第5章 网络安全

网络安全，通常指计算机网络的安全。计算机网络是指以共享资源为目的，利用通信手段把地域上若干相对分散的、独立的计算机系统、终端和数据设备连接起来，基于网络协议进行数据交换的系统。计算机网络的发展可以追溯到20世纪60年代，第一个真正意义上的计算机网络ARPANET出现，建立了一个分布式的、去中心化的网络，连接了斯坦福研究院、加州大学圣芭芭拉分校、加州大学洛杉矶分校和犹他大学4个节点。之后网络规模越来越大，TCP/IP成为基础协议，Internet逐渐普及，互联网的用户数量突飞猛进地增长。21世纪，移动互联网兴起，云计算、物联网等新兴技术的出现也促进了互联网的飞跃式发展，一个数智化的时代来临，但随之而来的安全问题也日益严重。

网络安全是指保护计算机网络中的数据、设备和通信渠道的完整性、机密性和可用性，确保网络系统不受未经授权的访问、使用、泄露、破坏、干扰或篡改等攻击。Internet可以让你和任何人连接，但同时任何人也可以和你相连。Internet IPv4协议没有提供必要的安全机制，在它的RFC中明确指出：Security issues are not discussed in this memo。IPv6虽然降低了IPv4的一些风险，但仍带来新的安全问题。因此，了解网络安全的黑客技术以及网络安全防范技术，能够有力促进网络技术的创新和发展，防范网络犯罪，保护网络基础设施和个人隐私。

5.1 常见的黑客技术


微课5.1

黑客最初是指热心于计算机技术、水平高超的电脑高手，尤其是程序设计人员。例如世界头号黑客Kevin Mitnick(凯文·米特尼克)，从小迷上无线电技术，15岁侵入“北美空中防护指挥系统”，查看美国和各盟国的军事机密，如各国核弹头数量等。他是“社会工程学”的创始人，曾上过美国联邦调查局(FBI)的通缉名单。2000年出狱后，他“金盆洗手”，变为美国国防部网络安全顾问，他曾与人合著完成4部书：*The Art Deception*：*Controlling the Human Element of Securit*，*The Art of Intrusion*：*The Real Stories Behind the Exploits of Hackers*，*Intruders & Deceivers*，*Ghost in the Wires*：*My Adventures as the World's Most Wanted Hacker* 和 *The Art of Invisibility*，2023年，年仅59岁的Kevin因胰腺癌逝世。1983年拍摄的一部电影《战争游戏》，电脑天才大卫·莱特曼自由进入学校计算机系统改动考试分数，全无学业之忧，之后他还误撞闯入北美空中防护指挥系统的一台超级计算机，玩起了“第三次世界大战”的模拟游戏。影片中的少年黑客大卫就是以Kevin为原型的。

现在的黑客是指利用安全漏洞闯入计算机或网络取得访问权限，谋取非法的个人、经济或政治利益的攻击者，也就是第 1 章提到的黑帽。

黑客攻击手段可分为以下 3 类。

(1) 利用合法渠道收集信息。信息收集可以利用的合法途径有：目标机构的网站、新闻报道、出版物、新闻组或论坛和搜索引擎，可为下一步采取攻击提供精准目标、推荐线路和攻击方法等。

(2) 借助社会工程学方式。使用非技术手段(如假冒他人获得第三方的信任)获得未经授权的访问。

(3) 黑客技术方式。通过专门设计的攻击工具或利用计算机系统的薄弱点进行攻击。下面主要讨论第三类的一些常用黑客攻击手段。

5.1.1 扫描技术

扫描攻击就是自动检测远程或本地主机安全性弱点的程序。通过连接所有已知的 TCP/IP 端口和服务，测试目标节点，并记录目标的回答，从而可以收集到关于目标主机的有用信息。比如端口扫描可发现开放了什么服务？有什么漏洞？操作系统的类型？网络扫描可以发现网络拓扑结构，主机是否在线？扫描器就像一把双刃剑，一方面可以帮助安全管理员提高网络安全性，另一方面，如被黑客利用发现攻击目标和突破口，就可以对网络进行攻击。

