

6 防火墙基础

2019年5月27日 10:02

[0 下一代防火墙颠覆传统安全理念](#)

[1 防火墙概论](#)

- [· 1.1 防火墙定义](#)
- [· 1.2 防火墙优点](#)
- [· 1.3 防火墙弱点](#)

[2 防火墙的基本结构](#)

- [· 2.1 屏蔽路由器](#)
- [· 2.2 双重宿主主机防火墙](#)
- [· 2.3 屏蔽主机防火墙](#)
- [· 2.4 屏蔽子网防火墙](#)
- [· 2.5 其他防火墙结构](#)

[3 防火墙的模型与分类](#)

[4 攻击方式与防火墙防御](#)

[5 防火墙的发展](#)

[0 下一代防火墙颠覆传统安全理念](#)

- 传统安全设备把企业网流量简单地分为两种——合法和非法。
- 防御手段简单——利用访问控制列表放行合法流量、阻塞非法流量
- 随着网络应用的日益发展，应用的数量、类型和特性都发生了巨大的变化。
- 应用不再只有简单的合法和非法之分，很多对企业非常重要的合法应用同样存在风险，可能会携带病毒和木马。
- 因此，简单的允许或阻止无法解决企业网的安全问题，安全设备必须要把关注的重点转移到如何安全地使用应用上。
- 从企业自身的角度来思考，企业网中都有哪些类型的应用：
 - 公司业务强烈依赖的应用，如OA系统、报销系统
 - 部分员工需要依赖的应用，如销售部门需要使用QQ、微信等即时通讯应用
 - 与工作无关但受员工喜爱的应用，如在线音乐、社交网站等
- 以上应用中有很多是部署在企业外部网络中的，而这些应用都有可能携带威胁。
- 这些应用会传输文件、占用带宽、携带木马、为其他应用打开隧道，部分应用还有逃逸识别的特性。
- 应用的误用可能会造成企业办公效率的降低、数据的泄露和业务的中断。
- 因此，企业需要权衡特定应用对公司业务的价值和风险，一方面要发挥这些应用为公司业务带来的便利，另一方面也要避免应用中可能携带的威胁对公司的影响。
- 为了实现对应用的安全使能，IT管理者首先需要知道企业中运行着哪些应用？
- 决定哪些应用是允许的，哪些应用是禁止的？
- 对合法应用的各项功能进行基于用户的细粒度权限划分和安全扫描，以实现企业网络的安全目标，这成为了对下一代安全产品首要要求。
- 下一代防火墙可以让企业的IT管理者清晰地看到网络中正在运行的应用种类和流量，并且支持对各种应用及其细化功能进行基于用户、时间段的管控，同时集成了入侵扫描和病毒扫描引擎，对应用中可能携带的病毒和木马进行全方位的查杀，配合独有的主动防御技术，确保企业网应用的安全使用。
- 为了实现企业对应用安全的要求，下一代的网络安全设备应该具有以下几种控制手段：
 - 阻塞、允许：阻塞和允许是传统安全设备的基本策略，而基于应用的黑白名单可以让IT管理者将企业需要的应用有条件地放开，将与企业无关的高风险应用进行彻底阻塞(如P2P、炒股、网络视频)。黑白名单的限制方式在下一代安全架构中仍然有它的作用，但除了阻塞以外，更重要的是如何安全地使用应用。
 - 多种条件的限制：新的安全架构需要基于各种条件对应用的使用做限制，如基于用户、用户群组、vlan、终端类型、时间段以及应用的细化功能等条件。企业可以严格地限制某些用户在某些时段可以使用某个应用的某些功能，通过限制应用使用的形式来最大程度地减少风险。
 - 安全扫描：对应用做安全扫描可以从另一个角度来减少威胁，通过对应用进行入侵扫描、病毒扫描和URL过滤来发现应用中所携带的风险。

