آزمایشگاه و مرکز تخصصی آپا

در حوزه پایگاه داده ها

روش‌های کشف شناسه سیستم در پایگاه داده‌های اوراکل (قسمت اول)

علی عباسی

abbasi@ustmb.ac.ir

فروردین ماه ۱۳۸۸

مقاله سفید

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

امروزه اطلاعات عمومی زیادی راجع به امنیت اوراکل و آسیب‌پذیری های مختلفی که نفوذگر میتواند به وسیله آنها به پایگاه داده‌ها دسترسی یابد وجود دارد. سناریو های رایج حمله به پایگاه داده‌ها به ترتیب شامل موارد زیر است :

- ✓ حمله به Listener (حملات سر ریزی بافر و یا فایل های رویداد نامه)
- ✓ حدس نام کاربری و کلمه عبور
- ✓ حدس شناسه سیستم (SID Guess)
- ✓ حملات ارتقاع سطح دسترسی (Privilege Escalation) در پایگاه داده (تززیق‌های PL/SQL ، سرریزی بافر، Cursor Snarfing ، شکاندن کلمات عبور در هم سازی شده از طریق حملات جستجوی تمام حالات و.....)
- ✓ دسترسی به سیستم عامل (از طریق Extproc ، Java ، UTL_File ، DBMS_LOB)
- ✓ نصب روت کیت و یا در پشتی (Back Door)
- ✓ پاکسازی فایل های رویداد نامه و ممیزی (مانند SYS.AUD$ و غیره...)

بسیاری از این مراحل به خوبی در منابع مختلف تشریح شده اند. حساب های کاربری پیش فرض مشکلات بزرگ شناخته شده ای هستند که اطلاعات زیادی راجع به آنها وجود دارد .با توجه به آسیب پذیری های موجود متاسفانه تنها ۱۰ درصد راهبران پایگاه داده (DBA) به طور منظم بسته های بروز رسانی مهم را نصب میکنند (گزارش شده توسط مرکز امنیت و کنترل فعالیت های پایگاه داده Sentrigo) . دسترسی به فایل های سیستم عامل و پوسته میتواند به وسیله تکنیک های مختلفی مانند Extproc ، جاوا ، DBMS_JOB ، UTL_FILE ، DBMS_LOB و ... اجرا گردد.

با توجه به روت کیت ها و پاکسازی داده های ممیزی ، در این حوزه نفوذگران یک قدم جلوتر از راهبر پایگاه داده هستند. در بین اطلاعات موجود راجع به امنیت اوراکل ، یک حوزه وجود دارد که به خوبی دیگر موارد تشریح نشده است . موضوع مورد اشاره ما به دست آوردن شناسه سیستم اوراکل است . بدون دانستن

شناسه سیستم پایگاه داده اوراکل ، نفوذگر حتی با دانستن نام کاربری و کلمه عبور نمیتواند به پایگاه داده دسترسی یابد.

پروسه دریافت شناسه سیستم پایگاه داده در اوراکل 10g به راحتی گذشته نیست. دلیل اصلی نگارش این مطلب نیز همین است . در این مقاله ما سعی کرده ایم تمامی روش های شناخته شده برای حدس و دریافت شناسه سیستم پایگاه داده و چند روش جدیدتر را مورد بررسی قرار دهیم.

اطلاعات اولیه راجع به شناسه سیستم و SERVICE NAME :

هر موردی در پایگاه داده به وسیله شناسه سیستم شناخته میشود. (System Identifier) . شناسه سیستم شامل علائم حروف و اعداد میباشد که در محل متغیر های سیستمی به نام ORACLE_SID ذخیره میشود. شناسه سیستم توسط ابزار های شبکه (network utility) موجود در اوراکل جهت دسترسی راه دور به پایگاه داده مورد استفاده قرار میگیرد. متغیر دیگری نیز به نام SERVICE NAME وجود دارد که بسیار شبیه به شناسه سیستم است ولی از بعضی از جهات با آن متفاوت است . SERVICE_NAME متغیر جدیدی است که در اوراکل 8i تعریف شد. SERVICE_NAME یک یا چند نام را برای سرویس پایگاه داده ای که به آن وصل میشود مشخص میکند. شما میتوانید نام های سرویس متعددی را برای تمیز دادن ما بین استفاده های متفاوت از یک پایگاه داده تعریف کنید.

