第3章 chapter 3

网络安全横切面

3.1 网络设备的工作原理与安全威胁

3.1.1 网络基础知识

在开始介绍网络设备之前，我们需要先了解一下计算机网络的相关知识，有助于我们更好地理解网络设备的工作原理与安全威胁。

1. 开放系统互连参考模型(OSI)

首先，我们先了解一下开放系统互连参考模型（Open System Interconnect，OSI）。开放系统互联参考模型是国际标准化组织(ISO)和国际电报电话咨询委员会(CCITT)联合制定的开放系统互连参考模型，为开放式互连信息系统提供了一种功能结构的框架。其结构从低到高分别是：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层的功能是独立的。它利用其下一层提供的服务并为其上一层提供服务，而与其他层的具体实现无关。这里所谓的“服务”就是下一层向上一层提供的通信功能和层之间的会话规定，一般用通信原语实现。两个开放系统中的同等层之间的通信规则和约定称之为协议。开放系统互连参考模型如图 3.1 所示。

(1) 物理层关注的是位流在信道上的传输。这一层规定了为传输数据所需要的物理链路创建、维持、拆除，而提供具有机械的、电子的、功能的和规范的特性。其功能是利用传输介质为数据链路层提供物理连接，实现比特流的透明传输。物理层的作用是实现相邻计算机节点之间比特流的透明传送，尽可能屏蔽掉具体传输介质和物理设备的差异。使其上面的数据链路层不必考虑网络的具体传输介质是什么。“透明传送比特流”表示经实际电路传送后的比特流没有发生变化，对传送的比特流来说，这个电路好像是看不见的。简单地说，物理层确保原始的数据可在各种物理媒体上传输。

(2) 数据链路层在物理层提供服务的基础上向网络层提供服务，通过各种控制协议，将有差错的物理信道变为无差错的、能可靠传输数据帧(frame)的数据链路。数据链路层的具体工作是接收来自物理层的位流形式的数据，并封装成帧，传送到上一层；同样，也将来自上层的数据帧，拆装为位流形式的数据转发到物理层；并且还负责处理接收端发回的确认帧的信息，以便提供可靠的数据传输。该层通常又被分为介质访问控制(MAC)

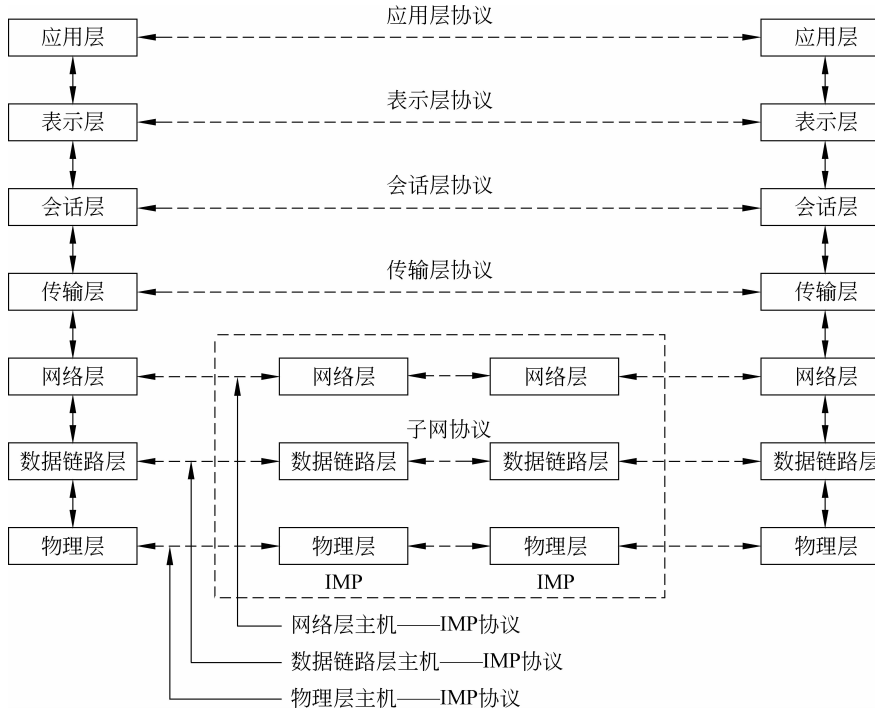

图 3.1 开放系统互连参考模型(OSI)

和逻辑链路控制(LLC)两个子层。MAC 子层的主要任务是解决共享型网络中多用户对信道竞争的问题,完成网络介质的访问控制;LLC 子层的主要任务是建立和维护网络连接,执行差错校验、流量控制和链路控制。

(3) 网络层是 OSI 参考模型中最复杂的一层,也是通信子网的最高一层。它的目的是实现两个端系统之间的数据透明传送,具体功能包括寻址和路由选择、连接的建立、保持和终止等。它提供的服务使传输层不需要了解网络中的数据传输和交换技术。在数据链路层仅仅是在相邻的两台主机间传送数据,而网络层的两台主机并不一定是相邻的,有可能要跨越几个网络。而网络层就是根据传送的数据包中携带的目的主机的地址,为它们选择合适的路径,直到数据包到达主机。并且数据包在穿越不同的网络时可能会产生兼容性问题,例如,地址格式、包的大小、使用的协议等。这些都需要网络层进行解决。

(4) 传输层实现的是端到端的数据传输。该层是两台计算机经过网络进行数据通信时,第一个端到端的层次,具有缓冲作用。传输层也是唯一负责总体的数据传输和数据控制的一层。传输层要向会话层提供通信服务的可靠性,避免报文的出错、丢失、延迟时间紊乱、重复、乱序等差错。

(5) 会话层是建立在传输层之上,利用传输层提供的服务,使应用建立和维持会话,并能使会话获得同步。其功能简单来说就是按照在应用进程之间的约定,按照正确的顺序收、发数据,进行各种形式的对话。

(6) 表示层向上对应用层服务,向下接受来自会话层的服务。表示层为在应用过程

之间传送的信息提供表示方法的服务，它只关心信息发出的语法和语义。例如，不同的主机可能对字符串实行不同的编码方式，为了不同编码的主机间信息交流就需要将传送的信息转换为双方都能理解的信息表示方式。

(7) 应用层通过使用下面各层所提供的服务，直接向用户提供服务，是计算机网络与用户之间的界面或接口。应用层由若干面向用户提供服务的应用程序和支持应用程序的通信组件组成。

根据上述内容，我们可以对网络设备按 OSI 模型进行粗略的归纳。这些归纳只是为了帮助读者建立一个概念，而现实中部分设备一定对应哪一层并没有那么明确，例如，UTM 是工作于 2～7 层的设备；应用网关实体在应用层，但跨多层工作等。

物理层的媒体包括架空明线、平衡电缆、光纤、无线信道等。通信用的互连设备指的是数据终端设备和数据通信设备间的互连设备。数据终端设备又称为物理设备，如计算机、终端等。数据通信设备在数据终端设备和传输线路之间提供信号变换和编码功能，并负责建立、保持和释放链路的连接，如调制解调器等。数据传输通常是在数据终端设备和数据通信设备路径间来回。而互连设备就是指将它们连接起来的各种装置，如各种插头、插座、各种同轴电缆、T 型接头、接收器、发送器、中继器等都是物理层的媒体和连接器。