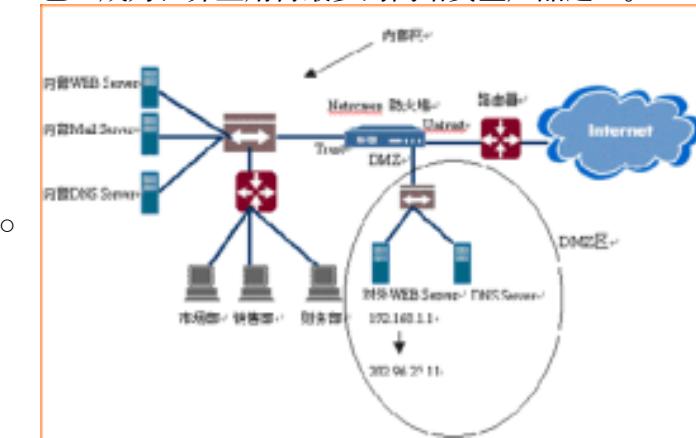
- 威胁的主动防御：由于威胁不断变化、善于隐藏，部分威胁可能会逃脱安全扫描，这时就需要有不基于特征识别技术的主动防御功能来发现未知的威胁。主动防御技术通过对用户的应用行为分析、安全基线对比分析、集成关联分析来发现潜在的僵尸主机和攻击行为，保障企业网的应用安全。
- 流量整形：基于应用的流量整形通过流量保障和流量控制技术来防止无关应用对企业关键应用的干扰，提升带宽的价值。

1 防火墙概论

- 网络安全—网络上的信息安全：机密性、完整性、可用性、真实性、实用性和占有性。
- [1.1 防火墙定义](#)
- [1.2 防火墙优点](#)
- [1.3 防火墙弱点](#)

1.1 防火墙定义

- 防火墙的由来
 - 防火墙的本义原是指古代人们房屋之间修建的那道墙，这道墙可以防止火灾发生的时候蔓延到别的房屋。
- 防火墙定义
 - 防火墙是指设置在不同网络（如可信任的内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。
 - 它是不同网络或网络安全域之间信息的唯一出入口，能根据安全策略控制（允许、拒绝、监测）出入网络的信息流。
 - 本身具有较强的抗攻击能力。
 - 提供信息安全服务，实现网络和信息安全的基础设施。
- 防火墙的作用
 - 防火墙是一种非常有效的网络安全模型
 - 可以隔离风险区域与安全区域（局域网）的连接
 - 不妨碍人们对风险区域的访问
 - 防火墙监控进出网络的通信量，仅让安全、核准了的信息进入
 - 抵制对安全区域构成威胁的数据
 - 防火墙的作用就是防止不希望的、未授权的信息进出被保护的网络。因此，防火墙是控制对网络系统访问的非常流行的方法。作为第一道安全防线，防火墙已经成为世界上用得最多的网络安全产品之一。



- 在逻辑上，防火墙为
 - 分离器
 - 限制器
 - 分析器
 - 它有效地监控了内部网和Internet之间的任何活动，保证了内部网络的安全。
 - 从具体实现上来看，防火墙是一个独立的进程或一组紧密联系的进程，运行于路由器或服务器上，控制经过它们的网络应用服务及传输的数据。
- 防火墙的三大要素
 - 安全、管理、速度

1.2 防火墙优点

- 防火墙能够提高主机整体的安全性，具有以下几方面的优点：
- 防火墙是网络安全的屏障

- 一个防火墙（作为阻塞点、控制点）能极大地提高内部网络的安全性，并过滤不安全的服务而降低风险。
- 控制对主机系统的访问
- 监控和审计网络访问
 - 如果所有的访问都经过防火墙，那么，防火墙就能记录下这些访问并作出日志记录，同时也能提供网络使用情况的统计数据。
- 防止内部信息的外泄
 - 利用防火墙对内部网络的划分，可实现内部网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。
- 部署网络地址翻译(NAT)机制
 - 可以缓解地址空间短缺问题，隐藏内部网络结构。

