链滴

Mysql 被黑客入侵及安全措施总结

作者：tianlong

原文链接：https://ld246.com/article/1487151405483

来源网站：链滴

许可协议：署名-相同方式共享 4.0 国际 (CC BY-SA 4.0)

情况概述

今天登陆在腾讯云服务器上搭建的Mysql数据库，发现数据库被黑了，黑客提示十分明显。

Mysql中只剩下两个数据库，一个是information_schema，另一个是黑客创建的PLEASE_READ，其有一张info表，内容如下：

- Info: Your DB is Backed up at our servers, to restore send 0.2 BTC to the Bitcoin Address th n send an email with your server ip
- Bitcoin_Address: 1F33LEJjdphD6YpaonNCHejwLcgkgDGQW9
- Email: mysqldata@mail2tor.com

显然，我这是遇到比特币敲诈了。我的数据在别人的服务器里安然的躺着，需要向黑客支付0.2比特才有可能恢复。按照当前的汇率，0.2比特币大约为1400人民币，这是我第一次遇到网络敲诈，金额不小。

所幸数据库里并没有值钱的数据，就当是送给黑客了，不过 **数据库安全问题** 引起了我的注意。

安全措施

由于缺乏必要的安全措施和备份机制，数据库中原有的数据均已丢失。为了恢复到Mysql初始的状态重新安装了Mysql数据库，并且重新创建原先存在的数据库，同时，为了防止再次被黑客入侵，对Mysql进行了一些安全配置。

- 禁用或限制远程访问。若允许远程访问，需要确保特定主机才拥有访问权。
    - 对用户进行合理授权，应用程序中最好不要直接使用 root用户。
    - 限制打开网络socket，此时仍可以建立与Mysql服务器的本地连接。

```
[mysqld]
skip-networking
```

- 强迫Mysql仅监听本机。

```
[mysqld]
bind-address=127.0.0.1
```

- 更改 root用户的登录名称和密码。
- 移除测试数据库和匿名账户及废弃的账户。
- 禁用 LOCAL INFILE。

```
[mysqld]
set-variable=local-infile=0
```

- 删除历史命令记录。

```
cat /dev/null > ~/.bash_history
```

```
cat /dev/null > ~/.mysql_history
```

- 及时安装Mysql安全补丁。
- 使用 chroot限制Mysql运行环境。
- 自动定期备份数据库。