

# ساخت Pyrit Cluster در کالی لینوکس

در این مقاله به آموزش ساخت کلاستر توسط pyrit در کالی لینوکس برای افزایش سرعت کرک WPA/WPA2 می پردازیم.

# KALI LINUX™

“the quieter you become, the more you are able to hear”

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. نویسندگان و سایت های ارائه دهنده هیچ مسئولیتی نخواهند داشت.

قانونمند رفتار کنیم.

نویسنده: سهیل رضاشعار

soheilshoar@gmail.com

1394-2015

ستامبر - شهر یور

# فهرست مطالب

صفحه	عنوان
۳.....	مقدمه.....
۴.....	ابزارهای مورد نیاز.....
۵.....	ساخت کلاستر توسط pyrit.....
۱۱.....	نتیجه گیری.....

یکی از روش های افزایش سرعت در حمله به کلید های WPA/WPA2 ترکیب چند سیستم باهم و استفاده از قدرت سخت افزاری آن ها در یک سیستم می باشد، به این روش کلاستر (Cluster) می گویند. معنی لغوی کلاستر ، خوشه بندی می باشد و در تعریف عبارت است از کار کرد چند سیستم به عنوان یک سیستم واحد به طوری که بازدهی یک سیستم چند برابر می شود .

کلاستر توسط یک سیستم به عنوان Server و تعدادی سیستم دیگر به عنوان Client کار می کند به این صورت که قدرت سخت افزاری کلاینت ها در یک سرور باهم ترکیب می شوند و سرعت بالایی را نتیجه می دهند. بدیهی است که هرچقدر تعداد کلاینت ها و قدرت سخت افزاری آن ها بالاتر باشد سرعت کرک کردن بالاتر خواهد بود. برنامه pyrit این امکان را می دهد که بتوان کلاستر را پیاده سازی کرد و از قدرت آن برای کرک کلید های WPA/WPA2 استفاده کنیم .

## ابزارهای مورد نیاز

۱. سیستم عامل کالی لینوکس : کالی لینوکس روی سرور و تمامی کلاینت ها باید نصب شود. از آدرس زیر می توانید نسخه ۶۴ بیتی آن را دانلود کنید:

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

۲. برنامه ماشین مجازی **VirtualBox** : ( این مورد اختیاری می باشد. شما می توانید کالی لینوکس را مستقیماً در سیستم خود اجرا کنید، مثال این مقاله براساس ماشین مجازی **VirtualBox** نوشته شده است.)

۳. فایل **4 Way Handshake** : این فایل باید قبلاً توسط برنامه **airodump-ng** بدست آمده باشد.

۴. سرور : سیستمی به عنوان سرور برای استفاده از سخت افزار کلاینت ها.

۵. کلاینت : تعداد کلاینت برای ایجاد کلاستر می تواند از یک تا ده ها سیستم باشد.

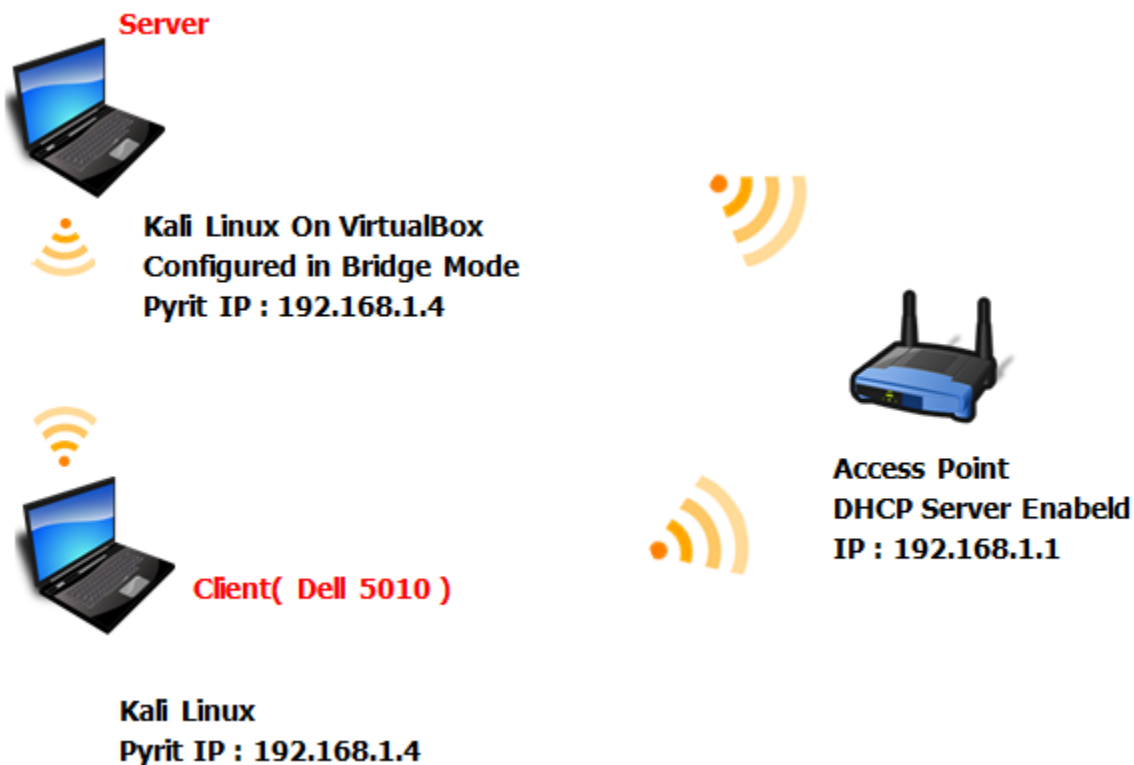
۶. برنامه **pyrit** : این برنامه وظیفه ساخت و پیکربندی کلاستر را بر عهده دارد که به طور پیش فرض در کالی لینوکس نصب است.

