Downloaded from: justpaste.it/jr1d

# The Best Hacking Tools

POLISH CYBER ARMY

| Passwords | |
|---|---|
| Cain & Abel | Cain & Abel is a password recovery tool for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network. |
| CacheDump | CacheDump, licensed under the GPL, demonstrates how to recover cache entry information: username and MSCASH. |
| John the Ripper | John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), Windows, DOS, BeOS, and OpenVMS. |
| FSCrack | GUI for John the Ripper. FSCrack is a front end for John the Ripper (JtR) that provides a graphical user interface (GUI) for access to most of JtR's functions. |
| Hydra | A very fast network logon cracker which support many different services.Number one of the biggest security holes are passwords, as every password security study shows. |
| 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 the usefulness of credentials across a network over SMB. |
| Medusa | Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. The goal is to support as many services which allow remote authentication as possible. |
| 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. |
| Ophcrack | Ophcrack is a Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. |
| RainbowCrack | RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. |
| phrasen\|drescher | 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. |

| | |
|---|---|
| LCP | Main purpose of LCP program is user account passwords auditing and recovery in Windows NT/2000/XP/2003. |
| 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. |
| Fcrackzip | Naturally, programs are born out of an actual need. The situation with fcrackzip was no different… I'm not using zip very much, but recently I needed a password cracker. |
| Enumiax | EnumIAX is an Inter Asterisk Exchange version 2 (IAX2) protocol username brute-force enumerator. enumIAX may operate in two distinct modes; Sequential Username Guessing or Dictionary Attack. |
| Wyd | wyd.pl was born out of those two of situations: 1. A penetration test should be performed and the default wordlist does not contain a valid password. 2. During a forensic crime investigation a password protected file must be opened without knowing the the password. |
| Bruter | Bruter is a parallel network login brute-forcer on Win32. This tool is intended to demonstrate the importance of choosing strong passwords. The goal of Bruter is to support a variety of services that allow remote authentication. |
| The ssh bruteforcer | Is a tool to perform dictionary attacks to the SSH servers, it's a simple tool, you set the target server, target account, wordlist, port and wait.. |
| Lodowep | Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver system. The tool supports both session- and basic-authentication. |
| SSHatter | SSHatter uses a brute force technique to determine how to log into an SSH server. It rigorously tries each combination in a list of usernames and passwords to determine which ones successfully log in. |

| **Scanning** | |
|---|---|
| Amap | Amap is a next-generation scanning tool, which identifies applications and services even if they are not listening on the default port by creating a bogus-communication and analyzing the responses. |
| Dr.Morena | Dr.Morena is a tool to confirm the rule configuration of a Firewall. The configuration of a Firewall is done by combining more than one rule. |
| 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. |
| Netcat | Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. |

