Week 7 : Security Audit and System Evaluation

A comprehensive security assessment was conducted to evaluate the overall security posture of the system.

1. Security Scanning with Lynis

Command:

```
sudo lynis audit system
```

- **Explanation:**
  Performs a full security audit of the system, checking for vulnerabilities, insecure configurations, and missing security controls.

```
liveuser@localhost-live:~$ sudo lynis audit system

[ Lynis 3.1.6 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2025, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.1.6
  Operating system:          Linux
  Operating system name:     Fedora Linux
  Operating system version:  43
  End-of-life:               UNKNOWN
  Kernel version:            6.17.1
  Hardware platform:         x86_64
  Hostname:                  localhost-live
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
```

```
vboxuser@ubuntu:~$ sudo lynis audit system
[sudo] password for vboxuser:

[ Lynis 3.0.9 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2021, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           3.0.9
  Operating system:          Linux
  Operating system name:     Ubuntu
  Operating system version:  24.04
  Kernel version:            6.14.0
  Hardware platform:         x86_64
  Hostname:                  ubuntu
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
```

2. Network Security Assessment with Nmap

Command:

```
nmap -sS localhost
```

- **Explanation:**
  Scans the local system to identify open ports and active services that could be exposed to network attacks.

```
liveuser@localhost-live:~$ sudo nmap -sS localhost
Starting Nmap 7.92 ( https://nmap.org ) at 2025-12-14 23:54 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000015s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

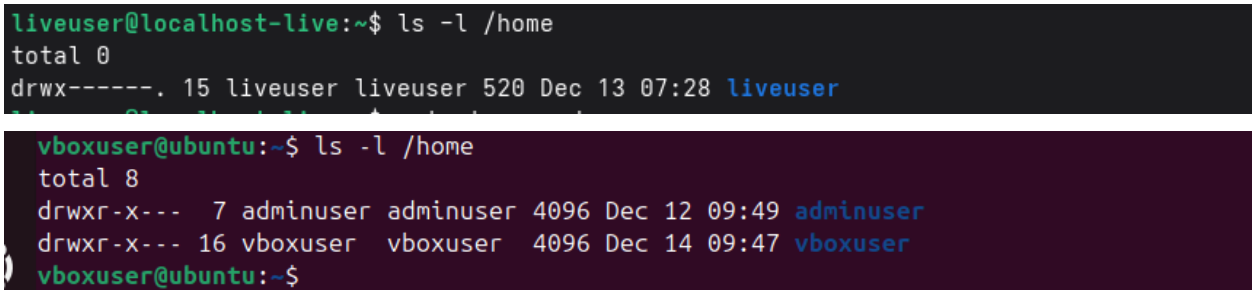
```
vboxuser@ubuntu:~$ sudo nmap -sS localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-14 23:40 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000028s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

3. Access Control Verification

Command:

```
ls -l /home
```

- **Explanation:**
  Displays file and directory permissions to verify correct access rights for users.



Command:

```
getent passwd
```

- **Explanation:**
  Lists all user accounts to ensure only authorised users exist on the system.

```
liveuser@localhost-live:~$ getent passwd
root:x:0:0:Super User:/root:/bin/bash
bin:x:1:1:bin:/bin:/usr/sbin/nologin
daemon:x:2:2:daemon:/sbin:/usr/sbin/nologin
adm:x:3:4:adm:/var/adm:/usr/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/usr/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/usr/sbin/nologin
operator:x:11:0:operator:/root:/usr/sbin/nologin
games:x:12:100:games:/usr/games:/usr/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/usr/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/usr/sbin/nologin
dbus:x:81:81:System Message Bus:/:/usr/sbin/nologin
tss:x:59:59:Account used for TPM access:/:/usr/sbin/nologin
systemd-oom:x:999:999:systemd Userspace OOM Killer:/:/usr/sbir
```

