[Utility Provider] Penetration Test Phase 4: Threat Assessment

Nathan Tendido
Cybersecurity Career Track, Springboard
Penetration Test Capstone
August 19, 2023

Phase 4 Introduction

Prior penetration test activities have identified nine vulnerabilities and associated risks in [Utility Provider]'s network.

Affected devices include:

- *Windows systems*
- *Linux systems*
- *ERP system*
- *Oracle 12c database*
- *Cisco devices*
- *Apache (on-prem) web servers*
- *AWS web servers*
- *AWS cloud storage*
- *Office 365 tenant applications*
- *Office 365 cloud storage*
- *PARS application*
- *APOLLO application*
- *Microsoft Exchange servers (cloud and on-prem)*

Risk Register

Link to Risk Register

Risk Register organizes observed vulnerabilities, identifies associated risks, potential attack vectors to exploit the vulnerability, potential blocking mechanisms, and remediation suggestions. Vulnerabilities are assessed using a CVSS calculator to generate a score, which is 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

Among nine total vulnerability observations, the number of severity ranks are:

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

Risks

Risks include potential unauthorized access to devices, installation of malware and unauthorized backdoors, unauthorized administrative privilege escalation, loss of database and web server integrity, exposure of sensitive system data, user information, and other confidential information, and non-compliance of privacy regulations.

Remediation

Remediation actions include:

- Updating all Windows devices, Apache web servers, Oracle 12c database, and Microsoft applications with latest vendor security patches and updates
- Removing all unsupported hardware
- Reviewing current access control lists and applying role-based access control following least-privilege principles
- Reconfiguring web server directory permissions
- Enabling Multi Factor Authentication on top of Single-Sign On, and applying strong password requirements (such as mixed case, letters, numbers, symbols, and use of a passphrase)