Assignment 2: Incident

Name : Andrei Cirlig

SRN:20049583

This document outlines an approach to addressing a cybersecurity breach classified as an Advanced Persistent Threat (APT). No changes in content have been made. The objectives of this strategy are to contain the breach, eradicate the threat, and recover from the incident. By effectively implementing these steps, we aim to minimize operational disruptions and reputational damage to our organization resulting from the APT incident. The language used is clear, objective, and value-neutral, with a formal register and precise word choice. The structure is logical and follows a clear progression, with causal connections between statements. The text is free from grammatical errors, spelling mistakes, and punctuation errors. This approach aims to minimize operational disruptions and reputational damage to our organization resulting from the breach.

Advanced Persistent Threats (APTs) are sophisticated cyber attacks that pose a significant risk to organizations. These threats are characterized by their secretive nature, long-lasting presence, and advanced methods of operation. APTs can result in unauthorized access to sensitive data, disruption of operations, and reputational damage. It is crucial for organizations to have a well-defined strategy to address APT incidents and minimize their impact. The current situation facing our organization involves an unauthorized intrusion into our server network. This intrusion is believed to have started several weeks ago and was discovered through the identification of aberrant directory structures on a server. It is crucial to address this incident promptly and effectively to prevent further unauthorized access and mitigate the potential damage. This report explores the ramifications of such threats and emphasizes the need for an effective and proactive response strategy.

**Incident response plan**

**Initial Response**

Subsequent to the identification of aberrant directory structures on a server, our Incident Response Team (IRT) was promptly mobilized. The nascent stages of our response encompassed the following measures:

1. **Securing the Scene**: This involved the immediate isolation of the affected server with the dual objectives of forestalling any further unauthorized modifications and averting potential data losses.
2. **Notification**: Expedient communication was initiated with pivotal stakeholders, encompassing the echelons of senior management and the IT security contingents.
3. **Documentation**: There was a systematic recording of all initial findings, accompanied by a thorough documentation of the preliminary actions undertaken.

**Team Composition**

The composition of our Incident Response Team is as follows:

Team Lead: This individual bears the responsibility for orchestrating the investigation, ensuring effective coordination amongst disparate team members.

Forensic analysts: They are charged with the collection and meticulous analysis of digital evidence.

Security specialists: They are tasked with discerning the precise nature of the breach and formulating appropriate containment strategies.

Legal Advisor: Their role is pivotal in guaranteeing compliance with the prevailing legal and regulatory frameworks.

Communication Officer: They are entrusted with the management of all internal and external communications pertinent to the incident.

**Investigation Methodology**

**Evidence Collection**

The evidence collection phase constitutes a cornerstone of the forensic investigation and encompasses several critical steps:

* **Disk Imaging**: This process entails the creation of exact, bit-by-bit replicas of the compromised drives. Utilizing tools such as DD or Clonezilla, this method ensures a verbatim copy of all data, permitting detailed examination without risking the integrity of the original evidence.
* **Log Analysis**: A meticulous examination of various log files, including server, firewall, and application logs, is conducted. This analysis is pivotal for identifying signs of unauthorized access and other anomalous activities that deviate from normal operational patterns.
* **Network Traffic Analysis**: The deployment of sophisticated tools like Wireshark or TCPDump is essential in this phase. These tools enable in-depth scrutiny of incoming and outgoing network traffic, aiding in the detection of suspicious patterns or anomalies that may indicate malicious activity.

**Timeline Reconstruction**

Reconstructing the timeline of events is a critical endeavour in understanding the attack's chronology.

* **Log Correlation**: This involves the synchronization of disparate log entries to construct a coherent timeline of the attack, thereby elucidating the sequence and interrelation of events.
* **Data Recovery**: Leveraging tools such as TestDisk, efforts are made to retrieve data that has been altered or expunged. This step is crucial in piecing together the attacker’s actions and understanding the full scope of the breach.

**Root Cause Analysis**

Root cause analysis is focused on unravelling the specifics of the breach.

