acccheck	The tool is designed as a password dictionary attack tool that targets windows authentication via the SMB protocol. It is really a wrapper script around the 'smbclient' binary, and as a result is dependent on it for its execution.
ace-voip	ACE (Automated Corporate Enumerator) is 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. In the same way that the "corporate directory" feature of VoIP hardphones enables users to easily dial by name via their VoIP handsets, ACE was developed as a research idea born from "VoIP Hopper" to automate VoIP attacks that can be targeted against names in an enterprise Directory. The concept is that in the future, attacks will be carried out against users based on their name, rather than targeting VoIP traffic against random RTP audio streams or IP addresses. ACE works by using DHCP, TFTP, and HTTP in order to download the VoIP corporate directory. It then outputs the directory to a text file, which can be used as input to other VoIP assessment tools.
Aircrack-ng	Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Amap	Amap was the first next-generation scanning tool for pentesters. It attempts to identify applications even if they are running on a different port than normal. It also identifies non-ascii based applications. This is achieved by sending trigger packets, and looking up the responses in a list of response strings.
android-sdk	The Android SDK provides you the API libraries and developer tools necessary to build, test, and debug apps for Android.
apache-users	This Perl script will enumerate the usernames on any system that uses Apache with the UserDir module.
apktool	It is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications; it makes possible to debug smali code step by step. Also it makes working with app easier because of project-like files structure and automation of some repetitive tasks like building apk, etc. It is NOT intended for piracy and other non-legal uses. It could be used for localizing, adding some features or support for custom platforms and other GOOD purposes. Just try to be fair with authors of an app, that you use and probably like. Features: decoding resources to nearly original form (including resources.arsc, XMLs and 9.png files) and rebuilding them smali debugging: SmaliDebugging helping with some repetitive tasks
Arachni	Arachni is an Open Source, feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications. It is smart, it trains itself by learning from the HTTP responses it receives during the audit process and is able to perform meta-analysis using a number of factors in order to correctly assess the trustworthiness of results and intelligently identify false-positives. It is versatile enough to cover a great deal of use cases, ranging from a simple command line scanner utility, to a global high performance grid of scanners, to a Ruby library allowing for scripted audits, to a multi-user multi-scan web collaboration platform.
Arduino	Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. It's intended for artists, designers, hobbyists, and anyone interested in creating interactive objects or environments.
Armitage	Armitage is a scriptable red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the advanced post-exploitation features in the framework. Through one Metasploit instance, your team will: Use the same sessions Share hosts, captured data, and downloaded files Communicate through a shared event log. Run bots to automate red team tasks. Armitage is a force multiplier for red team operations.
Asleap	Demonstrates a serious deficiency in proprietary Cisco LEAP networks. Since LEAP uses a variant of MS-CHAPv2 for the authentication exchange, it is susceptible to accelerated offline dictionary attacks. Asleap can also attack the Point-to-Point Tunneling Protocol (PPTP), and any MS-CHAPv2 exchange where you can specify the challenge and response values on the command line.
Automater	Automater is a URL/Domain, IP Address, and Md5 Hash OSINT tool aimed at making the analysis process easier for intrusion Analysts. Given a target (URL, IP, or HASH) or a file full of targets Automater will return relevant results from sources like the following: IPvoid.com, Robtex.com, Fortiguard.com, unshorten.me, Urlvoid.com, Labs.alienvault.com, ThreatExpert, VxVault, and VirusTotal.
Backdoor Factory	The goal of BDF is patch executable binaries with user desidered shellcode and continue normal execution of the prepatched state. Supporting: Windows PE x32/x64 and Linux ELF x32/x64 (System V) Some executables have built in protections, as such this will not work on all binaries. It is advisable that you test target binaries before deploying them to clients or using them in exercises.
BBQSQL	Blind SQL injection can be a pain to exploit. When the available tools work they work well, but when they don't you have to write something custom. This is time-consuming and tedious. BBQSQL can help you address those issues. BBQSQL is a blind SQL injection framework written in Python. It is extremely useful when attacking tricky SQL injection vulnerabilities. BBQSQL is also a semi-automatic tool, allowing quite a bit of customization for those hard to trigger SQL injection findings. The tool is built to be database agnostic and is extremely versatile. It also has an intuitive UI to make setting up attacks much easier. Python gevent is also implemented, making BBQSQL extremely fast. Similar to other SQL injection tools you provide certain request information. Must provide the usual information: URL HTTP Method Headers Cookies Encoding methods Redirect behavior Files HTTP Auth Proxies Then specify where the injection is going and what syntax we are injecting.

BED	BED is a program which is designed to check daemons for potential buffer overflows, format strings et. al.
BeEF	BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. Amid growing concerns about web-borne attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system, and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context.
bing-ip2hosts	Bing.com is a search engine owned by Microsoft formerly known as MSN Search and Live Search. It has a unique feature to search for websites hosted on a specific IP address. Bing-ip2hosts uses this feature to enumerate all hostnames which Bing has indexed for a specific IP address. This technique is considered best practice during the reconnaissance phase of a penetration test in order to discover a larger potential attack surface. Bing-ip2hosts is written in the Bash scripting language for Linux. This uses the mobile interface and no API key is required.
Binwalk	Binwalk is a tool for searching a given binary image for embedded files and executable code. Specifically, it is designed for identifying files and code embedded inside of firmware images. Binwalk uses the libmagic library, so it is compatible with magic signatures created for the Unix file utility. Binwalk also includes a custom magic signature file which contains improved signatures for files that are commonly found in firmware images such as compressed/archived files, firmware headers, Linux kernels, bootloaders, filesystems, etc.
BlindElephant	The BlindElephant Web Application Fingerprinter attempts to discover the version of a (known) web application by comparing static files at known locations against precomputed hashes for versions of those files in all all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.
Bluelog	Bluelog is a Linux Bluetooth scanner with optional daemon mode and web front-end, designed for site surveys and traffic monitoring. It's intended to be run for long periods of time in a static location to determine how many discoverable Bluetooth devices there are in the area.
BlueMaho	BlueMaho is GUI-shell (interface) for suite of tools for testing security of bluetooth devices. It is freeware, opensource, written on python, uses wxPyhon. It can be used for testing BT-devices for known vulnerabilities and major thing to do – testing to find unknown vulns. Also it can form nice statistics. Features: scan for devices, show advanced info, SDP records, vendor etc track devices – show where and how much times device was seen, its name changes loop scan – it can scan all time, showing you online devices alerts with sound if new device found on_new_device – you can spacify what command should it run when it founds new device it can use separate dongles – one for scaning (loop scan) and one for running tools or exploits send files change name, class, mode, BD_ADDR of local HCI devices save results in database form nice statistics (uniq devices by day/hour, vendors, services etc) test remote device for known vulnerabilities (see exploits for more details) test remote device for unknown vulnerabilities (see tools for more details) themes! you can customize it
Bluepot	Bluepot is a Bluetooth Honeypot written in Java, it runs on Linux. Bluepot was a third year university project attempting to implement a fully functional Bluetooth Honeypot. A piece of software designed to accept and store any malware sent to it and interact with common Bluetooth attacks such as "BlueBugging?" and "BlueSnarfing?". Bluetooth connectivity is provided via hardware Bluetooth dongles. The system also allows monitoring of attacks via a graphical user interface that provides graphs, lists, a dashboard and further detailed analysis from log files.
BlueRanger	BlueRanger is a simple Bash script which uses Link Quality to locate Bluetooth device radios. It sends l2cap (Bluetooth) pings to create a connection between Bluetooth interfaces, since most devices allow pings without any authentication or authorization. The higher the link quality, the closer the device (in theory). Use a Bluetooth Class 1 adapter for long range location detection. Switch to a Class 3 adapter for more precise short range locating. The recision and accuracy depend on the build quality of the Bluetooth adapter, interference, and response from the remote device. Fluctuations may occur even when neither device is in motion.
Bluesnarfer	A Bluetooth bluesnarfing Utility.
braa	Braa is a mass snmp scanner. The intended usage of such a tool is of course making SNMP queries – but unlike snmpget or snmpwalk from net-snmp, it is able to query dozens or hundreds of hosts simultaneously, and in a single process. Thus, it consumes very few system resources and does the scanning VERY fast. Braa implements its OWN snmp stack, so it does NOT need any SNMP libraries like net-snmp. The implementation is very dirty, supports only several data types, and in any case cannot be stated 'standard-conforming'! It was designed to be fast, and it is fast. For this reason (well, and also because of my laziness ;), there is no ASN.1 parser in braa – you HAVE to know the numerical values of OID's (for instance .1.3.6.1.2.1.1.5.0 instead of system.sysName.0).

bulk-extractor	bulk_extractor is a program that extracts features such as email addresses, credit card numbers, URLs, and other types of information from digital evidence files. It is a useful forensic investigation tool for many tasks such as malware and intrusion investigations, identity investigations and cyber investigations, as well as analyzing imagery and pass-word cracking. The program provides several unusual capabilities including: It finds email addresses, URLs and credit card numbers that other tools miss because it can process compressed data (like ZIP, PDF and GZIP files) and incomplete or partially corrupted data. It can carve JPEGs, office documents and other kinds of files out of fragments of compressed data. It will detect and carve encrypted RAR files. It builds word lists based on all of the words found within the data, even those in compressed files that are in unallocated space. Those word lists can be useful for password cracking. It is multi-threaded; running bulk_extractor on a computer with twice the number of cores typically makes it complete a run in half the time. It creates histograms showing the most common email addresses, URLs, domains, search terms and other kinds of information on the drive. bulk_extractor operates on disk images, files or a directory of files and extracts useful information without parsing the file system or file system structures. The input is split into pages and processed by one or more scanners. The results are stored in feature files that can be easily inspected, parsed, or processed with other automated tools. bulk_extractor also creates histograms of features that it finds. This is useful because features such as email addresses and internet search terms that are more common tend to be important. In addition to the capabilities described above, bulk_extractor also includes: A graphical user interface, Bulk Extractor Viewer, for browsing features stored in feature files and for launching bulk_extractor scans A small number of python programs for performing additional analysis on feature files
Bully	Bully is a new implementation of the WPS brute force attack, written in C. It is conceptually identical to other programs, in that it exploits the (now well known) design flaw in the WPS specification. It has several advantages over the original reaver code. These include fewer dependencies, improved memory and cpu performance, correct handling of endianness, and a more robust set of options. It runs on Linux, and was specifically developed to run on embedded Linux systems (OpenWrt, etc) regardless of architecture. Bully provides several improvements in the detection and handling of anomalous scenarios. It has been tested against access points from numerous vendors, and with differing configurations, with much success.
Burp Suite	Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. Burp gives you full control, letting you combine advanced manual techniques with state-of-the-art automation, to make your work faster, more effective, and more fun.
Capstone	Capstone is a disassembly framework with the target of becoming the ultimate disasm engine for binary analysis and reversing in the security community. Created by Nguyen Anh Quynh, then developed and maintained by a small community, Capstone offers some unparalleled features: Support multiple hardware architectures: ARM, ARM64 (aka ARMv8), Mips & X86 Having clean/simple/lightweight/intuitive architecture-neutral API Provide details on disassembled instruction (called "decomposer" by others) Provide semantics of the disassembled instruction, such as list of implicit registers read & written Implemented in pure C language, with lightweight wrappers for C++, Python, Ruby, OCaml, C#, Java and Go available Native support for Windows & *nix platforms (MacOSX, Linux & *BSD confirmed) Thread-safe by design.
CaseFile	CaseFile is the little brother to Maltego. It targets a unique market of 'offline' analysts whose primary sources of information are not gained from the open-source intelligence side or can be programmatically queried. We see these people as investigators and analysts who are working 'on the ground', getting intelligence from other people in the team and building up an information map of their investigation. CaseFile gives you the ability to quickly add, link and analyze data having the same graphing flexibility and performance as Maltego without the use of transforms. CaseFile is roughly a third of the price of Maltego. What does CaseFile do? CaseFile is a visual intelligence application that can be used to determine the relationships and real world links between hundreds of different types of information. It gives you the ability to quickly view second, third and n-th order relationships and find links otherwise undiscoverable with other types of intelligence tools. CaseFile comes bundled with many different types of entities that are commonly used in investigations allowing you to act quickly and efficiently. CaseFile also has the ability to add custom entity types allowing you to extend the product to your own data sets. What can CaseFile do for me? CaseFile can be used for the information gathering, analytics and intelligence phases of almost all types of investigates, from IT Security, Law enforcement and any data driven work. It will save you time and will allow you to work more accurately and smarter. CaseFile has the ability to visualise datasets stored in CSV, XLS and XLSX spreadsheet formats. We are not marketing people. Sorry. CaseFile aids you in your thinking process by visually demonstrating interconnected links between searched items. If access to "hidden" information determines your success, CaseFile can help you discover it.
CDPSnarf	CDPSnarf is a network sniffer exclusively written to extract information from CDP packets. It provides all the information a "show cdp neighbors detail" command would return on a Cisco router and even more. A feature list follows: Time intervals between CDP advertisements Source MAC address CDP Version TTL Checksum Device ID Software version Platform Addresses Port ID Capabilities Duplex Save packets in PCAP dump file format Read packets from PCAP dump files Debugging information (using the "-d" flag) Tested with IPv4 and IPv6
CeWL	CeWL is a ruby app which spiders a given url to a specified depth, optionally following external links, and returns a list of words which can then be used for password crackers such as John the Ripper. CeWL also has an associated command line app, FAB (Files Already Bagged) which uses the same meta data extraction techniques to create author/creator lists from already downloaded.

