[Utility Provider] Penetration Test Technical Report

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

Table of Contents

Note: When viewed in Google Docs, the outline sidebar function can be used to quickly go to sections.

Back to Table of Contents

1.0 Scope of Work

The penetration test generally focused on [Utility Provider] and its networks and systems. Activities included in the test were only those immediately relevant to reconnaissance, profiling, network/system scanning, and vulnerability assessments. Other activities and networks unrelated to [Utility Provider], unless specified, were considered out of scope and were not included in the penetration test.

1.1 In Scope

- Select and configure tools to perform reconnaissance, enumeration, and vulnerability scans during penetration test of [Utility Provider]
- Perform external perspective reconnaissance activities of [Utility Provider] to create a robust company profile
- Configure and perform scans to discover and enumerate [Utility Provider] networks and systems
- Configure and perform vulnerability scanning to identify potential vulnerabilities in [Utility Provider] networks and systems
- Perform a vulnerability assessment using vulnerability scan results and document recommendations for remediation, including risk, risk potential, affected systems, and CVSS scores
- Compile results of penetration test in a summarized executive summary report for [Utility Provider] executive stakeholders
- Compile results of penetration test in a detailed technical report for [Utility Provider] technical teams

1.2 Out of Scope

- Performing any penetration test activities requiring credentials or access which could not be obtained through reconnaissance and enumeration activities
- Testing physical controls at any of [Utility Provider] physical business sites
- Testing business processes, such as (but not limited to): business continuity activities, disaster response activities, technical support, and help desk activities

Back to Table of Contents

2.0 Project Objectives

2.1 Objectives

- Perform a structured external perspective walkthrough of [Utility Provider] to identify network and system vulnerabilities and provide remediation recommendations

2.2 Goals

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

Back to Table of Contents

3.0 Assumptions

- [Utility Provider]'s networks are operational and currently in use by its employees, contractors, and other clients
- [Utility Provider] will not be shutting down its networks in response to any penetration test activities
- [Utility Provider]'s security team will continue performing SOC tasks during the testing period
- [Utility Provider] has some publicly available information, such as employee names, profiles, contact numbers, etc.
- Tools requiring licensing will be ready by the start of during and will continue to be available over the course of the testing period.
- Testers will have the testing environment operational and ready by the beginning of the testing period.

3.1 Risks

Risks outlined have the potential to negatively impact business operations and should be given extra care during the testing period.

Risk	Description	Severity
Client networks are offline or shut down during the testing period	Will result in a complete halt to client's day-to-day business operations and will completely prevent testers from performing any testing activity directly interacting with the client's networks. Can lead to financial loss and delays in penetration testing activities.	Critical
Client's SOC does not perform regular SOC activities as they would normally	May result in inaccurate and incomprehensive test findings.	High
Testers are unable to find any publicly available information on [Utility	May hinder Reconnaissance activities and result in early end to testing period.	Medium

Back to Table of Contents

Provider] or its employees		
Testing tools are phased out due to lack of support during testing	May result in compromised security systems and lead to delays to testing period. Replacement tools would need to be acquired.	Critical
Testing environment is not ready for testing.	May result in delays to the beginning of the testing phase.	High

Back to Table of Contents

4.0 Timeline

Testing was performed over a one week period between August 13, 2023 and August August 20, 2023. Penetration testing was divided into five phases, each with its own objectives, testing tools and techniques, and deliverable.

4.1 Phase 1: Perform Reconnaissance (2 days)

Testing Objective	Build a robust profile of [Utility Provider] and potential testing targets using only publicly available information
Tools	• OSINT Framework • Google Dorks • theHarvester • Recon-ng • Maltego • Business Info Resources • Social Media Resources • Employment Resources • VoilaNorbert • Shodan • SecurityTrails by Recorded Future • Builtwith • PassiveDNS by Mnemonic • DNSDumpster • DNSlytics
Techniques	• Search Engine and Advanced Techniques • Automated OSINT Frameworks • Link Analysis and Data Visualization • Domain and Web Intelligence • Online Presence and Social Media Profiling • Email and Contact Gathering • Internet Scanning and Enumeration • DNS and Domain Discovery
Deliverables	1. Business and Target Profile (Google Doc) 2. Visualization Map (Maltego)

