A Study in Wireless Attacks and its Tools

José J. Flores
Polytechnic University of Puerto Rico, Hato Rey, PR, flores_jj@hotmail.com

Alfredo Cruz, PhD
Polytechnic University of Puerto Rico, Hato Rey, PR, alcruz@pupr.edu

ABSTRACT

Every day the world is becoming more connected through the use of networks, specifically wireless local area networks (WLANs). At the same time, the significance of wireless security continues to grow. Similar to others aspects of life, computers networks are susceptible to criminal activity. As new technologies emerge so does security vulnerabilities which threaten the stability of computer networks. These vulnerabilities can be exploited by criminals with a variety of purposes, which some could be related to causing damage or simply stealing information. This paper researches a set of wireless attacks and some of the tools used to perform them. Through their usage it tries to create awareness of today's usage of a specific wireless encryption that have been long proven to be unsecure.

Keywords: Hacking Tools, Security, Wireless, Wireless Attacks

1. INTRODUCTION

Nowadays mostly everyone is connected to a computer network, in particular the Internet. This network of computers has become critical for many institutions, including governments, universities, large and small companies, and private citizens that rely on it for professional activities.

However, similar to others aspects of life, computers networks are susceptible to criminal activity, such as causing damage to the computer, violating users' privacy, stealing information or rendering inoperable the network services on which an institution may rely. Also, as new technologies emerge so does security vulnerabilities which threaten the stability of computer networks. Criminals may take advantage of these vulnerabilities to perform attacks. These may be concerns for many institutions considering the possibilities of expanding their services online, or that may already be doing so but do not want their users to become victims.

This work will explore various topics related to wireless security with the purpose of understanding some of the existing vulnerabilities and some of the tools used to take advantage of them. It starts with the discussion of the main problems in wireless security. Then, it makes a special reference to the concept of ethical hacking because it serves as a necessary background in understanding how to properly approach the usage or implementation of the tools that will be studied in the project. It continues with the discussion of some wireless attacks and the usage of some tools.

2. WIRELESS SECURITY

Wireless networks provide various benefits such as mobility and flexibility. Mobility allows users to move through the covered area without the need of disconnecting and connecting. Flexibility allows the fast deployment of networks that permits multiple users to share connections without the need of running cables. For example, some coffee shops are able to offer Internet connectivity to their users through the use of wireless networks. Although, this may be possible with a wired network it would require running cables and enough connection points (Ethernet jacks) which would be more time consuming and expensive. Also, it could limit the number of customers that can connect at the same time. A wireless approach provides a simpler and cost effective way of

offering this service in comparison with a wired solution.

Despite the benefits, wireless networks present some challenges regarding security. Data is transmitted through radio waves which can propagate far beyond the desired area (Kurose and Ross, 2010). For example, Figure 1 illustrates one scenario where a home user installs an access point (AP) where the signal might propagate to his closest neighbors without his knowledge.

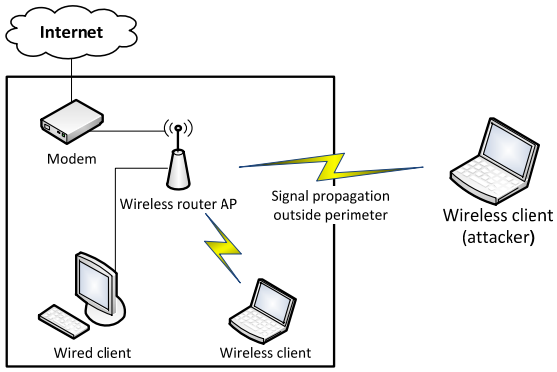

Figure 1: Signal Propagation Outside Perimeter

In a different scenario, as it being illustrated in Figure 2, an employee might install an access point in his office without knowing the signal could propagate beyond the walls of the business. On the other hand, the employee might be intentionally placing a rogue access point. The security problem is that an attacker could intercept those radio waves just as a computer detects an access point and connects to it.

