CMMC 2.0 LEVEL 1 ASSESSMENT REPORT

By: Aditya Deshpande, UID: 120333590

1. ACCESS CONTROL (AC)

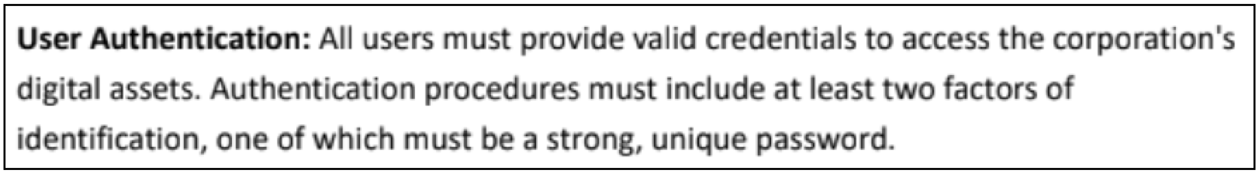
1.1 AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

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

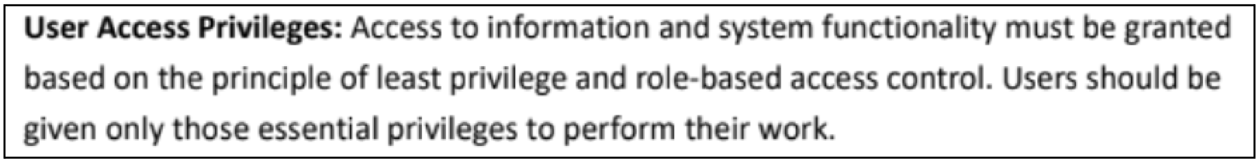
Is this requirement being met? **MET** NOT MET N/A

Evaluation/Evidence:

Within the given MSPC-Authentication-Policy, the following is defined:



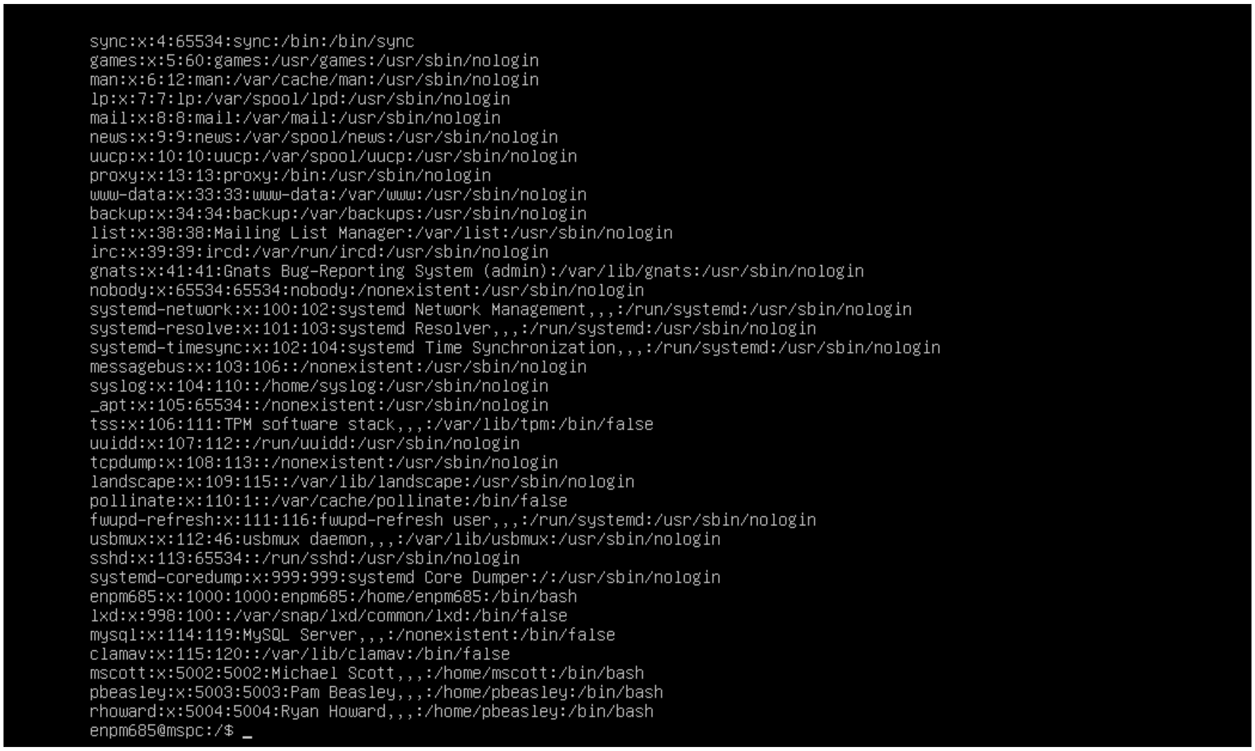
User Authentication: All users must provide valid credentials to access the corporation's digital assets. Authentication procedures must include at least two factors of identification, one of which must be a strong, unique password.



User Access Privileges: Access to information and system functionality must be granted based on the principle of least privilege and role-based access control. Users should be given only those essential privileges to perform their work.

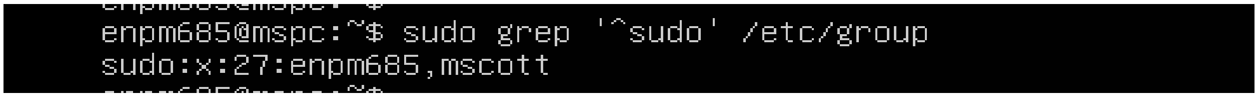
It can be concluded from the above policies that the Michael Scott Paper Company requires users to be authenticated and system access will be granted to users depending on their role. Since the least privilege principle is followed, every user will only have access to only what's required and unauthorized users will not be able to access, or change things in the system.

We can also check this in our virtual machine. Let’s run “ cat /etc/passwd ” to check users and processes present on the system.



```
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:/$ _
```

Now, we want to make sure that root access is limited to required users only.



```
enpm685@mspc:~$ sudo grep '^sudo' /etc/group
sudo:x:27:enpm685,mscott
```

As we can see there are only two users that have root access which are enpm685 and mscott, and the rest of the users like pbeasly don’t have higher access privileges.

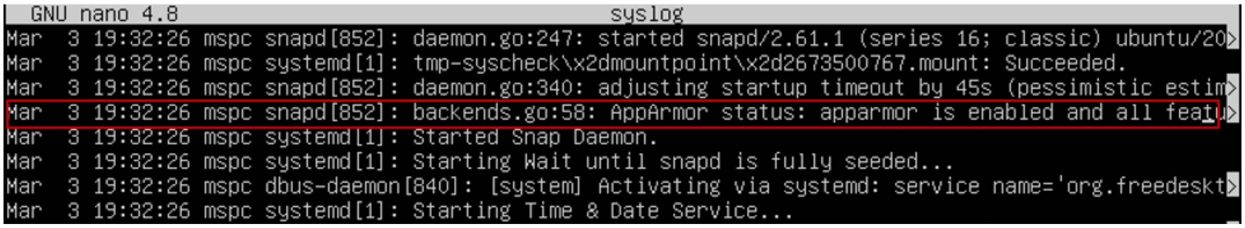
1.2 AC.L1-3.1.2 – TRANSACTION & FUNCTION CONTROL

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

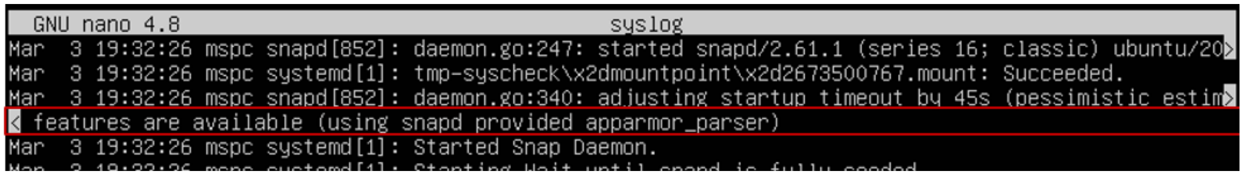
Is this requirement being met? **MET** NOT MET N/A

Evaluation/Evidence:

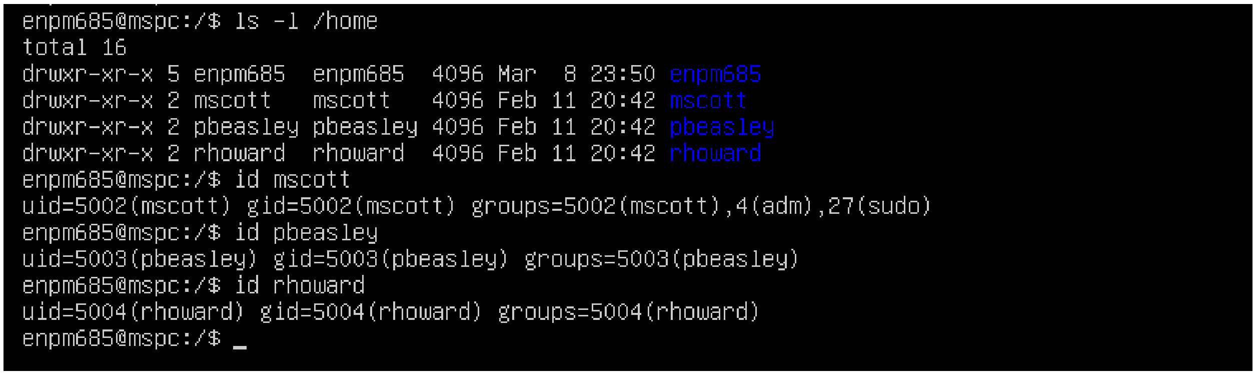
When we dive into the system logs, we can see that AppArmor is enabled. It is a security module which makes sure that programs can only perform actions they are allowed to, like accessing files or executing functions. It allows the administrator to create profiles and limit system access to permitted actions, satisfying the requirement of the policy.



```
 GNU nano 4.8                                          syslog
Mar  3 19:32:26 mspc snapd[852]: daemon.go:247: started snapd/2.61.1 (series 16; classic) ubuntu/20>
Mar  3 19:32:26 mspc systemd[1]: tmp-syscheck\x2dmountpoint\x2d2673500767.mount: Succeeded.
Mar  3 19:32:26 mspc snapd[852]: daemon.go:340: adjusting startup timeout by 45s (pessimistic estim>
Mar  3 19:32:26 mspc snapd[852]: backends.go:58: AppArmor status: apparmor is enabled and all featu>
Mar  3 19:32:26 mspc systemd[1]: Started Snap Daemon.
Mar  3 19:32:26 mspc systemd[1]: Starting Wait until snapd is fully seeded...
Mar  3 19:32:26 mspc dbus-daemon[840]: [system] Activating via systemd: service name='org.freedeskt>
Mar  3 19:32:26 mspc systemd[1]: Starting Time & Date Service...
```



```
 GNU nano 4.8                                          syslog
Mar  3 19:32:26 mspc snapd[852]: daemon.go:247: started snapd/2.61.1 (series 16; classic) ubuntu/20>
Mar  3 19:32:26 mspc systemd[1]: tmp-syscheck\x2dmountpoint\x2d2673500767.mount: Succeeded.
Mar  3 19:32:26 mspc snapd[852]: daemon.go:340: adjusting startup timeout by 45s (pessimistic estim>
< features are available (using snapd provided apparmor_parser)
Mar  3 19:32:26 mspc systemd[1]: Started Snap Daemon.
Mar  3 19:32:26 mspc systemd[1]: Starting Wait until snapd is fully seeded
```



```
enpm685@mspc:/$ ls -l /home
total 16
drwxr-xr-x 5 enpm685  enpm685  4096 Mar  8 23:50 enpm685
drwxr-xr-x 2 mscott   mscott   4096 Feb 11 20:42 mscott
drwxr-xr-x 2 pbeasley pbeasley 4096 Feb 11 20:42 pbeasley
drwxr-xr-x 2 rhoward  rhoward  4096 Feb 11 20:42 rhoward
enpm685@mspc:/$ id mscott
uid=5002(mscott) gid=5002(mscott) groups=5002(mscott),4(adm),27(sudo)
enpm685@mspc:/$ id pbeasley
uid=5003(pbeasley) gid=5003(pbeasley) groups=5003(pbeasley)
enpm685@mspc:/$ id rhoward
uid=5004(rhoward) gid=5004(rhoward) groups=5004(rhoward)
enpm685@mspc:/$ _
```

