典型的攻击方式

王世宏

引言

- 为了进一步讨论平安，你必须理解你有可能遭遇到的攻击的类型，为了进一步防御黑客，你还要了解黑客所采用的技术、工具及程序，所有类型的攻击经常被合在一起使用，一般情况下，攻击被结合起来产生一个具体的后果，例如：一个用户有可能将特洛伊木马程序放置在WEB效劳器，因为效劳器一执行这个程序，黑客将能在效劳器上实施拒绝效劳攻击，导致机器重启，一旦机器重启，它将载入木马程序。

攻击的分类

- 攻击可以分为两大类：意外威胁和成心威胁。
- 意外威胁：　由系统管理员和无知的用户因为没有预先思考或方案而引起的。
- 成心威胁：　是有企图的行为的结果，它是执行方案好的活动。

哄骗

- 哄骗和伪装都是偷窃身份的形式。通常CIW专家考试平安讨论的哄骗是指IP哄骗(ip spoofing)，它是一合机器模仿另一台机器的能力正如你所猜测的那样，IP哄骗是利用INTERNET的开放式网络设计和传统的UNIX系统之间建立的信任关系。记住，除非采取防范措施， 否那么所有使用IP的效劳器，都认定包是由合法的数据源产生的、但是．存在各种的应用程序，可以让windows和Linux系统伪造数据源和目标IP地址 哄骗使得明确地确定是谁发送了IP包给网络主机变得非常困难。

- 黑客使用IP哄骗的好处是可以生成用于发行被伪装的IP包的程序。黑客使用这些程序，并组合建立TCP连接的程序或进程，让 一个系统看上去像另一个系统。然后黑客就可以随意地攻击系统了，因为很难跟踪攻击来源。

IP哄骗和UNIX的R系列命令

R系列命令（rlogin，rexec等）是被设计成使登录远程系统更方便的。多数系统管理员努力减轻他们管理工作的负担，类似rlogin这样的应用已经成为流行的管理工具。rlogin是像Telnet一样的应用程序，允许用户在不需要提供口令的情况下登录到一个远程系统。为了使用rlogin，系统管理员必须创建被称为rhosts和rlogin的条目。

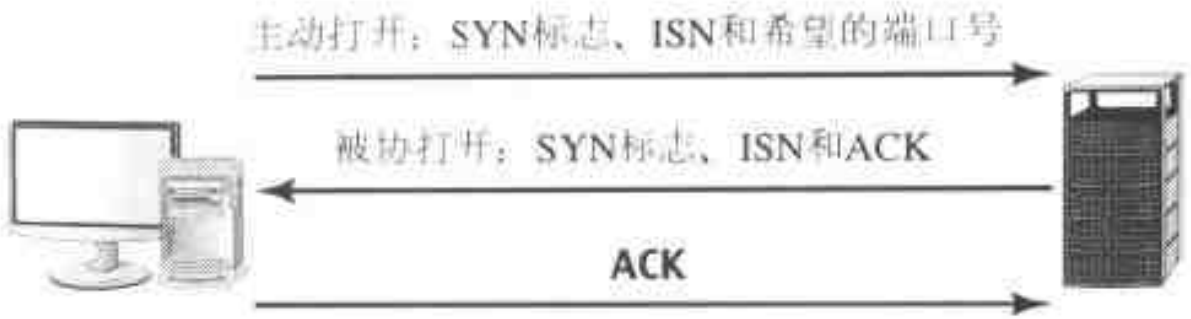
许多UNIX系统都包括rhosts和rlogin条目，用来在主机之间通过不可信任的网络（如Internet）上建立可信认的连接。一般惯例认为：rlogin的身份验证提供了足够的安全性，因为它结合了“你的位置”这种基于地址的验证与UNIX系统自身的验证方案。但是，rlogin“你的位置”的验证方式太依赖于：IP地址不可能被伪装的这种最初的假设。使用IP哄骗可能会使rlogin验证失效，因此，不应再使用r系列命令。

