# Incident Response Playbook: Brute-Force Attack

* Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a Brute-Force attack?
* Answer:

## Scenario

An attacker launches a brute-force or password spraying attack against internet-exposed or internal RDP services to gain access using weak or reused credentials. Successful access may lead to lateral movement, malware deployment or data exfiltration.

## Incident Classification

|  |  |
| --- | --- |
| Category | Details |
| Incident Type | Credential Attack – RDP Login Abuse |
| Severity | High (especially for privileged or sensitive systems) |
| Priority | Critical if access is gained |
| Detection Sources | SIEM, Windows Security Event Logs, EDR, IDS/IPS, Firewall logs, Threat Intel |

## Phase 1: Preparation

• Restrict RDP exposure: Use VPN, Zero Trust access, or firewall rules  
• Enforce strong authentication: Use MFA, disable default admin accounts  
• Monitor RDP login events: Enable logging for Event IDs 4625 (failed) and 4624 (success)  
• Apply account lockout policy: Limit failed login attempts  
• Deploy honeypots or decoys: Detect brute-force attempts proactively

## Phase 2: Detection and Analysis

• Alert from SIEM or EDR: Spike in failed RDP login attempts, password spraying  
• Review Event Logs: Filter Event ID 4625, identify common usernames/IPs  
• Correlate successful logins: Determine privilege escalation or lateral movement  
• MITRE ATT&CK mapping: T1110.001, T1078, T1021.001  
• Analyse attacker IPs: Check geolocation, reputation, and frequency of occurrence

## Phase 3: Containment

• Block attacker IPs: Use firewall, IDS, or VPN controls  
• Disable affected accounts: Lock/reset compromised accounts  
• Isolate affected hosts: If lateral movement or malware is suspected  
• Throttle or disable RDP: Temporarily on high-risk systems

## Phase 4: Eradication

• Remove unauthorised access: Kill sessions, reset passwords, revoke tokens  
• Patch exposed systems: Update RDP services, OS (e.g., BlueKeep)  
• Clean persistence mechanisms: Remove scheduled tasks, services, registry keys  
• Validate no lateral movement: Review EDR and logs

## Phase 5: Recovery

• Reinstate secure RDP access: Only via VPN or bastion with MFA  
• Notify users or IT teams: Communicate incidents and resets  
• Monitor closely post-incident: Watch for retry attempts  
• Conduct password audit: Enforce hygiene checks

## Phase 6: Post-Incident Activity (Lessons Learned)

• Analyse timeline: Review detection and response speed  
• Update SIEM rules: Improve brute-force detection logic  
• Revise access policies: Strengthen RDP controls  
• Share findings: With internal teams or external bodies  
• Test security controls: Ensure proper response mechanisms

## Tools Typically Involved

• SIEM (e.g., Splunk, Sentinel, QRadar)  
• EDR (e.g., CrowdStrike, Microsoft Defender for Endpoint, Cortex XDR)  
• Firewall and VPN logs (e.g., Fortinet, Palo Alto, Cisco ASA)  
• Windows Event Viewer (Event IDs: 4624, 4625, 4648, 4672)  
• Threat intelligence platforms  
• SOAR playbooks or brute-force detection scripts

## Success Metrics

|  |  |
| --- | --- |
| Metric | Target |
| Detection Time | <5 minutes from brute-force pattern onset |
| Containment Time | <30 minutes from confirmation |
| Credential Reset Time | <2 hours for compromised or targeted accounts |
| Exposure Time | No unauthorised RDP access exceeding 15 minutes |
| RDP Lockdown Coverage | 100% of internet-facing RDP endpoints secured or removed |