**INCIDENT RESPONSE REPORT**

# SSH Brute Force Attack Campaign

**Incident ID:** HONEY-001-BRUTEFORCE

**Analyst:** Yeury Perez

**Date:** September 17, 2024

**Classification:** **CONFIDENTIAL**

**Framework:** NIST SP 800-61r3 Computer Security Incident Handling Guide

## EXECUTIVE SUMMARY

AWS honeypot infrastructure detected and contained a sustained SSH brute force campaign targeting multiple system accounts. The campaign lasted 72+ hours with **912+ failed authentication attempts** from **3 primary threat** **actor** IPs.  
  
No compromise occurred due to strong detection and proactive containment.  
**Impact**: LOW

**Confidence**: HIGH (validated via GuardDuty, VPC Flow Logs, system logs)

## INCIDENT DETAILS

**Timeline (EDT)**

* **2024-09-14 00:08:15** - Initial attack detection (159.242.228.194)
* **2024-09-14 to 2024-09-17** - Sustained brute force campaign
* **2024-09-17 04:22:06** - Analysis completed

**Attack Vectors**

**Primary TTP:** T1110.001 - Brute Force: Password Guessing (MITRE ATT&CK)

**Tactic:** TA0006 – Credential Access

**Technique:** T1110 – Brute Force

**Primary Threat Actors:**

1. **36.20.126.21** - 420 failed attempts (46% of total)
2. **40.81.245.51** - 247 failed attempts (27% of total)
3. **51.222.50.114** - 245 failed attempts (27% of total)

**Targeted Accounts:**

* **"invalid"** - 1,837 attempts (67% - credential stuffing)
* **"root"** - 764 attempts (28% - privilege escalation intent)
* **"ubuntu"** - 100 attempts (4% - cloud-aware targeting)
* **"mysql"** - 28 attempts (1% - service account targeting)

## DETECTION & ANALYSIS

**Data Sources:**  
- AWS GuardDuty (Brute Force:EC2/SSH)  
- VPC Flow Logs (network telemetry)  
- CloudWatch Logs (SSH auth monitoring)  
- System logs (/var/log/auth.log)  
  
**IOC Summary:**  
IPs: 36.20.126.21 | 40.81.245.51 | 51.222.50.114 | 159.242.228.194  
Ports: 22/tcp  
Accounts: invalid, root, ubuntu, mysql  
Pattern: repeated password guessing attempts  
  
**Assessment:**  
- Campaign Duration: 72+ hours, persistence indicates botnet/proxy network.  
- Distribution: Coordinated, multi-source origin.  
- Risk: **Low** (all attempts failed), but highlights exposure of default/system accounts.

## CONTAINMENT, ERADICATION & RECOVERY

Actions Taken:  
- Enabled real-time log collection (CloudWatch Agent)  
- Configured custom CloudWatch alarms for escalation  
- Applied NACL deny rules to block malicious IPs  
- Conducted geo-IP reputation analysis on attackers  
  
Posture Validation:  
- No successful compromise confirmed.  
- Full visibility across logs.  
- Containment completed within detection window.

## POST-INCIDENT ACTIVITY

**Detection Enhancements:**

1. **Automated Blocking:** Implement fail2ban for automatic IP blocking after N attempts
2. **Geographic Filtering:** Consider geo-blocking high-risk countries
3. **Account Monitoring:** Enhanced monitoring for service accounts (mysql, postgres)

**Threat Intelligence:**

1. **IP Reputation:** Integrate threat intelligence feeds for known malicious IPs
2. **Attack Attribution:** Further analysis needed on coordinated campaign timing
3. **IOC Sharing:** Submit IOCs to threat intelligence platforms

**Portfolio Documentation:**

* **MITRE ATT&CK Mapping:** T1110.001 validated through real-world attack data
* **IR Methodology:** NIST SP 800-61 framework successfully applied
* **Detection Engineering:** Custom CloudWatch alerts prove effective
* **AWS Security:** GuardDuty integration demonstrates cloud security skills

## APPENDICES

### Appendix A – Raw Log Analysis

### #Command used for analysis

### *“sudo grep "Failed password" /var/log/auth.log | grep -oE '([0-9]{1,3}\.){3}[0-9]{1,3}' | sort | uniq -c | sort -nr”*

### #Attack volume by source

### **420** 36.20.126.21

### **247** 40.81.245.51

### **245** 51.222.50.114

### Appendix B – ATT&CK Mapping

* **Tactic:** Credential Access (TA0006)
* **Technique:** Brute Force (T1110)
* **Sub-technique:** Password Guessing (T1110.001)
* **Data Source:** Logon Session (DS0028)

Report Prepared By: Yeury Perez  
Security+ Certified | AWS Security Specialist (In Progress)  
Date: September 17, 2024