1.3 防火墙弱点

- 防火墙不能防范来自内部网络的攻击

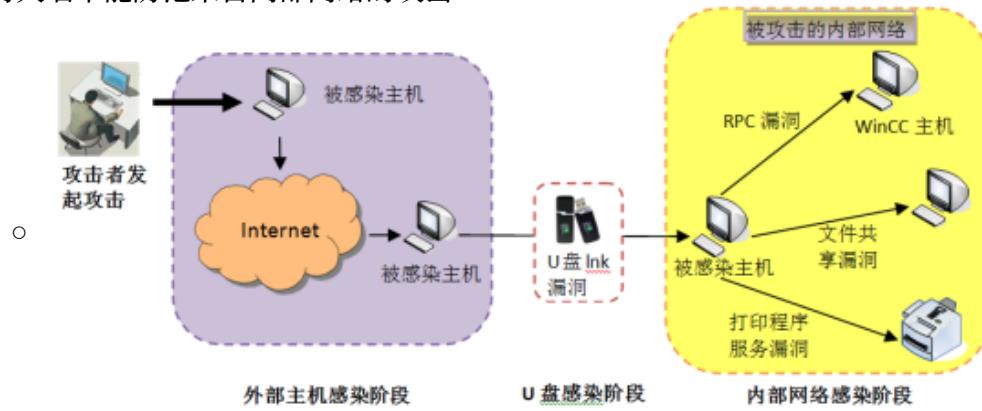
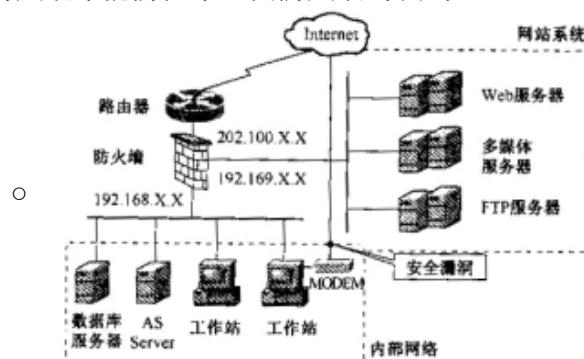


图 2：“震网”病毒的传播感染过程

- 防火墙不能防范不经由防火墙的攻击



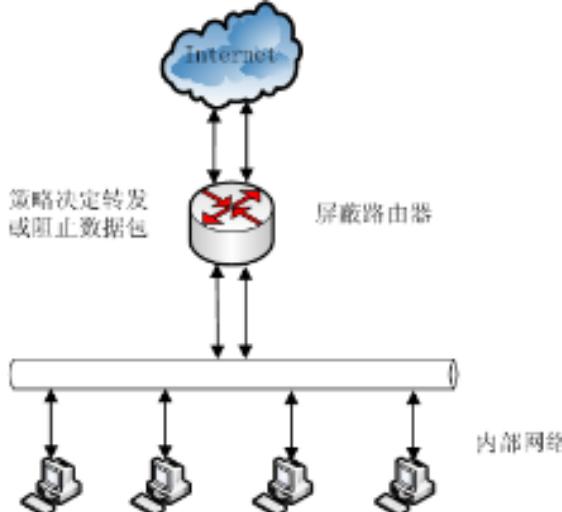
- 防火墙不能防范感染病毒的软件或文件的传输
- 防火墙不能防范数据驱动式攻击
 - 当有些表面看来无害的数据邮寄或复制到内部网的主机上并被执行时，可能会发生数据驱动式的攻击。
- 防火墙不能防范利用标准网络协议中的缺陷进行的攻击
 - 一旦防火墙准许某些标准网络协议，就不能防止利用该协议中的缺陷进行的攻击。
- 防火墙不能防范利用服务器漏洞进行的攻击
 - 防火墙不能防止黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击。
- 防火墙不能防范新的网络安全问题
 - 防火墙是一种被动式的防护手段，它只能对现在已知的网络威胁起作用。随着网络攻击手段的不断更新和一些新的网络应用的出现，不可能依靠一次性的防火墙设置来解决永远的网络安全问题。
- 防火墙可能限制有用的网络服务
 - 为提高被保护网络的安全性，防火墙可能限制或关闭了一些有用但存在安全缺陷的网络服务。

2 防火墙的基本结构

- [2.1 屏蔽路由器](#)
- [2.2 双重宿主主机防火墙](#)
- [2.3 屏蔽主机防火墙](#)
- [2.4 屏蔽子网防火墙](#)
- [2.5 其他防火墙结构](#)

