International Journal of Future Generation Communication and Networking
Vol. 8, No. 1 (2015), pp. 9-18

An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network

[1]Md Waliullah, [2]A B M Moniruzzaman and [3]Md. Sadekur Rahman
[2]*Member, IEEE*
[123]*Department of Computer Science and Engineering*
Daffodil International University
Dhaka, Bangladesh
waliullah.cse@daffodilvarsity.edu.bd, monir.cse@daffodilvarsity.edu.bd and sadekur.cse@daffodilvarsity.edu.bd

Abstract

IEEE802.11 wireless networks have become one of the most widely used networks. Due to open nature of wireless medium, hackers and intruders can make utilization of the loopholes of the wireless communication; as a result, there are many security threats associated with Wireless Local Area Network (WLAN). In this paper, we have worked an experimental analysis to study some of the well known attacks pertaining to IEEE 802.11 WLAN. At first, some of the open issues related to this fragile technology have been discussed. Based on this vulnerabilities and threats categories some of the major attack has been performed in a live environment by using open source software tools i.e Aircrak-nj, kismet. etc. The analysis and finding from this paper's proved that the complexity of attacks had increased by time and the Wifi technology are becoming more dangerous to the end users and business environment.

Keywords: *WLAN, Kismet, Aircrack-nj, Wifi hack, WEP, WPA/WPA2, Threats, Vulnerabilities, IDS etc.*

1. Introduction

Since its inception, the IEEE 802.11 Wireless Local Area Network has become one of the most popular means of setting up networking technology. It has been deployed in almost every possible sector of networking due to the rapid proliferation of mobile devices. One of the main reasons for its popularity is that it provides the support of a normal local area network and also allows the moving of any network device without the added complexity of cabling and costing within the coverage area of that Wireless LAN. Low cost of hardware and user friendly installation procedures allow anyone to set up their own wireless network without any specialist knowledge of computer networks. However, the greater availability of wireless LANs means increased danger from attacks and increased challenges to an organisation, IT staff and IT security professionals.

Following are the open Issues/problems pertaining to the 802.11 WLAN technologies are summarized below:

Issue1: Unlike a wired network, a WLAN uses radio frequency transmission as the medium for communication. This necessarily exposes layer_1 and layer_2 to whomever in the RF ranges on the network. Wireless insecurity has been a critical issue since Wired Equivalent Privacy (WEP), an IEEE standard security algorithm for wireless networks, was compromised [1]. To address the significant security flaws in the WEP standard, the Wi-Fi alliance developed the 802.11i standard, called Wi-Fi Protected Access (WPA) and WPA2 [1]. However, many researchers have shown that the IEEE 802.11i standard

ISSN: 2233-7857 IJFGCN

cannot prevent eavesdropping, various denial of service attacks including de-authentication and disassociation attacks. Moreover, 802.11i's pre-shared key mode of WEP for flexibility and backward compatibility has made it easier to the most hackers to perform a Dictionary and Brute force attack [3].

Issue2: In order to eliminate all well-known attacks and address the significant security flaws in WEP, the Wi-Fi alliances developed IEEE 802.11i security standard in 2004 which is called Wi-Fi Protected Access (WPA) and WPA2. WPA uses the same encryption algorithm (RC4) used in WEP but improved it with a 48 bit Temporary Key Integrity Protocol (TKIP) sequence counter (TSC) instead of WEP's 24bit key. Moreover, the 64 bit message integrity check (MIC) algorithm named Michael is used to ensure integrity [1]. Furthermore, to improve user authentication and access control, WPA uses Extensible Authentication protocol (EAP) and the IEEE 802.1x standard port based access control. This method uses the Radius (Remote Authentication Dial-in User Service) server to authenticate each user on the network [4]. In the absence of a Radius server, it uses a pre-shared key (PSK), which is called WPA-PSK or WPA-Personal and is mostly used in small-offices and by home users [1].

Although, WPA is considered stronger than WEP, it does reuse the WEP algorithm. As a result it is vulnerable to offline dictionary and brute force attacks against the 4-way handshake protocol [8]. More importantly, it is much more vulnerable to Denial-of-Service attacks which are carried out over in the MAC layer by sending out de-authentication and de-association messages to the client or AP resulting in the legitimate user being denied access to the service [4].

