Penetration Tester

Product Design Specification

Version 1.3

12/2/17

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 |
| 3 | All - Spencer | 12/2/18 |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

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)
* Gnu General Public License agreement

1. **Architecture Design**
   1. **Logical View**

There is no logical view for the architectural design for this product.

* 1. **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

The Wi-Fi Pineapple will be deployed on the customer’s network as a man-in-the-middle device for wireless network testing.

* 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 utilizing an encrypted e-mail service such as ProtonMail. This is to further protect the team’s communications where sensitive information may be relayed to each other and the customer before, during and after the test. The team is currently using Slack to communicate for the purposes or product production with documentation being maintained on GitHub.

* 1. **Performance**

This is dependent on the end-users hardware and infrastructure.

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. It is designed as a low cost, DIY penetration testing package that gives small businesses and non-profits a foundation in cybersecurity tools and hardware; That they can initially utilize and build their expertise with.

* 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 is a Linux distribution that has its own user interface. Rubber Ducky utilizes a simple scripting language called Ducky Script. LAN Turtle uses an interface called Turtle Shell to provide SSH in to networks. WIFI Pineapple software is called the Pineapp Suite.

* 1. **User Interface Design**

Most of the software that we will be including is free, open source and already includes well developed user interfaces. The included hardware (Rubber Ducky, Lan Turtle and WIFI Pineapple) have well developed and supported UI’s. We will be designing the user interfaces for the generated reports and documentation.

* 1. **Performance**

Performance of the project will have a pass/fail metric for each test. Each device and tool should expose a vulnerability that can then be mitigated by finding this weakness. We cannot simply attack, we must secure.

* 1. **Section 508 Compliance**

Non-applicable to hardware and software components.

1. **Product Design Specification Checklist**
   1. **Environment**
      1. **Transportation**

We have a waterproof and shock resistant container for the system that will be used to protect it from environmental hazards to and from the testing site.

* + 1. **Deployment**

This will be in the clients facilities that will more than likely be climate controlled. Due to the nature of this product these environments will already be conducive to the safe deployment of this system.

* 1. **Target product Cost**
     1. **Cost to build**

RubberDucky: $44.99

WiFi Pineapple Nano Tactical: $159.99

LAN Turtle: $49.99

Hack5 Field Kit: $20.00

Pelican 1060 Micro Series: $25.00

Estimated R&D cost: $10800.01

* + 1. **Projected MSRP**

$499.97 + Shipping and Handling

* 1. **Competition**

None that we could find.

* 1. **Quantity and Manufacturing**

Manufacturing will be completed to-order, with individual components being purchased from outside sources. All of the disparate pieces of the product will be assembled, packaged, and shipped by the team.

* 1. **Materials**

All instructional materials and relevant legal documentation will be included on a USB drive in the package.

* 1. **Quality and consistency**

Every component of the package will be pre-tested to ensure full operability within the specifications defined in this document. All devices will be upgraded to the latest versions of their respective firmware and software.

* 1. **Standards**
* 802.11 WIFI Standards
* RFC 2196
* NIST Cybersecurity Framework
* ISO/IEC 27000-27003 (Information Security Standard)
* Gnu General Public License agreement
* HIPAA
* ECPA
* RoHS
  1. **Patents**

*Find patent numbers for:*

* RubberDucky – US9582445B1
* WiFi Pineapple Nano Tactical – US9730075B1
* LAN Turtle – US7707348B2

*Patent numbers not needed:*

* Kali Linux
  1. **Packaging and shipping**

It will be packaged inside a Pelican 1060 Micro case. This will be contained within a custom designed box filled with bubble-wrap to ensure product integrity. We will then physically ship this to the customer via a mailing system.

* 1. **Aesthetics and ergonomics**

The aesthetics and ergonomics of the product are ideally matched to a penetration testing and cybersecurity testing environment. This is due to the nondescript housing of the hardware and the intuitive software that is utilized.

* 1. **Market Constraints**

This specific market does not currently exist, but it overlapped by other existing markets. The product is ephemeral due to the natural of the attack and defense industry. The physical hardware should last 1-5 years depending on amount of usage and deployment environment. June 2018 is the target release date for the product. Our customers expect effective and easy-to-use penetration testing tools, which allow them to ensure the integrity of their data.

**Appendix A: References**

**Appendix B: Key Terms**