APPENDIX B

Tools

This appendix provides a list of tools categorized according to the chapters in the book. Although the chapters contained in this book cover many of the popular software applications that you can use in penetration testing, numerous others are just as good. Use this appendix to research other tools that you might find useful in your penetration testing toolbox.

This appendix is broken down by chapter beginning with Chapter 5, "Performing Host Reconnaissance." All of the web references work as of the time of writing.

You can also find a hyperlinked PDF version of this appendix at http://www.ciscopress.com/title/1587052083 to easily launch your web browser to the URLs listed.

Performing Host Reconnaissance (Chapter 5)

Tool	URL	Description
7thportscan	http://www.zone-h.com/en/download/category=71/	A small port scanner.
AcePing	http://www.zone-h.com/en/download/category=28/	A tool that checks the network statistics and the state of remote computers.
Advanced Net Tool (ANT)	http://www.zone-h.com/en/download/category=71/	A tool that includes the following utilities: **portscan**, **traceroute**, **dns**, **sharescan**, **ping**, **whois**, and others.
Advanced Port Scanner	http://www.pcflank.com	A TCP Connect() and TCP SYN Port scanner.
Altavista	http://www.altalavista.com	A good tool for searching newsgroups.
Amap	http://www.thc.org	A next-generation scanning tool that identifies applications and services even if they are not listening on the default port by creating a bogus communication and analyzing the responses.

continues

Tool	URL	Description
Angry IP Scanner	http://www.snapfiles.com/Freeware/network/fwscanner.html	A fast and small IP scanner. It pings each IP address to check whether it is alive. Then, optionally, it resolves host names and tries to connect as specified in the Options dialog box TCP port.
Animal Port Scanner	http://www.zone-h.com/en/download/category=71/	A simple port scanner.
APNIC	http://www.apnic.net	Asia Pacific Internet Registrar.
Archaeoptery x	http://www.zone-h.com/en/download/category=28/	A passive mode OS identification tool.
Archive.org	http://www.archive.org	An archive of the web. Allows you to view old websites.
ARIN	http://www.arin.net	American Registry for Internet Numbers.
ARPing	http://www.habets.pp.se/synscan/programs.php?prog=arping	Broadcasts a who-has ARP packet on the network and prints answers.
AW Security Port Scanner	http://www.atelierweb.com	A high-speed TCP Connect scanning engine.
Central Ops Network Utilities	http://www.centralops.net	A tool that provides online Internet utilities including **traceroute**, **NSLookup**, **ping**, and others.
Cheops	http://www.marko.net/cheops/	An open source tool to locate, access, and diagnose network resources.
ClearSight Analyzer	http://www.spirentcom.com	A network and application analyzer with visual tools to detect problems.
DNS Stuff	http://www.dnsstuff.com	A tool that provides numerous Internet DNS tools including **Whois**, **NSLookup**, **ping**, **tracert**, and others.
Dsniff	http://naughty.monkey.org/~dugsong/dsniff/	A collection of tools for network auditing and penetration testing.
Email Tracker Pro	http://www.emailtrackerpro.com/index.html	A tool that analyzes e-mail to identify the e-mail address and location of the sender.
Fast Port Scanner	http://www.zone-h.com/en/download/category=71/	FPS stands for Fast Port Scanner.
FlameThrower	http://www.antara.net	Web and firewall stress-test tool.
FriendlyPinger	http://www.kilievich.com/	A powerful and user-friendly application for network administration, monitoring, and inventory.

Tool	URL	Description
FS32 Scanner	http://www.zone-h.com/en/download/category=71/	A tool that scans a range of IP addresses for FTP access. After you are logged in, FS32 proceeds to extract the following information: resume capability, FXP (PASV), and directory create/delete permissions.
GFI LANguard	http://www.gfi.com/lannetscan/	GFI LANguard Network Security Scanner (N.S.S.) checks your network for all potential methods that a hacker might use to attack it. By analyzing the operating system and the applications running on your network, GFI LANguard N.S.S. identifies possible security holes.
Gobbler	http://www.networkpenetration.com/downloads.html	A remote OS detection tool that spoofs your source address.
Googledorks	http://Johnny.ihackstuff.com	A great website to search Googled-for error messages on websites that reveal way too much information.
HPING2	http://www.hping.org/	A TCP/IP packet assembler/dissassembler.
ICMPID	http://www.nmrc.org/project/index.html	A utility that does remote OS identification using five ICMP packets only. Offers many extra features, including IP spoofing support.
IP Blocks	http://www.nologin.org/main.pl?action=codeList&	An IP subnetting and enumeration tool.
IP Tools	http://www.zone-h.com/en/download/category=71/	A tool that scans your network for servers and open ports.
IP Tracer 1.3	http://www.soft32.com	An IP tracer that discovers the country and city for a specific IP.
Java Port Scanner	http://www.zone-h.com/en/download/category=71/	A port scanner written in Java.
LACNIC	http://www.lacnic.net	Latin American Internet registrar.
LanDiscovery	http://www.snapfiles.com/Freeware/network/fwscanner.html	A small utility that enables you to browse the local network. It quickly enumerates all available network machines and lists them with their shares.
LanSpy	http://www.snapfiles.com/Freeware/network/fwscanner.html	A network security scanner that allows you to gather information about machines on the network. This includes domain and NetBIOS names, MAC address, server information, domain and domain controller information, remote control, time, discs, transports, users, global and local users groups, policy settings, shared resources, sessions, open files, services, registry and event log information.

