SOC Incident Report

```

SOC Incident Report

Incident ID: 20251130-SSH-BruteForce-01

Date of Report: 2025-11-30

Time of Report: 15:00 UTC

Reported By: SOC Manager

1. Executive Summary

On 2025-11-30 at 14:23:01 UTC, a SSH brute force attack was detected originating from IP address 45.12.34.7, targeting the system Finance-Database-01. The attack consisted of 450 failed login attempts within a 2-minute period, utilizing common usernames such as root, admin, oracle, and test. Threat intelligence indicates that the source IP is malicious with a high-risk score and a history of similar attacks. Immediate mitigation steps were initiated to block the offending IP and secure the targeted system. This report details the incident, threat intelligence findings, and comprehensive mitigation strategies.

2. Incident Details

* Event: SSH Brute Force Attack Detected

* Date/Time: 2025-11-30 14:23:01 UTC

* Source IP: 45.12.34.7

* Target System: Finance-Database-01

* Attempts: 450 failed login attempts in 2 minutes

* Usernames Tried: root, admin, oracle, test

* Status: Active - Mitigation in progress

3. Threat Intelligence

IP Address: 45.12.34.7

Risk Score: 85 (High)

Status: Malicious

Geolocation: Unknown/Proxy (Likely using proxy or VPN)

Attack History: SSH Brute Force, Port Scanning
```

ISP: BadActor Networks Ltd. (Known for malicious activity)

Additional Information: The IP address is associated with a known malicious network (BadActor Networks Ltd.) and has a history of involvement in brute force attacks and port scanning activities. The high-risk score (85) indicates a significant threat level. The use of a proxy or VPN makes accurate geolocation difficult, suggesting an attempt to obfuscate the source.

4. Mitigation Steps

Immediate Actions:

* Block IP Address:

* Action: Implemented a deny rule for inbound traffic from 45.12.34.7 on all network firewalls and the host-based firewall on Finance-Database-01.

* Expected Outcome: Immediate cessation of attack attempts from the identified IP.

* Status: Completed. Rule implemented on perimeter firewall FW-01, internal firewall FW-02, and host-based firewall on Finance-Database-01.

* Isolate Finance-Database-01 (If Necessary):

* Action: Determined isolation was not immediately necessary as no successful logins were detected. Monitoring continues.

* Expected Outcome: Containment of potential breach and prevention of further compromise (contingency plan).

* Status: Standby. Isolation procedures documented and ready for immediate implementation if needed.

* Investigate Recent Login Attempts:

* Action: Analyzed SSH logs (/var/log/auth.log and /var/log/secure) on Finance-Database-01 for successful logins.

* Expected Outcome: Identification of any compromised accounts.

* Status: Completed. No successful login attempts found coinciding with the brute force attack.

* Password Reset:

* Action: No successful logins were identified. However, a precautionary password reset was initiated for all administrative accounts on Finance-Database-01.

* Expected Outcome: Prevention of unauthorized access using compromised credentials.

* Status: Completed. Password reset enforced for all admin accounts. Users notified.

Short-Term Actions (Within 24 Hours):

* Strengthen SSH Security:

* Disable Password Authentication:

* Action: Edited the /etc/ssh/sshd_config file, setting PasswordAuthentication no and PubkeyAuthentication yes. Restarted the SSH service.

* Expected Outcome: Prevention of password-based brute force attacks.

* Status: Completed. Password authentication disabled. SSH service restarted.

* Change Default SSH Port:

* Action: Edited the /etc/ssh/sshd_config file, changing the Port directive to 2222. Restarted the SSH service. Updated firewall rules to allow traffic on port 2222.

* Expected Outcome: Reduction in automated attacks targeting the default SSH port.

* Status: Completed. SSH port changed to 2222. Firewall rules updated.

* Implement IP-Based Access Control:

* Action: Implemented firewall rules to restrict SSH access to Finance-Database-01 to only authorized IP addresses (internal management network).

