Task#3
Developing an Incident Response Plan

Best Practices for Effective Incident Management

Rayyan Alam

22 August 2024

Introduction

Objective:

- To create a structured approach for responding to and managing security incidents.
- Minimize damage and facilitate quick recovery.

Importance:

- Ensures systematic handling of security breaches.
- Helps in minimizing downtime and loss.

Key Components of an Incident Response Plan

1. Identifying Potential Security Incidents and Scenarios

- **Types of Incidents:**
  - **Data Breaches:** Unauthorized access to sensitive data.
  - **Ransomware Attacks:** Encryption of files demanding ransom.
  - **Insider Threats:** Malicious activities by employees.
  - **Denial-of-Service (DoS) Attacks:** Overloading services to cause disruption.
- **Risk Assessment:**
  - Identify threats and vulnerabilities.
  - Create scenarios based on potential risks.

2. Defining Roles and Responsibilities

Incident Response Team (IRT):

- **Incident Commander:** Oversees the incident response.
- **Technical Lead:** Handles technical analysis and resolution.
- **Communications Lead:** Manages internal and external communications.
- **Legal Advisor:** Ensures legal compliance and documentation.

Importance of Clear Roles:

- Ensures efficient handling of incidents.
- Reduces confusion and overlap in responsibilities.

3. Developing Response Procedures

1. **Detection:**
    - Monitor systems using tools like Nmap and Snort.
2. **Containment:**
    - Isolate affected systems to prevent further spread.
3. **Eradication:**
    - Remove threats using tools like ClamAV.
4. **Recovery:**
    - Restore systems from backups and validate integrity.
5. **Lessons Learned:**
    - Review incidents to improve future responses.

4. Conducting Training and Simulation Exercises

- **Importance:**
  - Prepares the team for real-world scenarios.
  - Identifies gaps in the plan and improves readiness.
- **Types of Exercises:**
  - **Tabletop Exercises:** Discuss scenarios and response strategies(discussion-based sessions where team members meet in an informal, classroom setting to discuss their roles during an emergency and their responses to a particular emergency situation.).
  - **Full-Scale Simulations:** Simulate real incidents and practice response.

5. Reviewing and Updating the Plan

- **Regular Reviews:**
  - Ensure the plan remains effective with evolving threats.
  - Update based on lessons learned from incidents and exercises(Keep stakeholders informed of any updates or changes, and establish transparent communication channels for reporting incidents).
- **Frequency:**
  - Conduct reviews and updates at least annually or after significant incidents.(It's important to conduct reviews and updates of your plan at least annually or after significant incidents to ensure its effectiveness against evolving threats. Additionally, updating the plan based on lessons learned from incidents and exercises can help improve security measures and response strategies.)

Tools and Techniques

- **Nmap:** used to discover hosts and services on a computer network. It operates mainly as a network scanner, analyzing IP addresses and ports by sending packets to detect devices and their services. It is available for various operating systems, including Linux, Windows, and UNIX..
- **Wireshark:** used for capturing and analyzing packets from network connections.
- **Snort:** For intrusion detection. lightweight network intrusion detection system (NIDS) and intrusion prevention system (IPS)
- **ClamAV:** For malware scanning.antivirus engine designed for detecting trojans, viruses, malware, and other malicious threats.

Ports Scan Results

- Conduct an Nmap scan on the IP address `192.168.1.1`.
- **Findings:**
  - **Open Ports:**
    - Port 22 (SSH) - Open
    - Port 80 (HTTP) - Open
    - Port 443 (HTTPS) - Open

- **Vulnerabilities:**
  - Outdated SSH version, potential for brute-force attacks.
  - HTTP server running an older version, susceptible to known vulnerabilities.
- **Response Action:**
  - Update the SSH server to a more secure version.
  - Apply security patches to the HTTP server.
  - Strengthen firewall rules to restrict access to critical services.

Conclusion

- Developing and maintaining an effective Incident Response Plan is crucial for the security and resilience of any organization.
- By identifying potential threats, defining clear roles, and conducting regular training and updates, organizations can minimize damage, ensure quick recovery, and continuously improve their readiness for future incidents.
- The integration of proper tools and regular reviews enhances the overall effectiveness of the response strategy, ultimately safeguarding the organization's assets and reputation.

THANK YOU