Security Incident Report

Client: 4Geeks Academy

Conducted by: Mohannad Darwish

Date: 14 July, 2025

---

1. Executive Summary

On October 8, suspicious root-level access was detected on the Debian-based production server. This prompted a full forensic investigation. Multiple configuration-based vulnerabilities were discovered, some of which had already been exploited. The response involved immediate containment, remediation, and hardening efforts across affected services.

---

2. Forensic Analysis Summary

A. SSH Root Access Exploitation

- Log evidence from `journalctl` and `sshd` revealed successful login to the root account from IP `192.168.0.134` on Oct 8.
- `sshd_config` permitted `PermitRootLogin yes` and `PasswordAuthentication yes`, creating a major attack surface.
- The attacker likely exploited these configurations to access the system using a brute-forced or known password.

B. Sudo Privilege Abuse via Weak User Credentials

- The default user `debian` had a weak password (`123456`) and full sudo rights.
- Journal logs showed the user was initially not in sudoers, but later executed root-level commands.
- This chain of activity indicated privilege escalation after successful login.

C. No Evidence of Exploitation (Yet Still Critical):

- FTP, MySQL, Apache, and WordPress misconfigurations were identified, but no clear exploit traces were found prior to analyst access.
- These were proactively corrected to reduce attack surface.

---

3. Corrective Measures Taken

SSH Hardening

- Disabled root login via `sshd_config`
- Enabled key-based authentication
- Limited max auth attempts to 3

User Access Security

- Password for `debian` user updated to a secure alternative
- Logs reviewed to ensure no remaining elevated shells

MySQL Remediation

- Passwords updated for weak/duplicate hashes (`root`, `mysql`, `wordpressuser`)
- `user` account locked due to suspicious full privileges and lack of traceability
- General log enabled for future auditability

FTP Server Secured

- Anonymous login disabled
- Global write access disabled
- Chroot jail enforced for local users

WordPress Fortification

- Weak default admin account replaced with new secure user
- Directory listing disabled via Apache
- `wp-config.php` permissions restricted to 600 and ownership reassigned

Apache & Open Ports

- Validated that Debian version of Apache was patched for relevant CVEs via backport
- Port 631 (IPP) closed by disabling the CUPS service
- Nmap scan confirmed minimized exposure

---

4. Preventive Measures Implemented

- General log enabled in MariaDB for ongoing query auditing
- SSH public-key-only login enforced
- Password rotation completed for all key accounts
- Nessus scan baseline created for continuous comparison
- Scheduled weekly backups and daily incremental snapshots implemented
- Security policies added to restrict directory listing, HTTP methods, and FTP/SSH access

---

5. Timeline of Events

Date	Event Description
Oct 8	SSH root login from 192.168.0.134 detected
Oct 8	Sudo privilege escalation via weak debian account observed
Oct 11	Full forensic analysis conducted
Oct 11	Corrective actions implemented (SSH, MySQL, FTP, WP)
Oct 14	Apache CVEs reviewed, logs inspected for payloads
Oct 15	Final validation, scanning, and hardening completed

---

6. Lessons Learned

- Even standard misconfigurations (FTP write, root login) become critical when paired with weak credentials.
- Early detection through log monitoring is vital to identifying exploited paths.

- Posture improvement must prioritize privilege reduction and access control over convenience.