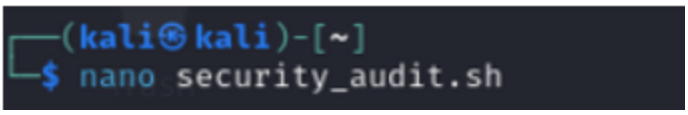
TASK 5:

Automated Security Auditing & Scripting Exploit:

Setup:

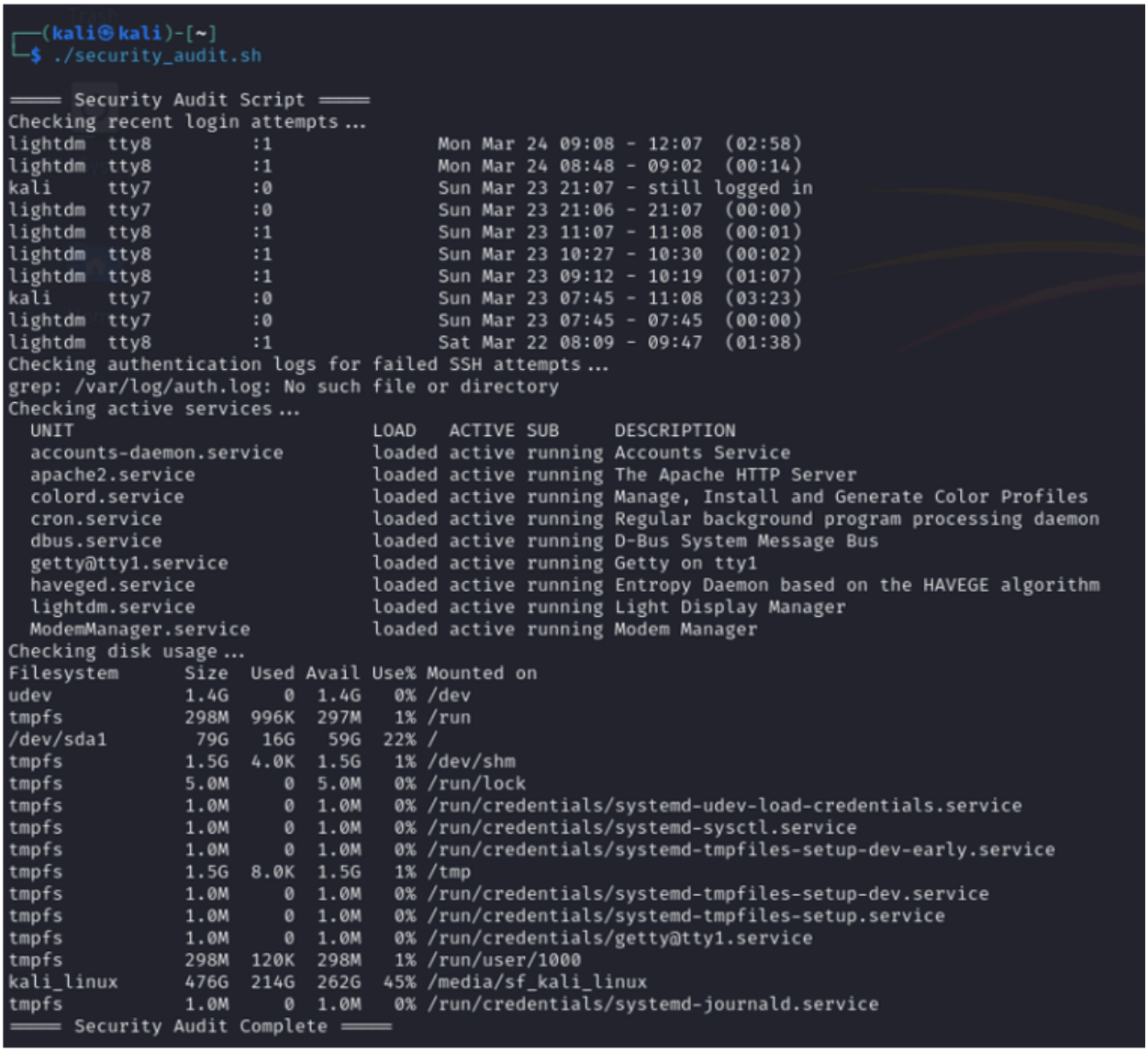
1. Open nano editor and create a new file: after creating a file save it.




```
 GNU nano 8.2
#!/bin/bash

echo "==== Security Audit Script ===="

# 1. Check user login attempts
echo "Checking recent login attempts..."
last | head -n 10  # Show last 10 logins

echo "Checking authentication logs for failed SSH attempts..."
grep "Failed password" /var/log/auth.log | tail -n 5  # Show last 5 failed attempts

# 2. Detect running services
echo "Checking active services..."
systemctl list-units --type=service --state=running | head -n 10  # Show first 10 running service

# 3. Monitor disk usage
echo "Checking disk usage..."
df -h  # Show disk usage in human-readable format

echo "==== Security Audit Complete ===="
```

Exploitation:

1. Monitor login: It lists logins and failed SSH attempts.
2. Check running service: Displays currently active service.
3. Monitor disk usage: Storage used and available