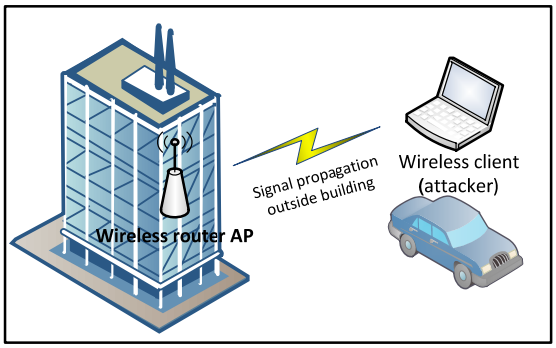

Figure 2: Signal Propagation Outside the Building

3. ETHICAL HACKING

An important part of every information security program is ethical hacking. This approach attempts to continuously increase security in systems by identifying and promoting the patching of known security vulnerabilities on systems. Ethical hackers may test beta unreleased software, stress test related software, and scan networks of computers for vulnerabilities (Smith et al., 2002).

When referring to hacking a distinction must be made between a hacker and a cracker. The latter obtains unauthorized access with the purpose of obtaining financial gain, sabotage systems, promote political causes or steal information.

To further help differentiate a good hacker from a bad one, hackers can be divided into the following three groups:

- **White Hats**: This group refers to ethical hackers who use their hacking skills for defensive purposes. White-hats hackers are security professionals that understand how hackers work and use that knowledge

to locate weaknesses and implement countermeasures. They hack with permission from the data owner.

- **Black Hats**: This group refers to malicious hackers or crackers who use their skills for illegal or malicious purposes.
- **Gray Hats**: This group refers to those hackers who may work offensively or defensively, depending on the situation.

Ethical hackers perform what is known as penetration tests. These tests consist of carrying out specific and controlled attacks by security personnel to compromise or disrupt their clients systems by exploiting documented vulnerabilities (Whitman and Hattord, 2008). This is commonly performed on network connections from outside the organization to simulate as it was from the typical attacker's position. The information security personnel who perform these tests are often consultants or outsourced contractors. Aside from ethical hackers or white-hat hackers, this personnel is also referred as tiger teams or red teams.

3.1 PHASES

The study guide for the certification of Certified Ethical Hacker (Kimberly, 2010), specifies that ethical hacking consists of a process that can be divided in five distinct phases. Each of these phases involves the use of different techniques and hacking tools. The usual phases followed when hacking a computer system are:

1. **Passive and Active Reconnaissance:** This phase involves gathering information about the target without the target's knowledge. This includes sniffing the network to obtain useful information such as Internet Protocol (IP) address ranges, naming conventions, hidden servers or networks, and other available services on the system or network. On the other hand, active reconnaissance involves probing the network to discover individual hosts, IP addresses and services on the network. This process increases the chances of getting caught or raising suspicion.
2. **Scanning:** In this phase the information previously gathered is used to examine the network more thoroughly using tools such as port scanners, network mappers, and vulnerability scanners. The purpose is to obtain information such a computer names, operating systems, installed software or user accounts that may help in the phase of gaining access.
3. **Gaining Access:** This phase consist of actually hacking the system by exploiting the vulnerabilities found during the first two phases.
4. **Maintaining Access:** In this phase hackers protect the system from other hackers or security personnel and install software that provides them with exclusive access for future exploitations and attacks. This involves the use of backdoors, rootkits, and Trojans.
5. **Covering Tracks:** This phase consists of removing all traces of the attack, such as log files or intrusion detection system (IDS) alarms.

Based on the descriptions of each of the phases, the attacker must already be connected to the network, except for passive reconnaissance. Either for wired or wireless attacks the attacker must find a way to gain access to the network. In the case of a wireless attack, gaining access to the network will depend primarily on what type of security the access point is using, if any. Once the attacker is able to decrypt the packets being transmitted he can start with the active reconnaissance phase and continue with the rest of phases.

4. WIRELESS ATTACKS

Based on the documentation previously discussed the first step in attacking a protected wireless network must be to gain access to it by breaking the encryption. Then we can proceed with other attacks. Although the following section discusses two different types of encryption, the main focus will be on the Wired Equivalent Privacy (WEP) protocol. The next two sections will explore other types of wireless attacks.

