CP3414- Ethical Hacking

Assessment Item 3: Vulnerability Assessment Report

Zwe Sett Aung

Professor Steve Kerrison

TR3. 2024

James Cook University Singapore

Contents

Pen-testing Report for Nessus Vulnerability Scan

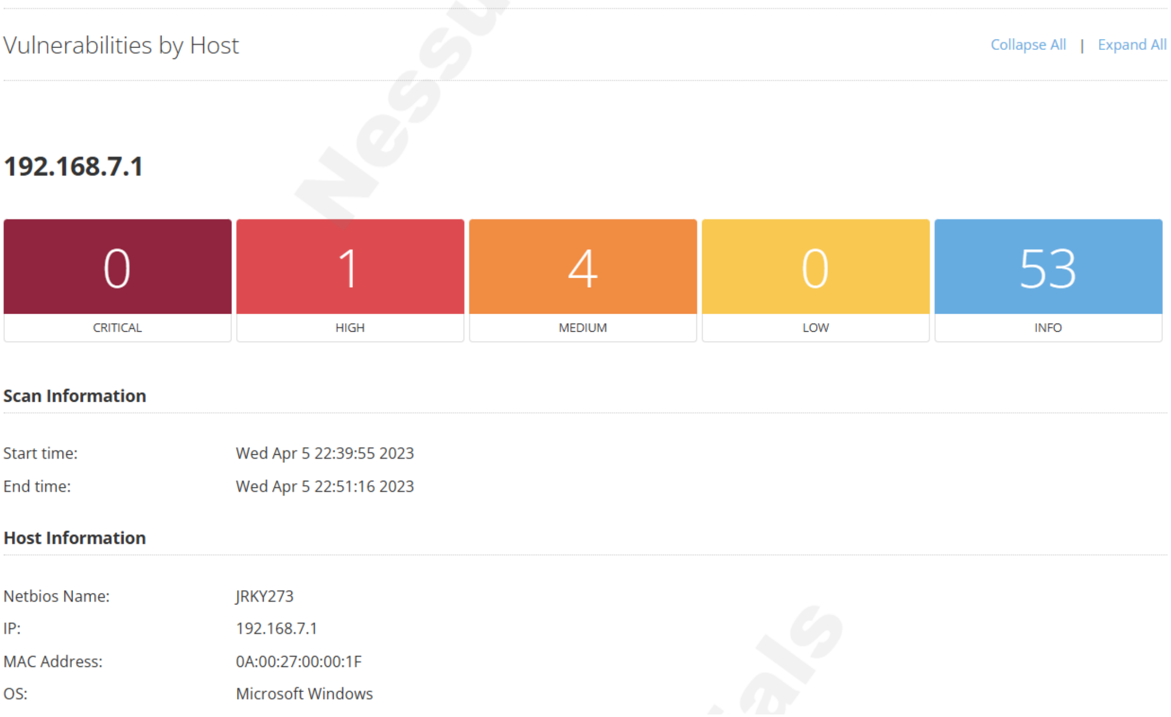
Executive Summary

In our penetration test, we identified several vulnerabilities in the client's network that need immediate attention. One high-criticality issue involves outdated SSL ciphers vulnerable to cryptographic attacks like SWEET32. Additionally, we found four medium-criticality vulnerabilities, including the lack of SMB signing, an untrusted SSL certificate, and the use of deprecated TLS 1.0 and TLS 1.1 protocols. These issues could lead to data interception, unauthorized access, and weakened security.

We also noted 53 informational vulnerabilities that, while not immediately dangerous, highlight areas where the network's configuration can be improved to reduce future risks. Our recommendations focus on upgrading encryption methods, enforcing SMB signing, and replacing outdated certificates and protocols. Taking these steps will help secure sensitive data, improve user trust, and align the systems with modern security standards.

Summary of Findings

Our scan uncovered a range of vulnerabilities across the network:



192.168.7.1

0	1	4	0	53
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Apr 5 22:39:55 2023
End time:	Wed Apr 5 22:51:16 2023

Host Information

Netbios Name:	JRKY273
IP:	192.168.7.1
MAC Address:	0A:00:27:00:00:1F
OS:	Microsoft Windows

Our assessment identified critical and medium-level vulnerabilities in the client’s network that require prompt action to mitigate security risks:

High Criticality

1. **SSL Medium Strength Cipher Suites Supported**
   The Linux server uses outdated SSL ciphers vulnerable to cryptographic attacks like SWEET32, which could compromise encrypted communications. Reconfiguring the server to use stronger ciphers, such as AES256, is critical.