continues

Tool	URL	Description
Libvsk	http://www.s0ftpj.org/en/site.html	A set of libraries for network traffic manipulation from the user level, with some functions of filtering and sniffing.
Local Port Scanner	http://www.zone-h.com/en/download/category=71/	Another small port scanner.
Mercury LoadRunner	http://www.mercury.com	A load-testing product for predicting system behavior and performance. Using limited hardware resources, LoadRunner emulates hundreds or thousands of concurrent users to put the application through the rigors of real-life user loads.
MooreR Port Scanner	http://www.snapfiles.com/Freeware/network/fwscanner.html	A basic, standalone network scanner that includes more than 3000 predefined ports to allow you to see what services are running on the machine.
NBTscan	http://www.inetcat.org/software/nbtscan.html	A program for scanning IP networks for NetBIOS name information. It sends a NetBIOS status query to each address in a supplied range and lists received information in human-readable form. For each responded host, it lists IP address, NetBIOS computer name, logged-in username, and MAC address.
Nessus	http://www.nessus.org/	An open-source vulnerability scanner.
NetScanTools Pro	http://www.netscantools.com/	A set of information-gathering utilities for Windows 2003/XP/2000.
NetView Scanner	http://www.snapfiles.com/Freeware/network/fwscanner.html	NetView Scanner is three security applications in one: NetView scans IP addresses for available Windows file and print sharing resources. PortScan scans IP addresses for listening TCP ports. WebBrute tests user password strength on HTTP Basic Authenticated websites.
NEWT	http://www.snapfiles.com/Freeware/network/fwscanner.html	A network scanner for administrators that scans machines on a network and attempts to retrieve as much detailed information as possible without the need to run a client on the remote computer.

Tool	URL	Description
Nikto	http://www.cirt.net/code/nikto.shtml	An open-source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including more than 3100 potentially dangerous files/CGIs, versions on more than 625 servers, and version-specific problems on more than 230 servers.
Nmap	http://www.insecure.org/nmap/	A popular port scanner with many options for various port-scanning methods.
Nscan	http://www.zone-h.com/en/download/category=71/	A fast port scanner for Windows (up to 200 ports per second) for both hosts and large networks with numerous features.
NSLookup	Included with most operating systems (On Linux, compare with the Dig utility)	A tool for discovering IP information on DNS names.
OneSixtyOne	http://www.phreedom.org/solar/onesixtyone/index.html	An SNMP scanner.
Packit (Packet toolkit)	http://packetfactory.net/projects/packit/	A network auditing tool that has the capability to customize, inject, monitor, and manipulate IP traffic.
P0f	http://lcamtuf.coredump.cx/p0f.shtml	A passive OS fingerprinting tool.
PORTENT Supreme	http://www.loadtesting.com	An HTTP load tester.
PromiScan	http://www.shareup.com	Network sniffing detection software.
Proport	http://www.zone-h.com/en/download/category=71/	A rapid port scanner.
Retina	http://www.eeye.com/html/Research/Tools/RPCDCOM.html	A vulnerability scanner.
Ripe	http://www.ripe.net	The European Internet registry.
Root Access Port Scanner	http://www.zone-h.com/en/download/category=71/	A Windows-based port scanner.
SamSpade	http://www.samspade.org/	A free network query tool with a variety of features, including the capability to scan for e-mail relays, perform DNS zone transfers, and crawl websites.
Scapy	http://www.secdev.org/projects/scapy	An interactive packet manipulation tool, packet generator, network scanner, network discovery, and packet sniffer.
SendIP	http://www.earth.li/projectpurple/progs/sendip.html	A command-line tool to allow sending of arbitrary IP packets.
Sentinel	http://www.packetfactory.net/projects/sentinel/	An implementation project of effective remote promiscuous detection techniques.

continues

Tool	URL	Description
ServersCheck	http://www.snapfiles.com/Freeware/network/fwscanner.html	A tool for monitoring, reporting, and alerting on network and system availability.
Smart Whois	http://www.tamos.com/products/smartwhois/	A useful network information utility that allows you to look up all the available information about an IP address, host name or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information.
Sniff-em	http://www.sniff-em.com	A program that captures, monitors, and analyzes network traffic, detecting bottlenecks and other network-related problems.
SNScan	http://www.snapfiles.com/Freeware/network/fwscanner.html	An SNMP detection utility that can quickly and accurately identify SNMP-enabled devices on a network.
SoftPerfect Network Scanner	http://www.snapfiles.com/Freeware/network/fwscanner.html	A multithreaded IP, SNMP, and NetBIOS scanner.
SuperScan	http://www.foundstone.com	Another simple port scanner.
Teleport Pro	http://www.tenmax.com/teleport/pro/home.htm	A tool to copy websites to your hard drive.
THC-RUT	http://www.thc.org/thc-rut	THC-RUT (pronounced root) is a wide range of network discovery utilities such as ARP lookup on an IP range, spoofed DHCP request, RARP, BOOTP, ICMP-ping, ICMP address mask request, OS fingerprinting, and high-speed host discovery.
THC-Scan	http://www.thc.org/	A war dialer/scanner for DOS and Windows.
TFP	http://xenion.antifork.org	An OS detection tool.
TIFNY	http://www.tucows.com/preview/195236.html	A utility that opens up to six simultaneous sessions to read and download binaries from newsgroups.
TraceProto	http://traceproto.sourceforge.net/index.php	A traceroute replacement that lets you specify the protocol and port to trace to.
Tracert (Windows)/ Traceroute	Included with UNIX/Linux/Cisco operating systems	A utility to trace a packet through a network.
Trellian Trace Route	http://www.tucows.com	A site spidering tool.
Trout	http://www.zone-h.com/en/download/category=71/	A visual **traceroute** and **Whois** program.
Visual Lookout	http://www.visuallookout.com	A tool to automatically monitor and log IP connection activity on your host.

