APPENDIX A

Tool, Sites, and References

Greetings, dear reader, and welcome to the best appendix you've ever read—or at least the most useful for your CEH exam, anyway. This appendix is filled with all the tools, websites, and write-ups I could think of that will help you become a better ethical hacker. Keep in mind I'm not providing a recommendation for, approval of, or security guarantee on any website or link you'll find here. Neither I nor my beloved publisher can be held liable for anything listed here. For example, URLs change, pages become outdated with time, tools become obsolete when new versions are released, and so on. Not to mention that, as I clearly pointed out in the text, you need to be very, very careful with some of this stuff: Your antivirus system will no doubt explode with activity simply by *visiting* some of these sites. I highly recommend you create a virtual machine or use a stand-by system to download to and test tools from.

These websites and tools are listed here because they will help you in your study efforts for the exam and further your professional development. I purposely did not provide tools on a CD, because it is important that you learn how to find and install what you're looking for. You're entering the big leagues now, so you simply need to know how it's really done.

Vulnerability Research Sites

- **National Vulnerability Database** nvd.nist.gov
- **SecurityTracker** www.securitytracker.com
- **SecuriTeam** www.securiteam.com
- **Secunia** www.secunia.com
- **Hackerstorm Vulnerability Database Tool** www.hackerstrom.com
- **HackerWatch** www.hackerwatch.org
- **SecurityFocus** www.securityfocus.com
- ***Security* Magazine** www.securitymagazine.com
- ***SC Magazine*** www.scmagazine.com
- **Exploit Database** www.exploit-db.com

Footprinting Tools

Website Research Tools

- **Netcraft** http://news.netcraft.com
- **Webmaster** http://webmaste-a.com/link-extractor-internal.php
- **iWEBTOOL** www/iwebtool.com
- **Archive** www.archive.org

DNS and WHOIS Tools

- **Nslookup**
- **Sam Spade** www.samspade.org
- **WebFerret** www.webferret.com
- **ARIN** www.whois.arin.net
- **DomainTools** www.domaintools.com
- **Network Solutions** www.networksolutions.com
- **WhereISIP** www./whereisipjufsoft.com/
- **DNSstuff** www.dnsstuff.com
- **BetterWhois** www.betterwhois.com/
- **DNS-Digger** http://dnsdigger.com
- **SpyFu** www.spyfu.com
- **Dig** www.isc.org/software/bind

NOTE Download BIND 9 or above—BIND 9.2.1 is a 1.28MB self-extracting ZIP file. When the download completes, extract the BIND files and copy them into an empty directory. Then install BIND by running the BINDINSTALL.EXE file—dig is part of the install.

Traceroute Tools and Links

- **VisualRoute Trace** www.visualware.com
- **3d Visual Route** http://3ndsmp.com
- **VisualIPTrace** www.visualiptrace.com

- **Trout** www.foundstone.com
- **PingPlotter** http://pingplotter.com
- **Path Analyzer Pro** www.pathanalyzer.com

Website Mirroring Tools and Sites

- **BlackWidow** http://softbytelabs.com
- **Reamweaver** http://reamweaver.com
- **Wget** http://www.gnu.net/s/wget
- **Teleport Pro** http://www.tenmax.com/teleport/pro/home.htm
- **Archive** www.archive.org
- **Google cache**

E-mail Tracking

- **eMailTrackerPro** www.emailtrackerpro.com
- **PoliteMail** www.politemail.com

Google Hacking

- **Google Hacking Database** www.hackersforcharity.org/ghdb/
- **Google Hacks** http://code.google.com/p/googlehacks/
- **Google Hacking Master List** http://it.toolbox.com/blogs/managing-infosec/google-hacking-master-list-28302

Scanning and Enumeration Tools

Ping Sweep

- **Angry IP Scanner** www.angryip.org
- **Colasoft Ping** http://colasoft.com
- **Ultra Ping Pro** http://ultraping.webs.com
- **Ping Scanner Pro** www.digilextechnologies.com
- **MegaPing** www.magnetosoft.com
- **Friendly Pinger** www.kilievich.com