Issue3: WPA2 employs the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of TKIP and uses Advance Encryption Standard (AES) block cipher. AES replaces the WPA's RC4 stream cipher [1]. Although WPA2-AES is still regarded as extremely secure, it is vulnerable to DoS, offline dictionary and internal attacks and fails to provide the availability aspect of the CIA triad [3]. More importantly, the robust encryption standard only applies to data frames and not currently to the management frames. All 802.11 management and control frames are vulnerable to replay or forgery, including the messages that are used to probe, associate, authenticates, disassociate, and de-authenticate users from WLAN. Besides, unlike the software upgrade required for migration from WEP to WPA, WPA2 requires the replacement of older hardware, extra processing power and higher cost [5].

Issue4: Our inability to effectively contain radio signals makes the WLAN vulnerable to a different set of attacks. Although businesses can position their access points and use antennas to focus their signals in a specific direction, it is hard to completely prevent wireless transmission from reaching undesirable locations like nearby lobbies, semi-public areas and parking lots. This makes it easier for intruders to sniff sensitive data [2].

Issue5: MAC address filtering can be configured in an access point in order to allow only the authorized client in the network. However, the various available open source hacking tools *i.e.* Kismet, SMAC *etc.* can be used to passively sniff a large amount of network traffic, including the MAC addresses of authorized computers. These can then be changed to act as legitimate client on the network. Moreover, in a large network the continually updated list of MAC address at the access point sometimes creates a security hole, if the list were not correctly updated [6].

Issue6: SSID is an identification that allows the clients to communicate with the appropriate access point. The available access points on the market come with a default SSID name and password. This creates potential security vulnerabilities, if these are not

changed by the administrator or user. For example some of the common default passwords are: "tsunami" –Cisco, "101" – 3Com, "Compaq" – Compaq *etc.* Furthermore, most of the hotspots and guest networks operate in an open system mode allowing any stations to connect to that network without requiring any form of authentication [07].

Issue7: Confidentiality Attacks - In this type of attack intruders attempt to intercept highly confidential or sensitive information that has been sent over the wireless association either in encrypted or clear text by the 802.11 or higher layer protocols. Passive attack categories here are Eavesdropping, Man-in-the-Middle attack, Traffic Analysis *etc.* However, Active attack categories of this attack are WEP Key Cracking, Evil Twin AP, and AP Phishing *etc*. [08].

Issue08: Access Control Attacks - This attack attempts to penetrate a network by bypassing the filters and firewall of the network to gain unauthorized access. War driving, Rogue Access Points, MAC address spoofing and Unauthorized Access are the most common types of attack in this category.

Issue09: Integrity Attacks - An Integrity attack alters the data while in transmission. In this type of attack, the intruder tries altering, deleting or adding management frame or data *i.e.* forged control to the network, which can mislead the recipient or facilitate another type of attack [09]. Denial-of-Service attacks are the most common example of this type of attack. Other types include Session Hijacking, Replay attacks, 802.11 Frame Injection, 802.11 Data Replay, and 802.11 Data deletion *etc.*

Issue10: Availability Attacks - This attack prevents or prohibits the legitimate clients by denying access to the requested information available on the network. Denial-of-Service attack is the most common type of availability attack which focuses on attacking a specific part of the network so the network is unreachable.

Issue11: Authentication Attacks - In an authentication attack, an intruder steals legitimate user's identities and credentials in order to gain access to the public or private WLAN and services. Dictionary attacks and Brute force attacks are the most common techniques in this category. Once they have got the required information, the attacker impersonates or masquerades as an authorized user. Thus, gain all the authorized privileges in the WLAN [2].

All the above observations have led us to study the vulnerability and threats of Wireless LAN security and the available solutions of the issues. In the following section some of the major attacks have been performed in a live environment.