chntpw	This little program provides a way to view information and change user passwords in a Windows NT/2000 user database file. Old passwords need not be known since they are overwritten. In addition it also contains a simple registry editor (same size data writes) and an hex-editor which enables you to fiddle around with bits and bytes in the file as you wish. If you want GNU/Linux bootdisks for offline password recovery you can add this utility to custom image disks or use those provided at the tools homepage.
cisco-auditing-tool	Perl script which scans cisco routers for common vulnerabilities.
cisco-global-exploiter	Cisco Global Exploiter (CGE), is an advanced, simple and fast security testing tool.
cisco-ocs	A mass Cisco scanning tool.
cisco-torch	Cisco Torch mass scanning, fingerprinting, and exploitation tool was written while working on the next edition of the “Hacking Exposed Cisco Networks”, since the tools available on the market could not meet our needs. The main feature that makes Cisco-torch different from similar tools is the extensive use of forking to launch multiple scanning processes on the background for maximum scanning efficiency. Also, it uses several methods of application layer fingerprinting simultaneously, if needed. We wanted something fast to discover remote Cisco hosts running Telnet, SSH, Web, NTP and SNMP services and launch dictionary attacks against the services discovered.
CmosPwd	CmosPwd is a cross-platform tool to decrypt password stored in CMOS used to access a computer’s BIOS setup. This application should work out of the box on most modern systems, but some more esoteric BIOSes may not be supported or may require additional steps.
Commix	Commix (short for [comm]and [i]njection e[x]ploiter) has a simple environment and it can be used, from web developers, penetration testers or even security researchers to test web applications with the view to find bugs, errors or vulnerabilities related to command injection attacks. By using this tool, it is very easy to find and exploit a command injection vulnerability in a certain vulnerable parameter or string. Commix is written in Python programming language.
Cookie Cadger	Cookie Cadger helps identify information leakage from applications that utilize insecure HTTP GET requests. Web providers have started stepping up to the plate since Firesheep was released in 2010. Today, most major websites can provide SSL/TLS during all transactions, preventing cookie data from leaking over wired Ethernet or insecure Wi-Fi. But the fact remains that Firesheep was more of a toy than a tool. Cookie Cadger is the first open-source pen-testing tool ever made for intercepting and replaying specific insecure HTTP GET requests into a browser. Cookie Cadgers Request Enumeration Abilities Cookie Cadger is a graphical utility which harnesses the power of the Wireshark suite and Java to provide a fully cross-platform, entirely open- source utility which can monitor wired Ethernet, insecure Wi-Fi, or load a packet capture file for offline analysis.
copy-router-config	Copies configuration files from Cisco devices running SNMP.
coWPAtty	Implementation of an offline dictionary attack against WPA/WPA2 networks using PSK-based authentication (e.g. WPA-Personal). Many enterprise networks deploy PSK-based authentication mechanisms for WPA/WPA2 since it is much easier than establishing the necessary RADIUS, supplicant and certificate authority architecture needed for WPA-Enterprise authentication. Cowpatty can implement an accelerated attack if a precomputed PMK file is available for the SSID that is being assessed.
crackle	crackle exploits a flaw in the BLE pairing process that allows an attacker to guess or very quickly brute force the TK (Temporary Key). With the TK and other data collected from the pairing process, the STK (Short Term Key) and later the LTK (Long Term Key) can be collected. With the STK and LTK, all communications between the master and the slave can be decrypted.
creddump	creddump is a python tool to extract various credentials and secrets from Windows registry hives. It currently extracts: LM and NT hashes (SYSKEY protected) Cached domain passwords LSA secrets It essentially performs all the functions that bkhive/samdump2, cachedump, and lsadump2 do, but in a platform-independent way. It is also the first tool that does all of these things in an offline way (actually, Cain & Abel does, but is not open source and is only available on Windows).
crunch	Crunch is a wordlist generator where you can specify a standard character set or a character set you specify. crunch can generate all possible combinations and permutations. Features: crunch generates wordlists in both combination and permutation ways it can breakup output by number of lines or file size now has resume support pattern now supports number and symbols pattern now supports upper and lower case characters separately adds a status report when generating multiple files new -l option for literal support of @,%^ new -d option to limit duplicate characters see man file for details now has unicode support
CryptCat	CryptCat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol while encrypting the data being transmitted. It is designed to be a reliable “back-end” tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

Cuckoo	Cuckoo Sandbox is a malware analysis system. You can throw any suspicious file at it and in a matter of seconds Cuckoo will provide you back some detailed results outlining what such file did when executed inside an isolated environment. Cuckoo generates a handful of different raw data which include: Native functions and Windows API calls traces Copies of files created and deleted from the filesystem Dump of the memory of the selected process Full memory dump of the analysis machine Screenshots of the desktop during the execution of the malware analysis Network dump generated by the machine used for the analysis. In order to make such results more consumable to the end users, Cuckoo is able to process them and generate different type of reports, which could include: JSON report HTML report MAEC report MongoDB interface HPFeeds interface
CutyCapt	CutyCapt is a small cross-platform command-line utility to capture WebKit's rendering of a web page into a variety of vector and bitmap formats, including SVG, PDF, PS, PNG, JPEG, TIFF, GIF, and BMP.
Cymothoa	Cymothoa is a stealth backdooring tool, that inject backdoor's shellcode into an existing process. The tool uses the ptrace library (available on nearly all * nix), to manipulate processes and infect them.
DAVTest	DAVTest 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. It is meant for penetration testers to quickly and easily determine if enabled DAV services are exploitable. DAVTest supports: Automatically send exploit files Automatic randomization of directory to help hide files Send text files and try MOVE to executable name Basic and Digest authorization Automatic clean-up of uploaded files Send an arbitrary file
dbd	dbd is a Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32. dbd features AES-CBC-128 + HMAC-SHA1 encryption (by Christophe Devine), program execution (-e option), choosing source port, continuous reconnection with delay, and some other nice features. dbd supports TCP/IP communication only. Source code and binaries are distributed under the GNU General Public License.
DBPwAudit	DBPwAudit is a Java tool that allows you to perform online audits of password quality for several database engines. The application design allows for easy adding of additional database drivers by simply copying new JDBC drivers to the jdbc directory. Configuration is performed in two files, the aliases.conf file is used to map drivers to aliases and the rules.conf tells the application how to handle error messages from the scan. The tool has been tested and known to work with: Microsoft SQL Server 2000/2005 Oracle 8/9/10/11 IBM DB2 Universal Database MySQL The tool is pre-configured for these drivers but does not ship with them, due to licensing issues.
dc3dd	dc3dd is a patched version of GNU dd with added features for computer forensics:. * on the fly hashing (md5, sha-1, sha-256, and sha-512) * possibility to write errors to a file * group errors in the error log * pattern wiping * progress report * possiblity to split output
ddrescue	Like dd, dd_rescue does copy data from one file or block device to another. You can specify file positions (called seek and Skip in dd). There are several differences: dd_rescue does not provide character conversions. The command syntax is different. Call dd_rescue -h. dd_rescue does not abort on errors on the input file, unless you specify a maximum error number. Then dd_rescue will abort when this number is reached. dd_rescue does not truncate the output file, unless asked to. You can tell dd_rescue to start from the end of a file and move backwards. It uses two block sizes, a large (soft) block size and a small (hard) block size. In case of errors, the size falls back to the small one and is promoted again after a while without errors.
deblaze	Through the use of the Flex programming model and the ActionScript language, Flash Remoting was born. Flash applications can make request to a remote server to call server side functions, such as looking up accounts, retrieving additional data and graphics, and performing complex business operations. However, the ability to call remote methods also increases the attack surface exposed by these applications. This tool will allow you to perform method enumeration and interrogation against flash remoting end points. Deblaze came about as a necessity during a few security assessments of flash based websites that made heavy use of flash remoting. I needed something to give me the ability to dig a little deeper into the technology and identify security holes. On all of the servers I've seen so far the names are not case sensitive, making it much easier to bruteforce. Often times HTTP POST requests won't be logged by the server, so bruteforcing may go unnoticed on poorly monitored systems. Deblaze provides the following functionality: Brute Force Service and Method Names Method Interrogation Flex Technology Fingerprinting
dex2jar	dex2jar contains following compments: dex-reader is designed to read the Dalvik Executable (.dex/.odex) format. It has a light weight API similar with ASM. dex-translator is designed to do the convert job. It reads the dex instruction to dex-ir format, after some optimize, convert to ASM format. dex-ir used by dex-translator, is designed to represent the dex instruction dex-tools tools to work with .class files. here are examples: Modify a apk, DeObfuscate a jar d2j-smali [To be published] disassemble dex to smali files and assemble dex from smali files. different implementation to smali/baksmali, same syntax, but we support escape in type desc "Lcom/dex2jar\\t\\u1234;" dex-writer [To be published] write dex same way as dex-reader.
DFF	DFF (Digital Forensics Framework) is a free and Open Source computer forensics software built on top of a dedicated Application Programming Interface (API). It can be used both by professional and non-expert people in order to quickly and easily collect, preserve and reveal digital evidences without compromising systems and data. Preserve digital chain of custody: Software write blocker, cryptographic hash calculation Access to local and remote devices: Disk drives, removable devices, remote file systems Read standard digital forensics file formats: Raw, Encase EWF, AFF 3 file formats Virtual machine disk reconstruction: VmWare (VMDK) compatible Windows and Linux OS forensics: Registry, Mailboxes, NTFS, EXTFS 2/3/4, FAT 12/16/32 file systems Quickly triage and search for (meta-)data: Regular expressions, dictionaries, content search, tags, time-line Recover hidden and deleted artifacts: Deleted files / folders, unallocated spaces, carving Volatile memory forensics: Processes, local files, binary extraction, network connections

DHCPig	DHCPig initiates an advanced DHCP exhaustion attack. It will consume all IPs on the LAN, stop new users from obtaining IPs, release any IPs in use, then for good measure send gratuitous ARP and knock all windows hosts offline. It requires scapy >=2.1 library and admin privileges to execute. No configuration necessary, just pass the interface as a parameter. It has been tested on multiple Linux distributions and multiple DHCP servers (ISC,Windows 2k3/2k8).
DIRB	DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analyzing the response. DIRB comes with a set of preconfigured attack wordlists for easy usage but you can use your custom wordlists. Also DIRB sometimes can be used as a classic CGI scanner, but remember is a content scanner not a vulnerability scanner. DIRB main purpose is to help in professional web application auditing. Specially in security related testing. It covers some holes not covered by classic web vulnerability scanners. DIRB looks for specific web objects that other generic CGI scanners can't look for. It doesn't search vulnerabilities nor does it look for web contents that can be vulnerables.
DirBuster	DirBuster is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. DirBuster attempts to find these. However tools of this nature are often as only good as the directory and file list they come with. A different approach was taken to generating this. The list was generated from scratch, by crawling the Internet and collecting the directory and files that are actually used by developers! DirBuster comes a total of 9 different lists, this makes DirBuster extremely effective at finding those hidden files and directories. And if that was not enough DirBuster also has the option to perform a pure brute force, which leaves the hidden directories and files nowhere to hide.
diStorm3	diStorm is a lightweight, easy-to-use and fast decomposer library. diStorm disassembles instructions in 16, 32 and 64 bit modes. Supported instruction sets: FPU, MMX, SSE, SSE2, SSE3, SSSE3, SSE4, 3DNow! (w/ extensions), new x86-64 instruction sets, VMX, AMD's SVM and AVX!. The output of new interface of diStorm is a special structure that can describe any x86 instruction, this structure can be later formatted into text for display too. diStorm is written in C, but for rapidly use, diStorm also has wrappers in Python/Ruby/Java and can easily be used in C as well. It is also the fastest disassembler library!. The source code is very clean, readable, portable and platform independent (supports both little and big endianity). diStorm solely depends on the C library, therefore it can be used in embedded or kernel modules. Note that diStorm3 is backward compatible with the interface of diStorm64 (however, make sure you use the newest header files).
DMitry	DMitry (Deepmagic Information Gathering Tool) is a UNIX/(GNU)Linux Command Line Application coded in C. DMitry has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more. The following is a list of the current features: An Open Source Project. Perform an Internet Number whois lookup. Retrieve possible uptime data, system and server data. Perform a SubDomain search on a target host. Perform an E-Mail address search on a target host. Perform a TCP Portscan on the host target. A Modular program allowing user specified modules
dnmap	dnmap is a framework to distribute nmap scans among several clients. It reads an already created file with nmap commands and send those commands to each client connected to it. The framework use a client/server architecture. The server knows what to do and the clients do it. All the logic and statistics are managed in the server. Nmap output is stored on both server and client. Usually you would want this if you have to scan a large group of hosts and you have several different internet connections (or friends that want to help you).
dns2tcp	Dns2tcp is a network tool designed to relay TCP connections through DNS traffic. Encapsulation is done on the TCP level, thus no specific driver is needed (i.e: TUN/TAP). Dns2tcp client doesn't need to be run with specific privileges. Dns2tcp is composed of two parts : a server-side tool and a client-side tool. The server has a list of resources specified in a configuration file. Each resource is a local or remote service listening for TCP connections. The client listen on a predefined TCP port and relays each incoming connection through DNS to the final service.
DNSChef	DNSChef is a highly configurable DNS proxy for Penetration Testers and Malware Analysts. A DNS proxy (aka "Fake DNS") is a tool used for application network traffic analysis among other uses. For example, a DNS proxy can be used to fake requests for "badguy.com" to point to a local machine for termination or interception instead of a real host somewhere on the Internet. There are several DNS Proxies out there. Most will simply point all DNS queries a single IP address or implement only rudimentary filtering. DNSChef was developed as part of a penetration test where there was a need for a more configurable system. As a result, DNSChef is cross-platform application capable of forging responses based on inclusive and exclusive domain lists, supporting multiple DNS record types, matching domains with wildcards, proxying true responses for nonmatching domains, defining external configuration files, IPv6 and many other features. You can find detailed explanation of each of the features and suggested uses below. The use of DNS Proxy is recommended in situations where it is not possible to force an application to use some other proxy server directly. For example, some mobile applications completely ignore OS HTTP Proxy settings. In these cases, the use of a DNS proxy server such as DNSChef will allow you to trick that application into forwarding connections to the desired destination.
dnsenum	Multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks. OPERATIONS: Get the host's addresse (A record). Get the namservers (threaded). Get the MX record (threaded). Perform axfr queries on nameservers and get BIND VERSION (threaded). Get extra names and subdomains via google scraping (google query = "allinurl: -www site:domain"). Brute force subdomains from file, can also perform recursion on subdomain that have NS records (all threaded). Calculate C class domain network ranges and perform whois queries on them (threaded). Perform reverse lookups on netranges (C class or/and whois netranges) (threaded). Write to domain_ips.txt file ip-blocks.

