Toggle navigation 

* [Home](http://docs.google.com/index.html)
* [Downloads](http://docs.google.com/downloads.html)
* [Guide](http://docs.google.com/guide.html)
* [Faq](http://docs.google.com/faq.html)
* [Tools](http://docs.google.com/tools.html)
* [Community](http://docs.google.com/community.html)
* [Blog](http://docs.google.com/blog.html)
* [Donate](http://docs.google.com/donate.html)

BlackArch Linux

Penetration Testing Distribution

Over 2600 tools

Tools

## Hacking Tools List

1. [Home](http://docs.google.com/index.html)
2. Tools

**Information**

Every package of the BlackArch Linux repository is listed in the following table. If you don't find your needed tool in this list simply open an [issue](https://github.com/BlackArch/blackarch/issues/new) or better do a [pull request](https://github.com/BlackArch/blackarch/pulls) for the tool you want to be in our repository. We are fast at packaging and releasing tools.

**Tool count:** 2670

**BlackArch Linux Complete Tools List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Version | Description | Category | Website |
| 0d1n | 252.7311867 | Web security tool to make fuzzing at HTTP inputs, made in C with libCurl. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| 0trace | 1.5 | A hop enumeration tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| 3proxy | 0.9.3 | Tiny free proxy server. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| 3proxy-win32 | 0.8.13 | Tiny free proxy server. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| 42zip | 42 | Recursive Zip archive bomb. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| a2sv | 140.cb24c4e | Auto Scanning to SSL Vulnerability. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| abcd | 4.2738809 | ActionScript ByteCode Disassembler. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| abuse-ssl-bypass-waf | 6.36a80af | Bypassing WAF by abusing SSL/TLS Ciphers. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| acccheck | 0.2.1 | A password dictionary attack tool that targets windows authentication via the SMB protocol. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ace | 1.10 | Automated Corporate Enumerator. A simple yet powerful VoIP Corporate Directory enumeration tool that mimics the behavior of an IP Phone in order to download the name and extension entries that a given phone can display on its screen interface | [blackarch-voip](http://docs.google.com/voip.html) |  |
| aclpwn | 4.81480cc | Active Directory ACL exploitation with BloodHound. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| activedirectoryenum | 0.5.0 | Enumerate AD through LDAP. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ad-ldap-enum | 44.1386673 | An LDAP based Active Directory user and group enumeration tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| adape-script | 43.4d0b9ff | Active Directory Assessment and Privilege Escalation Script. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| adfind | 29.179602f | Simple admin panel finder for php,js,cgi,asp and aspx admin panels. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| admid-pack | 0.1 | ADM DNS spoofing tools - Uses a variety of active and passive methods to spoof DNS packets. Very powerful. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| adminpagefinder | 0.1 | This python script looks for a large amount of possible administrative interfaces on a given site. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| admsnmp | 0.1 | ADM SNMP audit scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| aesfix | 1.0.1 | A tool to find AES key in RAM. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| aeskeyfind | 1.0 | A tool to find AES key in RAM. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| aespipe | 2.4f | Reads data from stdin and outputs encrypted or decrypted results to stdout. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| aesshell | 0.7 | A backconnect shell for Windows and Unix written in python and uses AES in CBC mode in conjunction with HMAC-SHA256 for secure transport. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| afflib | 3.7.19 | An extensible open format for the storage of disk images and related forensic information. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| aflplusplus | 3.12c.r5.gf7179e44 | American Fuzzing Lop fuzzer with community patches and additional features. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| afpfs-ng | 0.8.2 | A client for the Apple Filing Protocol (AFP) | [blackarch-networking](http://docs.google.com/networking.html) |  |
| agafi | 1.1 | A gadget finder and a ROP-Chainer tool for x86 platforms. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| against | 0.2 | A very fast ssh attacking script which includes a multithreaded port scanning module (tcp connect) for discovering possible targets and a multithreaded brute-forcing module which attacks parallel all discovered hosts or given ip addresses from a list. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| aggroargs | 51.c032446 | Bruteforce commandline buffer overflows, linux, aggressive arguments. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| aiengine | 2.0.1 | A packet inspection engine with capabilities of learning without any human intervention. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| aimage | 3.2.5 | A program to create aff-images. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| aiodnsbrute | 38.e773a4c | Python 3 DNS asynchronous brute force utility. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| air | 2.0.0 | A GUI front-end to dd/dc3dd designed for easily creating forensic images. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| aircrack-ng | 1.6 | Key cracker for the 802.11 WEP and WPA-PSK protocols | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| airflood | 0.1 | A modification of aireplay that allows for a DoS of the AP. This program fills the table of clients of the AP with random MACs doing impossible new connections. [Tool in Spanish] | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| airgeddon | 2463.7eba4f6 | Multi-use bash script for Linux systems to audit wireless networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| airopy | 5.b83f11d | Get (wireless) clients and access points. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| airoscript | 45.0a122ee | A script to simplify the use of aircrack-ng tools. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| airpwn | 1.4 | A tool for generic packet injection on an 802.11 network. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| ajpfuzzer | 0.6 | A command-line fuzzer for the Apache JServ Protocol (ajp13). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| albatar | 34.4e63f22 | A SQLi exploitation framework in Python. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| allthevhosts | 1.0 | A vhost discovery tool that scrapes various web applications. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| altdns | 68.689cc81 | Generates permutations, alterations and mutations of subdomains and then resolves them. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| amass | 1099.22dd146 | In-depth subdomain enumeration written in Go. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| amber | 254.a331b34 | Reflective PE packer. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| amoco | v2.4.1.r286.gd3c2fab | Yet another tool for analysing binaries. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| analyzemft | 125.79a33ce | Parse the MFT file from an NTFS filesystem. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| analyzepesig | 0.0.0.5 | Analyze digital signature of PE file. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| androbugs | 1.7fd3a2c | An efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| androguard | 2118.8d091cbb | Reverse engineering, Malware and goodware analysis of Android applications and more. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| androick | 8.522cfb4 | A python tool to help in forensics analysis on android. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| android-apktool | 2.5.0 | A tool for reverse engineering Android apk files. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| android-ndk | r22 | Android C/C++ developer kit | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| android-sdk | 26.1.1 | Google Android SDK | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| android-udev-rules | 427.254e497 | Android udev rules. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| androidpincrack | 2.ddaf307 | Bruteforce the Android Passcode given the hash and salt. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| androidsniffer | 0.1 | A perl script that lets you search for 3rd party passwords, dump the call log, dump contacts, dump wireless configuration, and more. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| androwarn | 135.626c02d | Yet another static code analyzer for malicious Android applications. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| angr | 8.20.7.27 | The next-generation binary analysis platform from UC Santa Barbaras Seclab. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| angr-management | 8.20.7.27 | This is the GUI for angr. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| angr-py2 | 7.8.9.26 | The next-generation binary analysis platform from UC Santa Barbaras Seclab. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| angrop | 184.dbb26d2 | A rop gadget finder and chain builder. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| anontwi | 1.1b | A free software python client designed to navigate anonymously on social networks. It supports Identi.ca and Twitter.com. | [blackarch-social](http://docs.google.com/social.html) |  |
| anti-xss | 166.2725dc9 | A XSS vulnerability scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| antiransom | 3.02 | A tool capable of detect and stop attacks of Ransomware using honeypots. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| apache-users | 2.1 | This perl script will enumerate the usernames on a unix system that use the apache module UserDir. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| apacket | 374.16e7036 | Sniffer syn and backscatter packets. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| aphopper | 0.3 | A program that automatically hops between access points of different wireless networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| apkid | 2.1.0 | Android Application Identifier for Packers, Protectors, Obfuscators and Oddities. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| apkstat | 18.81cdad3 | Automated Information Retrieval From APKs For Initial Analysis. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| apkstudio | 100.9e114ca | An IDE for decompiling/editing & then recompiling of android application binaries. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| apnbf | 0.1 | A small python script designed for enumerating valid APNs (Access Point Name) on a GTP-C speaking device. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| appmon | 173.eb773a9 | A runtime security testing & profiling framework for native apps on macOS, iOS & android and it is built using Frida. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| apt2 | 175.6732505 | Automated penetration toolkit. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| aquatone | 120.854a5d5 | A Tool for Domain Flyovers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| arachni | 1.5.1.2.gd869f0aa3 | A feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| aranea | 6.469b9ee | A fast and clean dns spoofing tool. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| archivebox | 903.59da482 | The open source self-hosted web archive. Takes browser history/bookmarks/Pocket/Pinboard/etc., saves HTML, JS, PDFs, media, and more. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| arduino | 1.8.13 | Arduino prototyping platform SDK | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| argon2 | 20190702 | A password-hashing function (reference C implementation) | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| argus | 3.0.8.2 | Network monitoring tool with flow control. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| argus-clients | 3.0.8.2 | Network monitoring client for Argus. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| arjun | 156.dfec996 | HTTP parameter discovery suite. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| armitage | 150813 | A graphical cyber attack management tool for Metasploit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| armor | 5.bae27a6 | A simple Bash script designed to create encrypted macOS payloads capable of evading antivirus scanners. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| armscgen | 98.c51b7d6 | ARM Shellcode Generator (Mostly Thumb Mode). | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| arp-scan | 1.9.7 | A tool that uses ARP to discover and fingerprint IP hosts on the local network | [blackarch-networking](http://docs.google.com/networking.html) |  |
| arpalert | 2.0.12 | Monitor ARP changes in ethernet networks. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| arpoison | 0.7 | The UNIX arp cache update utility | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| arpon | 2.7 | A portable handler daemon that make ARP protocol secure in order to avoid the Man In The Middle (MITM) attack through ARP Spoofing, ARP Cache Poisoning or ARP Poison Routing (APR) attacks. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| arpstraw | 27.ab40e13 | Arp spoof detection tool. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| arptools | 13.41cdb23 | A simple tool about ARP broadcast, ARP attack, and data transmission. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| arpwner | 26.f300fdf | GUI-based python tool for arp poisoning and dns poisoning attacks. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| artillery | 357.805a5d8 | A combination of a honeypot, file-system monitoring, system hardening, and overall health of a server to create a comprehensive way to secure a system. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| artlas | 152.bc26f20 | Apache Real Time Logs Analyzer System. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| arybo | 65.89d9a42 | Manipulation, canonicalization and identification of mixed boolean-arithmetic symbolic expressions. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| asleap | 2.2 | Actively recover LEAP/PPTP passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| asp-audit | 2BETA | An ASP fingerprinting tool and vulnerability scanner. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| assetfinder | 19.4e95d87 | Find domains and subdomains potentially related to a given domain. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| astra | 486.394d538 | Automated Security Testing For REST API's. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| atear | 139.245ec8d | Wireless Hacking, WiFi Security, Vulnerability Analyzer, Pentestration. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| atftp | 0.7.4 | Client/server implementation of the TFTP protocol that implements RFCs 1350, 2090, 2347, 2348, and 2349 | [blackarch-networking](http://docs.google.com/networking.html) |  |