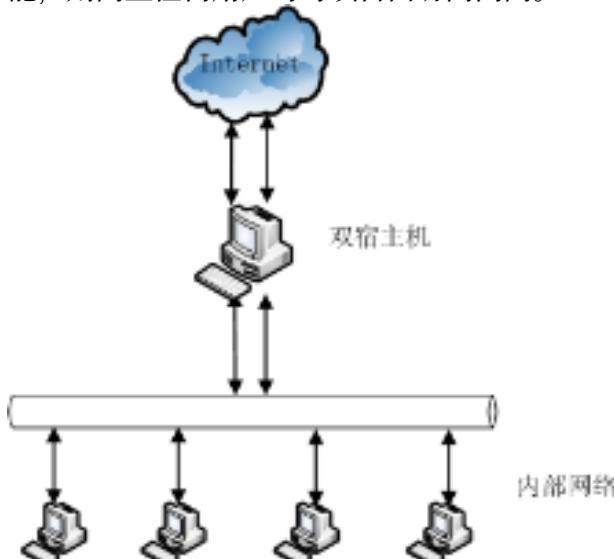
2.1 屏蔽路由器

- 屏蔽路由器是防火墙最基本的构件。
 - 屏蔽路由器作为内外连接的惟一通道，要求所有的报文都必须在此通过检查。
 - 路由器上可以安装基于IP层的报文过滤软件，实现报文过滤功能。
 - 许多路由器本身带有报文过滤配置选项，但一般比较简单。
 - 单纯由屏蔽路由器构成的防火墙的危险区域包括路由器本身及路由器允许访问的主机。
 - 屏蔽路由器的缺点是路由器一旦被控制后很难发现，而且不能识别不同的用户。



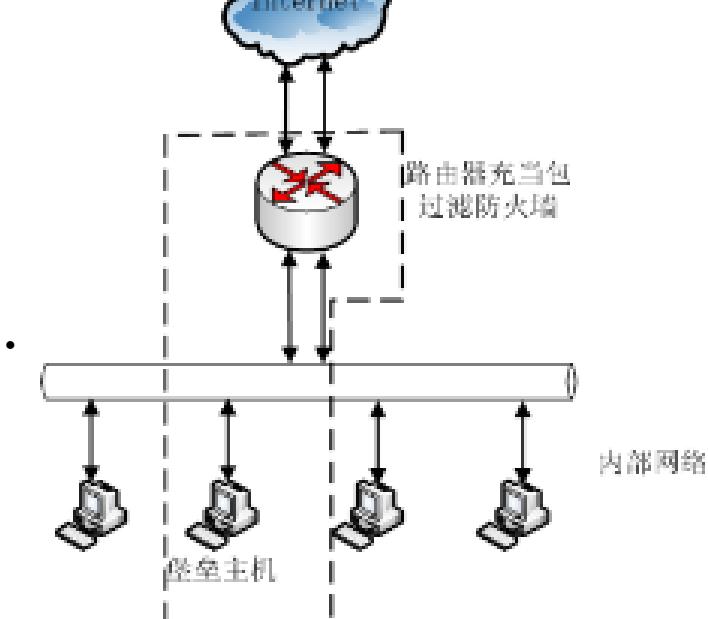
2.2 双重宿主主机防火墙

- 用一台装有两块网卡的堡垒主机做防火墙。
 - 两块网卡分别与内部网和外部网相连。
 - 堡垒主机上运行着防火墙软件，可以转发应用程序，提供服务等。
 - 内部网和外部网之间的直接通信被完全阻止。
- 双宿主机防火墙优于屏蔽路由器的方面：
 - 堡垒主机的系统软件可用于维护系统日志、硬件复制日志或远程日志。
 - 日志对于日后的检查很有用，但不能帮助网络管理者确认内网中哪些主机可能已被黑客人侵。
- 双宿主机防火墙的一个致命弱点：一旦入侵者侵入堡垒主机并使其只具有路由功能，则网上任何用户均可以自由访问内网。