2. Proposed Testbed Setup

Based on the above WLAN vulnerabilities, attack categories described, we have used Aircrack-ng suite VMware image for conducting the attack. Besides, open source intrusion detection software tools *i.e* Kismet are used. A live wireless local area network had been setup for performing the various attacks and monitoring or detecting them. Aircrack-ng suite VMware image was downloaded and installed in VMware player 3.0 in a desktop machine with an appropriate wireless USB adapter running on Windows-XP OS, which was acted as an attacker machine. Another Laptop with the same Aircrack-ng suit VMware images running on Windows7 OS was acting as a monitoring pc for detecting intrusions. Kismet and Wireshark were installed by default in the Aircrack-ng suite Vmware images. More importantly, all the machines were communicating via the wireless router in IEEE 802.11g WLAN technology with 54 Mbps data rates and 2.4 GHz ISM frequency bands.

Followings are the brief description of the necessary hardware and software required for this project to perform attack.

2.1 Hardware Requirements

The hardware requirements include a Desktop machine, 2 Laptops, Wireless Access point/Router and 2 special Wireless USB adapters for Desktop and Laptops.

Specification of the Hardware used for this experiment:

Belkin Enhanced Wireless Router (Model: F6D4230-4 v1000): Wireless Mode Used: IEEE 802.11g, Speed: 54Mbps, Bandwidth: 20MHz+40MHz auto, Operating Range: upto 300m, Wireless Channel: 6, Broadcast SSID: on, SSID: WIDS_TEST, Security Mode: WPA/WPA2-Personal(PSK), Authentication: WPA-PSK+WPA2-PSK, Mac Address: 00:22:75:E4:6B:A4

D-Link Wireless G USB Adapter (Model: DWL-G122): It is used in Attacker Desktop machine

IEEE standard: 802.11b/g, Bandwidth: Up to 54 Mbps, Frequency range: 2.4-2.4835, Security Support: WPA & WPA2, Mac Address: 00:24:01:0E:18:2D

ADDON Wireless LAN USB Adapter (Model: GWU180v4)

It is used in Wireless Intrusion Detection System (WIDS) monitoring Laptop machine.

IEEE Standard: 802.11g, Bandwidth: 54 Mbps, Frequency range: 2.4-2.485 GHz ISM band, Security Support: WPA & WPA2, Mac Address: 00:1E:E3:EB:18:55

Dell Desktop Machine (Model: T7570): It is used as an attacker machine.

Operating System: Windows XP (Service Pack 3), Processor: Intel Pentium 4 2.8 GHz, Ram: 2 GB, D-link DWL-G122 wireless USB adapter used.

ADVENT Laptop (Model: P7350): It is used as an Wireless IDS monitoring machine.

Operating System: Windows7, Processor: Intel Core 2 Duo 2.00 GHz, Ram: 2.00 GB, ADDON GWU180v4 wireless USB adapter used.

COMPAQ Laptop (Model: C730EM): It is used as an authorized wireless clientOperating System: Windows7, Processor: Intel Dual Core T2330 1.6 GHz, Ram: 2.0 GB, Built-in Atheros AR5007, 802.11 b/g Wi-Fi wireless card, Mac Address: 00:1E:4C:9F:E6:70

2.2 Software Requirements

We have used VMware player 3.0 for installing the Aircrack-ng suite VMware image. The open source intrusion detection software tools Kismet come up with the Aircrack-ng suite.

3. Analysis

3.1 Traffic Analysis

Kismet, is excellent tools that allows an attacker to do traffic analysis in the wireless local area network. An attacker can gain all the information about the network by running those tools, enabling wireless card in promiscuous, using the special type of Antenna and Global Positioning Mode (GPS) for covering as much range as possible and the location

of the specific network. Following are the test results without using the Antenna and GPS. However, the results are given in according to the signal range of my D-Link Wireless USB adapter.