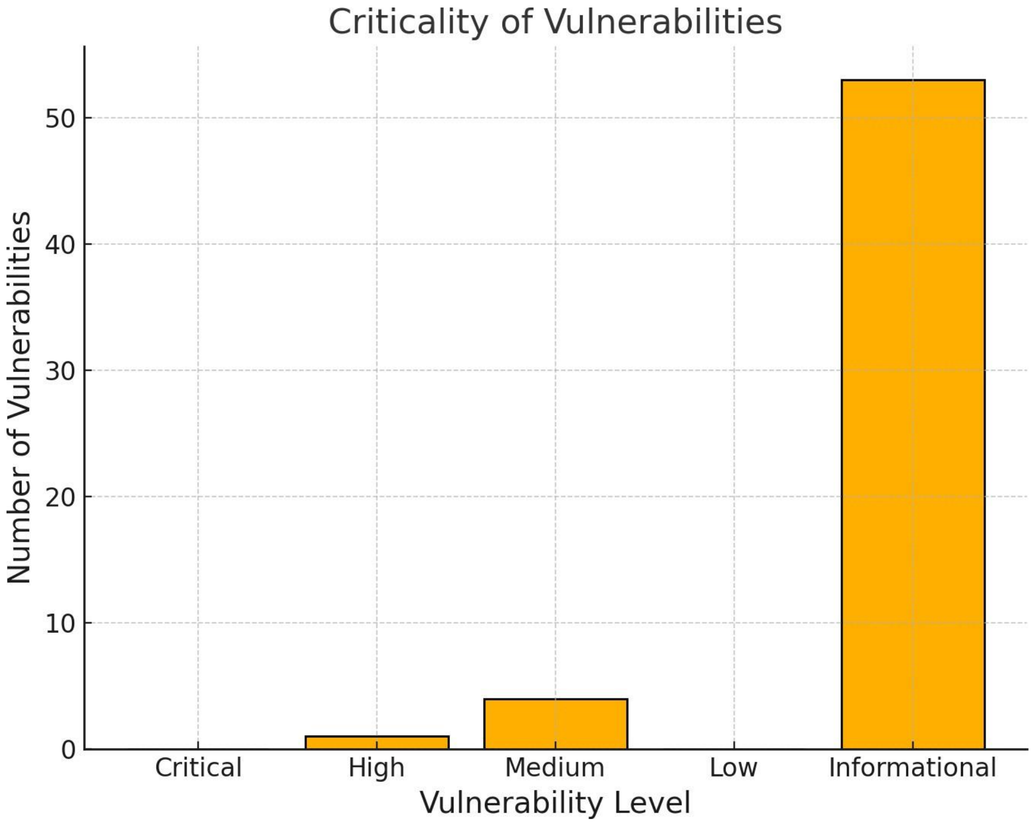
Medium Criticality

1. **SMB Signing Not Enforced**
   The Windows machine does not enforce SMB signing, exposing it to man-in-the-middle attacks. Enforcing SMB signing will prevent unauthorized interception and manipulation of SMB traffic.
2. **Untrusted SSL Certificate**
   A service is using an untrusted SSL certificate, which undermines the security of encrypted communications. Replacing it with a trusted certificate from a reliable authority will resolve this issue.
3. **TLS Version 1.0 Protocol Detection**
   The server allows connections using the outdated TLS 1.0 protocol, which has known cryptographic flaws. Disabling TLS 1.0 and enabling TLS 1.2 or higher is strongly recommended.
4. **TLS Version 1.1 Protocol Deprecated**
   The server supports TLS 1.1, an insecure protocol that lacks modern encryption capabilities. Disabling TLS 1.1 and enforcing the use of TLS 1.2 or higher is necessary.

Informational Vulnerabilities

We also identified **53 informational vulnerabilities** in the scan. While these don't pose an immediate threat, they highlight areas where we can improve the network's configuration and reduce potential exposure to future risks.

Graph of Criticality of Vulnerabilities



Graph of Criticality

The chart above illustrates the distribution of vulnerabilities by criticality level, highlighting the predominance of informational vulnerabilities while identifying high and medium-priority issues that require immediate attention.