数据链路层最常见的网络设备就是网卡、网桥、二层交换机等。其将本质上不可靠的传输媒体变成可靠的纯属通路提供给网络层。

在网络层中，具有开放特性的网络中的数据终端设备都要配置网络层的功能。现在市面上常见的网络设备主要是网关、路由器、三层交换机等。

由于 OSI 是一个理想的模型，因此一般网络系统只涉及其中的几层，很少有系统能够具有所有的 7 层，并完全遵循它的规定。在 7 层模型中，每一层都提供一个特殊的网络功能。从网络功能的角度观察：下面 4 层(物理层、数据链路层、网络层和传输层)主要提供数据传输和交换功能，即以节点到节点之间的通信为主；第 4 层作为上下两部分的桥梁，是整个网络体系结构中最关键的部分；而上 3 层(会话层、表示层和应用层)则以提供用户与应用程序之间的信息和数据处理功能为主。简而言之，下 4 层主要完成通信子网的功能，上 3 层主要完成资源子网的功能。OSI 与其说是一种模型，不如说是一种分层思想，虽然现实中的模型不是 OSI 模型，但都可以和 OSI 模型中的某几层相对应。例如，Internet 上使用的是 TCP/IP 参考模型。

2. TCP/IP 参考模型

TCP/IP(又称 TCP/IP 协议族)是一组用于实现网络互联的通信协议，其名称来源于该协议簇中两个重要的协议(IP 协议和 TCP 协议)。基于 TCP/IP 的参考模型将协议分成四个层次，它们分别是链路层(网络接口层)、网际层(IP 层)、传输层(TCP 层)和应用层。如图 3.2 所示，给出了 TCP/IP 模型以及该模型与 OSI 模型各层的对照关系和 TCP/IP 协议族。

在 TCP/IP 模型下，我们可以对各层的安全威胁进行归纳。这些内容也基本适用于对应的 OSI 模型。

OSI	TCP/IP	功能	TCP/IP 协议族
应用层	应用层	文件传输，电子邮件，文件服务，虚拟终端	TFTP，HTTP，SNMP，FTP，SMTP，DNS，Telnet 等
表示层		翻译、加密、压缩	没有协议
会话层		对话控制 建立同步点(续传)	没有协议
传输层	传输层	端口寻址、分段重组、流量、差错控制	TCP，UDP
网络层	网络层	逻辑寻址、路由选择	IP，ICMP，OSPF，EIGRP，IGMP,RIP，ARP，RARP
数据链路层	链路层	成帧、物理寻址、流量，差错，接入控制	SLIP，CSLIP，PPP，MTU
物理层		设置网络拓扑结构、比特传输、位同步	ISO2110，IEEE802，IEEE802.2

图 3.2 TCP/IP 结构对应 OSI 和 TCP/IP 协议族

1）在数据链路层中可能面临的威胁

(1) 拒绝服务：网络设备或者终端均需具有相邻设备的硬件地址信息表格。一个典型的网络侵入者会向该交换机提供大量的无效 MAC 源地址，直到硬件地址表格被填满。当这种情况发生的时候，设备将不能够获得正确的硬件地址，而无法进行正常的网络通信。

(2) 地址欺骗：在进行 MAC 欺骗攻击的过程中，已知某主机的 MAC 地址会被用来使目标交换机向攻击者转发以该主机为目的地址的数据帧。通过发送带有该主机以太网源地址的单个数据帧的办法，网络攻击者改写了目标设备硬件地址表格中的条目，使得交换机将以该主机为目的地址的数据包转发给该网络攻击者。通过这种方式，黑客们可以伪造 MAC 或 IP 地址，以便实施如下的两种攻击，即服务拒绝和中间人攻击。

2）在网络层中可能面临的威胁

(1) 拒绝服务：网络层的拒绝服务攻击以网络资源消耗为目的，它通过制造海量网络数据报文或者利用网络漏洞使系统自身循环产生大量报文将用户网络带宽完全消耗，使合法用户得不到应有的资源。典型的如 Ping flood 和 Smurf 攻击，一旦攻击成功实施，网络出口带宽甚至是整个局域网中将充斥这些非法报文，网络中的设备将无法进行正常通信。

(2) 地址欺骗：同链路层的地址欺骗目的是一样的，IP 地址欺骗同样是为了获得目标设备的信任，它利用伪造的 IP 发送地址产生虚假的数据分组，乔装成来自内部主机，使网络设备或者安全设备误以为是可信报文而允许其通过。

(3) 非授权访问：是指没有预先经过同意，就使用网络或计算机资源被看作非授权访问。对于一个脆弱的信息系统，这种威胁是最常见的。

3）在传输层中可能面临的威胁

(1) 拒绝服务：传输层的拒绝服务攻击以服务器资源耗尽为目的，它通过制造海量的 TCP/UDP 连接，耗尽服务器的系统连接资源或者内存资源。这种情况下，合法用户发出连接请求却因服务器资源耗尽而得不到应答。典型的如 TCP Flood 和 UDP Flood

攻击，目前在互联网上这类攻击工具随处可见，因其技术门槛低而被大量使用，是互联网的几大公害之一。某些情况下，攻击者甚至将攻击提升到应用层，即不仅仅是发出连接，而是发出应用数据，这样的攻击因不易与合法请求区分而更加难以控制。

(2) 端口扫描：端口扫描攻击是一种探测技术，攻击者可将它用于寻找他们能够成功攻击的服务。连接在网络中的所有计算机都会运行许多使用 TCP 或 UDP 端口的服务，而所提供的已定义端口达 6000 个以上。通常，端口扫描不会造成直接的损失。然而，端口扫描可让攻击者找到可用于发动各种攻击的端口。为了使攻击行为不被发现，攻击者通常使用缓慢扫描、跳跃扫描等技术来躲避检测。

4) 在应用层中可能面临的威胁

(1) 信息窃听与篡改：互联网协议是极其脆弱的，标准的 IP 协议并未提供信息隐秘性保证服务，因此众多应用协议也以明文进行传输，如 Telnet、FTP、HTTP 等最常用的协议，甚至连用户口令都是明文传输。这为攻击者打开了攻击之门，他们可以在网络的必经之路搭线窃听所关心的数据，盗取企业的关键业务信息；严重的甚至直接对网络数据进行修改并重放，达到更大的破坏目的。

(2) 非法信息传播：由于无法阻止非法分子进入网络世界，互联网上充斥着反动、色情、暴力、封建迷信等信息。非法分子通过电子邮件、Web 甚至是 IM 协议不断地发送各种非法信息到世界各地的网络终端上去。这些行为极大地破坏了社会的安定与和谐，对整个社会来讲，危害极大。

(3) 资源滥用：IDC 的统计曾显示，有 30%～40%的 Internet 访问是与工作无关的，而且这些访问消耗了相当大的带宽，一个不受控的网络中 90%的带宽被 P2P 下载所占用。这对于网络建设者来讲完全是灾难，它意味着投资利用率低于 10%。

(4) 漏洞利用：网络协议、操作系统以及应用软件自身存在大量的漏洞，通过这些漏洞，黑客能够获取系统最高权限，读取或者更改数据，典型的如 SQL 注入、缓冲区溢出、暴力猜解口令等。在众多威胁中，利用系统漏洞进行攻击所造成的危害是最全面的，一旦攻击行为成功，黑客就可以为所欲为。

(5) 病毒：病毒是最传统的信息系统破坏者，随着互联网的普及和广泛应用，计算机病毒的传播形式有了根本的改变，网络已经成为病毒的主要传播途径，用户感染计算机病毒的概率大大增加。同时病毒正在加速与黑客工具、木马软件的融合，可以说病毒的破坏力达到了前所未有的程度。