常用的扫描器软件包括以下几种。

(1) 扫描软件。比如 nmap、nessus 等。nmap 工具使用如图 5-1 所示。

```
[analyst@secOps ~]$ nmap -A -T4 localhost

Starting Nmap 7.40 ( https://nmap.org ) at 2024-06-26 09:37 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00086s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0               0 Apr 19  2017 ftp_test
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)
|_  256 94:33:25:a5:0e:02:d7:bc:c8:b0:90:8a:a2:16:59:e5 (ECDSA)
23/tcp open  telnet  Openwall GNU/*/Linux telnetd
80/tcp open  http    nginx 1.12.0
|_http-server-header: nginx/1.12.0
|_http-title: Welcome to nginx!
Service Info: Host: Welcome; OS: Linux; CPE: cpe:/o:linux:linux_kerne
l
```

图 5-1　nmap 工具使用

使用 nmap 扫描本机，可以观察到开放了 21，22，23，80 等端口，以及对应的服务 ftp、ssh、telnet 和 http，还可以看到本机使用的是 Linux 操作系统等信息。

(2) 信息收集命令。比如 ping 连通性、traceroute 路由跟踪、finger 查询系统用户信息、nslookup 查询 DNS 记录、域名解析是否正常，等等。例如图 5-2，traceroute 用来查看本机和 baidu 服务器之间的路由路径，默认数据包大小是 60 字节，最大存活数 TTL 为 30，第一个检测数据包的 TTL 值默认为 1，可以用-f 参数设置大小。默认每一个 hop 发送 3 个数据包，响应返回时间有 3 个(ms)。从第 11 行开始出现 3 个 *，可能是防火墙封掉了 ICMP 的

返回信息，故得不到相关的数据包返回数据。

```
[analyst@secOps ~]$ traceroute www.baidu.com
traceroute to www.baidu.com (183.2.172.185), 30 hops max, 60 byte pac
kets
 1  192.168.1.1 (192.168.1.1)  2.264 ms  2.201 ms  3.586 ms
 2  172.30.37.254 (172.30.37.254)  5.099 ms  4.651 ms  4.599 ms
 3  192.168.66.49 (192.168.66.49)  6.550 ms  6.513 ms  5.774 ms
 4  * * *
 5  192.168.66.250 (192.168.66.250)  5.227 ms  5.211 ms  4.853 ms
 6  * * *
 7  58.62.245.145 (58.62.245.145)  11.319 ms 113.65.112.81 (113.65.11
2.81)  5.209 ms 58.62.245.145 (58.62.245.145)  10.612 ms
 8  177.176.37.59.broad.dg.gd.dynamic.163data.com.cn (59.37.176.177)
 6.946 ms  6.553 ms  6.490 ms
 9  * * *
10  * 113.96.0.18 (113.96.0.18)  7.117 ms 113.96.4.242 (113.96.4.242)
  17.253 ms
11  * * *
```

图 5-2　traceroute 工具使用截图

5.1.2　嗅探器

嗅探器则是通过连接到交换机端口镜像的端口，捕获流量、分析协议和窃取信息。早期常用的工具有 NetXray、Sniffer Pro，目前用到的是 wireshark（前身 Ethereal），它是一个非常强大的开源网络协议分析器，如图 5-3 所示。

图 5-3　Wireshark 嗅探器示例

Wireshark 对捕获到的登录数据包进行协议解析，界面上段部分是 IP 数据包，中间是协议分层解析，下段部分是每层的原始数据包。由于 Telnet 协议是明文传输，所以通过协议分析，可以找到账号 anquan 和密码 123456。

5.1.3　电子欺骗攻击

电子欺骗攻击是利用目标网络的信任关系，获得计算机系统非授权访问的一种攻击方法。攻击者表现为“冒名顶替”或“中间人”角色。

常见的电子欺骗攻击方式有 3 种。

1. IP 地址欺骗

IP 地址欺骗是指黑客使用工具修改数据包头中的源地址，伪造合法网络上的一台机器的 IP 地址，冒充该机器与目标机通信，使得目标机误以为数据包来自它的受信任主机。例如图 5-4，攻击者 A′先攻击 A，使之死机，然后冒充 A，使用 TCP 序列号猜测方法与 B 建立 TCP 的 3 次握手连接，之后就可传输恶意数据（后门程序）给 B，达到后续非授权访问 B 的目的。

