# Laboratory Design for Wireless Network Attacks

Xiaohong Yuan Omari T. Wright Huiming Yu Kenneth A. Williams
North Carolina A&T State University
Computer Science department
Greensboro, NC 27411
(336) 334-7245
xhyuan@ncat.edu otwright@ncat.edu cshmyu@ncat.edu williams@ncat.edu

## ABSTRACT
There has been an increased awareness on the importance of a hands-on laboratory component in information security education in recent years. We developed a series of laboratory exercises for wireless network security. These laboratory exercises introduce to the students the following wireless network attacks: Wardriving, Eavesdropping, WEP Key Cracking/Decryption, Man in the Middle, MAC Spoofing, ARP Cache Poisoning, and ARP Request Replay. Open source tools such as Aircrack-ng, Cain and Abel, and Mac Makeup are used in these laboratory exercises to demonstrate how these attacks are conducted. The laboratory exercises were presented to two information security related courses at this university. The student feedback was very positive. Future work will include refining the laboratory design, conducting evaluation of the exercises extensively, developing more laboratory exercises for wireless network security and developing laboratory exercises for the Linux platform.

## Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General-security and protection; K3.2 [**Computers and Education**]: Computer and Information Science Education

## General Terms
Security, Experimentation

## Keywords
wireless security, WEP, network laboratory exercise

## 1. INTRODUCTION
Recent years have seen a large growth in the demand for computer security and information assurance education. There has been an increased awareness on the importance of a hands-on laboratory component in information security education. Laboratory experiments or exercises, laboratory-based courseware or courses have been developed for teaching computer and information security [1-5].

We developed a series of laboratory exercises for wireless network security. These laboratory exercises introduce to the students the following wireless network attacks: Wardriving, Eavesdropping, WEP Key Cracking/Decryption, Man in the Middle, MAC Spoofing, ARP Cache Poisoning, and ARP Request Replay. Open source tools such as Aircrack-ng [6], Cain and Abel [7], and Mac Makeup [8] are used in these laboratory exercises to demonstrate how these attacks are conducted. Understanding various wireless network attacks will allow the students to be better able to defend systems from those attacks. The students will also learn penetration testing techniques through using open source tools.

The laboratory exercises can be carried out by using laptop computers with wireless capability, and routers. The students can be paired up and each pair is given a router to carry out the laboratory exercises. This makes laboratory setup very convenient since the students do not need to go to a special laboratory. Laptop computers with the required software installed and routers can be brought to a regular classroom to carry out these laboratory exercises on wireless network attacks.

There have been different models for hands-on courses or laboratory exercises. Some use "cyberwar" exercises. For example, Wagner and Wudi [1] describe a cyberwar laboratory exercise in which students work in teams to secure a computer system and then try to gain access to other systems on the network. Hill et. al [2] describe the use of an isolated network laboratory to teach computer security, in which students work in persistent cooperative teams as either a black or gold team. Black teams attempt to break into other black team computers or attack the gold team. The gold team operates servers and attempts to defend their servers and role-play administrators. Some laboratory exercises avoid placing students in the role of attacker. Brustoloin [3] describes a sequence of laboratory experiments on network security that cast students successively in the roles of computer user, programmer, and system administrator. In each experiment, the instructor demonstrates an attack, and the students then learn how to use open-source defense tools appropriate for the role they are playing and the attack at hand. O'Leary [4] describes a laboratory based capstone course that focus on defensive and administrative tools with the goal of teaching potential security officers. Wagner and Phillips [5] present seven modules of hands-on laboratory components taught at their computer security training workshop. One of the modules is a cyberwar exercise, in which the participants harden their systems and are subjected to a series of common attacks by the instructors. There is no attack component in the workshop cyberwar exercise. The laboratory exercises we designed focus on attacks using open source tools. Our goal is to expose students to penetration testing techniques and open source tools in wireless network environment. Through an understanding of the wireless attacks, students are better able to defend systems they might manage in the future. Most of the laboratory exercises found in the literature are for wired network,


*InfoSecCD Conference'08*, September 26-27, 2008, Kennesaw, GA, USA. Copyright 2008 ACM 978-1-60558-333-4/00/0006…$5.00.

while our laboratory exercises are designed for wireless network environment.

The rest of the paper is organized as follows: In the next section we describe various wireless network attacks. In section 3 the laboratory design of various wireless network attacks are described in detail. Section 4 discusses the assessment of the laboratory exercises, and section 5 concludes the paper.

# 2. WIRELESS NETWORK ATTACKS

This section describes some of the common attacks against wireless networks, such as wardriving, eavesdropping, WEP key cracking and decryption, MAC spoofing, Man-in-the-Middle/ARP cache poisoning, and ARP request replay. Laboratory exercises are designed to demonstrate these wireless network attacks.

