VoodooPi

All-in-one Kali Linux Machine

by Brett Copeland Eder Aguilar Jonathan Coleman

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Brett Copeland	April 17, 2017 Date
Jonathan Coleman	April 17, 2017 Date
Eder Aguilar	April 17, 2017 Date
Bogdan Vykhovanyuk, Faculty Advisor	April 17, 2017 Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2017

Table of Contents

Tables and Figures

Acknowledgement

We would like to thank all our professors that have helped pave the way for us to make it this far in our IT career at the University of Cincinnati. Without their help and support, we wouldn't have had the knowledge nor the expertise to achieve what we are doing. We would also like to personally thank Professor Bogdan Vykhovanyuk for helping and guiding us to all the answers that we needed when working on our device.

Abstract

Dedicated hardware for penetration testing and digital forensics is expensive. Not everyone in the world has the necessary funds to purchase a computer device that has the necessary power or expertise to run Linux based operating systems to learn about the tools that are used in penetration test. With the advent of raspberry pie, a cheaper and more portable device can be made with just the right specifications to run Kali Linux, a popular Linux distribution that is designed for both digital forensics and penetration testing. The target client for this device is virtually anyone in the world that wants to learn more about penetration testing and using Linux-based operating systems without having to purchase expensive equipment. Schools that want to implement a security based curriculum for IT students would benefit greatly from this this since they would circumvent the need of having to purchase laptops for a classroom setting.

1 Problem Statement

1.1 Introduction

With the steady increase of cyber-attacks happening to major corporations, the need for network security has never been more relevant. Fortunately, network security professionals have a multitude of options on how to secure the company network. By setting up multiple safeguards and updating systems you can have a sense of security knowing that your network is fortified, but unless you invest in penetration testing from a third-party contractor, you can never truly know. Cost and mobility is a very important part of any company that hires a penetration testing contractor, as any IT employee knows that companies don't invest much money when it comes to protecting and improving the company network, that is until it's too late.

1.2 Description

We designed an all-in-one penetration testing toolkit for the purposes of training and educating anyone who is interested in the IT field. One of the main goals of our product is to build the device with budget priced accessories in order so that it can be sold at a budget price. We hope that by doing this we can attract the largest possible user base for the device. On top of that, we will also be creating this machine using a Raspberry Pi to ensure portability and a touchscreen will also be provided to ensure that the machine can be used as a replacement/supplementary computing device. The Raspberry Pi device will also ensure that we have just the right amount of memory to run most of the tools

provided with Kali Linux, which is our operating system of choice. We've selected Kali Linux as our choice of OS because it provides a wide range of tools for penetration testing and for network forensics, which is what our target demographics will use this machine for.

1.3 Problem

The problem that we are trying to fix is the lack of properly priced, entry-level devices that will help teach people about using network forensic tools. Our device will also be a great supplementary tool because of its portability. This is a product that security analysts can use on the move, whether between offices, between buildings or even between companies. It's compact and useful. It also has use for a teaching tool. Because of its ease of use, not only can IT professionals use it, students & educators can use it as well.

1.4 Solution

Our solution to the problem is to create a budget device that is small, portable and lightweight yet also powerful enough to run a distribution of Kali Linux. We went about doing this by simply purchasing a Raspberry Pi 3, the latest incarnation of the Raspberry Pi line of devices. Once we had the Raspberry Pi, we outfitted it with a 7-inch touch screen so that we can run the device like a miniature computer. We also purchased a power supply in order to supply it with the energy it needs to run efficiently. Once all of this was

set up and configured correctly, we installed an image of Kali Linux onto the Pi via SD Card. The SD card acts as a dedicated hard drive to our device as well as providing the device with additional virtual memory so the device runs more efficiently using more intensive programs such as nmap, a tool that scans an entire network and maps it out.

1.5 User Profile

For our project, there are two target audiences: Industry professionals, such as CIOs or network administrators, and educators & their students. Two different industries, one product. Table 1, seen below, breaks down the recommended users for our device.

1.5.1 Information Security Professionals:

Our first target audience are those who would use this device for work; for company networks and the people that keep them safe. Most system administrators should be familiar with Linux-based operating systems. Kali Linux also comes pre-loaded with all the programs a user would need for penetration testing and network security.

