Links to Tools Listed in the Book

Chapter 1: Footprinting

Wget	http://www.gnu.org/software/wget/wget.html for UNIX
Teleport Pro	http://www.tenmax.com/teleport/home.htm for Windows
FerretSoft	http://www.ferretsoft.com
axfr	http://ftp.cdit.edu.cn/pub/linux/www.trinux.org/src/netmap/axfr-0.5.2.tar.gz
traceroute	ftp://ftp.ee.lbl.gov/traceroute.tar.gz
VisualRoute	http://www.visualroute.com
NeoTrace	http://www.neotrace.com/
snort	http://www.snort.org/
RotoRouter	http://packetstormsecurity.org/UNIX/loggers/rr-1.0.tgz

Chapter 2: Scanning

fping	http://packetstormsecurity.org/Exploit_Code_Archive/fping.tar.gz
Legion 2.1 from Rhino9	http://www.nmrc.org/files/snt/
SolarWinds	http://www.solarwinds.net
WS_Ping ProPack	http://www.ipswitch.com
NetScanTools	http://www.nwpsw.com
Hping	http://www.kyuzz.org/antirez/
icmpenum, from Simple Nomad	http://www.nmrc.org/files/sunix/icmpenum-1.1.1.tgz
Genius version 3.1	http://www.indiesoft.com/

BlackICE from Network ICE	http://www.networkice.com
Scanlog	http://www.openwall.com/scanlogd
Courtney1.3	http://packetstormsecurity.org/UNIX/audit/courtney-1.3.tar.Z
Ippl 1.4.10	http://pltplp.net/ippl/
Protolog 1.0.8	http://packetstormsecurity.org/UNIX/loggers/protolog-1.0.8.tar.gz
loki	http://www.phrack.org/show.php?p=51&a=6
Pingd	http://packetstormsecurity.org/UNIX/ misc/pingd-0.5.1.tgz
icmpquery	http://packetstormsecurity.org/UNIX/scanners/icmpquery.c
icmpush	http://packetstormsecurity.org/UNIX/scanners/icmpush22.tgz
Strobe	ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz
udp_scan SATAN, now called SAINT	http://wwdsilx.wwdsi.com
netcat or nc	http://www.atstake.com/research/tools/nc11nt.zip
nmap. Nmap	http://www.insecure.org/nmap
NetScanTools Pro 2000	http://www.nwpsw.com
SuperScan, from Foundstone	http://www.foundstone.com/rdlabs/termsofuse.php?filename=superscan.exe
WinScan, Prosolve	http://www.prosolve.com
Windows UDP Port Scanner	http://ntsecurity.nu
IpEye	http://ntsecurity.nu
Fscan	http://www.foundstone.com/rdlabs/termsofuse.php?filename=fscan.exe
Tcp_scan	http://wwdsilx.wwdsi.com/saint/
scanlogd	http://www.openwall.com/scanlogd/

Psionic PortSentry	http://www.psionic.com/abacus/
Psionic Logcheck	http://www.psionic.com/abacus/logcheck/
alert.sh	http://www.enteract.com/~lspitz/intrusion.html
ZoneAlarm	http://www.zonelabs.com/
Tiny Software Firewall and Security Products	http://www.tinysoftware.com
queso	http://packetstormsecurity.org/UNIX/scanners/queso-980922.tar.gz
siphon	http://www.gravitino.net/projects/siphon
Cheops	http://www.marko.net/cheops/
Tkined	http://wwwhome.cs.utwente.nl/~schoenw/scotty/

Chapter 3: Enumeration

Windows NT Resource Kit	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/
ActiveState Perl distribution for Windows	http://www.activestate.com
nbtscan	http://www.inetcat.org/software/nbtscan.html
DumpSec	http://www.somarsoft.com
Legion from the Rhino9 group	http://packetstorm.securify.com/groups/rhino9/legion.zip
NetBIOS Auditing Tool	http://www.hackingexposed.com
epdump	http://packetstormsecurity.org/NT/audit/epdump.zip
getmac and netdom	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/
netviewx	http://www.ibt.ku.dk/jesper/NTtools/
Winfo	http://www.ntsecurity.nu

