ASEE's 123rd Annual • Conference & Exposition • New Orleans, LA • June 26-29, 2016

New Orleans Jazzed about Engineering Education

Paper ID #14777

Wireless Network Security Using Raspberry Pi

Dr. Chafic BouSaba, Guilford College

* Joined Guilford College in January 2008 * Serves as Assistant Professor in the Computing Technology and information Systems.

Ms. Tiera Kazar, Guilford College

I am a current student at Guilford College in the Computing Technology & Information Systems department. I am working on a Capstone project that will be submitted to the ASEE. The project focuses on Wireless Network Security using a Raspberry Pi.

Dr. Will C. Pizio, Guilford College

I am currently an Associate Professor of Justice and Policy Studies at Guilford College in Greensboro, NC. I have a Master's and PhD in Criminal Justice from the University at Albany and a Master's in Cyber Security from Utica College. I currently teach both criminal justice and cyber security courses at Guilford.

Wireless Network Security using Raspberry Pi

Abstract

This educational project uses a second generation Raspberry Pi that runs multiple Open Source software packages, to perform network penetration testing and to analyze the results. Implementing this project provides undergraduate students with practical hands-on experience and explains advanced concepts in computer hardware, operating systems, and network security. This project is fairly affordable, highly portable, easily deployable, alarmingly impactful, and highly rewarding. It also demonstrates the need for secure wireless networks against various attacks such as Man-in-the-Middle (MitM). This paper illustrates step-by-step instructions to assemble and integrate the project's hardware parts, to download and configure software packages, and to perform customized network operations such as packet sniffing and filtering. Kali Linux for Raspberry Pi is the chosen operating system due to its extensive and powerful collection of White Hat hacking tools such as Wireshark (Network Protocol Analyzer), Nmap (Network Mapper), and SSLstrip (Secure Sockets Layer strip). Additional wireless network auditing tools are used from the robust FruityWifi package. Wireshark filters, captures, and analyzes network packets, such as hypertext transfer protocol secure (HTTPS) requests. SSLstrip strips the secure connection and convert HTTPS to hypertext transfer protocol (HTTP), gaining access to sensitive information such as login credentials. This simple to implement yet powerful project, demonstrates the ease of hiding and discreetly deploying a Raspberry Pi on a vulnerable wireless network to sniff network packets that is considered protected behind firewalls, while maintaining a safe distance and anonymity from the target.

Introduction

The Raspberry Pi, see figure 1, is a miniature and affordable computer created by the Raspberry Pi Foundation, an educational charity based in the United Kingdom with a focus on encouraging the use of Raspberry Pi in classrooms to further the educational experience in computer sciences[15]. The Raspberry Pi offers an inexpensive option for students to experiment with various aspects of technology. A variety of Linux-based OS's can be used with the Raspberry Pi, but the device typically comes pre-loaded with the Raspbian OS, free software supplied by the Raspberry Pi foundation. The Pi can be accessed remotely or can be connected to any device that supports an HDMI interface.

The overall goal of this project is to experience aspects of information security using the Raspberry Pi and the Kali Linux OS. This project will consist of constructing a hacking arsenal for penetration testing, using open source software. The Raspberry Pi 2 is an inexpensive device that can be used for a variety of projects including, but not limited to, home security systems, temperature and humidity monitors, and video game consoles. Scholarly resources are limited when it comes to the Raspberry Pi, which explains why the majority of sources used for this particular project consisted of blogs, forums, and wikis. One book, which delves into significant detail on the use of Raspberry Pi with Kali Linux specifically, is called *Penetration Testing with Raspberry Pi*, which was released in 2015 by Aamir Lakhani and Joseph Muniz. Penetration testing is a significant concept on individual, organizational, and institutional levels, because penetration testing identifies vulnerabilities and security weaknesses on a network or web applications. The Raspberry Pi, even with its small size, has a variety of ports for input and output and has strong penetration testing capabilities, especially when utilizing the Kali Linux OS. According to Lakhani and Muniz, “Kali Linux is one of the most popular penetration testing platforms used by security professionals, hackers, and researchers around the world, and risk testing[9].” This project focuses on exploiting vulnerabilities in web applications and using those vulnerabilities for privilege escalation. The easily obtained open source software tools are used to gain access to a user’s social media account login information[10].

