Les outils de sécurité

Top Tools

List:

Kali (formerly BackTrack): http://www.kali.org/. "From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system."

NMAP: http://nmap.org/. "Nmap (”Network Mapper”) is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Nmap runs on most types of computers and both console and graphical versions are available. Nmap is free and open source."

Nessus Remote Security Scanner: Nessus: [/b]http://www.tenable.com/products/nessus. "Nessus is the world’s most popular vulnerability scanner used in over 75,000 organizations world-wide. Many of the world’s largest organizations are realizing significant cost savings by using Nessus to audit business-critical enterprise devices and applications."

Nikto: http://www.cirt.net/nikt02. "Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired)."

Wireshark: http://www.wireshark.org/. "Wireshark is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Wireshark features that are missing from closed-source sniffers."

Cain & Abel: http://www.oxid.it/cain.html. "Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols."

Kismet: http://www.kismetwireless.net/. "Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic."

Fingerprinting and Reconnaissance

Before you begin an attack, there should be a fair amount of planning and reasearch towards the target so you are not using all the tools blindly. This step involves accumulating data regarding a specific network environment, usually for the purpose of finding ways to intrude into the environment. Footprinting can reveal system vulnerabilities and improve the ease with which they can be exploited. These are some tools that can assist in the information gathering, however, allot of information does not exist on this page. For example, when getting information, such as a webserver, you can try to telnet into the device and see if a banner is returned when the telnet fails. For reconnaissance, you can search public forums, job postings, social networking accounts, and etc. Let's say that you perform a whois on a domain name and receive a generic email. The bounceback email might contain a specific name to an individual within that company. Using that information, you can explore different avenues of attack.

Collect Location Information Tools:

Google Earth: http://www.google.com/earth/index.html

DNS Interrogation Tools:

DNSData View: http://www.nirsoft.net

Email Tracking Tools:

eMailTrackerPro: http://www.emailtrackerpro.com
PoliteMail: http://www.politemail.com
Super Email Marketing Software: http://www.bulk-email-marketing-software.net
MSGTAG: http://www.msgtag.com/download/free/
Zendio: http://www.zendio.com/download

Google hacking Tools:

GMapCatcher: http://code.google.com
SiteDigger: http://www.mcafee.com
SearchDiggity: http://www.stachliu.com
Google Hacks: http://code.google.com
Google Hack Honeypot: http://ghh.sourceforge.net
BiLE Suite: http://www.sensepost.com
MetaGoofil: http://www.edge-security.com

Monitoring Web Updates Tools:

WebSite-Watcher: http://aignes.com/download.htm

Traceroute Tools:

Network Pinger: http://www.networkpinger.eom/en/downloads/#download
Magic NetTrace:
http://www.tialsoft.com/download/…
GEO Spider: http://oreware.com/viewprogram.php?prog=22
3D Traceroute: http://www.d3tr.de/download.html

Website Footprinting Tools:

Burp Suite: http://portswigger.net/burp/download.html
Zaproxy: https://code.google.eom/p/zaproxy/downloads/list

Website Mirroring Tools:

HTTrack Website Copier: http://www.httrack.c0m/page/2/
BlackWidow: http://softbytelabs.com/us/downloads.html
Webripper: http://www.calluna-software.com/Webripper
SurfOffline: http://www.surfoffline.com/
Website Ripper Copier: http://www.tensons.com/products/websiterippercopier/
GNU Wget: ftp://ftp.gnu.org/gnu/wget/

WHOIS Lookup Tools:

ActiveWhois: http://www.johnru.com/
Whois Lookup Multiple Addresses: http://www.sobolsoft.com/
WhoisThisDomain: http://www.nirsoft.net/utils/whois_this_domain.html
Whois Analyzer Pro: http://www.whoisanalyzer.com/download.opp

Other Links:

Extract Website Information from archive.org, Available from www.archive.org
Regional Internet Registry: http://en.wikipedia.org/wiki/Regional_lnternet_Registry
Email Lookup - Free Email Tracker: http://www.ipaddresslocation.org
Read Notify: http://www.readnotify.com
Pointofmail: http://www.pointofmail.com
DidTheyReadlt: http://www.didtheyreadit.com
Trace Email: http://whatismyipaddress.com/trace-email
myDNSTools: http://www.mydnstools.info/nslookup
DNSWatch: http://www.dnswatch.info
DomainTools: http://www.domaintools.com

Scanning Networks

Network Scanning is the process of examining the activity on a network, which can include monitoring data flow as well as monitoring the functioning of network devices. Network Scanning serves to promote both the security and performance of a network. Network Scanning may also be employed from outside a network in order to identify potential network vulnerabilities. This step is usually very "loud" and if done inproperly, can get you caught. During this phase, you are trying to determine which ports are open and which services are open. For example, if you determine port 80 is open, you can try to launch web service attacks. If you learn that the webserver is Apache, then you can launch attacks that is specifically for Apache.