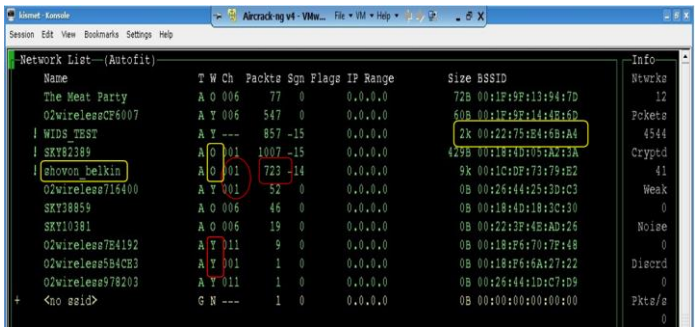


Figure 1. Kismet Console Interface

The above figure is the Kismet interface which shows the number of access point (AP), security protocol used, channel using, SSID, BSSID and the packets being sent by the access point in the whole network. For example, shovon_belkin is the SSID of my home wireless local area network and WIDS_TEST with 00:22:75:B4:6B:A4 BSSID router used for testing purpose. Kismet can able to show that shovon_belkin is using channel 1, "o" mean using WPA2-PSK rather than WEP, have sent total of 723 packets. On the other hand o2wireless978203 using WEP encryption which is might be my neighboured access point.

3.2 MAC Address Spoofing & Fake Authentication

MAC address can be easily spoofed to pose an authorized client in the network. The attacker can gain information about the authorized client by using Kismet, later he can change the MAC address to valid client MAC address in order to initiate the fake authentication attack.

The figure shows that the MAC address has been changed from 00:16: EA: 48:61:36 to 00:24:01:0E:18:2D

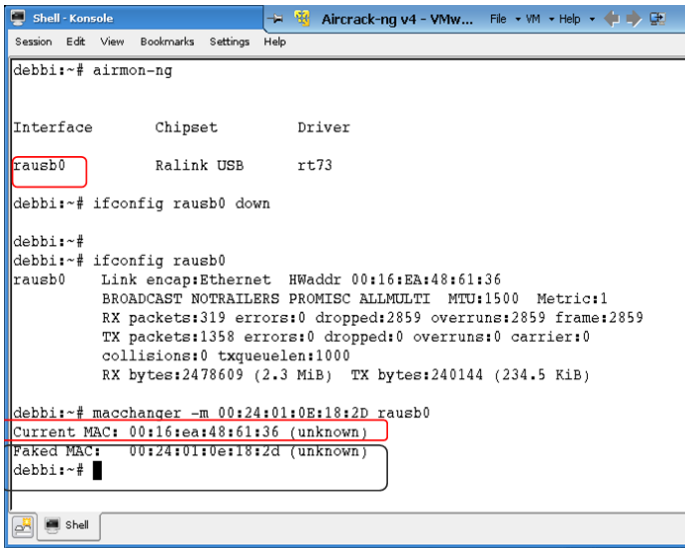


Figure 2. MAC Address Spoofing

Command:

```
# ifconfig rausbo down
# macchanger –m 00:24:01:OE:18:2D
```

The fake authentication attack is a type of Denial-of-Service attack whcih has been performed in order to authenticate and associates with the target AP. It could be done either Open or Shared key WEP authentication type. This attack is a part of the WEP key cracking attack. The main motive of this attack is to make the access point busy, so that enough IV (initialization vector) can be collected to make the job easier for cracking WEP key.

Aireplay-ng is a good tools that comes with the Aircrack-ng suite for conducting this attack.

Command:

```
# aireplay-ng -1 0 –e WIDS_TEST –a 00:22:75:E4:6B:A4 –h 00:24:01:0E:18:2D rausb0
```

- -1 means fake authentication
- 0 is the reassociation times is sec
- -e WIDS_TEST is the SSID of my router
- -a 00:22:75:E4:6B:A4 is MAC address of my rouer
- –h 00:24:01:0E:18:2D is the fake MAC address of my wireless USB card
- rausb0 is the interface of my wireless card

More importantly, if this attack can also be done without changing the attacker MAC address to valid client MAC address with the same command.

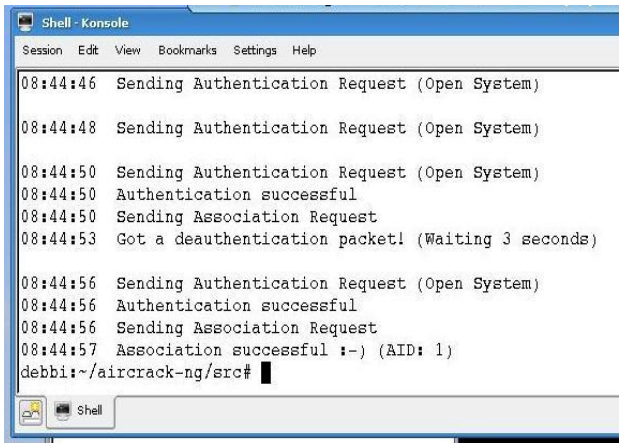


Figure 3. Fake Authentication Attack

Explanation: The above figure shows that after initiating the command Authentication and Association has been successfully performed with the legitimate AP.

