Cybersecurity Internship Tasks

Name: Safiullah Shahid

Assignment: Task # 3

Position: Cyber Security Intern

Department: Cyber Security

Date of Submission: July 23, 2024

Company: Digital Empowerment

To develop an incident response plan we will be using ClamAV, Snort, Wireshark, and Nmap, we'll break down the process into smaller steps. Please note that these tools are primarily used for threat detection and analysis, but we can utilize them to gather information and simulate scenarios for incident response planning.

Step 1 Identifying Potential Security Incidents and Scenarios

1) Use Nmap to scan the target IP (192.168.67.132) and gather information about open ports and services:

```
CMD: nmap -sS -O 192.168.67.132
```

Open ports and services potential entry points for attackers		
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

2) Use Snort to monitor network traffic and identify potential security incidents:

```
CMD: snort -i eth0 -c /etc/snort/snort.conf -l /var/log/snort
```

Nothing Intesting Found

Step 2 Incident Response Team Roles

Incident Response Team Lead:

- Oversees the entire incident response process
- Coordinates the efforts of team members
- Makes critical decisions during incidents
- Communicates with stakeholders and senior management

Network Administrator:

- Isolates affected systems or networks to contain the incident
- Monitors network traffic for suspicious activity
- Restores network connectivity after the incident

Security Analyst:

- Identifies and analyzes threats and vulnerabilities
- Investigates security incidents
- Implements security measures to prevent future attacks

System Administrator:

- Restores affected systems to a known good state
- Applies patches and updates to address vulnerabilities
- Provides technical support to other team members

Additional Roles:

- **Digital Forensics Analyst:** Collects and analyzes digital evidence
- **Public Relations Specialist:** Communicates with external stakeholders during incidents
- **Legal Counsel:** Provides legal guidance and advice
- **Business Continuity Planner:** Ensures that business operations can continue after an incident

Step 3 Developing step-by-step response procedures

1. Initial Response

- **Alert the Team:**
  - Notify the Incident Response Team (IRT) members through established communication channels (e.g., phone, email, messaging apps).
  - Ensure that all relevant team members are aware of the incident and their roles.
- **Contain the Incident:**
  - Isolate affected systems or networks to prevent further damage.
  - Disable unnecessary services or network connections.
  - Implement temporary security measures (e.g., firewall rules, intrusion detection systems) to contain the threat.

2. Assessment

- **Gather Information:**
  - Collect relevant logs, system information, and network traffic data.
  - Interview affected users or employees.
- **Analyze Logs and Data:**
  - Examine logs for suspicious activity, unusual patterns, or known indicators of compromise (IOCs).
  - Use security tools to analyze network traffic and identify potential threats.
- **Identify the Root Cause:**
  - Determine the origin of the incident and the specific vulnerabilities exploited.
  - Identify any weaknesses in existing security measures.

3. Eradication

- **Remove Malware:**
  - Use antivirus software and specialized tools to detect and remove any malware or malicious code.
  - Clean infected systems and restore them to a known good state.
- **Patch Vulnerabilities:**
  - Apply necessary software updates and patches to address the vulnerabilities exploited by the attackers.
  - Ensure that all systems are up-to-date with the latest security patches.

4. Recovery

- **Restore Systems:**
  - Restore affected systems from backups or rebuild them from scratch.
  - Ensure that data integrity and consistency are maintained during the recovery process.
- **Restore Data:**

    - Recover any lost or corrupted data from backups.
    - Verify the integrity of restored data.

5. Post-Incident Activities

- **Review the Incident:**
    - Conduct a thorough review of the incident to identify lessons learned and areas for improvement.
    - Document the incident response process, including any challenges or successes.
- **Update the Plan:**
    - Revise the incident response plan based on the findings of the review.
    - Incorporate new procedures or best practices to improve future responses.
- **Implement Preventive Measures:**
    - Implement additional security measures to prevent similar incidents from happening again.
    - Enhance security awareness training for employees.

Step 4 Conducting training and simulation exercises

1) Use ClamAV to simulate a malware outbreak

```
CMD: clamdscan -i -r /path/to/malware/sample
```

This will help test the response team's ability to detect and respond to malware incidents.

2) Use Wireshark to simulate a network attack:

```
CMD: wireshark -i eth0 -Y "http.request"
```

This will help test the response team's ability to analyze network traffic and identify suspicious activity.

Step 5 Reviewing and updating the plan regularly

1) Schedule regular review and update sessions for the incident response plan
2) Incorporate lessons learned from training exercises and real-world incidents
3) Ensure the plan remains relevant and effective