| athena-ssl-scanner | 0.6.2 | A SSL cipher scanner that checks all cipher codes. It can identify about 150 different ciphers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| atlas | 7.77bd6c8 | Open source tool that can suggest sqlmap tampers to bypass WAF/IDS/IPS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| atscan | 2451.ea67ace | Server, Site and Dork Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| atstaketools | 0.1 | This is an archive of various @Stake tools that help perform vulnerability scanning and analysis, information gathering, password auditing, and forensics. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| attacksurfacemapper | 41.3793ec4 | Tool that aims to automate the reconnaissance process. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| attk | 2.0.1023 | Trend Micro Anti-Threat Toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| aurebeshjs | 65.43c69e7 | Translate JavaScript to Other Alphabets. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| auto-eap | 18.ee36d37 | Automated Brute-Force Login Attacks Against EAP Networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| auto-xor-decryptor | 7.2eb176d | Automatic XOR decryptor tool. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| automato | 33.0561b59 | Should help with automating some of the user-focused enumeration tasks during an internal penetration test. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| autonessus | 24.7933022 | This script communicates with the Nessus API in an attempt to help with automating scans. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| autonse | 25.7c87f4c | Massive NSE (Nmap Scripting Engine) AutoSploit and AutoScanner. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| autopsy | 4.18.0 | The forensic browser. A GUI for the Sleuth Kit. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| autopwn | 190.fc80cef | Specify targets and run sets of tools against them. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| autorecon | 80.7481ac9 | A multi-threaded network reconnaissance tool which performs automated enumeration of services. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| autosint | 234.e1f4937 | Tool to automate common osint tasks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| autosploit | 281.9a6a5ef | Automate the exploitation of remote hosts. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| autovpn | 18.28b1a87 | Easily connect to a VPN in a country of your choice. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| avaloniailspy | 191.8799e6d | .NET Decompiler (port of ILSpy) | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| avet | 133.2f1d882 | AntiVirus Evasion Tool | [blackarch-binary](http://docs.google.com/binary.html) |  |
| avml | 27.52c1199 | A portable volatile memory acquisition tool for Linux. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| aws-extender-cli | 17.a351154 | Script to test S3 buckets as well as Google Storage buckets and Azure Storage containers for common misconfiguration issues. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| aws-inventory | 19.9a2fa8e | Discover resources created in an AWS account. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| awsbucketdump | 80.b704285 | A tool to quickly enumerate AWS S3 buckets to look for loot. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| azazel | 15.a41fbb5 | A userland rootkit based off of the original LD\_PRELOAD technique from Jynx rootkit. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| aztarna | 1.2.1 | A footprinting tool for ROS and SROS systems. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| backcookie | 51.6dabc38 | Small backdoor using cookie. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| backdoor-apk | 141.2710126 | Shell script that simplifies the process of adding a backdoor to any Android APK file | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| backdoor-factory | 205.896844f | Patch win32/64 binaries with shellcode. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| backdoorme | 308.f9755ca | A powerful utility capable of backdooring Unix machines with a slew of backdoors. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| backdoorppt | 88.d0e7f91 | Transform your payload.exe into one fake word doc (.ppt). | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| backfuzz | 1.b0648de | A network protocol fuzzing toolkit. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| backhack | 39.561ec86 | Tool to perform Android app analysis by backing up and extracting apps, allowing you to analyze and modify file system contents for apps. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| backoori | 55.988e507 | Tool aided persistence via Windows URI schemes abuse. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| backorifice | 1.0 | A remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| bad-pdf | 61.a8149ee | Steal NTLM Hashes with Bad-PDF. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| badkarma | 85.2c46334 | Advanced network reconnaissance toolkit. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| badministration | 16.69e4ec2 | A tool which interfaces with management or administration applications from an offensive standpoint. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bagbak | 123.990ef6b | Yet another frida based App decryptor. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| balbuzard | 67.d6349ef1bc55 | A package of malware analysis tools in python to extract patterns of interest from suspicious files (IP addresses, domain names, known file headers, interesting strings, etc). | [blackarch-malware](http://docs.google.com/malware.html) |  |
| bamf-framework | 35.30d2b4b | A modular framework designed to be a platform to launch attacks against botnets. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| bandicoot | 0.6.0 | A toolbox to analyze mobile phone metadata. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| barf | 923.9547ef8 | A multiplatform open source Binary Analysis and Reverse engineering Framework. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| barmie | 1.01 | Java RMI enumeration and attack tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| barq | 35.6f1a68c | An AWS Cloud Post Exploitation framework. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| base64dump | 0.0.12 | Extract and decode base64 strings from files. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| basedomainname | 0.1 | Tool that can extract TLD (Top Level Domain), domain extensions (Second Level Domain + TLD), domain name, and hostname from fully qualified domain names. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| bashfuscator | 338.7487348 | Fully configurable and extendable Bash obfuscation framework. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| batctl | 2021.0 | B.A.T.M.A.N. advanced control and management tool | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| batman-adv | 2019.2 | Batman kernel module, (included upstream since .38) | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| batman-alfred | 2021.0 | Almighty Lightweight Fact Remote Exchange Daemon | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| bbqsql | 261.b9859d2 | SQL injection exploit tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bbscan | 44.4b82032 | A tiny Batch web vulnerability Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bdfproxy | 105.3fecc12 | Patch Binaries via MITM: BackdoorFactory + mitmProxy | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| bdlogparser | 2 | This is a utility to parse a Bit Defender log file, in order to sort them into a malware archive for easier maintenance of your malware collection. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| bed | 0.5 | Collection of scripts to test for buffer overflows, format string vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| beebug | 25.cddb375 | A tool for checking exploitability. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| beef | 3922.90798571 | The Browser Exploitation Framework that focuses on the web browser. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| beeswarm | 1183.db51ea0 | Honeypot deployment made easy http://www.beeswarm-ids.org/ | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| beholder | 0.8.10 | A wireless intrusion detection tool that looks for anomalies in a wifi environment. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| belati | 72.49577a1 | The Traditional Swiss Army Knife for OSINT. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| beleth | 36.0963699 | A Multi-threaded Dictionary based SSH cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| bettercap | 2.30.2 | Swiss army knife for network attacks and monitoring | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| bettercap-ui | 1.3.0 | Official Bettercap's Web UI. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| bfac | 52.18dabcc | An automated tool that checks for backup artifacts that may disclose the web-application's source code. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| bfbtester | 2.0.1 | Performs checks of single and multiple argument command line overflows and environment variable overflows | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| bfuzz | 59.e82cbf4 | Input based fuzzer tool for browsers. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| bgp-md5crack | 0.1 | RFC2385 password cracker | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| bgrep | 24.28029c9 | Binary grep. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| billcipher | 32.97fba59 | Information Gathering tool for a Website or IP address. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| binaryninja-demo | 2.2.2487 | A new kind of reversing platform (demo version). | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| binaryninja-python | 13.83f59f7 | Binary Ninja prototype written in Python. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| bind | 9.16.13 | A complete, highly portable implementation of the DNS protocol | [blackarch-networking](http://docs.google.com/networking.html) |  |
| bindead | 4504.67019b97b | A static analysis tool for binaries | [blackarch-binary](http://docs.google.com/binary.html) |  |
| bindiff | 6.0.0 | A comparison tool for binary files, that assists vulnerability researchers and engineers to quickly find differences and similarities in disassembled code. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| binex | 1.0 | Format String exploit building tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| binflow | 5.7fb02a9 | POSIX function tracing. Much better and faster than ftrace. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| bing-ip2hosts | 1.0.3 | Enumerates all hostnames which Bing has indexed for a specific IP address. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| bing-lfi-rfi | 0.1 | Python script for searching Bing for sites that may have local and remote file inclusion vulnerabilities. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bingoo | 3.698132f | A Linux bash based Bing and Google Dorking Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| binnavi | 6.1.0 | A binary analysis IDE that allows to inspect, navigate, edit and annotate control flow graphs and call graphs of disassembled code. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| binproxy | 8.d02fce9 | A proxy for arbitrary TCP connections. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| binwalk | 2.3.0 | A tool for searching a given binary image for embedded files | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| binwally | 4.0aabd8b | Binary and Directory tree comparison tool using the Fuzzy Hashing concept (ssdeep). | [blackarch-binary](http://docs.google.com/binary.html) |  |
| bios\_memimage | 1.2 | A tool to dump RAM contents to disk (aka cold boot attack). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| birp | 65.b2e108a | A tool that will assist in the security assessment of mainframe applications served over TN3270. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| bitdump | 34.6a5cbd8 | A tool to extract database data from a blind SQL injection vulnerability. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| bittwist | 2.0 | A simple yet powerful libpcap-based Ethernet packet generator. It is designed to complement tcpdump, which by itself has done a great job at capturing network traffic. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| bkhive | 1.1.1 | Program for dumping the syskey bootkey from a Windows NT/2K/XP system hive. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| blackbox-scanner | 1.7a25220 | Dork scanner & bruteforcing & hash cracker with blackbox framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| blackeye | 27.dfcd597 | The most complete Phishing Tool, with 32 templates +1 customizable. | [blackarch-social](http://docs.google.com/social.html) |  |
| blackhash | 0.2 | Creates a filter from system hashes. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| blacknurse | 9.d2a2b23 | A low bandwidth ICMP attack that is capable of doing denial of service to well known firewalls. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| bleah | 53.6a2fd3a | A BLE scanner for "smart" devices hacking. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| bless | 0.6.3 | High-quality, full-featured hex editor | [blackarch-misc](http://docs.google.com/misc.html) |  |
| bletchley | 0.0.1 | A collection of practical application cryptanalysis tools. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| blind-sql-bitshifting | 54.5bbc183 | A blind SQL injection module that uses bitshfting to calculate characters. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| blindelephant | 7 | A web application fingerprinter. Attempts to discover the version of a (known) web application by comparing static files at known locations | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| blindsql | 1.0 | Set of bash scripts for blind SQL injection attacks. | [blackarch-database](http://docs.google.com/database.html) |  |
| blindy | 12.59de8f2 | Simple script to automate brutforcing blind sql injection vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| blisqy | 20.e9995fc | Exploit Time-based blind-SQL injection in HTTP-Headers (MySQL/MariaDB). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bloodhound | 1195.0da9efe | Six Degrees of Domain Admin | [blackarch-recon](http://docs.google.com/recon.html) |  |
| bloodhound-python | v1.0.1.r27.g2c1c178 | Bloodhound python data collector | [blackarch-recon](http://docs.google.com/recon.html) |  |
| bluebox-ng | 1.1.0 | A GPL VoIP/UC vulnerability scanner. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| bluebugger | 0.1 | An implementation of the bluebug technique which was discovered by Martin Herfurt. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluediving | 0.9 | A Bluetooth penetration testing suite. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluefog | 0.0.4 | A tool that can generate an essentially unlimited number of phantom Bluetooth devices. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluelog | 1.1.2 | A Bluetooth scanner and sniffer written to do a single task, log devices that are in discoverable mode. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluepot | 0.1 | A Bluetooth Honeypot written in Java, it runs on Linux | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| blueprint | 0.1\_3 | A perl tool to identify Bluetooth devices. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| blueranger | 1.0 | A simple Bash script which uses Link Quality to locate Bluetooth device radios. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| bluescan | 1.0.6 | A Bluetooth Device Scanner. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluesnarfer | 0.1 | A bluetooth attacking tool. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluphish | 9.a7200bd | Bluetooth device and service discovery tool that can be used for security assessment and penetration testing. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bluto | 142.25cad7a | Recon, Subdomain Bruting, Zone Transfers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| bmap-tools | 3.6 | Tool for copying largely sparse files using information from a block map file. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| bmc-tools | 21.4366855 | RDP Bitmap Cache parser. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| bob-the-butcher | 0.7.1 | A distributed password cracker package. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| bof-detector | 19.e08367d | A simple detector of BOF vulnerabilities by source-code-level check. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| bonesi | 12.733c9e9 | The DDoS Botnet Simulator. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| boopsuite | 170.16c902f | A Suite of Tools written in Python for wireless auditing and security testing. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| bopscrk | 72.34fb3fd | Tool to generate smart wordlists, eg. based on lyrics. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| botb | 61.585e741 | A container analysis and exploitation tool for pentesters and engineers. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| bowcaster | 230.17d69c1 | A framework intended to aid those developing exploits. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| box-js | 387.b945f8a | A tool for studying JavaScript malware. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| braa | 0.82 | A mass snmp scanner | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| braces | 0.4 | A Bluetooth Tracking Utility. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| brakeman | 3636.aef6253a8 | A static analysis security vulnerability scanner for Ruby on Rails applications. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| brosec | 277.4b335e5 | An interactive reference tool to help security professionals utilize useful payloads and commands. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| browselist | 1.4 | Retrieves the browse list ; the output list contains computer names, and the roles they play in the network. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| browser-fuzzer | 3 | Browser Fuzzer 3 | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| brut3k1t | 102.0dcde7d | Brute-force attack that supports multiple protocols and services. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| brute-force | 52.78d1d8e | Brute-Force attack tool for Gmail Hotmail Twitter Facebook Netflix. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| brute12 | 1 | A tool designed for auditing the cryptography container security in PKCS12 format. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| bruteforce-luks | 46.a18694a | Try to find the password of a LUKS encrypted volume. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| bruteforce-salted-openssl | 53.8a2802e | Try to find the password of a file that was encrypted with the 'openssl' command. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| bruteforce-wallet | 39.f6d8cc5 | Try to find the password of an encrypted Peercoin (or Bitcoin,Litecoin, etc...) wallet file. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| brutemap | 65.da4b303 | Penetration testing tool that automates testing accounts to the site's login page. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| brutespray | 187.182ac86 | Brute-Forcing from Nmap output - Automatically attempts default creds on found services. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| brutessh | 0.6 | A simple sshd password bruteforcer using a wordlist, it's very fast for internal networks. It's multithreads. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| brutex | 102.1970e16 | Automatically brute force all services running on a target. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| brutexss | 54.ba753df | Cross-Site Scripting Bruteforcer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| brutus | 2 | One of the fastest, most flexible remote password crackers you can get your hands on. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| bsdiff | 4.3 | bsdiff and bspatch are tools for building and applying patches to binary files. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| bsqlbf | 2.7 | Blind SQL Injection Brute Forcer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bsqlinjector | 13.027184f | Blind SQL injection exploitation tool written in ruby. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| bss | 0.8 | Bluetooth stack smasher / fuzzer | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bt\_audit | 0.1.1 | Bluetooth audit | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| btcrack | 1.1 | The world's first Bluetooth Pass phrase (PIN) bruteforce tool. Bruteforces the Passkey and the Link key from captured Pairing exchanges. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| btlejack | 82.7cd784a | Bluetooth Low Energy Swiss-army knife. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| btproxy-mitm | 71.cd1c906 | Man in the Middle analysis tool for Bluetooth. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| btscanner | 2.1 | Bluetooth device scanner. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| bulk-extractor | 1551.b287b06 | Bulk Email and URL extraction tool. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| bully | 1.1.12.g04185d7 | Retrieve WPA/WPA2 passphrase from a WPS enabled access point | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| bunny | 0.93 | A closed loop, high-performance, general purpose protocol-blind fuzzer for C programs. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| burpsuite | 2021.3.1 | An integrated platform for attacking web applications (community edition) + SHELLING plugin. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| buster | 92.131437e | Find emails of a person and return info associated with them. | [blackarch-social](http://docs.google.com/social.html) |  |
| buttinsky | 138.1a2a1b2 | Provide an open source framework for automated botnet monitoring. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| bvi | 1.4.1 | A display-oriented editor for binary files operate like "vi" editor. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| byepass | 213.8cbfd9b | Automates password cracking tasks using optimized dictionaries and mangling rules. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| bypass-firewall-dns-history | 33.c55b7ce | Firewall bypass script based on DNS history records. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| bytecode-viewer | 2.9.22 | A Java 8/Android APK Reverse Engineering Suite. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| c5scan | 30.be8845c | Vulnerability scanner and information gatherer for the Concrete5 CMS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cachedump | 1.1 | A tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| cadaver | 0.23.3 | Command-line WebDAV client for Unix | [blackarch-networking](http://docs.google.com/networking.html) |  |
| cafebabe | 0.1.2 | Java bytecode editor & decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| cameradar | 139.0984607 | Hacks its way into RTSP videosurveillance cameras. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| camscan | 1.0057215 | A tool which will analyze the CAM table of Cisco switches to look for anamolies. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| can-utils | 738.02b330a | Linux-CAN / SocketCAN user space applications. | [blackarch-automobile](http://docs.google.com/automobile.html) |  |
| canalyzat0r | 41.6bc251e | Security analysis toolkit for proprietary car protocols. | [blackarch-automobile](http://docs.google.com/automobile.html) |  |