| | |
|---|---|
| Ike Scan | Ike-scan is a command-line tool that uses the IKE protocol to discover, fingerprint and test IPSec VPN servers. It is available for Linux, Unix, MacOS and Windows under the GPL license. |
| Nmap | Nmap ('Network Mapper') is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. |
| Zenmap | Zenmap is the official Nmap Security Scanner GUI. It is a multi-platform (Linux, Windows, Mac OS X, BSD, etc. |
| Onesixtyone | onesixtyone is an SNMP scanner which utilizes a sweep technique to achieve very high performance. It can scan an entire class B network in under 13 minutes. |
| SuperScan 4 | Powerful TCP port scanner, pinger, resolver. SuperScan 4 is an update of the highly popular Windows port scanning tool, SuperScan |
| Autoscan | AutoScan-Network is a network scanner (discovering and managing application). No configuration is required to scan your network. The main goal is to print the list of connected equipments in your network. |
| Knocker | Knocker is a simple and easy to use TCP security port scanner written in C to analyze hosts and all of the different services started on them. |
| Nsat | NSAT is a robust scanner which is designed for: Different kinds of wide-ranging scans, keeping stable for days. Scanning on multi-user boxes (local stealth and non-priority scanning options). |
| OutputPBNJ | PBNJ is a suite of tools to monitor changes on a network over time. It does this by checking for changes on the target machine(s), which includes the details about the services running on them as well as the service state. |
| ScanPBNJ | ScanPBNJ performs an Nmap scan and then stores the results in a database. The ScanPBNJ stores information about the machine that has been scanned. ScanPBNJ stores the IP Address, Operating System, Hostname and a localhost bit. |
| glypeahead | By default the Glype proxy script has few restrictions on what hosts/ports can be accessed through it. In addition, the proxy script normally displays all cURL-related error messages. |
| Unicornscan | Unicornscan is a new information gathering and correlation engine built for and by members of the security research and testing communities. |
| TCP Fast Scan | A very very fast tcp port scanner for linux. Runs very quickly. Can scan a lot of hosts / ports + ranges at a time. |
| Multi Threaded TCP Port Scanner 3.0 | This tool could be used to scan ports of certain IP. It also could describe each port with standard name (well-known and registered ports). |
| MingSweeper | MingSweeper is a network reconnaissance tool designed to facilitate large address space,high speed node discovery and identification. |
| Umap(UPNP Map) | Umap (UPNP Map) attempts to scan open TCP ports on the hosts behind a UPNP enabled Internet Gateway Device(IGD) NAT. |
| SendIP | SendIP has a large number of command line options to specify the content of every header of a NTP, BGP, RIP, RIPng, TCP, UDP, ICMP or raw IPv4 and IPv6 packet. It also allows any data to be added to the packet. |

| | |
|---|---|
| PortSentry | The Sentry tools provide host-level security services for the Unix platform. PortSentry, Logcheck/LogSentry, and HostSentry protect against portscans, automate log file auditing, and detect suspicious login activity on a continuous basis. |
| CurrPorts | CurrPorts will display the list of all currently opened TCP/IP and UDP ports on your PC. For each port in the list, information about the process that opened the port is also displayed. |
| Nscan | NScan itself is a port scanner, which uses connect() method to find the list of the host's open ports. The difference from the most of other portscanners is it's flexibility and speed. |
| NetworkActiv Scan | NetworkActiv Port Scanner is a network exploration and administration tool that allows you to scan and explore internal LANs and external WANs. |
| Blues Port Scanner | A good port scanner is just one of the basic tools anyone who is seriously interested in the internet needs. The BluesPortScan is, i think, the fastest scanner for 32Bit windows which you can found in the net. |
| ZMap | ZMap is an open-source network scanner that enables researchers to easily perform Internet-wide network studies. With a single machine and a well provisioned network uplink, ZMap is capable of performing a complete scan of the IPv4 address space in under 45 minutes, approaching the theoretical limit of gigabit Ethernet. |
| subdomain-bruteforcer | Subdomain-bruteforcer is a multi-threaded python tool for enumerating subdomains from a dictionary file. Particularily useful for finding admin panels or other dodgy web practices. |
| ircsnapshot | Ircsnapshot is a python tool that connects a bot to a server in order to fetch users' hostmasks, names, and channel affiliations; also supports the creation of a world map using the scraped data. Useful for reconnaissance on a IRC server full of suspected bots. Supports SOCKS and TOR. |

| **Sniffer** | |
|---|---|
| Wireshark | Wireshark is used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education. |
| Chaosreader | A freeware tool to trace TCP/UDP/… sessions and fetch application data from snoop or tcpdump logs. This is a type of "any-snarf" program, as it will fetch telnet sessions, FTP files, HTTP transfers (HTML, GIF, JPEG, …), SMTP emails, … from the captured data inside network traffic logs. |
| dsniff | dsniff is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data. |
| Ettercap | Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. |
| NetworkMiner | NetworkMiner is a Network Forensic Analysis Tool (NFAT) for Windows. NetworkMiner can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. |

