**[Utility Provider] Penetration Test Executive Summary**

Nathan Tendido
Cybersecurity Career Track, Springboard
Penetration Test Capstone
August 20, 2023

# Executive Summary

A Penetration Test was performed on [Utility Provider] to identify vulnerabilities in its networks and systems. The test was conducted using only publicly available information, without using any provided knowledge (such as administrators, IP addresses, email addresses, and technology).

### Goals

- Improve the security of [Utility Provider] for all users and contractors accessing its networks and systems by identifying vulnerabilities and following recommendations to fix identified vulnerabilities
- Improve organization-wide awareness of regulatory system requirements and encourage [Utility Provider] to promote security within its teams

### Vulnerabilities

Vulnerabilities are assessed and ranked following CVSS v3.0 severity rankings as follows: None 0.0; Low 0.1 - 3.9; Medium 4.0 - 6.9; High 7.0 - 8.9; Critical 9.0 - 10.0. Amongst nine total risk observations, the number of severity ranks are:

| Critical | High | Medium | Low | None |
|---|---|---|---|---|
| 3 | 6 | 0 | 0 | 0 |

Key Findings and Recommendations

The recommendations below are detailed more in Technical Report: 6.0 Recommendations.

1. Windows devices are vulnerable to backdoor access using an unpatched service
    a. Recommendation: Patch Windows devices, disable the unpatched service, and fully implement existing VPN solution
2. Web application is vulnerable to database attacks
    a. Recommendation: Reconfigure input fields with validation configuration
3. Security devices can be accessed using publicly-known admin default passwords
    a. Recommendation: Change default admin passwords
4. Web servers are susceptible to unauthorized access and tampering
    a. Recommendation: Update web server systems with vendor patches

5. Web servers are currently exposing sensitive data
    a. Recommendation: Reconfigure web server permissions
6. Web application user privileges are broken
    a. Recommendation: Reorganize and reconfigure access privileges
7. Web servers are vulnerable to unauthorized remote access.
    a. Recommendation: Update web server systems with vendor patches
8. AWS Cloud Storage can be accessed by the public
    a. Recommendation: Reconfigure access controls for AWS
9. Mail server contents and attachments are vulnerable to unauthorized access.
    a. Recommendation: Update systems with Microsoft patches and put mail server into VPN

### Risk

Critical risks include loss of confidential proprietary information, financial information, data breaches leading to financial and reputational loss, as well as non-compliance with industry standard regulations. Non-remediation of all vulnerabilities will leave [Utility Provider], its executives, and customers susceptible to repeat attacks from cyber criminals.

### Conclusion

The penetration test has shown that there are currently critical and high risk vulnerabilities posing a threat to [Utility Provider], its executives, users, and customers. The identified vulnerabilities can be remediated quickly, but additional care should be applied by the security team in order to ensure that systems continue to stay updated and security practices are followed by all employees.

The full list of technical details can be found in the Technical Report.