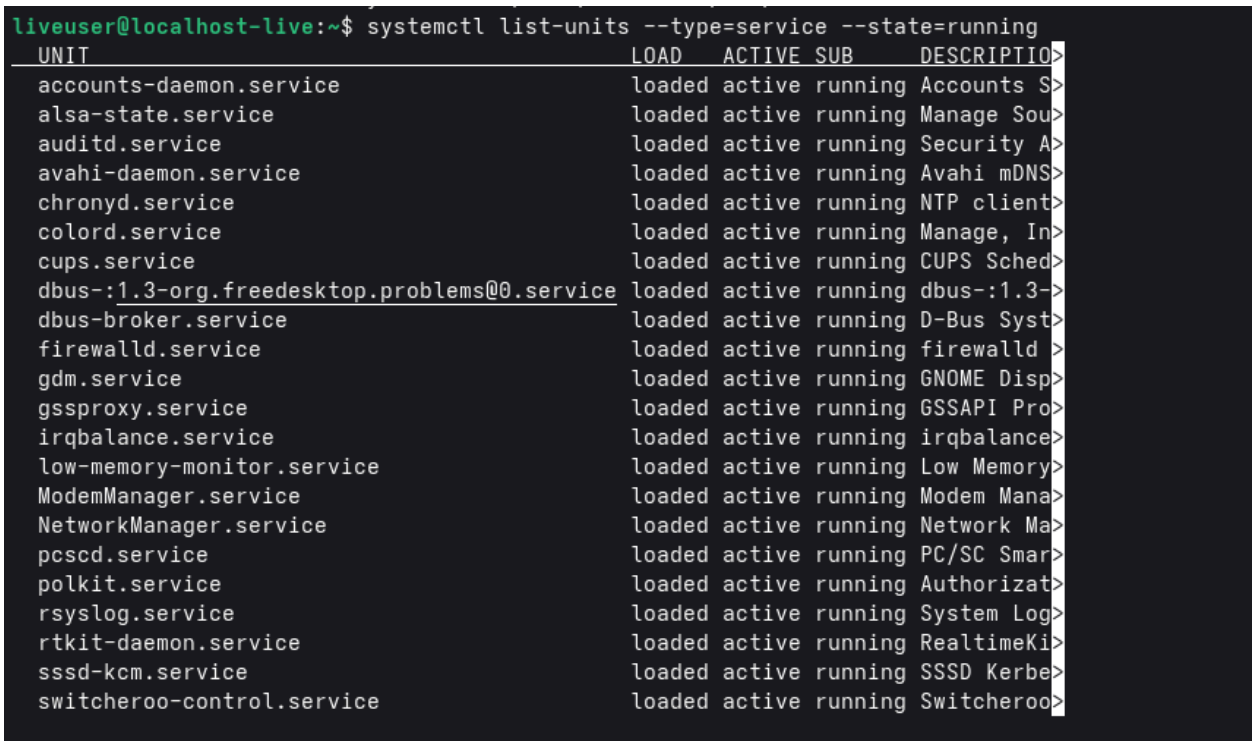
```
vboxuser@ubuntu:~$ getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
```

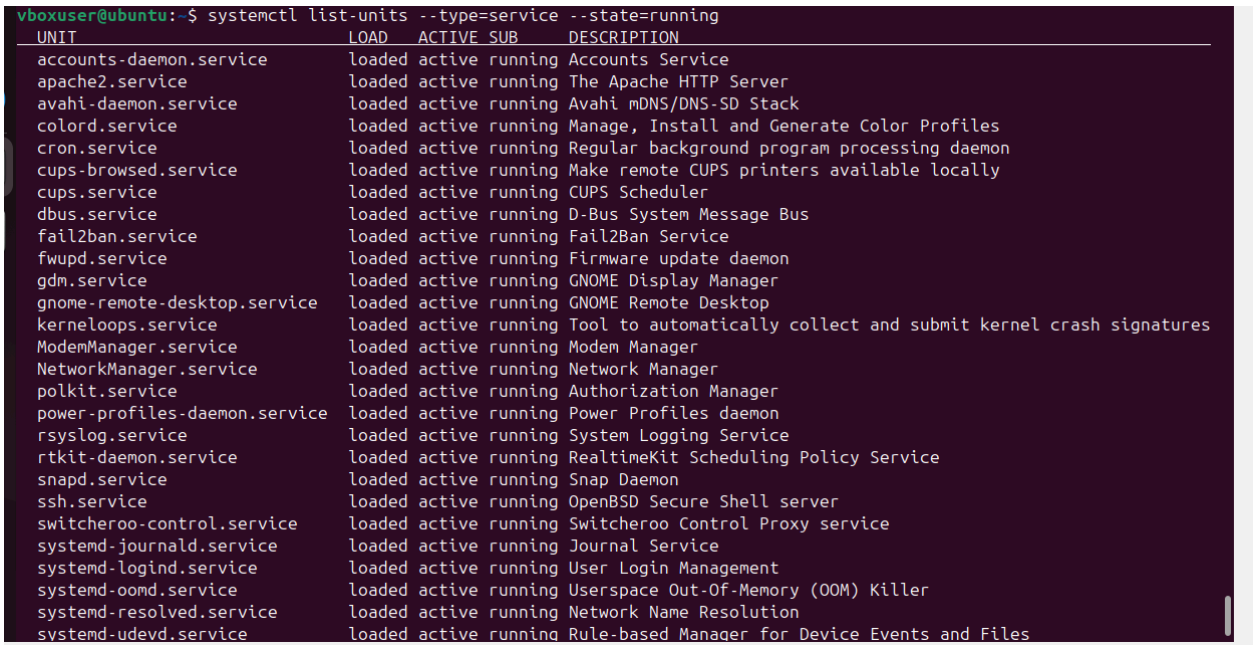
4. Service Audit (Justifying Running Services)

Command:

```
systemctl list-units --type=service --state=running
```

- **Explanation:**
  Lists all currently running services to verify that each service is required and justified.



