افزایش سرعت کرک WPA/WPA2 توسط Rainbow Table در کالی لینوکس

مطالب گفته شده در این مقاله فقط در جهت آشنایی مدیران و کاربران شبکه های بی سیم بوده و هرگونه استفاده نادرست برعهده خواننده می باشد . نویسنده و سایت های ارائه دهنده هیچ مسئولیتی نخواهند داشت.

قانونمند رفتار کنیم.

نویسنده: سهیل رضاشعار

soheilshoar@gmail.com

1394-2015

ستامبر – شهریور

فهرست مطالب

عنوان صفحه

مقدمه..... ۳

ابزارهای مورد نیاز..... ۴

Rainbow Table ها چگونه کار می کند؟..... ۵

ساخت Rainbow Table توسط pyrit..... ۷

ذخیره Rainbow Table های pyrit..... ۱۲

استفاده از Rainbow Table ها در برنامه cowpatty..... ۱۴

ساخت Rainbow Table توسط genpmk..... ۱۶

ساخت Rainbow Table توسط airolib-ng..... ۱۸

نتیجه گیری..... ۲۱

مقدمه :

در این مقاله قصد آموزش نفوذ به شبکه های بی سیم را نداریم بلکه می خواهیم فقط یکی از روش های حمله به WPA/WPA2 که توسط Rainbow Table ها انجام می شود را بررسی کنیم و به کمک آن به افزایش سرعت برای بدست آوردن کلید های WPA/WPA2 کمک کنیم. WPA/WPA2 به دلیل مکانیزم پیچیده ای که دارد مانند رمزنگاری WEP به راحتی کرک نمی شود . در رمزنگاری WEP با جمع آوری #Data می توان به کلید صحیح صرف نظر از طولانی و پیچیدگی آن در کمتر از حدود ۱۰ دقیقه دست پیدا کرد اما در WPA/WPA2 روشی که در WEP استفاده می شود دیگر کارساز نیست . سه روش معمول برای حمله به WPA/WPA2 وجود دارد :

۱ . دیکشنری : در روش دیکشنری برنامه کرک کننده با محاسبه هش برای هر کلمه داخل دیکشنری و SSID شبکه و مقایسه آن با هش موجود که از 4 Way Handshake بدست آمده است به کلید صحیح می رسد.فایل 4 Way Handshake حاوی هش شبکه مورد نظر برای کرک WPA/WPA2 می باشد و زمانی که یک کاربر جدید قصد اتصال به شبکه را دارد ایجاد می شود.

۲. Brute Force :در روش Brute Force با تعیین تعداد و نوع کاراکترها از نظر اعداد،الفبا و خاص مانند (×!@#$%^) یا ترکیبی از هر سه نوع ، برنامه تمامی حالات ممکن بین آن کاراکتر ها را می سازد،سپس برنامه کرک کننده ای مانند aircrack-ng یا pyrit و.. هش را برای هر حالت محاسبه و با هش موجود در فایل 4 Way Handshake مقایسه می کند اگر یکسان بود کلید صحیح پیدا می شود.

روش سومی که قرار است در این مقاله مورد بررسی قرار گیرد روش Rainbow Table می باشد ، Rainbow Table ها در ساده ترین تعریف هش های از پیش محاسبه شده ای هستند که توسط خودمان یا افراد دیگر برای دیکشنری ها و SSID های مختلف می تواند ساخته شود و برای استفاده در اختیار عموم قرار گیرد . Rainbow Table ها یکبار ساخته می شوند و بارها استفاده می شوند و بدلیل اینکه برنامه کرک کننده دیگر عمل محاسبه هش یعنی آنچه در روش دیکشنری انجام می شود را برای هر لغت داخل دیکشنری و SSID انجام نمی دهد با سرعت بسیار بالایی به تست کلید ها می پردازد.

ابزارهای مورد نیاز

۱ . سیستم عامل کالی لینوکس که از آدرس زیر قابل دانلود است:

```
http://cdimage.kali.org/kali-1.1.0a/kali-linux-1.1.0a-amd64.iso
```

۲ . فایل 4 Way Handshake : این فایل قبلا توسط برنامه airodump-ng باید بدست آمده است.

۳ . سیستم با سخت افزار قوی : هرچقدر سیستم از نظر سخت افزاری قوی تر باشد ساخت Rainbow Table ها با سرعت بیشتری انجام می شود.

۴ . فایل دیکشنری : هر نوع دیکشنری برای ساخت Rainbow Table ها می توان استفاده شود مثلا دیکشنری هایی فقط با شماره تلفن ، اعداد و .. . کلمات داخل دیکشنری باید دارای ۸ کاراکتر یا بیشتر باشند زیرا طول کلید WPA/WPA2 که داخل اکسس پوینت ها و کلاینت ها پیکربندی می شوند حداقل ۸ کاراکتر است .
در سایت زیر مجموعه ای از دیکشنری های WPA/WPA2 قابل دانلود است :

```
http://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.htm
```

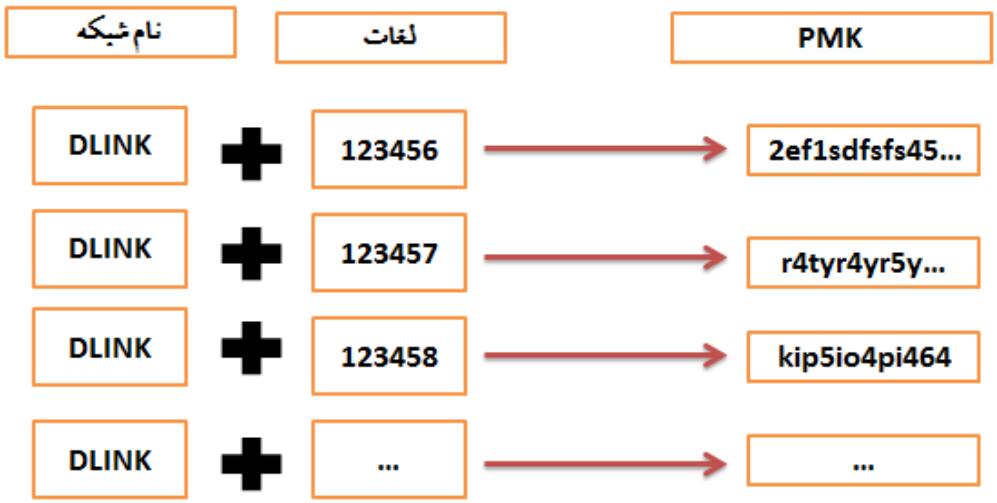
همچنین دیکشنری هایی به طور پیش فرض در کالی لینوکس موجود است:

```
usr/share/wordlists
```

در تست های این مقاله از کالی لینوکس 1.1.0a و لپ تاپ DELL (CPU Core i5,4 GB RAM) 5010 استفاده شده است .

