Wireless Vulnerability Assessment

A Project Report

Submitted to the Faculty

of the

UNITED STATES COAST GUARD ACADEMY

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

in

Electrical Engineering

by

1/C Ryan W. Maca

1/C David A. Pipkorn

Projects in Electrical and Computer Engineering
02 May 2007

Reviewed By:

LT Todd W. Moyer, Project Advisor

LCDR David J. Godfrey, Class Coordinator

Professor Keith C. Gross, Chief, Electrical & Computer Engineering Section

Abstract

Wireless networks are being deployed throughout the world because it is cheap, efficient, and effective method for providing mobile networks. The Coast Guard Telecommunication & Information Systems Command (TISCOM) is interested in implementing a wide scale wireless network but requires a high level of security that can be monitored and maintained. To ensure this level of security, TISCOM sponsored this project to develop a wireless vulnerability assessment methodology to assess Coast Guard networks and identify wireless vulnerabilities.

Project work involves the assessment of current Coast Guard installations, active penetration testing within laboratory settings, and a complete assessment methodology design based on the data collected throughout the project. This project completed two passive assessments on Coast Guard installations, a 64-bit and 128-bit Wired Equivalent Protection (WEP) key recovery, the decryption of the Wi-Fi Protected Access (WPA) protocol, the development of a Linux toolset distribution for Coast Guard assessment team usage, and a complete assessment methodology tutorial. Further work in this field would include active assessments of the Advanced Encryption Standard (AES) protocol under laboratory conditions, testing the AirFortress security system and the Wireless Intrusion Detection System (WIDS) under laboratory settings, and implementing a secure Coast Guard wireless network to conduct active assessments.

Table of Contents

Abstract page i
Table of Contents page ii
Introduction page 1
Background page 3
Wireless Network Configuration and Operation page 4
Figure 1: Generic Wireless Network page 4
Security Protocol page 5
Wired Equivalent Privacy page 5
Wi-fi Protected Access page 6
Advanced Encryption Standard page 6
Authentication and Certification page 6
Passive Data Collection page 7
Security Vulnerabilities page 8
Rouge Access Points page 8
Ad-Hoc Networks page 8
Excessive Signal Strength page 8
Probing Laptops page 9
Low Level Encryption page 9
Default Settings page 9
Active Attacks page 10
Denial of Service page 10
Man in the Middle page 10
Spoofing page 11
Objective page 11
Coast Guard Wireless Assessments page 12
Table 1: Target Vulnerabilities page 12
Identification of Existing Vulnerabilities page 12
Vulnerability Test-Bed Design page 13
Development of First Hand Assessment Knowledge page 13
Customized Linux Security Assessment Distribution page 14
Active Laboratory Test-Bed page 14
System Design page 15
Laboratory Test-Bed page 16
Table 2: Laboratory Equipment page 16
Table 3: Vulnerability Penetration Testing page 18
Figure 2: Laboratory Vulnerability Test-Bed page 19
Table 4: Vulnerability Penetration Testing page 19
Vulnerabilities page 20

Interactive Assessment page 21
Phase 1: Network Reconnaissance page 22
Table 5: Network Reconnaissance Information Sources page 22
Phase 2: Network Identification page 23
Table 6: Signal Identification page 24
Phase 3: External Assessment page 25
Table 7: Minimum Team Requirements for External Assessment page 25
Table 8: Considerations for Route Planning page 26
Table 9: Observable Physical Network Vulnerabilities page 26
Phase 4: Internal Assessment page 27
Table 10: Internal Assessment Assignments page 27
Phase 5: Data Analysis page 28
Table 11: Targeted Vulnerabilities page 28
Phase 6: Vulnerability Neutralization page 29
Customized Passive Assessment Linux Distribution page 29
Stage 1: Initial Software Download page 29
Stage 2: Familiarization of File System page 30
Stage 3: Hardware Preparation page 30
Stage 4: Program and Menu Modification page 30
Stage 5: Creation and Insertion of Desired Modules page 31
Stage 6: Modification of Icons, Boot Options and Kernel File System page 31
Stage 7: Iso Image Creation and Testing page 32
Results page 32
Coast Guard Wireless Assessments page 33
Laboratory Test-Bed page 34
Wired Equivalent Privacy page 34
Figure 2: WEP Recovery Testing page 34
Table 12: WEP Key Recovery page 36
Table 13: Injection Based WEP Key Recovery page 36
WIFI Protected Access page 36
Other Applications page 38
Assessment Methodology page 38
Customized Linux Distribution page 39
Conclusions page 40
References page 41
Appendices
Appendix A: Project Plan page A-1
Appendix B: Project Requirements page B-1
Appendix C: Support Plan page C-1
Appendix D: General Assessment Timeline page D-1

Appendix E: Assessment Assignments page E-1
Appendix F: External Assessment page F-1
Appendix G: General Test Plan For Laboratory Active Testing page G-1
Appendix H: Test Plan page H-1
Appendix I: Design Specifications page I-1
Appendix J: The IEEE 802.11 Standard page J-1

Introduction

In a post 9/11 and post Katrina environment the Coast Guard is looking for cheap effective methods for providing the Coast Guard Data Network Plus (CGDN+) to a very mobile and adaptable service. Although the Coast Guard has traditionally relied on permanently established wired networks as the backbone of the CGDN+ network, wireless networks have generated a large amount of interest because of their many benefits. Wireless networks provide a cost efficient method for distributing and managing a network. A wireless network can be adapted to meet the changing needs of the organization quickly and efficiently, be used to establish temporary mobile networks, and isolate different user groups from each other. These benefits provide the flexibility and control necessary for network administrators to easily manage a network.

Although wireless networks provide many benefits, security remains a major concern for networks that store vulnerable data. The Coast Guard daily uses its CGDN+ network to distribute sensitive data such as social security numbers, medical records, and extensive personal information of its members. The network also disseminates logistical and readiness information, such as the schedules of high ranking officers, cutter locations, and supply information, that requires robust security measures.

Wireless networks are vulnerable to weaknesses that can be exploited by malicious network attackers, known as hackers. Hackers have the ability to penetrate networks through common vulnerabilities and are able to then capture, modify or destroy data from within the network. Hackers cause billions of dollars of damage each year through data destruction and network reconfiguration [1]. Both wired and wireless networks are targeted by hackers, but wireless networks typically have more exploitable vulnerabilities.

One of the most effective methods of managing the security risks is provided by a wireless network vulnerability assessment. A wireless network vulnerability assessment is a set of procedures that use software tools to help network administrators identify weaknesses within a wireless network. A network that is not properly set up leaves itself vulnerable to unauthorized users exploiting these weaknesses. Vulnerabilities can be identified and secured prior to installation with a proper assessment methodology, which makes the network more secure. This project focuses on identifying the hardware, software, and procedures necessary for the collection and analysis of network data to accurately identify vulnerabilities (APP B).

The Telecommunication & Information Systems Command (TISCOM) has identified the need for a standard method of establishing and maintaining a consistent level of security prior to deploying wireless networks. This project will draw on the experiences and techniques learned during a cadet internship at the National Security Agency (NSA) to determine the current state of Coast Guard wireless networks, identify existing vulnerabilities, and providing the Coast Guard with a standard methodology for assessing wireless networks (APP A). Passive assessments will be conducted on Coast Guard facilities to identify existing vulnerabilities as well as test the tools and methods proposed in the methodology. The results from the passive assessments was then used to develop a laboratory test bed for investigating active testing tools and methods. The passive assessments and the laboratory test bed work then were combined to create an assessment methodology tutorial and a Linux distribution toolset to provide network administrators with the tools and techniques necessary to identify security threats.

The first phase of the project was devoted to setting up and completing passive wireless network assessments on Coast Guard installations and establishing a laboratory test bed. Research and

work was focused on developing a customized Linux distribution assessment tool kit and Coast Guard specific vulnerability assessment methodology during the second phase of the project. This paper will first provide basic definitions to common wireless network terms and concepts. Specifically, proper wireless network configuration and operation, security protocols, authentication and certification, passive data collection, security vulnerabilities, and active attacks will be explored and discussed. Next the paper will explain why the Coast Guard needs a wireless vulnerability assessment set of tools and techniques as well as the steps required to provide the Coast Guard with an assessment methodology. The paper will then describe how the project determined what elements would be used to provide a trial tested assessment methodology. This section will focus on the establishment of a laboratory test-bed, the creation of an interactive vulnerability assessment methodology, and the development of a customized Linux toolset distribution for Coast Guard usage. Finally, the progress completed on the project will be discussed, which will include the current state of Coast Guard wireless assessments, the assessment methodology and its Linux distribution, and the laboratory test-bed.

Background

TISCOM sponsored this senior design project to identify wireless network vulnerabilities and develop a methodology to manage and minimize wireless network security concerns. In 2005-2006, TISCOM sponsored a cadet design project to develop a wireless enterprise solution for implementation across the Coast Guard. That project focused on determining the necessary hardware requirements and configuration for developing a wireless network. This current project concentration is on establishing and maintaining a secure wireless network. Wireless network basics, vulnerabilities, and vulnerability exploitation methods will be discussed in this section.

Wireless Network Configuration and Operation

The structure of a wireless network is based upon a client's connection to a server through a wireless access point (AP). A generic wireless network consists of client computers, an access point, and a server acting as a Local Area Network (LAN) to a router and the Internet (Figure 1).

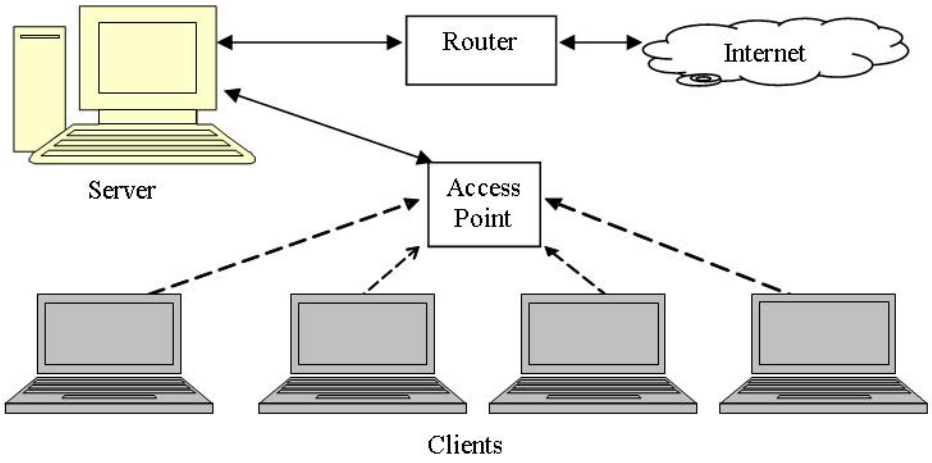


Figure 1: Generic Wireless Network

Computer servers govern the internal operations of the network on which legitimate clients operate. A legitimate client is any electronic device capable of connecting to a network in accordance with the server settings. An AP acts as the wireless contact point between a server and a client [2]. Clients and access points are both identified on a network based on their Basic Service Set Identification (BSSID). A BSSID is a 48 bit alphanumerical code that acts as an identification number for individual access points and clients [3]. Data is transmitted at small increments, known as data packets, on radio frequencies (RF) between APs and clients. The methods used to secure these packets are the key to the overall wireless security.

Each packet contains the address of both the sender and the receiver along with security information that enables transmission through an encrypted network. Data packets can be

captured by outside computers and used to gain unauthorized access to the network. The security of data packets, along with the network itself, depends upon proper system configurations and security protocols.

As the name implies, access points are devices that provide access to a network for either a wired or wireless client. Wireless network data packets are transmitted from the client using radio frequencies and are received and converted back into data packets at an access point. The capture of data packets can not be prevented because wireless networks publicly transmit data packets using published radio frequencies. Data within a packet can be secured by following specific security protocols. A protocol is a standard of operation for a network [4]. Several security protocols, such as the Wired Equivalent Protection (WEP), Wi-Fi Protected Access (WPA), and WPA2, are discussed in further detail below.

Security Protocol

Wired Equivalent Protection

Wired Equivalent Protection (WEP) is one of the earliest protocols implemented for wireless security [5]. WEP implements a the RC4 stream cipher algorithm to produce a 128 bit encryption and bit key stream random number generation [6]. This means that WEP uses 104 bits to create random sequences that correspond to the actual data being sent using RF. The remaining 24 bits make up the initialization vector (*iv*), which is the secret key that has been used for encryption and must be used again for decryption [7]. Because the *iv* values are transmitted with each packet, a 128 bit WEP encryption can be broken within 4 hours using openly available software. WEP provides little to no protection and lulls network administrators into a false sense of security.

WI-FI Protected Access

The Wi-Fi Protected Access (WPA) was developed to provide increased security in response to WEP's vulnerabilities. WPA uses the same encryption system as WEP in combination with the temporal key integrity protocol (TKIP) [8]. TKIP will constantly change the key used to encrypt and decrypt wireless data. WPA protocol will theoretically change the key within the time frame it takes an attacker to recover it. This system was considered reliable until security analysis tools implemented dictionary comparisons to recover a WPA key before the key could be changed. A WPA decryption tool will analyze the configuration of the targeted network and then compare all possible passwords to a data base of alphanumerical combinations.

Advanced Encryption Standard

WPA2 replaced WPA with the addition of the Advanced Encryption Standard (AES) and message authentication code for increased security [9]. The AES encryption uses a pool of 3.4×10^{38} possible keys. It would take a computer, processing 2^{55} potential keys per second, 149 trillion (thousand billion) years to test all of the possible combinations [10].

The Air Fortress network uses the AES encryption to deploy a fully secure layer 2 gateway system [11]. Layer 2 refers to the data link layer of communications. A gateway acts as a network controller and orchestrates the secure transmission of data within the network. This system will be tested as part of the proposed secure wireless policy.

Authentication and Certification

Authentication determines a client's ability to access a network. Authentication is the process used to verify a computer's true identity through the use of electronic certification [12]. Certificates are issued by a trusted source, known as a Certificate Authority, and act as a passport

for entering a network [13]. For a client to gain access to a network they need to have their certificate accepted by the network. Networks contain verifiable certificates that enable clients to validate the network they are entering. This method of authentication provides protected network access. Protected network access does not determine the safety of data, but simply prevents access to the network database.

Passive Data Collection

Passive data collection is gathering packets as they are transmitted between a client and an access point. This action remains undetectable within the network and can be done with any wireless connection. Software applications, such as Omnipeak™, have been designed to analyze packet security data and provide vital information about the network. Omnipeak™ is an open source program that will provide network security, authentication, and protocol information based upon the collection of network data transmissions [14]. Information gathered using this program can be used to identify legitimate clients, network security protocols, and the extended service set IDs (ESSID) of the server, access points, and clients. ESSIDs clearly distinguish wireless networks by assigning the entire network with a unique "name" [15]. Passive data collection enables a user to obtain network information but not the actual data being transmitted within each packet. Algorithms have been implemented to encrypt data to prevent unauthorized viewing of transmitted data. The authentication and encryption process of a particular network is determined by the settings of its specific security protocol.

