TASK 5

SSH Login Audit – PoC

This Proof of Concept demonstrates auditing SSH logins by parsing system authentication logs to track **successful** and **failed** login attempts.

Objective

Create a script `audit.sh` that:

- 📜 Parses `/var/log/auth.log` (or uses `journalctl` on systems with systemd).
- ✅ Shows **last 5 successful SSH logins**.
- ❌ Shows **last 5 failed SSH login attempts**.
- 💾 Saves the report to `ssh_audit.txt`.

Script: `audit.sh`

```
#!/bin/bash

OUTPUT_FILE="ssh_audit.txt"
TIMESTAMP=$(date '+%Y-%m-%d %H:%M:%S')

echo "SSH Login Audit Report - $TIMESTAMP" > "$OUTPUT_FILE"
echo "" >> "$OUTPUT_FILE"

# ✅ Last 5 successful SSH logins
echo "Last 5 Successful SSH Logins:" >> "$OUTPUT_FILE"
grep "sshd" /var/log/auth.log | grep "Accepted" | tail -n 5 >> "$OUTPUT_FIL
E"
echo "" >> "$OUTPUT_FILE"

# ❌ Last 5 failed SSH login attempts
echo "Last 5 Failed SSH Login Attempts:" >> "$OUTPUT_FILE"
grep "sshd" /var/log/auth.log | grep "Failed password" | tail -n 5 >> "$OUTPU
```

```
T_FILE"
echo "" >> "$OUTPUT_FILE"

echo "✅ Audit complete. Results saved to $OUTPUT_FILE"
```

Setup & Run

```
chmod +x audit.sh
sudo ./audit.sh
```