List of 💣s

1. Password system failures are the biggest single problem (page 11).
2. Sequence number attacks can be used to subvert address-based authentication (page 24).
3. It is easy to spoof UDP packets (page 25).
4. ICMP packets can tear down all connections between a pair of hosts (page 25).
5. ICMP `Redirect` messages can subvert routing tables (page 26).
6. IP source routing can subvert address-based authentication (page 26).
7. It is easy to generate bogus RIP messages (page 27).
8. The inverse DNS tree can be used for name-spoofing (page 28).
9. The DNS cache can be contaminated to foil crosschecks (page 28).
10. Return addresses in mail aren’t reliable (page 30).
11. *Sendmail* is a security risk (page 30).
12. Don’t blindly execute MIME messages (page 31).
13. It is easy to wiretap *telnet* sessions (page 32).
14. You can subvert NTP in order to attack authentication protocols (page 33).
15. *Finger* discloses too much information about users (page 33).
16. Don’t trust RPC’s machine name field (page 34).
17. The *portmapper* can call RPC services for its caller (page 35).
18. NIS can often be persuaded to give out password files (page 36).
19. It is sometimes possible to direct machines to phony NIS servers (page 37).
20. It is hard to revoke NFS access (page 37).

21. If misconfigured, TFTP will hand out `/etc/passwd` (page 39).
22. Don't make *ftp*'s home directory writable by *ftp* (page 41).
23. Don't put a real password file in the anonymous *ftp* area (page 42).
24. FSP is often abused to give out files to those who should not have them (page 42).
25. Be careful about interpreting WWW format information (page 44).
26. WWW servers should be careful about file pointers (page 44).
27. Attackers can use *ftp* to create *gopher* control information (page 44).
28. Poorly written query scripts pose a danger to WWW servers (page 45).
29. The MBone can be used to route through some firewalls (page 46).
30. An attacker anywhere on the Internet can probe for X11 servers (page 47).
31. Don't believe port numbers supplied by outside machines (page 56).
32. It is all but impossible to permit most UDP traffic through a packet filter safely (page 69).
33. A tunnel can be built on top of almost any transport mechanism (page 80).
34. Firewalls can't block attacks at higher levels of the protocol stack (page 82).
35. X11 is very dangerous, even when passed through a gateway (page 106).
36. Network monitoring tools can be very dangerous on an exposed machine (page 128).
37. Be careful about pointing *finger* at a subverted machine (page 138).
38. Watch out for booby-trapped file names (page 139).
39. Hackers plant silent password grabbers (page 155).
40. There are lots of ways to grab `/etc/passwd` (page 160).
41. Logging failed logins will often capture passwords (page 183).
42. You may be liable for a hacker's activities (page 206).