Security Vulnerabilities

Modern security protocols cannot prevent all vulnerabilities. Improper hardware configuration, unauthorized access points (rogues), ad-hoc networks, and excessive signal strength are four examples of simple, yet serious, security threats that go beyond the control of a protocol.

Rogue Access Point

A rogue access point is an unauthorized access point that is attached to a wired network to create an unsecured wireless connection. Rogue Access points are unsecured entrances to a network that are not configured to the proper security levels. Many times a rogue access point will have the default factory settings, which allow an attacker to completely bypass network authentication procedures.

Ad-Hoc Networks

Ad-hoc networks are networks made up of clients connecting to other clients until they find the server. The purpose of an Ad-hoc network is to increase the range of a network and minimize the need for physical access points by using client computers to act as the access point for other clients. Computers with wireless enabled cards continuously probe for wireless signals and automatically acquire a network connection when available. A server in this situation is unable to identify, authenticate, and certify all of the clients requesting access. This allows for an unauthorized user to gain access using the certification of a legitimate client computer.

Excessive Signal Strength

Excessive signal strength allows attackers to access the network well beyond its intended boundaries. Attackers will search for networks that have high signal strengths so they can access the network further away from the access point. They can use Ad-Hoc networks to reach the physical network from an even greater distance. Distance decreases the probability of detection,

allows the attacker to “hide” in the surroundings, and gives the attacker additional time for harmful activities.

Probing Laptops

Probing laptops are laptops with the wireless network connection turned on. Even if the computer is not running any program requiring a network, probing laptops seek out networks. Laptops set in this configuration mode may be granted access to a network through an Ad-hoc network and compromise that networks security integrity. Or the probing laptop can be directly connected to a network and give access to an unauthorized Ad-hoc client.

Low Level Encryption

Network security begins with the encryption that is being used to protect data packets. The WEP and WPA encryption protocols have known and documented vulnerabilities. Both commercial and open source software exists to allow unauthorized users the tools to decrypt and gain access to a “secure” network. Low level encryption protocols lull users into a false sense of security and complacency which attackers exploit.

Default Settings

Wireless access points are purchased from the manufacturer with default settings set for an open network with no security measures. Most basic users only require the ability to access their network and do not understand how to set up the security features properly. Manufacturers publish the user manuals and default settings publicly on the Internet, which allows attackers the ability to read and understand how the initial set up should be configured. Default settings are especially dangerous to a network when an unauthorized access point with default settings is placed on the network to create a rouge access point. This defeats the security measures being used by the network it is on and allows uncontrolled access to a network.

Active Attacks

An active attack is any action against a network that involves the transmission of data packets between the network and the attacker [16]. Although there is a wide range of active attacks, the Denial of Service, Man in the Middle, and Spoofing attacks are the most common and popular methods used.

Denial of Service

The most common type of active attack today is known as Denial of Service (DoS). A DoS attack floods a network with data packets that hinders or completely stops a network from carrying out normal operations [17]. DoS attacks do not involve gaining access to a network, but instead try to disrupt or temporarily shutdown a target network. DoS attacks can also be used to disrupt the network so the attacker can observe the network reestablish itself. During the reestablishment of the network the host and client reveal security information that an attacker can use to recover the encryption key.

Man in the Middle

A second attack, known as Man in the Middle (MIM), involves gaining access to network data without penetrating the network. A MIM attack is the routing of all data to and from a client through an unauthorized computer [18]. Attackers will first force a targeted client to log-off the network using a process called disassociation [19]. The attacker will then assume the identity of the server and prompt the dissociated user to log back on. The attacker then gains the username and password of the client and uses both to log into the server. The attacker will transfer data back and forth between the access point and the client in order to remain undetected.

Spoofing

Assuming the identity of a server or client to gain user names and passwords is known as spoofing. Spoofing is an attack in which an outside computer assumes the identity of either a legitimate client or network in order to obtain data from a targeted device [20]. It can involve a fake log on prompt window, website impersonation, or simply logging in with a known password or user name obtained in previous active penetration. Spoofing is a common attack that relies on unsuspecting users to provide log-on information, which is difficult to detect when using a wireless network.

Objectives

The primary objective of this project is to design a wireless vulnerability assessment methodology for Coast Guard deployment by the end of the 2007 Spring Semester. The assessment design consisted of full operation instructions, necessary equipment configurations, compiled software, and computer based tutorials for data analysis. The methodology was designed for a basic computer user with little to no experience with wireless vulnerability assessments and was based upon extensive wireless data analysis and assessment trials.

The assessment design was based upon data collected from existing Coast Guard networks and laboratory testing. Coast Guard network data was collected during assessments to identify existing vulnerabilities and gain the necessary experience to create a methodology specific for Coast Guard use. The assessments were also designed to simulate the costs, external considerations, and hardware and software considerations needed for an independent assessment team inspecting the network (APP C). Laboratory work will consist of active penetration testing of wireless network configurations. Data from both operations will then be used to develop a thorough methodology assessing the wireless vulnerabilities of Coast Guard networks.

Coast Guard Wireless Assessments

The first objective of the project was to assess Coast Guard networks to identify existing vulnerabilities. Coast Guard Headquarters and the Engineering Logistic Center (ELC) were identified by TISCOM as viable assessment sites for data collection. Networks operating in and around the facilities were identified and mapped using open source programs.

The goal of an assessment is to identify specific hardware and software vulnerabilities within a targeted network (Table 1)

Table 1: Target Vulnerability

Hardware	Rogue Access Points
	Improper Access Point Configuration
	Default Manufacturer Settings
Software	Exposed Encryption Packets
	Low Level Encryption
	Unauthorized Software

Each assessment was carried out in order to maximize data collection for the identification of theses specific vulnerabilities. A typical assessment consists of an external assessment on the first day followed by an internal assessment the second day (App D). Two complete assessments were carried out during the first semester of this project. Assessments were carried out to identify existing vulnerabilities, gather the necessary data for a laboratory test bed based on the existing vulnerabilities, and to develop the knowledge needed to conduct an assessment.

Identification of Existing Vulnerabilities

A Coast Guard specific vulnerability assessment methodology requires the identification of the vulnerabilities that exist currently within Coast Guard networks. Networking throughout the Coast Guard follows specific regulations, which creates a uniform network design with the same

general pattern of vulnerabilities. These two assessments provided data that allows the identification of these patterns, which are then analyzed to form the back-bone of the methodology.

Vulnerability Test-Bed Design

One of the base objectives of this project is to design a laboratory test bed to actively exploit Coast Guard specific vulnerabilities. The development of an accurate test-bed requires collection and analysis of Coast Guard network data. The assessment of Headquarters and ELC provided a diverse range of data, which resulted from the different network requirements for specific to each network. Headquarters does not deploy any wireless networking devices within its network, which made any wireless activity a vulnerability because it was unauthorized. In contrast, the only official Coast Guard wireless network is currently deployed at the ELC for inventory and product tracking purposes. The ELC network was analyzed and used as the basis of a Coast Guard wireless network. The results from both Headquarters and ELC provided the necessary data for the design of a Coast Guard modeled vulnerability test-bed.

Development of First-Hand Assessment Knowledge

The development of an efficient, and more importantly, a functional methodology is dependent upon the hands-on experience of the designer. The Headquarters and ELC assessments provided the group with the experience to plan and execute an effective vulnerability assessment. Through trial and error, the team members were able to identify the pit-falls and obstacles that face an assessment team. This was vital to develop a trial tested methodology to be provided to the Coast Guard for the identification of vulnerabilities in future wireless networks.

Customized Linux Security Tool Assessment Distribution

The second objective of this project is to devise a way of providing all of the necessary security software to the user in a comprehensive and organized fashion. The most effective method of meeting this need is the customization of a live Linux distribution. Linux is freeware-based operating system that is the result of the collaboration of computer programmers around the world. The Linux operating system is designed to be modified and customized for specific use. This flexibility in design allows the creation of a Coast Guard specific distribution for the deployment of passive wireless assessment tools.

The Linux distribution can then be launched directly from a live CD. A live CD is a fully independent operating system that is compressed onto CD or DVD media. A live CD allows for a portable operating system that can be deployed using any normal desktop or laptop computer. All Linux based assessment tools needed for the methodology can be organized and deployed directly within a Linux Live-CD. The assessment methodology was then based on the Linux distribution. Overall, the customization of a Linux distribution provides an organized method of passive security tool deployment that meets the requirements for conducting a Coast Guard vulnerability assessment.

Active Laboratory Test-Bed

A wireless assessment methodology is based upon identifying vulnerabilities that enable both active and passive attacks. Analyzing vulnerability penetration techniques provides the necessary knowledge to secure a network from attack. A laboratory test-bed allows for active penetration techniques within a closed network environment. This closed environment permits full testing without causing damage to operational networks. The test-bed will use network

configurations and vulnerabilities from existing Coast Guard networks and general wireless network configurations.

The test-bed must be modular, isolated from any external network, and use commercially available test equipment. For the test-bed to be modular the equipment needed to be interchangeable and the network be modifiable to simulate a vast array of network configurations. The test-bed needed to be completely isolated from any external network. Testing of active assessment tools may cause availability problems or damage to other networks and is minimized in the absence of outside networks. Finally, lab equipment needed to consist of commercially based equipment and that was analyzed using publicly available software. One of the goals behind the project is to identify the abilities of outside threats that have access only to openly available equipment. We did not analyze the capabilities of government designed and engineered equipment.

The test-bed was designed completely with commercially available laptops, access points, Direct Service Line (DSL) connections, and cables. All equipment fell within the 802.11 standard and complied with all planned network configurations. The assessment software was obtained from open source websites or public vendors. All network configurations were isolated from any other network within the lab. DSL connections were used strictly for data packet generation and not used for any external operations. The lab design fully met the necessary requirements.

System Design

The system design of this project wa based upon three separate segments that were combined to produce a trial tested assessment methodology (APP I). The first segment consisted of the design and construction of laboratory test-bed for wireless vulnerability exploitation. The

purpose of the test-bed was to provide a protected environment to understand the processes and network activity that was associated with vulnerability exploitation. The second segment of the design process was the creation of an interactive vulnerability assessment methodology that was accessible using a computer. The intention of this interactive tutorial was to provide a simple step-by-step guide that could be followed while using the assessment tool kit. The third part of the design process was the customization of a Linux distribution for Coast Guard wireless assessments. The reason for a customized distribution was to provide a completely passive network assessment software kit that met all the requirements to carry out the interactive assessment process.

Laboratory Test-Bed

The laboratory test-bed was designed and established using readily available commercial hardware components. The laboratory test-bed was designed for modular implementation using equipment listed in Table 2.

Table 2: Laboratory Equipment

Component	Type	Quantity
Cisco 1200	Access Point	1
Linksys 2.4 GHz	Access Point Router	1
Airfortress Gateway Security System	Wireless Gateway	1
Netgear 5-Port Switch	Internet Connection Switch	1
Domain Control Server	PC Desktop Computer	1
Wireless Intrustion Detection System (WIDS)	Intrusion Detection System	1
WIDS sensor	Wireless Sensor	2
Client Laptop	Computer	2

Each network component was chosen based on available resources, current Coast Guard approved equipment, and the necessity for wireless vulnerability simulation. The components were chosen to minimize project costs while maximizing the flexibility of the design.

The two types of access points used within the test-bed were the Cisco 1200 and the Linksys WRT54G. The Cisco 1200 series access point is currently approved to be used on the ELC wireless network. It was also readily available through the Academy's engineering department and TISCOM. The Linksys WRT54G access point is a multiple purpose unit that served as an access point for encryption testing and a router for multiple DSL grade internet connections. This device was also readily available through the Academy's Introduction to Electrical Engineering program. Each access point was incorporated into the design to comply with the Airfortress Gateway and WIDS system.

Testing the Airfortress Gateway system was vital for identifying the vulnerabilities of the current Coast Guard wireless network setup at the ELC. Two gateways are now available that were procured using TISCOM and Academy funding. The wireless intrusion detection system (WIDS) and sensors were made available through a previous wireless project being conducted at TISCOM. The WIDS will provide the foundation for future Academy projects involving active detection and neutralization of attackers within the network. The access points and security equipment described above were used within this project to provide the network security interface for the client and server computers. The client and server computers were chosen based mainly on available resources. The interoperable and modular nature of the equipment allowed the test-bed to be adapted to represent all applicable Coast Guard network configurations (Table 3).

Table 3: Network Configurations

Configuration	Description
Single access point network	Single access point connected directly to a server. Network is implemenated with one of the six possible encryption schemes
Dual access point	Two access points directly connected through a switch to the domain controller. Each access point can be configured with one of the six possible encryption schemes (36 combinations in all)
Secure Airfortress Gateway implementation (secured and unsecure)	Secure Airfortress Gateway used to control either single or dual access point configurations. The system can be tested given multiple security levels and mis-configurations.
Wireless Intrustion Detection System (WIDS)	The use of a wireless detection system used in conjunction with either single or dual access point configuration.
Airfortress and WIDS Implementation (Secure/Unsecured)	The use of the Airfortress Gateway in combination with the WIDS system under both secure and non-secure mode. This configuration can be used with either a single or dual access point configuration

Each configuration can be setup as an individual network or a combination networks within one system. The overall design of the network allows the deployment of the Airfortress, WIDS and one of the two types of access point arrangements for the simultaneous testing of three different configurations (Figure 2 on next page)

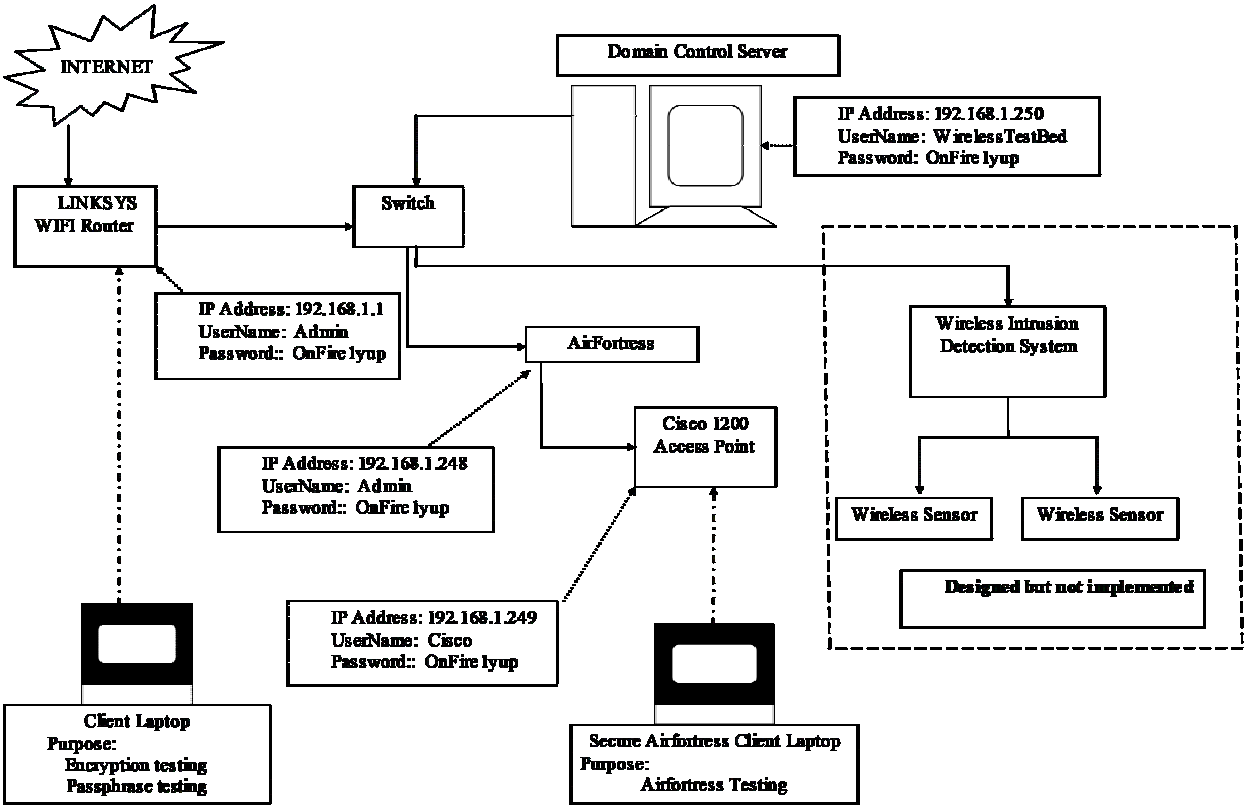


Figure 2: Laboratory Vulnerability Test-Bed

The network test-bed has been designed to address the following network vulnerabilities and the respective exploitation that the network faces. (Table 4).

