Network Security Development Toolkit

网络安全开发包详解

刘文涛 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络安全开发包详解

刘文涛　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书以计算机网络安全开发包技术为核心，详细讨论了几个著名的网络安全开发包，它们分别是网络数据包捕获开发包 Libpcap，Windows 网络数据包捕获开发包 WinPcap，数据包构造和发送开发包 Libnet，通用网络安全开发包 Libdnet，网络入侵检测开发包 Libnids。书中对每个开发包的功能、原理和安装步骤进行了介绍，对开发包的各种数据结构和输出函数进行了详细阐述，并通过举例对开发包的使用方法进行了详细说明，每个例子都给出了完整的源代码并有详细的注解和结果分析。

本书可作为计算机网络及网络安全专业的教学参考书，也可供网络安全研究和开发人员，以及网络安全爱好者参考。

图书在版编目（CIP）数据

网络安全开发包详解 / 刘文涛编著. —北京：电子工业出版社，2005.10
ISBN 7-121-01744-X

Ⅰ. 网… Ⅱ. 刘… Ⅲ. 计算机网络—安全技术—软件包 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2005）第 103947 号

责任编辑：张来盛 zhangls@phei.com.cn
印　　刷：北京智力达印刷有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：31　字数：872 千字
印　　次：2005 年 10 月第 1 次印刷
印　　数：5 000 册　　定价：42.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

随着网络技术的飞速发展，网络安全问题变得日益严重，对网络安全的研究也越来越重要。在网络安全领域，有很多网络安全技术，如防火墙、入侵检测、安全扫描、网络嗅探、协议分析、流量统计、网络管理以及蜜罐技术等，无论是研究这些技术的原理，还是直接使用这些技术来设计网络安全系统，都会遇到它们的程序设计与开发问题。例如，在研究这些技术的时候，通常要根据研究的理论来设计一个模型，以此模型来验证技术的正确性和性能；还有就是直接运用成熟的网络安全技术来设计一个应用系统，其中常见的有：防火墙系统（如 Netfilter，pktfilter 等），入侵检测系统（如 Snort 等），网络安全扫描系统（如 Nmap，Nessus 等），网络嗅探器（如 Tcpdump/Windump，Sniffer 等），网络协议分析系统（如 Ethereal，Ettercap 等），蜜罐系统（如 Honeyd）等。

无论是作为研究的模型还是成熟的应用系统，它们的设计和实现都离不开一些网络安全操作，其中一些操作是很基本的，使用频繁，而且很多都是底层操作，如网络地址的操作、网络接口的操作、数据包的捕获、数据包的构造、数据包的发送等。还有一些操作比较复杂，如流量的统计、路由的管理、ARP 缓存的配置、防火墙的管理和配置等。这些操作都会在开发模型或应用系统时碰到，如果这些功能都已经实现，就只需调用它们，这样会大大提高开发的效率，从而降低成本，节省时间和精力。

为了实现这一目标，人们开发了关于这些操作的专用网络安全开发包。网络安全开发包是指用于网络安全研究和开发的一些专业开发函数库，它的主要作用是实现网络安全研究和开发的基本功能，为研究者和开发者进一步研究和开发网络安全提供编程接口，使网络开发人员能够忽略网络底层细节的实现，从而专注于程序本身具体功能的设计与开发。使用它们，会大大加快程序设计的速度。由于这些开发包已经经过时间的考验，非常稳定，使用它们也会提高程序的稳定性。利用它们，网络安全开发者可以很方便地编写出具有结构化强、健壮性好、可移植性高等特点的网络安全应用程序。网络安全开发包实现的都是某一种或某一类网络安全技术，都是经过很多网络安全研究和开发者的长期研究而形成的，人们的不断测试和使用使它们逐渐成熟起来，在实际应用中得到了深入推广。

网络安全开发包有很多种，功能也大不相同，其中比较著名、应用广泛、最具代表性的开发包有以下几种：

- 网络数据包捕获开发包 Libpcap；
- Windows 网络数据包捕获开发包 WinPcap；
- 网络数据包构造和发送开发包 Libnet；
- 网络入侵检测开发包 Libnids；
- 通用网络安全开发包 Libdnet。

