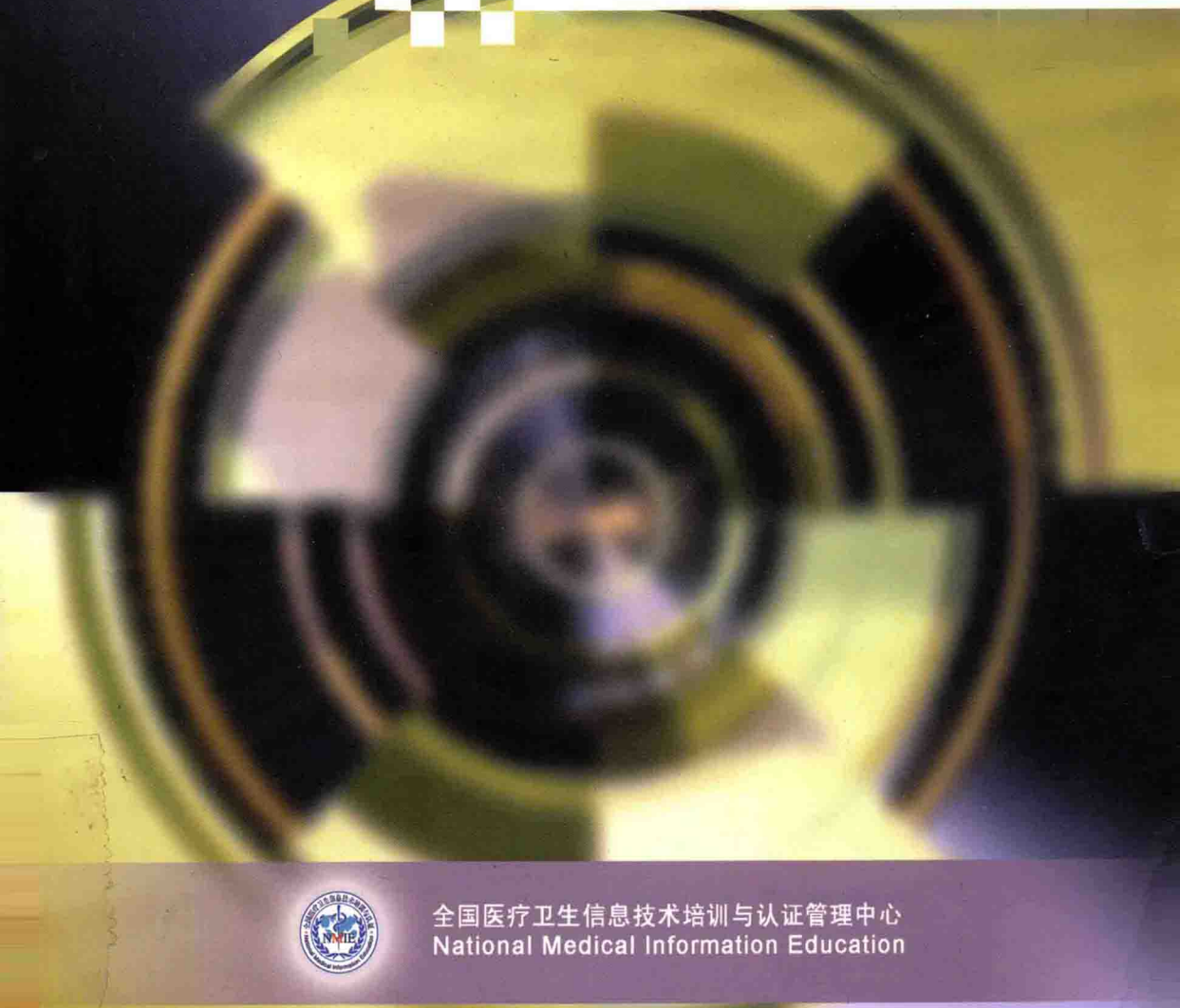
全国医疗卫生信息技术职业资格考试指定教材

网络与信息安全（医疗）

Network And Information Security（Medical）

INTERMEDIATE LEVEL 中级



全国医疗卫生信息技术培训与认证管理中心
National Medical Information Education

海潮出版社

网络与信息安全（医疗）

网络与信息安全

中级学员教材

学术顾问：饶克勤　王才有　李包罗　胡铮

主　　编：梁铭会

编审人员：杨颖辉　何永忠　范志伟　殷晓光

尚邦治　杜　晔　袁中兰　蔡予川

张宏阳　吴京美

图书在版编目（CIP）数据

网络与信息安全.医疗.初、中级/梁铭会主编.
北京：海潮出版社.2006

ISBN 7-80213-270-3

I.网络与信息安全　II．梁铭会　III.计算机网络-安全技术　IV.TP393.08

中国版本图书馆 CIP 数据核字（2006）第 101559 号

网络与信息安全（医疗）（初、中级）
梁铭会　主编
☆
海潮出版社出版发行　　电话（010）66969738
（北京市西三环中路 19 号　邮政编码：100841）
中国人民解放军第四二一零工厂印刷

开本：185×260 毫米　1/16　印张：23　　字数：278 千字
2006 年 9 月第 1 版　2006 年 9 月第 1 次印刷

印数：1000 册
ISBN 7-80213-270-3
总定价（两册）：106 元

内容提要

该教材较为全面的介绍了作为计算机网络安全理论基础的密码学，并对网络安全攻击、公开密码基础设施、常用计算机网络安全协议、边界安全防火墙技术、入侵检测技术和操作系统安全进行了全面、深入、系统的介绍。在医院网络安全方面具有丰富实践经验的专家，对医院网络安全问题作了综合分析，讲述了网络维护的经验。该教材可以作为卫生系统信息安全管理师的培训及认证教材，也是相关从业人员在实际工作中的必备工具参考书。同时该教材也适合医学高等院校相关专业的学生学习，作为今后工作的指导和参考。

前　言

随着计算机网络与信息技术的飞速发展及计算机网络应用的广泛和深入，计算机网络建设和应用是卫生信息化网络建设的重要组成部分之一，网络与信息安全问题正日益引起人们的关注。网络在给我们带来方便快捷获取信息、大大提高工作效率的同时，网络安全问题给我们也带来了一定的困扰。

