INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ANALYSIS OF PENETRATION TESTING AND COUNTERMEASURES FOR SECURING WIRELESS NETWORK USING KALI LINUX

SUMIT JAYKANT MESHRAM[1], DINESH DATAR[2], NILESH P. THOTANGE[3]

1. Computer Science & Engineering, G.H Raisoni College of Engineering and Management, Amravati, India.
2. CTA, G.H Raisoni College of Engineering and Management, Amravati, India.
3. Fabriconn Communications Inc.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Now-a-days, wireless networks are deployed everywhere. The increase of Wi-Fi hotspots to the rising number of cell phones, PDAs and laptops equipped with Wi-Fi radios, that's why, for many organizations wireless security is an ever increasing issue. So, it is important to have a basic security level of encryption protocols. This paper focuses on the penetration testing attack that break encrypted password of a wireless device with a file that contains an alphanumeric dictionary with the use of Kali Linux, that has a collection of forensics tools. This paper shows the penetration test on WEP and WPA/WPA2 protocols, how this protocol is breach with simple attacks using Kali Linux. This paper also classifies the most vulnerable access point to help network administrator, how they protect their networks for such a type of attacks and which type of the countermeasures they have to take.

Keywords: Security, Encryption, Kali Linux, Wireless Network, WEP, WPA/WPA2

Corresponding Author: MR. SUMIT JAYKANT MESHRAM

Access Online On:

www.ijpret.com

How to Cite This Article:

Sumit Jaykant Meshram, IJPRET, 2015; Volume 3 (9): 1384-1393

PAPER-QR CODE

INTRODUCTION

In day-to-day life, internet is commonly needed by everyone. People are accessing internet from wired or wireless technology. Now a day's people are widely using wireless network, because it is more efficient rather than wired network. It is also easy to configure, manage, and low cost. But wireless network is nothing but such a type of frequency, which is anybody, can access anywhere in that range and increasing attack on wireless network therefore, from this emerging technology have come various types of wireless encryption algorithms to make the wireless network more secure.

802.11 is a set of IEEE standards that govern wireless networking transmission methods. They are commonly used today in their 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac versions to provide wireless connectivity in the home, office and some commercial establishments. This encryption algorithm are used [3] Wired Equivalent Privacy (WEP), [3] Protected Access (WPA), and [3] Wi-Fi Protected Access 2 (WPA2). [1] If the protocol is WEP, so it indicates a weaker encryption protocol, if the protocol is WPA or WPA2 it indicates the protocol is stronger than the protocol WEP.

Much software works to discovery wireless passwords using different kinds of spy software's, between these software's are: [4] airmon/aircrack, [4] airodump, and [4] gerix-wifi-cracker but all these tool can be found together in one penetration OS which is Kali Linux, and can be started directly from CD (without install disk), removable media (pen drive), virtual machines or directly on the hard disk.

In some papers [2, 3] tell the lot of security aspect, but not giving any experimental practical guidance, what happening behind the tool of wireless discovery. This paper differs from others in the kind of approach because this is not only dedicated to describe the methods to break encryption protocols, but it is also intended to show the countermeasures of securing wireless network by using the open source tools that they come packaged in a Linux distribution called Kali Linux that is widely used by network administrators and security researchers for analysis of wireless network. The Kali Linux OS finding the most vulnerable access point protocol to help the networks administrators to protect their networks, and they know that this protocol is need to change into stronger one.

This paper is organized as follows. After this Introduction, Section II presents a brief theoretical revision; Section III describes the experimental results; Section IV countermeasures; Section V concludes the paper and proposes some future work.

I. THEORETICAL REVIEW

Basically all type of hacker hack the any system using SSID (Service Set Identifier). It used to maintain wireless connectivity. The SSID can be up to 32 characters long. Even if the access points (Aps) of this network are very close, the packets of the two are not going to interface. Thus, SSID can be considered a password for an AP, but it can be sent it clear text and can be easily discovered.

The most commonly used encryption protocols in a wireless network.

A. *Wired Equivalent Privacy (WEP)*

The WEP stands for Wired Equivalent Privacy, and previously it is used to provide security during the authentication process, security and reliability for communication between wireless devices. [6] It covers systems in which an omnidirectional wireless radio generates a nominal 2.4-GHz carrier wave that communicates over a theoretical range of 1,000 feet.