Anonymizers:

Anonymous Web Surfing Tool: http://www.anonymous-surfing.com
G-Zapper: http://www.dummysoftware.com/gzapper.html
Hide Your IP Address: http://www.hideyouripaddress.net
Hide My IP: http://www.privacy-pro.com/features.html
Spotflux: http://www.spotflux.com

Banner Grabbing Tools:

ID Serve: http://www.grc.com
Netcat: http://sourceforge.net/projec…/netcat/files/latest/download…

Censorship Circumvention Tools:

Psiphon: http://psiphon.ca
Your-Freedom: http://www.your-freedom.net

Custom Packet Creator:

Colasoft Packet Builder:
http://www.colasoft.com/…/produ…/download_packet_builder.php

Network Discovery and Mapping Tools:

CartoReso: http://cartoreso.campus.ecp.fr
FriendlyPinger: http://www.kilievich.com/fpinger/download.htm
Spiceworks-Network Mapper: http://www.spiceworks.com/download/
Switch Center Enterprise: http://www.lan-secure.c0m/d0wnl0ads.htrn#netw0rk
LANsurveyor:
http://www.solarwinds.com/register/MoreSoftware.aspx…
92&c=70150000OOOPjNE
OpManager: http://www.manageengine.com/network-monitoring/download.html
NetworkView: http://www.networkview.com/html/download.html
The Dude: http://www.mikrotik.com/thedude
LANState: http://www.10-strike.com/lanstate/download.shtml

Packet Crafter Tool:

Hping3: http://www.hping.org/hping3.html

Ping Sweep Tools:

Angry IP Scanner: http://angryip.0rg/w/D0wnl0ad
SolarWinds Engineer's Toolset:
http://downloads.solarwinds.com/…/Rele…/Toolset/ZPToolset/ZP-Toolset-Ol.html
Colasoft Ping Tool:
http://www.colasoft.com/dow…/products/download_ping_tool.php
Visual Ping Tester - Standard: http://www.pingtester.net
Ping Scanner Pro: http://www.digilextechnologies.com
Network Ping: http://www.greenline-soft.com/product_network_ping/index.aspx
Ultra Ping Pro: http://ultraping.webs.com/downloads.htm
Ping Monitor: http://www.niliand.com
PinglnfoView: http://www.nirsoft.net/utils/multiple_ping_tool.html
Pinkie: http://www.ipuptime.net/category/download/

Proxy Tools:

ezProxy: https://www.0clc.0rg/ezpr0xy/d0wnl0ad.en.h.tml
Charles: http://www.charlesproxy.com/
JAP Anonymity and Privacy: http://anon.inf.tu-dresden.de/win/download_en.html
UltraSurf: http://www.ultrasurf.us
CC Proxy Server: http://www.youngzsoft.net/ccproxy/proxy-server-download.htm
WideCap: http://widecap.ru
FoxyProxy Standard: https://addons.mozilla.org
ProxyCap: http://www.proxycap.com
TOR (The Onion Routing): https://www.torproject.org/download/download

Scanning Tools:

IP Tools: http://www.ks-soft.net/ip-tools.eng/downpage.htm
Advanced Port Scanner:
http://www.radmin.com/down…/previousversions/portscanner.php
MegaPing: http://www.magnetosoft.com/p…/megaping/megaping_features.htm
Netifera: http://netifera.com
Network Inventory Explorer: http://www.10-strike.com/networkinventoryexplor…/download.shtml.References
Free Port Scanner:
http://www.nsauditor.eom/network_to…/free_port_scanner.html…
NMAP: http://nmap.org/
Global Network Inventory Scanner:
http://www.magnetosoft.com/…/global_networ…/gni_features.htm
Net Tools: http://mabsoft.com/nettools.htm
SoftPerfect Network Scanner: http://www.softperfect.com/products/networkscanner/

