Wireless Network Penetration Testing Using Kali Linux on BeagleBone Black

Aparicio Carranza, PhD[1] and Casimer DeCusatis, PhD[2]

[1]The New York City College of Technology – CUNY, USA, acarranza@citytech.cuny.edu

[2]Marist College, USA, casimer.decusatis@marist.edu

Abstract – The development of powerful, low cost mobile compute platforms has enabled a host of new penetration testing applications. We investigate the Kali Linux operating system and its embedded security tools, hosted on the BeagleBone Black (BBB) hardware platform. This combination creates a powerful, portable ethical hacking tool. Specific tools offered by Kali Linux such as Ettercap-Graphical, Wireshark, Aircrack-ng, and ARP poison are used to perform in-depth, practical penetration testing. Experimental results include a demonstration of how Kali Linux on the BBB can be used to perpetuate a denial of service attack by de-authenticating wireless access from another host. Further, we demonstrate the collection of valuable data including user IDs, usernames, and passwords obtained from a reconnaissance attack.

Keywords-- Aircrack-ng, Beagle Bone Black (BBB), Ettercap-Graphical, Kali Linux, Wireshark, Vertical Scanning, Horizontal Scanning

Digital Object Identifier
(DOI):http://dx.doi.org/10.18687/LACCEI2016.1.1.095
ISBN: 978-0-9822896-9-3
ISSN: 2414-6390

Wireless Network Penetration Testing Using Kali Linux on BeagleBone Black

Aparicio Carranza, PhD[1] and Casimer DeCusatis, PhD[2]
[1]*The New York City College of Technology – CUNY, USA, acarranza@citytech.cuny.edu*
[2]*Marist College, USA, casimer.decusatis@marist.edu*

Abstract – The development of powerful, low cost mobile compute platforms has enabled a host of new penetration testing applications. We investigate the Kali Linux operating system and its embedded security tools, hosted on the BeagleBone Black (BBB) hardware platform. This combination creates a powerful, portable ethical hacking tool. Specific tools offered by Kali Linux such as Ettercap-Graphical, Wireshark, Aircrack-ng, and ARP poison are used to perform in-depth, practical penetration testing. Experimental results include a demonstration of how Kali Linux on the BBB can be used to perpetuate a denial of service attack by de-authenticating wireless access from another host. Further, we demonstrate the collection of valuable data including user IDs, usernames, and passwords obtained from a reconnaissance attack.

Keywords-- ***Aircrack-ng, Beagle Bone Black (BBB), Ettercap-Graphical, Kali Linux, Wireshark, Vertical Scanning, Horizontal Scanning***

I. Introduction

Cybersecurity continues to be a leading concern among large enterprises, service providers, and information technology (IT) organizations. According to the 2015 Verizon data breach report [1], network breaches continue to grow in both number and sophistication, with an annual cost easily exceeding several billion dollars. The increased use of wireless mobile devices (including smart phones, laptops, and tablets) has led to a growing need for better wireless network security and penetration testing methods. Recently, leading penetration suites such as the Debian-based Kali Linux operating system have become available on a variety of mobile hardware platforms. This makes it possible, for the first time, to conduct penetration testing from a portable device.

In this paper, we consider two basic types of cyberattacks, namely reconnaissance and denial of service (DoS). A reconnaissance attack is characterized by gathering data and looking for vulnerabilities within a network or host (i.e. packet sniffing and port scanning). A DoS attack affects the system's availability by flooding the system with traffic or resource requests. Vertical scanning is choosing a specific target from a network to attack, which is the main method for each of the two attacks performed in this paper. These attacks are facilitated by the Debian-based Kali Linux 1.0.6 operating system and its associated tools. It can be booted from a portable storage device such as a USB, a virtual machine such as VMware Workstation, and most importantly for our purposes it can be loaded onto a mobile microprocessor. We have successfully installed these tools on a portable hardware platform, the BeagleBone Black (BBB) [2] with an optional long range wireless adapter, making it possible to conduct penetration testing at any desired physical location and investigate in situ wireless network environments.