4.1 ENCRYPTION ATTACKS

WEP protocol was the first security mechanism initially standardized in the IEEE 802.11 specification. The purpose of WEP was to provide a level of security in wireless networks similar to that found in wired networks

(Kurose and Ross, 2010). However, WEP is no longer considered secure. Researchers (Fluhrer et al., 2001) identified design flaws in the encryption implementation that allowed them to recover the key through a series of attacks. In later years, more attacks were developed allowing the recovery of the key in a shorter time.

The alternative solution presented by the Wi-Fi Alliance was the Wi-Fi Protected Access (WPA) standard. In 2003, WPA certification addressed the security concerns of WEP and enabled the adoption of Wi-Fi across enterprise and consumer markets. An enhanced version was later published with the name WPA2 (Wi-Fi Alliance Timeline, 2011). Even though WPA provides security enhancements, it is still susceptible to dictionary attacks.

Nowadays, WEP encryption is still being used by home users and businesses. A quick scan of wireless networks might reveal a combination of access points that are open or protected either by WEP or WPA. There may be situations in which legacy devices cannot connect to access points with an encryption higher than WEP encryption. For these cases is better to lookup for alternatives such as firmware updates or new hardware.

4.2 WARDRIVING

WarDriving is the act of moving around a specific area, mapping the population of wireless access points for statistical purposes. These statistics are then used to raise awareness of the security problems associated with these types of networks (typically wireless). The commonly accepted definition of WarDriving is that it is not exclusive of surveillance and research by automobile. WarDriving is accomplished by anyone moving around a certain area looking for data, which includes: walking, which is often referred to as WarWalking; flying, which is often referred to as WarFlying; bicycling, and so forth. WarDriving does not utilize the resources of any wireless access point or network that is discovered, without prior authorization of the owner (Hurley et al., 2007).

As always, this process could be used by an attacker to obtain a list of unsecured or weak protected access points as a launch point for further attacks. Therefore it is necessary to understand how this process work and in which way it could be used to improve security.

There are applications for mobile phones that use the existing hardware to perform the WarDriving. However, a laptop setup requires:

- A wireless network interface card that accepts an external antenna for a better range performance
- A GPS Unit to record the location where the access point was captured
- A WarDriving software program such as Kismet to capture the data

4.3 MAN IN THE MIDDLE (MITM)

In a Man-in-the-Middle (MITM) attack, an attacker establishes connections to victim computers and serves as the host between them. For the victims it will seem like they are communicating directly, when in fact they are exchanging messages through the attacker's machine as shown in Figure 3.

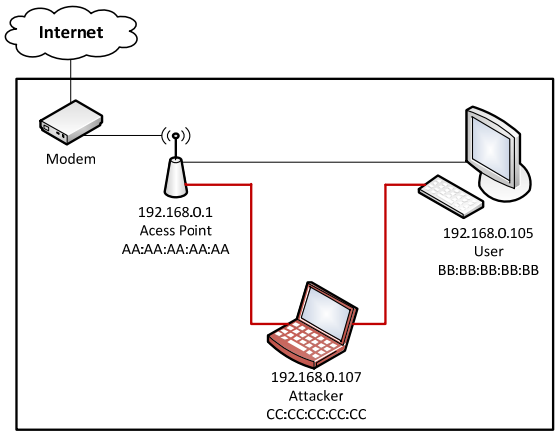

Figure 3. Typical MITM Scenario

The attacker redirects all the traffic between the hosts to be able to perform packet sniffing or data manipulation. Sniffing attacks allows an attacker to gain access to all the packets sent and received by a host, which may include sensitive data such as passwords and credit cards numbers. In order to achieve this attack the attacker takes advantage of security flaws in the implementation of the ARP protocol and exploit them at hosts (Belenguer and Calafate, 2007).

Before being able to successfully attack a wireless network using a MITM approach it is necessary to accomplish the following tasks (Hurley et al., 2007):

- Detect access points with connected wireless clients already.
- Identify the security controls and encryption scheme enabled on the target access point.
- Bypass the security controls and associate to the target access point.

The first two steps can be obtained through WarDriving as it was discussed in the previous section. The last step requires connecting to an already open access point or employing techniques to break the encryption where possible. Failing in associating with the target access point will result in a failed attack. Before the MITM attack can be performed the attacker must be connected to the access point. Once this is achieved, the attack can be launched.