dnsmap	dnsmap was originally released back in 2006 and was inspired by the fictional story “The Thief No One Saw” by Paul Craig, which can be found in the book “Stealing the Network – How to 0wn the Box”. dnsmap is mainly meant to be used by pentesters during the information gathering/enumeration phase of infrastructure security assessments. During the enumeration stage, the security consultant would typically discover the target company’s IP netblocks, domain names, phone numbers, etc … Subdomain brute-forcing is another technique that should be used in the enumeration stage, as it’s especially useful when other domain enumeration techniques such as zone transfers don’t work (I rarely see zone transfers being publicly allowed these days by the way).
DNSRecon	DNSRecon provides the ability to perform: Check all NS Records for Zone Transfers Enumerate General DNS Records for a given Domain (MX, SOA, NS, A, AAAA, SPF and TXT) Perform common SRV Record Enumeration. Top Level Domain (TLD) Expansion Check for Wildcard Resolution Brute Force subdomain and host A and AAAA records given a domain and a wordlist Perform a PTR Record lookup for a given IP Range or CIDR Check a DNS Server Cached records for A, AAAA and CNAME Records provided a list of host records in a text file to check Enumerate Common mDNS records in the Local Network Enumerate Hosts and Subdomains using Google
dnstracer	dnstracer determines where a given Domain Name Server (DNS) gets its information from for a given hostname, and follows the chain of DNS servers back to the authoritative answer.
dnswalk	dnswalk is a DNS debugger. It performs zone transfers of specified domains, and checks the database in numerous ways for internal consistency, as well as accuracy.
Doona	Doona is a fork of the Bruteforce Exploit Detector Tool (BED). BED is a program which is designed to check daemons for potential buffer overflows, format string bugs etc. Doona is Australian for duvet. It adds a significant number of features/changes to BED.
dos2unix	This package contains utilities dos2unix, unix2dos, mac2unix, unix2mac to convert the line endings of text files between UNIX (LF), DOS (CRLF) and Mac (CR) formats. Text files under Windows and DOS typically have two ASCII characters at the end of each line: CR (carriage return) followed by LF (line feed). Older Macs used just CR, while UNIX uses just LF. While most modern editors can read all these formats, there may still be a need to convert files between them. This is the classic utility developed in 1989.
DotDotPwn	It’s a very flexible intelligent fuzzer to discover traversal directory vulnerabilities in software such as HTTP/FTP/TFTP servers, Web platforms such as CMSs, ERPs, Blogs, etc. Also, it has a protocol-independent module to send the desired payload to the host and port specified. On the other hand, it also could be used in a scripting way using the STDOUT module. It’s written in perl programming language and can be run either under *NIX or Windows platforms. It’s the first Mexican tool included in BackTrack Linux (BT4 R2). Fuzzing modules supported in this version: HTTP HTTP URL FTP TFTP Payload (Protocol independent) STDOUT
Dradis	Dradis is an open source framework to enable effective information sharing, specially during security assessments. Dradis is a self-contained web application that provides a centralized repository of information to keep track of what has been done so far, and what is still ahead. Features include: Easy report generation. Support for attachments. Integration with existing systems and tools through server plugins. Platform independent.
Dumpzilla	Dumpzilla application is developed in Python 3.x and has as purpose extract all forensic interesting information of Firefox, Iceweasel and Seamonkey browsers to be analyzed. Due to its Python 3.x developement, might not work properly in old Python versions, mainly with certain characters. Works under Unix and Windows 32/64 bits systems. Works in command line interface, so information dumps could be redirected by pipes with tools such as grep, awk, cut, sed… Dumpzilla allows to visualize following sections, search customization and extract certain content. Cookies + DOM Storage (HTML 5). User preferences (Domain permissions, Proxy settings…). Downloads. Web forms (Searches, emails, comments..). Historial. Bookmarks. Cache HTML5 Visualization / Extraction (Offline cache). visited sites “thumbnails” Visualization / Extraction . Addons / Extensions and used paths or urls. Browser saved passwords. SSL Certificates added as a exception. Session data (Webs, reference URLs and text used in forms). Visualize live user surfing, Url used in each tab / window and use of forms. Dumpzilla will show SHA256 hash of each file to extract the information and finally a summary with totals. Sections which date filter is not possible: DOM Storage, Permissions / Preferences, Addons, Extensions, Passwords/Exceptions, Thumbnails and Session
eapmd5pass	EAP-MD5 is a legacy authentication mechanism that does not provide sufficient protection for user authentication credentials. Users who authenticate using EAP-MD5 subject themselves to an offline dictionary attack vulnerability. This tool reads from a live network interface in monitor-mode, or from a stored libpcap capture file, and extracts the portions of the EAP-MD5 authentication exchange. Once the challenge and response portions have been collected from this exchange, eapmd5pass will mount an offline dictionary attack against the user’s password.
edb-debugger	A Linux equivalent of the famous Olly debugger on the Windows platform. Some of its features are:. Intuitive GUI interface The usual debugging operations (step-into/step-over/run/break) Conditional breakpoints Debugging core is implemented as a plugin so people can have drop in replacements. Of course if a given platform has several debugging APIs available, then you may have a plugin that implements any of them. Basic instruction analysis View/Dump memory regions Effective address inspection The data dump view is tabbed, allowing you to have several views of memory open at the same time and quickly switch between them. Importing and generation of symbol maps Plugins

enum4linux	A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts. Overview: Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from www.bindview.com. It is written in Perl and is basically a wrapper around the Samba tools smbclient, rpclient, net and nmblookup. The tool usage can be found below followed by examples, previous versions of the tool can be found at the bottom of the page. Key features: RID cycling (When RestrictAnonymous is set to 1 on Windows 2000) User listing (When RestrictAnonymous is set to 0 on Windows 2000) Listing of group membership information Share enumeration Detecting if host is in a workgroup or a domain Identifying the remote operating system Password policy retrieval (using polenum)
enumIAX	enumIAX is an Inter Asterisk Exchange protocol username brute-force enumerator. enumIAX may operate in two distinct modes; Sequential Username Guessing or Dictionary Attack.
exploitdb	Searchable archive from The Exploit Database.
extundelete	extundelete is a utility that can recover deleted files from an ext3 or ext4 partition. The ext3 and ext4 file systems are the most common default file systems in Linux distributions like Mint, Mageia, or Ubuntu. extundelete uses information stored in the partition's journal to attempt to recover a file that has been deleted from the partition. There is no guarantee that any particular file will be able to be undeleted, so always try to have a good backup system in place, or at least put one in place after recovering your files.
Faraday	Faraday introduces a new concept – IPE (Integrated Penetration-Test Environment) a multiuser Penetration test IDE. Designed for distribution, indexation and analysis of the data generated during a security audit. The main purpose of Faraday is to re-use the available tools in the community to take advantage of them in a multiuser way. Designed for simplicity, users should notice no difference between their own terminal application and the one included in Faraday. Developed with a specialized set of functionalities that help users improve their own work. Do you remember yourself programming without an IDE? Well, Faraday does the same as an IDE does for you when programming, but from the perspective of a penetration test.
Fern Wifi Cracker	Fern Wifi Cracker is a Wireless security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library, the program is able to crack and recover WEP/WPA/WPS keys and also run other network based attacks on wireless or ethernet based networks. Fern Wifi Cracker currently supports the following features: WEP Cracking with Fragmentation,Chop-Chop, Caffe-Latte, Hirte, ARP Request Replay or WPS attack WPA/WPA2 Cracking with Dictionary or WPS based attacks Automatic saving of key in database on successful crack Automatic Access Point Attack System Session Hijacking (Passive and Ethernet Modes) Access Point MAC Address Geo Location Tracking Internal MITM Engine Bruteforce Attacks (HTTP,HTTPS,TELNET,FTP) Update Support
Fierce	First what Fierce is not. Fierce is not an IP scanner, it is not a DDoS tool, it is not designed to scan the whole Internet or perform any un-targeted attacks. It is meant specifically to locate likely targets both inside and outside a corporate network. Only those targets are listed (unless the -nopattern switch is used). No exploitation is performed (unless you do something intentionally malicious with the -connect switch). Fierce is a reconnaissance tool. Fierce is a PERL script that quickly scans domains (usually in just a few minutes, assuming no network lag) using several tactics.
fiked	FakeIKEd, or fiked for short, is a fake IKE daemon supporting just enough of the standards and Cisco extensions to attack commonly found insecure Cisco VPN PSK+XAUTH based IPsec authentication setups in what could be described as a semi MitM attack. Fiked can impersonate a VPN gateway's IKE responder in order to capture XAUTH login credentials; it doesn't currently do the client part of full MitM.
fimap	fimap is a little python tool which can find, prepare, audit, exploit and even google automaticly for local and remote file inclusion bugs in webapps. fimap should be something like sqlmap just for LFI/RFI bugs instead of sql injection. It's currently under heavy development but it's usable.
findmyhash	Accepted algorithms are: MD4 – RFC 1320 MD5 – RFC 1321 SHA1 – RFC 3174 (FIPS 180-3) SHA224 – RFC 3874 (FIPS 180-3) SHA256 – FIPS 180-3 SHA384 – FIPS 180-3 SHA512 – FIPS 180-3 RMD160 – RFC 2857 GOST – RFC 583 WHIRLPOOL – ISO/IEC 10118-3:2004 LM – Microsoft Windows hash NTLM – Microsoft Windows hash MYSQL – MySQL 3, 4, 5 hash CISCO7 – Cisco IOS type 7 encrypted passwords JUNIPER – Juniper Networks 9 encrypted passwords LDAP_MD5 – MD5 Base64 encoded LDAP_SHA1 – SHA1 Base64 encoded
Firewalk	Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway hostdoes not allow the traffic, it will likely drop the packets on the floor and we will see no response. To get the correct IP TTL that will result in expired packets one beyond the gateway we need to ramp up hop-counts. We do this in the same manner that traceroute works. Once we have the gateway hopcount (at that point the scan is said to be `bound`) we can begin our scan. It is significant to note the fact that the ultimate destination host does not have to be reached. It just needs to be somewhere downstream, on the other side of the gateway, from the scanning host.
Foremost	Foremost is a forensic program to recover lost files based on their headers, footers, and internal data structures. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data structures of a given file format allowing for a more reliable and faster recovery.

fragroute	fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host, implementing most of the attacks described in the Secure Networks “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection” paper of January 1998. It features a simple ruleset language to delay, duplicate, drop, fragment, overlap, print, reorder, segment, source-route, or otherwise monkey with all outbound packets destined for a target host, with minimal support for randomized or probabilistic behaviour. This tool was written in good faith to aid in the testing of network intrusion detection systems, firewalls, and basic TCP/IP stack behaviour. Please do not abuse this software.
fragrouter	Fragrouter is a network intrusion detection evasion toolkit. It implements most of the attacks described in the Secure Networks “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection” paper of January 1998. This program was written in the hopes that a more precise testing methodology might be applied to the area of network intrusion detection, which is still a black art at best. Conceptually, fragrouter is just a one-way fragmenting router – IP packets get sent from the attacker to the fragrouter, which transforms them into a fragmented data stream to forward to the victim.
FunkLoad	FunkLoad is a functional and load web tester, written in Python, whose main use cases are: Functional testing of web projects, and thus regression testing as well. Performance testing: by loading the web application and monitoring your servers it helps you to pinpoint bottlenecks, giving a detailed report of performance measurement. Load testing tool to expose bugs that do not surface in cursory testing, like volume testing or longevity testing. Stress testing tool to overwhelm the web application resources and test the application recoverability. Writing web agents by scripting any web repetitive task.
Galleta	Galleta is a forensic tool that examines the content of cookie files produced by Microsofts Internet Explorer. It parses the file and outputs a field separated that can be loaded in a spreadsheet.
Ghost Phisher	Ghost Phisher is a Wireless and Ethernet security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library, the program is able to emulate access points and deploy. Ghost Phisher currently supports the following features: HTTP Server Inbuilt RFC 1035 DNS Server Inbuilt RFC 2131 DHCP Server Webpage Hosting and Credential Logger (Phishing) Wifi Access point Emulator Session Hijacking (Passive and Ethernet Modes) ARP Cache Poisoning (MITM and DOS Attacks) Penetration using Metasploit Bindings Automatic credential logging using SQlite Database Update Support
GISKismet	GISKismet is a wireless recon visualization tool to represent data gathered using Kismet in a flexible manner. GISKismet stores the information in a database so that the user can generate graphs using SQL. GISKismet currently uses SQLite for the database and GoogleEarth / KML files for graphing.
Gobuster	Gobuster is a tool used to brute-force: URIs (directories and files) in web sites. DNS subdomains (with wildcard support). Because I wanted: something that didn’t have a fat Java GUI (console FTW). to build something that just worked on the command line. something that did not do recursive brute force. something that allowed me to brute force folders and multiple extensions at once. something that compiled to native on multiple platforms. something that was faster than an interpreted script (such as Python). something that didn’t require a runtime. use something that was good with concurrency (hence Go). to build something in Go that wasn’t totally useless.
GoLismero	GoLismero is an open source framework for security testing. It’s currently geared towards web security, but it can easily be expanded to other kinds of scans. The most interesting features of the framework are: Real platform independence. Tested on Windows, Linux, *BSD and OS X. No native library dependencies. All of the framework has been written in pure Python. Good performance when compared with other frameworks written in Python and other scripting languages. Very easy to use. Plugin development is extremely simple. The framework also collects and unifies the results of well known tools: sqlmap, xsser, openvas, dnsrecon, theharvester Integration with standards: CWE, CVE and OWASP. Designed for cluster deployment in mind (not available yet).
goofile	Use this tool to search for a specific file type in a given domain.
gpp-decrypt	A simple ruby script that will decrypt a given GPP encrypted string.
Gqrx	Gqrx is a software defined radio receiver powered by the GNU Radio SDR framework and the Qt graphical toolkit. Gqrx supports many of the SDR hardware available, including Funcube Dongles, rtl-sdr, HackRF and USRP devices. See supported devices for a complete list. Gqrx is free and hacker friendly software. It comes with source code licensed under the GNU General Public license allowing anyone to fix and modify it for whatever use. Currently it works on Linux and Mac and supports the following devices:. Funcube Dongle Pro and Pro+ RTL2832U-based DVB-T dongles (rtlsdr via USB and TCP) OsmoSDR USRP HackRF Jawbreaker Nuand bladeRF any other device supported by the gr-osmosdr library The latest stable version of Gqrx is 2.2, it is available for Linux, FreeBSD and Mac and it offers the following features: Discover devices attached to the computer. Process I/Q data from the supported devices. Change frequency, gain and apply various corrections (frequency, I/Q balance). AM, SSB, FM-N and FM-W (mono and stereo) demodulators. Special FM mode for NOAA APT. Variable band pass filter. AGC, squelch and noise blankers. FFT plot and waterfall. Record and playback audio to / from WAV file. Spectrum analyzer mode where all signal processing is disabled.
gr-scan	gr-scan is a program written in C++, and built upon GNU Radio, rtl-sdr, and the OsmoSDR Source Block. It is intended to scan a range of frequencies and print a list of discovered signals. It should work with any device that works with that block, including Realtek RTL2832U devices. This software was developed using a Compro U620F, which uses an E4000 tuner. That product doesn’t seem to be available on the US site, but the Newsky DVB-T Receiver (RTL2832U/E4000 Device) has good reviews.