Back to Table of Contents

4.2 Phase 2: Identify Targets and Run Scans (1 days)

Testing Objective	Run scans to perform host discovery and enumerate the target's network
Tools	● Nmap ● Netcat ● OpenVAS ● Nessus by Tenable ● Dirbuster by OWASP ● SQLmap
Techniques	● Network scanning ● Network enumeration ● Vulnerability assessment ● Web application testing
Deliverables	1. Host and Network Report (Google Doc)

4.3 Phase 3: Identify Vulnerabilities (1 days)

Testing Objective	Perform comprehensive vulnerability assessment scans to identify security weaknesses, misconfigurations, and security gaps in target systems
Tools	● Nessus by Tenable ● GVM ● BurpSuite ● ZAP Zed Attack Proxy ● OpenSCAP
Techniques	● Network Vulnerability Scanning ● Web Server Vulnerability Scanning ● Application Vulnerability Scanning ● Compliance Scanning
Deliverables	1. Compiled Scan Results (Google Doc)

Back to Table of Contents

4.4 Phase 4: Threat Assessment (2 days)

Testing Objective	Analyze previous scan results to identify system vulnerabilities, associated risks, attack vectors, and recommend steps for remediation.
Tools	● NIST CVSS v3.0 Calculator
Techniques	● Threat Assessment
Deliverables	1. Threat Assessment Summary (Google Docs 2. Risk Register (Google Sheet)

4.5 Phase 5: Reporting (2 days)

Testing Objective	Compile results and findings from previous phases into a summarized executive summary and a detailed technical report to be shared with [Utility Provider] stakeholders.
Tools	● Google Doc
Techniques	● Reporting
Deliverables	1. Executive Summary (Google Doc) 2. Technical Report (Google Doc)

Back to Table of Contents

5.0 Summary of Findings

Testers were able to complete all testing activities for this project.

Testers were able to create a detailed profile of [Utility Provider]'s business, business practices, executives, and employees, by using only publicly available information obtained using OSINT framework methodologies.

Testers were successful in performing scans and enumerating [Utility Provider]'s web servers, internal network, associated IP addresses, domains, and email addresses.

Testers were successful in performing vulnerability assessment scans and identified nine observed vulnerabilities. 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
- Low
- None: 0

5.1 Remediation Summary

Below are statements summarizing recommendations for remediation. Each statement is elaborated on in more detail in 6.0 Recommendations.

- ☐ Patch and update systems
- ☐ Remove/Replace EOL hardware
- ☐ Review and modify web application access controls
- ☐ Change all default passwords
- ☐ Fully implement Zscaler and block RDP connections
- ☐ Implement strong password mechanisms
- ☐ Review web directory permissions

Back to Table of Contents

- [ ] Remediation for Microsoft Exchange Server Vulnerability CVE-2021-26855
- [ ] Enable input validation for Oracle 12c database

Back to Table of Contents

6.0 Recommendations

6.1 Patch and update systems

Applicable systems: Windows devices, ERP, Cisco devices, on-prem Apache web servers

Several vulnerabilities found have been identified and fixed in vendor patches. However, these vendor patches are absent from client's systems at the time of testing. Security team should test and apply patch updates as soon as possible for immediate remediation. Additionally, implementing a patch routine process would significantly decrease the likelihood of future system exploits.

Risk if not remediated:

- Attacker backdoor access on all exploited Windows devices and on-prem web servers (Risk 1)
- Loss of web server file integrity (Risk 4)
- Attacker execution of arbitrary commands (Risk 7)
- Attacker access to user emails and attachments (Risk 9)
- Attacker access to confidential proprietary information (Risk 9)

6.2 Remove/Replace EOL hardware

Applicable systems: Windows devices, Cisco devices, on-prem Apache web servers

Security team should check with system vendors for up-to-date patch information and check for vendor support. If devices are no longer being supported by the vendor, the security team should make immediate steps to: 1) migrate any mission critical files and processes to new supported hardware and 2) decommission and destroy all old end-of-life devices. Security team should follow the organization's decommissioning process in order to ensure that data remnants cannot be obtained from decommissioned devices.