## 2.1 Wardriving

Wardriving is the process of discovering acess points (APs) while driving around a city or elsewhere with a Wi-Fi-equipped computer. Open source software such as Cain and Abel, KisMAC [9], Kismet [10] and Wireshark [11] can be used to perform Wardriving. Wardriving collects and logs such information such as the Service Set Identifiers (SSIDs) of the Wi-Fi networks, the security protocol used (e.g., WEP, WPA, etc.), the AP's MAC address and a list of clients currently connected to it along with their MAC addresses.

## 2.2 Eavesdropping

During eavesdropping, the hacker uses software to configure his/her network card onto a certain channel and collects all radio signals within the range of the network card. To monitor radio signals the hacker needs a capture card, a hardware device devoted entirely to collecting data such as AirPcap [12] or a network card configured to promiscuous/monitor mode. The software that can be used to capture data includes Kismet, Wireshark and Airodump (which is part of the Aircrack suite). The data captured by using these tools is usually saved in a file (called a capture file) with the extension .cap. The data in the capture file can be used in a number of attacks later.

## 2.3 WEP Key Cracking and Decryption

When sufficient amount of data packets are collected through eavesdropping, the hacker can proceed to crack the WEP key. The initialization vectors (IVs) in the data packets are needed for WEP key cracking. The number of captured IVs needed to crack the key depends on the AP's key size. For a 64-bit encryption, about 250,000 to 500,000 IVs are needed depending on the complexity of the key. The key consists of ten digits with values of A-F and 0-9. It is possible to crack a key with less IVs but the cracking process will take more time. To crack a 128-bit encryption, about 500,000 to 1 million IVs are needed. Programs capable of cracking a WEP key include KisMAC, Aircrack, and Cain and Abel. Once the key is cracked, the hacker can use the key to decrypt the network traffic using a tool such as Airdecap-ng (part of the Aircrack suite).

## 2.4 MAC Spoofing

MAC Spoofing refers to altering the MAC address on a NIC (network interface controller) card. Each network card is shipped from the factory with a unique MAC address. MAC address can be spoofed through hardware or software. The tools that allow MAC spoofing are Mac Makeup and AirJack [13]. A hacker can use MAC spoofing to takeover another computer's identity to enter a target network as an authorized user.

To do this, the hacker either disconnects the authorized computer by sending disassociation frames to it or waiting for it to disconnect to assume its identity. MAC spoofing can be used in a Denial of Service (DoS) attack, for example, in Authentication or Association Flood DoS attacks. In an Authentication flood DoS attack, the hacker sends association request frames consisting of random MAC addresses in an attempt to flood the AP with login requests.

## 2.5 MITM and ARP Cache Poisoning

Man in the Middle (MITM) is a category of confidentiality attack. The hacker intercepts packets intended for the AP, and then forwards the packets to the AP or vice versa. The MITM attacker may also modify the data before forwarding it to the destination.

ARP Cache Poisoning is one specific implementation of MITM. ARP stands for address resolution protocol. It is a TCP/IP protocol used to convert an IP address into a physical address, or MAC address. A host wishing to obtain a MAC address broadcasts an ARP request onto the network. The host on the network that has the address in the request then replies with its MAC address. In ARP Cache Poisoning, the attacker poisons the ARP cache table of a host by sending fake ARP replies to the network. The fake ARP reply maps the attacker computer's MAC address with the victim host's IP address. The hacker then receives all data destined for the victim host.

## 2.6 ARP Request Replay

ARP Request Replay attack is a technique used to produce more new IVs for WEP key cracking. The attacker uses a program to listen for ARP requests on the network. When an ARP request is captured it is retransmitted back to the network. The computer with the IP address in the ARP request will then send an ARP response to the network. Every time the computer sends an ARP response, it generates a new IV which is captured by the attacker. The attacker repeatedly sends out ARP requests until large quantities of IVs are captured. These IVs are then used to crack WEP key. ARP request replay makes IV generation for key cracking substantially faster.

# 3. LABORATORY DESIGN

This section describes the three laboratory exercises we have designed for wireless network security: WEP cracking, ARP Cache Poisoning, and MAC Spoofing. These laboratory exercises are designed for the Windows XP Operating System using hardware and software tools listed in Table 1.