Nbtdump	http://www.cerberus-infosec.co.uk/toolsn.shtml
IP Network Browser	http://www.solarwinds.net
sid2user and user2sid	http://www.chem.msu.su:8080/~rudnyi/NT/ sid.txt
enum	http://razor.bindview.com
nete	http://pr0n.newhackcity.net/~sd/
UserInfo	http://www.hammerofgod.com/download.htm
UserDump	http://www.hammerofgod.com/download.htm
GetAcct	http://www.securityfriday.com/
Samba	http://www.samba.org
Pscan	http://www.securityfocus.com/data/tools/auditing/network/pscan.c
rpcdump	http://www.atstake.com/research/tools/rpcdump.exe
Sam Spade from Blighty Design	http://samspade.org/ssw/

Chapter 4: Hacking Windows 95/98, ME, and Windows XP

AntiVirus eXpert	http://www.centralcommand.com/
Trojan Defense Suite	http://www.multimania.com/ilikeit/tds2.htm
SSBypass	http://www.amecisco.com/ssbypass.htm
ShoWin	http://www.foundstone.com/rdlabs/tools.php?category=Forensic
Unhide	http://www.webdon.com
pwltool	http://www.webdon.com
Elcomsoft's Advanced Zip Password Recovery	http://www.lostpassword.com

Chapter 5: Hacking Windows NT

NTInfoScan	http://packetstormsecurity.org/NT/audit/
NTLast and VisualLast from Foundstone, Inc.	http://www.foundstone.com
DumpEvt from Somarsoft	http://www.somarsoft.com
Centrax	http://www.cybersafe.com/
CyberCop Server	http://www.nai.com/
Desktop Sentry	http://www.foundstone.com
Intact	http://www.pedestalsoftware.com/
Intruder Alert	http://enterprisesecurity.symantec.com/products
Kane Security Monitor	http://www.securitydynamics.com/
RealSecure	http://www.iss.net
SeNTry	http://www.missioncritical.com
E Trust	http://www3.ca.com/Solutions/Product.asp?ID=163
Tripwire for NT	http://www.tripwiresecurity.com/
L0phtcrack	http://www.l0pht.com
PPTP sniffer	http://packetstormsecurity.org/sniffers/pptp-sniff.tar.gz
BOWall	http://developer.nizhny.ru/bo/eng/BOWall/
pwdump	http://www.webspan.net/~tas/pwdump2/
pwdump2	http://www.webspan.net/~tas/pwdump2/
John the Ripper	http://www.openwall.com/john/
Soon NTRK tool	ftp://ftp.microsoft.com/bussys/winnt/ winnt-public/reskit/
su from NTRK	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/
BUTTSniffer	http://packetstormsecurity.org/sniffers/buttsniffer/

Fsniff	http://www.foundstone.com
Dsniff	http://monkey.org/~dugsong/dsniff/
Secure Shell	http://www.ssh.com/download
Pretty Good Privacy	http://www.nai.com
Service Controller a NTRK tool	ftp://ftp.microsoft.com/bussys/winnt/ winnt-public/reskit/
NetBus	http://www.netbus.org
Netbus pro	http://www.multimania.com/cdc/netbus2pro.html
regdmp NTRK	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/
Back Orifice	http://www.cultdeadcow.com/tools/
Back Orifice 2000	http://sourceforge.net/projects/bo2k/
fpipe	http://www.foundstone.com
rkill.exe NTRK	ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/
Fport from Foundstone	http://www.foundstone.com
Windows NT/2000 acquired its own rootkit	http://www.rootkit.com
Tripwire	http://www.tripwire.com
BinText for Windows from Robin Keir	http://www.foundstone.com
UltraEdit32 for Windows	http://www.ultraedit.com
NTRK's auditpol	ftp://ftp.microsoft.com/bussys/winnt/ winnt-public/reskit
elsave	http://www.ibt.ku.dk/jesper/NTtools/
sfind in the Forensic Toolkit	http://www.foundstone.com/rdlabs/tools.php?category=Forensic

Chapter 6: Hacking Windows 2000/Windows Whistler Server

SMBRelay	http://pr0n.newhackcity.net/~sd/windoze.html
pwdump3e	http://www.ebiz-tech.com/html/pwdump.html
lsadump2	http://razor.bindview.com/tools/desc/lsadump2_readme.html
eLiTeWrap	http://www.holodeck.f9.co.uk/elitewrap/
Remote from the NTRK	ftp://ftp.microsoft.com/bussys/winnt/ winnt-public/reskit/