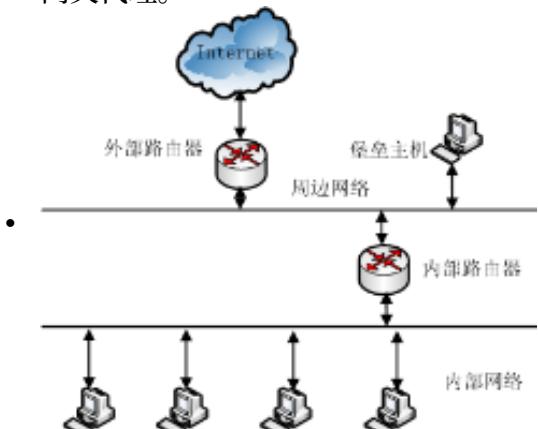
2.3 屏蔽主机防火墙

- 屏蔽主机防火墙易于实现也很安全，因此应用广泛。
 - 一个分组过滤路由器连接外部网络
 - 一个堡垒主机安装在内部网络上
 - 通常在路由器上设立过滤规则
 - 堡垒主机成为从外部网络惟一可直接到达的主机
 - 确保内部网络不受未被授权的外部用户的攻击



2.4 屏蔽子网防火墙

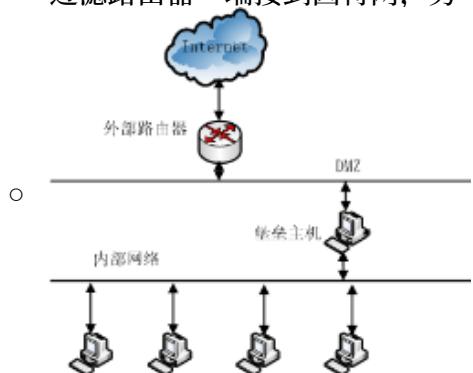
- 在内部网络和外部网络之间建立一个被隔离的子网（周边网络），用两台分组过滤路由器将这一子网分别与内部网络和外部网络分开。
- 在很多实现中，两个分组过滤路由器放在子网的两端，在子网内构成一个非军事区（DMZ）。
- 有的屏蔽子网中还设有一个堡垒主机作为唯一可访问点，支持终端交互或作为应用网关代理。



- 屏蔽子网体系结构防火墙的危险区域包括堡垒主机、子网主机及所有连接内网、外网和屏蔽子网的路由器。
- 如果攻击者试图完全破坏防火墙，他必须重新配置连接3个网的路由器，既不切断连接又不要把自己锁在外面，同时又不使自己被发现，这样的攻击还是可以完成的。
- 若禁止网络访问路由器或只允许内网中的某些主机访问，则攻击会变得很困难。在这种情况下，攻击者得先侵入堡垒主机，然后进入内网主机，再返回来破坏屏蔽路由器，而且整个过程中不能引发警报。