۷. ایجاد شبکه داخلی بین سرور و کلاینت ها توسط سویچ یا اکسس پوینت

## ساخت کلاستر بوسیله pyrit

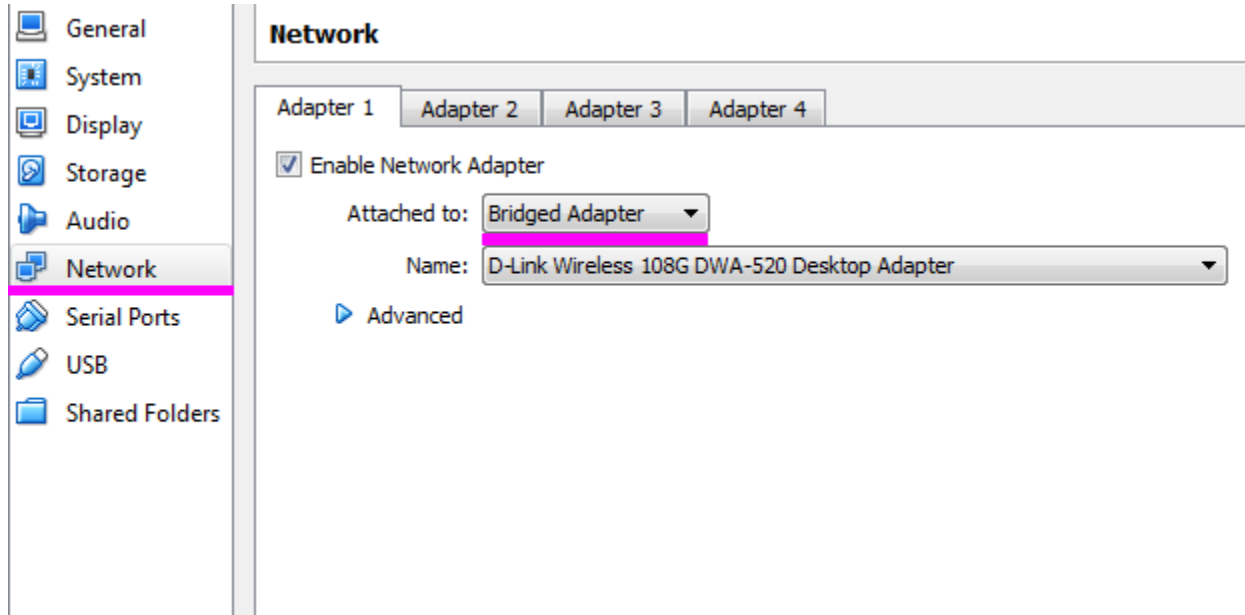
ساخت کلاستر به وسیله pyrit به سادگی انجام می شود، ابتدا نیاز به ایجاد شبکه ای بین سرور و کلاینت ها داریم که این کار را می توان با یک اکسس پوینت یا سویچ انجام داد بعد از بررسی اینکه سیستم ها توانایی ارتباط با یکدیگر را دارند یک سیستم را به عنوان سرور انتخاب می کنیم و کالی لینوکس را به صورت مستقیم یا توسط VirtualBox روی آن اجرا می کنیم سپس فایل پیکربندی مربوط به pyrit را در سرور ایجاد و IP سرور را در آن وارد می کنیم. کالی لینوکس را روی هر یک از کلاینت ها نصب می کنیم و IP سرور را در فایل پیکربندی pyrit آن ها وارد می کنیم این کار باعث می شود کلاینت ها توانایی برقراری ارتباط با سرور را داشته باشند، از سرور برنامه pyrit را اجرا می کنیم برنامه قدرت سخت افزار تمامی کلاینت ها را باهم ترکیب می کند و مراحل کرک کردن را دنبال می کنیم .