1.5.2 Education:

Our second target audiences are teachers and students; those who wish to use our device for educational purposes. The device will be easy to use for both students and teachers alike. While teachers will need a basic understanding of Linux and how the product functions to build and run labs for students, the device will be easy enough to use where students in IT-based curricula shouldn’t need a large amount of assistance using the device itself.

Table 1: User Profile

User Profile
Application: Kali Linux GUI
Potential Users: Information Security Professionals (CIO, Security Analyst, Network Admin, etc.) Education (Teachers, Students)
Software and Interface Experience: Experience with Linux commands and GUI-based Linux operating systems & their built-in software.
Experience with Similar Applications: Must have basic knowledge of Kali Linux operating systems and its built-in security tools.
Task Experience: Attaching plug-and-play device into a network and operating the built-in software to scan and identify vulnerabilities on the network.
Frequency of Use: Ideally every day, at minimum once a week; as deemed necessary by network administrator
Key Interface Design Requirements that the Profile Suggests: Portability to physically move the device around; ability to access and copy logged data from the device

2 Project Management

Table 2 covers our budget for our device. The pi itself along with all its components cost around $250. The cost to develop the case was estimated at $20.00, but actually costs $12.00. Labor isn't added in since we are students and work for free. Section 2.1 introduces the deliverables we wish to accomplish throughout the project

Table 2: Budget

Description	**Theoretical**	**Actual**
Raspberry Pi & Components:	$250.00	$250.00
Case:	$20.00	$12.00
Labor:	$50 X 500 Hrs = $25,000.00	$N/A

2.1 Deliverables

1. Research of vulnerability testing Open Source Software
2. Research compatibility with Raspberry Pi
3. Purchase Raspberry Pi
4. Configure OS on the machine
5. Complete finishing touches of prototype machine
6. Get together a testing plan
7. Testing the Prototype(Alpha)
8. Prototype Testing
9. Design & Print case
10. Create Image of OS for Backups
11. Implement Battery Power
12. Test updated configuration
13. Refine configuration
14. Design Expo booth and poster
15. Finalize Beta & prepare for Expo

2.2 Semester Schedules and Gantt Charts

As seen below, Table 3 illustrates our tentative semester schedule for the fall semester.

Table 3: 1st Semester Schedule

First Semester (Starting 9/19/16)	Week 1	• Research Possible vulnerability Software
	Week 2	• Determine if host machine can be a raspberry pi • If not look into Stand Alone Machine
	Week 3	• Research Equipment components • Purchasing the components
	Week 4	• Load Machine With selected software • Determine configurations for machine
	Week 5	• Implement Configurations on machines
	Week 6	• Finish up configurations
	Week 7	• Draw up Testing Plan
	Week 8-10	• Test Prototype(Alpha)

As seen below, Table 4 illustrates our tentative semester schedule for the spring semester.

Table 4: 2nd Semester Schedule

Second Semester (Starting 1/11/17)	Week 1	• Start Design Of custom built case • Cleanup Prototype
	Week 2	• Finish Design of Case • Print Case • Insert Machine in designed case
	Week 3	• Research Imaging software • Continuing Refinement of Prototype Alpha
	Week 4	• Refinements for configuration • Implement battery power
	Week 5	• Further Refinement of configurations • Update machine Image with current configurations
	Week 6	• Testing and Refinement of Beta • Prepare for final presentation
	Week 7	• Design Expo Booth (posters, interactive material) • Continue refinement and testing
	Week 8-10	• Finalize Prototype(Beta) Configurations • Finalize Image • Finalize Booth Design • Prepare for expo

Figure 1 and Figure 2, cover all the work that we plan to accomplish in two semesters organized in a Gantt chart.