Table 4: Vulnerability Penetration Testing

Network Configuration	Associated Penetration Tests
Rogue Access Points	WEP/WPA Key Recovery, MIM, DoS
Ad-Hoc Network Connection	MIM, DoS
Excessive Signal Strength	WEP/WPA Key Recovery, MIM, DoS
Probing Laptops	Spoofing
Low-level Encryption	WEP/WPA Key Recovery, MIM, DoS
Default Settings	WEP/WPA Key Recovery, MIM, DoS

The laboratory test-bed has been designed to be expanded and built upon as the complexity of attack software increases with the growth of technology.

Vulnerabilities

Although there were six main vulnerabilities were analyzed in this project the principal threat addressed was low level encryption. Current encryption levels, especially WEP and WPA, give the appearance of a secure network connection. The encryption key of both levels can easily be compromised using passive collection and data analysis tools. Once recovered, the encryption key can be used to gain undetectable access to the network. Movement within the network and the modification of database information can then be easily masked. Each access point was tested using the built in encryption protocols and was then evaluated using open source assessment tools. Decryption times were then compared to determine how long the software took to compromise each encryption level.

Rogue access points are difficult to simulate because by nature they are unauthorized and not necessarily configured. The largest threat rogue access points pose is the ability to use an illegal network connection while giving the appearance of a legitimate network administrated access point. The testing completed on low level encryption also covers the better case scenarios for a rogue access point. The next vulnerability similar in nature to rogue access points is Ad-Hoc network connections.

Ad-Hoc networks will be simulated by establishing a network using a secured access point and two laptops running in Ad-Hoc mode. Data collection and active penetration will be conducted by joining an attack computer to the ad-hoc network through one of the laptop clients. The attack computer uses the “host” client computer to gain access to the actual network access point through the Ad-Hoc network. Entry into the server will then be attempted through the access point and will simulate this attack upon both established network access points and rouge access points.

Another common method attacker's use, called probing, is designed to use the access granted to an authorized client to sneak past the security measures. For the laboratory test-bed, an attack computer will pose as a legitimate client and try to gain access to the network during the authentication of an authorized client. The simulation will be reset to include an Ad-Hoc network connection as another possible point of entry for a probe attack.

The final vulnerability that will be analyzed is default settings. Default settings are especially prevalent in access points because users do not realize that access points need to be initialized and set-up to have the encryption working. Most access points come from the factory without the encryption protocols activated, something that most users fail to realize and correct. For this test an access point will be activated straight from the box without any modifications and then penetration techniques will be used to gain access to the network. The automatic setup configurations offered by both Cisco and Linksys will be implemented and analyzed. Default settings represent the most significant vulnerability to a properly configured network and are the simplest to correct.

Interactive Assessment Methodology

The assessment methodology is broken down into seven phases for conducting an assessment (APP I). The first phase of the methodology involves gathering intelligence on the network. During the second phase the characteristics of the targeted network are identified and separated from all surrounding networks. Phase three and four involves the collection of internal and external network data. Data collected during phase three and four is then analyzed during the fifth phase to identify the specific configuration and settings of the network. During phase six

the specific network configurations and data is then used to identify existing vulnerabilities. The final phase involves the correction of network settings to help minimize existing vulnerabilities.

Phase 1: Network Reconnaissance

Network reconnaissance is gathering information from freely available sources. Any network information available to the public can be used to identify and exploit vulnerabilities. Four specific sources that are utilized by efficient network attackers are addressed in the methodology (Table 5).

Table 5 : Network Reconnaissance Information Sources

Reconnaissance Sources
Internet Search Engines
Governmental Document
Supply Vendors
Open Network Terminals

Internet search engines are the most widely used method for network information gathering used by attackers. The popularity of using search engines stems from the vast amount of information available that can be accessed anonymously. Information gathered using search engines have two purposes. The first is direct information that can be used to formulate a network attack. The second is to identify information that is available through the other three reconnaissance sources.

Governmental documentation of network configurations, equipment purchases, and administration is many times available to the public. Similar information is also available through contractors or supply vendors involved with the construction or maintenance of a network and may not be as readily available. Government, contractor, and/or vendor information can be used to launch a pre-planned attack, especially network configuration data is included in the documentation.

The largest source of network information is publicly available terminals within a facility. Customer service computers with a single remote network configuration can still be used to develop a systematic map of the target network. Attackers prefer this method for gathering information because it provides them with the raw network configuration without the need to actively attack the network.

Publishing small amounts of network information can be seen as mostly harmless, especially if it facilitates the maintenance and efficiency of the network, and therefore a justifiable thing to do. Small amounts of information can be collected to form a much larger picture, which can then be used to overcome the security procedures in place. The purpose of this phase of the methodology is to identify these information sources and to minimize their existence. Specific cases are addressed on a case by case basis.

Phase 2: Network Identification

Network identification is the systematic recognition of all available network signals that surround the targeted facility. Completing network identification is crucial for an assessment because it maximizes efficient data collection while minimizing the risk of unsanctioned network analysis. A targeted network in highly populated areas is normally operating amongst hundreds of outside networks. These signals overlap each other and form a congested area of signal traffic, which can make understanding collected data difficult. The purpose of this phase is to distinguish the network signals of the targeted facility from those being produced by outside networks.

A general overview of the area is first gained by driving through the targeted area surrounding the facility and observing network data traffic using Kismet. Kismet is an open source Linux

program that is designed to identify individual network signals. The signals of the targeted network are distinguished from outside networks using the following criteria (Table 6).

Table 6: Signal Identification

Network Mapping Criteria
Broadcasted network identification
Network signal strength
Packet rate transmission
Operation channels
Network frequencies

Broadcasted network identification is the most obvious method of network identification but is not always readily available. Some networks use a numerical based identification system that is indistinguishable from surrounding networks. Another method for identifying a network source is to observe the fluctuations in signal strength observed from an access point. As the signal strength rises the individual is approaching the access point and the team can observe the "hot" and "cold" areas to identify access point locations. Yet another network identification method is to identify the operating channels and networks frequencies being used. Signals within a network on different frequencies can easily be distinguished from one another.

Once the signals of individual target network(s) are identified, the assessment equipment can then be configured to filter out all non-targeted network data. This is vital not only to minimize the amount of unnecessary data traffic but to prevent the accidental collection and analysis of outside network data.

Another reason that filters are used is to protect assessment team members from being legally liable for any unauthorized network data. Assessments need to be officially sanctioned by the network administrator. A list of all officially sanctioned network identifiers needs to be read and understood by all team members so they have a base line for the filtering process. The filters protect the members of a team from any possible legal issues and let the teams identify and map

the target network. Once a network has been mapped, the assessment team can then proceed with the internal and external network assessment.

Phase 3: External Assessment

The external assessment is the collection of network data that is available outside of the physical structures of a targeted facility. The external assessment normally occurs prior to the internal survey because this order allows the assessment team to concentrate their efforts on buildings that were identified as having high levels of network traffic. This order can be modified depending on available resources and time restraints but requires a minimum of three team members (Table 7).

Table 7: Minimum Team Requirements for External Assessment

External Assessment Assignments	
Driver	Operates motor vehicle
Coordinator	Oversees operation and observes physical network vulnerabilites
Equipment Operator	Operates data collection program

The team will drive around the facility using a pre-planned route, which will later be plotted using Google Earth satellite based imagery. Google Earth is a mapping program that allows the user to plan a travel route based on specific latitude and longitude measurements. This program also allows the user to adjust travel routes based upon existing obstructions that are not indicated on a normal road atlas. The team coordinator will determine the most feasible route based upon specific characteristics of the facility (Table 8).

Table 8: Considerations for Route Planning

External Route Planning
Security check points
High traffic areas
Restricted areas
Road construction
Road blocks
Dead-end roads
One way roads

The main objective of the considerations is to efficiently use every roadway within the facility grounds along with a general sweep of the outside perimeter to cover the target network coverage. The outside perimeter should be determined by the network administrator. While conducting the external assessment of the facility, the assessment coordinator should be observing any physical vulnerability that exist either within the facility or along its perimeter (Table 9).

Table 9: Observable Physical Network Vulnerabilities

Physical Network Vulnerabilities

Vulnerability	Description
Local sit down coffee/eatery shops	Local shops normally offer free WI-FI service. This connection could be used as a cover to enter the network
External parking lots	Attackers can launch attacks or collect data without breaking trespassing laws
Waterfront areas	Mobile attacks can be launched by via a waterborne craft while engaging in fishing or other normal maritime activities
Residential area	Attacks via high power antennas can be operated within the cover of residential housing.

Throughout the entire assessment, the equipment operator should be observing the data being collected using the automated Kismet program. Equipment configuration and software setup is completed prior to the vehicle starting the assessment. The basic setup consists of a laptop computer running Kismet while simultaneously collecting GPS coordinates and network data packets (APP F). The main task of the equipment operator is to ensure that Kismet is collecting

a steady flow of data and also be observing for any abnormal network traffic. These observations are useful when faced with data discrepancies that may occur using Kismet.

Phase 4: Internal Assessment

The main purpose of an internal assessment is to identify the location of hardware based vulnerabilities such as rogue access points, ad-hoc connections, and illegitimate clients. An internal assessment is broken down based on the number of assessment team members and the size of the facility but the overall group is divided into two person teams (Table 10).

Table 10: Internal Assessment Assignments

Internal Assessment Assignments	
Equipment Operator	Operates data collection program
Observer	Maintains watch for hardware vulnerabilities and network configurations

The equipment operator will maintain the internal hardware and software configuration throughout the assessment. The freeware program "Omni-peak" has been chosen for internal data collection because Omni-peak has a user friendly interface and organized data reports for the user. The observer will watch for any visible network hardware or vulnerabilities as well as ensure the group maintains their pre-planned path through the facility. The pre-planned path is determined by the number of assessment teams and the number of targeted buildings.

Each building that is an internal assessment is conducted will be divided up based on the individual decks of the building. Each deck is further broken down into four equal quadrants, which will vary in size and shape based on the building being surveyed. Each assessment team will choose the most efficient path to cover each quadrant. Collected data should be saved upon the completion of each quadrant in a folder assigned to the deck that was completed on. Four files worth of quadrant data should be in each deck folder. Omni-peak should then be re-started

so that the data of each quadrant is isolated and therefore all for a systematic approach to data analysis.

Phase 5: Data Analysis

The data analysis section of the methodology is broken into two separate sections. The first section explains how to interpret the data that is obtained using Kismet and Omnipeak. Kismet provides raw data information without any statistical interpretation. Each category of network data collected using Kismet is defined along with its application in the assessment process. The tutorial then explains the process of interpreting the statistical data and graphs provided by Omnipeak. The second section of the tutorial is devoted to the identification of network vulnerabilities through the interpretation of network data. This section is concentrated upon fifteen targeted vulnerabilities and their associate network characteristics (Table 11).

Table 11: Targeted Vulnerabilities

Targeted Vulnerabilities
Rogue access points
External network access
Unidentified SSIDs
Man-In-The-Middle attack
Ad-Hoc network connections
Denial of service
Packet injection
Low-level encryption
Low-level passphrase
Default settings
Excessive signal strength
Leaking building signal
Unauthorized hardware configuration
Private computers in monitor mode
Unauthorized CGM+ connections

The final phase of the methodology explains the steps necessary to secure these vulnerabilities after being identified by the data analysis.

Phase 6: Vulnerability Neutralization

The fifteen vulnerabilities listed in Table 11 pose the greatest threat to wireless network security but are, ironically, the easiest to correct. Phase six is concentrated upon the step-by-step process to eliminate each of vulnerability listed in Table 11. Similar to the design of this overall project, each process is simplified into basic terms to accommodate an inexperienced computer user conducting the assessment and using the assessment methodology.

Customized Passive Assessment Linux Distribution

The design of the customized Coast Guard Linux distribution was based upon the design process of pre-existing security programs such as "Backtrack". "Backtrack" is an extensive security kit that was created using the base distribution SLAX. SLAX is a module based distribution that allows the user to customize Linux for any foreseeable purpose. Past distributions have concentrated on everything from business to graphic arts. The process of customizing SLAX involves seven stages (APP I)

Stage 1: Initial Software Download

The first phase of designing a customized Linux distribution is to download an existing base Linux distribution, which can be found on the web. SLAX , similar to most distributions, is available as an iso image. An iso image is a compressed file system that provides high operating speeds and space efficiency, which is vital when trying to minimize the size of a distribution. All Linux systems are built using the same fundamental file system, which acts as a foundation for a customized distribution. The specific programs and files within this system are unique for each distribution. The user must go through the entire file system in order to properly customize a base distribution.

Stage 2: Familiarization of File System

The SLAX root file system is the standard file system used for all modern Linux distributions. Despite its universal Linux root file system, each individual configuration file, script, and program is unique within SLAX because of its modular design. This uniqueness requires the user to explore each file in order to identify its purpose and the available methods of modification. The iso image is extremely compressed and cannot be directly modified on the physical CD. Instead the entire image must be moved to the hard drive of a computer for file expansion and system manipulation.

Stage 3: Hardware Preparation

The computer used to create the distribution must have two partitions, which can be accomplished using any Linux partition software. This project used the G-Parted free program because it is very efficient at partitioning a computer. The first partition is 7 gigabytes and was used to store the entire distribution that was expanded from its iso image. Direct file configuration requires that the iso image be fully expanded into its original 3 gigabytes size. The extra 4 gigabytes are used for additional files, programs, and compression work. The second partition is 3 gigabytes and is used to create and store the test iso images after it has been compressed within the 7 gigabytes partition. Files can be customized within the SLAX distribution once the original distribution has been expanded onto these hard drive partitions.