(6) 木马：特洛伊木马是一种恶意程序，它们悄悄地在宿主机器上运行，就在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。攻击者经常把特洛伊木马隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的机器上运行。最常见的情况是，上当的用户要么从不正规的网站下载和运行了带恶意代码的软件，要么不小心点击了带恶意代码的邮件附件。

3. 拓扑结构

除了 OSI 模型与 TCP/IP 协议，我们还需了解下计算机网络的拓扑结构。计算机网络的最主要的拓扑结构有总线型拓扑、环形拓扑、树形拓扑、星形拓扑、混合型拓扑以及

网状拓扑。其中环形拓扑、星形拓扑、总线型拓扑是三个最基本的拓扑结构。在局域网中,使用最多的是星形结构。

1）总线型拓扑

将所有的节点都连接到一条电缆上,把这条电缆作为总线。总线型网络是最为普及的网络拓扑结构之一。它的连接形式简单、易于安装、成本低,增加和撤销网络设备都比较灵活。但总线型的拓扑结构中,任意的节点发生故障,都会导致网络的阻塞。同时,这种拓扑结构还难以查找故障。总线型拓扑如图 3.3 所示。总线型拓扑结构的优点:所需电缆数量较少;结构简单,无源工作有较高可靠性;易于扩充。总线型拓扑结构的缺点:总线传输距离有限,通信范围受到限制;故障诊断和隔离比较困难;分布式协议不能保证信息的及时传送,不具有实时功能,站点必须有介质访问控制功能,从而增加了站点的硬件和软件开销。

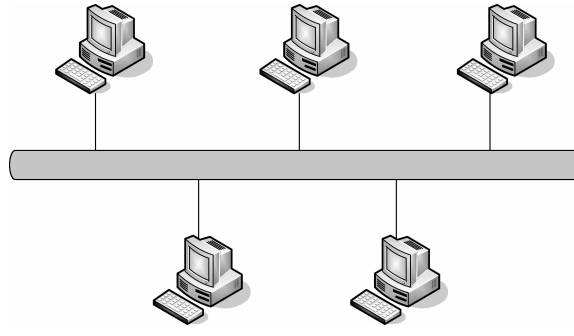

图 3.3 总线型拓扑

2）环形拓扑

入网设备通过转发器接入网络,一个转发器发出的数据只能被另一个转发器接收并转发,所有的转发器及其物理线路构成的环状网络系统。环形拓扑如图 3.4 所示。

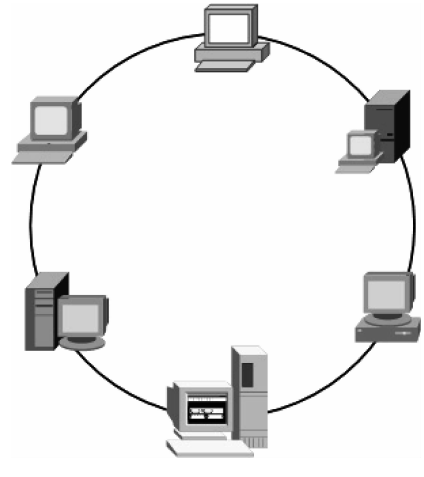

图 3.4 环形拓扑

3）树形拓扑

一种类似于总线拓扑的局域网拓扑。树型网络可以包含分支，每个分支又可包含多个结点，如图 3.5 所示。

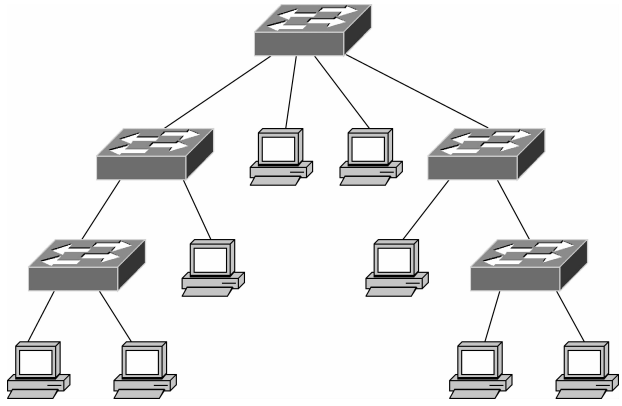

图 3.5　树形拓扑

4）星形拓扑

在星形拓扑结构中，网络中的各节点通过点到点的方式连接到一个中央节点（又称中央转接站，一般是集线器或交换机）上，由该中央节点向目的节点传送信息。中央节点执行集中式通信控制策略，因此中央节点相当复杂，负担比各节点重得多。在星形网中任何两个节点要进行通信都必须经过中央节点控制。星形拓扑如图 3.6 所示。

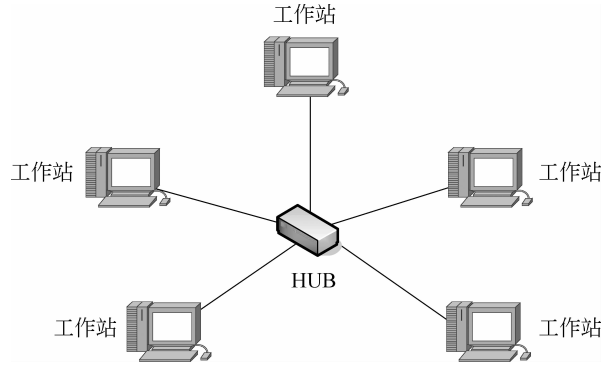

图 3.6　星形拓扑

5）混合型拓扑

这种网络拓扑结构是由前面所讲的星形结构和总线型结构的网络结合在一起的网络结构，这样的拓扑结构更能满足较大网络的拓展，解决星形网络在传输距离上的局限，而同时又解决了总线型网络在连接用户数量的限制。这种网络拓扑结构同时兼顾了星形网与总线型网络的优点，在缺点方面得到了一定的弥补。混合型拓扑如图 3.7 所示。