Tool	URL	Description
Visual Route Trace	http://www.visualware.com	A tool that has integrated **traceroute**, **ping**, reverse DNS, and **Whois** tools and will also show the connection route on a world map.
Webspy	http://www.snapfiles.com/Freeware/network/fwscanner.html	A small tool that lets you find web servers and automatically resolve their domain name (if any).
Whois	Built in to most operating systems	A tool that allows you to look up registration data for domains.
WotWeb	http://www.snapfiles.com/Freeware/network/fwscanner.html	A cut-down port scanner specifically made to scan for and display active web servers and show the server software running on them.
Xprobe	http://www.sys-security.com/index.php?page=xprobe	An active OS fingerprinting tool.
YAPS (Yet Another Port Scanner)	http://www.snapfiles.com/Freeware/network/fwscanner.html	YAPS is short for "Yet Another Port Scanner." and this is exactly what it is. In fact, YAPS is a basic but small and fast TCP/IP port scanner with little configuration options and a fairly plain interface.
Zodiac	http://www.packetfactory.net/projects/zodiac/	A DNS protocol analyzation and exploitation program.

Understanding and Attempting Session Hijacking (Chapter 6)

Tool	URL	Description
Arp0c	http://www.phenoelit.de/arpoc/index.html	A connection interceptor program that uses ARP spoofing.
arprelay	http://www.zone-h.com/en/download/category=28/	A tool that forwards IP packets between two machines on an Ethernet that have been told that the MAC address of the other is some random spoofed MAC address.
dsniff	http://naughty.monkey.org/~dugsong/dsniff/	A collection of tools for network auditing and penetration testing.
Fake	http://www.0xdeadbeef.info/	A utility that takes over an IP address using ARP spoofing.
fuzzy-fingerprint	http://www.thc.org/thc-ffp/	A technique that extends common man-in-the-middle (MITM) attacks by generating fingerprints that closely look like the public key fingerprint of the target.

continues

Tool	URL	Description
Hjksuite	http://www.pkcrew.org/tools/hjksuite/	A collection of programs for hijacking.
IP Watcher	http://engarde.com	A network security monitor for UNIX that provides the capability to control intruders in real-time.
Juggernaut	http://www.lot3k.org/tools/spoofing/1.2.tar.gz	A network sniffer that can also be used to hijack sessions.
NBTdeputy	http://www.zone-h.com/en/download/category=28/	A tool that registers a NetBIOS computer name on the network and is ready to respond to NetBT name-query requests.
OTU	http://www.s0ftpj.org/en/site.html	MITM concept code.
Remote TCP Session Reset	http://www.solarwinds.net	A tool that allows a network administrator to remotely reset a TCP session.
SMBRelay	http://pr0n.newhackcity.net/~sd/smbrelay.html	A tool that registers a fake SMB server, which can be used for MITM attacks.
Snarp	http://www.securityfocus.com/tools/1969	A tool for Windows NT 4.0 that uses an ARP poison attack to relay traffic between two hosts, allowing sniffing of the data on switched networks.
T-Sight	http://engarde.com	An intrusion detection and network monitoring tool for Windows that can monitor transaction data, control intruders in real-time, set alarms for certain activities, and produce reports or graphs of usage.
TTY Watcher	http://engarde.com	A host security monitor with active countermeasures.

Performing Web-Server Attacks (Chapter 7)

Tool	URL	Description
9x CGI Bug Finder	http://www.zone-h.com/en/download/category=71/	A tool to scan a host for CGI bugs.
Apache Scanner	http://www.zone-h.com/en/download/category=71/	An Apache vulnerability scanner.
Babelweb	http://www.zone-h.com/en/download/category=28/	A program that automates tests on an HTTP server. Babelweb follows the links and the HTTP redirect, but it is programmed to remain on the original server.
Burp proxy	http://portswigger.net/proxy/	An interactive HTTP/S proxy server for attacking and debugging web-enabled applications. It operates as a MITM between the end browser and the target web server. It also allows the user to intercept, inspect, and modify the raw traffic passing in both directions.

Tool	URL	Description
Domino Web Server Scanner	http://www.zone-h.com/en/download/category=71/	A vulnerability scanner for Domino web server.
DW PHP Scanner	http://www.zone-h.com/en/download/category=71/	A vulnerability scanner that checks for PHP vulnerabilities on web servers.
httprint	http://net-square.com/httprint/index.html	httprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they might have been obfuscated by changing the server banner strings, or by plug-ins such as mod_security or servermask.
IIS Security Scanner	http://www.zone-h.com/en/download/category=71/	A vulnerability scanner for Microsoft IIS servers.
Nikto	http://www.zone-h.com/en/download/category=71/	A web server scanner that performs comprehensive tests against web servers for multiple items, including more than 2200 potentially dangerous files/CGIs, versions on more than 140 servers, and problems on more than 210 servers.
PHPNuke	http://www.zone-h.com/en/download/category=71/	Scans for vulnerable PHP servers.
PHPBB Vulnerability Scanner	http://www.zone-h.com/en/download/category=71/	A PHP vulnerability scanner.
PTwebdav buffer overflow checker	http://www.zone-h.com/en/download/category=71/	A remote WebDAV buffer overflow checker.
TWWWScan	http://www.zone-h.com/en/download/category=71/	A Windows-based www vulnerability scanner that looks for 400 www/cgi vulnerabilities.
Unicodeuploader.pl	http://www.sensepost.com	A Perl script that exploits vulnerable web servers and uploads files.
URL Checker	http://www.zone-h.com/en/download/category=71/	A CGI scanner that checks for more than 700 vulnerabilities.
VoidEye CGI Scanner	http://www.zone-h.com/en/download/category=71/	A CGI scanner.
Wfetch	http://support.microsoft.com/support/kb/articles/Q284/2/85.ASP	A utility included with the IIS 6.0 Resource Kit from Microsoft. You can use this utility to retrieve files from a web server to test them for vulnerabilities.
Whisker	http://www.wiretrip.net/rfp	A CGI scanner.
WinSSLMiM (includes FakeCert)	http://www.zone-h.com/en/download/category=28/	WinSSLMiM is an HTTPS MITM attacking tool. It includes FakeCert, a tool to make fake certificates.

