Brute Force Attack Detection on SSH Logins

Abstract

A brute-force attack involves repeatedly attempting different username/password combinations to gain unauthorized access to a system. Attackers commonly target SSH (Secure Shell) logins to break into servers.

In this project, we will:

- Monitor failed SSH login attempts from logs (Linux-based systems).
- Track IPs with repeated failed logins.
- If an IP exceeds a threshold (e.g., 5 failed attempts), it will be automatically blocked using **Fail2Ban** integration.

This script is designed for Linux-based servers (Ubuntu, Debian, **CentOS**, etc.).

Fail2Ban is an intrusion prevention tool that automatically monitors log files for repeated failed login attempts and bans suspicious IPs by updating firewall rules. It helps prevent brute-force attacks and other security threats.

How Fail2Ban Works for SSH Protection?

- Monitors log files (e.g., `/var/log/auth.log`) for failed SSH logins.
- Temporarily or permanently bans malicious IPs.
- The banned IP cannot access SSH for a certain duration.
- Admins can unban IPs or customize the ban rules.
- Can protect SSH and other services.

Team Members:

K. Manjith Reddy	2320030003
N. Manikanta	2320030172
V. Ajay Charan	2320030033