Stage 4: Program and Menu Modification

Menu modification is important because it will simplify the distribution for the novice computer user. The menu consists of the taskbar selection button that allows a user to access all available programs. All programs that are not involved with the distribution are eliminated along with their menu options. This will minimize the size of the distribution while focusing the user's

attention on the tasks at hand. A simple user interface will help simplify the explanations within the methodology.

Stage 5: Creation and Insertion of Desired Modules

The SLAX distribution is module based. Modules are Linux programs with specific compression and file information added prior to being inserted into SLAX. A designer will layer these modules like bricks to build a distribution with desired functions and programs. Modules are created by modifying a Linux program for custom use, compressing it, and running specific scripts within the existing SLAX distribution. Modules are added within a designated file called /modules. These module file systems are then loaded automatically into the current iso image whenever a user boots up the distribution within a host computer.

Stage 6: Modification of Icons, Boot Options and Kernel File System

The distribution desktop icons that represent file system shortcuts are modified to represent the different aspects of the methodology. This is done through image manipulation and the creation of desktop modification modules. These modification modules are loaded along with all other modules upon booting up the host computer. In addition to desktop icons, boot options are modified in accordance to the desires of the user. Boot options are the customized settings that are executed when a distribution is initially loaded onto a computer. The project's Linux distribution was programmed to boot directly to random access memory because it enables full use of the CD drive during the assessment. Boot option modifications are done within designated script files that process the initial boot commands. The final modification in this process is customization of the base file system. The fundamental file system needs to be modified based upon the desired hardware drivers, system information, and distribution options. File system modification is completed by modifying an existing file according to the instructions

left by the original programmer, but should be kept to a minimum to prevent fatal system errors. The final stage of the system design is distribution testing.

Stage 7: Iso Image Creation and Testing

The modified file system and overall distribution is compressed into an iso image, which will allow the entire file system to be on a single CD rather then a large DVD. SLAX scripts are available within the distribution that will help create these images. All options and modifications are tested by directly running the distribution within a laptop at least twice. Any discrepancies should be recorded prior to retesting. If the second trial is successful possible sources of the problem may be system or human errors. Further research on file configuration is then conducted if the identical error occurs.

Results

All objectives and project requirements have been met for the past two semesters in accordance with the final requirements document, which has been modified throughout the project in order to meet the needs of the project sponsor. TISCOM's final specification was that top priority should be given to the assessment methodology and Linux distribution. All test-bed construction and testing should be considered additional work to set the foundation for future wireless vulnerability projects.

The project was divided into two segments: assessment research and assessment design. The first semester of work consisted of researching and executing vulnerability assessments in order to develop the necessary knowledge and experience to create an efficient methodology. The second semester consisted of developing a laboratory test-bed to further research while simultaneously designing an assessment methodology and customized Linux distribution.

Coast Guard Wireless Assessments

Successful passive assessments were completed at Coast Guard Headquarters and ELC. Specific details from each assessment are for official use only and will not be detailed within this paper. All assessment descriptions have been kept to general details to prevent the targeting of Coast Guard networks. Any and all vulnerabilities that were found by the passive assessments were discussed with network administrators and have been corrected.

ELC has implemented the state-of-the-art Airfortress Gateway system. Our assessment confirmed that the ELC system is able to withstand passive data collection for decryption purposes. It is also currently configured to eliminate unauthorized network access. The assessment at Headquarters was based upon identifying all wireless network devices and mapping their signals.

All network data was carefully sorted and organized into a comprehensive report for each assessment site. All possible vulnerabilities were explained and connected to the collected data. The data and vulnerability analysis was then provided to TISCOM representatives for the final reports of existing wireless projects. These reports met the specified requirement of current Coast Guard vulnerabilities identification (APP B). Each assessment provided an extensive amount of planning, software familiarization, and assessment execution, which was then reviewed and discussed by the assessment team. Assessment team discussions allowed group members to identify the positive and negative aspects of the assessment and provided invaluable knowledge for the development of an efficient assessment methodology.

Laboratory Test-Bed

Wired Equivalent Privacy

The first phase of testing involving low level encryption testing was successfully completed. Testing was focused upon WEP and WPA encryption protocols. WEP keys were successfully recover at 64 and 128 bit encryption levels. The simulation involved the passive collection of data between a client and a server and was set up as is shown in Figure 2. The laptops that have the Coast Guard Academy Seal displayed are clients connected to the network through the Linksys access point (blue box with two antennas). The remaining laptop (black screen) is a passive attacker collecting the data packets being transmitted to and from the host and clients.

Figure 2-WEP Recovery Testing

The first phase of testing involved the simulation of normal network traffic using streaming video and audio data over a DSL line that was being transmitted using the Linksys WRT54G access point (AP). Data was captured from the AP, which was using a basic 64-bit WEP encryption, by the passive attacker computer. This simulation was based on a single hacker collecting data from one client. Approximately 800,000 packets were collected over the course of seven and half hours using the Linux based program “Airodump”. After this data was collected, the WEP key recovery program, known as “Airocrack”, was able to then recover the WEP key with less then one second of processing time.

To achieve more precise results, the methodology of data collection and analysis was modified. The first method is an efficient method for demonstrating what an attacker with limited battery life can accomplish, but is not necessarily the only method that must be considered. Most hackers will run the decryption tools and the data collection tools at the same time, which saves processing time and battery life.

The simulation of 128 bit WEP recovery consisted of the same network configuration used for 64 bit WEP recovery. The AP was reconfigured for 128 bit encryption and all data from previous experiments were removed from the system. Data collection was run simultaneously with ‘Airocrack” for a greater level of precision. By running them simultaneously, we were able to see the exact time taken to collect and decrypt the minimum amount of data packets to recover the WEP key. Table 4, on the next page, shows the information that was collected to recover the WEP key, namely the amount of data packets as well as collection and decryption times.

Table 12: WEP Key Recovery

WEP Key Recovery		
Encryption Level	64-bit	128-bit
Data Packets	800,000	378,324
Collection Time	7:30:35	4:37:05
(hours:minutes:seconds)		
Decryption Time	0:00:00	4:37:05
(hours:minutes:seconds)		

This test was then expanded upon through the use of packet injection. Attackers are able to increase the speed of data collection by using legitimate clients to inject an access point with data requests. This increased flow of data traffic dramatically decreases the time taken to collect data and increase the efficiency of data decryption. The first step of packet injection is the identification of a legitimate network client. Using the Linux based program "Aireplay", this client information is then used to "hi-jack" it's wireless card and inject packets into the local network access point. "Aireplay" is a packet injection program that will stimulate a wireless card to output continuous network information requests. The network then responds with data packets that contain the necessary encryption information for passphrase recovery. This process improved the data collection and passphrase recovery dramatically.

Table 13: Injected Data Rates

Injection Based WEP Key Recovery		
Encryption Level	**64-bit**	**128-bit**
Data Packets	**750,000**	**805,000**
Collection Time	**1:15:10**	**1:30:05**
(hours; minutes; seconds)		
Decryption Time	**1:15:10**	**1:30:05**
(hours; minutes; seconds)		

WIFI Protected Access

The laboratory test-bed was also used to decrypt and recover the WPA passphrase. A passphrase is a phrase that acts as the password to allow a client to gain access to the secure network. The

WPA passphrase is only exchanged between a client and the host during the initial stages of establishing a secure network connection, known as a handshake. A handshake begins by the client requesting authentication and sending its private code to the host network. The host network determines if the client is authorized before issuing its private key. The host network will encrypt its private key using the clients sent private key. Theoretically only the client will be able to decrypt this private key to establish a secure network by sending packets encrypted using the host private key.

An attack on a WPA encrypted network relies more on obtaining a complete handshake between the host and the client. To decrypt the WPA encryption the correct passphrase is required, which means an attacker can use a brute force attack. Brute force attacks use large dictionary files and programs to generate different combinations and derivations of common words and phrases to try to gain access to the network. Stored and generated phrases are compared with the captured handshake to identify the correct passphrase.

Decryption of the WPA passphrase requires the capture of a complete handshake. Decryption times therefore depend on the complexity of the passphrase being used and how extensive the dictionary file is. Passphrase complexity is broken down into three categories which also correspond with the amount of time required for successful decryption. Low level passphrases are simple phrases that use different combinations of letters (abcdef) and require between one second and one hour for decryption. Medium level passphrases are more complex phrases using alphanumerical (abc123) combinations and require one to three days for decryption. High level passphrases are extremely robust phrases of alphanumerical and common symbols (ab12!@) which have decryption times that are case by case dependant.

Open source dictionary files and phrase generating programs were used to test the WPA decryption methods. A simulated attacker observed a successful handshake and then began the process of determining the passphrase. Results varied and several different dictionary files were used before the passphrase was decrypted and the attacker gain unauthorized access. To speed up this process an open source phrase generator called Jack the Ripper was used to expand upon downloaded dictionary files to aid in identifying medium and hard passphrases.

Other Applications

The design of the test-bed has also helped to set the foundation for future projects involving wireless vulnerability. Future usages of this network include testing the AirFortress Security system and the Wireless Intrusion Detection System (WIDS). The test-bed also helped assessment team members to gain vital knowledge on network configurations and vulnerability exploitation necessary to meet the specified requirements even if not a specified objective.

Assessment Methodology

The assessment methodology has been constantly re-designed and modified throughout the semester to better meet the needs of an assessment user. The initial design concept was to create a Word based document with each page devoted to an individual step that would contain hyperlinks to general terminology and the next step of the assessment. This method proved to be extremely disorganized and did not provide the simplicity necessary to meet sponsor requirements. The second design concept was derived from the format of the vulnerability reports discussed in the previous section. Excel spreadsheets were used to organize the assessment process with the user navigating sequentially through a workbook. Each page was devoted to a specific step in the assessment process but proved to be very cumbersome. The user could easily become lost within the workbook and unknowingly miss entire sections. The

current design consists of a web-based application that can be viewed directly from a re-writable CD. This design allows the user to simultaneously view the tutorial while operating all the required Linux and Windows based security programs.

The final format of the interactive methodology consists of an extensive webpage built using Windows Publisher. The webpage is segmented based upon the six phases of the assessment design and the user can move through the assessment sequentially with their current location indicated on the side task bar of the webpage. This design meets the specified requirement of a simplified user interface. (APP B).

The assessment methodology has been simplified for the basic computer user is broken into several steps. The assessment first introduces the user to what an assessment is and the purpose of the methodology. Next, the user is provided with an extensive glossary of computer and assessment terms that can be referred to throughout the assessment. The tools are then introduced to the user using photos and general descriptions. Once these sections have been reviewed, the assessment team can then proceed directly into the assessment process. All the information of previous pages can be reviewed with a simple click of the button. This flow of information meets the second specified requirement of a simple methodology process that can be followed by a basic computer user (APP B).

Customized Linux Distribution

A large amount of time was devoted during the second phase of the project to the design of a customized Linux distribution. The final customized process involving SLAX was determined after working with over ten base distributions and seven different compression and modification processes. The final customized Linux distribution is a compressed operating system that is completely concentrated upon passive wireless data collection and analysis. All unnecessary

programs have been eliminated to minimize the size of the distribution, which allows the distribution to be placed upon either a blank CD or a small USB memory drive. The passive assessment programs have been organized in sequential order to correspond to the steps of the assessment methodology, which further simplifies the process for the user. The overall design and final product far exceeds the sponsor determined requirements.

Conclusions

The Coast Guard would benefit from the applications of wireless networks such as cost effectiveness, improved efficiency, and mobility. However, the deployment of wireless networking in the Coast Guard requires a consistent level of data security. The CGDN+ network stores sensitive data and requires robust security measures to ensure data protection and integrity. The purpose of this project is to provide the Coast Guard with a wireless vulnerability assessment methodology in order to effectively evaluate the wireless security. Project work was focused on performing assessments on Coast Guard installations, active laboratory work involving wireless vulnerabilities, and an overall assessment methodology based upon the extensive data collected throughout the project.

The project was able to successfully complete passive assessments at Coast Guard Headquarters and ELC, establish a laboratory test-bed for active assessment and system design, decrypt and gain unauthorized access to a 64-bit and 128-bit WEP encrypted network within lab, decrypt and gain unauthorized access to a WPA encrypted network within lab, develop a Linux assessment tool distribution for passive assessments, and a user friendly assessment methodology tutorial. All work met or exceeded the requirements set out by TISCOM. It is recommended that work be continued on this project to establish an authorized Coast Guard wireless network, perform

active assessments on a Coast Guard network, as well as test the AirFortress Security system and the Wireless Intrusion Detection System. This current project was completed in May of 2007.

References

[1] Niccolai, James. "Analyst puts hacker damage at $1.2 billion and rising" 12 December 2006 http://www.infoworld.com/articles/ic/xml/00/02/10/000210icyankees.html

[2] Guo, F.; Chieuh, T.; "Scalable and robust WLAN connectivity using access point array". Dependable Systems and Networks, 2005. Proceedings. 28 June- 1 July 2005.

[3] Gast, Matthew S. 802.11 Wireless Networks. California, Oreilly & Associates. 2002 pg 55

[4] Hoferkamp, W, "A power and mobility-aware wireless protocol for ad-hoc networks". MILCOM 2000. 21st Century Military Communications Conference Proceedings. Volume 1, 22-25 Oct. 2000 Page(s): 292-296 vol.1

[5] Bittau, A.; Handley, M; Lackey, J.; "The Final Nail in WEP's Coffin" 2006 IEEE Symposium on Security and Privacy. 21-24 May 2006 Page 15.

[6] Bittau, A.; Handley, M; Lackey, J.; "The Final Nail in WEP's Coffin" 2006 IEEE Symposium on Security and Privacy. 21-24 May 2006 Page 15. .

[7] Bittau, A.; Handley, M; Lackey, J.; "The Final Nail in WEP's Coffin" 2006 IEEE Symposium on Security and Privacy. 21-24 May 2006 Page 15.

[8] Selim, Gamal, "New Protocol Design For Wireless Networks Security". Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference. Volume 1, 20-22 Feb. 2006 Page 4.

[9] Selim, G; Badawy, M; Abdul Salam, Mohamed; "New Protocol Design For Wireless Network Security". Advanced Communication Technology, 2006. The 8th International Conference. Volume 1, 20-22 Feb. 2006 pg 4.