شکل زیر ساده ترین نوع کلاستر را نشان می دهد که در سیستم سرور کالی لینوکس در VirtualBox نصب شده است و برای آنکه کالی لینوکس در ماشین مجازی به عنوان یک سیستم واقعی در شبکه عمل کند آن را در حالت Bridge پیکربندی می کنیم با این کار کالی لینوکس داخل ماشین مجازی به طور خود کار از DHCP Server آی پی دریافت می کند. سپس یک لپ تاپ به عنوان کلاینت انتخاب کرده ایم و IP سرور را در آن وارد کرده ایم :

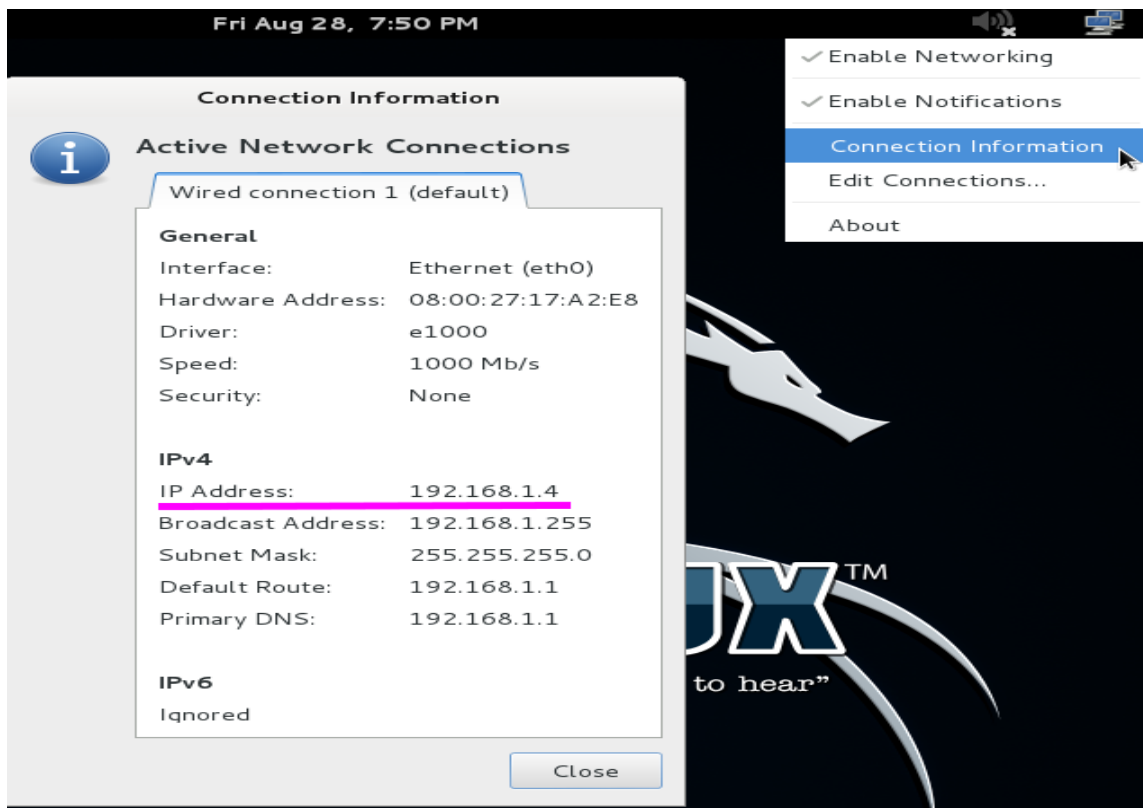


## پیکربندی pyrit

برای ساخت کلاستر ابتدا ماشین مجازی را در حالت Bridge پیکربندی می کنیم ، برای این کار وارد تنظیمات ماشین مجازی شوید و مانند عکس زیر آن را در حالت Bridge قرار دهید :



بعد از اجرای کالی لینوکس در ماشین مجازی، آی پی ماشین مجازی را توسط کلیک راست روی کانکشن بالا سمت راست دسکتاپ بدست می آوریم :



فایل مربوط به پیکربندی pyrit را برای کار در حالت کلاستر ایجاد می کنیم:  
با دستور زیر یک دایرکتوری به نام pyrit ایجاد می شود:

```
mkdir ~/.pyrit
```

```
root@kali:~# mkdir ~/.pyrit
```





با دستور زیر فایللی به اسم config باز می کنیم :

```
nano ~/.pyrit/config
```

```
root@kali:~# nano ~/.pyrit/config
```