中间人攻击

- man-in-the-middle attack:是黑客企图对一个网络的主机发送到另一台主机的包进灯操作的攻击。这类攻击相当普遍，因为它包括了当网络数据通过网络传输的所有可能发生的攻击所有这一类攻击的共同八是黑客必须在物理位置上位于两个被攻击的合法主机之河 以下是中间人攻击类型中最常见的几种。
- 包捕获 这类攻击涉及到为获得用户名称和口令信息探测包的攻击方法。任何用明文发送的信息(如电子邮件内容)都可能被捕获。在LAN与INTERNET上此攻击很普遍。但交换机的出现降低了这种攻击的可能性。但像ettercap这类使用ARP抑制策略的应用程序能够在交换网络进行探测。
- 包修改 是使用各仲应用程序编辑被捕获的包。如NetDude这类应用程序就能对包做“烹饪”然后再传输
- 包植入 即包修改之后，把改后的包发给受害效劳器以获得黑客的目的，如反复发送一个改后的包。获得被害效劳器的访问权。
- 连接劫持 这种类型的攻击包括中途截取和接管正在处理中的连接。恶意的用户可以实际监控一个Telnet或IRc聊大会话，然后植入任何他想要的文本；为捕获网络传输的内容。 也可以让一台主机扮核另—台主机的角色。

连接劫持与其他攻击策略的组台

- 在劫持一个连接时，必然涉及三种独立的攻击方法。首先以劫持攻击开始，然后执行拒绝效劳攻击和哄骗IP地址。第一阶段的攻击即劫持发生在以下三次握手的第一次之后。〔通常强加密是防止数据劫持的最好手段〕



例　子

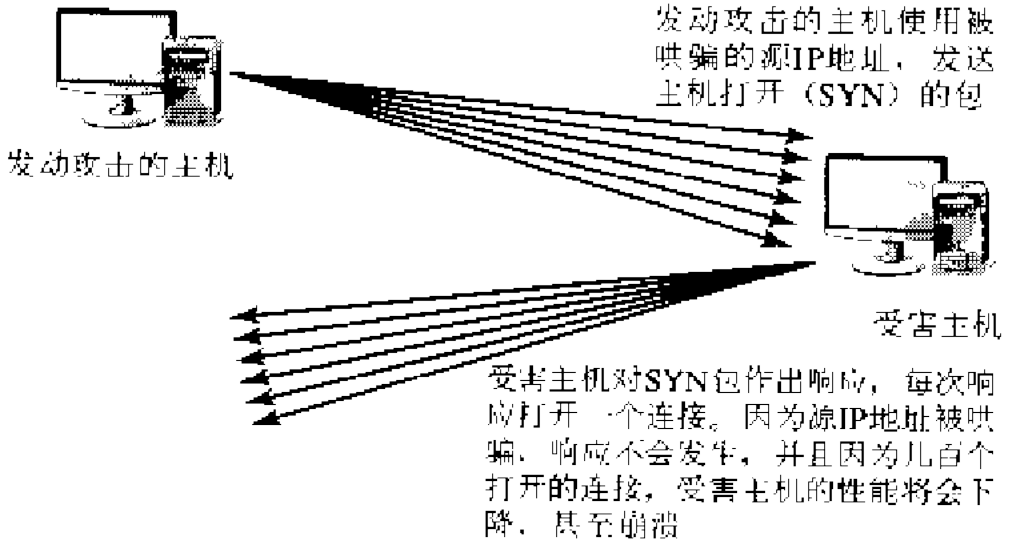
- 假设合三台主机：主机A、主机B和主机C。当主机A和主机B开始通信时，攻击者主机c找到了一个方法假用主机B的身份。一旦这种情况发生，主机c就扮演主机B并开始接收和传输从主机A发来的数据。在成功的攻击中，合法的主机认为它们彼此间在相互直接通信，实际情况是黑客截获了所有的传输并路由到每个主机。这样，黑客就可以对数据做任何他想做的操作。想劫持连接的攻击者必须对他正扮演的主机执行拒绝效劳攻击。例如，如果攻击者假们主机B的身份，那么攻击者必须让这台主机从网络上消失。
- 黑客进行IP哄骗攻击需要几种程序，其中有：
- ·包探测器
- ·中断TCP连接或崩溃整个效劳器的应用程序
- ·产生TcP连接和哄骗IP包的应用程序
- 有些应用程序如：hunt可以做到所有这三项功能