The remainder of this paper is organized as follows. First, we review the BBB hardware platform, describe the modifications required to support Kali Linux, and review the relevant Kali Linux penetration testing tools. We then present experimental results demonstrating a successful wireless DoS attack including ARP cache poisoning, and a man-in-the middle (MITM) reconnaissance attack on a wireless network. In conclusion, we discuss mitigation techniques and next steps for this research.

II. Hardware and Software Environment

The BeagleBone Black, illustrated in Figure 1, [2] is a low-cost, community-supported ARM-based development platform aimed at developers and hobbyists. The BeagleBone Black runs a 1GHz Cortex-A8 CPU and includes hardware-based floating point and 3D acceleration. While much lower-powered than a desktop or laptop system, its affordability and portability makes it an excellent option for a light weight Linux system.

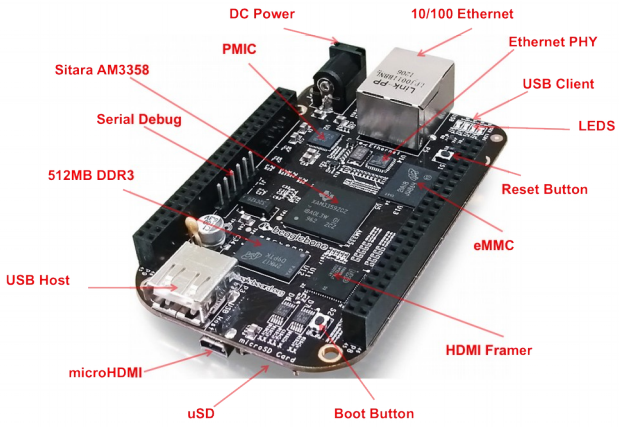

Figure 1 – BeagleBone Black micro-computer

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2016.1.1.095
ISBN: 978-0-9822896-9-3
ISSN: 2414-6390

The BeagleBone Black provides a micro-SD card slot for mass storage, and if that device is bootable, the BBB will use it in preference to the board's "burned-in" Angstrom or Debian operating system. By default, the Kali Linux BeagleBone Black image contains a minimum toolset, similar to all the other ARM images. It is also possible to upgrade the installation to a standard desktop image by including the extra tools available in the **kali-linux-full** metapackage (*for convenience, we will denote key software package names and command line inputs in bold throughout the text*)

The first step in our installation process is to create an ARM file on a micro SD card for the BeagleBone Black. The BeagleBone Black has a built in 4 GB flash memory, however, Kali Linux requires approximately 3.5 GB [3], so a micro SD card is required for this install. The standard image contains the minimum toolset, but we also installed the metapackage tools (including the Ettercap Graphical tool which is used for packet sniffing and in the ARP cache poisoning tests). A wireless network USB card is added to the design, as the standard BBB does not include a wireless card. The BBB uses a Mini HDMI port for video, so a mini HDMI to HDMI cable is used to view the Graphical User Interface (GUI). A USB Hub is used to connect a keyboard and mouse for use. Turning on the BBB, the screen will show a standard terminal screen, and the command ***startx*** will load the built in GUI.

There are several other important tools and commands that are used to perform the ethical hacks in this paper. These include **Aircrack-ng** (*air cracking*) [5] which is a cracking program that can recover keys once enough data packets have been captured. It contains a set of tools for auditing wireless networks. **Airmon-ng** (*air monitoring*) is a script/command used to enable monitor mode on wireless interfaces, and to toggle between monitor-mode and manage-mode. Entering the command without parameters will show the interface status. **Airodump-ng** is another command used for packet capturing. The captured packets can be used with the aircrack-ng script to speed up the network hacking. The script will list any detected access points. **Airbase-ng** is a multipurpose tool that focuses on attacking clients as a whole instead of just an access point; this is also known as horizontal scanning. We also use the popular packet sniffing program WireShark.

III. Denial of Service Attack

Using the command ***iwconfig*** shows a list of available network cards. This commonly includes wireless local area network (wlan) adapters with default values such as wlan0/1/2. For this test wlan0 is used. When a scan is performed on hosts or servers, the user can then choose the target points by knowing the IP or the MAC address. Tools available in Kali Linux enable the user to alter, or spoof the MAC address, which is our first step. Typing ***ifconfig wlan0 down*** will turn off the network card. ***Macchanger –r wlan0*** will give the wlan0 card a random MAC address [6, 7]. The screen will show both the original MAC address, and the new randomized one. Typing ***ifconfig wlan0 up*** turns the card back on with the new MAC address.