6）网状拓扑

这种拓扑结构主要指各节点通过传输线互联连接起来，并且每一个节点至少与其他

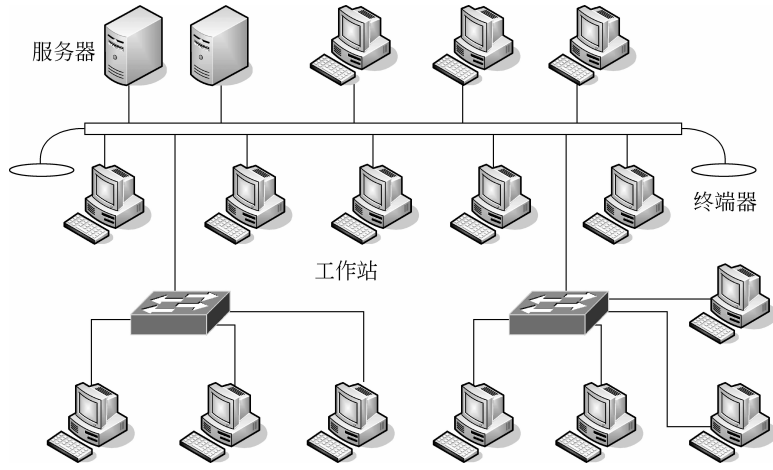

图 3.7 混合型拓扑

两个节点相连。网状拓扑结构具有较高的可靠性,但其结构复杂,实现起来费用较高,不易管理和维护,不常用于局域网。网状拓扑如图 3.8 所示。

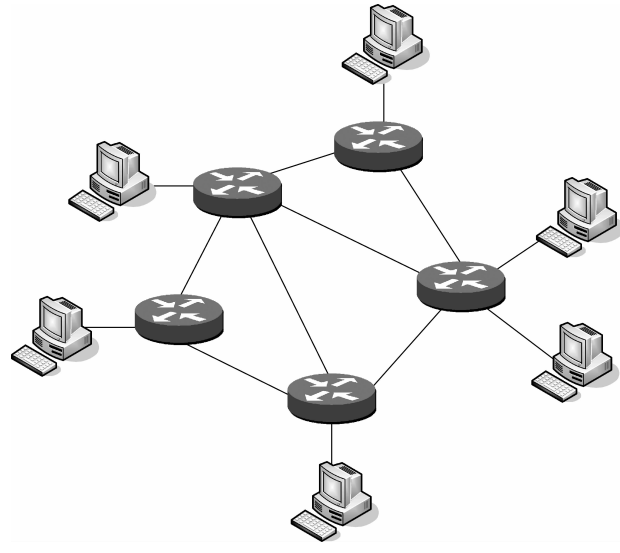

图 3.8 网状拓扑

3.1.2 常见网络设备的工作原理与安全威胁

1. 集线器的工作原理与安全威胁

集线器,英文名称为 Hub,是一种用于组建物理结构、形状为星形的网络设备。集线器的主要功能是对接收到的信号进行再生整形放大,以扩大网络的传输距离,因此它有延长物理线路距离的特性,同时把所有节点集中在以它为中心的节点上。它工作于开放

系统互联参考模型(OSI)第一层,即“物理层”。集线器属于纯硬件网络底层设备,基本上不具有类似于交换机的“智能记忆”能力和“学习”能力。但是集线器在放大正常信号的同时也放大了噪声信号,噪声信号是网络上的干扰信号,它将对正常的网络通信造成影响。集线器的端口比中继器密集,所以在某种情况下人们把集线器叫作“多端口的中继器”。集线器在接入网络后如图 3.9 所示。

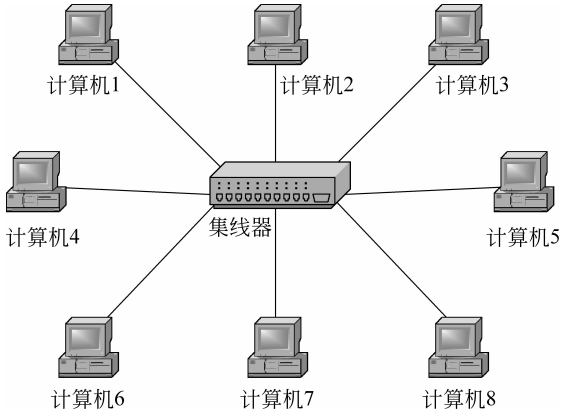

图 3.9 集线器

其工作原理是这样的,计算机 1 要给计算机 7 发送数据,计算机 1 会把数据广播到除原端口以外的所有端口上。此时接收到数据的计算机中,除了计算机 7 外的计算机解开广播包后,发现目标的 IP 地址不是计算机 7 网卡上的 IP 地址,所以将数据帧丢弃。但计算机 7 解开广播包后,发现目标的 IP 是本机网卡上的 IP 地址,它就会将数据帧从网卡复制到内存中,然后内存在将其交给 CPU 处理。

集线器也有着一些不足。首先,集线器通信时以广播的方式将用户数据包向所有节点发送,很可能带来数据通信的不安全因素,一些别有用心的人很容易就能非法截获他人的数据包。例如,接入集线器的主机,可以利用协议分析器对收到的数据进行分析,则很有可能获取发往别的主机的信息。其次,从集线器的工作方式可以看出,它在网络中只起到信号放大和重发作用,其目的是扩大网络的传输范围,而不具备信号的定向传送能力,是一个标准的共享式设备。其所有数据包都是向所有节点同时发送,加上其共享带宽方式(如果四个设备共享 10M 的集线器,那么每个设备的理论带宽就只有 2.5M),就更加可能造成网络塞车现象,更加降低了网络执行效率。接着,集线器为非双工传输,网络通信效率低。集线器所有端口连接的主机全部处于一个冲突域内,不能有多个主机同时发送数据,因此其同一时刻每一个端口只能进行一个方向的数据通信,而不能像交换机那样进行双向双工传输,网络执行效率低,不能满足较大型网络通信需求。最后,集线器不能隔离广播。所以不能将集线器连接成环状,否则广播会在环路上一直循环,形成广播风暴。广播风暴(broadcast storm)是指广播数据充斥网络无法处理,并占用大量网络带宽,导致正常业务不能运行,甚至彻底瘫痪。一个数据帧或包被传输到本地网段(由广播域定义)上的每个节点就是广播;由于网络拓扑的设计和连接问题,或其他原因导致广播在网段内大量复制,传播数据帧,导致网络性能下降,甚至网络瘫痪,这就是广

播风暴。

由于集线器的安全威胁是设备工作原理上的天生缺陷，没有办法进行补救。所以没有更有效的防御措施，唯一的办法是选用更为智能的设备，例如，采用二层交换机去替代集线器。

2. 网桥、二层交换机的工作原理与安全威胁

1）网桥

网桥(Bridge)也叫桥接器，是连接两个局域网的一种存储、转发设备，它能将一个大的局域网分割为多个网段，或将两个以上的局域网互联为一个逻辑局域网，使局域网上的所有用户都可访问服务器。简单来说就像是一个局域网与另一个局域网之间建立连接的桥梁。其工作于数据链路层上，不但能扩展网络的距离或范围，而且可提高网络的性能、可靠性和安全性。

网桥能够划分或减少冲突域，性能比集线器良好；能够基于 MAC 地址进行数据链路层选路；能够基于自学习构建 MAC 地址表；不能隔离广播，所以不能让网桥形成环路。后来，网桥被具有更多端口、同时也可隔离冲突域的交换机(Switch)所取代。

在以网桥连接的网络上，主机间发送数据并不会像集线器那样将源主机发送的数据广播到所有的接口上。这是因为在网桥的内部存有一张 MAC 表，该表记录着网桥物理接口所连接的主机 MAC 地址。这张 MAC 表简单来理解就像是我们平常路口的路牌，我们只需要看路牌就可以选择我们的目的地，而不需要走到所有路口的尽头来确认是否是我们想去的地方。例如，网络中现在有 1、2、3、4 四台计算机共同连接着一个网桥，对于模型我们可以参考图 3.9，只不过将其中的集线器换为网桥。计算机 1 给计算机 4 发送数据，数据进入网桥时，网桥通过查询 MAC 地址得知计算机 4 对应的物理接口，所以网桥就将数据直接转发到该物理接口，而不需要把数据再广播到所有接口。计算机 2 与计算机 3 的信道没有受到干扰，因此在计算机 1 与计算机 4 交换数据时，计算机 2 与计算机 3 也可以同时交换数据。

也许有人会问：计算机难道不是同时通信吗？因为计算机发送数据是以毫秒级计算，人无法感知其中细微的差别，所以很多人认为在一个网络中计算机是可以同时通信，共用一根线路的。这个说法是不准确的。计算机确实是共用一根线路，但却是轮流使用。例如，图 3.9 中，所有计算机用集线器连接在一起，当其中一台计算机向别的计算机发送数据时，因为集线器要广播到所有地址，因此占用了所有的信道。此时若是非目的主机的计算机要发送数据给别的计算机，它会先检查线路是否繁忙，如果繁忙则不能发送。因此可以得出一个结论：以太网上的多个主机在一个冲突域内，同一时刻只能有一个主机向另一个主机发送数据，如果违反了该原则就会有冲突产生。在以太网中，如果某个 CSMA/CD 网络上的两台计算机在同时通信时会发生冲突，那么这个 CSMA/CD 网络就是一个冲突域(collision domain)。图 3.9 中的计算机都处在一个冲突域内。