拒绝效劳攻击

- 在一个拒绝效劳攻击中，一个黑客阻止合法用户获得效劳。这些效劳可以是网络连接，或者任何一个系统提供的效劳。
- DOS攻击在WINDOWS 效劳器上非常流行，击败一个UNIX系统的平安防范是容易的，所有的用户都是善意和有能力的，在拒绝攻击效劳有两种目的：
- ● 摧毁效劳器，使它对于任何人都不能效劳。
- ● 获取黑客止在摧毁的任何一个效劳器的身份，黑客的策略，例如欺骗和 “man-in-the-middle"攻击，必须使得他们正在欺骗的主机失效，拒绝效劳攻击并不能使黑客拒绝个人的身份，但是可以使得这个合法的个人不能被响应。

DOS攻击常见类型

- SYN溢出(SYN flood)是渗透攻击INTERNET效劳器中最常用的—种。它用一种不同于正常行为的方式建立一个TcP握手。黑客能够建立多个TcP半边接。

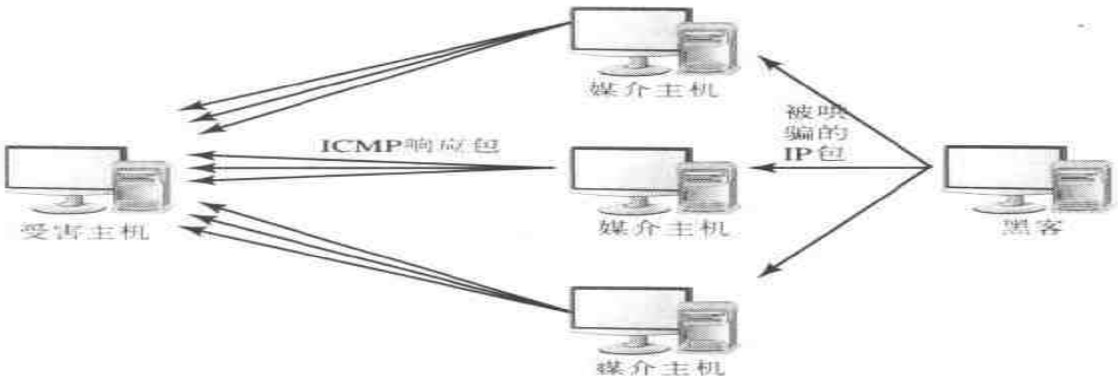


- 以上图示中说明的在DOS攻击中的IP哄骗使攻击更有力量，因为攻击者不用再去回应效劳器发回的二次握手信息。而且这样的攻击很难预防，因为防火墙默认不会对SYN溢出做配置。

说明：包探测器和netstat命令也许是最好的两种工具，用于试图识别和辨认SYN溢出和其他跨网络的攻击时。包探测器准许浏览任何包（ICMP、IP、TCP和UDP等）的细节信息。Netstat命令用于揭示系统中活动的TCP和UDP连接。

DOS攻击类型

- Smurf攻击和Fraggle攻击 Smurf 涉及操纵网间控制报文协议(ICMP)，此协以由Ping程序调用，如图黑客先创立一个包，它看起来好似来源于即将成为受害者的主机。然后，黑客把这个包发送给一个不知情的第三方，它将成为媒介主机。这台主机很自然地对它门己的IcMP回应包做山反响。 因此，在smurf攻击中成为了不知情的同谋者。



- 如果黑客发送了足够的ICMP包，回应将淹没被害人的主机。如果你就是那个不走运的被害者，在你的效劳崩溃后，黑客将借你的IP去哄骗别人。以躲避攻击责任。你就是替罪羊。