[10] "Advanced Encryption Standard- Questions and Answers." Date accessed: 23 January 2007 http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html

[11] "Government Airfortress Technology" Date accessed: 15 December 2006 http://epsfiles.intermec.com/eps_files/eps_spec/airfortress_spec_web.pdf

[12] Gast, Matthew S. 802.11 Wireless Networks. California, Oreilly,& Associates. 2002 pg 120

[13] Al-Sulaiman, L.A.; Abdel-Wahab, H; "Cooperative cashing techniques for increasing the availability of MANET certificate authority services". Computer Systems and Applications, 2005. The 3rd ACS/IEEE International Conference on. 2005 Page 88

[14] www.omnipeak.com Date accessed: December 15, 2006

[15] http://www.cryer.co.uk/glossary/e/essid.htm Date Accessed: 23 January 2007

[16] "NSA Security Terms" Date accessed: December 15 2006 http://www.engineering.sdstate.edu/~salehnia/cs303/secterm.html

[17] Sherr, M; Greenwald, M; Gunter, Carl; "Mitigation DoS Attack Through Selective Bin Verification" Secure Network Protocals, 2005. (NPSec). Workshop on 1st IEEE ICNP. 6 Nov. 2006 Pg 7-12.

[18] Serpanos, D.N; Lipton, R.J. "Defense Against Man-in-the-middle Attack in Client-Server Systems" Computers and Communications, 2001. Proceddings. Sixth IEEE on. 3-5 July 2001 Page(s): 9-14

[19] Vladimirov, Andrew; Gavrilenko, Konstantin, Mikhailovsky, Andrei; WI-FOO The Secrets of Wireless Hacking Boston: Addison-Wesley 2004, pg 193.

[20] Guo, F; Chen, Jiawa; Chiueh, Tzi-cker; "Spoof Detection for Preventing DoS Attacks against DNS Servers" Distributed Computing Systems, 2006. ICDCS 2006. 26th IEEE International Conference on. 04-07 July 2006 Pg 27-37.

Appendices

Appendix A:	Project Plan	page A-1
Appendix B:	Project Requirements	page B-1
Appendix C:	Supporting Plan	page C-1
Appendix D:	General Assessment Timeline	page D-1
Appendix E:	Assessment Assignments	page E-1
Appendix F:	External Assessment	page F-1
Appendix G:	General Test Plan For Laboratory Active Testing	page G-1
Appendix H:	Test Plan	page H-1
Appendix I:	Design Specifications	page I-1
Appendix J:	The IEEE 802.11 Standard	page J-1
Appendix K:	Linux Distribution	page K-1

APPENDIX A: Project Plan

WIRELESS VULNERABILITY ASSESSMENT
PROJECT PLAN
October 12, 2006

Purpose: Access the present Coast Guard wireless network, identify current vulnerabilities, and design the methodology to secure both existing and future deployable networks.

Organization

Project Sponsor: TISCOM and NSA.

Project Advisor(s): LT. Moyer, LT Benin, Mr. Obrien

Team Member(s): 1/c Ryan Maca, 1/c David Pipkorn

Goal:

The main focus is identifying the security vulnerabilities that exist within the wireless networks of the Coast Guard Headquarters and the Electronic Logistics Center. Information assurance within the Coast Guard is vital given the expanding wireless and intelligence community. A lack of knowledge and experience entailing wireless security places this information at high risk. The overall project will concentrate on assessing current vulnerabilities and providing recommendations to secure them. The project will consist of a thorough assessment of the network utilizing open source software and commercially available hardware. The assessment will be based upon civilian and military personnel security threats.

Technical Challenges

Challenge 1: Develop the necessary knowledge and experience to complete a thorough assessment. Each team member will complete NSA (unclassified) specified open source literature and manuals. Practice assessment techniques on simulated networks.

Challenge 2: Collecting the necessary information and hardware to deploy a simulated Coast Guard Network. We will base the simulated network configuration on data collected during the passive assessments at both Coast Guard Headquarters and Engineering Logistics Center.

Challenge 3: Gaining adequate data from Coast Guard Headquarters may be a problem because Headquarters officially does not have a wireless network. Assessing is based upon rogue access point and the number of these access points will

determine the availability of data. We will be using laptop computers to walk through the buildings to collect data.

Challenge 4: Simulating and testing potential attacks on the simulated Coast Guard Headquarters and Engineering Logistics Center. These attacks should demonstrate what vulnerabilities exist with the current settings. These attacks will be conducted using both the settings for Coast Guard Headquarters and the Engineering Logistics Center.

Action Items/Responsibilities

1. Researching Engineering Logistics Center for passive and active assessments. Research will be based upon open source data collection on the Internet.
   Responsible: 1/c Ryan Maca

2. Researching U.S. Coast Guard Headquarters for passive and active assessments.
   Responsible: 1/c David Pipkorn

3. Design an assessment methodology for both passive facility surveys.
   Responsible: 1/c Ryan Maca and 1/c David Pipkorn

4. Provide project documentation by December 27, 2006 to LCDR Kuhn.
   Responsible: 1/c Ryan Maca and 1/c David Pipkorn.

4. Assembling test bed network for simulated active assessment.
   Responsible: 1/c Ryan Maca and 1/c David Pipkorn.

5. Design assessment methodology for active facility assessments (Feb. TBD)
   Responsible: 1/c Ryan Maca and 1/c David Pipkorn

6. Complete lab and field analysis (APR TBD).
   Responsible: 1/c Ryan Maca and 1/c David Pipkorn

Timeline

- Sep 20 : Initial Project Proposal
- Sep 25 : Project Website
- Oct 2 : Initial Research Project
- Oct 16 : Passive Assessment on CG HQ
- Nov 14 : Passive Assessment on Engineering Logistic Center
- Dec 18 : Fall Paper/Project Notebooks due
- Dec 27 : Documentation of Project Progress to LCDR Kuhn
- Feb TBD: Build Test Bed
- Mar TBD: Tentative Active Assessment
- Apr TBD: Complete Lab and Field Test Analysis
- May 7 : Spring Paper/Project Notebooks due
- May TBD: Spring Presentations

Project Members:

_____ Date: _____
1/c Ryan Maca

_____ Date: _____
1/c David Pipkorn

Project Advisor:

_____ Date: _____
LT Todd Moyer

Project Sponsors:

_____ Date: _____
LCDR (sel.) Roger Kuhn

_____ Date: _____
LT Lars McCarter

APPENDIX B: Requirements Specification

Wireless Vulnerability Assessment
Requirements Specification
October 23, 2006

Background: The Wireless Vulnerability Assessment project is based upon worked carried over from 1/c Ryan Maca internship at the National Security Agency. TISCOM requested an assessment on existing Coast Guard wireless networks setup in Head Quarters and the Engineering Logistic Center. The main goal of TISCOM is to identify vulnerabilities within wireless networks in order to justify the creation of an official wireless policy within Coast Guard regulations. A strong policy will help bring a secure transition from wired to wireless networks within the Coast Guard.

Problem Statement: Assess the security of current wireless networks implemented in U.S Coast Guard facilities. Identify existing vulnerabilities and exploit them within a controlled test bed. Based upon findings, design an assessment methodology that can be implemented for future wireless networks.

Requirements:

Level	Sponsor Need	Engineering Requirement	Justification
1	Identify hardware vulnerabilities within U.S Coast Guard network.		Reference 1
1A		Identify number of rogue access points (AP)	Same
1B		Identify improper AP setup locations.	Same
1C		Identify vulnerabilities due to manufacturing default settings	Same
2	Identify software vulnerabilities within U.S Coast Guard network		Reference 1
2A		Determine time necessary to bypass encryption levels	Same
2B		Determine exposed unencrypted data packets	Same
2C		Determine unauthorized software.	Same

3	Design a network assessment methodology for U.S Coast Guard implementation		Reference 2
3A		Provide a step-by-step guide that covers internal and external data collection, data analysis, and vulnerability identification procedures	Same
3B		Create a full assessment kit consisting of the following:	Same
3B1		Instructions for laptop setup with integrated GPS and antenna for external data collection	Mobility during assessment.
3B2		Instructions for antenna mounted laptop setup for internal data collection	Mobility during assessment.
3B3		Assessment software suite consisting of open source software for wireless data collection.	Open source is cost effective and proves what any level of computer user can accomplish on a network
3B4		Data analysis hardware and software setup based upon open source programs	
4	Demonstrate the necessity of securing wireless network vulnerabilities.	Create a test bed simulating the vulnerabilities found within U.S Coast Guard wireless and wireless networks in general.	Reference 3
4A		Test bed will be constructed using equipment available through the Academy's engineering department	Equipment needs to be readily available and within project budget restraints.
5	Provide recommendations for a	Create a document that	Reference 4

	USCG wireless policy.	recommends policy that will provide wireless security based on current network conditions.	

References:

1. Phone conversations with LCDR Kuhn of TISCOM at beginning of senior project.
2. Meeting with LCDR Kuhn at CGHQ on October 16-17, 2006
3. Teleconference with LCDR Kuhn during September 8th, 2006
4. Meeting with LCDR Kuhn and CDR Whiteman on October 17, 2006.

APPENDIX C: Support Plan

Wireless Vulnerability Assessment
SUPPORT PLAN
November 21, 2006

Purpose: The purpose of this project is to design a wireless vulnerability assessment methodology and a general wireless network policy for the Coast Guard. The project consists of assessing existing Coast Guard networks and identifying their vulnerabilities. The vulnerabilities of Coast Guard specific wireless networks will be exploited under laboratory settings. This data is then used to recommend Coast Guard Policy that will enable secure wireless networks throughout the Coast Guard. The collection and analysis of data also allows us to explore different assessment methods. This will allow for the design of a trial tested assessment methodology that can be deployed at any Coast Guard wireless location. The proper use of this methodology will ensure that the targeted wireless network remains within the proposed regulations and secure from outside threats.

Design Solution: We are proposing an assessment methodology that will allow the identification of wireless vulnerabilities in existing networks. We are also proposing a general Coast Guard wireless policy that will help ensure the deployment of future secure wireless networks. The assessment methodology will be based in accordance with the proposed regulations.

Support Considerations:

Economic:

1. Funding Source: Our funding source is TISCOM and the U.S Coast Guard Academy
2. Project Budget: The project budget is based on travel accommodations for assessment trips. It is also based on the purchase of necessary hardware and software for wireless assessments and laboratory setup:
    a. Travel: Funding required for each assessment varies based on team size
        a. 1 Cadet: $ 500
        b. 2 Cadets: $1000
        c. 2 Cadets, 2 advisors: $4000

    b. Costs of trips based upon:
        a. Transportation
            i. Flights
            ii. Rental car
        b. Hotel
        c. Paradigm
    b. Assessment Equipment
        a. Wireless cards: $50-$75
        b. Antennas: $75-$200

        c. Power sources (computer batteries, A/C adapters): $50-100
        d. Commercial assessment software: $1000
    c. Laboratory Setup
        a. Data analysis laptop : $2000
        b. Access points: $75-$500

Manufacturability:

1. Design construction: The vulnerability test bed will be constructed within the project lab by 1/c Maca and 1/c Pipkorn. LT Moyer and Chief Fournier will be technical advisors. No outside contract work is needed. It will consist of server computers, laptop clients, access points, and analysis computers. The vulnerability assessment kit will consist of applicable hardware.

2. Number of systems:
    1. One deployable assessment test kit prototype
    2. One laboratory vulnerability test bed.
3. Design construction concerns:
    1. Assessment kit
        i. Kit needs to be able to fit within a case that can be carried by single person and be within a reasonable weight range.
        ii. Kit components must be easily replace
        iii. Active assessment components of free-ware software must be disabled
    2. Laboratory set-up
        i. Simulate existing Coast Guard vulnerabilities

Sustainability and Reliability:

1. **Sponsor's sustainability and reliability requirements**: The assessment kit must be within a protective case. Components must be secured within the case. Kit should require little upkeep if used and stored properly

2. **Type and Quantity of Spare Parts**: Spare components will be stored within the assessment kit. Each component within the kit will have a spare to use while a new component is ordered.

3. **Spare Part Storage**: There will be two of each component within the assessment kit. Each kit will have ordering information for each component and recommended companies

Life-Cycle Costs:

There are no life-cycle costs for this project. The project will last for the Fall and Spring Semester of 2007 academic year.

External Considerations:

Environmental:

Environment Impact:

a. Computer battery disposal: The only concern is the proper disposal of computer batteries when they are no longer able to hold an adequate charge.

Equipment disposal:

a. All functioning equipment will be returned to the Academy's EE section. All malfunctioning equipment will be disposed of in accordance with CG regulations

Federal and State Regulations

a. All electronic equipment will be kept within the acceptable 2.4 and 5 GHz microwave ranges.

Health and Safety:

There are no foreseeable health or safety factors with our design process. The power of all signals will fall below the OSHA standard of the permissible exposure limit of the 2.4 GHz to 5 GHz range. Operators will not require training on heath risks involving final product.

Ethical, Social & Political:

This project is concentrated on securing wireless networks. At no time will active assessments be performed on networks outside the lab test bed without the written consent of the targeted network's administrator. This project in no way supports malicious acts against un-expecting networks.

Software Considerations:

Privacy:

Data will be collected using password protected computers that remain isolated from network connections during assessments. All data will remain For Official Use Only (FOUO) and will not be used directly in any public document. Data distribution and handling is described within the Security section.

Security

The following is the security document presented to each network administrator:

DATA HANDLING

Data Distribution

All collected data will be stored on DVD disks. The following parties will receive a copy of data:

1. Coast Guard Headquarters
2. National Security Agency
3. Coast Guard Academy

Data Security

Data will be kept completely confidential. All public reports will based upon the vulnerabilities that exist within open source wireless equipment. Coast Guard Headquarters will not be indicated as an assessment target. No connections will be made between any vulnerability within HQ and those discussed in project documents that will be viewed by anyone outside project work. Any deviation from these procedures will be discussed with and approved by customer.

DVD protection

DVDs will be kept secure following the guidelines set up by each agency within the data distribution list.