**Table 1. Required HW and SW for laboratory exercises**

| | |
|---|---|
| Hardware | Router (to act as an isolated AP)<br>AirPcap wireless packet capture card<br>Ethernet cable (used to configure router)<br>A laptop computer<br>A second computer within the network (victim for ARP Cache Poisoning)<br>Internet connection (optional for download of files) |
| Software | Cain and Abel v4.9.14<br>Mac Makeup<br>Aircrack-ng suite |

## 3.1 Cracking WEP

The laboratory exercise of cracking WEP includes four phases: (1) Preparing the environment; (2) Wardriving and eavesdropping; (3) Cracking the key; and (4) Decrypting network traffic.

### *3.1.1 Preparing the Environment*

In this step, we configure the key of the access point to allow for a quick cracking process, ensure that AirPcap adapter is functioning, and install software Cain and Abel, and Aircrack-ng. For easy cracking, we select 64-bit encryption key, and a WEP key of 1111111111.

### *3.1.2 Wardriving and Eavesdropping*

To crack the WEP key on a router/AP, the information on the AP needs to be collected first. This is done through wardriving. Next packets from/to the AP are collected through eavesdropping. In this step, ARP Request Replay attack is used to collect a large amount of IVs in a short period of time. Without using ARP Request Replay attack, it may take several days to collect sufficient IVs for WEP key cracking. This is not practical for a lab environment. Cain and Abel is used for wardriving and ARP Replay attack. Airodump-ng, which is part of the Aircrack-ng suite, is used for eavesdropping.

The procedure for this laboratory exercise is listed below:

(1) Start Cain and Abel and select "Passive Scan" to begin discovering APs.

(2) Check "ARP" Requests to enable ARP request replay attack. The AirPcap adapter will capture ARP requests and then repeatedly resend them to the AP in order to greatly increase the amount of IVs generated.

(3) Start Airodump to begin collecting IVs. For quick key cracking, it is advisable to collect at least 150,000 IVs. This process could take approximately 30 to 90 minutes.

(4) When a sufficient amount of IVs are collected, close Airodump and stop capturing packets. The IVs will be saved to C:\Aircrack\aircrack-ng\bin\Capture.ivs (if Aircrack was extracted to this path).

### *3.1.3 Cracking the Key*

In this step, Aircrack-ng and the captured IV file from the previous step (Capture.ivs) are used to crack the WEP key. Run Aircrack-ng_GUI.exe, and select the file Capture.ivs that contains the captured IVs. Select 64-bit encryption key for the key size then click Launch to start cracking the key. The key will be displayed.

### *3.1.4 Network Traffic Decryption*

In this step, the cracked WEP key is used to decrypt intercepted network traffic into plaintext. Airodump-ng in the Aircrack-ng suite is used for eavesdropping. Airdecap-ng in the Aircrack-ng suite is used for WEP decryption. The procedure for decrypting network traffic is described below:

(1) Run Airodump-ng.exe from the Aircrack bin directory, and enter appropriate options to start collecting data packets.

(2) Open a web browser to generate network traffic on the AP for decryption.

(3) Close Airodump and stop capturing packets.

(4) Run Aircrack-ng_GUI.exe from the Aircrack bin folder and select the Airdecap-ng tab. Configure Airdecap-ng to decrypt the captured network traffic file. Enter the WEP key in hex (1111111111), and click Launch to start the decryption process. A command prompt will open and the information of the decryption process will be displayed. The information includes the total number of packets read, the total number of WEP/WPA packets, the number of plaintext data packets and the number of decrypted WEP/WPA packets.

(5) Open the decryption file Network-dec.cap in WordPad to see the network traffic in plaintext. Some encrypted text will still be present. These are beacons and ping replies.

## 3.2 ARP Cache Poisoning

In this laboratory exercise, two laptops and a router will be used to demonstrate ARP cache poisoning attack. One laptop (victim) is connected to the router using an Ethernet cable. The other laptop (attacker) connects to the router wirelessly. The attacker uses Cain and Abel to launch an ARP Cache Poisoning attack on the victim.

### *3.2.1 Discovering Hosts Connected to the AP*

The laboratory exercise starts with finding the IP addresses of the router and the attacker PC. Install Cain and Abel on the attacker PC. Configure Cain and Abel such that the adapter associated with the attacker PC's IP address is selected (Figure 1). Activate the sniffer function of Cain and Abel to discover clients connected to the AP. Select the Hosts tab in the bottom left of Cain and Abel's GUI and click on the blue cross icon (or select File→Add to List) and the "MAC Address Scanner" dialog appears (Figure 2). Click OK and a list of all hosts found on the subnet is displayed (Figure 3).