这些著名的网络安全开发包与上述网络安全技术密切相关，它们在网络安全领域得到了广泛的应用。这些网络安全开发包实现了一些网络安全技术，并为其他网络安全技术的开发打下坚实的基础，因而对于研究网络安全技术和开发网络安全应用程序是很有帮助的。

本书对上述网络安全开发包进行了详细讨论，详细阐述开发包的原理、数据结构、输出函数和使用方法。

本书的特点如下：

- 介绍当今最著名的网络安全开发包，包括 Libpcap，WinPcap，Libnet，Libdnet 和 Libndis 等，全部以最新版本进行介绍。
- 讲解详细、透彻，对每个网络安全开发包的数据结构、输出函数以及使用方法都进行了详细阐述，特别对其使用方法进行了深入而细致的讨论。
- 针对每个网络安全开发包，提供了丰富的例程，每个程序短小精悍，都有全部源代码（需要这些源代码电子文档的读者，请与作者或本书责任编辑联系），对程序都做了详细注解，对其编译过程和运行结果都进行了详细分析。

在本书的编写过程中，得到了很多朋友的帮助，在此对他们表示真挚的感谢。同时也感谢我的亲人，他们的支持和理解是我创作的动力。

由于作者水平有限，再加上网络安全技术的发展十分迅速，书中难免有不妥和错误之处，恳请广大读者赐教。读者可以通过 E-mail 与作者联系。

E-mail：securitybook@163.com（作者）；zhangls@phei.com.cn（责任编辑）

刘文涛

2005 年 7 月于武汉

目　　录

第1章 网络安全

1.1 网络安全问题

1.1.1 网络安全重要性

随着网络技术的飞速发展和网络时代的到来，网络安全问题变得越来越严重。现在，全球每年关于网络安全问题的损失是巨大的。每年关于网络安全问题的报道层出不穷，产生的损失越来越大，为解决网络安全问题而投入的资金也越来越多。

网络安全问题严重影响了人们的生活和工作，以至整个国家的安全。它可能对国家的重大部门造成严重后果，如金融部门、政府机构、军事设施、公共基础设施等。因为现在大多数部门都实现了网络信息系统，这样就为网络安全问题提供了可能产生的土壤。

特别是现在网络技术的普及和发展，更为网络安全问题的发展提供了条件。可以肯定地说，哪里有网络哪里就有网络安全问题。现在，很多个人和家庭都连接到网络，他们的网络安全意识薄弱，是最容易受到网络安全问题困扰的群体。

互联网的影响已经逐渐渗透到我国国民经济的各个领域和人民生活的各个方面。但是，随着互联网应用的不断创新与发展，网络安全也面临着前所未有的严峻形势，网络安全领域所面临的挑战日益严峻。

所谓网络安全，是指网络系统的硬件、软件及系统中的数据信息能够受到保护，不会因为偶然或者恶意原因而遭破坏、更改、泄露，系统能够连续、可靠地运行，网络服务不被中断。但在现实中，绝对的网络安全是没有的。

由于网络安全问题是多种多样的，很多新的网络安全问题不断涌现，防不胜防。已知的网络安全问题就包括很多种，目前比较有影响的有以下几种：

（1）网络病毒感染。这可以说是最容易遇到的网络安全问题。网络病毒层出不穷，其传播的方式也不断发展，既可以通过邮件传播，也可以通过网络即时通信系统传播，还可以通过网页传播。而且，新的病毒还跟其他网络安全技术（如木马、间谍软件）相结合，产生综合病毒，极难防范。因此，病毒经常给用户带来巨大的经济损失。

（2）木马问题。这个网络安全问题变得越来越突出，很多木马程序在网络上可以轻易得到，而且其使用方法极其简单，但是其危害程度非常高。如果计算机被植入木马，就相当于整个计算机被别人所控制，任人为所欲为了。由于新的木马程序不断涌现，感染木马后又难以察觉，所以木马问题值得重视。