اگر ما بتوانیم شناسه سیستم یا SERVICE_NAME پایگاه داده را به دست آوریم میتوانیم مراحل دیگر را نیز برای دسترسی به پایگاه داده امتحان کنیم. به عنوان مثال اگر ما از شناسه سیستم اطلاع داشته باشیم میتوانیم برای اجرای حمله ی جستجوی تمام حالات به حساب های پایگاه داده اقدام کنیم.

بدست آوردن شناسه سیستم و SERVICE_NAME :

راه عمومی و استاندارد بدست آوردن شناسه سیستم استفاده از ابزار lsnrctl (Listener Control) به همراه گزینه "Services" است .

```
LSNRCTL> services
```

```
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC)))
Services Summary...
Service "PLSExtProc" has 1 instance(s).
Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
Service "orcl" has 1 instance(s).
Instance "orcl", status READY, has 1 handler(s) for this service...
The command completed successfully
```

در خروجی این فرمان ما میتوانیم شناسه سیستم (با نام instance) و SERVICE_NAME (با نام Service) را در پایگاه داده مشاهده کنیم. در این مثال ما میتوانیم ببینیم که شناسه سیستم پایگاه داده "ORCL" میباشد.

اتصال به پایگاه داده با SERVICE_NAME :

اگر ما SERVICE_NAME را بدانیم به سادگی میتوانیم به وسیله ابزار شبکه ای sqlplus به پایگاه داده متصل شویم.

```
C:\ >sqlplus system/manager@192.168.40.33/orcl
SQL*Plus: Release 10.1.0.5.0 - Production on Wed Apr 08 17:18:23 2009
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options
SQL>
```

اتصال به پایگاه داده به وسیله شناسه سیستم :

برای اتصال به پایگاه داده به وسیله شناسه سیستم لازم است که در ابتدا یک توصیف کننده اتصال در فایل تنظیمات tnsnames.ora اضافه کنیم .

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

(SERVER = DEDICATED))

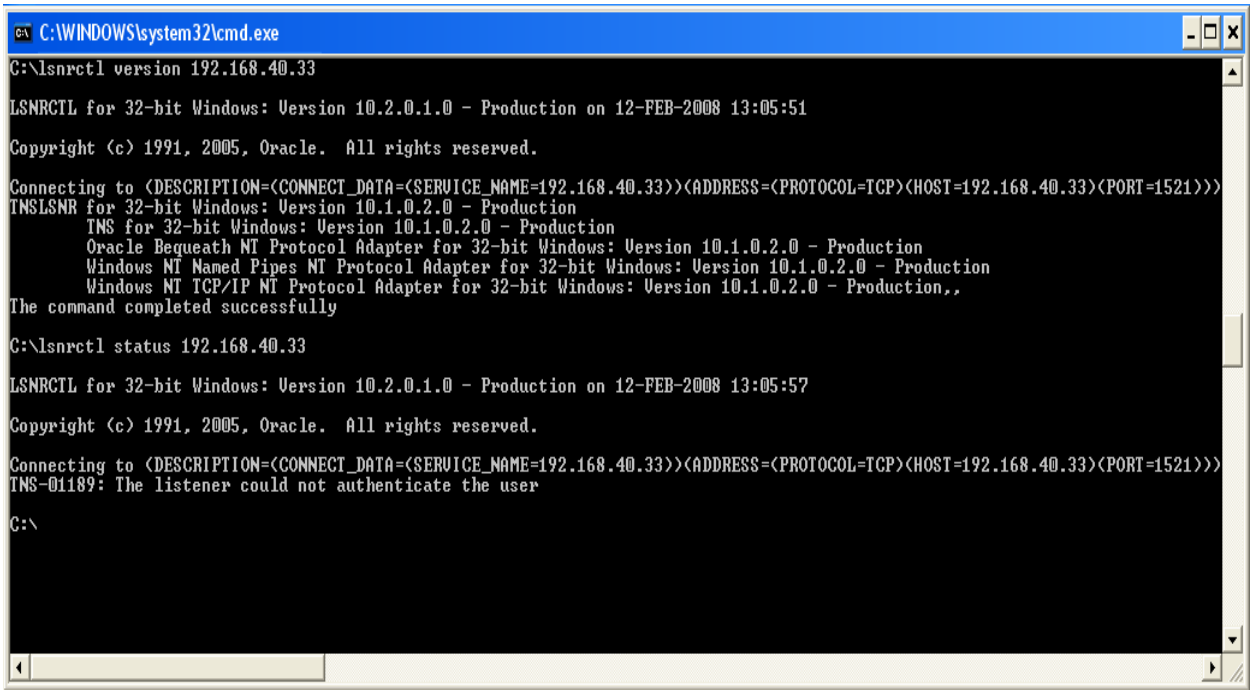
)

