanitization techniques installed are Shred version 8.30 for Shredding and dd version 8.30 for Data Wiping

```
enpm685@mspc:~$ shred --version
shred (GNU coreutils) 8.30
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Written by Colin Plumb.

```
enpm685@mspc:~$ dd --version
dd (coreutils) 8.30
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Written by Paul Rubin, David MacKenzie, and Stuart Kemp.

5. Secure storage for media, Media not accessible by unauthorized personnel.

```
enpm685@mspc:~$ fdisk -l
fdisk: cannot open /dev/loop0: Permission denied
fdisk: cannot open /dev/loop1: Permission denied
fdisk: cannot open /dev/loop3: Permission denied
fdisk: cannot open /dev/loop4: Permission denied
fdisk: cannot open /dev/loop5: Permission denied
fdisk: cannot open /dev/sda: Permission denied
fdisk: cannot open /dev/mapper/ubuntu--vg-ubuntu--lv: Permission denied
```

6. Media Device Encryption

Managed data storage not encrypted. No encryption mechanism used for media devices.

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

```
enpm685@mspc:~$ lsblk -lpno name,fstype,MOUNTPOINT
/dev/loop0           squashfs   /snap/core20/1614
/dev/loop1           squashfs   /snap/1xd/22761
/dev/loop3           squashfs   /snap/snapd/20674
/dev/loop4           squashfs   /snap/core20/2186
/dev/loop5           squashfs   /snap/1xd/24065
/dev/sda
/dev/sda1           vfat        /boot/efi
/dev/sda2           ext4        /boot
/dev/sda3           LVM2_member
/dev/sr0
/dev/mapper/ubuntu--vg-ubuntu--lv ext4          /
```

Recommendation: Managed data storage can be encrypted using LUKS (Linux Unified key Setup) which is a de facto standard for disk encryption under linux. For example: using crypto_LUKS fstype.

Physical Protection

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:

Access control is a part of the Data Center Policy. The following screenshot shows the access control segment of the policy.

Access Control

Authorized Personnel: Only authorized personnel with a legitimate business need shall be granted access to the data center facility. Access privileges will be granted based on job role and responsibilities.

Access Approval Process: Access to the data center facility must be requested through the appropriate channels, such as the IT department or facility management. All access requests must be approved by the designated authority before access is granted.

Access Levels: Access privileges will be granted based on the principle of least privilege. Personnel will only be provided with the level of access necessary to perform their job duties effectively.

Visitor Access: Visitors to the data center facility must be pre-authorized and accompanied by an authorized employee or contractor at all times. Visitors must sign in and out, providing appropriate identification, and adhere to all data center access policies.

However, there is no proof of physical access being limited to only authorized personnel since we are not able to physically access the Michael Scott Paper Company data center.

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:

Although the data center policy mentions visitor access being monitored, there is no actual proof of physical access mechanisms or controls being implemented at the facility. Visiting the facility was not a possibility for our team to verify this requirement.

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:

Even though the data center policy mentions logs being maintained for physical access to the data center, there is no information regarding any physical access logs in the VM nor can we physically verify that by visiting the data center.

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:

Managing physical access is a part of the datacenter policy. However, there is no concrete evidence as to how the physical access devices are managed or any kind of documentation regarding that.

System and Communications Protection

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 IP tables are set in the default configuration and not modified to protect the server network. All kinds of incoming and outgoing traffic is allowed to pass through the network and this is not considered as a safe configuration for an organization. The below screenshot shows that there are no traffic filters added and relies on the default configurations.

```
enpm685@mspc:~$ sudo iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
enpm685@mspc:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
enpm685@mspc:~$ |
```

The network traffic must be filtered to protect from malicious traffic flow by explicitly allowing only the traffic that needs to be in the network and setting the default filters to deny all traffic.

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:

There is no mention of separation of internal and external networks or any other network infrastructure for the web application in any of their policy documents. Hence, this requirement remains inconclusive and not applicable for this organization.

System and Information Integrity

SI.L1-3.14.1 - Flaw Remediation

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

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

Evaluation/Evidence:

- Patches for ubuntu-keyring: ARM64 are recorded in `/var/log/apt/history.log`

```
Start-Date: 2022-08-31 07:00:00
Commandline: apt-get --yes -oDebug::pkgDepCache::AutoInstall=yes install ubuntu-keyring
Upgrade: ubuntu-keyring:arm64 (2020.02.11.2, 2020.02.11.4)
End-Date: 2022-08-31 07:00:00

Start-Date: 2022-08-31 07:00:10
Commandline: apt-get --yes -oDebug::pkgDepCache::AutoInstall=yes --force-yes upgrade
Upgrade: libpam0g:arm64 (1.3.1-5ubuntu4, 1.3.1-Subuntu4.3), fdisk:arm64 (2.34-0.1ubuntu9, 2.34-0.1ubuntu9.3), perl-base:arm64 (5.30-0~ubu001, 5.30-0~ubu001.3), libplan9:arm64 (0.39-0ubuntu1, 0.104-0ubuntu20.04.2), libseccomp2:arm64 (2.4.3-1ubu001, 2.5.1-1ubu001~20.04.2), libcom-err2:arm64 (1.45.5-2ubu001, 1.45.5-2ubu001.1), libdbus-1-3:arm64 (1.12.16-2ubu002, 1.12.16-2ubu002.2), networkd-dispatcher:arm64 (2.0.1-1, 2.1-2ubu0020.04.3), libfdisk1:arm64 (2.34-0.1ubuntu9, 2.34-0.1ubuntu9.3), vim-c
common:arm64 (2.8.1.2269-1ubu005, 2.8.1.2269-1ubu005.7), libpam-modules:arm64 (1.3.1-Subuntu4, 1.3.1-Subuntu4.3), openssh:arm64 (1.1.1f-1ubu002, 1.1.1f-1ubu002.16), libgirepository-1.0:arm64 (1.64-0.2, 1.64.1-2ubu0020.04.1), libpython3.8-minimal:arm64 (3.8.2-1ubu001, 3.8.10-0ubu001~20.04.5), libsystemd:arm64 (245.4-4ubu003, 245.4-4ubu003.17), gcc-10-base:arm64 (10-20200
411-ubu001, 10.3.0-1ubu001~20.04), apt:arm64 (2.0.2, 2.0.9), dbus:arm64 (1.12.16-2ubu002, 1.12.16-2ubu002.2), libkmod2:arm6
4 (27-1ubu002, 27-1ubu002.1), libmount1:arm64 (2.34-0.1ubu003, 2.34-0.1ubu003.9), libsqlite3-0:arm64 (3.31.1-4, 3.31.1-4ubu
tu003), libicu6:arm64 (66.1-2ubu002, 66.1-2ubu002.1), e2fsprogs:arm64 (1.45.5-2ubu001.1), zlib1g:arm64 (1:1
.2.11.dfsg-2ubu001, 1:1.2.11.dfsg-2ubu001.3), sudo:arm64 (1.8.31-ubu001, 1.8.31-ubu001.8), libssl:arm64 (2.31-0ubu009, 2.3
1-0ubu009.9), util-linux:arm64 (2.34-0.1ubu009, 2.34-0.1ubu009.3), python3.8:arm64 (3.8.2-1ubu001, 3.8.10-0ubu001~20.04.5),
libsep01:arm64 (3.0-1, 3.0-1ubu000.1), udev:arm64 (245.4-4ubu003, 245.4-4ubu003.17), locales:arm64 (2.31-0ubu009, 2.31-0ub
u009.9), passwd:arm64 (114.8.1-ubu005, 1:4.8.1-1ubu005.20.04.2), procps:arm64 (2:3.3.16-1ubu002, 2:3.3.16-1ubu002.3) , libp
am-runtime:arm64 (1.3.1-Subuntu4, 1.3.1-Subuntu4.3), isc-dhcp-common:arm64 (4.4.1-2.1ubu005, 4.4.1-2.1ubu005.20.04.3), libisp
-export1105:arm64 (1:9.11.16+dfsg-3ubu001, 1:9.11.16+dfsg-3ubu001.1), libprocps8:arm64 (2:3.3.16-1ubu002, 2:3.3.16-1ubu002.3),
libapt-pkg6.0:arm64 (2.0.2, 2.0.9), libexpat1:arm64 (2.2.9-1ubu001, 2.2.9-1ubu001.0), kmod:arm64 (27-1ubu002, 27-1ubu002.1),
libudev1:arm64 (245.4-4ubu003, 245.4-4ubu003.17), rsyslog:arm64 (8.2001-0ubu001, 8.2001-0ubu001.3), libapparmor1:arm64