APPENDIX D: General Assessment Timeline

Day 1	Travel Day
Day 2	Assessment Day 1
0530-0600	Departure for Assessment site
0700-0730	Arrival at Network sight
0730-0800	Initial Orientation (Comparison To Maps)
	Note any changes in the plan given initial overlay
0800-0830	Initial Meeting With Network Administration
0830-1000	In brief with Network Administration
	Legal permission letters signed
	Information passed
0930-1030	Equipment setup
1030-1130	Start External Assessment
1230-1330	Compile external assessment
	Secure all external data
	Visually filter out external network traffic and identify
	data packets from targeted network
1230-1330	Break for Lunch
1300-1400	Begin Internal Assessment
1600-1800	End Internal assessment
1700-2000	Analyze all data
	Identify the following
	Access points
	Ad-hoc networks
	Admin Computers
	Client Computers
	External Networks
	Interference
	Plan out the next day's full internal assessment based on collected data

Day 3	Assessment Day 2
0430-0530	Departure for Assessment site
0530-0630	Arrival at Assessment site
0600-0700	Collect all initial log on information
0800-0900	Stop log on data and continue internal assessment from previous day
1130-1200	Stop internal assessment
1130-1200	Lunch
1200-1230	Assessment Debrief finalization
1300-1330	Debrief
1400-1430	Equipment Breakdown Collective Data storage.
1430-1530	Lockheed Lab work
1600-1700	Departure for Academy

Day 1
Travel

Day 2

0530-0600	Departure for Assessment site
0700-0730	Arrival at Network sight
0730-0800	Initial Orientation (Comparision To Maps)
	Note any changes in the plan given intial overlay
0800-0830	Initial Meeting With Network Administration
0830-1000	Inbrief with Network Administration
	Legal permission letters signed
	Information passed
0930-1030	Equipment setup
1030-1130	Start External Assessment
1230-1330	Comple exernal assessment
	Secure all external data
	Visually filter out external network traffic and identify
	data packets from targeted network
1230-1330	Break for Lunch
1300-1400	Begin Internal Assessment
1600-1800	End Internal assessment
1700-2000	Analyze all data
	Identify the following
	Access points
	Ad-hoc networks
	Admin Computers
	Client Computers
	External Networks
	Interference
	Plan out the next day's full internal assessment based on collected data

Day 3

0430-0530	Departure for Assessment site
0530-0630	Arrival at Assessment site
0600-0700	Collect all initial log on information
0800-0900	Stop log on data and continue internal assessment from previous day
1130-1200	Stop internal assessment
1130-1200	Lunch
1200-1230	Assessment Debrief finalization
1300-1330	Debrief
1400-1430	Equipment Breakdown
	Collective Data storage.
1430-1530	Lockheed Lab work
1600-1700	Departure for Academy

Device (s)	0900-1200	1200	1200-1500	1500	1500-Death
NSA Laptop(1-4)	Operating	Battery Switch	Operating	Battery Switch	Operating
CDX Car Laptop	AC/DC SOURCE CHARGING				
Tablet	Operating	Battery Switch	Operating	Battery Switch	Operating

APPENDIX F: Basic External Assessment Procedures

1	Download all electronic maps of the geographic area in which the network lies.

2	Take a preliminary drive around targeted network Observe the following
	a. Road Closings
	b. Surrounding facilities that may be carrying heavy wireless traffic
	c. Stoplights
	d. Heavily trafficked roads

3	Assemble assessment Equipment
	a. Run Kismet upon assessment laptop
	b. Hook up GPS receivers and omni directional antenna
	c. Assemble rig within assessment vehicle

4	Plan out final route for data assessment. Try for the following
	a. Continual movement
	b. Ability to slow down
	c. Avoid traffic
	d. Pre-filter channels around heavy external traffic

5	Engage Kismet packet collection program

6	Run planned route
	Modify when necessary

Basic External Assessment Procedures

1	Download all electronic maps of the geographic area in which the network lies.

2	Take a preliminary drive around targeted network. Observe the following
	a. Road Closings
	b. Surrounding facilities that may be carrying heavy wireless traffic
	c. Stoplights
	d. Heavily trafficked roads

3	Assemble assessment Equipment
	a. Run Kismet upon assessment laptop
	b. Hook up GPS recievers and omnidirectional antenna
	c. Assemble rig within assessment vehicle.

4	Plan out final route for data assessment. Try for the following
	a. Continuous movement
	b. Ability to slow down.
	c. Avoid traffic
	d. Pre-filter channels around heavy external traffic.

5	Engage Kismet packet collection program.

6	Run planned route. Modify when necessary

APPENDIX G: General Test Plan for Laboratory Active Test-Bed

The following security protocols will be analyzed.

1. WEP
2. WPA
3. WPA2
4. WPA Enterprise
5. Airfortress Technology

Each security protocol will be test with the following active attacks

1. Network key recovery
2. Spoofing
    a. Client
    b. Server
3. Denial of Service (DoS)
4. De-authentication of legitimate clients
5. Packet Injection
6. De-encryption of individual packets
7. Data-base recovery: simulation of stealing or modifying vital information within a database within a wireless network.

The following vulnerabilities will be tested under each protocol

1. Rogue access point
2. Ad-hoc network
3. Remote login
4. Default settings
5. Signal strength beyond the bounds of the intended network.
6. Probing clients
7. Stationary data collectors.

APPENDIX H: Test Plan

Wireless Vulnerability Assessment
TEST PLAN

Test #1 – Booting live distribution directly to random access memory (RAM)

Objective: Procedure will test that the Linux distribution automatically boots to the RAM disk of the host computer. This eliminates the need for the CD during test methodology and frees up the CD drive to record assessment data

Requirements:

1) Linux distribution must boot directly to random access memory (RAM) to free up available CD drive for recording information

Test Overview: This test is the first of a four part series. Each test builds off the previous test results. Test 1 evaluates the ability of the live distribution CD to be booted directly to RAM.

Test Procedure

1) Distribution setup:
    a. Hit power button on laptop (specific for each computer)
    b. During initial boot-up and prior to the windows log-on, hit the following
        i. For Gateway computers: F10
        ii. For Fujitsu computers: F11
        iii. For Dell computers: F12
    c. Boot options will appear
        i. Choose "CD/DVD/CD-RW Drive"
    d. System will go through automatic configuration. A static screen should appear within 10 seconds with the following information in the format below

    Expected Results:
    * Creating /dev entries for block devices
    * Setup directory for changes
    * Setup union directory
    * Looking for data modules
    * Live data mounted to mnt/hdc
    * Copying data to RAM, This may take sometime

Failing Result:
Failed boot to RAM will not be indicated by any error message. The system will automatically boot off the CD and none of the above messages will appear.

e. If information fails to appear:
   i. Re-boot system
   ii. When the initial command line screen appears, type “Slax toram”
   iii. Wait during boot-up operations
f. Upon log screen, enter the following in the respective areas
   i. User name: root
   ii. Password: toor
   iii. When a blank log on screen appears, type “startx”

Results

Test Success Level	

	Reasons For Failures
1	
2	
3	
4	
5	
6	

Test #2 – Wireless card configuration and initialization

Objective: Procedure will test that the Linux distribution can successfully configure and initialize a wireless card.

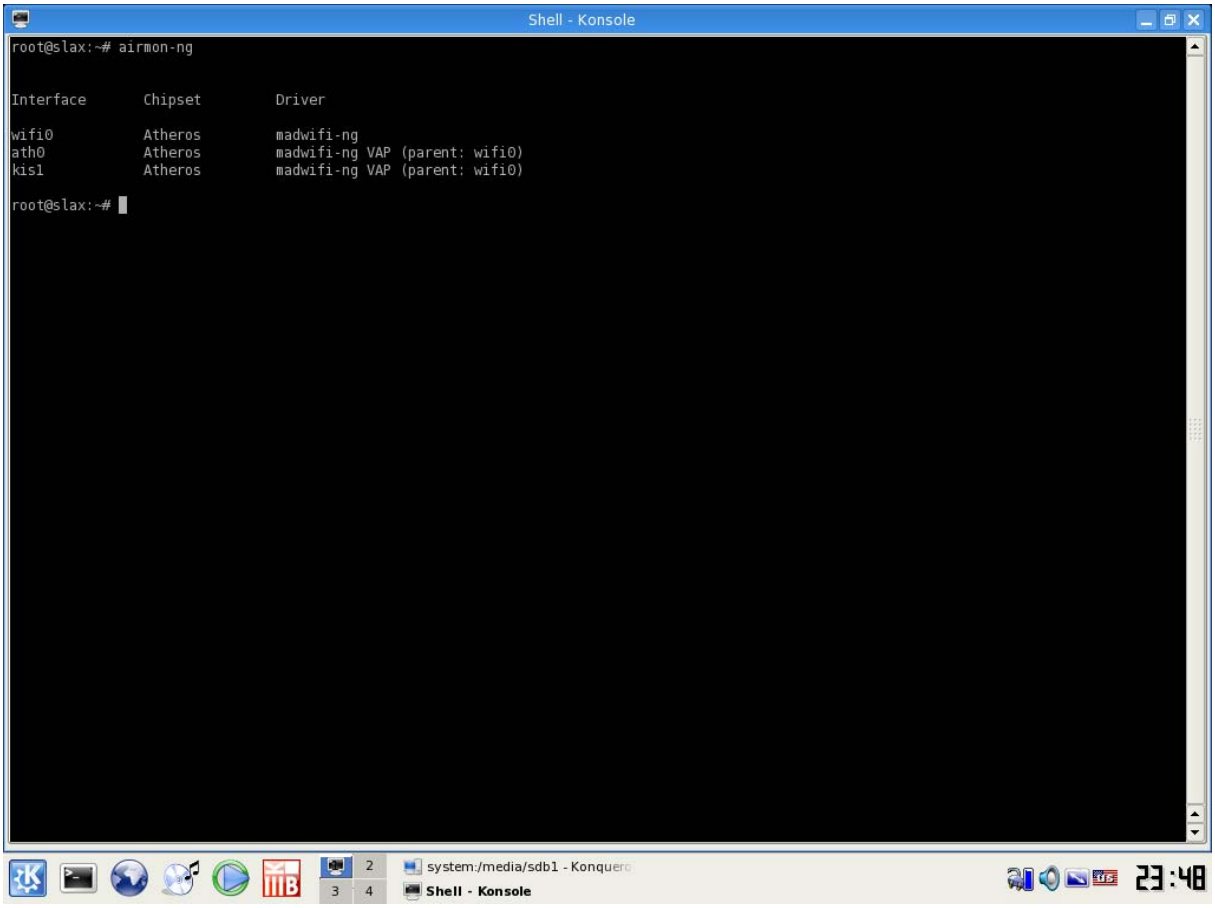
Requirements:

2) The Linux distribution must have the programs to detect and configure wireless cards That are placed within the valid PCMCIA slot.

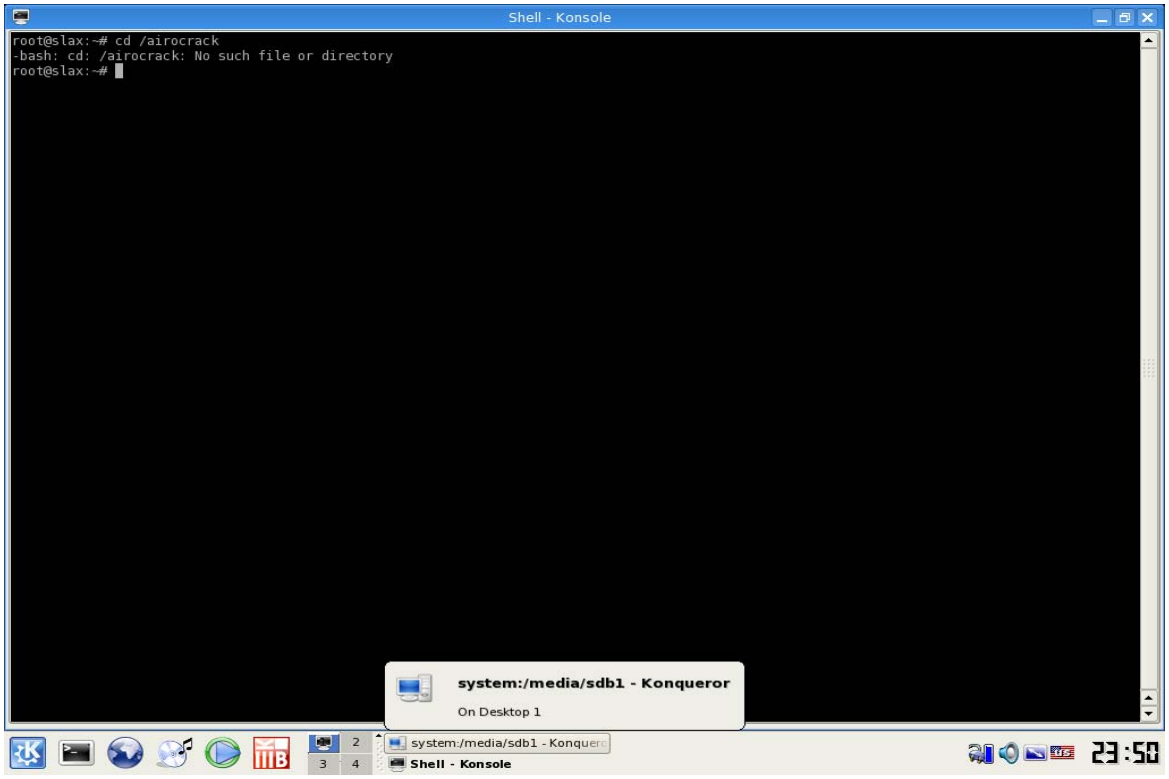
Test Overview: This test is the second of a four part series. Each test builds off the previous test results. Test 2 evaluates the ability to successfully configure and launch a wireless card for data packet collection.

Test Procedure

1) Open up a command prompt window. Open using the small computer Icon located at the lower left hand side of the screen (2nd icon).
2) Type the following command: airmon-ng
3) The following screen information should appear



4) The following error message will appear if program does not work correctly



Results:

Test Success Level	

	Reasons For Failures
1	
2	
3	
4	
5	
6	

Test #3 – Passive wireless packet collection program

Objective: Procedure will test that the Linux distribution has a fully functional passive packet collection program.

Requirements:

2) The Linux distribution must employee a program for passive data packet collection for both internal and external assessments. Packets must be associated with the following categories:
    a. BSSID
    b. Associate Network
    c. Operating Channel
    d. Network Signal Strength

Test Overview: This test is the second of a four part series. Each test builds off the previous test results. Test 2 evaluates the ability to successfully launch the passive data collection program "Kismet" from the live distribution.