Rainbow Table ها چگونه کار می کنند؟

کرک کردن کلیدهای WPA/WPA2 که توسط برنامه های رایجی مانند aircrack-ng، hashcat، John the Ripper و pyrit به دو روش دیکشنری و بروت فرس انجام می شود سرعت بسیار پایینی برای تست کلید ها در هر ثانیه دارد و بسیار طولانی از نظر زمان و فشار به سیستم می باشد. روشی دیگری وجود دارد که سرعت بسیار بالایی نسبت به روش های قبل دارد نام این روش Rainbow Table می باشد. همانطور که گفتیم Rainbow Table ها جدول های هش از پیش محاسبه شده برای هر SSID و Password است ، در واقع ما با محاسبه جداگانه ی هش برای هر کلمه داخل دیکشنری و SSID از فشار به سیستم و طولانی شدن زمان کرک جلوگیری می کنیم . برای آنکه در مکانیزم رمزنگاری WPA/WPA2 از SSID شبکه استفاده می شود برای ساخت Rainbow Table نیاز داریم SSID شبکه را هم وارد کنیم. در برنامه های aircrack و مشابه آن هنگامی که از دیکشنری استفاده می کنیم برنامه ابتدا از ترکیب SSID و پسورد داخل دیکشنری هش را محاسبه می کند سپس این هش را با هش داخل فایل 4 Way Handshake مقایسه می کند اگر یکسان بود پسورد صحیح نمایش داده می شود ولی در Rainbow Table ها این هش ها توسط برنامه دیگری محاسبه و در فایل جداگانه ای ذخیره می کنیم، سپس وقتی این فایل هش را وارد برنامه ای مانند aircrack-ng می کنیم برنامه دیگر عمل محاسبه هش را انجام نمی دهد و فقط به مقایسه هش های داخل فایل ساخته شده با هش موجود در فایل 4 Way Handshake می پردازد و به همین دلیل است که در این روش به سرعت بسیار بالایی برای تست هش ها در هر ثانیه می رسیم. در شکل زیر PMK ساخته شده توسط Rainbow Table با PMK داخل Handshake مقایسه می شود و در صورت یکسان بودن کلید صحیح نمایش داده می شود:



PMK Handshake = **kip5io4pi464** **Password:123458**

ساخت این Table ها برای دیکشنری های که دارای کلمات بسیار زیادی هستند زمان بسیار زیادی را صرف می کند به همین دلیل برای راحتی معمولا توسط افراد دیگر که دارای سخت افزارهای قوی هستند یکبار ساخته می شود و بارها توسط دیگران استفاده می شود . Table ها به دلیل حجم بالایی که دارند معمولا روی هارد های اکسترنال به فروش می رسد . نکته ای دیگر که باید در مورد Rainbow Table ها توجه داشت بحث SSID است . همانطور که گفتیم SSID برای ساخت هش استفاده می شود پس اگر Rainbow Table ای برای SSID مثلا DLink ساخته شود من می توانم این Rainbow Table ساخته شده برای SSID شبکه DLink استفاده کنم اما اگر نام شبکه فرق کند مانند SuperMan دیگر Rainbow Table شبکه با نام DLink برای آن قابل استفاده نیست و باید از نو Rainbow Table برای آن SSID ساخته شود .

مجموعه ای از Rainbow Table ها برای SSID های مختلف را از سایت های زیر قابل دانلود است :

https://nodegun.wordpress.com/2012/10/22/pre-computed-hashes

http://www.renderlab.net/projects/WPA-tables/

حجم فایل Rainbow Table چندین برابر حجم فایل دیکشنری است و ممکن است به چندین گیگابایت هم برسد پس قبل از شروع کار از داشتن فضای کافی در هارد سیستم اطمینان حاصل کنید.
سه برنامه رایج برای ساخت این Table ها وجود دارد که به ترتیب اولویت از نظر سرعت در ساخت لیست شده اند:

pyrit < genpmk < airolib

زمان ساخت Table ها توسط pyrit بسیار کمتر از ساخت با برنامه های genpmk و airolib است به طوری که برای ساخت Table از یک دیکشنری حدود ۱ میلیون کلمه ای توسط pyrit حدود ۱۵ دقیقه زمان لازم است اما در برنامه های genpmk و airolib-ng این زمان حدود ۵۰ دقیقه می باشد.

ساخت Rainbow Table توسط pyrit

Pyrit یکی از برنامه های حمله به WPA/WPA2 توسط استفاده از قدرت CPU و کارت گرافیک می باشد.
می توان سه روش دیکشنری و بروت فرس و Rainbow Table را با آن انجام داد.

بعد از اینکه فایل 4 Way Handshake و دیکشنری خود را آماده کردید دستور زیر را در خط فرمان تایپ کنید :

این دستور SSID شبکه هدف را وارد دیتابیس pyrit می کند :

```
pyrit –e Dlink create_essid
```

-e : باید نام شبکه مورد نظر نوشته شود .(برای هدف من Dlink است .)

