TASK 3

Cyber Security Internship Report

DIGITAL EMPOWERMENT NETWORK

Presented to:

Digital Empowerment Network

Presented by:

Ali Aitazaz [LinkedIn]

+92 332 5890142

www.digitalempowermentnetwork.org

Contents

Incident Response Plan

Executive Summary

- **Date:** August 14, 2024
- **System:** C-ICAP
- **Host IP:** 192.168.1.10
- **Reported by:** C-ICAP Antivirus Service
- **Event Type:** Virus Detection and Mitigation
- **Affected Systems:** LAN device with IP 192.168.1.10
- **Incident Severity:** Low
- **Status:** Resolved

1. *Detection*

- Log Analysis:
  - Regularly review and analyze Wazuh logs to identify malware detections and unusual activities.
- Alert Configuration:
  - Set up alerts for the detection of known malware types and suspicious URLs.

2. *Analysis*

- Verify Alerts:
  - Validate the authenticity of the detections. Confirm whether they are actual threats or test files.
- Impact Assessment:
  - Determine if the malware has caused any harm or data breaches.
- Investigate Source:

- Examine the source IP (192.168.1.10) to identify the origin of the threat and assess potential impact.

3. *Containment*

- Isolate Affected Systems:
  - Disconnect the affected machine (192.168.1.10) from the network to prevent further spread of the malware.
- Block Malicious URLs:
  - Update firewall rules or web filters to block access to the identified malicious URLs.

4. *Eradication*

- Remove Malicious Files:
  - Perform a full system scan and remove any detected viruses or malicious files.
- Update Signatures:
  - Ensure antivirus and security systems have the latest virus definitions and signatures.

5. *Recovery*

- System Restoration:
  - Restore affected systems from clean backups to a known good state.
- Monitor Systems:
  - Continuously monitor the systems for any signs of residual malware or further issues.

6. *Post-Incident Review*

- Incident Analysis:
  - Review the incident to understand what occurred and why.
- Update Procedures:
  - Revise incident response procedures and policies based on lessons learned from the incident.
- Training:
  - Provide training to relevant personnel on new threats and updated response strategies.

7. *Conclusion*

The logs indicate several instances of virus detections involving both test files and known malware types. The incident response plan outlined adheres to industry standards, covering detection, analysis, containment, eradication, and recovery processes.

8. *Industry Standards*

The incident response plan is based on the following industry standards:

1. NIST Special Publication 800-61 Rev. 2: Computer Security IncidentHandling Guide
    - Provides guidelines for creating an incident response capability and handlingincidents efficiently.
2. ISO/IEC 27035:2016 - Information technology — Security techniques — **Incident management**
    - Offers a framework for incident management including detection, response, andrecovery.
3. SANS Institute - Incident Handler's Handbook
    - Outlines practical steps for incident handling, including detection, analysis,containment, eradication, and recovery.
4. CIS Controls - CIS Control 17: Incident Response Management
    - Provides best practices for incident response management, includingpreparation, detection, and response strategies.

These standards ensure a comprehensive approach to incident response, leveraging best practices and proven methodologies to handle security incidents effectively.

About the Company

At Digital Empowerment, we envision a future where youth are equipped with the skills, knowledge, and mindset needed to thrive in a rapidly evolving world. Our mission is to bridge the digital divide, foster leadership development, and enhance academic growth, empowering young minds to realize their full potential.

To achieve this, we offer comprehensive virtual internships across various domains, providing students with invaluable hands-on experience and practical skills essential for success. Furthermore, we are committed to assisting exceptional students in securing positions at prestigious companies, helping to launch their careers and build a brighter future for themselves and future generations.

Digital Empowerment Pakistan

Author's Note

This incident response plan was meticulously crafted to ensure a comprehensive approach to managing security incidents, particularly focusing on virus detection and mitigation. Each phase of the plan—detection, analysis, containment, eradication, and recovery—was designed with clarity and precision, providing actionable steps that align with industry standards such as NIST SP 800-61, ISO/IEC 27035, and CIS Controls.

The plan emphasizes the importance of a structured response, integrating best practices from leading frameworks while being tailored to the specific needs of the C-ICAP system. By incorporating a thorough post-incident review and referencing relevant standards, this document serves not only as a guide for immediate action but also as a tool for continuous improvement and preparedness against future threats.

This plan reflects a commitment to maintaining a strong security posture, ensuring that incidents are handled efficiently and effectively, with lessons learned being systematically integrated into future responses.