Security Tapestry

Vulnerability Assessment

&

Penetration Testing

Report For

Gossett Motor Cars

Contents

Executive Summary

Introduction

The vulnerability assessment and penetration test were conducted using the cutting-edge Tenable Nessus tool, to identify potential security weaknesses within the network infrastructure of Gossett Motor Cars. This report aims to provide insights into vulnerabilities that may be exploited, thereby posing risks to the organization.

To learn more about our partner Tenable, please visit the following link https://www.tenable.com/about-tenable/about-us.

Scope

The assessment covered multiple subnets within the Gossett Motor Cars' network, specifically the **10.2.0.0/16**, **10.3.0.0/16**, **10.4.0.0/16**, **10.5.0.0/16**, and **10.6.0.0/16** ranges.

Key Findings

The assessment identified several vulnerabilities, ranging from informational to critical. Some of the most critical vulnerabilities include unsupported application versions, unencrypted communication protocols, and vulnerable Windows registry keys.

If left unaddressed, these vulnerabilities could lead to unauthorized data access, potential data breaches, service disruptions, and potential harm to the organization's reputation.

Risk Overview

The vulnerabilities were categorized into various risk levels:

- Critical: These vulnerabilities present immediate and severe risks and can be easily exploited, possibly leading to significant damages.
- High: These vulnerabilities represent significant risks, though they might have some constraints that reduce immediate exploitability.
- Medium: These vulnerabilities carry moderate risks and might require certain conditions to be fully exploited.
- Low: These pose minimal risks and are less likely to be exploited in typical scenarios.

Recommendations

1. Prioritize the patching and updating of critical systems, especially those with known vulnerabilities.
2. Consider migrating away from outdated or unsupported software and systems.
3. Implement robust encryption protocols to safeguard data in transit.

For a detailed breakdown and specific remediation steps for each vulnerability, please refer to the main body of the report.

Conclusion

Addressing the identified vulnerabilities is crucial for ensuring the security and integrity of Gossett Motor Cars' network infrastructure. Timely remediation will not only safeguard the organization's data but also its reputation and trust with stakeholders.

Next Steps

1. Prioritize and address critical vulnerabilities immediately.
2. Schedule regular vulnerability assessments to keep abreast of new potential threats.

Vulnerability Scan & Assessment

Objective

The main objective of this phase was to gain a deep understanding of the security posture of Gossett Motor Cars' digital infrastructure. Security Tapestry aimed to identify vulnerabilities that could potentially be exploited by malicious entities, thereby providing actionable insights to fortify the digital defenses.

Scope

The following IP ranges within Gossett Motor Cars' network were selected for scanning:

- 10.2.0.0/16
- 10.3.0.0/16
- 10.4.0.0/16
- 10.5.0.0/16
- 10.6.0.0/16

Methodology

Preparation

Prior to initiating the scans, our team coordinated with the IT leaders at Gossett Motor Cars to ensure minimal disruption to daily operations. Necessary permissions and schedules were duly established.

Randomized Scanning

Over the course of several weeks, our team ran vulnerability scans on the aforementioned IP ranges at random intervals. This approach mimics the unpredictable nature of real-world cyberattacks, ensuring a more realistic assessment.

Usage of Tenable Nessus

Tenable Nessus, a premier vulnerability assessment tool, was employed for the scanning process. Its vast database of known vulnerabilities, combined with advanced scanning capabilities, ensured a thorough examination of the targeted IP ranges.

Analysis of Scan Results

Once the scans were completed, the results were carefully analyzed. Tenable Nessus categorized the vulnerabilities based on their severity—critical, high, medium, low, and informational. Each vulnerability was then assessed based on its potential impact and the likelihood of it being exploited.

Verification

Vulnerabilities flagged as 'critical' or 'high' were further verified to ascertain their authenticity. This step is crucial to eliminate false positives and focus on genuine threats.

Findings

The scans revealed a diverse set of vulnerabilities spread across the IP ranges. While a detailed breakdown will be provided in subsequent sections, it is imperative to note that several critical vulnerabilities were identified, which require immediate attention.

Recommendations

Patch Management

Regularly update and patch all systems, software, and applications to the latest versions to mitigate known vulnerabilities.

Regular Scanning

Adopt a strategy of regular vulnerability scanning, preferably monthly or quarterly, to ensure emerging threats are identified in a timely manner.

Employee Training

Cybersecurity awareness among employees can significantly reduce the risk of vulnerabilities being exploited. Consider regular training sessions.

Reporting and Remediation Strategy

To ensure a systematic and effective approach to vulnerability management, we have prepared a set of structured reports tailored for IT leaders at Gossett Motor Cars:

Top 10 Vulnerabilities Report

This report provides an overview of the most pressing vulnerabilities within each subnet, ranked by severity and potential impact. Addressing these vulnerabilities should be of the highest priority.

Vulnerabilities by Host

A granular view of the vulnerabilities is essential for comprehensive risk management. This report offers a detailed breakdown of vulnerabilities based on each host within the subnet, facilitating targeted remediation efforts.