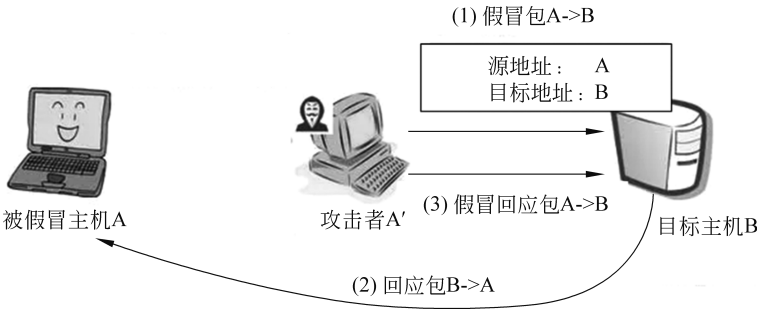

图 5-4　IP 地址欺骗示意图

TCP 协议头（RFC793）由 20 字节＋选项和填充项组成，如图 5-5 所示。

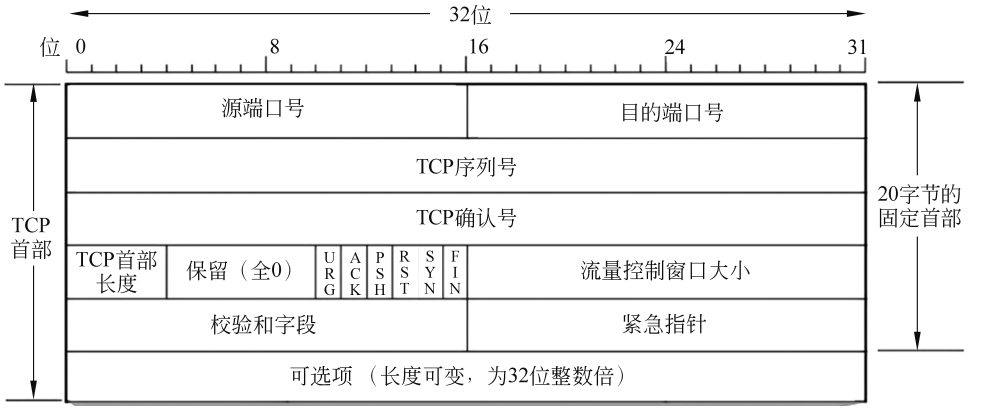

图 5-5　TCP 协议头的组成

其中，TCP 序列号（seq）表示本报文段所发送数据的第一字节的编号，在建立 TCP 连接时由内核生成的随机数作为初始序列号，RFC793 指出 seq 可被视作一个 32 位的虚拟计数器，取值空间为 0～($2^{32}-1$)，每 4 微秒（μs）加 1，seq 循环一次大概需要 4.55 小时。TCP 序列号用来解决网络包乱序问题，确保字段原始位置按顺序传输。值得注意的是，Wireshark 等抓包工具通常显示相对序列号/确认号，而不是实际序列号/确认号，这样跟踪更小的值，观察更方便。TCP 确认号（ack）表示下一次期望收到的数据的第一字节的编号。发送端收到接收端发来的 ACK 报文，如果 seq＝N，就表示序号 N 以前的（即到序号 $N-1$ 为止）的所有数据均已正常接收。TCP 确认号用来解决丢包问题。

如何计算 TCP 序列号和确认号呢？

seq＝上一次发送的 seq＋len（传输数据的字节数大小）。如果上一次发送的是 SYN 报文或 FIN 报文，虽然不携带用户数据，但 TCP 将它们视为 1 字节的数据，故 seq＝上一次发

送的 seq+1。ack=上一次收到的报文中的序列号 seq+len(传输数据的字节数大小),如果收到的是 SYN 报文或 FIN 报文,则 ack=上一次收到的报文中的序列号 seq+1。