[1] The WEP is part of the IEEE 802.11 standard and it is used to protect the wireless network of the type Wi-Fi. This protocol is not so stronger, because [3] the secret key used in WEP algorithm is 40-bit long with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key. [6] In other words, when enabled, WEP encrypts the data portion of each packet exchanged between the station and the Access Point. It uses either a 40- or 128-bit encryption algorithm and share secret key in between station and access point. This are some weakness point of WEP protocol [3] first is, WEP does not Prevent forgery of packets. Second is, WEP does not prevent replay attacks. An attacker cans simply record and replay packets as desired and they will be accepted as legitimate, and another thinks is that WEP protocol allows an attacker to undetectably modify a message without knowing the encryption key. These are some basic point why now a days WEP protocol not so used. Now I found this enhancements WEP protocol stronger, they need to [3] improved data encryption (TKIP), user authentication (Use EAP Method), Integrity (Michael Method). This feature is fundamental to the security of your wireless network.

A. Wi-Fi Protected Access (WPA)

The WPA came with the purpose of solving the problems in the WEP cryptography method, without the user's needs to change the hardware. [3] The standard WPA similar to WEP specifies two operation manners: first is, Personal WPA or WPA-PSK (Key Pre-Shared) that use for small office and home for domestic use authentication. Second is, Enterprise WPA or Commercial that the authentication is made by an authentication server 802.1x, which is

generating an excellent control and security of the wireless network. But in some paper [1] also called WEP2 or TKIP [14] (Temporal Key Integrity Protocol), fighting some of the vulnerabilities of WEP. [5] ASMiTM attack can break the protocols that rely on broadcast/multicast traffic, sniff private data of clients, inject malwares etc. ASMiTM attack remains a pertinent insider threat in a WPA2 encrypted Wi-Fi networks.

[3] In the comparison between TKIP and WEP there are four improvements in Encryption algorithm of WPA that added to WEP:

1. To defeat forgeries, MIC (Michael) which is cryptographic message integrity code is used.
2. A new IV sequencing discipline is used to remove replay attacks from the attacker's arsenal.
3. A per-packet key mixing function is used for IV weak keys.
4. To provide fresh encryption and integrity keys, the rekeying mechanism are used.

B. Wi-Fi Protected Access 2 (WPA2)

WPA2 or IEEE 802.11i was a replacement for Wi-Fi Alliance in 2004 to the WPA technology, because although it securely over the previous standard WEP. [1] This used a protocol called Advanced Encryption Standard (AES).

C. GUI based Gerix-Wifi-Cracker

The Gerix-Wifi-Cracker is the GUI (Graphical User Interface) based automate a wireless network attack. [4] Gerix comes installed by default on Kali Linux and will speed up your wireless network cracking efforts. This software is basically not installed; we have to install it on our Kali Linux OS. [4] This software is called automating wireless network cracking, because you just have to install it and doing some procedure it will automatically cracked the network password. A supported wireless card configured for packet injection will be required to complete this recipe and in the case of a wireless card, packet injection involves sending a packet, or injecting it, onto an already established connection between two parties.

First you have to download Gerix packet's by using *wget*. After that once the file has been downloaded, we now need to extract the data from the RAR file. Next thinks is that you have to go on directory and to start the Gerix you have to type command *python gerix.py* and Gerix software will be ready to use.

D. Kali Linux - Penetration Testing Distribution

Kali OS is a Penetration Testing and Security Auditing GNU/Linux Distribution used for analysis and penetration testing, and it can be launched directly without installing to disk using CD or remove able drive. But it is better to install it on disk as some of other features will not be work properly or some time it may not support user hardware.

Generally this OS doesn't work efficiently in as it is form. Hence this OS must be customize as per user requirements. Sometimes some of the packages need to be customized and reprogramed to help generate desired result. This also includes kernel recompilation and frequent updation to its installed packages. Every package, kernel configuration and script is optimized to be used by security penetration testers.

Some of the features of Kali Linux 1.1.0a are:

- Kali Linux has more advance Evil Wireless Access Point feature which enables for batter wireless penetration testing.
- This OS can also be deployed on Cloud platform.
- Kali Linux also has support for braille hardware support which also enables blind user to use this OS same as normal users.
- Kali Linux supports hardware architectures suitable for Raspberry Pi and ARM platforms also.
- This OS also supports Forensic mode tools which are useful for forensic mode inspection.
- It can also be deployed on Android OS platform.