（3）恶意扫描。对网络主机的扫描，是攻击者最先做的事情，它能够检查出主机存在多少漏洞，以及漏洞的种类等很多有价值的信息，它是攻击者进行攻击的基础。本来网络安全扫描技术是一个非常有效的网络防御技术，但是如果被攻击者所使用，就变成了危害网络安全的技术了。

（4）网络监听。它可以监听整个网络的数据包，然后查看其数据内容。本来，网络监听可以用于网络管理和网络流量检测，但是攻击者使用它就变成了窃取网络信息的行为了。

（5）垃圾邮件。这也是人们普遍遇到的网络安全问题。由于邮件的使用非常广泛，它已成为人们一种重要的通信方式。但是，与邮件相关的安全问题也非常多，其中最严重的就是垃圾邮件，严重影响了人们正常地使用电子邮件。

（6）网络仿冒。它使用假的网络信息来代替真的网络信息，最明显的表现形式就是使用假的网页来代替真的网页。例如，使用一个假的登录网页套取你的银行账号和密码。现在，这样的仿冒问题变得越来越多，有时分不清是真是假。

（7）网页篡改。这是很多攻击者攻击服务器后的一种典型行为。网页被篡改了就证明此服务器已经被攻击者控制了，攻击者可以修改网页，也可以进行很多其他的破坏行为，如删除服务器的重要数据。但给公众最大的影响还是网页被更改，用户不能正常访问服务，这是很多服务器拥有者觉得最难堪的事情。不仅影响了服务器的正常服务功能，也有损于形象。

（8）拒绝服务攻击。这也是现在遇到的比较常见的一个网络问题，它使得正常的网络服务不能进行而导致损失。特别是在一些重要的网络服务上，此问题的危害性更突出。由于网络协议本身固有的缺陷，使得解决拒绝服务攻击变得非常棘手。

不断涌现的新的攻击方式使网路安全问题变得更加严重，如果不能很好地解决网络安全问题，对整个网络的发展会产生巨大的负面影响。网络安全问题的发生范围不断扩大，就连现在的手机等无线网络产品都有可能受到网络攻击。

现在，攻击者的水平在不断提高，他们攻击的对象由以前小型的主机到现在大型的服务器以及大型的网络。他们的攻击经常是有组织和有目的的攻击，其破坏性不断增加；攻击者发现漏洞和找出漏洞的攻击方法越来越快，甚至赶在软件厂商发布漏洞补丁的前面。

1.1.2 网络安全目标

现实中网络存在很多安全问题，人们不断研究并积极地解决这些问题。很多网络安全技术相继问世，不断发展，其根本目的是确保网络的安全。网络安全的目标包括以下内容：

（1）保密性——网络数据不被泄漏给非授权的用户、实体和过程，或供其利用的特性。

（2）完整性——网络数据未经授权不能被改变的特性，即信息在存储或传输过程中保持不被修改，不被破坏和丢失的特性。

（3）可用性——网络信息可被授权实体访问并按需求使用的特性，即：网络信息服务在需要时，允许授权用户或实体使用，或者在网络部分受损或需要降级使用时，仍然能够为授权用户提供有效服务的特性。

（4）可控性——对信息的传播及内容具有控制能力的特性。

（5）可靠性——网络信息系统能够在规定的条件下和规定的时间内完成规定的功能的特性。

（6）不可否认性——在网络信息系统的信息交互过程中，确信参与者的真实同一性，所有参与者都不可能否认曾经完成的操作。

要实现上述目标不是一件容易的事情，不可能只使用某一种网络安全技术就能够解决。在现实的实践中，一般都需要结合多种网络安全技术来达到这个目的。即使这样，也只是接近这个目标，而不能够完全满足。要实现这个目标，需要网络安全研究者不断努力。

1.1.3 网络安全策略

网络安全问题产生的原因是多种多样的，它可能是由于系统本身的问题，如目前使用最广泛的 TCP/IP 协议，由于历史的原因，TCP/IP 协议存在很多的安全漏洞；也可能是用户管理出现的问题，如由于管理不当或管理的疏忽而造成网络存在安全问题。所以，网络的管理至关重要，很多出现的网络安全问题并不是由于外在的网络攻击造成的，而是由于管理的漏洞而产生的。