Scanning Tools

- **SuperScan** www.foundstone.com
- **Nmap (ZenMap)** http://nmap.org/
- **NetScan Tools Pro** www.netscantools.com
- **Hping** www.hping.org
- **LAN Surveyor** www.solarwinds.com
- **MegaPing** www.magnetosoft.com
- **NScan** www.nscan.hypermart.net
- **Infilitrator** www.infiltration-systems.com
- **Netcat** http://netcat.sourceforge.net
- **IPEye** http://ntsecurity.nu
- **THC-Amap** www.thc.org

War Dialing

- **THC-SCAN** http://www.thc.org/thc-tsng/
- **TeleSweep** www.securelogix.com
- **ToneLoc** www.securityfocus.com/tools/48
- **PAWS** www.wyae.de
- **WarVOX** http://warvox.org/

Banner Grabbing

- **Telnet**
- **ID Serve** www.grc.com
- **Netcraft** http://netcraft.com
- **Xprobe** http://sourceforge.net/apps/mediawiki/xprobe/index.php?title=Main_Page
- **THC-AMAP** http://freeworld.thc.org

Vulnerability Scanning

- **Nessus** www.nessus.org
- **SAINT** http://saintcorporation.com
- **GFI LanGuard** www.gfi.com

- **Retina** http://eeye.com
- **Core Impact** www.coresecurity.com
- **MBSA** http://technet.microsoft.com
- **Nikto** http://cirt.net/nikto2
- **WebInspect** http://download.spidynamics.com/webinspect/default.htm
- **GFI Languard** www.gfi.com/lannetscan/

Proxy, Anonymizer, and Tunneling

- **Tor** https://www.torproject.org/
- **ProxyChains** http://proxychains.sourceforge.net/
- **SoftCab** www.softcab.com/proxychain/index.php
- **Proxifier** www.proxifier.com
- **HTTP Tunnel** www.http-tunnel.com
- **Anonymouse** http://anonymouse.org/
- **Anonymizer** http://anonymizer.com
- **Psiphon** http://psiphon.ca

Enumeration

- **PSTools** http://technet.microsoft.com
- **P0f** http://lcamtuf.coredump.cx/p0f.shtml
- **SuperScan** www.foundstone.com
- **User2Sid/Sid2User** www.svrops.com/svrops/dwnldutil.htm
- **SNMP Scanner** www.secure-bytes.com
- **NSauditor** www.nsauditor.com
- **SolarWinds** www.solarwinds.com
- **LDAP Admin** www.ldapsoft.com
- **LEX** www.ldapexplorer.com
- **Ldp.exe** www.microsoft.com
- **User2Sid/Sid2User** http://windowsecurity.com
- **SNMPUTIL** www.wtcs.org
- **IP Network Browser** www.solarwinds.com
- **Xprobe** www.sys-security.com/index.php?page=xprobe

System Hacking Tools

Password Hacking Tools

- **Cain** www.oxid.it
- **John the Ripper** www.openwall.com
- **LCP** www.lcpsoft.com
- **THC-Hydra** http://www.thc.org/thc-hydra/
- **ElcomSoft** www.elcomsoft.com/
- **Lastbit** http://lastbit.com/
- **Ophcrack** http://ophcrack.sourceforge.net
- **Aircrack** www.aircrack-ng.org/
- **Rainbow crack** www.antsight.com/zsl/rainbowcrack/
- **Brutus** www.hoobie.net/brutus/
- **Windows Password Recovery** www.windowspasswordsrecovery.com
- **KerbCrack** http://ntsecurity.nu

Sniffing

- **Wireshark** www.wireshark.org/
- **Ace** www.effetech.com
- **KerbSniff** http://ntsecurity.nu
- **Ettercap** http://ettercap.sourceforge.com