当网桥的 MAC 地址表不完整时，网桥是无法利用 MAC 地址表进行选路转发的，此时网桥只能跟集线器一样将数据帧广播到除源接口外的所有接口。此时网桥的广播只是单纯的 ARP 广播，不像集线器的广播，它没有带真实数据，并且只广播一次，为的是构

造 MAC 地址表，利用网桥的 MAC 地址表自学习功能记录计算机的源 MAC 地址对应的网桥接口。简单来说，这种情况就像是十字路口刚开始设立路牌，我们先得去到每个地方才知道每个路口到底通向何处，路牌才能有个正确的名字。在 MAC 地址表被成功构造后，网桥不再进行广播，此时就跟之前说的一样，利用 MAC 地址表进行快速选路并转发。网桥是不能成环的，因为网桥无法隔离广播，成环会形成广播风暴，并且会导致 MAC 地址表自学习错误。但在实际工程中，网桥通常需要物理链路成环，此时也可以靠生成树技术来解决网桥成环引发的问题。

2）二层交换机

二层交换机是一种代替网桥的产物，其工作原理与网桥是一样的，所实现的功能基本类似。差别在网桥实现功能是靠网桥内的软件来完成的，因此会出现瓶颈现象。但二层交换机采用了集成电路来决定交换逻辑算法的，没有瓶颈现象，转发速度更快，接口更密集。因此二层交换机替代了网桥。

我们之前说到了，一个典型的网络侵入者会向该交换机提供大量的无效 MAC 源地址，直到硬件地址表格被填满。这也被称为内容寻址存储器(CAM)表格淹没。CAM 是一种专用存储器件，我们之前所说的 MAC 地址就存储在 CAM 表当中，除此之外还包括对应的端口号，端口所属的虚拟局域网等。当交换机收到主机发来的一个帧，就会查看帧中的源 MAC 地址，并查找 CAM 表，如果有就什么也不做，开始转发数据。如果没有就存入 CAM 表，以便当其他人向这个 MAC 地址上发送数据时，可以决定向哪个端口转发数据。一般 CAM 表的容量可以容纳许多 MAC 记录，但不同的交换机品牌与等级也是有许多差异的。如果 CAM 表在短时间内被攻击入侵者充满，那么交换机就会 CAM 表溢出，导致正常的记录无法被交换机成功的学习到，交换机就无法选取正常的 MAC 地址与端口对应关系的选路。

生成树协议可用于交换网络中以防止在以太网拓扑结构中产生桥接循环。通过攻击生成树协议，网络攻击者希望将自己的系统伪装成该拓扑结构中的根网桥。要达到此目的，网络攻击者需要向外广播生成树协议配置、拓扑结构改变网桥协议数据单元(BPDU)，企图迫使生成树进行重新计算。网络攻击者系统发出的 BPDU 声称发出攻击的网桥优先权较低。如果获得成功，该网络攻击者能够获得各种各样的数据帧。

MAC 欺骗攻击的过程中，已知某其他主机的 MAC 地址会被用来使目标交换机向攻击者转发以该主机为目的地址的数据帧。通过发送带有该主机以太网源地址的单个数据帧的办法，网络攻击者改写了 CAM 表格中的条目，使得交换机将以该主机为目的地址的数据包转发给该网络攻击者。除非该主机向外发送信息，否则它不会收到任何信息。当该主机向外发送信息的时候，CAM 表中对应的条目会被再次改写，以便它能恢复到原始的端口。

为了防御对于二层交换机的攻击，我们一般要实现端口安全与在端口上阻止单播洪范。对于端口安全我们可以在交换机上配置端口安全选项，这么做可以防止 CAM 表淹没攻击。该选择项要么可以提供特定交换机端口的 MAC 地址说明，要么可以提供一个交换机端口可以获得的 MAC 地址的数目方面的说明。当无效的 MAC 地址在该端口被检测出来之后，该交换机要么可以阻止所提供的 MAC 地址，要么可以关闭该端口。对于

该选项的设置同时也防止 MAC 欺骗攻击。端口安全命令能够提供指定系统 MAC 地址连接到特定端口的功能。该命令在端口的安全遭到破坏时，还能够提供指定需要采取何种措施的能力。然而，如同防止 CAM 表淹没攻击一样，在每一个端口上都要指定一个 MAC 地址是一种并不足够好的解决方案。

而要防止操纵生成树协议的攻击，需要使用根目录保护和 BPDU 保护加强命令来保持网络中主网桥的位置不发生改变，同时也可以强化生成树协议的域边界。根目录保护功能可提供保持主网桥位置不变的方法。生成树协议 BPDU 保护使得网络设计者能够保持有源网络拓扑结构的可预测性。尽管 BPDU 保护也许看起来是没有必要的，因为管理员可以将网络优先权调至 0，但仍然不能保证它将被选做主网桥，因为可能存在一个优先权为 0，但 ID 却更低的网桥。使用在面向用户的端口中，BPDU 保护能够发挥出最佳的用途，能够防止攻击者利用伪造交换机进行网络扩展。

3. 路由器的原理与安全威胁

路由器(Router)，是连接因特网中各局域网、广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径，按前后顺序发送信号。在理解路由器的工作原理之前，我们应先了解什么叫作路由。路由(routing)是指分组从源到目的地时，决定端到端路径的网络范围的进程。我们可以用个形象、生动的比喻来解释这个过程。就像是寄信，我们的信就是数据，将信放入信封并填写收件人的地址与寄件人的地址，这就像是 OSI 第三层中封装 IP 报文，在报头中写入源 IP 地址(寄件人地址)与目标 IP 地址(收件人地址)。IP 数据报如图 3.10 所示。

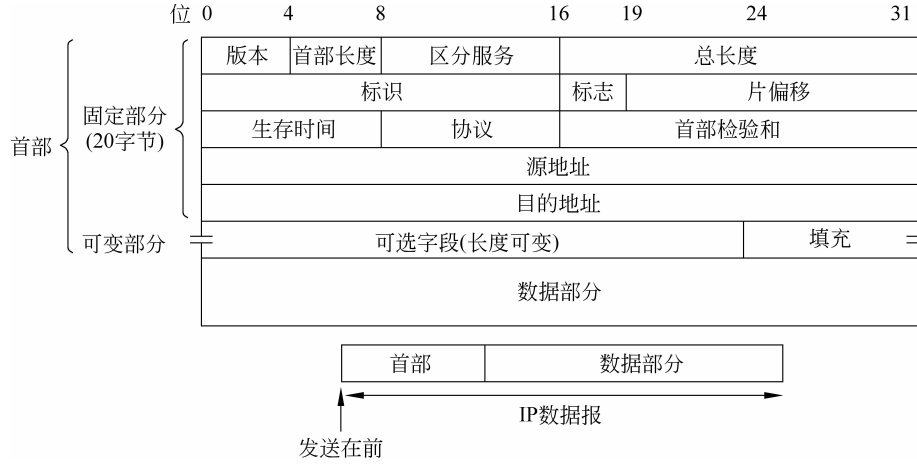

图 3.10 IP 数据报

当信密封好后，我们自然要将其投递到最近的公用邮箱以使邮政收取信件。在网络中也是这样，目标 IP 与源 IP 往往距离很远，不在同一个子网内，这时就要将源 IP 产生的数据报文投递到距离最近的路由。我们投递完信封，邮局收取邮箱里的邮件之后会将所有信件进行汇总、归类，对运送邮件做准备。路由器也是这样，路由器将所有网络的路由进行汇总或策略化后再发出本地的自治区域。信件可以采用不同的方式运送，例如，空