II. EXPERIMENTAL DETAILS

A GNU BASH shell script was implemented to classify the vulnerability levels of the security protocols (WEP, WPA, WPA2 or another), if the protocol is WEP, Then it is easier to crack. But the protocol is WPA/WPA2 then it is not so easy to crack as compare to WEP. For doing pen test, maximum people will be used the backtrack operating system.

To run the pen tests, at first, you need to make a live cd/dvd of kali 1.1.0 operating system which is released in 9TH February 2015. But in some time live cd/dvd will not work properly at that time you are also install it on your PC by using virtual box or direct booting and do the

following steps, where the statements that are placed with capital letters require that you replace with actual data of your network:

- First up on download the Kali 1.1.0 Linux OS.
- Give Boot with Kali Linux and start the Graphical User Interface (GUI). No need to type the command startx.

After that you need to open new terminal and type command airmon-ng. This script can be used to enable monitor mode on wireless interfaces. The typical use of this command is, to start wlan0 in monitor mode: airmon-ng start wlan0.

To cracking WPA/WPA2 encrypted password using dictionary and brute-force attacks. [1] It is based on four-way handshake, where a series of four packets is used to negotiate an encryption key between the client and access point.

- After that type the airodump-ng command to captures packets from a wireless router. After that write INTERFACE in front of command. Like airodump-ng wlan0, which menace that will help you to search the network around you.
- Next, type the airodump-ng channel x –w wireless attack BSSID INTERFACE. In above command x is channel number which is use by focusing access point and wireless attack is the file name where will be recorded the capture packets. Hence on that current directory it will generate the file wirelessattack.cap.
- Open new terminal, type the command aireplay-ng ----deauth 1. Specifying the MAC address of access point (-a) and MAC address of the client (-c), as in: aireplay-ng –deauth 1 –a 09:AC:90:AB:78 –c 00:11:22:33:44:55 wlan0. This command causes your Personal Computer (PC) to send a faked package to the access point, science the access point can't accept the faked package send by client, which causes it to re-authenticate then a process carried out automatically by most operating systems. With this, the authentication process will be recorded by the capture started at another terminal.
- After that wait until the information reaches nearby (more or less) to 30000.
- Finally used this aircrack-ng command for cracking the encrypted password. Like aircrack-ng wirelessattack.cap INTERFACE.

At least, you have managed to access the network from its target, but you have to wait least by 10000 packages to get the password.

How to do it…

- Open a terminal window and bring up a list of wireless network interfaces:

airmon-ng

- Under the interface column, select one of your interfaces like wlan0 or mon0. If wlan0 is available then no need to enter the stop command, but mon0 is available then we need to stop the wlan0 interface and take it down so that we can change our MAC address in the next step.

airmon-ng stop

ifconfig wlan0 down

- Next, we need to hidden our MAC address, Science the MAC address of your machine identifies you on network.

macchanger –mac 00:11:22:33:44:55 wlan0

- Now we need to start the airmon-ng

airmon-ng start wlan0

- After that you see bottom of executed command the wlan0 is enable like name is (mon0,mon1, so on..)

- Next, we will use airodump to locate/search the available wireless networks nearby.

airodump-ng wlan0

- A listing of available networks will begin to appear. After that choose the network which you want to attack, and press Ctrl+C to stop search. Then copy BSSID and remember the channel number.

➢ –c allows us to select our channel.

➢ –w allows us to select the name of our file.

- –bssid allows us to select our BSSID.

airodump-ng –c 10 –w wirelessattack --bssid 09:AC:90:AB:78 wlan0

- A new terminal window will open, and displaying the output of the previous command. Don't do any think on that terminal just leave this window open.
- Now to make an association, open new terminal window and used aireplay command. This process may take few minutes.

- –a used BSSID number
- –c our chosen MAC address

aireplay-ng --deauth 1 –a 09:AC:90:AB:78 –c 00:11:22:33:44:55 wlan0

- Finally, we run AirCrack to crack the WPA/WPA2 key.

