<<网络安全实验教程>>

图书基本信息

书名：<<网络安全实验教程>>

13位ISBN编号：9787512112988

10位ISBN编号：751211298X

出版时间：2013-01-01

出版时间：程光 清华大学出版社 (2012-12出版)

作者：程光，杨望 著

页数：176

<<网络安全实验教程>>

内容概要

《高等学校计算机科学与技术教材：网络安全实验教程》是针对高等学校学生的网络安全教学而编写的实验教程，其目的是使得学生掌握使用各种安全工具以保护其主机与网络的安全，提高学生对网络的攻防能力。
全书共分12章，每章包括若干个安全实验，每个实验分别介绍实验原理、环境设置、实验指南和思考与练习等4个部分内容，《高等学校计算机科学与技术教材：网络安全实验教程》基本覆盖了当前网络安全实验的主要分支和领域，主要包括以下内容：建立安全实验环境，安装和使用扫描器和侦听工具，口令破解，中间人攻击，欺骗攻击，拒绝服务攻击，配置防火墙，Rootkits技术，木马创建后门的过程，蠕虫病毒工作过程，僵尸网络的原理和方法，Web应用程序的攻击和防护等。
《高等学校计算机科学与技术教材：网络安全实验教程》适合作为计算机科学与技术、网络和信息安全相关专业本科生和研究生的网络安全相关课程配套教材，还为自学网络安全的读者提供非常理想的指导，也适合企、事业单位的网络和系统管理维护人员作为工具书。

<<网络安全实验教程>>

书籍目录

章节摘录

版权页： 插图： 首先，请求端（客户端）发送一个包含SYN标志的TCP报文，SYN即同步（Synchronize），同步报文会指明客户端使用的端口和TCP连接的初始序号。
第二步，服务器在收到客户端的SYN报文后，将返回一个SYN+ACK的报文，表示客户端的请求被接收，同时TCP序号被加一，ACK即确认（Acknowledgement）。
第三步，客户端也返回一个确认报文ACK给服务器端，同样TCP序列号被加一，到此一个TCP连接完成。
以上的连接过程在TCP协议中被称为三次握手（Three—way Handshake）。
问题就出在7CP连接的三次握手中，如图6—4所示。
假设一个用户向服务器发送了SYN报文后突然死机或掉线，那么服务器在发出SYN+ACK应答报文后是无法收到客户端的ACK报文的（第三次握手无法完成），这种情况下服务器端一般会重试（再次发送SYN+ACK给客户端）并等待一段时间后丢弃这个未完成的连接，这段时间的长度称为SYN：Timeout，一般来说，这个时间是分钟的数量级（大约为30秒～2分钟）。
一个用户出现异常导致服务器的一个线程等待1分钟并不是什么很大的问题，但如果有一个恶意的攻击者大量模拟这种情况，服务器端将为了维护一个非常大的半连接列表而消耗非常多的资源——数以万计的半连接，即使是简单的保存并遍历也会消耗非常多的CPU时间和内存，何况还要不断对这个列表中的IP进行SYN+ACK的重试。
实际上，如果服务器的TCP/IP栈不够强大，最后的结果往往是堆栈溢出崩溃。
即使服务器端的系统足够强大，服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正常请求（毕竟客户端的正常请求比率非常之小），此时从正常客户的角度看来，服务器失去响应，这种情况就称作：服务器端受到了TCP SYN Flood攻击。
6.2.2碎片攻击原理 Teardrop是基于UDP的病态分片数据包的攻击方法，其工作原理是向被攻击者发送多个分片的IP包（IP分片数据包中包括该分片数据包属于哪个数据包及在数据包中的位置等信息），某些操作系统收到含有重叠偏移的伪造分片数据包时将会出现系统崩溃、重启等现象。
例如，假设原始IP包有150字节数据（不含IP头），该数据包被分成两块，前一块有120字节，偏移为0；后一部分则是30字节，偏移为120。
当接收方收到第一分片后，如果收到第二个长度为30字节，偏移量为120的分片时，其将第二个数据包的长度加上偏移量作为第一分片和第二分片的总长度（这里是150）。
由于已经拷贝了第一分片的120字节，因此系统从第二个分片中拷贝150—120=30字节数据到为重组开设的缓冲区。
这样，一切正常。
但是，如果攻击者修改第二个分片，使其数据长度为30，偏移量为80，结果就不一样了。
系统在收到第二个分片时，计算80+30=110作为两个分片的总长度。
为了确定应该从第二个分片中拷贝多少字节，系统需要用总长度110减去第一个分片的长度120，结果是—10字节。
由于系统采用的是无符号的整数，则—10相当于一个很大的整数，这时系统处理将出现异常。
通常会导致堆栈损坏、IP模块不起作用和系统挂起，甚至导致系统崩溃。

<<网络安全实验教程>>

编辑推荐

《高等学校计算机科学与技术教材:网络安全实验教程》适合作为计算机科学与技术、网络和信息安全相关专业本科生和研究生的网络安全相关课程配套教材，还为自学网络安全的读者提供非常理想的指导，也适合企、事业单位的网络和系统管理维护人员作为工具书。

<<网络安全实验教程>>

版权说明