Keyloggers and Screen Capture

- **KeyProwler** www.keyprowler.com
- **Handy Key Logger** www.handy-keylogger.com
- **Actual Keylogger** www.actualkeylogger.com
- **Actual Spy** www.actualspy.com
- **Ghost** www.keylogger.net
- **Hidden Recorder** www.oleansoft.com
- **IcyScreen** www.16software.com
- **DesktopSpy** www.spyarsenal.com
- **USB Grabber** http://digitaldream.persiangig.com

Covering Tracks

- **ELsave** www.ibt.ku.dk
- **EraserPro** www.acesoft.net
- **WindowWasher** www.webroot.com
- **Auditpol** www.microsoft.com
- **WinZapper** www.ntsecurity.nu
- **Evidence Eliminator** www.evidence-eliminator.com

Packet Crafting/Spoofing

- **Komodia** www.komodia.com
- **Hping2** www.hping.org/
- **PackEth** http://sourceforge.net
- **Packet generator** http://sourceforge.net
- **Netscan** http://softperfect.com
- **Scapy** www.secdev.org/projects/scapy/
- **Nemesis** http://nemesisi.sourceforge.net

Session Hijacking

- **Paros Proxy** www.parosproxy.org/
- **Burp Suite** http://portswigger.net
- **Firesheep** http://codebutler.github.com
- **Hamster/Ferret** http://erratasec.blogspot.com/2009/03/hamster-20-and-ferret-20.html
- **Ettercap** http://ettercap.sourceforge.net
- **Hunt** http://packetstormsecurity.com

Cryptography and Encryption

Encryption Tools

- **TrueCrypt** www.truecrypt.org
- **BitLocker** http://microsoft.com
- **DriveCrypt** www.securstar.com

Hash Tools

- **MD5 Hash** www.digitalvolcano.co.uk/content/md5-hash
- **HashCalc** http://nirsoft.net

Steganography

- **ImageHide** www.dancemammal.com
- **gifShuffle** www.darkside.com.au
- **QuickStego** www.quickcrypto.com
- **EZStego** www.stego.com
- **Open Stego** http://openstego.sourceforge.net/
- **S Tools** http://spychecker.com
- **JPHIDE** http://nixbit.com
- **wbStego** home.tele2.at/wbailer/**wbstego**/
- **MP3Stegz** http://sourceforge.net
- **OurSecret** www.securekit.net
- **OmniHidePro** http://omnihide.com
- **AudioStega** www.mathworks.com
- **StegHide** http://steghide.sourceforge.net
- **XPTools** www.xptools.net

Cryptanalysis

- **Cryptanalysis** http://cryptanalysisto.sourceforge.net
- **Cryptobench** http://addario.org
- **EverCrack** http://evercrack.sourceforge.net

Sniffing

Packet Capture

- **Wireshark** http://wireshark.org
- **CACE** www.cacetech.com

- **tcpdump** http://tcpdump.org
- **Capsa** www.colasoft.com
- **OmniPeek** www.wildpackets.com
- **NetWitness** www.netwitness.com
- **Windump** www.winpcap.org
- **dsniff** http://monkey.org
- **EtherApe** http://etherape.sourceforge.net

Wireless

- **Kismet** www.kismetwireless.net
- **NetStumbler** www.netstumbler.net

MAC Flooding/Spoofing

- **Macof** http://www.irongeek.com/i.php?page=backtrack-3-man/macof (Linux tool)
- **SMAC** www.klcconsulting.net

ARP Poisoning

- **Cain** www.oxid.it
- **UfaSoft** http://ufasoft.com
- **WinARP Attacker** http:www.xfocus.net

Trojans and Malware

Wrappers

- **EliteWrap** http://homepage.ntlworld.com

Monitoring Tools

- **HiJackThis** http://free.antivirus.com
- **What's Running** www.whatsrunning.net
- **CurrPorts** www.nirsoft.net

- **SysAnalyzer** http://labs.idefense.com
- **Regshot** http://sourceforge.net/projects/regshot
- **Driver Detective** www.driveshq.com
- **SvrMan** http://tools.sysprogs.org
- **ProcessHacker** http://processhacker.sourceforge.net
- **Fport** www.foundstone.com/knowledge/proddesc/fport.html