| | |
|---|---|
| RawCap | RawCap is a free command line network sniffer for Windows that uses raw sockets. |
| Spike proxy | Not all web applications are built in the same ways, and hence, many must be analyzed individually. SPIKE Proxy is a professional-grade tool for looking for application-level vulnerabilities in web applications. |
| Tcpdump | Tcpdump prints out the headers of packets on a network interface that match the boolean expression. |
| Tcpreplay | Tcpreplay is a suite of BSD licensed tools written by Aaron Turner for UNIX (and Win32 under Cygwin) operating systems which gives you the ability to use previously captured traffic in libpcap format to test a variety of network devices |
| Pirni Sniffer | Pirni is the worlds first native network sniffer for iPhone. The iPhone's wifi has some major drawbacks in it's hardware design, thus we can not properly set the device in promiscious mode. |
| Ufasoft Snif | Ufasoft Snif is a network sniffer, designed for capturing and analysis of the packets going through the network. Using the packet driver, it requests all the packets from the network card driver (even the packets not addressed to this computer). |

| **Enumeration** | |
|---|---|
| dnsenum | The purpose of Dnsenum is to gather as much information as possible about a domain. |
| DumpSec | SomarSoft's DumpSec is a security auditing program for Microsoft Windows NT/XP/200x. |
| LDAP Browser | LDAP Browser is a premier Windows Explorer-like LDAP Directory client available for Win32 platforms. |
| NBTEnum | NetBIOS Enumeration Utility (NBTEnum) is a utility for Windows that can be used to enumerate NetBIOS information from one host or a range of hosts. |
| nbtscan | This 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. |
| wmi client | This DCOM/WMI client implementation is based on Samba4 sources. It uses RPC/DCOM mechanisms to interact with WMI services on Windows 2000/XP/2003 machines. |
| Dnsmap | Dnsmap is mainly meant to be used by pentesters during the information gathering/enumeration phase of infrastructure security assessments. |
| Dnsrecon | I wrote this tool back in late 2006 and it has been my favorite tool for enumeration thru DNS, in great part because I wrote it and it gives the output in a way that I can manipulate it in my own style. One of the features that I used the most and gave me excellent results is the SRV record enumeration. |
| Dnstracer | Dnstracer determines where a given Domain Name Server (DNS) gets its information from, and follows the chain of DNS servers back to the servers which know the data. |

| Networking Tools | |
|---|---|
| fragroute | fragroute intercepts, modifies, and rewrites egress traffic destined for a specified host. |
| hping | hping is a command-line oriented TCP/IP packet assembler/analyzer. |
| Scapy | Scapy is a powerful interactive packet manipulation program. It is able to forge or decode packets of a wide number of protocols, send them on the wire, capture them, match requests and replies, and much more. |
| Stunnel | The stunnel program is designed to work as an SSL encryption wrapper between remote client and local (inetd-startable) or remote server. |
| tcptraceroute | tcptraceroute is a traceroute implementation using TCP packets. The more traditional traceroute(8) sends out either UDP or ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. |
| tracetcp | tracetcp is a command line traceroute utility for WIN32 that uses TCP SYN packets rather than ICMP/UDP packets that the usual implementations use, thus bypassing gateways that block traditional traceroute packets. |
| Yersinia | Yersinia is a network tool 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. |
| Nemesis | Nemesis is a command-line network packet crafting and injection utility for UNIX-like and Windows systems. Nemesis, is well suited for testing Network Intrusion Detection Systems, firewalls, IP stacks and a variety of other tasks. As a command-line driven utility, Nemesis is perfect for automation and scripting. |

| Wireless | |
|---|---|
| Aircrack-ng | Aircrack is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. |
| Kismet | Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. |
| NetStumbler | NetStumbler delivers a tool that helps you detect 802.11 a/b/g WLAN standards. While wardriving is its main use, the application also facilitates the verifying of network configurations. |
| AirGrab WiFi Radar | AirGrab WiFi Radar is a tool to display information about Apple Airport base stations and other WiFi (802.11b/g/n) wireless access points. |
| AirMobile agent | Client application is downloaded in to your PDA or Windows cellular Phone where it will run in quite mode in the background. If the application finds a rouge access point it will investigate the AP and see if it posed a direct threat to your network. |

