Penetration Tester

Product Design Specification

Version 1.1

11/6/17

Authors:

Jacob Wild

Anson Lytkchiuofoousefache (Lichtfuss)

Spencer Ollila

T. A. Marquard

Eric Mill

Version History

[info]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version  # | Implemented  By | Revision  Date | Approved  By | Approval  Date | Reason |
| 1 | T.A. Marquard | 10/25/17 | Spencer Ollila | 10/25/17 | Getting Started |
| 2 | Eric Mill | 11/6/17 |  |  | Adding some |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Notes

Table of Contents

**INTRODUCTION1**

1.1 Purpose of Product Design Specification Document2

**GENERAL OVERVIEW AND DESIGN GUIDELINES/APPROACH4**

2.1 Assumptions / Constraints / Standards5

**ARCHITECTURE DESIGN**…………………………………………………………………………………………………………………………..6

3.1 Logical View…………………………………………………………………………………………………………………………………..7

3.2 Hardware Architecture………………………………………………………………………………………………………………….8

3.3 Software Architecture……………………………………………………………………………………………………………………9

3.4 Security Architecture…………………………………………………………………………………………………………………..10

3.5 Communication Architecture………………………………………………………………………………………………………11

3.6 Performance……………………………………………………………………………………………………………………………….12

**SYSTEM DESIGN**…………………………………………………………………………………………………………………………………….12

4.1 Use-Cases…………………………………………………………………………………………………………………………………….12

4.2 Database Design………………………………………………………………………………………………………………………….12

4.3 Data Conversions…………………………………………………………………………………………………………………………12

4.4 Application Program Interfaces……………………………………………………………………………………………………12

4.5 User Interface Design………………………………………………………………………………………………………………….11

4.6 Performance……………………………………………………………………………………………………………………………….12

4.7 Section 508 Compliance………………………………………………………………………………………………………………12

**PRODUCT DESIGN SPECIFICATION APPROVAL**………………………………………………………………………………………12

**APPENDIX A: REFERENCES**……………………………………………………………………………………………………………………12

APPENDEX B: Key Terms……………………………………………………………………………………………………………………….12

1. **Introduction**
   1. **Purpose of the Product Design Specification Document**

The Product Design Specification document will document and track the design and planning of the Mobile Penetration Tester.

1. **General Overview and Design Guidelines/Approach**

Principals/Strategies to be used as guidelines when designing/implementing.

1. Identify what we need to protect.

2. Determine what we need to protect it from.

3. Determine how likely the threats are.

4. Implement measures to protect assets in cost effective manner.

5. Review and continuously improve when weakness is found.

* 1. **Assumptions / Constraints / Standards**

Multiple standards exist when testing cyber security some good ones are:

* RFC 2196
* NIST Cybersecurity Framework
* ISO/IEC 27000-27003 (Information Security Standard)

1. **Architecture Design**
   1. **Logical View**
   2. **Hardware Architecture**

There are many hardware components to our design. We will interface with and attempt to penetrate a network from multiple angles, and this requires a diversity of hardware.

1. Rubber Ducky

The Rubber Ducky will need to be plugged into a computer connected to the network in question. It will attempt to gather information and send it/ store it in a secure way.

1. LAN Turtle

The LAN Turtle will also need to be physically plugged into the network. It will mimic a standard Ethernet to USB connector. Its purpose will be to expose vulnerabilities in the network so they can be fixed.

1. Wi-Fi Pineapple
2. Raspberry Pi
3. Server (?)
4. DoS Attacks (?)
   1. **Software Architecture**

We will have scripted actions and some automation in much of what happens, including an automated report. This will involve shell scripting. We also will need a program to gather and sort information. We may potentially want some communication among our hardware that will involve some communication program.

* 1. **Security Architecture**

Since all the information we are dealing with is potentially sensitive, we will need strong encryptions, as well as secure connections.

* 1. **Communication Architecture**

We will be potentially communicating and relaying info with an external server.

* 1. **Performance**

We will have a baseline computer that proves our stuff does work.

1. **System Design**
   1. **Use-Cases**

This system is designed to be used on small networks to expose vulnerabilities so they can be quickly fixed before a malicious attack occurs.

* 1. **Database Design**

The database will need to hold the results from all of our tests so we can quickly see how the network performed with each test. We will also have large amounts of raw data in the form of logs and filtered packets. This raw data will need to be put into a large database so that we can sort out only the pertinent information.

* 1. **Data Conversions**

Raw data and logs will need to be compiled into a form that makes it easy for the user of the testing system to see necessary information. This may involve writing SQL queries and custom filters for large databases.

* 1. **Application Program Interfaces**

Kali Linux, Rubber Ducky interface software, LAN Turtle interface software, SSH, any others…

* 1. **User Interface Design**

If we have some custom program to compile and display the results of our tests.

* 1. **Performance**

Need to discuss and research pass/fail criteria for each test.

* 1. **Section 508 Compliance**

1. **Product Design Specification Approval**

**Appendix A: References**

**Appendix B: Key Terms**