Attack Tools

- **Netcat** http://netcat.sourceforge.net
- **Nemesis** www.packetfactory.net/projects/nemesis/

IDS

- **Snort** www.snort.org

Evasion Tools

- **ADMutate** http:// www.ktwo.ca
- **NIDSBench** http:// PacketStormsecurity.org/UNIX/IDS/nidsbench/
- **IDSInformer** http:// www.net-security.org
- **Inundator** http://inundator.sourceforge.net

Wireless

- **WIGLE** http://wiggle.net
- **AirPcap** www.cacetech.com
- **Madwifi** http://madwifi-project.org
- **Kismet** www.kismetwireless.net
- **NetStumbler** www.netstumbler.com
- **AirMagnet WiFi Analyzer** http://airmagnet.com
- **Airodump** http:// Wirelessdefence.org/Contents/Aircrack_airodump.htm
- **Aircrack** http:// www.Aircrack-ng.org

- **AirSnort** http://airsnort.shmoo.com/
- **BT Browser** http:// www.BluejackingTools.com
- **BlueScanner** http://sourceforge.net
- **Bluediving** http://bluediving.sourceforge.net
- **SuperBlueTooth Hack** www.brothersoft.com
- **KisMAC** http://kismac.de/
- **NetSurveyor** http://performancewifi.net
- **inSSIDer** www.metageek.net
- **WiFi Pilot** http://cacetech.com
- **OmniPeek** http://wildpackets.com

Web Attacks

- **Wfetch** http://microsoft.com
- **Httprecon** www.computec.ch
- **ID Serve** http:www.grc.com
- **WebSleuth** http://sandsprite.com
- **BlackWidow** http://softbytelabs.com
- **cURL** http://curl.haxx.ce
- **CookieDigger** www.foundstone.com
- **WebScarab** http://owasp.org
- **Nstalker** http://nstalker.com
- **NetBrute** www.rawlogic.com

SQL Injection

- **BSQL Hacker** http://labs.portcullis.co.uk
- **Marathon** http://marathontool.codeplex.com
- **Havil** http://itsecteam.com
- **SQL Injection Brute** http://code.google.com
- **SQL Brute** http://gdssecurity.com
- **SQLNinja** http://sqlninja.sourceforge.net
- **SQLGET** http://darknet.ord.uk

Miscellaneous

Pen Test Suites

- **Core Impact** www.coresecurity.com
- **CANVAS** http://immunitysec.com
- **Metasploit** www.metaspolit.org
- **Armitage** www.fastandeasyhacking.com
- **Codenomicon** http://codenomicon.com

Extras

- **SysInternals** www.microsoft.com/technet/sysinternals/default.mspx
- **Tripwire** www.tripwire.com/
- **Core Impact Demo** https://coresecurity.webex.com/ec0605lc/eventcenter/recording/recordAction.do;jsessionid=l2T1N8Lc1nQ6HHsxy0qcv8NxyFT2kVGvBB5LJq6c2mM6X9v2Q9PK!1120902094?theAction=poprecord&actname=%2Feventcenter%2Fframe%2Fg.do&apiname=lsr.php&renewticket=0&renewticket=0&actappname=ec0605lc&entappname=url0107lc&needFilter=false&&isurlact=true&entactname=%2FnbrRecordingURL.do&rID=12649862&rKey=ab1a8bb5a77fe5d3&recordID=12649862&rnd=7966714724&siteurl=coresecurity&SP=EC&AT=pb&format=short

Linux Distributions

- **Distrowatch** http://distrowatch.com
- **BackTrack** www.remote-exploit.org/index.php/BackTrack

Tools, Sites, and References Disclaimer

All URLs listed in this appendix were current and live at the time of publication. McGraw-Hill makes no warranty as to the availability of these World Wide Web or Internet pages. McGraw-Hill has not reviewed or approved the accuracy of the contents of these pages and specifically disclaims any warranties of merchantability or fitness for a particular purpose.