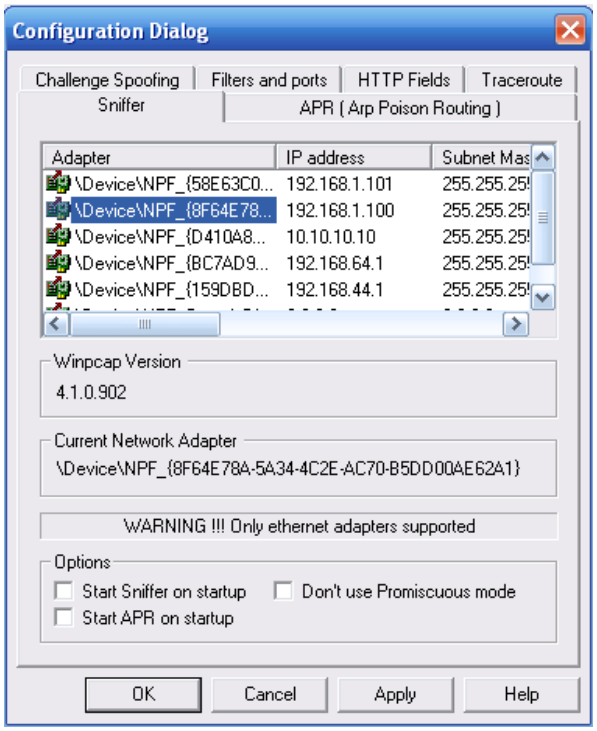


**Figure 1. Cain and Abel Sniffer Configuration Dialog**

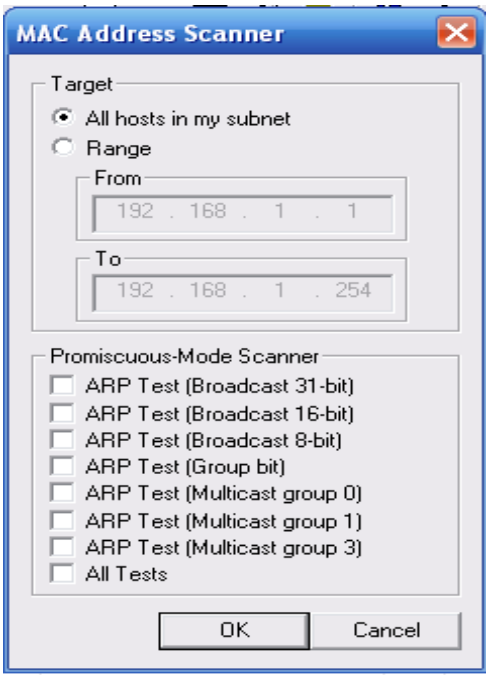


**Figure 2. Host scanner test option dialog**

### *3.2.2 Poisoning Host/Clients*

The procedure of poisoning clients is listed below:

(1) Click the ARP tab at the bottom to open the poison routing page.

(2) Both panes on the right should be empty. Notice that the blue cross icon is now inactive. Click inside the top pane and the blue cross icon should become active. Click the blue cross icon to open the New ARP Poison Routing dialog (see Figure 4).

(3) On the left side, select the AP's IP address (i.e., 192.168.1.1). Doing this tells the tool that you would like to assume the identity of the AP. The right side is now populated with the IP addresses of other clients.

(4) Select one or more clients on the right to be the victim(s). In this case it will be 192.168.1.102 (see Figure 5).

(5) Click OK. Cain and Abel is now poisoning the selected hosts (see Figure 6).

(6) The connection is now poisoned and any traffic sent by the victim computer to the AP will be intercepted by the attacker PC.