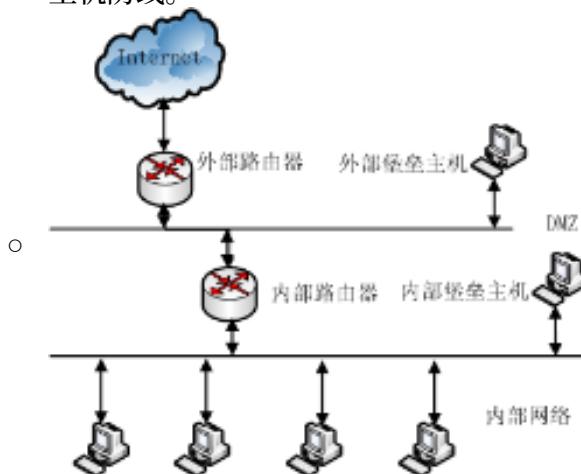
2.5 其他防火墙结构

- 一个堡垒主机和一个非军事区
 - 堡垒主机一个网络接口接到非军事区（DMZ）另一个网络接口接到内部网络，过滤路由器一端接到因特网，另一端接到非军事区。



- 配置过滤路由器，只有过滤路由器规则允许的网络流量才能转发给堡垒主机。
- 入侵者必须首先穿过过滤路由器，然后还必须穿过或者控制堡垒主机。

- 在非军事区内没有主机。因为只有两个网络接口，所以它可以用专用的点对点连接代替，这就使得通过协议分析来获取这个连接变得更加困难。
- 在这种结构中，堡垒主机使用双宿主机，提高了系统的安全性，可以防止入侵者绕过堡垒主机，入侵到内部网络中。
- 两个堡垒主机和两个非军事区
 - 这种结构使用两台双宿堡垒主机，有两个非军事区，并在网络中分成了4个部分：内部网络、外部网络、内部非军事区和外部非军事区。
 - 过滤路由器和外部堡垒主机是外部非军事区上仅有的两个网络接口。
 - 内部非军事区受到过滤路由器和外部堡垒主机的保护，具有一定的安全性，可以把一些相对而言不是很机密的服务器放在这个网络上，并把敏感的主机隐藏在内部网络中。
- 两个堡垒主机和一个非军事区
 - 使用两个具有单一网络接口的堡垒主机，加上一个内部过滤路由器作为阻塞器。
 - 内部过滤路由器位于DMZ和内部网络之间。
 - 该结构中，必须保证堡垒主机不被越过，还应保证两个过滤路由器使用静态路由方式。
 - 这种结构要比标准的屏蔽主机的结构更为安全。因为内部网络受到双重保护，入侵者即使控制了第一个堡垒主机也不能为所欲为，还需设法攻破第二道堡垒主机防线。



3 防火墙的模型与分类

国际标准化组织ISO的计算机专业委员会 (ISO/IEC JTC1 /SC21)

制定的OSI/RM网络安全体系结构

安全服务 网络层次	对等实体鉴别	访问控制	连接保密	选择字段保密	报文流安全	数据源鉴别	数据的完整性	禁止否认服务
应用层	Y	Y	Y	Y	Y	Y	Y	Y
表示层			Y	Y			Y	
会话层								
传输层	Y	Y	Y				Y	
网络层	Y	Y	Y		Y		Y	
数据链路层		Y	Y					
物理层		Y	Y		Y			

防火墙的模型

- 防火墙目的在于实现安全访问控制，因此按照OSI/RM模型防火墙可以在OSI/RM七层中的五层设置。



数据链路层	网桥级
物理层	中继器级



防火墙的分类

- 包过滤防火墙
 - 第一代也是最基本形式的防火墙。根据所建立的一套规则，检查每一个通过的网络包，或者丢弃，或者放行，这称为包过滤防火墙。目的是放行正常的数据包，截住有危害的数据包
 - 例：
 - 规则1：阻断FTP、TELNET、SMTP、POP3等连接；
 - 规则2：允许HTTP连接；
 - 查看网络包的目的地址端口号，目的端口为21、23、25、110的丢弃，目的端口为80的放行。
- 状态/动态检测防火墙
 - 包过滤防火墙见到的每一个网络包都是孤立存在的，包中没有包含任何描述它在信息流中的位置的信息，该包被认为是无状态的，包中没有防火墙所关心的历史信息或未来状态。
 - 一个有状态包检查防火墙跟踪的不仅是包中包含的信息。为了跟踪包的状态，防火墙还记录有用的信息以帮助识别包，例如已有的网络连接、数据的传出请求等。
 - 状态/动态检测防火墙是在使用基本包过滤防火墙的通信上，跟踪通过防火墙的网络连接和包，以使用一组附加的标准，确定允许或拒绝通信。
 - 例1：对于传入的TCP包，只有它是在响应一个已建立的连接时，才会被允许通过。
 - 例2：对于传入的UDP包，若它所使用的地址和UDP包携带的协议与传出的连接请求相匹配，则该包就被允许通过。
- 应用程序代理防火墙
 - 应用程序代理防火墙实际上并不允许它连接的网络之间直接通信。相反，它接受来自内部网络特定用户应用程序的通信，然后建立与公共网络服务器单独的连接。网络内部的用户不直接与外部服务器通信，所以外部服务器不能直接访问内部网的任何一部分。同时，如果不为特定的应用程序安装代理程序，则这种服务是不会被支持的，不能建立任何连接。这种建立方式拒绝任何没有明确配置的连接，从而提供了额外的安全性和控制性。
 - 例：一个用户的Web浏览器可能在80端口或8080端口连接到了内部网络的HTTP代理防火墙。防火墙会接受这个连接请求并把它转到所请求的Web服务器。这种连接和转移对该用户是透明的，因为它完全是由代理防火墙自动处理的。
 - 代理防火墙通常支持的一些常见的应用程序有：HTTP, HTTPS/SSI, SMTP, POP3, IMAP, NNTP, TELNET, FTP, IRC。
- 个人防火墙
 - 个人防火墙是一种能够保护个人计算机系统安全的软件，一般是应用程序级的。它可以直接在用户的计算机上运行，使用与状态/动态检测防火墙相同的方式保护一台计算机免受攻击。
 - 通常，个人防火墙安装在计算机网络接口的较低级别上，使其可以监视传入传出网卡的所有网络通信。
 - 例：用户安装了一台个人Web服务器，个人防火墙可能将第一个传入的Web连接加上标志，并询问用户是否允许它通过，用户可能允许所有的Web连接，也可能只允许来自某些特定IP地址范围的连接等，个人防火墙会把这条规则应用于所有传入的Web连接。