Next, the DoS attack can be performed. The ***airmon-ng*** command is used and this command shows the available wireless cards. Typing ***airmon-ng start wlan0*** will enable monitor mode using wlan0 and will create mon0, a virtual monitoring card. Next, typing ***iwconfig mon0*** will configure mon0 and put it into monitor mode. This is needed for the next step. Once the mon0 card is configured, the ***airodump-ng mon0*** command is used. This will search for packets from nearby wireless networks, and will list them. After stopping the command, a list of nearby wireless networks is shown and the penetration test can begin. Noting the wireless signal levels (via the PWR indicator) and the encryption type allows us to choose which network to attack. The next step uses the *airodump-ng* command again, this time focusing on a specific channel, using this structure:
airodump-ng –channel –bssid **:**:**:**:**:** mon0 where ** is the BSSID. With this command, we now see the different devices on that specific network. The next step is the de-authentication attack, in which the airodump-ng command is used for collecting WEP keys for the intent of using them with aircrack-ng. The command is: ***aireplay-ng –ignore-negative-one –deauth 10000 –a 00:25:9c:3B:b8:8B –c 08:3E:8C:C1:52:BD mon0,*** where 10000 is the number of packets being sent to the target device, followed by the target access point, followed by the clients MAC address. The DoS attack involves flooding the target with external communication requests such as pings. This overload prevents the target from responding to legitimate traffic; rather, it slows the response so drastically that the target is deemed effectively unavailable.

IV. ARP Poisoning and MITM Attack

Ettercap-Graphical is available as part of the Kali Linux package, however for our purposes it was downloaded as a separate metapackage and installed/updated from the command line [3]. It is used in this application to ARP poison the targets, such that packets can be captured and filtered by an external tool. The first target should be the router and the second target should be a selected host. We use the unified sniffing method option, and either wlan0, wlan1 or eth0 can be selected based on the type of available connection (wireless for the wlan prefix ports and wired for the eth prefix ports). Ettercap will scan the entire net-mask for hosts. Before proceeding with this attack, changes must be made to the Ettercap configuration file, as noted in the following steps.
locate etter.conf (locate the configuration file, and then use any text editor to make changes).
vim /etc/ettercap/etter.conf (in this file, change lines 16 and 17 to zero as noted below)

ec_uid=0
ec_gid=0

In the same file, uncomment lines 171 and 172 because the IP table is needed; then save changes made and quit. Next, the IP forward setting has to be changed in another file as noted below:
cd /proc/sys/net/ipv4 (change your directory and use ls to find the file, ip_forward, per the command #vim ip_forward. In this file, change zero to one, save and exit.

At this point, the user can successfully proceed to use the Ettercap Graphical tool. '**Scan for hosts'** is then selected, which enables the tool to scan a specific network for all connected hosts. Select two hosts which will be targeted for ARP poisoning to set up the MITM attack. The ethical hacker takes the role of MITM to capture packets being sent between the two targets. In this scenario, the attacker can even use their host and router IP address to obtain information passing between their device and an Internet host. Once packets of data are obtained, the man in the middle can eavesdrop, inject malicious files, or perform other attacks.

By selecting MITM > ARP Poisoning > Sniff Remote Connections, the ethical hacker can choose the desired targets and use Wireshark for filtering the captured packets. Wireshark is a tool used for sniffing, capturing and filtering the packets of data traveling wirelessly between the poisoned targets. Note that packets of data can be obtained on Ettercap once sniffing is initiated. Wireshark enables a wide range of information gathering techniques, including packet capturing, web traffic capturing, email capturing, and display filtering. When the filtering process begins, packets start to display while information is transferred. The displayed information is sorted by packet number, time, source, destination, protocol, and length. When filtering is stopped, the packet analyzing process begins, allowing packets to be processed based on many attributes, including port number, IP address, and protocol. Viewing the contents of an unencrypted packet, after filtering allows the attacker to obtain confidential information including user names, login ID's, passwords, PINs, email content and much more. The process is more efficient for a skilled attacker who knows what to look for in the filtered data; or how to set up more specific filters to obtain specific desired information.