网络如何连续、可靠、高效、安全运行，是网络系统不可缺少的部分，也是卫生系统信息安全管理人员的重要职责。随着技术的不断改进，在卫生系统内多套信息应用系统同时运行是普遍现象，各系统相互独立又互相联系，如何安全、有效的保证各系统的安全运行是各单位面临的一个共同问题。本书就是为能有效解决这些问题而编写的。网络安全管理师培训教材是由编委会结合多年的从事网络安全的经验，并参考借鉴相关的技术文献整理编写的，它适合于具有初步的信息安全知识和技能的人进一步深入学习网络安全相关知识使用。可作为网络与信息安全师的认证教材，也适合高等院校相关专业的学生学习网络安全知识。

本书较全面介绍了作为计算机网络安全理论基础的密码学，并对黑客攻击技术、密码算法、公钥基础设施、常用计算机网络安全协议、边界安全防火墙技术、入侵检测技术和操作系统安全配置进行了全面的、详细的介绍，并且对医院网络安全问题进行了综合分析，介绍了医院网络维护的实践经验等。

目前，国家卫生部和信息产业部电子行业职业技能鉴定指导中心就网络与信息安全，设立了专门的培训考核认证，英文全称为：Net and Information Management Technology，简称为“NIMT”，使得网络及信息管理、网络与信息安全这一行业从此有了国家的行业认证标准。这一“国标”的出台，也昭示着基于国家标准的 IT 培训认证项目随着国内网络厂商逐步进入国内国际市场的同时，将逐步在国内国际市场起到一定的引导作用及中立于国内、国外厂商。

该书由卫生部医管所信息化教育办公室杨颖辉教授负责组织编写。各章执笔人为：（前言及大纲：杨颖辉）、（第 1 至 7 章：何永忠）、（第 8 章：范志伟）。校对：（第 1 至 7 章：尚邦治）、（第 8 章：蔡予川）、（前言及大纲：殷晓光）。

由于编写时间仓促、加之水平有限，书中错漏在所难免，恳请广大读者批评指正。

编　者

2006 年 7 月于北京　卫生部医管所信息化教育办公室

目　录

第1章 黑客攻击技术

黑客攻击是当前计算机网络系统面临的主要安全威胁。作为一个网络安全管理者，了解黑客攻击的常用技术有助于提高安全意识，增进对安全防范技术的理解，提高安全防范的能力。本章首先简单介绍了黑客攻击概念，分类和黑客攻击的一般步骤；详细介绍了黑客攻击常用的技术。