TCP 的传输流程示例如图 5-6 所示。

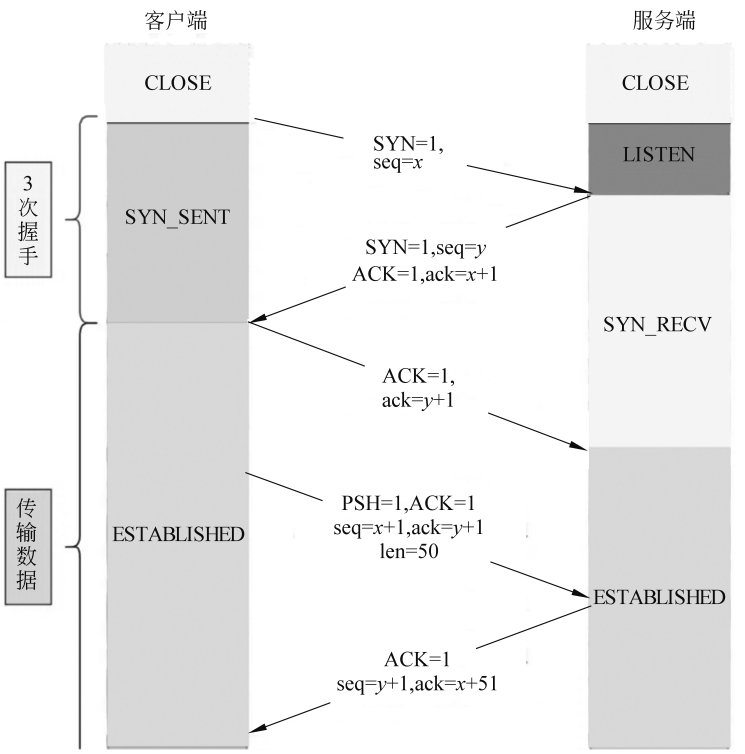

图 5-6　TCP 的传输流程示例

TCP 序列号猜测的前提有 4 点。

(1) 攻击者 A′在短时间内向目标主机 B 的某个开放端口发起若干次 TCP 连接请求,用于分析目标机器 B 的 seq 增长规律,从而推断出下一次连接的 seq 的可能值。如果目标主机 B 在攻击者发起攻击的这一段时间内没有建立其他连接,则其下一次连接建立的 seq 被攻击者猜测成功的概率就很高。

(2) 攻击者 A′能够阻止被假冒主机 A 在攻击过程对目标主机 B 发来的 SYN/ACK 报文做出响应。

(3) 攻击者 A′不能利用密钥协商或加密密钥认证等高层认证协议和目标主机 B 通信,而是依赖简单的地址认证和授权的应用协议。

(4) 攻击者 A′无法获得目标主机 B 使用基于连接标识符计算序列号空间的函数,只能猜测或推断序列号。

TCP 序列号的猜测攻击步骤如下。

(1) 攻击者 A′以真实身份向目标主机 B 发一个 SYN 包,获取 B 当前的 TCP 序列号 ISN B1。

A′→B: SYN=1,seq=ISN A1′

B→ A′: SYN=1,seq= ISN B1, ACK=1, ack= ISN A1′+1

(2) 紧接着,攻击者 A′冒充被假冒主机 A,向目标主机 B 发送一个 SYN 包,攻击者收不到 B 当前的序列号 ISN B2。

A′→B: SYN=1,seq=ISN A2′,SrcIP=A

B→ A: SYN=1,seq= ISN B2, ACK=1, ack= ISN A2′+1

(3) 攻击者 A′计算上述两步的往返时间 RTT(μs),进而算出 ISN B2:

ISN B2= ISN B1+RTT/4

(4) 攻击者 A′冒充 A 发回 ACK 报文,与主机 B 完成 3 次握手。

A′→B: ACK=1,ack=ISN B2+1,SrcIP=A

接下来,攻击者 A′就可冒充 A 向 B 传输恶意数据了。

2. ARP 欺骗

ARP 是基于网络中主机之间互相信任的基础,根据 IP 地址获取物理地址 MAC 的地址解析协议。主机发送信息时,将包含目标 IP 地址的 ARP 请求广播到局域网的所有主机,并接收返回消息,以确定目标的物理地址。收到返回消息后,将该 IP 地址和 MAC 地址存入本机 ARP 缓存并保存一定时间,下次请求时直接查询 ARP 缓存。arp -a 命令可显示 ARP 缓存表中的所有条目,即 IP 地址到 MAC 地址的映射关系。