Tunneling Tools:

Super Network Tunnel: http://www.networktunnel.net
HTTP-Tunnel: http://www.http-tunnel.com
Bitvise: http://www.bitvise.com

Vulnerability Scanning Tools:

GFI LanGuard: http://www.gfi.com/downloads/mirrors.aspx?pid=lanss

Nessus: http://www.tenable.com/products/nessus

MBSA: http://www.microsoft.com/en-us/download/details.aspx?id=7558

Nsauditor Network Security Auditor: http://www.nsaudit0r.c0m/net…/netw0rk_security_audit0r.html…

Lzvrw

Security Auditor's Research Assistant (SARA): http://www-arc.com/sara/

Security Manager Plus: http://www.manageengine.com/products/securitymanager/ download, html

System Hacking

Anti Keyloggers:

CoDefender: https://www.encassa.com/downloads/default.aspx

DataGuard AntiKeylogger Ultimate: http://www.maxsecuritylab.com/dataguard-antikeylogger/download-anti-keyloger.php

PrivacyKeyboard: http://www.privacykeyboard.com/privacy-keyboard.html

Elite Anti Keylogger: http://www.elite-antikeylogger.com/free-download.html

Anti-Rootkits:

Stinger: http://www.mcafee.com/us/downloads/free-tools/how-to-use-stinger.aspx

UnHackMe: http://www.greatis.com/unhackme/download.htm

Virus Removal Tool: http://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx

Hypersight Rootkit Detector: http://northsecuritylabs.com/

Avira Free Antivirus: http://www.avira.com/en/avira-free-antivirus

Anti-Spywares:

MacScan: http://macscan.securemac.com/

Spybot - Search & Destroy: http://www.safer-networking.org/dl/

Malwarebytes Anti-Malware PRO: http://www.malwarebytes.org/products/malwarebytes_pro/

SpyHunter: http://www.enigmasoftware.com/products/

SUPERAntiSpyware: http://superantispyware.com/index.html

Spyware Terminator 2012: http://www.pcrx.com/spywareterminator/

Covering Tracks Tools:

CCIeaner: http://www.piriform.com/download

MRU-Blaster: http://www.brightfort.com/mrublaster.html

Wipe: http://privacyroot.com/software/www/en/wipe.php

Tracks Eraser Pro: http://www.acesoft.net/features.htm

BleachBit: http://bleachbit.sourceforge.net/news/bleachbit-093

AbsoluteShield Internet Eraser Pro: http://www.internet-track-eraser.com/ineteraser.php

Clear My History: http://www.hide-my-ip.com/clearmyhistory.shtml

EvidenceEraser: http://www.evidenceeraser.com/

WinTools.net Professional: http://www.wintools.net/

RealTime Cookie & Cache Cleaner (RtC3): http://www.kleinsoft.co.za/buy.html

AdvaHist Eraser: http://www.advacrypt.cjb.net/

Free Internet Window Washer: http://www.eusing.com/Window_Washer/Window_Washer.htm

Keyloggers:

StaffCop Standard: http://www.staffcop.com/download/

iMonitorPC: http://www.imonitorpc.com/

PC Activity Monitor Standard: http://www.pcacme.com/download.html

KeyProwler: http://keyprowler.com/download.aspx

Keylogger Spy Monitor: http://ematrixsoft.com/download.php?p=keylogger-spy-monitor-software

REFOG Personal Monitor: http://www.refog.com/personal-monitor.html

Actual Keylogger: http://www.actualkeylogger.com/download-free-key-logger.html

Spytector: http://www.spytector.com/download.html

KidLogger: http://kidlogger.net/download.html

PC Spy Keylogger: http://www.pc-spy-keylogger.com

Revealer Keylogger: http://www.logixoft.com/free-keylogger-download

Spy Keylogger: http://www.spy-key-logger.com/download.html

Actual Spy: http://www.actualspy.com/download.html

SpyBuddy® 2013: http://www.exploreanywhere.com/products/spybuddy/

Password Cracking Tools:

Windows Password Recovery Tool: http://www.windowspasswordsrecovery.com/

Hash Suite: http://hashsuite.openwall.net/download

Windows Password Recovery: http://www.passcape.com/windows_password_recovery

Password Recovery Bundle: http://www.top-password.com/password-recovery-bundle.html

krbpwguess: http://www.cqure.net/wp/tools/password-recovery/krbpwguess/

Windows Password Breaker Enterprise: http://www.recoverwindowspassword.com/windowspassword-breaker.html

