APRIL 26, 2017

TUTORIALS & EXPLOITS

LEAVE A COMMENT

List of some Penetration Testing Tools

- **0trace** 1.5 A hop enumeration tool http://jon.oberheide.org/0trace/
- **3proxy** 0.7.1.1 Tiny free proxy server. http://3proxy.ru/
- **3proxy-win32** 0.7.1.1 Tiny free proxy server. http://3proxy.ru/
- **42zip 42** Recursive Zip archive bomb. http://blog.fefe.de/?ts=b6cea88d
- **acccheck** 0.2.1 A password dictionary attack tool that targets windows authentication via the SMB protocol. http://labs.portcullis.co.uk/tools/acccheck/
- **ace 1.10** Automated Corporate Enumerator. A simple yet powerful VoIP Corporate Directory enumeration tool that mimics the behavior of an IP Phone in order to download the name and extension entries that a given phone can display on its screen interface http://ucsniff.sourceforge.net/ace.html
- **admid-pack 0.1** ADM DNS spoofing tools – Uses a variety of active and passive methods to spoof DNS packets. Very powerful. http://packetstormsecurity.com/files/10080/ADMid-pkg.tgz.html
- **adminpagefinder 0.1** This python script looks for a large amount of possible administrative interfaces on a given site. http://packetstormsecurity.com/files/112855/Admin-Page-Finder-Script.html
- **admsnmp 0.1** ADM SNMP audit scanner.
- **aesfix 1.0.1** A tool to find AES key in RAM http://citp.princeton.edu/memory/code/
- **aeskeyfind 1.0** A tool to find AES key in RAM http://citp.princeton.edu/memory/code/
- **aespipe 2.4c** Reads data from stdin and outputs encrypted or decrypted results to stdout. http://loop-aes.sourceforge.net/aespipe/
- **afflib 3.7.3** An extensible open format for the storage of disk images and related forensic information. http://www.afflib.org
- **afpfs-ng 0.8.1** A client for the Apple Filing Protocol (AFP) http://alexthepuffin.googlepages.com/
- **against 0.2** A very fast ssh attacking script which includes a multithreaded port scanning module (tcp connect)

- **aiengine 339.58dfb85** A packet inspection engine with capabilities of learning without any human intervention. https://bitbucket.org/camp0/aiengine/
- **aimage 3.2.5** A program to create aff-images. http://www.afflib.org
- **air 2.0.0** A GUI front-end to dd/dc3dd designed for easily creating forensic images. http://air-imager.sourceforge.net/
- **airflood 0.1** A modification of aireplay that allows for a DOS in in the AP. This program fills the table of clients of the AP with random MACs doing impossible new connections. http://packetstormsecurity.com/files/51127/airflood.1.tar.gz.html
- **airgraph-ng 2371** Graphing tool for the aircrack suite http://www.aircrack-ng.org
- **airoscript 45.0a122ee** A script to simplify the use of aircrack-ng tools. http://midnightresearch.com/projects/wicrawl/
- **airpwn 1.4** A tool for generic packet injection on an 802.11 network. http://airpwn.sourceforge.net
- **allthevhosts 1.0** A vhost discovery tool that scrapes various web applications http://labs.portcullis.co.uk/tools/finding-all-the-vhosts/
- **american-fuzzy-lop 0.89b** A practical, instrumentation-driven fuzzer for binary formats. https://code.google.com/p/american-fuzzy-lop/
- **androguard 1.9** Reverse engineering, Malware and goodware analysis of Android applications and more. https://code.google.com/p/androguard/
- **androick 5.35048d7** A python tool to help in forensics analysis on android. https://github.com/Flo354/Androick
- **android-apktool 1.5.2** A tool for reengineering Android apk files. http://forum.xda-developers.com/showthread.php?t=1755243
- **android-ndk r9c** Android C/C++ developer kit. http://developer.android.com/sdk/ndk/index.html
- **android-sdk-platform-tools r19** Platform-Tools for Google Android SDK (adb and fastboot) http://developer.android.com/sdk/index.html
- **android-sdk r22.3** Google Android SDK http://developer.android.com/sdk/index.html
- **android-udev-rules 8340.db8ef4a** Android udev rules. https://github.com/bbqlinux/android-udev-rules
- **androidsniffer 0.1** A perl script that lets you search for 3rd party passwords, dump the call log, dump contacts, dump wireless configuration, and more. http://packetstormsecurity.com/files/97464/Andr01d-Magic-

- **anontwi 1.0** A free software python client designed to navigate anonymously on social networks. It supports Identi.ca and Twitter.com. http://anontwi.sourceforge.net/
- **aphopper 0.3** AP Hopper is a program that automatically hops between access points of different wireless networks. http://aphopper.sourceforge.net/
- **apnbf 0.1** A small python script designed for enumerating valid APNs (Access Point Name) on a GTP-C speaking device. http://www.c0decafe.de/
- **arachni 1.0.6** A feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications. https://www.arachni-scanner.com
- **arduino 1.0.5** Arduino SDK (includes patched avrdude and librxtx) http://arduino.cc/en/Main/Software
- **argus 3.0.8** Network monitoring tool with flow control. http://qosient.com/argus/
- **argus-clients 3.0.8** Network monitoring client for Argus. http://qosient.com/argus/
- **armitage 141120** A graphical cyber attack management tool for Metasploit. http://www.fastandeasyhacking.com/
- **arp-scan 1.9** A tool that uses ARP to discover and fingerprint IP hosts on the local network http://www.nta-monitor.com/tools/arp-scan/
- **arpalert 2.0.12** Monitor ARP changes in ethernet networks http://www.arpalert.org/
- **arpantispoofer 1.0.1.32** A utility to detect and resist BIDIRECTIONAL ARP spoofing. It can anti-spoof for not only the local host, but also other hosts in the same subnet. It is also a handy helper for gateways which don't work well with ARP. http://arpantispoofer.sourceforge.net/
- **arpoison 0.6** The UNIX arp cache update utility http://www.arpoison.net
- **arpon 2.7** A portable handler daemon that make ARP protocol secure in order to avoid the Man In The Middle (MITM) attack through ARP Spoofing, ARP Cache Poisoning or ARP Poison Routing (APR) attacks. http://arpon.sourceforge.net/
- **arpwner 26.f300fdf** GUI-based python tool for arp posioning and dns poisoning attacks. https://github.com/ntrippar/ARPwner
- **artillery 1.0.2** A combination of a honeypot, file-system monitoring, system hardening, and overall health of a server to create a comprehensive way to secure a system https://www.trustedsec.com/downloads/artillery/
- **asleap 2.2** Actively recover LEAP/PPTP passwords. http://www.willhackforsushi.com/Asleap.html

- **athena-ssl-scanner 0.5.2** a SSL cipher scanner that checks all cipher codes. It can identify about 150 different ciphers. http://packetstormsecurity.com/files/93062/Athena-SSL-Cipher-Scanner.html
- **atstaketools 0.1** This is an archive of various @Stake tools that help perform vulnerability scanning and analysis, information gathering, password auditing, and forensics. http://packetstormsecurity.com/files/50718/AtStakeTools.zip.html
- **auto-xor-decryptor 3.6a1f8f7** Automatic XOR decryptor tool. http://www.blog.mrg-effitas.com/publishing-of-mrg-effitas-automatic-xor-decryptor-tool/
- **autopsy 2.24** A GUI for The Sleuth Kit. http://www.sleuthkit.org/autopsy
- **azazel 10.401e3aa** A userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit. https://github.com/chokepoint/azazel
- **b2sum 20140114** BLAKE2 file hash sum check. Computes the BLAKE2 (BLAKE2b or -s, -bp, -sp) cryptographic hash of a given file. https://blake2.net/
- **backcookie 44.cbf5b8b** Small backdoor using cookie. https://github.com/mrjopino/backcookie
- **backdoor-factory 98.89d87b2** Patch win32/64 binaries with shellcode. https://github.com/secretsquirrel/the-backdoor-factory
- **backfuzz 36.8e54ed6** A network protocol fuzzing toolkit. https://github.com/localh0t/backfuzz
- **balbuzard 65.546c5dcf629c** A package of malware analysis tools in python to extract patterns of interest from suspicious files (IP addresses, domain names, known file headers, interesting strings, etc). https://bitbucket.org/decalage/balbuzard/
- **bamf-framework 35.30d2b4b** A modular framework designed to be a platform to launch attacks against botnets. https://github.com/bwall/BAMF
- **basedomainname 0.1** Tool that can extract TLD (Top Level Domain), domain extensions (Second Level Domain + TLD), domain name, and hostname from fully qualified domain names. http://www.morningstarsecurity.com/research
- **batman-adv 2013.4.0** batman kernel module, (included upstream since .38) http://www.open-mesh.net/
- **bbqsql 1.2** SQL injection exploitation tool. https://github.com/neohapsis/bbqsql
- **bdfproxy 38.43e83e4** Patch Binaries via MITM: BackdoorFactory + mitmProxy https://github.com/secretsquirrel/BDFProxy

- **beef 0.4.5.0.181.g80a9f8e** The Browser Exploitation Framework that focuses on the web browser http://beefproject.com/
- **beholder 0.8.9** A wireless intrusion detection tool that looks for anomalies in a wifi environment. http://www.beholderwireless.org/
- **beleth 36.0963699** A Multi-threaded Dictionary based SSH cracker. https://github.com/chokepoint/Beleth
- **bfbtester 2.0.1** Performs checks of single and multiple argument command line overflows and environment variable overflows http://sourceforge.net/projects/bfbtester/
- **bgp-md5crack 0.1** RFC2385 password cracker http://www.c0decafe.de/
- **bing-ip2hosts 0.4** Enumerates all hostnames which Bing has indexed for a specific IP address. http://www.morningstarsecurity.com/research/bing-ip2hosts
- **bing-lfi-rfi 0.1** This is a python script for searching Bing for sites that may have local and remote file inclusion vulnerabilities. http://packetstormsecurity.com/files/121590/Bing-LFI-RFI-Scanner.html
- **binwalk 2.0.1** A tool for searching a given binary image for embedded files. http://binwalk.org
- **binwally 3.ca092a7** Binary and Directory tree comparison tool using the Fuzzy Hashing concept (ssdeep). https://github.com/bmaia/binwally
- **bios_memimage 1.2** A tool to dump RAM contents to disk (aka cold boot attack). http://citp.princeton.edu/memory/code/
- **birp 60.1d7c49f** A tool that will assist in the security assessment of mainframe applications served over TN3270. https://github.com/sensepost/birp
- **bittwist 2.0** A simple yet powerful libpcap-based Ethernet packet generator. It is designed to complement tcpdump, which by itself has done a great job at capturing network traffic. http://bittwist.sourceforge.net/
- **bkhive 1.1.1** Program for dumping the syskey bootkey from a Windows NT/2K/XP system hive. http://sourceforge.net/projects/ophcrack
- **blackarch-menus 0.2** BlackArch specific XDG-compliant menu http://www.blackarch.org/
- **blackhash 0.2** Creates a filter from system hashes http://16s.us/blackhash/
- **bletchley 0.0.1** A collection of practical application cryptanalysis tools. https://code.google.com/p/bletchley/
- **blindelephant 7** A web application fingerprinter. Attempts to discover the version of a (known) web application by comparing static files at known locations http://blindelephant.sourceforge.net/

- **bluebugger 0.1** An implementation of the bluebug technique which was discovered by Martin Herfurt. http://packetstormsecurity.com/files/54024/bluebugger.1.tar.gz.html
- **bluelog 1.1.1** A Bluetooth scanner and sniffer written to do a single task, log devices that are in discoverable mode. http://www.digifail.com/software/bluelog.shtml
- **bluepot 0.1** A Bluetooth Honeypot written in Java, it runs on Linux https://code.google.com/p/bluepot/
- **blueprint 0.1_3** A perl tool to identify Bluetooth devices. http://trifinite.org/trifinite_stuff_blueprinting.html
- **blueranger 1.0** A simple Bash script which uses Link Quality to locate Bluetooth device radios. http://www.hackfromacave.com/projects/blueranger.html
- **bluesnarfer 0.1** A bluetooth attacking tool http://www.alighieri.org/project.html
- **bmap-tools 3.2** Tool for copying largely sparse files using information from a block map file. http://git.infradead.org/users/dedekind/bmap-tools.git
- **bob-the-butcher 0.7.1** A distributed password cracker package. http://btb.banquise.net/
- **bokken 376.caaa65c431a8** GUI for radare2 and pyew. http://inguma.eu/projects/bokken/
- **bowcaster 0.1** This framework, implemented in Python, is intended to aid those developing exploits by providing useful set of tools and modules, such as payloads, encoders, connect-back servers, etc. Currently the framework is focused on the MIPS CPU architecture, but the design is intended to be modular enough to support arbitrary architectures. https://github.com/zcutlip/bowcaster
- **braa 0.82** A mass snmp scanner http://s-tech.elsat.net.pl/braa/
- **braces 0.4** A Bluetooth Tracking Utility. http://braces.shmoo.com/
- **browser-fuzzer** 3 Browser Fuzzer 3 http://www.krakowlabs.com/dev.html
- **brutessh 0.5** A simple sshd password bruteforcer using a wordlist, it's very fast for internal networks. It's multithreads. http://www.edge-security.com/edge-soft.php
- **brutus 2** One of the fastest, most flexible remote password crackers you can get your hands on. http://www.hoobie.net/brutus/
- **bsdiff 4.3** bsdiff and bspatch are tools for building and applying patches to binary files. http://www.daemonology.net/bsdiff/
- **bsqlbf 2.7** Blind SQL Injection Brute Forcer. http://code.google.com/p/bsqlbf-v2/
- **bss 0.8** Bluetooth stack smasher / fuzzer http://www.secuobs.com/news/15022006-bss_0_8.shtml

- **btcrack 1.1** The world's first Bluetooth Pass phrase (PIN) bruteforce tool. Bruteforces the Passkey and the Link key from captured Pairing exchanges. http://www.nruns.com/_en/security_tools_btcrack.php
- **btscanner 2.1** Bluetooth device scanner. http://www.pentest.co.uk
- **bulk-extractor 1.5.5** Bulk Email and URL extraction tool. https://github.com/simsong/bulk_extractor
- **bully 19.ba33677** A wifi-protected-setup (WPS) brute force attack tool. http://code.google.com/p/bully/
- **bunny 0.93** A closed loop, high-performance, general purpose protocol-blind fuzzer for C programs. http://code.google.com/p/bunny-the-fuzzer/
- **burpsuite 1.6** An integrated platform for attacking web applications (free edition). http://portswigger.net/burp/
- **buttinsky 138.1a2a1b2** Provide an open source framework for automated botnet monitoring. https://github.com/buttinsky/buttinsky
- **bvi 1.4.0beta** A display-oriented editor for binary files operate like "vi" editor. http://bvi.sourceforge.net/
- **cadaver 0.23.3** Command-line WebDAV client for Unix http://www.webdav.org/cadaver
- **canari 1.1** A transform framework for maltego http://www.canariproject.com/
- **cansina 93.abc6577** A python-based Web Content Discovery Tool. https://github.com/deibit/cansina
- **capstone 3.0** A lightweight multi-platform, multi-architecture disassembly framework. http://www.capstone-engine.org/index.html
- **carwhisperer 0.2** Intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys. http://trifinite.org/trifinite_stuff_carwhisperer.html
- **casefile 1.0.1** The little brother to Maltego without transforms, but combines graph and link analysis to examine links between manually added data to mind map your information http://www.paterva.com/web6/products/casefile.php
- **cdpsnarf 0.1.6** Cisco discovery protocol sniffer. https://github.com/Zapotek/cdpsnarf
- **cecster 5.15544cb** A tool to perform security testing against the HDMI CEC (Consumer Electronics Control) and HEC (HDMI Ethernet Channel) protocols https://github.com/nccgroup/CECster
- **centry 72.6de2868** Cold boot & DMA protection https://github.com/0xPoly/Centry
- **cewl 4.3** A custom word list generator http://www.digininja.org/projects/cewl.php

- **chaosmap 1.3** An information gathering tool and dns / whois / web server scanner http://freecode.com/projects/chaosmap
- **chaosreader 0.94** A freeware tool to trace tcp, udp etc. sessions and fetch application data from snoop or tcpdump logs. http://chaosreader.sourceforge.net/
- **chapcrack 17.ae2827f** A tool for parsing and decrypting MS-CHAPv2 network handshakes. https://github.com/moxie0/chapcrack
- **check-weak-dh-ssh 0.1** Debian OpenSSL weak client Diffie-Hellman Exchange checker. http://packetstormsecurity.com/files/66683/check_weak_dh_ssh.pl.bz2.html
- **checkiban 0.2** Checks the validity of an International Bank Account Number (IBAN). http://kernel.embedromix.ro/us/
- **checkpwd 1.23** Oracle Password Checker (Cracker) http://www.red-database-security.com/software/checkpwd.html
- **checksec 1.5** The checksec.sh script is designed to test what standard Linux OS and PaX security features are being used. http://www.trapkit.de/tools/checksec.html
- **chiron 0.7** An all-in-one IPv6 Penetration Testing Framework. http://www.secfu.net/tools-scripts/
- **chkrootkit 0.50** Checks for rootkits on a system http://www.chkrootkit.org/
- **chntpw 140201** Offline NT Password Editor – reset passwords in a Windows NT SAM user database file http://pogostick.net/~pnh/ntpasswd/
- **chownat 0.08b** Allows two peers behind two separate NATs with no port forwarding and no DMZ setup on their routers to directly communicate with each other http://samy.pl/chownat/
- **chrome-decode 0.1** Chrome web browser decoder tool that demonstrates recovering passwords. http://packetstormsecurity.com/files/119153/Chrome-Web-Browser-Decoder.html
- **chromefreak 22.336e323** A Cross-Platform Forensic Framework for Google Chrome http://osandamalith.github.io/ChromeFreak/
- **cidr2range 0.9** Script for listing the IP addresses contained in a CIDR netblock http://www.cpan.org/authors/id/R/RA/RAYNERLUC
- **ntruder 0.2.0** An automatic pentesting tool to bypass captchas. http://cintruder.sourceforge.net/
- **ciphertest 14.7f49ea7** A better SSL cipher checker using gnutls.

