专注APT攻击与防御

https://micropoor.blogspot.com/

msf 内置关于mysql插件如下（部分非测试mysql 插件）

关于msf常用攻击mysql插件如下：

1. auxiliary/scanner/mysql/mysql\_login

2. exploit/multi/mysql/mysql\_udf\_payload

3. exploit/windows/mysql/mysql\_mof

4. exploit/windows/mysql/scrutinizer\_upload\_exec

5. auxiliary/scanner/mysql/mysql\_hashdump

6. auxiliary/admin/mysql/mysql\_sql

7. auxiliary/scanner/mysql/mysql\_version

以下本地靶机测试：

靶机1：x86 Windows7

靶机2 ：x86 windows 2003 ip:192.168.1.115

1.auxiliary/scanner/mysql/mysql\_login

常用于内网中的批量以及单主机的登录测试。

2.exploit/multi/mysql/mysql\_udf\_payload

常用于root启动的mysql 并root的udf提权。

3.exploit/windows/mysql/mysql\_mof

以上类似，提权。

4.exploit/windows/mysql/scrutinizer\_upload\_exec

上传文件执行。

5.auxiliary/scanner/mysql/mysql\_hashdump

mysql的mysql.user表的hash

而在实战中，mysql\_hashdump这个插件相对其他较为少用。一般情况建议使用sql语句：

更直观，更定制化

6.auxiliary/admin/mysql/mysql\_sql

执行sql语句。尤其是在目标机没有web界面等无法用脚本执行的环境。

7.auxiliary/scanner/mysql/mysql\_version

常用于内网中的批量mysql主机发现。

后者的话：

在内网横向渗透中，需要大量的主机发现来保证渗透的过程。而以上的插件，在内网横

向或者mysql主机发现的过程中，尤为重要。

Micropoor