3.3 WEP Key Cracking

WEP is a really crappy and old encryption technique to secure a wireless connection. It uses 3 byte IV (Initialization Vector) that is append to the each packets, which consists the pre-shared-key that needs to know the all authenticated clients in order to communicates. So, WEP key can be easily cracked, if enough IV can be captured.

Aircrack-ng suite has been used to crack the WEP key. Fortunately, Airodump-ng comes with the Aircrack-ng suite which can dump the beacon frame for a specific AP in order to grabbing enough IV. During the test, Fake authentication, Frame injection and De-authentication/Disassociation attack was also performed to grab more IV during

capturing the beacon frame with Airodump-ng. The more IV gathered the more chances to crack the WEP key. Later, Aircrack-ng another tools comes with the Aircrack-ng suite was run against the save file in order to crack the WEP key

Following are the description of step by step method of cracking the WEP key. Fortunately, Airoscript is a good scripting shell comes with the suite which makes the jobs easier instead of typing all the commands in the terminal.

Step1:

airoscriot.sh.

This window will appear which show the available interface that uses to capturing the beacon frame.

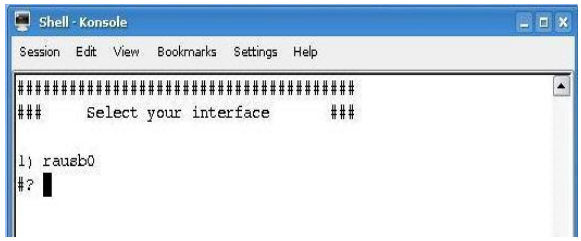
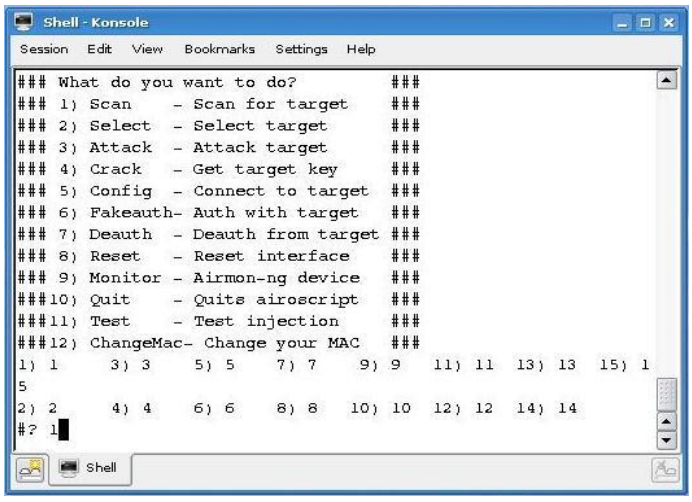


Figure 4: Selecting Interface

Step 2:

After selecting the interface it asked what to do. Obviously, scanned was selected in order to dumping the beacon frame



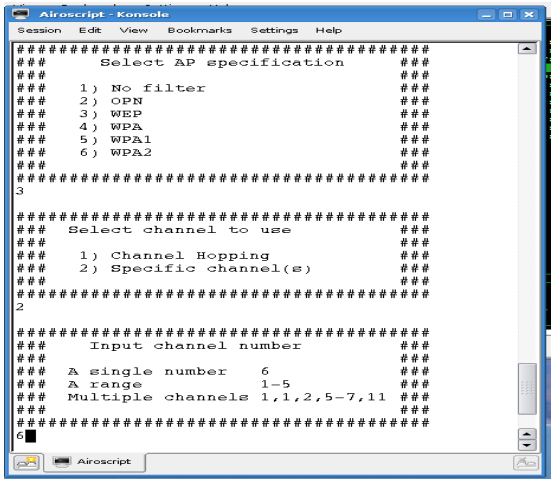
Step 2:

After selecting the interface it asked what to do. Obviously, scanned was selected in order to dumping the beacon frame

Figure 5. Scan for the Network

Step 3:

When I was selected scan it asked me to select the type of protocol frame and the channel used for capturing the beacon frame.
The following command is actually working behind this task:
airodump-ng <interface> <output prefix> <channel> <IVs flag>



Step 3:

When I was selected scan it asked me to select the type of protocol frame and the channel used for capturing the beacon frame.