- **cisco-auditing-tool 1** Perl script which scans cisco routers for common vulnerabilities. Checks for default passwords, easily guessable community names, and the IOS history bug. Includes support for plugins and scanning multiple hosts. http://www.scrypt.net
- **cisco-global-exploiter 1.3** A perl script that targets multiple vulnerabilities in the Cisco Internetwork Operating System (IOS) and Catalyst products. http://www.blackangels.it
- **cisco-ocs 0.2** Cisco Router Default Password Scanner. http://www.question-defense.com/2013/01/11/ocs-version-2-release-ocs-cisco-router-default-password-scanner
- **cisco-router-config 1.1** copy-router-config and merge-router-config to copy and merge Cisco Routers Configuration
- **cisco-scanner 0.2** Multithreaded Cisco HTTP vulnerability scanner. Tested on Linux, OpenBSD and Solaris. http://wayreth.eu.org/old_page/
- **cisco-torch 0.4b** Cisco Torch mass scanning, fingerprinting, and exploitation tool. http://www.arhont.com
- **cisco5crack 2.c4b228c** Crypt and decrypt the cisco enable 5 passwords. https://github.com/madrisan/cisco7crack
- **cisco7crack 2.f1c21dd** Crypt and decrypt the cisco enable 7 passwords. https://github.com/madrisan/cisco7crack
- **ciscos 1.3** Scans class A, B, and C networks for cisco routers which have telnet open and have not changed the default password from cisco.
- **climber 23.f614304** Check UNIX/Linux systems for privilege escalation. https://github.com/raffaele-forte/climber
- **clusterd 129.0f04a49** Automates the fingerprinting, reconnaissance, and exploitation phases of an application server attack. https://github.com/hatRiot/clusterd
- **cmospwd 5.0** Decrypts password stored in CMOS used to access BIOS setup. http://www.cgsecurity.org/wiki/CmosPwd
- **cms-explorer 1.0** Designed to reveal the specific modules, plugins, components and themes that various cms driven websites are running http://code.google.com/p/cms-explorer
- **cms-few 0.1** Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python. http://packetstormsecurity.com/files/64722/cms_few.py.txt.html

- **complemento 0.7.6** A collection of tools for pentester: LetDown is a powerful tcp flooder ReverseRaider is a domain scanner that use wordlist scanning or reverse resolution scanning Httsquash is an http server scanner, banner grabber and data retriever http://complemento.sourceforge.net
- **conpot 0.3.1** ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting industrial control systems url="http://conpot.org"
- **conscan 1.1** A blackbox vulnerability scanner for the Concre5 CMS. http://nullsecurity.net/tools/scanner.html
- **cookie-cadger 1.07** An auditing tool for Wi-Fi or wired Ethernet connections. https://cookiecadger.com/
- **cowpatty 4.6** Wireless WPA/WPA2 PSK handshake cracking utility http://www.wirelessdefence.org/Contents/Files/
- **cpfinder 0.1** This is a simple script that looks for administrative web interfaces. http://packetstormsecurity.com/files/118851/Control-Panel-Finder-Script.html
- **cppcheck 1.67** A tool for static C/C++ code analysis http://cppcheck.wiki.sourceforge.net/
- **cpptest 1.1.2** A portable and powerful, yet simple, unit testing framework for handling automated tests in C++. http://cpptest.sourceforge.net/
- **crackhor 2.ae7d83f** A Password cracking utility. https://github.com/CoalfireLabs/crackHOR
- **crackle 39.3e93196** Crack and decrypt BLE encryption https://github.com/mikeryan/crackle/
- **crackserver 31.c268a80** An XMLRPC server for password cracking. https://github.com/averagesecurityguy/crack
- **create-ap 112.1c89b44** This script creates a NATed or Bridged WiFi Access Point. https://github.com/oblique/create_ap
- **creddump 0.3** A python tool to extract various credentials and secrets from Windows registry hives. https://code.google.com/p/creddump/
- **creds 8340.db8ef4a** Harvest FTP/POP/IMAP/HTTP/IRC credentials along with interesting data from each of the protocols. https://github.com/DanMcInerney/creds.py
- **creepy 137.9f60449** A geolocation information gatherer. Offers geolocation information gathering through social networking platforms. http://github.com/ilektrojohn/creepy.git
- **crunch 3.6** A wordlist generator for all combinations/permutations of a given character set. http://sourceforge.net/projects/crunch-wordlist/

- **crypthook** 17.0728cd1 TCP/UDP symmetric encryption tunnel wrapper. https://github.com/chokepoint/CryptHook
- **cryptonark 0.4.9** SSL security checker. http://blog.techstacks.com/cryptonark.html
- **csrftester 1.0** The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws. http://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project
- **ctunnel 0.6** Tunnel and/or proxy TCP or UDP connections via a cryptographic tunnel. http://nardcore.org/ctunnel
- **cuckoo 1.1.1** A malware analysis system. http://cuckoosandbox.org/
- **cupp 3.0** Common User Password Profiler http://www.remote-exploit.org/?page_id=418
- **cutycapt 10** A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page. http://cutycapt.sourceforge.net/
- **cvechecker 3.5** The goal of cvechecker is to report about possible vulnerabilities on your system, by scanning the installed software and matching the results with the CVE database. http://cvechecker.sourceforge.net/
- **cymothoa 1** A stealth backdooring tool, that inject backdoor's shellcode into an existing process. http://cymothoa.sourceforge.net/
- **darkbing 0.1** A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection. http://packetstormsecurity.com/files/111510/darkBing-SQL-Scanner.1.html
- **darkd0rk3r 1.0** Python script that performs dork searching and searches for local file inclusion and SQL injection errors. http://packetstormsecurity.com/files/117403/Dark-D0rk3r.0.html
- **darkjumper 5.8** This tool will try to find every website that host at the same server at your target http://sourceforge.net/projects/darkjumper/
- **darkmysqli 1.6** Multi-Purpose MySQL Injection Tool https://github.com/BlackArch/darkmysqli
- **darkstat 3.0.718** Network statistics gatherer (packet sniffer) http://dmr.ath.cx/net/darkstat/
- **davoset 1.2.3** A tool for using Abuse of Functionality and XML External Entities vulnerabilities on some websites to attack other websites. http://websecurity.com.ua/davoset/
- **davtest 1.0** Tests WebDAV enabled servers by uploading test executable files, and then (optionally) uploading files which allow for command execution or other actions directly on the target http://code.google.com/p/davtest/

- **dbpwaudit 0.8** A Java tool that allows you to perform online audits of password quality for several database engines http://www.cqure.net/wp/dbpwaudit/
- **dc3dd 7.1.614** A patched version of dd that includes a number of features useful for computer forensics http://sourceforge.net/projects/dc3dd
- **dcfldd 1.3.4.1** DCFL (DoD Computer Forensics Lab) dd replacement with hashing http://dcfldd.sourceforge.net/
- **ddrescue 1.19** GNU data recovery tool http://www.gnu.org/software/ddrescue/ddrescue.html
- **deblaze 0.3** A remote method enumeration tool for flex servers http://deblaze-tool.appspot.com/
- **delldrac 0.1a** DellDRAC and Dell Chassis Discovery and Brute Forcer. https://www.trustedsec.com/september/owning-dell-drac-awesome-hack/
- **depant 0.3a** Check network for services with default passwords. http://midnightresearch.com/projects/depant/
- **device-pharmer** 35.c1d449e Opens 1K+ IPs or Shodan search results and attempts to login. https://github.com/DanMcInerney/device-pharmer
- **dex2jar 0.0.9.13** A tool for converting Android's .dex format to Java's .class format http://code.google.com/p/dex2jar
- **dff-scanner 1.1** Tool for finding path of predictable resource locations. http://netsec.rs/70/tools.html
- **dhcdrop 0.5** Remove illegal dhcp servers with IP-pool underflow. Stable version http://www.netpatch.ru/dhcdrop.html
- **dhcpig 69.cc4109a** Enumerates hosts, subdomains, and emails from a given domain using google https://github.com/kamorin/DHCPig
- **dinouml 0.9.5** A network simulation tool, based on UML (User Mode Linux) that can simulate big Linux networks on a single PC http://kernel.embedromix.ro/us/
- **dirb 2.04** A web content scanner, brute forceing for hidden files http://dirb.sourceforge.net/
- **dirbuster 1.0_RC1** An application designed to brute force directories and files names on web/application servers http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
- **directorytraversalscan 1.0.1.0** Detect directory traversal vulnerabilities in HTTP servers and web applications. http://sourceforge.net/projects/httpdirscan/
- **dirs3arch 119.6a3b68a** HTTP(S) directory/file brute forcer. https://github.com/maurosoria/dirs3arch

- **dislocker 0.3** A tool to exploit the hash length extension attack in various hashing algorithms. With FUSE capabilities built in. http://www.hsc.fr/ressources/outils/dislocker/
- **dissector 1** This code dissects the internal data structures in ELF files. It supports x86 and x86_64 archs and runs under Linux. http://packetstormsecurity.com/files/125972/Coloured-ELF-File-Dissector.html
- **dissy 10** A graphical frontend to the objdump disassembler for compiler-generated code. http://dissy.googlecode.com/
- **dizzy 0.8.2** A Python based fuzzing framework with many features. http://www.c0decafe.de/
- **dmitry 1.3a** Deepmagic Information Gathering Tool. Gathers information about hosts. It is able to gather possible subdomains, email addresses, and uptime information and run tcp port scans, whois lookups, and more. http://www.mor-pah.net/
- **dnmap 0.6** The distributed nmap framework http://sourceforge.net/projects/dnmap/
- **dns-spoof 12.3918a10** Yet another DNS spoof utility. https://github.com/maurotfilho/dns-spoof
- **dns2geoip 0.1** A simple python script that brute forces DNS and subsequently geolocates the found subdomains. http://packetstormsecurity.com/files/118036/DNS-GeoIP.html
- **dns2tcp 0.5.2** A tool for relaying TCP connections over DNS. http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en
- **dnsa 0.5** DNSA is a dns security swiss army knife http://packetfactory.openwall.net/projects/dnsa/index.html
- **dnsbf 0.2** search for available domain names in an IP range http://code.google.com/p/dnsbf
- **dnsbrute 2.b1dc84a** Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads. https://github.com/d4rkcat/dnsbrute
- **dnschef 0.3** A highly configurable DNS proxy for pentesters. http://thesprawl.org/projects/dnschef/
- **dnsdrdos 0.1** Proof of concept code for distributed DNS reflection DoS http://nullsecurity.net/tools/dos.html
- **dnsenum 1.2.4.1** Script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results. http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=dnsenum
- **dnsgoblin 0.1** Nasty creature constantly searching for DNS servers. It uses standard dns querys and waits for the replies http://nullsecurity.net/tools/scanner.html
- **dnsmap 0.30** Passive DNS network mapper http://dnsmap.googlecode.com

- **dnsrecon 0.8.8** Python script for enumeration of hosts, subdomains and emails from a given domain using google. https://github.com/darkoperator/dnsrecon
- **dnsspider 0.5** A very fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation. http://nullsecurity.net/tools/scanner.html
- **dnstracer 1.9** Determines where a given DNS server gets its information from, and follows the chain of DNS servers http://www.mavetju.org/unix/dnstracer.php
- **dnsutils 9.9.2.P2** DNS utilities: dig host nslookup http://www.isc.org/software/bind/
- **dnswalk 2.0.2** A DNS debugger http://sourceforge.net/projects/dnswalk/
- **domain-analyzer 0.8.1** Finds all the security information for a given domain name. http://sourceforge.net/projects/domainanalyzer/
- **doona 118.ff1e17b** A fork of the Bruteforce Exploit Detector Tool (BED). https://github.com/wireghoul/doona
- **dotdotpwn 3.0** The Transversal Directory Fuzzer http://dotdotpwn.blogspot.com
- **dpeparser beta002** Default password enumeration project http://www.toolswatch.org/dpe/
- **dpscan 0.1** Drupal Vulnerabilty Scanner. https://github.com/insaneisnotfree/Blue-Sky-Information-Security
- **dradis 2.9.0** An open source framework to enable effective information sharing. http://dradisframework.org/
- **driftnet 0.1.6** Listens to network traffic and picks out images from TCP streams it observes. http://www.ex-parrot.com/~chris/driftnet/
- **_dripper v1.r1.gc9bb0c9** A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS. http://www.blackhatlibrary.net/Dripper
- **dscanner 709.f00026f** Swiss-army knife for D source code. https://github.com/Hackerpilot/Dscanner
- **dsd 84.60807e0** Digital Speech Decoder https://github.com/szechyjs/dsd
- **dsniff 2.4b1** Collection of tools for network auditing and penetration testing http://www.monkey.org/~dugsong/dsniff/
- **dumb0 19.1493e74** A simple tool to dump users in popular forums and CMS. https://github.com/0verl0ad/Dumb0
- **dump1090 386.bff92c4** A simple Mode S decoder for RTLSDR devices. https://github.com/MalcolmRobb/dump1090
- **dumpacl 0.0** Dumps NTs ACLs and audit settings. http://www.systemtools.com/cgi-bin/download.pl?DumpAcl

- **eapmd5pass 1.4** An implementation of an offline dictionary attack against the EAP-MD5 protocol http://www.willhackforsushi.com/?page_id=67
- **easy-creds 3.9 A** bash script that leverages ettercap and other tools to obtain credentials. https://github.com/brav0hax/easy-creds
- **easyfuzzer 3.6** A flexible fuzzer, not only for web, has a CSV output for efficient output analysis (platform independant). http://www.mh-sec.de/downloads.html.en
- **eazy 0.1** This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more. http://packetstormsecurity.com/files/117572/EAZY-Web-Scanner.html
- **edb 0.9.20** A QT4-based binary mode debugger with the goal of having usability on par with OllyDbg. http://www.codef00.com/projects.php#Debugger
- **eindeutig 20050628_1** Examine the contents of Outlook Express DBX email repository files (forensic purposes) http://www.jonesdykstra.com/
- **elettra 1.0** Encryption utility by Julia Identity http://www.winstonsmith.info/julia/elettra/
- **elettra-gui 1.0** Gui for the elettra crypto application. http://www.winstonsmith.info/julia/elettra/
- **elite-proxy-finder 42.b92f75a** Finds public elite anonymity proxies and concurrently tests them. https://github.com/DanMcInerney/elite-proxy-finder
- **enabler 1** attempts to find the enable password on a cisco system via brute force. http://packetstormsecurity.org/cisco/enabler.c
- **encodeshellcode 0.1b** This is an encoding tool for 32-bit x86 shellcode that assists a researcher when dealing with character filter or byte restrictions in a buffer overflow vulnerability or some kind of IDS/IPS/AV blocking your code. http://packetstormsecurity.com/files/119904/Encode-Shellcode.1b.html
- **ent 1.0** Pseudorandom number sequence test. http://www.fourmilab.ch/random
- **enum-shares 7.97cba5a** Tool that enumerates shared folders across the network and under a custom user account. https://github.com/dejanlevaja/enum_shares
- **enum4linux 0.8.9** A tool for enumerating information from Windows and Samba systems. http://labs.portcullis.co.uk/application/enum4linux/
- **enumiax 1.0** IAX enumerator http://sourceforge.net/projects/enumiax/
- **enyelkm 1.2** Rootkit for Linux x86 kernels v2.6. http://www.enye-sec.org/programas.html

http://sourceforge.net/projects/epicwebhoneypot/

- **erase-registrations 1.0** IAX flooder http://www.hackingexposedvoip.com/
- **etherape 0.9.13** A graphical network monitor for various OSI layers and protocols http://etherape.sourceforge.net/
- **ettercap 0.8.1** A network sniffer/interceptor/logger for ethernet LANs – console http://ettercap.github.com/ettercap/
- **evilgrade 2.0.0** Modular framework that takes advantage of poor upgrade implementations by injecting fake updates http://www.infobyte.com.ar/developments.html
- **evilmaid 1.01** TrueCrypt loader backdoor to sniff volume password http://theinvisiblethings.blogspot.com
- **exiv2 0.24** Exif and Iptc metadata manipulation library and tools http://exiv2.org
- **exploit-db 1.6** The Exploit Database (EDB) – an ultimate archive of exploits and vulnerable software – A collection of hacks http://www.exploit-db.com
- **extracthosts 14.ec8b89c** Extracts hosts (IP/Hostnames) from files. https://github.com/bwall/ExtractHosts
- **extundelete 0.2.4** Utility for recovering deleted files from ext2, ext3 or ext4 partitions by parsing the journal http://extundelete.sourceforge.net
- **eyepwn 1.0** Exploit for Eye-Fi Helper directory traversal vulnerability http://www.pentest.co.uk
- **eyewitness 278.e72c21e** Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. https://github.com/ChrisTruncer/EyeWitness
- **facebot 23.57f6025** A facebook profile and reconnaissance system. https://github.com/pun1sh3r/facebot
- **facebrute 7.ece355b** This script tries to guess passwords for a given facebook account using a list of passwords (dictionary). https://github.com/emerinohdz/FaceBrute
- **fakeap 0.3.2** Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. http://www.blackalchemy.to/project/fakeap/
- **fakedns 17.87d4216** A regular-expression based python MITM DNS server with correct DNS request passthrough and "Not Found" responses. https://github.com/Crypt0s/FakeDns
- **fakemail 1.0** Fake mail server that captures e-mails as files for acceptance testing. http://sourceforge.net/projects/fakemail/
- **fakenetbios 7.b83701e** A family of tools designed to simulate Windows hosts (NetBIOS) on a LAN.

