

## <<IP网络安全技术>>

### 图书基本信息

书名：<<IP网络安全技术>>

13位ISBN编号：9787115170132

10位ISBN编号：7115170134

出版时间：2008-2

出版时间：人民邮电

作者：《IP网络安全技术》编写组

页数：123

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

## <<IP网络安全技术>>

### 内容概要

本书以问答的形式介绍了IP网络安全方面的基本知识，共分10篇，包括网络安全基础篇、攻击和防范篇、病毒木马及恶意代码防范篇、Linux/UNIX安全篇、Windows安全篇、网络设备安全篇、网上交易安全篇、即时通信安全篇、数据安全篇和安全产品篇。

本书通俗易懂，供信息通信工程技术人员、管理人员以及设备厂商和科研机构的相关人员阅读，可作为电信运营企业员工的培训教材，也可供高等学校通信工程专业学生参考。

## &lt;&lt;IP网络安全技术&gt;&gt;

## 书籍目录

- 一、网络安全基础篇
- Q1. 为什么网络安全不是绝对的？
- Q2. 什么是网络安全的“木桶原理”？
- Q3. 为什么系统会存在网络安全漏洞？
- Q4. 使用他人计算机时需要注意哪些安全问题？
- Q5. 如何选择一個易记难猜的口令？
- Q6. 使用代理服务器上网安全吗？
- Q7. 浏览网页时需要注意哪些安全问题？
- Q8. 在浏览器中输入的口令等信息是否会被别人看到？
- Q9. 发邮件时如何对敏感的邮件内容进行保护？
- Q10. 如何降低邮件附件中恶意代码带来的风险？
- Q11. 如何判断一封电子邮件是否经过伪造？
- Q12. 如何对重要的Word文档进行安全保护？
- Q13. 如何减少收到的垃圾邮件？
- Q14. 哪些计算机端口容易受到网络攻击？
- Q15. 通过无线上网有哪些安全隐患？
- Q16. 如何提高无线上网的安全性？
- Q17. WLAN支持哪些安全加密协议？支持哪些认证协议？
- 二、攻击和防范篇
- Q18. 常见的网络攻击方式有哪些？
- Q19. 什么是缓冲区溢出攻击？
- Q20. 如何防范对计算机的扫描探测攻击？
- Q21. Windows系统账号是弱口令时会导致哪些严重后果？
- Q22. 如何防止计算机系统账号、共享等敏感信息被远程窃取？
- Q23. 如何避免个人计算机成为网络攻击的跳板？
- Q24. 什么是TCP-SYN flood攻击，网络攻击对系统有何影响？
- Q25. 什么是ARP欺骗？
- Q26. 局域网环境内如何防止通信数据被监听？
- Q27. 拒绝服务攻击主要有哪几种类型？
- Q28. DDoS攻击对网络或系统有何影响？
- Q29. 对于DDoS攻击，一般可以利用路由器的哪些安全特征进行控制？
- Q30. 网络蠕虫会对网络或系统造成哪些影响？
- Q31. 异常流量监测方式主要有哪几种，有何特点？
- Q32. TCP拦截技术可以用来防范何种攻击，它是如何工作的？
- Q33. 如果网络流量突然异常增大，应该如何处理？
- Q34. 通过哪些网络安全手段可以提高IP承载网的安全性？
- Q35. 网络安全建设主要包括哪几方面的内容？
- 三、病毒、木马及恶意代码防范篇
- Q36. 什么是计算机病毒？有什么特征？
- Q37. 病毒入侵计算机的常见途径有哪些？
- Q38. 计算机感染病毒的症状有哪些？
- Q39. 如何预防计算机病毒？
- Q40. 如何减少邮件病毒的危害？
- Q41. 为什么病毒会反复出现？
- Q42. 蠕虫病毒与一般病毒的区别在哪里？
- Q43. 安装防病毒软件后，为何还会被病毒感染？