Performing Database Attacks (Chapter 8)

Tool	URL	Description
Database Scanner	http://www.iss.net	A vulnerability scanner that specifically checks popular database applications.
EMS MySQL Manager	http://ems-hitech.com/mymanager	A tool for managing MySQL databases.
OSQL	Built into Microsoft SQL Server	A tool that performs command-line SQL queries.
SqlBF	http://packetstormsecurity.org/Crackers/sqlbf.zip	A brute force password-cracking program for SQL servers.
SqlDict	http://packetstormsecurity.org/Win/sqldict.exe	A SQL password-cracking tool.
SQeal	http://www.hammerofgod.com/download.htm	A SQL2000 server impersonator.
SqlPoke	http://packetstormsecurity.org/NT/scanners/Sqlpoke.zip	A Windows NT-based tool that locates MSSQL servers and tries to connect with the default SA account. A list of SQL commands is executed if the connection is successful.
SqlScan	http://www.zone-h.com/en/download/category=42/	A MySQL database vulnerability scanner.

Cracking Passwords (Chapter 9)

Tool	URL	Description
Dictionaries / Wordlists	ftp://coast.cs.purdue.edu/pub/dict/, http://packetstormsecurity.org/Crackers/wordlists/dictionaries/	Word lists that can be used in most password-cracking utilities.
Hydra	http://www.thc.org/thc-hydra/	A fast network logon cracker that supports many different services.
John the Ripper	http://www.openwall.com/john/	A password-cracking utility.
L0phtCrack	http://www.atstake.com/research/lc3/index.html	A password-cracking utility for Windows.
LSADump2	http://razor.bindview.com/tools/files/lsadump2.zip	An application to dump the contents of the LSA secrets on a machine, provided you are an administrator.
PWDump2	http://razor.bindview.com/tools/files/pwdump2.zip	A utility to extract the Windows SAM database.
PDDump3	http://www.ebiz-tech.com/html/pwdump.html	A utility to remotely extract the Windows SAM database.
VNC Crack	http://www.phenoelit.de/vncrack/	A password-cracking tool for VNC.

Attacking the Network (Chapter 10)

Tool	URL	Description
9x_c1sco	http://www.packetstormsecurity.com/cisco/	A tool that kills all Cisco 7xx routers running IOS/700 v4.1(x).
anwrap.pl	http://www.packetstormsecurity.com/cisco/	A wrapper for ancontrol that serves as a dictionary attack tool against LEAP-enabled Cisco wireless networks. It traverses a user list and password list attempting authentication and logging the results to a file.
AW Firewall Tester (awft31)	http://www.zone-h.com/en/download/category=71/	A scanner to test the security of your firewall.
brute_cisco.exe	http://www.packetstormsecurity.com/cisco/	A brute force utility for Cisco password authentication.
Cisco677.pl Denial of Service	http://mail.dhbit.ca	A denial-of-service (DoS) tool that attacks 600 series routers.
CiscoCasumEst	http://www.phenoelit.de/ultimaratio/download.html	A Cisco IOS 12.x/11.x remote exploit for HTTP integer overflow.
Cisco Configuration Security Auditing Tool (CCSAT)	http://hotunix.com/tools/	A script to allow automated auditing of configuration security of numerous Cisco routers and switches.
Cisco Crack	http://www.packetstormsecurity.com/cisco/	A Cisco device login brute force tool.
Cisco 760 Denial of Service	http://www.packetstormsecurity.com/cisco/	A DoS tool that attacks 760 series routers.
Cisco Torch	http://www.arhont.com	A mass scanning, fingerprinting, and exploitation tool for Cisco routers.
Confuse Router	http://pedram.redhive.com/projects.php	A tool that sniffs partial traffic in a switched environment where ARP requests/replies are not broadcasted to every node.
CrashRouter	http://www.packetstormsecurity.com/cisco/index2.html	A Mirc script that crashes Cisco 600 series routers with CBOS of v2.4.2 or earlier.
Datapipe	http://www.covertsystems.org/blackbag.html	A TCP port redirection utility that is useful for firewall evasion.
DNS Hijacker	http://pedram.redhive.com/projects.php	A libnet/libpcap-based packet sniffer and spoofer.