5. TOOLS

There are a variety of tools freely available on the Internet that can be used through each of the phases that involve the process of ethical hacking. For example,

- **Footprinting** also known as information gathering involves the uses of tools such as domain name lookup, Whois, and NSLookup. An Internet search reveals many links of websites providing access to these tools. Some of these tools are web-based while others may be downloaded and installed in the user's computer.
- **Scanning** involves the use of tools such as ping and Nmap to identify online hosts in a network and their open ports, among other things.
- **Gaining Access** tools may vary based on the situation. When trying to break a wireless network tools such as aircrack-ng will prove to be useful. If trying to gain access to a computer physically available tools such as ophcrack will prove useful when trying to recover user password from the operating system (OS).
- Other techniques include the use of Trojans and backdoors to maintain access to the system and the use of sniffers, such as Wireshark, to monitor and analyze packets.

The following sections intend to explore some of the techniques and tools used in one or more phase of the hacking process. They provide a way to understand how some hacking techniques are employed with goal of knowing what can be done to protect the system.

5.1 KISMET AND WARDRIVE

Kismet is an application created for systems running any variation of the Linux operating system. It is defined as a wireless network detector, sniffer, and intrusion detection system capable of identifying networks, named or hidden, by passively collecting packets. Figure 4 illustrates the Kismet application detecting new wireless access points. At the time this screenshot was taken, the application had been running for 57 minutes and 10 seconds, a total of 1585 networks had been detected and a total of 44,148 packets had been captured.

The data captured by Kismet can be used to create maps of the location of the access points and their security, if any. A tool named GisKismet can process the data and stored it in a SQLite3 database format allowing for easier extraction and filtering of the data. The result is a file named wireless.dbl.

Wardrive is an application created for mobile devices running the Android operating system. Although this application does not break any type of security, it provides the attacker with quick information about the surrounding access points by simply using a mobile device. This application scans available details, such as type

of encryption, of all the wireless access points within the range of the mobile device. The data generated is automatically stored on a SQLite3 database format.

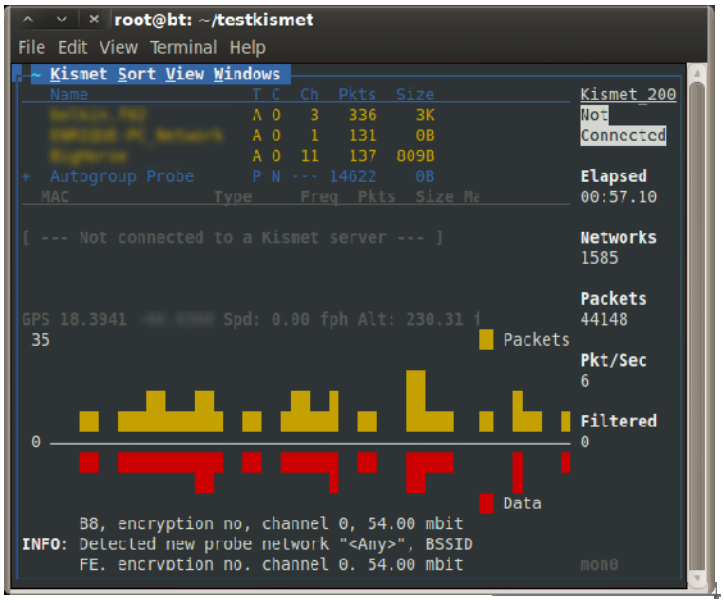

Figure 4. Kismet Main Window Showing Detected Networks

Figure 5 illustrates the main window of the Wardrive application. The main window provides a menu with different options, displays a map of the current location obtained by GPS and the access points captured. In this case, the map is being filtered to display only the access points with no encryption (Open) which are represented by the green color.

Figure 5. Wardrive Showing Captured Access Points

The configuration of the Wardrive application, allows the user to change various parameters such as which type of access points to shown in the main window.

5.2 NMAP

Scanning is the second phase of ethical hacking. This phase consists of gathering information about any type of network and its individual host system such as IP addresses, operating systems, services, and installed applications. This information can be used to identify vulnerabilities in the system that could be exploited to gain access to the systems.

