Information Security - Tools of the Trade

Sajeev Nair
CEH, GCFW, GCWN, CCNP
mlist[at]networkpentest.com

This is a compilation of a variety of tools that has proven useful for various security assessment / penetration testing assignments. Some of the tools listed here may appear in multiple categories and there may be other tools which may do the same job, I leave that to the reader's judgment.

Tool Category	Tool	Link
Passive Intelligence gathering	Google	http://Google.com
	samspade	http://samspade.org/
	netcraft	http://netcraft.com
	web archive	http://www.archive.org/
	edgar	http://www.sec.gov/edgar.shtml
	wikto (with GHDB)	http://www.sensepost.com/research/wikto/
	Whois, dig	Unix tools
Web Anonymizer	Tor	http://tor.eff.org
Wardialers	Phonesweep	http://www.sandstorm.net/
	THC-Scan	http://www.thc.org
Ping Tools	Angry IP scanner	http://www.angryziber.com/ipscan/
	WS_ping_propack	http://www.ipswitch.com/
	Superscan	http://foundstone.com/
	NMAP	http://insecure.org/
Traceroute tools	Trout	http://foundstone.com/
	Visualroute	http://www.visualroute.com/
	tcptraceroute	http://michael.toren.net/code/tcptraceroute/
Router / Firewall enumeration	Hping2	http://www.hping.org/
	NMAP	http://insecure.org/
	Firewalk	http://packetfactory.net
Scanning	NMAP	http://insecure.org/
	Superscan	http://foundstone.com/
	Unicornscan	http://www.unicornscan.org/
	SMTP Relay scanner	http://www.cirt.dk/tools/relayscanner/
	scanssh	http://www.monkey.org/%7Eprovos/scanssh/
	Txdns	http://www.txdns.net/
	Ike-scan	http://www.nta-monitor.com/tools/ike-scan/
	PBNJ	http://pbnj.sourceforge.net/
Banner grabber	Netcat	http://www.vulnwatch.org/netcat/
	scanline	http://foundstone.com/
Passive fingerprinting	P0f	http://lcamtuf.coredump.cx/p0f.shtml
Active fingerprinting	Xprobe2	http://www.sys-security.com/index.php?page=xprobe

	NMAP	http://insecure.org/
	AMAP	http://www.thc.org
Windows Enumeration	user2sid & sid2user	http://evgenii.rudnyi.ru/soft/sid/
	dumpsec	http://www.somarsoft.com/
	LDP	Resource kit tool
	superscan	http://foundstone.com/
	Cain & abel	http://www.oxid.it/cain.html
	CredDigger	http://foundstone.com/
	Pstools	http://www.sysinternals.com/Utilities/PsTools.html
SNMP tools	SolarWinds	http://www.solarwinds.net
	SNMPUtil	Resource Kit tool
	SNScan	http://www.foundstone.com/resources/proddesc/snscan.htm
	Cain & abel	http://www.oxid.it/cain.html
	net-snmp	http://net-snmp.sourceforge.net/
	ADMsnmp	http://examples.oreilly.com/networksa/tools/
Vulnerability Assessment	Nessus	http://www.nessus.org/
	GFI Languard	http://www.gfi.com/lannetscan/
	Retina	http://www.eeye.com
	Core Impact	http://www.coresecurity.com
	Cisco torch	http://www.arhont.com/
Application level scanner	Wikto	http://www.sensepost.com/research/wikto/
	Webinspect	http://www.spidynamics.com/products/webinspect/
	Paros	http://www.parosproxy.org
	Nessus	http://www.nessus.org/
Offline browser / site ripper	Teleport pro	http://tenmax.com
	wget	http://www.gnu.org/software/wget/
Web proxy	Paros	http://www.parosproxy.org
	Burp proxy	http://portswigger.net/proxy/
Password audit / cracker	NAT	http://www.cotse.com/tools/netbios.htm
	Cain & Abel	http://www.oxid.it/cain.html
	Kerbcrack	http://ntsecurity.nu/toolbox/kerbcrack/
	THC-Hydra	http://thc.org
	pwdump	http://www.foofus.net/fizzgig/pwdump/
	John	http://www.openwall.com/john/
	ophcrack	http://ophcrack.sourceforge.net/
SQL tools	SQLDict	http://ntsecurity.nu/toolbox/sqldict/
	Database tools	http://www.cqure.net/wp/
	Paros	http://www.parosproxy.org
	THC-Hydra	http://thc.org
	NGSSQuirreL	http://www.ngssoftware.com

