**Comprehensive Incident Response Process: User Account Containment and Log Analysis**

**Introduction**

I have provided detailed documentation of the incident response process conducted on a Kali Linux system. The incident involved a compromised user account named 'malicious\_user.' My response process involved containment, log analysis, investigation of active processes, and verification that the system was clear of malicious activity.

**Step 1: Identifying Suspicious Activity**

The first indication of a potential compromise was through system log files, where failed login attempts and sudo command failures were noticed. I used the following commands to identify and investigate these suspicious activities.

- \*\*Checking for failed login attempts:\*\*  
 sudo grep 'Failed' /var/log/auth.log  
  
- \*\*Checking sudo command attempts for unusual activity:\*\*  
 sudo grep 'sudo' /var/log/auth.log  
  
- \*\*Viewing system activity logs:\*\*  
 sudo tail -n 100 /var/log/syslog  
  
- \*\*Attempt to access the auth.log for additional information:\*\*  
 sudo tail -n 100 /var/log/auth.log

**Step 2: Containing the Compromised User Account**

Once suspicious activity from the 'malicious\_user' was confirmed, immediate steps were taken to lock the account. I used the following commands to disable the account and prevent further login attempts:

- \*\*Lock the compromised user account:\*\*  
 sudo usermod -L malicious\_user  
  
- \*\*Confirm that the account is disabled:\*\*  
 su malicious\_user  
 (This returned 'Authentication failure,' verifying the account was locked.)

**Step 3: Investigating Running Processes**

After locking the account, it was essential to check for any active processes that the 'malicious\_user' might still be running. The following steps were used to identify and terminate those processes:

- \*\*List active processes for the user 'malicious\_user':\*\*  
 ps aux | grep malicious\_user  
  
- \*\*Kill any suspicious processes:\*\*  
 sudo kill <process\_id>  
  
In this case, processes such as those with PIDs 6396 and 211729 were identified but already terminated when further commands were issued.

**Step 4: Reviewing Network Connections**

It was necessary to check if the malicious user had established suspicious network connections. The following command I used to view open network connections and services listening on specific ports:

- \*\*List all active network connections and listening services:\*\*  
 sudo netstat -tulnp  
  
No suspicious connections or services were identified.

**Step 5: Reviewing Logs for Further Suspicious Activity**

A critical part of the incident response process was reviewing system logs to ensure no additional suspicious activities after locking the account. I used the following commands to analyze system logs:

- \*\*Check for failed login attempts in auth.log:\*\*  
 sudo grep 'Failed' /var/log/auth.log  
  
- \*\*Review sudo activities:\*\*  
 sudo grep 'sudo' /var/log/auth.log  
  
- \*\*Check the syslog for any further suspicious activity:\*\*  
 sudo tail -n 100 /var/log/syslog  
  
The logs indicated repeated failed login attempts and unsuccessful sudo commands by the compromised user.

**Step 6: Verifying and Restarting Logging Services**

To ensure that all logging mechanisms were working correctly, the rsyslog service was checked and restarted. This guaranteed that all system events were properly logged during the investigation process.

- \*\*Check the status of rsyslog service:\*\*  
 sudo service rsyslog status  
  
- \*\*Restart the rsyslog service if needed:\*\*  
 sudo systemctl restart rsyslog

**Step 7: Final Cleanup and User Deletion**

Once the system was confirmed to be clean, the 'malicious\_user' account was deleted to ensure the user could not log back into the system. The following command I used to remove the user:

- \*\*Delete the malicious user account:\*\*  
 sudo userdel malicious\_user  
  
- \*\*Verify that the user account was removed:\*\*  
 cat /etc/passwd | grep malicious\_user

**Conclusion**

The incident response process was successfully completed, and the system was secured. The compromised 'malicious\_user' account was disabled, and no further suspicious activity was detected in system logs or active processes. This case demonstrates a thorough approach to incident response, emphasizing the importance of log analysis, user containment, and process investigation.