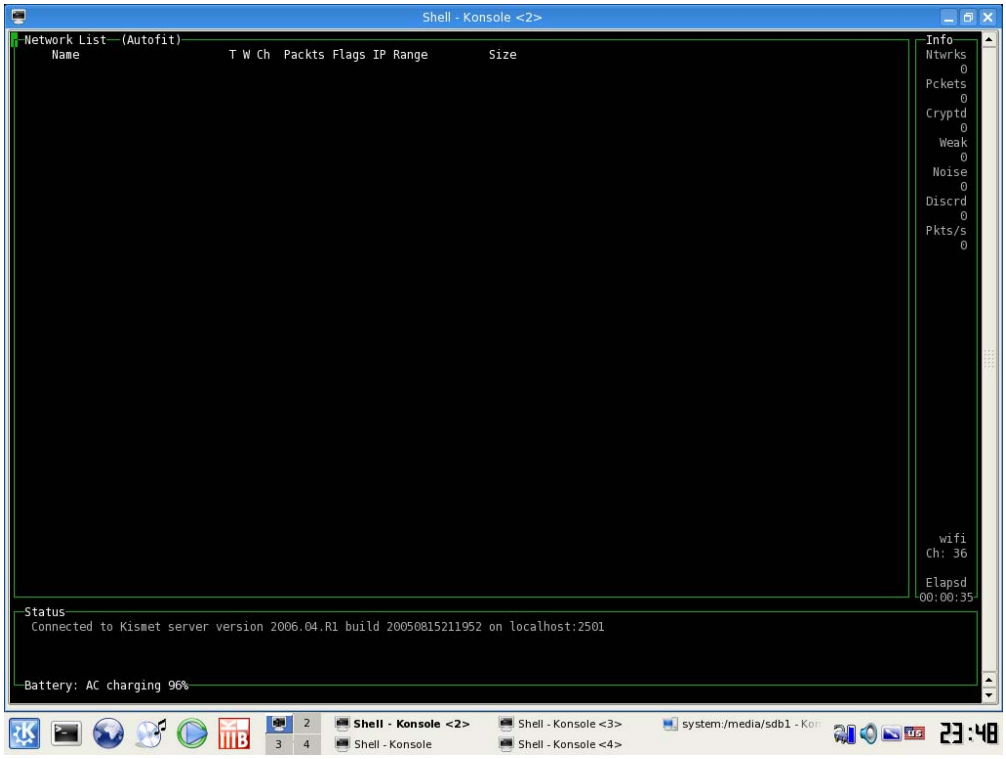
Test Procedure

3) Kismet Testing
    a. Enter task bar menu screen (K icon)
    b. Select "Wireless Security Suite" menu option
    c. Select "Kismet Program" within menu task bar
    d. Select desired packet storage location
        i. //root is recommended
    e. Confirm selection by hitting "OK"
    f. Confirm current wifi card selection
        i. If wifi card is unavailable
        ii. Open up a command line (small computer screen on bottom of task bar)
        iii. Type "airmon-ng start wifi0 –channel 6"
        iv. Should initiate desired wireless card

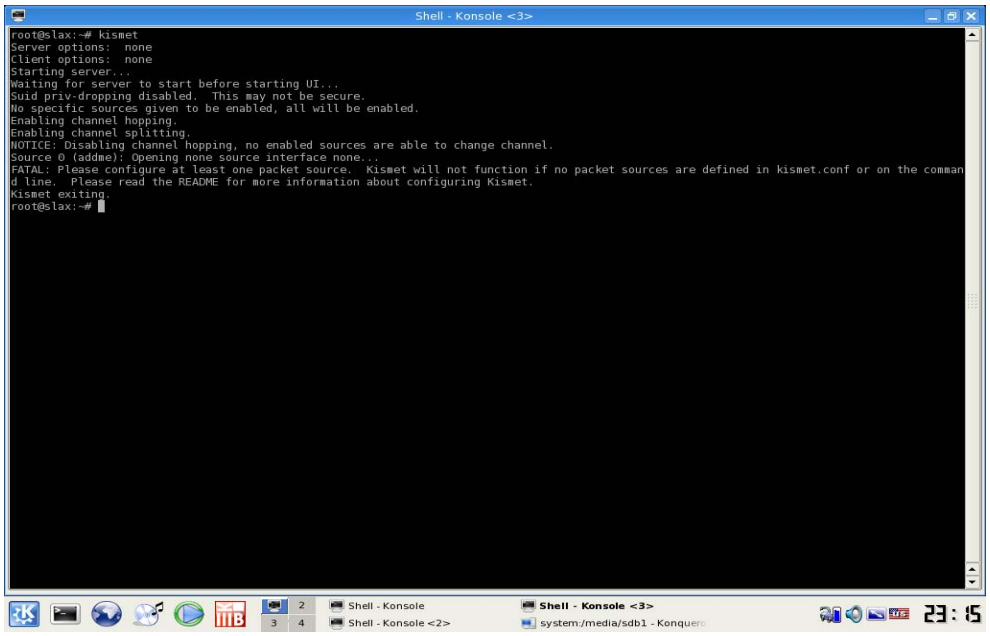
    g. Observe initial screen. The following information should be displayed
        i. Main window (Network List)
            1. Network name
            2. Frequency channel
            3. Level of noise within channel
            4. Number of packets collected
            5. Signal strength
            6. Packet size
            7. I.P Range
        ii. Side window (Info)
            1. Number of networks
            2. Number of total packets collected
            3. Number of encrypted packets

4. Number of weak signal packets
5. Noise level
6. Number of packets discarded
7. Packet Rate

Expected Successful Result



Failed Test Output



Results

Test Success Level	

	Reasons For Failures
1	
2	
3	
4	
5	
6	

Test #4– Saving collected data and Kismet output

Objective: Procedure will test that the files and data packets collected during passive surveys are saved to the proper file system.

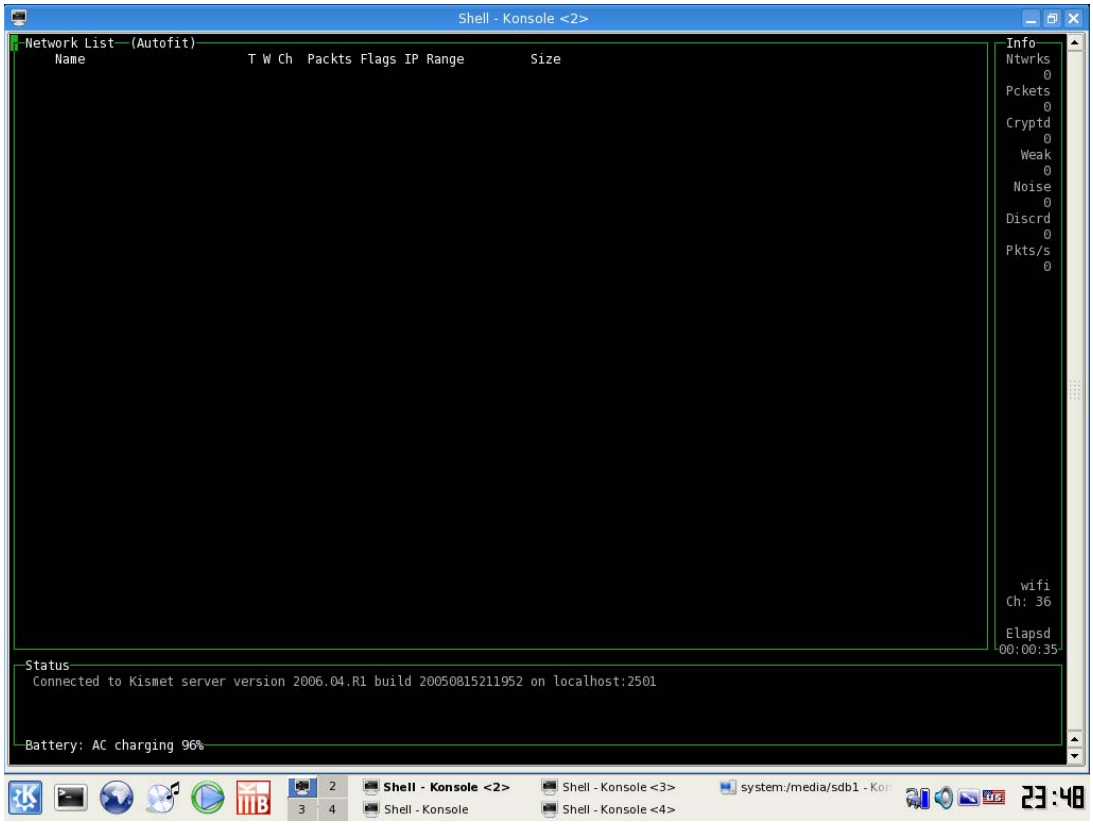
Requirements:

2) All kismet files must be securely saved for future analysis.

Test Overview: This test is the fourth test in a four part series. Each test builds off the previous test results. Test 2 evaluates the ability to successfully save data packets and network information collected during passive data surveys.

Test Procedure

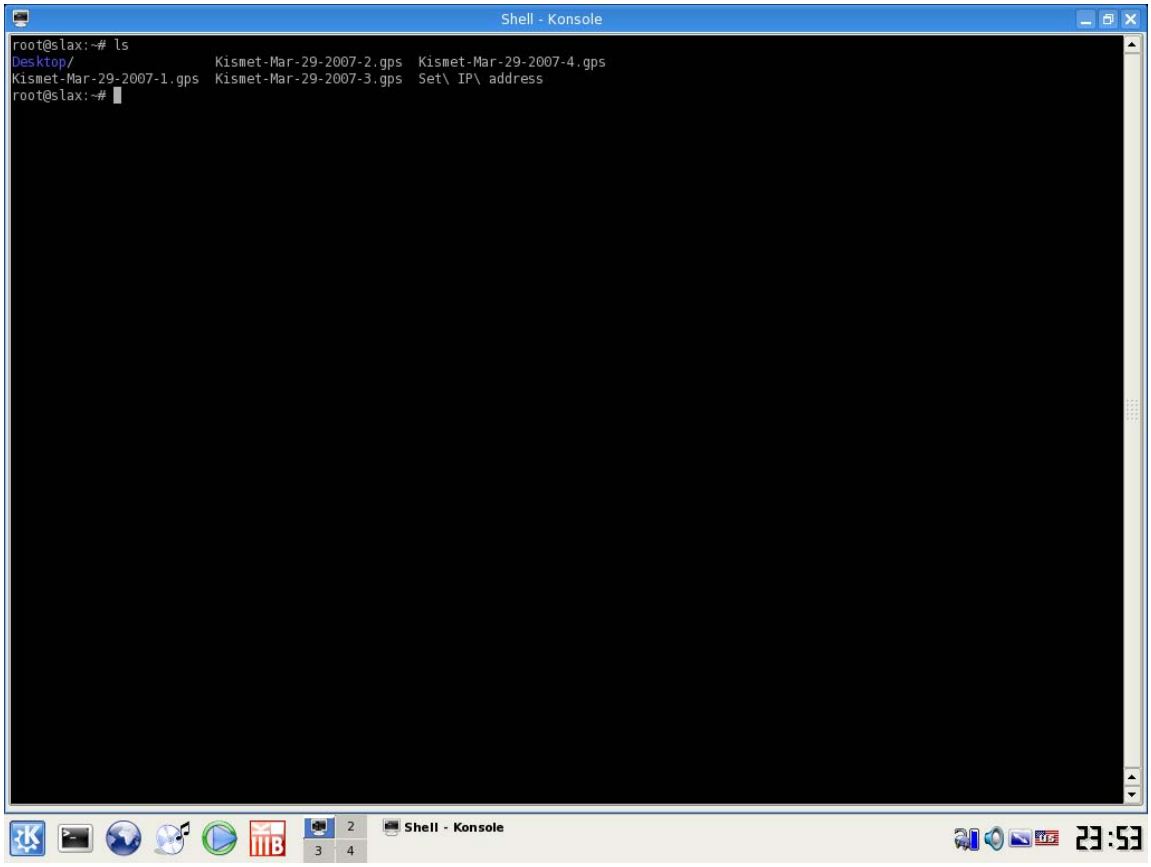
1) The Kismet window below should be open at this point in testing:



2) Type “shift-Q” on the keyboard. This will not be displayed on the screen.
3) Program should shut down and command window should automatically close.
4) Open up a command prompt window. Open using the small computer Icon located at the lower left hand side of the screen (2nd icon).
5) Type “cd /root”.

6) Type “ls” to list the current file system. The following information should appear on the command screen:

Expected Successful Results:



Expected Failure Results

The following systems folders will be the only ones within /root if the data packet information was not saved correctly.

a) Destktop/
b) Set\
c) IP\ address

Results:

Test Success Level	

	Reasons For Failures
1	
2	
3	
4	
5	
6	

Appendix I-Design Specification

Wireless Vulnerability Assessment Methodology

Design Specification

April 20, 2007

Purpose: The Coast Guard does not currently have a secure wireless configuration that provides maintainable security. The purpose of this project is to provide the Coast Guard with the methodology to perform vulnerability assessments for secure wireless networks. Project work consists of the following:

1. Conduction of wireless vulnerability analysis of existing Coast Guard networks.
2. Configuration of a wireless vulnerability test-bed.
3. Production of a customized Coast Guard Linux distribution,.
4. Interactive wireless vulnerability assessment methodology.

Design Solution:

A. Assessment Methodology

a. Flow Chart: Appendix 1.

b. Network Reconnaissance: Network reconnaissance is the gathering of network information that is freely available to the public. Network attackers use design configurations, IP addresses, administration identification, and hardware configurations found on the internet to identify and exploit network vulnerabilities. The first step of vulnerability assessment is to identify any network information that is available on the internet. This allows the network administration to take two actions:

i. Change all compromised network data
ii. Eliminate the source of network information on the internet.

This portion of the tutorial covers effective methods of network information gathering through

i. Internet search engines
ii. Government documents
iii. Social networks
iv. Commercial vendors
v. Network blog information

c. **<u>Network Identification</u>:** Network identification is vital for two main reasons:

i. Maintaining a legal network assessment
ii. Maximizing the efficiency of the assessment.

Assessment members must all be given permission from the network administrator to collect and analyze network data. Any unauthorized monitoring or analysis outside of the targeted network places the assessment team at risk. The purpose of network identification is to ensure that the assessment is concentrated only on the actual target. This part of the assessment involves the filtering of outside network signals through signal identification numbers, operating channels, and network data. Filtering will also focus the efforts of an assessment team and maximize the quality of data collected from the network.

d. **<u>External and Internal Network Assessment</u> :** Data collection and network analysis is separated into an external and internal assessment. The following information is collected during the external assessment

i. Signal strength relative to the radial distance from the facility
    1. Identifies the overlay of outside network signals onto the targeted network.
    2. Identifies the distances required to acquire network signals
    3. Identifies the distances required to recognize the network signal but not acquire a connection.
    4. Identifies network information and data available to surrounding public areas.

ii. Permits the GPS mapping of data signal information
iii. Measures the total signal perimeter of the network

The data collected from the external collection is then used to compare to the data collected within the physical structures of the targeted facilities. During the internal assessment, the network is mapped based upon wireless access points, legitimate client computers, and possible illegally connected hardware.

e. **<u>Data Analysis</u>**: Effective data analysis is vital in the identification of network vulnerabilities. This specific section of the methodology instructs the user on interpreting the following network data:

1. Signal strength.
2. Network identification codes.
3. Ad-hoc signals
4. Packet traffic levels
5. Log-on traffic.
6. Log-on patterns.

7. Bluetooth connection traffic
8. Wireless beacon strength and operational frequencies.
9. Peak network use in accordance with common network history.
10. Unidentified traffic and signal strengths of external networks.
11. External network overlay patterns.

The necessary insight is provided to understand how to interpret network information. The user is shown how to identify vulnerabilities based upon general patterns found within the data.

f. <u>Vulnerability Identification</u>: The purpose of this section of the methodology is to connect the data analysis performed in the previous section with specific network vulnerabilities. The methodology is concentrated on the identification of the following vulnerabilities:

1. Rogue Access Points
2. External Network Access
3. Unidentified SSIDs
4. Man-In-The-Middle Attack
5. Ad-Hoc Network Connections
6. Denial Of Service
7. Packet Injection
8. Low-Level Encryption
9. Low-Level Passphrase
10. Default Settings
11. Excessive Strength
12. Leaking Building Signal
13. Unauthorized Hardware Configuration
14. Private Computers in Monitor Mode
15. Unauthorized CGM+ Connections

Patterns in network data are then associated with each vulnerability. The user is shown how to connect specific network characteristics with existing vulnerabilities.

e. <u>Vulnerability Neutralization</u>: The purpose of this section is to instruct the user on how to correct the vulnerabilities identified during the previous recognition section. Each step is clearly defined along with methods used to prevent these vulnerabilities from occurring in the future.

