Incident Response Guide: Handling Indicators of Compromise (IoC)

Introduction

This guide provides a comprehensive step-by-step approach for responding to a security incident involving the detection of a backdoor script (`/backdoor.sh`). It outlines the necessary actions to identify, mitigate, and report the compromise, ensuring that the system is secured from further unauthorized access.

1. Initial Detection and Identification

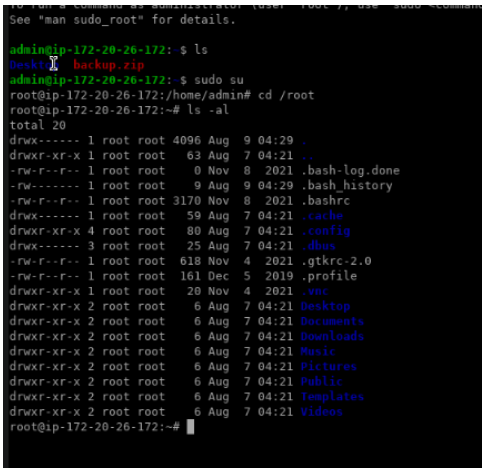
1.1 Detect Malicious Files

- *Identified File:* `/backdoor.sh`
  - *Risk:* This script allows attackers to execute commands on the system, which can lead to unauthorized access or control over the system.
- *Detection Method:*
  - Security software or manual inspection identified this file as potentially malicious.

1.2 Investigate Potential Malicious Activities

- *Commands to Investigate*:
  - List files and directories in `/etc/`:
    bash
    ls -al /etc/

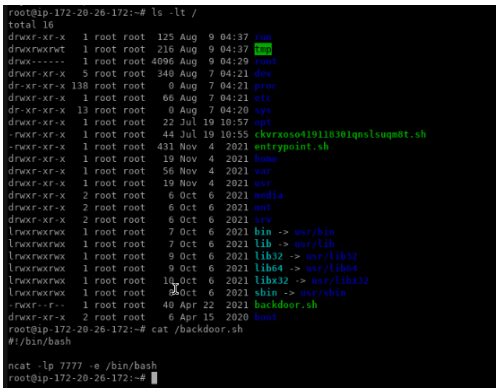
  - View the contents of the `/etc/passwd` file:
    bash
    cat /etc/passwd
    - List files and directories in `/root/`:
    bash
    ls -al /root/



2. Attack Investigation

2.1 Examine Running Processes and Scheduled Tasks

- *Objective:* Identify any processes or tasks that may be related to the malicious file.
- *Commands:*
  - List scheduled tasks (cron jobs):
    bash
    crontab -l
    - Check if any processes are associated with cron:
    bash
    ps aux | grep cron
    ps aux | grep crond



2.2 Evaluate Data Exfiltration Risks

-*Objective:* Assess whether the backdoor script was used to exfiltrate data.

- *Actions:*
  - Analyze network configurations:
    bash
    ifconfig

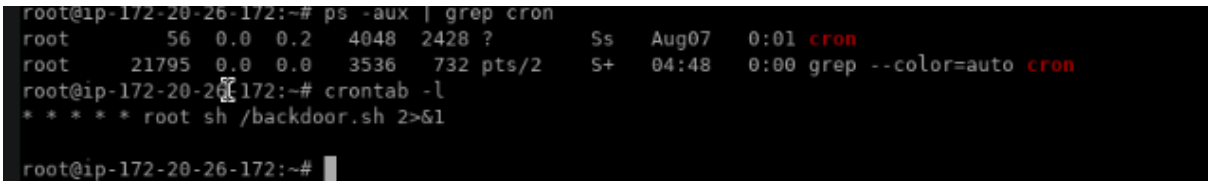
  - Recheck scheduled tasks to ensure no unauthorized cron jobs exist:
    bash
    crontab -e

3. Assessment of Compromised Components

3.1 Check for Unauthorized Programs and Files

- *Objective:* Identify any unauthorized or unusual programs running on the system.
- *Commands:*
  - List running processes:
    bash

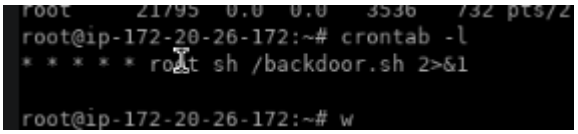
ps aux
- Check directories for unusual files:
bash
ls -al /root/