V. Experimental Results

A. Denial of Service (DoS) Attack

When the DoS attack was performed, the targeted computer was on the same network as the hacker. The ESSID or Network ID used for this attack was **MythiLNetwork** with WPA2 encryption and PSK authentication protocol. The router's default gateway address was **192.168.1.1.** The targeted host's IPv4 address on the same network was **192.168.1.118** with a MAC address of **08:3E:8E:C1:52:BD**. The DoS attack was initiated by initiating air monitoring for the wlan0 NIC using the command **airmon-ng start wlan0**. Then the **airodump-ng** command was used to obtain and list the details of access points and clients seen on the network. A typical output received from airodump-ng wlan0 is shown in Figure 2.

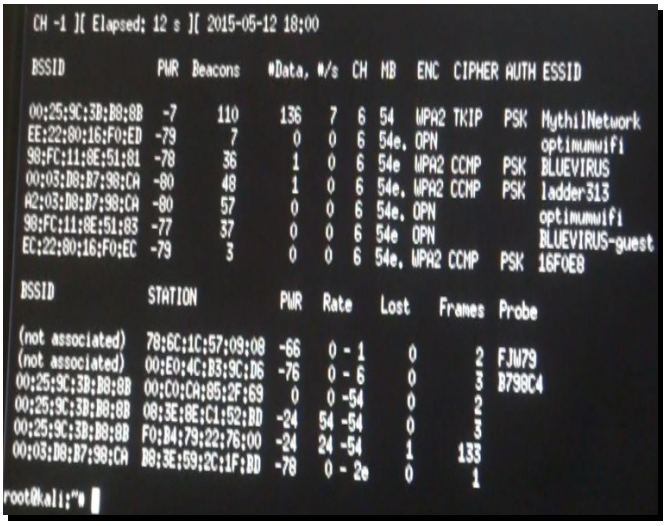

Figure 2 –WLAN access point results

Figure 2 shows the output of all the access points within the signal strength of the wireless network. The test network MythiLNetwork is listed first because its signal strength was the greatest (-7 dBm). Its BSSID is listed as **00:25:9C:3B:B8:8B** with 110 beacons. Beacons are the number of announcements packets sent by the access point (AP). Each access point sends about ten beacons per second at the lowest data rate (1 Mbps), therefore the beacon packets can usually be picked up by servers far away from the AP [5]. This output provides the hacker with minimal yet sufficient data to perform the DoS attack.

Another airodump-ng command is executed to capture data specifically on channel 6, namely **airodump-ng –channel 6 –bssid 00:25:9C:3B:B8:8B wlan0.** Finally, the **aireplay-ng –ignore-negative-one –death 100 –a 00:25:9C:3B:8B –c 08:3E:8E:C1:52:BD wlan0** is executed which denies access of the target's wireless AP. In this command syntax, the number 100 is the number of de-authentication packets to send (this value is somewhat arbitrary, and was selected to provide good results on our test network). Further examining the command syntax, -a 00:25:9C:3B:8B is the MAC address of the access point and -c 08:3E:8E:C1:52:BD is the MAC address of the target that the attacker is de-authenticating [5]. The output after this de-authentication command is executed is shown in Figure 3.