دیکشنری مورد نظر را وارد دیتابیس pyrit می کنیم :

```
pyrit -i darkc0de.lst import_passwords
```

-r : مسیر فایل دیکشنری (darkc0de.lst نام فایل دیکشنری است.)

```
root@kali:~#
root@kali:~#
root@kali:~# pyrit -i darkc0de.lst import_passwords
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
1707658 lines read. Flushing buffers....  ..
All done.
root@kali:~#
root@kali:~#
root@kali:~#
```

با دستور زیر SSID و دیکشنری را در دیتابیس می بینیم :

```
pyrit eval
```

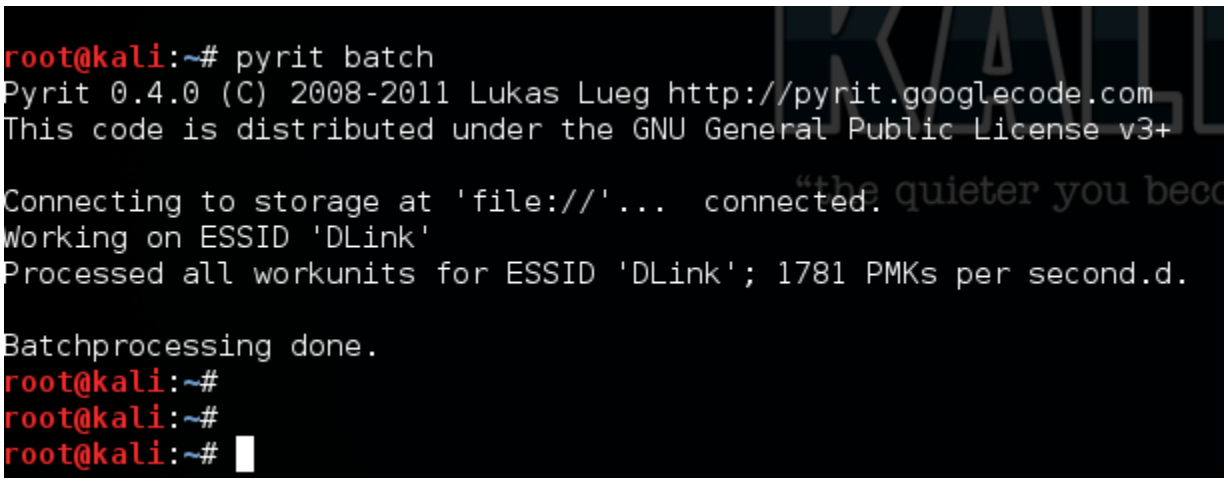
```
root@kali:~#
root@kali:~#
root@kali:~# pyrit eval
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Connecting to storage at 'file://'...  connected.
Passwords available: 993933

ESSID 'DLink' : 0 (0.00%)
```

این دستور نشان می دهد که ۹۹۳۹۳۳ پسورد در دیکشنری وجود دارد اما اگر در مرحله قبل دقت کرده باشید برنامه ۱۷۰۷۶۵۸ پسورد را می خواند علت این است pyrit کلمات کمتر از ۸ کاراکتر و نامناسب برای WPA/WPA2 را فیلتر می کند و بدین ترتیب از اتلاف زمان جلوگیری می کند.0.00% به این معنی است هنوز هیچ Table ای برای کلمات ساخته نشده است .

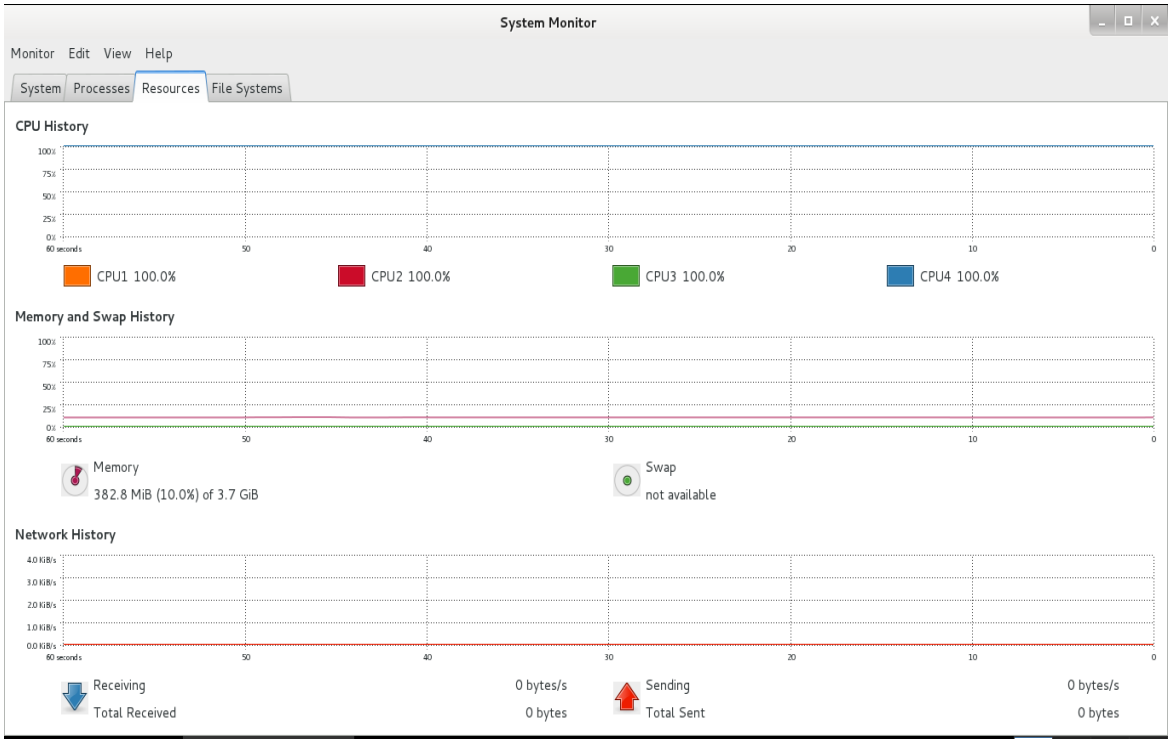
با دستور زیر Table سازی را شروع می کنیم :

```
pyrit batch
```