Chapter 7: Novell NetWare Hacking

Finger	ftp://ftp.cdrom.com/.1/novell/finger.zip
bindin	ftp://.edv-himmelbauer.co.at/pub/Novell.3x/TESTPROG/
nlist	http://www.nmrc.org/files/snetware/nut18.zip
chknull	http://www.nmrc.org/files/netware/chknull.zip
NDSSnoop	ftp://ftp.iae.univ-poitiers.fr/pc/netware/UTIL/ndssnoop.exe
Nwpcrack	http://www.nmrc.org/files/netware/nwpcrack.zip
Pandora	http://www.nmrc.org/pandora/download.html
Dsmaint DS411P.EXE	http://support.novell.com/servlet/filedownload/pub/ds411p.exe
Imp	http://www.wastelands.gen.nz/

Chapter 8: Hacking Unix/Linux

nessus	http://www.nessus.org
Brutus	http://www.hoobie.net/brutus/
brute_web.c	http://packetstormsecurity.org/Exploit_Code_Archive/brute_web.c
pop.c	http://packetstormsecurity.org/groups/ADM/ADM-pop.c
TeeNet	http://www.phenoelit.de/tn/
Pwscan.pl	http://razor.bindview.com/tools/vlad/index.shtml

One Time Passwords In Everything	ftp://ftp.gbnet.net/pub/security/nrl-opie/
Cracklib	http://www.users.dircon.co.uk/~crypto/download/cracklib,2.7.tgz
Npasswd	http://www.utexas.edu/cc/unix/software/npasswd/
Secure Remote Password	http://www-cs-students.stanford.edu/~tjw/srp/
Open SSH	http://www.openssh.org/
Hellkit and other shellcode creation tools	http://teso.scene.at/releases.php3
StackGuard from Immunix	http://immunix.org
Libsafe	http://www.avayalabs.com/project/libsafe/index.html
TCP Wrappers and xinetd	http://www.synack.net/xinetd/
Saint Jude	http://prdownloads.sourceforge.net/stjude/
FormatGuard	http://download.immunix.org/ImmunixOS/7.0/i386/SRPMS/glibc-2.2-12_imnx_7.src.rpm
Smap and smapd	http://www.tis.com/research/software/
Qmail	http://www.qmail.org
Postifx	http://www.postfix.com/
nfsshell	ftp://ftp.cs.vu.nl/pub/leendert/nfsshell.tar.gz
Bastille	http://www.bastille-linux.org/
md5	http://www.fourmilab.ch/md5/md5.zip
arpredirect on twister, part of the dsniff package	http://www.monkey.org/~dugsong/dsniff/
AntiSniff	http://www.securitysoftwaretech.com/antisniff/
Secure Shell	http://www.ssh.com/download/
Secure syslog from Core Labs	http://www.core-sdi.com/english/freesoft.html

Solaris Loadable Kernel Modules	http://packetstormsecurity.org/groups/thc/slkm-1.0.html
knark	http://packetstormsecurity.org/UNIX/penetration/rootkits/knark-0.59.tar.gz
adore	http://teso.scene.at/releases/adore-0.14.tar.gz.
carbonite	http://www.foundstone.com/rdlabs/proddesc/carbonite.html

Chapter 9: Dial-up, PBX, Voicemail, and VPN

THC-Scan	http://www.infowar.co.uk/thc/
PhoneSweep Sandstorm Enterprises	http://www.sandstorm.net
Telesweep	http://www.securelogix.com

Chapter 10: Network Devices

SNMPsniff	http://elektra.porto.ucp.pt/snmpsniff/snmpsniff-1.0.tar.gz
Hobbit	http://www.avian.org
ciscocrack.c	http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/ciscocrack.c.html
Palm Pilot by the L0pht's Dr. Mudge	http://www.l0pht.com~kingpin/cisco.zip
Cisco decryptor	http://www.solarwinds.net
fragrouter	http://www.anzen.com/research/nidsbench/fragrouter.html
Sniffit	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html
tcpdump 3.x	http://www-nrg.ee.lbl.gov/
linsniff	http://www.rootshell.com/
solsniff	http://www.rootshell.com/
snmpsniff from Nuno Leitao	http://nuno.leitao@convex.pt

