Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

Penetration Testing of Wireless Networks

Mohammed F. Abdulqader[1] , Adnan Y. Dawod[2]

[1]Kirkuk University / College of Engineering / Electrical Engineering Dept.

mohammed_mf81@yahoo.com[1]

[2]Kirkuk University / College of Nursing / Basic Nursing Science Dept.

adnanalsheq@gmail.com[2]

Received date : 9 / 11 / 2015 **Accepted date : 23 / 3 / 2016**

ABSTRACT

This project focuses on performing security assessment on wireless networks, and to crack the password assigned to it. The idea of wireless network brings to mind lot of ways of attacking and penetrating a network compared to the traditionally wired network. Because wireless typically extends beyond walls and boundaries, it has become prone to attacks.

This project intends to find the password of near-by wireless networks and focuses on performing security assessment on wireless networks, and to crack the password assigned to it. As WPA2 is considered as the most secured password encryption algorithm for wireless network, we will be performing penetration testing on it and will crack the password for WPA2 encryption.

This project mimics the penetration testing scope to find the password of one of the trusted wireless network.

Keywords: *WLAN: Wireless Local Area Network, WPA: Wi-Fi Protected Access, WPA2: Wi-Fi Protected Access II, WEP: Wired Equivalent Privacy.*

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

إختبار الاختراق من الشبكات اللاسلكية

محمد فخرالدين عبدالقادر [1] ، عدنان يوسف داوود [2]

[1]جامعة كركوك / كلية الهندسة / قسم الهندسة الكهربائية

mohammed_mf81@yahoo.com[1]

[2]جامعة كركوك / كلية التمريض / قسم علوم التمريض الأساسي

adnanalsheq@gmail.com[2]

تاريخ استلام البحث: ٩ / ١١ / ٢٠١٥ تاريخ قبول البحث: ٢٣ / ٣ / ٢٠١٦

الملخص

يُركز هذا المشروع على تقييم الأداء الأمني على الشبكات اللاسلكية، وكسر كلمة السر المسندة إليها. فكرة شبكة لاسلكية تعيد إلى الأذهان الكثير من الطرق لمهاجمة واختراق شبكة بالمقارنة مع الشبكة السلكية التقليدية. لأن اللاسلكية يمتد عادة وراء الجدران والحدود، فقد أصبح عرضة للهجمات.

ويهدف هذا المشروع إلى العثور على كلمة السر من قريب من الشبكات اللاسلكية، ويركز على أداء لتقييم الأمن على الشبكات اللاسلكية، وكسر كلمة السر المسندة إليها. كما يعتبر (WPA2) كما خوارزمية تشفير كلمة المرور الأكثر تأمينا لشبكة الاتصال اللاسلكية، وسوف يتم تنفيذ اختبار الاختراق على ذلك، وسوف نكسر كلمة السر لتشفير (WPA2).

هذا المشروع يحاكي نطاق اختبار الاختراق للعثور على كلمة واحدة من شبكة لاسلكية موثوق بها.

الكلمات الدالة: WLAN: شبكة لاسلكية محلية المنطقة، WPA: وصول واي فاي المحمية، WPA2: وصول واي فاي المحمية الثانية، WEP: سلكي الخصوصية المكافئة، IEEE: معهد مهندسي الكهرباء والإلكترونيات.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

1. INTRODUCTION

This project intends to find the password of near-by wireless networks. Often people use easy to remember password consisting of alphabets & numbers or date of birth or dictionary word. This project mimics the penetration testing scope to find the password of one of the trusted wireless network [1].

We should to know what the Cracking of wireless networks is; it is the defeating of security devices in Wireless local-area networks. Wireless local-area networks WLANs also called Wi-Fi networks are inherently vulnerable to security lapses that wired networks are exempt from [2].

Cracking is a kind of information network attack that is akin to a direct intrusion. There are two basic types of vulnerabilities associated with WLANs: those caused by poor configuration and those caused by weak encryption [3].

We will be working on some of the tools/software's present in backtrack which have different capabilities starting from finding near-by access points, capturing packets and then software's used to break the password from those captured packets [4].

As WPA2 is considered as the most secured password encryption algorithm for wireless network, we will be performing penetration testing on it and will crack the password for WPA2 encryption [5].

Related Works:

After almost a decade of research into ad hoc networking, MANET technology has not yet affected our way of using wireless networks. Anderw Whitaker, Daniel P. Newman – 2005, discussed lessons to draw and back them with experiences from our experimental work. They found that simulations have to be complemented to a much higher degree by real-world experiments, that there is a lack of mature implementations and integration and that efforts should be focused on more realistic settings inside the "ad hoc horizon" where decent network services still can be provided [8].