ARP 欺骗利用这种网络中主机间的相互信任关系,即局域网上的主机可自主发送 ARP 应答消息,其他主机收到应答报文时不会检测该报文的真实性,而是直接存入本机 ARP 缓存。因此,攻击者可以向某一主机发送虚假 ARP 应答报文,改变被欺骗主机的 ARP 缓存表(即 IP-MAC 条目),使其发送的消息无法到达预期的主机或到达错误的主机,造成网络中断或中间人攻击,这就构成了一个 ARP 欺骗,如图 5-7 所示。

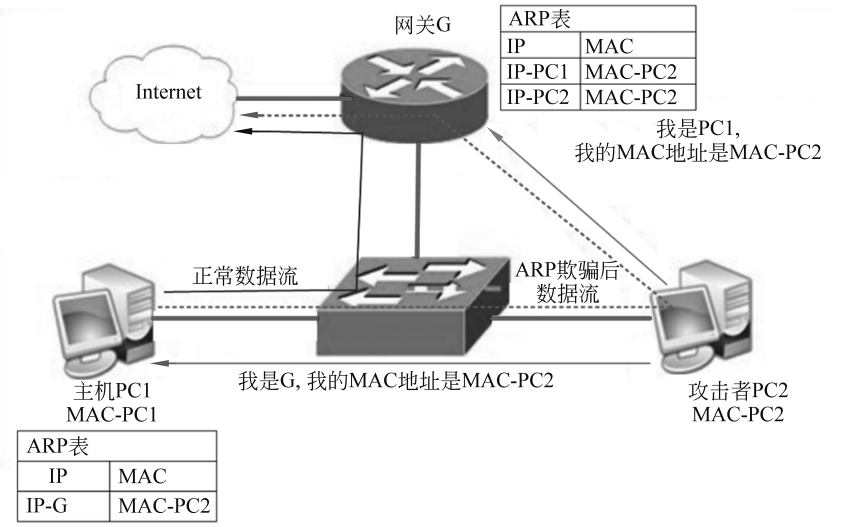

图 5-7 ARP 欺骗示意图

攻击者 PC2 分别实施 ARP 欺骗攻击,向网关 G 和主机 PC1 各发送一个伪造 ARP 应答报文,修改网关 G 和 PC1 的 ARP 缓存表,将它们的 IP 地址对应的 MAC 地址全部修改为 PC2 的 MAC 地址 MAC-PC2,这样,PC1 和网关之间的数据包都会被攻击者 PC2 截获,PC2 就充当了中间人角色,它可以将信息存起来,再转发给真正的接收者,达到偷听的效

果；也可以篡改数据后再转发给真正的接收者，达到破坏目的。

3. DNS 欺骗

DNS 协议用来解析域名，将域名和 IP 地址进行映射。比如，要访问 www.baidu.com，首先要向本地 DNS 服务器发 DNS 请求，查询 www.baidu.com 的 IP 地址。如果在本地 DNS 缓存表中没有找到记录，就会向根服务器查询，根服务器会将 com 域服务器的地址返回给本地 DNS 服务器。于是，本地 DNS 继续向 com 域服务器发查询请求，com 域服务器会将 baidu.com 授权域名服务器地址返回本地 DNS 服务器。接着，本地 DNS 服务器向 baidu.com 授权域名服务器查询，最终获得 www.baidu.com 的 IP 地址，并向用户返回 DNS 应答包，同时更新本地 DNS 缓存表。

只要攻击者拥有一台授权的 DNS 服务器，能控制这台服务器，或修改服务器上的 DNS 记录，DNS 欺骗就可能成功。如图 5-8 所示，攻击者冒充 DNS 服务器，把查询的 www.baidu.com 的 IP 地址改为钓鱼网站的 IP 地址，这样用户访问 www.baidu.com 网站时，将被引导至钓鱼网站，而不是真实网站的主页。

