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 suspicious network activity effectively?

Answer:

Title: Incident Response Playbook for Handling Suspicious Network Activity

1. Preparation:

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

- \*\*Intrusion Detection Systems (EDR, NIPS, IPS)\*\*:

- Ensure monitoring tools are updated and functional.

- Maintain contacts with network and security operation teams.

- Define and communicate alert notification processes to relevant parties.

- Verify access to devices and ensure monitoring capabilities for concerned perimeters.

- Ensure endpoint and area isolation capabilities using EDR or Firewall.

- \*\*Network\*\*:

- Maintain an up-to-date inventory of network access points with versioning.

- Provide current network maps and configurations to network teams, emphasizing concerned zones and operational teams.

- Regularly close unwanted network access points.

- Monitor VPN and Cloud access, especially from rare locations.

- Deploy and monitor traffic management tools.

- \*\*Baseline Traffic\*\*:

- Identify baseline traffic and critical business flows.

- Train personnel on effective use of monitoring tools.

- Ensure operational logs are retained for more than six months.

2. Detection and Analysis:

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

- \*\*Sources of Detection\*\*:

- Notifications from users or helpdesk.

- IDS/IPS/NIDS/EDR logs, alerts, and reports.

- Firewall and proxy logs.

- Detection by network staff.

- Honeypots or deceptive solutions.

- External complaints.

- \*\*Record Suspicious Network Activity\*\*:

- Use network capture tools (tshark, windump, tcpdump) to gather malicious traffic.

- Engage the incident response team for network forensics.

- Use port mirroring or a hub to collect valuable data from affected LANs.

- \*\*Analyze the Attack\*\*:

- Review IDS alerts and network device logs.

- Map malicious traffic to business risks for prioritization.

- Identify technical characteristics such as:

- Source IP addresses

- Ports used, TTL, Packet ID, protocols

- Targeted machines/services

- Exploits and remote accounts logged in

- Forensic Investigations:

- Determine impacted machines and modus operandi of the attack.

- Refer to specific intrusion response procedures for compromised computers.

3. Containment:

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

- \*\*Strategic Response\*\*:

- Activate a crisis management cell for strategic issues.

- \*\*Network Isolation\*\*:

- Disconnect compromised areas from the network.

- Isolate affected computers for deeper investigation.

- \*\*Mitigation Controls\*\*:

- Implement MFA and geo-filtering for critical flows in agreement with business managers.

- Terminate unwanted connections or processes on affected machines.

- Use firewall/IPS/EDR rules to block malicious traffic.

- Update IDS rules to match malicious behavior and notify technical staff.

- \*\*Ad Hoc Actions\*\*:

- Deny egress destinations in EDR, proxies, and firewalls.

- Configure security controls to reject connections from compromised machines.

- Limit access to critical and confidential data.

- Create booby-trapped documents with watermarking for theft-proofing.

- Notify business users about required and forbidden actions.

- Configure verbose logging on targeted environments and store logs securely.

4. Eradication:

Objective: Take actions to stop malicious behavior.

- \*\*Block the Source\*\*:

- Identify and block communication channels used by attackers.

- Involve management, HR, and legal teams for insider threats.

- Engage abuse teams and law enforcement for external threats.

- \*\*Technical Remediation\*\*:

- Define and validate a remediation process with the incident response team.

- Use intrusion response procedures for different operating systems.

- \*\*Test and Enforce\*\*:

- Test the remediation process to ensure no service damage.

- Apply the validated process approved by IT and business teams.

5. Recovery:

Objective: Restore systems to normal operations.

- \*\*Traffic Restoration\*\*:

- Ensure network traffic returns to normal.

- Gradually re-allow connections to previously contained network segments.

- \*\*Authentication and Infrastructure Recovery\*\*:

- Follow detailed steps for recovery, ensuring careful monitoring and execution.

6. Lessons Learned:

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

- \*\*Report\*\*:

- Document the incident cause, actions taken, timelines, successes, failures, cost, and indicators of compromise.

- Share the report with relevant actors.

- \*\*Capitalize\*\*:

- Reflect on preparation steps to improve response efficiency.

- Update contact lists with effective methods for involved parties.

- Strengthen relationships inside and outside the organization for future incident handling.

- Review and enhance DKIM, SPF, and DMARC filters.

- Collaborate with legal teams for necessary actions.

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

- Conduct a meeting to analyze what went well, what didn’t, and areas for improvement.

- Update incident response plans and processes based on findings.