中南大學
CENTRAL SOUTH UNIVERSITY

网络安全实验报告

题　　目 TCP/IP攻击

学生姓名 李永强

指导教师 王伟平

学　　院 信息科学与工程学院

专业班级 信安1401

学　　号 0906140121

二〇一六 年 十一 月 十九 日

1、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,学生可以学习安全设计的原则,安全编程,和安全测试。

TCP /
IP协议的漏洞是一种特殊类型的漏洞在协议的设计和实现,他们提供了一个宝贵的教训为什么安全应设计从一开始,而不是添加为马后炮。此外,研究这些漏洞帮助学生理解网络安全的挑战,为什么许多网络安全措施是必要的。

实验室概述：
本实验的学习目标是让学生获得关于漏洞的第一手经验，如同对这些漏洞的攻击一样。明智的人从错误中学习。在安全教育，我们导致软件漏洞的研究错误。学习过去的错误不仅帮助学生了解为什么系统是易受攻击的，为什么一个看似良性的错误可能变成灾难，为什么需要许多安全机制。更重要的是，它也帮助学生学习共同的模式的漏洞，所以他们可以避免在将来出现类似的错误。此外，使用漏洞。作为案例研究，学生可以学习安全设计，安全编程和安全测试的原因，包括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，
配置在图1中描述。
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。

SEED实验室 - TCP / IP攻击实验室2
互联网
机器1
192.168.0.122
机器2
192.168.0.123
机器3
192.168.0.124
网关
192.168.0.1
图1：环境设置
Netwox由一套工具组成，每个工具都有一个特定的数字。你可以运行一个命令（参数取决于您使用的工具）。对于一些工具，你必须运行它
root权限：
＃netwox number [parameters ...]
如果您不确定如何设置参数，可以通过发出“netwox number”查看手册--help“。您还可以通过为每个执行的命令运行Netwag：来了解参数设置
从图形界面，Netwag实际上调用相应的Netwox命令，并显示
参数设置。因此，您可以简单地复制和粘贴显示的命令。
Wireshark工具。您还需要一个良好的网络流量嗅探器工具为这个实验室。虽然Netwox
附带一个嗅探器，你会发现另一个工具Wireshark是一个更好的嗅探器工具。都Netwox和Wireshark可以下载。如果你使用我们预先构建的虚拟机，两个工具已安装。要嗅探所有网络流量，这两个工具都需要由根运行。
启用ftp和telnet服务器。对于本实验，您可能需要启用ftp和telnet
服务器。为了安全起见，这些服务通常在默认情况下被禁用。启用他们在我们的
预建Ubuntu虚拟机，您需要以root用户身份运行以下命令：
启动ftp服务器
＃service vsftpd start
启动telnet服务器
＃service openbsd-inetd start

二、SYN洪流攻击

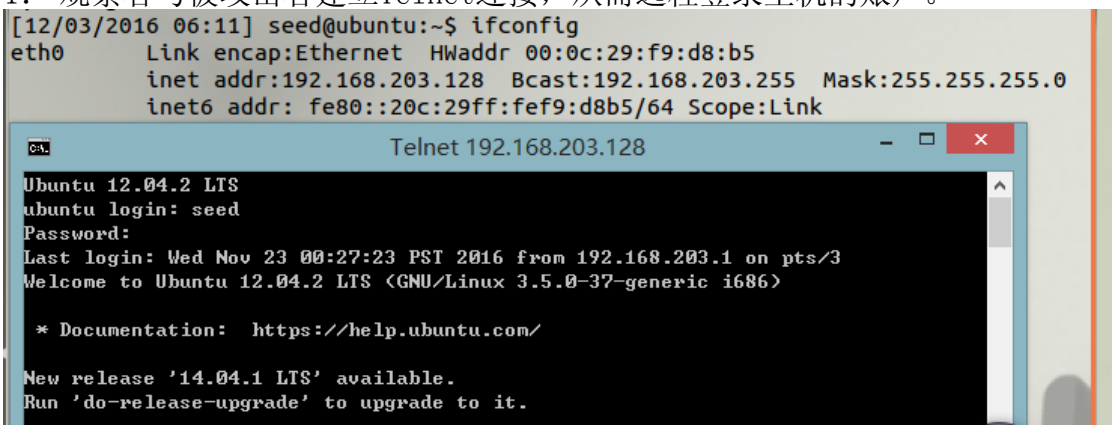
SYN洪流攻击是DOS攻击的一种形式。攻击者发现许多SYN请求给受害者的TCP端口，但是攻击者没有完成三次握手的意向。攻击者或使用虚假的IP地址，或者不继续过程。在这个过程中，攻击者可以使受害者的用于半连接的队列溢出。例如，一个完成SYN，SYN-ACK