在网络安全中，除了采用各种网络安全技术措施之外，加强网络的安全管理，制定有关规章制度，对于确保网络安全、可靠地运行，将起到十分有效的作用。网络的安全管理策略有很多，如确定安全管理等级和安全管理范围，制定网络系统的维护制度和应急措施等。

确定一个完整的网络安全策略是保证网络安全的一个重要手段。现在比较流行的一个网络安全模型 PPDR（Policy Protection Detection Response）就是以网络安全策略为核心的。PPDR 安全模型是一个动态模型，它包括策略（Policy）、防护（Protection）、检测（Detection）、响应（Response）四个部分。策略是这个模型的核心，反映了整个网络所要具备的网络安全目标，网络安全的其他几个方面要围绕着策略而进行。PPDR 是一个基于时间的模型，首先是防护，对整个网络进行保护，但它是被动的；然后就是对网络进行不断的检测，检测在这个模型中占据重要的地位；如果在检测的过程中发现有问题存在，就要及时作出响应，这时就要执行响应模块。

1.2 网络安全技术

随着对网络安全的不断研究，涌现出了很多网络安全技术，如网络安全扫描技术、网络数据包生成技术、网络防火墙技术、入侵检测技术、协议分析技术、蜜罐技术、加密技术以及认证技术等。

网络安全包括的内容极其广泛，它跟其他领域的知识联系得非常紧密。由于网络上传输的数据是信息，所以信息安全技术也与网络安全密切相关。信息安全与网络安全密不可分，有人把网络安全归纳到信息安全之中，也说明了网络安全和信息安全之间有密切联系。其中，最能体现这种联系的就是密码技术。密码技术是信息安全的核心技术，而加密技术是密码技术的一个重要内容。若在网络中传播的信息不想让别人知道，就需要进行加密。信息交换加密技术主要分为两类：对称加密和非对称加密。在对称加密技术中，对信息的加密和解密都使用相同的密钥。这种加密方法可简化加密处理过程，信息交换双方都不必彼此研究和交换专用的加密算法。如果在交换阶段私有密钥未曾泄露，那么机密性和报文完整性就可以得到保证。在非对称加密体系中，密钥被分解为一对。这对密钥中任何一个都可以作为公开密钥通过非保密方式向他人公开，而另一个作为私有密钥加以保存。公开密钥用于加密，私有密钥用于解密，私有密钥只能由生成密钥的交换方掌握，公开密钥可广泛公布，但它只对应于生成密钥的交换方。非对称加密方式可以使通信双方无须事先交换密钥就可以建立安全通信，广泛应用于身份认证、数字签名等信息交换领域。非对称加密体系一般建立在某些已知的数学难题之上，是计算机复杂性理论发展的必然结果，其中最具代表性的是 RSA 公钥密码体制。

密码技术是信息安全的基石，有了它就可以发展很多其他安全系统，包括计算机网络系统。与密码技术密切相关的网络安全技术就是安全协议，如 Kerberos 协议、IPSec 协议。它

们是安全协议，只是一种协议，但跟密码技术密切联系。由密码技术而发展起来的 PKI 技术更是一个重点内容，PKI（Public Key Infrastructure）是用公钥原理和技术实施和提供安全服务的具有普适性的安全基础设施。它主要使用了两种技术，即数字签名技术和消息认证码技术。还有为了保护 Web 通信的安全，于是产生了 SSL（Secure Socket Layer）/TLS（Transport Layer Security）安全协议。它们的主要目的是为两个通信个体之间提供保密性和完整性。其中比较著名的是 OpenSSL，其他安全协议还有 S/MIME, SET, SSH 和 HTTPS。

网络安全除了与信息安全技术密切相关外，还与其他方面的内容有直接联系，如计算机网络，特别是网络协议方面。由于计算机网络的核心是网络协议，所以讨论协议与网络安全的关系是一个重要的网络安全内容。注意这里讨论的协议与网络安全不是指安全协议（Ipsec 协议、Kerberos 协议等），而是指由于网络协议而产生的一些网络安全问题。例如由于 TCP/IP 协议的一些缺陷而产生的网络安全问题等。