* Expected Outcome: Prevention of unauthorized access from untrusted networks.

* Status: Completed. Access restricted to authorized IPs.

* Enable Two-Factor Authentication (2FA):

* Action: Implemented 2FA using Google Authenticator for all users with SSH access to Finance-Database-01.

* Expected Outcome: Enhanced security against credential compromise.

* Status: Completed. 2FA enabled and tested. Users enrolled.

* Review Firewall Rules:

* Action: Audited all firewall rules related to Finance-Database-01 and removed any unnecessary open ports or permissive rules.

* Expected Outcome: Reduced attack surface and improved security posture.

* Status: Completed. Firewall rules reviewed and tightened.

* Update Software:

* Action: Ran system updates (apt update && apt upgrade) on Finance-Database-01.

* Expected Outcome: Mitigation of known vulnerabilities.

* Status: Completed. System updated with latest security patches.

Long-Term Actions (Within 1-2 Weeks):

* Implement Intrusion Detection System (IDS):

* Action: Deploying Snort IDS to monitor network traffic and system logs for suspicious activity.

* Expected Outcome: Early detection of future attacks.

* Status: In Progress. Snort installation and configuration ongoing. ETA: 2025-12-05.

* Implement a Security Information and Event Management (SIEM) System:

* Action: Integrating logs from Finance-Database-01 and firewalls into the existing Splunk SIEM system for centralized monitoring and analysis.

* Expected Outcome: Improved visibility into security events and faster incident response.

* Status: In Progress. Log forwarding configured. Dashboard creation in progress. ETA: 2025-12-03.

* Conduct a Vulnerability Assessment:

* Action: Scheduling a vulnerability assessment on Finance-Database-01 using Nessus.

* Expected Outcome: Identification and remediation of any security weaknesses.

* Status: Scheduled. Scan to be performed on 2025-12-02.

* Review and Update Security Policies:

* Action: Reviewing and updating security policies related to password management, access control, and incident response.

* Expected Outcome: Improved security awareness and adherence to security standards.

* Status: In Progress. Policy review scheduled for 2025-12-06.

* Monitor for Similar Attacks:

* Action: Continuously monitoring network traffic and system logs for similar brute force attacks targeting other systems using SIEM and IDS.

* Expected Outcome: Proactive identification and mitigation of threats.

* Status: Ongoing. SIEM and IDS rules configured to detect similar attacks.

Specific Considerations for IP Address 45.12.34.7:

* Reputation Monitoring: Continue to monitor the reputation of IP address 45.12.34.7 and any associated IP ranges using threat intelligence feeds.

* Share Threat Intelligence: Shared the threat intelligence about this IP address with relevant security communities and threat intelligence platforms (e.g., AlienVault OTX, VirusTotal).

5. Lessons Learned

* The incident highlights the importance of strong password policies and the need for multi-factor authentication, especially for critical systems like Finance-Database-01.

* Regular security assessments and penetration testing are crucial for identifying and addressing vulnerabilities before they can be exploited.

* Proactive threat intelligence gathering and sharing can help organizations stay ahead of emerging threats.

6. Recommendations

* Enforce multi-factor authentication for all users with access to sensitive systems.

* Conduct regular security awareness training for employees to educate them about phishing attacks and other social engineering tactics.

* Implement a robust vulnerability management program to identify and remediate vulnerabilities in a timely manner.

* Continuously monitor network traffic and system logs for suspicious activity.

* Maintain an up-to-date incident response plan and conduct regular exercises to test its effectiveness.

7. Conclusion

The SSH brute force attack on Finance-Database-01 was successfully mitigated through a combination of immediate containment measures and longer-term security enhancements. The organization's security posture has been strengthened as a result of this incident. Continuous monitoring and proactive security measures are essential for protecting against future attacks.

8. Report Distribution

* CIO

* CISO

* IT Director

* Security Team

```
```