Title: Brute Force Login Attempts 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 login attempts targeting web apps, VPNs, or internal systems?

Answer:

1. Preparation:

Objective: Prepare systems and personnel to detect and respond effectively to brute force login attempts.

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

- Configure log monitoring tools to capture authentication events (e.g., Apache/Nginx logs, Windows Security logs, VPN/SSO provider logs).

- Maintain updated IP reputation databases for validation.

- Enforce strong password policies and multi-factor authentication (MFA) across all systems.

- Conduct regular training sessions with IT and security teams on brute force detection and mitigation strategies.

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

- Conduct awareness campaigns on risks associated with brute force attacks.

- Mandate security training for employees managing accounts and authentication systems.

2. Detection and Analysis:

Objective: Detect brute force activity and validate its authenticity.

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

- Look for multiple failed login attempts (e.g., HTTP 401 errors, Windows Event ID 4625).

- Monitor spikes in login attempts from the same IP or user.

- Identify any successful logins following multiple failures.

- \*\*Validation Steps\*\*:

- Confirm high volume of failed logins within a short timeframe.

- Cross-check offending IP addresses with known bad IP reputation databases.

- Investigate successful logins post-failure for potential compromise.

3. Containment:

Objective: Mitigate the impact of brute force login attempts on targeted systems.

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

- Block offending IP addresses at the firewall or web application firewall (WAF).

- Disable affected user accounts immediately.

- Force password resets for compromised accounts with MFA enforcement.

4. Eradication:

Objective: Remove the threat and prevent further compromise.

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

- Verify there are no persistence mechanisms or lateral movement in the system.

- Check for signs of privilege escalation or unauthorized data access.

5. Recovery:

Objective: Restore affected systems and accounts to a secure operational state.

- \*\*Recovery Actions\*\*:

- Re-enable user accounts with new credentials and MFA enforced.

- Tune detection rules to reduce false positives and improve detection accuracy.

6. Lessons Learned:

Objective: Evaluate response effectiveness and implement improvements.

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

- Document the timeline, actions taken, and impact of the brute force attack.

- Include recommendations for enhancing detection and response mechanisms.

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

- Assess whether detection rules were tuned effectively.

- Review MFA enforcement and identify areas for expansion.

Appendix A: Indicators of Brute Force Login Attempts

- \*\*Failed Login Attempts\*\*: HTTP 401 errors, Windows Event ID 4625.

- \*\*Spike in Login Activity\*\*: High volume of login attempts from the same IP address or user.

- \*\*Successful Logins Post-Failure\*\*: Successful authentication after multiple failures.