§1.1 攻击的概念和分类

§1.1.1 攻击的概念

谈起网络安全，人们总会想起 Hacker 这个词，可见网络安全和黑客是形影不离的，两者是矛盾的两个对立面。那么什么是黑客(Hacker)呢？简单来说，黑客就是指企图入侵别人的计算机或网络的人。该定义几乎涵盖了所有现代网络系统的入侵，从计算机网络到电话系统。在现代社会里任何远程复杂控制都是由计算机来实现的，因为联网的计算机能发挥更大的作用和更易于管理。

最初的黑客是指具有熟练的编写和调试计算机程序的技巧，并使用这些技巧来获得非法或未授权的网络或文件访问，入侵进入企业内部网的人。随着各种强大的黑客工具的广泛传播，对计算机技术了解很少的人也可以实施黑客攻击行为，因此网络系统受到黑客攻击的可能性大大提高了。

所有导致一个网络安全性受到破坏、网络服务受到影响的行为都称为攻击。比如，获得了没有授权的读写特权，或者滥用权限对系统的数据进行破坏，或者使得系统不能正常为其他用户提供服务的行为。

§1.1.2 攻击的分类

根据不同的分类标准，攻击可以有不同的分类。根据攻击者是否直接改变网络的服务，攻击可以分为被动攻击和主动攻击。

被动攻击：被动攻击不直接改变网络状态和服务。包括分析通信流，监视未被保护的通讯，解密弱加密通讯，获取鉴别信息(比如口令)。被动攻击可能造成在没有得到用户同意或告知用户的情况下，将信息或文件泄露给攻击者。这样的例子如泄露个人的敏感信息。

主动攻击：主动攻击会造成网络系统状态和服务的改变。主动攻击包括试图阻断或攻破保护机制、引入恶意代码、偷窃或篡改信息。主动进攻可能造成数据资料的泄露和散播，或导致拒绝服务以及数据的篡改。包括大多数的未授权用户企图以非正常手段和

正常手段进入远程系统。

另一种攻击分类是根据攻击者是否是系统正常用户可以分为外部人员攻击和内部人员攻击。

外部人员攻击：不是系统用户，不能通过正常的途径进入系统的攻击者发起的攻击。一般黑客攻击都是指外部人员发起的攻击。

内部人员攻击：具有系统正常的用户身份，拥有系统用户帐号和授权。

内部人员攻击常常被忽略。与外部人员攻击不同，由于内部人员对被攻击系统更了解，有较多的访问权限，内部人员发起的攻击往往更容易造成危害。因此，要高度重视内部人员攻击。

§1.2 攻击的一般流程

攻击者的每一次攻击都是一个完整的过程，需要大量的时间，这个过程会因攻击者的技术及习惯不同而有差异，对于相同的目标机，有些攻击者可能需要三天，有些攻击者可能需要三周甚至三个月；有些也可能只需二步就可完成，有些需要三、四步方可完成。一般完整的攻击过程都是先隐藏自身，在隐藏好自己后再进行预攻击探测，检测目标机器的各种属性和具备的被攻击条件；然后采取相应的攻击方法进行破坏，达到自己的目的之后攻击者会删除自己行为在目标系统中的日志。

§1.2.1 隐藏自身

攻击者隐藏自身的目的是逃避责任追究。常见隐藏自身方式有几下几种：

1) 从一个跳板主机通过 telnet 或 rsh 登录到攻击目标主机（称为穿梭）；

2) 从 windows 主机上通过 wingates 等代理服务进行穿梭；

3) 利用配置不当的代理服务器进行穿梭；

4) 利用电话交换技巧先通过拨号找寻并连入某台主机，然后通过这台主机再联入因特网来穿梭。

通过多次穿梭，攻击者就可以把它的实际地址隐藏起来。

§1.2.2 预攻击探测

预攻击探测的主要任务是发现攻击目标，收集被攻击目标的有关信息，试探攻击目标的安全漏洞，为发动真正攻击做准备。发现攻击目标是寻找正在活动的主机或者网络；收集攻击目标信息包括目标计算机的硬件信息，运行的操作系统信息，运行的应用程序(服务)的信息，目标计算机所在网络的信息，目标计算机的用户信息，存在的漏洞等等；试探攻击目标的漏洞则是根据收集到的信息，尝试寻找攻击目标上可以被利用的安全漏洞。

