Brute Force Attack Detection on SSH Logins

Detection and Mitigation Techniques

Manjith-2320030003 , Ajay-2320030033 , Manikanta-2320030172

Department of Computer Science Engineering
KL University, Bachupally

March 25, 2025

Overview

Brute force attacks on SSH logins are a major cybersecurity threat. This presentation explores detection methodologies and mitigation strategies to secure SSH access.

Introduction

- **Definition of Brute Force Attacks:** A brute force attack is a trial-and-error method used to obtain credentials or encryption keys by systematically trying all possible combinations.
- **Why SSH Logins are Vulnerable:** SSH services are a common target for brute force attacks due to weak passwords, open ports, and lack of rate limiting.
- **Real-World Impact:** Brute force attacks can lead to unauthorized access, data breaches, and system compromise, making detection critical.
- **Importance of Detection and Prevention:** Implementing strong authentication mechanisms, monitoring login attempts, and using automated detection tools can mitigate risks.

Key Insights on Brute Force Attack Detection

Detection Strategies

- Implementing **fail2ban** to block repeated failed login attempts.
- Monitoring SSH logs to identify suspicious activities.
- Using rate-limiting techniques to prevent excessive login attempts.

Critical Security Risks

- Weak passwords increase vulnerability to brute force attacks.
- Unmonitored SSH ports allow continuous attack attempts.
- Lack of Multi-Factor Authentication (MFA) makes systems easier to breach.

Examples

- Implementing IP-based restrictions to block unauthorized access.
- Deploying honeypots to track attacker behavior.
- Logging and analyzing failed authentication attempts for proactive security.

Detection Techniques

Detection Methods

1. Log Analysis
2. Machine Learning Approaches
3. Two-Factor Authentication (2FA)

Monitoring authentication logs and identifying abnormal login patterns can help detect brute force attacks before they succeed.

Implementing Two-Factor Authentication (2FA) adds an extra layer of security by requiring a second verification step beyond just passwords.

Python Script for SSH Attack Detection

```
import re
from collections import Counter

with open("/var/log/auth.log") as log:
    ips = re.findall(r"Failed password.* from (\d+\.\d+\.\d+\.\d+)", log

for ip, count in Counter(ips).most_common(10):
    print(f"{ip}: {count} attempts")
```

This script extracts and counts failed SSH login attempts by IP address.

Table: Prevention Methods

Method	**Effectiveness**	**Implementation Complexity**
Fail2Ban	High	Medium
IP Whitelisting	Very High	Low
Two-Factor Authentication	Very High	Medium
Public Key Authentication	High	Low

Table: Comparison of SSH Security Measures

Theorem: Login Attempts Bound

Theorem (Brute Force Limit)

If an attacker is rate-limited to n attempts per minute, the expected time to guess a strong password of length l with an alphabet of size a is at least:

$$\frac{a^l}{n} \textit{ minutes}$$

Citation

This analysis is based on previous research in cybersecurity [1].
Further insights into SSH brute-force attack patterns and mitigation strategies can be found in [2].

References

Smith, J. ”Detecting SSH Brute Force Attacks: Anomaly-Based Intrusion Detection”. Journal of Cybersecurity, 2022.

Fail2Ban Documentation, `https://www.fail2ban.org`, last accessed 2025/03/11.

Thank You!