Cybersecurity Documentation Project

I. Vulnerability Assessment Report

2nd May 2024

System Description

The server hardware consists of a powerful CPU processor and 128GB of memory. It runs on the latest version of Linux operating system and hosts a MySQL database management system. It is configured with a stable network connection using IPv4 addresses and interacts with other servers on the network. Security measures include SSL/TLS encrypted connections.

Scope

The scope of this vulnerability assessment relates to the current access controls of the system. The assessment will cover a period of three months, from March 2024 to May 2024. NIST SP 800-30 Rev. 1 is used to guide the risk analysis of the information system.

Purpose

The database server hosts valuable PII of the e-commerce company's customers. If this information is not secure, not only will business operations be halted, but the company could face fines for not complying with required data safety practices (e.g. GDPR) and leaving private data publicly available. Many of the firm's employees work remotely and use the remote server to access the internal network and do their jobs. If the server goes offline, the company's operations would grind to a halt, resulting in significant losses and regulatory fines.

Risk Assessment

Threat source	Threat event	Likelihood	Severity	Risk
E.g. Competitor	*Obtain sensitive information via exfiltration*	*3*	*3*	*9*
Hacker	*Install persistent and targeted network sniffers*	*2*	*3*	*6*
Malicious Software	*Alter/Delete critical information*	*2*	*3*	*9*

Approach

The aforementioned risks are identified as most likely because of the fact that the company uses a public server. This makes it easy it significantly easier for threat actors to infiltrate it by increasing the attack surface and damaging the confidentiality, integrity of availability of the server's data. Because this is an e-commerce company, competitors would have a lot to gain to accessing internal information by exploiting the company's public server. A public server is also a textbook target for individual hackers and hacker groups because of the multiple attack vectors that they could employ infiltrate it. Threat actors such as these can easily inject malware into the exposed internal system of the company which can do all kinds of damage such as altering or deleting critical information. The current analysis is only a small example of the possible ways that the company's information security could be compromised.

Remediation Strategy

This section provides specific and actionable recommendations to remediate or mitigate the risks that were assessed. Any recommendations that you make should be realistic and achievable. Overall, the remediation section of a vulnerability assessment report helps to ensure that risks are addressed in a timely and effective manner.

Currently, the server uses an SSL/TLS encrypted connection which a good starting point but that is not nearly enough the secure a public server such as this one. Implementing security controls such as 2FA (two-factor authentication) would make it a lot harder to threat actors to gain access to internal information. Additionally, better encryption practices need to be incorporated. Introducing public key infrastructure (PKI) would address possible exfiltration of sensitive information by securely encrypting employee's connection to the server. Lastly, proper log monitoring of the server would make it possible to respond to potential attacks before they have done irreparable damage to the database. The proposed security improvements would vastly reduce the potential for catastrophic threat events by introducing a two-factor authentication system, so that the correct users are let into the system, properly encrypting existing data with the help of PKI, so that threat actors that do get in do not have access to sensitive information, and introduction of a log-monitoring system so that the IT team can quickly detect and respond to security incident and better improve the system for future attacks.

II. Incident Report: Data Leak

Incident summary: A sales manager shared access to a folder of internal-only documents with their team during a meeting. The folder contained files associated with a new product that has not been publicly announced. It also included customer analytics and promotional materials. After the meeting, the manager did not revoke access to the internal folder, but warned the team to wait for approval before sharing the promotional materials with others.

However, during a video call with a business partner, a member of the sales team forgot the warning from there manager. The sales representative intended to share a link to the promotional materials so that the business partner could circulate the materials to their customers. However, the sales representative accidentally shared a link to the internal folder instead. Later, the business partner posted the link on their company's social media page assuming that it was the promotional materials.

Control	**Least privilege**
Issue(s)	The member of the sales team was given unrestricted access to an internal file for longer than necessary and only had his manager's warning as a means to prevent sharing confidential information with unauthorized users. The principle of least privilege was not observed as the business partner should not have been given access to any of the materials before approval.
Review Framework	The NIST SP 800-53: AC-6 refers to the principle of least privilege and suggests control enhancements to prevent unauthorized access of data.
Recommendation(s)	Instead of sending all sensitive data to the sales employee, he should have only been shown the data during the meeting without giving him the option to download it. He should have gotten access only after the approval for sharing the promotional materials was received and he should have never had access to the entire folder. In accordance with NIST 800-53: AC-6, access should be restricted based on user role. An access timeout should also be put in place to make sure that access sensitive information is automatically revoked after a certain period of time in the case of human error such as the manager's. This should be combined with regular audits of user privileges to optimize data security.
Justification	These improvements will make sure that the appropriate users have access to sensitive information only when required and that that access is revoked after elevated access is no longer necessary.

