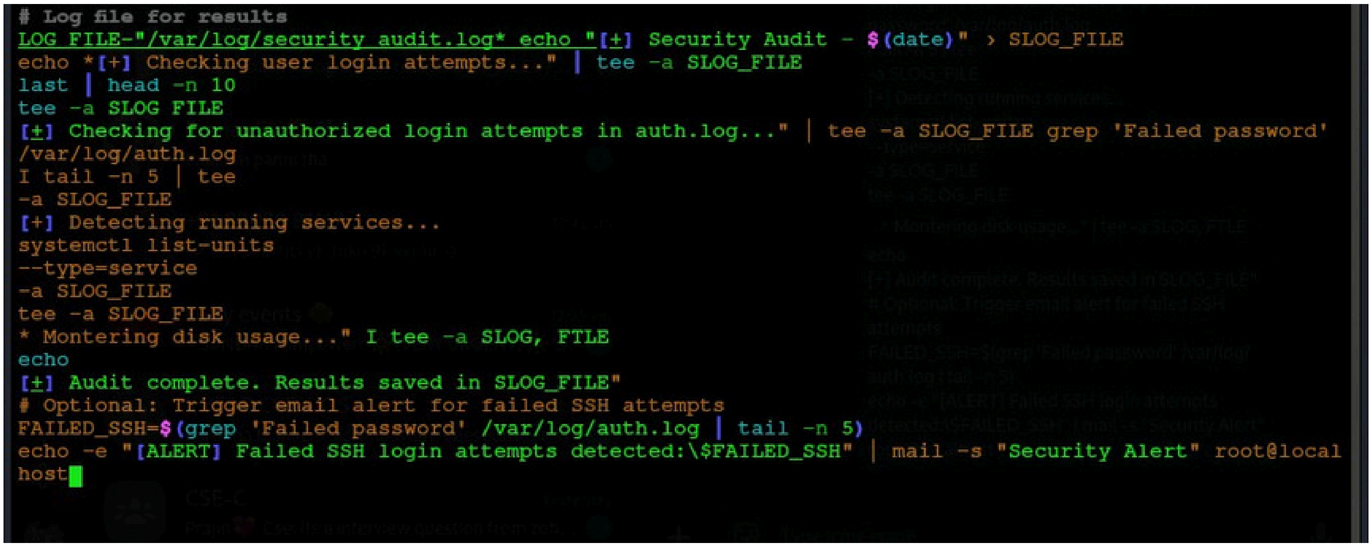
Task 5

Automated Security Auditing & Scripting

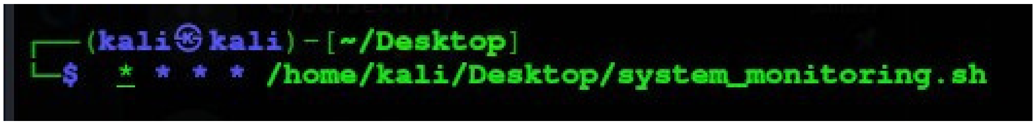
Exploit



```
# Log file for results
LOG FILE-"/var/log/security audit.log* echo "[+] Security Audit - $(date)" › SLOG_FILE
echo *[+] Checking user login attempts..." | tee -a SLOG_FILE
last | head -n 10
tee -a SLOG FILE
[+] Checking for unauthorized login attempts in auth.log..." | tee -a SLOG_FILE grep 'Failed password'
/var/log/auth.log
I tail -n 5 | tee
-a SLOG_FILE
[+] Detecting running services...
systemctl list-units
--type=service
-a SLOG_FILE
tee -a SLOG_FILE
* Montering disk usage..." I tee -a SLOG, FTLE
echo
[+] Audit complete. Results saved in SLOG_FILE"
# Optional: Trigger email alert for failed SSH attempts
FAILED_SSH=$(grep 'Failed password' /var/log/auth.log | tail -n 5)
echo -e "[ALERT] Failed SSH login attempts detected:\$FAILED_SSH" | mail -s "Security Alert" root@local
host
```

We generate a script as an example exploitation scenario which may involve identifying weak accounts from the previous output, such as old or inactive accounts. Additionally, detecting unused or vulnerable services through systemctl can reveal potential entry points for attackers. Lastly, noticing excessive storage usage could indicate a risk of Denial of Service ≣DoS≣ attacks exploiting resource exhaustion.