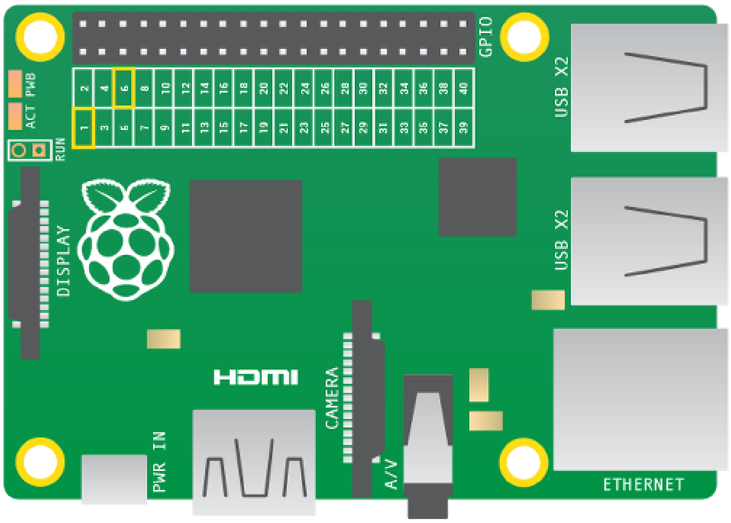

Figure 1: Diagram of Raspberry Pi 2, Model B

The first part of the paper elaborates on the functionality of the Raspberry Pi device, including hardware and software components and their modifications, and the sequence in which the tasks will be completed. The second part demonstrates the steps for the project to be successfully reproduced. The final part discusses the results of the project, how this project contributes to furthering the educational experience of future students of technology, and closes with potential modifications for future projects.

The Raspberry Pi can be purchased as part of a kit or individually. For this project, a kit was purchased that included the Raspberry Pi itself, a case, Micro SD card, SD Card Adapter, power supply, HDMI cable, WiFi dongle, 2 heat sinks, and a quick start guide totaling approximately $80+tax. The model of Raspberry Pi used for this project is the Raspberry Pi 2 Model B, which “replaced the original Raspberry Pi 1 Model B+ in February 2015[16].” Shared features include four USB ports, 40 general-purpose input/output (GPIO) pins, full High-Definition Multimedia Interface (HDMI) video output, Ethernet port, combined 3.5mm audio jack and composite video, a camera serial interface (CSI), display interface (DSI), Micro SD card slot, and VideoCore IV

3D graphics core. Raspberry Pi 1 Model B+ has a Broadcom BCM2835 700 MHz ARM11 processor, whereas the Raspberry Pi 2 Model B has an updated Broadcom BCM2836 900 MHz quad-core ARM7 processor, which boosts performance approximately six times its former counterpart. Memory for the Raspberry Pi 2 Model B has increased to 1GB LPDDR2 SDRAM, two times the memory of the Raspberry Pi 1 Model B+[16].

To begin the project, all necessary hardware and software components were obtained. Then the Kali Linux OS will be installed and configured to suit the needs of this project. System software will be updated to the most recent versions. Additional tools will be installed. The default password will be changed for security purposes. An Ad-Hoc WiFi network will be created on the Raspberry Pi using a static IP address, so that the Raspberry Pi can be accessed at a later time, bypassing the need to determine the new IP address the Raspberry Pi would obtain when reconnected to a network, which is due to dynamic host configuration protocol (DHCP) [4].

There are two methods of obtaining login credentials discussed in this paper. The first method focuses on the network analyzing capabilities of Wireshark[25]. Wireshark is one of the open-source software's used in this project, and is a valuable tool for understanding both White Hat and Black Hat hacking abilities. Wireshark captures packets with plain-text login credentials for seemingly encrypted web sites. This project provides a brief introduction on the usefulness of Wireshark as well as bring awareness to the vulnerabilities of some web sites. The second method involves SSLstrip, which was created by Moxie Marlinspike. SSLstrip is designed to hijack an SSL session and replace the SSL encryption with plain-text, unknown to the user[7]. By viewing the sslstrip.log file, a user's login credentials are listed. Both methods are simple to implement and reproduce. No purchases are required for any of the software used, which makes this an affordable project for any student interested in experimenting with the Raspberry Pi and wireless network security. The details of each method will be explained later in greater detail.