C Hurley, R Rogers, F Thornton – 2007, provided evidence through a study of how users configure and protect their wireless Internet access points (APs). Wireless networks require a Service Set Identifier (SSID), which represents the name of the wireless network, high distinguishes between the wireless networks and offers the ability for the users to identify and use them. If configured to auto-connect, is practical for a client adapter to connect to an AP,

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

or simply click on the SSID of a selected AP (SSIDs can be found in the client's list of available wireless networks under "Network and Sharing Center") [10].

V Ramachandran – 2011, introduced concepts and definitions related to penetration testing, together with different models and methodologies to conduct a penetration test. A wide range of penetration testing state-of-the-art, as well as related tools both commercial and free open source available on the market are also presented in relatively rich details [9].

2. Proposal Design

Planning and Penetration:

All Wi-Fi equipment supports some form of *encryption*. Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. However, the way these technologies work, all Wi-Fi devices on your network must share the identical encryption settings. Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance, to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy) [8].

WPA (sometimes referred to as the *draft IEEE 802.11i* standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is common shorthand for the full IEEE 802.11i standard [10].

A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability. This project focuses on performing security assessment on wireless networks, and to crack the password assigned to it.

We will be working on some of the tools/software's present in backtrack which have different capabilities starting from finding near-by access points, capturing packets and then software's used to break the password from those captured packets. As WPA2 is considered

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

as the most secured password encryption algorithm for wireless network, we will be performing penetration testing on it and will crack the password for WPA2 encryption [6].

There is another important difference between cracking WPA/WPA2 and WEP. This is the approach used to crack the WPA/WPA2 pre-shared key. Unlike WEP, where statistical methods can be used to speed up the cracking process, only plain brute force techniques can be used against WPA/WPA2. That is, because the key is not static, so collecting IVs like when cracking WEP encryption does not speed up the attack. The only thing that does give the information to start an attack is the handshake between client and AP. Handshaking is done when the client connects to the network. Although not absolutely true, for the purposes of this tutorial, consider it true. Since the pre-shared key can be from 8 to 63 characters in length, it effectively becomes impossible to crack the pre-shared key [13].

- Proposal Implementation:

Assessment Agreement:

The assessment agreement will include:

- Scope: We had to follow external approach as the company wanted to find the chances of hacking wireless network from external sources and we had to follow black box approach as this has to be done stealthily but at the same time with pre-approved permission.

Table (1): Penetration Tests Scope

Penetration Testing Scope	
In Scope	**Out of Scope**
1. Wireless Router	1.VoIP
2.Alfa AWUS036H USB Adapter	2.Router
3. PC supporting Bootable Backtrack	3.DMZ
4. Network configurations	4.Zigbee

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

Table (2): Penetration Testing Tools Scope

Penetration Testing Tools Scope	
In Scope	**Out of Scope**
1. Backtrack 5r3 2.Aircrack-ng 3.airodump-ng 4.airmon-ng	1.NMAP 2.W3AF 3.Core Impact 4.SQL map

- Deliverables:

Table (3): Deliverables

Deliverable	Description	Acceptance Criteria
Presentation	Electronic Document	As defined in scope, vetted by Team Lead, approved by Project Manager
Report	Electronic Document & Presentation	As defined in scope, vetted by Team Lead, approved by Project Manager

- Team Members:

Table (4): Team Members

Penetration Team Project Members	
Role	**Responsibility Description**
Project Manager	Gregory Funk – Manage team, ultimately responsible for success of project.
Project Sponsor	Anthony Barba – Handles escalated personnel issues, represents project and team to third parties.
Team Members	Name.
Stakeholders	Wilmington University, IT Department Heads

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

- Penetration Testing Team Members:

Table (5): Penetration Testing Team Members

Engineer	Specialty	Duty	Email	Phone Number	Alternate
Gregory Funk	Project Management, Wireless Penetration	Project Manager	gregoryfunk@wilmu.edu	1-800-943-225	Anthony, Barba
Nanda Kishore	Database, Email, Web Server Penetration	Engineer	vundecoden@wilmu.edu	203-400-5829	Gutlapally, Srikanth
Srikanth	Network admin	Engineer	Sri.1852@wilmu.edu	2016065349.	Peter, Haynes
Dhanunjay	SQL database specialist	Engineer	Dhanu@wilmu.edu	201-224-1253	Patrick,John
Vaishnavi	Additional support team	Engineer	vaishnavi@wilmu.edu	201-3333-5829	Will, turner
Syed	Addl. Team support	Engineer	syedmohammed@wilmu.edu	201-777-8253	Kirk,Patrick

Escalation Path: All the problems and unethical data would be reported to our manager Mr. Gregory Funk and to the team leaders at participating teams.