Mitigation

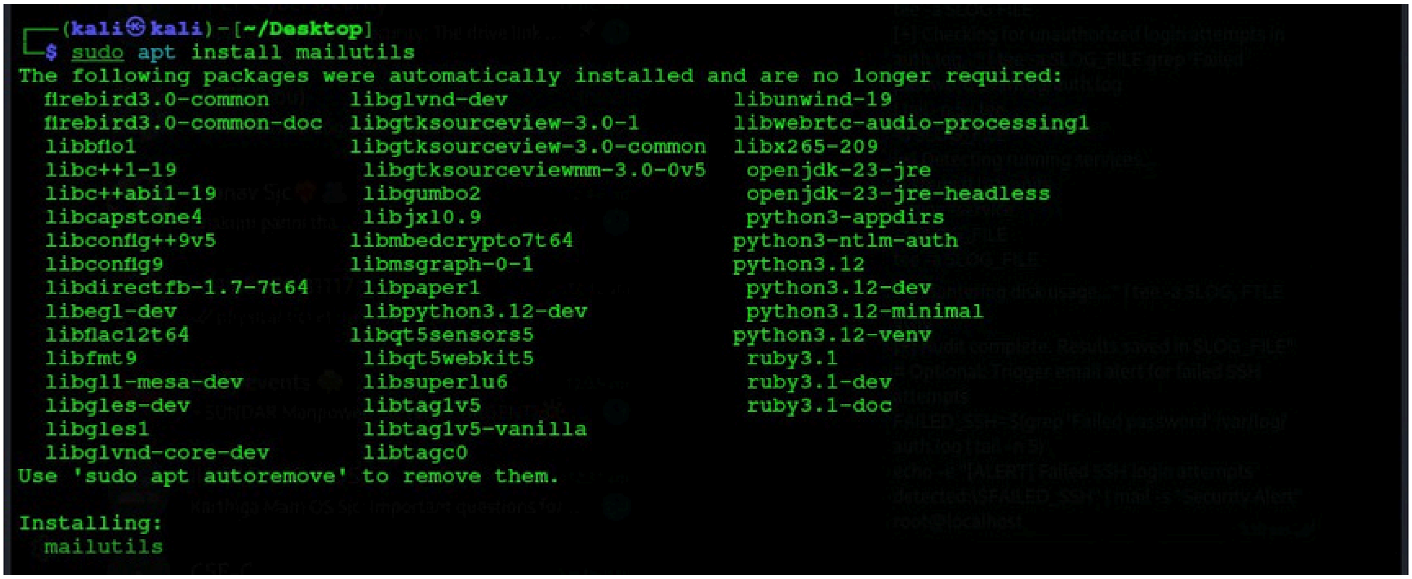


```
┌──(kali㉿kali)-[~/Desktop]
└─$ * * * * /home/kali/Desktop/system_monitoring.sh
```

To automate proactive monitoring with cron, add the following line to your cron jobs:

`0 * * * * /path/to/system_monitoring.sh`

This configuration schedules the script to run hourly, ensuring consistent system monitoring.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt install mailutils
The following packages were automatically installed and are no longer required:
  firebird3.0-common      libglvnd-dev                 libunwind-19
  firebird3.0-common-doc  libgtksourceview-3.0-1       libwebrtc-audio-processing1
  libbfio1                libgtksourceview-3.0-common  libx265-209
  libc++1-19               libgtksourceviewmm-3.0-0v5   openjdk-23-jre
  libc++abi1-19            libgumbo2                    openjdk-23-jre-headless
  libcapstone4             libjxl0.9                    python3-appdirs
  libconfig++9v5          libmbedcrypto7t64            python3-ntlm-auth
  libconfig9              libmsgraph-0-1               python3.12
  libdirectfb-1.7-7t64     libpaper1                    python3.12-dev
  libegl-dev               libpython3.12-dev            python3.12-minimal
  libflac12t64            libqt5sensors5               python3.12-venv
  libfmt9                  libqt5webkit5                ruby3.1
  libgl1-mesa-dev          libsuperlu6                  ruby3.1-dev
  libgles-dev              libtag1v5                    ruby3.1-doc
  libgles1                 libtag1v5-vanilla
  libglvnd-core-dev        libtagc0
Use 'sudo apt autoremove' to remove them.

Installing:
  mailutils
```

For enhanced security, implement email alerts for unauthorized SSH attempts. First, ensure `mailutils` is installed using the command:

`sudo apt install mailutils`

This solution improves your system's security posture by providing timely notifications and valuable insights into potential attack vectors.