| | |
|---|---|
| AirRadar 2 | AirRadar allows you to scan for open networks and tag them as favourites or filter them out. View detailed network information, graph network signal strength, and automatically join the best open network in range. |
| iStumbler | iStumbler is the leading wireless discovery tool for Mac OS X, providing plugins for finding AirPort networks, Bluetooth devices, Bonjour services and Location information with your Mac. |
| KisMAC | KisMAC is an open-source and free sniffer/scanner application for Mac OS X. It has an advantage over MacStumbler / iStumbler / NetStumbler in that it uses monitor mode and passive scanning. |
| WirelessMon | WirelessMon is a software tool that allows users to monitor the status of wireless WiFi adapter(s) and gather information about nearby wireless access points and hot spots in real time. |
| Vistumbler | Vistumbler is a wireless network scanner written in AutoIT for Vista, Windows 7, and Windows 8. WiFiDB is a database written in php to store Vistumbler VS1 files. Keeps track of total access points w/gps, maps to kml, signal graphs, statistics, and more. |
| WaveStumbler | WaveStumbler is console based 802.11 network mapper for Linux. It reports the basic AP stuff like channel, WEP, ESSID, MAC etc. |
| Xirrus Wi-Fi Inspector | Xirrus Wi-Fi Inspector is a powerful tool for managing and troubleshooting the Wi-Fi on a Windows XP SP2 or later, Vista, or 7 laptop. Built in tests enable you to characterize the integrity and performance of your Wi-Fi connection. |
| AirMagnet VoFi Analyzer | AirMagnet VoFi Analyzer is the industry's only solution for troubleshooting voice-over-WLAN problems in the field. VoFi Analyzer provides full analysis of encrypted WLAN traffic, scoring all calls in terms of call quality and proactively identifying all types of problems including phone issues, roaming issues, QoS issues, and RF. |
| Airpwn | Airpwn is a framework for 802.11 (wireless) packet injection. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected "spoofed" from the wireless access point. From the perspective of the wireless client, airpwn becomes the server. |
| WifiScanner | WifiScanner is a tool that has been designed to discover wireless node (i.e access point and wireless clients). It is distributed under the GPL License.<br>It work with CISCO® card and prism card with hostap driver or wlan-ng driver, prism54g, Hermes/Orinoco, Atheros, Centrino, …<br>An IDS system is integrated to detect anomaly like MAC usurpation. |

| **Bluetooth** | |
|---|---|
| Haraldscan | A Bluetooth Scanner for Linux and Mac OS X. Harald Scan is able to determine Major and Minor device class of device, as well as attempt to resolve the device's MAC address to the largest known Bluetooth MAC address Vendor list. |
| FTS4BT | Frontline FTS4BT Bluetooth Protocol Analyzer. Developers and test engineers rely on FTS4BT to get them through the design, debug, test, verify, and qualification cycle. |

| | |
|---|---|
| BlueScanner | BlueScanner is a bash script that implements a scanner for Bluetooth devices. It's a tool designed to extract as much information as possible from Bluetooth devices without the requeriment to pair. |
| Blooover II | Blooover II is a tool for audit based on Java (J2ME). It exists in version Blooover II for audit J2ME mobiles and as a breeeder edition. Easy utility for vulnerability testing. |
| BTScanner | BTScanner for XP is a Bluetooth environment auditing tool for Microsoft Windows XP, implemented using the bluecove libraries (an open source implementation of the JSR-82 Bluetooth API for Java). |
| BlueSpam | BlueSpam searches for all discoverable bluetooth devices and sends a file to them (spams them) if they support OBEX. By default a small text will be send. To customize the message that should be send you need a palm with an SD/MMC card, then you create the directory /PALM/programs/BlueSpam/Send/ and put the file (any type of file will work .jpg is allways fun) you would like to send into this directory. |
| BTCrawler | An application used to to discover Bluetooth devices and the services they provide. Runs on J2ME enabled devices supporting MIDP 2.0 and JSR082 (Java API for Bluetooth) |
| Bluediving | Bluediving is a Bluetooth penetration testing suite.<br>It implements attacks like Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, has features such as Bluetooth address spoofing, an AT and a RFCOMM socket shell and implements tools like carwhisperer, bss, L2CAP packetgenerator, L2CAP connection resetter, RFCOMM scanner and greenplaque scanning mode (using more than one hci device). |
| Bluesnarfer | Bluesnarfer steals informations from a wireless device through a Bluetooth connection. The connection can be between mobile phones, PDAs or Laptops. You can access to a calendar, contact list, emails and text messages. |

