请在网络攻防实验环境(以 SEED_VM 作为攻击机，Linux Metasploitable/Windows Metasploitable 作为靶机)中完成 TCP/IP 协议栈重点协议的攻击实验。

实验概述

本实验的学习目标是让学生获得关于 TCP/IP 协议漏洞以及攻击这些漏洞的第一手经验。TCP/IP 协议中的漏洞代表了协议设计和实现中的漏洞一类特殊类型。它们提供了宝贵的经验教训，告诉我们为什么安全性设计在一开始就应当被考虑，而不是作为一种事后的补充。此外，学习这些漏洞帮助学生理解网络安全中存在的挑战以及为什么我们需要大量的网络安全措施。TCP/IP 协议漏洞几乎发生在每一层。

实验任务

本实验中，你需要实施 TCP/IP 协议攻击。你可以在攻击中使用 netwox 或其它工具。攻击可在 Linux 或其它操作系统上进行。为了简化对 TCP 序列号及源端口号的猜测工作，我们假设攻击者与被攻击者在同一物理网络。因此，你可以使用嗅探器（sniffer）得到那些信息。以下是需要实现的攻击的列表：

- 网络层攻击：

(1) ARP 缓存欺骗

ARP 缓存是 ARP 协议的重要组成部分。当使用 ARP 协议解析了某个 MAC 地址和 IP 地址的映射关系，该映射便会被缓存下来。因此就不用再使用 ARP 协议来解析已存在缓存中的映射关系。但是因为 ARP 协议是无身份认证的，所以 ARP 缓存很容易被恶意的虚假 ARP 数据报实施欺骗。这样的攻击被称为 ARP 缓存欺骗(或 ARP 缓存投毒)。

在这样的攻击中，攻击者通过伪造 ARP 数据报来欺骗被攻击主机的电脑使之缓存错误的 MAC 地址和 IP 地址映射。因攻击者的动机不同，攻击的结果也有很多。例如，攻击者可以使被攻击主机的默认网关 IP 映射到一个不存在的 MAC 地址达到 DoS 攻击，攻击者也可以使被攻击主机的通信重定向至其他机器等等。

你的任务是演示 ARP 缓存欺骗攻击是怎么工作的。任务中一些有用的命令：linux 下可以使用 arp 来检查当前的 ARP 缓存。

(2) ICMP 重定向攻击

ICMP 重定向报文是路由器为网络中的机器提供最新的路由信息以达到最短路由而使用的。当主机收到一个 ICMP 重定向报文就会根据报文来更新自己的路由表。由于缺乏确认机制，如果攻击者想要使被攻击主机使用特定路由，他们只要向被攻击主机发送欺骗性的 ICMP 重定向报文，使它改变路由表即可。

你的任务是演示 ICMP 重定向攻击是如何工作的，并描述一下观察到的结果。在 linux 可以使用 route 命令检查路由表。

- 传输层攻击：

(1) SYN flood 攻击

SYN flood 攻击是 DoS 攻击的一种形式，攻击者向被攻击主机的 TCP 端口大量发送 SYN 请求包，但不去完成 TCP 的”三次握手”的过程，例如攻击使用一个假的 IP 地址，或只是简单地不再继续建立 TCP 连接的过程，这都使被攻击主机处于”半连接”状态(即在”三次握手”过程中，有了前两次握手，SYN 包和 SYN-ACK 包的传输，但没有最后一次 ACK 包的确认)。被攻击主机的主机会使用一个队列来保存这种半连接的状态，当这个队列存储空间满了的时

候，目标主机便无法再接受任何其它连接。这一队列的空间大小事实上是一个系统变量，在 Linux 中，可以这样查看它的大小:

 # sysctl –q net.ipv4.tcp_max_syn_backlog

我们还可以使用”netstat -na”命令去检查队列的使用情况。处于半连接的连接状态被标示为”SYN-RECV”，完成了”三次握手”的连接被标示为”ESTABLISHED”.