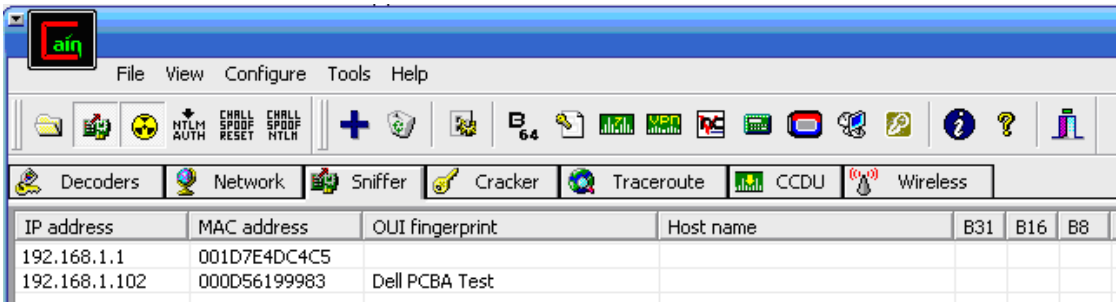


**Figure 3. Cain and Abel Host list**

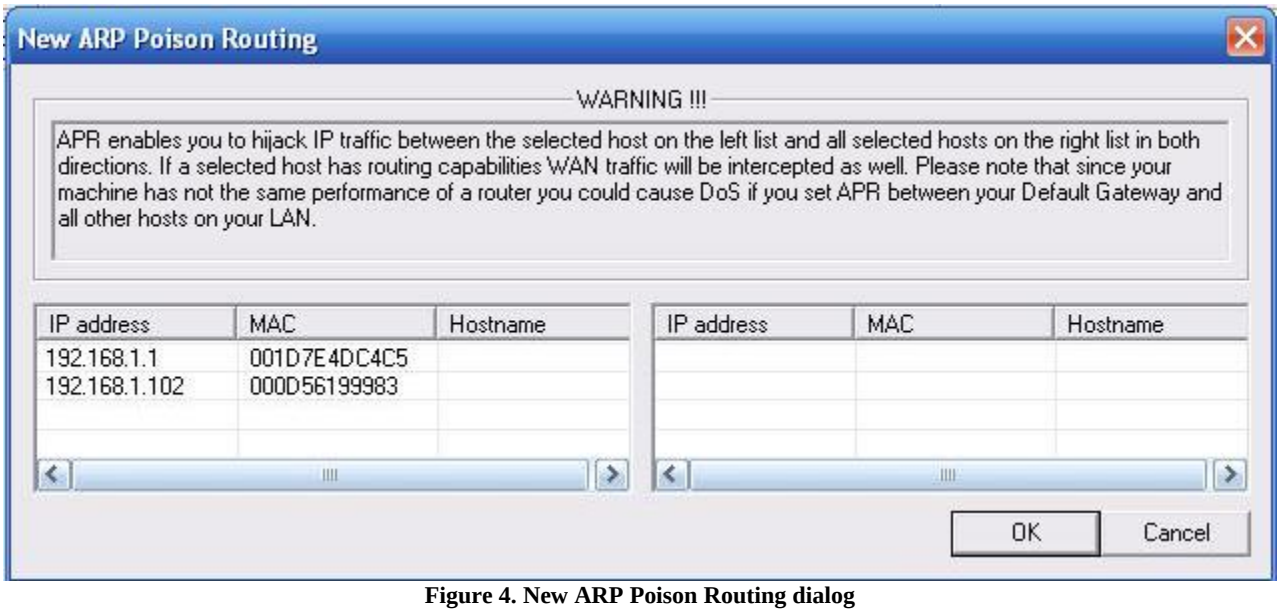


**Figure 4. New ARP Poison Routing dialog**

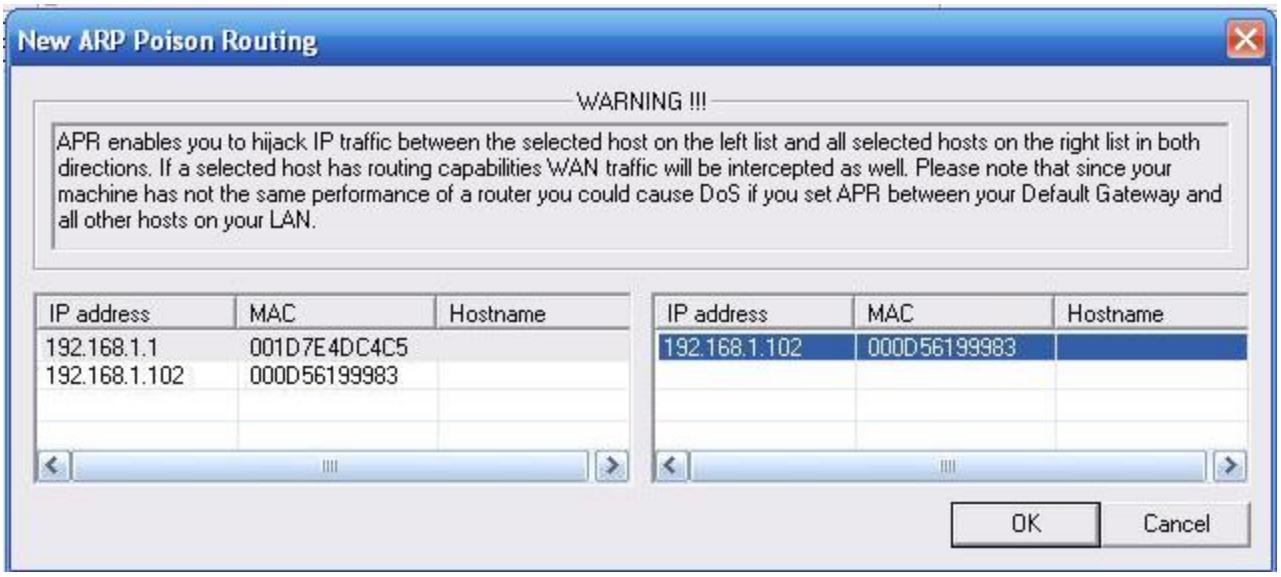


**Figure 5. New ARP Poison Routing dialog with AP selected on left and poison victim selected on right**

### *3.2.3 Intercepting Victim's Passwords*

(1) While the poisoning process is still active, we will now generate traffic using the victim PC. On the victim computer, open a web browser and type in the router's address http://<router's IP> (i.e., http://192.168.1.1). Log into the configuration page.

(2) On the attacker PC, click the Passwords tab at the bottom. Select the HTTP option on the left. The username/password information used by the victim will be shown in the list (see Figure 7). This process illustrates how to intercept HTTP passwords but the same procedure can be followed for many different protocols.

## 3.3 MAC Spoofing

In this laboratory exercise, Mac Makeup is used to change the MAC address. MAC Spoofing allows attackers to gain access to a network that utilizes MAC filtering. When an AP has MAC filtering enabled, only users with MAC addresses in the Access Control List (ACL) are allowed to be connected to the AP. The attacker can change his MAC address to be one found in the AP's ACL and connect to the AP. This laboratory exercise includes two steps: preparing the environment and MAC spoofing. These two steps are explained below.

### *3.3.1 Preparing the Environment*

(1) Use ipconfig/all to find your network adapter's information (i.e., Wireless Network Connection) and write down the Physical Address (i.e., 00-18-DE-18-3D-A6), the Description (i.e., Intel® PRO/Wireless 3945ABG Networking Connection), and the router's IP address (i.e., 192.168.1.1). (See Figure 8.) The description will be the name displayed in Mac Makeup for your network adapter.

(2) Open the AP's configuration page by typing http://192.168.1.1 into the address bar of a web browser.

(3) Enable MAC filtering on the AP by selecting Wireless→Wireless MAC Filter. Click Permit only and then click the Edit MAC Filter button. This procedure is for a Linksys router. The procedure for enabling MAC filtering may be different for a different type of router. Enter a valid MAC address into the ACL. Write this MAC address down.

(4) Save the settings and close the browser.

(5) Extract the Mac Makeup zip file to C:/MacMakeup.

