

PoC Task 5: Automated Security Auditing & Scripting

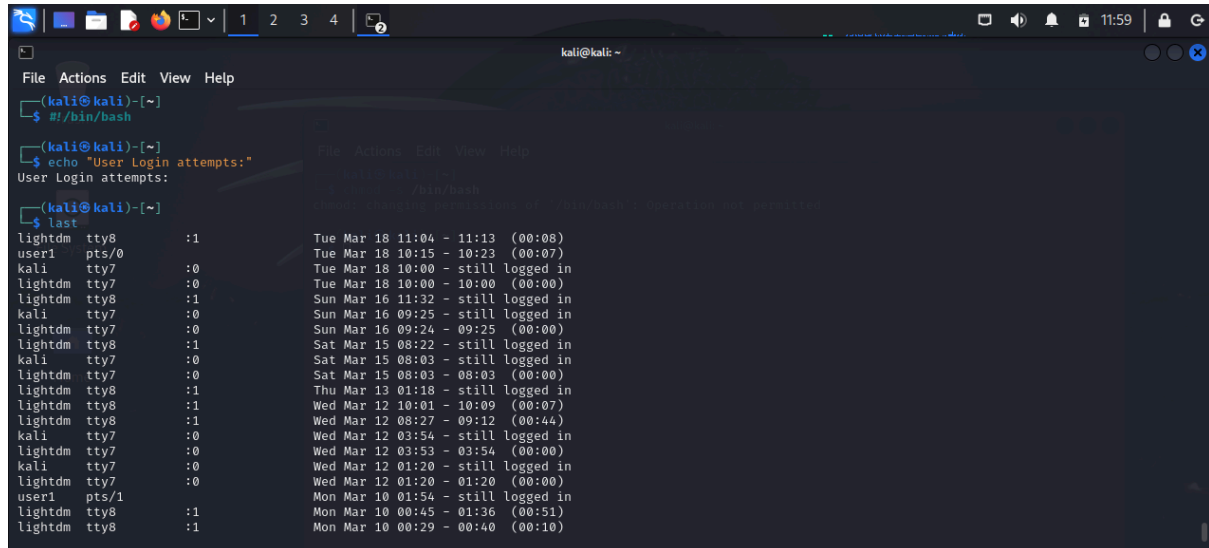
1) Setup

1.1) Write a Bash script for security auditing:

```
#!/bin/bash
```

```
echo "User login attempts:"
```