There are three types of scanning (Kimberly, 2010):

- Port scanning – used to determine open ports and services
- Networking scanning – used to identify IP addresses on a given network
- Vulnerability scanning – used to discover the presence of known weaknesses on target systems

Nmap ("Network Mapper") is an open source network scanning tool that provides an array of functionalities to cover the three types of scanning discussed in the previous section. This tool can be installed in multiple operating systems and is continuously enhanced by volunteers from the open source community. The user can use either the command line version or the graphical user interface. See Figure 6 below.

Zenmap is the official graphical user interface for Nmap. It aims to provide an easier way for beginners to interact with Nmap functionality, while still providing advanced features for experienced users. Along many of its features, Zenmap provides a set of predefined common profiles to perform different types of scans (Lyon, 2009).

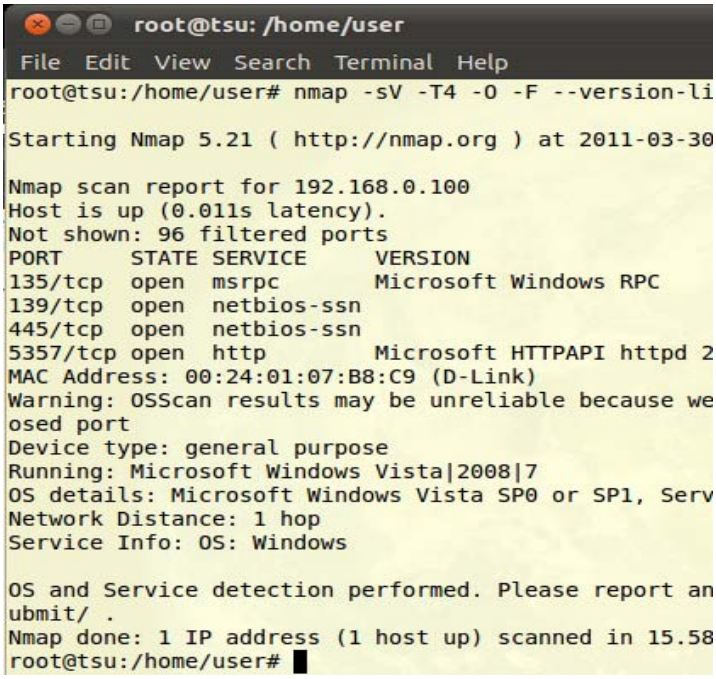

Figure 6. Nmap Using the Predefined Command "Quick scan plus".

5.3 SSLSTRIP AND ARPSPOOF

Gaining access is the third phase of the ethical hacking (Kimberly, 2010). Many attempts to gain access to a system starts by guessing or cracking a password. Once this is done, an attacker can perform a series of actions such as maintaining access and covering tracks.

Passive online attacks are one of the methods used to identify a password and gain access to a system. These types of attacks are also known as sniffing the password on a network. One way to achieve this is by using the man-in-the-middle (MITM) attack.

In a MITM attack, once the attacker is connected it can monitor the messages between the victim computers. However, messages exchanged protected by Secure Socket Layer (SSL) cannot be simply intercepted as these are encrypted. HTTPS provides end-to-end Secure Socket Layer (SSL) protection against eavesdropping and man-in-

the-middle attacks (Fung and Cheung, 2010).

SSLStrip was created by a computer researcher named Moxie Marlinspike to provide a demonstration of the HTTPS stripping attacks (Sslstrip). This tool "transparently hijacks HTTP traffic on a network by parsing the given stream and then giving back the new crafted stream to the right session" (Prandini, et al., 2010). Basically, the tool intercepts an HTTPS link, replaces it with a very similar HTTP link and forwards it back to the victim. Then, when the user tries to log in into a website the POST, containing the username and password, is captured in plaintext and saved in a log file.

The author's website provides a list of required files, clear and concise instructions on how to use the tool and an explanation of how it works. The tool was originally presented in 2009 and the last version was deployed on May 15, 2011.

6. WARDRIVING EXPLORATION

Using the tools discussed in section 5.2 a wardrive was conducted to determine the extent of unsecured access points still being used in a given area. Table 1 illustrates a summary of the differences found between the tools used for the experiment. These differences were divided in the process required to setup the test in each of the devices, how much data was captured and how this data could be analyzed based on the format chosen by each program.