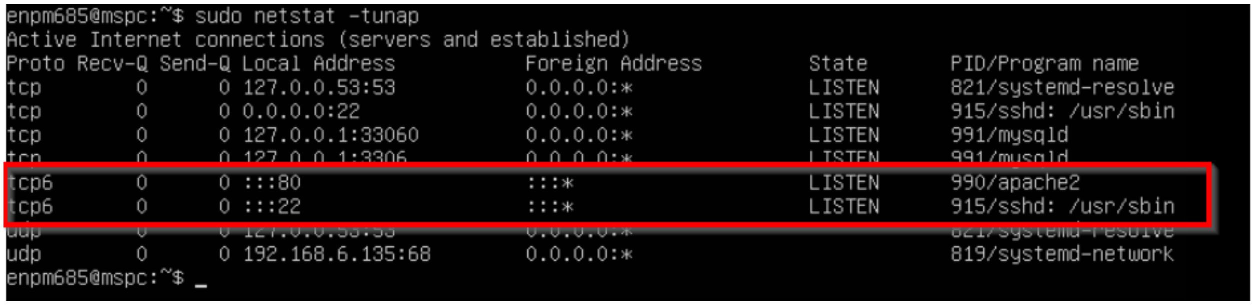
1.3 AC.L1-3.1.20 – EXTERNAL CONNECTIONS

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

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

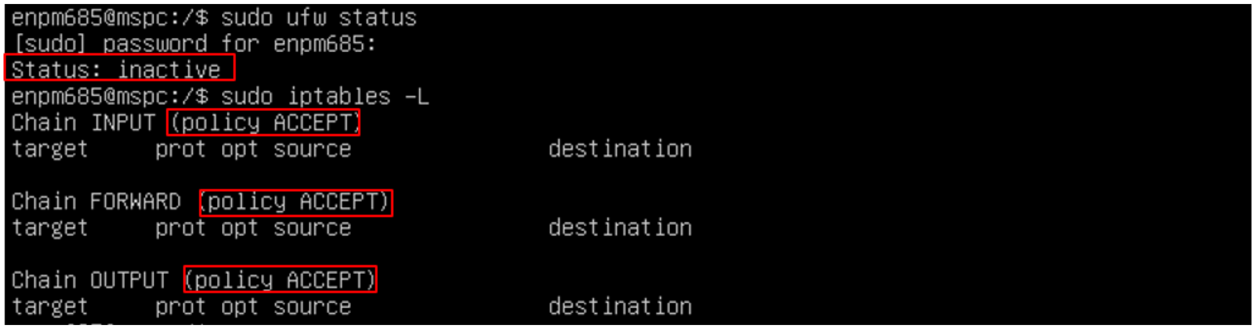
Evaluation/Evidence:

First, we will check the active network connections and ports listening on our system.



```
enpm685@mspc:~$ sudo netstat -tunap
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      821/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      915/sshd: /usr/sbin
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      991/mysqld
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      991/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN      990/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      915/sshd: /usr/sbin
udp        0      0 127.0.0.53:53           0.0.0.0:*                           821/systemd-resolve
udp        0      0 192.168.6.135:68        0.0.0.0:*                           819/systemd-network
enpm685@mspc:~$ _
```

From the above screenshot, it can be seen that "::" denotes there is no specified IPv6 address and the asterisk "*" means connections from any IP will be accepted. This is highly insecure as there are no restrictions when it comes to external network connectivity



```
enpm685@mspc:/$ sudo ufw status
[sudo] password for enpm685:
Status: inactive
enpm685@mspc:/$ sudo iptables -L
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
```

On checking the firewall status, we get to know that it is inactive. The firewall rules define that for all chains (Input, Output, and Forward), all packets are allowed to pass through the firewall without any restrictions. This can result in unauthorized access to sensitive data owned by the Michael Scott Paper Company.

Recommendations

- The Firewall should be active/functioning and strict rules should be implemented. Rules should be applied to restrict incoming and outgoing traffic.
- There should be monitoring and logging mechanisms to have more control over the network activities.
- These recommendations can help limit connections to information systems and improve the overall security posture of the Michael Scott Paper Company.

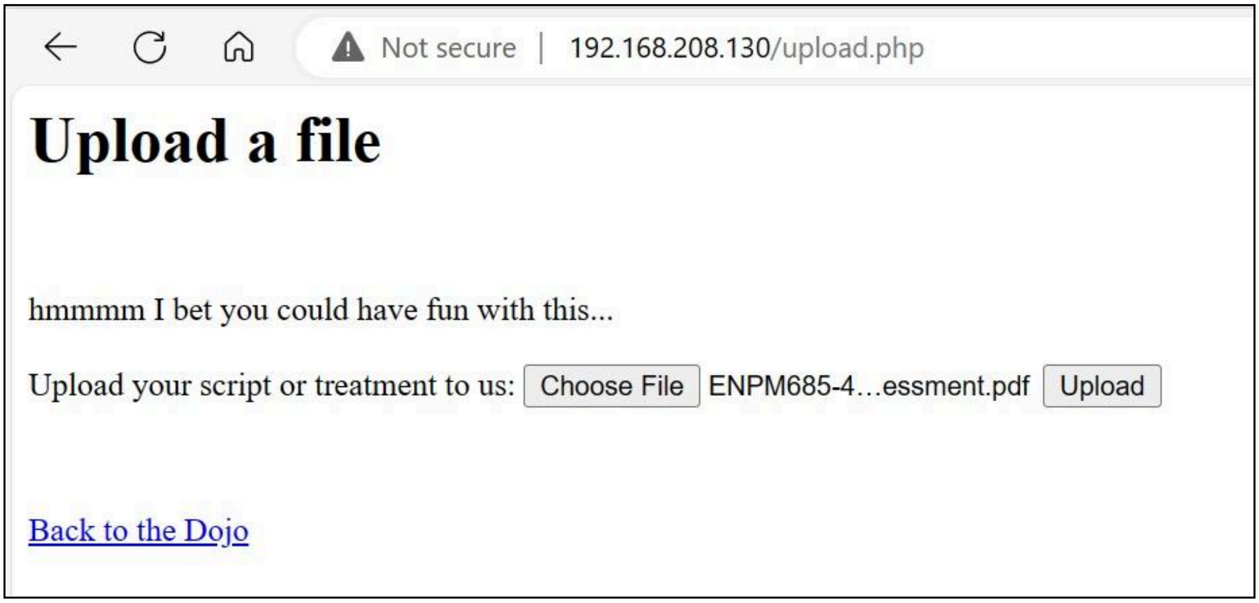
1.4 AC.L1-3.1.22 – CONTROL PUBLIC INFORMATION

Control information posted or processed on publicly accessible information systems.

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

Evaluation/Evidence:

The below screenshot depicts that any user can upload files on the Michael Scott Paper Company website. There are no credentials asked anywhere. This can be dangerous as hackers can also upload malicious files to inject malware, or gain unauthorized remote access since there is no restriction on file type upload. Thus, the requirement of controlling publicly accessible information is not met.



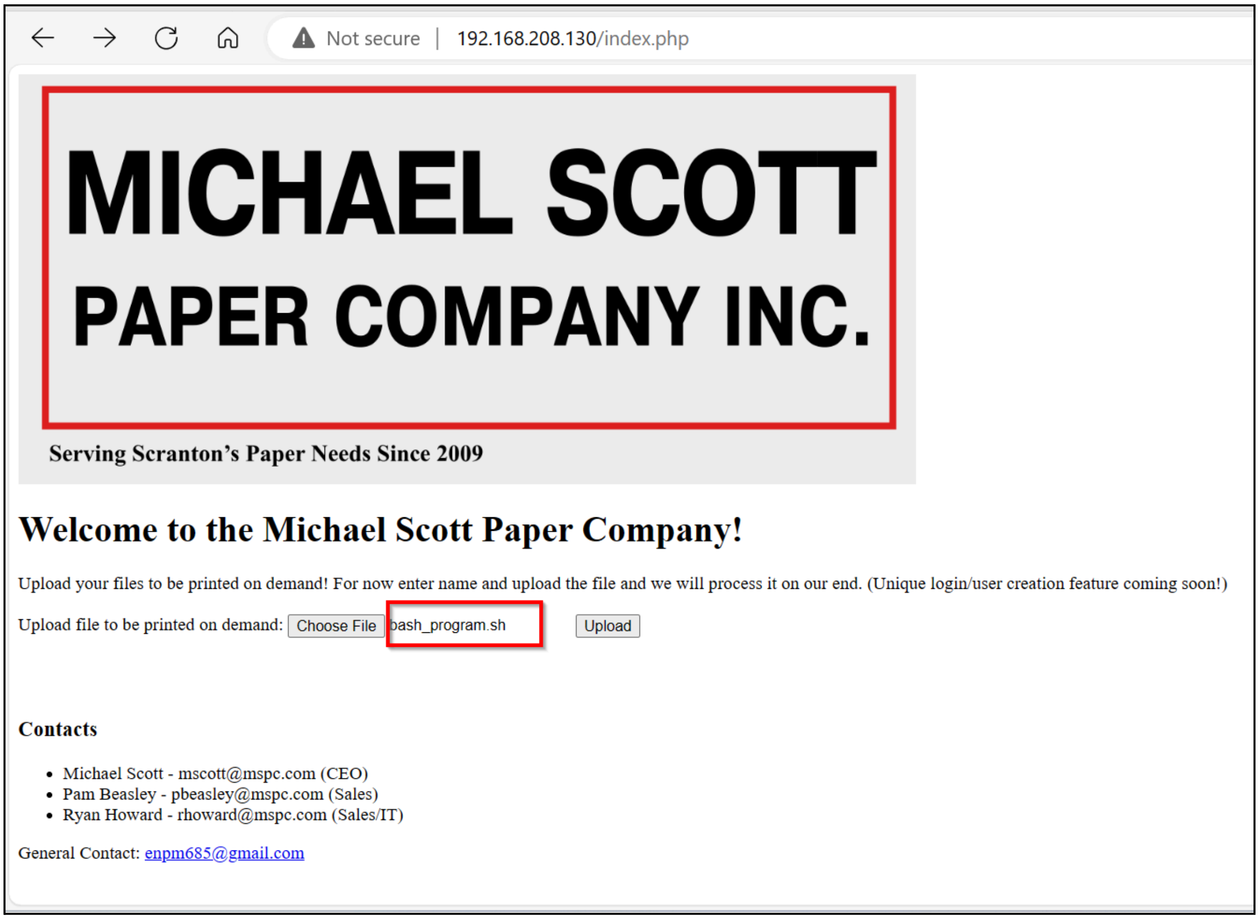
Upload a file

hmmmm I bet you could have fun with this...

Upload your script or treatment to us: Choose File ENPM685-4…essment.pdf Upload

Back to the Dojo

The hacker can even write a bash program and upload it.We can see from the image below that there is no restriction when it comes to uploading files.


Not secure
192.168.208.130/index.php
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!)

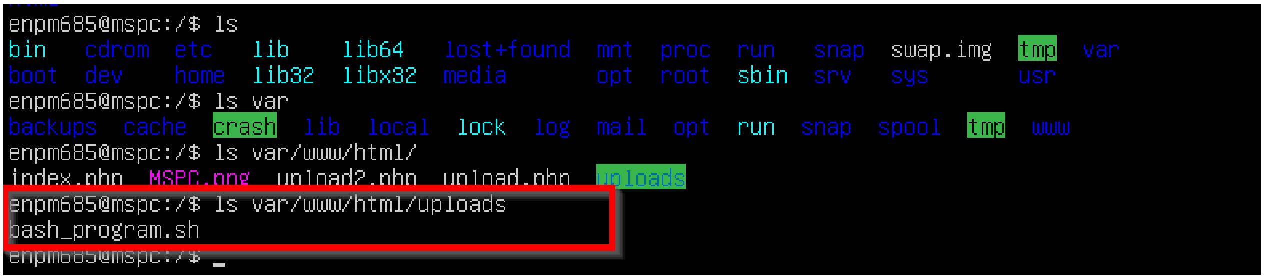
Upload file to be printed on demand: Choose File bash_program.sh Upload

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

The above file can be located in the system:



```
enpm685@mspc:/$ ls
bin   cdrom  etc   lib    lib64   lost+found  mnt   proc   run   snap   swap.img  tmp  var
boot  dev    home  lib32  libx32  media       opt   root   sbin  srv    sys       usr
enpm685@mspc:/$ ls var
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp  www
enpm685@mspc:/$ ls var/www/html/
index.php  MSPC.png  upload2.php  upload.php  uploads
enpm685@mspc:/$ ls var/www/html/uploads
bash_program.sh
enpm685@mspc:/$ _
```

Recommendations:

- Establish a login mechanism that demands authentication from users before file uploads. Restrict access to certain users who have access to upload files. This way, sensitive data will not be exposed to the public and not all users can upload files onto the system. Thus, security and accountability are enhanced.
- File uploads should be validated and sanitized. Any unacceptable file types should be rejected straightaway.