Figure 1: Gantt chart 1st Semester

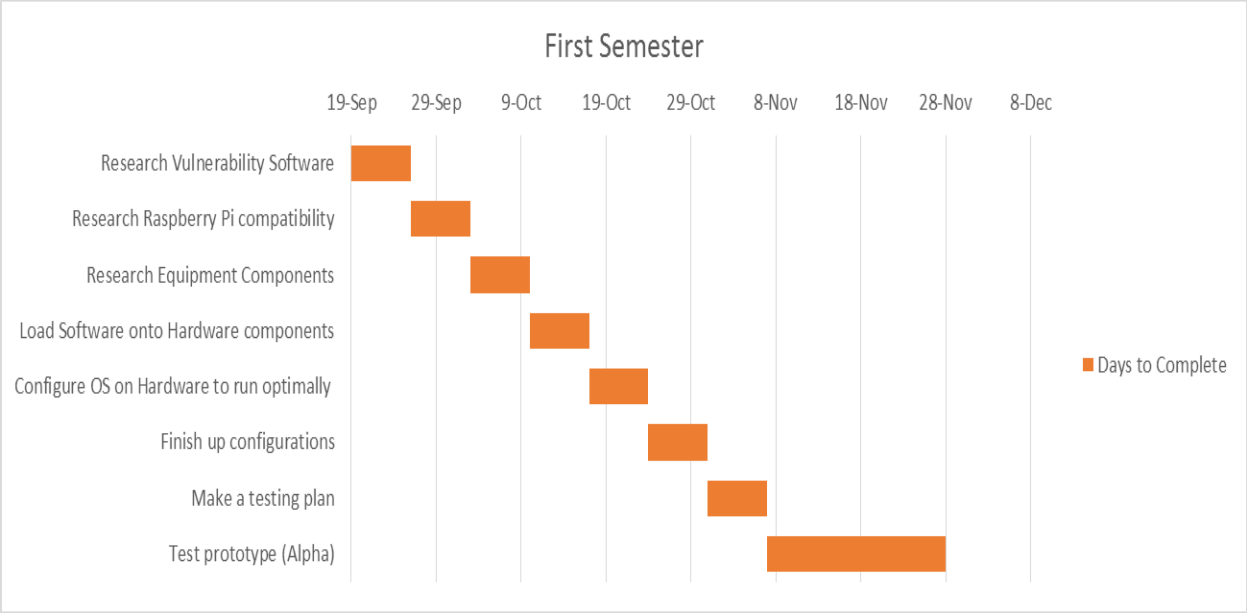
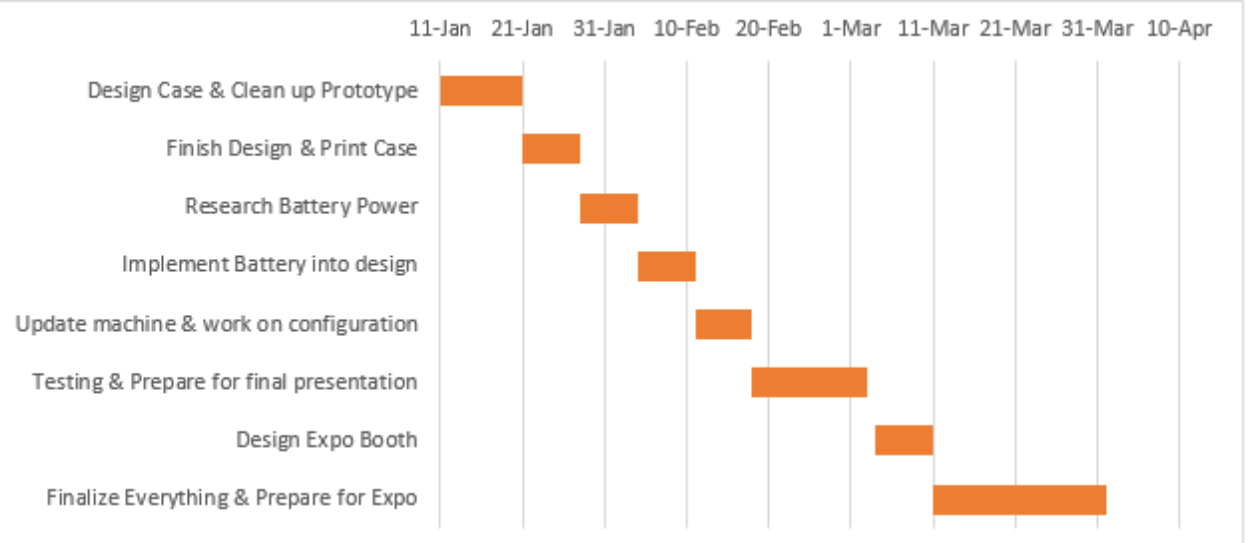


Figure 2: Gantt chart 2nd Semester



3 Technical Elements

3.1 Hardware

The main portion of the hardware will be a Raspberry Pi Model B. This model has 4 USB ports, and HDMI port, Ethernet port, Wi-Fi, Bluetooth, and a micro SD port. The system has a 1.2GHz CPU, 1 GB of memory, and no installed hard drive. The Raspberry pi will have a 32 GB micro SD card installed. A 7" touch screen designed by Element 14 will be installed into the Raspberry Pi. The device will have the option to be battery powered or plugged into the wall. A lithium-ion battery is connected to an Adafruit power controller. An on/off switch is installed into the power controller. This can be seen below in Figure 4. A case will be 3D printed to enclose all the hardware of the system.