Rekeysoft Windows Password Recovery Enterprise: http://www.rekeysoft.com/reset-windowspassword.html

pwdump7: http://www.tarasco.org/security/pwdump_7/

LOphtCrack: http://www.lOphtcrack.com/download.html

Ophcrack: http://ophcrack.sourceforge.net/download.php

Viruses and Worms

A computer virus is a type of malware that, when executed, replicates by inserting copies of itself (possibly modified) into other computer programs, data files, or the boot sector of the hard drive; when this replication succeeds, the affected areas are then said to be "infected". Viruses often perform some type of harmful activity on infected hosts, such as stealing hard disk space or CPU time, accessing private information, corrupting data, displaying political or humorous messages on the user's screen, spamming their contacts, or logging their keystrokes. However, not all viruses carry a destructive payload or attempt to hide themselves—the defining characteristic of viruses is that they are self-replicating computer programs which install themselves without the user's consent.

Virus Construction Kits:

ADMmutate: http://www.ktwo.ca/security.html

Virus programs and Generators:

BatchEncryt: <N/A>
BTGO.0.7: <N/A>
BWGen5.03: <N/A>
codeevolution: <N/A>
encrypter: <N/A>
looper 1.0: <N/A>
polydropd: <N/A>
rsbg: <N/A>
splitt: <N/A>

Viruses:

TOO MANY TO LIST: <N/A>

Worms Maker:

Internet Worm Make Thing: <N/A>
LogicalMines: <N/A>
PersonalCAKE: <N/A>
VBS Worm Generator: <N/A>
WSHWC: <N/A>
XVGL: <N/A>

Sniffing

This section has several tools that employ several methods for capturing data. ARP Poisoning, DHCP Starvation Attacks, and MAC address spoofing tools are some methods that are used. Another method not included on this list is a DNS zone transfer, which can be done using Windows command line. These tools will not help you if you are not familiar with basic networking.

ARP Poisoning Tools:

Cain & Abel: http://www.oxid.it/cain.html
Ufasoft Snif: http://ufasoft.com/sniffer/
WinArpAttacker: http://www.xfocus.org/index.html

ARP Spoofing Detection Tools:

XArp: http://www.chrismc.de/development/xarp/index.html
macof: http://www.monkey.org
Yersinia: http://www.yersinia.net/download.htm
Dhcpstarv: http://dhcpstarv.sourceforge.net/
Gobbler: http://gobbler.sourceforge.net/

DHCP Starvation Attack Tools:

DHCPstarv: http://dhcpstarv.sourceforge.net/
Gobbler: http://gobbler.sourceforge.net/

MAC Flooding Tools:

Yersinia: http://www.yersinia.net/

MAC Spoofing Tools:

SMAC: http://www.klcconsulting.net/smac/index.html#download

Sniffing Tools:

Ace Password Sniffer: http://www.effetech.com/aps/
RSA NetWitness Investigator: http://www.emc.c0m/security/rsa-netwitness.htm#lfreeware
Big-Mother: http://www.tupsoft.com/download.htm
EtherDetect Packet Sniffer: http://www.etherdetect.com/download.htm
dsniff: http://monkey.org/~dugsong/dsniff/
EffeTech HTTP Sniffer: http://www.effetech.com/download/
Ntop: http://www.ntop.org/products/ntop/
Ettercap: http://ettercap.sourceforge.net/downloads.html
Wireshark: http://www.wireshark.org/

Social Engineering

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. One type of social engineer term used in hacking is Phishing and Spear Phishing. Social engineer is not usually done by using tools, but by using the person to gain access to a system.