2. IDENTIFICATION AND AUTHENTICATION (IA)

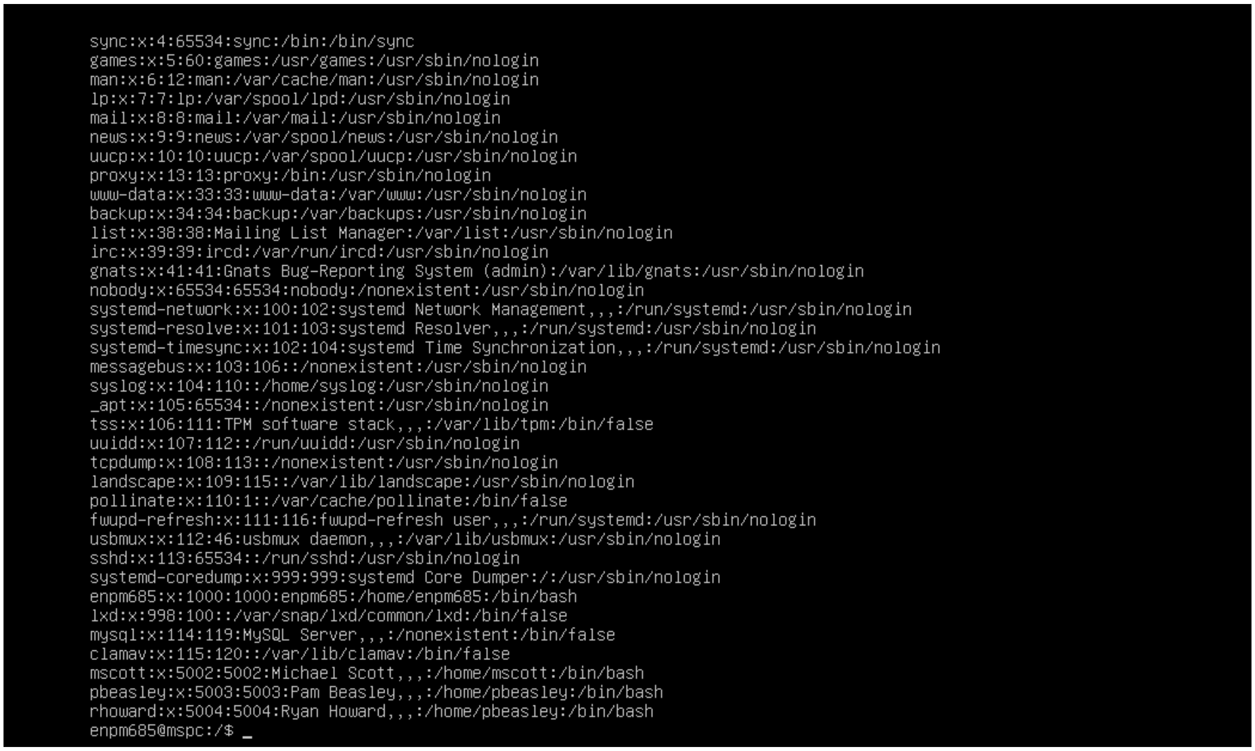
2.1 IA.L1-3.5.1 – IDENTIFICATION

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

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

Evaluation/Evidence:

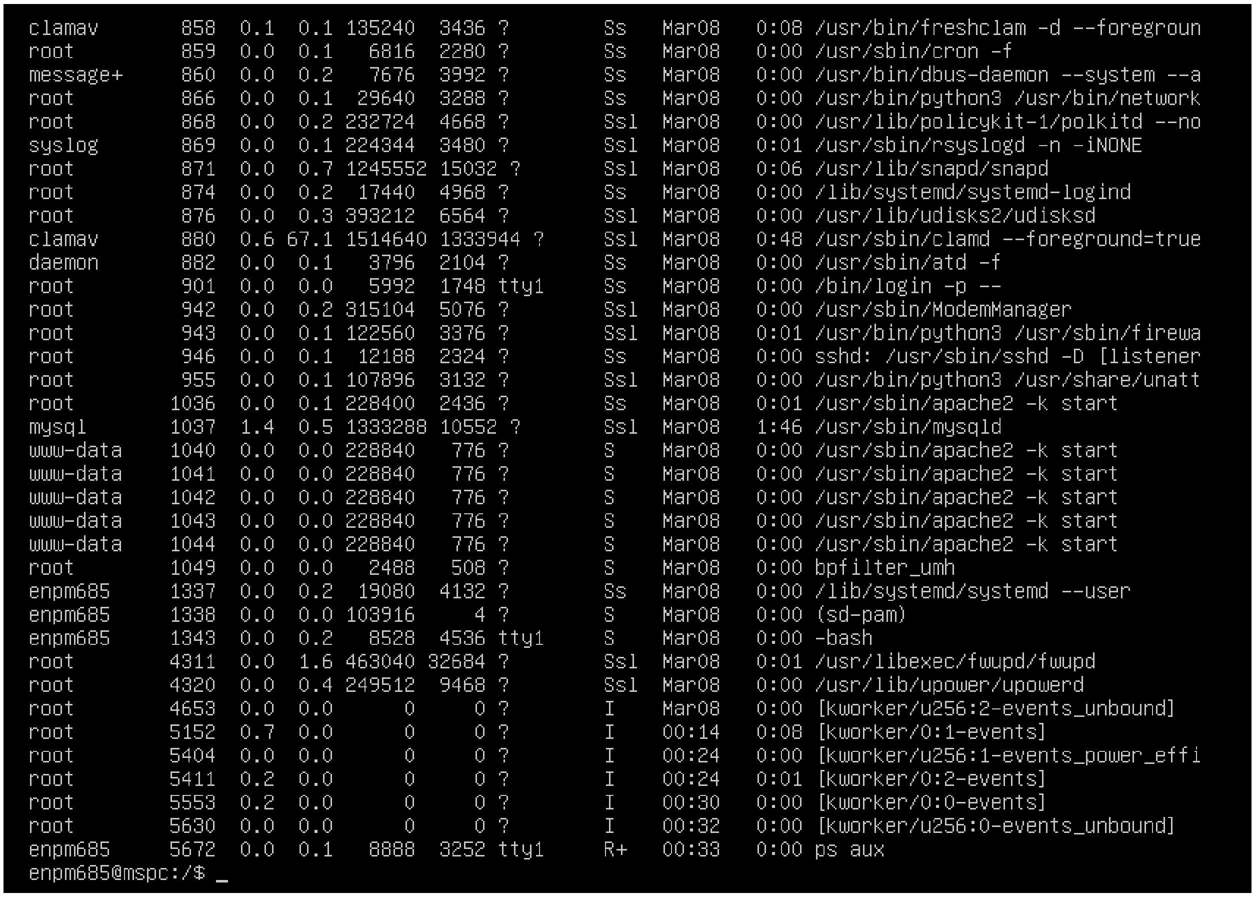
Successful identification is achieved by utilizing the "/etc/passwd" file. It is a plain text-based database that has a list of all user accounts created. This allows easy identification of all the users that exist in the database.



```
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:/$ _
```

It is evident that the processes associated with users "root, syslog, daemon, ClamAV, MySQL, www-data, enpm685" can be seen in the below image. Detailed examination of these users' processes would follow for the root user as an example, multiple processes were identified.

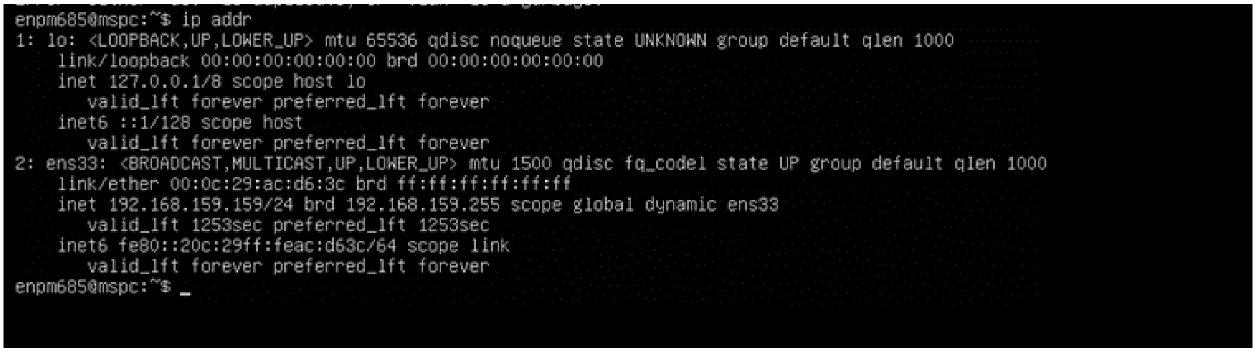
.Command: ps aux



```
clamav       858  0.1  0.1 135240  3436 ?        Ss   Mar08   0:08 /usr/bin/freshclam -d --foregroun
root         859  0.0  0.1   6816  2280 ?        Ss   Mar08   0:00 /usr/sbin/cron -f
message+     860  0.0  0.2   7676  3992 ?        Ss   Mar08   0:00 /usr/bin/dbus-daemon --system --a
root         866  0.0  0.1  29640  3288 ?        Ss   Mar08   0:00 /usr/bin/python3 /usr/bin/network
root         868  0.0  0.2 232724  4668 ?        Ssl  Mar08   0:00 /usr/lib/policykit-1/polkitd --no
syslog       869  0.0  0.1 224344  3480 ?        Ssl  Mar08   0:01 /usr/sbin/rsyslogd -n -iNONE
root         871  0.0  0.7 1245552 15032 ?       Ssl  Mar08   0:06 /usr/lib/snapd/snapd
root         874  0.0  0.2  17440  4968 ?        Ss   Mar08   0:00 /lib/systemd/systemd-logind
root         876  0.0  0.3 393212  6564 ?        Ssl  Mar08   0:00 /usr/lib/udisks2/udisksd
clamav       880  0.6 67.1 1514640 1333944 ?     Ssl  Mar08   0:48 /usr/sbin/clamd --foreground=true
daemon       882  0.0  0.1   3796  2104 ?        Ss   Mar08   0:00 /usr/sbin/atd -f
root         901  0.0  0.0   5992  1748 tty1     Ss   Mar08   0:00 /bin/login -p --
root         942  0.0  0.2 315104  5076 ?        Ssl  Mar08   0:00 /usr/sbin/ModemManager
root         943  0.0  0.1 122560  3376 ?        Ssl  Mar08   0:01 /usr/bin/python3 /usr/sbin/firewa
root         946  0.0  0.1  12188  2324 ?        Ss   Mar08   0:00 sshd: /usr/sbin/sshd -D [listener
root         955  0.0  0.1 107896  3132 ?        Ssl  Mar08   0:00 /usr/bin/python3 /usr/share/unatt
root        1036  0.0  0.1 228400  2436 ?        Ss   Mar08   0:01 /usr/sbin/apache2 -k start
mysql       1037  1.4  0.5 1333288 10552 ?       Ssl  Mar08   1:46 /usr/sbin/mysqld
www-data    1040  0.0  0.0 228840   776 ?        S    Mar08   0:00 /usr/sbin/apache2 -k start
www-data    1041  0.0  0.0 228840   776 ?        S    Mar08   0:00 /usr/sbin/apache2 -k start
www-data    1042  0.0  0.0 228840   776 ?        S    Mar08   0:00 /usr/sbin/apache2 -k start
www-data    1043  0.0  0.0 228840   776 ?        S    Mar08   0:00 /usr/sbin/apache2 -k start
www-data    1044  0.0  0.0 228840   776 ?        S    Mar08   0:00 /usr/sbin/apache2 -k start
root        1049  0.0  0.0   2488   508 ?        S    Mar08   0:00 bpfilter_umh
enpm685     1337  0.0  0.2  19080  4132 ?        Ss   Mar08   0:00 /lib/systemd/systemd --user
enpm685     1338  0.0  0.0 103916     4 ?        S    Mar08   0:00 (sd-pam)
enpm685     1343  0.0  0.2   8528  4536 tty1     S    Mar08   0:00 -bash
root        4311  0.0  1.6 463040 32684 ?        Ssl  Mar08   0:01 /usr/libexec/fwupd/fwupd
root        4320  0.0  0.4 249512  9468 ?        Ssl  Mar08   0:00 /usr/lib/upower/upowerd
root        4653  0.0  0.0      0     0 ?        I    Mar08   0:00 [kworker/u256:2-events_unbound]
root        5152  0.7  0.0      0     0 ?        I    00:14   0:08 [kworker/0:1-events]
root        5404  0.0  0.0      0     0 ?        I    00:24   0:00 [kworker/u256:1-events_power_effi
root        5411  0.2  0.0      0     0 ?        I    00:24   0:01 [kworker/0:2-events]
root        5553  0.2  0.0      0     0 ?        I    00:30   0:00 [kworker/0:0-events]
root        5630  0.0  0.0      0     0 ?        I    00:32   0:00 [kworker/u256:0-events_unbound]
enpm685     5672  0.0  0.1   8888  3252 tty1     R+   00:33   0:00 ps aux
enpm685@mspc:/$ _
```

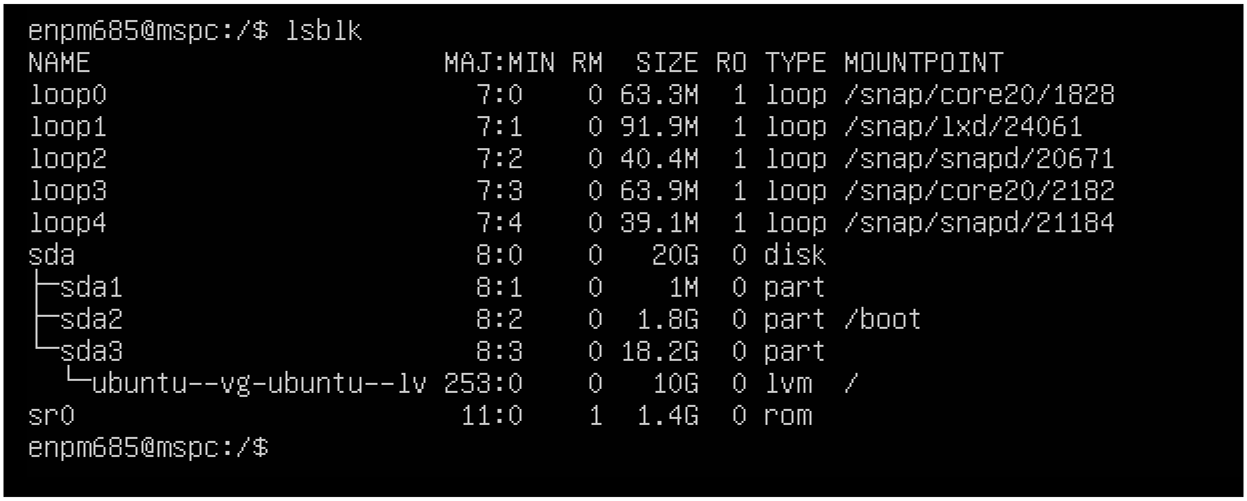
For common devices, identifiers are based on media access control (MAC), Internet Protocol (IP) addresses, or device-unique tokens or identifiers. The following are snippets for reference:

Used the “ip addr” command to list network interfaces along with their MAC address.