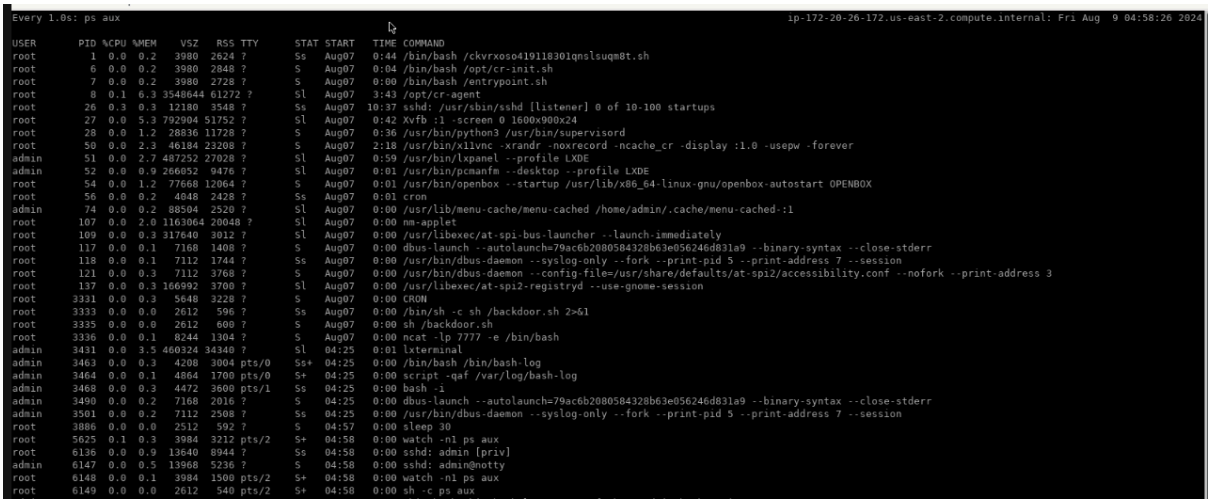


4.Network Traffic Analysis

4.1 Monitor Network Traffic for Suspicious Activity

- *Objective:* Analyze network traffic to detect any ongoing malicious activities.
- *Tool:*
- Use `iftop` to monitor real-time network connections:
bash
Iftop

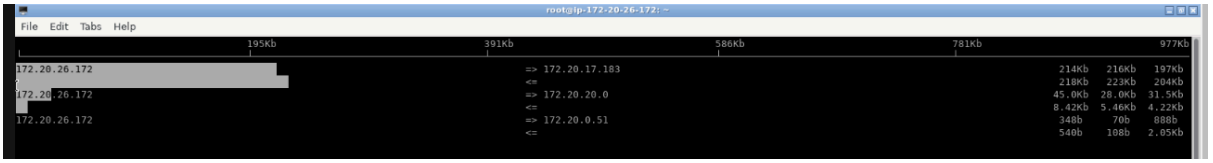




5. Immediate Remediation Actions

5.1 Stop the SSH Service

- *Objective:* Prevent further unauthorized access by disabling the SSH service.
- *Command:*
bash
service ssh stop



5.2 Remove Unauthorized SSH Keys

-*Objective:* Ensure that attackers cannot regain access using SSH keys.

- *Commands:*
  - Remove root's authorized SSH keys:
    bash
    rm /root/.ssh/authorized_keys

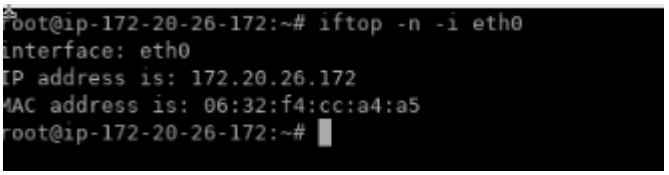
  - Remove user's authorized SSH keys:
    bash
    rm /home/[username]/.ssh/authorized_keys

6. Remove the Malicious Cron Job

6.1 Review and Edit Cron Jobs

-*Objective:* Remove the malicious cron job that executes the backdoor script.