一些网络攻击方式主要是针对计算机网络协议而发生的攻击。由于流行的 TCP/IP 协议存在固有的缺陷，所以会产生各种各样的网络安全问题。为了解决这些网络安全问题，于是就提出了很多与网络协议密切相关的网络安全技术，如上述的防火墙技术、入侵检测技术、网络安全扫描技术、协议分析技术和数据包生成技术等。这些技术的出现，都是为了解决与协议相关的网络安全问题的。

在此着重介绍一些与网络协议密切相关的网络安全技术。

1.2.1 网络数据包捕获技术

很多网络安全系统最首要的任务就是捕获网络上的数据信息，而网络数据包捕获技术就解决了这个问题。网络数据包捕获技术是从网络上捕获所有的或者特定的网络数据包信息，供其他网络安全系统所用。它的功能非常简单，就是捕获网络上的数据包信息。

不同的网络有不同的捕获技术，不同的操作系统其捕获的机理也稍有不同，所以在选择捕获技术的时候要慎重考虑。由于现在用得最多的网络形式是以太网，所以下面讨论最多的是以太网环境下的数据包捕获。而以太网采用了 CSMA/CD 技术，它使用了广播机制，所有与网络连接的机器都可以看到网络上传播的数据。在以太网环境下捕获数据包是非常容易的。操作系统提供的捕获机制主要有以下三种。

1．SOCK_PACKET 类型套接口

Linux 中套接字类型中有一种套接字类型 SOCK_PACKET。SOCK_PACKET 类型的 socket 可以接收网络上所有数据包。它的实现由操作系统提供的编程接口来进行。

2．数据链路提供者接口（DLPI）

数据链路提供者接口（DLPI，Data Link Provider Interface）定义了数据链路层向网络层提供的服务，是数据链路服务的提供者和使用者间的一种标准接口，在实现上基于 UNIX 的流（Streams）机制。数据链路服务的使用者既可以是用户的应用程序，也可以是访问数据链路服务的高层协议，如 TCP/IP 等。

3．伯克利数据包过滤器（BPF）

伯克利数据包过滤器（BPF，Berkeley Packet Filter ）是一个高效的数据包捕获机制。它工作在操作系统的内核层。BPF 主要由两部分组成：网络转发部分和数据包过滤部分。网

络转发部分是从链路层中捕获数据包并把它们转发给数据包过滤部分，数据包过滤部分是从接收到的数据包中接收过滤规则决定的网络数据包，其他数据包就被抛弃。

这两个部分都是在操作系统内核层实现的，它提供给应用层的数据包是过滤后的数据包，所以捕获数据包和过滤数据包都是在内核中完成的，效率很高。而且，它使用了数据缓存机制，使捕获数据包缓存在内核中，达到一定量的时候就传递给应用程序，这样也提高了处理的效率。基于 BSD 的系统使用 BPF，基于 SVR4 的系统一般使用 DLPI。从效率上来讲，BPF 比 DLPI 性能好很多，而 SOCK_PACKET 更弱。

在实际应用中，实现网络数据包捕获技术的代表是 Libpcap。Libpcap 是一个专业的跨平台的网络数据包捕获开发包。使用 Libpcap 可以很轻松地实现网络数据包的捕获功能，它的捕获机制就是 BPF 捕获机制。

另外，在 Windows 平台有与 Libpcap 兼容的 Winpcap 开发包，它是专门针对 Windows 平台而开发的，是 Windows 平台下的专业网络数据包捕获开发包，它也屏蔽了不同 Windows 操作系统的区别。

1.2.2 网络协议分析技术

由于网络的核心是网络协议，所以网络协议分析技术在网络安全领域也是一项重要的技术。网络协议分析是指对网络上的数据进行相应的协议分析。网络上的协议是多种多样的，所以产生的数据也是不同的，但是一个网络数据归根结底是基于协议产生的，也就是说任意一个网络数据都使用了一定的协议。究竟是什么协议呢？那就要对数据包进行协议分析，得出数据包的整个协议内容。