Technical Findings

SSL Medium Strength Cipher Suites Supported (SWEET32)

- **Description**: The Linux server supports medium-strength SSL ciphers, such as DES-CBC3-SHA, which are vulnerable to the SWEET32 attack. This attack leverages the weaknesses of 64-bit block ciphers, allowing an attacker to decrypt HTTPS traffic by analyzing a large volume of encrypted data. The SWEET32 vulnerability has been documented in-depth by the OpenSSL project and affects systems using older cryptographic standards.
- **Affected System**: Linux Server (192.168.7.7)
- **Impact**: An attacker in a shared network could exploit this weakness to decrypt sensitive information, such as login credentials or personal data, and compromise the integrity of encrypted communications (K.Bhargavan & G.Leurent,2016).
- **Severity**: High (CVSS v3.0 Base Score: 7.5)
- This vulnerability represents a significant security risk and should be remediated immediately to safeguard encrypted communications and sensitive data.

SMB Signing Not Required

- **Description**: We discovered that SMB signing is not enforced on the Windows machine. This vulnerability allows unauthenticated attackers to perform man-in-the-middle attacks, intercepting and manipulating SMB traffic. This poses a risk to the confidentiality and integrity of data shared over the network.
- **Affected System**: Windows Server (192.168.7.9)
- **Impact**: The risks of having SMB signing disabled are serious and can greatly weaken an organization's overall security. Without SMB signing, attackers can intercept and alter data being transmitted, all without raising any alarms. This opens the door to data theft, unauthorized changes, and other harmful activities that could compromise the integrity and confidentiality of sensitive information (J.Zacharia,2023)
- **Severity**: Medium (CVSS v3.0 Base Score: 5.3)

We believe addressing this vulnerability promptly will significantly reduce the risk of unauthorized interception or tampering of SMB traffic.

SSL Certificate Cannot Be Trusted

- **Description**: We found that the SSL certificate for this service cannot be trusted. This may be due to it being self-signed, having an incomplete or invalid certificate chain, or using an expired or mismatched signature. These issues break the chain of trust, making it difficult for users to verify the authenticity of the server.
- **Affected System**: Affected web service.
- **Impact**: Without an SSL certificate, we risk exposing sensitive customer data, such as payment details, to hackers, making it easier for them to exploit vulnerabilities. This can lead to a loss of customer trust, warnings from search engines, and even a drop in our website's search rankings, which could ultimately harm our reputation and impact our business success.(Tech Funnel,2019)
- **Severity**: Medium (CVSS v3.0 Base Score: 6.5)

By addressing this issue, we can protect sensitive data, ensure secure communications, and strengthen trust in the affected service.

TLS Version 1.0 Protocol Detection

- **Description**: We found that the server allows connections using the outdated TLS 1.0 protocol. TLS 1.0 has cryptographic flaws that make it insecure for modern communications, as it lacks the protections offered by newer protocols like TLS 1.2 and 1.3.
- **Affected System**: Affected web service.
- **Impact**: Continued use of TLS 1.0 puts encrypted communications at risk of interception and exploitation. As many browsers and systems have deprecated support for TLS 1.0, using it may also result in compatibility issues and warnings to users (K.Moriarty & S.Farrell,2018).
- **Severity**: Medium (CVSS v3.0 Base Score: 6.5)

TLS Version 1.1 Protocol Deprecated

- **Description**: The server also supports TLS 1.1, which is an outdated protocol lacking modern cryptographic safeguards. It does not support current encryption standards such as authenticated encryption with AES-GCM, making it vulnerable to attacks.
- **Affected System**: Affected web service.
- **Impact**: The use of TLS 1.1 not only weakens security but also limits compatibility with browsers and systems that no longer support this protocol. This can lead to reduced functionality and potential exploitation of vulnerabilities in outdated cryptographic algorithms (K.Moriarty & S.Farrell,2018).
- **Severity**: Medium (CVSS v3.0 Base Score: 6.5)

By addressing these outdated protocols, we can strengthen encryption, improve compatibility with modern systems, and ensure secure communications.

Recommendations

SSL Medium Strength Cipher Suites Supported (SWEET32)

To address the risk posed by outdated encryption methods, we recommend updating the server to use stronger, more secure encryption algorithms like AES256. This will ensure that sensitive information, such as login credentials and personal data, remains protected from attackers. Regularly reviewing encryption settings is essential to prevent vulnerabilities. (K.Bhargavan & G.Leurent,2016).

SMB Signing Not Required

The lack of SMB signing makes it easier for attackers to intercept or alter data shared over the network. Enabling SMB signing on the Windows server will protect shared data by ensuring it is authenticated and secure. We also recommend restricting file-sharing access to trusted networks and monitoring for unusual activity (J.Zacharia,2023).