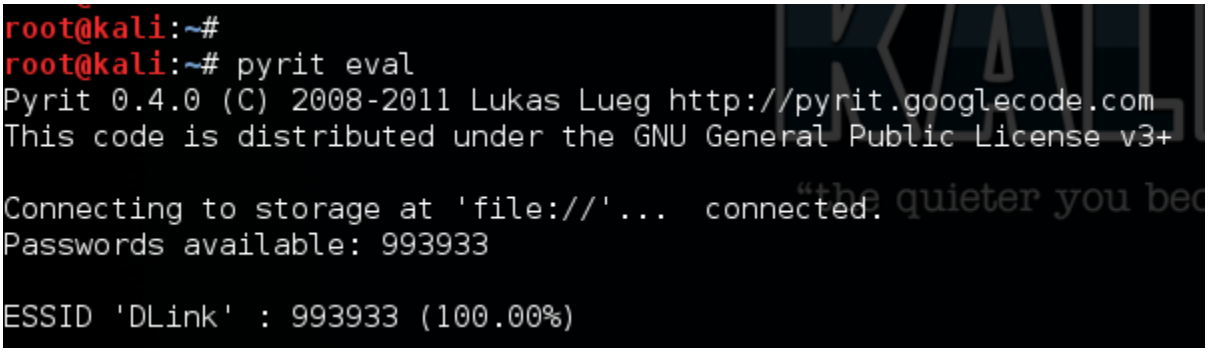
منتظر می مانیم تا برنامه کار خود را انجام دهد، هنگامی که Table سازی به پایان برسد با پیغام Batchprocessing done مواجه می شویم.



ساخت Table ها باعث کار ۱۰۰ ٪ cpu و بالا رفتن دمای آن می باشد، می توانید توسط برنامه system monitor در کالی لینوکس وضعیت سخت افزار را مشاهده کنید :



دوباره با دستور pyrit eval ساخت Table ها را مشاهده می کنیم :



100% نشان دهنده ساخت کامل Table ها برای ۹۹۳۹۳۳ کلمه داخل دیکشنری است.

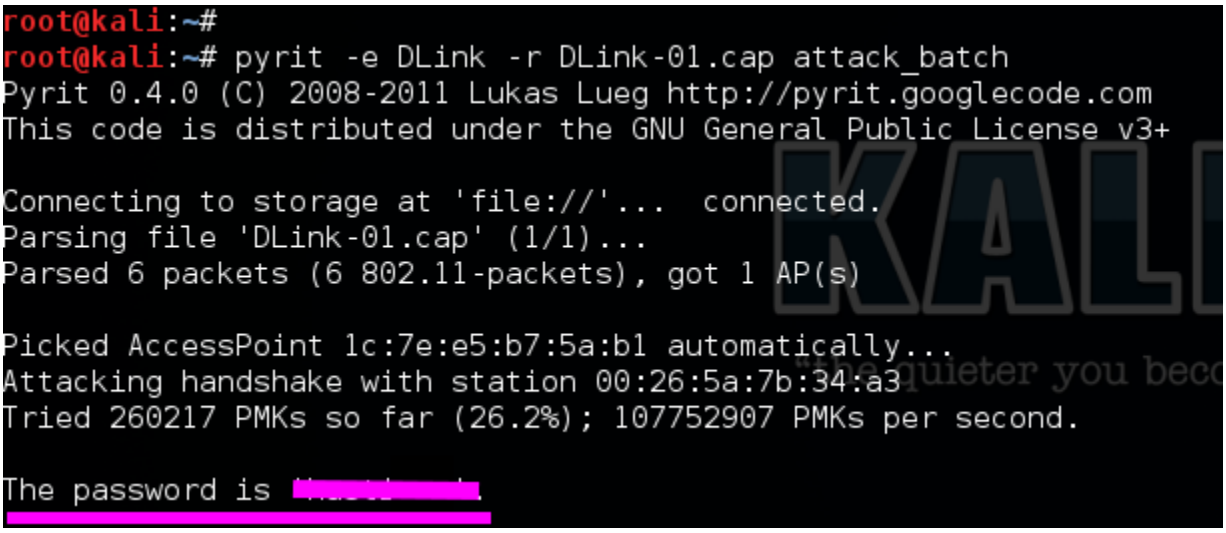
سپس این Table ها را برای کرک کردن وارد برنامه pyrit می کنیم :

```
pyrit –e Dlink –r Dlink-01.cap attack_batch
```

e- : نام شبکه

r- : فایل Handshake

attack_batch : حمله Rainbow Table



که در صورت یکسان بودن هش های ساخته شده توسط برنامه و هش داخل فایل هندشیک کلید صحیح در قسمت The Password is نمایش داده می شود. در مثال بالا بعد از چند ثانیه پسورد صحیح برای من نمایش داده شد.
اما زمان تست تقریبا همین لغت ها به روش دیکشنری توسط برنامه aircrack-ng ، ۱۱ دقیقه می باشد:

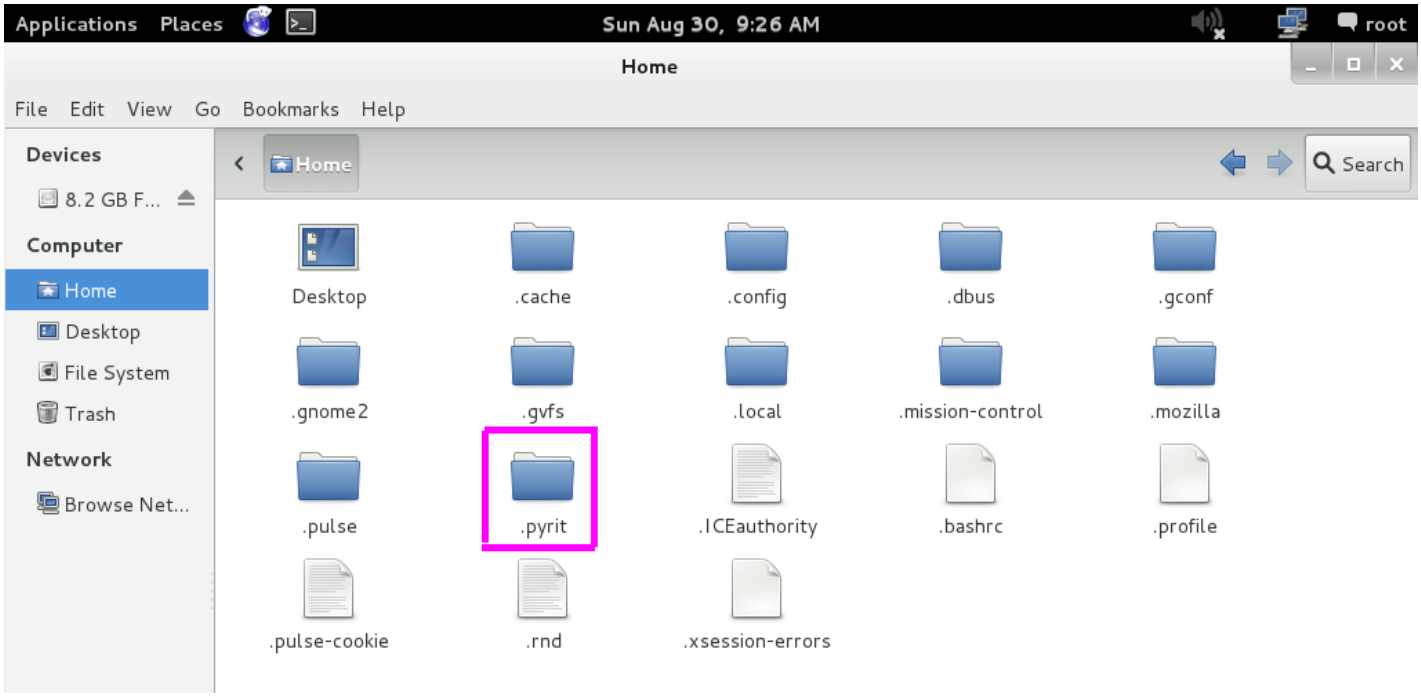
ذخیره Rainbow Table های pyrit

یکی از سوالاتی مهمی که ممکن است برای خوانندگان ایجاد شود این است که آیا می توان Rainbow Table ساخته توسط pyrit را برای استفاده های بعدی ذخیره کرد؟ بله می توان این کار را به سادگی انجام داد.

دیتابیس pyrit به طور پیش فرض در مسیر زیر ذخیره می شود:

Computer→Home

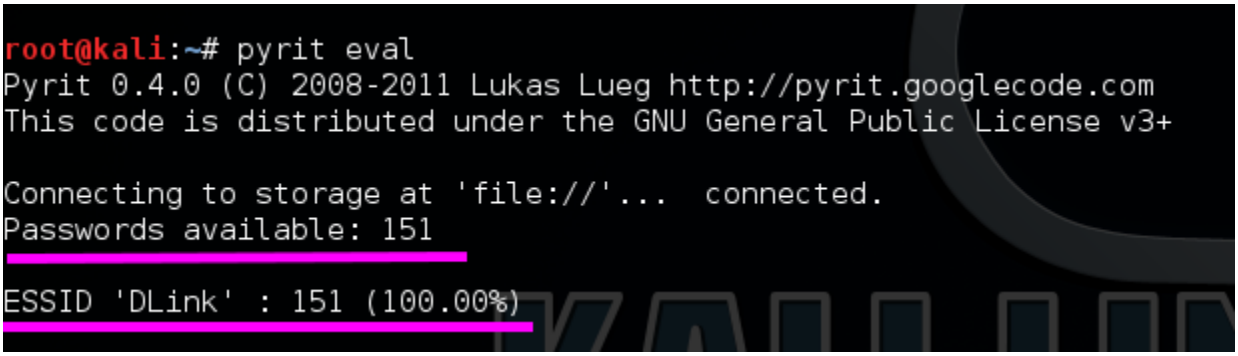
اما وقتی وارد این مسیر می شوید به دلیل اینکه فایل ها مخفی شده اند شما فایلی مشاهده نمی کنید با فشار دادن کلید های Ctrl + H فایل های مخفی ظاهر می شوند :



پوشه .pyrit حاوی Rainbow Table ساخته شده توسط برنامه pyrit است . کل این فایل را به صورت فشرده در می آوریم و در هارد یا فلش خود ذخیره می کنیم. برای استفاده های بعدی فایل فشرده را Extract می کنیم و کل Folder را با نام .pyrit در مسیر Computer→Home قرار می دهیم.

با دستور زیر اطمینان حاصل می کنیم آیا Rainbow Table به درستی داخل برنامه pyrit وارد شده اند:

```
pyrit eval
```



نتیجه این دستور نشان می دهد که Rainbow Table ها با موفقیت وارد برنامه شده اند.

استفاده از Rainbow Table ها توسط cowpatty

cowpatty هم مانند pyrit برنامه ای برای کرک کلید های WPA/WPA2 می باشد. می توانیم Table ای را که توسط pyrit ساخته ایم وارد برنامه cowpatty کنیم و توسط آن کرک را انجام دهیم :

ابتدا باید فایل Rainbow Table که در مرحله قبل ساختیم را برای برنامه cowpatty آماده کنیم :

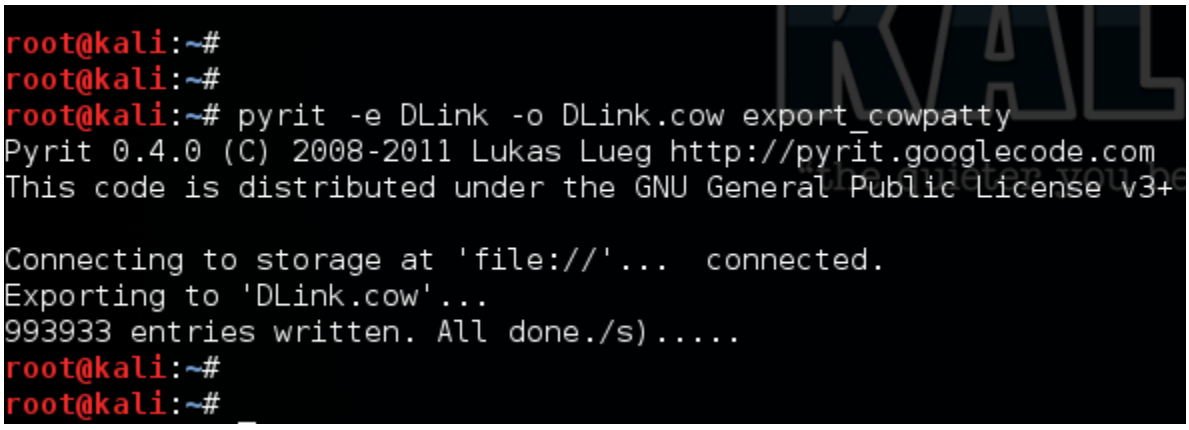
دستور زیر را تایپ کنید :

```
pyrit –e Dlink –o Dlink.cow export_cowpatty
```