(2.19.3-7ubu005, 2.19.3-7ubu005.1), systemd-timesyncd:arm64 (245.4-4ubu003, 245.4-4ubu003.17), libss2:arm64 (1.45.5-2ubu001
, 1.45.5-2ubu001.1), mount:arm64 (2.34-0.1ubu009, 2.34-0.1ubu009.3), libext2fs2:arm64 (1.45.5-2ubu001, 1.45.5-2ubu001.1), u
buntu-minimal:arm64 (1.450, 1.450.2), libblkid1:arm64 (2.34-0.1ubu009, 2.34-0.1ubu009.3), dpkg:arm64 (1.19.7ubu003, 1.19.7ubu
ntu003.2), libc-bin:arm64 (2.31-0ubu009, 2.31-0ubu009.9), gir1.2-glib2.0:arm64 (1.64.0-2, 1.64.1-1ubu0020.04.1), libpcres3:arm
64 (2:8.39-12ubu002, 2:8.39-12ubu002.1), python3.8-minimal:arm64 (3.8.2-1ubu001, 3.8.10-0ubu001~20.04.5), tar:arm64 (1.30+dfs
g-7, 1.30+dfsg-7ubu0020.04.2), systemd-sysv:arm64 (245.4-4ubu003, 245.4-4ubu003.17), libuuuid1:arm64 (2.34-0.1ubu009, 2.34
-0.1ubu009.3), libgcrypt20:arm64 (1.8.5-5ubu001, 1.8.5-5ubu001.1), liblzo2-1:arm64 (1.9.2-2, 1.9.2-2ubu0020.04.1), gpgv:arm6
4 (2.2.19-3ubu002, 2.2.19-3ubu002.2), libpam-systemd:arm64 (245.4-4ubu003, 245.4-4ubu003.17), distro-info-data:arm64 (0.43ub
u001, 0.43ubu001.10), xz-utils:arm64 (5.2.4-1, 5.2.4-1ubu001.1), python3-yaml:arm64 (5.3.1-1, 5.3.1-1ubu000.1), systemd:arm6
4 (245.4-4ubu003, 245.4-4ubu003.17), libsmartcols1:arm64 (2.34-0.1ubu009, 2.34-0.1ubu009.3), login:arm64 (1:4.8.1-1ubu005,
1:4.8.1-1ubu005.20.04.2), xxd:arm64 (2:8.1.2269-1ubu005, 2:8.1.2269-1ubu005.7), libhogweed5:arm64 (3.5.1+really3.5.1-2, 3.5.1
+really3.5.1-2ubu002), libpam-modules-bin:arm64 (1.3.1-Subuntu4, 1.3.1-Subuntu4.3), apt-utils:arm64 (2.0.2, 2.0.9), libdns-ex
port1109:arm64 (1:9.11.16+dfsg-3ubu001, 1:9.11.16+dfsg-3ubu001.1), libnss-systemd:arm64 (245.4-4ubu003, 245.4-4ubu003.17), bs
dutils:arm64 (1:2.34-0.1ubu009, 1:2.34-0.1ubu009.3), libnetplan0:arm64 (0.99-0ubu001, 0.104-0ubu002~20.04.2), libgcc-s1:arm6
4 (2:10.20200411-0ubu001, 10.3.0-1ubu001~20.04), liblbb1.2:0-data:arm64 (2.64.2-1*fakesync1, 2.64.6-1ubu0020.04.4), libnettle87:
arm64 (3.5.1+really3.5.1-2, 3.5.1+really3.5.1-2ubu002), bash:arm64 (5.0-ubu001, 5.0-ubu001.2), libxml2:arm64 (2.9.10+dfsg
-5, 2.9.10+dfsg-5ubu0020.04.4), libpython3.8-stdlib:arm64 (3.8.2-1ubu001, 3.8.10-0ubu001~20.04.5), libgnutls30:arm64 (3.6.1
-3ubu001, 3.6.13-2ubu001.7), ca-certificates:arm64 (20190110ubu001, 20211016~20.04.1), vim-tiny:arm64 (2:8.1.2269-1ubu005,
2:8.1.2269-1ubu005.7), libp11-kit0:arm64 (0.23.20-1ubu001, 0.23.20-1ubu001.1), libzstd1:arm64 (1.4.4+dfsg-3, 1.4.4+dfsg-3ubu
001), libcryptsetup12:arm64 (2:2.2.2-3ubu002, 2:2.2.2-3ubu002.4), logsave:arm64 (1.45.5-2ubu001, 1.45.5-2ubu001.1), libssl1
.1:arm64 (1.1.1f-1ubu002, 1.1.1f-1ubu002.16), gzip:arm64 (1.10-0ubu004, 1.10-0ubu004.1), libjson-c4:arm64 (0.13.1+dfsg-7, 0
./var/log/apt/history.log
```