| **Web Scanners** | |
|---|---|
| Arachni | Arachni is a fully automated system which tries to enforce the fire and forget principle. As soon as a scan is started it will not bother you for anything nor require further user interaction. |
| Burp Suite | Burp Suite is an integrated platform for performing security testing of web applications. |
| CAL9000 | CAL9000 is a collection of web application security testing tools that complement the feature set of current web proxies and automated scanners. CAL9000 gives you the flexibility and functionality you need for more effective manual testing efforts. |
| CAT | CAT is designed to facilitate manual web application penetration testing for more complex, demanding application testing tasks. |
| CookieDigger | CookieDigger helps identify weak cookie generation and insecure implementations of session management by web applications. The tool works by collecting and analyzing cookies issued by a web application for multiple users. |
| 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 analizing the response. |

| | |
|---|---|
| Fiddler | Fiddler is a Web Debugging Proxy which logs all HTTP(S) traffic between your computer and the Internet. Fiddler allows you to inspect all HTTP(S) traffic, set breakpoints, and 'fiddle' with incoming or outgoing data. |
| Gamja | Gamja will find XSS(Cross site scripting) & SQL Injection weak point also URL parameter validation error. Who knows that which parameter is weak parameter? Gamja will be helpful for finding vulnerability[ XSS , Validation Error , SQL Injection]. |
| Grendel-Scan | A tool for automated security scanning of web applications. Many features are also present for manual penetration testing. |
| HTTrack | HTTrack is a free and easy-to-use offline browser utility. It allows you to download a World Wide Web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to your computer. |
| LiLith | LiLith is a tool written in Perl to audit web applications. This tool analyses webpages and looks for html <form> tags, which often refer to dynamic pages that might be subject to SQL injection or other flaws. |
| Nikto2 | Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6500 potentially dangerous files/CGIs. |
| Paros | A program called 'Paros' for people who need to evaluate the security of their web applications. It is free of charge and completely written in Java. |
| 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. |
| ProxyScan.pl | proxyScan.pl is a security penetration testing tool to scan for hosts and ports through a Web proxy server. Features include various HTTP methods such as GET, CONNECT, HEAD as well as host and port ranges. |
| Ratproxy | A semi-automated, largely passive web application security audit tool, optimized for an accurate and sensitive detection, and automatic annotation, of potential problems and security-relevant design patterns based on the observation of existing, user-initiated traffic in complex web 2.0 environments. |
| ScanEx | This is a simple utility which runs against target site and look for external references and cross domain malicious injections. There are several vulnerable sites which get manipulated with these types of injections and compromised. |
| Scrawlr | Scrawlr, developed by the HP Web Security Research Group in coordination with the MSRC, is short for SQL Injector and Crawler. Scrawlr will crawl a website while simultaneously analyzing the parameters of each individual web page for SQL Injection vulnerabilities. |
| Springenwerk | Springenwerk is a free Cross Site Scripting (XSS) security scanner written in Python. |
| 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. |
| Sqlsus | sqlsus is an open source MySQL injection and takeover tool, written in perl. |
| THCSSLCheck | Windows tool that checks the remote ssl stack for supported ciphers and version. |