- **fbht r12.a284878** A Facebook Hacking Tool https://github.com/chinoogawa/fbht-linux
- **fcrackzip 1.0** Zip file password cracker http://oldhome.schmorp.de/marc/fcrackzip.html
- **fern-wifi-cracker 219** WEP, WPA wifi cracker for wireless penetration testing http://code.google.com/p/fern-wifi-cracker/
- **fernmelder 6.c6d4ebe** Asynchronous mass DNS scanner. https://github.com/stealth/fernmelder
- **fgscanner 11.893372c** An advanced, opensource URL scanner. http://www.fantaghost.com/fgscanner
- **fhttp 1.3** This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more. http://packetstormsecurity.com/files/104315/FHTTP-Attack-Tool.3.html
- **fierce 0.9.9** A DNS scanner http://ha.ckers.org/fierce/
- **fiked 0.0.5** Fake IDE daemon http://www.roe.ch/FakeIKEd
- **filibuster 161.37b7f9c** A Egress filter mapping application with additional functionality. https://github.com/subinacls/Filibuster
- **fimap 1.00** A little tool for local and remote file inclusion auditing and exploitation http://code.google.com/p/fimap/
- **findmyhash 1.1.2** Crack different types of hashes using free online services http://code.google.com/p/findmyhash/
- **firewalk 5.0** An active reconnaissance network security tool http://packetfactory.openwall.net/projects/firewalk/
- **firmware-mod-kit 099** Modify firmware images without recompiling! http://code.google.com/p/firmware-mod-kit
- **firstexecution 6.a275793** A Collection of different ways to execute code outside of the expected entry points. https://github.com/nccgroup/firstexecution
- **fl0p 0.1** A passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks. http://lcamtuf.coredump.cx/
- **flare 0.6** Flare processes an SWF and extracts all scripts from it. http://www.nowrap.de/flare.html
- **flasm 1.62** Disassembler tool for SWF bytecode http://www.nowrap.de/flasm.html

- **flowinspect 94.01c8921** A network traffic inspection tool. https://github.com/7h3rAm/flowinspect
- **flunym0us 2.0** A Vulnerability Scanner for WordPress and Moodle. http://code.google.com/p/flunym0us/
- **foremost 1.5.7** A console program to recover files based on their headers, footers, and internal data structures http://foremost.sourceforge.net/
- **fpdns 0.9.3** Program that remotely determines DNS server versions http://code.google.com/p/fpdns/
- **fping 3.10** A utility to ping multiple hosts at once http://www.fping.org/
- **fport 2.0** Identify unknown open ports and their associated applications. http://www.foundstone.com/us/resources/proddesc/fport.htm
- **fraud-bridge 10.775c563** ICMP and DNS tunneling via IPv4 and IPv6. https://github.com/stealth/fraud-bridge
- **freeipmi 1.4.5** Sensor monitoring, system event monitoring, power control, and serial-over-LAN (SOL). http://www.gnu.org/software/freeipmi/
- **freeradius 3.0.4** The premier open source RADIUS server http://www.freeradius.org/
- **frisbeelite 1.2** A GUI-based USB device fuzzer. https://github.com/nccgroup/FrisbeeLite
- **fs-nyarl 1.0** A network takeover & forensic analysis tool – useful to advanced PenTest tasks & for fun and profit. http://www.fulgursecurity.com/en/content/fs-nyarl
- **fsnoop 3.3** A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods"). http://vladz.devzero.fr/fsnoop.php
- **fstealer 0.1** Automates file system mirroring through remote file disclosur vulnerabilities on Linux machines. http://packetstormsecurity.com/files/106450/FStealer-Filesystem-Mirroring-Tool.html
- **ftester 1.0** A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities. http://www.inversepath.com/ftester.html
- **ftp-fuzz 1337** The master of all master fuzzing scripts specifically targeted towards FTP server sofware http://nullsecurity.net/tools/fuzzer.html
- **ftp-scanner 0.2.5** Multithreaded ftp scanner/brute forcer. Tested on Linux, OpenBSD and Solaris. http://wayreth.eu.org/old_page/
- **ftp-spider 1.0** FTP investigation tool – Scans ftp server for the following: reveal entire directory tree structures, detect anonymous access, detect directories with write permissions, find user specified data within repository.

- **ftpmap 0.4** scans remote FTP servers to identify what software and what versions they are running. http://wcoserver.googlecode.com/files/
- **fusil 1.4** Fusil the fuzzer is a Python library used to write fuzzing programs. It helps to start process with a prepared environment (limit memory, environment variables, redirect stdout, etc.), start network client or server, and create mangled files http://bitbucket.org/haypo/fusil/wiki/Home
- **fuzzap 14.f13932c** A python script for obfuscating wireless networks. https://github.com/lostincynicism/FuzzAP
- **fuzzball2 0.7** A little fuzzer for TCP and IP options. It sends a bunch of more or less bogus packets to the host of your choice. http://nologin.org/
- **fuzzdb 1.09** Attack and Discovery Pattern Database for Application Fuzz Testing https://code.google.com/p/fuzzdb/
- **fuzzdiff 1.0** A simple tool designed to help out with crash analysis during fuzz testing. It selectively 'un-fuzzes' portions of a fuzzed file that is known to cause a crash, re-launches the targeted application, and sees if it still crashes. http://vsecurity.com/resources/tool
- **fuzztalk 1.0.0.0** An XML driven fuzz testing framework that emphasizes easy extensibility and reusability. https://code.google.com/p/fuzztalk
- **g72x++ 1** Decoder for the g72x++ codec. http://www.ps-auxw.de/
- **galleta 20040505_1** Examine the contents of the IE's cookie files for forensic purposes http://www.jonesdykstra.com/
- **gdb 7.8.1** The GNU Debugger http://www.gnu.org/software/gdb/
- **genlist 0.1** Generates lists of IP addresses.
- **geoedge 0.2** This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool).
- **geoip 1.6.2** Non-DNS IP-to-country resolver C library & utils http://www.maxmind.com/app/c
- **geoipgen 0.4** GeoIPgen is a country to IP addresses generator. http://code.google.com/p/geoipgen/
- **getsids 0.0.1** Getsids tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener. Like doing 'lsnrctl service'. http://www.cqure.net/wp/getsids/
- **gggooglescan 0.4** A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames. http://www.morningstarsecurity.com/research/gggooglescan

- **ghost-py 0.1b3** Webkit based webclient (relies on PyQT). http://jeanphix.github.com/Ghost.py/
- **giskismet 20110805** A program to visually represent the Kismet data in a flexible manner. http://www.giskismet.org
- **gnuradio 3.7.5.1** General purpose DSP and SDR toolkit. With drivers for usrp and fcd. http://gnuradio.org
- **gnutls2 2.12.23** A library which provides a secure layer over a reliable transport layer (Version 2) http://gnutls.org/
- **goldeneye 16.7a38fe9** A HTTP DoS test tool. Attack Vector exploited: HTTP Keep Alive + NoCache. https://github.com/jseidl/GoldenEye
- **golismero 2.0** Opensource web security testing framework. https://github.com/golismero/golismero
- **goodork 2.2** A python script designed to allow you to leverage the power of google dorking straight from the comfort of your command line. http://goo-dork.blogspot.com/
- **goofile 1.5** Command line filetype search https://code.google.com/p/goofile/
- **goog-mail 1.0** Enumerate domain emails from google. http://www.darkc0de.com/others/goog-mail.py
- **googlesub 1.2** A python script to find domains by using google dorks. https://github.com/zombiesam/googlesub
- **gooscan 1.0.9** A tool that automates queries against Google search appliances, but with a twist. http://johnny.ihackstuff.com/downloads/task,doc_details&Itemid=/gid,28/
- **gqrx 2.3.1** Interactive SDR receiver waterfall for many devices. http://gqrx.dk/
- **grabber 0.1** A web application scanner. Basically it detects some kind of vulnerabilities in your website. http://rgaucher.info/beta/grabber/
- **grepforrfi 0.1** Simple script for parsing web logs for RFIs and Webshells v1.2 http://www.irongeek.com/downloads/grepforrfi.txt
- **grokevt 0.5.0** A collection of scripts built for reading Windows® NT/2K/XP/2K eventlog files. http://code.google.com/p/grokevt/
- **gtalk-decode 0.1** Google Talk decoder tool that demonstrates recovering passwords from accounts. http://packetstormsecurity.com/files/119154/Google-Talk-Decoder.html
- **gtp-scan 0.7** A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts. http://www.c0decafe.de/

- **gwcheck 0.1** A simple program that checks if a host in an ethernet network is a gateway to Internet. http://packetstormsecurity.com/files/62047/gwcheck.c.html
- **gwtenum 7.f27a5aa** Enumeration of GWT-RCP method calls. http://www.gdssecurity.com/l/t/d.php?k=GwtEnum
- **hackersh 0.2.0** A shell for with Pythonect-like syntax, including wrappers for commonly used security tools http://www.hackersh.org/
- **halberd 0.2.4** Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing. http://halberd.superadditive.com/
- **halcyon 0.1** A repository crawler that runs checksums for static files found within a given git repository. http://www.blackhatlibrary.net/Halcyon
- **hamster 2.0.0** Tool for HTTP session sidejacking. http://hamster.erratasec.com/
- **handle 0.0** An small application designed to analyze your system searching for global objects related to running proccess and display information for every found object, like tokens, semaphores, ports, files,.. http://www.tarasco.org/security/handle/index.html
- **hasere 1.0** Discover the vhosts using google and bing. https://github.com/galkan/hasere
- **hash-identifier 1.1** Identifies the different types of hashes used to encrypt data, especially passwords http://code.google.com/p/hash-identifier
- **hashcat 0.47** A multithreaded cross platform hash cracker. http://hashcat.net/hashcat/
- **_hashcat-utils 1.0** Utilites for Hashcat http://hashcat.net/wiki/doku.php?id=hashcat_utils
- **hasher 32.e9d1394** A tool that allows you to quickly hash plaintext strings, or compare hashed values with a plaintext locally. https://github.com/ChrisTruncer/Hasher
- **hashid 2.6.0** Software to identify the different types of hashes used to encrypt data https://github.com/psypanda/hashID
- **hashpump 34.0b3c286** A tool to exploit the hash length extension attack in various hashing algorithms. https://github.com/bwall/HashPump
- **hashtag 0.41** A python script written to parse and identify password hashes. https://github.com/SmeegeSec/HashTag
- **haystack 1035.ac2ffa4** A Python framework for finding C structures from process memory – heap analysis –

- **hcraft 1.0.0** HTTP Vuln Request Crafter http://sourceforge.net/projects/hcraft/
- **hdcp-genkey 18.e8d342d** Generate HDCP source and sink keys from the leaked master key. https://github.com/rjw57/hdcp-genkey
- **hdmi-sniff 5.f7fbc0e** HDMI DDC (I2C) inspection tool. It is designed to demonstrate just how easy it is to recover HDCP crypto keys from HDMI devices. https://github.com/ApertureLabsLtd/hdmi-sniff
- **heartbleed-honeypot 0.1** Script that listens on TCP port 443 and responds with completely bogus SSL heartbeat responses, unless it detects the start of a byte pattern similar to that used in Jared Stafford's http://packetstormsecurity.com/files/126068/hb_honeypot.pl.txt
- **hex2bin 1.0.7** Converts Motorola and Intel hex files to binary. http://hex2bin.sourceforge.net/
- **hexinject 1.5** A very versatile packet injector and sniffer that provides a command-line framework for raw network access. http://hexinject.sourceforge.net
- **hexorbase 6** A database application designed for administering and auditing multiple database servers simultaneously from a centralized location. It is capable of performing SQL queries and bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL). https://code.google.com/p/hexorbase/
- **hharp 1beta** This tool can perform man-in-the-middle and switch flooding attacks. It has 4 major functions, 3 of which attempt to man-in-the-middle one or more computers on a network with a passive method or flood type method. http://packetstormsecurity.com/files/81368/Hackers-Hideaway-ARP-Attack-Tool.html
- **hidattack 0.1** HID Attack (attacking HID host implementations) http://mulliner.org/bluetooth/hidattack.php
- **honeyd 1.6.7** A small daemon that creates virtual hosts on a network. https://github.com/DataSoft/Honeyd/
- **honssh 47.0de60ec** A high-interaction Honey Pot solution designed to log all SSH communications between a client and server. https://code.google.com/p/honssh/
- **hookanalyser 3.0** A hook tool which can be potentially helpful in reversing applications and analyzing malware. It can hook to an API in a process and search for a pattern in memory or dump the buffer. http://hookanalyser.blogspot.de/
- **host-extract 9** Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL. https://code.google.com/p/host-extract/
- **hostbox-ssh 0.1.1** A ssh password/account scanner. http://stridsmanit.wordpress.com/2012/12/02/brute-

- **hotpatch 0.2** Hot patches executables on Linux using .so file injection http://www.selectiveintellect.com/hotpatch.html
- **hotspotter 0.4_** Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names. http://www.remote-exploit.org/?page_id=418
- **hpfeeds** 138.249b2f7 Honeynet Project generic authenticated datafeed protocol. https://github.com/rep/hpfeeds
- **hping 3.0.0** A command-line oriented TCP/IP packet assembler/analyzer. http://www.hping.org
- **hqlmap 35.081395e** A tool to exploit HQL Injections. https://github.com/PaulSec/HQLmap
- **htexploit 0.77** A Python script that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process http://www.mkit.com.ar/labs/htexploit/
- **htrosbif 134.9dc3f86** Active HTTP server fingerprinting and recon tool. https://github.com/lkarsten/htrosbif
- **htshells 760b5e9** Self contained web shells and other attacks via .htaccess files. https://github.com/wireghoul/htshells
- **http-enum 0.3** A tool to enumerate the enabled HTTP methods supported on a webserver. https://www.thexero.co.uk/tools/http-enum/
- **http-fuzz 0.1** A simple http fuzzer. none
- **http-put 1.0** Simple http put perl script
- **http-traceroute 0.5** This is a python script that uses the Max-Forwards header in HTTP and SIP to perform a traceroute-like scanning functionality. http://packetstormsecurity.com/files/107167/Traceroute-Like-HTTP-Scanner.html
- **httpbog 1.0.0.0** A slow HTTP denial-of-service tool that works similarly to other attacks, but rather than leveraging request headers or POST data Bog consumes sockets by slowly reading responses. http://sourceforge.net/projects/httpbog/
- **httpforge 11.02.01** A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the security of Web servers, apps, and sites. An accompanying Python library is available for extensions. http://packetstormsecurity.com/files/98109/HTTPForge.02.01.html
- **httping 2.3.4** A 'ping'-like tool for http-requests. http://www.vanheusden.com/httping/

