Incident Report

Linux SSH Brute Force Investigation

Name: Sejal Sonar
Date: (Write today's date)
Log Source: /var/log/auth.log
System: Linux Server

1. Summary

During log monitoring, I found multiple failed SSH login attempts on a Linux server.
The activity looked suspicious and similar to a brute force attack.

After investigation, I confirmed that the attacker was not successful.

2. Incident Details

- Service Targeted: SSH (Port 22)
- User Targeted: user1
- Source IP Address: 185.220.101.45
- Activity Type: Multiple failed password attempts
- Successful Login: Not found

3. Investigation Steps

1. Opened the Linux authentication log file (/var/log/auth.log).
2. Checked login activity related to SSH.
3. Found multiple failed login attempts from the same IP address.
4. Checked for any successful login entries ("Accepted password").
5. Confirmed that no successful login occurred.

4. Analysis

- Multiple failed attempts from the same IP address indicate password guessing behavior.
- SSH provides remote access to the server.
- Since no successful login was found, the attacker could not access the system.
- This matches the pattern of a brute force attack attempt.

5. Conclusion

The investigation confirms that a brute force attack attempt occurred.
However, the attack was unsuccessful because no login was successful.

Severity Level: Medium

6. Recommendations

- Block the suspicious IP address.
- Use strong password policies.
- Enable account lockout settings.
- Monitor logs regularly for unusual login attempts.