

Berline Beauvais

Cohort 8/8/2023

Date : 3/17/2023

Dear Boss,

I am pleased to submit to you the information requested for the upcoming PCI audit.

PCI: Payment Card Industry.

1.0A- Inventory of systems that are in-scope

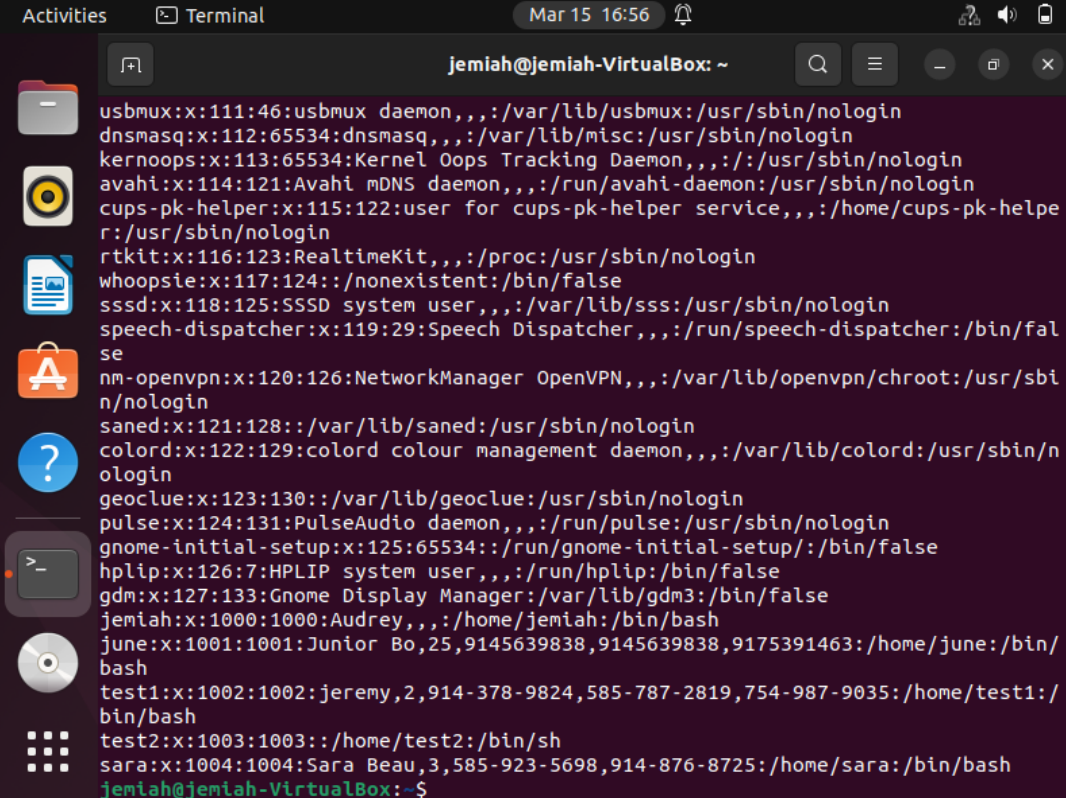
System information :

Name of System	IP address	Purpose	System owner
PCI-DS.100	10.44.21.0/24, 10.44.22.0/24	PCI Servers/suppose to be on purpose	Network Security
	10.44.20.0/24	Supporting systems	IT
	10.44.20.1, 10.44.20.2, 10.44.21.1, 10.44.21.2, 10.44.22.1, and 10.44.22.2	Firewalls	Network Security
	10.44.20.3, 10.44.20.4, 10.44.21.3, 10.44.21.4, 10.44.22.3, and 10.44.22.4	Load Balancers	IT
	None	WAFs	
	10.44.21.27, 10.44.21.76, 10.44.21.29, 10.44.22.73, 10.44.22.103	Databases	Cloud & DevOps

	10.44.21.105, 10.44.21.106, 10.44.21.107, 10.44.22.211, 10.44.22.187, and 10.44.22.53	Webservers	Web Development
	10.44.21.17, 10.44.21.107, 10.44.22.17, and 10.44.22.107	Domain controllers	Network
	10.44.21.18, 10.44.21.19, 10.44.21.20, 10.44.21.88, 10.44.21.91, 10.44.22.224, 10.44.22.244, 10.44.22.92, 10.44.22.123, 10.44.22.22, 10.44.22.82, 10.44.22.90, 10.44.22.190, and 10.44.22.197	Other systems (NTP, jump hosts, backup systems, AV, etc.)	IT

