BRUTE FORCE ATTACK: DETECTION, INVESTIGATION, AND REMEDIATION FOR SOC ANALYSTS

VAISHALI SHISHODIA

Introduction to Brute Force Attack

A **Brute Force Attack** is a method used by attackers to gain unauthorized access to systems by trying all possible combinations of passwords, encryption keys, or other authentication credentials until the correct one is found. This attack is often used against systems that rely on password authentication, and it may involve the use of automated tools or scripts to execute thousands or even millions of guesses per minute.

Key Points:

- Brute Force is a trial-and-error method of cracking passwords or encryption keys.
- Can be applied to any system with login credentials (SSH, RDP, web applications, etc.).
- Often detected by abnormal login patterns, especially multiple failed login attempts in a short time span.

Indicators of a Brute Force Attack:

1. **Unusual Login Patterns:**
   - **Multiple failed login attempts** within a short time window.
   - Logins from **multiple geographic locations** in a short period.
   - **Repetitive login attempts** to the same account or multiple accounts.
2. **High Frequency of Authentication Failures:**
   - Unusually high **failed login attempts** (e.g., more than 5 to 10 within a minute or hour).
   - Systems logging "invalid username/password" or "access denied" events frequently.
3. **Unsuccessful Attempts from Single IP:**
   - Multiple login attempts from the **same IP address** to various user accounts.
4. **Brute Force Tool Signatures:**
   - Presence of tools commonly used for brute force attacks, such as **Hydra**, **John the Ripper**, **Aircrack-ng**, or **Medusa**.
5. **Unusual Patterns in Logs:**
   - Login failures followed by successful login attempts after a certain number of failures, which could indicate a successful brute force attack.
6. **Anomalous Traffic to Login Pages:**
   - Unexpected spikes in traffic to login pages (HTTP, RDP, SSH), which may indicate an attempt to hit login systems with brute force methods.

Steps for Investigating a Brute Force Attack

1. Collect and Review Logs:

- **System Logs:** Review failed login attempts from systems and devices. Logs should include timestamps, usernames, IP addresses, and error codes (e.g., "wrong password").
- **Authentication Logs:** These include failed and successful login attempts, often stored in system files such as /var/log/auth.log for Linux systems or Event Viewer on Windows.
- **Web Server Logs:** Review logs for failed HTTP authentication attempts, such as those for web applications, which may provide a clue to brute force attempts.

Example Log Entry:

```
Feb 25 14:03:45 server sshd[13456]: Failed password for invalid user admin from 192.168.1.100 port 22 ssh2

Feb 25 14:03:47 server sshd[13456]: Failed password for invalid user admin from 192.168.1.100 port 22 ssh2

Feb 25 14:03:50 server sshd[13456]: Failed password for invalid user admin from 192.168.1.100 port 22 ssh2
```

2. Investigate Source IP Addresses:

- Identify any **suspicious IPs** that show up repeatedly in logs.
- Use threat intelligence feeds to check if the IP addresses are associated with known malicious sources or botnets.
- Investigate geolocation to see if the login attempts are coming from an unusual or unexpected location.

3. Correlate the Data:

- Look for correlation between multiple events such as:
  - Multiple failed login attempts from the same IP or user across different accounts.
  - Spikes in failed login attempts followed by a successful login.

Example Query:

```
SELECT * FROM login_attempts WHERE failed_attempts > 5 AND timestamp BETWEEN '2025-02-25 14:00:00' AND '2025-02-25 14:05:00';
```

4. Check for Any Malicious Activity:

- Check if there was **privilege escalation** or successful login on any critical accounts following failed login attempts.
- Investigate whether any new user accounts or security settings were modified.

5. Track Progression of the Attack:

- Investigate if there were any **lateral movements** or attempts to access more systems or escalate privileges (such as attempts to compromise administrator accounts after breaching lower-level user accounts).

How SOC Analysts Can Remediate a Brute Force Attack

1. Block the Attacker's IP Address:

- **Block or throttle** suspicious IP addresses or IP ranges that are attempting the brute force attacks.
- Consider using **geolocation-based blocking** for countries where no valid login attempts should come from.

Example:

```
iptables -A INPUT -s 192.168.1.100 -j DROP
```

2. Enable Account Lockout Policies:

- Enforce an **account lockout** mechanism where a user's account is temporarily locked after a specified number of failed login attempts (e.g., after 3-5 failed login attempts).

3. Implement Multi-Factor Authentication (MFA):

- Enforce **MFA** for critical systems to reduce the effectiveness of brute force attacks.
- MFA can help prevent attackers from gaining access even if they successfully guess a password.

4. Increase Complexity of Password Policies:

- Enforce **strong password policies** (e.g., minimum length, special characters, numbers) and encourage users to change passwords regularly.
- Use **password hashing** to ensure that passwords are stored securely, making brute forcing less effective.

5. Intrusion Detection Systems (IDS) and Firewalls:

- Enable **IDS/IPS** systems to detect and alert when a brute force attack is underway.
- Use **rate-limiting** or **web application firewalls (WAFs)** to limit the number of login attempts from a particular IP or account.

6. Monitor and Review Security Logs Continuously:

- Ensure continuous monitoring of **authentication logs** and set up automated alerts for suspicious login patterns (e.g., too many failed logins within a short time).

Search Queries for Brute Force Attack Detection

1. **Failed Login Attempts Query:**
2. SELECT username, COUNT(*) AS failed_attempts
3. FROM auth_logs
4. WHERE status = 'failed'
5. GROUP BY username
6. HAVING failed_attempts > 5
7. **Correlation Between Failed and Successful Logins:**
8. SELECT username, COUNT(*) AS failed_attempts, success_attempts.timestamp AS success_timestamp
9. FROM auth_logs failed_attempts
10. LEFT JOIN auth_logs success_attempts ON failed_attempts.username = success_attempts.username
11. WHERE failed_attempts.status = 'failed'
12. AND success_attempts.status = 'success'
13. GROUP BY username
14. **IP Address with Multiple Failed Logins:**
15. SELECT ip_address, COUNT(*) AS failed_attempts
16. FROM auth_logs
17. WHERE status = 'failed'
18. GROUP BY ip_address
19. HAVING failed_attempts > 10

Correlation Rule for SIEM Systems

Brute Force Detection Correlation Rule:

- **Condition:** Multiple failed login attempts within a short time window (e.g., 5 failed attempts in 5 minutes).
- **Trigger:** Alert if the threshold is exceeded.
- **Action:** Investigate source IP, investigate system access logs, and block IP if suspicious.

Example Rule in a SIEM (like Splunk):

```
index=security sourcetype=auth_log "failed password"

| stats count by src_ip, user

| where count > 5
```

Anomalous Login Behavior Rule:

- **Condition:** Multiple login attempts from different locations for the same user in a short period.
- **Trigger:** Alert when such behavior is detected.
- **Action:** Validate source IPs, investigate geolocation, and check for any unauthorized access.

Conclusion

Brute Force Attacks remain one of the most common forms of cyberattacks against systems that rely on password-based authentication. The ability to **detect**, **investigate**, and **remediate** such attacks is crucial for a Security Operations Center (SOC) to protect critical assets.

By actively monitoring logs, setting up strong password policies, using MFA, and blocking suspicious activities, SOC analysts can minimize the damage of brute force attacks. Additionally, by creating effective search queries and correlation rules in SIEM systems, SOC analysts can automate detection, speed up investigations, and efficiently respond to security incidents.