continues

Tool	URL	Description
ICMP Router Discover Protocol Discovery Tool	http://www.zone-h.com/en/download/category=28/	A tool for testing IRDP on Cisco routers.
IOS Memory Leak Remote Sniffer	http://www.phenoelit.de/ultimaratio/download.html	A tool that exploits a memory leak vulnerability on some Cisco routers.
IOS W3 Vulnerability Checker	http://www.packetstormsecurity.com/cisco/index2.html	A tool that checks for vulnerabilities with the IP HTTP service on Cisco routers.
IRPAS	http://www.phenoelit.de/irpas/index.html	A collection of tools to test common protocols such as CDP, IRDP, IGRP, RIP, HSRP, and DHCP.
Network Config Audit Tool (NCAT)	http://ncat.sourceforge.net	A tool that facilitates the checking of security configuration settings on numerous Cisco IOS configurations.
ngrep	http://packetfactory.net/projects/ngrep/	A pcap-aware tool that allows you to specify extended regular or hexadecimal expressions to match against data payloads of packets. It currently recognizes TCP, UDP, ICMP, IGMP, and Raw protocols across Ethernet, PPP, SLIP, FDDI, Token Ring, 802.11, and null interfaces.
OCS	http://www.hacklab.tk	A scanner for Voice over IP (VoIP) networks.
OneSixtyone	http://www.phreedom.org/solar/onesixtyone/index.html	An SNMP scanner that sends SNMP requests to multiple IP addresses, trying different community strings and waiting for a reply.
RFS FTP Scanner	http://www.zone-h.com/en/download/category=71/	A command-line-based FTP scanner that runs in the background.
Ripper-RipV2	http://www.spine-group.org/toolIG.htm	A tool that allows you to inject routes to RIPv2 routers specifying the metric associated with them.
Thong.pl	http://hypoclear.cjb.net	An exploit script that attacks Cisco routers.
UDPpipe	http://www.covertsystems.org/blackbag.html	A UDP port redirection utility that is useful for firewall evasion.
Zodiac	http://www.packetfactory.net/projects/zodiac/	A DNS protocol analysis and exploitation program.

Scanning and Penetrating Wireless Networks (Chapter 11)

Tool	URL	Description
802.11b Network Discovery Tools	http://www.zone-h.com/download/file=4988/	A gtk tool to scan for 802.11b networks using wavelan/Aironet hardware and Linux wireless extensions.
Access Point SNMP Utils for Linux	http://www.zone-h.com/en/download/category=28/	A set of utilities to configure and monitor Atmel-based wireless access points (the case for most Intersil clone vendors) under Linux.
Aerosol	http://www.zone-h.com/en/download/category=72/	A fast and reliable war-driving application for Windows. Supports many type of wireless card chipsets.
Aircrack	http://www.zone-h.com/en/download/category=74/	An 802.11 WEP-cracking program that can recover a 40-bit or 104-bit WEP key after enough encrypted packets have been gathered.
AIRE	http://www.zone-h.com/en/download/category=72/	An 802.11 network discovery utility for Microsoft Windows XP. After finding a wireless access point, it displays pertinent information (timestamp, ESSID, channel, mode, and so on) and has various useful features like a power meter display and other APs within range.
Airpwn	http://www.zone-h.com/en/download/category=74/	A platform for injecting application layer data on an 802.11b network.
Airsnarf	http://www.zone-h.com/en/download/category=74/	A simple rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.
AirSnort	http://www.zone-h.com/en/download/category=74/ Asleap	A wireless LAN (WLAN) tool that recovers encryption keys.
ApSniff	http://www.zone-h.com/en/download/category=72/	A wireless (802.11) access point sniffer for Windows 2000.
bsd-airtools	http://www.zone-h.com/en/download/category=74/	A package that provides a complete toolset for wireless 802.11b auditing.
Btscanner	http://www.zone-h.com/en/download/category=74/	A tool that extracts as much information as possible from a Bluetooth device without the requirement to pair.

continues

Tool	URL	Description
Fake AP	http://www.zone-h.com/en/download/category=74/	A tool that generates thousands of counterfeit 802.11b access points.
Kismet	http://www.zone-h.com/en/download/category=74/	An 802.11 Layer 2 wireless network sniffer. It can sniff 802.11b, 802.11a, and 802.11g traffic.
Libradiate	http://www.packetfactory.net/projects/libradiate/	A tool to capture, create, and inject 802.11b frames.
MiniStumbler	http://www.zone-h.com/en/download/category=72/	A network stumbler for Pocket PC 3.0 and 2002.
NetStumbler	http://www.zone-h.com/en/download/category=72/	A Windows utility for 802.11b-based wireless network auditing.
Redfang v2.5	http://www.zone-h.com/en/download/category=74/	An enhanced version of the original application that finds nondiscoverable Bluetooth devices by brute-forcing the last six bytes of the device Bluetooth address and doing a read_remote_name().
waproamd	http://www.zone-h.com/en/download/category=74/	A Linux WLAN roaming daemon for IEEE 802.11b cards supported by a driver with the wireless extension API.
WaveStumbler	http://www.zone-h.com/en/download/category=74/	A console-based 802.11 network mapper for Linux.
Wellenreiter	http://www.zone-h.com/en/download/category=74/	A wireless network discovery and auditing tool.
WEPCrack	http://www.zone-h.com/en/download/category=72/	An open-source tool for breaking 802.11 WEP secret keys.
WifiScanner	http://www.zone-h.com/en/download/category=74/	A tool that has been designed to discover wireless nodes (that is, access points and wireless clients).

Using Trojans and Backdoor Applications (Chapter 12)

Tool	URL	Description
aes-netcat	http://mixter.void.ru/code.html	A strong encryption patch for netcat.
cd00r.c	http://www.phenoelit.de/stuff/cd00rdescr.html	A working proof-of-concept code for a nonlistening remote shell on UN*X systems.
Covert TCP	http://www.covertsystems.org/blackbag.html	A program that manipulates the TCP/IP header to transfer a file one byte at a time to a destination host.

