Incident Response & Security Breach Simulation

Executive Summary:
A simulated brute-force SSH attack was detected via repeated failed login attempts in Linux authentication logs.

Incident Details:
- Attack Type: Brute Force
- Target: SSH (Port 22)
- Source IP: 192.168.1.50
- Severity: Medium

Detection:
Multiple 'Failed password' entries identified in /var/log/auth.log.

Containment:
- Blocked malicious IP using UFW
- Disabled root SSH login
- Restarted SSH service

Eradication:
Installed and configured Fail2Ban to auto-block repeated attempts.

Recovery:
Verified no successful unauthorized logins and confirmed system integrity.

Recommendations:
- Enable MFA
- Use SSH key authentication
- Regular log monitoring
- Deploy IDS like Snort