§ 1.2.3 采取攻击行为

在上一步骤中，如果攻击者发现目标机有可以被利用的漏洞或弱点，则可以立即采取攻击行为。在此过程中具体采用的攻击行为要视目标机系统类型而定，目前较流行的手段有强力口令猜测、缓冲区溢出、拒绝服务、社会工程、伪装欺骗等攻击技术。

§ 1.2.4 清除痕迹

为了避免攻击行为被发现，攻击者在攻击行动结束后，还需要清除攻击行为相关的系统记录。清除攻击痕迹主要就是清除系统日志和服务日志。有些工具可以帮助清除日志，如 THC 提供的 cleara.c。该工具可以清除 utmp/utmpx,wtmp/wtmpx, 修复 lastlog 让其仍然显示该用户的上次登录信息。攻击者也可以自己对日志文件进行修改，但不同的 UNIX 版本日志存储位置不同，大致位置如下：

- UTMP : /etc 或 /var/adm 或 /usr/adm 或 /usr/var/adm 或 /var/log
- WTMP : /etc 或 /var/adm 或 /usr/adm 或 /usr/var/adm 或 /var/log
- LASTLOG : /usr/var/adm 或 /usr/adm 或 /var/adm 或 /var/log

在一些旧 unix 版本中 lastlog 数据被写到$HOME/.lastlog 文件中。

一般的黑客都会把自己的行为痕迹从日志中删除，但他们往往忘记删掉在机器中留下的其他一些痕迹：在/tmp 和$HOME 中的 shell 记录文件；一些 shell 会保留一个 history 文件(依赖于环境设置)记录用户执行的命令。因此，要消除这些痕迹最好的方法就是登录以后先启动一个新 shell，然后在$HOME 中查找历史纪录。可以直接使用 ls –alt ./* 来查看当前的记录文件情况，可以使用 cat /dev/null >./*history 来清空记录文件。需要注意的是，启动新的 shell 的这条命令也会在 root 所分配的 shell 记录文件里，这可能成为追踪入侵者的一个关键命令。

不同 shell 工具的历史记录文件名称如下：

- sh : .sh_history
- csh : .history
- ksh : .sh_history
- bash: .bash_history
- zsh : .history

§ 1.3 攻击技术方法

§ 1.3.1 预攻击探测

预攻击探测技术主要可以分为 Ping 扫描、操作系统识别扫描、防火墙规则扫描、端口扫描以及漏洞扫描（vulnerability scan）等。Ping 扫描用于发现攻击目标；操作系统识别扫描就是对目标主机运行的操作系统进行识别；防火墙规则扫描用于获取被防火墙保护的远端网络的资料；而端口扫描用于查看攻击目标处于监听或运行状态的服务。目前

主流的扫描工具包括 Nmap, Nessus 都实现了这些技术。这些技术既可以作为安全管理员检验安全措施是否有效的方法，也会被黑客利用作为发动攻击的探测手段。下面介绍主要的预攻击探测技术。

§1.3.1.1 发现攻击目标

对于 Linux 操作系统，通常是从已攻入系统中的.rhosts 和.netrc 文件所列机器中挑选出作为攻击目标的机器，从系统的/etc/hosts 文件中可以得到一个很全的主机列表。但大多数情况下，选定一个攻击目标是一个比较盲目的过程，除非攻击者有明确的目的和动机。攻击者也可能查询 DNS(域名服务器)，通过 DNS 获知机器名、Internet 地址、机器类型，甚至是机器的属主和单位等信息。

另一个发现攻击目标的方法就是采用 Ping 扫描，通过向一个 IP 地址区间中所有 IP 地址发送 ping 包来发现正在活动的主机。

§1.3.1.2 操作系统识别扫描

操作系统识别扫描的目的是探测被攻击系统使用的操作系统的类型和版本，从而根据对系统的已知信息（包括漏洞信息）对目标系统发起试探攻击。操作系统识别扫描最基本的技术就是根据各种版本的操作系统提供的服务的差异编写探测程序。当综合利用了足够多的不同特征时，对操作系统版本的探测精度就可以大大的提高。主要的操作系统识别扫描探测技术有：