3.2 Software

The main component of the software will be a Kali Linux Operating system and its built-in tools. The operating system will be modified to run optimally on the limited system hardware. Once the OS is completely configured imaging software will be used to make an installable image of the OS for rapid production of the product. G-parted will be installed onto the OS to partition a portion of the micro SD card into physical memory on the Raspberry Pi. Figure 3 features screens shots of the VoodooPi working within the MS framework.

Figure 3: VoodooPi MSFramework Screenshots

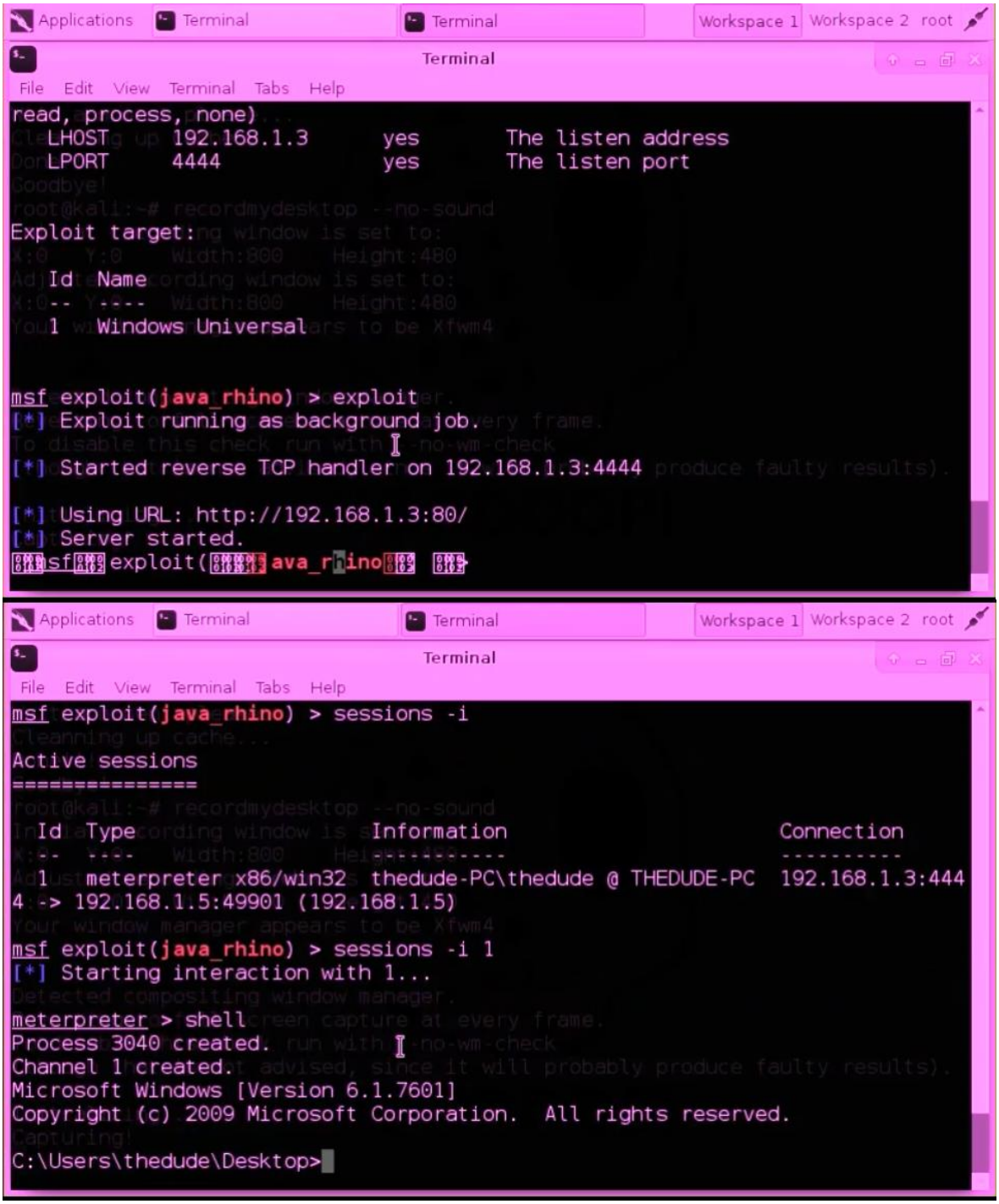
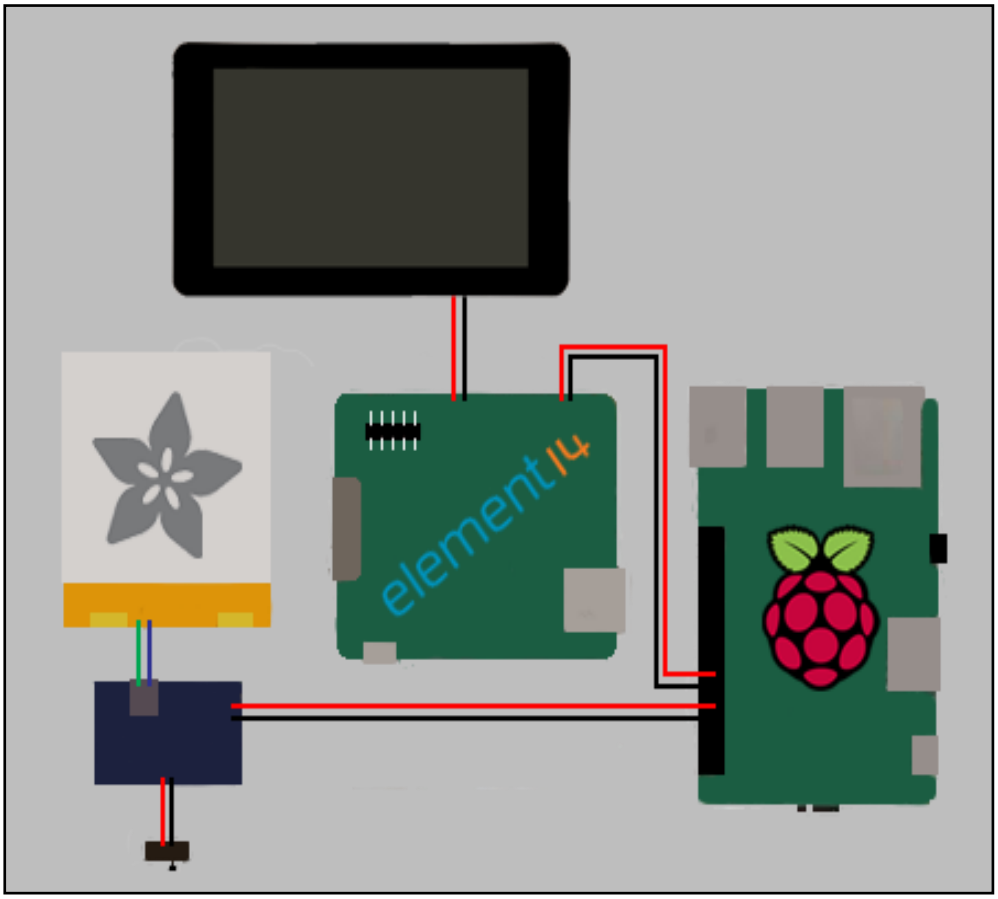