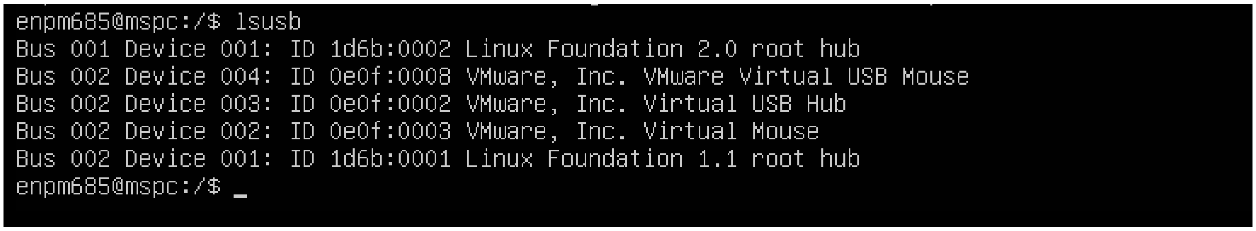
```
enpm685@mspc:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ac:d6:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.159.159/24 brd 192.168.159.255 scope global dynamic ens33
       valid_lft 1253sec preferred_lft 1253sec
    inet6 fe80::20c:29ff:feac:d63c/64 scope link
       valid_lft forever preferred_lft forever
enpm685@mspc:~$ _
```

Used commands like lsblk to list storage devices along with their UUIDs.



```
enpm685@mspc:/$ lsblk
NAME                      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0                       7:0    0 63.3M  1 loop /snap/core20/1828
loop1                       7:1    0 91.9M  1 loop /snap/lxd/24061
loop2                       7:2    0 40.4M  1 loop /snap/snapd/20671
loop3                       7:3    0 63.9M  1 loop /snap/core20/2182
loop4                       7:4    0 39.1M  1 loop /snap/snapd/21184
sda                         8:0    0   20G  0 disk
├─sda1                      8:1    0    1M  0 part
├─sda2                      8:2    0  1.8G  0 part /boot
└─sda3                      8:3    0 18.2G  0 part
  └─ubuntu--vg-ubuntu--lv 253:0    0   10G  0 lvm  /
sr0                        11:0    1  1.4G  0 rom
enpm685@mspc:/$
```

.Used the lsusb command to list USB devices connected to the system along with their details.



```
enpm685@mspc:/$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0e0f:0008 VMware, Inc. VMware Virtual USB Mouse
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
enpm685@mspc:/$ _
```

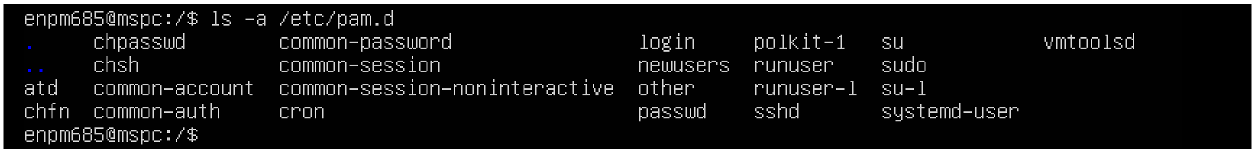
2.2 IA.L1-3.5.2 – AUTHENTICATION

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

Is this requirement being met? [✓ MET] NOT MET N/A

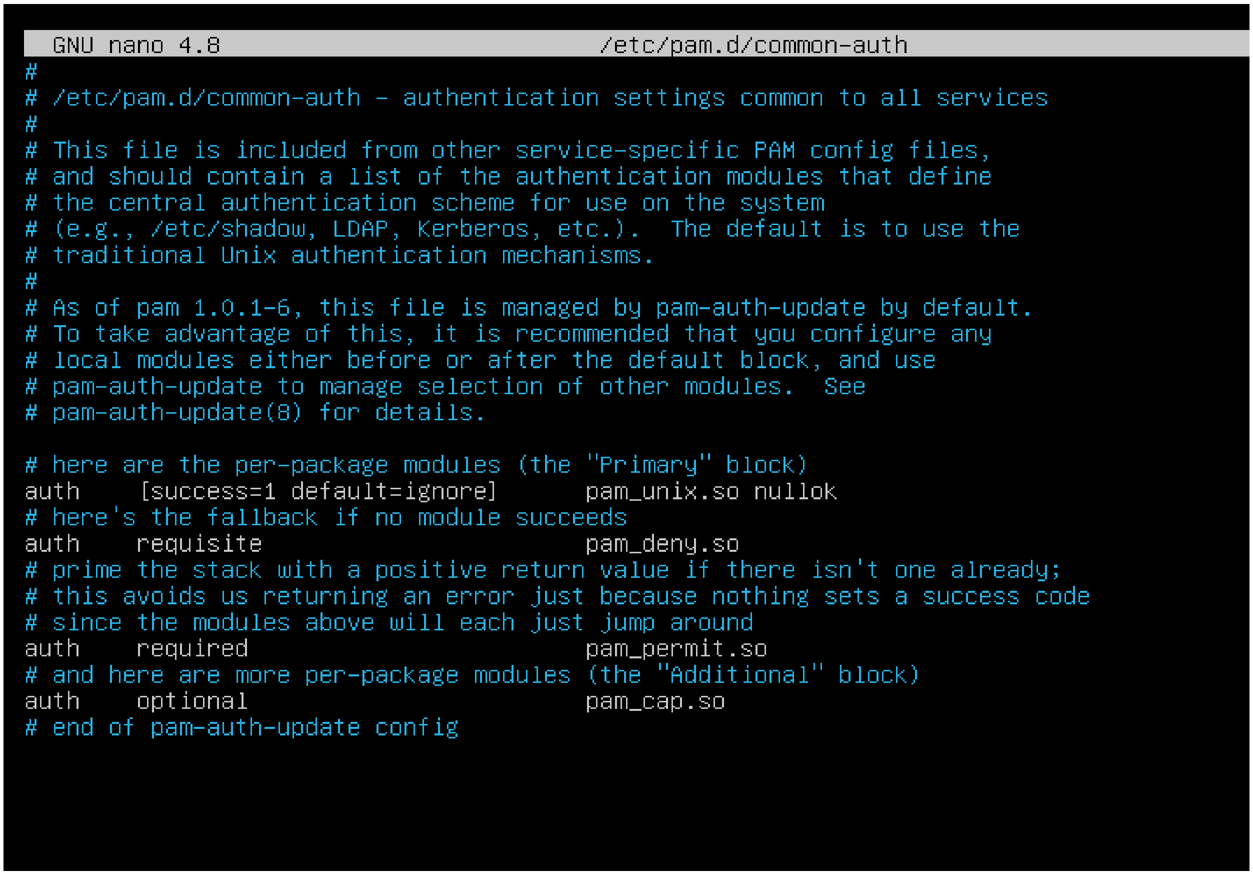
Evaluation/Evidence:

PAM provides a mechanism for authenticating users and authorizing access to system resources. When we list the pam.d directory, we can see the configuration files for the Pluggable Authentication Modules (PAM) framework.



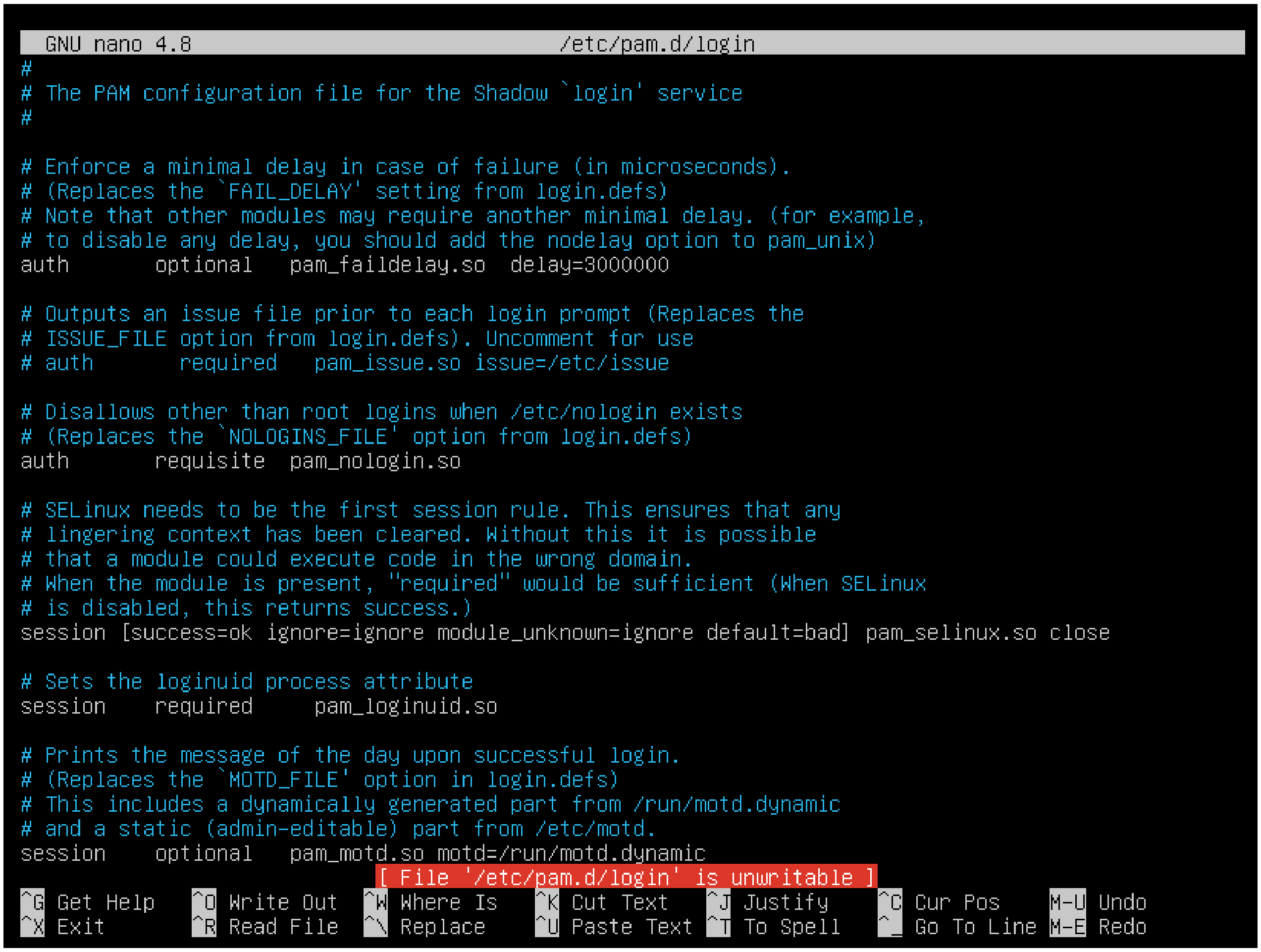
```
enpm685@mspc:/$ ls -a /etc/pam.d
.     chpasswd        common-password                login     polkit-1   su            vmtoolsd
..    chsh            common-session                 newusers  runuser    sudo
atd   common-account  common-session-noninteractive  other     runuser-l  su-l
chfn  common-auth     cron                           passwd    sshd       systemd-user
enpm685@mspc:/$
```

The “/etc/pam.d/common-auth” file contains authentication rules and settings that are shared among various services and applications on the system.



