Penetration Tester for Non-Profits and Small Businesses

Product Design Specification

Version 1.3

12/12/17

Authors:

Jacob Wild

Anson Lichtfuss

Spencer Ollila

T. A. Marquard

Eric Mill

Version History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | 12/2/17 |  |  |  |
| 4 | All | 12/12/17 | Marquard | 12/12/17 | Dr. Borowczak thought it needed more work. |
|  |  |  |  |  |  |

# Table of Contents

[Introduction 5](#_Toc500860699)

[Purpose of the Product Design Specification Document 5](#_Toc500860700)

[General Overview and Design Guidelines/Approach 5](#_Toc500860701)

[Assumptions / Constraints / Standards 5](#_Toc500860702)

[Architecture Design 5](#_Toc500860703)

[Logical View 5](#_Toc500860704)

[Hardware Architecture 5](#_Toc500860705)

[Software Architecture 6](#_Toc500860706)

[Security Architecture 6](#_Toc500860707)

[Communication Architecture 6](#_Toc500860708)

[Performance 6](#_Toc500860709)

[System Design 7](#_Toc500860710)

[Use-Cases 7](#_Toc500860711)

[Database Design 7](#_Toc500860712)

[Data Conversions 7](#_Toc500860713)

[Application Program Interfaces 7](#_Toc500860714)

[User Interface Design 7](#_Toc500860715)

[Performance 7](#_Toc500860716)

[Section 508 Compliance 7](#_Toc500860717)

[Product Design Specification Checklist 8](#_Toc500860718)

[Environment 8](#_Toc500860719)

[Transportation 8](#_Toc500860720)

[Deployment 8](#_Toc500860721)

[Target product Cost 8](#_Toc500860722)

[Cost to build 8](#_Toc500860723)

[Projected MSRP 8](#_Toc500860724)

[Competition 8](#_Toc500860725)

[Quantity and Manufacturing 8](#_Toc500860726)

[Materials 8](#_Toc500860727)

[Quality and consistency 8](#_Toc500860728)

[Standards 8](#_Toc500860729)

[Patents 9](#_Toc500860730)

[Packaging and shipping 9](#_Toc500860731)

[Aesthetics and ergonomics 9](#_Toc500860732)

[Market Constraints 9](#_Toc500860733)

[Use Cases 9](#_Toc500860734)

[Users in a Wireless and Wired Environment 9](#_Toc500860735)

[Tools Used: 10](#_Toc500860736)

[Outcome: 10](#_Toc500860737)

[Users in a Wireless Environment 11](#_Toc500860738)

[Tools Used: 11](#_Toc500860739)

[Outcome: 11](#_Toc500860740)

[Users in a Wired Environment 11](#_Toc500860741)

[Tools Used: 11](#_Toc500860742)

[Outcome: 12](#_Toc500860743)

[Re-evaluation of a previously scanned network 12](#_Toc500860744)

[Tools Used: 12](#_Toc500860745)

[Outcome: 13](#_Toc500860746)

[Goals & Dates 13](#_Toc500860747)

[January 13](#_Toc500860748)

[March 13](#_Toc500860749)

[May 13](#_Toc500860750)

[Long Term 13](#_Toc500860751)

# Introduction

## 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.

# 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.

## 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

# Architecture Design

## Logical View

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

## 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. The information it is after should be things such as network information, and password files. The Rubber Ducky will primarily perform keystroke injection attacks and keystroke logging to get sensitive information directly from the targeted computer.

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. Once in place the full functionality of the LAN Turtle can be leveraged off-site through an SSH client like Putty. Through this access we can sniff URLs, transfer files, and create a back door to a shell on the target computer. Because the Turtle is physically plugged into the network it can also do network manipulation such as DNS spoofing and malicious payload injection.

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. The Pineapple provides a broad overview of the wireless landscape in the area where it is deployed. Wireless devices that access the Pineapple have their information scanned and logged to allow the tester to analyze and identify vulnerable access points.