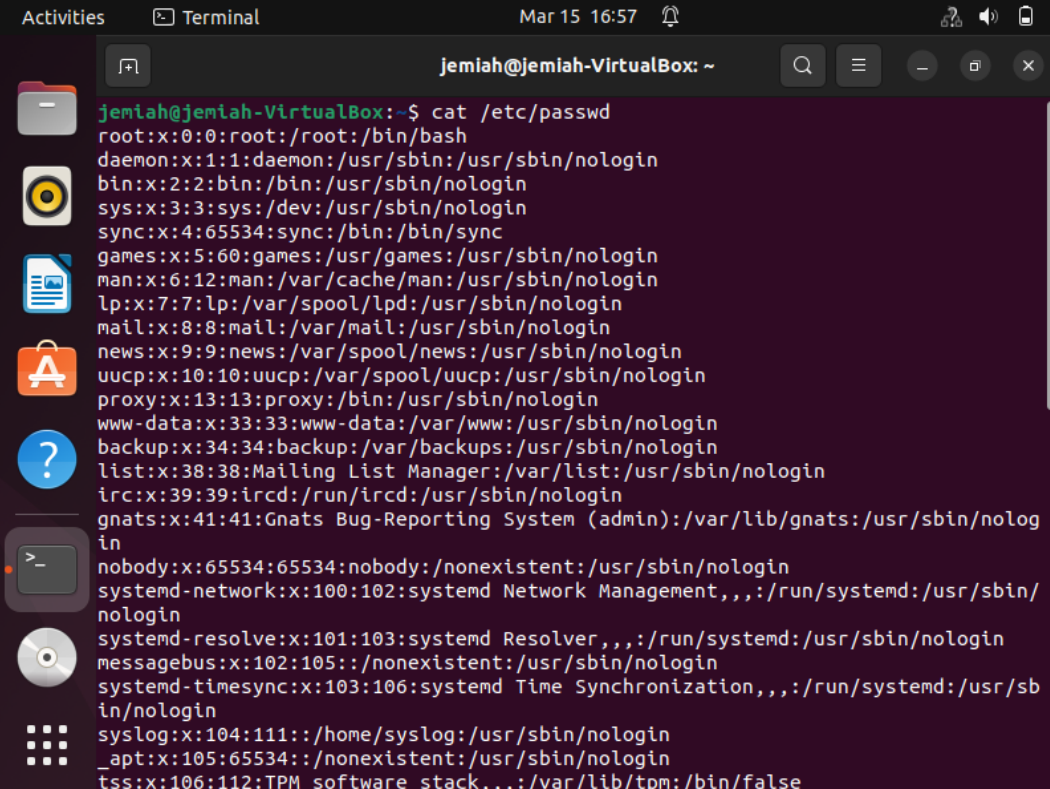
1.0B- Evidence of users on in-scope systems

Screenshot showing users on the system:



A terminal window titled 'jemiah@jemiah-VirtualBox: ~' showing a list of system users. The users are listed in a single column, each on a new line. The list includes: usbmux, dnsmasq, kernoops, avahi, cups-pk-helper, rtkit, whoopsie, sssd, speech-dispatcher, nm-openvpn, saned, colord, geoclue, pulse, gnome-initial-setup, hplip, gdm, jemiah, june, test1, test2, sara, and jemiah. Each entry shows the username, UID, GID, and home directory or shell path.

```
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helpe
r:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124:./nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/fal
se
nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbi
n/nologin
saned:x:121:128:./var/lib/saned:/usr/sbin/nologin
colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/n
ologin
geoclue:x:123:130:./var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534:./run/gnome-initial-setup:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
jemiah:x:1000:1000:Audrey,,,:/home/jemiah:/bin/bash
june:x:1001:1001:Junior Bo,25,9145639838,9145639838,9175391463:/home/june:/bin/
bash
test1:x:1002:1002:jeremy,2,914-378-9824,585-787-2819,754-987-9035:/home/test1:/
bin/bash
test2:x:1003:1003:./home/test2:/bin/sh
sara:x:1004:1004:Sara Beau,3,585-923-5698,914-876-8725:/home/sara:/bin/bash
jemiah@jemiah-VirtualBox:~$
```



A terminal window titled 'jemiah@jemiah-VirtualBox: ~' showing a list of system users. The users are listed in a single column, each on a new line. The list includes: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, systemd-network, systemd-resolve, messagebus, systemd-timesync, syslog, _apt, and tss. Each entry shows the username, UID, GID, and home directory or shell path.