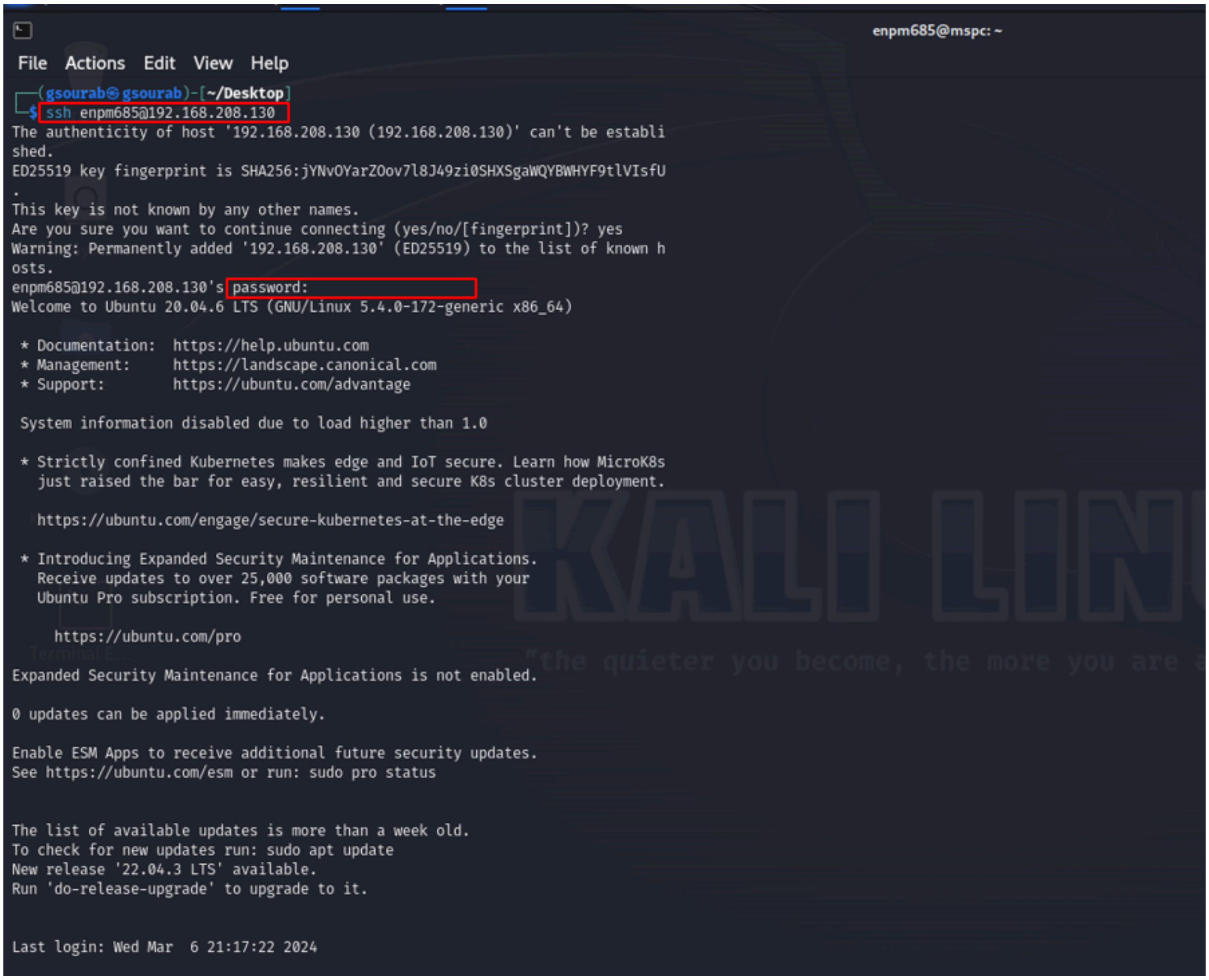
```
  GNU nano 4.8                          /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=1 default=ignore]      pam_unix.so nullok
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional                        pam_cap.so
# end of pam-auth-update config
```

The "/etc/pam.d/login" file defines how authentication and authorization are handled when a user logins into the system.



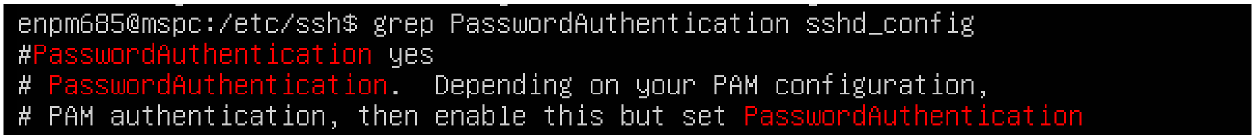
```
  GNU nano 4.8                              /etc/pam.d/login
#
# The PAM configuration file for the Shadow `login' service
#

# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the `FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth       optional   pam_faildelay.so  delay=3000000

# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth       required   pam_issue.so issue=/etc/issue

# Disallows other than root logins when /etc/nologin exists
# (Replaces the `NOLOGINS_FILE' option from login.defs)
auth       requisite  pam_nologin.so

# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without this it is possible
# that a module could execute code in the wrong domain.
# When the module is present, "required" would be sufficient (When SELinux
# is disabled, this returns success.)
session [success=ok ignore=ignore module_unknown=ignore default=bad] pam_selinux.so close

# Sets the loginuid process attribute
session    required     pam_loginuid.so

# Prints the message of the day upon successful login.
# (Replaces the `MOTD_FILE' option in login.defs)
# This includes a dynamically generated part from /run/motd.dynamic
# and a static (admin-editable) part from /etc/motd.
session    optional   pam_motd.so motd=/run/motd.dynamic
                             [ File '/etc/pam.d/login' is unwritable ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

The system is also running SSH, so it authenticates users while asking for login details whenever the user tries to connect through SSH.

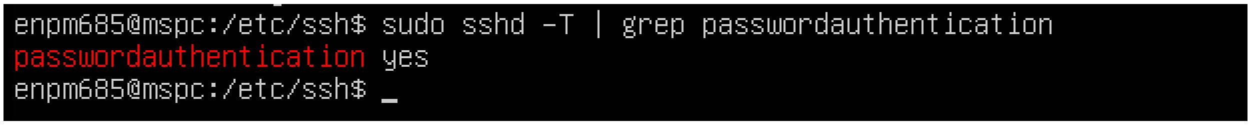


```
┌──(gsourab㉿gsourab)-[~/Desktop]
└─$ ssh enpm685@192.168.208.130
The authenticity of host '192.168.208.130 (192.168.208.130)' can't be establi
shed.
ED25519 key fingerprint is SHA256:jYNvOYarZOov7l8J49zi0SHXSgaWQYBWHYF9tlVIsfU
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.208.130' (ED25519) to the list of known h
osts.
enpm685@192.168.208.130's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-172-generic x86_64)

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

 System information disabled due to load higher than 1.0

 * 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.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Wed Mar  6 21:17:22 2024
```

Further checking the SSH daemon config and we found that the password authentication is present (Yes) from the below figure



```
enpm685@mspc:/etc/ssh$ grep PasswordAuthentication sshd_config
#PasswordAuthentication yes
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication, then enable this but set PasswordAuthentication
```



```
enpm685@mspc:/etc/ssh$ sudo sshd -T | grep passwordauthentication
passwordauthentication yes
enpm685@mspc:/etc/ssh$ _
```

3. MEDIA PROTECTION (MP)

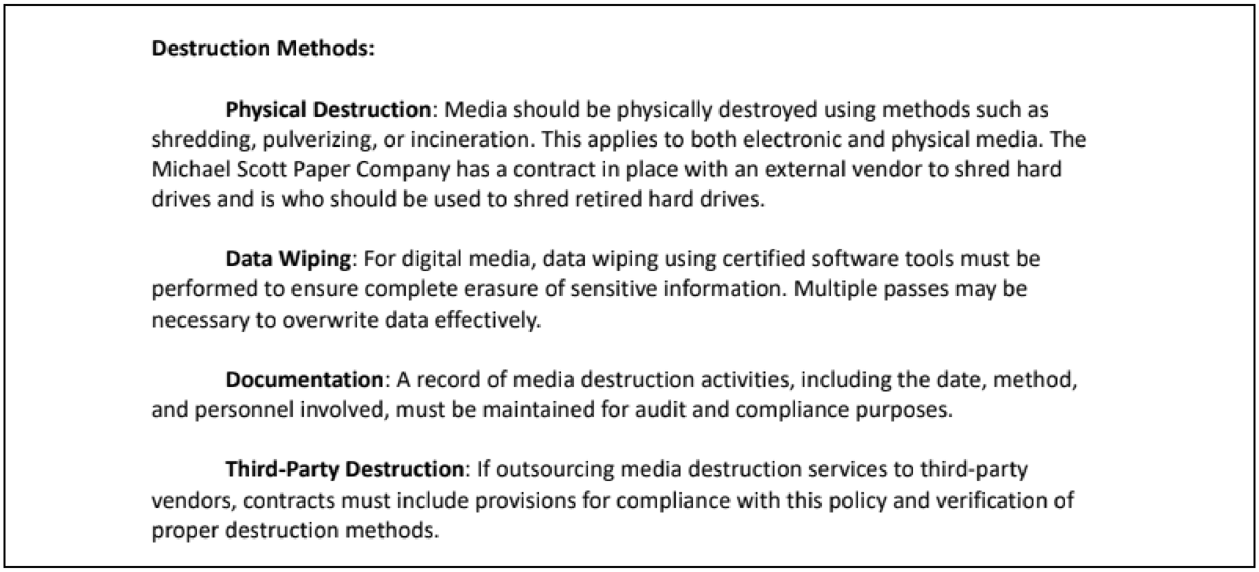
3.1 MP.L1-3.8.3 – MEDIA DISPOSAL

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 has a process in place concerned with Media Disposal, which is mentioned in the "MSPC-Media-Destruction-Policy" document found among the potential evidence. It mentions various destruction methods that the company follows. One of them is the physical destruction of the media through shredding the physical data. There is also routine data removal taking place so that confidential information is not exposed and can't be used to take advantage to hack into the company's systems. Documentation of all the data removal and destruction is also regularly maintained by the company. While dealing with media that is associated with third-party sources, appropriate guidelines and policies must be followed to ensure compliance with proper media destruction processes.



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.

4. PHYSICAL PROTECTION

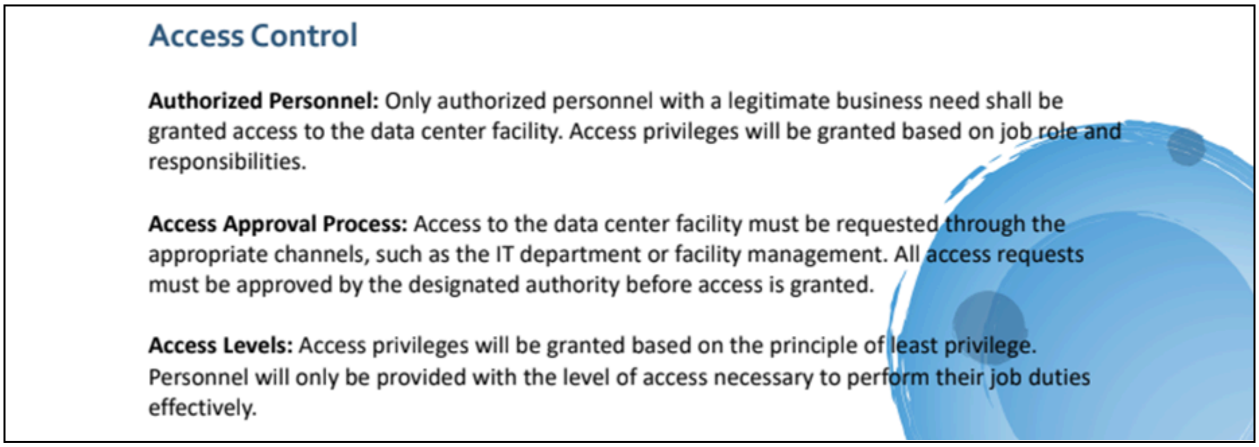
4.1 PE.L1-3.10.1 – LIMIT PHYSICAL ACCESS

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:

According to the Data Centre Policy, only authorized individuals will be granted physical access and this access shall be provided as per the least privilege principle, guaranteeing that users have the minimal amount of authority needed to access any system or equipment belonging to the organization.



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.

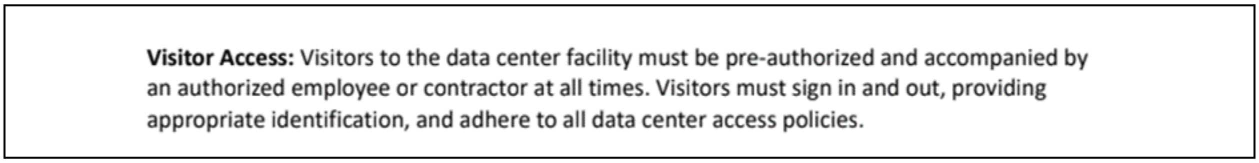
4.2 PE.L1-3.10.3 – ESCORT VISITORS

Escort visitors and monitor visitor activity

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

Evaluation/Evidence:

The organization has defined a strict policy for Visitor access, as mentioned in the “MSPC-Data -Center -Policy” document found among the potential evidence. The document specifies that visitors must sign in and out, provide proper identification and must be pre-authorized and escorted by an authorized employee.



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.

4.3 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 information given in the Data Center policy, it has not been stated anywhere explicitly about the maintenance of audit logs by the organization. Thus, since it only specifies the requirement that visitors sign in and out and does not go into depth about the types of audit logs used or the length of time these logs are retained, there is no evidence that any kind of logs of people entering and leaving the building are recorded anywhere physically.

Recommendations:

There should be a physical logbook or logs on the system to keep track of activities like logging in and out of the data center. Specifically, we should consider that it is necessary to specify the retention period for access records and the type of audit logs (automated, procedural, or a combination of both) that are being maintained for both authorized access and visitor access.

4.4 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:

The data center policy briefly describes how only authorized personnel will be granted access due to business needs, access must be requested through IT department/ facility management, and access privileges will be granted on the principle of least privilege. But, it does not include sufficient detail about the types of physical access devices that are in use, the processes for managing these devices, the assignment, and tracking of these devices, how to handle personnel changes or the maintenance of the access control systems.

To meet CMMC 2.0 Level 1 requirements, the policy should include detailed information about physical access devices in use such as keys, locks, card readers, biometric scanners, and combinations given to every employee, and the company must explain how those devices are managed or controlled. Like whether the process management follows is manual or automated. There should be a clear, documented process for assigning access devices (e.g., keys, cards) to individuals based on their role and need for access. First, create an assignment list (for example, who gets what type of key) and a process for updating the access system (e.g., who changes it when people change jobs); second, provide detailed information about how the assignment list process will be used and modified when personnel changes, e.g., revoking the access when an employee leaves the company, changing locks, how often the access control devices and systems will be maintained, etc.

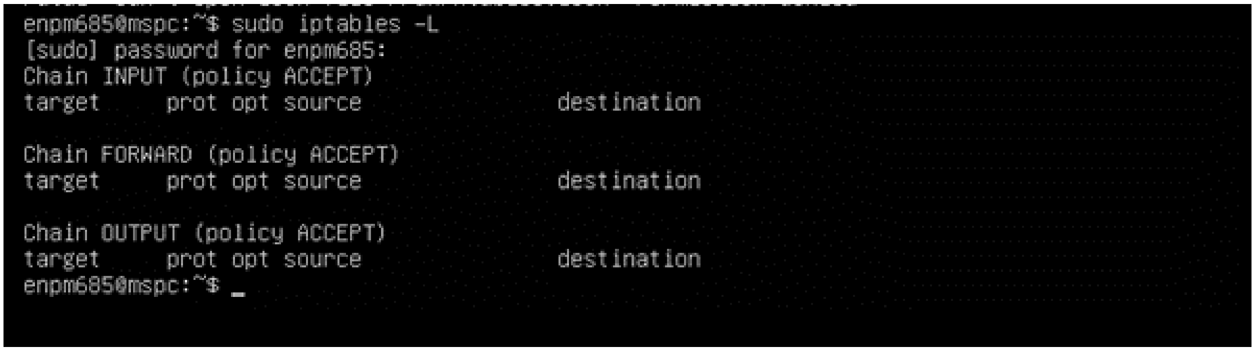
1. SYSTEMS AND COMMUNICATIONS PROTECTION (SC)

5.1 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.

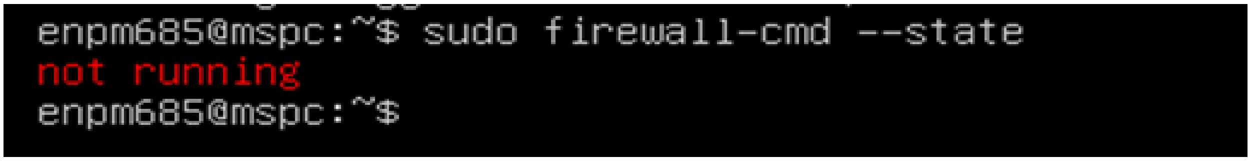
Is this requirement being met?   MET   **NOT MET**   N/A

Evaluation/Evidence:



```
enpm685@mspc:~$ sudo iptables -L
[sudo] password for enpm685:
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:~$ _
```

From the screenshot displayed above, we can see that rules are not defined in the FORWARD, OUTPUT, or INPUT chains inside the IP table. All three chains have the policy set to ACCEPT, which in general means that all incoming, forwarded, and outgoing traffic is by default permitted. In general, organizations use firewall rules to regulate traffic flow between internal or external networks, or between various network segments, to provide boundary protection. But in the figure, IP tables with no rules mentioned allow all traffic through without any filtering, indicating a lack of active boundary protection measures.



```
enpm685@mspc:~$ sudo firewall-cmd --state
not running
enpm685@mspc:~$
```

Now, we run the above command to check if any active firewall is running to determine the boundary protection. But as visible in the screenshot above, no firewall is active. This means there is no process in place for filtering, monitoring, or controlling network traffic that enters or leaves the system.

Recommendations:

Firewalls play a very major role in boundary protection. We have also observed that by default the firewall is not running. A firewall should be enabled as this will act as the first line of defense for the Michael Scott Paper Company when a threat actor tries to infiltrate the company's network.

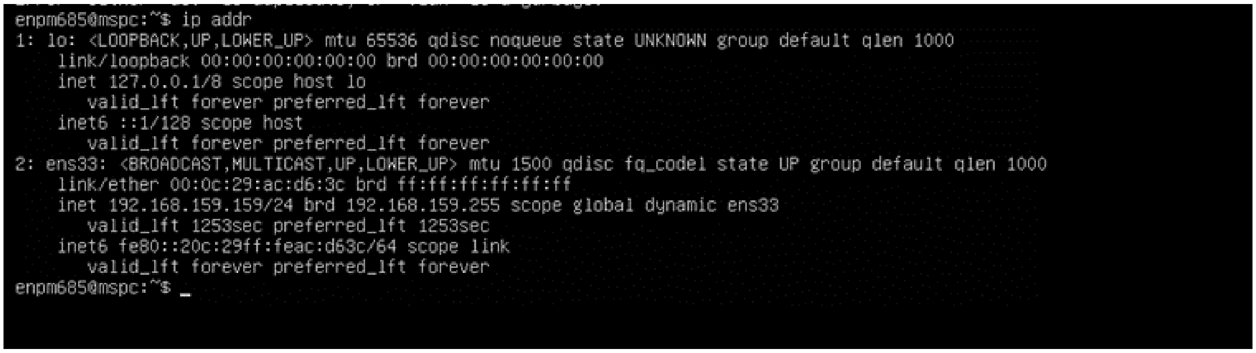
It is recommended to configure rules in IP tables to control network traffic and implement boundary protection. These rules ensure boundary protection by allowing or blocking traffic based on protocols, source IP address and destination IP address.

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

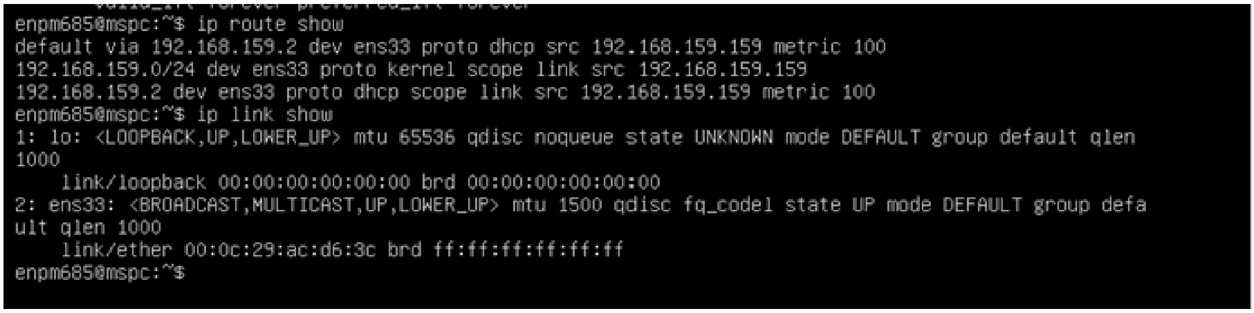
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

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

Evaluation/Evidence:

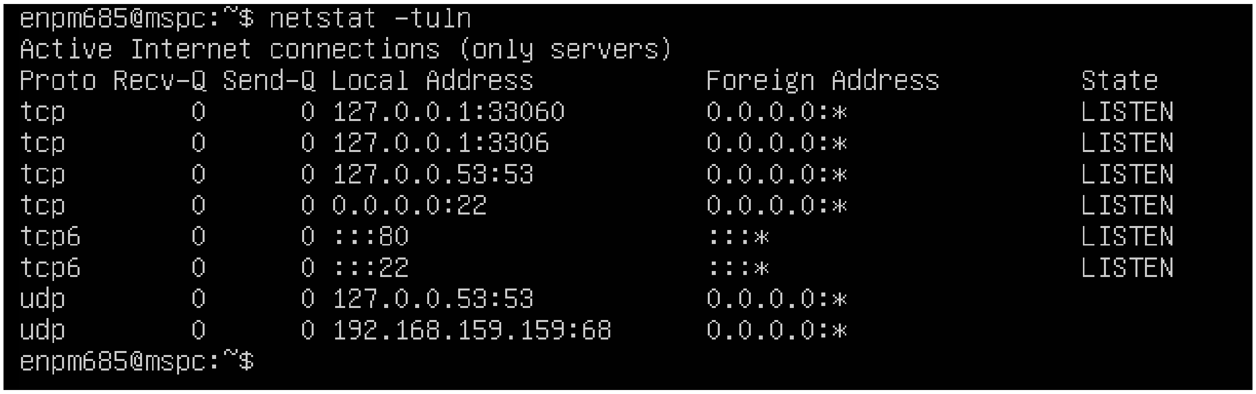


```
enpm685@mspc:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:ac:d6:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.159.159/24 brd 192.168.159.255 scope global dynamic ens33
       valid_lft 1253sec preferred_lft 1253sec
    inet6 fe80::20c:29ff:feac:d63c/64 scope link
       valid_lft forever preferred_lft forever
enpm685@mspc:~$ _
```



```
enpm685@mspc:~$ ip route show
default via 192.168.159.2 dev ens33 proto dhcp src 192.168.159.159 metric 100
192.168.159.0/24 dev ens33 proto kernel scope link src 192.168.159.159
192.168.159.2 dev ens33 proto dhcp scope link src 192.168.159.159 metric 100
enpm685@mspc:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen
1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group defa
ult qlen 1000
    link/ether 00:0c:29:ac:d6:3c brd ff:ff:ff:ff:ff:ff
enpm685@mspc:~$
```

The system is described as not having any internet-facing services or components available to the public. From the figure it is evident that the system is using a single network interface (ens33) with a private IP address (192.168.159.159) within the IP range of 192.168.159.0/24, The use of a private IP address range reinforces the observation that this system is not meant to be reached from the public internet. Because private IP addresses are not routable on the internet. The IP range of 192.168.159.0/24 is reserved for private, non-routable systems. This is common for internal, non-exposed systems which don't need to talk directly to external entities.



```
enpm685@mspc:~$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 192.168.159.159:68      0.0.0.0:*
enpm685@mspc:~$
```

From the figure netstat -tuln, the output indicates that the system does not host any services configured to listen on public (internet-facing) interfaces. Services like MySQL and DNS are bound to the loopback interface (127.0.0.1 and 127.0.0.53, respectively), which is not accessible from outside the host itself. That is, the machine is not hosting any service accessible from the internet. Its components all operate within a private IP range, and no components are designed to listen on public interfaces.

Therefore, the control to implement subnetworks for publicly accessible system components would not be relevant in this case. Because publicly accessible components simply don't exist in this system that would require such segregation.

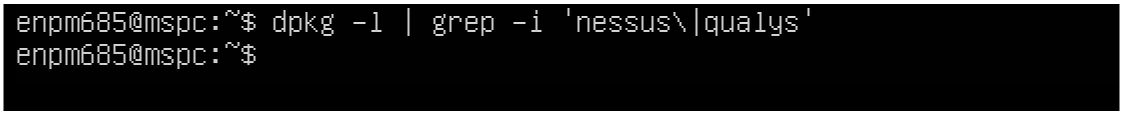
2. SYSTEM AND INFORMATION INTEGRITY (SI)

6.1 SI.L1-3.14.1 – FLAW REMEDIATION

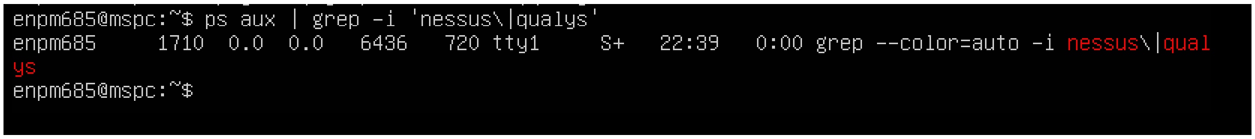
Identify, report, and correct information and information system flaws promptly

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

Evaluation/Evidence:



```
enpm685@mspc:~$ dpkg -l | grep -i 'nessus\|qualys'
enpm685@mspc:~$
```



```
enpm685@mspc:~$ ps aux | grep -i 'nessus\|qualys'
enpm685     1710  0.0  0.0   6436   720 tty1     S+   22:39   0:00 grep --color=auto -i nessus\|qual
ys
enpm685@mspc:~$
```

On checking the system, as we can see from the above figures that there were no processes found related to any vulnerability scanner software. Generally, when vulnerability scanners like Nessus or Qualys are present on the system, activities related to processes like when the scans were initiated or completed are visible. Even when such software encounters errors during the scanning process, they are reflected in the error logs of a system, which seems to be missing here.

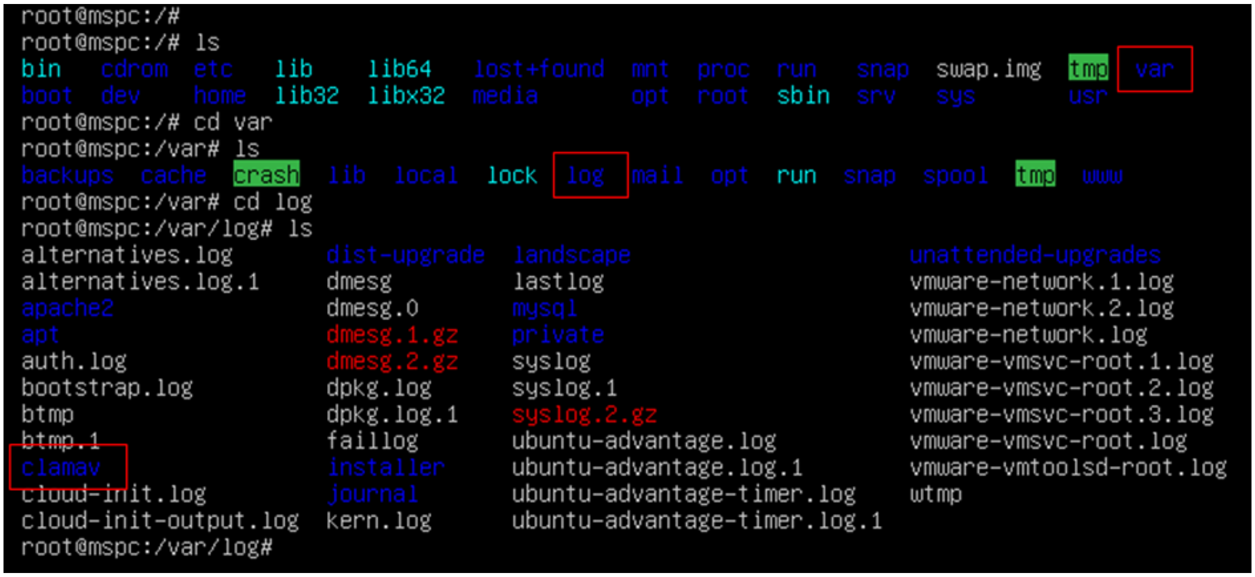
6.2 SI.L1-3.14.2 – MALICIOUS CODE PROTECTION

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

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

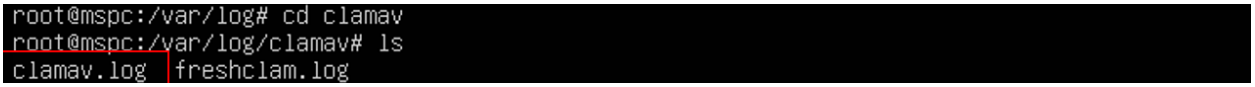
Evaluation/Evidence:

On navigating the logs folder, within the var directory, we can see ClamAV logs. ClamAV is a software used to detect malware like viruses or worms. Since we can see the logs, it means that the software has been installed on the machine. It will detect and block malicious code and prevent it from getting executed.

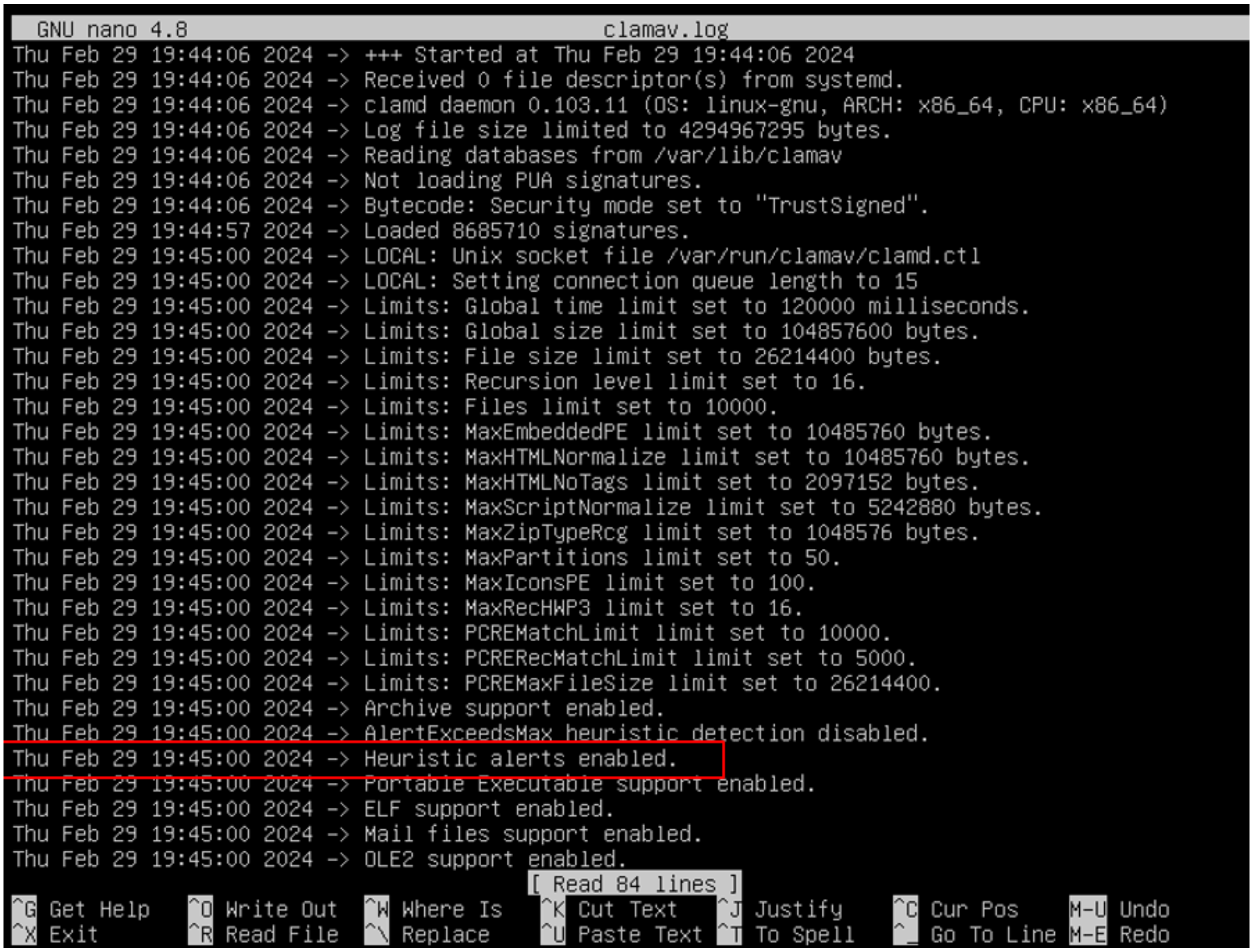


```
root@mspc:/#
root@mspc:/# ls
bin   cdrom  etc   lib    lib64   lost+found  mnt  proc  run   snap  swap.img  tmp  var
boot  dev    home  lib32  libx32  media       opt  root  sbin  srv   sys       usr
root@mspc:/# cd var
root@mspc:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  snap  spool  tmp  www
root@mspc:/var# cd log
root@mspc:/var/log# ls
alternatives.log       dist-upgrade  landscape                   unattended-upgrades
alternatives.log.1     dmesg         lastlog                     vmware-network.1.log
apache2                dmesg.0       mysql                       vmware-network.2.log
apt                    dmesg.1.gz    private                     vmware-network.log
auth.log               dmesg.2.gz    syslog                      vmware-vmsvc-root.1.log
bootstrap.log          dpkg.log      syslog.1                    vmware-vmsvc-root.2.log
btmp                   dpkg.log.1    syslog.2.gz                 vmware-vmsvc-root.3.log
btmp.1                 faillog       ubuntu-advantage.log        vmware-vmsvc-root.log
clamav                 installer     ubuntu-advantage.log.1      vmware-vmtoolsd-root.log
cloud-init.log         journal       ubuntu-advantage-timer.log  wtmp
cloud-init-output.log  kern.log      ubuntu-advantage-timer.log.1
root@mspc:/var/log#
```

ClamAV has an important component known as Heuristic Analysis. Due to this component, ClamAV is equipped with the capability of detecting new/previous threats and blocking them to prevent attacks. We can see these alerts are enabled in the logs



```
root@mspc:/var/log# cd clamav
root@mspc:/var/log/clamav# ls
clamav.log  freshclam.log
```



```
  GNU nano 4.8                              clamav.log
Thu Feb 29 19:44:06 2024 -> +++ Started at Thu Feb 29 19:44:06 2024
Thu Feb 29 19:44:06 2024 -> Received 0 file descriptor(s) from systemd.
Thu Feb 29 19:44:06 2024 -> clamd daemon 0.103.11 (OS: linux-gnu, ARCH: x86_64, CPU: x86_64)
Thu Feb 29 19:44:06 2024 -> Log file size limited to 4294967295 bytes.
Thu Feb 29 19:44:06 2024 -> Reading databases from /var/lib/clamav
Thu Feb 29 19:44:06 2024 -> Not loading PUA signatures.
Thu Feb 29 19:44:06 2024 -> Bytecode: Security mode set to "TrustSigned".
Thu Feb 29 19:44:57 2024 -> Loaded 8685710 signatures.
Thu Feb 29 19:45:00 2024 -> LOCAL: Unix socket file /var/run/clamav/clamd.ctl
Thu Feb 29 19:45:00 2024 -> LOCAL: Setting connection queue length to 15
Thu Feb 29 19:45:00 2024 -> Limits: Global time limit set to 120000 milliseconds.
Thu Feb 29 19:45:00 2024 -> Limits: Global size limit set to 104857600 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: File size limit set to 26214400 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: Recursion level limit set to 16.
Thu Feb 29 19:45:00 2024 -> Limits: Files limit set to 10000.
Thu Feb 29 19:45:00 2024 -> Limits: MaxEmbeddedPE limit set to 10485760 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: MaxHTMLNormalize limit set to 10485760 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: MaxHTMLNoTags limit set to 2097152 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: MaxScriptNormalize limit set to 5242880 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: MaxZipTypeRcg limit set to 1048576 bytes.
Thu Feb 29 19:45:00 2024 -> Limits: MaxPartitions limit set to 50.
Thu Feb 29 19:45:00 2024 -> Limits: MaxIconsPE limit set to 100.
Thu Feb 29 19:45:00 2024 -> Limits: MaxRecHWP3 limit set to 16.
Thu Feb 29 19:45:00 2024 -> Limits: PCREMatchLimit limit set to 10000.
Thu Feb 29 19:45:00 2024 -> Limits: PCRERecMatchLimit limit set to 5000.
Thu Feb 29 19:45:00 2024 -> Limits: PCREMaxFileSize limit set to 26214400.
Thu Feb 29 19:45:00 2024 -> Archive support enabled.
Thu Feb 29 19:45:00 2024 -> AlertExceedsMax heuristic detection disabled.
Thu Feb 29 19:45:00 2024 -> Heuristic alerts enabled.
Thu Feb 29 19:45:00 2024 -> Portable Executable support enabled.
Thu Feb 29 19:45:00 2024 -> ELF support enabled.
Thu Feb 29 19:45:00 2024 -> Mail files support enabled.
Thu Feb 29 19:45:00 2024 -> OLE2 support enabled.
                                          [ Read 84 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

Therefore the requirement of malicious code protection is satisfied.

6.3 SI.L1-3.14.4 – UPDATE MALICIOUS CODE PROTECTION

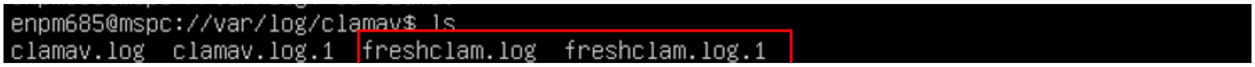
Update malicious code protection mechanisms when new releases are available

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

Evaluation/Evidence:

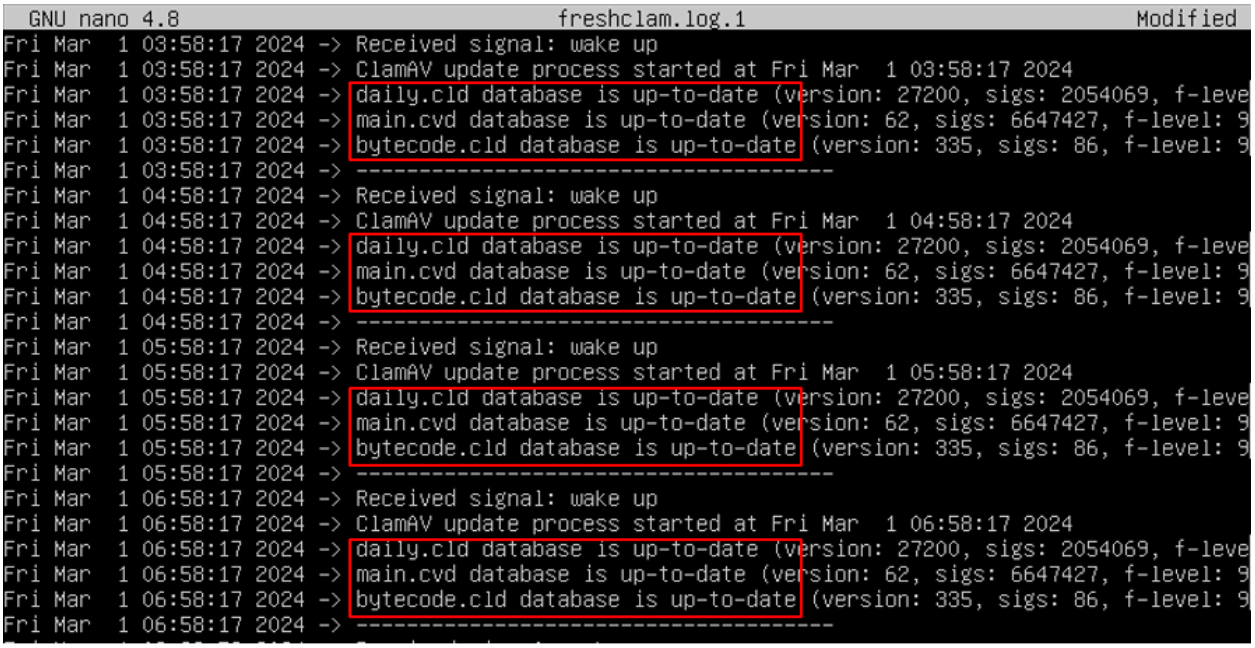
Now that we know that the Michael Scott Paper Company web application has ClamAV installed, we have to make sure whether there are mechanisms installed for updates.

Within the ClamAV directory, we can see Freshclam logs. Freshclam's functionality is to check and update the virus signature database which will be used by ClamAV.