The following command is actually working behind this task:

airodump-ng <interface> <output prefix> <channel> <IVs flag>

Figure 6. Channel Selecting

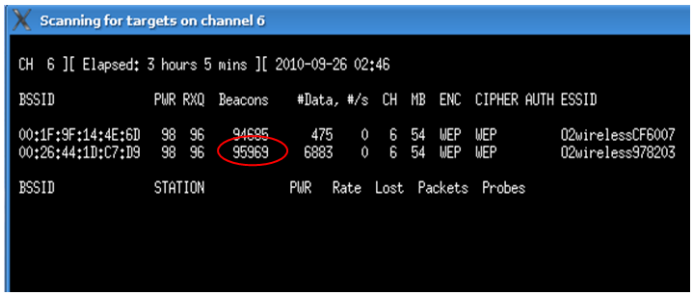


Figure 7. Frame Capturing

Step 4:

Whilst the airodum-ng was grabbing the IVs the following command was executed with the Aircrak-ng in oder to crack the key

aircrack-ng rausb0 –a 1 –b 00:26:44:1D:C7:D9 –n 64 dump1.cap

Here –a 1 means forces WEP attack

-b 00:26:44:1D: C7:D9 is the BSSID for o2wireless978203, which is my neighbours BSSID.

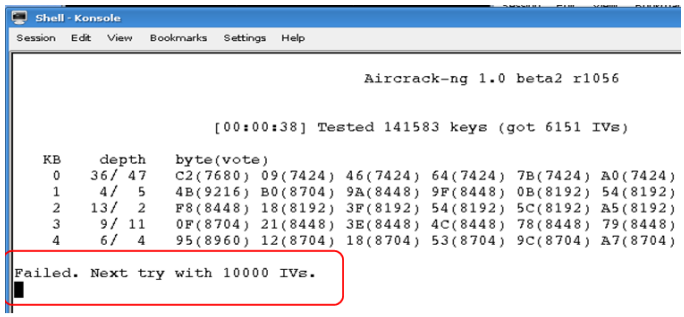


Figure 8. WEP Key Testing

The figure shows that if enough IVs are collected then its possible to get the WEP key.

3.4 WPA/WPA2-PSK Cracking

WPA is the encryption algorithm that comes to mitigate the vulnerabilities involves with the WEP protocol. WPA comes with PSK. PSK uses a user defined password to

initialize the TKIP, temporal key integrity protocol. So, in order to crack the WPA key, WPA handshake frame needs to be captured. Later, initiate the Brute-force or dictionary attack against the captured files.
During this test, the above method was involved for capturing the authenticate handshake. The only difference is to select AP specification for WPA. Or the following commands also work for this dumping beacon frame:
#airodum-ng rausb0 dump1.cap 6
Here rausb0 is my card interface name and 6 is the channel the target AP working.

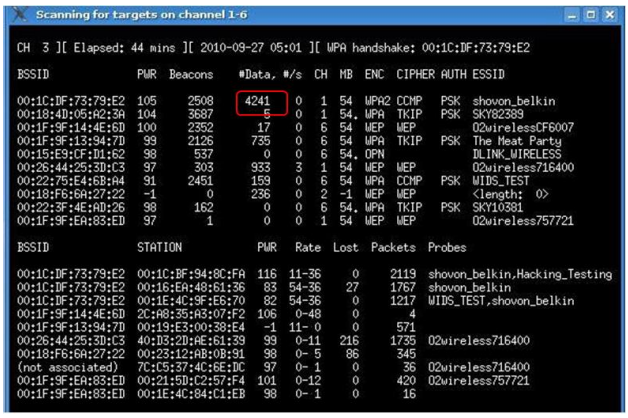


Figure 9. Dumping Beacon

The figure shows that the packet is dumping for 44 mins. My target AP was shovon_belkin. De-authentication/disassociation attack also involved to get more WPA handshake. I intentionally logged out and logged in the valid wireless client of shovon_belkin AP in order to get more WPA handshake.