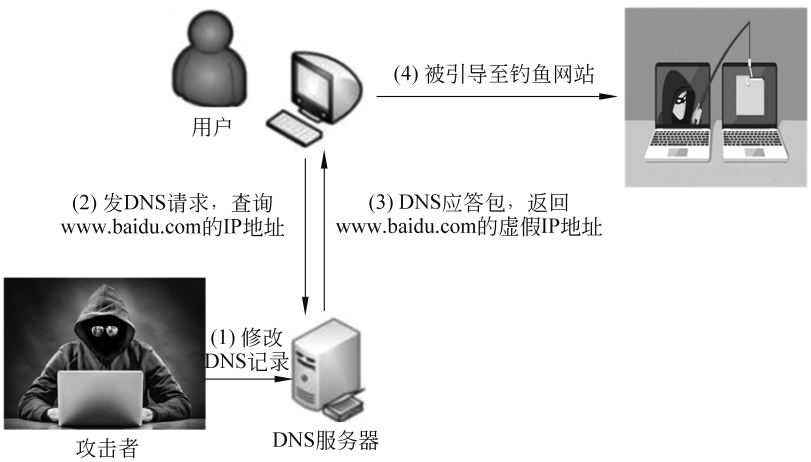

图 5-8　DNS 欺骗示意图

Kali Linux 中的 Ettercap 就是一个可用来实施 DNS 欺骗攻击的工具。Ettercap 是一个基于 ARP 地址欺骗的网络嗅探工具，主要用于交换局域网络。具体实施步骤为：首先进行 ARP 欺骗攻击，将目标机的网关 MAC 地址修改为攻击机的 MAC 地址。然后修改 DNS 映射文件/etc/ettercap/etter.dns，冒充 DNS，确保目标机首先访问虚假网关的 DNS，这样 DNS 欺骗就成功了。

DNSSEC(DNS Security Extensions)是由 IETF 提供的一种 DNS 安全认证机制(RFC2535)。它通过数字签名保证 DNS 应答报文的真实性和完整性，保护用户不被重定向到非预期地址，为了从互联网中消除该漏洞，必须在从根区域到最终域名的查找过程中的每一步都部署该技术。DNSSEC 开启后，可有效防止 DNS 欺骗和缓存污染等攻击。

5.1.4　拒绝服务攻击

拒绝服务(Denial-of-Service，DoS)是一种通过耗尽 CPU、内存、网络带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。任何对服务的干

涉，使其可用性降低或失去可用性都称为拒绝服务。使计算机或网络无法提供正常服务而造成拒绝服务的攻击行为就是拒绝服务攻击。例如，A 商家试图让存在竞争关系的隔壁 B 商店无法正常营业，他们可以采取如下类似拒绝服务攻击的手段：A 雇佣大量伪客户一直拥挤在 B 商店里，装作挑选商品，并赖着不走，让真正的消费者无法进入 B 商店；或者一直不停地和 A 店店员咨询或聊天，让店员无法为正常客户提供服务等。

拒绝服务攻击的分类方法有 3 种，如图 5-9 所示。

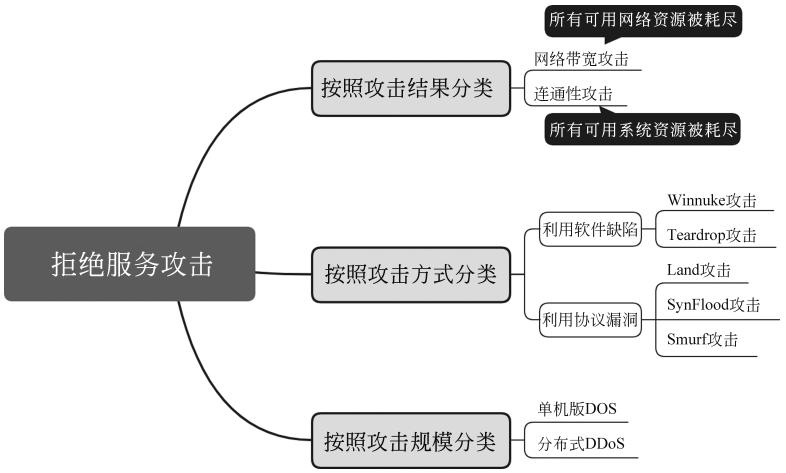

图 5-9　拒绝服务攻击的分类

(1) 按照攻击结果，可分为两类。

① 网络带宽攻击。以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过。

② 连通性攻击。用大量的连接请求冲击计算机，使得所有可用的系统资源(如接收数据包的临时缓冲区、打开连接表、一些内存数据结构等)都被消耗殆尽，最终计算机或应用服务器无法处理合法用户的请求。