Grabber	Grabber is a web application scanner. Basically it detects some kind of vulnerabilities in your website. Grabber is simple, not fast but portable and really adaptable. This software is designed to scan small websites such as personals, forums etc. absolutely not big application: it would take too long time and flood your network. Features: Cross-Site Scripting SQL Injection (there is also a special Blind SQL Injection module) File Inclusion Backup files check Simple AJAX check (parse every JavaScript and get the URL and try to get the parameters) Hybrid analysis/Crystal ball testing for PHP application using PHP-SAT JavaScript source code analyzer: Evaluation of the quality/correctness of the JavaScript with JavaScript Lint Generation of a file [session_id, time(t)] for next stats analysis.
Guymager	Guymager is a free forensic imager for media acquisition. Its main features are: Easy user interface in different languages Runs under Linux Really fast, due to multi-threaded, pipelined design and multi-threaded data compression Makes full usage of multi-processor machines Generates flat (dd), EWF (E01) and AFF images, supports disk cloning Free of charges, completely open source
hamster-sidejack	Hamster is a tool or “sidejacking”. It acts as a proxy server that replaces your cookies with session cookies stolen from somebody else, allowing you to hijack their sessions. Cookies are sniffed using the Ferret program. You need a copy of that as well.
hash-identifier	Software to identify the different types of hashes used to encrypt data and especially passwords.
HexInject	HexInject is a very versatile packet injector and sniffer, that provide a command-line framework for raw network access. It’s designed to work together with others command-line utilities, and for this reason it facilitates the creation of powerful shell scripts capable of reading, intercepting and modifying network traffic in a transparent manner.
HexorBase	HexorBase is 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). HexorBase allows packet routing through proxies or even metasploit pivoting antics to communicate with remotely inaccessible servers which are hidden within local subnets.
hostapd-wpe	hostapd-wpe is the replacement for
hping3	hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired to the ping(8) unix command, but hping isn’t only able to send ICMP echo requests. It supports TCP, UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. While hping was mainly used as a security tool in the past, it can be used in many ways by people that don’t care about security to test networks and hosts. A subset of the stuff you can do using hping: Firewall testing Advanced port scanning Network testing, using different protocols, TOS, fragmentation Manual path MTU discovery Advanced traceroute, under all the supported protocols Remote OS fingerprinting Remote uptime guessing TCP/IP stacks auditing hping can also be useful to students that are learning TCP/IP.
http-tunnel	Creates a bidirectional virtual data stream tunnelled in HTTP requests. The requests can be sent via a HTTP proxy if so desired. This can be useful for users behind restrictive firewalls. If WWW access is allowed through a HTTP proxy, it’s possible to use httptunnel and, say, telnet or PPP to connect to a computer outside the firewall.
HTTPTunnel	HTTPTunnel is a tunneling software that can tunnel network connections through restrictive HTTP proxies over pure HTTP “GET” and “POST” requests. HTTPTunnel consists of two components: The client that resides behind the firewall and accepts network connections on ports that will either be mapped to a specific remote target server/port (portmapping) or will act as a SOCKS (v4 and v5) proxy. The SOCKS authentication source can be a fixed user list, an LDAP or MySQL directory. The client is available as platform-independent Perl script or as Win32 binary. The server that resides on the internet and accepts HTTP requests from the client which will be translated and forwarded to network connections to the remote servers. Two different servers are available: The hosted server, which is basically a PHP script that must be put on a PHP enabled web server. Putting the PHP script on a webserver enables the webserver to act as your HTTP tunnel server. The standalone server, which is available as platform-independent Perl script or as Win32 binary. This server can be used if you have a box on the internet where you can run your own programs (e.g. your box at home). Using the standalone server (as opposed to the hosted server) is recommended as it does not suffer from many restrictions that the webserver may impose on the PHP script, e.g. maximum script runtime (which will limit the duration of your connections), load-balanced server environments, provider policies etc. Configuration of all components is done over a web-based GUI. SOCKS proxy cascading is supported.
iaxflood	A UDP Inter-Asterisk_eXchange (i.e. IAX) packet was captured from an IAX channel between two Asterisk IP PBX’s. The content of that packet is the source of the payload for the attack embodied by this tool. While the IAX protocol header might not match the Asterisk PBX you’ll attack with this tool, it may require more processing on the part of the PBX than a simple udpflood without any payload that even resembles an IAX payload.
ident-user-enum	ident-user-enum is a simple PERL script to query the ident service (113/TCP) in order to determine the owner of the process listening on each TCP port of a target system. This can help to prioritise target service during a pentest (you might want to attack services running as root first). Alternatively, the list of usernames gathered can be used for password guessing attacks on other network services.

Inguma	Inguma is a penetration testing toolkit entirely written in python. The framework includes modules to discover hosts, gather information about, fuzz targets, brute force user names and passwords and, of course, exploits. While the current exploitation capabilities in Inguma may be limited, this program provides numerous tools for information gathering and target auditing.
Intersect	Intersect 2.5 is the second major release in the project line. This release is much different from the previous, in that it gives the user complete control over which features the Intersect script includes and lets them easily import their own features, among other new functionality. This release focuses mainly on the individual modules(features) and the capability to generate your own customized Intersect scripts. By using the Create.py application, the user is guided through a menu-driven process which allows them to select which modules they would like to include, import their own custom modules and ultimately create an Intersect script that is built around the specific modules they choose.
InTrace	InTrace is a traceroute-like application that enables users to enumerate IP hops exploiting existing TCP connections, both initiated from local network (local system) or from remote hosts. It could be useful for network reconnaissance and firewall bypassing.
Inundator	Inundator is a multi-threaded, queue-driven, anonymous intrusion detection false positives generator with support for multiple targets.
inviteflood	A tool to perform SIP/SDP INVITE message flooding over UDP/IP. It was tested on a Linux Red Hat Fedora Core 4 platform (Pentium IV, 2.5 GHz), but it is expected this tool will successfully build and execute on a variety of Linux distributions.
iPhone Backup Analyzer	iPhone Backup Analyzer is an utility designed to easily browse through the backup folder of an iPhone (or any other iOS device). Read configuration files, browse archives, lurk into databases, and so on.
ipv6-toolkit	The SI6 Networks' IPv6 toolkit is a set of IPv6 security assessment and trouble-shooting tools. It can be leveraged to perform security assessments of IPv6 networks, assess the resiliency of IPv6 devices by performing real-world attacks against them, and to trouble-shoot IPv6 networking problems. The tools comprising the toolkit range from packet-crafting tools to send arbitrary Neighbor Discovery packets to the most comprehensive IPv6 network scanning tool out there (our scan6 tool). Included tools: addr6: An IPv6 address analysis and manipulation tool flow6: A tool to perform a security asseessment of the IPv6 Flow Label frag6: A tool to perform IPv6 fragmentation-based attacks and to perform a security assessment of a number of fragmentation-related aspects icmp6: A tool to perform attacks based on ICMPv6 error messages jumbo6: A tool to assess potential flaws in the handling of IPv6 Jumbograms na6: A tool to send arbitrary Neighbor Advertisement messages ni6: A tool to send arbitrary ICMPv6 Node Information messages, and assess possible flaws in the processing of such packets ns6: A tool to send arbitrary Neighbor Solicitation message ra6: A tool to send arbitrary Router Advertisement messages rd6: A tool to send arbitrary ICMPv6 Redirect messages rs6: A tool to send arbitrary Router Solicitation messages scan6: An IPv6 address scanning tool tcp6: A tool to send arbitrary TCP segments and perform a variety of TCP- based attacks.
iSMTP	Test for SMTP user enumeration (RCPT TO and VRFY), internal spoofing, and relay.
isr-evilgrade	Evilgrade is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates. It comes with pre-made binaries (agents), a working default configuration for fast pentests, and has it's own WebServer and DNSServer modules. Easy to set up new settings, and has an autoconfiguration when new binary agents are set.
jad	Java decompiler
javasnoop	Normally, without access to the original source code, testing the security of a Java client is unpredictable at best and unrealistic at worst. With access the original source, you can run a simple Java program and attach a debugger to it remotely, stepping through code and changing variables where needed. Doing the same with an applet is a little bit more difficult. Unfortunately, real-life scenarios don't offer you this option, anyway. Compilation and decompilation of Java are not really as deterministic as you might imagine. Therefore, you can't just decompile a Java application, run it locally and attach a debugger to it. Next, you may try to just alter the communication channel between the client and the server, which is where most of the interesting things happen anyway. This works if the client uses HTTP with a configurable proxy. Otherwise, you're stuck with generic network traffic altering mechanisms. These are not so great for almost all cases, because the data is usually not plaintext. It's usually a custom protocol, serialized objects, encrypted, or some combination of those. JavaSnoop attempts to solve this problem by allowing you attach to an existing process (like a debugger) and instantly begin tampering with method calls, run custom code, or just watch what's happening on the system.
jboss-autopwn	This JBoss script deploys a JSP shell on the target JBoss AS server. Once deployed, the script uses its upload and command execution capability to provide an interactive session. Features include: Multiplatform support – tested on Windows, Linux and Mac targets Support for bind and reverse bind shells Meterpreter shells and VNC support for Windows targets
JD-GUI	JD-GUI is a standalone graphical utility that displays Java source codes of ".class" files. You can browse the reconstructed source code with the JD-GUI for instant access to methods and fields.

John the Ripper	John the Ripper is designed to be both feature-rich and fast. It combines several cracking modes in one program and is fully configurable for your particular needs (you can even define a custom cracking mode using the built-in compiler supporting a subset of C). Also, John is available for several different platforms which enables you to use the same cracker everywhere (you can even continue a cracking session which you started on another platform). Out of the box, John supports (and autodetects) the following Unix crypt(3) hash types: traditional DES-based, “bigcrypt”, BSDI extended DES-based, FreeBSD MD5-based (also used on Linux and in Cisco IOS), and OpenBSD Blowfish-based (now also used on some Linux distributions and supported by recent versions of Solaris). Also supported out of the box are Kerberos/AFS and Windows LM (DES-based) hashes, as well as DES-based tripcodes. When running on Linux distributions with glibc 2.7+, John 1.7.6+ additionally supports (and autodetects) SHA-crypt hashes (which are actually used by recent versions of Fedora and Ubuntu), with optional OpenMP parallelization (requires GCC 4.2+, needs to be explicitly enabled at compile-time by uncommenting the proper OMPFLAGS line near the beginning of the Makefile). Similarly, when running on recent versions of Solaris, John 1.7.6+ supports and autodetects SHA-crypt and SunMD5 hashes, also with optional OpenMP parallelization (requires GCC 4.2+ or recent Sun Studio, needs to be explicitly enabled at compile-time by uncommenting the proper OMPFLAGS line near the beginning of the Makefile and at runtime by setting the OMP_NUM_THREADS environment variable to the desired number of threads). John the Ripper Pro adds support for Windows NTLM (MD4-based) and Mac OS X 10.4+ salted SHA-1 hashes. “Community enhanced” -jumbo versions add support for many more password hash types, including Windows NTLM (MD4-based), Mac OS X 10.4-10.6 salted SHA-1 hashes, Mac OS X 10.7 salted SHA-512 hashes, raw MD5 and SHA-1, arbitrary MD5-based “web application” password hash types, hashes used by SQL database servers (MySQL, MS SQL, Oracle) and by some LDAP servers, several hash types used on OpenVMS, password hashes of the Eggdrop IRC bot, and lots of other hash types, as well as many non-hashes such as OpenSSH private keys, S/Key skeykeys files, Kerberos TGTs, PDF files, ZIP (classic PKZIP and WinZip/AES) and RAR archives. Unlike older crackers, John normally does not use a crypt(3)-style routine. Instead, it has its own highly optimized modules for different hash types and processor architectures. Some of the algorithms used, such as bitslice DES, couldn’t have been implemented within the crypt(3) API; they require a more powerful interface such as the one used in John. Additionally, there are assembly language routines for several processor architectures, most importantly for x86-64 and x86 with SSE2.
Johnny	Johnny provides a GUI for the John the Ripper password cracking tool.
joomscan	Joomla! is probably the most widely-used CMS out there due to its flexibility, user-friendlinesss, extensibility to name a few. So, watching its vulnerabilities and adding such vulnerabilities as KB to Joomla scanner takes ongoing activity. It will help web developers and web masters to help identify possible security weaknesses on their deployed Joomla! sites. The following features are currently available: Exact version Probing (the scanner can tell whether a target is running version 1.5.12) Common Joomla! based web application firewall detection Searching known vulnerabilities of Joomla! and its components Reporting to Text & HTML output Immediate update capability via scanner or svn
jSQL	jSQL Injection is a lightweight application used to find database information from a distant server. jSQL is free, open source and cross-platform (Windows, Linux, Mac OS X, Solaris).
kalibrate-rtl	Kalibrate, or kal, can scan for GSM base stations in a given frequency band and can use those GSM base stations to calculate the local oscillator frequency offset.
KeepNote	KeepNote is a note taking application that works on Windows, Linux, and MacOS X. With KeepNote, you can store your class notes, TODO lists, research notes, journal entries, paper outlines, etc in a simple notebook hierarchy with rich-text formatting, images, and more. Using full-text search, you can retrieve any note for later reference. KeepNote is designed to be cross-platform (implemented in Python and PyGTK) and stores your notes in simple and easy to manipulate file formats (HTML and XML). Archiving and transferring your notes is as easy as zipping or copying a folder. Features: Rich-text formatting (e.g. Bullet point lists, Inline images) Hierarchical organization for notes Web links and note-to-note links Full-text search Integrated screenshot File attachments Spell checking (via gtkspell) Auto-saving Built-in backup and restore (archive to zip files) Extensions (i.e. “plugins”) Cross-platform (Linux, Windows, MacOS X)
keimpx	keimpx is an open source tool, released under a modified version of Apache License 1.1. It can be used to quickly check for valid credentials across a network over SMB. Credentials can be: Combination of user / plain-text password. Combination of user / NTLM hash. Combination of user / NTLM logon session token. If any valid credentials has been discovered across the network after its attack phase, the user is asked to choose which host to connect to and which valid credentials to use, then he will be prompted with an interactive SMB shell where the user can: Spawn an interactive command prompt. Navigate through the remote SMB shares: list, upload, download files, create, remove files, etc. Deploy and undeploy his own service, for instance, a backdoor listening on a TCP port for incoming connections. List users details, domains and password policy.
KillerBee	KillerBee is a Python based framework and tool set for exploring and exploiting the security of ZigBee and IEEE 802.15.4 networks. Using KillerBee tools and a compatible IEEE 802.15.4 radio interface, you can eavesdrop on ZigBee networks, replay traffic, attack cryptosystems and much more. Using the KillerBee framework, you can build your own tools, implement ZigBee fuzzing, emulate and attack end-devices, routers and coordinators and much more.
Kismet	Kismet is an 802.11 layer-2 wireless network detector, sniffer, and intrusion detection system. It will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11a/b/g/n traffic. It can use other programs to play audio alarms for network events, read out network summaries, or provide GPS coordinates. This is the main package containing the core, client, and server.