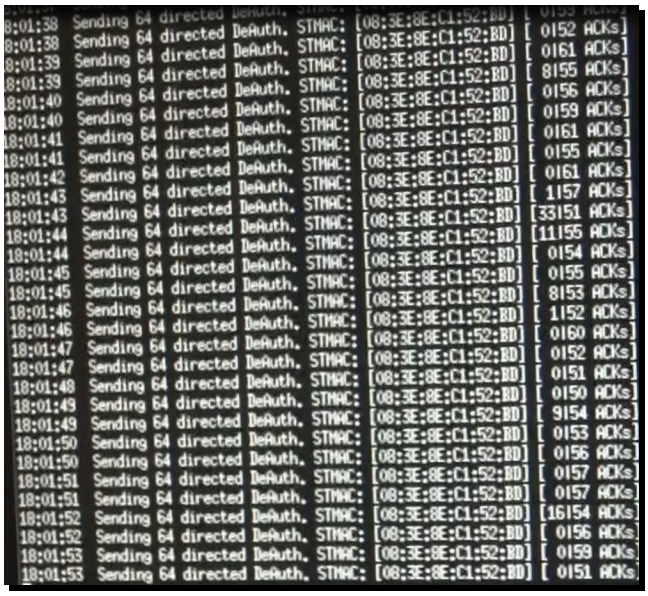

Figure 3 – Output of the de-authentication command

As indicated in Figure 3, **aireplay-ng** sends out a total of 128 packets for each de-authentication which the attacker specifies, where 64 packets are sent to the AP and 64 packets are sent to the target [5]. In this example, we receive more than 64 ACKs from the target, indicating that the target receiving the de-authentication requests is nearby. This resulted in the target being denied network access until the attacker stops the de-authentication requests; the target's monitor confirms this, as shown in Figure 4. During our penetration testing, the de-authentication command was manually stopped by entering CTRL+C which allowed the target to regain network access. In a similar manner, other well-known attacks could be executed at this point, including SYN floods (*which exploit the TCP three-way open handshake*).

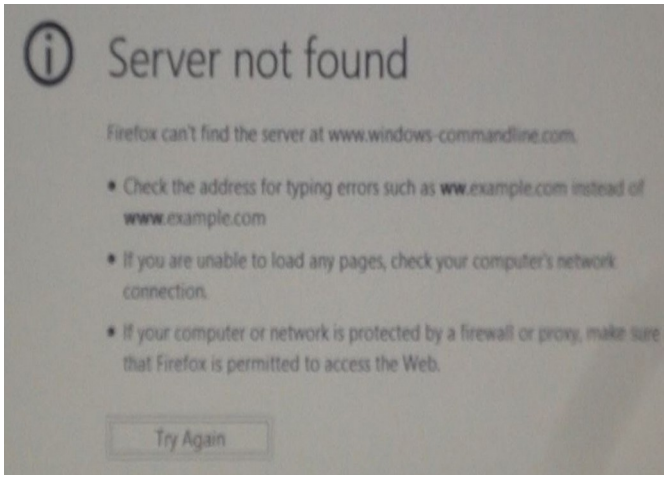

Figure 4 – Target monitor during DoS attack

B. Reconnaissance Attack (Man in the Middle)

The second attack performed in our test network is the Man in the Middle Attack (MITM). This attack is classified as a reconnaissance attack because its purpose is gathering data which may include the application type, application version and even the operating system type and version. It is useful to know the IP address for both the attacker and target computers. For the purpose of our test, the target used was the website http://www.hackforums.net where we created an account with username RACHELRACKAL and password CET4960. The attacker's address, of course, can be found by issuing the **ifconfig** command; a typical result is shown in Figure 5, which includes a list of IPv4, IPv6, MAC, subnet, broadcast, and mask address for wlan0.

Figure 5 – Server Address Information

This attack uses Ettercap-Graphical to scan an interface for hosts and then assign the router and host as target one and two respectively. ARP poison is then selected from the MITM options. The status of Ettercap when these options are selected is shown in Figure 7.

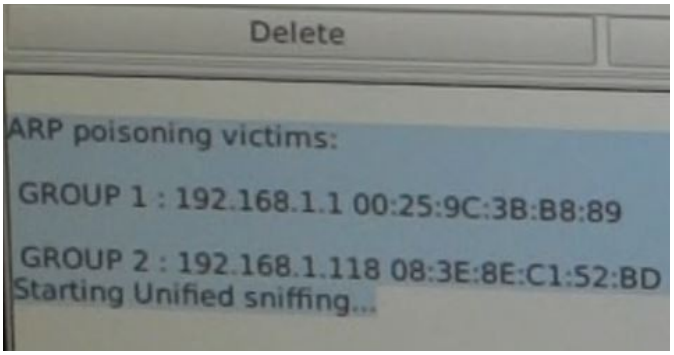

Figure 6 – Organization of ARP cache poisioning targets

Figure 6 shows the ARP poisoning victims organized into two groups. The routers default gateway IP and MAC address is 192.168.1.2 00:25:9C:3B:B8:89 and is assigned to group 1. The target's IP and MAC address is 192.168.1.118 08:3E:8E:C1:52:BD and is assigned to group 2. When the option "unified start sniffing" is selected, the two groups are ARP poisoned and the MITM is injected between the two groups. Intead of the packets traveling directly from the host to the server, the packets are traveling from the host to the man in the middle and then to the server.