| | |
|---|---|
| w3af | w3af is a Web Application Attack and Audit Framework. The project's goal is to create a framework to help you secure your web applications by finding and exploiting all web application vulnerabilities. |
| Wapiti | Wapiti allows you to audit the security of your web applications. It performs "black-box" scans, i.e. it does not study the source code of the application but will scans the webpages of the deployed webapp, looking for scripts and forms where it can inject data. |
| Webfuzzer | Webfuzzer is a tool that can be useful for both pen testers and web masters, it's a poor man web vulnerability scanner. |
| WebGoat | WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons. |
| Websecurify | The Websecurify Suite is a web application security solution designed to run entirely from your web browser. |
| WebSlayer | WebSlayer is a tool designed for bruteforcing Web Applications, it can be used for finding not linked resources (directories, servlets, scripts, etc), bruteforce GET and POST parameters, bruteforce Forms parameters (User/Password), Fuzzing, etc. The tools has a payload generator and a easy and powerful results analyzer. |
| WhatWeb | WhatWeb identifies websites. Its goal is to answer the question, "What is that Website?". WhatWeb recognises web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices. |
| Wikto | Wikto is Nikto for Windows – but with a couple of fancy extra features including Fuzzy logic error code checking, a back-end miner, Google assisted directory mining and real time HTTP request/response monitoring. |
| WSDigger | WSDigger is a free open source tool designed by McAfee Foundstone to automate black-box web services security testing (also known as penetration testing). WSDigger is more than a tool, it is a web services testing framework. |
| XSSploit | XSSploit is a multi-platform Cross-Site Scripting scanner and exploiter written in Python. It has been developed to help discovery and exploitation of XSS vulnerabilities in penetration testing missions. |
| Fireforce | Fireforce is a Firefox extension designed to perform brute-force attacks on GET and POST forms. Fireforce can use dictionaries or generate passwords based on several character types. |
| Netsparker | Netsparker is a web application security scanner, with support for both detection and exploitation of vulnerabilities. It aims to be false positive–free by only reporting confirmed vulnerabilities after successfully exploiting or otherwise testing them. |
| Havij | Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. |

| **Database Vulnerabilities** | |
|---|---|

| | |
|---|---|
| Berkeley DB | Oracle Berkeley DB is a family of open source, embeddable databases that allows developers to incorporate within their applications a fast, scalable, transactional database engine with industrial grade reliability and availability. |
| Database browser | Database browser is an universal table editor. This easy to use tool allows user to connect to any database and browse or modify data,run sql scripts, export and print data. |
| Db2utils | db2utils is a small collection of db2 utilities. It currently features three different tools db2disco, db2fakesrv and db2getprofile. |
| Oracle Auditing Tools | The Oracle Auditing Tools is a toolkit that could be used to audit security within Oracle database servers. |
| Oscanner | Oscanner is an Oracle assessment framework developed in Java. It has a plugin-based architecture and comes with a couple of plugins. |
| SQL Auditing Tools | SQLAT is a suite of tools which could be usefull for pentesting a MS SQL Server. The tools are still in development but tend to be quite stable. The tools do dictionary attacks, upload files, read registry and dump the SAM. |
| THC-ORACLE | THC presents a crypto paper analyzing the database authentication mechansim used by oracle. THC further releases practical tools to sniff and crack the password of an oracle database within seconds. |
| thc-orakelcrackert11g | OrakelCrackert is an Oracle 11g database password hash cracker using a weakness in the Oracle password storage strategy. With Oracle 11g, case sensitive SHA1 based hashing is introduced. |
| 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. |
| MYSQLAudit | Python Script for basic auditing of common security misconfigurations in MySQL. |
| sqlininja | sqlininja exploits web applications that use Microsoft SQL Server as a database backend. Its focus is on getting a running shell on the remote host. sqlninja doesn't find an SQL injection in the first place, but automates the exploitation process once one has been discovered. |
| GreenSql | GreenSQL is an Open Source database firewall used to protect databases from SQL injection attacks. GreenSQL works as a proxy and has built in support for MySQL and PostgreSQL. |

| **Vuln Scanners** | |
|---|---|
| Metasploit Framework | The Metasploit Framework is an advanced open-source platform for developing, testing, and using exploit code. |
| OpenVAS | OpenVAS is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. |
| Nessus | Nessus detects, scans, and profiles numerous devices and resources to increase security and compliance across your network. |