但没有收到最后ACK回复的ACK回复连接。当这个队列满了的时候，受害者不能够在进行更多的连接。

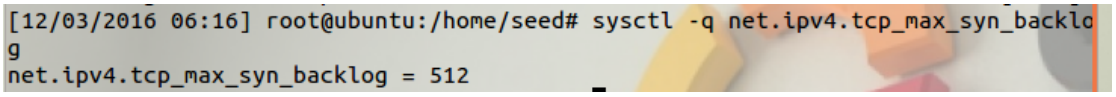
SYN缓存策略：SYN缓存是对抗SYN洪流攻击的一种防御机制。如果机器检测到它正在被SYN洪流攻击，这种机制会被kick in。

说明：观察者使用windows宿主，被攻击者和攻击者使用虚拟机Linux。

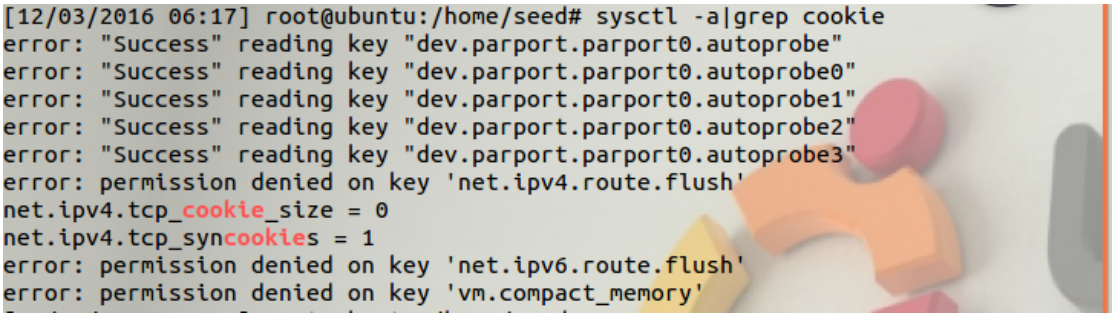
1. 观察者与被攻击者建立Telnet连接，从而远程登录主机的账户。



2. 在被攻击者上查看半开队列的最大长度。

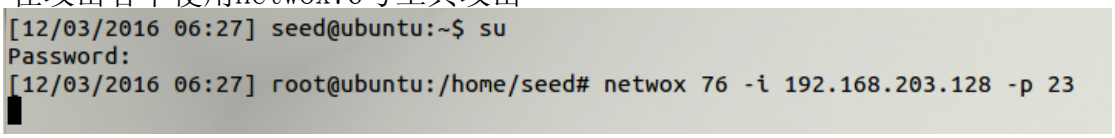


3. 在被观察者上查看缓冲保护状态



4. 断开观察者与被攻击者的连接

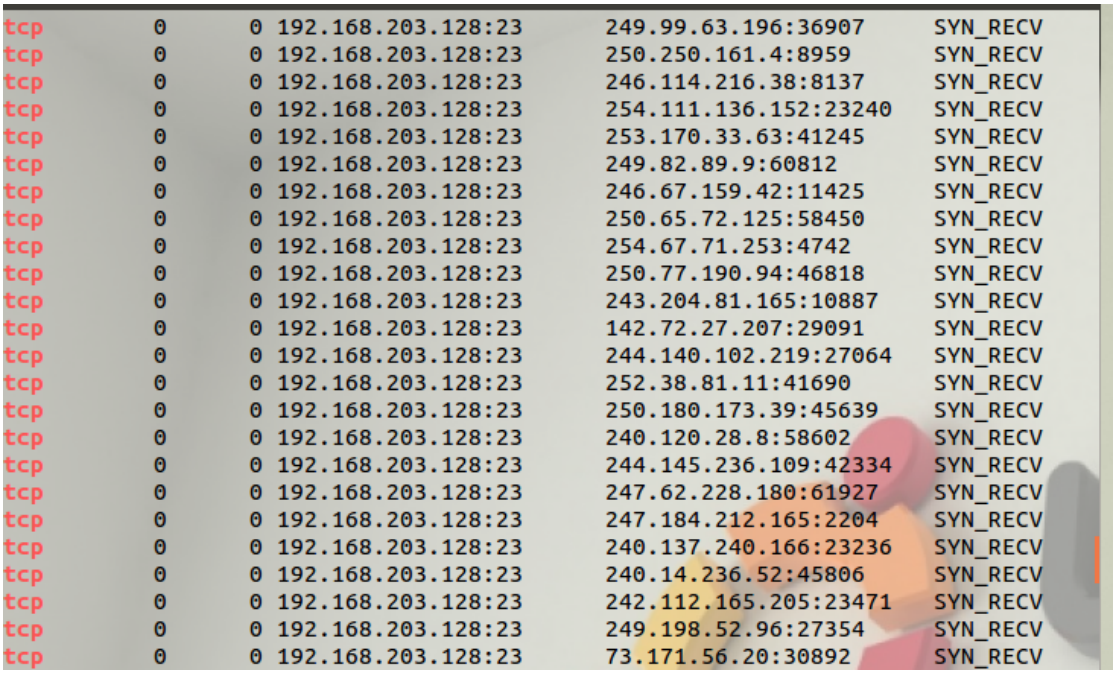
5. 在攻击者中使用netwox76号工具攻击



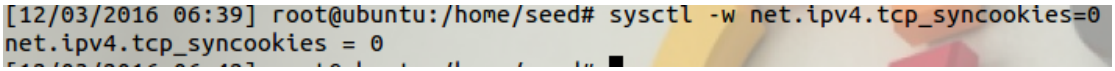
6. 尝试连接观察者与被攻击者

   此时可以连接，因为被攻击者处于缓冲保护状态

