Uber



Penetration Test Report

Prepared By: David Pierre

January 2, 2024

TABLE OF CONTENTS

Executive Summary 3

Scope 3

Methodology 4

Risk Assessment 5

Findings & Recommendations 6

Conclusion 11

EXECUTIVE SUMMARY

This executive summary provides a condensed overview of the recent penetration testing engagement conducted on CyberKlan Security. The primary goal of the assessment was to identify and evaluate potential vulnerabilities in the systems, networks, and applications to enhance overall security posture.

SCOPE

The testing scope encompassed [list of systems, networks, and applications] and followed a comprehensive methodology, including reconnaissance, enumeration, vulnerability analysis, exploitation, and post-exploitation activities.

Methodology

### **1. Reconnaissance:**

* Objective: Gather information about the target systems, networks, and applications
* Activities:
  + DNS Enumeration
  + Intelligence gathering

### **2. Enumeration:**

* Objective: Identify active hosts, services, and users within the target environment
* Activities:
  + Network Scanning
  + User Account identification

### **3. Vulnerability Analysis:**

* Objective: Identify and analyze potential vulnerabilities in systems and applications
* Activities:
  + Vulnerability Scanning
  + Score rankings for each vulnerability identified

### **4. Exploitation:**

* Objective: Exploit identified vulnerabilities
* Activities:
  + Exploiting targets of vulnerabilities
  + Attempts to elevate privileges

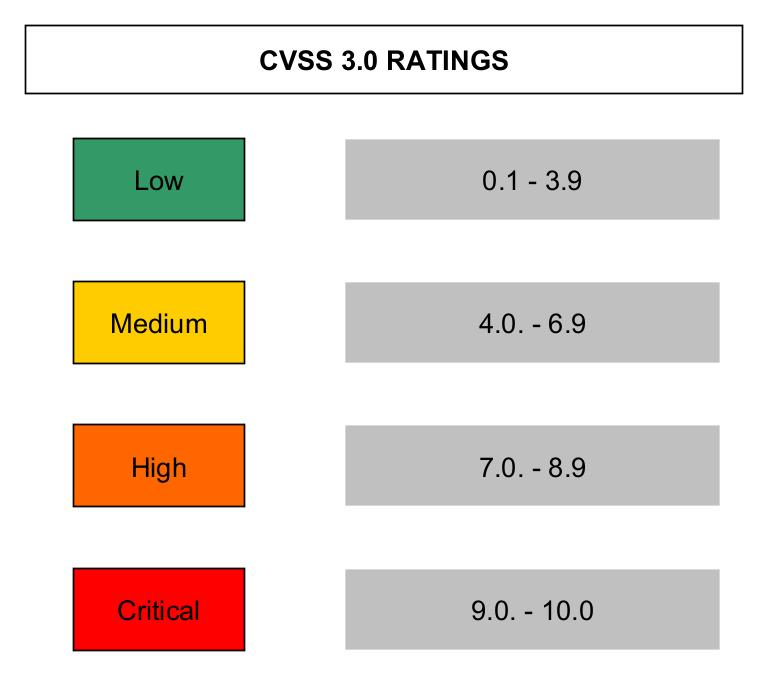
### **5. Post-Exploitation:**

* Objective: Analyze the security of systems after exploitation
* Activities:
  + Data exfiltration
  + Verification of elevated privileges

**Risk Assessment**

### **Severity Ratings**

* The Common Vulnerability Scoring System (CVSS) was designed to rank the vulnerabilities that are discovered. The rankings for the vulnerabilities are:



### **Business Impact**

* The effects of the vulnerabilities that are discovered include some of the following:
  + Reputational Damage
  + Intellectual Property Theft
  + Disruption of Operations
  + Data Manipulation
  + Legal Consequences

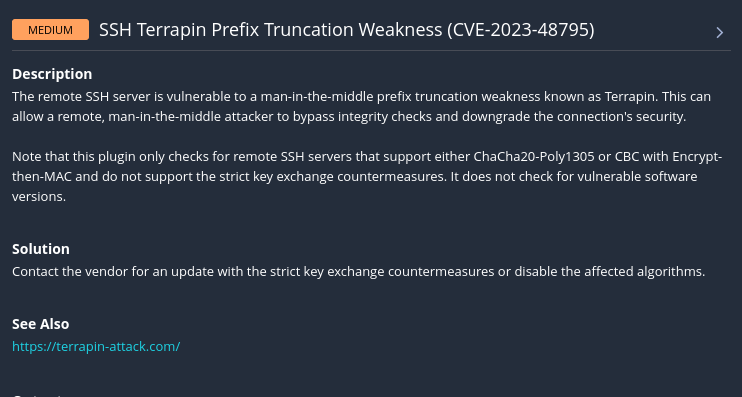
### **Risk Mitigation**

* This process is dedicated towards identifying and prioritizing risks that could impact an organization's objectives. Risk management is composed of these elements:
  + Risk Assessment: analyzing a risk to determine its severity to an organization’s capabilities of operating
  + Risk Identification: identifying risks that can pose a threat to an organization’s capabilities of operating
  + Risk Mitigation: the development of ideas and strategies that may serve as a solution to reduce the impact of the risks identified