(2) 按照攻击方式，可分为两类。

① 利用软件缺陷实现的攻击。软件开发过程中对某种特定类型的报文或请求没有处理，遇到这种类型的报文运行时就出现异常，导致软件崩溃，甚至系统崩溃。常见的攻击实例有 Winnuke 攻击和 Teardrop 攻击等。

② 利用协议漏洞的攻击。例如 TCP 的 3 次握手机制缺陷、IP 的源 IP 地址不做真实性确认漏洞等。常见的攻击实例有 Land 攻击、SynFlood 攻击和 Smurf 攻击等。

(3) 按照攻击规模，可分为两类，即针对单机的 DOS 攻击和针对多机系统的分布式拒绝服务攻击(Distributed Denial of Service，DDoS)。

下面详细介绍几个典型的拒绝服务攻击。

1. Winnuke 攻击

当发送方希望一些紧急数据能尽快被接收方的上层拿到时，会发送 TCP 带外数据(Out of Band，OoB)，即使 TCP 首部的标志位 URG＝1，将要传递的紧急数据混在普通数据中，同时使用 16 位紧急指针指明紧急数据在数据中的具体位置。紧急数据一般占 1 字

节，因为报文都是按序到达然后被读取，如果紧急数据太多，读取的时间太长，就会破坏 TCP 按序到达。

Winnuke 攻击又称为带外传输攻击，它利用 Windows 操作系统中的 NetBios 协议（提供若干网络服务）的缺陷进行拒绝服务攻击，即向 Windows 系统中的 TCP 139（会话服务 NBSS），UDP 138（数据报服务 NBDS），UDP/TCP 137（名称服务 NBNS）等发送一些非正常携带 TCP 带外数据的报文，但其指针字段和数据的实际位置不相符，存在重合，当操作系统（Windows 95 及之前系统）处理这些数据时，会瞬间蓝屏，并且网络功能完全瘫痪。

2. Teardrop 攻击

IPv4 协议的 IP 报文格式如图 5-10 所示。

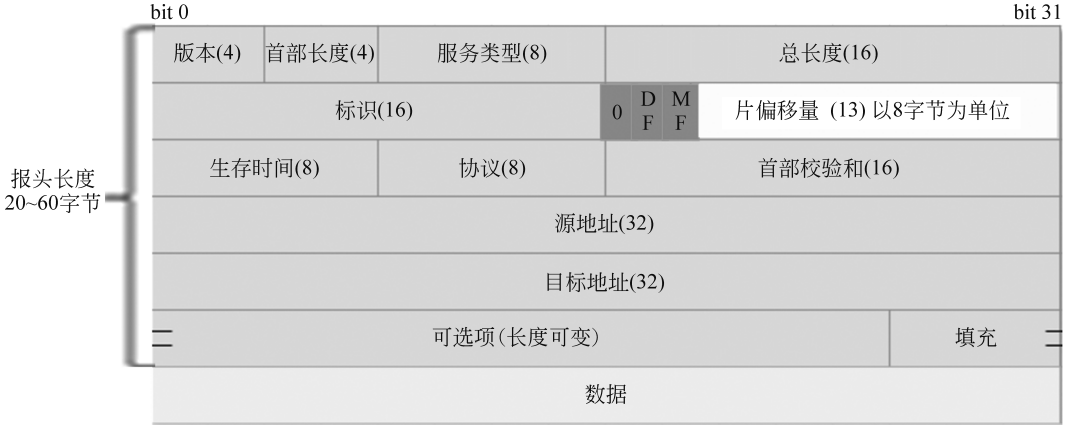

图 5-10　IPv4 协议的 IP 报文格式

其中，3 位标志位中，第 1 位为保留位，必须为 0；第 2 位 DF（Don't Fragment），DF＝1 表示不能分片；第 3 位 MF（More Fragment），MF＝1 表示后面还有分片，MF＝0 为最后一片。片偏移在分片重组时要用到，表示该片在原分组中的相对位置，以 8 字节为偏移单位，即分片长度必须是 8 的整数倍。由于分片发生在 IP 层，被分片的数据来自上层（即 TCP/UDP 层），因此首个分片带有 TCP/UDP 报头（UDP 报头：8 字节，TCP 报头 20～60 字节），其他分片不带。