- **httpry 0.1.8** A specialized packet sniffer designed for displaying and logging HTTP traffic. http://dumpsterventures.com/jason/httpry/
- **httpsniff 0.4** Tool to sniff HTTP responses from TCP/IP based networks and save contained files locally for later review. http://www.sump.org/projects/httpsniff/
- **httpsscanner 1.2** A tool to test the strength of a SSL web server. https://code.google.com/p/libre-tools/
- **httptunnel 3.3** Creates a bidirectional virtual data connection tunnelled in HTTP requests http://www.nocrew.org/software/httptunnel
- **hulk 11.a9b9ad4** A webserver DoS tool (Http Unbearable Load King) ported to Go with some additional features. https://github.com/grafov/hulk
- **hwk 0.4** Collection of packet crafting and wireless network flooding tools http://www.nullsecurity.net/
- **hydra 8.1** A very fast network logon cracker which support many different services. http://www.thc.org/thc-hydra/
- **hyenae 0.36_1** flexible platform independent packet generator http://sourceforge.net/projects/hyenae/
- **hyperion 1.1** A runtime encrypter for 32-bit portable executables. http://nullsecurity.net/tools/binary.html
- **iaxflood 0.1** IAX flooder. http://www.hackingexposedvoip.com/
- **iaxscan 0.02** A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts. http://code.google.com/p/iaxscan/
- **ibrute 12.3a6a11e** An AppleID password bruteforce tool. It uses Find My Iphone service API, where bruteforce protection was not implemented. https://github.com/hackappcom/ibrute/
- **icmpquery 1.0** Send and receive ICMP queries for address mask and current time. http://www.angio.net/security/
- **icmptx 0.01** IP over ICMP http://thomer.com/icmptx/
- **iheartxor 0.01** iheartxor is a tool for bruteforcing encoded strings within a boundary defined by a regular expression. It will bruteforce the key value range of 0x1 through 0x255. http://hooked-on-mnemonics.blogspot.com.es/p/iheartxor.html
- **ike-scan 1.9** A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers http://www.nta-monitor.com/tools/ike-scan/
- **ikecrack 1.00** An IKE/IPSec crack tool designed to perform Pre-Shared-Key analysis of RFC compliant aggressive

- **ikeprobe 0.1** Determine vulnerabilities in the PSK implementation of the VPN server. http://www.ernw.de/download/ikeprobe.zip
- **ikeprober 1.12** Tool crafting IKE initiator packets and allowing many options to be manually set. Useful to find overflows, error conditions and identifiyng vendors http://ikecrack.sourceforge.net/
- **ilty 1.0** An interception phone system for VoIP network. http://chdir.org/~nico/ilty/
- **imagejs 48.1faf262** Small tool to package javascript into a valid image file. https://github.com/jklmnn/imagejs
- **inception 416.2e7b723** A FireWire physical memory manipulation and hacking tool exploiting IEEE 1394 SBP DMA. http://www.breaknenter.org/projects/inception/
- **indxparse 150.1b50750** A Tool suite for inspecting NTFS artifacts. http://www.williballenthin.com/forensics/mft/indxparse/
- **inetsim 1.2.5** A software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples. http://www.inetsim.org
- **infip 0.1** A python script that checks output from netstat against RBLs from Spamhaus. http://packetstormsecurity.com/files/104927/infIP.1-Blacklist-Checker.html
- **inguma 0.1.1** A free penetration testing and vulnerability discovery toolkit entirely written in python. Framework includes modules to discover hosts, gather information about, fuzz targets, brute force usernames and passwords, exploits, and a disassembler. http://inguma.sourceforge.net
- **intercepter-ng 0.9.8** A next generation sniffer including a lot of features: capturing passwords/hashes, sniffing chat messages, performing man-in-the-middle attacks, etc. http://intercepter.nerf.ru/#down
- **interrogate 0.0.4** A proof-of-concept tool for identification of cryptographic keys in binary material (regardless of target operating system), first and foremost for memory dump analysis and forensic usage. https://github.com/carmaa/interrogate
- **intersect 2.5** Post-exploitation framework https://github.com/ohdae/Intersect.5
- **intrace 1.5** Traceroute-like application piggybacking on existing TCP connections http://intrace.googlecode.com
- **inundator 0.5** An ids evasion tool, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real attack. http://inundator.sourceforge.net/
- **inviteflood 2.0** Flood a device with INVITE requests https://launchpad.net/~wagungs/+archive/kali-

- **iosforensic 1.0** iOS forensic tool https://www.owasp.org/index.php/Projects/OWASP_iOSForensic https://github.com/Flo354/iOSForensic
- **ip-https-tools 5.b22e2b3** Tools for the IP over HTTPS (IP-HTTPS) Tunneling Protocol. https://github.com/takeshixx/ip-https-tools
- **ipaudit 1.0BETA2** IPAudit monitors network activity on a network. http://ipaudit.sourceforge.net
- **ipba2 032013** IOS Backup Analyzer http://www.ipbackupanalyzer.com/
- **ipdecap 69.f3a08f6** Can decapsulate traffic encapsulated within GRE, IPIP, 6in4, ESP (ipsec) protocols, and can also remove IEEE 802.1Q (virtual lan) header. http://www.loicp.eu/ipdecap#dependances
- **iphoneanalyzer 2.1.0** Allows you to forensically examine or recover date from in iOS device. http://www.crypticbit.com/zen/products/iphoneanalyzer
- **ipscan 3.3.2** Angry IP scanner is a very fast IP address and port scanner. http://www.angryziber.com/
- **iputils 20121221** Network monitoring tools, including ping http://www.skbuff.net/iputils/
- **ipv6toolkit 2.0beta** SI6 Networks' IPv6 Toolkit http://www.si6networks.com/tools/ipv6toolkit/
- **ircsnapshot 93.9ba3c6c** Tool to gather information from IRC servers. https://github.com/bwall/ircsnapshot
- **irpas 0.10** Internetwork Routing Protocol Attack Suite. http://phenoelit-us.org/irpas
- **isr-form 1.0** Simple html parsing tool that extracts all form related information and generates reports of the data. Allows for quick analyzing of data. http://www.infobyte.com.ar/
- **jad 1.5.8e** Java decompiler http://www.varaneckas.com/jad
- **javasnoop 1.1** A tool that lets you intercept methods, alter data and otherwise hack Java applications running on your computer https://code.google.com/p/javasnoop/
- **jboss-autopwn 1.3bc2d29** A JBoss script for obtaining remote shell access. https://github.com/SpiderLabs/jboss-autopwn
- **jbrofuzz 2.5** Web application protocol fuzzer that emerged from the needs of penetration testing. http://sourceforge.net/projects/jbrofuzz/
- **jbrute 0.99** Open Source Security tool to audit hashed passwords. http://sourceforge.net/projects/jbrute/
- **jd-gui 0.3.5** A standalone graphical utility that displays Java source codes of .class files http://java.decompiler.free.fr/?q=jdgui
- **jhead 2.97** EXIF JPEG info parser and thumbnail remover http://www.sentex.net/~mwandel/jhead/

- **jnetmap 0.5.3** A network monitor of sorts http://www.rakudave.ch/jnetmap/?file=introduction
- **john 1.7.9** John The Ripper – A fast password cracker (jumbo included) http://www.openwall.com/john/
- **johnny 20120424** GUI for John the Ripper. http://openwall.info/wiki/john/johnny
- **jomplug 0.1** This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components. http://packetstormsecurity.com/files/121390/Janissaries-Joomla-Fingerprint-Tool.html
- **joomlascan 1.2** Joomla scanner scans for known vulnerable remote file inclusion paths and files. http://packetstormsecurity.com/files/62126/joomlascan.2.py.txt.html
- **joomscan 2012.03.10** Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site. http://joomscan.sourceforge.net/
- **js-beautify 1.4.2** This little beautifier will reformat and reindent bookmarklets, ugly JavaScript, unpack scripts packed by Dean Edward?s popular packer, as well as deobfuscate scripts processed by javascriptobfuscator.com. https://github.com/einars/js-beautify
- **jsql** 0.5 A lightweight application used to find database information from a distant server. https://code.google.com/p/jsql-injection/
- **junkie 1338.baa4524** A modular packet sniffer and analyzer. https://github.com/securactive/junkie
- **jwscan 6.b0306f0** Scanner for Jar to EXE wrapper like Launch4j, Exe4j, JSmooth, Jar2Exe. https://github.com/katjahahn/JWScan
- **jynx2 2.0** An expansion of the original Jynx LD_PRELOAD rootkit http://www.blackhatlibrary.net/Jynx2
- **kalibrate-rtl 11.aae11c8** Fork of http://thre.at/kalibrate/ for use with rtl-sdr devices. https://github.com/steve-m/kalibrate-rtl
- **katsnoop 0.1** Utility that sniffs HTTP Basic Authentication information and prints the base64 decoded form. http://packetstormsecurity.com/files/52514/katsnoop.tbz2.html
- **kautilya 0.5.0** Pwnage with Human Interface Devices using Teensy++2.0 and Teensy 3.0 devices http://code.google.com/p/kautilya
- **keimpx 0.2** Tool to verify the usefulness of credentials across a network over SMB. http://code.google.com/p/keimpx/
- **khc 0.2** A small tool designed to recover hashed known_hosts fiels back to their plain-text equivalents.

- **killerbee 85** Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks. https://code.google.com/p/killerbee/
- **kippo 0.9** A medium interaction SSH honeypot designed to log brute force attacks and most importantly, the entire shell interaction by the attacker. https://github.com/desaster/kippo
- **kismet 2013_03_R1b 802.11** layer2 wireless network detector, sniffer, and intrusion detection system http://www.kismetwireless.net/
- **kismet-earth 0.1** Various scripts to convert kismet logs to kml file to be used in Google Earth. http://
- **kismet2earth 1.0** A set of utilities that convert from Kismet logs to Google Earth .kml format http://code.google.com/p/kismet2earth/
- **klogger 1.0** A keystroke logger for the NT-series of Windows. http://ntsecurity.nu/toolbox/klogger/
- **kolkata 3.0** A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion. http://www.blackhatlibrary.net/Kolkata
- **kraken 32.368a837** A project to encrypt A5/1 GSM signaling using a Time/Memory Tradeoff Attack. http://opensource.srlabs.de/projects/a51-decrypt
- **laf 12.7a456b3** Login Area Finder: scans host/s for login panels. https://github.com/takeshixx/laf
- **lanmap2 124.4f8afed** Passive network mapping tool http://github.com/rflynn/lanmap2
- **lans 1.0** A Multithreaded asynchronous packet parsing/injecting arp spoofer. https://github.com/DanMcInerney/LANs.py
- **latd 1.31** A LAT terminal daemon for Linux and BSD. http://sourceforge.net/projects/linux-decnet/files/latd/1.31/
- **laudanum 1.0** A collection of injectable files, designed to be used in a pentest when SQL injection flaws are found and are in multiple languages for different environments. http://laudanum.inguardians.com/#
- **lbd 20130719** Load Balancing detector http://ge.mine.nu/code/lbd
- **lbmap 145.93e6b71** Proof of concept scripts for advanced web application fingerprinting, presented at OWASP AppSecAsia 2012. https://github.com/wireghoul/lbmap
- **ldapenum 0.1** Enumerate domain controllers using LDAP. https://gobag.googlecode.com/svn-history/r2/trunk/ldap/ldapenum/
- **leo 4.11** Literate programmer's editor, outliner, and project manager http://webpages.charter.net/edreamleo/front.html

- **levye 85.419e817** A brute force tool which is support sshkey, vnckey, rdp, openvpn. https://github.com/galkan/levye
- **lfi-autopwn 3.0** A Perl script to try to gain code execution on a remote server via LFI http://www.blackhatlibrary.net/Lfi_autopwn.pl
- **lfi-exploiter 1.1** This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability.. http://packetstormsecurity.com/files/124332/LFI-Exploiter.1.html
- **lfi-fuzzploit 1.1** A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications. http://packetstormsecurity.com/files/106912/LFI-Fuzzploit-Tool.1.html
- **lfi-scanner 4.0** This is a simple perl script that enumerates local file inclusion attempts when given a specific target. http://packetstormsecurity.com/files/102848/LFI-Scanner.0.html
- **lfi-sploiter 1.0** This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities. http://packetstormsecurity.com/files/96056/Simple-Local-File-Inclusion-Exploiter.0.html
- **lfimap 1.4.8** This script is used to take the highest benefits of the local file include vulnerability in a webserver. https://code.google.com/p/lfimap/
- **lft 3.72** A layer four traceroute implementing numerous other features. http://pwhois.org/lft/
- **libdisasm 0.23** A disassembler library. http://bastard.sourceforge.net/libdisasm.html
- **libpst 0.6.63** Outlook .pst file converter http://www.five-ten-sg.com/libpst/
- **liffy 63.238ce6d** A Local File Inclusion Exploitation tool. https://github.com/rotlogix/liffy
- **linenum 18.b4c2541** Scripted Local Linux Enumeration & Privilege Escalation Checks https://github.com/rebootuser/LinEnum
- **linux-exploit-suggester 32.9db2f5a** A Perl script that tries to suggest exploits based OS version number. https://github.com/PenturaLabs/Linux_Exploit_Suggester
- **list-urls 0.1** Extracts links from webpage http://www.whoppix.net
- **littleblackbox 0.1.3** Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices. http://code.google.com/p/littleblackbox/wiki/FAQ
- **lodowep 1.2.1** Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver

- **loki 0.2.7_** Python based framework implementing many packet generation and attack modules for Layer 2 and 3 protocols http://c0decafe.de/loki.html
- **lorcon 2.0.0.20091101** Generic library for injecting 802.11 frames http://802.11ninja.net/
- **lotophagi 0.1** a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases. http://packetstormsecurity.com/files/55250/lotophagi.rar.html
- **lsrtunnel 0.2** lsrtunnel spoofs connections using source routed packets. http://www.synacklabs.net/projects/lsrtunnel/
- **luksipc 0.01** A tool to convert unencrypted block devices to encrypted LUKS devices in-place. http://www.johannes-bauer.com/linux/luksipc
- **lynis 1.6.4** An auditing tool for Unix (specialists). http://www.rootkit.nl/projects/lynis.html
- **mac-robber 1.02** A digital investigation tool that collects data from allocated files in a mounted file system. http://www.sleuthkit.org/mac-robber/download.php
- **macchanger 1.6.0** A small utility to change your NIC's MAC address http://ftp.gnu.org/gnu/macchanger
- **maclookup 0.3** Lookup MAC addresses in the IEEE MA-L/OUI public listing. https://github.com/paraxor/maclookup
- **magicrescue 1.1.9** Find and recover deleted files on block devices http://freshmeat.net/projects/magicrescue/
- **magictree 1.3** A penetration tester productivity tool designed to allow easy and straightforward data consolidation, querying, external command execution and report generation http://www.gremwell.com
- **make-pdf 0.1.5** This tool will embed javascript inside a PDF document. http://blog.didierstevens.com/programs/pdf-tools/
- **makepasswd 1.10_9** Generates true random passwords with the emphasis on security over pronounceability (Debian version) http://packages.qa.debian.org/m/makepasswd.html malheur 0.5.4 A tool for the automatic analyze of malware behavior. http://www.mlsec.org/malheur/ maligno 1.2 An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS. http://www.encripto.no/tools/ malmon 0.3 Hosting exploit/backdoor detection daemon. It's written in python, and uses inotify (pyinotify) to monitor file system activity. It checks files smaller then some size, compares their md5sum and hex signatures against DBs with known exploits/backdoor. http://sourceforge.net/projects/malmon/ maltego 3.5.3 An open source intelligence and forensics application,

directly from the sources as listed at a number of sites. https://github.com/technoskald/maltrieve malware-check-tool 1.2 Python script that detects malicious files via checking md5 hashes from an offline set or via the virustotal site. It has http proxy support and an update feature. http://packetstormsecurity.com/files/93518/Malware-Check-Tool.2.html malwareanalyser 3.3 A freeware tool to perform static and dynamic analysis on malware. http://malwareanalyser.blogspot.de/2011/10/malware-analyser.html malwaredetect 0.1 Submits a file's SHA1 sum to VirusTotal to determine whether it is a known piece of malware http://www.virustotal.com malwasm 0.2 Offline debugger for malware's reverse engineering. https://code.google.com/p/malwasm/ marc4dasm 6.f11860f This python-based tool is a disassembler for the Atmel MARC4 (a 4 bit Harvard micro). https://github.com/ApertureLabsLtd/marc4dasm maskprocessor 0.71 A High-Performance word generator with a per-position configurable charset. http://hashcat.net/wiki/doku.php?id=maskprocessor masscan 391.a60cc70 TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes. https://github.com/robertdavidgraham/masscan mat 0.5 Metadata Anonymisation Toolkit composed of a GUI application, a CLI application and a library. https://mat.boum.org/ matahari 0.1.30 A reverse HTTP shell to execute commands on remote machines behind firewalls. http://matahari.sourceforge.net mausezahn 0.40 A free fast traffic generator written in C which allows you to send nearly every possible and impossible packet. http://www.perihel.at/sec/mz/ mbenum 1.5.0 Queries the master browser for whatever information it has registered. http://www.cqure.net/wp/mbenum/ mboxgrep 0.7.9 Mboxgrep is a small, non-interactive utility that scans mail folders for messages matching regular expressions. It does matching against basic and extended POSIX regular expressions, and reads and writes a variety of mailbox formats. http://mboxgrep.sourceforge.net md5deep 4.3 Advanced checksum hashing tool http://md5deep.sourceforge.net mdbtools 0.7.1 Utilities for viewing data and exporting schema from Microsoft Access Database files http://sourceforge.net/projects/mdbtools/ mdcrack 1.2 MD4/MD5/NTLM1 hash cracker http://c3rb3r.openwall.net/mdcrack/ mdk3 6 WLAN penetration tool http://homepages.tu-darmstadt.de/~p_larbig/wlan/ mdns-scan 0.5 Scan mDNS/DNS-SD published services on the local network. medusa 2.1.1 A speedy, massively parallel, modular, login brute-forcer for network. http://www.foofus.net/jmk/medusa/medusa.html melkor 1.0 An ELF fuzzer that mutates the existing data in an ELF sample given to create orcs (malformed ELFs), however, it does not change values randomly (dumb fuzzing), instead, it fuzzes certain metadata with semi-valid values through the use of fuzzing rules (knowledge