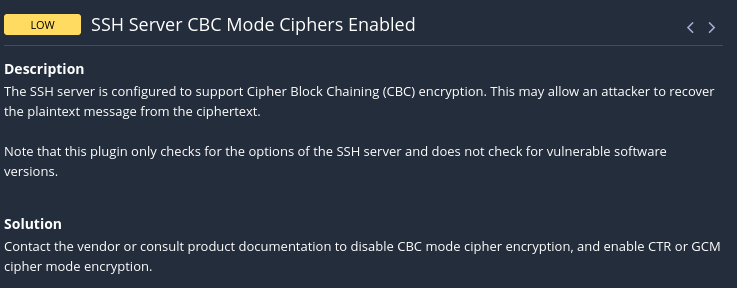
**Findings & Recommendations**

### **Findings**

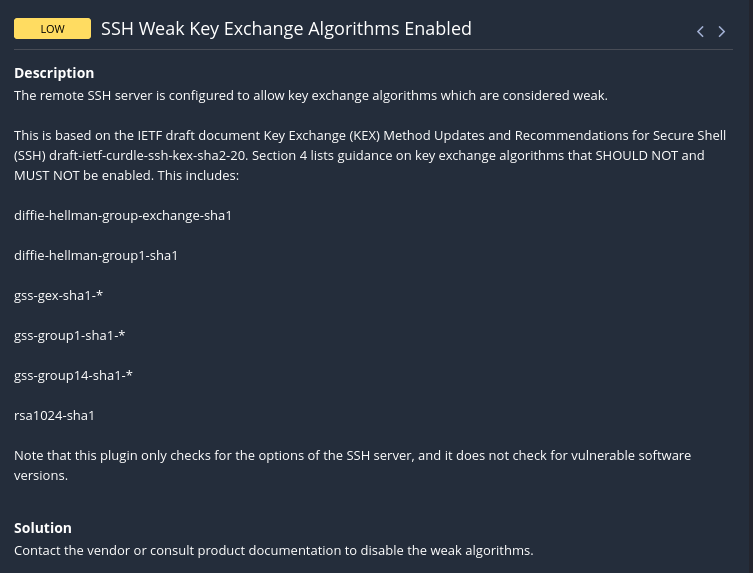
* The remote SSH server is vulnerable to a man-in-the-middle prefix truncation weakness known as Terrapin. This can allow a remote, man-in-the-middle attacker to bypass integrity checks and downgrade the connection's security (CVSS Score: 5.9)



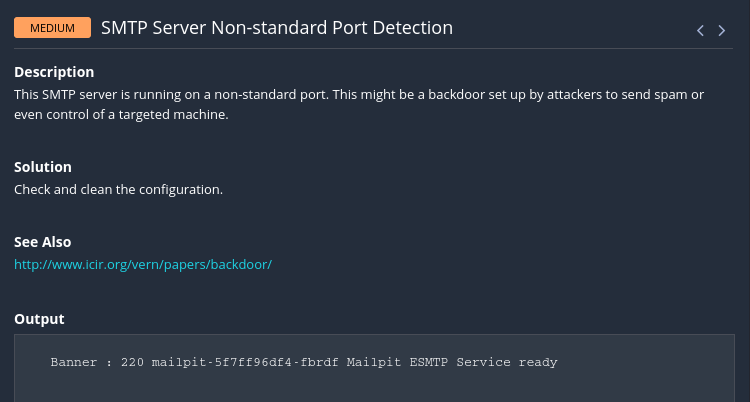
* The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext (CVSS Score: 3.7)



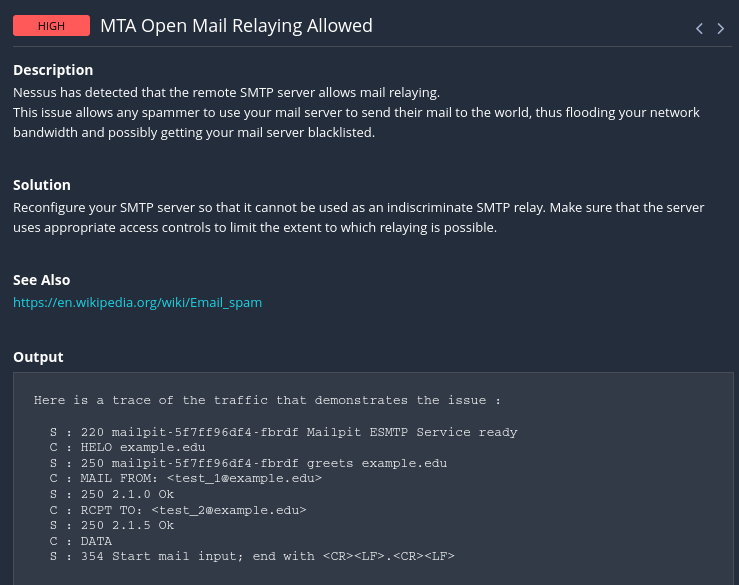
* The remote SSH server is configured to allow key exchange algorithms which are considered weak (CVSS Score: 3.7)