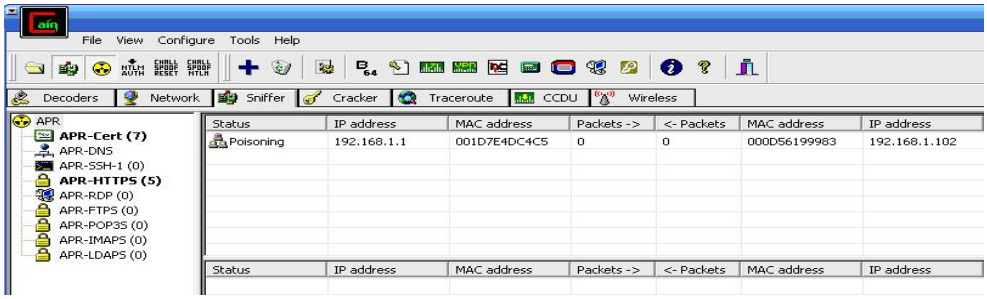


**Figure 6. Cain and Abel during active poisoning session**

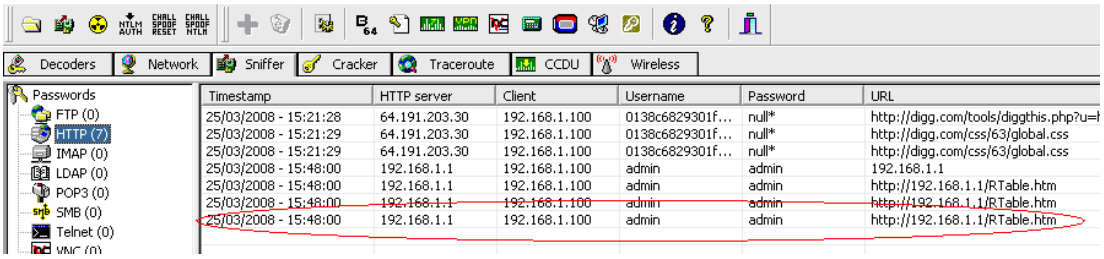


**Figure 7. Recovered password in Cain and Abel**

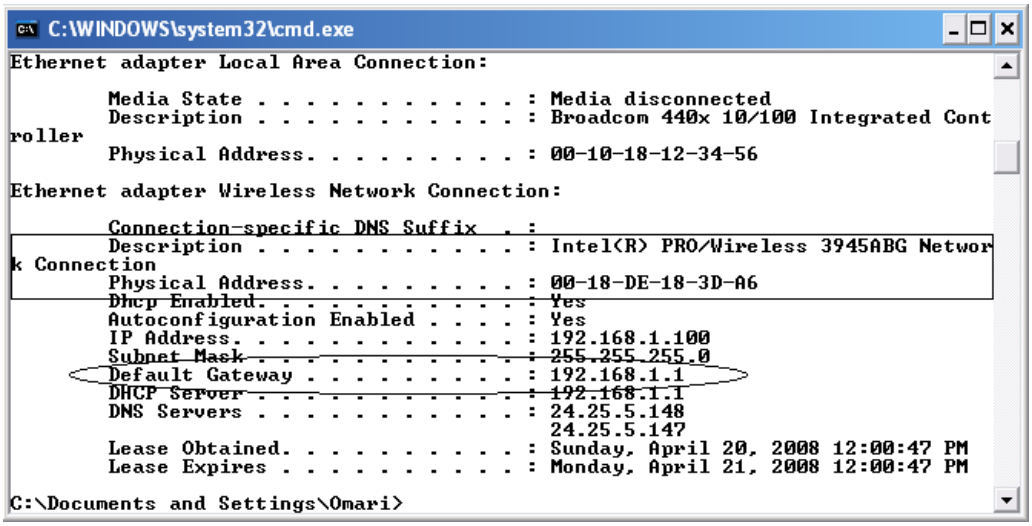


**Figure 8. Ipconfig window showing connection info**

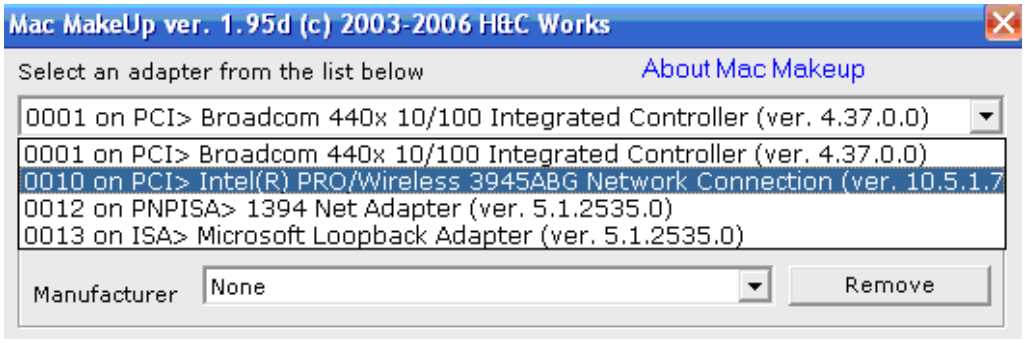


**Figure 9. Wireless adapter selected in Mac Makeup dropdown box**

### *3.3.2 MAC Spoofing*

(1) Attempt to connect to the AP with your current configuration. Since the AP's MAC filtering is enabled, the attempt should fail.

(2) Run Mac Makeup to change your MAC address.

(3) Select your network adapter from the dropdown at the top. This should be the same name you wrote down earlier (see Figure 9).

(4) In the MAC address section, enter the new MAC address which is the MAC address inserted in the AP's ACL. Enter the value without punctuation.

(5) Ensure that "Auto Nic Off/On" is checked and click the Change button to finalize the change. The network adapter will be shutdown and re-enabled to allow the change.

(6) Attempt to connect to the AP again. This time you should connect to the AP successfully.

(7) To clean up, change your MAC address back to its previous value.

## 4. ASSESSMENT

The designed laboratory exercises have been presented to two classes in the computer science department at this university. For one of these classes, a laboratory section was conducted. Fourteen students attended and participated in the laboratory exercises. Each student was given a laptop computer with wireless capability. The students were paired up and each pair was given a router to carry out the laboratory exercises. The students were able to carry out four attacks: Wardriving, WEP Key Cracking, WEP Decryption and ARP Cache Poisoning. Before the laboratory session, all participating students were asked to sign a disclaimer. This disclaimer proclaimed they would not use the knowledge gained for malicious purposes. The students were also given a questionnaire survey to assess their overall satisfaction with the laboratories and get their feedback. The student survey results are listed in Table 2. The survey results show that the students had very positive experiences with the laboratory exercises.

