

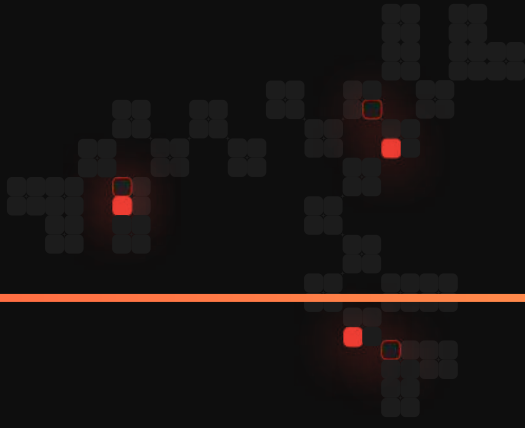


CASE STUDY

MITIGATING A POTENTIAL CYBER ATTACK ON A DATABASE SERVER AT A LEADING LOGISTICS COMPANY IN THE MIDDLE EAST



CONTENTS



Introduction		3
Overview		3
Scope		4
Analysis		4
Reasons for the Attack		4
Recommendations		5
Conclusion		6

Introduction

Cyber Heals was tasked with providing comprehensive Incident Response to assess the security posture of a database server operated by a Leading Logistics Company. This case study delves into the analysis conducted by Cyber Heals to identify and address potential vulnerabilities, particularly focusing on a brute-force attack targeting the company's database server.

Overview:

Cyber Heals was engaged to conduct a thorough Incident Response analysis focused on the database server of a Leading logistics company, to detect potential cyber threats. The analysis revealed a significant risk posed by a potential brute-force attack targeting the company's database server. Through an examination of SQL log files provided by Companies Network Security Team, Cyber Heals identified multiple failed login attempts originating from various malicious IP addresses. The attack vector exploited the server's publicly accessible database, highlighting critical security vulnerabilities within the company's infrastructure.

Scope

The scope of the analysis conducted by Cyber Heals encompassed an in-depth examination of the SQL log files to identify indicators of a potential cyber-attack on Companies database server. The analysis focused on understanding the nature of the attack, including its origin, methods, and potential impact. Additionally, the scope extended to providing actionable recommendations to mitigate the identified vulnerabilities and strengthen the company's security posture. These recommendations aimed to prevent future attacks and safeguard the integrity of Companies database server.

Analysis

Upon analyzing the SQL log files, Cyber Heals identified a potential brute-force attack targeting Companies database server. Several failed login attempts originating from various malicious IP addresses were noted, indicating unauthorized access attempts.

Reasons for the Attack:

- Database server's accessibility over the public internet.
- Absence of brute-force protection in the application.
- Lack of DDoS protection measures.

Recommendations:

- Provision of a list of malicious IP addresses and domains to block.
- Blocking attacker IP addresses via network firewall.
- Disabling public access to Remote Desktop Protocol (RDP) and SQL.
- Implementation of brute-force protection mechanisms.
- Enforcement of stringent password policies.
- Implementation of two-factor authentication for enhanced security.



Conclusion:

Cyber Heals' analysis revealed critical vulnerabilities within Companies database server infrastructure, particularly regarding the lack of protection against brute-force attacks. By providing actionable recommendations, Cyber Heals aimed to bolster the company's security posture and mitigate the risk of future cyber threats. This case underscores the importance of proactive security measures in safeguarding sensitive data and mitigating potential Cyber-attacks.

**To get the free security assessment:
<https://cyberheals.com/free-pentest>**