memfetch 0.05b dumps any userspace process memory without affecting its execution http://lcamtuf.coredump.cx/ metacoretex 0.8.0 MetaCoretex is an entirely JAVA vulnerability scanning framework for databases. http://metacoretex.sourceforge.net/ metagoofil 1.4b An information gathering tool designed for extracting metadata of public documents http://www.edge-security.com/metagoofil.php metasploit 29270.738fc78 An open source platform that supports vulnerability research, exploit development and the creation of custom security tools representing the largest collection of quality-assured exploits. http://www.metasploit.com metoscan 05 Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests. http://www.open-labs.org/ mfcuk 0.3.8 MIFARE Classic Universal toolKit http://code.google.com/p/mfcuk/ mfoc 0.10.7 Mifare Classic Offline Cracker http://code.google.com/p/mfoc/ mfsniffer 0.1 A python script for capturing unencrypted TSO login credentials. http://packetstormsecurity.com/files/120802/MF-Sniffer-TN3270-Password-Grabber.html mibble 2.9.3 Mibble is an open-source SNMP MIB parser (or SMI parser) written in Java. It can be used to read SNMP MIB files as well as simple ASN.1 files. http://www.mibble.org/ middler 1.0 A Man in the Middle tool to demonstrate protocol middling attacks. http://code.google.com/p/middler/ minimysqlator 0.5 A multi-platform application used to audit web sites in order to discover and exploit SQL injection vulnerabilities. http://www.scrt.ch/en/attack/downloads/mini-mysqlat0r miranda-upnp 1.3 A Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices http://code.google.com/p/miranda-upnp/ miredo 1.2.6 Teredo client and server. http://www.remlab.net/miredo/ missidentify 1.0 A program to find Win32 applications http://missidentify.sourceforge.net/ missionplanner 1.2.55 A GroundControl Station for Ardupilot. https://code.google.com/p/ardupilot-mega/wiki/Mission mitmap 0.1 Shell Script for launching a Fake AP with karma functionality and launches ettercap for packet capture and traffic manipulation. http://www.darkoperator.com/tools-and-scripts/ mitmer 22.b01c7fe A man-in-the-middle and phishing attack tool that steals the victim's credentials of some web services like Facebook. https://github.com/husam212/MITMer mitmf 169.83b4a93 A Framework for Man-In-The-Middle attacks written in Python. https://github.com/byt3bl33d3r/MITMf mitmproxy 0.10.1 SSL-capable man-in-the-middle HTTP proxy http://mitmproxy.org/ mkbrutus 1.0.2 Password bruteforcer for MikroTik devices or boxes running RouterOS. http://mkbrutusproject.github.io/MKBRUTUS/ mobiusft 0.5.21 An open-source forensic framework written in

TCP based network. https://code.google.com/p/modscan/ moloch 0.9.2 An open source large scale IPv4 full PCAP capturing, indexing and database system. https://github.com/aol/moloch monocle 1.0 A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network. http://packetstormsecurity.com/files/99823/Monocle-Host-Discovery-Tool.0.html morxbrute 1.01 A customizable HTTP dictionary-based password cracking tool written in Perl http://www.morxploit.com/morxbrute/ morxcrack 1.2 A cracking tool written in Perl to perform a dictionary-based attack on various hashing algorithm and CMS salted-passwords. http://www.morxploit.com/morxcrack/ mp3nema 0.4 A tool aimed at analyzing and capturing data that is hidden between frames in an MP3 file or stream, otherwise noted as "out of band" data. http://packetstormsecurity.com/files/76432/MP3nema-Forensic-Analysis-Tool.html mptcp 1.9.0 A tool for manipulation of raw packets that allows a large number of options. http://packetstormsecurity.com/files/119132/Mptcp-Packet-Manipulator.9.0.html mptcp-abuse 6.b0eeb27 A collection of tools and resources to explore MPTCP on your network. Initially released at Black Hat USA 2014. https://github.com/Neohapsis/mptcp-abuse ms-sys 2.4.0 A tool to write Win9x-.. master boot records (mbr) under linux – RTM! http://ms-sys.sourceforge.net/ mssqlscan 0.8.4 A small multi-threaded tool that scans for Microsoft SQL Servers. http://www.cqure.net/wp/mssqlscan/ msvpwn 0.1.r23.g328921b Bypass Windows' authentication via binary patching. https://bitbucket.org/mrabault/msvpwn mtr 0.85 Combines the functionality of traceroute and ping into one tool (CLI version) http://www.bitwizard.nl/mtr/ multiinjector 0.3 Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation. http://chaptersinwebsecurity.blogspot.de/2008/11/multiinjector-v03-released.html multimac 1.0.3 Multiple MACs on an adapter http://sourceforge.net/projects/multimac/ multitun 43.9804513 Tunnel arbitrary traffic through an innocuous WebSocket. https://github.com/covertcodes/multitun mutator 51.164132d This project aims to be a wordlist mutator with hormones, which means that some mutations will be applied to the result of the ones that have been already done, resulting in something like: corporation -> C0rp0r4t10n_2012 https://bitbucket.org/alone/mutator/ mysql2sqlite 1.dd87f4 Converts a mysqldump file into a Sqlite 3 compatible file https://gist.github.com/esperlu/943776 nacker 23.b67bb39 A tool to circumvent 802.1x Network Access Control on a wired LAN. https://github.com/carmaa/nacker nbnspoof 1.0 NBNSpoof – NetBIOS Name Service Spoofer http://www.mcgrewsecurity.com/tools/nbnspoof/ nbtenum 3.3 A utility for Windows that can

http://wiki.skullsecurity.org/Nbtool nbtscan 1.5.1 NBTscan is a program for scanning IP networks for NetBIOS name information. http://www.inetcat.net/software/nbtscan.html ncpfs 2.2.6 Allows you to mount volumes of NetWare servers under Linux. http://www.novell.com/ ncrack 0.4a A high-speed network authentication cracking tool http://nmap.org/ncrack/ nemesis 1.4 command-line network packet crafting and injection utility http://nemesis.sourceforge.net/ netactview 0.6.2 A graphical network connections viewer for Linux similar in functionality with Netstat http://netactview.sourceforge.net/index.html netbios-share-scanner 1.0 This tool could be used to check windows workstations and servers if they have accessible shared resources. http://www.secpoint.com/netbios-share-scanner.html netcommander 1.3 An easy-to-use arp spoofing tool. https://github.com/evilsocket/netcommander netcon 0.1 A network connection establishment and management script. http://www.paramecium.org/~leendert/ netdiscover 0.3 An active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks. http://nixgeneration.com/~jaime/netdiscover/ netmap 0.1.3 Can be used to make a graphical representation of the surounding network. http://netmap.sourceforge.net netmask 2.3.12 Helps determine network masks http://packages.qa.debian.org/n/netmask.html netreconn 1.76 A collection of network scan/recon tools that are relatively small compared to their larger cousins. http://packetstormsecurity.com/files/86076/NetReconn-Scanning-Tool-Collection.76.html netscan 1.0 Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection). http://packetstormsecurity.com/files/125569/Netscan-Port-Scanner.0.html netsed 1.2 Small and handful utility design to alter the contents of packets forwarded thru network in real time. http://silicone.homelinux.org/projects/netsed/ netsniff-ng 0.5.8 A high performance Linux network sniffer for packet inspection. http://netsniff-ng.org/ netzob 0.4.1 An open source tool for reverse engineering, traffic generation and fuzzing of communication protocols. http://www.netzob.org/ nfcutils 0.3.2 Provides a simple 'lsnfc' command that list tags which are in your NFC device field http://code.google.com/p/nfc-tools nfex 2.5 A tool for extracting files from the network in real-time or post-capture from an offline tcpdump pcap savefile. It is based off of the code-base from the apparently defunct project tcpxtract. https://code.google.com/p/nfex/ nfspy 1.0 A Python library for automating the falsification of NFS credentials when mounting an NFS share. https://github.com/bonsaiviking/NfSpy nfsshell 19980519 Userland NFS command tool. http://www.paramecium.org/~leendert/ ngrep 1.45 A grep-like utility that allows you to search for network

address(IPv4,IPv6), routing, FIB rules, traffic control. http://nield.sourceforge.net/ nikto 2.1.5 A web server scanner which performs comprehensive tests against web servers for multiple items http://www.cirt.net/nikto2 nimbostratus 54.c7c206f Tools for fingerprintinging and exploiting Amazon cloud infrastructures. https://github.com/andresriancho/nimbostratus nipper 0.11.7 Network Infrastructure Parser https://www.titania-security.com/ nishang 0.4.0 Using PowerShell for Penetration Testing. https://code.google.com/p/nishang/ nkiller2 2.0 A TCP exhaustion/stressing tool. http://sock-raw.org/projects.html nmap 6.47 Utility for network discovery and security auditing http://nmap.org/ nmbscan 1.2.6 Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols. http://nmbscan.gbarbier.org/ nomorexor 0.1 Tool to help guess a files 256 byte XOR key by using frequency analysis https://github.com/hiddenillusion/NoMoreXOR notspikefile 0.1 A Linux based file format fuzzing tool http://packetstormsecurity.com/files/39627/notSPIKEfile.tgz.html nsdtool 0.1 A netgear switch discovery tool. It contains some extra features like bruteoforce and setting a new password. http://www.curesec.com/en/publications/tools.html nsec3walker 20101223 Enumerates domain names using DNSSEC http://dnscurve.org/nsec3walker.html ntds-decode 0.1 This application dumps LM and NTLM hashes from active accounts stored in an Active Directory database. http://packetstormsecurity.com/files/121543/NTDS-Hash-Decoder.b.html o-saft 513.6bcc35b A tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. https://www.owasp.org/index.php/O-Saft oat 1.3.1 A toolkit that could be used to audit security within Oracle database servers. http://www.cqure.net/wp/test/ obexstress 0.1 Script for testing remote OBEX service for some potential vulnerabilities. http://bluetooth-pentest.narod.ru/ obfsproxy 0.2.12 A pluggable transport proxy written in Python. https://pypi.python.org/pypi/obfsproxy oclhashcat 1.30 Worlds fastest WPA cracker with dictionary mutation engine. http://hashcat.net/oclhashcat/ ocs 0.2 Compact mass scanner for Cisco routers with default telnet/enable passwords. http://packetstormsecurity.com/files/119462/OCS-Cisco-Scanner.2.html ohrwurm 0.1 A small and simple RTP fuzzer. http://mazzoo.de/ ollydbg 201g A 32-bit assembler-level analysing debugger http://www.ollydbg.de onesixtyone 0.7 An SNMP scanner that sends multiple SNMP requests to multiple IP addresses http://labs.portcullis.co.uk/application/onesixtyone/ onionshare 439.027d774 Securely and anonymously share a file of any size. https://github.com/micahflee/onionshare/ openstego 0.6.1 A tool implemented in Java for generic steganography, with support for password-based encryption of the data.

Command-Line Interface http://www.openvas.org/ openvas-libraries 7.0.6 The OpenVAS libraries http://www.openvas.org/ openvas-manager 5.0.7 A layer between the OpenVAS Scanner and various client applications http://www.openvas.org/ openvas-scanner 4.0.5 The OpenVAS scanning Daemon http://www.openvas.org/ ophcrack 3.6.0 A free Windows password cracker based on rainbow tables http://ophcrack.sourceforge.net orakelcrackert 1.00 This tool can crack passwords which are encrypted using Oracle's latest SHA1 based password protection algorithm. http://freeworld.thc.org/thc-orakelcrackert11g/ origami 1.2.7 Aims at providing a scripting tool to generate and analyze malicious PDF files. http://code.google.com/p/origami-pdf oscanner 1.0.6 An Oracle assessment framework developed in Java. http://www.cqure.net/wp/oscanner/ ostinato 0.5.1 An open-source, cross-platform packet/traffic generator and analyzer with a friendly GUI. It aims to be "Wireshark in Reverse" and thus become complementary to Wireshark. http://code.google.com/p/ostinato/ osueta 65.90323e2 A simple Python script to exploit the OpenSSH User Enumeration Timing Attack. https://github.com/c0r3dump3d/osueta owabf 1.3 Outlook Web Access bruteforcer tool. http://netsec.rs/70/tools.html owasp-bywaf 26.e730d1b A web application penetration testing framework (WAPTF). https://github.com/depasonico/OWASP-ByWaf owtf 1016.fef357e The Offensive (Web) Testing Framework. https://www.owasp.org/index.php/OWASP_OWTF p0f 3.08b Purely passive TCP/IP traffic fingerprinting tool. http://lcamtuf.coredump.cx/p0f3/ pack 0.0.4 Password Analysis and Cracking Kit http://thesprawl.org/projects/pack/ packerid 1.4 Script which uses a PEiD database to identify which packer (if any) is being used by a binary. http://handlers.sans.org/jclausing/ packet-o-matic 351 A real time packet processor. Reads the packet from an input module, match the packet using rules and connection tracking information and then send it to a target module. http://www.packet-o-matic.org/ packeth 1.7.2 A Linux GUI packet generator tool for ethernet. http://packeth.sourceforge.net/ packit 1.0 A network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. http://packit.sourceforge.net/ pacumen 1.92a0884 Packet Acumen – Analyse encrypted network traffic and more (side-channel attacks). https://github.com/bniemczyk/pacumen padbuster 0.3.3 Automated script for performing Padding Oracle attacks. http://www.gdssecurity.com/l/t.php paketto 1.10 Advanced TCP/IP Toolkit. http://www.doxpara.com/paketto panoptic 178.73b2b4c A tool that automates the process of search and retrieval of content for common log and config files through LFI vulnerability. https://github.com/lightos/Panoptic paros 3.2.13 Java-based HTTP/HTTPS proxy for assessing web app

tool. https://github.com/behindthefirewalls/Parsero pasco 20040505_1 Examines the contents of Internet Explorer's cache files for forensic purposes http://www.jonesdykstra.com/ passcracking 20131214 A little python script for sending hashes to passcracking.com and milw0rm http://github.com/jensp/passcracking passe-partout 0.1 Tool to extract RSA and DSA private keys from any process linked with OpenSSL. The target memory is scanned to lookup specific OpenSSL patterns. http://www.hsc.fr/ressources/outils/passe-partout/index.html.en passivedns 1.1.3 A network sniffer that logs all DNS server replies for use in a passive DNS setup. https://github.com/gamelinux/passivedns pastenum 0.4.1 Search Pastebins for content, fork from nullthreat corelan pastenum2 http://github.com/shadowbq/pastenum patator 80.5a140c1 A multi-purpose bruteforcer. https://github.com/lanjelot/patator pathod 0.11.1 Crafted malice for tormenting HTTP clients and servers. http://pathod.net/ pblind 1.0 Little utility to help exploiting blind sql injection vulnerabilities. http://www.edge-security.com/pblind.php pcapsipdump 0.2 A tool for dumping SIP sessions (+RTP traffic, if available) to disk in a fashion similar to 'tcpdump -w' (format is exactly the same), but one file per sip session (even if there is thousands of concurrect SIP sessions). http://pcapsipdump.sourceforge.net/ pcredz 0.9 A tool that extracts credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, and more from a pcap file or from a live interface. https://github.com/lgandx/PCredz pdf-parser 0.4.2 Parses a PDF document to identify the fundamental elements used in the analyzed file http://blog.didierstevens.com/programs/pdf-tools/ pdfbook-analyzer 2 Utility for facebook memory forensics. http://sourceforge.net/projects/pdfbook/ pdfcrack 0.12 Password recovery tool for PDF-files. http://pdfcrack.sourceforge.net/ pdfid 0.1.2 scan a file to look for certain PDF keywords http://blog.didierstevens.com/programs/pdf-tools/ pdfresurrect 0.12 A tool aimed at analyzing PDF documents. http://packetstormsecurity.com/files/118459/PDFResurrect-PDF-Analyzer.12.html pdgmail 1.0 A password dictionary attack tool that targets windows authentication via the SMB protocol http://www.jeffbryner.com/code/pdgmail peach 3.0.202 A SmartFuzzer that is capable of performing both generation and mutation based fuzzing http://peachfuzzer.com/ peda 51.327db44 Python Exploit Development Assistance for GDB. https://github.com/longld/peda peepdf 0.3 A Python tool to explore PDF files in order to find out if the file can be harmful or not http://eternal-todo.com/tools/peepdf-pdf-analysis-tool pentbox 1.8 A security suite that packs security and stability testing oriented tools for networks and systems. http://www.pentbox.net perl-image-exiftool 9.76 Reader and rewriter of EXIF informations that supports raw

