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 to compromised credentials incidents effectively?

Answer:

Title: Incident Response Playbook for Compromised Credentials

1. Preparation:

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

- \*\*Cybersecurity Incident Response Team (CSIRT)\*\*:

- \*\*Core Members\*\*: Include individuals responsible for cybersecurity and IT roles, depending on organization size. Keep the team small for confidentiality and efficiency.

- \*\*Extended Members\*\*: Include Legal, Compliance, Public Relations, and Executive Leadership for high-severity incidents.

- \*\*Roles and Responsibilities\*\*: Assign and document clear responsibilities for all members. Ensure redundancy for critical roles.

- \*\*Escalation Paths\*\*: Define escalation paths to handle incidents that evolve in severity.

- \*\*Logging\*\*:

- Ensure appropriate logging levels for account login systems (Active Directory, VPN, Remote Access, etc.) with a minimum retention of 90 days.

- Store logs securely, preferably on a secondary system like a SIEM.

2. Detection and Analysis:

Objective: Detect the incident, determine its scope, and involve appropriate parties.

- \*\*Evidence Collection\*\*:

- Gather evidence leading to notification of compromise (e.g., phishing emails, abnormal login behavior, unexplained user actions).

- \*\*Method Identification\*\*:

- Determine the method of compromise (e.g., phishing, credential scraping, brute force attacks).

- Interview impacted users to identify potential points of compromise:

- Suspicious emails or links clicked.

- Unexpected software downloads or document attachments.

- Abnormal workstation behavior.

- \*\*Search for Indicators\*\*:

- Search for phishing emails containing credential harvesting links.

- Check user web history for malicious sites.

- Investigate malware on user workstations (e.g., credential harvesters, keystroke recording software).

- \*\*Environment Analysis\*\*:

- Use Indicators of Compromise (IoCs) to identify other victims and track the infection across the organization.

- Query email systems, SIEM logs, and login databases for anomalies (e.g., unusual locations, browser fingerprints).

- \*\*Sensitive Information Assessment\*\*:

- Evaluate victim accounts for sensitive information access, including centralized storage (OneDrive, Google Drive, SharePoint, shared mailboxes).

- Consult legal counsel if sensitive data exposure is possible.

3. Containment:

Objective: Mitigate the attack’s effects on the targeted environment.

- \*\*Account Actions\*\*:

- Reset all passwords associated with identified victims. Disable compromised accounts.

- Enable Multi-Factor Authentication (MFA) for impacted accounts.

- Revoke authentication tokens for victim accounts across email systems and other platforms.

- \*\*External Notifications\*\*:

- Notify external organizations of compromises if relevant. Work with legal counsel during this process.

- Block identified external domains from sending emails to the organization.

- \*\*Malware Handling\*\*:

- Preserve malware samples and analyze them using tools (e.g., VirusTotal, Hybrid-Analysis).

- Submit file hashes for community analysis and characteristics identification.

- Isolate infected systems without powering them off. Preserve systems for forensic investigations.

- Block IoCs (URLs, domains, message IDs, file hashes, IPs) through email systems, firewalls, and endpoint protection.

4. Eradication:

Objective: Take actions to remove the threat and avoid future incidents.

- \*\*Artifact Preservation\*\*:

- Preserve artifacts, systems, and backups for forensic analysis.

- Save physical hard disks, solid-state drives, or forensically sound images of storage drives.

- Collect volatile data (log files, backups, malware samples, memory images) from affected systems.

- \*\*System Recovery\*\*:

- Rebuild or replace compromised systems using clean backups or known-good images.

5. Recovery:

Objective: Restore systems to normal operations.

- \*\*System Restoration\*\*:

- Restore impacted systems from clean backups taken prior to infection.

- Rebuild machines from bare metal if backups are unavailable.

- \*\*Remediation Actions\*\*:

- Address vulnerabilities identified during the investigation.

- Reset passwords for impacted accounts and create replacement accounts where necessary.

- Monitor for residual malicious activity using configured alerts.

6. Lessons Learned:

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defenses.

- \*\*Post-Incident Review\*\*:

- Conduct a meeting to analyze investigation successes, failures, and identified vulnerabilities.

- \*\*Documentation\*\*:

- Create a detailed report covering the incident’s cause, actions taken, timeline, successes, failures, and cost.

- Share the report with relevant teams.

- \*\*Security Enhancements\*\*:

- Review and update security measures:

- Authentication practices

- Multi-Factor Authentication

- Password complexity

- Network segmentation

- Firewall configurations

- Application security

- Patch management procedures

- Enhance training programs to include lessons learned and updated scenarios.