现在流行的协议是 TCP/IP 协议栈。它里面最核心的协议有以太网协议、ARP/RARP 协议、IP 协议、UDP 协议、TCP 协议、ICMP 协议等。当然还有很多应用层协议，如 HTTP 协议、FTP 协议、Telenet 协议、DNS 协议、POP3 协议等。新的协议层出不穷，各种各样的网络系统使用各种各样的协议，然后它们之间才能够通信。协议是公开的，不然就不可能进行通信，所以对协议的分析是可行的。

协议分析的过程主要包括三部分内容：捕获数据包、过滤数据包和具体协议分析。

1．捕获数据包

对网络数据包的协议分析，第一步就是要捕获网络上的数据包。可以使用专业的捕获数据包的开发包，如比较著名的开发包 Libpcap 和 Winpcap，在本书的后面章节将对它们进行详细讨论。

当然，也可以不使用专业的捕获数据包的开发包，而利用操作系统提供的功能来实现，但是那样是比较烦琐的，容易出错。在不同的操作系统下面，捕获数据包的实现不尽相同。

2．过滤数据包

由于网络上的数据信息量是庞大的，不可能对每个数据进行协议分析，并且在实际应用中有时只想分析某种具体的协议，其他协议都不用考虑。这样，就需要对捕获到的数据包进行过滤。

过滤的方式有两种，一种是在内核层就过滤掉，另一种是在应用层过滤。显然，第一种的效率要高一些，因为从内核层到应用层之间的转换是费时费力的，这样对性能有很大的影响。

如果使用开发包 Libpcap，它里面提供了 BPF 过滤机制，它是在内核层实现过滤的，效率很高，而且 BPF 过滤机制进行了优化处理，效果明显改善。所以，使用 Libpcap 不仅实现了数据包的捕获功能，也可以实现数据包的过滤功能。

3. 具体协议分析

捕获到特定的网络数据包之后，就可以分析网络协议了。根据 TCP/IP 协议层次的概念，对网络数据包的协议分析是从链路层开始的。首先分析数据包的链路层协议，如以太网协议等。其次根据链路层协议的分析结果分析网络层协议，判断网络层的协议是什么，如 IP 协议等。然后再根据网络层协议分析的结果分析传输层协议，如 TCP 协议、UDP 协议等。最后根据传输层协议分析应用层协议，如 HTTP 协议、FTP 协议等。这样，一层一层地分析下去，就可以把整个数据包的协议都分析出来。

使用网络协议分析技术可以设计专门的网络协议分析系统和各种网络嗅探器，如著名的网络嗅探器 Tcpdump 和 Windump，著名的网络协议分析系统 Ethereal 等。

网络协议分析技术还可以应用到其他各种系统中。例如，它可以应用于网络流量统计系统、网络监视系统、网络入侵检测系统、网络安全扫描系统等。可以说，网络协议分析技术是各种网络安全系统的基础，掌握网络协议分析技术对于研究和设计其他网络安全系统是很有裨益的。

1.2.3 网络数据包生成技术

数据包生成技术是指人工构造网络数据包，然后把此网络数据包发送到网络上，让它们像正常的网络数据信息一样传输的技术。网络数据包捕获技术实现的是被动地从网络上捕获数据包，而数据包生成技术是主动地构造网络数据包，并把它们放到网络上。网络数据包构造技术的功能包括构造各种各样的网络协议数据包，如 TCP/IP 协议栈中的各种协议，然后把构造的数据包发送到网络上。由于网络协议是多种多样的，所以构造的网络数据包也应该是多种多样的。

