mysql抓包工具

simeon / 2017-06-08 00:51:09 / 浏览数 12308 安全工具 工具 顶(0) 踩(0)

---

https://github.com/Qihoo360/mysql-sniffer

简介

MySQL Sniffer 是一个基于 MySQL 协议的抓包工具，实时抓取 MySQLServer 端或 Client 端请求，并格式化输出。输出内容包括访问时间、访问用户、来源 IP、访问 Database、命令耗时、返回数据行数、执行语句等。有批量抓取多个端口，后台运行，日志分割等多种使用方式，操作便捷，输出友好。

同时也适用抓取 Atlas 端的请求，Atlas 是奇虎开源的一款基于MySQL协议的数据中间层项目，项目地址：https://github.com/Qihoo360/Atlas

同类型工具还有vc-mysql-sniffer，以及 tshark 的 -e mysql.query 参数来解析 MySQL 协议。

使用

建议在 centos6.2 及以上编译安装，并用 root 运行。

依赖

glib2-devel、libpcap-devel、libnet-devel

安装

```
git clone git@github.com:Qihoo360/mysql-sniffer.git
cd mysql-sniffer
mkdir proj
cd proj
cmake ../
make
cd bin/
```

参数：

```
./mysql-sniffer -h
Usage mysql-sniffer [-d] -i eth0 -p 3306,3307,3308 -l /var/log/mysql-sniffer/ -e stderr
 [-d] -i eth0 -r 3000-4000
 -d daemon mode.
 -s how often to split the log file(minute, eg. 1440). if less than 0, split log everyday
 -i interface. Default to eth0
 -p port, default to 3306. Multiple ports should be splited by ','. eg. 3306,3307
this option has no effect when -f is set.
 -r port range, Don't use -r and -p at the same time
 -l query log DIRECTORY. Make sure that the directory is accessible. Default to stdout.
 -e error log FILENAME or 'stderr'. if set to /dev/null, runtime error will not be recorded
 -f filename. use pcap file instead capturing the network interface
 -w white list. dont capture the port. Multiple ports should be splited by ','.
 -t truncation length. truncate long query if it's longer than specified length. Less than 0 means no truncation
 -n keeping tcp stream count, if not set, default is 65536. if active tcp count is larger than the specified count, mysql-snif
```

示例

1. 实时抓取某端口信息并打印到屏幕

输出格式为：时间，访问用户，来源 IP，访问 Database，命令耗时，返回数据行数，执行语句。

```
mysql-sniffer -i eth0 -p 3306
2017-02-23 14:47:45     testuser     10.xx.xx.xx     NULL              0ms              1     select @@version_comment limit 1
2017-02-23 14:47:45     testuser     10.xx.xx.xx     NULL              0ms              1     select USER()
2017-02-23 14:47:48     testuser     10.xx.xx.xx     NULL              0ms             13     show databases
2017-02-23 14:47:51     testuser     10.xx.xx.xx     NULL              0ms              1     SELECT DATABASE()
2017-02-23 14:47:51     testuser     10.xx.xx.xx     mysql              0ms              0     use mysql
2017-02-23 14:47:53     testuser     10.xx.xx.xx     mysql              0ms             29     show tables
2017-02-23 14:47:54     testuser     10.xx.xx.xx     mysql              0ms              1     select 1
2017-02-23 14:48:01     testuser1     10.xx.xx.xx     NULL              0ms              0     set autocommit=1
2017-02-23 14:48:01     testuser1     10.xx.xx.xx     NULL              0ms              0     set autocommit=1
```

2. 实时抓取某端口信息并打印到文件

-l 指定日志输出路径，日志文件将以 port.log 命名。

```
mysql-sniffer -i eth0 -p 3306 -l /tmp
```

3. 实时抓取多个端口信息并打印到文件

-l 指定日志输出路径，-p 指定需要抓取的端口列表逗号分割。日志文件将以各自 port.log 命名。

```
mysql-sniffer -i eth0 -p 3306,3307,3310 -l /tmp
```

.....

问题

- 有lvs环境下，如果client IP是保存在在每个连接阶段的tcp opt字段中，那么mysql-sniffer提取的真实的client IP而不是lvs的IP。
- 只能抓取新建的链接，如果是之前创建的链接将获取不到用户名和库名，并有一定几率丢包。

上一篇：针对西门子PLC蠕虫的实现 下一篇：hashcat-utils密码综合...

1. 1 条回复

c0de 2017-06-29 08:29:01

不错，端口镜像后，能用来做简单的mysql数据库审计。

0 回复Ta