-e : SSID شبکه

-o : نام فایل هش برای استفاده در برنامه cowpatty (این فایل در پوشه Home قرار می گیرد. می توانید روی هارد خود ذخیره کنید و در کرک های بعدی از آن استفاده کنید.)

export_cowpatty : ساخت فایل هش برای استفاده در برنامه cowpatty



با دستور زیر کرک را شروع می کنیم :

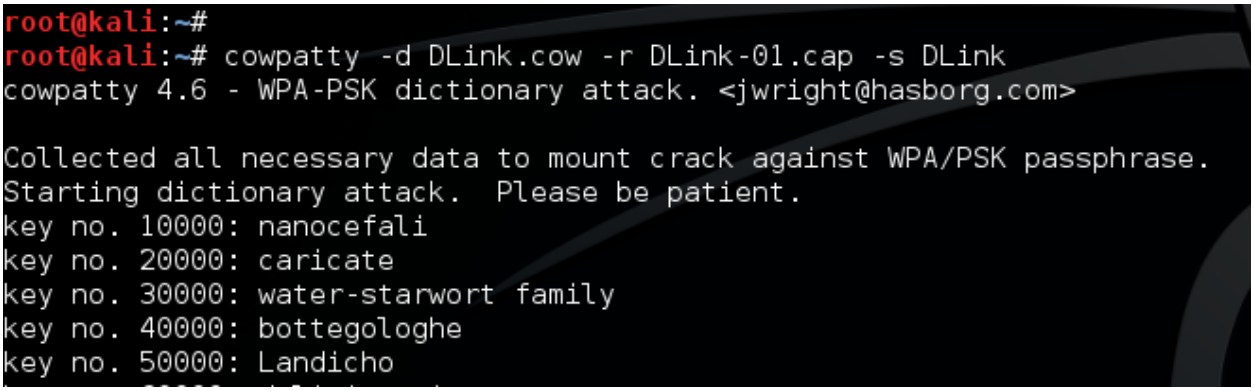
```
cowpatty –d Dlink.cow –r Dlink-01.cap –s Dlink
```

-d : فایل ساخته شده توسط برنامه pyrit

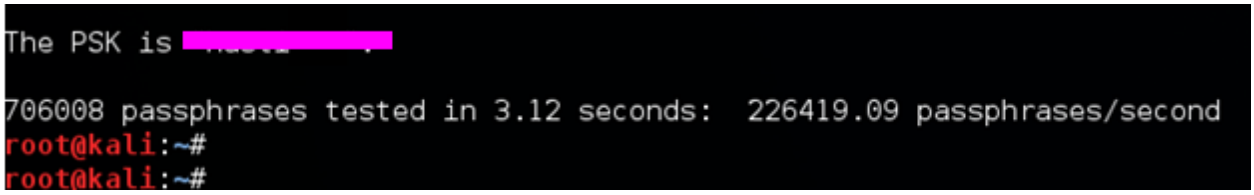
-r : فایل 4 Way Handshake

-s : SSID شبکه

بعد از اجرای دستور بالا برنامه شروع به تست هش ها می کند :



بعد از حدود ۳ ثانیه :



کلید صحیح در قسمت The PSK is پیدا شد . سرعت تست برنامه همانطور که می بینید ۲۲۶/۴۱۹ هش هر ثانیه است یعنی ۷۰۶ هزار هش در ۳ ثانیه بررسی شد و پسورد درست برای ما پیدا شد در حالی که این سرعت در برنامه aircrack-ng حدود ۱۶۰۰ هش هر ثانیه بود.

ساخت Rainbow Table ها توسط genpmk

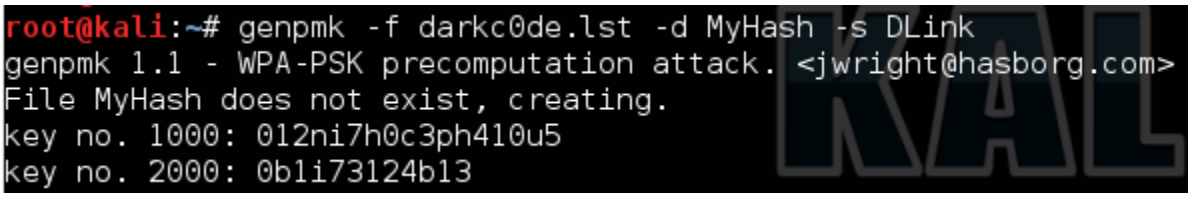
Table ها را می توان توسط برنامه genpmk هم ساخت ، اما زمان آن طولانی تر از pyrit است :