4 攻击方式与防火墙防御

踩点->扫描->攻击

- 踩点信息收集
 - SNMP协议
 - 简单网络管理协议（SNMP）允许你从网络主机上查询相关的数据。例如，你可以收集TCP/IP方面的信息，还有在路由器、工作站和其它网络组件上运行的服务情况。SNMP由网络管理系统（NMS）和代理Agent组成。

成。NMS通常安装在一台工作站上，再将代理安装在任何需要接受管理和配置的主机上。

○ Traceroute程序

- 用于路由追踪，如判断从你的主机到目标主机经过哪些路由器、跳计数、响应时间如何、是否有路由器当掉等。大多数操作系统，包括UNIX, Novell和Windows NT，若配置了TCP/IP协议的话都会有自己版本的traceroute程

○ Whois协议

- [类似于finger] 是一种internet的目录服务，whois提供了在Internet上一台主机或某个域的所有者的信息，如管理员的姓名、通信地址、电话号码和Email地址等信息，这些信息是在官方网站whoisserver上注册的，如保存在InterNIC的数据库内。Whois命令通常是安全审计人员了解网络情况的开始。一旦你得到了Whois记录，从查询的结果还可得知primary和secondary域名服务器的信息。

○ DNS服务器

○ Finger协议

- 服务使你可以获取远程服务器上的用户信息。使用Finger，你可以得到：用户名，服务器名，E-mail账号，用户当前是否在线，用户登录时间等。
- 序。

○ Ping实用程序

- 一个公司的Web服务器可帮助你获得该公司所使用的IP地址范围。一旦你得知了HTTP服务器的IP地址，你可以使用Ping扫描工具Ping该子网的所有IP地址，这可以帮助你得到该网络的地址图。

· 扫描漏洞侦测

○ 使用自制工具

○ 使用专用工具SATAN等

- SATAN是为UNIX设计的，它主要是用C和Perl语言编写的。
- SATAN用于扫描远程主机的许多已知的漏洞，可写的FTP目录，Sendmail

· 攻击

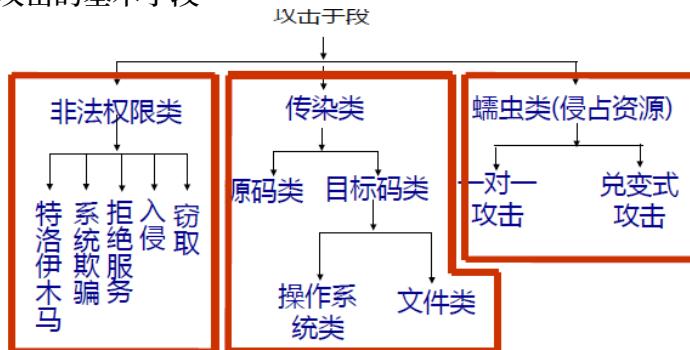
○ 建立帐户

○ 安装远程控制器

○ 发现信任关系全面攻击

○ 获取特权

网络攻击的基本手段



特洛伊木马

- 一种未经授权的程序，或在合法程序中有一段未经授权的程序代码，或在合法程序中包含有一段用户不了解的程序功能。上述程序对用户来说具有恶意的行为。
- 陷阱入口类
- 功能欺骗类
- 信息窃取类
- 逻辑炸弹类

