Title: Simulated Logging Environment Setup and Analysis

Objective:

To simulate a real-world SOC (Security Operations Center) environment by performing log file operations, access controls, directory management, and basic system forensics using Linux command-line tools.

Tools Used:

- **OS**: Kali Linux
- **Terminal**: Bash (Kali Terminal)

Skills Learned:

- Linux directory and file management
- Log file simulation and manipulation
- Permission hardening for security
- Recursive search and analysis
- Disk usage inspection
- Archival and backup strategies
- Hands-on SOC operations for incident simulation

Challenge Tasks & Solutions

1.Environment Setup

Command:

```
mkdir -p ~/audit_lab/{logs,configs,backups}

cd ~/audit_lab
```

2. Log Files Initialization

Command:

```
touch logs/error.log logs/access.log logs/debug.log
```

3. Simulated Log Injection

Command:

```
echo "CRITICAL" > logs/error.log
```

echo "WARNING" >> logs/error.log

4. Secure Log Movement

Command:

```
mv logs/debug.log backups/debug_backup.log
```

5. Log Duplication

Command:

```
cp logs/access.log configs/access.log

cp logs/access.log backups/access.log
```

6. Log File Discovery

Command:

```
find ~/audit_lab -type f -name "*.log"
```

7. Log File Lockdown

Command:

```
chmod 600 logs/*.log
```

8. Directory Size Report

Command:

```
du -sh logs
du -sh configs
du -sh backups
```

9. Log Preview

Command:

```
head -n 1 logs/error.log
```

0. Keyword Search in Logs

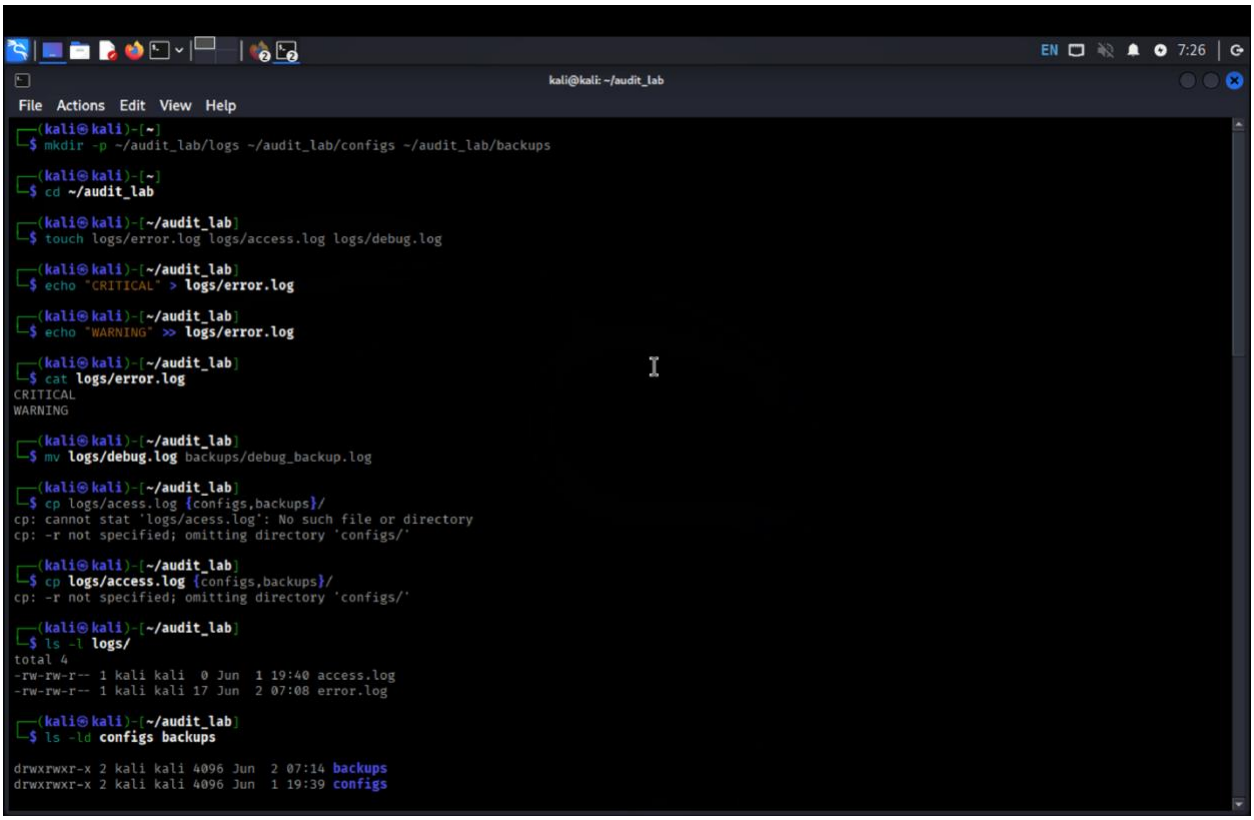
Command:

```
grep -rl "Disk" ~/audit_lab
```