پس از تعریف کلمه اتصال با نام "orcl_192.168.40.33" ما میتوانیم از آن در sqlplus استفاده کنیم:

```
C:\ >sqlplus system/manager@orcl_192.168.40.33
SQL*Plus: Release 10.1.0.5.0 - Production on Wed Apr 08 17:18:23 2009
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production
With the Partitioning, OLAP and Data Mining options
SQL>
```

مشکلات دریافت شناسه سیستم و SERVICE_NAME در ویراش های جدیدتر اوراکل :

در ویرایش های جدیدتر اوراکل از نسخه 10g R1 به بالا از یک ویژگی امنیتی به نام LOCAL_OS_AUTHENTICATION به صورت پیش فرض استفاده میشود که اجازه استفاده از فرمان های Listener مانند "services" و "status" را از راه دور نمیدهد. این ویژگی امنیتی دلیل اصلی عدم امکان دریافت شناسه سیستم و SERVICE_NAME از طریق متد معرفی شده در بخش " بدست آوردن شناسه سیستم و SERVICE_NAME" میباشد.



همانطور که در بالا مشاهده میکنید ، اجرای فرمان "lsnrctl status" دراوراکل 10g ناموفق بود.

همچنین اگر راهبر سیستم در listener ویرایش ۹.۲.۰.۶ و پس از آن اقدام به نصب کلمه عبور کند ما امکان اجرای فرمان هایی از قبیل "services" و "status" را بدون دانستن کلمه عبور Listener نخواهیم داشت.

همانطور که مشاهده کردید در ویرایش های جدید پایگاه داده اوراکل ما باید به دنبال راه های جدیدی برای بدست آوردن شناسه سیستم باشیم. تمام راه های شناخته شده جهت بدست آوردن شناسه سیستم پایگاه داده را میتوانیم به ۳ گروه تقسیم کنیم:

۱- حدس زدن شناسه سیستم

۲- کشف شناسه سیستم به وسیله برنامه های ثالث

۳- بدست آوردن شناسه سیستم به وسیله دسترسی بیشتر

حدس زدن شناسه سیستم :

اولین قدم وقتی که ما نمیتوانیم شناسه سیستم را به وسیله فرمان های lsnrctl پیدا کنیم حدس شناسه سیستم میباشد.

۴ راه برای حدس زدن شناسه سیستم پایگاه داده وجود دارد :