Table 1. Differences Between Kismet and Wardrive

	Kismet	**Wardrive**
Platform	Laptop with BackTrack operating system	Mobile phone with Android operating system
Setup	More complicated laptop, USB wireless adapter, USB GPS receiver, installing drivers, setting up external devices, processing data	Easier Enable Wi-Fi and GPS in mobile device Start application
Data captured	924 access points	563 access points
Data format	Stored in across various files. Can be easily exported to a SQLite3 database format with the tool GISKismet.	Stored in a SQLite3 database format.
Mapping	Using GISKismet to create KML files based on SQL queries. Provides more flexibility.	Has a function to export the data to KML and group the access points by Open, WEP, and Closed.

Setting up Kismet took more time than with Wardrive because it required not only the software but additional hardware in order to capture the location of the access points. In contrast, the mobile device already had GPS capability easily accessible.

As shown in Table 1, Kismet was able to capture more data. However, Kismet was being executed in a laptop that had more processing power and an external antenna with more range. Even then, Wardrive was able to capture a good amount of access points.

The WarDriving experiment took approximately one hour to complete. However, that does not include the time required to get the proper equipment and prepare the laptop. The time invested in the wardrive was affected by the chosen driving speed. In order to get better results for the location of the access points being captured, the driving was mostly reduced to an average of 25 to 30 miles per hour.

The fact that the data of both programs is in a SQLite3 database format, allows an easy extraction of data for further analysis through the use of SQL commands. For example, we can generate data to graph the types of encryptions, the most common access point names, the manufacturers more deployed, or the channels most used.

Based on the data captured by Kismet a total of 924 access points were found during the scan. Figure 7 shows that from that data sample a 44% of the access points were protected by some type of WPA encryption. Surprisingly, the percentage of access points using WEP was almost the same as those using WPA. This document has presented a couple of tools that prove this type of security is easily broken. After so many years it would be expected that access points, specifically provided by ISPs, would be protected with better encryption.

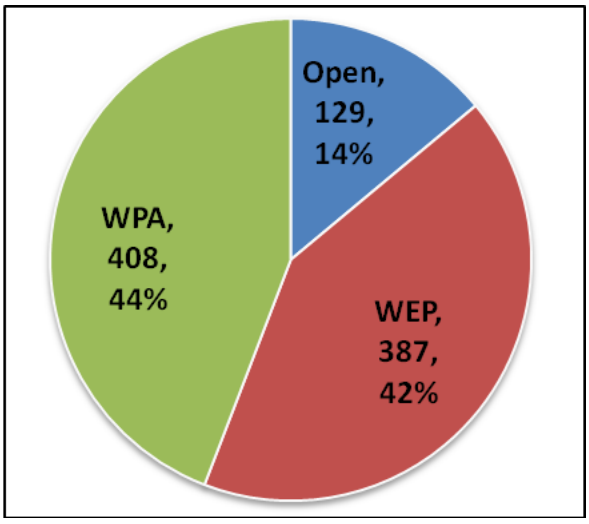

Figure 7. Access Points Captured by Type of Encryption

The data captured can be transformed into a file that Google Earth can interpret. This provides the user with a graphical representation of the location of each access point.

With this information, an attacker would have a list of all the access points with WEP encryption and their locations. A wireless attack could then be launched to break the encryption, retrieve the key, connect to the access point, scan the network and launch a MITM attack.

Figure 8 shows the manufacturers with a quantity greater than 40. The rest of the access point are grouped under the "Others" category. Based on these results the manufacturer with most access points is Thompson with a 30% representation. It is likely these access points are provided by an ISP.

