IT PENETRATION TESTING
AUD23-02

January 4, 2024

City of West Palm Beach
Internal Auditor's Office

Beverly Mahaso Esq., CIA, CFE
Chief Internal Auditor

EXECUTIVE SUMMARY

The City's Internal Auditor's Office engaged RSM US LLP (RSM) to perform an external penetration test, which simulated an attack against the City's external cybersecurity environment. Technical based attacks were leveraged in an attempt to gain access to sensitive information and systems.

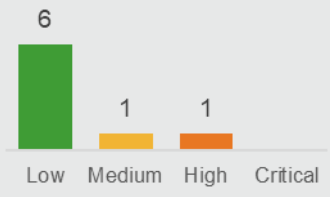
Observations

External Penetration Test

We were not able to compromise the City's external network. Common attacks were unsuccessful, and no unauthorized access was achieved. We identified vulnerabilities relating to misconfigured communication protocols and insecure system settings. In a real attack, these issues are not likely to lead to a direct compromise of the network, user accounts, or sensitive data. As such, we have determined the City's external network to have a ***low*** potential for compromise.

However, this does ***not*** mean that a determined bad actor could not exploit a vulnerability in a real attack. There is no organization today that is not in some way susceptible to a breach from a highly determined bad actor. The fact that no organization can ever say they are 100% protected from a breach is well known amongst security professionals.

Summary of Results	
Overall Rating	Low
Level of Compromise	None
Total Vulnerabilities	8



Vulnerabilities by Rating

Results

At a high level, we pinpointed the following issues along with overarching recommendations:

- **Insecure Software Development** - Develop applications and enable security settings in alignment with application security best practices.
- **Patch Management** – Implement a process to identify and update vulnerable 3rd party software updates especially on external applications.
- **Configuration Management** – Examine the issues tied to insecure configurations and assess the feasibility of reconfiguring the service in accordance with best practices.

Internal Auditor's Office
P.O. Box 3366
West Palm Beach, Florida 33402
Tel: 561-822-1380
Fax: 561-822-1424

January 4, 2024

Audit Committee
City of West Palm Beach
401 Clematis Street
West Palm Beach, Florida

RE: IT PENETRATION TEST, AUD23-02

Dear Audit Committee Members:

Attached is the City of West Palm Beach's Internal Auditor's Office report on the IT Penetration Test performed by RSM US LLP. The subject matter covered is confidential in nature and thus exempt from Florida Statute 119. As such, specific details and evidence are not disclosed to avoid the possibility of compromising the City's information and security.

All confidential matters have been communicated to the appropriate personnel. Further, we have provided management with the results related to the penetration testing.

We thank the management and staff of the IT Department for their time, assistance, and cooperation during this testing.

Respectfully Submitted,

/s/ Beverly Mahaso
Chief Internal Auditor

cc: Keith James, Mayor
Faye Johnson, City Administrator
Paul Jones, Chief Information Officer

Contents

Background

Cybersecurity holds paramount importance for municipalities as they increasingly rely on digital systems to manage critical infrastructures, public services, and sensitive data. Municipalities store vast amounts of information, ranging from citizen records to financial transactions, making them attractive targets for cyber threats. A breach in security could not only compromise sensitive data, but also disrupt essential services, leading to potential loss of public funds and public trust. With the rise of smart cities and interconnected technologies, the attack surface for malicious actors has expanded, making robust cybersecurity measures crucial for safeguarding against cyberattacks, ensuring the integrity of City operations, and upholding the trust and well-being of the communities served.

Statement of Scope

The external penetration test simulated a real-world attack against the City's external cybersecurity presence. It included testing on all external assets owned and managed by the City. Once we discovered vulnerabilities through either manual or automated processes, we attempted to exploit the specific exposures or combine multiple flaws to achieve a larger attack (vulnerability linkage theory). Our ultimate goal was to gain full administrative access to the City's networks and/or access sensitive data.

Statement of Objectives

The objective of the external penetration testing was to assess the City's current cybersecurity controls in an effort to determine the actionable impact from an attacker attempting to bypass perimeter security controls and accessing the internal network or sensitive data. The focus of penetration testing is not to prove that the network is free of all vulnerabilities, but rather, to validate the organization's security posture and configuration standards through assessing the resiliency of the external network against a determined attacker. This level of testing relies heavily on the techniques and toolsets favored by real-world threat actors in order to closely simulate an attack scenario, and leverages both manual and automated testing methods. The product of external penetration testing is a report that 1. documents the organization's existing security posture, 2. identifies specific weaknesses and vulnerabilities, 3. provides purpose-built exploit codes, 4. Provides examples that tell a compelling story of risk from any given vulnerability and 5. makes recommendations for remediation. Systems that were in-scope for this engagement included, but were not limited to, the following:

- Application Servers
- Network Devices (load balancers, firewalls, etc.)
- Cloud Infrastructure
- Mail Servers

Statement of Methodology

Considering that this was an external penetration test, we closely aligned to the Penetration Testing Execution Standard and followed the below approach:

- Footprinting
  The footprinting process was used to determine the amount of information available through public sources concerning the City.
- Service and Port Identification
  The service and port identification process was performed to identify services and ports, as well as the associated versions running on systems identified through the footprinting process.
- Vulnerability Identification and Exploitation
  From the information obtained in the service and port identification process, we used available resources both online and through well-known hacking tools to identify applicable vulnerabilities and potential public exploits. In the event that a public exploit existed, we attempted to execute it with the objective of obtaining access to the affected system or application.
- Limited Vulnerability Scanning
  Basic vulnerability scanning involved using various commercial and open-source tools to identify vulnerabilities on the City's systems and devices.

