

Task 5: SSH Login Audit:

1. Create the script:

```
nano ssh_audit.sh
```

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

```
OUTPUT="ssh_audit.txt"
```

```
"$OUTPUT"
```

```
echo "=== Last 5 Successful SSH Logins ===" >> "$OUTPUT"
```

```
grep "Accepted" /var/log/auth.log | tail -n 5 >> "$OUTPUT"
```

```
echo -e "\n=== Last 5 Failed SSH Login Attempts ===" >> "$OUTPUT"
```

```
grep "Failed password" /var/log/auth.log | tail -n 5 >> "$OUTPUT"
```

```
echo -e "\nAudit saved to $OUTPUT"
```

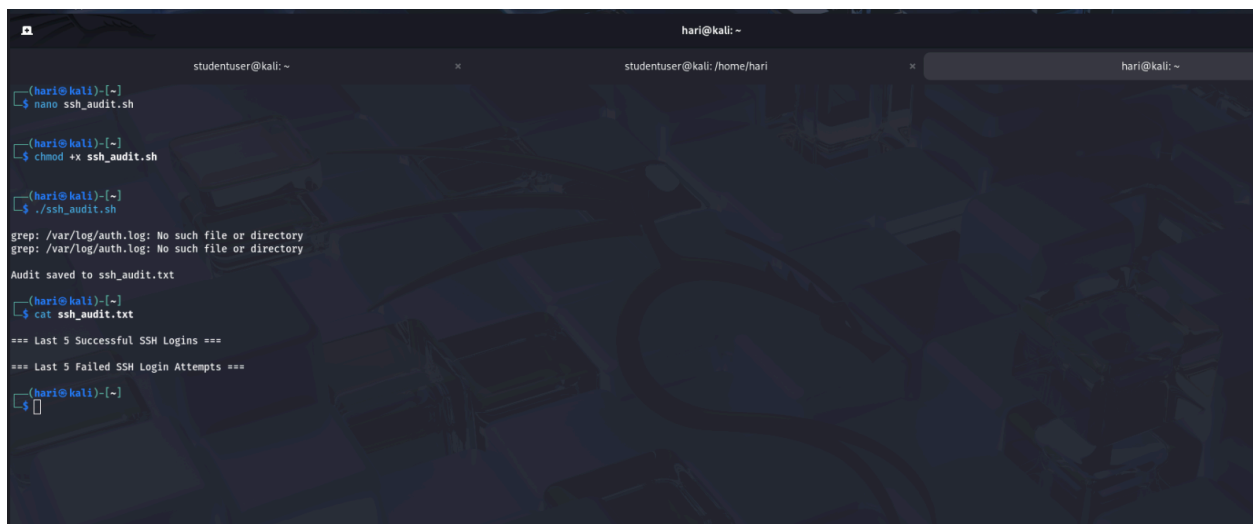
2. Make the script executable:

```
chmod +x ssh_audit.sh
```

```
./ssh_audit.sh
```

3. View the audit output:

```
cat ssh_audit.txt
```



```
hari@kali: ~  
studentuser@kali: ~  
studentuser@kali: /home/hari  
hari@kali: ~  
hari@kali: ~  
$ nano ssh_audit.sh  
$ chmod +x ssh_audit.sh  
$ ./ssh_audit.sh  
grep: /var/log/auth.log: No such file or directory  
grep: /var/log/auth.log: No such file or directory  
Audit saved to ssh_audit.txt  
$ cat ssh_audit.txt  
=== Last 5 Successful SSH Logins ===  
=== Last 5 Failed SSH Login Attempts ===  
$
```

Conclusion: Task 5 focused on auditing SSH login activity. We extracted and logged the last 5 successful and failed login attempts from `/var/log/auth.log` (or via `journalctl`) into `ssh_audit.txt`. This task highlighted basic log parsing for security monitoring.