Recommended Remediations

Remediation is as vital as detection. This report offers actionable recommendations tailored for each subnet, guiding the IT team on the best practices and steps to mitigate the identified vulnerabilities.

Special Note to IT Leaders

While the above reports provide a consolidated view, a more detailed perspective is often necessary for comprehensive risk management. IT leaders wishing to access a full list of all vulnerabilities by host, along with specific remediation steps, can request this information by emailing reports@securitytapestry.com. This extended data will equip you with the knowledge and tools to ensure the continued security and resilience of Gossett Motor Cars' digital infrastructure.

Penetration Testing

Objective

The primary goal of the penetration test was to identify exploitable vulnerabilities within Gossett Motor Cars' digital infrastructure, simulating a real-world cyberattack scenario. This would provide a clearer understanding of potential attack vectors and areas of risk within the network.

Scope

While the vulnerability scanning was broad, the penetration test focused mostly on the vulnerabilities identified as 'critical', 'high', or 'medium' severity within the scanned IP ranges.

Methodology

Engagement Planning

Before the penetration test, coordination with Gossett Motor Cars' IT team was crucial to determine the boundaries of the test and ensure minimal disruptions.

Usage of Tenable Nessus

Nessus, known for its vulnerability assessment capabilities, also provides tools to analyze the exploitability of vulnerabilities. Leveraging its vast database and advanced analysis tools, our team aimed to identify which vulnerabilities could potentially be exploited by attackers.

Non-Intrusive Approach

It's crucial to mention that this was a non-intrusive penetration test. While vulnerabilities deemed exploitable were identified, at no point were they exploited. This approach ensured that no harm or disruption occurred to any system within Gossett Motor Cars' network.

Findings

A set of exploitable vulnerabilities was identified across various systems. The specifics of these vulnerabilities, along with their potential impact, will be detailed in the exploitable vulnerabilities report for each subnet. Importantly, while these vulnerabilities are exploitable, they remain unexploited during this test to maintain the integrity and safety of Gossett Motor Cars' systems.

Recommendations

Immediate Remediation

Focus on patching or mitigating the identified exploitable vulnerabilities as a top priority.

Access Control

Review and strengthen user access controls, ensuring that potential attackers cannot easily escalate privileges or access sensitive data.

Regular Penetration Testing

Conducting regular non-intrusive penetration tests will help in keeping abreast of new vulnerabilities and ensuring the continued security of the network.

Detailed Exploration of Exploitable Vulnerabilities

For a comprehensive understanding of the risk landscape and to prioritize remediation efforts, it's essential to delve deep into the exploitable vulnerabilities identified during our penetration test.

Exploitable Vulnerabilities

Accompanying this report, we have prepared a detailed section labeled "Exploitable Vulnerabilities" for each subnet. This section is the cornerstone of our findings, providing:

Vulnerability Details

A thorough breakdown of each exploitable vulnerability, including its classification, potential impact, and the system or application it affects.

Exploitability Analysis

An assessment of how a potential attacker might exploit the vulnerability and the ease of exploitation.

Conclusive Remarks

Summary

The comprehensive vulnerability assessment and penetration testing conducted on Gossett Motor Cars' digital infrastructure have highlighted several areas of concern. Ranging from informational to critical, these vulnerabilities, if left unaddressed, can pose significant threats to the organization’s data integrity, operational continuity, and overall reputation.

Key Highlights

The use of Tenable Nessus allowed for a thorough examination of the targeted IP ranges, revealing a diverse set of vulnerabilities that require varying degrees of attention.

The penetration testing, although non-intrusive, identified exploitable vulnerabilities that demonstrate the potential risks in a real-world cyberattack scenario.

Reports tailored for IT leaders at Gossett Motor Cars, such as the "Top 10 Vulnerabilities Report" and "Vulnerabilities by Host", provide actionable insights for a structured remediation approach.

The detailed section labeled "Exploitable Vulnerabilities" underscores the significance of each vulnerability within the broader network, offering a contextual risk rating to guide prioritization.

Final Recommendations

Immediate attention to critical vulnerabilities is paramount. These pose the highest risk and can lead to severe consequences if exploited.

Continued collaboration with cybersecurity experts, like Security Tapestry, will ensure that Gossett Motor Cars stays ahead of emerging threats.

Ongoing employee training and awareness programs can significantly reduce the human error element, which often serves as an entry point for cyber threats.

Regular vulnerability assessments and penetration tests should become a standard part of Gossett Motor Cars' cybersecurity strategy, ensuring a proactive approach to potential threats.

Appreciation

Security Tapestry would like to express gratitude to Gossett Motor Cars for entrusting us with this crucial task. We value our partnership and are committed to assisting you in safeguarding your digital assets and maintaining the trust of your stakeholders.

Looking Forward

Cybersecurity is an ongoing journey, not a destination. As technology evolves, so do the threats. Staying vigilant, informed, and proactive is the best defense against future cyber risks. We hope that the insights and recommendations provided in this report will serve as a solid foundation for Gossett Motor Cars' cybersecurity endeavors in the future.