Methods

The first step consists of assembling the 16x2 Character LCD and Keypad Kit. The Raspberry Pi requires no physical setup, other than plugging in the HDMI cable, power supply, WiFi adapter, mouse, and keyboard. Adafruit offers a thorough tutorial on constructing the LCD kit[1]. Table 1 lists the necessary software to complete this project. Table 2 lists necessary hardware, temporary hardware, and tools needed for setup and construction. Figure 2 illustrates the major steps for the project, such as hardware construction and software configuration.

The SD card should be formatted for FAT32 (File Allocation Table) file system in preparation for software configuration. The image for the latest distribution of Kali Linux should be written on it using SD Association's formatting tool, which is available for Windows or Mac. Insert the Micro SD card in the Raspberry Pi 2. Before plugging in the power supply, the HDMI cable, keyboard, mouse, and WiFi adapter should be connected. Once power is connected, the Raspberry will boot directly to the Kali Linux desktop. From here, we can open a terminal, granting access to the command-line.

Table 1: Required Software

Software	Description	Version	Logo
Kali Linux	An open source, Debian-based Linux distribution used in security auditing and penetration testing. Kali contains hundreds of tools to aid in various information security tasks[10].	2.0.1	KALI LINUX
Wireshark	An open source network protocol analyzer[25].	1.12.7	WIRESHARK
FruityWifi	An open source tool to audit wireless networks[3].	2.2	Fruity WiFi Wireless Network Auditing Tool WWW.FRUITYWIFI.COM
Nmap	An open source utility for network discovery and security auditing[11].	6.49BETA2	NMAP
TCPdump	An open source, command-line packet analyzer[22].	4.7.4	TCPDUMP
SSLstrip	An open source tool that hijacks HTTPS traffic, redirects, and converts to HTTP traffic[7].	0.9	
Dsniff	An open source package that includes a collection of tools for network auditing & penetration testing[20].	2.3	
ARPspoof	Distributed in the Dsniff package; Redirects packets from a target host intended for another host[20].	2.3	
Fierce	An open source domain scanner that will query a list of qualified domain names to a target DNS server within a specified domain[6].	v2	

Table 2: Hardware & Tools

Required Hardware:	*Temporary Hardware (needed for setup):*	*Required tools (needed for construction):*
Micro USB Cable Raspberry Pi 2 Model B 16x2 Character LCD & Keypad kit 2000mA Micro USB Power Supply SD Micro SD & adapter card with 8GB storage capacity Edimax EW-7811 Un 150 Mbps 11n Wifi – USB Adapter	HDMI cable Corded Mouse Corded Keyboard HDMI compatible TV/Monitor Laptop (with wireless capabilities)	Soldering iron, solder Wire cutters

A standard OS for Raspberry Pi beginners is Raspbian. Raspbian comes equipped with a tool called Raspi-Config that allows the user to expand the file system with ease[17]. Expanding the file system allows the OS to use the entire SD card, instead of a small portion. The Raspi-Config tool is not available for the Kali Linux distribution, so another means of expanding the file system had to be found. An online blog explained how to expand the root partition using a script available online by typing ‘wget’ in the command-line. Simply make the script executable, then actually execute the script, reboot, and the root partition has been expanded[24].