Source Code scanner	Flaw finder	http://www.dwheeler.com/flawfinder/
	RATS	http://www.securesoftware.com
	SLAM	http://research.microsoft.com/slam
Vulnerability / exploit research	securityfocus	http://www.securityfocus.com
	secunia	http://secunia.com/
	milw0rm	http://milw0rm.com/
	packtstorm	http://packetstormsecurity.org
	SANS	http://isc.sans.org
	securiteam	http://www.securiteam.com/
	secwatch	http://secwatch.org/
	WVE	http://wve.org
	OSVDB	http://www.osvdb.org/
Vulnerability exploitation	Metasploit	http://www.metasploit.com/
	Core Impact	http://www.coresecurity.com
	CGE	http://www.vulnerabilityassessment.co.uk/cge.htm
Traffic monitor	EtherApe	http://etherape.sourceforge.net/
	SolarWinds	http://www.solarwinds.net
Sniffers	Wireshark	http://www.wireshark.org/
	Tcpdump	http://www.tcpdump.org/
	dsniff	http://www.monkey.org/~dugsong/dsniff/
	Cain	http://www.oxid.it/cain.html
	NGSsniff	http://www.ngssoftware.com
	Ettercap	http://ettercap.sourceforge.net/
Port redirectors	Fpipe	http://foundstone.com/
	Netcat / cryptcat	http://www.vulnwatch.org/netcat/
Packet crafting	Hping2	http://www.hping.org/
MAC flooding	Etherflood	http://ntsecurity.nu/toolbox/etherflood/
	Macof	http://www.monkey.org/~dugsong/dsniff/
MAC spoofer	SMAC	http://www.klcconsulting.net/smac/
ARP spoofing / MitM attacks	Ettercap	http://ettercap.sourceforge.net/
	Cain & Abel	http://www.oxid.it/cain.html
	dsniff	http://www.monkey.org/~dugsong/dsniff/
Layer 2 attacks	Yersinia	http://www.yersinia.net/
Trojans / Rootkits	BackOrifice	http://www.bo2k.com/
	Tini	http://ntsecurity.nu/toolbox/tini/
	Netcat	http://www.vulnwatch.org/netcat/

Covert channels	Loki	http://www.packetstormsecurity.org
	ACKCMD	http://www.ntsecurity.nu/toolbox/ackcmd/
	Netcat	http://www.vulnwatch.org/netcat/
log erasers	auditpol	Resource Kit tool
	winzapper	http://ntsecurity.nu/toolbox/winzapper/
	Unix log wipers	http://packetstormsecurity.org/UNIX/penetration/log-wipers/
Rootkit detection	chkrootkit	http://www.chkrootkit.org
	Rootkit Hunter	http://www.rootkit.nl/projects/rootkit_hunter.html
	RootkitRevealer	http://www.sysinternals.com
Wrapping tools	Elitewrap	http://homepage.ntlworld.com/chawmp/elitewrap/
	Restorator	http://www.bome.com/Restorator/
DoS tools	TFN2K	http://www.packetstormsecurity.org/distributed
	stacheldraht	http://www.packetstormsecurity.org/distributed
	Mstream	http://www.packetstormsecurity.org/distributed
Keystroke loggers	keyghost	www.keyghost.com
	FakeGina	http://ntsecurity.nu/toolbox/fakegina/
	Eblaster	http://www.eblaster.com/
Process Viewer	Tlist	Resource kit tool
	Inzider	http://ntsecurity.nu/toolbox/inzider/
	TCPview	http://www.sysinternals.com/Utilities/TcpView.html
	lsof	ftp://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/
Bootable OS	NTFSDOS	http://www.sysinternals.com/Utilities/NtfsDos.html
	Auditor	http://www.remote-exploit.org
	BackTrack	http://www.remote-exploit.org
Cookie viewing	cookie viewer	http://www.karenware.com/powertools/ptcookie.asp
IDS evasion	Mendax	http://www.packetstormsecurity.org
ADS detection tools	sfind	http://foundstone.com/
	LNS	http://ntsecurity.nu/toolbox/lns/
Steganography	Imagehide	http://www.dancemammal.com/
	S-Tools	ftp://idea.sec.dsi.unimi.it/pub/security/crypt/code/
Wireless Detection / Sniffer	Kismet	http://www.kismetwireless.net/
	Netstumbler	http://www.netstumbler.com/
	Wireshark	http://www.wireshark.org/
Wireless key cracking	Aircrack-ng	www.aircrack-ng.org

	wepattack	http://wepattack.sourceforge.net/
	cowPatty	http://www.churchofwifi.org/
	asleap	http://asleap.sourceforge.net/
	wepwedgie	http://sourceforge.net/projects/wepwedgie/
Wireless packet crafting	file2air	http://802.11ninja.net/code/file2air-1.0RC1.tgz
	airjack	http://sourceforge.net/projects/airjack/
Wireless Honeypots	Karma	http://www.theta44.org/karma/
	FakeAP	http://www.blackalchemy.to/project/fakeap/
Wireless DoS tools	void11	http://www.wlsec.net/void11/
	file2air	http://802.11ninja.net/code/file2air-1.0RC1.tgz
	airjack	http://sourceforge.net/projects/airjack/
Bluetooth tools	Redfang	http://www.net-security.org/software.php?id=519
	Bluesniff	http://bluesniff.shmoo.com/
	Btscanner	http://www.pentest.co.uk/
	BT audit	http://trifinite.org/trifinite_stuff_btaudit.html