| | |
|---|---|
| Porkbind | Porkbind is a multi-threaded nameserver scanner that can recursively query nameservers of subdomains for version strings. (i.e. sub.host.dom's nameservers then host.dom's nameservers) |
| Canvas | Immunity's CANVAS makes available hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework to penetration testers and security professionals worldwide. |
| Social-Engineer Toolkit (SET) | The Social-Engineer Toolkit (SET) is specifically designed to perform advanced attacks against the human element. SET was designed to be released with the http://www.social-engineer.org launch and has quickly became a standard tool in a penetration testers arsenal. |
| Acunetix | Acunetix web vulnerability scanner is a tool designed to discover security holes in your web applications that an at-tacker would likely abuse to gain illicit access to your systems and data. It looks for multiple vulnerabilities includingSQL injection, cross site scripting, and weak passwords. |
| RIPS | RIPS is a tool written in PHP to find vulnerabilities in PHP applications using static code analysis. |
| Rapid7 NeXpose | Rapid7 NeXpose is a vulnerability scanner which aims to support the entire vulnerability management lifecycle, including discovery, detection, verification, risk classification, impact analysis, reporting and mitigation. It integrates with Rapid7's Metasploit for vulnerability exploitation |
| VulnDetector | VulnDetector is a project aimed to scan a website and detect various web based security vulnerabilities in the website. Currently, VulnDetector can detect Cross Site Scripting (XSS) and SQL Injection (SQLI) vulnerabilities on a web based script, but has no easy to use interface. |
| Damn Small SQLi Scanner | DSSS supports blind/error SQLi tests, depth 1 crawling and advanced comparison of different attributes to distinguish blind responses (titles, HTTP status codes, filtered text only lengths and fuzzy comparison of contents itself). If you are satisfied with your commercial tool scanning results then I believe that you could even be more satisfied with this one. |
| CAT.NET | CAT.NET is a binary code analysis tool that helps identify common variants of certain prevailing vulnerabilities that can give rise to common attack vectors such as Cross-Site Scripting (XSS), SQL Injection and XPath Injection. |
| Peach Fuzzer | Peach is a SmartFuzzer that is capable of performing both generation and mutation based fuzzing. Peach requires the creation of PeachPit files that define the structure, type information, and relationships in the data to be fuzzed. |
| GFI LanGuard | GFI LanGuard is a network security and vulnerability scanner designed to help with patch management, network and software audits, and vulnerability assessments. The price is based on the number of IP addresses you wish to scan. A free trial version (up to 5 IP addresses) is available. |
| MBSA | Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed for the IT professional that helps small and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. |

| Vuln Apps | |
|---|---|
| Damn Vulnerable Web Application (DVWA) | Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. |
| Damn Vulnerable Linux | Damn Vulnerable Linux (DVL) is everything a good Linux distribution isn't. Its developers have spent hours stuffing it with broken, ill-configured, outdated, and exploitable software that makes it vulnerable to attacks. DVL isn't built to run on your desktop – it's a learning tool for security students |
| Metasploitable | Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques. |
| Kioptrix | This Kioptrix VM Image are easy challenges. The object of the game is to acquire root access via any means possible (except actually hacking the VM server or player). The purpose of these games are to learn the basic tools and techniques in vulnerability assessment and exploitation. |
| HoneyDrive | HoneyDrive is a virtual appliance (OVA) with Xubuntu Desktop 12.04 32-bit edition installed. It contains various honeypot software packages such as Kippo SSH honeypot, Dionaea malware honeypot, Honeyd low-interaction honeypot, Glastopf web honeypot along with Wordpot, Thug honeyclient and more. |
| Badstore | Badstore.net is dedicated to helping you understand how hackers prey on Web application vulnerabilities, and to showing you how to reduce your exposure. |
| OWASP Insecure Web App Project | InsecureWebApp is a web application that includes common web application vulnerabilities. It is a target for automated and manual penetration testing, source code analysis, vulnerability assessments and threat modeling. |
| VulnApp | VulnApp, is a BSD licensed ASP.net application implementing some of the most common applications we come across on our penetration testing engagements. |
| OWASP Vicnum | Vicnum is an OWASP project consisting of vulnerable web applications based on games commonly used to kill time. These applications demonstrate common web security problems such as cross site scripting, sql injections, and session management issues. |
| OWASP Broken Web Applications Project | The Broken Web Applications (BWA) Project produces a Virtual Machine running a variety of applications with known vulnerabilities |
| LAMPSecurity | LAMPSecurity training is designed to be a series of vulnerable virtual machine images along with complementary documentation designed to teach linux,apache,php,mysql security. |
| Virtual Hacking Lab | A mirror of deliberately insecure applications and old softwares with known vulnerabilities. Used for proof-of-concept /security training/learning purposes. Available in either virtual images or live iso or standalone formats. |
| WAVSEP | The Web Application Vulnerability Scanner Evaluation Project, is a vulnerable web application designed to help assessing the features, quality and accuracy of web application vulnerability scanners. This evaluation platform |