逻辑炸弹

- 逻辑炸弹是程序中的一部分，满足一定条件时激活某种特定的程序，并产生系统自毁，并附带破坏。

功能欺骗类

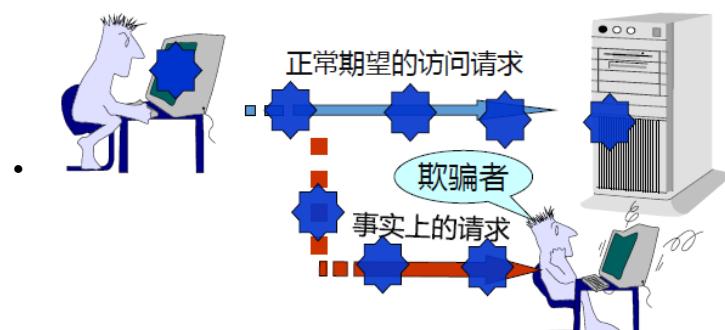
- ActiveX的强大功能：下载的结果可能是

- 格式化你的硬盘
- 关闭你的机器
- 预防方法：数字签名
 - 由签名者保证所提供的控件不具有安全方面的破坏性
 - 由IE负责警告用户是否要下载一个无数字签名的控件

系统欺骗

- 系统欺骗是利用程序所提供的合法功能来达到破坏系统的目的。
 - 外部欺骗类
 - 本机欺骗类

外部欺骗类



拒绝服务

- 以利用计算机协议处理的漏洞来攻击网上计算机使之死机为目的的网络程序。

入侵

- 以利用计算机协议处理的漏洞来非法获得本机ROOT权限或通过特殊方法来分析他人（包括系统员）的口令以达到非法操作目的的操作过程。

诱骗式入侵方法

- 很多系统命令(如EJECT)是具有ROOT权限的，即在ROOT权限下来执行。利用操作系统的漏洞，通过导致这类操作出现异常终止，便获得ROOT权限(此时并不知道系统口令)。

缓冲区溢出的入侵方法



5 防火墙的发展

- 第一代防火墙
 - 包过滤路由器或屏蔽路由器，即通过检查经过路由器的数据包源地址、目的地址、TCP端口号、UDP端口号等参数来决定是否允许该数据包通过，并对其进行路由选择转发。例如Cisco路由器提供的防火墙功能是接入控制表。
 - 第一代防火墙只有分组过滤的功能，且与路由器是一体的。这种防火墙很难抵御地址欺骗等攻击，审计功能差。
- 第二代防火墙
 - 代理服务器，可提供应用服务级的控制，起到外部网络向被保护的内部网申请服务时中间转接作用。
 - 内部网只接受代理服务器提出的的服务请求，拒绝外部网络其他节点的直接请求。
 - 代理服务器可以根据服务类型对服务的操作内容等进行控制，防止对内部网络的直接攻击。
 - 对于每一种网络应用服务都必须为其设计一个代理软件模块来进行安全控制。
 - 每一种网络应用服务的安全问题各不相同，分析困难，因此实现也困难，同时代理的时间延迟一般比较大。

- 第三代防火墙
 - 第三代防火墙是建立在通用操作系统上的商用防火墙产品。特点：
 - 具有分组过滤或者借用路由器的分组过滤功能；
 - 装有专用的代理系统，监控所有协议的数据和指令；
 - 保护用户编程空间和用户可配置内核参数的设置；
 - 安全性和速度大为提高。
 - 第三代防火墙有以纯软件实现的，也有以硬件方式实现的，其安全性依赖于防火墙厂商和操作系统厂商两方面。
- 第四代防火墙
 - 第四代防火墙是具有安全操作系统的防火墙。
 - 安全操作系统有两种实现方法：
 - 一种是通过许可证方式向操作系统提供商获得操作系统的源码，然后对其进行改进，去掉一些不必要的系统特性和网络服务，加上内核特性，强化安全保护，实现安全内核，并通过固化操作系统内核来提高可靠性。
 - 另外一种是编制一个专用的防火墙操作系统，保密系统内核细节，增强系统安全性。同时，各种新的信息安全技术被广泛应用在防火墙系统中，如网络环境下的用户身份鉴别技术等。
 - 此外，新一代防火墙技术采用了一些动态网络安全技术，如网络安全性分析、网络信息安全管理等。