利用网络数据包生成技术，可以构造各种各样的网络安全系统，如网络安全扫描系统、网络安全测试系统。

网络安全扫描系统扫描网络或主机的漏洞，可以利用数据包生成技术来完成构造数据包的功能，然后发送给远程主机来探测远程主机，根据返回的信息来检查远程主机的漏洞。

使用网络安全测试系统可检测其他安全系统（如防火墙系统、入侵检测系统）的性能。构造各种各样的网络数据包来检测防火墙的性能，是测试网络防火墙的一个重要手段。同样的道理，对入侵检测系统的测试，也可以构造不同的网络数据包进行测试。所构造的网络数据包不仅可以是正常的网络数据包（符合协议规定），也可以构造异常的网络数据包（不符合协议规定）。通过构造异常的网络数据包来检测入侵检测系统的性能，是非常有效的一个检测方法。

利用网络数据包生成技术可以产生各种各样的网络攻击手段。例如，TCP SYN 拒绝服务攻击（SynFlood）、死亡之 ping（ping of death），攻击泪滴（teardrop）等，都可以使用数据包生成技术来实现。可以说，数据包生成技术是攻击者用得最多的一种技术。

在实际应用中，数据包生成技术的代表是 Libnet。Libnet 是一个专业的网络数据包生成开发包。利用 Libnet 可以构造任意的网络协议数据包，然后发送到网络上。Libnet 现在支持

的协议种类很多，并且开发者只要根据 Libnet 的规范还可以对其进行其他协议的扩展。

1.2.4 网络安全扫描技术

网络安全扫描技术是通过 Internet 远程检测网络或主机的漏洞的网络安全技术，它是网络安全领域的重要技术之一。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。

网络安全扫描系统是通过网络安全扫描技术实现的一个安全工具，它在网络安全领域占有重要的地位。利用它可以做很多事情。如果是管理员，利用网络安全扫描系统可以查看系统存在的漏洞，及时进行防御和修补。如果是攻击者，利用网络安全扫描系统就可以发现被攻击者的漏洞，然后对其进行攻击。扫描技术的重要性在于它把烦琐的安全检测，通过程序来自动完成，这不仅减轻了网络管理员的工作，而且缩短了检测时间。同时，也可以认为扫描系统是一种网络安全评估软件，利用扫描器，可以快速、深入地对远程主机或网络进行安全评估。现在网络安全扫描系统的发展趋势也是向着网络安全评估专家系统进行转变的。

网络安全扫描技术很多，其中主要有以下几种。

1. 端口扫描

端口扫描是最简单的一种扫描技术，通过端口扫描就可以发现系统中哪些端口是开放的，哪些端口是关闭的。这是扫描的第一步，它表示了哪些服务是开放的。例如，如果端口 80 是开放的，一般说明 Web 服务器是打开的。然后，可以进一步对特定的端口进行其他方面的扫描，如漏洞扫描。

2. 漏洞扫描

漏洞扫描是扫描技术的核心，因为扫描的目的就是要发现漏洞。如果知道了哪些端口是开放的，就知道对应的服务器是打开的，然后就可以针对特定的服务进行漏洞扫描。不同的服务器，其漏洞的形式是不一样的，所以就可以使用专门的漏洞扫描系统，如针对 Web 服务器的 CGI 漏洞扫描。

3. 特殊扫描

特殊扫描指的是对一些特殊对象的扫描。例如，对操作系统的指纹识别，利用扫描技术来识别出远程主机使用的是什么操作系统，它的版本号是多少等信息。还有数据库扫描，它针对数据库的特点，找出与数据库相关的一些漏洞。

实际应用中的网络安全扫描系统的佼佼者是 Nmap 软件。Nmap 是一个非常优秀而著名的网络安全扫描工具，使用它可以实现很多形式的扫描技术，实现很多功能。它支持多种协议的扫描，如 UDP，TCP connect, TCP SYN (half open), ftp proxy(bounce attack), Reverse-ident, ICMP(ping sweep), FIN, ACK sweep, Xmas Tree, SYN sweep 和 Null 扫描。Nmap 还提供一些实用功能，如通过 TCP/IP 来甄别操作系统类型、秘密扫描、动态延迟和重发、平行扫描、通过并行的 PING 侦测下属的主机、欺骗扫描、端口过滤探测、直接 RPC 扫描、分布扫描、灵活的目标选择以及端口的描述。可以说，Nmap 是网络扫描系统的集大成者。