<<网络安全与管理>>

图书基本信息

书名：<<网络安全与管理>>

13位ISBN编号：9787811324549

10位ISBN编号：7811324547

出版时间：2009-2

出版时间：涂敏、 胡颖辉 江西高校出版社 (2009-02出版)

作者：涂敏，胡颖辉

<<网络安全与管理>>

内容概要

网络安全与管理，ISBN：9787811324549，作者：涂敏，胡颖辉主编

<<网络安全与管理>>

书籍目录

章节摘录

版权页： 插图： 4.1.4 网络攻击步骤 网络攻击步骤可以说变幻莫测，但纵观其整个攻击过程，还是有一定规律可循的，一般可以分：攻击前奏、实施攻击、巩固控制、继续深入这几个过程。
下面我们来具体了解一下这几个过程：1.攻击前奏 网络攻击者在发动攻击之前，首先要锁定目标，了解目标的网络结构，收集各种目标系统的信息等。
锁定目标：在网络上有许多主机，网络攻击者首先要寻找到他要找的站点。
运用Ping这样的程序探测目标地址，对此作出响应的表示其存在。
然后利用IP地址就可以找到目标主机。
了解目标的网络结构：确定要攻击的目标后，网络攻击者就会设法了解其所在的网络结构，哪里是网关路由，哪里有防火墙，IDS，哪些主机与要攻击的目标主机关系密切等，最简单地就是用Tracert命令追踪路由，也可以发一些数据包看其是否能通过来猜测其防火墙过滤规则的设定等。
当然老练的网络攻击者在干这些的时候都会利用别的计算机来间接的探测，从而隐藏他们真实的IP地址。
收集系统信息：在收集到目标的第一批网络信息之后，网络攻击者会对网络上的每台主机进行全面的系统分析，以寻求该主机的安全漏洞或安全弱点。
收集系统信息的方法有：技术手段收集和社会工程收集。
因特网上的主机大部分都提供WWW、Mail、FTP、Telnet等日常网络服务，通常情况下Telnet服务的端口是23，WWWW服务的端口是80，FTP服务的端口是23。
利用Snmp服务、Tracemute程序、Whois服务来查阅网络系统路由器的路由表，从而了解目标主机所在网络的拓扑结构及其内部细节。
Traceroute程序能够获得到达目标主机所要经过的网络数和路由器数，Whois协议服务能提供有关的DNS域和相关的管理参数，Finger协议可以用Finger服务来获取一个指定主机上所有用户的详细信息（如用户注册名、电话号码、最后注册时间以及他们有没有读邮件等等）。
所以如果没有特殊的需要，管理员应该关闭这些服务。
收集系统信息当然少不了安全扫描器，网络攻击者会利用一些安全扫描器来帮他们发现系统的各种漏洞，包括各种系统服务漏洞、应用软件漏洞、弱口令用户等等。
除了上述技术手段获取相关信息外，还可以利用社会工程来收集信息。
通过一些公开的信息，如办公室电话号码、管理员生日、姓氏姓名、家庭电话，来尝试弱口令，通过搜索引擎来了解目标网络结构、关于主机更详细的信息，虽然几率很小，但至今仍会有管理员犯一些错误，例如某高能所将自己网络改进方案放在网上，详细地列出每台设备的地址配置。

<<网络安全与管理>>

编辑推荐

《21世纪高校规划教材:网络安全与管理》吸收了国内外教材的优点，结合我们多年的网络安全教学经验，充分强调实践操作，突出培养职业技能。
在编写本教材时，对计算机网络安全的理论知识和工作原理介绍得简单一些，更多的内容侧重于对计算机具体网络安全技术应用的介绍，体现出注重培养学生实际应用技术能力的特点。

版权说明