Incident Response Report

# 1. Alert Analysis

The simulated log file was analyzed to identify potential security events.  
Key alerts observed:  
- Multiple failed login attempts from the same IP.  
- Successful login after several failed attempts.  
- Privilege escalation activity detected.  
These indicators suggest a possible brute-force attack followed by privilege escalation.

# 2. Incident Classification

|  |  |  |
| --- | --- | --- |
| Incident Type | Severity | Reason |
| Failed login attempts | Medium | Could indicate brute force attempt |
| Successful login after multiple failed attempts | High | Possible account compromise |
| Privilege escalation attempt | High | Indicates post-compromise activity |

# 3. Remediation Recommendations

- Enforce strong password policies and enable MFA.  
- Block suspicious IPs and monitor login attempts.  
- Investigate compromised accounts and reset credentials.  
- Review privilege escalation logs and patch vulnerabilities.  
- Implement continuous monitoring via SIEM tools (Splunk / ELK).  