http://pev.sourceforge.net/ pextractor 0.18b A forensics tool that can extract all files from an executable file created by a joiner or similar. http://packetstormsecurity.com/files/62977/PExtractor_v0.18b_binary_and_src.rar.html pgdbf 94.baa1d95 Convert XBase / FoxPro databases to PostgreSQL https://github.com/kstrauser/pgdbf phoss 0.1.13 Sniffer designed to find HTTP, FTP, LDAP, Telnet, IMAP4, VNC and POP3 logins. http://www.phenoelit.org/fr/tools.html php-mt-seed 3.2 PHP mt_rand() seed cracker http://www.openwall.com/php_mt_seed/ php-rfi-payload-decoder 30.bd42caa Decode and analyze RFI payloads developed in PHP. https://github.com/bwall/PHP-RFI-Payload-Decoder php-vulnerability-hunter 1.4.0.20 An whitebox fuzz testing tool capable of detected several classes of vulnerabilities in PHP web applications. https://phpvulnhunter.codeplex.com/ phpstress 5.f987a7e A PHP denial of service / stress test for Web Servers running PHP-FPM or PHP-CGI. https://github.com/nightlionsecurity/phpstress phrasendrescher 1.2.2 A modular and multi processing pass phrase cracking tool http://www.leidecker.info/projects/phrasendrescher/ pipal 1.1 A password analyser http://www.digininja.org/projects/pipal.php pirana 0.3.1 Exploitation framework that tests the security of a email content filter. http://www.guay-leroux.com/projects.html plcscan 0.1 This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols. http://packetstormsecurity.com/files/119726/PLC-Device-Scanner.html plecost 2 WordPress finger printer tool search and retrieve information about the plugins versions installed in WordPress systems. http://code.google.com/p/plecost/ plown 13.ccf998c A security scanner for Plone CMS. https://github.com/unweb/plown pmcma 1.00 Automated exploitation of invalid memory writes (being them the consequences of an overflow in a writable section, of a missing format string, integer overflow, variable misuse, or any other type of memory corruption). http://packetstormsecurity.com/files/104724/Post-Memory-Corruption-Memory-Analyzer.00.html pnscan 1.11 A parallel network scanner that can be used to survey TCP network services. http://www.lysator.liu.se/~pen/pnscan/ pompem 69.b2569c4 A python exploit tool finder. https://github.com/rfunix/Pompem portspoof 100.70b6bf2 This program's primary goal is to enhance OS security through a set of new techniques. http://portspoof.org/ posttester 0.1 A jar file that will send POST requests to servers in order to test for the hash collision vulnerability discussed at the Chaos Communication Congress in Berlin. http://packetstormsecurity.com/files/109010/MagicHash-Collision-Testing-Tool.html powerfuzzer 1_beta Powerfuzzer is a highly automated web fuzzer based on many other Open Source fuzzers

239.dc1a5e5 A PowerShell Post-Exploitation Framework. https://github.com/mattifestation/PowerSploit praeda 37.093d1c0 An automated data/information harvesting tool designed to gather critical information from various embedded devices. https://github.com/percx/Praeda prometheus 175.497b2ce A Firewall analyzer written in ruby https://github.com/averagesecurityguy/prometheus propecia 2 A fast class scanner that scans for a specified open port with banner grabbing http://www.redlevel.org protos-sip 2 SIP test suite. https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c07-sip proxychains-ng 4.8.1 A hook preloader that allows to redirect TCP traffic of existing dynamically linked programs through one or more SOCKS or HTTP proxies https://github.com/rofl0r/proxychains proxycheck 0.1 This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver. http://packetstormsecurity.com/files/61864/proxycheck.pl.txt.html proxyp 2013 Small multithreaded Perl script written to enumerate latency, port numbers, server names, & geolocations of proxy IP addresses. http://sourceforge.net/projects/proxyp/ proxyscan 0.3 A security penetration testing tool to scan for hosts and ports through a Web proxy server. http://packetstormsecurity.com/files/69778/proxyScan.3.tgz.html proxytunnel 1.9.0 a program that connects stdin and stdout to a server somewhere on the network, through a standard HTTPS proxy http://proxytunnel.sourceforge.net pscan 1.3 A limited problem scanner for C source files http://deployingradius.com/pscan/ pshitt 21.85cde65 A lightweight fake SSH server designed to collect authentication data sent by intruders. https://github.com/regit/pshitt pstoreview 1.0 Lists the contents of the Protected Storage. http://www.ntsecurity.nu/toolbox/pstoreview/ ptunnel 0.72 A tool for reliably tunneling TCP connections over ICMP echo request and reply packets http://www.cs.uit.no/~daniels/PingTunnel/#download pwd-hash 2.0 A password hashing tool that use the crypt function to generate the hash of a string given on standard input. http://vladz.devzero.fr/pwd-hash.php pwdump 7.1 Extracts the binary SAM and SYSTEM file from the filesystem and then the hashes. http://www.tarasco.org/security/pwdump_7/index.html pwnat 0.3 A tool that allows any number of clients behind NATs to communicate with a server behind a separate NAT with *no* port forwarding and *no* DMZ setup on any routers in order to directly communicate with each other http://samy.pl/pwnat/ pwntools 2.1.3 The CTF framework used by #Gallopsled in every CTF. https://github.com/Gallopsled/pwntools pyew 2.3.0 A python tool to analyse malware. https://code.google.com/p/pyew/ pyfiscan 1015.072ce1e Free web-application vulnerability and version scanner. https://github.com/fgeek/pyfiscan pyinstaller 2.1 A program that converts

127.0.0.1 A-record http://code.activestate.com/recipes/491264/ pyrasite 2.0 Code injection and introspection of running Python processes. http://pyrasite.com/ pyrit 0.4.0 WPA/WPA2-PSK attacking with gpu and cluster http://code.google.com/p/pyrit pytacle alpha2 Automates the task of sniffing GSM frames http://packetstormsecurity.com/files/124299/pytacle-alpha2.tar.gz pytbull 2.0 A python based flexible IDS/IPS testing framework shipped with more than 300 tests http://pytbull.sourceforge.net/ python-utidylib 0.2 Python bindings for Tidy HTML parser/cleaner. http://utidylib.berlios.de python2-binaryornot 0.3.0 Ultra-lightweight pure Python package to check if a file is binary or text. https://github.com/audreyr/binaryornot python2-yara 3.2.0 A malware identification and classification tool. https://github.com/plusvic/yara quickrecon 0.3.2 A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing. http://packetstormsecurity.com/files/104314/QuickRecon.3.2.html radamsa 0.3 General purpose data fuzzer. https://code.google.com/p/ouspg/wiki/Radamsa radare2 0.9.8 Open-source tools to disasm, debug, analyze and manipulate binary files. http://radare.org/ radiography 2 A forensic tool which grabs as much information as possible from a Windows system. http://www.security-projects.com/?RadioGraPhy rainbowcrack 1.2 Password cracker based on the faster time-memory trade-off. With MySQL and Cisco PIX Algorithm patches. http://project-rainbowcrack.com/ rarcrack 0.2 This program uses bruteforce algorithm to find correct password (rar, 7z, zip). http://rarcrack.sourceforge.net/ ratproxy 1.58 A passive web application security assessment tool http://code.google.com/p/ratproxy/ rawr 42.ff1bfa1 Rapid Assessment of Web Resources. A web enumerator. https://bitbucket.org/al14s/rawr/wiki/Home rcracki-mt 0.7.0 A tool to perform rainbow table attacks on password hashes. It is intended for indexed/perfected rainbow tables, mainly generated by the distributed project www.freerainbowtables.com http://rcracki.sourceforge.net/ rdesktop-brute 1.5.0 It connects to windows terminal servers – Bruteforce patch included. http://www.rdesktop.org/ reaver 1.4 Implements a brute force attack against wifi protected setup WPS registrar PINs in order to recover WPA/WPA2 passphrases http://code.google.com/p/reaver-wps rebind 0.3.4 DNS Rebinding Tool http://code.google.com/p/rebind/ recon-ng 885.f42ffbe A full-featured Web Reconnaissance framework written in Python. https://bitbucket.org/LaNMaSteR53/recon-ng recoverjpeg 2.2.2 Recover jpegs from damaged devices. http://www.rfc1149.net/devel/recoverjpeg recstudio 4.0_20130717 Cross platform interactive decompiler http://www.backerstreet.com/rec/rec.htm redfang 2.5 Finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the devices' Bluetooth addresses and calling read_remote_name().

http://www.hackingexposedvoip.com/ regeorg 26.22fb8a9 The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. https://github.com/sensepost/reGeorg reglookup 1.0.1 Command line utility for reading and querying Windows NT registries http://projects.sentinelchicken.org/reglookup relay-scanner 1.7 An SMTP relay scanner. http://www.cirt.dk replayproxy 1.1 Forensic tool to replay web-based attacks (and also general HTTP traffic) that were captured in a pcap file. https://code.google.com/p/replayproxy/ responder 117.6c7a5dd A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. https://github.com/SpiderLabs/Responder/ rfcat 130515 RF ChipCon-based Attack Toolset http://code.google.com/p/rfcat rfdump 1.6 A back-end GPL tool to directly inter-operate with any RFID ISO-Reader to make the contents stored on RFID tags accessible http://www.rfdump.org rfidiot e302bb7 An open source python library for exploring RFID devices. http://rfidiot.org/ rfidtool 0.01 A opensource tool to read / write rfid tags http://www.bindshell.net/tools/rfidtool.html ridenum 39.ebbfaca A null session RID cycle attack for brute forcing domain controllers. https://github.com/trustedsec/ridenum rifiuti2 0.5.1 A rewrite of rifiuti, a great tool from Foundstone folks for analyzing Windows Recycle Bin INFO2 file. https://code.google.com/p/rifiuti2/ rinetd 0.62 internet redirection server http://www.boutell.com/rinetd ripdc 0.2 A script which maps domains related to an given ip address or domainname. http://nullsecurity.net/tools/scanner rkhunter 1.4.2 Checks machines for the presence of rootkits and other unwanted tools. http://rkhunter.sourceforge.net/ rlogin-scanner 0.2 Multithreaded rlogin scanner. Tested on Linux, OpenBSD and Solaris. http://wayreth.eu.org/old_page/ rootbrute 0.1 Local root account bruteforcer. http://www.packetstormsecurity.org/ ropeadope 1.1 A linux log cleaner. http://www.highhacksociety.com/ ropeme 1.0 ROPME is a set of python scripts to generate ROP gadgets and payload. http://www.vnsecurity.net/2010/08/ropeme-rop-exploit-made-easy/ ropgadget 5.3 Lets you search your gadgets on your binaries (ELF format) to facilitate your ROP exploitation. https://github.com/JonathanSalwan/ROPgadget ropper 91.212d5da It can show information about files in different file formats and you can find gadgets to build rop chains for different architectures. For disassembly ropper uses the awesome Capstone Framework. https://github.com/sashs/Ropper rpdscan 2.a71b0f3 Remmina Password Decoder and scanner. https://github.com/freakyclown/RPDscan rrs 1.70 A reverse (connecting) remote shell. Instead of listening for incoming connections it will connect out to a listener (rrs in listen mode).

http://www.randomstorm.com/rsmangler-security-tool.php rtlsdr-scanner 856.a47ba2e A cross platform Python frequency scanning GUI for the OsmoSDR rtl-sdr library. https://github.com/EarToEarOak/RTLSDR-Scanner rtp-flood 1.0 RTP flooder http://www.hackingexposedvoip.com/ rtpbreak 1.3a Detects, reconstructs and analyzes any RTP session http://xenion.antifork.org/rtpbreak/ rubilyn 0.0.1 64bit Mac OS-X kernel rootkit that uses no hardcoded address to hook the BSD subsystem in all OS-X Lion & below. It uses a combination of syscall hooking and DKOM to hide activity on a host. http://nullsecurity.net/tools/backdoor.html ruby-msgpack 0.5.8 MessagePack, a binary-based efficient data interchange format. http://msgpack.org/ ruby-ronin 1.5.0 A Ruby platform for exploit development and security research. http://ronin-ruby.github.io/ ruby-ronin-support 0.5.1 A support library for Ronin. http://ronin-ruby.github.io/ ruby-uri-query_params 0.7.0 Access the query parameters of a URI, just like in PHP. http://github.com/postmodern/uri-query_params rww-attack 0.9.2 The Remote Web Workplace Attack tool will perform a dictionary attack against a live Microsoft Windows Small Business Server's 'Remote Web Workplace' portal. It currently supports both SBS 2003 and SBS 2008 and includes features to avoid account lock out. http://packetstormsecurity.com/files/79021/Remote-Web-Workplace-Attack-Tool.html safecopy 1.7 A disk data recovery tool to extract data from damaged media http://safecopy.sourceforge.net/ sakis3g 0.2.0e An all-in-one script for connecting with 3G http://www.sakis3g.org/ sambascan 0.5.0 Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds. http://sourceforge.net/projects/sambascan2/ samdump2 3.0.0 Dump password hashes from a Windows NT/2k/XP installation http://sourceforge.net/projects/ophcrack/files/samdump2/ samydeluxe 2.2ed1bac Automatic samdump creation script. http://github.com/jensp/samydeluxe sandy 6.531ab16 An open-source Samsung phone encryption assessment framework https://github.com/donctl/sandy sasm 3.1.0 A simple crossplatform IDE for NASM, MASM, GAS and FASM assembly languages. https://github.com/Dman95/SASM sb0x 19.04f40fe A simple and Lightweight framework for Penetration testing. https://github.com/levi0x0/sb0x-project sbd 1.36 Netcat-clone, portable, offers strong encryption – features AES-CBC + HMAC-SHA1 encryption, program execution (-e), choosing source port, continuous reconnection with delay + more http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=sbd scalpel 2.0 A frugal, high performance file carver http://www.digitalforensicssolutions.com/Scalpel/ scanmem 0.13 A utility used to locate the address of a variable in an executing process. http://code.google.com/p/scanmem/ scanssh 2.1 Fast

dhcp 0.1 schnappi can fuck network with no DHCP http://www.emanuelegentili.eu/ scout2 196.7cc58b4 Security auditing tool for AWS environments. http://isecpartners.github.io/Scout2/ scrapy 4419.c485a05 A fast high-level scraping and web crawling framework. http://www.scrapy.org/ scrounge-ntfs 0.9 Data recovery program for NTFS file systems http://memberwebs.com/stef/software/scrounge/ sctpscan 1.0 A network scanner for discovery and security http://www.p1sec.com/ seat 0.3 Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities. http://thesprawl.org/projects/search-engine-assessment-tool/ secscan 1.5 Web Apps Scanner and Much more utilities. http://code.google.com/p/secscan-py/ secure-delete 3.1 Secure file, disk, swap, memory erasure utilities. http://www.thc.org/ sees 67.cd741aa Increase the success rate of phishing attacks by sending emails to company users as if they are coming from the very same company's domain. https://github.com/galkan/sees/ sergio-proxy 0.2.1 A multi-threaded transparent HTTP proxy for manipulating web traffic https://github.com/darkoperator/dnsrecon sessionlist 1.0 Sniffer that intents to sniff HTTP packets and attempts to reconstruct interesting authentication data from websites that do not employ proper secure cookie auth. http://www.0xrage.com/ set 6.1.2 Social-engineer toolkit. Aimed at penetration testing around Social-Engineering https://www.trustedsec.com/downloads/social-engineer-toolkit sfuzz 0.7.0 A simple fuzzer. http://aconole.brad-x.com/programs/sfuzz.html shellcodecs 0.1 A collection of shellcode, loaders, sources, and generators provided with documentation designed to ease the exploitation and shellcode programming process. http://www.blackhatlibrary.net/Shellcodecs shellme 3.8c7919d Because sometimes you just need shellcode and opcodes quickly. This essentially just wraps some nasm/objdump calls into a neat script. https://github.com/hatRiot/shellme shellnoob 2.1 A toolkit that eases the writing and debugging of shellcode https://github.com/reyammer/shellnoob shortfuzzy 0.1 A web fuzzing script written in perl. http://packetstormsecurity.com/files/104872/Short-Fuzzy-Rat-Scanner.html sidguesser 1.0.5 Guesses sids/instances against an Oracle database according to a predefined dictionary file. http://www.cqure.net/wp/tools/database/sidguesser/ siege 3.0.8 An http regression testing and benchmarking utility http://www.joedog.org/JoeDog/Siege silk 3.9.0 A collection of traffic analysis tools developed by the CERT NetSA to facilitate security analysis of large networks. https://tools.netsa.cert.org/silk/ simple-ducky 1.1.1 A payload generator. https://code.google.com/p/simple-ducky-payload-generator simple-lan-scan 1.0 A simple