lbd	lbd (load balancing detector) detects if a given domain uses DNS and/or HTTP Load-Balancing (via Server: and Date: header and diffs between server answers).
Linux Exploit Suggester	As the name suggests, this is a Linux Exploit Suggester, with no frills and no fancy features; just a simple script to keep track of vulnerabilities and suggest possible exploits to use to gain 'root' on a legitimate penetration test, or governing examining body
Lynis	Lynis is an open source security auditing tool. Its main goal is to audit and harden Unix and Linux based systems. It scans the system by performing many security control checks. Examples include searching for installed software and determine possible configuration flaws. Many tests are part of common security guidelines and standards, with on top additional security tests. After the scan a report will be displayed with all discovered findings. To provide you with initial guidance, a link is shared to the related Lynis control.
MagicTree	MagicTree is a penetration tester productivity tool. It is designed to allow easy and straightforward data consolidation, querying, external command execution and (yeah!) report generation. In case you wonder, "Tree" is because all the data is stored in a tree structure, and "Magic" is because it is designed to magically do the most cumbersome and boring part of penetration testing – data management and reporting.
Maltego Teeth	Maltego is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. Maltego's unique advantage is to demonstrate the complexity and severity of single points of failure as well as trust relationships that exist currently within the scope of your infrastructure. The unique perspective that Maltego offers to both network and resource based entities is the aggregation of information posted all over the internet – whether it's the current configuration of a router poised on the edge of your network or the current whereabouts of your Vice President on his international visits, Maltego can locate, aggregate and visualize this information. Maltego offers the user with unprecedented information. Information is leverage. Information is power. Information is Maltego. What does Maltego do? Maltego is a program that can be used to determine the relationships and real world links between: People Groups of people (social networks) Companies Organizations Web sites Internet infrastructure such as: Domains DNS names Netblocks IP addresses Phrases Affiliations Documents and files These entities are linked using open source intelligence. Maltego is easy and quick to install – it uses Java, so it runs on Windows, Mac and Linux. Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate – making it possible to see hidden connections. Using the graphical user interface (GUI) you can see relationships easily – even if they are three or four degrees of separation away. Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements. What can Maltego do for me? Maltego can be used for the information gathering phase of all security related work. It will save you time and will allow you to work more accurately and smarter. Maltego aids you in your thinking process by visually demonstrating interconnected links between searched items. Maltego provide you with a much more powerful search, giving you smarter results. If access to "hidden" information determines your success, Maltego can help you discover it.
Maskprocessor	Maskprocessor is a High-Performance word generator with a per-position configureable charset packed into a single stand-alone binary. Maskprocessor is a High-Performance word generator with a per-position configureable charset packed into a single stand-alone binary.
masscan	This is the fastest Internet port scanner. It can scan the entire Internet in under 6 minutes, transmitting 10 million packets per second. It produces results similar to nmap, the most famous port scanner. Internally, it operates more like scanrand, unicornscan, and ZMap, using asynchronous transmission. The major difference is that it's faster than these other scanners. In addition, it's more flexible, allowing arbitrary address ranges and port ranges. NOTE: masscan uses a custom TCP/IP stack. Anything other than simple port scans will cause conflict with the local TCP/IP stack. This means you need to either use the -S option to use a separate IP address, or configure your operating system to firewall the ports that masscan uses.
mdk3	MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses. IMPORTANT: It is your responsibility to make sure you have permission from the network owner before running MDK against it.
Metagoofil	Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.
Metasploit Framework	Metasploit is a penetration testing platform that enables you to find, exploit, and validate vulnerabilities. It provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing and thanks to the open source community and Rapid7's own hard working content team, new modules are added on a regular basis, which means that the latest exploit is available to you as soon as it's published.
mfcuk	Toolkit containing samples and various tools based on and around libnfc and crapto1, with emphasis on Mifare Classic NXP/Philips RFID cards. Special emphasis of the toolkit is on the following: mifare classic weakness demonstration/exploitation demonstrate use of libnfc (and ACR122 readers) demonstrate use of Crapto1 implementation to confirm internal workings and to verify theoretical/practical weaknesses/attacks
mfoc	MFOC is an open source implementation of "offline nested" attack by Nethemba. This program allow to recover authentication keys from MIFARE Classic card. Please note MFOC is able to recover keys from target only if it have a known key: default one (hardcoded in MFOC) or custom one (user provided using command line).

mfterm	mfterm is a terminal interface for working with Mifare Classic tags. Tab completion on commands is available. Also, commands that have file name arguments provide tab completion on files. There is also a command history, like in most normal shells.
Miranda	Miranda is a Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices, particularly Internet Gateway Devices (aka, routers). It can be used to audit UPNP-enabled devices on a network for possible vulnerabilities. Some of its features include: Interactive shell with tab completion and command history Passive and active discovery of UPNP devices Customizable MSEARCH queries (query for specific devices/services) Full control over application settings such as IP addresses, ports and headers Simple enumeration of UPNP devices, services, actions and variables Correlation of input/output state variables with service actions Ability to send actions to UPNP services/devices Ability to save data to file for later analysis and collaboration Command logging Miranda was built on and for a Linux system and has been tested on a Linux 2.6 kernel with Python 2.5. However, since it is written in Python, most functionality should be available for any Python-supported platform. Miranda has been tested against IGDs from various vendors, including Linksys, D-Link, Belkin and ActionTec. All Python modules came installed by default on a Linux Mint 5 (Ubuntu 8.04) test system.
mitmproxy	mitmproxy is an SSL-capable man-in-the-middle HTTP proxy. It provides a console interface that allows traffic flows to be inspected and edited on the fly. Also shipped is mitmdump, the command-line version of mitmproxy, with the same functionality but without the frills. Think tcpdump for HTTP. Features: intercept and modify HTTP traffic on the fly save HTTP conversations for later replay and analysis replay both HTTP clients and servers make scripted changes to HTTP traffic using Python SSL interception certs generated on the fly
multiforcer	A CUDA & OpenCL accelerated rainbow table implementation from the ground up, and a CUDA hash brute forcing tool with support for many hash types including MD5, SHA1, LM, NTLM, and lots more.
Multimon-NG	MultimonNG a fork of multimon. It decodes the following digital transmission modes: POCSAG512 POCSAG1200 POCSAG2400 EAS UFSK1200 CLIPFSK AFSK1200 AFSK2400 AFSK2400_2 AFSK2400_3 HAPN4800 FSK9600 DTMF ZVEI1 ZVEI2 ZVEI3 DZVEI PZVEI EEA EIA CCIR MORSE CW
nbtscan-unixwiz	This is a command-line tool that scans for open NETBIOS nameservers on a local or remote TCP/IP network, and this is a first step in finding of open shares. It is based on the functionality of the standard Windows tool nbtstat, but it operates on a range of addresses instead of just one.
Ncrack	Ncrack is a high-speed network authentication cracking tool. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords. Security professionals also rely on Ncrack when auditing their clients. Ncrack was designed using a modular approach, a command-line syntax similar to Nmap and a dynamic engine that can adapt its behaviour based on network feedback. It allows for rapid, yet reliable large-scale auditing of multiple hosts. Ncrack's features include a very flexible interface granting the user full control of network operations, allowing for very sophisticated bruteforcing attacks, timing templates for ease of use, runtime interaction similar to Nmap's and many more. Protocols supported include RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet.
Nipper-ng	Nipper-ng is the next generation of nippper, and will always remain free and open source. This software will be used to make observations about the security configurations of many different device types such as routers, firewalls, and switches of a network infrastructure. This is a fork from nipper 0.11.10 release of the GNUv3 GPL code.
Nishang	Nishang is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security and post exploitation during Penetraion Tests. The scripts are written on the basis of requirement by the author during real Penetration Tests. It contains many interesting scripts like Keylogger, DNS TXT Code Execution, HTTP Backdoor, Powerpreter, LSA Secrets and much more.

Nmap	Nmap (“Network Mapper”) is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping). Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum. Nmap is … Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page. Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines. Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more. Easy: While Nmap offers a rich set of advanced features for power users, you can start out as simply as “nmap -v -A targethost”. Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source. Free: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license. Well Documented: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here. Supported: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the Nmap mailing lists. Most bug reports and questions should be sent to the nmap-dev list, but only after you read the guidelines. We recommend that all users subscribe to the low-traffic nmap-hackers announcement list. You can also find Nmap on Facebook and Twitter. For real-time chat, join the #nmap channel on Freenode or EFNet. Acclaimed: Nmap has won numerous awards, including “Information Security Product of the Year” by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the press page for further details. Popular: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.
ntop	ntop is a tool that shows the network usage, similar to what the popular top Unix command does. ntop is based on pcapture (ftp://ftp.ee.lbl.gov/pcapture.tar.Z) and it has been written in a portable way in order to virtually run on every Unix platform. ntop can be used in both interactive or web mode. In the first case, ntop displays the network status on the user’s terminal whereas in web mode a web browser (e.g. netscape) can attach to ntop (that acts as a web server) and get a dump of the network status. In the latter case, ntop can be seen as a simple RMON-like agent with an embedded web interface. ntop uses libpcap, a system-independent interface for user-level packet capture.
oclgausscrack	The goal of the program is to crack the verification hash of the encrypted payload of the Gauss Virus. Uses OpenCL to accelerate the 10k MD5 loop Uses optimizations also used in oclHashcat-plus for maximum performance Able to handle multi-GPU setups (of the same type) VCL (Virtual CL) v1.18 compatible Open Source Supports integration into distributed computing environments Supports resume.
ohrwurm	ohrwurm is a small and simple RTP fuzzer that has been successfully tested on a small number of SIP phones. Features: reads SIP messages to get information of the RTP port numbers reading SIP can be omitted by providing the RTP port numbers, sothat any RTP traffic can be fuzzed RTCP traffic can be suppressed to avoid that codecs learn about the “noisy line” special care is taken to break RTP handling itself the RTP payload is fuzzed with a constant BER the BER is configurable requires arpspoof from dsniff to do the MITM attack requires both phones to be in a switched LAN (GW operation only works partially)
OllyDbg	OllyDbg is a 32-bit assembler level analysing debugger for Microsoft Windows. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable. Features: Intuitive user interface, no cryptical commands Code analysis – traces registers, recognizes procedures, loops, API calls, switches, tables, constants and strings Directly loads and debugs DLLs Object file scanning – locates routines from object files and libraries Allows for user-defined labels, comments and function descriptions Understands debugging information in Borland® format Saves patches between sessions, writes them back to executable file and updates fixups Open architecture – many third-party plugins are available No installation – no trash in registry or system directories Debugs multithread applications Attaches to running programs Configurable disassembler, supports both MASM and IDEAL formats MMX, 3DNow! and SSE data types and instructions, including Athlon extensions Full UNICODE support Dynamically recognizes ASCII and UNICODE strings – also in Delphi format! Recognizes complex code constructs, like call to jump to procedure Decodes calls to more than 1900 standard API and 400 C functions Gives context-sensitive help on API functions from external help file Sets conditional, logging, memory and hardware breakpoints Traces program execution, logs arguments of known functions Shows fixups Dynamically traces stack frames Searches for imprecise commands and masked binary sequences Searches whole allocated memory Finds references to constant or address range Examines and modifies memory, sets breakpoints and pauses program on-the-fly Assembles commands into the shortest binary form Starts from the floppy disk

Oscanner	Oscanner is an Oracle assessment framework developed in Java. It has a plugin-based architecture and comes with a couple of plugins that currently do: Sid Enumeration Passwords tests (common & dictionary) Enumerate Oracle version Enumerate account roles Enumerate account privileges Enumerate account hashes Enumerate audit information Enumerate password policies Enumerate database links The results are given in a graphical java tree.
p0f	P0f is a tool that utilizes an array of sophisticated, purely passive traffic fingerprinting mechanisms to identify the players behind any incidental TCP/IP communications (often as little as a single normal SYN) without interfering in any way. Version 3 is a complete rewrite of the original codebase, incorporating a significant number of improvements to network-level fingerprinting, and introducing the ability to reason about application-level payloads (e.g., HTTP). Some of p0f's capabilities include: Highly scalable and extremely fast identification of the operating system and software on both endpoints of a vanilla TCP connection – especially in settings where NMap probes are blocked, too slow, unreliable, or would simply set off alarms. Measurement of system uptime and network hookup, distance (including topology behind NAT or packet filters), user language preferences, and so on. Automated detection of connection sharing / NAT, load balancing, and application-level proxying setups. Detection of clients and servers that forge declarative statements such as X-Mailer or User-Agent. The tool can be operated in the foreground or as a daemon, and offers a simple real-time API for third-party components that wish to obtain additional information about the actors they are talking to. Common uses for p0f include reconnaissance during penetration tests; routine network monitoring; detection of unauthorized network interconnects in corporate environments; providing signals for abuse-prevention tools; and miscellanous forensics.
PACK	PACK was developed in order to aid in a password cracking competition "Crack Me If You Can" that occurred during Defcon 2010. The goal of this toolkit is to aid in preparation for the "better than bruteforce" password attacks by analyzing common ways that people create passwords. After the analysis stage, the statistical database can be used to generate attack masks for tools such as oclHashcat. NOTE: This tool itself can not crack passwords, but helps other tools crack more passwords faster.
PadBuster	PadBuster is a Perl script for automating Padding Oracle Attacks. PadBuster provides the capability to decrypt arbitrary ciphertext, encrypt arbitrary plaintext, and perform automated response analysis to determine whether a request is vulnerable to padding oracle attacks.
Paros	A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on-the-fly. Other featuers include spiders, client certificate, proxy-chaining, intelligent scanning for XSS and SQL injections etc.
Parsero	Parsero is a free script written in Python which reads the Robots.txt file of a web server and looks at the Disallow entries. The Disallow entries tell the search engines what directories or files hosted on a web server mustn't be indexed. For example, "Disallow: /portal/login" means that the content on www.example.com/portal/login it's not allowed to be indexed by crawlers like Google, Bing, Yahoo… This is the way the administrator have to not share sensitive or private information with the search engines. But sometimes these paths typed in the Disallows entries are directly accessible by the users without using a search engine, just visiting the URL and the Path, and sometimes they are not available to be visited by anybody… Because it is really common that the administrators write a lot of Disallows and some of them are available and some of them are not, you can use Parsero in order to check the HTTP status code of each Disallow entry in order to check automatically if these directories are available or not. Also, the fact the administrator write a robots.txt, it doesn't mean that the files or directories typed in the Dissallow entries will not be indexed by Bing, Google, Yahoo… For this reason, Parsero is capable of searching in Bing to locate content indexed without the web administrator authorization. Parsero will check the HTTP status code in the same way for each Bing result.
patator	Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage. Currently it supports the following modules: ftp_login : Brute-force FTP ssh_login : Brute-force SSH telnet_login : Brute-force Telnet smtp_login : Brute-force SMTP smtp_vrfy : Enumerate valid users using the SMTP 'VRFY' command smtp_rcpt : Enumerate valid users using the SMTP 'RCPT TO' command finger_lookup : Enumerate valid users using Finger http_fuzz : Brute-force HTTP pop_login : Brute-force POP3 pop_passd : Brute-force poppassd (http://netwinsite.com/poppassd/) imap_login : Brute-force IMAP4 – ldap_login : Brute-force LDAP smb_login : Brute-force SMB smb_lookupsid : Brute-force SMB SID-lookup vmauthd_login : Brute-force VMware Authentication Daemon mssql_login : Brute-force MSSQL oracle_login : Brute-force Oracle mysql_login : Brute-force MySQL pgsql_login : Brute-force PostgreSQL vnc_login : Brute-force VNC dns_forward : Brute-force DNS dns_reverse : Brute-force DNS (reverse lookup subnets) snmp_login : Brute-force SNMPv1/2 and SNMPv3 unzip_pass : Brute-force the password of encrypted ZIP files keystore_pass : Brute-force the password of Java keystore files
pdf-parser	This tool will parse a PDF document to identify the fundamental elements used in the analyzed file. It will not render a PDF document.
pdfid	This tool is not a PDF parser, but it will scan a file to look for certain PDF keywords, allowing you to identify PDF documents that contain (for example) JavaScript or execute an action when opened. PDFiD will also handle name obfuscation. The idea is to use this tool first to triage PDF documents, and then analyze the suspicious ones with my pdf-parser. An important design criterium for this program is simplicity. Parsing a PDF document completely requires a very complex program, and hence it is bound to contain many (security) bugs. To avoid the risk of getting exploited, I decided to keep this program very simple (it is even simpler than pdf-parser.py).
pdgmail	Python script to gather gmail artifacts from a pd process memory dump. It'll find what it can out of the memory image including contacts, emails, last acccess times, IP addresses etc.