The next part was to execute the Brute-force or Dictionary attack against the captured file by the following command:

aircrack-ng –w password.lst *.cap

Here –w password.lst is the name of the default password file.

Figure 10. Select the Network for WPA Key Crack

The above figure asks me to select the target network that key needs to crack. After identified shovon_belkin the following result have been found:

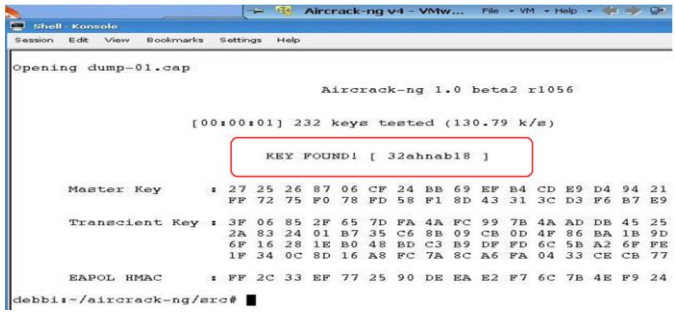


Figure 11. WPA Key Found

The above figure indicates that the key was successfully found by the dictionary attack method. I was actually save this password in the password.lst file to see if this works. Which means that if, the enough packets are captured and then execute it with the strong password file such as Openwall wordlists collection CD which includes 40 million password lists it could be possible to crack the WPA key.

4. Conclusion

Wireless LAN technology is still an emerging technology and vulnerabilities are comparatively easy to detect. So, LAN users may become a target for different kinds of attacks. The paper attempted to analyze attacks that a Wireless Local Area Network may be subject to. But we could not suggest any solution to protect the network from these attacks. So the technology provides opportunities to find solutions. Cryptographic studies-in-progress are working on how to detect unauthorized intruders on the network. As of yet there is no complete and fully trusted system or protocol developed yet to provide security as intruders' behaviors are noticeably different from each other which demand a huge amount of unauthorized actions for detection and thus protecting a network. Introducing new technology may provide some sort of support for the time being but as time goes on hackers are able to work on the vulnerabilities and script new programs to exploit the vulnerabilities.

So finally we can say that protecting WLAN is going to be a challenge always and all we have to ensure is to mitigate the risks by updating our knowledge by following the good practices over the industries to detect threatening and frequent attacks for a better security solution.

References

[1] F. Sheldon, J. Weber, S. Yoo and W. Pan, "The Insecurity of Wireless Networks", IEEE Computer Society, vol. 10, no. 4, **(2012)**, pp. 54-61.
[2] L. Phifer, "Wireless Lunchtime Learning Security School", **(2009)**, http://searchsecurity.techtarget.com /guides/Wireless-Security-School.
[3] L. Wang, B. Srinivasan and N. Bhattacharjee, "Security Analysis and Improvements on WLANs", Journal of Networks, vol. 6, no. 3, **(2011)**, pp. 470-481.
[4] J. Li, and M. Garuba, "Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities", Fifth International Conference on Information Technology: New Generations, **(2008)**; Las Vegas, Nevada.
[5] P. Kahai, and S. Kahai, "Deployment Issues And Security Concerns With Wireless Local Area Networks: The Deployment Experience At A University", Journal of Applied Business Research, vol. 20, no. 4, **(2004)**, pp. 11-24.
[6] M. Mathews, and R. Hunt, "Evolution of wireless LAN security architecture", IEEE 802.11i (WPA2). New Zealand: University of Canterbury.
[7] SANS Institute Infosec Reading Room, "Wireless LAN: Security Issues and Solution", US: SANS Institute, vol. 1.4, **(2003)**.
[8] Search Security, "Information security tutorials", **(2011)**, http://searchsecurity.techtarget.com /tutorial/Information-security-tutorials.
[9] M. Roche, "Wireless Hacking Tools", **(2007)**, http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html, [Accessed on: 29/08/14].