1) FIN 探测

通过发送一个 FIN 数据包(或任何未设置 ACK 或 SYN 标记位的数据包)到一个打开的端口，并等待回应。RFC793 定义的标准行为是“不”响应，但诸如 MS Windows、BSDi、CISCO、HP/UX、MVS 和 IRIX 等操作系统会回应一个 RESET 包。大多数的探测器都使用了这项技术。

2) 伪造标记位

原理是在一个 SYN 数据包 TCP 头中设置未定义的 TCP“标记”字段(64 或 128)。低于 2.0.35 版本的 Linux 内核会在回应包中保持这个标记，而其它操作系统一般不会。不过，有些操作系统当接收到一个 SYN+BOGUS 数据包时会复位连接。所以这种方法能够比较有效地识别出操作系统。

3) TCP 的 ISN 分析

其原理是通过在操作系统对连接请求的回应中寻找 TCP 连接初始化序列号的特征。目前可以区分的类别有传统的 64K(旧 UNIX 系统使用)、随机增加(新版本的 Solaris、IRIX、FreeBSD、DigitalUNIX、Cray 和其它许多系统使用)、真正“随机”(Linux 2.0.* 及更高版本、OpenVMS 和新版本的 AIX 等操作系统使用)等。Windows 平台(还有其它一些平台)使用“基于时间”方式产生的 ISN 会随着时间的变化而有着相对固定的增长。老式的 64K 方式很容易受到攻击，而采用“固定”ISN 的系统最容易识别。确实有些机器总是使用相同的 ISN，如某些 3Com 集线器（使用 0x83）和 Apple LaserWriter 打印机

(使用 0xC7001)。根据计算 ISN 的变化、最大公约数和其它一些有迹可循的规律，还可以将这些类别分得更细、更准确。

4) “无碎片”标记位

许多操作系统逐渐开始在它们发送的数据包中设置 IP“不分片(无碎片)”位。这对于提高传输性能有好处(虽然有时它很讨厌——这也是为什么 nmap 不对 Solaris 系统进行碎片探测的原因)。但并不是所有操作系统都有这个设置，或许并不总是使用这个设置，因此通过留意这个标记位的设置可以收集到关于目标主机操作系统的更多有用信息。

5) TCP 初始化“窗口”

就是检查返回数据包的“窗口”大小。以前的探测器仅仅通过 RST 数据包的非零“窗口”值来标识为“起源于 BSD 4.4”。而象 queso 和 nmap 这些新的探测器会记录确切的窗口值，因为该窗口随操作系统类型有较为稳定的数值。这种探测能够提供许多有用的信息，因某些系统总是使用比较特殊的窗口值(例如，AIX 是唯一使用 0x3F25 窗口值的操作系统)。而在声称“完全重写”的 NT5 的 TCP 栈中，Microsoft 使用的窗口值总是 0x402E。有意思的是，这个数值同时也被 OpenBSD 和 FreeBSD 使用。

6) ACK 值

向一个关闭的 TCP 端口发送一个 FIN|PSH|URG 包，许多操作系统会将 ACK 值设置为 ISN 值，但 Windows 和某些愚蠢的打印机会设置为 seq+1。如果向打开的端口发送 SYN|FIN|URG|PSH 包，Windows 的返回值就会非常不确定。有时是 seq 序列号值，有时是 S++，有时回送的是一个似乎很随机性的数值。令人疑惑的是为什么 MS 总是能写出这种莫名其妙的代码。

7) ICMP 错误包频率

有些操作系统根据 RFC 1812 的建议对某些类型的错误信息发送频率作了限制。例如，Linux 内核(在 net/ipv4/icmp.h)限制发送“目标不可到达”信息次数为每 4 秒 80 次，如果超过这个限制则会再减少 1/4 秒。一种测试方法是向随机选择的高段 UDP 端口发送成批的数据包，并计算接收到的“目标不可到达”数据包的数量。在 nmap 中只有 UDP 端口扫描使用了这个技术。这种探测操作系统方法需要稍微长的时间，因为需要发送大量的数据包并等待它们的返回。这种数据包处理方式也会对网络性能造成一定程度的影响。