Statement of Auditing Standards

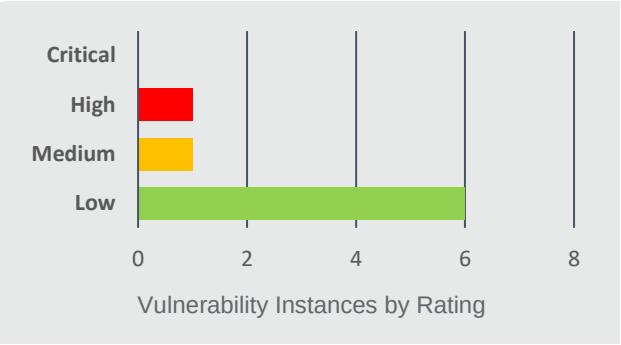
We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. It should be noted that the type and extent of evidence obtained differed because of the nature of the work that was outsourced, proprietary tools used, and the security risks posed.

Conclusions and Summary of Findings

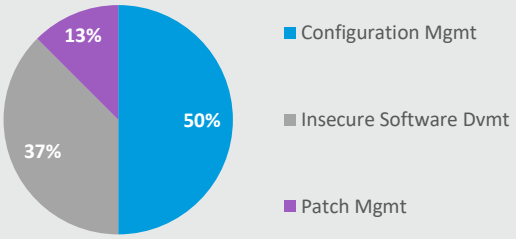
During the external penetration test, the security controls in place were such that we were unable to breach the City's external cybersecurity for the purpose of gaining remote access to the City's internal network. However, this does not mean that a determined bad actor in a real attack could not exploit a vulnerability. There is no organization that can say they are fully protected from a breach.

The following table provides a summary of the vulnerabilities we identified along with their corresponding root causes.

Overall Rating	Low



Vulnerability Instances by Rating



Vulnerability Root Causes

Opportunities for Improvement

Findings and Recommendations

We found vulnerabilities related to configuration management, insecure software development, and patch management. The following tables provide the findings, root causes, recommendations, and management responses at a high level.

Finding Area	Root Cause Description
Configuration Management	Software or network devices have been deployed without the appropriate security settings or are misconfigured, thus increasing the risk of application or system compromise. This introduces avenues for exploitation, weak encryption, and cleartext passwords.
Insecure Software Development	These are findings resulting from poor secure software development practices, such as not properly validating user input and lack of cryptography.
Patch Management	Patches related to single software deployments can introduce vulnerabilities if the system software is not monitored for updates.

The following are the associated recommendations and management responses:

Finding Area	Recommendation
Configuration Management	Disable support for outdated communication protocols. Properly configure the Domain-based Message Authentication, Reporting and Conformance (DMARC) policy to mitigate the risks associated with phishing attacks.
Insecure Software Development	Apply web application best practices such as security response headers, generic error handling, and cookie flags.
Patch Management	Implement a patch management program to ensure that security updates for 3rd party software are applied promptly.
Management Response	Although we agree with the overall findings of the audit, both the audit findings and recommendations are not representative of our current systems or issues. See notes below: **Configuration Management –** the current findings that were referenced are not due to software or network devices having been deployed without the appropriate security settings, nor are they due to misconfigurations. The reported devices and applications are past end-of-life and cannot be upgraded or reconfigured to eliminate older communication protocols or configurations. **Insecure Software Development** – It is important to note that the City's IT Team does not do any in-house software development. The findings associated with insecure software development are the result of older applications that cannot be properly upgraded or configured. As this is known, we have implemented security mitigations to minimize the potential for exploitation. **Patch Management** – The City's IT Team has a very robust patch management

process in place. The findings referenced in the audit are once again due to older, outdated systems and applications.

In summary, all three of the areas where findings were reported are representative of the same issue: needing to replace end-of life hardware and software.

Over the last several years, the IT Team has focused on upgrading and/or replacing outdated or end-of-life systems. As this process has progressed, numerous security mitigations have been implemented with the goal of minimizing or eliminating concerns such as what the audit reported.

The reported findings were known and securely mitigated, and the fact that these devices were not able to be compromised is a testament to the effectiveness of these mitigations.

The IT Team is currently implementing secure configurations where possible and continues to monitor and remediate all vulnerabilities. Additionally, when the conversion to Tyler EPL is complete, some of these end-of-life systems will be removed from the environment and this is scheduled for the end of December 2024.

Target Implementation Date: December 2024