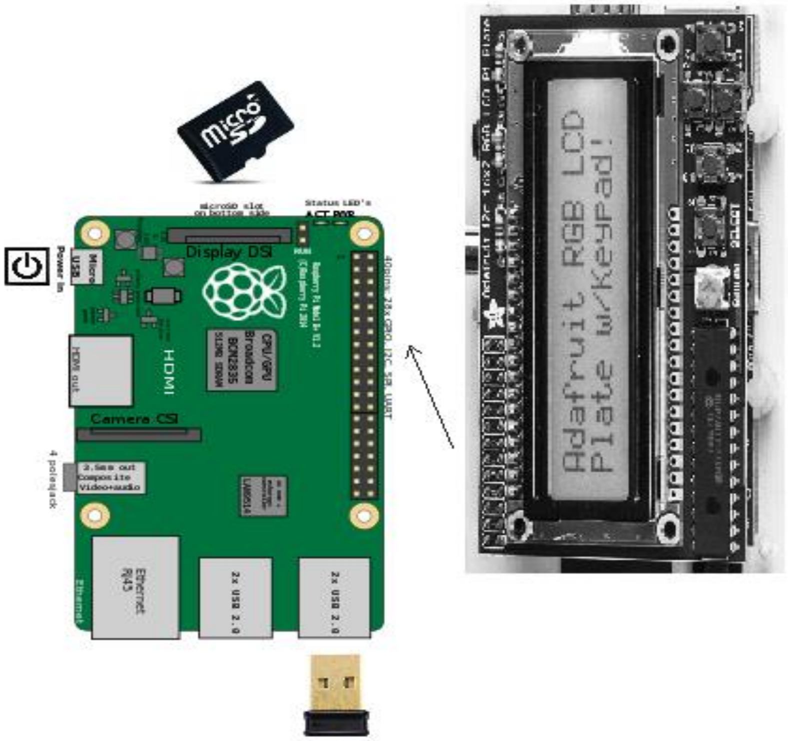
microSD
microSD slot on bottom side
Status LED's ACT PWR
Micro USB Power in
Display DSI
HDMI
HDMI out
CPU/GPU Broadcom BCM2835 512MB SDRAM
40pins 28xGPIO, I2C, SPI, UART
Camera CSI
4 pole jack
3.5mm out Composite Video+audio
Ethernet RJ45
2x USB 2.0
2x USB 2.0
Adafruit RGB LCD Plate w/Keypad!

Figure 2: System Diagram for all hardware components

The default password of ‘toor’ will be changed for security purposes using `passwd`. The hostname should also be changed to something that does not easily identify the system. Next, the default host keys will be removed: `rm /etc/ssh/ssh_host_*`, and new set of public and private key pairs are created: `dpkg-reconfigure openssh-server`. The Raspberry Pi should be updated using the standard command for Debian Linux: `apt-get update && apt-get upgrade –y`. Once the Raspberry Pi is updated, we additional programs necessary to complete the project, such as SSLstrip, dnsiff, fierce, fruitywifi, and tcpdump are installed. In order to access the Raspberry Pi at any time, a static IP address must be set. This can be done by typing and accessing the file: `nano /etc/network/interfaces`. The following lines should be added to the bottom of the file:

```
## AD-HOC WIFI
auto wlan0
iface wlan0 inet static
     address 192.168.1.15
     netmask 255.255.255.0
     wireless-mode ad-hoc
     wireless-essid KALIPI
```

Save the settings and restart the networking service. To verify the settings, type `ifconfig wlan0` or `iwconfig`. Now the Raspberry Pi is prepared to execute the attacks[4].

Python Developer and GPIO should now be installed. This particular process proved challenging because there was limited documentation on using the Raspberry Pi's GPIO library with the Kali Linux operating system. The standard installation commands were unsuccessful, so the following code was used to complete a successful installation of RPi.GPIO library.

```
sudo apt-get update
sudo apt-get install build-essential
export ARCH=arm
export CROSS_COMPILE=/usr/bin/

apt-get update
apt-get install -y python-dev
apt-get install -y python-pip
easy_install -b /home/osmc -U distribute
pip install rpi.gpio[12]
```

Once the GPIO library is installed, the i2c bus can be configured. To do this, kernel support must be installed. First, enter:

```
sudo apt-get install python-smbus
sudo apt-get install i2c-tools
```

The tools may already be installed, so the Raspberry Pi will state that the tool is the newest version. To test i2c, enter: `sudo i2cdetect –y 1`, showing that two i2c addresses are in use[8]. After the GPIO library is installed and i2c tools are configured, clone into Adafruit's Python code repository and test the python script for the LCD to make sure it is functioning properly.

The first method to carry out the attack uses Wireshark to capture the packets. Both methods consist of similar steps, such as enabling IP forwarding, discovering the default gateway IP address, locating the target IP address, and inserting the Raspberry Pi as MitM device. The purpose of IP forwarding is to ensure that the packets arrive at their destination, otherwise this will create a Denial of Service, which might alert the user to the attack. To enable IP forwarding, enter: `echo 1 > /proc/sys/net/ipv4/ip_forward`. To test that the commands were executed correctly, enter: `cat /proc/sys/net/ipv4/ip_forward`. The command should return a value of 1. Next step is to find the current default gateway. To do so, enter: `netstat –nr`. The default gateway will be used in the ARPspoofing attack, as well as the target IP address. To find the target IP address, Nmap, an open source utility, will be used. Nmap has much stealthier capabilities than what are used in this particular project, so using default settings of the program could alert a Security Administrator to your presence. The arguments used for this project will consist of "R" for reverse DNS lookup and "sn" to prevent port scanning. The command used to find the default gateway also reveals information about which class is associated with the network. In this case it is Class C, with the mask being