III. Incident Handler's Journal

Date: 04.05.2024	**Entry:** #1
Description	Documenting a small healthcare clinic ransomware incident. NIST Incident Response Lifecycle phases: *Detection and Analysis & Containment, Eradication, and Recovery*.
Tool(s) used	None
The 5 W's	• **Who** *caused the incident?* – known organized hacker Group • **What** *happened?* – Ransomware was deployed via employee phishing emails • **When** *did the incident occur?* – Tuesday, 9:00 AM • **Where** *did the incident happen?* Healthcare clinic's internal network • **Why** *did the incident happen?* – Targeted phishing emails installed ransomware on the company's systems and encrypted its data. A ransom note was left demanding a large sum of money for the encryption key.
Additional notes	Prevention: An employee awareness campaign is needed as well as tools to mitigate damage from such attacks like regular backups. Response: The potential losses need to be calculated to decide whether paying the ransom is it worth the risk.

Date: 06.05.2024	**Entry:** #2
Description	Investigating a suspicious file hash and responding to an alert ticket.

	NIST Incident Response Lifecycle phase: *Detection and Analysis*.
Tool(s) used	VirusTotal website, phishing incident response playbook
The 5 W's	• **Who** – Company employee • **What** – The employee downloaded a suspicious attachment from an email with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b • **When** – IDS alert received at 1:20 PM • **Where** – Financial services company • **Why** – Employee was a subject of a phishing email. They downloaded a malicious attachment which created multiple unauthorized executable files on their machine. IDS detected the files and alerted the SOC.
Additional notes	Employees need to be educated on the dangers of suspicious email attachments. The IDS system could be upgraded to an IPS to automatically block the execution of known malware. This is a known malware by the name of Flagpro. A well-configured IPC could have mitigated the damage of this incident. Incident was escalated to a level-two SOC analyst for review and resolution.

Date: 06.05.2024	**Entry:** #3
Description	Reviewing a final report of a data theft incident. NIST Incident Response Lifecycle phase: *Post-incident Activity*.
Tool(s) used	None

The 5 W's	• **Who** – Unknown hacker • **What** – Company data was stolen • **When** – December 28, 2022 at 7:20 PM PT • **Where** – Retail company • **Why** – A vulnerability in the e-commerce web application was exploited by an attacker to perform a forced browsing attack. Customer transaction data was then collected and exfiltrated. An employee then received 2 emails demanding a cryptocurrency payment in exchange for not leaking the data.
Additional notes	To prevent future breaches, the security team recommended routine vulnerability scans and penetration testing, and implemented new access control mechanisms – allowlisting for a specified set of URLs which block all requests outside of this range and ensuring only authenticated users can access content such as the purchase confirmation pages of other customers.

Date: 07.05.2024	**Entry:** #4
Description	Exploring failed SSH logins for the root account on the mail server of an e-commerce store. NIST Incident Response Lifecycle phase: *Detection and Analysis*.
Tool(s) used	Splunk Cloud
The 5 W's	N/A
Additional notes	Over 1000 failed SSH logins were recorded for the root account.

Date: 07.05.2024	**Entry:** #5
Description	Investigating a suspicious domain from a phishing email. NIST Incident Response Lifecycle phase: *Detection and Analysis*.
Tool(s) used	Google Chronicle
The 5 W's	• **Who** – Unknown attacker • **What** – Phishing email sent to employee inbox • **When** – No time of alert given in exercise • **Where** – Financial services company • **Why** – Employee received a phishing email from a suspicious domain which triggered a security alert. I investigated the domain using the SIEM tool *Chronicle* to determine whether it was malicious.
Additional notes	Investigation concluded that the signin.office365x24.com domain was malicious. Three POST requests were made to the resolved IP address which signifies that sensitive login information was submitted to the malicious domain and these accounts could be compromised.

IV. Incident Analysis with NIST CSF

Summary	Internal network was offline for 2 hours as a result of a ICMP Flood DDoS attack. It appears a firewall vulnerability was exploited by a malicious actor to overwhelm the network with multiple ICMP pings.
Identify	The cybersecurity team investigated the event and discovered that the company's unconfigured firewall allowed the attacker to overload the network.
Protect	The team configured the firewall to prevent future attacks of a similar nature. It did so by implementing a new rule to limit the rate of incoming ICMP packets and source IP address verification to check for spoofed IP addresses on incoming ICMP packets. Additionally, network monitoring software was installed to detect abnormal traffic patterns and an intrusion prevention system (IPS) was put in place to automatically filter out suspicious ICMP traffic.
Detect	To detect new unauthorized access attacks in the future, the team will use a firewall logging tool and an intrusion detection system (IDS) to monitor all incoming traffic from the internet.
Respond	The incident management team responded by blocking incoming ICMP packets and stopping all non-critical network services offline. Network logs will be analyzed by the security team and report the incident to management and to the necessary authorities, if required.
Recover	The team restored critical network services first and later non-critical services after all ICMP packets timed out.