Tool	URL	Description
datapipe_http_proxy.c	http://net-square.com/datapipe_http/index.html	A modified version of the datapipe port redirector. This version allows tunneling arbitrary TCP protocols through an HTTP proxy server that supports the CONNECT method.
Double Dragon Backdoor	http://www.pkcrew.org/index.php	A backdoor that allows you to keep remote access to a shell on a LAN protected by masquerading, getting rid of the inability for a nonpublic address to listen to a port that is reacheable from the Internet.
Dr. VBS Virus Builder	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A program that allows you to add source code and generate your own worm/virus, it has some samples of code inside the zip too.
EliteWrap	http://www.holodeck.f9.co.uk/elitewrap/index.html	An advanced EXE wrapper for Windows 95/98/2000/NT that is used for SFX-archiving and secretly installing and running programs.
Metasploit	http://www.metasploit.com/	A complete environment for writing, testing, and using exploit code. This environment provides a solid platform for penetration testing, shellcode development, and vulnerability research.
NT Rootkit	http://www.rootkit.com	A rootkit for Microsoft NT systems that allows you to hide files.
P0ke's Worm Generator	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A utility that allows you to create your own Trojans.
Q	http://mixter.void.ru/code.html	A remote shell and admin tool that has strong encryption.
Residuo Virus Builder	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A tool to create your own viruses.
Rial	http://www.pkcrew.org/index.php	A backdoor Trojan that can hide files and processes.
RPC Backdoor	http://www.s0ftpj.org/en/site.html	A backdoor that uses an RPC program to introduce a remote access facility in the host.
SAdoor	http://cmn.listprojects.darklab.org/	Although SAdoor can be used as a backdoor (which requires some work to avoid obvious detection), the intention is to provide an alternative way of remote access to sensitive systems.
sbd	http://www.covertsystems.org/blackbag.html	A Netcat-clone that is designed to be portable and offer strong encryption.
SennaSpy Worm Generator	http://sennaspy.cjb.net	Another tool to create your own worms.

continues

Tool	URL	Description
Sp00fed_TCP Shell	http://www.pkcrew.org/index.php	A backdoor that works by sending data in TCP packets without creating a connection.
Subseven	http://subseven.slak.org	A remote administration Trojan.
syslogd-exec	http://www.s0ftpj.org/en/site.html	These patches applied to syslogd 1.3-31 sources add a new priority. You can locally execute new commands without being logged in.
TFTP Scan	http://www.zone-h.com/en/download/category=28/	A scanner that detects running TFTP servers in a range of IP addresses.
THC Backdoor (Linux)	http://www.s0ftpj.org/en/site.html	A simple but useful backdoor for Linux.
VBSwg Virus Builder	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A utility to create your own virus.
Virus Source Code	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A site that has the source code for several popular viruses.
VNC	http://www.uk.research.att.com/vnc	A remote administration utility.
Z3ng	http://violating.us/releases.html	A backdoor that can modify a firewall.

Penetrating UNIX, Microsoft, and Novell Servers (Chapter 13)

Tool	URL	Description
Bindery	http://www.packetstormsecurity.com/Netware/penetration/	Utilities for extracting, importing, and exporting bindery information.
Burglar	http://www.packetstormsecurity.com/Netware/penetration/	An NLM that will either create a Supe user or make an existing user Supe equivalent. For Netware 3.x.
Burn	http://www.packetstormsecurity.com/Netware/penetration/	A tool that burns up drive space on the SYS: volume by filling up the SYS$ERR.LOG. About 1 MB per minute.
Chknull	http://www.packetstormsecurity.com/Netware/penetration/	A tool that checks for users that have no password.
CyberCop Scanner	http://www.tlic.com/security/cybercopscanner.cfm	A vulnerability scanner that tests Windows and UNIX workstations, servers, hubs, and switches.
DelGuest	http://ntsecurity.nu/toolbox/	A tool that deletes the built-in Guest account in Windows NT.
DumpSec	http://www.somarsoft.com	A security auditing program for Microsoft Windows NT/2000. It dumps the permissions (DACLs) and audit settings (SACLs) for the file system, registry, printers, and shares in a concise, readable format so that holes in system security are readily apparent.

Tool	URL	Description
enum	http://www.bindview.com/Services/Razor/Utilities/	A console-based Win32 information enumeration utility. Using null sessions, enum can retrieve userlists, machine lists, sharelists, namelists, group and member lists, passwords, and LSA policy information.
Essential Net Tools (ENT) 3	http://www.zone-h.com/en/download/category=28/	A tool to get NetBIOS information and remote access.
GetAcct	http://www.securityfriday.com/tools/GetAcct.html	A tool that sidesteps "RestrictAnonymous=1" and acquires account information on Windows NT/2000 machines.
Infiltrator Network Security Scanner	http://www.network-security-scan.com	An easy-to-use, intuitive network security scanner that can quickly scan and audit your network computers for vulnerabilities, exploits, and information enumerations.
InfoServer	http://www.zone-h.com/en/download/category=71/	A vulnerability scanner for Windows.
Inzider	http://ntsecurity.nu/toolbox/inzider	A tool that lists processes in your Windows system and the ports that each one listen on.
Lkminject	http://minithins.net/release.html	A tool to inject a Linux kernel module into another Linux kernel module.
Metasploit	http://www.metasploit.com/	A complete environment for writing, testing, and using exploit code. This environment provides a solid platform for penetration testing, shellcode development, and vulnerability research.
N-Stealth v3.5	http://www.zone-h.com/en/download/category=71/	A vulnerability assessment tool for Windows that scans webservers for bugs that allow attackers to gain access.
NetBrute	http://www.zone-h.com/en/download/category=71/	A tool that scans a range of IP addresses for resources that have been shared via Microsoft File and Printer Sharing.
Nbtdump	http://www.zone-h.com/en/download/category=28/	A utility that dumps NetBIOS information from Windows NT, Windows 2000, and UNIX Samba servers such as shares, user accounts with comments, and the password policy.
NBTScan	http://www.inetcat.org/software/nbtscan.html	A program for scanning IP networks for NetBIOS name information.
NCPQuery	http://razor.bindview.com/tools/index.shtml	A free, open-source tool that allows probing of a Novell NetWare server running IP to be queried to enumerate objects.
Nessus	http://www.nessus.org	A popular vulnerability scanner.
NetDDE.c	http://www.zone-h.com/en/download/category=71/	A Microsoft Windows scanner that uses a remote code execution vulnerability because of an unchecked buffer.