255.255.255.0. The command used to find the target IP address will be: `nmap –Rsn 192.168.1.0/24`. This will reveal all hosts on the local network. Find the target IP address that is of interest, and this will be used in the ARPspoofing attack. To issue the ARP cache poisoning command, use this syntax: `arpspoof –i interface –t target IP -r gateway IP`. For this project, the command will appear as `arpspoof –i wlan0 –t 192.168.1.1 –r 192.168.1.0`. Once the ARPspoof command is executed, the next step is to open Wireshark on the Raspberry Pi and begin the packet capture[4].

Before initializing the packet capture with Wireshark, it is essential to run a TCPdump command that will enable the packets to be saved to a text file that can eventually be sent to the LCD screen for display[21]. To begin the packet capture on Wireshark, select the 'eth0' interface, which is the built-in network card on the Raspberry Pi. Click start to begin capturing data and click stop once enough data is captured. At this point, the user will be accessing an encrypted website while the packet capture is occurring. Once the packet capture has been stopped, we can filter the captured data by inputting `ip.src == 192.168.1.1 and http.request.full_uri contains login` in the Filter box on Wireshark. The IP address entered is the target's IP address. The packet that will provide the login information has the html 'POST.' Right-click on the packet and select 'Follow TCP Stream.' Locate the login name and password in the raw data[4].

To perform the same login and password capture with SSLstrip, follow the same steps regarding enabling IP forwarding, discovering the default gateway IP addressing, locating the target IP address, and initiating the ARP cache poisoning commands. An additional step is included before finding the default gateway. Packets that are going out on port 80 need to be redirected to port 8080, which will route outgoing connections from SSLstrip to port 8080. To execute this redirection, type: `ip tables –t nat –A PREROUTING –p –tcp --destination-port 80 –j REDIRECT --to-port 8080.` Issue the TCPdump command that was mentioned previously. Once those commands are executed, start a new SSH session with the Raspberry Pi and execute the SSLstrip command to monitor for data being sent out on port 8080 using this syntax: `sslstrip –l 8080`. While SSLstrip is running, an encrypted webpage is being accessed on the target computer, such as Facebook. To stop SSLstrip, hit `Ctrl + C`[4]. To see the results of the attack, type: `tail –n 50 –f sslstrip.log` in another terminal window[9]. With the following results, the login information should be revealed, allowing access to the user's account.

Results and Discussion

This project was done to complete a Capstone requirement in order to graduate. The student worked on the project individually with assistance from the professor, whenever necessary. The project could potentially be a group project for two or more students, allowing each student to focus on a particular aspect of the project, such as hardware or software. Approximately, the overall time to complete configuration and construction of the project, assuming no prior experience and proper guidance, is 20 to 25 hours. If no obstacles occurred and the student has experience with all components, the project could take approximately 15 hours.

Challenges, Conclusion, and Future Work

This project included a number of challenges, resulting in a partial completion of the project. Most of the documentation accessed online was missing configuration steps and not all potential issues were addressed. Both, *A Penetration Test: Raspberry Pi and Kali Linux* and *Penetration Testing with Raspberry Pi*, provided detailed explanations on each step of the project and were followed accordingly, but this still did not result in a total successful project. The packets that were intercepted when running both Wireshark and SSLstrip were not the packets needed in order to view the user's login information. The commands were executed according to the documentation, but the desired results did not come to fruition. One possible explanation is HTTP Strict Transport Security (HSTS), which was proposed in 2009 when the creator of SSLstrip, Moxie Marlinspike, demonstrated how a secure connection with HTTPS could be interrupted and redirected. "When a browser knows that a domain has enabled HSTS, it does two things: Always uses an https:// connection, even when clicking on an http:// link or after typing a domain into the location bar without specifying a protocol; Removes the ability for users to click through warnings about invalid certificates[23]." Multiple browsers were tested in this project, including Internet Explorer, Google Chrome, and Mozilla Firefox, as well as multiple websites with varying accounts, including Yahoo Mail, Facebook, and Google Mail. No combination of websites and browsers intercepted the packets needed to access the necessary login information.