在这一任务中，你需要演示 SYN flood 攻击。你可以使用 Netwox 去实施攻击，并使用嗅探器来获取数据包。攻击实施的过程中，在被攻击主机上运行”netstat -na”命令去观察受攻击的情况。请描述你的攻击是否成功。

SYN Cookie 保护机制：如果你的攻击看起来并不成功，你可以检查一下目标主机的 SYN Cookie 机制是否被开启。 SYN cookie 是针对 SYN flood 攻击的一种保护机制。这一机制会在探测到 SYN flood 攻击时开始生效。你可以使用 sysctl 命令去打开或关闭这一机制:

 # sysctl -a | grep cookie (查看 SYN cookie 的当前状态)

 # sysctl -w net.ipv4.tcp_syncookies=0 (关闭 SYN cookie)

 # sysctl –w net.ipv4.tcp_syncookies=1 (打开 SYN cookie)

请分别在 SYN cookie 机制打开和关闭两种情况下实施你的 SYN flood 攻击，并比较结果。请在你的报告中尝试描述为什么 SYN cookie 能有效地抵御你的攻击。(如果课堂上没有讲解 SYN cookie 的原理，你可以从网络上找到相关的信息)

(2) TCP RST 攻击

你需要实施 TCP RST 攻击。这里推荐一个较为有趣的实验方法：对一个视频流的 TCP 连接实施攻击。大多数的视频分享网站会通过 TCP 连接来传输数据，你的目标是干扰被攻击主机与视频源之间的 TCP 连接(已经假定你和被攻击主机在同一局域网内)

访问视频网站并观看视频的过程一般如下：

- 被攻击者使用浏览器访问一个视频网站，并选择播放某个视频
- 大多数情况下视频的完整内容被存放在一个不同的主机上，该主机接下来会与被攻击主机建立起 TCP 连接，从而使被攻击主机能够接收视频的内容

你的任务是通过破坏上述 TCP 连接来干扰视频流的传输。你可以让被攻击主机试图去访问一个假的 IP 地址或是攻击主机的 IP 地址来获取视频(从而它无法成功获得视频内容)，但请注意，攻击的目标应该是被攻击主机，这是受你控制的一台主机，不要针对提供视频的主机(不受你控制的主机)。你的攻击实验应出于学习目的而不要造成真正的危害。

(3) TCP 会话劫持 (bonus)

TCP 会话劫持的目标是劫持一个已经存在于两台被攻击主机之间的 TCP 连接，在会话中注入恶意的内容。如果这是一个 telnet 会话连接，攻击者可以注入一些恶意的命令，使得被攻击主机运行这些恶意的命令。在这个任务中，我们使用 telnet 作为例子，并且仍然假定攻击机与目标主机在同一个局域网内。

关于 wireshark 的一些提示:如果你使用 wireshark 进行监听，请注意在默认情况下 wireshark 显示的 TCP 连接的序列号(sequence number)是相对序列号(relative sequence)，也就是当前序列号减去 TCP 连接建立之初的起始序列号，要查看真实的”绝对”序列号，右键点击协议内容，在”protocol preference”菜单中去掉”Relative Sequence Number and Window Scaling”这一项前面的勾。

实验报告

你需要提交一份实验报告，报告应包括以下部分：

设计：攻击的设计，包括攻击的策略，攻击中使用的数据包类型和参数，攻击中使用的工具等。

观察到的现象：你的攻击是否成功？你如何知道它是否成功？你希望看到什么？你实际观察到了什么？观察到的现象是否让你惊讶？

解释：有些攻击也许失败，如果是这样，你需要找出失败的原因。你可以从自己的实验中(推荐)或者从网络上找到解释，如果是从网络上找到的解释，你仍然需要通过自己的实验去证实你得到的解释。你需要使我们相信，你从网上找到的解释确实能够说明你所观察到的现象。