Penetration Testing of Wireless Networks

Mohammed F. Abdulqader¹, Adnan Y. Dawod²

¹Kirkuk University / College of Engineering / Electrical Engineering Dept.
mohammed_mf81@yahoo.com¹

²Kirkuk University / College of Nursing / Basic Nursing Science Dept.
adnanalsheq@gmail.com²

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.
اختبار الاختراق من الشبكات اللاسلكية

محمد فخر الدين عبدالقادر 1، عدنان يوسف داوود 2
1جامعة كركوك / كلية الهندسة / قسم الهندسة الكهربائية
mohammed_mf81@yahoo.com
2جامعة كركوك / كلية التمريض / قسم علوم التمريض الأساسي
adnanalsheq@gmail.com

تاريخ قبول البحث: 9/11/15
تاريخ استلام البحث: 23/3/15

المخز

يركز هذا المشروع على تقييم الأداء الأمني على الشبكات اللاسلكية، وكسر كلمة السر المسندة إليها. فكرة شبكة اللاسلكية تعني إلى الأذهان الكثير من الطرق لمهاجمة واختراق شبكة بالمقارنة مع الشبكة السمكية التقليدية. لأن شبكات اللاسلكية عمود عادة وراء الجدران والحدود، فقد أصبحت عرضة للهجمات.

ويهدف هذا المشروع إلى العثور على كلمة السر من قريب من الشبكات اللاسلكية، ويركز على أداء تقييم الأمن على الشبكات اللاسلكية، وكسر كلمة السر المسندة إليها. كما يعتبر WPA2 كخوارزمية تشفير كلمة المرور الأكثر تأمينا لشبكة الاتصال اللاسلكية، وسيتم تنفيذ اختبار الاختراق على ذلك، وسوف نكسر كلمة السر لتسخير WPA2.

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

الكلمات الدالة: إختراق الشبكات اللاسلكية، WPA2، WPA، VLC...
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,
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
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>
<thead>
<tr>
<th>Penetration Testing Scope</th>
<th>Out of Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In Scope</strong></td>
<td><strong>Out of Scope</strong></td>
</tr>
<tr>
<td>1. Wireless Router</td>
<td>1. VoIP</td>
</tr>
<tr>
<td>2. Alfa AWUS036H USB Adapter</td>
<td>2. Router</td>
</tr>
<tr>
<td>3. PC supporting Bootable Backtrack</td>
<td>3. DMZ</td>
</tr>
</tbody>
</table>
Table (2): Penetration Testing Tools Scope

<table>
<thead>
<tr>
<th>Penetration Testing Tools Scope</th>
<th>In Scope</th>
<th>Out of Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Backtrack 5r3</td>
<td></td>
<td>1. NMAP</td>
</tr>
<tr>
<td>2. Aircrack-ng</td>
<td></td>
<td>2. W3AF</td>
</tr>
<tr>
<td>3. airodump-ng</td>
<td></td>
<td>3. Core Impact</td>
</tr>
<tr>
<td>4. airmon-ng</td>
<td></td>
<td>4. SQL map</td>
</tr>
</tbody>
</table>

- Deliverables:

Table (3): Deliverables

<table>
<thead>
<tr>
<th>Deliverable</th>
<th>Description</th>
<th>Acceptance Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation</td>
<td>Electronic Document</td>
<td>As defined in scope, vetted by Team Lead, approved by Project Manager</td>
</tr>
<tr>
<td>Report</td>
<td>Electronic Document &amp;</td>
<td>As defined in scope, vetted by Team Lead, approved by Project Manager</td>
</tr>
<tr>
<td></td>
<td>Presentation</td>
<td></td>
</tr>
</tbody>
</table>

- Team Members:

Table (4): Team Members

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Manager</td>
<td>Gregory Funk – Manage team, ultimately responsible for success of project.</td>
</tr>
<tr>
<td>Project Sponsor</td>
<td>Anthony Barba – Handles escalated personnel issues, represents project and team to third parties.</td>
</tr>
<tr>
<td>Team Members</td>
<td>Name.</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>Wilmington University, IT Department Heads</td>
</tr>
</tbody>
</table>
- Penetration Testing Team Members:

**Table (5): Penetration Testing Team Members**

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

**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, Delaware.


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.
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.
- 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:
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

```
airdump-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
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:
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 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 mon0
```

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
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.
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.
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


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.