Now that the MITM is between the targets points, the packets of data can be captured using the well known packet sniffer WireShark [4]. When wlan0 is selected, the packet capturing process begins. For this test, Wireshark displayed all of the data by the number of packets, time, source (IP address), destination (IP address), Protocol, Length, and Info (see Figure 7).

.

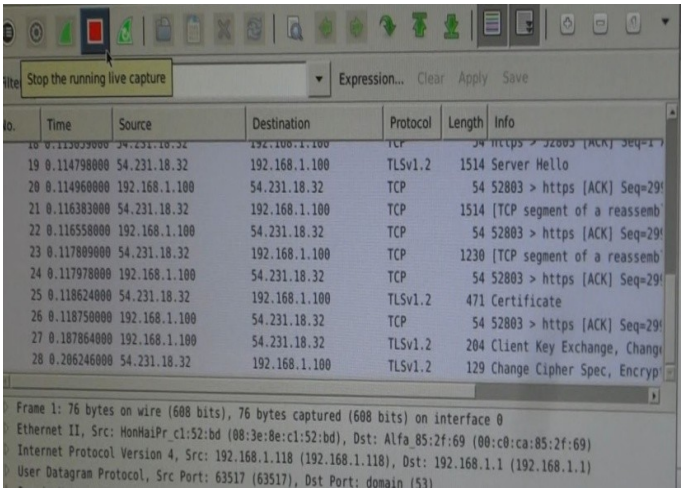

Figure 7 – WireShark output during MITM attack

As shown in Figure 7, the MITM can obtain all the data being sent across the network. The filtering process helps the attacker know where to find commands such as POST or GET Since we are attacking a website, filtering on HTTP port 80 yields the typical result shown in Figure 8.

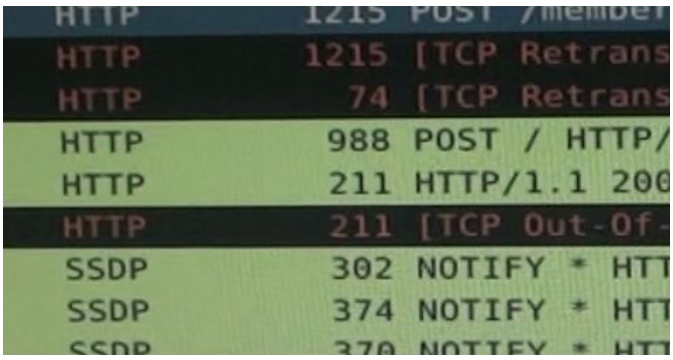

Figure 8 – WireShark HTTP filter output

Since the website used for the attack was not secured or encrypted, it was not difficult to obtain the login and password information when the target sends a POST command to its nearest router. Figure 9 shows how the userid and password can be viewed in plain text within the packet capture trace.