۱- استفاده از شناسه های سیستمی پیشفرض

۲- استقاده از شناسه های سیستمی رایج و عمومی

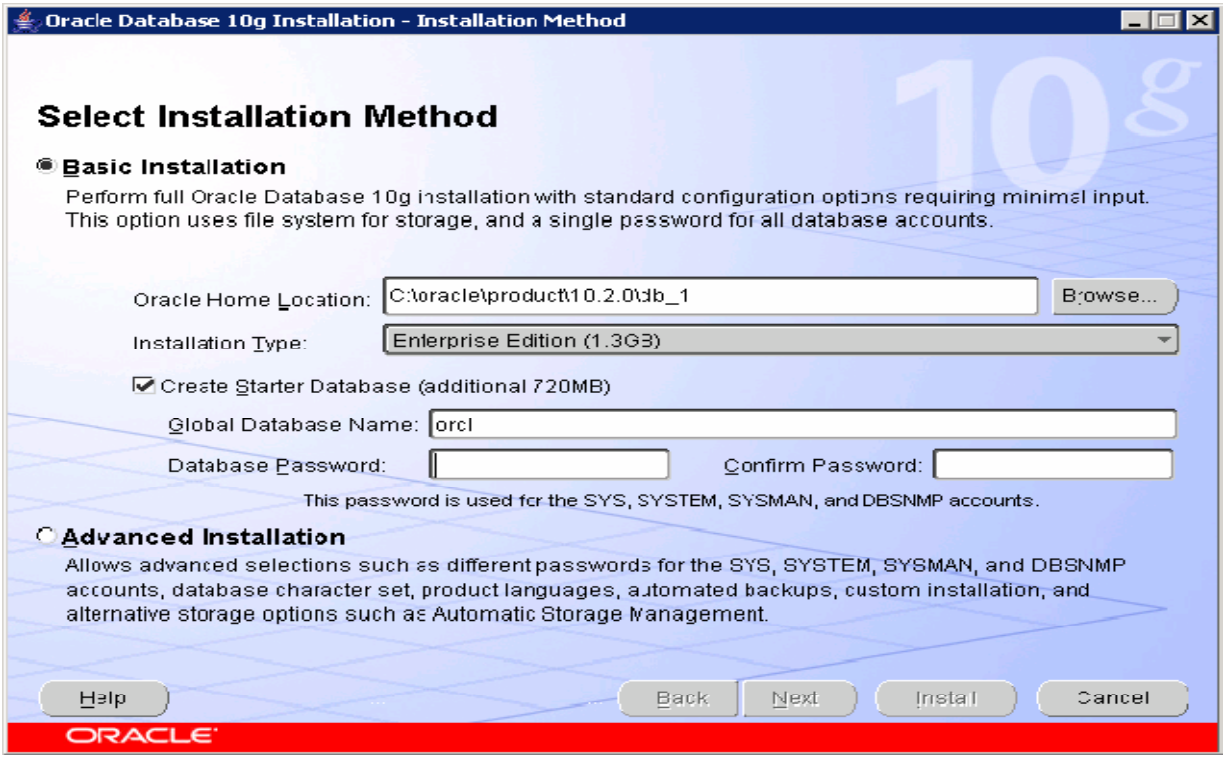
۳- حدس زدن شناسه سیستم با استفاده از حمله واژه نامه (Dictionary Attack)

۴- حمله جستجوی تمام حالات به شناسه سیستم (Brute Force Attack)

استفاده از شناسه های سیستمی پیش فرض (Default SID) :

همه میدانیم که بسیاری از مدیران پایگاه داده شناسه سیستمی پیشفرض در هنگام نصب اوراکل را بدون هیچ تغییری انتخاب میکنند. به عنوان مثال شناسه سیستم پیش فرض در هنگام نصب پایگاه داده اوراکل

”ORCL“ میباشد. همچنین شناسه سیستم پیشفرض در هنگام نصب Oracle 10g Express Edition کلمه ی ”XE“ میباشد.



تصویر نصب پایگاه داده اوراکل 10g با شناسه سیستم پیش فرض ”ORCL“

لیستی از شناسه سیستم های پیش فرض از آدرس http://www.red-database-security.com/scripts/sid.txt قابل دریافت است. اگر میخواهید مقادیر پیش فرض شناسه سیستم ها را به صورت اتوماتیک امتحان کنید میتوانید از ابزار هایی که در ادامه معرفی خواهد شد استفاده کنید.

انجام تست شناسه های سیستمی رایج :

مرحله بعد استفاده از مقادیر شناسه سیستم های عمومی و رایج مانند اطلاعات عمومی راجع به شرکت هدف است . به عنوان مثال نام شرکت و یا سازمان میتواند به عنوان شناسه سیستم مورد استفاده قرار گیرد. به عنوان مثال اگر ما شرکتی به اسم ”Sharif Network Security Center“ داشته باشیم میتوانیم شناسه سیستم هایی مانند ”SNSC“ و یا ”NSC“ را امتحان کنیم. بر اساس آمار های شرکت DSG ۱۰ درصد پایگاه داده ها از شناسه سیستم های رایج و عمومی استفاده میکنند. همچنین بر اساس آمار های منتشر شده

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

توسط DSG ۵ درصد از شرکت ها از DNS یا NETBIOS و ۸ در صد آنان شناسه سیستمی با نام کارگزار نام دامنه و یا Netbios Name خود با کمی تغییر استفاده میکنند.

ادامه دارد.....