Tools:

Netcraft Toolbar: http://toolbar.netcraft.com/install
PhishTank: http://www.phishtank.com/
ReadNotify: http://www.readnotify.com/
Social Engineering Toolkit (SET): https://www.trustedsec.com/downloads/social-engineer-toolkit/

DoS

Tools:

BLANK - ALREADY LISTED IN GUIDE: <N/A>

Session Hijacking

Packet Crafting Tools:

Colasoft Packet Builder: http://www.colasoft.com/packet_builder/
Session Hijacking Tools:
Burp Suite: http://portswigger.net/burp/download.html
Ettercap: http://sourceforge.net/proj…/ettercap/files/latest/download…
WhatsUp Gold Engineer's Toolkit:
http://www.whatsupgold.com/…/downl…/network_management.aspx…
ing-sweep-tool
Hunt: http://packetstormsecurity.com/files/download/21968/hunt-l.5bin.tgz
Juggernaut: http://www.securiteam.com
TamperlE: http://www.bayden.com/TamperlE/
Cookie Cadger: https://www.cookiecadger.com/?page_id=19

Hacking Webservers

Hacking Web Passwords Tools:

Brutus: http://www.hoobie.net/brutus/brutus-download.html
THC-Hyrda: https://www.thc.org/thc-hydra/
Information Gathering Tools:
ActiveWhois: http://www.johnru.com/
Webserver Attack Tools:
Metasploit: http://www.metasploit.com/download/
Session Hijacking Tools:
Burp Suite: http://portswigger.net/burp/download.html
Hamster: http://erratasec.blogspot.in/2009/03/hamster-20-and-ferret-20.html

Vulnerability Scanning Tools:

Nessus: http://www.tenable.com/products/nessus
Web Application Security Scanners:
N-Stalker Web Application Security Scanner:
http://www.nstalker.com/products/editions/free/

Webserver Footprinting Tools:
httprecon: http://www.computec.ch/projekte/httprecon/?s=download
ID Serve: http://www.grc.com
Webserver Security Tools:
Arirang: http://www.monkey.org/~pilot/arirang/
N-Stalker Web Application Security Scanner:
http://www.nstalker.com/products/editions/free/
Infiltrator: http://www.infiltration-systems.com/download.shtml
WebCruiser: http://sec4app.com/download.htm
Nscan: http://nscan.hypermart.net
Retina CS: http://www.beyondtrust.com/Landers/TY-Page-RetinaCSCommunity/index.html
NetlQ Secure ConfigurationManager: https://www.netiq.com/products/secure-configurationmanager/

Hacking Web Applications

Cookie Poisoning:

OWASP Zed Attack Proxy:
https://code.google.com/p/zaproxy/downloads/detail…
&can=2&q=
Session Token Sniffing:
Wireshark: http://www.wireshark.org/

Web Application Hacking Tools:

Teleport Pro: http://www.tenmax.com/teleport/pro/download.htm
BlackWidow: http://softbytelabs.com/us/downloads.html
CookieDigger: http://www.mcafee.com/apps/free-tools/termsofuse.aspx7urh/us/downloads/freetools/cookiedigger.aspx
GNU Wget: ftp://ftp.gnu.org/gnu/wget/
Web Service Attack Tools:
soapUl: http://www.soapui.org/
XMLSpy: http://www.altova.com/xmlspy.html
Web Spidering Tools:
Burp Spider: http://blog.portswigger.net/2008/ll/mobp-all-new-burp-spider.html
WebScarab: https://www.0wasp.0rg/inde…/Categ0ry:0WASP_WebScarab_Pr0ject
Webserver Hacking Tools:
UrIScan:
http://www.microsoft.com/web/gallery/install.aspx…
an
Nikto: http://www.cirt.net/nikt02
Web Application Pen Testing Tools:
BeEF: http://beefproject.com/
XSS-Proxy: http://sourceforge.net/projects/xss-proxy/files/latest/download
sqlbftools: http://packetst0rmsecurity.c0m/fi…/d0wnl0ad/43795/sqlbft00ls -l.2.tar.gz
Softerra LDAP Browser: http://www.ldapadministrator.com/download.htm

Hibernate: http://www.hibernate.org/downloads
NHibernate: http://nhforge.org/
Soaplite: http://soaplite.com/download.html
cURL: http://curl.haxx.se/download.html
WSDigger: http://www.mcafee.com/apps/free-tools/termsofuse.aspx?url=/us/downloads/freetools/wsdigger.aspx
Sprajax: https://www.0wasp.0rg/index.…/Categ0ry:0WASP_Sprajax_Pr0ject

Web Application Security Tools:

KeepNI: http://www.keepni.com/
WSDigger: http://www.mcafee.com/apps/free-tools/termsofuse.aspx?url=/us/downloads/freetools/wsdigger.aspx
Arachni: http://arachni-scanner.com/latest
XSSS: http://www.sven.de/xsss/
Vega: http://www.subgraph.com/vega_download.php
Websecurify:
https://code.google.com/p/websecurify/downloads/detail…
%201.0.0.exe&can=2&q=
OWASP ZAP:
https://code.google.com/p/zaproxy/downloads/detail…
&can=2&q=
NetBrute: http://www.rawlogic.com/netbrute/
skipfish: https://c0de.g00gle.c0m/p/skipfish/
X5s: http://xss.codeplex.com/downloads/get/115610
SecuBat Vulnerability Scanner: http://secubat.codeplex.com/
SPIKE Proxy: http://www.immunitysec.com/resources-freesoftware.shtml
Ratproxy: https://c0de.g00gle.c0m/p/ratpr0xy/
Wapiti: http://wapiti.sourceforge.net/

SQL Injection

SQL Injection is one of the many web attack mechanisms used by hackers to steal data from organizations. It is perhaps one of the most common application layer attack techniques used today. It is the type of attack that takes advantage of improper coding of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain access to the data held within your database.

SQLi Detection Tools:

HP Weblnspect: http://www.hpenterprisesecurity.com/products/hp-fortify-software-securitycenter/hp-webinspect
SQLDict: http://ntsecurity.nu/toolbox/sqldict/
HP Scrawlr: https://h30406.www3.hp.com/campaigns/2008/wwcampaign/l-57C4K/index.php
SQL Block Monitor: http://sql-tools.net/blockmonitor/
Acunetix Web Vulnerability Scanner: http://www.acunetix.com/vulnerability-scanner/
GreenSQL Database Security: http://www.greensql.com/content/greensql-

databasesecurity#&sliderl=l
Microsoft Code Analysis Tool .NET (CAT.NET): http://www.microsoft.com/enus/download/details.aspx?id=5570
NGS SQuirreL Vulnerability Scanners: http://www.nccgroup.com/en/our-services/security-testingaudit-compliance/information-security-software/ngs-squirrel-vulnerability-scanners/
WSSA - Web Site Security Scanning Service: http://www.beyondsecurity.com/sql-injection.html
N-Stalker Web Application Security Scanner: http://www.nstalker.com/products/editions/free/
SQLi Injection Tools:
Absinthe: http://www.darknet.org.uk/2006/07/absinthe-blind-sql-injection-toolsoftware/
Blind Sql Injection Brute Forcer: h ttp://c0de.g00gle.c0m/p/bsqlbf-v2/
sqlmap: http://sqlmap.org/
SQL Injection Digger: http://sqid.rubyforge.org
Pangolin: http://nosec.org/en/evaluate/
SQLPAT: http://www.cqure.net/wp/tools/password-recovery/sqlpat/
FJ-lnjector Framework: http://sourceforge.net/projects/injection-fwk/
Exploiter (beta): http://www.ibm.com/…/ration…/downloads/08/appscan_exploiter/
SQLIer: http://bcable.net/project.php7sqlier
SQL Power Injector: http://www.sqlpowerinjector.com/download.htm
Havij: http://www.itsecteam.com
SQL Brute: http://www.gdssecurity.c0m/l/t.php
BobCat: http://www.northern-monkee.co.uk/pub/bobcat.html
Sqlninja: http://sqlninja.sourceforge.net/download.html

Hacking Wireless Networks

AirPcap -Enabled Open Source tools:

Cain and Abel: http://www.oxid.it/cain.html
Aircrack: http://www.airpcap.nl/
Airpcap: http://www.airpcap.nl/
Kismet: http://www.kismetwireless.net/

Bluetooth Hacking Tools:

BH Bluejack: http://croozeus.com/blogs/?p=33
Bluediving: http://bluediving.sourceforge.net/
Blooover: http://trifinite.org/trifinite_stuff_blooover.html
BTScanner: http://www.pentest.co.uk/downloads.html…
CIHwBT: http://sourceforge.net/projects/cih-with-bt/files/
Super Bluetooth Hack: http://gallery.mobile9.eom/f/317828/
GPS Mapping Tools:
WIGLE: http://wigle.net/gps/gps/main/download/