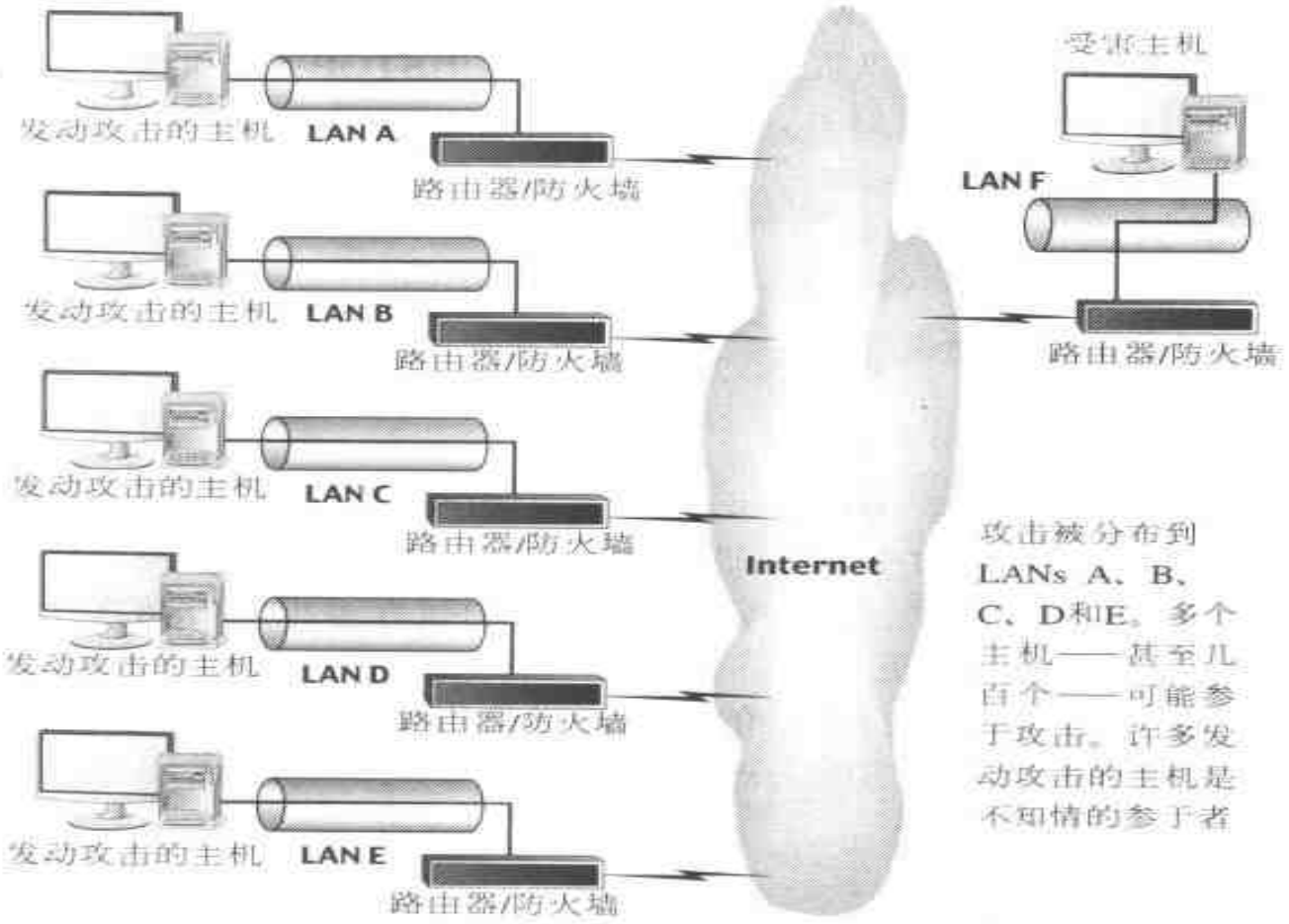
DOS常见攻击

- Frggle攻击与smurf攻击类似，只不过是使用UDP.虽然端口7(回应瑞口)是最典型的，但绝大多数发动此攻击的程序准许你可以指定想要的端口。保护系统免受smurf和Frggle攻击的最好的方法是在防火墙过滤掉IcMP包或不允泞在效劳器上使用PING但是，在发生问题时，这些措施会使连通性的测试变得相当困难。
- 泪珠 / 泪珠2 泪珠(Teardorp)系列的攻击是利用没有完全重编译的代码覆盖UDP包的方法。如果windows与linux没有更新补丁，刚会蓝屏。现在一般都有打过补丁后，该攻击主要用来消耗被攻击者的带宽和处理器时间。泪珠攻击被称为Boink,泪珠2攻击被称为Bonk
- 死亡之PING与PING欺骗 攻击者会造出多个PING包，到对端结合成一个超过65535字节的包，让对方缓冲区溢出死机。或者LINUX系统支持的PING –f 会短时间发送大量包来阻瑟通信。

分布式拒绝效劳(DDoS)攻击

(distributed denial-of-service(DDoS)attack)是指几个远程系统在一起工作并产生网络传输，意在崩溃一个远程主机的方法。这些攻击一股把i大的传输量集中于一台主机，因为负载过重而引起这台主机崩溃。另一种例于是，DDos攻击集中在“网络管道”(例如TI或T3线路)，并用欺骗性的传输填满它。系统也许还能够运行，但没有人能够访问它们的效劳了。DDos传输虽然也可以使用uDP和TcP，们一船包含虚假的ICMP包。如以下图所示，多台主机被联合起来产生一个数据流用于使受害主机瘫痪。

了解DDOS攻击图示


受害主机
LAN F
路由器/防火墙
发动攻击的主机
LAN A
路由器/防火墙
发动攻击的主机
LAN B
路由器/防火墙
发动攻击的主机
LAN C
路由器/防火墙
Internet
发动攻击的主机
LAN D
路由器/防火墙
发动攻击的主机
LAN E
路由器/防火墙
