Incident Response Playbook: Brute Force / SSH/RDP Attacks

Team AnubisX

Version 1.0
September 23, 2025

Document Control

Attribute	Value
Version	1.0
Status	Draft
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

This playbook defines incident response procedures for handling "Brute Force / SSH/RDP Attacks". It provides roles, responsibilities, detection indicators, containment steps, and recovery guidance to minimize impact and restore services.

1.2 Scope

This playbook applies to systems, network components, cloud services, and personnel. It is intended for use by incident responders, SOC analysts, IT operations, legal, and leadership.

2 Overview of the Attack

Brute force attacks target authentication services (SSH, RDP) attempting credential guessing at scale. Key risks include:

- Account lockouts, service disruption
- Compromise of remote admin accounts
- Unauthorized lateral movement and persistence

3 Incident Response Phases

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a brute force incident before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensics, IT, Communications).
- **Tools & Resources:** Ensure logging and centralized authentication audits are enabled. Deploy specialized detection rules and maintain playbooks for the specific alert type.
- **Training:** Conduct regular tabletop exercises for remote access compromise scenarios.
- **Hardening:** Implement regular backups and least-privilege access models.

3.2 Phase 2: Identification & Analysis

Goal: Confirm the activity and determine scope and severity.

1. **Initial Triage:** Collect authentication logs and alerts, open an incident ticket, and assemble the response team.
2. **Initial Analysis and IOC Evaluation:** Analyze logs for Indicators of Compromise (IOCs). Common IOCs include:
    - Multiple failed login attempts from single IP.
    - Rapid authentication attempts across many accounts.
    - Successful login followed by suspicious activity.

3. **Severity Level Assessment:** Severity is based on operational impact, criticality of affected systems/data, scope of attack, and detection/recovery timelines (MTTD/MTTR).

Level	Description	Example	MTTD	MTTR
Low	Limited failed attempts against single non-critical account.	Few SSH attempts from external IP blocked by firewall.	<1 hr	<24 hrs
Medium	Repeated attempts against several accounts; partial service impact.	Multiple accounts show failed SSH attempts; one compromised account isolated.	1-4 hrs	1-3 days
High	Successful compromise of administrative accounts, lateral movement.	RDP compromised for administrative user; sensitive services affected.	4-12 hrs	3-7 days
Critical	Compromise of domain admin or widespread access to sensitive systems.	Attack leads to AD account takeover and mass deployment of payloads.	12+ hrs	7-21 days

Table 1: Incident Severity Matrix

3.3 Phase 3: Containment

Goal: To limit attacker actions and preserve evidence.

- Block offending IPs, enable rate limiting and geo-blocking.
- Force password reset for targeted accounts.
- Isolate affected hosts and revoke sessions.

3.4 Phase 4: Eradication

Goal: To remove the attacker's presence and harden systems.

- Collect auth logs and memory, remove attacker-created accounts, ensure MFA is enforced.
- Harden remote access, patch RDP/SSH vulnerabilities, and rotate keys and credentials.

3.5 Phase 5: Recovery

Goal: To safely restore systems and business operations.

- Restore affected services from backups if needed.
- Reinstate hardened access controls and monitor for re-use of credentials.
- Communicate to stakeholders about service restoration.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- Conduct a blameless post-mortem and update playbooks.
- Produce a final incident report and recommended mitigations.
- Implement controls to reduce recurrence.

4 MITRE ATT&CK Framework Mapping

Brute Force / SSH/RDP Attack ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1110 – Brute Force.*
  - *T1078 – Valid Accounts.*
- **Tactic: Credential Access**
  - *T1003 – OS Credential Dumping.*
- **Tactic: Lateral Movement**
  - *T1021 – Remote Services.*
- **Tactic: Defense Evasion**
  - *T1070 – Indicator Removal on Host.*