SSL Certificate Cannot Be Trusted

The current SSL certificate on the website is not trusted, which could expose sensitive data like payment information to hackers and reduce user trust. Installing a valid SSL certificate from a trusted provider will secure communications and reassure customers. Additionally, enabling certificate monitoring to prevent expiration issues is crucial (Tech Funnel,2019).

TLS Version 1.0 Protocol Detection

Using the outdated TLS 1.0 protocol puts encrypted communication at risk of being intercepted by attackers. Disabling TLS 1.0 and using TLS 1.2 or 1.3 ensures stronger encryption. Before making this change, systems should be tested for compatibility (K.Moriarty & S.Farrell,2018).

TLS Version 1.1 Protocol Deprecated

TLS 1.1 is another outdated protocol that lacks modern encryption capabilities. Disabling it and transitioning to TLS 1.2 or 1.3 improves security and compatibility with modern systems. Regularly updating encryption settings can help prevent similar issues(K.Moriarty & S.Farrell,2018).

Conclusion

We identified several critical and medium-level vulnerabilities that could compromise the security of the client’s systems if not addressed. These include outdated SSL ciphers, the lack of SMB signing, an untrusted SSL certificate, and the use of deprecated TLS protocols. While technical, these issues can lead to data breaches, unauthorized access, and a loss of trust from users.

By implementing our recommendations—upgrading encryption methods, enabling SMB signing, and replacing outdated certificates and protocols—the client can significantly reduce risks and strengthen their network's security. We are available to assist with these fixes and provide ongoing support to ensure the systems remain secure. Let us know how we can help!

Appendix

Appendix A: Acronyms and Definitions

- **SSL**: Secure Sockets Layer – A protocol for encrypting communications over a network.
- **SMB**: Server Message Block – A protocol for sharing files, printers, and other resources on a network.
- **TLS**: Transport Layer Security – A protocol that provides secure communication over a network.
- **SWEET32**: A cryptographic attack exploiting weaknesses in 64-bit block ciphers.
- **CVE**: Common Vulnerabilities and Exposures – A reference system for publicly known security vulnerabilities.
- **CVSS**: Common Vulnerability Scoring System – A framework for rating the severity of security vulnerabilities.
- **MITM**: Man-in-the-Middle – A type of cyberattack where communication between two parties is intercepted or altered by an unauthorized entity.

Appendix B: Tools and Methodologies

- **Tools Used**:
  - Nessus Vulnerability Scanner
  - Manual validation of vulnerabilities
  - Industry-standard references such as OpenSSL and IETF guidelines.
- **Methodology**:
  - Scanned the client's network to identify vulnerabilities.
  - Assessed vulnerabilities based on their criticality and potential impact.
  - Provided recommendations aligned with best practices and security standards.

Appendix C: CVSS Scoring Breakdown

- **SSL Medium Strength Cipher Suites Supported**:
    - CVSS v3.0 Base Score: 7.5 (High)
    - Exploitability: High
    - Impact: High
- **SMB Signing Not Required**:
    - CVSS v3.0 Base Score: 5.3 (Medium)
    - Exploitability: Medium
    - Impact: Medium
- **SSL Certificate Cannot Be Trusted**:
    - CVSS v3.0 Base Score: 6.5 (Medium)
    - Exploitability: Medium
    - Impact: Medium
- **TLS Version 1.0 Protocol Detection**:
    - CVSS v3.0 Base Score: 6.5 (Medium)
    - Exploitability: Medium
    - Impact: Medium
- **TLS Version 1.1 Protocol Deprecated**:
    - CVSS v3.0 Base Score: 6.5 (Medium)
    - Exploitability: Medium
    - Impact: Medium

References

K.Bhargavan & G.Leurent .(2016).Sweet 32:Practical Impact . INRIA.From Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN

J.Zacharia.(1st June,2023).Risks and Consequences of Disabling SMB Signing.Redfox Security.From https://redfoxsec.com/blog/how-to-find-and-fix-smb-signing-disabled-vulnerability/

Tech Funnel.(4th Novemner,2019).What are the consequences of not having an SSLcertificate?.From https://www.techfunnel.com/information-technology/what-are-the-consequences-of-not-having-an-ssl-certificate/

K.Moriarty & S.Farrell.(14th September,2018). Do not use TLSv1.0 .Trinity College Dublin. From draft-ietf-tls-oldversions-deprecate-00

K.Moriarty & S.Farrell.(14th September,2018). Do not use TLSv1.1 .Trinity College Dublin. From draft-ietf-tls-oldversions-deprecate-00