Date of the test: 29th November, 2014.

Start time: 05:00am.

Miscellaneous Points of Contact:

- **a.** Law Enforcement (City, State, County): Wilmington State Police, Delaware – 19702, USA. Ph# 919-564-5656.
- **b.** Internet Service Provider: Comcast Services, 2nd Floor, Patrick Avenue, Newark, Delware.
- **c.** Consultants: Rosie Johnson Consultants, Dover, Wilmington.
- **d.** Subject Matter Experts: Panel of heads of departments, Wilmington University.
- **e.** Lawyers: Andrew Augustine advocates services, Newyork.

Retest Policy: A total of 3 recurring tests are performed to maintain accuracy and to decrease errors.

Working conditions: Wilmington University using Dell personal computers.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

Non-disclosure Agreement:

Liability Insurance or Approval in Writing: ISO insurance company New York.

Assessment: This phase include several steps like checking the consistency of wireless network, how frequently it is used, i: e we need to know, stability of wireless network on which we are cracking password, collecting packets of access point, cross-checking the available licensed tools, establishing the network map of the company, assessing the likely vulnerabilities, methods to bypass the internal security, literature review, making final decisions of the methods of approach.

- Information Gathering:

We will be finding near-by wireless networks, for that we need to enable our wireless card in monitoring mode, which will help us to capture the packets. We start by running the command

airmon-ng start wlan0 and then

airodump-ng mon0

It will list out the entire available wireless network within our range of wireless card, from where we need to note down ESSID (Name of access point), BSSID (MAC Address of router), Encryption Algorithm used by the company to secure their wireless network and Channel Number of Router.

- Network Mapping:

Once we find near-by access point, we need to test and make sure whether we are able to capture the packets of our specific wireless network. The purpose of this step is to run airodump-ng to capture the 4-way authentication handshake for the AP we are interested in.

Enter:

airodump-ng -c 9 --bssid 00:14:6C:7E:40:80 -w psk mon0 Where:

- -c 9 is the channel for the wireless network
- --bssid 00:14:6C:7E:40:80 is the access point MAC address. This eliminates extraneous traffic.
- -w psk is the file name prefix for the file which will contain the IVs.
- mon0 is the interface name.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

- Penetration Testing:

The overall method is as follows:

1. Start the wireless interface in monitor mode on the specific AP channel.
2. Start airodump-ng on AP channel with filter for bssid to collect authentication handshake.
3. Use aireplay-ng to deauthenticate the wireless client.
4. Run aircrack-ng to crack the pre-shared key using the authentication handshake.

Step 1: Checking the pre-requisites:

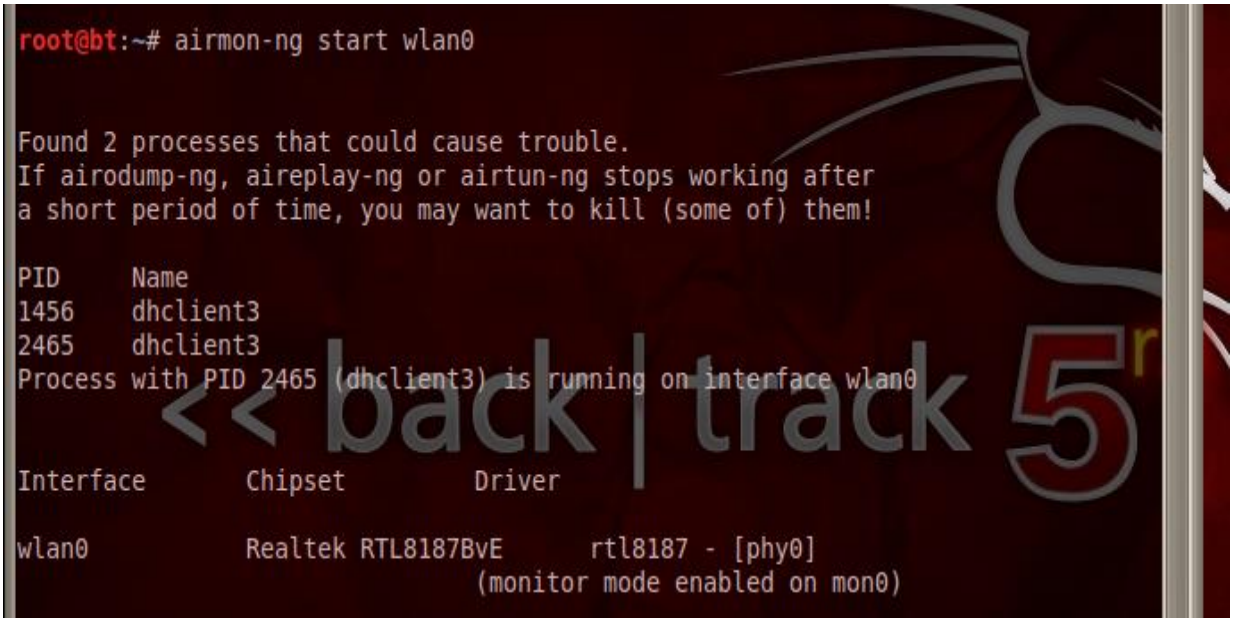
We will check whether our wireless card is detected or not.