## &lt;&lt;IP网络安全技术&gt;&gt;

- Q44. 正常情况下，当病毒不能被成功清除时该如何处理？
- Q45. 病毒是怎么利用U盘传播的？
- Q46. 如何防范病毒通过U盘传播？
- Q47. 什么是木马？  
有什么危害？
- Q48. 我的计算机是否已被装了木马？  
如何检测？
- Q49. 如何识别木马的伪装？
- Q50. 木马防范工具有哪些？
- Q51. 为什么电脑总是莫名其妙地弹出很多窗口、广告？
- Q52. 什么是流氓软件？Q53. 如何清除计算机上的流氓软件？
- Q54. 什么是僵尸网络？
- Q55. 什么是僵尸程序？
- Q56. 僵尸程序与蠕虫、木马有什么联系和区别？
- Q57. 企业网应如何防范病毒？
- Q58. 网吧该如何防病毒？
- 四、Linux/UNIX安全篇
- Q59. 忘记Linux的root用户口令怎么办？
- Q60. 如果没有对Linux引导装载程序进行口令保护，有什么风险？  
应如何保护？
- Q61. Linux账号长期保持登录状态可能会导致对账号的非法使用，应如何让Linux账号登录在超时时自动注销？
- Q62. 普通用户使用su命令可以切换到root用户，为防止对root的滥用，希望限制可使用su命令的用户，应如何实现？
- Q63. 怎样禁止root用户远程登录以防止对root身份的滥用？
- Q64. 为防止用户大量挤占磁盘空间，应如何对用户设置磁盘配额限制？
- Q65. 普通用户登录到Linux控制台后，将可以执行poweroff、halt、reboot等普通用户通常无权执行的命令，应如何禁用这些命令以保护控制台？
- Q66. 如何设置最短口令长度以增强Linux用户口令的强壮性？
- Q67. 如何调整Linux系统参数以增强其抵御syn flood攻击的能力？
- Q68. 不必要的SUID权限会给系统带来什么风险？
- Q69. 异常的网络开放端口可能意味着系统已经被入侵，因此应定期查看端口开放情况。  
对于Linux系统，应如何查看其正在监听的网络端口？
- Q70. 怎样阻止对Linux系统的ping扫描？
- Q71. 怎样保护Linux系统的重要配置文件不被非法删除？
- Q72. 如何配置Linux的防火墙保护？
- Q73. 为什么使用Linux-PAM可方便替换Linux应用程序的验证机制？
- Q74. 在UNIX系统中怎样进行文件权限控制？
- Q75. 如何保障UNIX系统的网络服务安全？
- Q76. 怎样利用syslog记录UNIX系统日志？
- Q77. 如何解决Telnet、rsh、rlogin等常见的UNIX远程管理方式存在的安全隐患？
- Q78. \$HOME/.rhosts和hosts.e Quiv信任机制存在什么安全隐患？
- Q79. 如何发现UNIX文件系统被非法篡改的迹象？
- Q80. 如何通过安全配置降低UNIX系统遭受缓冲区溢出攻击的风险？
- Q81. 典型的安全加固流程是怎样的？
- 五、Windows安全篇
- Q82. 忘记Windows 2000管理员密码怎么办？
- Q83. 如何使用“密码保护”功能来加强计算机的物理安全？
- Q84. Windows系统为什么要经常打补丁呢？

