**Testing Document and Specification**

Test Plan

BIT Team 17

CS 451, WS 2006

|  |  |  |
| --- | --- | --- |
| Andrew Taylor | Liam Floyd | Ryan Sheppard |
|  |  |  |

# **Introduction**

This document outlines the test plan for the Network that is being designed for Monstrosity Inc. The network and database need to be secure and the customer and employee wifi need to be separate. The testing activities discussed in this document will verify that the customers will not have access to the employee network and that the database is secure from those that do not have access.

# **Terminology**

This section defines potentially unfamiliar or ambiguous words, acronyms, and abbreviations.

**Network** - refers to the physical infrastructure of a group of two or more computer systems linked together. There are many types of computer networks, including Local Area Networks (LAN), Wireless Internet (wifi), and Wide Area Networks (WAN).

**SQL injection** - placement of malicious code in SQL statements

**Feature/Subfeature Tested**

Items that will be tested during the testing phase will be:

* Access of Employee Network through customer network
* Security of database against SQL injections ·
* Security of Office Network against unauthorized access

**Purpose**

* Ensure customers cannot gain access to the company network
* Ensure only authorized access to company resources
* Ensure data integrity of database systems
* Ensure the availability of system resources and services
* Ensure customer and employee internet access is partitioned
* Prevent hacking and unauthorized penetration of the system

**Items Not Tested**

There are features that will not be included in the current testing procedure. This does not mean that these features will not be implemented, but that they have not been implemented and are not available for testing. Most cloud-hosted services would not be tested, as they are outside the reach of Monstrosity IT to rectify issues. Large cloud providers such as AWS and Azure are operated by large, trusted technology companies. While security can never be perfect, Microsoft has very robust security and manages all hosted apps for Monstrosity.

# **Approach**

A series of penetration tests will be performed on the employee network to ensure that no one has access to it. A series of SQL injection tests will be performed on the database to ensure that it is safe from SQL attacks. Various test users will be created to test logins and all access across different security groups, email between users within the organization and outside. Monstrosity would hire a third party pentesting service such as Rapid7, to perform comprehensive penetration testing of the corporate network.

# **Item Pass/Fail Criteria**

In order to pass, no attempt to penetrate the employee network from the customer network will be successful, and no SQL injection attempts can be successful. The ability to hijack access to restricted networks would result in a failure. However, no network is absolutely perfect so there is a tolerance for failure but the end goal of penetration and injection testing is to highlight where improvements can be made to the network configuration or webpage connection to the database and implemented.

# **Testing Tasks**

The following lists the testing deliverables and the activities required to produce the deliverable.

|  |  |
| --- | --- |
| **Deliverables** | **Activities** |
| **Test Plan** | * Develop Approach/Method for testing * Determine Task and Estimate Efforts * Develop Schedule for Testing |
| **Test Specifications** | * Analyze Requirements * Define Tests as Outlined by the Test Plan |
| **Test Data** | * Create a series of ‘correct’ testing data to use for authorized access * Create a series of ‘incorrect’ testing data to ensure denial of access |
| **Test Actions** | * Perform penetration testing * Attempt authorized access * Attempt unauthorized access * Test routing and switching of network |
| **Expected Results** | * Only authorized test data would gain access to network and system resources * Any unauthorized test data would be denied access to network and system resources * Intrusion detection system and firewalls would log the access * Firewall, switches, routers would all function properly |
| **Test reports** | * Implement Tests as Outlined by the Test Specifications * Document Incidents and Defects * Determine Changes that Need to be Made to Network or database * Document and Submit Change Request |