continues

Tool	URL	Description
netinfo	http://www.zone-h.com/en/download/category=71/	A complete scanner for the Windows system.
NetRecon	http://www.symantec.com	A vulnerability scanner by Symantec.
NetViewX	http://www.ibt.ku.dk/jesper/NTtools/	A console application to list servers in a domain/workgroup that run specific services.
Novell Fake Login	http://www.packetstormsecurity.com/Netware/penetration/	A fake Novell NetWare login screen that stores the username and password in the file c:\os31337.sys.
NTLast	http://www.foundstone.com/	A security log analyzer to identify and track who has gained access to your system and then document the details.
NetView Scanner	http://www.zone-h.com/en/download/category=71/	Freeware penetration analysis software that runs on your Windows workstation.
NWPcrack	http://www.packetstormsecurity.com/Netware/penetration/	A password-cracking utility for Novell servers.
Pandora	http://www.nmrc.org/project/pandora/index.html	A set of tools for hacking, intruding, and testing the security and insecurity of Novell NetWare. It works on versions 4 and 5.
PC Anywhere Scan	http://www.zone-h.com/en/download/category=71/	A small utility that can scan any range of two IP addresses and show the list of pcANYWHERE hosts within that range.
PipeUp Admin	http://www.dogmile.com/files	A utility to execute commands with administrative privileges, even if you do not have admin rights on a Windows system.
ProbeTS	http://www.hammerofgod.com/download.htm	A utility to scan for Windows Terminal Services.
RPC Dump	http://www.zone-h.com/en/download/category=28/	A utility that dumps SUN RPC information from UNIX systems.
Sara	http://www-arc.com/sara	A popular vulnerability scanner.
Security Analyzer	htt://www.netiq.com	A commercial vulnerability scanner made by NetIQ.
Shadow NW Crack	http://www.packetstormsecurity.com/Netware/penetration/	Code for breaking into Novell NetWare 4.x.
STAT Analyzer	http://www.stat.harris.com/techinfo/reskit/default.asp	A tool that automatically consolidates multiple network scanning and modeling results and provides a single, flexible reporting mechanism for reviewing those results.
Transport Enum	http://www.hammerofgod.com/download.htm	A tool that allows you to get the transport names (devices) in use on a box.

Tool	URL	Description
TSEnum	http://www.hammerofgod.com/download.htm	A tool that quickly scans the network for rogue terminal servers.
TSGrinder	http://www.hammerofgod.com/download.htm	A brute force terminal server tool.
unix2tcp	http://www.zone-h.com/en/download/category=28/	A connection forwarder that converts UNIX sockets into TCP sockets. You can use it to trick some X applications into thinking that they are talking to a local X server when it is remote, or moving local MySQL databases to a remote server.
User2sid / Sid2user	http://www.chem.msu.su/~rudnyi/welcome.html	Tools to determine a SID based on the username (User2sid) or determine username based on a known SID (Sid2user).
UserDump	http://www.hammerofgod.com/download.htm	A SID Walker that can dump every user in a domain in a single command line.
Userinfo	http://www.hammerofgod.com/download.htm	A tool that retrieves all available information about any known user from any NT/Windows 2000 system that you can hit 139 on.
VigilEnt	http://www.interwork.com/vendors/netiq_security_vsms.html	NetIQ's VigilEnt Security Manager Suite (VigilEnt Security Manager) proactively secures systems by assessing policy compliance, identifying security vulnerabilities, and helping you correct exposures before they result in failed audits, security breaches, or costly downtime.
Windows 2000 Resource Kit	http://www.microsoft.com/windows2000/	A suite of utilities for managing Windows 2000 networks.
Winfo	http://www.ntsecurity.nu	A Windows enumeration tool.
Yet Another NetWare Game (YANG)	http://www.packetstormsecurity.com/Netware/penetration/	A tool that loads the server and its clients with bogus broadcast packets.

Understanding and Attempting Buffer Overflows (Chapter 14)

Tool	URL	Description
Assembly Language Debugger (ald)	http://ald.sourceforge.net	A tool for debugging executable programs at the assembly level. It currently runs only on Intel x86 platforms.
Buffer Overflow Examples	http://www.covertsystems.org/research.html	A number of buffer overflow code examples to show proof of concept.
Bytecode examples	http://www.covertsystems.org/bytecode.html	Examples of shellcode (bytecode) that could be used in buffer overflows.
Flawfinder	http://www.zone-h.com/en/download/category=28/	A tool that searches through source code for potential security flaws, listing potential security flaws sorted by risk, with the most potentially dangerous flaws shown first.
LibExploit	http://www.packetfactory.net/projects/libexploit/	A generic exploit creation library to help the security community when writing exploits to test a vulnerability. Using the API, you can write buffer overflows (stack/heap/remote/local) and format strings easily and quickly.