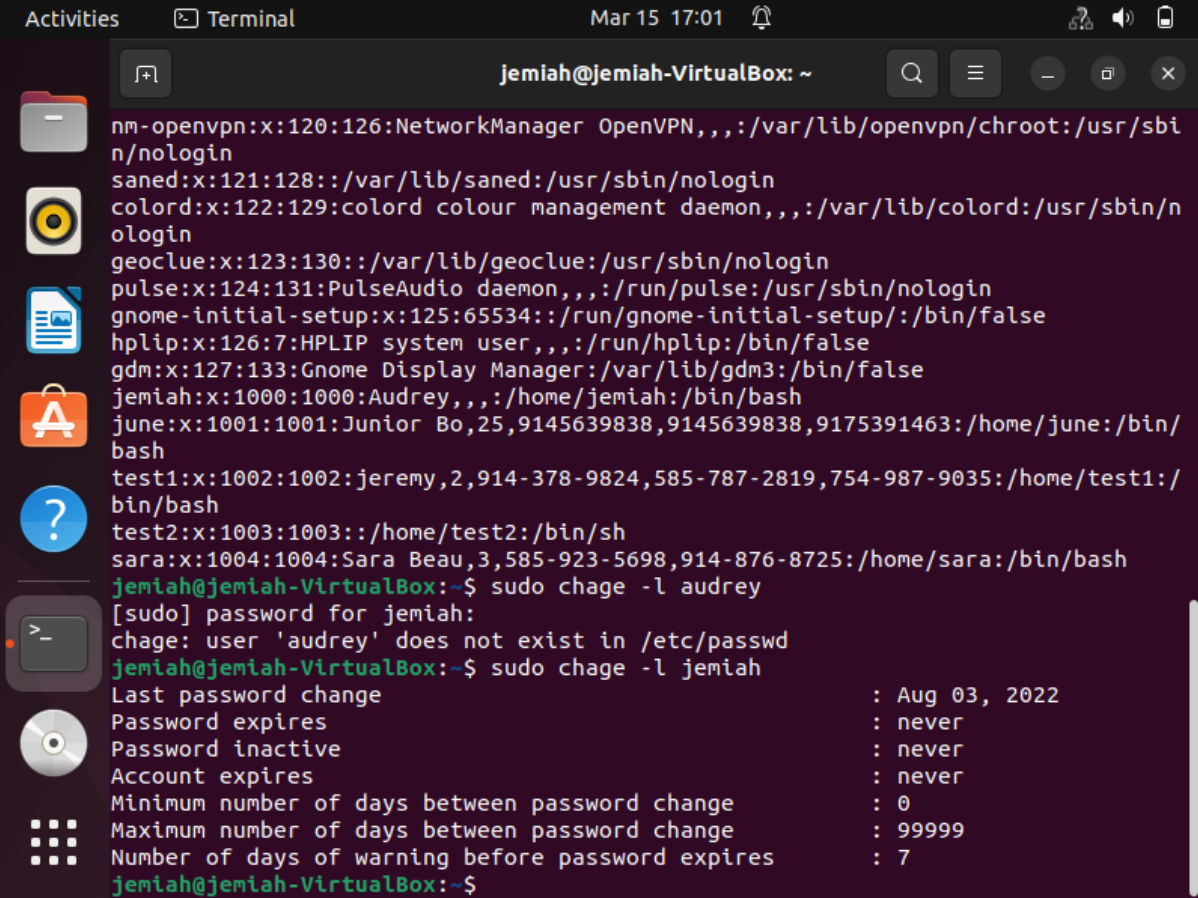
```
jemiah@jemiah-VirtualBox:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nolog
in
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
messagebus:x:102:105:./nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sb
in/nologin
syslog:x:104:111:./home/syslog:/usr/sbin/nologin
_apt:x:105:65534:./nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
```

Activities Terminal Mar 15 16:58

jemiah@jemiah-VirtualBox: ~

```
syslog:x:104:111::/home/syslog:/usr/sbin/nologin
apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uidd:x:107:115::/run/uidd:/usr/sbin/nologin
systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false
sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:121:128::/var/lib/saned:/usr/sbin/nologin
colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:123:130::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
```

1.0C-Evidence for password policy for in-scope systems



The screenshot shows a terminal window titled "jemiah@jemiah-VirtualBox: ~" with a search bar and window controls. The terminal displays the output of the `cat /etc/passwd` command, listing system users and regular users. It then shows the output of `sudo chage -l jemiah`, which displays the password policy for the 'jemiah' user.

```
nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:121:128:/:/var/lib/saned:/usr/sbin/nologin
colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:123:130:/:/var/lib/geoclue:/usr/sbin/nologin
pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534:/:/run/gnome-initial-setup:/bin/false
hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:127:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
jemiah:x:1000:1000:Audrey,,,:/home/jemiah:/bin/bash
june:x:1001:1001:Junior Bo,25,9145639838,9145639838,9175391463:/home/june:/bin/bash
test1:x:1002:1002:jeremy,2,914-378-9824,585-787-2819,754-987-9035:/home/test1:/bin/bash
test2:x:1003:1003:/:/home/test2:/bin/sh
sara:x:1004:1004:Sara Beau,3,585-923-5698,914-876-8725:/home/sara:/bin/bash
jemiah@jemiah-VirtualBox:~$ sudo chage -l audrey
[sudo] password for jemiah:
chage: user 'audrey' does not exist in /etc/passwd
jemiah@jemiah-VirtualBox:~$ sudo chage -l jemiah
Last password change                : Aug 03, 2022
Password expires                     : never
Password inactive                    : never
Account expires                     : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
jemiah@jemiah-VirtualBox:~$
```