运、火车、轮船等。在网络中也是这样，不同的路由可能会采取不同的策略以及不同的成本路径开销，从某一条路径将数据报文送到目标所在的区域。当信件到达目标所在的区域后，又由当地的邮政再次进行汇总、分类之后分发下去，直到目标客户收取邮件。在网络中同样是如此，当数据报文到达目标所在的区域，运营商的路由器会将报文再次分发下去，直到转发给了目标 IP。

这个例子能让人较为容易地理解路由器的工作原理。但详细细节是这样的，当数据报文发出前，主机会对源 IP 的子网掩码与目标 IP 进行与运算，若是两个主机不在同一个子网中。这种情况下，主机确定两个 IP 间通信需要路由器进行路由的。此时，主机利用默认网关接口确定路由器的位置后，将报文投递到该路由器。路由器中存放着路由表，路由表或称路由择域信息库(RIB)，是一个存储在路由器或者联网计算机中的电子表格(文件)或类数据库。路由表存储着指向特定网络地址的路径(在有些情况下，还记录有路径的路由度量值)。路由表中含有网络周边的拓扑信息。该路由器会根据路由表选择到达目标子网的最佳路径后进行转发。

目前路由器已经广泛应用于各行各业，各种不同档次的产品已成为实现各种骨干网内部连接、骨干网间互联和骨干网与互联网互联互通业务的主力军。路由和交换机之间的主要区别具体如下：

1) 工作层次不同

最初的交换机是工作在 OSI 开放体系结构的数据链路层，也就是第二层，而路由器一开始就设计工作在 OSI 模型的网络层，也就是第三层。由于交换机工作在 OSI 的第二层(数据链路层)，所以它的工作原理比较简单，而路由器工作在 OSI 的第三层(网络层)，可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

2) 数据转发所依据的对象不同

交换机是利用物理地址或者说 MAC 地址来确定转发数据的目的地址。而路由器则是利用不同网络的 ID 号(即 IP 地址)来确定数据转发的地址。IP 地址是在软件中实现的，描述的是设备所在的网络，有时这些第三层的地址也称为协议地址或者网络地址。MAC 地址通常是硬件自带的，由网卡生产商来分配的，而且已经固化到了网卡中去，一般来说是不可更改的。而 IP 地址则通常由网络管理员或系统自动分配。

3) 路由器可以分割广播域

传统的交换机只能分割冲突域，不能分割广播域，而路由器可以分割广播域。由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第三层以上交换机具有虚拟局域网功能，也可以分割广播域，但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

4) 路由器提供了防火墙的服务

路由器仅仅转发特定地址的数据包，不传送、不支持路由协议的数据包传送和未知目标网络数据包的传送，从而可以防止广播风暴。

交换机一般用于局域网与局域网间的连接，交换机归于网桥，是数据链路层的设备，

有些交换机也可实现第三层的交换。路由器用于广域网与广域网之间的连接，可以解决异性网络之间转发分组，作用于网络层。他们只是从一条线路上接受输入分组，然后向另一条线路转发。这两条线路可能分属于不同的网络，并采用不同协议。相比较而言，路由器的功能较交换机要强大，但速度相对也慢，价格昂贵，第三层交换机既有交换机线速转发报文能力，又有路由器良好的控制功能，因此得以广泛应用。

那么路由器是怎么被攻击的呢？这些网络设备看似安全，但是却有不少的漏洞与后门。从最近来说，安全公司 FireEye 在许多国家的思科路由器上发现 SYNful Knock 后门程序。路由器的后门或者漏洞该如何查看？常见的方法有访问 routerpwn.com。其实，不少国内外路由器厂家，为了后期维护管理方便，都在管理固件中留下了后门。这个网站包括对许多路由器后门或漏洞的总结。利用里面所提供的信息，我们可以直接登录到留有后门或漏洞的路由器后台，窃取用户信息，甚至进行会话劫持。

4. 防火墙的原理与安全威胁

防火墙技术是对外界的网络信息进行过滤、访问控制特殊的互联网装备，通过自动清除对内部网络（将用户使用的网络称为内部网络，外界网络则被称为外部网络）存在风险的通信数据，达到保护企业内部信息安全的目的。防火墙的作用我们可归结为如下几点：

- 限制他人进入内部网络，过滤掉不安全服务和非法用户。
- 防止入侵者接近防御设施。
- 限定用户访问特殊站点。
- 为监视 Internet 安全提供方便。

1）防火墙的分类

防火墙实现技术虽然出现了许多，但总体来讲可分为“包过滤型”和“应用代理型”两大类（其中包过滤型又分为简单包过滤型和状态检测型，应用代理型又分为应用网关型和自适应代理型）。前者以以色列的 Checkpoint 防火墙和美国 Cisco 公司的 PIX 防火墙为代表；后者以美国 NAI 公司的 Gauntlet 防火墙为代表。

（1）包过滤型防火墙。

包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过，如 TCP、UDP、ICMP 等，并通过不同的 TCP 协议端口号识别基于 TCP 的各种应用等。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，而是适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙多数是由路由器集成的；之所以有效，是因为它能很大程度上满足绝大多数企业安全要求。

但如果有黑客进行 IP 地址欺骗，伪装成合法的 IP 地址，包过滤防火墙将无法进行识别，因为包过滤防火墙不能分析“会话状态”，只能针对 IP 报文的源 IP、目标 IP、源端口和目标端口进行静态检测。

根据包过滤技术的特点，参照隔离交换系统通用体系结构，可以得出，采用包过滤技术的隔离交换系统的数据接收和转发模块所面向的是单个网络数据包。根据对数据包的处理策略的不同，包过滤型防火墙可分为：简单包过滤型和状态检测型。包过滤型防火墙工作原理如图 3.11 所示。

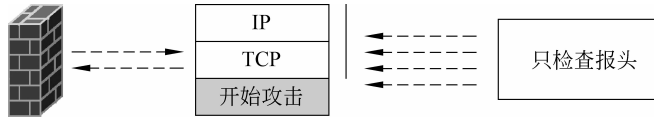

图 3.11　包过滤防火墙工作原理

（2）应用网关防火墙。

应用级网关防火墙技术又称“代理服务器”，主要是针对 OSI 七层参考模型中的应用层而设计的，如检测 HTTP 与 FTP。其对所有应用层的信息数据包进行检查，其决策过程也将放入检查的内容。这样，网络的安全性就大大提高了。然而，应用网关防火墙是通过拆解 Client/Server 模式实现其功能。一组 Client/Server 通信所需的连接是两个：一个是从 Client 到防火墙，另一个是从防火墙到 Server。另外，每个代理的应用进程都不相同，一个后台运行的服务程序也需要单独设置，对每个新的应用，如果要使用该服务必须添加针对此应用的服务程序。所以，应用网关防火墙可伸缩性差，不易操作，是它的缺点之一，如图 3.12 所示，为应用网关防火墙工作原理。