## &lt;&lt;IP网络安全技术&gt;&gt;

- Q85. Windows SP补丁和hotfix修补程序有何区别和联系？
- Q86. 如何进行Windows系统安全补丁安装？
- Q87. 为什么最好不要启用Windows系统的账号锁定功能？
- Q88. 如何提高系统用户密码的安全性？
- Q89. 如何控制用户对某些磁盘或者文件夹的本地访问？
- Q90. 如何对Windows主机进行简单的网络访问控制？
- Q91. 在Windows系统中如何发现黑客入侵的痕迹？
- Q92. Windows 2000系统的安全架构是怎么样的？
- Q93. 用户的安全标识符(SID)能够唯一标识每个用户吗？
- Q94. Windows用户的访问令牌(Access tokens)有何作用？
- Q95. Windows系统自带防火墙吗，怎样启用？
- Q96. 为什么要禁止Windows系统不必要的服务，如何关闭？
- Q97. 怎样查看Windows主机开放了哪些端口？
- Q98. 缺省情况下，Windows系统开放了哪些端口，有什么风险？
- Q99. 如何关闭Windows系统中的一些高风险的端口？
- Q100. 网络共享文件有何风险？  
怎样降低风险？
- Q101. 如何防止别人远程扫描到我的Windows主机？
- Q102. Windows系统的“本地安全设置”有何功能？
- Q103. 如何知道Windows系统已经建立了哪些网络连接？
- Q104. Windows XP系统的“安全中心”有什么作用呢？
- Q105. 用户如何选择比较强壮的密码，不设置有什么风险？
- Q106. 在安装某些软件或更改配置后，Windows XP系统工作不正常，能否恢复到以前的配置？
- Q107. 如何知道Windows系统已经共享了哪些文件夹？
- Q108. 怎样提高Windows系统注册表的安全性？
- Q109. 对Windows系统进行安全加固，主要包括哪些方面？
- 六、网络设备安全篇
- Q110. 哪些措施可以提高网络设备远程访问的安全性？
- Q111. 为保证网络的安全性，在配置路由器时应注意关闭哪些路由选项？
- Q112. 什么是AAA协议，主要有哪几种标准？
- Q113. 访问网络设备时，对用户进行AAA认证授权有何优点？
- Q114. 如何提高网络设备SNMP服务的安全性？
- Q115. 在用户配置网络设备时，如何保证操作的安全性？
- Q116. 目前哪些路由协议提供了认证机制，分别支持哪种认证方式？
- Q117. 访问控制列表在网络安全方面主要有哪些应用？
- Q118. 为什么我的ADSL Modem设备会遭到攻击？
- Q119. 攻击者是怎样通过ADSL Modem设备远程获得宽带用户上网口令的？
- Q120. 为什么要修改ADSL Modem设备的缺省口令？  
如何修改缺省口令？
- Q121. ADSL Modem设备有哪些默认的服务？  
如何保证这些服务的安全性？
- Q122. 黑客是如何入侵无线网络路由器的？  
如何防范？
- Q123. 保证用户正常使用的情况下，如何让无线路由器隐身？
- Q124. 如何限制只有特定的主机才能够接入到无线网络中？
- Q125. 忘记交换机的密码怎么办？
- Q126. 交换机生成树协议存在什么安全问题？
- Q127. 交换机CAM表攻击是怎么一回事，具有什么危害？

## &lt;&lt;IP网络安全技术&gt;&gt;

- Q128. 如何防范交换机的CAM表溢出？
- Q129. 如何利用交换机来防范DHCP欺骗？
- Q130. 如何利用交换机防范ARP欺骗？
- Q131. 忘记路由器的密码怎么办？
- 七、网上交易安全篇
- Q132. 把银行账号、网上交易口令等信息存储在计算机里，安全吗？
- Q133. 如何提高网上交易的安全性？
- Q134. 网上购物时，对方要求提供信用卡账号时，该怎么办？
- Q135. 网上交易时经常会遇到软键盘输入方式，它有什么作用？
- Q136. 网上银行一般向用户提供两种数字证书，两者有何不同？
- Q137. 手机动态密码是如何保护网上银行安全的？
- Q138. 什么是网络钓鱼？
- Q139. 网上交易过程中有哪些常见的钓鱼方式？
- Q140. 为什么有时在浏览器上输入网站的正确地址也会进入钓鱼网站？
- Q141. 网上银行操作时应该注意什么问题？
- Q142. 网上进行证券交易存在哪些风险？
- Q143. 如何减少网上证券交易的风险？
- 八、即时通信安全篇
- Q144. 用QQ、MSN是通过明文传递即时消息吗？有何加密工具可对即时消息的传递加密？
- Q145. 为什么有的网络游戏、QQ等账号口令容易被盗，有什么防范措施？
- Q146. 如何保护QQ/MSN聊天记录？
- Q147. 如何检查QQ/MSN是否被植入了木马？
- Q148. 通过QQ/MSN接收文件时，应该具备哪些安全意识？
- Q149. QQ如何自动拒收特定类型的文件以防范有害程序的入侵？
- Q150. 在网吧上QQ/MSN聊天有哪些安全注意事项？
- Q151. QQ/MSN也需要定期更新升级吗？
- Q152. 如何保护QQ共享空间的文件安全？
- Q153. QQ的通讯录上存放了朋友的个人资料，该如何保护这些信息的安全？
- 九、数据安全篇
- Q154. 数据有哪些安全属性？
- Q155. 对称加密和非对称加密有什么区别？
- Q156. DES、3DES和AES，哪种对称加密算法更安全？
- Q157. 如何通过数据摘要验证数据的完整性？
- Q158. 如何实现口令等信息的安全存储？
- Q159. 想把机密信息通过网络途径安全地传递给对方，有哪些方法？
- Q160. VPN如何保障数据传输安全？
- Q161. 什么是IPSec VPN？
- Q162. IPSec VPN如何实现企业分支机构之间的安全互联？
- Q163. IPSec VPN如何实现出差人员以安全方式访问企业内网？
- Q164. IPSec VPN设备是否支持Radius认证方式，对用户进行集中认证管理？
- Q165. IPSec如何防范重放攻击？
- Q166. 怎样保护Web服务器和用户浏览器之间的信息传输安全？
- Q167. Telnet采用明文传输口令，如何解决这个问题？
- Q168. FTP口令是明文传输的，有什么办法实现口令的加密传递？
- Q169. 可以参考哪些标准或协议开发一个基于指定端口的加密应用？
- Q170. 能否通过加密的方式实现不同PC机之间文件的网络拷贝？
- Q171. 如何在局域网内实现基于二层身份认证的安全接入？
- Q172. 802.1x认证机制是如何工作的？
- Q173. 什么是数字证书？
- Q174. 什么是数字签名？