Snort	http://www.snort.org
Ethereal	http://www.ethereal.com/
sentinel	http://www.packetfactory.net/ Projects/Sentinel/
arpwatch	ftp://ftp.ee.lbl.gov/ arpwatch-2.1a6.tar.gz

Chapter 11: Firewalls

BindView EMS/NOSadmin 4.*x* & 5.*x* v6	http://www.bindview.com
Hidden Object Locator	http://www.netwarefiles.com/utils/hobjloc.zip
port scan detection	http://www.enteract.com/~lspitz/intrusion.html
Hping	http://www.kyuzz.org/antirez/hping.html
Firewalk	http://www.packetfactory.net/projects/firewalk/
loki	http://phrack.infonexus.com/search.phtml?view&article=p49-6) (paper on the tool)
lokid	http://phrack.infonexus.com/search.phtml?view&article=p49-6) (paper on the tool)
Wietse Venema's TCP Wrappers program	ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/tcp_wrappers

Chapter 12: Denial of Service (DoS) Attacks

TFN	http://staff.washington.edu/dittrich/misc/ddos
DDOSPing	http://www.foundstone.com
Zombie Zapper	http://razor.bindview.com
find_ddos	http://www.nipc.gov
WinTrinoo by the Bindview Razor team	http://razor.bindview.com

Chapter 13: Remote Control Insecurities

nmap	http://www.insecure.org/nmap
SnadBoy	http://www.snadboy.com
SnifferPro	http://www.nai.com
Virtual Network Computing	http://www.uk.research.att.com/vnc
TSProbe	http://www.hammerofgod.com
TSEnum.exe	http://www.hammerofgod.com)
TSProbe.exe	http://www.hammerofgod.com
TSEnum.exe	http://www.hammerofgod.com

Chapter 14: Advanced Techniques

Juggernaut	http://www.packetfactory.net/
Hunt	http://lin.fsid.cvut.cz/~kra/index.html#HUNT
remote.exe NT Resource Kit	ftp://ftp.microsoft.com/bussys/winnt/ winnt-public/reskit/
BackOfficer Friendly	http://www.nfr.net/products/bof/
datapipe	http://packetstormsecurity.org/unix-exploits/tcp-exploits/datapipe.c
rinetd	http://www.boutell.com/rinetd/
fpipe	http://www.foundstone.com
The Cleaner	http://www.moosoft.com/cleaner.html
lsof	ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/NEW
MD5sum	ftp://ftp.gnu.org/ pub/gnu/textutils/
Cygwin	http://sourceware.cygnus.com/cygwin/
DumpEvt)	http://www.somarsoft.com
eLiTeWrap,	http://www.holodeck.f9.co.uk/elitewrap/index.html
UNIX rootkits	http://packetstormsecurity.org/UNIX/penetration/rootkits/
Image MASSter	http://www.ics-iq.com

OmniClone line	http://www.logicube.com
Drive Image	http://www.powerquest.com
FlashClone	http://www.ics-iq.com
ImageCast	http://www.innovativesoftware.com
Norton Ghost	http://www.symantec.com
RapiDeploy	http://www.altiris.com
VMWare	http://www.vmware.com
SecondChance	http://www.powerquest.com

Chapter 15: Web Hacking

Teleport Pro for NT	http://www.tenmax.com
Grinder v1.1	http://hackersclub.com/km/files/hfiles/rhino9/grinder11.zip
whisker by Rain.forest.puppy	http://www.wiretrip.net/rfp/
hk.exe from Todd Sabin	http://www.nmrc.org
iishack	http://www.technotronic.com
SSLProxy	http://www.kuix.de/sslproxy/
SSLdump	http://www.rtfm.com/ssldump/

Chapter 16: Hacking the Internet User

SpyNet/PeepNet	http://www.packetstormsecurity.com/
Cookie Pal from Kookaburra Software	http://www.kburra.com/cpal.html
mpack	http://www.21st-century.net/Pub/Utilities/Archivers/
passdump by janker	http://www.hackersclub.com/km/files/hfiles/
Wrapster, by Octavian	http://download.cnet.com
Finjan's SurfinGate technology	http://www.finjan.com