- Anti-virus signatures like bytecode.cld, daily.cld, freshclam.dat, main.cvd are installed in directory `/var/lib/clamav`

```
enpm685@mspc:~$ cat /var/lib/clamav
cat: /var/lib/clamav: Is a directory
enpm685@mspc:~$ cd /var/lib/clamav
enpm685@mspc:/var/lib/clamav$ ls
bytecode.cld  daily.cld  freshclam.dat  main.cvd
enpm685@mspc:/var/lib/clamav$
```

3. To keep the ClamAV Antivirus Server definition database up-to-date, freshclam is configured to check for new definitions. The default is set to 24 times per day.

```
enpm685@mspc:/etc/clamav$ cat 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
```

4. List of vendors in our system to ensure timely access to updates.

```
enpm685@mspc:~$ sudo lshw | grep -i "vendor"
      vendor: Parallels International GmbH.
      vendor: Parallels ARM Virtual Machine
      vendor: Parallels International GmbH.
      vendor: Apple
      vendor: Intel Corporation
      vendor: Intel Corporation
      vendor: Linux 5.4.0-171-generic ehci_hcd
      vendor: NEC Corporation
      vendor: Linux 5.4.0-171-generic xhci-hcd
      vendor: Linux 5.4.0-171-generic xhci-hcd
      vendor: Parallels
      vendor: Parallels
      vendor: Red Hat, Inc.
      vendor: Parallels, Inc.
      vendor: Red Hat, Inc.
      vendor: mkfs.fat
      vendor: Linux
```

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:

Michael Scott paper company website allows all file types to be uploaded regardless of their extensions. This way, attackers can exploit this vulnerability by uploading malicious PHP web shells to get backdoor access to the server.

The screenshot shows the homepage of the Michael Scott Paper Company. The main title 'MICHAEL SCOTT PAPER COMPANY INC.' is displayed in large, bold, black font within a red-bordered box. Below the title, a subtitle 'Serving Scranton's Paper Needs Since 2009' is visible. A prominent 'Welcome to the Michael Scott Paper Company!' message is centered on the page. Below this, there is a form field for file upload with the placeholder 'Upload file to be printed on demand:' followed by a 'Choose File' button and an 'enpm685.php' file name, and an 'Upload' button. To the right of the file input, there is a link 'General Contact: enpm685@gmail.com'. The bottom portion of the screenshot shows a browser status bar with navigation icons, a 'Not Secure' warning, and the URL '10.211.55.4/upload2.php'. The main content area below the status bar displays the message 'The file has been uploaded.'

Always validate and verify the file type that is being uploaded to prevent such vulnerabilities.

SI.L1-3.14.4 - Update Malicious Code Protection

When new releases are available

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

Evaluation/Evidence:

Freshclam downloads and updates ClamAV's official virus signature databases can be seen available in the virtual machine.

```
enpm695@mspc:~$ ls
alternatives.log  bootstrap.log  cloud-init-output.log  dpkg.log  kern.log  private
apache2          btmp           dist-upgrade        faillog   landscape  syslog
apt              clamav         dmesg             installer  lastlog   ubuntu-advantage.log
auth.log          cloud-init.log  dmesg.0           Journal    mysql     ubuntu-advantage-timer.log
enpm695@mspc:~$ tail syslog
Feb 28 20:09:12 mspc systemd[1]: Starting Clean php session files...
Feb 28 20:09:12 mspc systemd[1]: phsessionclean.service: Succeeded.
Feb 28 20:09:12 mspc systemd[1]: Finished Clean php session files.
Feb 28 20:12:01 mspc CRON[8012]: (root) CMD ( test -x /etc/cron.daily/popularity-contest && /etc/cron.daily/popularity-contest
--cron)
Feb 28 20:17:01 mspc CRON[8837]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)
Feb 28 20:28:13 mspc freshclam[695]: Wed Feb 28 20:28:13 2024 -> Received signal: wake up
Feb 28 20:28:13 mspc freshclam[695]: Wed Feb 28 20:28:13 2024 -> ClamAV update process started at Wed Feb 28 20:28:13 2024
Feb 28 20:28:13 mspc freshclam[695]: Wed Feb 28 20:28:13 2024 -> daily.cld database is up-to-date (version: 27199, sigs: 2054066
, f-level: 90, builder: raynman)
Feb 28 20:28:13 mspc freshclam[695]: Wed Feb 28 20:28:13 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-
level: 90, builder: signingr)
Feb 28 20:28:13 mspc freshclam[695]: Wed Feb 28 20:28:13 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-
level: 90, builder: raynman)
```

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:

Anti-malware software like ClamAV is used to scan for and identify viruses, but it can only be run manually i.e. the anti-virus scan is not performed automatically.

```
enpm685@mspc:~$ which freshclam
/usr/bin/freshclam
enpm685@mspc:~$ clamscan --version
ClamAV 0.103.11/27199/Wed Feb 28 09:31:56 2024
enpm685@mspc:~$ pwd
/home/enpm685
enpm685@mspc:~$ clamscan --infected --remove --recursive /home/enpm685

----- SCAN SUMMARY -----
Known viruses: 8685772
Engine version: 0.103.11
Scanned directories: 3
Scanned files: 4
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 39.404 sec (0 m 39 s)
Start Date: 2024:02:28 15:00:06
End Date: 2024:02:28 15:00:46
```

Set up automated tasks to run anti-virus scans on a frequent basis to prevent any kind of malware in the system.