## 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.

* Rubber Ducky
  + Scripts will work to go through the user environment to find info on network protocols.
  + It will track key strokes to find common websites and usernames and passwords.
  + Disconnect the user from the network, and have them reenter the password.
* WiFi Pineapple
  + The PineAP will allow users to quickly scan the network and start gathering information almost instantly.
  + PineAP suite also allows testers to target specific devices or access points in the network without effecting the entire network.
* Phishing
  + Will download an executable that starts retrieving information and downloading more malicious software. There will also be some that redirect to fake login pages so that passwords and users can be gained.
* LAN Turtle
  + Putty and AutoSSH will be set up to provide access from any location.
  + URLSnarf can sniff and log any URL to analyze network traffic.
  + DNS-Spoof and DNSmasq-Spoof can be used to redirect legitimate traffic to malicious sites.
  + SSHFS can be used to transfer files to or from the target computer.
  + The Turtle itself allows remote access to a shell on the target computer through its TurtleShell program.

## Security Architecture

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

## 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.

## Performance

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

# System Design

## 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.

## 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.

## 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.

## 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 Pineapple Suite.

## 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.

## 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.

## Section 508 Compliance

Non-applicable to hardware and software components.

# Product Design Specification Checklist

## Environment

### 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.

### 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.

## Target product Cost

### 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

### Projected MSRP

$499.97 + Shipping and Handling

## Competition

None that we could find.

## 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.

## Materials

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

## 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.

## 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

## Patents

*Find patent numbers for:*

* Rubber Ducky – US9582445B1
* WiFi Pineapple Nano Tactical – US9730075B1
* LAN Turtle – US7707348B2

*Patent numbers not needed:*

* Kali Linux

## 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.

## 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.

## 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.

# Use Cases

## Users in a Wireless and Wired Environment

The User will be using all aspects of the product. First step will be to plug in the Rubber Ducky, LAN Turtle, and WiFi Pineapple in the recommended locations. When the products, or a sub-set of the products are in place, a verification email will be sent to the specified user at the company to let them know it is going, and if only some are working, they will be given instructions on what they should look for to get it working. The hardware is coordinated with a central server that will be monitoring the hardware at all times to measure performance and reliability. At the time of verification, phishing and web attacks will also begin. The basic scripts will coordinate with one another to ensure performance, and pass valuable information such as common phrases likely to appear as passwords to aide in the cracking of the security. The product is suggested to run for 1 month, and reports generated at the 2, and 4 week mark in addition to the verifications of operation.

### Tools Used:

* Rubber Ducky - Simulates user input.
  + May recover passwords and other details of the local network. Will help the Wi-Fi Pineapple identify pertinent network information.
* LAN Turtle – Intercepts wired network communications.
  + May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
  + Can remotely access and control a targeted computer.
* Wi-Fi Pineapple – Intercepts wireless network communication
  + May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
* Phishing Attacks – Attack via social engineering
  + Attempt to gain sensitive information for critical business tools by sending attacks built using social engineering.

### Outcome:

After the initial evaluation period, the User will be sent a final report summarizing all successful attacks and vulnerabilities discovered. The report will be generated automatically via a proprietary system. If certain issues are discovered, the User will be given instructions on how to fix the issues. Another evaluation period will be conducted to verify the found problems are successfully fixed.

## Users in a Wireless Environment

The User will be using some aspects of the product. First step will be to plug in the Rubber Ducky and WiFi Pineapple in the recommended locations. When the products, or a sub-set of the products are in place, a verification email will be sent to the specified user at the company to let them know it is going, and if only some are working, they will be given instructions on what they should look for to get it working. The hardware is coordinated with a central server that will be monitoring the hardware at all times to measure performance and reliability. At the time of verification, phishing and web attacks will also begin. The basic scripts will coordinate with one another to ensure performance, and pass valuable information such as common phrases likely to appear as passwords to aide in the cracking of the security. The product is suggested to run for 1 month, and reports generated at the 2, and 4 week mark in addition to the verifications of operation.

### Tools Used:

* + Rubber Ducky - Simulates user input.
    - May recover passwords and other details of the local network. Will help the Wi-Fi Pineapple identify pertinent network information.
  + Wi-Fi Pineapple – Intercepts wireless network communication
    - May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
  + Phishing Attacks – Attack via social engineering
    - Attempt to gain sensitive information for critical business tools by sending attacks built using social engineering.

### Outcome:

After the initial evaluation period, the User will be sent a final report summarizing all successful attacks and vulnerabilities discovered. The report will be generated automatically via a proprietary system. If certain issues are discovered, the User will be given instructions on how to fix the issues. Another evaluation period will be conducted to verify the found problems are successfully fixed.

