Incident Report

1. **What triggered the alert?**
   Manual inspection detected a suspicious script (**fakebackup.sh**) running in the background that was not part of standard operations.

2. **What was the script doing?**
   The script printed a message indicating a **Simulated backup operation** and then slept for **60 seconds**. While harmless in this case, such behaviour is typical in malware to delay execution or appear legitimate.

3. **Which user executed it?**
   User **karthik** executed the script.

Recommendations:

1. **Enable File Integrity Monitoring**
   Deploy tools such as **AIDE (Advanced Intrusion Detection Environment)** or **OSSEC** to monitor critical system files for unauthorized changes. This helps detect tampering or stealthy script deployments early.

2. **Restrict Execution in /tmp Directory**
   Reconfigure the system to mount the /tmp directory with the noexec option to prevent execution of scripts or binaries stored there:

   sudo mount -o remount,noexec /tmp

You can also update /etc/fstab to make this change persistent across reboots.

3. **User Awareness and Training**
   Educate users on the risks of executing unknown or unverified scripts. Conduct regular cybersecurity awareness sessions and simulate phishing/script-based attack scenarios to reinforce best practices.