8) ICMP 错误包长度

RFC 定义了一些 ICMP 错误信息格式。如对于一个端口不可到达信息，几乎所有操作系统都只回送 IP 请求头加上 8 字节长度的包，但 Solaris 返回的包会稍微长一点，Linux 则返回更长的包。这样即使操作系统没有监听任何端口，nmap 仍然有可能确定 Linux 和 Solaris 操作系统的主机。

9) ICMP 错误包内容

在前面已谈到，机器必须根据接收到的数据包返回“端口不可到达”(如果确实是这样)数据包。有些操作系统会在初始化处理过程中弄乱了请求头，这样当你接收到这种数据包时会出现不正常。例如，AIX 和 BSDI 返回的 IP 包中的“总长度”域会被设置为 20 字节(太长了)。某些 BSDI、FreeBSD、OpenBSD、ULTRIX 和 VAX 操作系统甚至会修改请求头中的 IP 、ID 值。另外，由于 TTL 值的改变导致包校验和需要修改时，某些系统(如 AIX、FreeBSD 等)返回数据包的校验和会不正确或为 0。有时这种情况也出现在 UDP 的包检验和中。nmap 使用了九种不同的 ICMP 错误信息探测技术来区分不同的操作系统。

10) 服务类型

对于 ICMP 的“端口不可到达”信息，经过对返回包的服务类型(TOS)值的检查，几乎所有的操作系统使用的是 ICMP 错误类型 0，而 Linux 使用的值是 0xC0。

11) 碎片处理

不同操作系统在处理 IP 片段重叠时采用了不同的方式。有些用新的内容覆盖旧的内容，而又有些是以旧的内容为优先。有很多探测方法能确定这些包是被如何重组的，从而能帮助确定操作系统类型。

12) TCP 字段选项

这也是收集操作系统类型及版本的方法之一，主要原理在于：

(1) 由于在 RFC 推荐标准中对 TCP 字段选项的实现要求不是强制性的，因此并不是所有的操作系统都支持它们。

(2) 向目标主机发送带有可选项标记的数据包时，如果操作系统支持这些选项，会在返回包中也设置这些标记。

(3) 可以一次在数据包中设置多个可选项，从而增加了探测的准确度。

§1.3.1.3 端口扫描

端口是主机与外部通信的途径，一个端口就是一个潜在的通信通道，也可能是一个入侵通道。对目标主机进行端口扫描，能得到许多有用的信息。

常用的端口扫描方式有以下几种：

- TCP connect 端口扫描
- TCP SYN 端口扫描
- TCP FIN 标志端口扫描
- TCP ACK 标志端口扫描
- TCP NULL 标志端口扫描
- TCP SYN\ACK 标志端口扫描
- TCP XMAS 标志端口扫描
- UDP 应答端口扫描
- UDP 端口不可到达扫描

在介绍端口扫描技术之前，我们先回忆一下正常情况下，与一个端口建立TCP连接和关闭一个TCP连接的步骤。

在应用层，与一个端口建立TCP连接使用connect( )系统调用，而在传输层(TCP层)他是经过三次握手过程，在很多高级扫描技术中主要是利用这三次握手特性来进行。我们来看看这三次握手的简单过程：

请求主机通过一个同步标志置位的数据段发出会话请求(SYN)。

接收主机通过发回以下数据段表示回复(SYN|ACK)：同步标志置位、即将发送的数据段的起始字节的顺序号、应答并带有将收到的下一个数据段的字节顺序号。

请求主机再回送一个数据段(ACK)，并带有确认顺序号和确认号。这里我们用CLIENT和SERVER分别表示扫描器所在主机和目标主机(这里我们假设远程主机是处于激活状态，其中没有防火墙等阻断设备)。

建立一个TCP连接过程：

连接成功的流程如下：

```
CLIENT  ->  SYN      //CLIENT 向 SERVER 发送一个 SYN 数据报
SERVER  ->  SYN|ACK  //SERVER 向 CLIENT 发送回一个 SYN|ACK 数据包
CLIENT  ->  ACK      //CLINET 再向 SERVER 发送一个 ACK，建立连接成功
```

连接不成功的流程如下：

```
CLIENT  ->  SYN      //CLIENT 向 SERVER 发送一个 SYN 数据报
SERVER  ->  RST|ACK  //SERVER 向 CLIENT 发送回一个 RST|ACK 数据包
CLIENT  ->  RST      //CLINET 再向 SERVER 发送一个 RST，表示连接不成功
```