## Users in a Wired Environment

The User will be using some aspects of the product. First step will be to plug in the Rubber Ducky and LAN Turtle in the recommended locations. When the products, or a sub-set of the products are in place, a verification email will be sent to the specified user at the company to let them know it is going, and if only some are working, they will be given instructions on what they should look for to get it working. The hardware is coordinated with a central server that will be monitoring the hardware at all times to measure performance and reliability. At the time of verification, phishing and web attacks will also begin. The basic scripts will coordinate with one another to ensure performance, and pass valuable information such as common phrases likely to appear as passwords to aide in the cracking of the security. The product is suggested to run for 1 month, and reports generated at the 2, and 4 week mark in addition to the verifications of operation.

### Tools Used:

* + Rubber Ducky - Simulates user input.
    - May recover passwords and other details of the local network. Will help the Wi-Fi Pineapple identify pertinent network information.
  + LAN Turtle – Intercepts wired network communications.
    - May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
    - Can remotely access and control a targeted computer.
  + Phishing Attacks – Attack via social engineering
    - Attempt to gain sensitive information for critical business tools by sending attacks built using social engineering.

### Outcome:

After the initial evaluation period, the User will be sent a final report summarizing all successful attacks and vulnerabilities discovered. The report will be generated automatically via a proprietary system. If certain issues are discovered, the User will be given instructions on how to fix the issues. Another evaluation period will be conducted to verify the found problems are successfully fixed.

## Re-evaluation of a previously scanned network

In this case, the User's network has already undergone the initial and follow-up scans for vulnerabilities. For either verifying those vulnerabilities are fixed, or searching for more vulnerabilities the network will be scanned again. The User will be using some or all aspects of the product. First step will be to plug in the necessary tools in their recommended locations, which may Rubber Ducky, LAN Turtle, and WiFi Pineapple. When the products, or a sub-set of the products are in place, a verification email will be sent to the specified user at the company to let them know it is going, and if only some are working, they will be given instructions on what they should look for to get it working. The hardware is coordinated with a central server that will be monitoring the hardware at all times to measure performance and reliability. At the time of verification, phishing and web attacks will also begin. The basic scripts will coordinate with one another to ensure performance, and pass valuable information such as common phrases likely to appear as passwords to aide in the cracking of the security. The product is suggested to run for 1 month, and reports generated at the 2, and 4 week mark in addition to the verifications of operation.

### Tools Used:

* + Rubber Ducky - Simulates user input.
    - May recover passwords and other details of the local network. Will help the Wi-Fi Pineapple identify pertinent network information.
  + LAN Turtle – Intercepts wired network communications.
    - May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
  + Wi-Fi Pineapple – Intercepts wireless network communication
    - May recover passwords and other sensitive, unsecured information passing through the network and to the internet.
  + Phishing Attacks – Attack via social engineering
    - Attempt to gain sensitive information for critical business tools by sending attacks built using social engineering.

### Outcome:

After the initial evaluation period, the User will be sent a final report summarizing all successful attacks and vulnerabilities discovered. The report will be generated automatically via a proprietary system. If certain issues are discovered, the User will be given instructions on how to fix the issues. Another evaluation period will be conducted to verify the found problems are successfully fixed.

# Goals & Dates

## January

By January we are planning on having all of the hardware together, and starting to get to a point where we are understanding the basics of how to use it all.

## March

By March we plan on getting to a semi-coagulated state with all of our pieces of hardware and getting to a solid state on not only what we are going to be doing with all our respective projects, but exactly how to do them.

## May

By May the project and all of its parts should be finished and in a place where we can knock the socks off of anyone who dares to inquire about our fantastic works. A simple guide should be put together by this point which would allow most of anyone (regardless of their level of tech-savviness) to be shipped a package of the hardware, follow the instructions, and start up the process without needing one of us present (because driving out to Gillette sucks).

## Long Term

Long term goals for the project include creating a repository of in-depth instructional videos for users to watch in order to watch how we would set up the system ourselves, and ones to show how to help protect themselves from all manners of attacks.

Figuring out which data points we collect that would make the biggest impact on the users would also be good. (How would we most impress upon them WHY they should be more careful, and what would a malicious hacker easily been able to grab?)