Limited Executive Summary

The results of the penetration test and some advice on how to fix security flaws will be outlined here.

Introduction

The primary objective of this penetration test is to assess the susceptibility of company assets to unauthorized access and to aid the company in enhancing its security posture through actionable guidance. An external penetration test of the network, an external penetration test of the web applications, and an internal penetration test of the company network (if access is obtained) will be conducted.

The parties involved in the test and their contact information is outlined here:

Position	Name	Contact Information
Principal Penetration Tester	Areej Ali	areeja132000@gmail.com

The timeline of the penetration test will be as follows:

Phase of penetration test	Date
Pre-engagement interactions	3 days
Intelligence gathering	1 week
Threat Modelling	1 day
Vulnerability Analysis	1 week
Exploitation	1 week
Post Exploitation	1 week
Reporting	3 days

The cost of the penetration test will be $4000.

Scope

Targets include all internet facing hosts, services, and web applications. The internal network can also be made subject to the penetration test if access is obtained.

As outlined by the company, the following items are out of scope:

- Vendor-hosted VPN provider
- Physical penetration test
- Existing NBN Subs and BP accounts
- Distributed Denial of Service attacks

Rules of engagement will be determined in the pre-engagement interactions.

Methodology

Testing

The types of tests that will be carried out are as follows:

1. External Network Pen Testing
    - All internet facing hosts and services
2. External Web App Pen Testing
    - All internet facing web applications
3. Internal Network Pen Test
    - If penetration tester can gain internal network access

Steps

The steps followed in this penetration test are based on the Penetration Testing Execution Standard (PTES)

1. Pre-engagement interactions

This will allow the penetration tester to gain further details about the test. Some questions to be addressed include the following:

a. What is in/out of scope (e.g., social engineering)
b. Confirm what equipment is owned by the company (e.g., the DNS server, the email server, the hardware on which the web servers run, firewall/IDS/IPS)
c. Confirm the dates and times (after hours, during weekends) during which it is acceptable for the penetration tester to engage in port scanning, enumeration, and exploitation
d. Ask if the penetration test is being conducted to meet a specific compliance requirement

2. Intelligence gathering

Intelligence gathering can be further separated into roughly three steps. The steps are as follows:

a. OSINT and recon-ng to obtain list of users, emails
b. Determine domains and network blocks owned (WHOIS lookup, BGP looking glass, recon-ng)
c. Port scanning (with Nmap) and banner grabbing to obtain information about which applications, hosts, and services are being run. Shodan will be used to identify further services

3. Threat Modelling

Threat modelling is done to determine which assets hold the most importance to the company and what threat actors could be looking for. It provides additional context to determine the risk score in later steps. Threat modelling can be further divided into the following four steps:

a. Get company documents outlining policies, plans, and procedures
b. Identify assets and determine rank them in order of importance
c. Identify threat actors and categorize them by capability
d. Determine likely targets of relevant threat actors

4. Vulnerability Analysis
    a. Automated vulnerability detection with OpenVAS and Nessus
    b. Look through port scanning output to manually determine if there are any other services that could be vulnerable
    c. Examine web applications for vulnerabilities like SQL injections, XSS, CSRF, and more

5. Exploitation

This phase of the penetration test will focus on bypassing security.

6. Post Exploitation

This phase will focus on determining whether the machine compromised can lead to a compromise of a valued asset of the company. Furthermore, the penetration tester will look to maintain control of the machine compromised for future use.

7. Reporting

The results of the penetration test are recorded.

Risk Scoring Methodology

Risk is determined by considering the factors of likelihood and impact (Risk = Likelihood * Impact). The following table incorporates likelihood/ease-of-exploitation (easy, moderate, or requiring social engineering) and the resulting impact (usually being a compromise of company assets), to assign a score indicating the severity of the security flaw.

The following table and CVSS V3 score ranges will be used to assess risk:

CVSS Score Range	Severity	Definition
9-10	Critical	Exploitation is easy and attacker gains full control of a system. This control gives them access to company assets. Should be patched immediately.
7-8.9	High	Exploitation is more difficult, but elevated privileges can be obtained, and company assets

		could be compromised. Should be patched as soon as possible.
4-6.9	Moderate	Exploitation can be achieved, but social engineering is required. It is recommended that higher priority security flaws be addressed first.
0.1-3.9	Low	The vulnerability is not exploitable because of the way the system is set up or other security controls that are in place. It is recommended that these be solved whenever maintenance is done in the future