| | |
|---|---|
| | contains a collection of unique vulnerable web pages that can be used to test the various properties of web application scanners. |
| Moth | Moth is a VMware image with a set of vulnerable Web Applications and scripts, that you may use for, testing Web Application Security Scanners, testing Static Code Analysis tools (SCA), giving an introductory course to Web Application Security |
| SecuriBench | Stanford SecuriBench is a set of open source real-life programs to be used as a testing ground for static and dynamic security tools. Release .91a focuses on Web-based applications written in Java. |
| NETinVM | NETinVM is a single VMware or VirtualBox virtual machine image that contains, ready to run, a series of User-mode Linux (UML) virtual machines which, when started, conform a whole computer network inside the VMware or VirtualBox virtual machine. |

| **Live CD** | |
|---|---|
| BackTrack | BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. |
| Kali Linux | Kali Linux (formerly known as BackTrack) is a Debian-based distribution with a collection of security and forensics tools. It features timely security updates, support for the ARM architecture, a choice of four popular desktop environments, and seamless upgrades to newer versions. |
| BackBox | BackBox is a Linux distribution based on Ubuntu. It has been developed to perform penetration tests and security assessments. Designed to be fast, easy to use and provide a minimal yet complete desktop environment, thanks to its own software repositories, always being updated to the latest stable version of the most used and best known ethical hacking tools. |
| Samurai | The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites. |
| Katana | Katana is a portable multi-boot security suite which brings together many of today's best security distributions and portable applications to run off a single Flash Drive. It includes distributions which focus on Pen-Testing, Auditing, Forensics, System Recovery, Network Analysis, and Malware Removal. Katana also comes with over 100 portable Windows applications; such as Wireshark, Metasploit, NMAP, Cain & Abel, and many more. |
| blackbuntu | Penetration Testing Distribution based on Ubuntu 10.10 which was specially designed for security training students and practitioners of information security. |
| Bugtraq | Bugtraq is a distribution based on the 2.6.38 kernel has a wide range of penetration and forensic tools. Bugtraq can install from a Live DVD or USB drive, the distribution is customized to the last package, configured and updated the kernel and the kernel has been patched for better performance and to recognize a variety of hardware, including wireless injection patches pentesting other distributions do not recognize. |

| | |
|---|---|
| Network Security Toolkit (NST) | This bootable ISO live CD/DVD (NST Live) is based on Fedora. The toolkit was designed to provide easy access to best-of-breed Open Source Network Security Applications and should run on most x86/x86_64 platforms. |
| Pentoo | Pentoo is a penetration testing LiveCD distribution based on Gentoo. It features a lot of tools for auditing and testing a network, from scanning and discovering to exploiting vulnerabilities |
| BlackArch | BlackArch is an Arch-based security distribution. There are over 600 tools in BlackArch's package repository. The BlackArch live ISO comes with multiple window managers, including dwm, Awesome, Fluxbox, Openbox, wmii, i3, and Spectrwm. The BlackArch package repository is compatible with existing Arch installs. |