The purpose of this step is to put your card into what is called monitor mode. Monitor mode is the mode whereby your card can listen to every packet in the air. Normally your card will only "hear" packets addressed to you. By hearing every packet, we can later capture the WPA/WPA2 4-way handshake. As well, it will allow us to optionally de-authenticate a wireless client in a later step.

The exact procedure for enabling monitor mode varies depending on the driver you are using. To determine the driver (and the correct procedure to follow), run the following command:

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

Step 2: Starting wireless card in monitoring mode, which will help us to capture the packets. Below picture shows monitoring mode is enabled on ***mon0.***



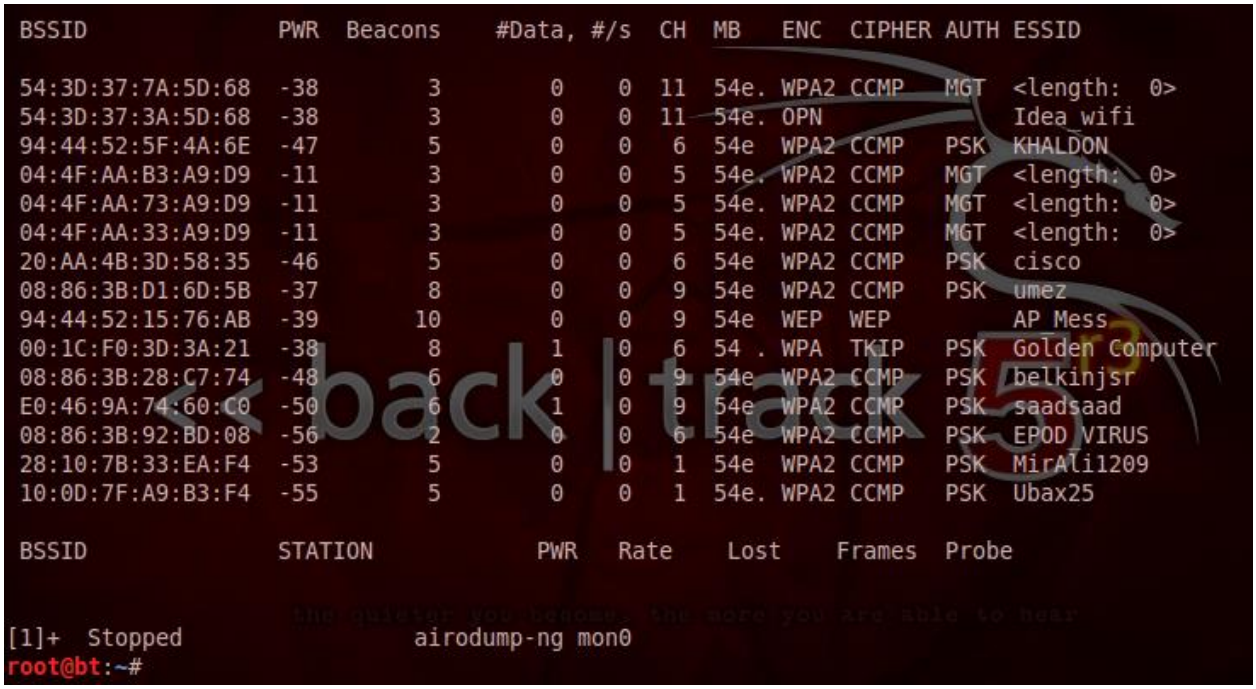
Step 3: Displaying near-by wireless network by running the command

airodump-ng mon0

We need to be aware of following terminologies:

- MAC address of PC running aircrack-ng suite: 00:0F:B5:88:AC:82
- MAC address of the wireless client using WPA2: 00:0F:B5:FD:FB:C2
- BSSID (MAC address of access point): 00:14:6C:7E:40:80
- ESSID (Wireless network name): EPOD VIRUS
- Access point channel: 9
- Wireless interface: ath0

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

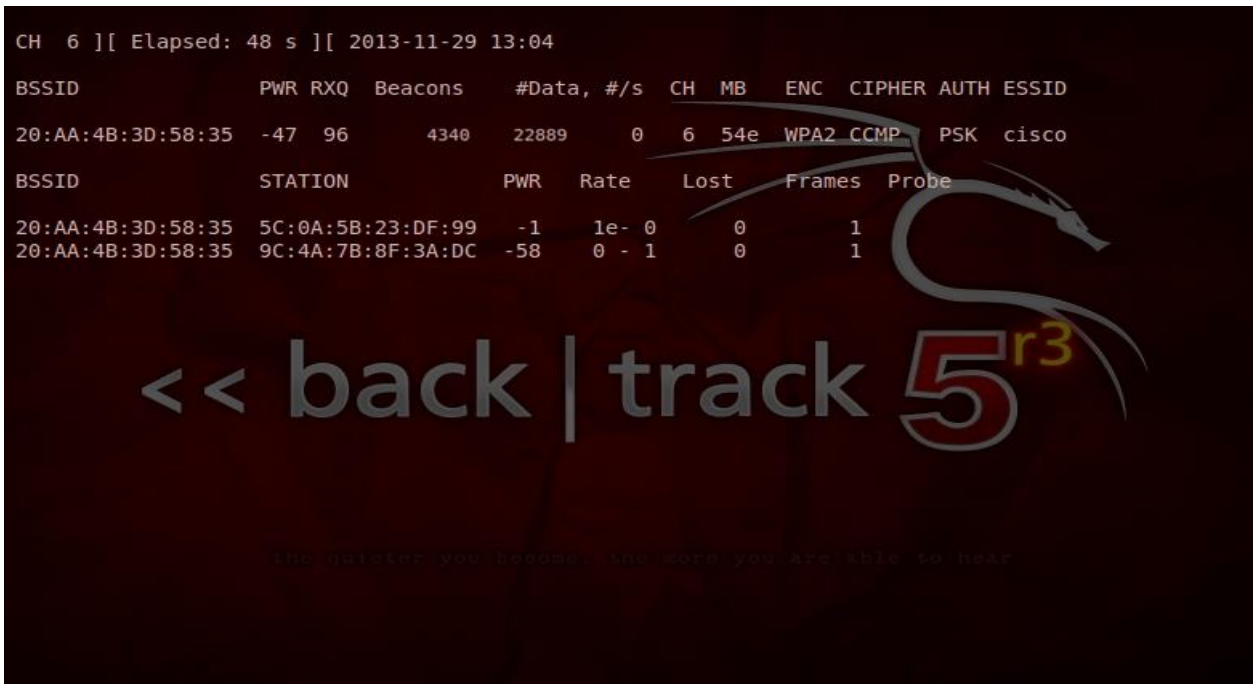


Step 4: Now the most important step is to select the target wireless network, here we have selected the wireless network by the name netgear which is using WPA2 encryption.

We will run this command to capture packets

airodump-ng –c 1 –bssid 20: AA: 4B:3D:58:35 –w delaware mon0

Also, we need to note down from below image that –w delaware is the name of file which will store all the capture packets:



Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

Step 5: Use aireplay-ng to deauthenticate the wireless client:

This step is optional. If you are patient, you can wait until airodump-ng captures a handshake when one or more clients connect to the AP. You only perform this step if you opted to actively speed up the process. The other constraint is that there must be a wireless client currently associated with the AP. If there is no wireless client currently associated with the AP, then you have to be patient and wait for one to connect to the AP so that a handshake can be captured. Needless to say, if a wireless client shows up later and airodump-ng did not capture the handshake, you can backtrack and perform this step.