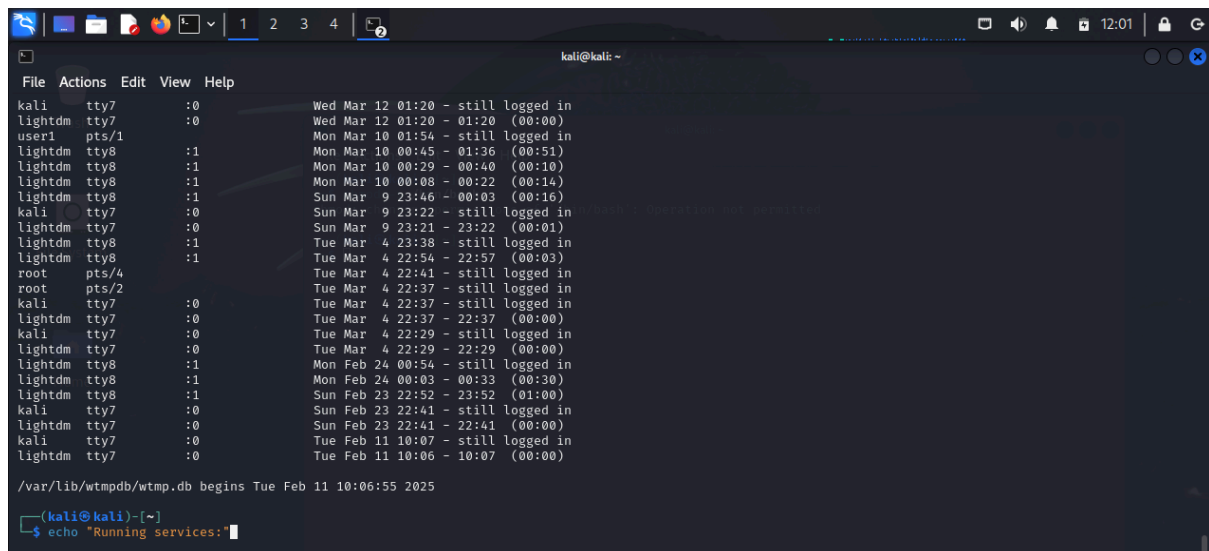
```
last
```



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ #!/bin/bash  
(kali@kali)-[~]  
$ echo "User login attempts:"  
User login attempts:  
(kali@kali)-[~]  
$ last  
lightdm tty8 :1 Tue Mar 18 11:04 - 11:13 (00:08)  
user1 pts/0 :0 Tue Mar 18 10:15 - 10:23 (00:07)  
kali tty7 :0 Tue Mar 18 10:00 - still logged in  
lightdm tty7 :0 Tue Mar 18 10:00 - 10:00 (00:00)  
lightdm tty8 :1 Sun Mar 16 11:32 - still logged in  
kali tty7 :0 Sun Mar 16 09:25 - still logged in  
lightdm tty7 :0 Sun Mar 16 09:24 - 09:25 (00:00)  
lightdm tty8 :1 Sat Mar 15 08:22 - still logged in  
kali tty7 :0 Sat Mar 15 08:03 - still logged in  
lightdm tty7 :0 Sat Mar 15 08:03 - 08:03 (00:00)  
lightdm tty8 :1 Thu Mar 13 01:18 - still logged in  
lightdm tty8 :1 Wed Mar 12 10:01 - 10:09 (00:07)  
lightdm tty8 :1 Wed Mar 12 08:27 - 09:12 (00:44)  
kali tty7 :0 Wed Mar 12 03:54 - still logged in  
lightdm tty7 :0 Wed Mar 12 03:53 - 03:54 (00:00)  
kali tty7 :0 Wed Mar 12 01:20 - still logged in  
lightdm tty7 :0 Wed Mar 12 01:20 - 01:20 (00:00)  
user1 pts/1 Mon Mar 10 01:54 - still logged in  
lightdm tty8 :1 Mon Mar 10 00:45 - 01:36 (00:51)  
lightdm tty8 :1 Mon Mar 10 00:29 - 00:40 (00:10)  
lightdm tty8 :1 Mon Mar 10 00:08 - 00:22 (00:14)  
lightdm tty8 :1 Sun Mar 9 23:46 - 00:03 (00:16)  
kali tty7 :0 Sun Mar 9 23:22 - still logged in  
lightdm tty7 :0 Sun Mar 9 23:21 - 23:22 (00:01)  
lightdm tty8 :1 Tue Mar 4 23:38 - still logged in  
lightdm tty8 :1 Tue Mar 4 22:54 - 22:57 (00:03)  
root pts/4 Tue Mar 4 22:41 - still logged in  
root pts/2 Tue Mar 4 22:37 - still logged in  
kali tty7 :0 Tue Mar 4 22:37 - still logged in  
lightdm tty7 :0 Tue Mar 4 22:37 - 22:37 (00:00)  
kali tty7 :0 Tue Mar 4 22:29 - still logged in  
lightdm tty7 :0 Tue Mar 4 22:29 - 22:29 (00:00)  
lightdm tty8 :1 Mon Feb 24 00:54 - still logged in  
lightdm tty8 :1 Mon Feb 24 00:03 - 00:33 (00:30)  
lightdm tty8 :1 Sun Feb 23 22:52 - 23:52 (01:00)  
kali tty7 :0 Sun Feb 23 22:41 - still logged in  
lightdm tty7 :0 Sun Feb 23 22:41 - 22:41 (00:00)  
kali tty7 :0 Tue Feb 11 10:07 - still logged in  
lightdm tty7 :0 Tue Feb 11 10:06 - 10:07 (00:00)  
  
/var/lib/wtmpdb/wtmp.db begins Tue Feb 11 10:06:55 2025  
(kali@kali)-[~]  
$ echo "Running services:"
```

```
echo "Running services:"
```

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