攻击被分布到LANs A、B、C、D和E。多个主机——甚至几百个——可能参于攻击。许多发动攻击的主机是不知情的参于者

从DoS和DDoS攻击中恢复

- 如果DoS和Ddos攻击引起系统崩溃，那么只需要一次简单的重新启动就能恢复。但是，DDos攻击一般要求重新调用交换和路电程序，才能结束这钟可恶的传输：在windows2000系统中你可以檄活IPsec策略，它准许你限制或禁止来自于某些主机的传输，在LINUX可能使用iptables来阻断DDOS
- 防止DOS与DDOS的方法在于1、升级操作系统2、密切关注企业定制的相关软件带码有没有异样3、不要在生产环境中用试用版软件。

内部攻击

- 往往来自LAN内部的攻击会被忽略掉。但这也是常见攻击的一种手段，如：内部员工得知了效劳器帐号，取得效劳器控制权。另外内部攻击还常见于物理攻击。

前门攻击和暴力攻击

- 前门和暴力攻击它们都试图击败认证过程。在一个前门攻击中一个黑客伪装成一个合法的用户进入系统，因为一个黑客拥有一个合法用户的所有信息，他(她)就能够很简单地从系统的“前门”正当地进入。
- 黑客使用IP哄骗的好处是可以生成用于发行被伪装的IP包的程序。黑客使用这些程序，并组合建六TCP连接的程序或进程，让 一个系统看上去像另一个系统。然后黑客就可以随意地攻击系统了，因为很难跟踪攻击来源。

暴力攻击类似于前门攻击，因为一个黑客试图通过作过一个合法用户获得通过。两者的区别是在暴力攻击中一个黑客使用所有的他认为能够击败认证利获得一个合法用户密码的字母、单词、字符。一个暴力攻击是一个并不精密复杂的企图尝试每一样东西包括字典文件，嗅探器和重复的登陆企图。暴力攻击的一个具体例子是，一个黑客试图使用计算机和信息的结合去破解一个密码。在—种情况下一个黑客需要破解—段单一的被用RC4算法和非对称密钥加密的信息，为了破解这种算法，一个黑客需要求助于非常精密复杂的方法，它使用120个工作站，两个超级计算机利从三个主要的研究中心获得的信息，即使拥有这种配备，它也将花掉八天的时间去破解加密算法，实际上破解加密过程八天已是非常短暂的时间了。