* This SMTP server is running on a non-standard port. This might be a backdoor set up by attackers to send spam or even control of a targeted machine (CVSS Score: 5.0)



* The remote SMTP server allows mail relaying. This issue allows any spammer to use your mail server to send their mail to the world, thus flooding your network bandwidth and possibly getting your mail server blacklisted (CVSS Score: 7.5)



* The remote host supports the use of SSL ciphers that offer medium strength encryption (CVSS Score: 7.5)

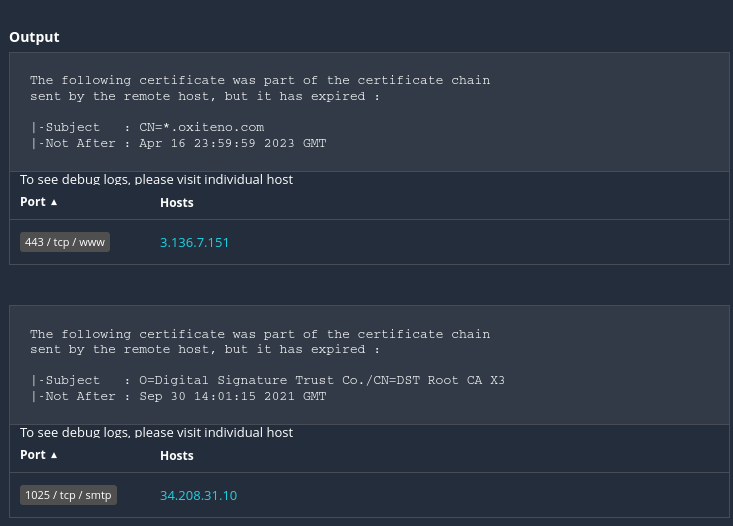
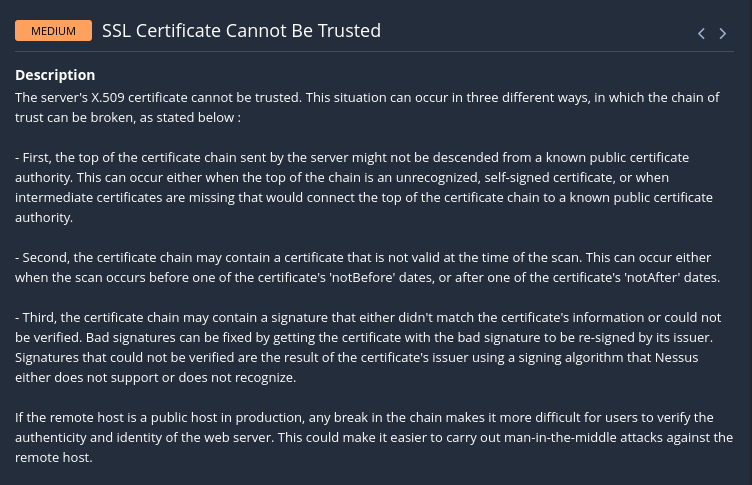


* The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below (CVSS Score: 6.5):

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.



* The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws (CVSS Score: 6.5)

### 

### **Recommendations**

* Contact the vendor for an update with the strict key exchange countermeasures or disable the affected algorithms
* Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption
* Contact the vendor or consult product documentation to disable the weak algorithms
* Check and clean the configuration
* Reconfigure your SMTP server so that it cannot be used as an indiscriminate SMTP relay. Make sure that the server uses appropriate access controls to limit the extent to which relaying is possible
* Reconfigure the affected application if possible to avoid use of medium strength ciphers
* Purchase or generate a proper SSL certificate for this service
* Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0

## **Conclusion**

In conclusion, the comprehensive penetration test conducted on Uber has provided valuable insights into the security posture of the IT infrastructure. it is imperative to address the vulnerabilities and weaknesses uncovered during the testing process.The identified vulnerabilities pose potential risks to the confidentiality, integrity, and availability of critical systems and sensitive data. It is strongly recommended that Uber takes immediate action to remediate these vulnerabilities to enhance the overall security posture. The prioritization of remediation efforts should be based on the potential impact on business operations and the sensitivity of the information at risk. Uber should employ ongoing security awareness training for employees and continuous monitoring of the IT environment are crucial components for maintaining a robust security posture. Regularly scheduled penetration testing, vulnerability assessments, and proactive threat intelligence monitoring are recommended to ensure that the organization stays ahead of evolving cyber threats.