## <<IP网络安全技术>>

- Q175. 如何对邮件进行签名和加密保护？
- Q176. 如何规避数据存储所面临的安全风险？
- Q177. 怎样合理制订数据备份策略？
- Q178. 有哪些常见的数据库防入侵保护措施？
- Q179. 如何实现数据库加密？
- 十、安全产品篇
- Q180. 目前有哪些种类的防病毒产品，各自的功能是什么？
- Q181. 如何合理部署防病毒产品？
- Q182. 选购防病毒产品应遵循哪些原则？
- Q183. 个人电脑在安装了防病毒产品之后为什么还需安装个人防火墙？
- Q184. 什么是防火墙？
- Q185. 防火墙有哪些组网模式？
- Q186. 配置防火墙时应该遵循什么原则？
- Q187. 为什么在部署防火墙产品之后需要定期检查其安全策略？
- Q188. 防火墙也能被渗透吗？
- Q189. 安全扫描工具有什么作用，目前有哪些种类的安全扫描产品，其主要的功能定位是什么？
- Q190. 使用安全扫描工具时需要注意什么问题？
- Q191. IDS与IPS有何异同？
- Q192. 如何看待IDS的漏报和误报？
- Q193. 使用IDS时需要注意哪些问题？
- Q194. 异常流量检测系统有何作用？
- Q195. 内容过滤系统有何作用？
- Q196. 有哪些产品可以提高储存在计算机上的文档或数据的安全性？
- Q197. 终端安全管理产品的主要功能是什么？
- Q198. 为什么部署终端安全管理产品可以防范蠕虫病毒的传播？
- Q199. 目前针对Windows系统有哪几种补丁管理产品，其作用是什么？
- Q200. 部署安全审计产品能起到什么作用？
- 在哪些安全需求下需要部署安全审计产品？
- Q201. 目前有哪些种类的安全审计产品？
- Q202. 数据库安全审计产品一般能完成哪些审计功能？
- Q203. 统一身份认证系统的主要功能是什么？
- Q204. 什么是动态令牌，采用动态令牌有什么好处？
- Q205. 什么是USB Key，采用这类产品能够防止哪些网络安全问题？
- Q206. 部署VPN等远程接入类产品时如何防止非安全终端接入网络？
- Q207. 什么是统一威胁管理(UTM)安全设备？
- Q208. 在哪些环境下适合部署UTM系统？
- Q209. 什么是安全操作中心(SOC)，其主要功能和作用是什么？

缩略语参考文献

## <<IP网络安全技术>>

### 编辑推荐

《IP 网络安全技术》通俗易懂，供信息通信工程技术人员、管理人员及设备厂商和科研机构的相关人员阅读，可作为电信运营企业员工的培训教材，也可供高等学校通信工程专业学生参考。

## <<IP网络安全技术>>

### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>