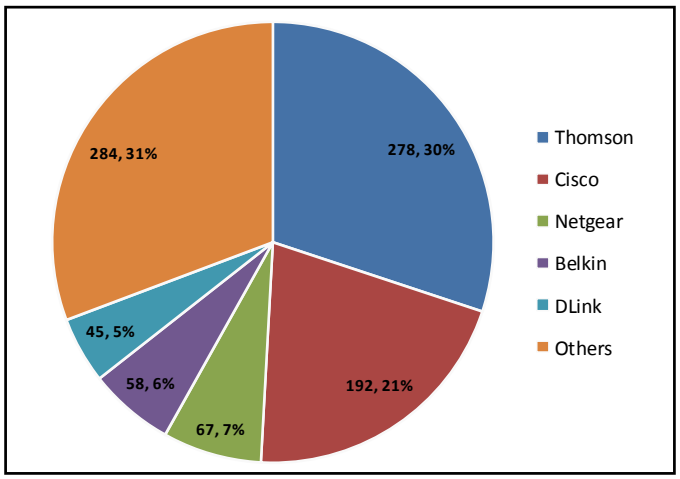

Figure 8. Access Points Captured by Type of Manufacturer

7. CONCLUSION

In today's computing environment, ethical hacking seems to provide valuable knowledge in the protection of systems. It develops in an individual a new way of thinking and seeing things from a different angle, the hacker perspective. Also, it provides the methodologies for testing the security of computer network in an organized manner with the purpose of being able to produce clear and concise results about what actions need to be taken to correct existing security issues.

One study (Young et al., 2007) was conducted to capture the perception of hacker regarding the legal consequences of being captured. The result, among other things, presented that punishment severity, which involves prison time, fines and community services, does not appear to deter illegal hacking simply because hackers consider their behavior morally right and believe that the probabilities of being caught are low. Recent events of attacks to private business, such as credit card companies, have demonstrated this behavior prove to be valid. Therefore, it is to be expected that organizations will be looking for candidates with the expertise and knowledge in the domain of network security.

ACKNOWLEDGEMENT

This material is based upon work supported by, or in part by, the U. S. Army Research Laboratory and the U. S. Army Research Office under contract/grant number W911NF1110174.

REFERENCES

Belenguer, J., & Calafate, C. T. (2007). "A Low-Cost Embedded IDS to Monitor and Prevent Man-in-the-Middle Attacks on Wired LAN Environments". *International Conference on Emerging Security Information, Systems and Technologies*, pp. 122-127.

Fluhrer, S., Mantin, I., & Shamir, A. (2001). "Weaknesses in the Key Scheduling Algorithm of RC4". *In S. Vaudenay, & A. Youssef, Selected Areas in Cryptography*, Vol. 2259 of Lecture Notes in Computer Science, pp. 1-24. Springer Berlin / Heidelberg.

Fung, A. P., & Cheung, K. (2010). "HTTPSLock: Enforcing HTTPS in Unmodified Browsers with Cached Javascript". *2010 Fourth International Conference on Network and System Security*, pp. 269-274.

Hurley, C., Rogers, R., Thornton, F., Connelly, D., & Baker, B. (2007). *WarDriving and Wireless Penetration Testing*. Syngress.

Kimberly, G. (2010). *CEH: Official Certified Ethical Hacker Study Guide*. Sybex.

Kurose, J. F., & Ross, K. W. (2010). *Computer Networking: A Top-Down Approach*, 5th edition, Addison-Wesley.

Lyon, G. F. (2009). "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning". *Insecure.*

Prandini, M., Ramilli, M., Cerroni, W., & Callegati, F. (2010). "Splitting the HTTPS Stream to Attack Secure Web Connections". *IEEE Security and Privacy*, 80-84.

Smith, B., Yurcik, W., & Doss, D. (2002, June). "Ethical Hacking: The Security Justification Redux". *IEEE International Symposium on Technology and Society* (ISTAS), pp. 374-379.

Tews, E., Weinmann, R.-P., & Pyshkin, A. (2007). "Breaking 104 Bit WEP in less than 60 seconds". *Proceedings of the 8th International Conference on Information Security Applications*, pp. 188-202. Springer-Verlag.

Whitman, M. E., & Hattord, H. J. (2008). *Management of Information Security*, 2nd edition. Thompson.

Wi-Fi Alliance Timeline, http://www.wi-fi.org/sites/default/files/uploads/files/WFA_ Timeline_Updated_-PDF.pdf, 04/03/11. (date accessed).

Young, R., Zhang, L., & Prybutok, V. R. (2007, January). "Hacking into the Minds of Hackers". *Information Systems Management*, 24(4), pp. 281-287.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.