Denial-of-Service Attacks (Chapter 15)

Tool	URL	Description
4to6ddos	http://www.pkcrew.org/	A distributed DoS against IPv6 that works without installing IPv6 support.
6TunnelDos	http://www.packetstormsecurity.com/DoS/	An IPv6 connection flooder that also works as a DoS for 6tunnel.
7plagues.pl	http://www.packetstormsecurity.com/DoS/	A threaded 7-headed DoS that you should use to test/audit the TCP/IP stack stability on your different operating systems, under extreme network conditions.
ackergaul	http://www.packetstormsecurity.com/DoS/	A distributed DoS tool that spoofs SYNs to consume the bandwidth of a host by flooding it with SYN-ACKs.
ACME-localdos.c	http://www.packetstormsecurity.com/DoS/	A local Linux DoS attack tested on Slackware 8.1 and 9.1, RedHat 7.2, and OpenBSD 3.2.

Tool	URL	Description
aimrape	http://sec.angrypacket.com/	A remote DoS exploit for AOL Instant Messenger (AIM) v4.7.2480 and below.
Aix433noflag.c	http://www.frapes.org/	A tool that exploits a weakness in a function in the AIX kernel that handles the incoming/outgoing network connection. Setting no flags in the TCP header causes a 100% CPU usage (DoS). Tested On IBM RS6000/SMP-M80/4) on AIX 4.3.3.
AolCrash	http://www.packetstormsecurity.com/DoS/	An AOLserver v3.0 and 3.2 remote DoS bug. Sends a long HTTP request.
ApacheDos.pl	http://www.packetstormsecurity.com/DoS/	An Apache 1.3.xx/Tomcat server with mod_jk remote DoS exploit that uses chunked encoding requests.
APSR	http://www.elxsi.de/	A TCP/IP packet sender to test firewalls and other network applications.
arb-dos	http://www.packetstormsecurity.com/DoS/	Three Perl scripts to exploit recent Windows application DoS vulnerabilities.
arpgen	http://www.packetstormsecurity.com/DoS/	A DoS tool that demonstrates that a flood of ARP requests from a spoofed Ethernet and IP address would be a practical attack on a local network.
Assult	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	An ICMP and UDP flooder.
Battle Pong	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A DoS tool that lets you choose the ping size and the speed to flood.
Blitznet	http://www.packetstormsecurity.com/distributed/	A tool that launches a distributed SYN flood attack with spoofed source IP, without logging.
Click v2.2	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A tool that allows you to disconnect an IRC user from the server.
DDoSPing	http://www.foundstone.com	A network admin utility for remotely detecting the most common DDoS programs.
Distributed DNS Flooder	http://www.packetstormsecurity.com/distributed/	A tool to attack DNS servers.
IGMP Nuker	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A tool that crashes a TCP stack of Windows 98 boxes.
Inferno Nuker	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A nuker that sends different attacks to the computer of the victim, forcing him to reboot.
Kaiten	http://www.packetstormsecurity.com/distributed/index2.html	An IRC distributed denial-of-service (DDoS) tool.

continues

Tool	URL	Description
Knight	http://www.packetstormsecurity.com/distributed/index2.html	A DDoS client that is lightweight and powerful. It goes on IRC, joins a channel, and then accepts commands via IRC.
Mstream	http://www.packetstormsecurity.com/distributed/index2.html	A popular DDoS tool.
Nemesy Nuker	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A program that generates random packets that you can use to launch a DoS attack against a host.
Omega v3	http://www.packetstormsecurity.com/distributed/index2.html	Another DDoS tool.
Orgasm	http://www.packetstormsecurity.com/distributed/	A distributed reflection DoS attack (reflects off of BGP speakers on TCP port 179).
Panther	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A tool for crashing firewalls.
Pud	http://www.packetstormsecurity.com/distributed/index2.html	A peer-to-peer DDoS client/server that does not rely on hubs or leaves to function properly. It can connect as many nodes as you like, and if one node dies, the rest stays up.
Rocket	http://users.otenet.gr/~nicktrig/nsitexz/index.htm	A nuker that sends the +++ath0 command to a modem and disconnects it.
Skydance v3.6	http://www.packetstormsecurity.com/distributed/index3.html	A DDoS tool for Windows.
Stacheldraht v4	http://www.packetstormsecurity.com/distributed/index3.html	German for "barbed wire." Combines features of the "trinoo" DDoS tool with those of the original TFN. It adds encryption of communication between the attacker and stacheldraht masters and automated update of the agents.
Stick DDOS	http://www.eurocompton.net/stick/	A resource starvation attack against IDS systems.
Tribe Flood Network 2000 (TFN2k)	http://1337.tsx.org/	Using distributed client/server functionality, stealth and encryption techniques, and a variety of functions, you can use TFN to control any number of remote machines to generate on-demand, anonymous DoS attacks and remote shell access.

Tool	URL	Description
UDPer	http://www.packetstormsecurity.com/distributed/index4.html	A logic bomb written in ASM for Windows. It floods a victim with packets at a certain date.
webdevil	http://www.packetstormsecurity.com/distributed/index4.html	A tool used to create a distributed performance test against web servers by keeping connections alive until the server times them out. Slave daemon is included to assist in stress testing.