peepdf	peepdf is a Python tool to explore PDF files in order to find out if the file can be harmful or not. The aim of this tool is to provide all the necessary components that a security researcher could need in a PDF analysis without using 3 or 4 tools to make all the tasks. With peepdf it's possible to see all the objects in the document showing the suspicious elements, supports the most used filters and encodings, it can parse different versions of a file, object streams and encrypted files. With the installation of PyV8 and Pylibemu it provides Javascript and shellcode analysis wrappers too. Apart of this it is able to create new PDF files, modify existent ones and obfuscate them.
phrasendrescher	phrasen|drescher (p|d) is a modular and multi processing pass phrase cracking tool. It comes with a number of plugins but a simple plugin API allows an easy development of new plugins. The main features of p|d are: Modular with the use of plugins Multi processing Dictionary attack with or without permutations (uppercase, lowercase, l33t, etc.) Incremental brute force attack with custom character maps Runs on FreeBSD, NetBSD, OpenBSD, MacOS and Linux
pipal	All this tool does is to give you the stats and the information to help you analyse the passwords. The real work is done by you in interpreting the results.
PixieWPS	Pixiewps is a tool written in C used to bruteforce offline the WPS pin exploiting the low or non-existing entropy of some APs (pixie dust attack). It is meant for educational purposes only. All credits for the research go to Dominique Bongard. Features: Checksum optimization: it'll try first for valid PINs (11'000); Reduced entropy of the seed from 32 to 25 bits for the C LCG pseudo-random function; Small Diffie-Hellman keys: don't need to specify the Public Registrar Key if the same option is used with Reaver. The program will also try first with E-S0 = E-S1 = 0, then it'll tries to bruteforce the seed of the PRNG if the –e-nonce option is specificed.
plecost	WordPress finger printer tool, plecost search and retrieve information about the plugins versions installed in WordPress systems. It can analyze a single URL or perform an analysis based on the results indexed by Google. Additionally displays CVE code associated with each plugin, if there. Plecost retrieves the information contained on Web sites supported by WordPress, and also allows a search on the results indexed by Google.
polenum	polenum is a python script which uses the Impacket Library from CORE Security Technologies to extract the password policy information from a windows machine. This allows a non-windows (Linux, Mac OSX, BSD etc..) user to query the password policy of a remote windows box without the need to have access to a windows machine.
Powerfuzzer	Powerfuzzer is a highly automated and fully customizable web fuzzer (HTTP protocol based application fuzzer) based on many other Open Source fuzzers available and information gathered from numerous security resources and websites. It was designed to be user friendly, modern, effective and working. Currently, it is capable of identifying these problems: Cross Site Scripting (XSS) Injections (SQL, LDAP, code, commands, and XPATH) CRLF HTTP 500 statuses (usually indicative of a possible misconfiguration/security flaw incl. buffer overflow) Designed and coded to be modular and extendable. Adding new checks should simply entail adding new methods.
PowerSploit	PowerSploit is a series of Microsoft PowerShell scripts that can be used in post-exploitation scenarios during authorized penetration tests.
protos-sip	The purpose of this test-suite is to evaluate implementation level security and robustness of Session Initiation Protocol (SIP) implementations.
ProxyStrike	ProxyStrike is an active Web Application Proxy. It's a tool designed to find vulnerabilities while browsing an application. It was created because the problems we faced in the pentests of web applications that depends heavily on Javascript, not many web scanners did it good in this stage, so we came with this proxy. Right now it has available Sql injection and XSS plugins. Both plugins are designed to catch as many vulnerabilities as we can, it's that why the SQL Injection plugin is a Python port of the great DarkRaver "Sqlibf". The process is very simple, ProxyStrike runs like a proxy listening in port 8008 by default, so you have to browse the desired web site setting your browser to use ProxyStrike as a proxy, and ProxyStrike will analyze all the paremeters in background mode. For the user is a passive proxy because you won't see any different in the behaviour of the application, but in the background is very active. :) Some features: Plugin engine (Create your own plugins!) Request interceptor Request diffing Request repeater Automatic crawl process Http request/response history Request parameter stats Request parameter values stats Request url parameter signing and header field signing Use of an alternate proxy (tor for example ;D) Sql attacks (plugin) Server Side Includes (plugin) Xss attacks (plugin) Attack logs Export results to HTML or XML
pwnat	pwnat, pronounced "poe-nat", is 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. The server does not need to know anything about the clients trying to connect. Simply put, this is a proxy server that works behind a NAT, even when the client is behind a NAT, without any 3rd party.
RainbowCrack	RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. It crack hashes with rainbow tables. RainbowCrack uses time-memory tradeoff algorithm to crack hashes. It differs from brute force hash crackers. A brute force hash cracker generate all possible plaintexts and compute the corresponding hashes on the fly, then compare the hashes with the hash to be cracked. Once a match is found, the plaintext is found. If all possible plaintexts are tested and no match is found, the plaintext is not found. With this type of hash cracking, all intermediate computation results are discarded. A time-memory tradeoff hash cracker need a pre-computation stage, at the time all plaintext/hash pairs within the selected hash algorithm, charset, plaintext length are computed and results are stored in files called rainbow table. It is time consuming to do this kind of computation. But once the one time pre-computation is finished, hashes stored in the table can be cracked with much better performance than a brute force cracker.
rcracki-mt	rcracki_mt is a modified version of rcrack which supports hybrid and indexed tables. In addition to that, it also adds multi-core support.

Reaver	Reaver implements a brute force attack against Wifi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, as described in http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. Reaver has been designed to be a robust and practical attack against WPS, and has been tested against a wide variety of access points and WPS implementations. On average Reaver will recover the target AP's plain text WPA/WPA2 passphrase in 4-10 hours, depending on the AP. In practice, it will generally take half this time to guess the correct WPS pin and recover the passphrase
rebind	Rebind is a tool that implements the multiple A record DNS rebinding attack. Although this tool was originally written to target home routers, it can be used to target any public (non RFC1918) IP address. Rebind provides an external attacker access to a target router's internal Web interface. This tool works on routers that implement the weak end system model in their IP stack, have specifically configured firewall rules, and who bind their Web service to the router's WAN interface. Note that remote administration does not need to be enabled for this attack to work. All that is required is that a user inside the target network surf to a Web site that is controlled, or has been compromised, by the attacker.
Recon-ng	Recon-ng is a full-featured Web Reconnaissance framework written in Python. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly. Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework. However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance. If you want to exploit, use the Metasploit Framework. If you want to Social Engineer, us the Social Engineer Toolkit. If you want to conduct reconnaissance, use Recon-ng! See the Usage Guide for more information. Recon-ng is a completely modular framework and makes it easy for even the newest of Python developers to contribute. Each module is a subclass of the "module" class. The "module" class is a customized "cmd" interpreter equipped with built-in functionality that provides simple interfaces to common tasks such as standardizing output, interacting with the database, making web requests, and managing API keys. Therefore, all the hard work has been done. Building modules is simple and takes little more than a few minutes. See the Development Guide for more information.
redfang	RedFang is a small proof-of-concept application to find non discoverable Bluetooth devices. This is done by brute forcing the last six (6) bytes of the Bluetooth address of the device and doing a read_remote_name().
RegRipper	RegRipper is an open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis. RegRipper consists of two basic tools, both of which provide similar capability. The RegRipper GUI allows the analyst to select a hive to parse, an output file for the results, and a profile (list of plugins) to run against the hive. When the analyst launches the tool against the hive, the results go to the file that the analyst designated. If the analyst chooses to parse the System hive, they might also choose to send the results to system.txt. The GUI tool will also create a log of it's activity in the same directory as the output file, using the same file name but using the .log extension (i.e., if the output is written to system.txt, the log will be written to system.log). RegRipper also includes a command line (CLI) tool called rip. Rip can be pointed against to a hive and can run either a profile (a list of plugins) or an individual plugin against that hive, with the results being sent to STDOUT. Rip can be included in batch files, using the redirection operators to send the output to a file. Rip does not write a log of it's activity. RegRipper is similar to tools such as Nessus, in that the application itself is simply an engine that runs plugins. The plugins are individual Perl scripts that each perform a specific function. Plugins can locate specific keys, and list all subkeys, as well as values and data, or they can locate specific values. Plugins are extremely valuable in the sense that they can be written to parse data in a manner that is useful to individual analysts. Note: Plugins also serve as a means of retaining corporate knowledge, in that an analyst finds something, creates a plugin, and adds that plugin to a repository that other analysts can access. When the plugin is shared, this has the effect of being a force multiplier, in that all analysts know have access to the knowledge and experience of one analyst. In addition, plugins remain long after analysts leave an organization, allowing for retention of knowledge.
responder	This tool is first an LLMNR and NBT-NS responder, it will answer to *specific* NBT-NS (NetBIOS Name Service) queries based on their name suffix (see: http://support.microsoft.com/kb/163409). By default, the tool will only answers to File Server Service request, which is for SMB. The concept behind this, is to target our answers, and be stealthier on the network. This also helps to ensure that we don't break legitimate NBT-NS behavior. You can set the -r option to 1 via command line if you want this tool to answer to the Workstation Service request name suffix.
RidEnum	Rid Enum is a RID cycling attack that attempts to enumerate user accounts through null sessions and the SID to RID enum. If you specify a password file, it will automatically attempt to brute force the user accounts when its finished enumerating.
RouterSploit	The RouterSploit Framework is an open-source exploitation framework dedicated to embedded devices. It consists of various modules that aids penetration testing operations: exploits – modules that take advantage of identified vulnerabilities creds – modules designed to test credentials against network services scanners – modules that check if a target is vulnerable to any exploit
RSMangler	RSMangler will take a wordlist and perform various manipulations on it similar to those done by John the Ripper the main difference being that it will first take the input words and generate all permutations and the acronym of the words (in order they appear in the file) before it applies the rest of the mangles.
RTLSDR Scanner	A cross platform Python frequency scanning GUI for USB TV dongles, using the OsmoSDR rtl-sdr library. In other words a cheap, simple Spectrum Analyser. The scanner attempts to overcome the tuner's frequency response by averaging scans from both the positive and negative frequency offets of the baseband data.