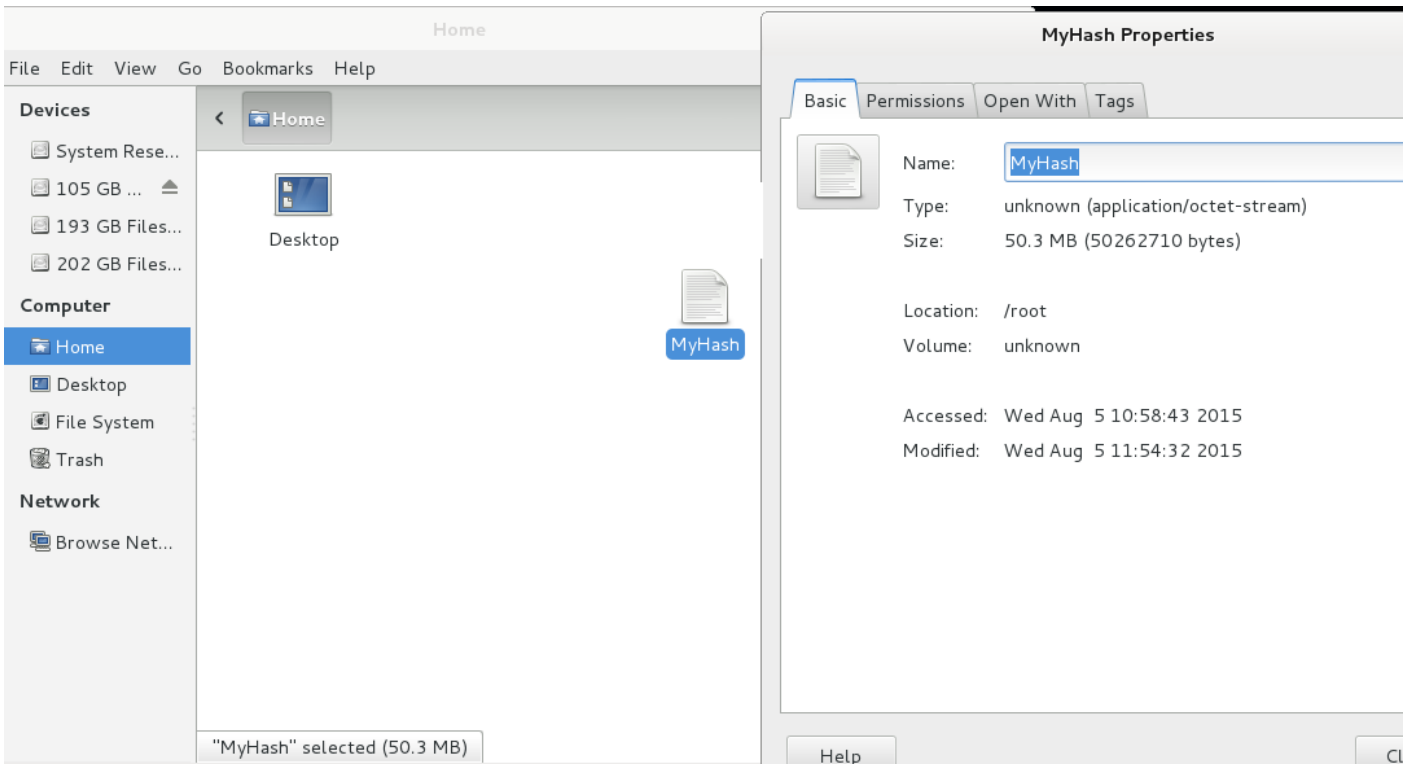
```
genpmk –f darkc0de.lst –d MyHash –s Dlink
```

-f : نام فایل دیکشنری (darkc0de.lst نام فایل دیکشنری است.)

-d : نام فایل خروجی Table(این فایل در پوشه Home ایجاد می شود.)

-s : نام شبکه





محل ایجاد فایل هش توسط برنامه genpmk

سپس بعد از مدتی Table ها ایجاد می شود:

```
1148075 passphrases tested in 3349.70 seconds:  342.74 passphrases/second
```

اکنون فایل هش ساخته شده در برنامه cowpatty وارد می کنیم :

```
cowpatty –d MyHash –r Dlink-01.cap –s Dlink
```

-d : فایل هش

-r : فایل هندشیک

-s : نام شبکه

```
root@kali:~#
root@kali:~# cowpatty -d MyHash -r DLink-01.cap -s DLink
cowpatty 4.6 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.
Starting dictionary attack.  Please be patient.
key no. 10000: 1 CATARINA
key no. 20000: 1 MEDUNA
key no. 30000: 10177312312
key no. 40000: 13uc0cidin
```

و بعد از ۵ ثانیه کلید در The PSK is نمایش داده شد !!

```
The PSK is "[redacted]".

1148074 passphrases tested in 5.13 seconds:  223898.72 passphrases/second
```

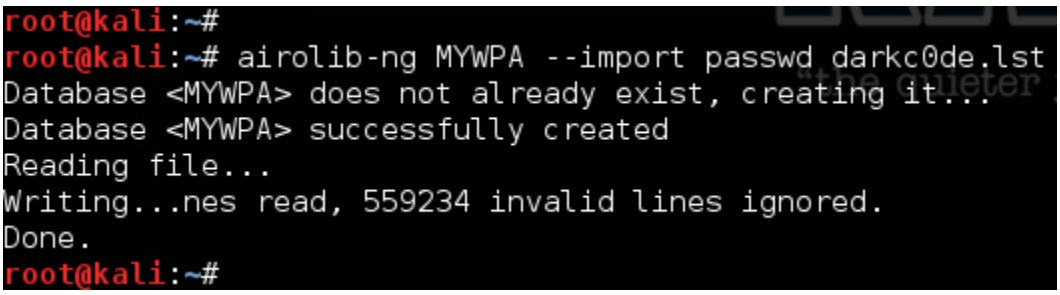
ساخت Rainbow Table ها توسط برنامه airolib-ng

Table ها را می توان توسط برنامه دیگری به نام airolib ایجاد کرد. این برنامه از دو برنامه قبل زمان طولانی تر برای ساخت Table ها می گیرد و پیشنهاد استفاده از دو برنامه بالا می باشد.

دستور زیر فایلی را ایجاد می کند و محتویات فایل دیکشنری به آن وارد می شود :

```
airolib-ng MYWPA --import passwed darkc0de.lst
```

MYWPA : نام فایل خروجی Table
darkc0de.lst : نام فایل دیکشنری



با دستور echo فایلی حاوی نام SSID ایجاد و آن را به airolib-ng وارد می کنیم:

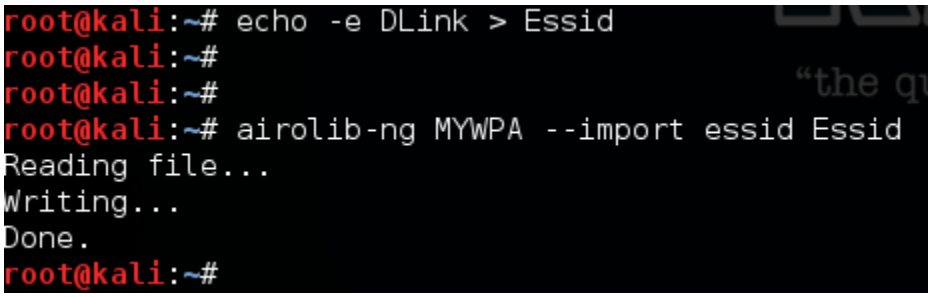
```
echo –e Dlink > Essid
```

-e : SSID شبکه

سپس SSID را به برنامه airolib-ng وارد می کنیم :