Risk if not remediated:

- Potential infiltration of malware/ransomware on EOL devices (Risk 1, 4, 7)

Back to Table of Contents

- Lack of vendor support in the event of future system attacks (Risk 1, 4, 7

6.3 Review and modify web application access controls.

Applicable systems: PARS, APOLLO

Broken access control has been identified in the PARS and APOLLO applications. Security team should review access control privileges and re-assign access following the least privilege principle. Role-Based Access Control (RBAC) is recommended (assigning access to Roles, and then assigning Roles to individuals) in order to ease management and monitoring of access controls.

Risk if not remediated:

- Loss of non-repudiation (vulnerability to session hijacking) (Risk 6)
- Exposure of sensitive data such as PID, passwords, and financial details (Risk 6)

6.4 Change all default passwords

Applicable systems: Cisco devices

Default admin passwords have been identified on the Cisco Admin Portal. Default passwords are publicly documented and well-known amongst cybercriminals. Changing the password to a non-default password is immediate remediation.

Two-factor or Multi-factor authentication is also recommended for Cisco devices.

Risk if not remediated:

- Attacker brute-force access to Cisco systems (Risk 3)

6.5 Fully implement Zscaler and block RDP connections.

Applicable systems: Windows devices

Back to Table of Contents

Unpatched RDP has been found to be exposed to the internet. Client is already using Zscaler for secure remote application access. A listing of users requiring remote application access should be created and evaluated before granted access to Zscaler. Additionally, a formal onboarding/training process should be developed and tracked for employees being granted access to Zscaler. Employees should be trained on secure remote working practices using Zscaler and discouraged to use RDP for all remote activities.
RDP should be closed on all Windows systems. Cisco, Fortinet, Palo Alto, and F5 firewalls should be configured to block inbound and outbound RDP connections.

Risk if not remediated:

- Attacker backdoor access on all exploited Windows devices and on-prem web servers (Risk 1)
- Potential attacker lateral movement throughout the network (Risk 1)

6.6 Implement strong password mechanisms

Applicable systems: Cisco devices, Windows devices, PARS, APOLLO

Client is currently utilizing Single Sign-On (SSO) but with only single-factor authentication. Client should review password requirements and implement the use of mixed character, mixed case, punctuation, and prohibit the use of common dictionary passwords.

Security team should also implement quarterly password expiration and user session limits. Multi-factor authentication is also recommended for all user accounts, especially accounts with admin privileges.

Risk if not remediated:

- Attacker gaining access to user accounts via brute-force or rainbow table attacks (Risk 3, 6)

6.7 Review web directory permissions

Applicable systems: On-prem Apache web servers, AWS servers

Back to Table of Contents

Sensitive web server data and cloud storage data has been identified and found using Google Dorks techniques. Security team should review and adjust web directory permissions to ensure that potential threat actors would not be able to directly access exposed directories and block attempts at directory traversal.

Additionally, S3 bucket permissions should be reviewed and reconfigured.

Risk if not remediated:

- Extraction of sensitive user data (Risk 5)
- Identity theft (Risk 5)
- Attackers accessing and modifying critical cloud data (Risk 8)

6.8 Remediation for Microsoft Exchange Server Vulnerability CVE-2021-26855

Applicable systems: Windows devices, ERP, Cisco devices, on-prem Apache web servers

Several vulnerabilities found have been identified and fixed in vendor patches. However, these vendor patches are absent from client's systems at the time of testing. Security team should test and apply patch updates as soon as possible for immediate remediation. Additionally, implementing a patch routine process would significantly decrease the likelihood of future system exploits.

Risk if not remediated:

- Attacker backdoor access on all exploited Windows devices and on-prem web servers (Risk 1)
- Loss of web server file integrity (Risk 4)
- Attacker execution of arbitrary commands (Risk 7)
- Attacker access to user emails and attachments (Risk 9)
- Attacker access to confidential proprietary information (Risk 9)

6.9 Enable input validation for Oracle 12c Database

Applicable systems: ERP, Oracle 12c Database

Back to Table of Contents

A vulnerability to SQL injection via the web application input fields has been identified. Security team can enable server-side input validation, to reject unusual/invalid inputs (such as comments, script commands, and overflow attempts) and also disable client-side input validation.

Risk if not remediated:

- Exfiltration of sensitive user data (Risk 2)
- Attacker gaining ability to execute arbitrary SQl queries (Risk 2)

Back to Table of Contents