fingerprinting suite. http://www.networecon.com/tools/sinfp/ siparmyknife 11232011 A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications. http://packetstormsecurity.com/files/107301/sipArmyKnife_11232011.pl.txt sipcrack 0.2 A SIP protocol login cracker. http://www.remote-exploit.org/codes_sipcrack.html sipp 3.3 A free Open Source test tool / traffic generator for the SIP protocol. http://sipp.sourceforge.net/ sipsak 0.9.6 A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications. http://sipsak.org sipscan 0.1 A sip scanner. http://www.hackingvoip.com/sec_tools.html sipshock 6.1d636ab A scanner for SIP proxies vulnerable to Shellshock. https://github.com/zaf/sipshock sipvicious 0.2.8 Tools for auditing SIP devices http://blog.sipvicious.org skipfish 2.10b A fully automated, active web application security reconnaissance tool http://code.google.com/p/skipfish/ skyjack 7.5f7a25e Takes over Parrot drones, deauthenticating their true owner and taking over control, turning them into zombie drones under your own control. https://github.com/samyk/skyjack skype-dump 0.1 This is a tool that demonstrates dumping MD5 password hashes from the configuration file in Skype. http://packetstormsecurity.com/files/119155/Skype-Hash-Dumper.0.html skypefreak 30.14a81cb A Cross Platform Forensic Framework for Skype. http://osandamalith.github.io/SkypeFreak/ sleuthkit 4.1.3 File system and media management forensic analysis tools http://www.sleuthkit.org/sleuthkit slowhttptest 1.5 A highly configurable tool that simulates application layer denial of service attacks http://code.google.com/p/slowhttptest slowloris 0.7 A tool which is written in perl to test http-server vulnerabilites for connection exhaustion denial of service (DoS) attacks so you can enhance the security of your webserver. http://ha.ckers.org/slowloris/ smali 1.4.1 An assembler/disassembler for Android's dex format http://code.google.com/p/smali/ smartphone-pentest-framework 95.20918b2 Repository for the Smartphone Pentest Framework (SPF). https://github.com/georgiaw/Smartphone-Pentest-Framework smbbf 0.9.1 SMB password bruteforcer. http://packetstormsecurity.com/files/25381/smbbf.9.1.tar.gz.html smbexec 148.7827616 A rapid psexec style attack with samba tools. https://github.com/pentestgeek/smbexec smbrelay 3 SMB / HTTP to SMB replay attack toolkit. http://www.tarasco.org/security/smbrelay/ smtp-fuzz 1.0 Simple smtp fuzzer none smtp-user-enum 1.2 Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO. http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum smtp-vrfy 1.0 An SMTP Protocol Hacker. smtpmap 0.8.234_BETA Tool to identify the running smtp software on a given host. http://www.projectiwear.org/~plasmahh/software.html smtpscan

http://www.nullsecurity.net/tools/automation.html sniffjoke 0.4.1 Injects packets in the transmission flow that are able to seriously disturb passive analysis like sniffing, interception and low level information theft. http://www.delirandom.net/sniffjoke/ snmp-fuzzer 0.1.1 SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl. http://www.arhont.com/en/category/resources/tools-utilities/ snmpattack 1.8 SNMP scanner and attacking tool. http://www.c0decafe.de/ snmpcheck 1.8 A free open source utility to get information via SNMP protocols. http://www.nothink.org/perl/snmpcheck/ snmpenum 1.7 snmp enumerator http://www.filip.waeytens.easynet.be/ snmpscan 0.1 A free, multi-processes SNMP scanner http://www.nothink.org/perl/snmpscan/index.php snoopy-ng 93.e305420 A distributed, sensor, data collection, interception, analysis, and visualization framework. https://github.com/sensepost/snoopy-ng snort 2.9.6.1 A lightweight network intrusion detection system. http://www.snort.org snow 20130616 Steganography program for concealing messages in text files. http://darkside.com.au/snow/index.html snscan 1.05 A Windows based SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network. http://www.mcafee.com/uk/downloads/free-tools/snscan.aspx socat 1.7.2.4 Multipurpose relay http://www.dest-unreach.org/socat/ soot 2.5.0 A Java Bytecode Analysis and Transformation Framework. http://www.sable.mcgill.ca/soot spade 114 A general-purpose Internet utility package, with some extra features to help in tracing the source of spam and other forms of Internet harassment. http://www.hoobie.net/brutus/ sparty 0.1 An open source tool written in python to audit web applications using sharepoint and frontpage architecture. http://sparty.secniche.org/ spectools 2010_04_R1 Spectrum-Tools is a set of utilities for using the Wi-Spy USB spectrum analyzer hardware. Stable version. http://www.kismetwireless.net/spectools/ speedpwn 8.3dd2793 An active WPA/2 Bruteforcer, original created to prove weak standard key generation in different ISP labeled routers without a client is connected. https://gitorious.org/speedpwn/ spiderfoot 2.1.5 The Open Source Footprinting Tool http://spiderfoot.net/ spiderpig-pdffuzzer 0.1 A javascript pdf fuzzer https://code.google.com/p/spiderpig-pdffuzzer/ spiga 7240.3a804ac Configurable web resource scanner https://github.com/getdual/scripts-n-tools/blob/master/spiga.py spike 2.9 IMMUNITYsec's fuzzer creation kit in C http://www.immunitysec.com/resources-freesoftware.shtml spike-proxy 148 A Proxy for detecting vulnerabilities in web applications http://www.immunitysec.com/resources-freesoftware.shtml spiped 1.4.1 A utility for creating symmetrically encrypted and authenticated pipes between socket addresses. https://www.tarsnap.com/spiped.html spipscan 8340.db8ef4a SPIP (CMS) scanner for penetration testing

search exploit archives from exploit sites like exploit-db and packetstorm. https://github.com/BlackArch/sploitctl sploitego 153.d9568dc Maltego Penetration Testing Transforms. https://github.com/allfro/sploitego spooftooph 0.5.2 Designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain sight http://www.hackfromacave.com/projects/spooftooph.html sps 4.2 A Linux packet crafting tool. Supports IPv4, IPv6 including extension headers, and tunneling IPv6 over IPv4. https://sites.google.com/site/simplepacketsender/ sqid 0.3 A SQL injection digger. http://sqid.rubyforge.org/ sqlbrute 1.0 Brute forces data out of databases using blind SQL injection. http://www.justinclarke.com/archives/2006/03/sqlbrute.html sqlmap 6445.20c272b An automatic SQL injection tool developed in Python. http://sqlmap.sourceforge.net sqlninja 0.2.6_r1 A tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end http://sqlninja.sourceforge.net/ sqlpat 1.0.1 This tool should be used to audit the strength of Microsoft SQL Server passwords offline. http://www.cqure.net/wp/sqlpat/ sqlping 4 SQL Server scanning tool that also checks for weak passwords using wordlists. http://www.sqlsecurity.com/downloads sqlsus 0.7.2 An open source MySQL injection and takeover tool, written in perl http://sqlsus.sourceforge.net/ ssh-privkey-crack 0.3 A SSH private key cracker https://code.google.com/p/lusas/ sshatter 1.2 Password bruteforcer for SSH http://www.nth-dimension.org.uk/downloads.php?id=34 sshscan 7401.3bfd4ae A horizontal SSH scanner that scans large swaths of IPv4 space for a single SSH user and pass. https://github.com/getdual/scripts-n-tools/blob/master/sshscan.py sshtrix 0.0.2 A very fast multithreaded SSH login cracker http://nullsecurity.net/tools/cracker.html sshuttle 198.9ce2fa0 Transparent proxy server that works as a poor man's VPN. Forwards all TCP packets over ssh (and even DNS requests when using –dns option). Doesn't require admin privileges on the server side. https://github.com/apenwarr/sshuttle ssl-hostname-resolver 1 CN (Common Name) grabber on X.509 Certificates over HTTPS. http://packetstormsecurity.com/files/120634/Common-Name-Grabber-Script.html ssl-phuck3r 2.0 All in one script for Man-In-The-Middle attacks. https://github.com/zombiesam/ssl_phuck3r sslcat 1.0 SSLCat is a simple Unix utility that reads and writes data across an SSL enable network connection. http://www.bindshell.net/tools/sslcat sslcaudit 522.5b6be3e Utility to perform security audits of SSL/TLS clients. https://github.com/grwl/sslcaudit ssldump 0.9b3 an SSLv3/TLS network protocol analyzer

http://thesprawl.org/projects/latest/ sslnuke 5.c5faeaa Transparent proxy that decrypts SSL traffic and prints out IRC messages. https://github.com/jtripper/sslnuke sslscan 239.1328b49 Tests SSL/TLS enabled services to discover supported cipher suites. https://github.com/DinoTools/sslscan sslsniff 0.8 A tool to MITM all SSL connections on a LAN and dynamically generate certs for the domains that are being accessed on the fly http://www.thoughtcrime.org/software/sslsniff/ sslsplit 0.4.9 A tool for man-in-the-middle attacks against SSL/TLS encrypted network connections. http://www.roe.ch/SSLsplit sslstrip 0.9 Transparently hijack http traffic on a network, watch for https links and redirects, then map those links. http://www.thoughtcrime.org/software/sslstrip sslyze 0.10 Python tool for analyzing the configuration of SSL servers and for identifying misconfigurations. https://github.com/nabla-c0d3/sslyze/ stackflow 2.2af525d Universal stack-based buffer overfow exploitation tool. https://github.com/d4rkcat/stackflow starttls-mitm 7.b257756 A mitm proxy that will transparently proxy and dump both plaintext and TLS traffic. https://github.com/ipopov/starttls-mitm statsprocessor 0.10 A high-performance word-generator based on per-position Markov-attack. http://hashcat.net/wiki/doku.php?id=statsprocessor steghide 0.5.1 Embeds a message in a file by replacing some of the least significant bits http://steghide.sourceforge.net stompy 0.0.4 an advanced utility to test the quality of WWW session identifiers and other tokens that are meant to be unpredictable. http://lcamtuf.coredump.cx/ storm-ring 0.1 This simple tool is useful to test a PABX with “allow guest” parameter set to “yes” (in this scenario an anonymous caller could place a call). http://packetstormsecurity.com/files/115852/Storm-Ringing-PABX-Test-Tool.html stunnel 5.06 A program that allows you to encrypt arbitrary TCP connections inside SSL http://www.stunnel.org subdomainer 1.2 A tool designed for obtaining subdomain names from public sources. http://www.edge-security.com/subdomainer.php subterfuge 5.0 Automated Man-in-the-Middle Attack Framework http://kinozoa.com sucrack 1.2.3 A multi-threaded Linux/UNIX tool for brute-force cracking local user accounts via su http://labs.portcullis.co.uk/application/sucrack sulley 1.0.cb5e62c A pure-python fully automated and unattended fuzzing framework. https://github.com/OpenRCE/sulley/ superscan 4 Powerful TCP port scanner, pinger, resolver. http://www.foundstone.com/us/resources/proddesc/superscan.htm suricata 2.0.3 An Open Source Next Generation Intrusion Detection and Prevention Engine. http://openinfosecfoundation.org/index.php/download-suricata svn-extractor 28.3af00fb A simple script to extract all web resources by means of .SVN folder exposed over network. https://github.com/anantshri/svn-

analyzer for SWF external movies. It helps to find flaws in Flash. http://code.google.com/p/swfintruder/ synflood 0.1 A very simply script to illustrate DoS SYN Flooding attack. http://thesprawl.org/projects/syn-flooder/ synner 1.1 A custom eth->ip->tcp packet generator (spoofer) for testing firewalls and dos attacks. http://packetstormsecurity.com/files/69802/synner.c.html synscan 5.02 fast asynchronous half-open TCP portscanner http://www.digit-labs.org/files/tools/synscan/ sysdig 1314.45921f5 Open source system-level exploration and troubleshooting tool. http://www.sysdig.org/ sysinternals-suite 1.2 Sysinternals tools suite. http://sysinternals.com/ t50 5.4.1 Experimental Multi-protocol Packet Injector Tool http://t50.sourceforge.net/ taof 0.3.2 Taof is a GUI cross-platform Python generic network protocol fuzzer. http://taof.sf.net tbear 1.5 Transient Bluetooth Environment Auditor includes an ncurses-based Bluetooth scanner (a bit similar to kismet), a Bluetooth DoS tool, and a Bluetooth hidden device locator. http://freshmeat.net/projects/t-bear tcgetkey 0.1 A set of tools that deal with acquiring physical memory dumps via FireWire and then scan the memory dump to locate TrueCrypt keys and finally decrypt the encrypted TrueCrypt container using the keys. http://packetstormsecurity.com/files/119146/tcgetkey.1.html tcpcontrol-fuzzer 0.1 2^6 TCP control bit fuzzer (no ECN or CWR). https://www.ee.oulu.fi/research/ouspg/tcpcontrol-fuzzer tcpdump 4.6.2 A tool for network monitoring and data acquisition http://www.tcpdump.org tcpextract 1.1 Extracts files from captured TCP sessions. Support live streams and pcap files. https://pypi.python.org/pypi/tcpextract/1.1 tcpflow 1.4.4 Captures data transmitted as part of TCP connections then stores the data conveniently http://afflib.org/software/tcpflow tcpick 0.2.1 TCP stream sniffer and connection tracker http://tcpick.sourceforge.net/ tcpjunk 2.9.03 A general tcp protocols testing and hacking utility http://code.google.com/p/tcpjunk tcpreplay 4.0.5 Gives the ability to replay previously captured traffic in a libpcap format http://tcpreplay.appneta.com tcptraceroute 1.5beta7 A traceroute implementation using TCP packets. http://michael.toren.net/code/tcptraceroute/ tcpwatch 1.3.1 A utility written in Python that lets you monitor forwarded TCP connections or HTTP proxy connections. http://hathawaymix.org/Software/TCPWatch tcpxtract 1.0.1 A tool for extracting files from network traffic. http://tcpxtract.sourceforge.net teardown 1.0 Command line tool to send a BYE request to tear down a call. http://www.hackingexposedvoip.com/ tekdefense-automater 52.6d0bd5a IP URL and MD5 OSINT Analysis https://github.com/1aN0rmus/TekDefense-Automater termineter 0.1.0 Smart meter testing framework https://code.google.com/p/termineter/ tftp-bruteforce 0.1 TFTP-bruteforcer is a fast TFTP filename bruteforcer written in perl.

requested content from an upstream tftp server. Meanwhile modifications to the content can be done by pluggable modules. So this one's nice if your mitm with some embedded devices. http://www.c0decafe.de/ thc-ipv6 2.5 A complete tool set to attack the inherent protocol weaknesses of IPv6 and ICMP6, and includes an easy to use packet factory library. http://thc.org/thc-ipv6/ thc-keyfinder 1.0 Finds crypto keys, encrypted data and compressed data in files by analyzing the entropy of parts of the file. https://www.thc.org/releases.php thc-pptp-bruter 0.1.4 A brute force program that works against pptp vpn endpoints (tcp port 1723). http://www.thc.org thc-smartbrute 1.0 This tool finds undocumented and secret commands implemented in a smartcard. https://www.thc.org/thc-smartbrute/ thc-ssl-dos 1.4 A tool to verify the performance of SSL. To be used in your authorized and legitimate area ONLY. You need to accept this to make use of it, no use for bad intentions, you have been warned! http://www.thc.org/thc-ssl-dos/ theharvester 2.2a Python tool for gathering e-mail accounts and subdomain names from different public sources (search engines, pgp key servers) http://www.edge-security.com/theHarvester.php themole 0.3 Automatic SQL injection exploitation tool. http://sourceforge.net/projects/themole/ tiger 3.2.3 A security scanner, that checks computer for known problems. Can also use tripwire, aide and chkrootkit. http://www.nongnu.org/tiger/ tilt 90.2bc2ef2 An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup. https://github.com/AeonDave/tilt timegen 0.4 This program generates a *.wav file to "send" an own time signal to DCF77 compatible devices. http://bastianborn.de/radio-clock-hack/ tinc 1.0.24 VPN (Virtual Private Network) daemon http://www.tinc-vpn.org/ tinyproxy 1.8.3 A light-weight HTTP proxy daemon for POSIX operating systems. https://banu.com/tinyproxy/ tlsenum 75.6618285 A command line tool to enumerate TLS cipher-suites supported by a server. https://github.com/Ayrx/tlsenum tlspretense 0.6.2 SSL/TLS client testing framework https://github.com/iSECPartners/tlspretense tlssled 1.3 A Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. http://blog.taddong.com/2011/05/tlssled-v10.html tnscmd 1.3 a lame tool to prod the oracle tnslsnr process (1521/tcp) http://www.jammed.com/~jwa/hacks/security/tnscmd/ topera 19.3e230fd An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort. https://github.com/toperaproject/topera tor 0.2.5.10 Anonymizing overlay network. http://www.torproject.org/ tor-autocircuit 0.2 Tor Autocircuit was developed to give users a finer control over Tor circuit creation. The tool exposes the functionality of TorCtl library which allows its users to control circuit length, speed, geolocation, and other parameters.