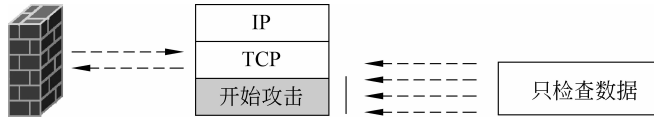

图 3.12　应用网关防火墙工作原理

（3）状态检测防火墙。

状态检测不是单纯的如包过滤防火墙那样只进行 IP 地址和几个孤立信息的检测，而是检测一个完整的“会话状态”。IP 地址可以伪造，但是状态信息却不容易伪造。该防火墙性能优良，兼顾简单包过滤防火墙的优点，又对应用透明。对于安全性，状态监测防火墙也有了大幅度升级。简单包过滤防火墙仅仅考察进出网络的数据包，而不关心数据包状态，会给网络黑客留下可乘之机。而状态检测防火墙会将进出网络的数据当成一个个的事件处理，在防火墙的核心部分建立状态连接表，维护连接。可以说状态检测包过滤防火墙规范了网络层和传输层行为，而应用代理型防火墙则是规范了特定的应用协议上的行为，如图 3.13 所示。

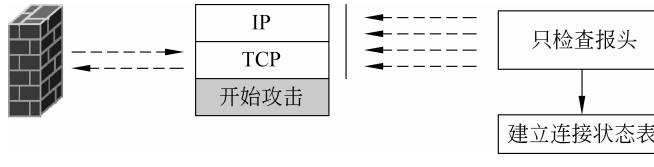

图 3.13　状态检测防火墙工作原理

(4) 复合型防火墙。

它是综合了状态检测与透明代理的新一代防火墙。复合型防火墙进一步基于 ASIC 架构,把防病毒、内容过滤整合到防火墙里,其中还包括 VPN、IDS 功能,多单元融为一体,是一种新突破。常规的防火墙并不能防止隐蔽在网络流量里的攻击,而复合型防火墙在网络界面对应用层进行扫描,把防病毒、内容过滤与防火墙综合实现,这体现了网络与信息安全新的发展趋势和思维。复合型防火墙之所以能够实现实时在网络边缘部署病毒防护、内容过滤等应用层服务措施,是因为它在网络边界实施 OSI 第七层的内容扫描,如图 3.14 所示。

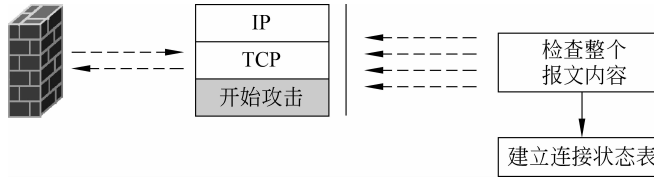

图 3.14 复合型防火墙工作原理

(5) 按区域划分的防火墙。

① 非安全区域(Untrust,外部网络):通常指 Internet 区域,在防火墙划分的 3 个区域中,安全性最低,也就是防火墙的外部接口所连接的网络。

② 安全区域(Trust,内部网络):通常指企业内部区域。防火墙所划分的 3 个区域中其安全性最高的,也是防火墙的内部。一般情况下,该区域可以任意访问比自己安全级别更低的区域。如外部区域和 DMZ 区域。但是不允许低安全区域主动访问该区域。

③ DMZ 区域(Demilitarized Zone,非武装军事区):它是为了解决安装防火墙后外部网络的访问用户不能访问内部网络服务器的问题,而设立的一个非安全系统与安全系统之间的缓冲区。该缓冲区位于企业内部网络和外部网络之间的小网络区域内。在这个小网络区域内可以放置一些必须公开的服务器设施,如企业 Web 服务器、FTP 服务器和论坛等。另一方面,通过这样一个 DMZ 区域,更加有效地保护了内部网络。因为这种网络部署,比起一般的防火墙方案,对来自外网的攻击者来说又多了一道关卡。

当然针对不同的现实情况,对区域的划分也有所不同。例如,有的组织与企业网络只划分为内部与外部两个安全区域,外部区域不允许访问内部区域,而内部区域访问外部区域受安全策略控制。有的组织与企业分为内部、外部、DMZ 三个安全区域,外部区域不允许访问内部区域和 DMZ 区域,只有内部特定用户允许访问 DMZ 的应用服务(例如,财务与 ERP 应用),DMZ 只响应来自内部特定用户的财务和 ERP 应用访问请求。有的组织与企业网络分为内部、外部和 DMZ 三个安全区域,内部和外部只允许访问 DMZ 区域的 WWW 和 E-mail 应用,DMZ 区域只允许主动访问外部的 DNS 和 SMTP 应用。有的组织与企业将网络划分为内部、外部、DMZ 和 DMZ2 四个安全区域,内部和 DMZ2 区域访问内部受安全策略控制,只有内部和 DMZ2 特定用户访问 DMZ 的财务或 ERP 应用,内部区域和 DMZ2 区域之间不允许互相访问。上述例子,只为说明组织与企业对网络的划分需要根据自身的实际情况,可采取的方案非常多且非常灵活。

2）防火墙的缺陷

防火墙是网络安全的基本防御措施之一，应用广泛。但是，防火墙也存在一些自身的不足：

（1）有些网络连接未通过防火墙，防火墙则起不到保护作用。

防火墙一般处于两个网络的边界处，负责检查所有进出的流量数据。但是，不能防止敌对分子通过电磁辐射等方式绕过防火墙入侵我们的指挥自动化网络。

（2）对于有些威胁防火墙无能为力。

防火墙是通过制定安全策略来阻止入侵，策略的制定是建立在已知的安全威胁上。对于未知的威胁，防火墙所制定的策略对其没有约束力。

（3）防火墙不能防止病毒的传播。

防火墙一般对通过的数据包的包头信息，即 IP 地址、端口、服务类型等进行检查，但是对于数据包封装的具体内容不检查，因此就给病毒以可乘之机，将病毒隐藏在数据中进行传输。

（4）不能防止内部用户的入侵。

如果是内部人员非法操作，窃取主机数据，位于网络边界的防火墙也起不到作用。

鉴于以上原因，为保证指挥自动化网络安全，采用防火墙的同时，还需要综合采用入侵检测等技术，实现彼此联动的效果。

3.2 常见网络攻击的原理

3.2.1 跨站脚本攻击

我们在之前的章节中已经大致知道了跨站脚本攻击，但它是如何实现的，具体能做什么，这是我们接下去要探讨的。

1. 跨站脚本攻击基础

1）JavaScript

JavaScript 是用于开发客户端网页的脚本语言，最常见的应用是给静态 HTML 网页添加脚本以实现动态交互性。其最初的设计者是 Netscape 的 Brendan Eich。它不仅是一种动态、弱类型、基于原型的语言，而且具有面向对象的功能。目前多种浏览器，如 Netscape、IE 和 Mozilla 等，都包含了 JavaScript 语言的核心。

程序员通过在 HTML 网页中使用标签＜script＞＜/script＞引入一段 JavaScript 脚本，这段脚本由浏览器执行后，可以在 HTML 网页中生成动态的内容。

例如，有以下脚本：

```
<html>
    <body>
    <script type="text/javascript">
        hello="welcome"
```

```
document.write("<h2>"+hello+"</h2>");
</script>
</body>
</html>
```

