Incident Recovery Plan

Client: 4Geeks Academy

Conducted by: Mohannad Darwish

Date: 14 July, 2025

Objective:

To ensure the rapid and effective restoration of critical services in the event of a cybersecurity incident. This plan defines the specific procedures, responsible parties, and validation processes for service recovery while minimizing data loss, disruption, and financial impact.

Scope:

This recovery plan applies to all systems and services affected by the security vulnerabilities identified in the penetration test and forensic analysis, including:

- SSH Access (root login, credential abuse)
- FTP Misconfigurations
- MySQL Account Vulnerabilities
- WordPress Configuration Issues
- Open Ports & Apache Exposure

Recovery Goals:

- Restore business-critical services within **4 hours** of incident confirmation
- Contain and eliminate any persistent malicious access
- Preserve the integrity of restored data
- Reinforce configuration against re-exploitation
- Ensure recovery measures are testable and repeatable

Critical Services and Systems:

Service	System/Software	Criticality Level	Recovery Time Objective (RTO)
Web Server (Apache)	apache2 v2.4.62	High	1 hour
WordPress CMS	WordPress 6.x	High	1 hour
Database	MariaDB 10.11.6	High	2 hours
SSH Access	OpenSSH	Medium	1 hour
FTP Server	vsftpd	Medium	3 hours

Recovery Team Roles & Responsibilities:

Role	Assigned To	Responsibilities
Incident Coordinator	System Administrator	Lead recovery execution, escalate as needed
Network Analyst	Cybersecurity Analyst	Validate network configurations and firewall rules
Application Engineer	Web Developer	Restore WordPress and verify patching
DBA	Database Administrator	Confirm database integrity and user security
Forensic Specialist	External Support	Confirm exploit traces have been fully removed

---

Recovery Procedures:

1. SSH Configuration Recovery

- Restore sshd_config to known-good state: disable root login, password auth, and set MaxAuthTries=3
- Deploy pre-generated SSH keys
- Test remote login from trusted admin machine

2. MySQL User Cleanup & Reconfiguration

- Lock unused or suspicious accounts (user, wordpressuser)
- Reset shared/weak passwords (e.g., root, mysql)
- Reassign ownership where applicable
- Verify privileges using:

  SELECT user, super_priv, grant_priv **FROM** mysql.user;

3. WordPress Restoration

- Verify integrity of wp-config.php, plugin list, and database connections
- Confirm secure admin account in place
- Disable directory listing via Apache conf or .htaccess

4. Apache Hardening

- Confirm Apache version compliance with patched Debian backports
- Validate virtual host configs and disable indexing, TRACE, etc.
- Restart service and test via curl, browser access, and logs

5. FTP Lockdown

- Confirm vsftpd.conf settings:
  - anonymous_enable=NO
  - write_enable=NO
  - chroot_local_user=YES
- Restart FTP service and run penetration check using ftp or Nessus

6. Remove Unnecessary Services/Ports

- Disable CUPS to close port 631:

  sudo systemctl stop cups
  sudo systemctl disable cups

- Re-scan using Nmap to confirm closure

Verification Procedures:

After each recovery step:

- Validate fix via command output, logs, or scans
- Capture before-and-after screenshots (archived securely)
- Document remaining vulnerabilities and mitigation date

Post-Recovery Activities:

- Submit recovery report to senior management
- Schedule follow-up scans with Nessus or equivalent
- Conduct incident postmortem with all IT and security staff
- Archive forensic logs in secure offline storage

Recommendations for Business Continuity:

- Enable full-system backups weekly and incremental daily
- Apply strict firewall rules based on service necessity
- Monitor logs daily and alert on login attempts, permission changes, or config edits
- Conduct tabletop incident response exercises quarterly