rtpbreak	With rtpbreak you can detect, reconstruct and analyze any RTP session. It doesn't require the presence of RTCP packets and works independently form the used signaling protocol (SIP, H.323, SCCP, …). The input is a sequence of packets, the output is a set of files you can use as input for other tools (wireshark/tshark, sox, grep/awk/cut/ cat/sed, …). It supports also wireless (AP_DLT_IEEE802_11) networks. reconstruct any RTP stream with an unknown or unsupported signaling protocol reconstruct any RTP stream in wireless networks, while doing channel hopping (VoIP activity detector) reconstruct and decode any RTP stream in batch mode (with sox, asterisk, …) reconstruct any already existing RTP stream reorder the packets of any RTP stream for later analysis (with tshark, wireshark, …) build a tiny wireless VoIP tapping system in a single chip Linux unit build a complete VoIP tapping system (rtpbreak would be just the RTP dissector module!)
rtpflood	A command line tool used to flood any device that is processing RTP.
rtpinsertsound	A tool to insert audio into a specified audio (i.e. RTP) stream was created in the August – September 2006 timeframe. The tool is named rtpinsertsound. It was tested on a Linux Red Hat Fedora Core 4 platform (Pentium IV, 2.5 GHz), but it is expected this tool will successfully build and execute on a variety of Linux distributions.
rtpmixsound	A tool to mix pre-recorded audio in real-time with the audio (i.e. RTP) in the specified target audio stream.
Sakis3G	Sakis3G is a tweaked shell script which is supposed to work out-of-the-box for establishing a 3G connection with any combination of modem or operator. It automagically setups your USB or Bluetooth™ modem, and may even detect operator settings. You should try it when anything else fails.
sbd	sbd is a Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32. sbd features AES-CBC-128 + HMAC-SHA1 encryption (by Christophe Devine), program execution (-e option), choosing source port, continuous reconnection with delay, and some other nice features. sbd supports TCP/IP communication only.
sctpscan	SCTPscan is a tool to scan SCTP enabled machines. Typically, these are Telecom oriented machines carrying SS7 and SIGTRAN over IP. Using SCTPscan, you can find entry points to Telecom networks. This is especially useful when doing pentests on Telecom Core Network infrastructures. SCTP is also used in high-performance networks (internet2).
SET	The Social-Engineer Toolkit is an open-source penetration testing framework designed for Social-Engineering. SET has a number of custom attack vectors that allow you to make a believable attack in a fraction of the time.
sfuzz	simple fuzz is exactly what it sounds like – a simple fuzzer. don't mistake simple with a lack of fuzz capability. this fuzzer has two network modes of operation, an output mode for developing command line fuzzing scripts, as well as taking fuzzing strings from literals and building strings from sequences. simple fuzz is built to fill a need – the need for a quickly configurable black box testing utility that doesn't require intimate knowledge of the inner workings of C or require specialized software rigs. the aim is to just provide a simple interface, clear inputs/outputs, and reusability. Features: simple script language for creating test cases support for repeating strings as well as fixed strings ('sequences' vs. 'literals') variables within test cases (ex: strings to be replaced with different strings) tcp and udp payload transport (icmp support tbd) binary substitution support (see basic.a11 for more information) plugin support (NEW!) see plugin.txt for more information. previous packet contents inclusion
ShellNoob	Writing shellcodes has always been super fun, but some parts are extremely boring and error prone. Focus only on the fun part, and use ShellNoob! Features: convert shellcode between different formats and sources. Formats currently supported: asm, bin, hex, obj, exe, C, python, ruby, pretty, safeasm, completec, shellstorm. (All details in the "Formats description" section.) interactive asm-to-opcode conversion (and viceversa) mode. This is useful when you cannot use specific bytes in the shellcode and you want to figure out if a specific assembly instruction will cause problems. support for both ATT & Intel syntax. Check the –intel switch. support for 32 and 64 bits (when playing on x86_64 machine). Check the –64 switch. resolve syscall numbers, constants, and error numbers (now implemented for real! :-)). portable and easily deployable (it only relies on gcc/as/objdump and python). It is just one self-contained python script, and it supports both Python2.7+ and Python3+. in-place development: you run ShellNoob directly on the target architecture! built-in support for Linux/x86, Linux/x86_64, Linux/ARM, FreeBSD/x86, FreeBSD/x86_64. "prepend breakpoint" option. Check the -c switch. read from stdin / write to stdout support (use "-" as filename) uber cheap debugging: check the –to-strace and –to-gdb option! Use ShellNoob as a Python module in your scripts! Check the "ShellNoob as a library" section. Verbose mode shows the low-level steps of the conversion: useful to debug / understand / learn! Extra plugins: binary patching made easy with the –file-patch, –vm-patch, –fork-nopper options! (all details below)
SidGuesser	Guesses sids/instances against an Oracle database according to a predefined dictionary file. The speed is slow (80-100 guesses per second) but it does the job.
SIPArmyKnife	SIP Army Knife is a fuzzer that searches for cross site scripting, SQL injection, log injection, format strings, buffer overflows, and more.

SIPp	SIPp is a free Open Source test tool / traffic generator for the SIP protocol. It includes a few basic SipStone user agent scenarios (UAC and UAS) and establishes and releases multiple calls with the INVITE and BYE methods. It can also reads custom XML scenario files describing from very simple to complex call flows. It features the dynamic display of statistics about running tests (call rate, round trip delay, and message statistics), periodic CSV statistics dumps, TCP and UDP over multiple sockets or multiplexed with retransmission management and dynamically adjustable call rates. Other advanced features include support of IPv6, TLS, SCTP, SIP authentication, conditional scenarios, UDP retransmissions, error robustness (call timeout, protocol defense), call specific variable, Posix regular expression to extract and re-inject any protocol fields, custom actions (log, system command exec, call stop) on message receive, field injection from external CSV file to emulate live users. SIPp can also send media (RTP) traffic through RTP echo and RTP / pcap replay. Media can be audio or video. While optimized for traffic, stress and performance testing, SIPp can be used to run one single call and exit, providing a passed/failed verdict. Last, but not least, SIPp has a comprehensive documentation available both in HTML and PDF format. SIPp can be used to test various real SIP equipment like SIP proxies, B2BUAs, SIP media servers, SIP/x gateways, SIP PBX, … It is also very useful to emulate thousands of user agents calling your SIP system.
SIPVicious	SIPVicious suite is a set of tools that can be used to audit SIP based VoIP systems. It currently consists of four tools:. svmap – this is a sip scanner. Lists SIP devices found on an IP range svwar – identifies active extensions on a PBX svcrack – an online password cracker for SIP PBX svreport – manages sessions and exports reports to various formats svcrash – attempts to stop unauthorized svwar and svcrack scans.
Skipfish	Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments. Key features: High speed: pure C code, highly optimized HTTP handling, minimal CPU footprint – easily achieving 2000 requests per second with responsive targets. Ease of use: heuristics to support a variety of quirky web frameworks and mixed-technology sites, with automatic learning capabilities, on-the-fly wordlist creation, and form autocompletion. Cutting-edge security logic: high quality, low false positive, differential security checks, capable of spotting a range of subtle flaws, including blind injection vectors.
SlowHTTPTest	SlowHTTPTest is a highly configurable tool that simulates some Application Layer Denial of Service attacks. It works on majority of Linux platforms, OSX and Cygwin – a Unix-like environment and command-line interface for Microsoft Windows. It implements most common low-bandwidth Application Layer DoS attacks, such as slowloris, Slow HTTP POST, Slow Read attack (based on TCP persist timer exploit) by draining concurrent connections pool, as well as Apache Range Header attack by causing very significant memory and CPU usage on the server. Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service. This tool is sending partial HTTP requests, trying to get denial of service from target HTTP server.
smali	smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation. The syntax is loosely based on Jasmin's/dedexer's syntax, and supports the full functionality of the dex format (annotations, debug info, line info, etc.)
smtp-user-enum	smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands. It could be adapted to work against other vulnerable SMTP daemons, but this hasn't been done as of v1.0.
SniffJoke	SniffJoke is an application for Linux that handle transparently your TCP connection, delaying, modifyng and inject fake packets inside your transmission, make them almost impossible to be correctly read by a passive wiretapping technology (IDS or sniffer).
snmp-check	Like to snmpwalk, snmp-check allows you to enumerate the SNMP devices and places the output in a very human readable friendly format. It could be useful for penetration testing or systems monitoring. Distributed under GPL license and based on "Athena-2k" script by jshaw. Features snmp-check supports the following enumerations: contact description detect write access (separate action by enumeration) devices domain hardware and storage informations hostname IIS statistics IP forwarding listening UDP ports location motd mountpoints network interfaces network services processes routing information software components system uptime TCP connections total memory uptime user accounts
SPARTA	SPARTA is a python GUI application that simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase. It allows the tester to save time by having point-and-click access to their toolkit and by displaying all tool output in a convenient way. If less time is spent setting up commands and tools, more time can be spent focusing on analysing results.
Spooftooph	Spooftooph is designed to automate spoofing or cloning Bluetooth device information. Make a Bluetooth device hide in plain site. Features: Clone and log Bluetooth device information Generate a random new Bluetooth profile Change Bluetooth profile every X seconds Specify device information for Bluetooth interface Select device to clone from scan log
SQLdict	SQLdict is a dictionary attack tool for SQL Server.

sqlmap	sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections. Features: Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase and SAP MaxDB database management systems. Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band. Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port and database name. Support to enumerate users, password hashes, privileges, roles, databases, tables and columns. Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack. Support to dump database tables entirely, a range of entries or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry. Support to search for specific database names, specific tables across all databases or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain string like name and pass. Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL or Microsoft SQL Server. Support to execute arbitrary commands and retrieve their standard output on the database server underlying operating system when the database software is MySQL, PostgreSQL or Microsoft SQL Server. Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying operating system. This channel can be an interactive command prompt, a Meterpreter session or a graphical user interface (VNC) session as per user's choice. Support for database process' user privilege escalation via Metasploit's Meterpreter getsystem command.
Sqlninja	Fancy going from a SQL Injection on Microsoft SQL Server to a full GUI access on the DB? Take a few new SQL Injection tricks, add a couple of remote shots in the registry to disable Data Execution Prevention, mix with a little Perl that automatically generates a debug script, put all this in a shaker with a Metasploit wrapper, shake well and you have just one of the attack modules of sqlninja! Sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end. Its main goal is to provide a remote access on the vulnerable DB server, even in a very hostile environment. It should be used by penetration testers to help and automate the process of taking over a DB Server when a SQL Injection vulnerability has been discovered.
sqlsus	sqlsus is an open source MySQL injection and takeover tool, written in perl. Via a command line interface, you can retrieve the database(s) structure, inject your own SQL queries (even complex ones), download files from the web server, crawl the website for writable directories, upload and control a backdoor, clone the database(s), and much more… Whenever relevant, sqlsus will mimic a MySQL console output. sqlsus focuses on speed and efficiency, optimizing the available injection space, making the best use (I can think of) of MySQL functions. It uses stacked subqueries and an powerful blind injection algorithm to maximize the data gathered per web server hit. Using multi-threading on top of that, sqlsus is an extremely fast database dumper, be it for inband or blind injection. If the privileges are high enough, sqlsus will be a great help for uploading a backdoor through the injection point, and takeover the web server. It uses SQLite as a backend, for an easier use of what has been dumped, and integrates a lot of usual features (see below) such as cookie support, socks/http proxying, https.
sslcaudit	The goal of sslcaudit project is to develop a utility to automate testing SSL/TLS clients for resistance against MITM attacks. It might be useful for testing a thick client, a mobile application, an appliance, pretty much anything communicating over SSL/TLS over TCP.
SSLsplit	SSLsplit is a tool for man-in-the-middle attacks against SSL/TLS encrypted network connections. Connections are transparently intercepted through a network address translation engine and redirected to SSLsplit. SSLsplit terminates SSL/TLS and initiates a new SSL/TLS connection to the original destination address, while logging all data transmitted. SSLsplit is intended to be useful for network forensics and penetration testing. SSLsplit supports plain TCP, plain SSL, HTTP and HTTPS connections over both IPv4 and IPv6. For SSL and HTTPS connections, SSLsplit generates and signs forged X509v3 certificates on-the-fly, based on the original server certificate subject DN and subjectAltName extension. SSLsplit fully supports Server Name Indication (SNI) and is able to work with RSA, DSA and ECDSA keys and DHE and ECDHE cipher suites. SSLsplit can also use existing certificates of which the private key is available, instead of generating forged ones. SSLsplit supports NULL-prefix CN certificates and can deny OCSP requests in a generic way. SSLsplit removes HPKP response headers in order to prevent public key pinning.
sslstrip	sslstrip is a tool that transparently hijacks HTTP traffic on a network, watch for HTTPS links and redirects, and then map those links into look-alike HTTP links or homograph-similar HTTPS links. It also supports modes for supplying a favicon which looks like a lock icon, selective logging, and session denial.
SSLyze	SSLyze is a Python tool that can analyze the SSL configuration of a server by connecting to it. It is designed to be fast and comprehensive, and should help organizations and testers identify mis-configurations affecting their SSL servers. Key features include: Multi-processed and multi-threaded scanning (it's fast) SSL 2.0/3.0 and TLS 1.0/1.1/1.2 compatibility Performance testing: session resumption and TLS tickets support Security testing: weak cipher suites, insecure renegotiation, CRIME, Heartbleed and more Server certificate validation and revocation checking through OCSP stapling Support for StartTLS handshakes on SMTP, XMPP, LDAP, POP, IMAP, RDP and FTP Support for client certificates when scanning servers that perform mutual authentication XML output to further process the scan results
Statsprocessor	Statsprocessor is a high-performance word-generator based on per-position markov-attack packed into a single stand-alone binary.

t50	Multi-protocol packet injector tool for *nix systems, actually supporting 15 protocols. Features: – Flooding – CIDR support – TCP, UDP, ICMP, IGMPv2, IGMPv3, EGP, DCCP, RSVP, RIPv1, RIPv2, GRE, ESP, AH, EIGRP and OSPF support. – TCP Options. – High performance. – Can hit about 1.000.000 packets per second.
Termineter	Termineter is a framework written in python to provide a platform for the security testing of smart meters. It implements the C12.18 and C12.19 protocols for communication. Currently supported are Meters using C12.19 with 7-bit character sets. Termineter communicates with Smart Meters via a connection using an ANSI type-2 optical probe with a serial interface.
THC-Hydra	Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely. It supports: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)-GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SNMP v1+v2+v3, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.
THC-IPV6	A complete tool set to attack the inherent protocol weaknesses of IPV6 and ICMP6, and includes an easy to use packet factory library.
THC-pptp-bruter	Brute force program against pptp vpn endpoints (tcp port 1723). Fully standalone. Supports latest MSChapV2 authentication. Tested against Windows and Cisco gateways. Exploits a weakness in Microsoft's anti-brute force implementation which makes it possible to try 300 passwords the second.
THC-SSL-DOS	THC-SSL-DOS is a tool to verify the performance of SSL. Establishing a secure SSL connection requires 15x more processing power on the server than on the client. THC-SSL-DOS exploits this asymmetric property by overloading the server and knocking it off the Internet. This problem affects all SSL implementations today. The vendors are aware of this problem since 2003 and the topic has been widely discussed. This attack further exploits the SSL secure Renegotiation feature to trigger thousands of renegotiations via single TCP connection.
theHarvester	The objective of this program is to gather emails, subdomains, hosts, employee names, open ports and banners from different public sources like search engines, PGP key servers and SHODAN computer database. This tool is intended to help Penetration testers in the early stages of the penetration test in order to understand the customer footprint on the Internet. It is also useful for anyone that wants to know what an attacker can see about their organization. This is a complete rewrite of the tool with new features like: Time delays between request All sources search Virtual host verifier Active enumeration (DNS enumeration, Reverse lookups, TLD expansion) Integration with SHODAN computer database, to get the open ports and banners Save to XML and HTML Basic graph with stats New sources
TLSSLed	TLSSLed is a Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. It is based on sslscan, a thorough SSL/TLS scanner that is based on the openssl library, and on the "openssl s_client" command line tool. The current tests include checking if the target supports the SSLv2 protocol, the NULL cipher, weak ciphers based on their key length (40 or 56 bits), the availability of strong ciphers (like AES), if the digital certificate is MD5 signed, and the current SSL/TLS renegotiation capabilities.
tnscmd10g	A tool to prod the oracle tnslsnr process on port 1521/tcp.
TrueCrack	TrueCrack is a brute-force password cracker for TrueCrypt volumes. It works on Linux and it is optimized for Nvidia Cuda technology. It supports: PBKDF2 (defined in PKCS5 v2.0) based on key derivation functions: Ripemd160, Sha512 and Whirlpool. XTS block cipher mode for hard disk encryption based on encryption algorithms: AES, SERPENT, TWOFISH. File-hosted (container) and Partition/device-hosted. Hidden volumes and Backup headers. TrueCrack is able to perform a brute-force attack based on: Dictionary: read the passwords from a file of words. Alphabet: generate all passwords of given length from given alphabet. TrueCrack works on gpu and cpu
twofi	When attempting to crack passwords custom word lists are very useful additions to standard dictionaries. An interesting idea originally released on the "7 Habits of Highly Effective Hackers" blog was to use Twitter to help generate those lists based on searches for keywords related to the list that is being cracked. This idea has been expanded into twofi which will take multiple search terms and return a word list sorted by most common first.
U3-Pwn	U3-Pwn is a tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install. This is performed by removing the original iso file from the device and creating a new iso with autorun features.
ua-tester	This tool is designed to automatically check a given URL using a list of standard and non-standard User Agent strings provided by the user (1 per line). The results of these checks are then reported to the user for further manual analysis where required.
Uniscan	Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.
unix-privesc-check	Unix-privesc-checker is a script that runs on Unix systems (tested on Solaris 9, HPUX 11, Various Linuxes, FreeBSD 6.2). It tries to find misconfigurations that could allow local unprivileged users to escalate privileges to other users or to access local apps (e.g. databases). It is written as a single shell script so it can be easily uploaded and run (as opposed to un-tarred, compiled and installed). It can run either as a normal user or as root (obviously it does a better job when running as root because it can read more files).
URLCrazy	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage. Features Generates 15 types of domain variants Knows over 8000 common misspellings Supports cosmic ray induced bit flipping Multiple keyboard layouts (qwerty, azerty, qwertz, dvorak) Checks if a domain variant is valid Test if domain variants are in use Estimate popularity of a domain variant