This step sends a message to the wireless client saying that that it is no longer associated with the AP. The wireless client will then hopefully reauthenticate with the AP. The reauthentication is what generates the 4-way authentication handshake we are interested in collecting. This is what we use to break the WPA/WPA2 pre-shared key.

Based on the output of airodump-ng in the previous step, you determine a client which is currently connected. You need the MAC address for the following. Open another console session and enter:

aireplay-ng -0 1 -a 20: AA: 4B:3D:58:35 *-c 9C:4A:7B:8F:3A: DC mon*0

Where:

- -0 means de-authentication
- 1 is the number of deauths to send (you can send multiple if you wish)
- -a 20:AA:4B:3D:58:35 is the MAC address of the access point
- -c *9C:4A:7B:8F:3A:DC* is the MAC address of the client you are de-authenticating
- mon0 is the interface name

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

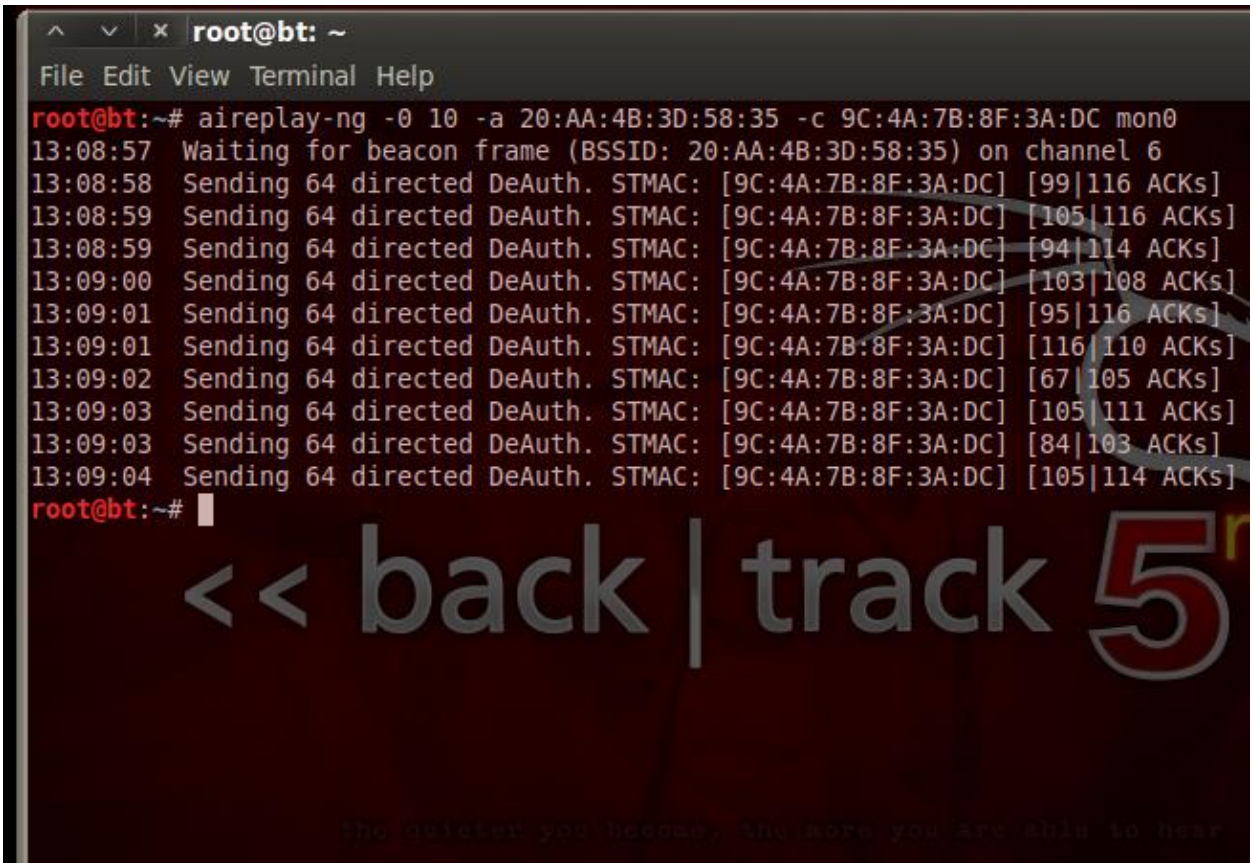


Fig. (1): Image shows de-authenticate the client who is already connected to wireless router

Step 6: Run aircrack-ng to crack the pre-shared key:

The purpose of this step is to actually crack the WPA/WPA2 pre-shared key. To do this, you need a dictionary of words as input. Basically, aircrack-ng takes each word and tests to see if this is in fact the pre-shared key.