经过在线代码编辑器执行后的 HTML 网页如图 3.15 所示。

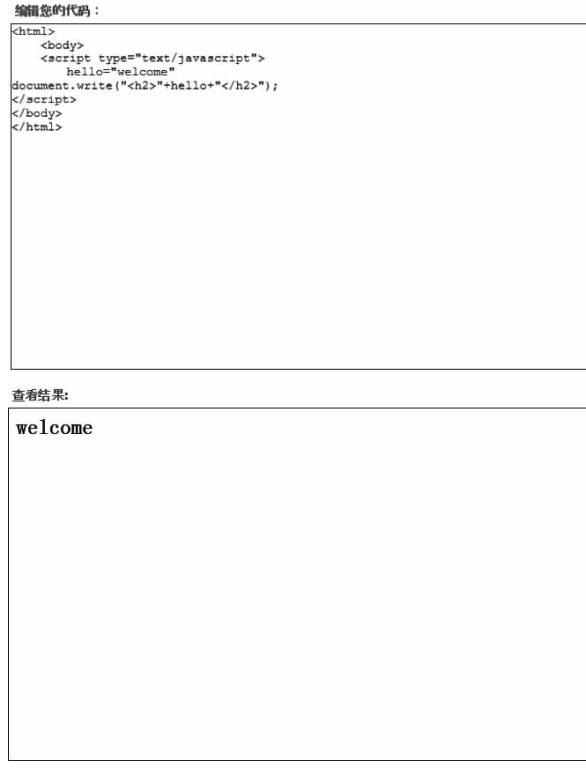

图 3.15 代码执行结果

JavaScript 脚本在发往浏览器之前不需要经过服务器的编译而只是由浏览器解释执行，这样就减少了服务器的负担。但随着 JavaScript 脚本的广泛使用，其跨平台的特点带来了一个备受关注的问题，即程序的安全性问题。JavaScript 不仅可以读取和修改 HTML 网页的内容，还能响应页面事件。如果网页的输入信息包含恶意的 JavaScript 脚本，那么 Web 程序将极易受到 XSS 攻击。

2）DOM

文档对象模型(Document Object Model，DOM)，是 W3C 组织推荐的处理可扩展标志语言的标准编程接口。其可以动态地访问和修改文档的内容和结构而独立于平台和语言。它是表示和处理 HTML 或 XML 文档的常用方法，是 HTML 或 XML 的应用编程接口。DOM 定义了 HTML 或 XML 文档的逻辑结构，并将一个文档映射成一棵相应的 DOM 树，文档的每个元素或属性都是 DOM 树的一个节点。这样，程序员对文档元素或属性的操作可以转换为对 DOM 树节点的操作，即可以遍历、查找、删除和修改 DOM 树的各个结点以遍历文档结构、查找文档元素、删除以及修改文档内容、改变文档的显示

方式等。

例如，有如下 HTML 网页，其对应的 DOM 树如图 3.16 所示。

```
<html>
    <head>
        <title>你好</title>
    </head>
  <body>
        <h1>欢迎您!</h1>
        <a href="linklist.html">点击</a>
    </body>
</html>
```

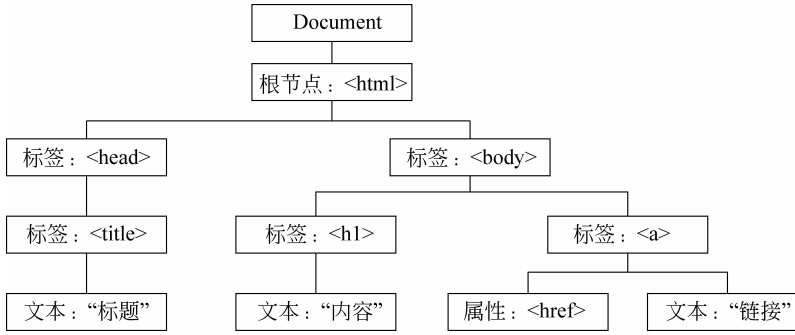

图 3.16　该 HTML 网页对应的 DOM 树

3）浏览器的工作原理

XSS 攻击与浏览器的组成有着一定的关系。目前的浏览器在结构上存在着一些差异，但基本的主要组件如图 3.17 所示。

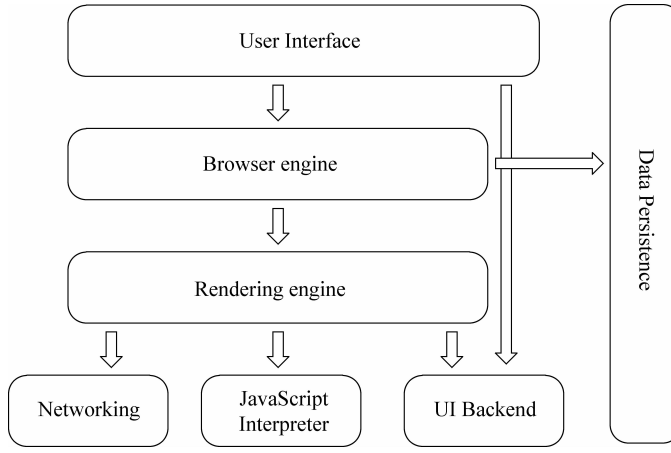

图 3.17　浏览器的主要组件

（1）User Interface、用户界面：浏览器用户直接可以看到的界面，包括书签目录、地址栏、后退/前进按钮等，也就是你所看到的除了用来显示你所请求页面的主窗口之外的

其他部分。

(2) Browser engine、浏览器引擎：用来查询及操作渲染引擎的接口。

(3) Rendering engine、渲染引擎：用来显示请求的内容。例如，如果用户请求内容为 HTML 网页，那么它就负责解析网页中的 HTML 文本及 css 样式，然后显示解析后的结果。

(4) Networking、网络连接：主要完成网络调用的工作。例如，对于 http 请求而言，它可以工作在不同的平台上，并且通过与平台无关的接口进行相关的工作。

(5) UI Backend、UI 后端：用来绘制类似组合选择框及对话框等基本组件，具有不特定于某个平台的通用接口，底层使用操作系统的用户接口。

(6) JavaScript Interpreter、JS 解释器：用来解释执行 JS 代码。

(7) Data Persistence、数据存储：用于保存类似 cookie 的各种数据。

Web 页面的最终显示是由几个解析器共同协作的结果。

2. 跨站脚本攻击原理

之前我们已经初步了解跨站脚本攻击的类型，那到底 XSS 是什么呢？我们来看个简单的例子。

首先，这里有一段很简单的 HTML 代码，包括一段 JavaScript 语句块，该语句块调用了 alert()函数，效果为弹出一个消息框，框内显示“xss”。我们可以将代码复制到记事本中，另存为.html 文件，双击浏览器打开，就可以看到浏览器弹窗，如图 3.18 所示。

```
<html>
    <body>
        <script type="text/javascript">
            alert("xss")
        </script>
    </body>
</html>
```

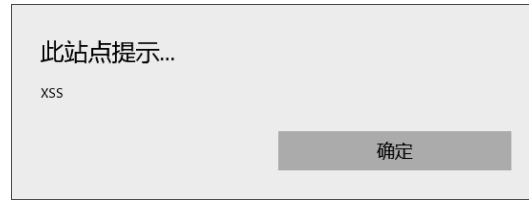

图 3.18 浏览器弹窗

这段代码一定程度上说明了 JavaScript 的作用。当浏览器遇到<script>标签时，它会将内容的控制权转交给脚本引擎处理。JavaScript 强大的功能包括嵌入动态文本于 HTML 页面、对浏览器事件做出响应、读写 HTML 元素、在数据被提交到服务器之前验证数据、控制 cookie，包括创建和修改等。但若是将非法的 JavaScript、VBscript 等脚本注入网页上执行，浏览器只负责解释和执行脚本语言，并不会对代码本身是否对用户有害做出基本的判断，这就使得这种注入方式大有可为。