Figure 4: Hardware Diagram



4 Testing

4.1 Overview

This section will explain the testing methods utilized for our Kali Linux Voodoo Pi machine. The following should be used as a guide to verify that the machine itself is working as intended. It is recommended that students or those that have purchased the machine to mainly use this guide.

4.2 Scope

The scope of our testing is testing the hardware of the VoodooPi itself, while also testing the applications that are installed with the Kali Linux distribution. Since we are working with a minimum amount of RAM, we needed to test how well some of the more memory-intensive applications will run with the limited amount of resources that we have. We installed an application on our machine called G-Parted that solved our memory issues by creating virtual RAM. We also tested to see how efficiently the memory application function.

4.3 Objective

The objective of testing is to ensure that our machine is working properly while having the sufficient resources to run applications. Memory was our biggest issue so the major focus of this testing was on the G-Parted application itself. Application testing was done in tandem to ensure that both the applications and the memory itself is working as intended.

4.4 Entry and Exit Criteria

Entry Criteria:

- Device Set-up
- Self-testing complete
- Test environment is setup

Exit Criteria:

- All test are run
- Errors are documented and fixed

4.5 Logging Test and Reporting

If any problems or bugs were found during testing, we documented them. Once documented, our group would decide the best course of action. The nice thing about Kali Linux is that there are multiple applications that do the same thing. We could always just use an alternate application for testing in case we noticed that one of the applications isn't working correctly. We also documented any hardware issues we found.

4.6 System Testing

Our Kali Linux VoodooPi machine comes with a plethora of applications divided into different categories depending on what they need to do. We selected one application from each category and test them out one by one. We will also be testing the hardware itself by restarting the system every week to ensure that it's properly working. G-Parted will be tested simultaneously with our applications because the applications will be relying on G-Parted for additional resources.

4.7 Testing Procedures

The following are the steps we took for testing:

- Create all testing scenarios and testing cases
- Prepare a table for documenting test results
- Specify any issues within the report

We have conducted the following tests:

1. Boot Test – This test focuses on the stability of the machine when restarting.
2. Application Test – This test focuses on testing applications on the VoodooPi machine to ensure that they work. We will be testing the following applications: Wireshark, nmap, Ghost Phisher, Websploit, p0f, Armitage, and Termineter.
3. Memory Test – This test focuses on G-Parted and how well it works in giving applications additional memory for their processes.
4. Battery Life Test – We tested the battery life of our VoodooPi machine without any applications running and then another test for when applications are running. We want to know want to know what the average battery life of our machine will be.

Table 5: Pass/Fail Conditions

BOOT TEST

- 5 simultaneous standard boot ups/shutdowns = PASS

TEST DATE	TESTER		PASS	FAIL
4/10/2017	Brett Copeland		X	
4/7/2017	Eder Aguilar		X	
4/6/2017	Jonathan Coleman		X	

APPLICATION TEST

- Proper 5 minute functionality of application = PASS

TEST DATE	TESTER	APP	PASS	FAIL
4/10/2017	Brett Copeland	WIRESHARK	X	
3/31/2017	Eder Aguilar	NMAP	X	
3/31/2017	Jonathan Coleman	GHOST PHISHER	x	
3/31/2017	Eder Aguilar	WEBSPLOIT	x	
3/31/2017	Eder Aguilar	P0F	x	
3/31/2017	Jonathan Coleman	MSF	x	
4/7/2017	Brett Copeland	TERMINETER	x	
4/7/2017	Brett Copeland	WIRESHARK	x	
4/7/2017	Eder Aguilar	NMAP	x	
4/7/2017	Eder Aguilar	GHOST PHISHER	x	
4/7/2017	Jonathan Coleman	WEBSPLOIT	x	
4/7/2017	Jonathan Coleman	P0F	x	
4/7/2017	Eder Aguilar	MSF	x	
4/7/2017	Eder Aguilar	TERMINETER	x	

MEMORY TEST (Internal + GParted memory)

- 100% pass of Kali Linux-Raspberry Pi built-in memory test = PASS

TEST DATE	TESTER		PASS	FAIL
4/10/2017	Brett Copeland		X	
4/7/2017	Eder Aguilar		X	
4/6/2017	Jonathan Coleman		X	

BATTERY LIFE TEST

- 2+ hour battery life (passive, no app running); 1+ hour battery life (active, app running) = PASS

TEST DATE	TESTER		PASS	FAIL
4/10/2017	Brett Copeland		X	
4/7/2017	Eder Aguilar		X	
4/6/2017	Jonathan Coleman		X	

5 Conclusion

At the end of the day, we hope to make a useful device that can pull its own weight when it comes to penetration testing and for teaching and introducing people into the field of IT networking and forensics. The only way to improve your skills in IT is to actively participate and engage in learning the ins and outs of networks and how to go about securing them. With our device, we hope that people will learn more about networks and how vulnerable they really are and that once this is realized for them to better secure them using their knowledge of penetration testing. The final working model performs as expected.

6 References

Novaspirit Tech. “Kali Linux on Raspberry Pi 3”. Filmed [April 2016]. YouTube video, 08:11. Posted [April 2016]. https://www.youtube.com/watch?v=6xXnUGR_e4E

Verkamp, Brian. Interview with Brett Copeland. Personal interview. Cincinnati, September 6, 2016

Vykhovanyuk, Bogdan. Interview with Brett Copeland. Phone interview. Cincinnati, September 14, 2016.

Vykhovanyuk, Bogdan. Interview with Brett Copeland. Phone interview. Cincinnati, October 24, 2016.