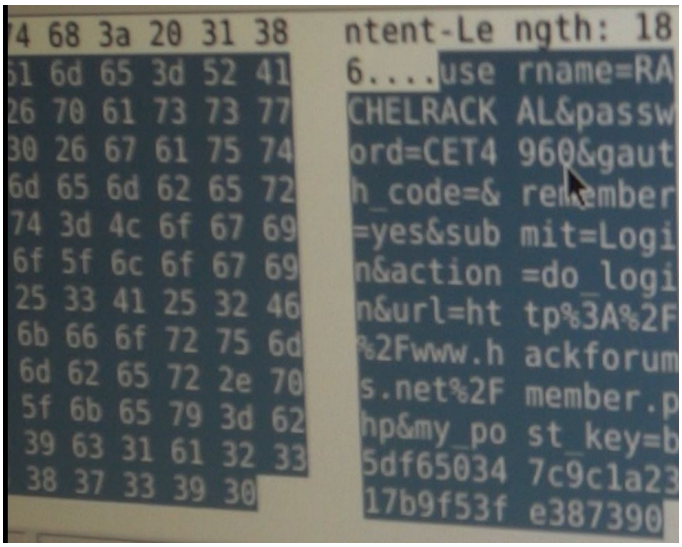

Figure 9 – Capturing userid and password data

Note that packets of data can also be captured and listed from Ettercap-Graphical, however it lacks the filtering capabilities of WireShark. If the user is browsing or entering confidential information on a secured website with HTTPS protocol, the output will be encrypted. However, we can apply several tools to crack WEP keys [8] or compare a dictionary of hashed values against a password hash recovered from the WireShark trace.

VI. CONCLUSIONS

We have shown the feasibility of installing Kali Linux with the Ettercap Graphical tools on an augmented BeagleBone Black micro-computer to conduct successful penetration testing. The capabilities of this platform were demonstrated using a Denial of Service attack and a Reconaissance attack consisting of a poisoned ARP cache and a man-in-the middle attack.

The Denial of Service attack was executed such that the target would be de-authenticated from the network and not allowed access again until the attack was stopped. This attack included flooding the target's computer with 100 de-authentications, with each de-authentication consisting of 128 packets to received and be acknowledged. The target was automatically disconnected from that network and failed to connect when attempts were made to re establish a connection. However, when the de-authentication process was manually stopped by the attacker, the target once again successfully gained Internet access.

The Man in the Middle Attack was performed by Ettercap-Graphical and Wireshark. The attacker was introduced and intercepted between the server and target's connection, enabling them to receive all information transferring back and forth between the router and the target device. The ARP poison method was used along with unified sniffing across the wireless LAN. After packets of data were captured they were analyzed using Wireshark filtering for HTTP POST commands to obtain the target website's username and password.

Future research in this area will focus on effectiveness of countermeasures such as selecting dictionary-resistant passwords, and the use of VPNs and IP address spoofing counter-measures. Due to the relatively small physical size and low power consumption requirements of a BeagleBone Black, it can be easily carried inside the physical perimeter of a secure facility. This provides an interesting new threat vector for wireless network protection, which we plan to study further.

REFERENCES

[1] Verizon 2015 annual cyber threat report, online http://news.verizonenterprise.com/2015/04/2015-data-breach-report-info/ (last accessed Jan. 18, 2016)

[2] Molloy, Derek "The BeagleBone Hardware." *Exploring BeagleBone: Tools and Techniques for Building with Embedded Linux.* Indianapolis: John Wiley & Sons, 2015. 3 – 22.

[3] Offensive-security.com, 'Kali Linux Downloads', 2015. [Online]. Available:https://www.offensive-security.com/kali-linux-vmware-arm-image-download/. [Accessed: 07- May- 2015]; see also Ettercap.github.io, 'About « Ettercap', 2015. [Online]. Available: http://ettercap.github.io/ettercap/about.html. [Accessed: 07- May- 2015].

[4] Wireshark.org, 'Wireshark • Documentation', 2015. [Online]. Available: https://www.wireshark.org/docs/. [Accessed: 07- May- 2015].

[5] Aircrack-ng.org, 'airmon-ng [Aircrack-ng]', 2015. [Online]. Available: http://www.aircrack-ng.org/doku.php?id=airmon-ng. [Accessed: 07- May- 2015].

[6] Boyle, Randall. "Packet Sniffer."*Applied Information Security: A Hands -on Guide to Information Security Software.* 2nd ed. Boston: Prentice Hall, 2010. 150 - 157.

[7] S. Chaudhary, 'Penetration Testing - Hacking XP', Kalitutorials.net, 2014. [Online]. Available: http://www.kalitutorials.net/2014/02/penetration-testing-hacking-xp.html. [Accessed: 07- May- 2015].

[8] H. Handshake, 'Hack WPA-2 PSK Capturing the Handshake', Kalitutorials.net, 2014. [Online]. Available: http://www.kalitutorials.net/2014/06/hack-wpa-2-psk-capturing-handshake.html. [Accessed: 07- May- 2015].