* **Entry Points**: Determining the initial vector of the intrusion is paramount. This could involve identifying tactics such as phishing, exploitation of unpatched system vulnerabilities, or the leverage of weak authentication credentials.
* **Lateral Movements**: Tracing the trajectory of the intruder within the network infrastructure is essential to gauge the extent and reach of the breach.
* **Vulnerabilities Exploited**: A critical part of this analysis is the identification of specific software vulnerabilities or configuration flaws that the attacker might have exploited to gain unauthorized access.

**Forensic Tools**

A suite of specialized forensic tools will be employed in the investigation:

* **Encase and FTK**: These tools are instrumental for comprehensive disk and file analysis, enabling deep dives into data storage and retrieval processes.
* **Wireshark**: Primarily utilized for network packet inspection, Wireshark facilitates a granular analysis of network communications.
* **Custom Scripts**: The use of bespoke scripts is planned for the automation of specific analytical tasks and the parsing of unique log formats, enhancing the efficiency and efficacy of the investigative process.

**Containment Strategies**

Upon identifying the breach, immediate steps were taken to contain the incident:

* **Network Segmentation**: Isolating the affected server to prevent lateral movement of the threat.
* **Access Control Changes**: Resetting passwords and disabling remote access to prevent further unauthorized entry.
* **Traffic Restriction**: Implementing firewall rules to block suspicious external connections.

The objective during this phase is to prevent further damage while maintaining critical business operations.

**Eradication and Recovery**

**Eradication Measures**

After containment, the focus shifts to eradicating the threat:

* **System Cleansing**: Removing malware, backdoors, and any other tools installed by the attacker.
* **Patch Management**: Applying updates to fix vulnerabilities exploited in the attack.
* **Verification**: Ensuring that all malicious components are removed from the system.

**Recovery Process**

The recovery phase includes:

* **System Restoration**: Using clean backups to restore affected systems.
* **Data Integrity Checks**: Verifying that restored data is complete and unaltered.
* **Monitoring**: Continuously monitor the systems for signs of recurring malicious activity.

**Post-Incident Activities**

**Lessons Learned**

A review meeting will be held to discuss:

* **Incident Analysis: Evaluating the response effectiveness and areas for improvement. For example, identifying any delays in detection and response, gaps in security measures, or weaknesses in incident management processes.**
* **Knowledge Sharing: Disseminating the findings across the organization to prevent similar incidents. This could involve conducting training sessions, creating awareness materials, or implementing new policies and procedures based on the lessons learned.**

**Report Writing**

Comprehensive documentation of the incident will be maintained, detailing:

* **Incident Timeline**: A chronological account of the incident and the response.
* **Action Taken**: A record of all decisions and actions taken during the incident.

**Future Prevention Strategies**

To mitigate future risks, the following recommendations are proposed:

**Enhanced Security Infrastructure**: Upgrading security tools and technologies to detect and prevent sophisticated attacks. For example, implementing advanced threat detection systems, enhancing network segmentation, and deploying intrusion detection and prevention systems.

**Regular Employee Training**: Conducting ongoing cybersecurity awareness training for all staff members. This could include educating employees about common phishing techniques, promoting strong password practices, and raising awareness about social engineering tactics.

**Continuous Monitoring and Auditing**: Implementing round-the-clock surveillance of our network and regular security audits to identify and address vulnerabilities proactively. This could involve implementing security information and event management (SIEM) systems, conducting penetration testing, and performing regular vulnerability assessments.

This report has outlined a structured approach to responding to an APT incident. The containment, eradication, and recovery processes are critical in mitigating the impact and preventing recurrence. Ongoing vigilance and improvement of security practices are essential in the ever-evolving landscape of cyber threats. Regular updates and enhancements to our cybersecurity protocols should be implemented to stay ahead of emerging threats. Additionally, establishing a strong incident response team and conducting regular drills can help ensure a swift and effective response in the event of an APT incident.