There is a small dictionary that comes with aircrack-ng - “password.lst”. This file can be found in the “test” directory of the aircrack-ng source code.

Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

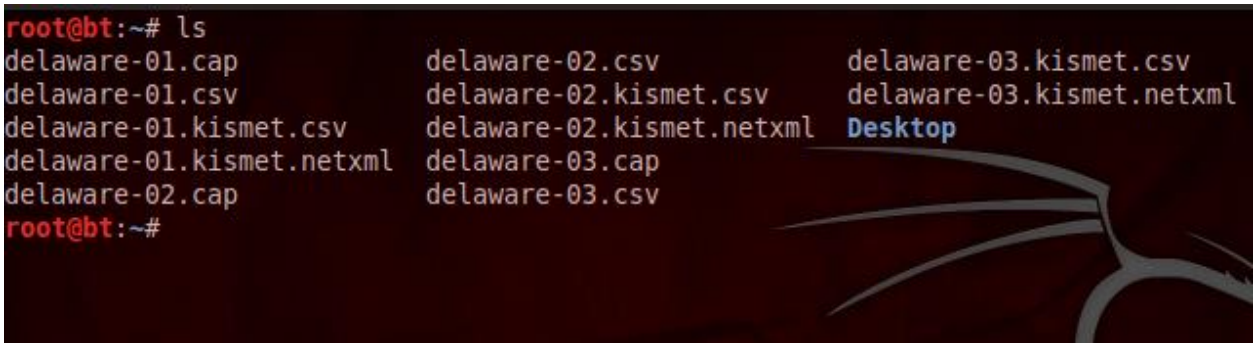


Fig. (2): Image shows our captured packets in root directory by the name delaware

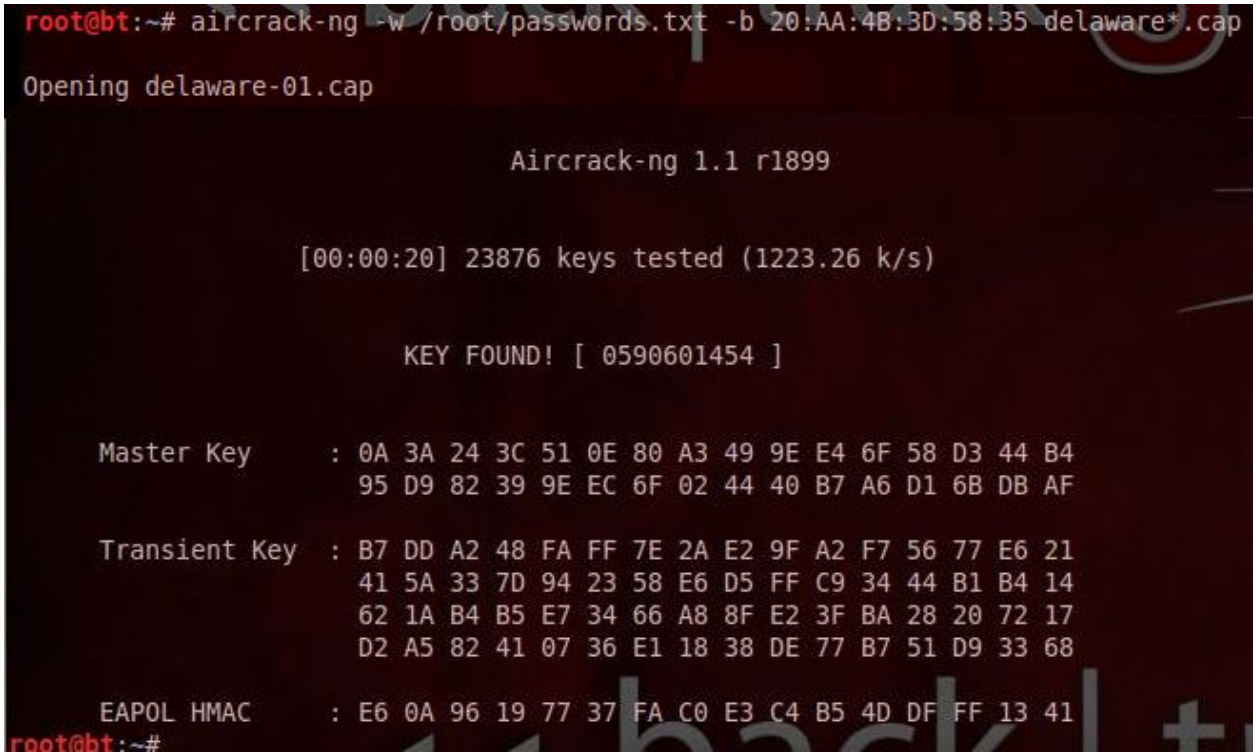
Open another console session and enter:

aircrack-ng -w /root/passwords.txt -b 20: AA: 4B:3D:58:35 delaware*.cap

Where:

- -w password.lst is the name of the dictionary file. Remember to specify the full path if the file is not located in the same directory.
- *.cap is name of group of files containing the captured packets. Notice in this case that we used the wildcard * to include multiple files.

Now, we will run the aircrack-ng to get the password from captured packets.



Kirkuk University Journal /Scientific Studies (KUJSS)
Volume 11, Issue 3, September 2016 , p.p(136-151)
ISSN 1992 – 0849

3. Results

Closing Activities:

Reporting:

The report attached has the detailed procedure with all the screen shots in sequential order detailing the procedure. The method we used is very effective and accurate. This method employed by is what which separates us from other companies.

4. Conclusions

Follow-on Actions:

The entire data was cleaned up, systems were wiped off. We also notified law enforcement and the Internet Service Provider and stakeholders that the penetration test is concluded. Also we destroyed the information and data gathered during the process. We are also happy to inform that no unethical incidents, physical or cyber happened during the pentest process.

Archiving

The procedure and final results would be stored with us for future analysis.

References

[1] C. McNab, "***Network Security Assessment***", Know Your Network, Paperback, Nov. 8, 2007, pp. 50-55. (Book style)

[2] E. S. Schetina, K. Green and J. Carlson, "***Internet Site Security***", 2002, pp. 400-417. (Book style)

[3] P. Engebretson, "***The Basics of Hacking and Penetration Testing***", 2011. (Google Books, General Internet site)

[4] D. Maynor, "***Metasploit Toolkit***" for Penetration Testing, Exploit Development, and Vulnerability Research, 1st Edition, 18 Sep. 2007, pp. 350. (Book style)

[5] R. Baloch, "***Ethical Hacking and Penetration Testing Guide***", Paperback – Import, 28 Jul 2014, kindle edition with free application, pp. 94-164. (Book style)

[6] W. Pritchett and D. D. Smet, "***Backtrack 5 Cookbook***", Paperback, 21 Dec. 2012, pp. 45-47. (Book style)

[7] http://www.aircrack-ng.org/doku.php?id=cracking_wpa/. [Accessed: Sept. 10, 2015]. (General Internet site)

[8] http://news.netcraft.com/. [Accessed: Jun. 22, 2015]. (General Internet site)

[9] http://www.backtrack-linux.org/wiki/index.php/Basic_Usage. [Accessed: Auge. 11, 2015]. (General Internet site)

[10] http://www.backtrack-linux.org/forums/showthread.php?t=18072. (General Internet site)

[11] J. Scambray, S. McClure and G. Kurtz, "***Hacking Exposed 2nd Edition***", 20 Nov. 2001, p. 25-29. (Book style)

[12] M. Sutton, A. Grenne and P. Amini, "***Fuzzing: brute force vulnerability discovery***", Paperback – Import, 29 Jun. 2007, pp. 32-40. (Book style)

[13] J. O'Gorman, D. Kearns, D. Kennedy and M. Aharoni "***Metasploit - The Penetration Tester's Guide***", July 2011, pp. 328, ISBN: 978-59327-288-3. (Book style)

[14] S. Kiyota, "***Creating an Integrated Internal and E-Business Information Security Architecture***", 2001, pp. 66-68. (Book style)

[15] R. E. Haeni, "***Firewall Penetration Testing***", the George Washington University, 1997, pp. 77-80. (Book style)

AUTHORS

Mohammed Fakhrulddin Abdulqader: received B.Sc. in Computer Software Engineering from Technical Faculty Kirkuk / Kirkuk-Iraq in 2003 and M.S. degrees in Computer Engineering from Sam Higginbottom Institute / Allahabad-India, in 2014. During 2004-2006, he worked as an engineer in Ministry of Kirkuk University, then in 2006 joined to the Engineering College / Kirkuk University. He now lecturer in Engineering College / Kirkuk University / Kirkuk-Iraq and, the responsible of the Internet & Computer Centre in the College.