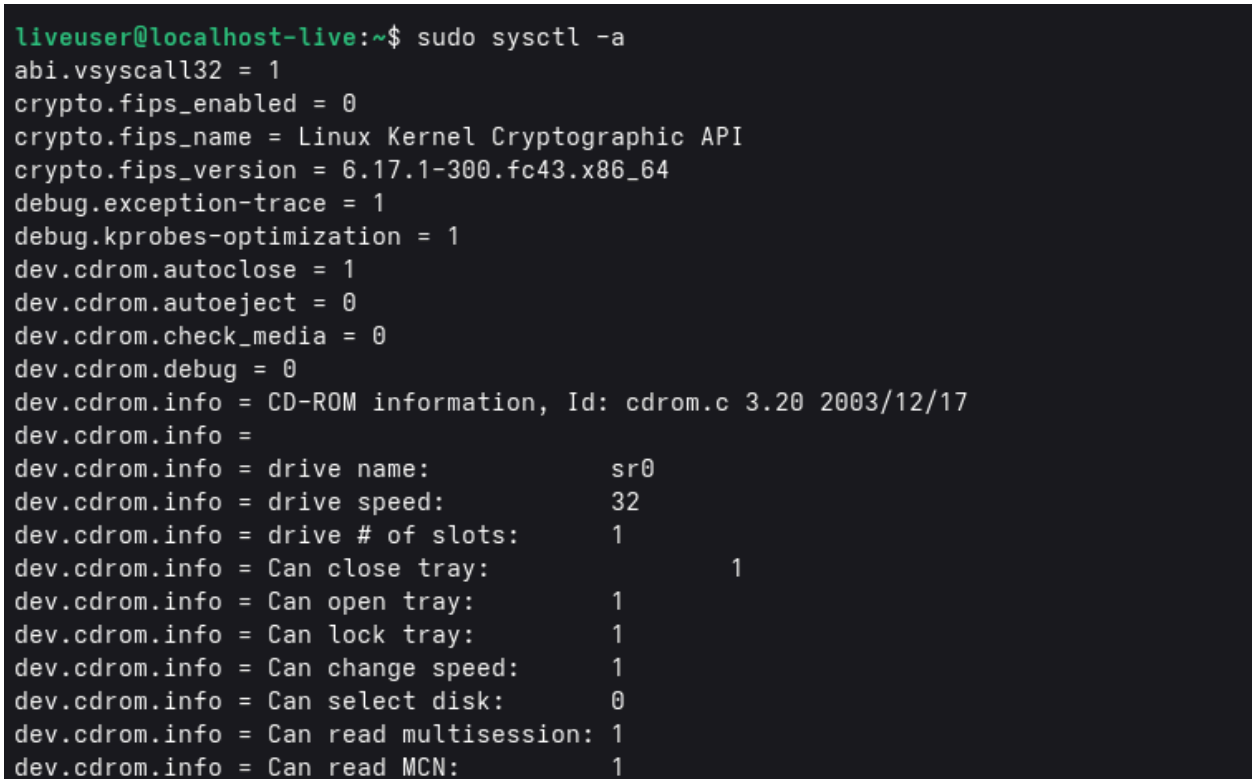
- 

5. System Configuration Review

Command:

```
sudo sysctl -a
```

- **Explanation:**
  Displays kernel configuration parameters to review system-level security settings.



```
vboxuser@ubuntu:~$ sudo sysctl -a
abi.vsyscall32 = 1
debug.exception-trace = 1
debug.kprobes-optimization = 1
dev.cdrom.autoclose = 1
dev.cdrom.autoeject = 0
dev.cdrom.check_media = 0
dev.cdrom.debug = 0
dev.cdrom.info = CD-ROM information, Id: cdrom.c 3.20 2003/12/17
dev.cdrom.info =
dev.cdrom.info = drive name:            sr0
dev.cdrom.info = drive speed:           32
dev.cdrom.info = drive # of slots:      1
dev.cdrom.info = Can close tray:                1
dev.cdrom.info = Can open tray:         1
dev.cdrom.info = Can lock tray:         1
dev.cdrom.info = Can change speed:      1
dev.cdrom.info = Can select disk:       0
dev.cdrom.info = Can read multisession: 1
dev.cdrom.info = Can read MCN:          1
dev.cdrom.info = Reports media changed: 1
dev.cdrom.info = Can play audio:                1
dev.cdrom.info = Can write CD-R:                0
dev.cdrom.info = Can write CD-RW:       0
dev.cdrom.info = Can read DVD:          1
dev.cdrom.info = Can write DVD-R:       0
```