- ***Steps:***
  1. *Open the crontab editor:*
     bash
     crontab -e



  2. *Locate the following line:*
     bash
     * * * * * root sh /backdoor.sh 2>&1

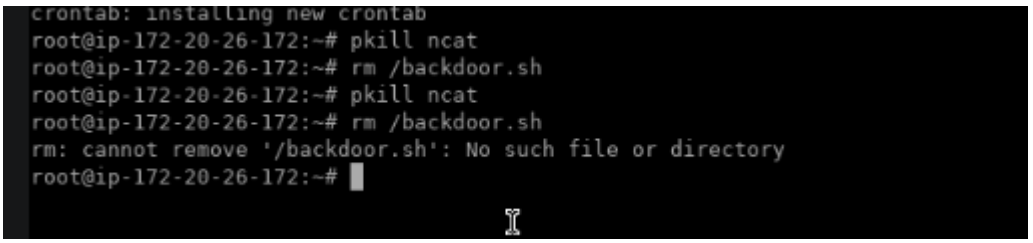
  3. *Delete the line* to prevent the script from running.
  4. *Save and exit* the editor:
     - In *GNU nano:* Press `CTRL + X`, then `Y` to confirm, and `Enter` to save.

- In *Vim*: Press `Esc`, type `:wq`, and press `Enter`.

6.2 Ensure the Attacker's Access is Revoked

- *Objective:* Make sure the attacker's access is permanently revoked.
- *Commands:*
  - Ensure SSH service is stopped:
    bash
    service ssh stop

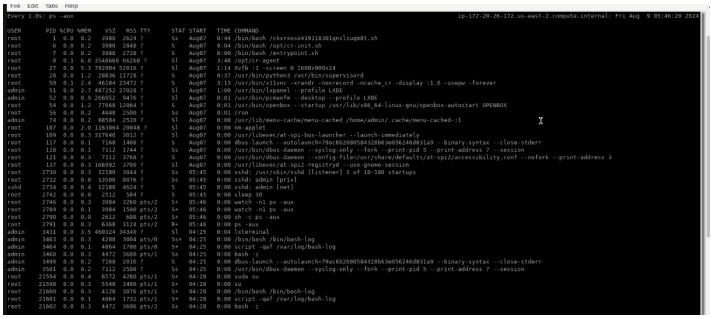
  - Permanently remove SSH keys:
    bash
    rm -rf /root/.ssh/authorized_keys



7. Final Cleanup

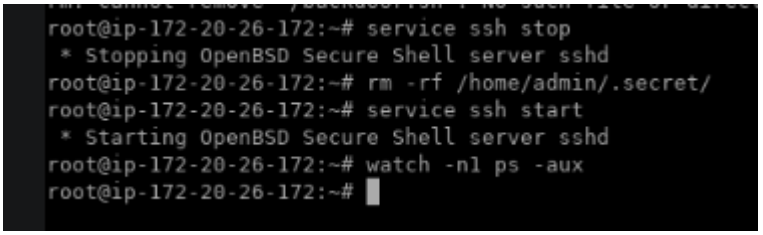
7.1 Remove the Backdoor Script

- *Objective:* Delete the backdoor script to ensure it cannot be executed.
- *Command*:
  bash
  rm /backdoor.sh



7.2 Verify No Unauthorized Access Exists

- **Objective:** Double-check that no unauthorized processes or SSH services are running.
- *Command:*
  bash
  ps aux | grep ssh



8. Incident Reporting

8.1 Document and Report the Incident

- Objective: Write a detailed report of the incident, including all actions taken, findings, and any data that may have been compromised.
- *Actions:*
  - Report the theft of private financial or other sensitive data if applicable.
  - Provide a comprehensive analysis to the relevant stakeholders.

9.Post-Incident Actions

9.1 Write a Final Analysis

- Objective:Summarize the incident, response actions, and provide recommendations to prevent future attacks.
- *Deliverable:* A final report that includes:
  - The nature of the compromise.
  - Detailed steps taken to mitigate the threat.
  - Recommendations for future security measures.

9.2 Conclusion

- **Final Note:** Taking these steps will help secure the system and prevent further unauthorized access. Regularly review and update your security protocols to adapt to new threats.