B. Customized Linux Distribution

a. <u>Flow Chart:</u> Appendix 4

b. <u>Initial Software Download</u> : The first phase of designing a customized Linux distribution is downloading an existing base Linux distribution. A base distribution is any Linux operating system that can be found on the web. All Linux systems are built using the same fundament file system.

This fundamental system acts as the foundation for a customized distribution. The most efficient Linux file system format is known as iso images. An iso image is a compressed file system that provides high operating speeds and space efficiency. This is vital when trying to minimize the size of a distribution.

c. **Hardware Preparation :** The computer used to create the distribution must have two partitions. This can be done using any Linux partition software. G-Parted is a free program that is very efficient. The first partition is 7 gigabytes and will be used to store the entire distribution that has been expanded from its iso image. Direct file configuration requires that the iso image be fully expanded into its original 3 gigabytes size. The extra 4 gigabytes are used for addition files, programs, and compression work. The second partition is 3 gigabytes and used to create and store the test iso images after they have been compressed within the 7 gigabytes partition.

d. **Menu Modification :** Menu modification is important because it will simplify the distribution for the novice computer user. The menu consists of the taskbar selection button that allows a user to access all available programs. All programs that are not involved with the distribution have been eliminated along with their menu options. This will minimize the size of the distribution while focusing the user's attention on the task at hand. A simple user interface will help simplify the explanations within the methodology.

e. **Creation of Desired Module :** The SLAX distribution is module based. Modules are Linux programs with specific compression and file information added prior to being inserted into SLAX. A designer will layer these modules like bricks to build a distribution with desired functions and programs. Modules are created by modifying a Linux program for custom use, compressing it, and running specific scripts within the existing SLAX distribution.

f. **Addition of Modules to Distribution :** Modules are added within a designated file called /modules. These module file systems are then loaded automatically into the current iso image whenever a user boots up the distribution within a host computer.

g. **Modification of Icons :** The distribution desktop icons that represent file system short cuts are modified to represent the different aspects of the methodology. This is done through image manipulation and the creation of modules. These icons are loaded along with all other modules upon booting up the host computer.

h. **Modification of Boot Options :** Boot options are modified in accordance to the desires of the user. This specific distribution has been programmed to boot directly to random access memory. This enables full use of the CD

drive during the assessment. These modifications are done within designated script files that process the initial boot commands.

i. **Modification of All Kernel Files :** The fundamental file system needs to be modified based upon the desired hardware drivers, system information, and distribution options. This is done through researching the specific program on line and conducting file modification in accordance with the original programmer's instructions.

j. **Creation of Iso Image :** The modified file system and overall distribution are then compressed into an iso image. This will allow the entire file system to be on a single CD rather then a large DVD. SLAX scripts are available within the distribution that will help create these images.

k. **Iso Image Testing :** All options and modifications are then tested by directly running the distribution within a laptop. All discrepancies should be recorded. Try a modification twice and assume the initial error was caused either by human or system error. If the modification fails a second time, conduct research within the Linux search engine to identify the error. www.google.com/linux.

C. Test-Bed

a. **Flow Chart:** Appendix 5

b. **Linksys WRT54G Router/Access** Point:

   i. The Linksys acts as a network router which allows us to establish additional test networks. This entails using a new set of IP addresses from the internet network provider. With this we can manually set the IP addresses of the test network for greater control.

   ii. The Linksys router is also being used as a wireless beacon for client connection. This means that clients can gain access to the wired network over radio waves through the access point. This connection is then monitored using a laptop to gather network information and run test involving encryption, network connection control, and passphrase testing

c. **Netgear 5-Port Switch**: A switch is a connection device that allows multiple components to be linked together. The switch then ensures that information being passed reaches the specified network component. This improves processing speeds and data rates within a network while minimizing packet collisions.

d. **Domain Control Server**: A domain control server is a computer that is used to configure network components. This can be accomplished through

the supplied graphical user interface (GUI), serial connections, telnet access, or command line instructions.

e. **AirFortress Gateway**: The gateway controls client access to a secure wireless network. The gateway also provides an additional layer of security and encryption for the AirFortress network. The objective is to perform vulnerability assessments upon the gateway to help the Coast Guard determine its future use within its network.

f. **Access Control Server**: This software provides network administrators with the ability to rapidly establish, configure, and monitor an AirFortress network. This software is primarily used within the test-bed for updating the configuration files of multiple AirFortress gateways.

g. **AirFortress Client Software**: This software is used to secure a wireless user laptop/PC and provide the proper access identification necessary for the client to access the secure AirFortress network.

h. **Wireless Intrusion Detection System (WIDS)**: A WIDS system is a passive network of sensors that collect information from clients accessing a network. This system identifies questionable and/or suspicious behavior and denies service to offenders until a network administrator reauthorizes them.

Design Decisions:

A. Assessment Methodology

a. **Network Reconnaissance**: The network reconnaissance section of the methodology has been restricted to openly available network information. Openly available information is considered to be any network data available on the unsecured internet. The idea of the assessment is to analyze the vulnerabilities posed by outside sources utilizing freely available software. This allows those using the methodology to concentrate on securing vulnerabilities that pose the highest risk.

b. **Network Identification:** This section was separated from the external and internal network assessment sections because of the importance of network identification. Prior to any network assessment, data must be passively collected and all network signals within the area must be identified. This is vital to ensuring that the assessment is conducted in accordance with legal regulations. It also ensures that proper filters are implemented in order to completely concentrate efforts on the targeted network. This step is absolutely vital and needed to be treated as a separate entity.

i. **External and Internal Network Assessment :** The network methodology is divided into an internal and external assessment. This design decision was made because of the differences in network analysis activities while inside and outside of the physical structures at a facility. One of the main differences is equipment setup and software use. The separation of these two segments minimizes the number of hardware and software re-configurations. This then maximizes the efficiency of the methodology.

j. **Data Analysis**: Data analysis is based mainly on the information and network data provided through the Omnipeak program. This is a Windows based program that is used during the internal assessment. Omnipeak provides organized network reports on collected data that can be interpreted to identify known vulnerabilities. The output of Omnipeak is used because it provides an organized interpretation of data for basic computer users.

k. **Vulnerability Identification and Neutralization**: We have concentrated these two sections on the identification and neutralization of 15 specific vulnerabilities. These vulnerabilities were chosen because they pose the highest threats to network security. These vulnerabilities can also be corrected by following a list of commands that can be followed by the basic computer user.

B. Customized Linux Distribution

a. Linux Base Distribution : A base distribution is a pre-existing Linux operating system that is built upon using the original Linux kernel files and basic program scripts. The customization of a Linux distribution can be accomplished using one of three basic concepts that involve a base distribution.

i. Completely eliminating all excess files from an existing base distribution.
ii. Modifying an existing network analysis program.
iii. Create a distribution based upon the module distribution known as "SLAX". SLAX is a base distribution that is based upon individual module programs that can be combined to create a customized distribution.

The major design decision was to build the distribution based on the SLAX module distribution. This decision was based upon the following reasons:

i. SLAX provides a reliable base distribution that has a minimized amount of software issues
ii. Customized modules can be created that will minimize the s pace taken up by individual programs. This will minimize the size of the program overall and will decrease the time it takes to boot the distribution to random access memory. This will enable the user to use the CD-drive for data storage during the assessment.

iii. The majority of existing network analysis programs were created using SLAX. This is trial proven method of producing an effective customized Linux distribution.

l. **Linux Tool Selection:** The customized distribution was created with all software that is freely available on the internet. This minimized the cost of the distribution. All tools are for passive data collection and analysis. There are no programs within the distribution that will cause destruction of an operating network. This ensures the integrity of Coast Guard networks and any surrounding networks within the area of an assessment.

C. Wireless Test-Bed Design

m. **DSL Internet Connection:** The wireless test-bed is not allowed to be established on any Coast Guard network (CGDN or edu). The Electrical Engineering Department already has a separate DSL network connection that we used to meet this requirement.

n. **Linksys Router/Access Point:** The WRT54G Router/Access Point was chosen for several reasons.

i. Linksys can operate as a router and an access point. This means fewer components that can fail for easier troubleshooting.

ii. The Linksys is easily configurable by using an internet GUI. From here we can set the wired network settings, wireless network security settings, and control access to either network.

o. **Netgear Switch:** Necessary because the Domain Control Server PC only has one Ethernet connection. This component was favored over the Linksys built -in switch because the Netgear switch isolates the Linksys from other components. This allows for easier troubleshooting.

p. **PC Client Computer:** The AirFortress Client Security software was installed on a PC with a PCI card because of the unavailability of a laptop. A PCI card is used to allow a desktop PC access to wireless networks. This decision was made based upon funding available.

q. **ACS (Access Control Server):** The ACS Software was chosen to control the AirFortress network because it is designed to implement network-wide changes, has an easier user interface, and provides additional options for network configurations.

Requirements: The specific requirements of this project have been modified throughout the year. The following are the final requirements as agreed upon with TISCOM:

1) Create a Coast Guard Wireless Assessment Methodology

a. Must be tailored for the basic computer user.
b. Must provide the necessary steps to analyze and identify major network vulnerabilities.

2) Customize a version of the LINUX operating system for Coast Guard use.
   a. Must provide the necessary tools to carry out the assessment methodology.
   b. Must not contain any tools or programs for active network penetration tools.

3) Design a wireless test-bed to analyze wireless vulnerabilities.
   a. Test-bed operations must be isolated from any operational network.
   b. Test-bed must be module based. It must have the ability to be re-configured to analyze various types of network setups.

1) Requirement 1 has been met.

   a. The methodology has been tailored to the basic computer user by providing the step-by-step process for each aspect of the assessment in great detail. The tutorial fully explains the function and operational procedures for each piece of equipment and software. All command line prompt commands are provided along with instructions on how to initialize and operate all wireless tools within the customized Coast Guard distribution. A section of the assessment interactive tutorial has also been devoted to basic computer terms and definitions that provide the base vocabulary to follow the tutorial.

   b. The assessment methodology has been designed to instruct the user in the collection of the following network data:

      1. Publicly available network information
      2. External wireless network signals.
      3. Internal wireless network signals.

      The assessment methodology instructs the user in identifying the following major vulnerabilities based on the analysis of the collected data:

      16. Rogue Access Points
      17. External Network Access
      18. Unidentified SSIDs
      19. Man-In-The-Middle Attack
      20. Ad-Hoc Network Connections
      21. Denial Of Service
      22. Packet Injection
      23. Low-Level Encryption
      24. Low-Level Passphrase
      25. Default Settings
      26. Excessive Strength
      27. Leaking Building Signal
      28. Unauthorized Hardware Configuration
      29. Private Computers in Monitor Mode

30. Unauthorized CGM+ Connections

2) Requirement 2 has not been fully met.
    a. The distribution has all Linux tools required for the assessment. The internal data collection and analysis program "Omnipeak" though cannot be implemented within a Linux distribution because it is windows based

       Solution: The Linux distribution has been formatted into an .iso image. An .iso image is a compressed file version of the operating system that can be booted directly from a CD or run using a virtual machine. Virtual machine software (VMware) enables a windows operating system to run multiple operating systems simultaneously. The user will operate in Omnipeak within Windows for the internal assessment and switch directly to tools within the distribution through the virtual image that is brought up directly in Windows.

    b. The customized Coast Guard Linux distribution has no active network penetration software or tools. All software is for passive network collection and data analysis.

3) Requirement 2 has been met.
    a. The wireless test-bed has been designed to contain all penetration testing within the network. The only connection outside of the network is a DSL internet connection operated by the Coast Guard Academy. This connection is solely used for data packets and to simulate network activity for passive network observation and data collection. At no time does any testing go beyond the Domain Control Server or any access point. All active testing requires the network to be disconnected from the internet.

    b. The test-bed has been designed to be fully module. All hardware and access points are interchangeable. No permanent connections have been made. The network can be used to operate four different network configurations simultaneously for multiple vulnerability tests.

APPENDIX J: The IEEE 802.11 standard

The Institute of Electrical and Electronics Engineers (IEEE) is the leading global authority in electrical and computer engineering [i]. IEEE set the 802.11 wireless standards in 1989 in order to provide uniformity and compatibility in wireless networking as industrial interest rapidly expanded in the field [ii]. The IEEE 802.11 standard governs all aspects of wireless networks, ranging from operating frequencies to the configuration of wireless hardware circuitry. 802.11 is divided into different subsections, called protocols, based on system capability and operating frequencies as is shown in Table 1.

Table 1: Operating Protocols [iii]

802.11 Protocals		
Protocal	Frequency	Operating Speed
802.11a	5 GHz	54 Mbit/s
802.11b	2.4 GHz	11 Mbit/s
802.11g	2.4 GHz	54 Mbit/s

Wireless networks predominantly transmit on the 2.4 GHz microwave frequency band, which is heavily used by commercial and private based products such as microwave ovens and 'Bluetooth' devices[iv]. Networks operating in accordance with the 802.11a standard transmit on the 5 GHz band, which allows for less interference and a lower level of competitive signal traffic [v]. This project will concentrate on wireless activity on both the 2.4 GHz and 5 GHz bandwidth.

---

[i] "About the IEEE" Date accessed: 15 December 2006 http://www.ieee.org/web/aboutus/home/index.html

[ii] Boland, H; Mousavi, H; "Security Issues of the IEEE 802.11b Wireless LAN" Electrical and Computer Engineering. Vol 1, 2-5 May 2004..

[iii] "Wireless Networking" Date accessed: 15 December, 2006 http://en.wikipedia.org/wiki/Wireless_networking

[iv] Biggs, M; Henley, A; Clarkson, T, "Occupancy analysis of the 2.4 GHz ISM band" Communications, IEEE Proceedings. 24 Oct 2004.
[v] Kapp, S, "802.11a. More bandwidth without the wires" Internet Computing, IEEE, July-Aug 2002.

Appendix K– Linux Distribution

Customized Linux Distribution

Initial Software Download
1. Base SLAX distribution .iso image (www.slax.org)
2. Desired programs
   a. KISMET
   b. Airocrack
   c. Airodump
   d. MadWIFI Drivers
3. Pre-made modules

Hardware Preparation
1. Partition hard drive
   a. (1) 7 GB
   b. (1) 2.3 GB
2. Copy entire iso image to 7 GB partition
3. Place all modules onto 2.3 GB partition

Menu Modification
1. Deletion of unnecessary options
   a. Games
   b. System configuration
   c. Media
   e. OpenOffice

2. Addition of necessary program selections

Creation of Desired Module
1. Modification of existing Linux program.
2. Creation of modules
   a. Isolation of file
   b. Creation of module iso

Addition Of Modules To Distribution
1. Insertion of selected programs modules
   a. KISMET
   b. Airocrack
   c. Airodump
   d. MadWIFI drivers
2. Insertion of created modules

Modification of Icons
1. Creation of icons
2. Modification of icon file

Modification of Boot Options
1. Modifying the necessary boot scripts and command files

Modification Of All Kernel Files

Creation of Distribution Iso Image
1. All system file configuration saved as a module
2. Iso creation

Iso Image Testing
1. Burn current ISO image on CD
2. Boot directly to CD
3. Check modification
4. Run system check
5. Check the performance of all pre-made modules