اکنون دستورات زیر را در آن کپی می کنیم و آی پی ای که در مرحله قبل بدست آوردیم را می نویسیم:

```
default_storage = file://  
limit_ncpus = 0  
rpc_announce = true  
rpc_announce_broadcast = false  
rpc_knownclients = 192.168.1.4  
rpc_server = true  
workunit_size = 75000
```

```
Applications Places   Fri Aug 28, 7:57 PM   root
root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.2.6 New Buffer Modified
default_storage = file://
limit_ncpus = 0
rpc_announce = true
rpc_announce_broadcast = false
rpc_knownclients = 192.168.1.4
rpc_server = true
workunit_size = 75000
KALI LINUX™
"the quieter you become, the more you are able to hear"
^G Get Help      ^O WriteOut     ^R Read File    ^V Prev Page   ^K Cut Text     ^C Cur Pos
^X Exit          ^J Justify      ^W Where Is    ^N Next Page   ^U UnCut Text  ^T To Spell
```

فایل را ذخیره کنید. پیکربندی Server انجام شد. برای پیکربندی کلاینت ها کالی لینوکس را روی هر کدام نصب و مراحل قبل یعنی ایجاد فایل config و وارد کردن آی پی سرور را برای هر کدام انجام می دهیم. اکنون به سرور مراجعه می کنیم و بررسی می کنیم که آیا قدرت کلاینت در سرور وارد می شود یا نه؟! برای این کار دستور زیر را تایپ کنید :

```
pyrit list_cores
```

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

The following cores seem available...
#1: 'CPU-Core (SSE2)'
#2: 'Network-Clients'
root@kali:~#
```



از نتیجه این دستور می توان متوجه شد که pyrit آماده استفاده از CPU سرور و کلاینت های داخل شبکه برای کرک کردن می باشد.

برای فعال سازی کلاستر دستور زیر را در سرور اجرا کنید:

pyrit serve

```
root@kali:~# pyrit serve
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+
Serving 0 active clients; 0 PMKs/s; 0.0 TTS
```

برای اینکه ببینیم سرعت تست کلیدها در هر ثانیه توسط کلاینت ها چقدر است از دستور استفاده می کنیم:

یک Tab دیگر در خط فرمان باز کنید و تایپ کنید:

pyrit benchmark

```
root@kali:~# pyrit benchmark
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+
Running benchmark (555.4 PMKs/s)... -
Computed 555.41 PMKs/s total.
#1: 'CPU-Core (SSE2)': 410.1 PMKs/s (RTT 3.0)
#2: 'Network-Clients': 264.4 PMKs/s (RTT 10.1)
```

در حالی که benchmark اجرا است به pyrit serve نگاهی می اندازیم :

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

Serving 1 active clients; 105 PMKs/s; 3.6 TTS
```

می بینیم که برنامه از وجود یک کلاینت فعال در شبکه اطلاع می دهد و سرعت تست کلید ها توسط کلاینت 105 PMK/s می باشد.

فایل هندشیک خود را آماده می کنیم و با دستور زیر به روش دیکشنری با برنامه pyrit کرک را شروع می کنیم :

```
root@kali:~# pyrit -r MYWPA-01.cap -i rockyou.txt attack_passthrough
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'MYWPA-01.cap' (1/1)...
Parsed 6 packets (6 802.11-packets), got 1 AP(s)

Picked AccessPoint 1c:7e:e5:b7:5a:b1 ('DLink') automatically.
Tried 80004 PMKs so far; 1307 PMKs per second.
```

سرعت تست 1307 PMK/s است. این سرعت از ترکیب سیستم سرور و کلاینت به دست آمده است.

در همین حال به pyrit serve نگاهی می اندازیم و می بینیم که pyrit برای کرک کردن از قدرت کلاینت در حال استفاده است:

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

Serving 1 active clients; 421 PMKs/s; 11.9 TTS
```

نکته ای باید توجه داشت این است به دلیل اینکه کالی لینوکس در VirtualBox و در کلاینت توسط USB اجرا شده است و همزمان برنامه های دیگر هم در حال اجرا می باشند سخت افزار سیستم بسیار درگیر است و سرعت دقیق و واقعی را نشان نمی دهد. ما در این مقاله برای نشان دادن مثال کلاستر آن را در VirtualBox اجرا کنیم. نصب کالی لینوکس به طور مستقیم بر روی سرور و تمامی کلاینت ها بهترین کار برای ساخت کلاستر می باشد.

**نتیجه گیری:** کلاستر ها می توانند راه حل خوبی برای افزایش سرعت حمله به کلید های WPA/WPA2 باشد مخصوص زمانی که سیستم ها از قدرت سخت افزاری بالا برخوردار باشند. کلاستر را می توان در سیستم عامل ویندوز هم ایجاد کرد و قدرت کارت گرافیک را هم در آن وارد نمود و به سرعت بالاتری نسبت به CPU رسید.