Title: Brute Force Attack Playbook

* 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 targeting Acme's systems?
* Answer:

1. Preparation:

Objective: Establish a robust response mechanism, educate personnel, and configure systems to detect and respond to brute force attacks.

- \*\*Prepare to Respond\*\*:

- Review and exercise brute force attack response procedures, including technical and business roles.

- Configure monitoring tools (e.g., SecGuard Log Analyzer, SecGuard Threat Analyzer) to detect malicious login attempts.

- Ensure centralized log storage via SecLogDB for detailed analysis.

- Harden backend authentication mechanisms and enforce access control measures specific to Acme’s systems.

- Establish and maintain contact details for security teams, legal representatives, and third-party vendors.

- \*\*Inform Employees\*\*:

- Conduct regular awareness campaigns to educate employees about brute force attack risks and reporting mechanisms.

- Mandate security training for personnel handling authentication systems, user databases, and patch management systems.

- Exercise brute force scenarios using tactical, operational, and strategic levels.

2. Detection and Analysis:

Objective: Detect and analyze brute force attack patterns to assess the scope and impact.

- \*\*Detect and Report\*\*:

- Use SecGuard Log Analyzer and SecGuard Threat Analyzer to monitor login attempt logs for unusual patterns.

- Identify malicious IPs targeting customer login portals, administrative panels, APIs, and backend systems.

- Report incidents via the CIRP and assign classification based on severity.

- \*\*Initial Investigation\*\*:

- Mobilize the Core IT CIRT team to investigate the incident.

- Collate data such as targeted systems, attack timelines, affected users/services, and malicious IPs.

- Validate incident categorization as a brute force attack using thresholds for login attempts and success rates.

- \*\*Incident Reporting\*\*:

- Share intelligence with other organizations via CiSP and report to regulators if necessary (e.g., ICO, NCSC).

3. Containment:

Objective: Mitigate the impact of brute force attacks on Acme's systems and users.

- \*\*Containment Actions\*\*:

- Block malicious IPs using AcmeNet Firewall.

- Enforce account lockout policies for accounts targeted by brute force attempts.

- Notify affected users via AcmeMail/AcmeUserNotification systems.

- Implement multi-factor authentication (MFA) for high-risk accounts and systems.

- Segregate critical systems from those under attack to prevent lateral movement.

4. Eradication:

Objective: Remove the threat and prevent recurring brute force incidents.

- \*\*Eradication Measures\*\*:

- Patch vulnerabilities in authentication mechanisms using AcmePatch Management System.

- Remove compromised accounts and reset passwords for affected users.

- Update monitoring rules to prevent similar attack patterns.

5. Recovery:

Objective: Restore systems and user confidence after a brute force attack.

- \*\*Assess End of Attack\*\*:

- Ensure systems targeted by the attack are operational and no longer under threat.

- Verify that affected user accounts are secure and functional.

- \*\*Rollback Mitigation Measures\*\*:

- Restore blocked IP addresses (if verified as benign) and resume normal operations.

6. Lessons Learned:

Objective: Document the incident response process, discuss lessons learned, and plan improvements.

- \*\*Incident Report\*\*:

- Draft a report detailing the attack, impact, response actions, and recommendations for future improvements.

- \*\*Lessons Identified\*\*:

- Update brute force prevention policies based on the incident analysis.

- Share findings with stakeholders and conduct root cause analysis to identify underlying vulnerabilities.

- \*\*Employee Training\*\*:

- Conduct post-incident training sessions to reinforce knowledge about brute force attack detection and response.

Appendix A: Brute Force Attack Types

- \*\*Credential Stuffing\*\*: Attackers use stolen credentials to attempt logins across multiple systems.

- \*\*Dictionary Attack\*\*: Sequential attempts using commonly used passwords.

- \*\*Reverse Brute Force Attack\*\*: Attackers use one password against multiple usernames to exploit shared credentials.

- \*\*Credential Cracking\*\*: Automated tools used to guess passwords systematically.