```
kali@kali: ~  
File Actions Edit View Help  
kali tty7 :0 Wed Mar 12 01:20 - still logged in  
lightdm tty7 :0 Wed Mar 12 01:20 - 01:20 (00:00)  
user1 pts/1 Mon Mar 10 01:54 - still logged in  
lightdm tty8 :1 Mon Mar 10 00:45 - 01:36 (00:51)  
lightdm tty8 :1 Mon Mar 10 00:29 - 00:40 (00:10)  
lightdm tty8 :1 Mon Mar 10 00:08 - 00:22 (00:14)  
lightdm tty8 :1 Sun Mar 9 23:46 - 00:03 (00:16)  
kali tty7 :0 Sun Mar 9 23:22 - still logged in  
lightdm tty7 :0 Sun Mar 9 23:21 - 23:22 (00:01)  
lightdm tty8 :1 Tue Mar 4 23:38 - still logged in  
lightdm tty8 :1 Tue Mar 4 22:54 - 22:57 (00:03)  
root pts/4 Tue Mar 4 22:41 - still logged in  
root pts/2 Tue Mar 4 22:37 - still logged in  
kali tty7 :0 Tue Mar 4 22:37 - still logged in  
lightdm tty7 :0 Tue Mar 4 22:37 - 22:37 (00:00)  
kali tty7 :0 Tue Mar 4 22:29 - still logged in  
lightdm tty7 :0 Tue Mar 4 22:29 - 22:29 (00:00)  
lightdm tty8 :1 Mon Feb 24 00:54 - still logged in  
lightdm tty8 :1 Mon Feb 24 00:03 - 00:33 (00:30)  
lightdm tty8 :1 Sun Feb 23 22:52 - 23:52 (01:00)  
kali tty7 :0 Sun Feb 23 22:41 - still logged in  
lightdm tty7 :0 Sun Feb 23 22:41 - 22:41 (00:00)  
kali tty7 :0 Tue Feb 11 10:07 - still logged in  
lightdm tty7 :0 Tue Feb 11 10:06 - 10:07 (00:00)  
  
/var/lib/wtmpdb/wtmp.db begins Tue Feb 11 10:06:55 2025  
(kali@kali)-[~]  
$ echo "Running services:"
```

```
echo "Disk usage:"
```

```
df -h
```

```
(kali@kali)-[~]
$ echo "Disk usage:"
Disk usage:

(kali@kali)-[~]
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            925M    0  925M   0% /dev
tmpfs           198M  980K  197M   1% /run
/dev/sda1       79G   16G   60G  21% /
tmpfs           987M   4.0K  987M   1% /dev/shm
tmpfs           5.0M    0   5.0M   0% /run/lock
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-journald.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           987M   1.3M  986M   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           198M  120K  198M   1% /run/user/1000

(kali@kali)-[~]
$ echo "Disk usage:"
```

1.2) Save as security_audit.sh and make executable:
chmod +x security_audit.sh

```
(kali@kali)-[~]
$ nano security_audit.sh

(kali@kali)-[~]
$ chmod +x security_audit.sh

(kali@kali)-[~]
$ ./security_audit.sh
User login attempts:
lightdm tty8 :1 Tue Mar 18 11:04 - 11:13 (00:08)
user1 pts/0 Tue Mar 18 10:15 - 10:23 (00:07)
kali tty7 :0 Tue Mar 18 10:00 - still logged in
lightdm tty7 :0 Tue Mar 18 10:00 - 10:00 (00:00)
lightdm tty8 :1 Sun Mar 16 11:32 - still logged in
kali tty7 :0 Sun Mar 16 09:25 - still logged in
lightdm tty7 :0 Sun Mar 16 09:24 - 09:25 (00:00)
lightdm tty8 :1 Sat Mar 15 08:22 - still logged in
kali tty7 :0 Sat Mar 15 08:03 - still logged in
lightdm tty7 :0 Sat Mar 15 08:03 - 08:03 (00:00)
lightdm tty8 :1 Thu Mar 13 01:18 - still logged in
lightdm tty8 :1 Wed Mar 12 10:01 - 10:09 (00:07)
lightdm tty8 :1 Wed Mar 12 08:27 - 09:12 (00:44)
kali tty7 :0 Wed Mar 12 03:54 - still logged in
lightdm tty7 :0 Wed Mar 12 03:53 - 03:54 (00:00)
kali tty7 :0 Wed Mar 12 01:20 - still logged in
lightdm tty7 :0 Wed Mar 12 01:20 - 01:20 (00:00)
```

2) Exploit

Run the script and analyze security weaknesses:

./security_audit.sh