Skyhook: http://www.skyhookwireless.com/location-technology/sdk.php
WeFi: http://www.wefi.com/download/
Mobile-based Wi-Fi Discovery Tools:
WiFi Manager: http://kmansoft.com/
WiFiFoFum - WiFi Scanner: http://www.wififofum.net/downloads
RF Monitoring Tools:
DTC-340 RFXpert: http://www.dektec.com/Products/Apps/DTC-340/index.asp
KOrinoco: http://korinoco.sourceforge.net/
NetworkManager: https://wiki.gnome.org/Projects/NetworkManager
xosview: http://xosview.sourceforge.net/
Spectrum Analyzing Tools:
AirSleuth-Pro: http://nutsaboutnets.com/airsleuth-spectrum-analyzer/
BumbleBee-LX Handheld Spectrum Analyzer:
http://www.bvsystems.com/Products/Spectrum/BumbleBee-LX/bumblebee-lx.htm
Wi-Spy: http://www.metageek.net/products/wi-spy/
WEP Encryption:
Aircrack: http://www.airpcap.nl/
Cain and Abel: http://www.oxid.it/cain.html
WEP/WPA Cracking Tools:
Aircrack: http://www.airpcap.nl/
Cain and Abel: http://www.oxid.it/cain.html

Wi-Fi Discovery Tools:

inSSIDer: http://www.metageek.net/products/inssider/
Netsurveyor: http://www.performancewifi.net/performance-wifi/products/netsurveyor-networkdiscovery.htm
Vistumbler: http://www.vistumbler.net/
WirelessMon: http://www.passmark.com/products/wirelessmonitor.htm
WiFi Hopper: http://www.wifihopper.com/download.html
AirCheck Wi-Fi Tester: http://www.flukenetworks.com/enterprise-network/networktesting/AirCheck-Wi-Fi-Tester
AirRadar 2: http://www.koingosw.com/products/airradar.php
Wi-Fi Packet Sniffer:
OmniPeek: http://www.wildpackets.com/produc…/omnipeek_network_analyzer
Sniffer Portable Professional Analyzer:
http://www.netscout.com/…/Sniffer_Portable_Ana…/Sniffer_Portable_Professional_Analyzer/Pages/default.aspx
Capsa WiFi: http://www.colasoft.com/download/products/capsa_free.php
ApSniff: http://www.monolith81.de/apsniff.html
Wireshark: http://www.wireshark.org/download.html
Wi-Fi Predictive Planning Tools:
TamoGraph Site Survey: http://www.tamos.com/products/wifi-site-survey/wlan-planner.php
Wi-Fi Security Auditing Tools:
AirMagnet WiFi Analyzer: http://www.flukenetworks.com/enterprise-network/wirelessnetwork/AirMagnet-WiFi-Analyzer

Wi-Fi Sniffer:

Kismet: http://www.kismetwireless.net/
Wi-Fi Traffic Analyzer Tools:
Network Traffic Monitor & Analyzer CAPSA: http://www.javvin.com/packet-traffic.html
Observer:
http://www.networkinstruments.com/produ…/observer/index.php…
Ufasoft Snif: http://ufasoft.com/sniffer/
vxSniffer: http://www.cambridgevx.com/vxsniffer.html
Wi-Fi Vulnerability Scanning Tools:
Nessus: http://www.tenable.com/products/nessus
Nexpose Community Edition: http://www.rapid7.com/products/nexpose/compare-downloads.jsp
WiFish Finder: http://www.airtightnetworks.com/home/resources/knowledge-center/wifishfinder.html
OSWA: http://securitystartshere.org/page-downloads.htm
WiFiZoo: http://c0mmunity.c0rest.c0m/~h0ch0a/wifiz00/index.html…

Evading IDS, Firewalls, and Honeypots

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. A firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on applied rule set. A honeypot is a trap set to detect, deflect, or, in some manner, counteract attempts at
unauthorized use of information systems. Generally, a honeypot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers.