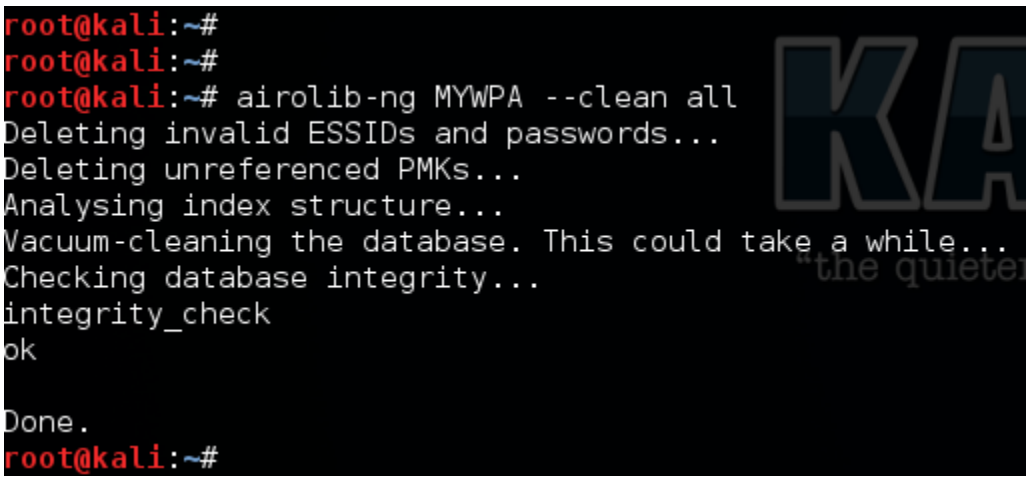
```
airolib-ng MYWPA --import essid Essid
```

MYWPA : نام فایل خروجی Table



دستور زیر برای پاکسازی فایل های اضافی ایجاد شده توسط airolib-ng اجرا می کنیم:

```
airolib-ng MYWPA --clean all
```



دستور زیر را برای Table سازی اجرا می کنیم:

```
airolib-ng MYWPA --batch
```

MYWPA : نام فایل خروجی Table

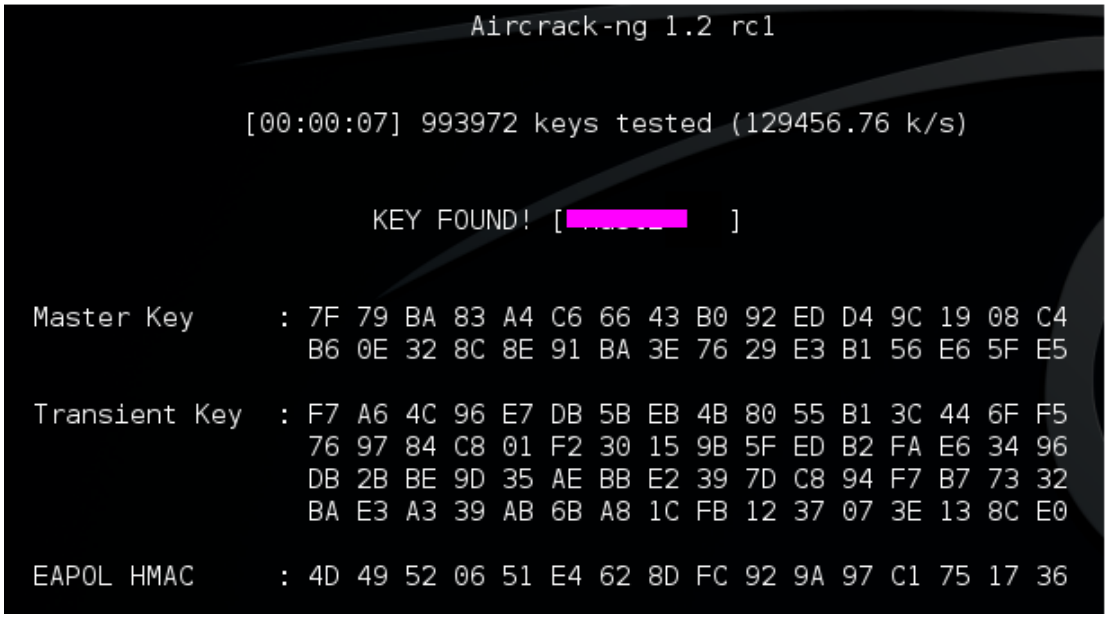
```
root@kali:~# airolib-ng MYWPA --batch
Computed 993974 PMK in 2812 seconds (353 PMK/s, 0 in buffer). All ESSID processed.

root@kali:~#
```

Table با موفقیت ایجاد شد سپس فایل MYWPA را برای کرک به برنامه aircrack-ng وارد می کنیم :

```
aircrack-ng –r MYWPA Dlink-01.cap
```

r- : نام فایل خروجی Table

Dlink-01.cap : نام فایل 4 Way Handshake



نتیجه گیری:

اساس روش Rainbow Table ها دیکشنری می باشد و یک حمله موفق نیاز به دانستن دقیق طول کلید و نوع کاراکترهای WPA/WPA2 می باشد هر چند که روش Rainbow Table ممکن است با شکست در پیدا کردن کلید مواجه شود اما برهرحال یکی سریع ترین روش های عمومی برای حمله به WPA/WPA2 است .برای انجام روش Rainbow Table اولویت با برنامه pyrit و cowpatty به دلیل سرعت بالایی که دارند می باشد برای جلوگیری از حمله WPA/WPA2 انتخاب کلید های طولانی و پیچیده می توان شبکه شما را امن نگه دارد همچنین به کاربران خود آموزش دهید که این کلید را در اختیار دیگران قرار ندهند.