7. 在被攻击者中查看端口的连接情况，发现大量SYN半开连接



8. 断开连接
9. 在被攻击者中关闭缓冲保护



10. 再次在攻击者中发动攻击

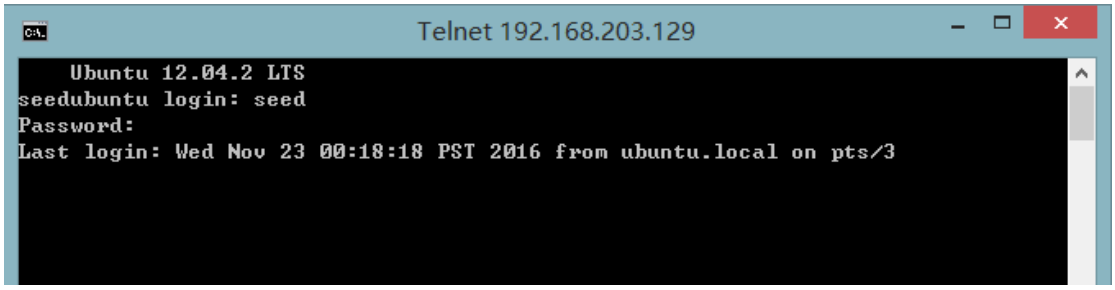
11. 再次连接，发现无法连接，且tcp端口无连接状态

三、在telnet和ssh连接上TCP RST攻击

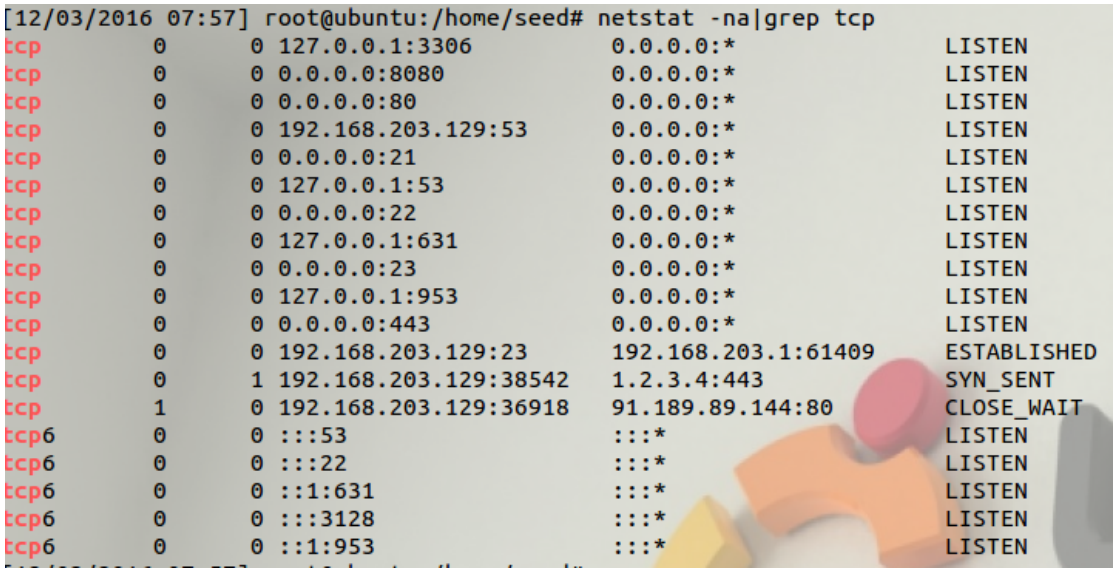
TCP

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



2. 在192.168.203.129查看tcp端口连接情况



3. 通过netwox 78号进行RST攻击

4. 在192.168.203.129查看tcp端口连接情况，发现断开连接

四、心得体会

这个实验进行得还是比较艰难的，我只做到了连接的那一部，之后就一直卡在那个地方过不去了，PING不通，然后学长帮忙看过，当时也没有搞清楚不通的原因。所以也非常地遗憾，因为时间的缘故，没有完整地实现这个实验的全部步骤和功能。这个寒假回去，我要再回去把接下去的步骤自己再全部完成一遍，争取能够实现。