例如，如果以太网发送一个长度为 1800 字节（包含 1772 字节的数据＋20 字节的头部＋8 字节的 UDP 报头）的 IP 分组，以太网最大传输单元 MTU＝1500，正常分片情况见表 5-1。第 1 块分片偏移量为 0，数据长度为 1480，第 2 块分片偏移量为 185，数据长度为 300。

表 5-1　正常分片示例

分片次数	总长度	用户数据长度	头部长度	剩余数据	分片偏移量	MF
原始	1800	1772	20（IP 报头）＋8（UDP 报头）		0	
第 1 次	1500	1472	20＋8	待发送数据：1772－1472＝300	0	1
第 2 次	320	300	20		1480/8＝185	0

正常分片 IP 报文示意图如图 5-11 所示。

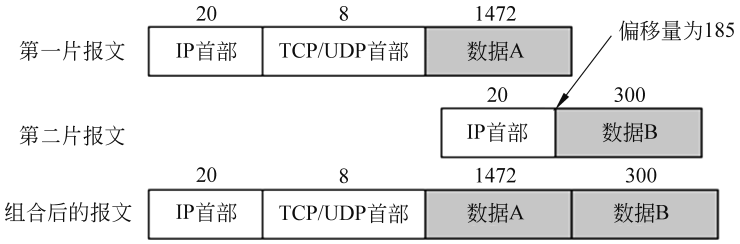

图 5-11　正常分片 IP 报文示意图

如果 IP 层分片时，会出现分片部分相交重叠（即数据包中第 2 片 IP 包的偏移量小于第 1 片结束的位移），或一个分片内嵌在另一分片中（即数据包中第 2 片 IP 包的偏移量小于第 1 片结束的位移，并且整个分片（包含数据）未超过第 1 片的尾部），将无法重新组装，重组时第二个分片长度 len＜0，执行 memcpy(* dest, * src,len)，会出现缓冲区溢出，耗尽内存资源，导致目标系统崩溃。如图 5-12 所示，这就是 Teardrop 攻击产生的原因。

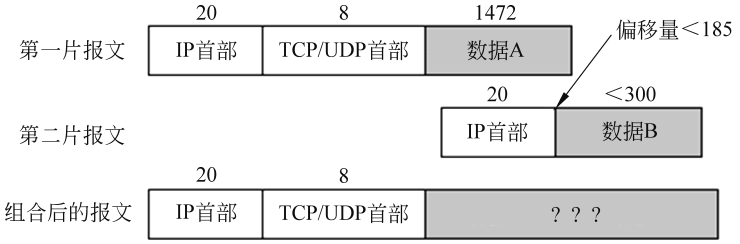

图 5-12　非正常分片 IP 报文示意图

在旧版本的 Linux 内核（1.x－2.0.x）以及 Win3.1x/95/NT 系统中处理这样的分片会崩溃，导致蓝屏死机。新的操作系统均打补丁，会自动丢弃这种病态分片数据包，防火墙可被设置分段重组功能，以防御这种重叠字段攻击。

3. Land 攻击

Land 攻击，全称为 Local Area Network Denial Attack，即局域网拒绝服务攻击，1997 年也被称为“m3lt”。它利用 TCP/IP 的 3 次握手协议漏洞，通过精心构造“伪造源 IP 地址＝目标 IP 地址，源端口＝目的端口的 TCP SYN”数据包，发给攻击目标，导致攻击目标向其自己的地址发送 SYN-ACK 包，从而创建大量无效 TCP 空连接，攻击目标和自己完成 3 次握手，直至连接超时，消耗了大量的系统资源，从而可能造成系统瘫痪或死机。不同操作系统对 Land 攻击的反应有所不同，比如 WinNT 系统响应可能会变得非常缓慢，约持续 5 分钟，而 UNIX 系统可能会崩溃。

Kali Linux 中渗透测试工具 hping3 可以定制发送 Land 攻击，例如：

```
hping3 -n -a 192.168.0.20 -S -d 100 -p 123 -flood 192.168.0.20
```

这里，-n 数字化输出主机地址

-a 源地址欺骗

-S 发送 syn 包

-d 发送数据包的大小