```
kali@kali: ~
File Actions Edit View Help
UNIT                                LOAD    ACTIVE SUB    DESCRIPTION
accounts-daemon.service            loaded active running Accounts Service
colord.service                      loaded active running Manage, Install and Generate Color Profiles
console-setup.service              loaded active exited Set console font and keymap
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
ifupdown-pre.service               loaded active exited Helper to synchronize boot up for ifupdown
keyboard-setup.service              loaded active exited Set the console keyboard layout
kmod-static-nodes.service           loaded active exited Create List of Static Device Nodes
lightdm.service                    loaded active running Light Display Manager
ModemManager.service               loaded active running Modem Manager
networking.service                 loaded active exited Raise network interfaces
NetworkManager-wait-online.service loaded active exited Network Manager Wait Online
NetworkManager.service             loaded active running Network Manager
plymouth-quit-wait.service          loaded active exited Hold until boot process finishes up
plymouth-read-write.service         loaded active exited Tell Plymouth To Write Out Runtime Data
plymouth-start.service              loaded active exited Show Plymouth Boot Screen
polkit.service                     loaded active running Authorization Manager
rpc-statd-notify.service            loaded active exited Notify NFS peers of a restart
rtkit-daemon.service               loaded active running RealtimeKit Scheduling Policy Service
ssh.service                        loaded active running OpenSSH Secure Shell server
systemd-binfmt.service             loaded active exited Set Up Additional Binary Formats
systemd-journal-flush.service       loaded active exited Flush Journal to Persistent Storage
systemd-journald.service            loaded active running Journal Service
systemd-logind.service              loaded active running User Login Management
systemd-modules-load.service        loaded active exited Load Kernel Modules

lines 1-28
```

```

kali@kali: ~
File Actions Edit View Help
systemd-binfmt.service loaded active exited Set Up Additional Binary Formats
systemd-journal-flush.service loaded active exited Flush Journal to Persistent Storage
systemd-journald.service loaded active running Journal Service
systemd-logind.service loaded active running User Login Management
systemd-modules-load.service loaded active exited Load Kernel Modules
systemd-random-seed.service loaded active exited Load/Save OS Random Seed
systemd-remount-fs.service loaded active exited Remount Root and Kernel File Systems
systemd-sysctl.service loaded active exited Apply Kernel Variables
systemd-tmpfiles-setup-dev-early.service loaded active exited Create Static Device Nodes in /dev gracefully
systemd-tmpfiles-setup-dev.service loaded active exited Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service loaded active exited Create System Files and Directories
systemd-udev-load-credentials.service loaded active exited Load udev Rules from Credentials
systemd-udev-trigger.service loaded active exited Coldplug All udev Devices
systemd-udevd.service loaded active running Rule-based Manager for Device Events and Files
systemd-update-utmp.service loaded active exited Record System Boot/Shutdown in UTMP
systemd-user-sessions.service loaded active exited Permit User Sessions
udisks2.service loaded active running Disk Manager
upower.service loaded active running Daemon for power management
user-runtime-dir@1000.service loaded active exited User Runtime Directory /run/user/1000
user@1000.service loaded active running User Manager for UID 1000
virtualbox-guest-utils.service loaded active running Virtualbox guest utils

Legend: LOAD → Reflects whether the unit definition was properly loaded.
ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
SUB → The low-level unit activation state, values depend on unit type.

43 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
lines 24-51/51 (END)

```

3) Mitigation

3.1) Automate via cron:

crontab -e

Add:

o o * * * /path/to/security_audit.sh > /var/log/security_audit.log

```

kali@kali: ~
File Actions Edit View Help
upower.service loaded active running Daemon for power managemen
user-runtime-dir@1000.service loaded active exited User Runtime Directory /ru
user@1000.service loaded active running User Manager for UID 1000
virtualbox-guest-utils.service loaded active running Virtualbox guest utils

Legend: LOAD → Reflects whether the unit definition was properly loaded.
ACTIVE → The high-level unit activation state, i.e. generalization of SUB.
SUB → The low-level unit activation state, values depend on unit type.

43 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.

zsh: suspended ./security_audit.sh

(kali@kali)-[~]
$ crontab -e
no crontab for kali - using an empty one
Select an editor. To change later, run select-editor again.
1. /bin/nano ← easiest
crontab: installing new crontab

(kali@kali)-[~]
$

```

3.2) Send alerts for failed SSH logins:

tail -f /var/log/auth.log | grep "Failed password"