Firewall Evasion Tools:

Atelier W eb Firewall Tester: http://www.atelierweb.com/products/firewall-tester/
Freenet: https://freenetproject.org/
GTunnel: http://gardennetworks.org/download
Hotspot Shield: http://www.anchorfree.com/hotspot-shield-VPN-download-windows.php
Proxifier: http://www.proxifier.com/
Vpn One Click: http://www.vpnoneclick.com/download/index.html
Firewalls:
Comodo Firewall: http://personalfirewall.comodo.com/
Online Armor: http://www.online-armor.com/products-online-armor-free.php

Honeypot Detecting Tools:

Hping3: http://www.hping.org/hping3.html
Nessus: http://www.tenable.com/products/nessus
Send-Safe Honeypot Hunter: http://www.send-safe.com/honeypot-hunter.html

Honeypot Tools:
Argos: http://www.few.vu.nl/argos/?page=2
Glastopf: http://glastopf.org/
Honeyd: http://www.honeyd.org/
KFSensor: http://www.keyfocus.net/kfsensor/
Symantec Decoy Server: http://www.symantec.com/press/2003/n030623b.html
Tiny Honeypot: http://freecode.com/projects/thp
LaBrea: http://labrea.sourceforge.net/labrea-info.html
PatriotBox: http://www.alkasis.com/?action=products&pid=6
Kojoney: http://kojoney.sourceforge.net/
HoneyBOT: http://www.atomicsoftwaresolutions.com/honeybot.php
Google Hack Honeypot: http://ghh.sourceforge.net/
WinHoneyd: http://www2.netvigilance.com/winhoneyd
HI HAT: http://hihat.sourceforge.net/
Packet Fragment Generators:
Multi-Generator (MGEN): http://cs.itd.nrl.navy.mil/work/mgen/index.php
Net-lnspect: http://search.cpan.org/~sullr/Net-lnspect/lib/Net/lnspect/L3/IP.pm
NConvert: http://www.xnview.com/en/nconvert/
fping3: http://fping.org/

Buffer Overflow

A buffer overflow, or buffer overrun, is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. This is a special case of violation of memory safety. If this happened, the attacker can use this anomaly to run specific machine instructions and send sensitive information to a third party.

BoF Tools:

Netcat: http://netcat.sourceforge.net/download.php
LCLint: http://www.linuxjournal.com/article/3599
Code::Blocks: http://www.codeblocks.org/
eEye Retina: http://www.eeye.com/
Spike: http://spike.lazypics.de/dl_index_en.html
Brute Force Binary Tester (BFB): http://bfbtester.sourceforge.net/
Immunity CANVAS: http://www.immunityinc.com/products-canvas.shtml
Immunity Debugger: http://www.immunityinc.com/products-immdbg.shtml
Splint: http://www.splint.org/download.html
Flawfinder: http://www.dwheeler.com/flawfinder/
BLAST: http://mtc.epfl.ch/software-tools/blast/index-epfl.php
Stack Shield: http://www.angelfire.com/sk/stackshield/download.html
Valgrind: http://valgrind.org/downloads/current.html
PolySpace C Verifier: http://www.mathworks.in/products/polyspace/
Insure++: http://www.parasoft.com/jsp/products/insure.jsp?itemld=63
/GS: http://microsoft.com
BufferShield: http://www.sys-manage.com/PR0DUCTS/BufferShield/tabid/61/Default.aspx

DefenseWall: http://www.softsphere.com/online-help/defenceplus/
TIED:
http://www.security.iitk.ac.in/index.php…
eplus
LibsafePlus:
http://www.security.iitk.ac.in/index.php…
afeplus
Comodo Memory Firewall:
http://www.comodo.com/news/press_releases/16_01_08.html
Clang Static Analyzer: http://clang-analyzer.llvm.org/
FireFuzzer: https://c0de.g00gle.c0m/p/firefuzzer/
BOON: http://www.cs.berkeley.edu/~daw/boon/
The Enhanced Mitigation Experience Toolkit:
http://www.microsoft.com/enus/download/details.aspx?id=29851
CodeSonar® Static Analysis Tool: http://www.grammatech.com/codesonar
CORE IMPACT Pro: http://www.coresecurity.com/core-impact-pro

SSL / TLS / HTTPS

Is TLS fast yet – A great site debunking the myths of SSL/TLS speed cost
Firesheep – A watershed moment for SSL by demonstrating the ease with which unprotected traffic can be intercepted and sessions hijacked
Qualys SSL Labs – Tests a variety of attributes of the SSL implementation by pointing it at any URL
CloudFlare – Get SSL for free on any website
Let's Encrypt – It's coming, and it promises to fix the current mess that is CAs and configuring certs
Betsy's free wifi – Shows a young girl standing up a rogue wifi hot spot
Chromium HSTS preload list – All the sites submitted for HTTP strict transport security preload (a depressingly small number of them)
HTTP Shaming – Sensitive data sent insecurely? Name and shame!.