11. Full Directory Archival

Command:

```
tar -czvf ~/Desktop/audit_lab_archive.tar.gz ~/audit_lab
```



kali@kali: ~/audit_lab

File Actions Edit View Help

```
└─$ ls -ld configs backups

drwxrwxr-x 2 kali kali 4096 Jun  2 07:14 backups
drwxrwxr-x 2 kali kali 4096 Jun  1 19:39 configs

┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -f configs backups
rm: cannot remove 'configs': Is a directory
rm: cannot remove 'backups': Is a directory

┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -r configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -rf configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ mkdir configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ cp logs/access.log {configs,backups}/
cp: -r not specified; omitting directory 'configs/'

┌──(kali㉿kali)-[~/audit_lab]
└─$ ls configs/

┌──(kali㉿kali)-[~/audit_lab]
└─$ ls backups/
access.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ find ~/audit_lab -name "*.log"
/home/kali/audit_lab/backups/access.log
/home/kali/audit_lab/logs/access.log
/home/kali/audit_lab/logs/error.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ chmod 600 logs/*.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ du -sh ~/audit_lab/*
4.0K    /home/kali/audit_lab/backups
4.0K    /home/kali/audit_lab/configs
```

kali@kali: ~/audit_lab

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -f configs backups
rm: cannot remove 'configs': Is a directory
rm: cannot remove 'backups': Is a directory

┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -r configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ rm -rf configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ mkdir configs backups

┌──(kali㉿kali)-[~/audit_lab]
└─$ cp logs/access.log {configs,backups}/
cp: -r not specified; omitting directory 'configs/'

┌──(kali㉿kali)-[~/audit_lab]
└─$ ls configs/

┌──(kali㉿kali)-[~/audit_lab]
└─$ ls backups/
access.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ find ~/audit_lab -name "*.log"
/home/kali/audit_lab/backups/access.log
/home/kali/audit_lab/logs/access.log
/home/kali/audit_lab/logs/error.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ chmod 600 logs/*.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ du -sh ~/audit_lab/*
4.0K    /home/kali/audit_lab/backups
4.0K    /home/kali/audit_lab/configs
8.0K    /home/kali/audit_lab/logs

┌──(kali㉿kali)-[~/audit_lab]
└─$ head -n 1 logs/error.log
```

kali@kali: ~/audit_lab

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/audit_lab]
└─$ head -n 1 logs/error.log
CRITICAL

┌──(kali㉿kali)-[~/audit_lab]
└─$ grep -r "Disk" ~/audit_lab

┌──(kali㉿kali)-[~/audit_lab]
└─$ tar -czvf ~/Desktop/audit_lab_archive.tar.gz ~/audit_lab
tar: Removing leading `/' from member names
/home/kali/audit_lab/
/home/kali/audit_lab/backups/
/home/kali/audit_lab/backups/access.log
/home/kali/audit_lab/configs/
/home/kali/audit_lab/logs/
/home/kali/audit_lab/logs/access.log
/home/kali/audit_lab/logs/error.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ tar -tzvf ~/Desktop/audit_lab_archive.tar.gz

drwxrwxr-x kali/kali         0 2025-06-02 07:19 home/kali/audit_lab/
drwxrwxr-x kali/kali         0 2025-06-02 07:19 home/kali/audit_lab/backups/
-rw-rw-r-- kali/kali         0 2025-06-02 07:19 home/kali/audit_lab/backups/access.log
drwxrwxr-x kali/kali         0 2025-06-02 07:19 home/kali/audit_lab/configs/
drwxrwxr-x kali/kali         0 2025-06-02 07:10 home/kali/audit_lab/logs/
-rw------- kali/kali         0 2025-06-01 19:40 home/kali/audit_lab/logs/access.log
-rw------- kali/kali        17 2025-06-02 07:08 home/kali/audit_lab/logs/error.log

┌──(kali㉿kali)-[~/audit_lab]
└─$ tree ~/audit_lab
/home/kali/audit_lab
├── backups
│   └── access.log
├── configs
└── logs
    ├── access.log
    └── error.log

4 directories, 3 files

┌──(kali㉿kali)-[~/audit_lab]
```