List of 💣s

21. If misconfigured, TFTP will hand over sensitive files (page 53).
22. Don't make *ftp*'s home directory writable by *ftp* (page 56).
23. Don't put a real password file in the anonymous *ftp* area (page 56).
24. It is easy to wiretap *telnet* sessions (page 58).
25. The *r* commands rely on address-based authentication (page 60).
26. Be careful about interpreting WWW format information (page 65).
27. WWW servers should be careful about URLs (page 65).
28. Poorly written query scripts pose a danger to WWW servers (page 66).
29. The MBone can be used to route through some firewalls (page 67).
30. Scalable security administration of peer-to-peer nodes is difficult (page 69).
31. An attacker anywhere on the Internet can probe for X11 servers (page 70).
32. UDP-based services can be abused to create broadcast storms (page 72).
33. Web servers shouldn't believe uploaded state variables (page 76).
34. Signed code is not necessarily safe code (page 80).
35. JavaScript is dangerous (page 82).
36. Users are ill-equipped to make correct security choices (page 83).
37. Humans choose lousy passwords (page 96).
38. There are lots of ways to grab `/etc/passwd` (page 98).
39. There is no absolute remedy for a denial-of-service attack (page 107).
40. Hackers plant sniffers (page 128).
41. Network monitoring tools can be very dangerous on an exposed machine (page 159).
42. Don't believe port numbers supplied by outside machines (page 178).
43. It is all but impossible to permit most UDP traffic through a packet filter safely (page 207).
44. A tunnel can be built on top of almost any transport mechanism (page 235).
45. If the connection is vital, don't use a public network (page 236).