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 phishing attacks effectively?

Answer:

Title: Phishing Attack Playbook

1. Preparation:

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

- \*\*Security Controls\*\*:

- Deploy email filtering solutions to detect and block phishing emails.

- Enable domain-based email authentication (e.g., SPF, DKIM, DMARC).

- Use anti-phishing browser extensions and tools for employees.

- Regularly update email clients and security software.

- \*\*Asset Inventory\*\*:

- Maintain an inventory of business-critical email accounts and systems.

- Identify high-value targets (e.g., executives, HR, and finance personnel).

- \*\*Access Controls\*\*:

- Enforce MFA for all email accounts, especially for privileged users.

- Regularly audit and update access permissions for sensitive data.

- \*\*Monitoring Tools\*\*:

- Configure SIEM tools to monitor:

- Unusual email login locations.

- Sudden email forwarding rule changes.

- Suspicious email activity, such as mass outbound emails.

- \*\*Incident Drills\*\*:

- Simulate phishing attacks (e.g., spear-phishing exercises) to assess employee awareness.

- Train employees to recognize phishing indicators, such as mismatched domains and suspicious links.

2. Detect:

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

- \*\*Identify Threat Indicators\*\*:

- \*\*Alerts\*\*:

- \*\*Email Gateway\*\*:

- Detection of malicious attachments or links.

- \*\*SIEM\*\*:

- Login attempts from unusual locations or devices.

- \*\*Logs\*\*:

- \*\*Email Server Logs\*\*:

- Emails containing suspicious links or attachments.

- Anomalies in sent or received email volumes.

- \*\*User Reports\*\*:

- Suspicious emails forwarded to the security team.

- \*\*Identify Risk Factors\*\*:

- \*\*Common Risks\*\*:

- Credential theft via phishing pages.

- Data exfiltration or unauthorized access to accounts.

- \*\*Company-Specific Risks\*\*:

- Financial fraud through compromised accounts.

- Breach of sensitive customer or employee data.

- \*\*Data Collection\*\*:

- Analyze email headers for sender IPs and domains.

- Inspect URLs for signs of phishing (e.g., typosquatting, shortened links).

- Retrieve user activity logs for suspicious actions after clicking links.

- \*\*Categorize\*\*:

- \*\*Phishing Types\*\*:

- Spear Phishing: Targeted at specific individuals or departments.

- Whaling: Targeting executives or high-profile employees.

- Clone Phishing: Mimicking legitimate emails.

- \*\*Is it an Advanced Attack?\*\*:

- Indicators include:

- Use of compromised legitimate email accounts.

- Sophisticated phishing kits with evasion techniques.

- Multi-stage attacks involving malware or additional phishing.

- \*\*Triage\*\*:

- Prioritize incidents involving:

- High-value accounts (e.g., executives, finance).

- Access to sensitive data or financial systems.

- \*\*False Positive Assessment\*\*:

- Validate suspicious emails by cross-referencing with legitimate communications.

- Confirm with users if unusual activities (e.g., new email rules) were intentional.

3. Analyze:

Objective: Verify the attack, evaluate its scope, and correlate findings with threat intelligence.

- \*\*Verify\*\*:

- Reproduce email actions in a secure environment (e.g., opening links in isolated browsers).

- Check for phishing indicators in the email's content, attachments, and URLs.

- \*\*Identify IOCs\*\*:

- Common indicators include:

- Phishing domains or URLs.

- Email sender addresses and IPs.

- Malicious attachments (e.g., .exe, .xlsm).

- \*\*Extract IOCs\*\*:

- Document all malicious indicators, including timestamps and user interactions.

- \*\*Submit to Partners\*\*:

- Share phishing indicators with email security vendors and threat intelligence providers.

- \*\*Scan Enterprise\*\*:

- Check other users for emails from the same sender or with similar indicators.

- Monitor for additional login attempts or suspicious activities linked to phishing.

4. Contain/Eradicate:

Objective: Mitigate the attack’s effects and remove the threat.

- \*\*Contain the Threat\*\*:

- Block phishing domains and sender IPs at the email gateway.

- Quarantine suspicious emails from all user inboxes.

- Reset credentials for affected accounts immediately.

- \*\*Eradicate the Root Cause\*\*:

- Remove malicious email rules or auto-forwarding set by attackers.

- Strengthen email authentication (e.g., SPF, DKIM, DMARC).

- \*\*Validate\*\*:

- Conduct phishing tests to ensure users recognize similar future threats.

- Review logs to confirm no residual malicious activity.

5. Recover:

Objective: Restore systems and email services to normal operations.

- \*\*Restore Operations\*\*:

- Re-enable affected accounts and email services after thorough checks.

- Notify impacted users about the steps taken and additional precautions.

- \*\*Communicate\*\*:

- Inform stakeholders of the incident resolution and preventive measures implemented.

6. Lessons Learned:

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

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

- Review how the phishing email bypassed existing security controls.

- \*\*Strengthen Security\*\*:

- Update employee training programs with lessons from the incident.

- Strengthen detection and response procedures for email-based threats.

- Update the playbook with new phishing tactics and IOCs.