This project enabled the student to expand knowledge on networking concepts and the use of various open-source tools to complement networking concepts. Wireshark, in particular, is a useful tool for understanding the different protocols used in the transport of packets across a network. Despite the correct packets not being captured, analyzing the packets that were captured developed an understanding of intercepting the desired IP address. The use of Nmap was a particularly useful for understanding how to analyze IPs on a specific subnet. Wireless and wired networking was tested in an attempt to determine why the correct packets were not being captured. One possibility for future testing is using a different tool to crack a wireless network's password, instead of using an unencrypted wireless network. The research on HSTS provided a possibility for the unsuccessful completion of intercepting password login information via SSLstrip. Since SSLstrip's introduction, websites have become more aware of the vulnerabilities. More research can be done to find a means of bypassing HSTS. The Kali Linux operating system offers more than 600 penetration testing tools, and this project only scratched the surface of the capabilities of the Kali Linux operating system. Kali Linux has tools that focus on information gathering, vulnerability analysis, wireless attacks, web applications, exploitation tools, forensics tools, stress testing, sniffing and spoofing, password attacks, maintaining access, reverse engineering, reporting tools, and hardware hacking. The utilization of other tools offered by the Kali Linux operating system could assist in the successful completion of this project.

The next challenge involved the LCD screen. Installing the GPIO library, which enables the Raspberry Pi to control the GPIO pins, and in turn the LCD screen, was a challenge in itself. The next step involved downloading the i2c tools or updating the tools to the most recent version. These steps were completed successfully and without complication, but when the LCD screen was finally attached to the Raspberry Pi, the device appeared to shutdown with no lights indicating that the operating system was functioning. This could be due the insufficient power supply, an unforeseen problem due to the student's inexperience. The LCD screen was left on the Raspberry Pi as the device was rebooted. The student attempted to remote back into the device to see if it was indeed running. This was unsuccessful. The next attempt to troubleshoot was to remove the LCD screen, and trying booting the Pi while connected to a monitor. After the boot finished and the login screen came up, an error was repeatedly issued on the screen. After researching the error, it appears that the SD card may have been corrupted from attempting to boot the Raspberry Pi with the LCD screen attached.

Future work would include continuing to research this project and discover what challenges could have been overcome and to find a way to bypass the new HSTS standard in order to capture the packets. Utilizing other tools offered by the Kali Linux operating systems could improve the chances of intercepting the correct packets. Obtaining a different power supply would allow the LCD screen to function properly with the Raspberry Pi. To take this project a step further would be to test the Raspberry Pi's penetration testing capabilities against a network with a stronger firewall. Kali Linux has the ability to gain access to seemingly secure networks. The project, even if partially successful, would be a great learning experience for any student or person interested in furthering their knowledge in computer science or hardware construction.

Bibliography

[1] Adafruit. (n.d.). Adafruit 16x2 Character LCD + Keypad for Raspberry Pi: Overview. [Online]. Available: https://learn.adafruit.com/adafruit-16x2-character-lcd-plus-keypad-for-raspberry-pi?view=all. Accessed September 10, 2015.

[2] Edimax Wifi Adapter. (n.d.). [Online]. Available: http://www.nerdgenie.com/wp-content/uploads/2015/11/Edimax-EW-7811Un-150Mbps-11n-Wi-Fi-USB-Adapter-Nano-Size-Lets-You-Plug-it-and-Forget-it-Ideal-for-Raspberry-Pi-Supports-Windows-Mac-OS-Linux-0-0.jpg. Accessed November 19, 2015.

[3] Github. (July 8). FruityWifi. [Online]. Available: https://github.com/xtr4nge/FruityWifi/wiki. Accessed: October 27, 2015.

[4] Hansen, B. (2014, March 10). A Penetration Test: Raspberry Pi & Kali Linux. [Online]. Available: http://bahansen.info/. Accessed August 18, 2015.

[5] Hawkins, Matt. (2012, July 27). 16x2 LCD Module Control Using Python. [Online]. Available: http://www.raspberrypi-spy.co.uk/2012/07/16x2-lcd-module-control-using-python/. Accessed September 20, 2015.