- –w option will allow us to finding the location of wordlist.

aircrack-ng –w ./wordlist.lst wirelessattack.cap

III. COUNTERMEASURES

A. Cisco LEAP

Cisco LEAP is an 802.1X authentication type for wireless LANs (WLANs) that supports strong mutual authentication between the client and a RADIUS server using a logon password as the shared secret. It provides dynamic per-user, per-session encryption keys. Cisco LEAP can be used with WPA and WPA2 networks. Cisco LEAP takes advantage of the standard 802.1X framework. Cisco was the pioneer in introducing Extensible Authentication Protocol (EAP) support for WLANs at a time when none of the existing client operating systems provided EAP support. Cisco introduced Cisco LEAP in December 2000 as a way to quickly improve the overall security of WLAN authentication. Cisco LEAP overcomes the major limitations of 802.11 wireless security through extensible authentication support to other back-end directories (Windows NT, Windows Active Directory, and Open Database Connectivity

B. RADIUS

Remote Authentication Dial in User Service (RADIUS) is a networking authentication protocol that provides centralized Authentication, Authorization, and Accounting (AAA)

management for users who connect and use a network service. RADIUS was developed as a client access server authentication liable for both wired and wireless user for security and authorized authentication purpose. Due to its broad support and the scalable nature of the RADIUS, this system is generally deployed by ISPs, commercial networks and secure PAN networks for enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may include cable modems, ADSL, access points, VPNs, network ports, web servers, wireless hotspots and shared cloud resources etc.

RADIUS is a client/server authentication protocol that deploys in the application layer, using UDP as transport protocol. RADIUS has a client /user access credentials stored in its database which authenticates its clients base on three parameters which includes username, secure password and MAC. When a user connects to server configured to RADIUS it asks for user credentials. If they match then only it authenticates its client to grant access to its secure resources. RADIUS is often the backend of choice for 802.11x authentication as well. A dynamic encryption key is generated during this authentication both at the client and the RADIUS server side. The RADIUS server sends the dynamic encryption key to the access point via a secure channel which is encrypted with AES encryption. After the access point receives the key, regular network traffic forwarding is enabled at the access point for the authenticated client. The credentials used for authentication, such as a login password, are never transmitted over the wireless medium without encryption. Upon client logoff, the client association entry in the access point returns to the non-authenticated mode.

C. PEAP

The protected extensible authentication protocol, embed the extensible authentication protocol with an encryption and authentication base transport layer security channel. This protocol was jointly developed by Cisco, Microsoft Corporation and RSA security.

IV. CONCLUSIONS

As presented in this paper, wireless networks are more prone to many types of threats. This is due to its seamless scope, its open feature and its popularity. Vast availability of the hacking tools and devices opens up wide path for hackers to breach security, while the advancement of mobile computing making any wireless network more vulnerable to threats. The security of wireless network systems and their authentication must be managed very well to avoid leakage and breach of information and resources.

Wireless network is an easy access to local system if the network is not properly segregated. The developments of wireless network give flexible access. For this to work in a secure environment set of rules must be followed and adhered parallel to security measures.

ACKNOWLEDGEMENT

The authors thanks to G. H Raisoni College of Engineering & Management Amravati and Fabriconn Communications Inc. for their motivation and support to researches in cyber security and network administration

REFERENCE

1. R. L. Rosa, D. Z. Rodríguezy, G. Pívaroz, J. Sousax, "Analysis of Security and Penetration Tests for Wireless Networks with Backtrack Linux," Instituto Nokia de Tecnologia (INdT), 2010.

2. N. Sklavos, X. Zhang, "Wireless Security and Cryptography: Specications and Implementations," CRC-Press, A. Taylor and Francis Group, ISBN: 084938771X, 2007.

3. A. H. Lashkari, M. Mansoor, A. S. Danesh, "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)," International Conference on Signal Processing Systems, pp. 445449, 2009.

4. W. L. Pritchett, D. D. Smet, "Kali Linux Cookbook," PACKT Publishing, 2013.

5. M. Agarwal, S. Biswas, and S. Nandi, "Advanced Stealth Man in the Middle Attack in WPA2 Encrypted Wi-Fi Networks," IEEE Communications Letters, 2015.

6. J. Williams, "The IEEE 802.11b Security Problem, Part 1," IEEE IT Professional, 2001.