SOC INCIDENT RESPONSE REPORT

Incident Title

Unauthorized Access Attempts on Web Server Services

Incident ID: SOC-WS-001

Incident Severity: High

Incident Status: Resolved

Environment: Controlled Lab

Analyst Name: Kiran Karenavar

Date: 22 January 2026

Executive Summary

A series of unauthorized access attempts were detected on multiple web server services including SSH, FTP, MySQL, and SMTP. The activity originated from a simulated attacker machine within a controlled lab environment. Logs indicated brute-force attempts, credential abuse, and service misconfiguration exploitation.

Affected Assets

- Ubuntu Web Server (LAMP Stack)
- Services:
  - SSH
  - FTP
  - MySQL
  - SMTP

Incident Detection

The incident was detected through manual log analysis of system and application logs during SOC monitoring activities.

Detection Sources:

- `/var/log/auth.log`
- `/var/log/vsftpd.log`
- `/var/log/mysql/error.log`
- `/var/log/mail.log`

Incident Timeline

Time	Activity
T1	Service reconnaissance detected
T2	Multiple authentication failures observed
T3	Brute-force attack identified
T4	Unauthorized access confirmed
T5	Mitigation actions applied

Indicators of Compromise (IOCs)

- Repeated failed login attempts
- Login attempts from unknown IP addresses
- Anonymous FTP access
- Unauthorized database access attempts
- SMTP relay misuse attempts

Attack Analysis

The attacker attempted to gain access using brute-force techniques and weak credentials. Misconfigured services such as anonymous FTP and exposed MySQL access increased the attack surface. The attack aligns with MITRE ATT&CK credential access and initial access techniques.

Containment Actions

- Blocked attacking IP addresses
- Stopped vulnerable services temporarily
- Disabled anonymous FTP access

Eradication Actions

- Implemented Fail2Ban for SSH
- Restricted MySQL access to localhost
- Enforced strong password policies
- Secured SMTP relay configuration

Recovery Actions

- Restarted secured services
- Verified system integrity
- Monitored logs for further suspicious activity

Post-Incident Recommendations

- Deploy centralized logging (SIEM)
- Enable real-time alerting
- Conduct regular vulnerability assessments
- Apply least privilege principles

Lessons Learned

- Log monitoring is essential for early detection
- Weak credentials remain a major risk
- Defense-in-depth significantly reduces attack impact
- SOC readiness depends on visibility and response speed

Conclusion

This incident response exercise demonstrates the SOC lifecycle: detection, analysis, containment, eradication, and recovery. The project reflects real-world SOC analyst responsibilities and aligns with industry frameworks such as MITRE ATT&CK.