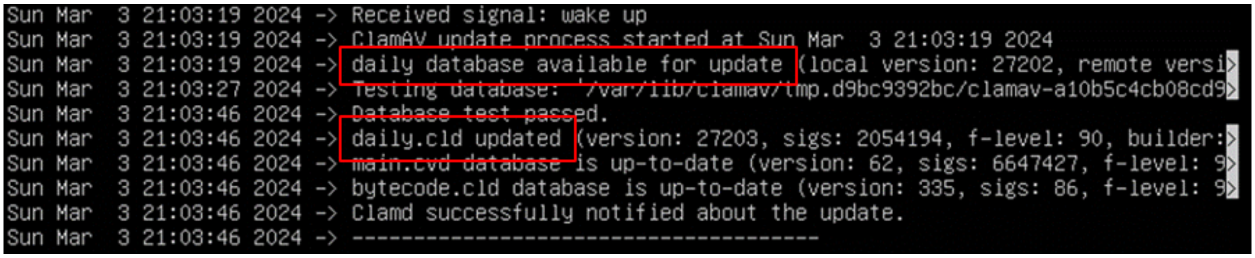
```
enpm685@mspc://var/log/clamav$ ls
clamav.log  clamav.log.1  freshclam.log  freshclam.log.1
```

On opening freshclam.logs, it is observed that the virus signature databases are being checked. The contents that are being checked for updates are shown below:



```
  GNU nano 4.8                          freshclam.log.1                          Modified
Fri Mar  1 03:58:17 2024 -> Received signal: wake up
Fri Mar  1 03:58:17 2024 -> ClamAV update process started at Fri Mar  1 03:58:17 2024
Fri Mar  1 03:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve
Fri Mar  1 03:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9
Fri Mar  1 03:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9
Fri Mar  1 03:58:17 2024 -> --------------------------------------
Fri Mar  1 04:58:17 2024 -> Received signal: wake up
Fri Mar  1 04:58:17 2024 -> ClamAV update process started at Fri Mar  1 04:58:17 2024
Fri Mar  1 04:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve
Fri Mar  1 04:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9
Fri Mar  1 04:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9
Fri Mar  1 04:58:17 2024 -> --------------------------------------
Fri Mar  1 05:58:17 2024 -> Received signal: wake up
Fri Mar  1 05:58:17 2024 -> ClamAV update process started at Fri Mar  1 05:58:17 2024
Fri Mar  1 05:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve
Fri Mar  1 05:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9
Fri Mar  1 05:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9
Fri Mar  1 05:58:17 2024 -> --------------------------------------
Fri Mar  1 06:58:17 2024 -> Received signal: wake up
Fri Mar  1 06:58:17 2024 -> ClamAV update process started at Fri Mar  1 06:58:17 2024
Fri Mar  1 06:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve
Fri Mar  1 06:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9
Fri Mar  1 06:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9
Fri Mar  1 06:58:17 2024 -> --------------------------------------
```

Here is one such instance where a database update was identified, tested, updated and notified



```
Sun Mar  3 21:03:19 2024 -> Received signal: wake up
Sun Mar  3 21:03:19 2024 -> ClamAV update process started at Sun Mar  3 21:03:19 2024
Sun Mar  3 21:03:19 2024 -> daily database available for update (local version: 27202, remote versi>
Sun Mar  3 21:03:27 2024 -> Testing database: '/var/lib/clamav/tmp.d9bc9392bc/clamav-a10b5c4cb08cd9>
Sun Mar  3 21:03:46 2024 -> Database test passed.
Sun Mar  3 21:03:46 2024 -> daily.cld updated (version: 27203, sigs: 2054194, f-level: 90, builder:>
Sun Mar  3 21:03:46 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9>
Sun Mar  3 21:03:46 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9>
Sun Mar  3 21:03:46 2024 -> Clamd successfully notified about the update.
Sun Mar  3 21:03:46 2024 -> --------------------------------------
```

Therefore the requirement of updating malicious code protection (ClamAV) is satisfied.

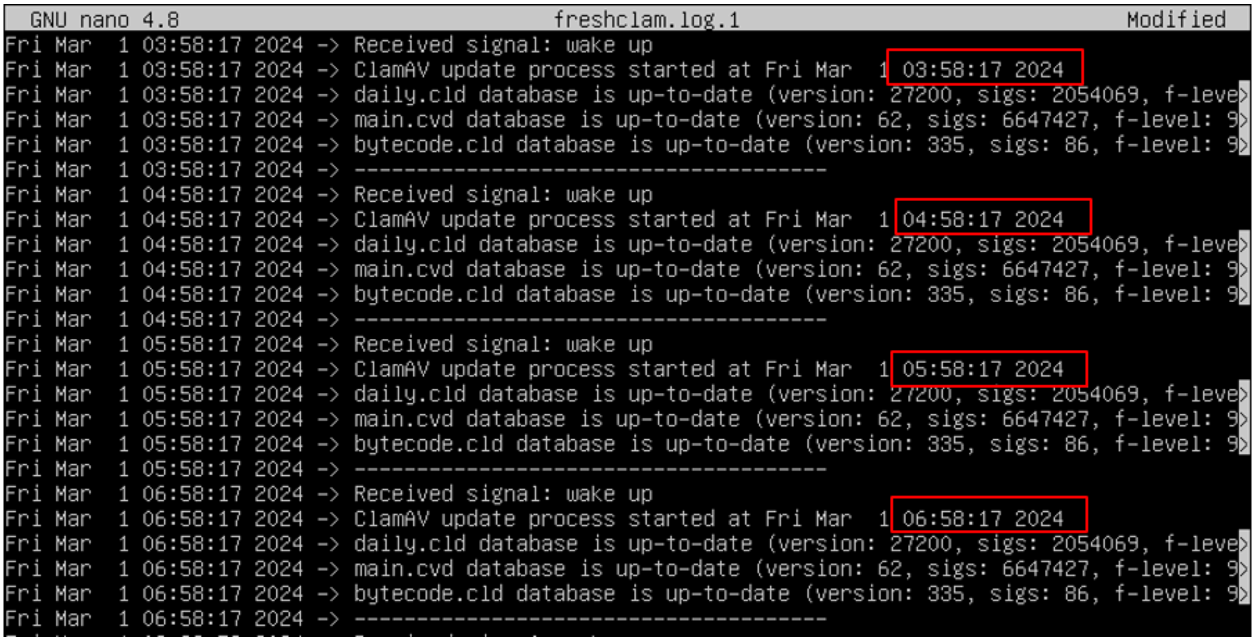
6.4 SI.L1-3.14.5 – SYSTEM & FILE SCANNING

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

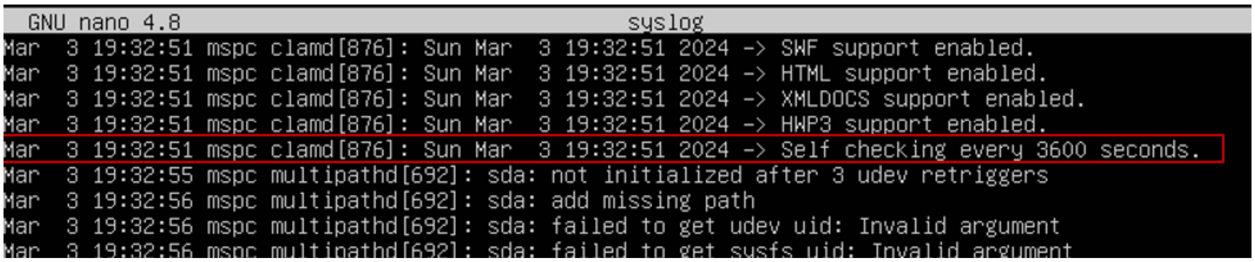
Evaluation/Evidence:

Malicious code scans are performed with the frequency of 3600 seconds (1 hour) which can be seen below



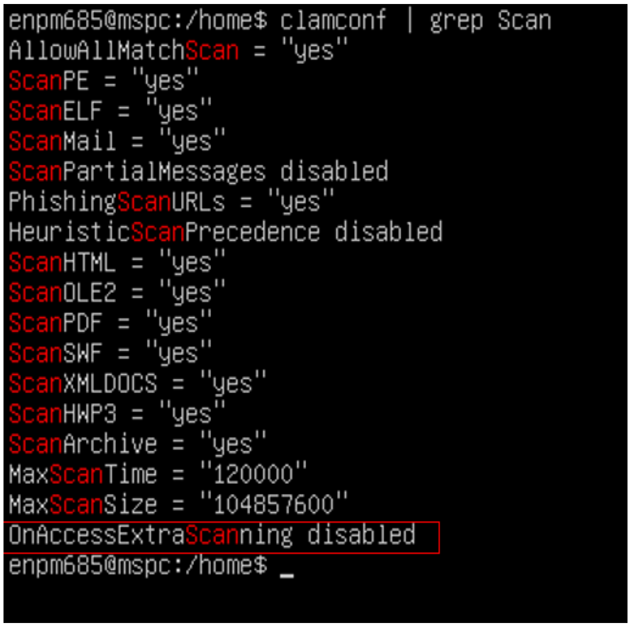
```
  GNU nano 4.8                         freshclam.log.1                        Modified
Fri Mar  1 03:58:17 2024 -> Received signal: wake up
Fri Mar  1 03:58:17 2024 -> ClamAV update process started at Fri Mar  1 03:58:17 2024
Fri Mar  1 03:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve>
Fri Mar  1 03:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9>
Fri Mar  1 03:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9>
Fri Mar  1 03:58:17 2024 -> --------------------------------------
Fri Mar  1 04:58:17 2024 -> Received signal: wake up
Fri Mar  1 04:58:17 2024 -> ClamAV update process started at Fri Mar  1 04:58:17 2024
Fri Mar  1 04:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve>
Fri Mar  1 04:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9>
Fri Mar  1 04:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9>
Fri Mar  1 04:58:17 2024 -> --------------------------------------
Fri Mar  1 05:58:17 2024 -> Received signal: wake up
Fri Mar  1 05:58:17 2024 -> ClamAV update process started at Fri Mar  1 05:58:17 2024
Fri Mar  1 05:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve>
Fri Mar  1 05:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9>
Fri Mar  1 05:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9>
Fri Mar  1 05:58:17 2024 -> --------------------------------------
Fri Mar  1 06:58:17 2024 -> Received signal: wake up
Fri Mar  1 06:58:17 2024 -> ClamAV update process started at Fri Mar  1 06:58:17 2024
Fri Mar  1 06:58:17 2024 -> daily.cld database is up-to-date (version: 27200, sigs: 2054069, f-leve>
Fri Mar  1 06:58:17 2024 -> main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 9>
Fri Mar  1 06:58:17 2024 -> bytecode.cld database is up-to-date (version: 335, sigs: 86, f-level: 9>
Fri Mar  1 06:58:17 2024 -> --------------------------------------
```

It is also important to point out that ClamAV also performs self-checks every 1 hour (3600 seconds) to ensure its integrity and reliability.



```
 GNU nano 4.8                                  syslog
Mar  3 19:32:51 mspc clamd[876]: Sun Mar  3 19:32:51 2024 -> SWF support enabled.
Mar  3 19:32:51 mspc clamd[876]: Sun Mar  3 19:32:51 2024 -> HTML support enabled.
Mar  3 19:32:51 mspc clamd[876]: Sun Mar  3 19:32:51 2024 -> XMLDOCS support enabled.
Mar  3 19:32:51 mspc clamd[876]: Sun Mar  3 19:32:51 2024 -> HWP3 support enabled.
Mar  3 19:32:51 mspc clamd[876]: Sun Mar  3 19:32:51 2024 -> Self checking every 3600 seconds.
Mar  3 19:32:55 mspc multipathd[692]: sda: not initialized after 3 udev retriggers
Mar  3 19:32:56 mspc multipathd[692]: sda: add missing path
Mar  3 19:32:56 mspc multipathd[692]: sda: failed to get udev uid: Invalid argument
Mar  3 19:32:56 mspc multipathd[692]: sda: failed to get sysfs uid: Invalid argument
```

However when we uploaded a file on the web server there was no real-time scanning performed by ClamAV. From the below figure we can see that OnAccessExtraScanning is disabled, it indicates that ClamAV is not doing any real-time scans when files are uploaded to the web server. Instead, ClamAV might be doing on-demand scans, which are initiated manually or scheduled to occur at regular intervals, rather than real time scans where files are being accessed or uploaded. which confirmed that there are no real-time scans of files from external sources.



```
enpm685@mspc:/home$ clamconf | grep Scan
AllowAllMatchScan = "yes"
ScanPE = "yes"
ScanELF = "yes"
ScanMail = "yes"
ScanPartialMessages disabled
PhishingScanURLs = "yes"
HeuristicScanPrecedence disabled
ScanHTML = "yes"
ScanOLE2 = "yes"
ScanPDF = "yes"
ScanSWF = "yes"
ScanXMLDOCS = "yes"
ScanHWP3 = "yes"
ScanArchive = "yes"
MaxScanTime = "120000"
MaxScanSize = "104857600"
OnAccessExtraScanning disabled
enpm685@mspc:/home$ _
```

Recommendations: ClamAV should be configured to scan for external files in real-time.

REFERENCES

- https://apparmor.net/
- https://www.algosec.com/resources/what-are-firewall-rules/#:~:text=Firewall%20rules%20are%20the%20major,by%20malicious%20or%20unauthorized%20traffic.
- https://www.techtarget.com/searchsecurity/definition/firewall
- https://en.wikipedia.org/wiki/ClamAV#:~:text=ClamAV%20(antivirus)%20is%20a%20free,As%20of%20version%200.97.
- https://www.opensourceforu.com/2021/07/using-clamav-to-detect-and-prevent-malware/
- An introduction to Pluggable Authentication Modules (PAM) in Linux | Enable Sysadmin (redhat.com)