Valgrind	Valgrind is a system for debugging and profiling Linux programs. With its tool suite you can automatically detect many memory management and threading bugs, avoiding hours of frustrating bug-hunting and making your programs more stable. You can also perform detailed profiling to help speed up your programs and use Valgrind to build new tools. The Valgrind distribution currently includes six production-quality tools: a memory error detector (Memcheck) two thread error detectors (Helgrind and DRD) a cache and branch-prediction profiler (Cachegrind) a call-graph generating cache and branch-prediction profiler (Callgrind) a heap profiler (Massif) It also includes three experimental tools: a stack/global array overrun detector (SGCheck) a second heap profiler that examines how heap blocks are used (DHAT) a SimPoint basic block vector generator (BBV)
Vega	Vega is a free and open source scanner and testing platform to test the security of web applications. Vega can help you find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities. It is written in Java, GUI based, and runs on Linux, OS X, and Windows. Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. The Vega scanner finds XSS (cross-site scripting), SQL injection, and other vulnerabilities. Vega can be extended using a powerful API in the language of the web: Javascript. Automated Crawler and Vulnerability Scanner Consistent UI Website Crawler Intercepting Proxy SSL MITM Content Analysis Extensibility through a Powerful Javascript Module API Customizable alerts Database and Shared Data Model
VoIPHopper	VoIP Hopper is a GPLv3 licensed security tool, written in C, that rapidly runs a VLAN Hop into the Voice VLAN on specific ethernet switches. VoIP Hopper does this by mimicking the behavior of an IP Phone, in Cisco, Avaya, Nortel, and Alcatel-Lucent environments. This requires two important steps in order for the tool to traverse VLANs for unauthorized access. First, discovery of the correct 12 bit Voice VLAN ID (VVID) used by the IP Phones is required. VoIP Hopper supports multiple protocol discovery methods (CDP, DHCP, LLDP-MED, 802.1q ARP) for this important first step. Second, the tool creates a virtual VoIP ethernet interface on the OS. It then inserts a spoofed 4-byte 802.1q vlan header containing the 12 bit VVID into a spoofed DHCP request. Once it receives an IP address in the VoIP VLAN subnet, all subsequent ethernet frames are “tagged” with the spoofed 802.1q header. VoIP Hopper is a VLAN Hop test tool but also a tool to test VoIP infrastructure security.
Volatility	The Volatility Framework is a completely open collection of tools, implemented in Python under the GNU General Public License, for the extraction of digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer unprecedented visibility into the runtime state of the system. The framework is intended to introduce people to the techniques and complexities associated with extracting digital artifacts from volatile memory samples and provide a platform for further work into this exciting area of research. Volatility supports memory dumps from all major 32- and 64-bit Windows versions and service packs including XP, 2003 Server, Vista, Server 2008, Server 2008 R2, and Seven. Whether your memory dump is in raw format, a Microsoft crash dump, hibernation file, or virtual machine snapshot, Volatility is able to work with it. We also now support Linux memory dumps in raw or LiME format and include 35+ plugins for analyzing 32- and 64-bit Linux kernels from 2.6.11 – 3.5.x and distributions such as Debian, Ubuntu, OpenSuSE, Fedora, CentOS, and Mandrake. We support 38 versions of Mac OSX memory dumps from 10.5 to 10.8.3 Mountain Lion, both 32- and 64-bit. Android phones with ARM processors are also supported. Support for Windows 8, 8.1, Server 2012, 2012 R2, and OSX 10.9 (Mavericks) is either already in svn or just around the corner
w3af	w3af is a Web Application Attack and Audit Framework which aims to identify and exploit all web application vulnerabilities. This package provides a graphical user interface (GUI) for the framework. If you want a command-line application only, install w3af-console. The framework has been called the “metasploit for the web”, but it’s actually much more than that, because it also discovers the web application vulnerabilities using black-box scanning techniques!. The w3af core and it’s plugins are fully written in Python. The project has more than 130 plugins, which identify and exploit SQL injection, cross site scripting (XSS), remote file inclusion and more.
WebScarab	WebScarab is designed to be a tool for anyone who needs to expose the workings of an HTTP(S) based application, whether to allow the developer to debug otherwise difficult problems, or to allow a security specialist to identify vulnerabilities in the way that the application has been designed or implemented.
Webshag	Webshag is a multi-threaded, multi-platform web server audit tool. Written in Python, it gathers commonly useful functionalities for web server auditing like website crawling, URL scanning or file fuzzing. Webshag can be used to scan a web server in HTTP or HTTPS, through a proxy and using HTTP authentication (Basic and Digest). In addition to that it proposes innovative IDS evasion functionalities aimed at making correlation between request more complicated (e.g. use a different random per request HTTP proxy server).
Webshells	A collection of webshells for ASP, ASPX, CFM, JSP, Perl, and PHP servers.
WebSlayer	Webslayer is a tool designed for brute forcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts,files, etc), brute force GET and POST parameters, bruteforce Forms parameters (User/Password), Fuzzing, etc. The tools has a payload generator and an easy and powerful results analyzer. You can perform attacks like: Predictable resource locator, recursion supported (Discovery) Login forms brute force Session brute force Parameter brute force Parameter fuzzing and injection (XSS, SQL) Basic and Ntml authentication brute forcing Some features: Recursion Encodings: 15 encodings supported Authentication: supports Ntml and Basic Multiple payloads: you can use 2 payloads in different parts Proxy support (authentication supported) For predictable resource location it has: Recursion, common extensions, non standard code detection Multiple filters for improving the performance and for producing cleaner results Live filters Multithreads Session saving Integrated browser (webKit) Time delay between requests Attack balancing across multiple proxies Predefined dictionaries for predictable resource location, based on known servers

WebSploit	WebSploit Is An Open Source Project For: Social Engineering Works Scan,Crawler & Analysis Web Automatic Exploiter Support Network Attacks Autopwn – Used From Metasploit For Scan and Exploit Target Service wmap – Scan,Crawler Target Used From Metasploit wmap plugin format infector – inject reverse & bind payload into file format phpmyadmin Scanner CloudFlare resolver LFI Bypasser Apache Users Scanner Dir Bruter admin finder MLITM Attack – Man Left In The Middle, XSS Phishing Attacks MITM – Man In The Middle Attack Java Applet Attack MFOD Attack Vector USB Infection Attack ARP Dos Attack Web Killer Attack Fake Update Attack Fake Access point Attack Wifi Honeypot Wifi Jammer Wifi Dos Bluetooth POD Attack
Weevely	Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.
Wfuzz	Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP,etc), bruteforce Forms parameters (User/Password), Fuzzing,etc. Some features: Multiple Injection points capability with multiple dictionaries Recursion (When doing directory bruteforce) Post, headers and authentication data brute forcing Output to HTML Colored output Hide results by return code, word numbers, line numbers, regex Cookies fuzzing Multi threading Proxy support SOCK support Time delays between requests Authentication support (NTLM, Basic) All parameters bruteforcing (POST and GET) Multiple encoders per payload Payload combinations with iterators Baseline request (to filter results against) Brute force HTTP methods Multiple proxy support (each request through a different proxy) HEAD scan (faster for resource discovery) Dictionaries tailored for known applications (Weblogic, Iplanet, Tomcat, Domino, Oracle 9i, Vignette, Coldfusion and many more
Wifi Honey	This script creates five monitor mode interfaces, four are used as APs and the fifth is used for airodump-ng. To make things easier, rather than having five windows all this is done in a screen session which allows you to switch between screens to see what is going on. All sessions are labelled so you know which is which.
wifiphisher	Wifiphisher is a security tool that mounts automated phishing attacks against Wi-Fi networks in order to obtain credentials or infect the victims with ‘malware’. It is a social engineering attack that can be used to obtain WPA/WPA2 secret passphrases and unlike other methods, it does not require any brute forcing. After achieving a man-in-the-middle position using the Evil Twin attack, Wifiphisher redirects all HTTP requests to an attacker-controlled phishing page. From the victim’s perspective, the attack takes place in three phases: Victim is deauthenticated from their access point. Victim joins a rogue access point. Wifiphisher sniffs the area and copies the target access point settings. Victim is served a realistic specially-customized phishing page.
Wifitap	Wifitap is a proof of concept for communication over WiFi networks using traffic injection. Wifitap allows any application do send and receive IP packets using 802.11 traffic capture and injection over a WiFi network simply configuring wj0, which means : setting an IP address consistent with target network address range routing desired traffic through it In particular, it’s a cheap method for arbitrary packets injection in 802.11 frames without specific library. In addition, it will allow one to get rid of any limitation set at access point level, such as bypassing inter-client communications prevention systems (e.g. Cisco PSPF) or reaching multiple SSID handled by the same access point.
Wifite	To attack multiple WEP, WPA, and WPS encrypted networks in a row. This tool is customizable to be automated with only a few arguments. Wifite aims to be the “set it and forget it” wireless auditing tool. Features: sorts targets by signal strength (in dB); cracks closest access points first automatically de-authenticates clients of hidden networks to reveal SSIDs numerous filters to specify exactly what to attack (wep/wpa/both, above certain signal strengths, channels, etc) customizable settings (timeouts, packets/sec, etc) “anonymous” feature; changes MAC to a random address before attacking, then changes back when attacks are complete all captured WPA handshakes are backed up to wifite.py’s current directory smart WPA de-authentication; cycles between all clients and broadcast deauths stop any attack with Ctrl+C, with options to continue, move onto next target, skip to cracking, or exit displays session summary at exit; shows any cracked keys all passwords saved to cracked.txt
Winexe	Winexe remotely executes commands on Windows NT/2000/XP/2003 systems from GNU/Linux (and possibly also from other Unices capable of building the Samba 4 software package).
Wireshark	Wireshark is the world’s foremost network protocol analyzer. It lets you see what’s happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998. Wireshark has a rich feature set which includes the following: Deep inspection of hundreds of protocols, with more being added all the time Live capture and offline analysis Standard three-pane packet browser Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility The most powerful display filters in the industry Rich VoIP analysis Capture files compressed with gzip can be decompressed on the fly Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform) Coloring rules can be applied to the packet list for quick, intuitive analysis Output can be exported to XML, PostScript®, CSV, or plain text Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2 Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network * General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others

WOL-E	WOL-E is a suite of tools for the Wake on LAN feature of network attached computers, this is now enabled by default on many Apple computers. These tools include: Bruteforcing the MAC address to wake up clients Sniffing WOL attempts on the network and saving them to disk Sniffing WOL passwords on the network and saving them to disk Waking up single clients (post sniffing attack) Scanning for Apple devices on the network for WOL enabling Sending bulk WOL requests to all detected Apple clients
wordlists	This package contains the rockyou wordlist and contains symlinks to a number of other password files present in the Kali Linux distribution. This package has an installation size of 134 MB.
WPScan	WPScan is a black box WordPress vulnerability scanner that can be used to scan remote WordPress installations to find security issues.
Xplico	The goal of Xplico is extract from an internet traffic capture the applications data contained. For example, from a pcap file Xplico extracts each email (POP, IMAP, and SMTP protocols), all HTTP contents, each VoIP call (SIP, MGCP, H323), FTP, TFTP, and so on. Xplico is not a network protocol analyzer.
xspy	Sniffs keystrokes on remote or local X-Windows servers.
XSSer	Cross Site “Scripter” (aka XSSer) is an automatic -framework- to detect, exploit and report XSS vulnerabilities in web-based applications. It contains several options to try to bypass certain filters, and various special techniques of code injection.
YARA	With YARA you can create descriptions of malware families based on textual or binary patterns contained on samples of those families. Each description consists of a set of strings and a boolean expression which determines its logic. This package contains the command-line interface.
Yersinia	Yersinia is a framework for performing layer 2 attacks. It is designed to take advantage of some weakeness in different network protocols. It pretends to be a solid framework for analyzing and testing the deployed networks and systems. Attacks for the following network protocols are implemented in this particular release: Spanning Tree Protocol (STP) Cisco Discovery Protocol (CDP) Dynamic Trunking Protocol (DTP) Dynamic Host Configuration Protocol (DHCP) Hot Standby Router Protocol (HSRP) 802.1q 802.1x Inter-Switch Link Protocol (ISL) VLAN Trunking Protocol (VTP)
zaproxy	The OWASP Zed Attack Proxy (ZAP) is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications. It is designed to be used by people with a wide range of security experience and as such is ideal for developers and functional testers who are new to penetration testing as well as being a useful addition to an experienced pen testers toolbox.

source: https://tools.kali.org/tools-listing