[6] Kali Tools. (2014, February 18). Fierce. [Online]. Available: http://tools.kali.org/information-gathering/fierce. Accessed August 18, 2015.

[7] Marlinspike, M. (2009, February 21). Software: SSLstrip. [Online]. Available: http://www.thoughtcrime.org/software/sslstrip/. Accessed August 18, 2015.

[8] Monk, Simon. (2015, May 4). Configuring I2C. [Online]. Available: https://learn.adafruit.com/adafruits-raspberry-pi-lesson-4-gpio-setup/configuring-i2c. Accessed November 19, 2015.

[9] Muniz, J., & Lakhani, A. (2015). Penetrating Testing with Raspberry Pi. GBR: Packt Publishing Ltd. [Online]. Available: http://file.allitebooks.com/20150909/Penetration%20Testing%20with%20Raspberry%20Pi.pdf. Accessed October 15, 2015.

[10] Muniz, J., & Lakhani, A. (2013). Web Penetration Testing with Kali Linux. Birmingham, GBR: Packt Publishing Ltd. [Online]. Available: http://www.ebrary.com. Accessed September 10, 2015.

[11] Nmap Security Scanner. (n.d.). Introduction. [Online]. Available: https://nmap.org/. Accessed September 20, 2015.

[12] OSMC Forums. (June 2015). GPIO Control. [Online]. Available: https://discourse.osmc.tv/t/gpio-control-need-some-help/3246/3. Accessed December 10, 2015.

[13] Power. (n.d.) [Online]. Available: http://rlv.zcache.com/power_button_symbol_jewelry_box-rc527500a3a704059afaa1edd129782f4_agl0h_8byvr_324.jpg. Accessed November 19, 2015.

[14] Raspberry Pi Diagram. (n.d.). [Online]. Available: https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=0CAcQjRxqFQoTCO2xoan7ssgCFUGNDQod140FYQ&url=https%3A%2F%2Fwww.raspberrypi.org%2Flearning%2Frobot-antenna%2Fworksheet%2F&psig=AFQjCNG9MWf-2bzcSvvTmdadxa7t1KjZOg&ust=1444396721593289. Accessed: September 22, 2015.

[15] Raspberry Pi Foundation. (n.d.). About Us. [Online]. Available: https://www.raspberrypi.org/about/. Accessed September 20, 2015.

[16] Raspberry Pi Foundation. (n.d.). Raspberry Pi 2 Model B. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-2-model-b/. Accessed September 20, 2015.

[17] Raspberry Pi Foundation (n.d.). Raspi-Config. [Online]. Available: https://www.raspberrypi.org/documentation/configuration/raspi-config.md. Accessed November 19, 2015.

[18] Raspberry Pi Forums. (2013, May 22). Adafruit 16x2 RGB LCD and Read a Text File. [Online]. Available: https://www.raspberrypi.org/forums/viewtopic.php?&t=44617. Accessed November 19, 2015.

[19] Raspberry Pi SD Card. (n.d.). [Online]. Available: http://product-image.bdstall.com/giant_11203.jpg. Accessed November 19, 2015.

[20] Song, D. (n.d.). Dsniff. [Online]. Available: http://www.monkey.org/~dugsong/dsniff/. Accessed: August 18, 2015.

[21] TCPdump. (2015, September 17). General Commands Manual. [Online]. Available: http://www.tcpdump.org/manpages/tcpdump.1.txt. Accessed September 20, 2015.

[22] TCPdump & Libpcap. (2015). Latest Release. [Online]. Available: http://www.tcpdump.org/. Accessed August 18, 2015.

[23] United States Chief Information Officer Council. (2015). HTTP Strict Transport Security. [Online]. Available: https://https.cio.gov/hsts/. Accessed December 20, 2015.

[24] Ventura, Luis. (2015, May 4). Expand the Root Partition in Kali Linux for the Raspberry Pi. [Online]. Available: https://linhost.info/2015/05/expand-the-root-partition-in-kali-linux-for-the-raspberry-pi/. Accessed October 30, 2015.

[25] Wireshark. (n.d.). Wireshark Documentation. [Online]. Available: https://www.wireshark.org/docs/. Accessed: August 18, 2015.

[26] Wooley, J. (2013, February 21). Packet Sniffing using the Raspberry Pi. [Online]. Available: http://jamesdotcom.com/?p=400. Accessed August 20, 2015.