**Table 2. Student Survey Results (number of students = 12)**

| Question | Response |
|---|---|
| 1. Do you enjoy using the tool? | 58% strongly agree<br>42% agree |
| 2. Do you think the lab is easy to follow and straightforward? | 8% strongly agree<br>67% agree<br>25% neither agreed or disagreed |
| 3. Do you feel you understand the concept better after performing the lab? | 25% strongly agreed<br>58% agree<br>17% neither agreed or disagreed |
| 4. How likely are you to recommend this tool to others? | 50% definitely<br>33% probably<br>17% not sure |
| 5. Would you like to see more of these labs (or similar labs) in your courses? | 58% strongly agree<br>42% agree |
| 6. How much do you think you learned from these labs | 42% I learned a lot<br>33% I learned quite a few things<br>25% I leaned something |
| 7. What do you think could be improved in the labs to enhance learning? | Give more time to complete them<br>Provide more explanation |

## 5. CONCLUSION

In computer science and information security education it is widely accepted that hands-on experiences engage students in learning, raise their interest, and help them to retain knowledge and master skills. To provide students with hands-on experience in information security, three laboratory exercises are designed for information security instruction. These laboratory exercises can be used in computer network and information security courses. The laboratory exercises introduce to the students the following wireless attacks: Wardriving, Eavesdropping, WEP Key Cracking/Decryption, Man in the Middle, MAC Spoofing, ARP Cache Poisoning, and ARP Request Replay. Detailed description on how to conduct these attacks using popular open source tools is provided.

Future work will include refining the laboratory design, conducting evaluation of the exercises extensively, developing more laboratory exercises for wireless network security and developing laboratory exercises for the Linux platform. Plans for these activities are elaborated below.

(1) Refining the laboratory design
Through using these laboratory exercises in computer network and information security classes in the future and through the feedback received from the students, the laboratory exercises will be refined so they can be used most effectively. Exercise questions will be designed along with the laboratory exercises to help students master the concepts.

(2) Conducting extensive evaluations of the exercises
These laboratory exercises will be used in more computer science classes at this university in the future. The students' pre-test, post-test, and questionnaire results will be analyzed to evaluate the effectiveness of the laboratory exercises. The laboratory exercises will also be disseminated to instructors and students in other universities to get their feedback.

(3) Developing more laboratory exercises for wireless network security
In the future, more laboratory exercises can be designed for wireless network security. Laboratory exercises for various types of Denial of Service, such as Authentication flood attack, SYN flood, RF Jamming, etc., will be designed in the future.

(4) Developing laboratory exercises for Linux platform
All of the laboratory exercises are currently designed in the Windows XP Operating System. Due to the popularity of the Linux Operating System and its large open source support, laboratory exercises will also be developed for the Linux Operating System.

## 6. REFERENCES


[1] Wagner, P. J. and Wudi, J. M. "Designing and implementing a cyberwar laboratory exercise for a computer security course," *Proceedings of SIGCSE'04 - the 35th technical symposium on computer science education*, 2004, pp. 402 – 406.

[2] Hill, J. M. D., Carver, C. A., Humphries, J. W. and Pooch U. W. "Using an isolated network laboratory to teach advanced networks and security," *Proceedings of SIGCSE'01 - the 32th technical symposium on computer science education*, 2001, pp. 36 – 40.

[3] Brustoloni, J. C. "Laboratory experiments for network security instruction," *ACM Journal on Educational Resources in Computing*, Vol. 6, No. 4, 2006.

[4] O'Leary, M. "A laboratory based capstone course in computer security for undergraduates," *Proceedings of SIGCSE'06 - the 37th technical symposium on Computer science education*, 2006, pp. 2-6.

[5] Wagner, P. J. And Phillips, A. T. "A portable computer security workshop,", *ACM Journal on Educational Resources in Computing*, Vol. 6, No. 4, 2006.

[6] Aircrack-ng, http://www.aircrack-ng.org/doku.php, accessed on June 9, 2008.

[7] Cain and Abel v4.9.14. http://www.oxid.it/cain.html, accessed on June 9, 2008.

[8] Mac Makeup, http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp, accessed on June 9, 2008.

[9] KisMAC, http://KisMAC.macpirate.ch, accessed on June 9, 2008.

[10] Kismet. http://www.kismetwireless.net, accessed on June 9, 2008.

[11] Wireshark, http://www.Wireshark.org, accessed on June 9, 2008.

[12] AirPcap, CACE Technologies, http://www.cacetech.com/products/airpcap_family.htm, accessed on June 9, 2008.

[13] Airjack, http://sourceforge.net/projects/airjack, accessed on June 9, 2008.