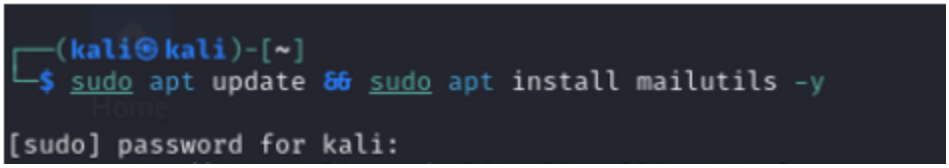
```
┌──(kali㉿kali)-[~]
└─$ ./security_audit.sh

==== Security Audit Script ====
Checking recent login attempts...
lightdm  tty8         :1               Mon Mar 24 09:08 - 12:07  (02:58)
lightdm  tty8         :1               Mon Mar 24 08:48 - 09:02  (00:14)
kali     tty7         :0               Sun Mar 23 21:07 - still logged in
lightdm  tty7         :0               Sun Mar 23 21:06 - 21:07  (00:00)
lightdm  tty8         :1               Sun Mar 23 11:07 - 11:08  (00:01)
lightdm  tty8         :1               Sun Mar 23 10:27 - 10:30  (00:02)
lightdm  tty8         :1               Sun Mar 23 09:12 - 10:19  (01:07)
kali     tty7         :0               Sun Mar 23 07:45 - 11:08  (03:23)
lightdm  tty7         :0               Sun Mar 23 07:45 - 07:45  (00:00)
lightdm  tty8         :1               Sat Mar 22 08:09 - 09:47  (01:38)
Checking authentication logs for failed SSH attempts...
grep: /var/log/auth.log: No such file or directory
Checking active services...
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service       loaded active running Accounts Service
  apache2.service               loaded active running The Apache HTTP Server
  colord.service                loaded active running Manage, Install and Generate Color Profiles
  cron.service                  loaded active running Regular background program processing daemon
  dbus.service                  loaded active running D-Bus System Message Bus
  getty@tty1.service            loaded active running Getty on tty1
  haveged.service               loaded active running Entropy Daemon based on the HAVEGE algorithm
  lightdm.service               loaded active running Light Display Manager
  ModemManager.service          loaded active running Modem Manager
Checking disk usage...
Filesystem      Size  Used Avail Use% Mounted on
udev            1.4G     0  1.4G   0% /dev
tmpfs           298M  996K  297M   1% /run
/dev/sda1        79G   16G   59G  22% /
tmpfs           1.5G  4.0K  1.5G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.5G  8.0K  1.5G   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           298M  120K  298M   1% /run/user/1000
kali_linux      476G  214G  262G  45% /media/sf_kali_linux
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
==== Security Audit Complete ====
```

```
┌──(kali㉿kali)-[~]
└─$ bash security_audit.sh

═══ Security Audit Script ═══
Checking recent login attempts...
lightdm  tty8         :1               Mon Mar 24 09:08 - 12:07  (02:58)
lightdm  tty8         :1               Mon Mar 24 08:48 - 09:02  (00:14)
kali     tty7         :0               Sun Mar 23 21:07 - still logged in
lightdm  tty7         :0               Sun Mar 23 21:06 - 21:07  (00:00)
lightdm  tty8         :1               Sun Mar 23 11:07 - 11:08  (00:01)
lightdm  tty8         :1               Sun Mar 23 10:27 - 10:30  (00:02)
lightdm  tty8         :1               Sun Mar 23 09:12 - 10:19  (01:07)
kali     tty7         :0               Sun Mar 23 07:45 - 11:08  (03:23)
lightdm  tty7         :0               Sun Mar 23 07:45 - 07:45  (00:00)
lightdm  tty8         :1               Sat Mar 22 08:09 - 09:47  (01:38)
Checking authentication logs for failed SSH attempts...
grep: /var/log/auth.log: No such file or directory
Checking active services...
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service       loaded active running Accounts Service
  apache2.service               loaded active running The Apache HTTP Server
  colord.service                loaded active running Manage, Install and Generate Color Profiles
  cron.service                  loaded active running Regular background program processing daemon
  dbus.service                  loaded active running D-Bus System Message Bus
  getty@tty1.service            loaded active running Getty on tty1
  haveged.service               loaded active running Entropy Daemon based on the HAVEGE algorithm
  lightdm.service               loaded active running Light Display Manager
  ModemManager.service          loaded active running Modem Manager
Checking disk usage...
Filesystem      Size  Used Avail Use% Mounted on
udev            1.4G     0  1.4G   0% /dev
tmpfs           298M  988K  297M   1% /run
/dev/sda1        79G   16G   59G  22% /
tmpfs           1.5G  4.0K  1.5G   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.5G   96K  1.5G   1% /tmp
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs           1.0M     0  1.0M   0% /run/credentials/getty@tty1.service
tmpfs           298M  120K  298M   1% /run/user/1000
kali_linux      476G  214G  262G  45% /media/sf_kali_linux
tmpfs           1.0M     0  1.0M   0% /run/credentials/systemd-journald.service
═══ Security Audit Complete ═══
```

Mitigation:

```
┌──(kali㉿kali)-[~]
└─$ sudo crontab -e

[sudo] password for kali:
no crontab for root - using an empty one
Select an editor.  To change later, run select-editor again.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny

Choose 1-3 [1]: 1
No modification made
```

send email alerts for SSH attacks for enhanced security, implementation of email alerts for unauthorized SSH attempts. First , ensure mailutils is installed using the command.



by this potential threats can be detected and mitigated properly.