POST Denial of Service testing tool written in Python. http://sourceforge.net/projects/torshammer/ torsocks 2.0.0 Wrapper to safely torify applications http://code.google.com/p/torsocks tpcat latest TPCAT is based upon pcapdiff by the EFF. TPCAT will analyze two packet captures (taken on each side of the firewall as an example) and report any packets that were seen on the source capture but didn't make it to the dest. http://sourceforge.net/projects/tpcat/ traceroute 2.0.21 Tracks the route taken by packets over an IP network http://traceroute.sourceforge.net/ trid 2.11 An utility designed to identify file types from their binary signatures http://mark0.net/soft-trid-e.html trinity 3728.985a087 A Linux System call fuzzer. http://codemonkey.org.uk/projects/trinity/ trixd00r 0.0.1 An advanced and invisible userland backdoor based on TCP/IP for UNIX systems http://nullsecurity.net/tools/backdoor.html truecrack 35 Password cracking for truecrypt(c) volumes. http://code.google.com/p/truecrack/ truecrypt 7.1a Free open-source cross-platform disk encryption software http://www.truecrypt.org/ tsh 0.6 An open-source UNIX backdoor that compiles on all variants, has full pty support, and uses strong crypto for communication. http://packetstormsecurity.com/search/?q=tsh tsh-sctp 2.850a2da An open-source UNIX backdoor. https://github.com/infodox/tsh-sctp tuxcut 5.0 Netcut-like program for Linux written in PyQt http://bitbucket.org/a_atalla/tuxcut/ twofi 2.0 Twitter Words of Interest. http://www.digininja.org/projects/twofi.php u3-pwn 2.0 A tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install http://www.nullsecurity.net/tools/backdoor.html uatester 1.06 User Agent String Tester http://code.google.com/p/ua-tester/ ubertooth 2012.10.R1 A 2.4 GHz wireless development board suitable for Bluetooth experimentation. Open source hardware and software. Tools only http://sourceforge.net/projects/ubertooth/ ubitack 0.3 Tool, which automates some of the tasks you might need on a (wireless) penetration test or while you are on the go. https://code.google.com/p/ubitack/ udis86 1.7.2 A minimalistic disassembler library http://udis86.sourceforge.net/ udptunnel 19 Tunnels TCP over UDP packets. http://code.google.com/p/udptunnel/ uefi-firmware-parser 103.9d4d220 Parse BIOS/Intel ME/UEFI firmware related structures: Volumes, FileSystems, Files, etc https://github.com/theopolis/uefi-firmware-parser ufo-wardriving 4 Allows you to test the security of wireless networks by detecting their passwords based on the router model http://www.ufo-wardriving.com/ ufonet 9.5484a90 A tool designed to launch DDoS attacks against a target, using 'Open Redirect' vectors on third party web applications, like botnet. https://github.com/epsylon/ufonet umap 25.3ad8121 The USB host security assessment tool.

http://sourceforge.net/projects/unhide/ unicorn 9.a18cb5d A simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. https://github.com/trustedsec/unicorn unicornscan 0.4.7 A new information gathering and correlation engine. http://www.unicornscan.org/ uniofuzz 1337 The universal fuzzing tool for browsers, web services, files, programs and network services/ports http://nullsecurity.net/tools/fuzzer.html uniscan 6.2 A simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner. http://sourceforge.net/projects/uniscan/ unix-privesc-check 1.4 Tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases) http://pentestmonkey.net/tools/audit/unix-privesc-check unsecure 1.2 Bruteforces network login masks. http://www.sniperx.net/ upnpscan 0.4 Scans the LAN or a given address range for UPnP capable devices. http://www.cqure.net/wp/upnpscan/ upx 3.91 Ultimate executable compressor. http://upx.sourceforge.net/ urlcrazy 0.5 Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage. http://www.morningstarsecurity.com/research/urlcrazy urldigger 02c A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code https://code.google.com/p/urldigger/ username-anarchy 0.2 Tools for generating usernames when penetration testing http://www.morningstarsecurity.com/research/username-anarchy usernamer 7.813139d Pentest Tool to generate usernames/logins based on supplied names. https://github.com/jseidl/usernamer uw-loveimap 0.1 Multi threaded imap bounce scanner. http://uberwall.org/bin/download/45/UWloveimap.tgz uw-offish 0.1 Clear-text protocol simulator. http://uberwall.org/bin/download/42/UW_offish.1.tar.gz uw-udpscan 0.1 Multi threaded udp scanner. http://uberwall.org/bin/download/44/UWudpscan.tar.gz uw-zone 0.1 Multi threaded, randomized IP zoner. http://uberwall.org/bin/download/43/UWzone.tgz v3n0m 77.cdaf14e Popular linux version of Balthazar/NovaCygni's 'v3n0m' scanner. Searches 18k+ dorks over 13 search engines. https://github.com/v3n0m-Scanner/V3n0M-Scanner valgrind 3.10.1 A tool to help find memory-management problems in programs http://valgrind.org/ vanguard 0.1 A comprehensive web penetration testing tool written in Perl thatidentifies vulnerabilities in web applications. http://packetstormsecurity.com/files/110603/Vanguard-Pentesting-Scanner.html vbrute 1.11dda8b Virtual hosts brute forcer. https://github.com/nccgroup/vbrute vega 1.0 An open source platform to test the security of web applications https://github.com/subgraph/Vega/wiki veil 276.f6dc4ff A tool designed to generate metasploit payloads that bypass common anti-virus solutions.

https://www.torproject.org/vidalia videosnarf 0.63 A new security assessment tool for pcap analysis http://ucsniff.sourceforge.net/videosnarf.html vinetto 0.07beta A forensics tool to examine Thumbs.db files http://vinetto.sourceforge.net viper 501.5f6a19a A Binary analysis framework. https://github.com/botherder/viper viproy-voipkit 2.0 VoIP Pen-Test Kit for Metasploit Framework http://viproy.com/ vivisect 20140803 A Python based static analysis and reverse engineering framework, Vdb is a Python based research/reversing focused debugger and programatic debugging API by invisigoth of kenshoto http://visi.kenshoto.com/ vnak 1.cf0fda7 Aim is to be the one tool a user needs to attack multiple VoIP protocols. https://www.isecpartners.com/vnak.html vnc-bypauth 0.0.1 Multi-threaded bypass authentication scanner for VNC servers <= 4.1.1. http://pentester.fr/resources/tools/techno/VNC/VNC_bypauth/ vncrack 1.21 What it looks like: crack VNC. http://phenoelit-us.org/vncrack voiper 0.07 A VoIP security testing toolkit incorporating several VoIP fuzzers and auxilliary tools to assist the auditor. http://voiper.sourceforge.net/ voiphopper 2.04 A security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN. http://voiphopper.sourceforge.net/ voipong 2.0 A utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to seperate wave files. http://www.enderunix.org/voipong/ volatility 2.4.1 A memory forensics toolkit. https://www.volatilesystems.com/default/volatility vstt 0.5.0 VSTT is a multi-protocol tunneling tool. It accepts input by TCP stream sockets and FIFOs, and can send data via TCP, POP3, and ICMP tunneling. http://www.wendzel.de/dr.org/files/Projects/vstt/ vulscan 2.0 A module which enhances nmap to a vulnerability scanner http://www.computec.ch/projekte/vulscan/ w3af 1.6 Web Application Attack and Audit Framework. http://w3af.sourceforge.net/ waffit 30 A set of security tools to identify and fingerprint Web Application Firewall/WAF products protecting a website http://code.google.com/p/waffit/ wafp 0.01_26c3 An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints. http://packetstormsecurity.com/files/84468/Web-Application-Finger-Printer.01-26c3.html wapiti 2.3.0 A vulnerability scanner for web applications. It currently search vulnerabilities like XSS, SQL and XPath injections, file inclusions, command execution, LDAP injections, CRLF injections... http://wapiti.sourceforge.net/ wavemon 0.7.6 Ncurses-based monitoring application for wireless network devices http://eden-feed.erg.abdn.ac.uk/wavemon/ web-soul 2 A plugin based scanner for attacking and data mining web sites

responses using dynamically generated queries and more. Useful for penetration tests against web servers. http://code.google.com/p/webenum/ webhandler 0.8.5 A handler for PHP system functions & also an alternative 'netcat' handler. https://github.com/lnxg33k/webhandler webpwn3r 35.3fb27bb A python based Web Applications Security Scanner. https://github.com/zigoo0/webpwn3r webrute 3.3 Web server directory brute forcer. https://github.com/BlackArch/webrute webscarab 20120422.001828 Framework for analysing applications that communicate using the HTTP and HTTPS protocols http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project webshag 1.10 A multi-threaded, multi-platform web server audit tool. http://www.scrt.ch/en/attack/downloads/webshag webshells 6.690ebd9 Web Backdoors. https://github.com/BlackArch/webshells webslayer 5 A tool designed for brute forcing Web Applications https://code.google.com/p/webslayer/ websockify 0.6.0 WebSocket to TCP proxy/bridge. http://github.com/kanaka/websockify webspa 0.7 A web knocking tool, sending a single HTTP/S to run O/S commands. http://sourceforge.net/projects/webspa/ websploit 3.0.0 An Open Source Project For, Social Engineering Works, Scan, Crawler & Analysis Web, Automatic Exploiter, Support Network Attacks http://code.google.com/p/websploit/ weevely 1.1 Stealth tiny web shell http://epinna.github.io/Weevely/ wepbuster 1.0_beta_0.7 script for automating aircrack-ng http://code.google.com/p/wepbuster/ wfuzz 24.1c6ecd8 Utility to bruteforce web applications to find their not linked resources. https://github.com/xmendez/wfuzz whatweb 0.4.7 Next generation web scanner that identifies what websites are running. http://www.morningstarsecurity.com/research/whatweb wi-feye 1.0 An automated wireless penetration testing tool written in python, its designed to simplify common attacks that can be performed on wifi networks so that they can be executed quickly and easily. http://wi-feye.za1d.com/download.php wifi-honey 1.0 A management tool for wifi honeypots http://www.digininja.org/projects/wifi_honey.php wifi-monitor 0.r22.71340a3 Prints the IPs on your local network that're sending the most packets https://github.com/DanMcInerney/wifi-monitor wificurse 0.3.9 WiFi jamming tool. https://github.com/oblique/wificurse wifijammer 43.4a0fe56 A python script to continuosly jam all wifi clients within range. https://github.com/DanMcInerney/wifijammer wifiphisher 17.09cf393 Fast automated phishing attacks against WPA networks. https://github.com/sophron/wifiphisher wifitap 2b16088 WiFi injection tool through tun/tap device. https://github.com/GDSSecurity/wifitap wifite 2.28fc5cd A tool to attack multiple WEP and WPA encrypted networks at the same time. http://code.google.com/p/wifite/ wig 291.14f19bd WebApp

Windows NT/2000/XP/2003 systems. http://sourceforge.net/projects/winexe/ winfo 2.0 Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. http://www.ntsecurity.nu/toolbox/winfo/ wireless-ids 24.b132071 Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets. https://github.com/SYWorks/wireless-ids wireshark-cli 1.12.2 a free network protocol analyzer for Unix/Linux and Windows – CLI version http://www.wireshark.org/ wireshark-gtk 1.12.2 a free network protocol analyzer for Unix/Linux and Windows – GTK frontend http://www.wireshark.org/ wirouter-keyrec 1.1.2 A powerful and platform independent software to recover the default WPA passphrases of the supported router models (Telecom Italia Alice AGPF, Fastweb Pirelli, Fastweb Tesley, Eircom Netopia, Pirelli TeleTu/Tele 2). http://www.salvatorefresta.net/tools/ witchxtool 1.1 A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner. http://packetstormsecurity.com/files/97465/Witchxtool-Port-LFI-SQL-Scanner-And-MD5-Bruteforcing-Tool.1.html wlan2eth 1.3 re-writes 802.11 captures into standard Ethernet frames. http://www.willhackforsushi.com/?page_id=79 wmat 0.1 Automatic tool for testing webmail accounts http://netsec.rs/70/tools.html wnmap 0.1 A shell script written with the purpose to automate and chain scans via nmap. You can run nmap with a custom mode written by user and create directories for every mode with the xml/nmap files inside. http://nullsecurity.net/tools/automation.html wol-e 2.0 A suite of tools for the Wake on LAN feature of network attached computers http://code.google.com/p/wol-e/ wordpot 37.e42eeda A WordPress Honeypot. https://github.com/gbrindisi/wordpot wpbf 7.11b6ac1 Multithreaded WordPress brute forcer. https://github.com/dejanlevaja/wpbf wpscan 1803.88808db A vulnerability scanner which checks the security of WordPress installations using a black box approach. http://wpscan.org ws-attacker 1.3 A modular framework for web services penetration testing. http://ws-attacker.sourceforge.net/ wsfuzzer 1.9.5 A Python tool written to automate SOAP pentesting of web services. https://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project wyd 0.2 Gets keywords from personal files. IT security/forensic tool. http://www.remote-exploit.org/?page_id=418 x-scan 3.3 A general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable. http://www.xfocus.org/ xcavator 5.bd9e2d8

http://www.spice-space.org/ xorbruteforcer 0.1 Script that implements a XOR bruteforcing of a given file, although a specific key can be used too. http://eternal-todo.com/category/bruteforce xorsearch 1.11.1 Program to search for a given string in an XOR, ROL or ROT encoded binary file. http://blog.didierstevens.com/programs/xorsearch/ xortool 0.96 A tool to analyze multi-byte xor cipher. https://github.com/hellman/xortool/ xplico 33.0f6d8bc Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT). http://www.xplico.org/ xprobe2 0.3 An active OS fingerprinting tool. http://sourceforge.net/apps/mediawiki/xprobe/index.php?title=Main_Page xspy 1.0c A utility for monitoring keypresses on remote X servers http://www.freshports.org/security/xspy/ xsser 1.6 A penetration testing tool for detecting and exploiting XSS vulnerabilites. http://xsser.sourceforge.net/ xssless 35.9eee648 An automated XSS payload generator written in python. https://github.com/mandatoryprogrammer/xssless xsss 0.40b A brute force cross site scripting scanner. http://www.sven.de/xsss/ xssscan 8340.db8ef4a Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS. https://github.com/gwroblew/detectXSSlib xsssniper 0.9 An automatic XSS discovery tool https://github.com/gbrindisi/xsssniper xssya 13.15ebdfe A Cross Site Scripting Scanner & Vulnerability Confirmation. https://github.com/yehia-mamdouh/XSSYA yara 3.2.0 A malware identification and classification tool. https://plusvic.github.io/yara/ ycrawler 0.1 A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support. http://packetstormsecurity.com/files/98546/yCrawler-Web-Crawling-Utility.html yersinia 0.7.1 A network tool designed to take advantage of some weakness in different network protocols http://www.yersinia.net/ yinjector 0.1 A MySQL injection penetration tool. It has multiple features, proxy support, and multiple exploitation methods. http://packetstormsecurity.com/files/98359/yInjector-MySQL-Injection-Tool.html zackattack 5.1f96c14 A new tool set to do NTLM Authentication relaying unlike any other tool currently out there. https://github.com/urbanesec/ZackAttack/ zaproxy 2.3.1 A local intercepting proxy with integrated penetration testing tool for finding vulnerabilities in web applications. http://code.google.com/p/zaproxy/ zarp 0.1.5 A network attack tool centered around the exploitation of local networks. https://defense.ballastsecurity.net/wiki/index.php/Zarp zerowine 0.0.2 Malware Analysis Tool – research project to dynamically analyze the behavior of malware http://zerowine.sf.net/ zmap 1.2.1 Fast network scanner designed for Internet-wide network surveys. https://zmap.io/ zulu 0.1 A light weight 802.11 wireless frame

derived on some models of ZyXEL routers. http://packetstormsecurity.com/files/119156/Zykeys-Wireless-Tool.html zzuf 0.13 Transparent application input fuzzer. http://sam.zoy.org/zzuf/

Share this:

Twitter Facebook

Like

Be the first to like this.

PREVIOUS

NEXT

Leave a Reply

Enter your comment here...