系统函数CloseSocket( )可以实现关闭一个TCP连接，该函数为用户或者开发人员屏蔽了中间的过程。建立一个连接需要三次握手，而终止一个连接需要经过4次握手。终止一个连接的步骤如下：

初始化主机通过一个同步标志置位的数据段发出结束会话请求(FIN)；

目标主机发回一个包含数据段ACK的数据包表示回复；

目标主机再发回一个结束回话请求FIN；

主机接收到目标主机发送的回话结束请求，发送回复包ACK。到此完成整个结束过程。

关闭一个TCP连接过程

```
CLIENT  ->  FIN  //CLIENT 向 SERVER 发送一个 FIN 数据报(通知 SERVER 关闭);
SERVER  ->  ACK  //SERVER 向 CLIENT 发送回一个 FIN 的 ACK 数据包(确认);
SERVER  ->  FIN  //SERVER 向 CLIENT 发送回一个 FIN 数据包(通知 CLIENT 关闭);
CLIENT  -->  ACK  //CLINET 再向 SERVER 发送一个 FIN 的 ACK(确认)。
```

下面我们介绍各种端口扫描技术。

1) TCP connect 端口扫描

这是最基本的TCP扫描。使用操作系统提供的connect( )系统调用，来对目标主机的端口逐个进行TCP连接。如果一个端口处于打开状态，那么connect( )就能成功。否则这个端口是关闭的。这种方式是最原始的一种端口扫描方式，很容易被防火墙屏蔽。

2) TCP SYN 端口扫描

这种扫描方式又叫“TCP 半连接端口扫描”，这种不需要打开一个完全的 TCP 连接。使用 TCP SYN 方式扫描一个端口，只要向目标端口发送一个只有 SYN 标志位的 TCP 数据报，如果目标主机返回一个 SYN|ACK 数据包，那么目标主机的该端口处于打开状态。如果返回的是 RST 数据包，那么目标主机的该端口没有打开。

对于 SERVER 的监听端口，CLIENT 和 SERVER 间不进行 TCP 三次握手：

CLIENT --> SYN

SERVER --> SYN|ACK //返回 SYN|ACK 表明端口开放

如果是 SERVER 的关闭端口，则是这样的流程：

CLIENT --> SYN

SERVER --> RST|ACK //返回 RST|ACK 表明端口关闭

如果收到一个 SYN|ACK，则扫描程序必须再发送一个 RST 信号，来关闭这个连接过程。在 Unix/Linux 下，必须要有 root 权限才能构造 SYN 数据包。

3) TCP FIN 扫描

这是一种反转的扫描方法，是通过扫描找到目标主机关闭的 TCP 端口。这种扫描方式是向目标主机的一个端口发送一个 TCP FIN 数据报，如果主机没有任何反馈，那么这个主机是存在且这个端口处于打开状态；如果主机返回一个 TCP RST 数据包，那么这台主机存在，但这个端口处于关闭状态。

对某端口发送一个 TCP FIN 数据报给远端主机。如果主机没有任何反馈，那么这个主机是存在的，而且正在监听这个端口；主机反馈一个 TCP RST 回来，那么说明该主机是存在的，但是没有监听这个端口。

得到其监听端口，扫描过程如下：

对于 SERVER 的监听端口，CLIENT 和 SERVER 间不进行 TCP 三次握手：

CLIENT --> FIN //向 SERVE 发出 FIN

SERVER --> //SERVER 没有响应

如果 SERVER 的端口是关闭端口，则扫描过程是这样的：

CLIENT --> FIN

SERVER --> RST //SERVER 返回 RST 数据包

需要注意的是：这种方法和系统的实现有一定的关系。有的系统不管端口是否打开，都回复 RST，这样这种扫描方法就不适用了。此扫描方法适合于扫描 UNIX 系统类型的主机,但是容易出现误报。

4) TCP ACK 标志端口扫描

这种扫描方法是向目标主机的一个端口发送一个只有 ACK 标志的 TCP 数据报，如果主机反馈一个 TCP RST 数据包，表示这个主机是存在的。如果返回的这个 TCP RST 数据包中 TTL 值不大于 64 或者 WINDOW 值为非零，表明这个端口处于打开状态，否则端口就为关闭状态

TCP ACK 标志端口扫描是“半开”扫描方法的一种，扫描过程如下：