| canari | 3.3.10 | Maltego rapid transform development and execution framework. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| cangibrina | 123.6de0165 | Dashboard Finder. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cansina | 51.9d171bd | A python-based Web Content Discovery Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cantoolz | 425.82d330b | Framework for black-box CAN network analysis. | [blackarch-automobile](http://docs.google.com/automobile.html) |  |
| capfuzz | 34.97ac312 | Capture, fuzz and intercept web traffic. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| capstone | 4.0.2 | Lightweight multi-platform, multi-architecture disassembly framework | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| captipper | 74.3fb2836 | Malicious HTTP traffic explorer tool. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| cardpwn | 32.166abf9 | OSINT Tool to find Breached Credit Cards Information. | [blackarch-social](http://docs.google.com/social.html) |  |
| carwhisperer | 0.2 | Intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| casefile | 1.0.1 | The little brother to Maltego without transforms, but combines graph and link analysis to examine links between manually added data to mind map your information | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| catnthecanary | 7.e9184fe | An application to query the canary.pw data set for leaked data. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| catphish | 44.768d213 | For phishing and corporate espionage. | [blackarch-social](http://docs.google.com/social.html) |  |
| ccrawldns | 4.0bebd49 | Retrieves from the CommonCrawl data set unique subdomains for a given domain name. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cdpsnarf | 0.1.6 | Cisco discovery protocol sniffer. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| cecster | 5.15544cb | A tool to perform security testing against the HDMI CEC (Consumer Electronics Control) and HEC (HDMI Ethernet Channel) protocols. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| centry | 72.6de2868 | Cold boot & DMA protection | [blackarch-misc](http://docs.google.com/misc.html) |  |
| certgraph | 157.41f78b5 | Crawl the graph of certificate Alternate Names. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cewl | 108.12e9fa0 | A custom word list generator. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| cflow | 1.6 | A C program flow analyzer. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| cfr | 150 | Another Java decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| chameleon | 27.a2f0cf1 | A tool for evading Proxy categorisation. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| chameleonmini | 394.29f3d85 | Official repository of ChameleonMini, a freely programmable, portable tool for NFC security analysis that can emulate and clone contactless cards, read RFID tags and sniff/log RF data. | [blackarch-social](http://docs.google.com/social.html) |  |
| changeme | 266.89f59d4 | A default credential scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| chankro | 21.7b6e844 | Tool that generates a PHP capable of run a custom binary (like a meterpreter) or a bash script (p.e. reverse shell) bypassing disable\_functions & open\_basedir). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| chaos-client | 83.623cb47 | Go client to communicate with Chaos dataset API. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| chaosmap | 1.3 | An information gathering tool and dns / whois / web server scanner | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| chaosreader | 0.94 | A freeware tool to trace tcp, udp etc. sessions and fetch application data from snoop or tcpdump logs. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| chapcrack | 17.ae2827f | A tool for parsing and decrypting MS-CHAPv2 network handshakes. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cheat-sh | 6 | The only cheat sheet you need. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| check-weak-dh-ssh | 0.1 | Debian OpenSSL weak client Diffie-Hellman Exchange checker. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| checkiban | 0.2 | Checks the validity of an International Bank Account Number (IBAN). | [blackarch-misc](http://docs.google.com/misc.html) |  |
| checkpwd | 1.23 | Oracle Password Checker (Cracker). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| checksec | 2.4.0 | Tool designed to test which standard Linux OS and PaX security features are being used | [blackarch-automation](http://docs.google.com/automation.html) |  |
| chiasm-shell | 33.e20ed9f | Python-based interactive assembler/disassembler CLI, powered byKeystone/Capstone. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| chipsec | 1075.9a2536c | Platform Security Assessment Framework. | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| chiron | 48.524abe1 | An all-in-one IPv6 Penetration Testing Framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| chisel | 160.92d90be | A fast TCP tunnel over HTTP. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| chkrootkit | 0.54 | Checks for rootkits on a system. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| chntpw | 140201 | Offline NT Password Editor - reset passwords in a Windows NT SAM user database file | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| chopshop | 413.3dfb7be | Protocol Analysis/Decoder Framework. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| choronzon | 4.d702c31 | An evolutionary knowledge-based fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| chownat | 0.08b | Allows two peers behind two separate NATs with no port forwarding and no DMZ setup on their routers to directly communicate with each other | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| chrome-decode | 0.1 | Chrome web browser decoder tool that demonstrates recovering passwords. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| chromefreak | 24.12745b1 | A Cross-Platform Forensic Framework for Google Chrome | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| chromensics | 1.0 | A Google chrome forensics tool. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| chw00t | 39.1fd1016 | Unices chroot breaking tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| cidr2range | 1.0 | Script for listing the IP addresses contained in a CIDR netblock. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| cintruder | 14.f8a3f12 | An automatic pentesting tool to bypass captchas. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cipherscan | 419.c67f3ee | A very simple way to find out which SSL ciphersuites are supported by a target. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ciphertest | 22.e33eb4a | A better SSL cipher checker using gnutls. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| ciphr | 127.5da7137 | A CLI tool for encoding, decoding, encryption, decryption, and hashing streams of data. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| cirt-fuzzer | 1.0 | A simple TCP/UDP protocol fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| cisco-auditing-tool | 1 | Perl script which scans cisco routers for common vulnerabilities. Checks for default passwords, easily guessable community names, and the IOS history bug. Includes support for plugins and scanning multiple hosts. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cisco-global-exploiter | 1.3 | A perl script that targets multiple vulnerabilities in the Cisco Internetwork Operating System (IOS) and Catalyst products. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| cisco-ocs | 0.2 | Cisco Router Default Password Scanner. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cisco-router-config | 1.1 | Tools to copy and merge Cisco Routers Configuration. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| cisco-scanner | 0.2 | Multithreaded Cisco HTTP vulnerability scanner. Tested on Linux, OpenBSD and Solaris. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cisco-snmp-enumeration | 10.ad06f57 | Automated Cisco SNMP Enumeration, Brute Force, Configuration Download and Password Cracking. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| cisco-snmp-slap | 5.daf0589 | IP address spoofing tool in order to bypass an ACL protecting an SNMP service on Cisco IOS devices. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| cisco-torch | 0.4b | Cisco Torch mass scanning, fingerprinting, and exploitation tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| cisco5crack | 2.c4b228c | Crypt and decrypt the cisco enable 5 passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cisco7crack | 2.f1c21dd | Crypt and decrypt the cisco enable 7 passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ciscos | 1.3 | Scans class A, B, and C networks for cisco routers which have telnet open and have not changed the default password from cisco. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| citadel | 95.3b1adbc | A library of OSINT tools. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cjexploiter | 6.72b08d8 | Drag and Drop ClickJacking exploit development assistance tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| clair | 2.1.4 | Vulnerability Static Analysis for Containers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| clamscanlogparser | 1 | This is a utility to parse a Clam Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your malware collection. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| climber | 30.5530a78 | Check UNIX/Linux systems for privilege escalation. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cloakify | 117.f45c3b3 | Data Exfiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of Analysts; Evade AV Detection. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| cloud-buster | 194.b55e4a1 | A tool that checks Cloudflare enabled sites for origin IP leaks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cloudfail | 77.fcd9016 | Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cloudflare-enum | 10.412387f | Cloudflare DNS Enumeration Tool for Pentesters. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cloudget | 64.cba10b1 | Python script to bypass cloudflare from command line. Built upon cfscrape module. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cloudlist | 13.680250c | A tool for listing Assets from multiple Cloud Providers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cloudmare | 67.032751f | A simple tool to find origin servers of websites protected by CloudFlare with a misconfiguration DNS. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cloudsploit | 770.9d5683d3 | AWS security scanning checks. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cloudunflare | 14.b91a8a7 | Reconnaissance Real IP address for Cloudflare Bypass. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| clusterd | 143.d190b2c | Automates the fingerprinting, reconnaissance, and exploitation phases of an application server attack. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| cminer | 25.d766f7e | A tool for enumerating the code caves in PE files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| cmospwd | 5.1 | Decrypts password stored in CMOS used to access BIOS setup. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cms-explorer | 15.23b58cd | Designed to reveal the specific modules, plugins, components and themes that various cms driven websites are running. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| cms-few | 0.1 | Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cmseek | 349.d22deab | CMS (Content Management Systems) Detection and Exploitation suite. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cmsfuzz | 5.6be5a98 | Fuzzer for wordpress, cold fusion, drupal, joomla, and phpnuke. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cmsmap | 8.59dd0e2 | A python open source Content Management System scanner that automates the process of detecting security flaws of the most popular CMSs. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cmsscan | 41.45a0360 | CMS scanner to identify and find vulnerabilities for Wordpress, Drupal, Joomla, vBulletin. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cmsscanner | 0.13.3.2.gd3c6dcb | CMS Scanner Framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cnamulator | 5.4667c68 | A phone CNAM lookup utility using the OpenCNAM API. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| cntlm | 4.b35d55c | An NTLM, NTLM2SR, and NTLMv2 authenticating HTTP proxy. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| codeql | 2.2.5 | The CLI tool for GitHub CodeQL | [blackarch-automation](http://docs.google.com/automation.html) |  |
| codetective | 45.52b91f1 | A tool to determine the crypto/encoding algorithm used according to traces of its representation. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| comission | 203.67b890e | WhiteBox CMS analysis. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| commix | 1594.c2d1ab53 | Automated All-in-One OS Command Injection and Exploitation Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| commonspeak | 36.f0aad23 | Leverages publicly available datasets from Google BigQuery to generate wordlists. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| complemento | 0.7.6 | A collection of tools for pentester: LetDown is a powerful tcp flooder ReverseRaider is a domain scanner that use wordlist scanning or reverse resolution scanning Httsquash is an http server scanner, banner grabber and data retriever | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| configpush | 0.8.5 | This is a tool to span /8-sized networks quickly sending snmpset requests with default or otherwise specified community string to Cisco devices. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| conpot | 0.6.0 | ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting industrial control systems. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| conscan | 1.2 | A blackbox vulnerability scanner for the Concre5 CMS. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| cookie-cadger | 1.08 | An auditing tool for Wi-Fi or wired Ethernet connections. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| corkscrew | 2.0 | A tool for tunneling SSH through HTTP proxies | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| corscanner | 92.65f6de3 | Fast CORS misconfiguration vulnerabilities scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| corstest | 10.beffd0b | A simple CORS misconfigurations checker. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| corsy | 64.06f4d4a | CORS Misconfiguration Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cottontail | 93.b7f5222 | Capture all RabbitMQ messages being sent through a broker. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| cowpatty | 4.8 | Wireless WPA/WPA2 PSK handshake cracking utility | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| cpfinder | 0.1 | Simple script that looks for administrative web interfaces. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cppcheck | 2.4.1 | A tool for static C/C++ code analysis | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| cpptest | 2.0.0 | A portable and powerful, yet simple, unit testing framework for handling automated tests in C++. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| cr3dov3r | 46.99a1660 | Search for public leaks for email addresses + check creds against 16 websites. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| crabstick | 47.bb7827f | Automatic remote/local file inclusion vulnerability analysis and exploit tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| crackhor | 2.ae7d83f | A Password cracking utility. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| crackle | 111.d83b4b6 | Crack and decrypt BLE encryption. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| crackmapexec | 620.15df163 | A swiss army knife for pentesting Windows/Active Directory environments. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| crackq | 48.89b7318 | Hashcrack.org GPU-accelerated password cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| crackserver | 33.e5763ab | An XMLRPC server for password cracking. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| crawlic | 51.739fe2b | Web recon tool (find temporary files, parse robots.txt, search folders, google dorks and search domains hosted on same server). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| creak | 40.52b0d74 | Poison, reset, spoof, redirect MITM script. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| create\_ap | 265.462c09f | A shell script to create a NATed/Bridged Software Access Point. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| creddump | 3.ed95e1a | A python tool to extract various credentials and secrets from Windows registry hives. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| credmap | 116.d862247 | The Credential mapper - Tool that was created to bring awareness to the dangers of credential reuse. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| creds | 17.1ec8297 | Harvest FTP/POP/IMAP/HTTP/IRC credentials along with interesting data from each of the protocols. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| credsniper | 21.f52461b | Phishing framework written with the Python micro-framework Flask and Jinja2 templating which supports capturing 2FA tokens. | [blackarch-social](http://docs.google.com/social.html) |  |
| creepy | 137.9f60449 | A geolocation information gatherer. Offers geolocation information gathering through social networking platforms. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cribdrag | 5.2d27dbf | An interactive crib dragging tool for cryptanalysis on ciphertext generated with reused or predictable stream cipher keys. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| crlf-injector | 8.abaf494 | A python script for testing CRLF injecting issues. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| crosslinked | 24.ac99bba | LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping. | [blackarch-social](http://docs.google.com/social.html) |  |
| crosstool-ng | 1.24.0 | Versatile (cross-)toolchain generator. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| crowbar | 111.4b563dc | A brute forcing tool that can be used during penetration tests. It is developed to support protocols that are not currently supported by thc-hydra and other popular brute forcing tools. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| crozono | 5.6a51669 | A modular framework designed to automate the penetration testing of wireless networks from drones and such unconventional devices. | [blackarch-drone](http://docs.google.com/drone.html) |  |
| crunch | 3.6 | A wordlist generator for all combinations/permutations of a given character set. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| crypthook | 18.690dcae | TCP/UDP symmetric encryption tunnel wrapper. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| cryptohazemultiforcer | 1.31a | High performance multihash brute forcer with CUDA support. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cryptonark | 0.5.7 | SSL security checker. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| csrftester | 1.0 | The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ct-exposer | 23.23e8c84 | An OSINT tool that discovers sub-domains by searching Certificate Transparency logs. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ctf-party | v1.4.0.r1.gd765c87 | A CLI tool & library to enhance and speed up script/exploit writing for CTF players. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ctunnel | 0.7 | Tunnel and/or proxy TCP or UDP connections via a cryptographic tunnel. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| ctypes-sh | 153.6982e6c | Allows you to call routines in shared libraries from within bash. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| cuckoo | 2.0.7 | Automated malware analysis system. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| cudahashcat | 2.01 | Worlds fastest WPA cracker with dictionary mutation engine. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cupp | 77.56547fd | Common User Password Profiler | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| cutycapt | 10 | A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| cve-api | 170.8e9c247 | Unofficial api for cve.mitre.org. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| cve-search | v4.0.r121.ga5398de | A tool to perform local searches for known vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| cvechecker | 4.0 | The goal of cvechecker is to report about possible vulnerabilities on your system, by scanning the installed software and matching the results with the CVE database. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| cybercrowl | 111.f7cac52 | A Python Web path scanner tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| cyberscan | 75.ca85794 | A Network Pentesting Tool | [blackarch-networking](http://docs.google.com/networking.html) |  |
| cymothoa | 1 | A stealth backdooring tool, that inject backdoor's shellcode into an existing process. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| d-tect | 13.9555c25 | Pentesting the Modern Web. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dagon | 244.f065d7b | Advanced Hash Manipulation. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| dalfox | 680.1fae39d | Parameter Analysis and XSS Scanning tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| damm | 32.60e7ec7 | Differential Analysis of Malware in Memory. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| daredevil | 41.dfa025e | A tool to perform (higher-order) correlation power analysis attacks (CPA). | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| dark-dork-searcher | 1.0 | Dark-Dork Searcher. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| darkarmour | 4.f10228a | Store and execute an encrypted windows binary from inside memory, without a single bit touching disk. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| darkbing | 0.1 | A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| darkd0rk3r | 1.0 | Python script that performs dork searching and searches for local file inclusion and SQL injection errors. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| darkdump | 16.e43aefb | Search The Deep Web Straight From Your Terminal. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| darkjumper | 5.8 | This tool will try to find every website that host at the same server at your target. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| darkmysqli | 1.6 | Multi-Purpose MySQL Injection Tool | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| darkscrape | 68.2ca0e37 | OSINT Tool For Scraping Dark Websites. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| darkspiritz | 6.4d23e94 | A penetration testing framework for Linux, MacOS, and Windows systems. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| darkstat | 3.0.719 | Network statistics gatherer (packet sniffer) | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| datajackproxy | 42.f75f3a3 | A proxy which allows you to intercept TLS traffic in native x86 applications across platform. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| datasploit | 367.a270d50 | Performs automated OSINT and more. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| davoset | 1.3.7 | A tool for using Abuse of Functionality and XML External Entities vulnerabilities on some websites to attack other websites. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| davscan | 30.701f967 | Fingerprints servers, finds exploits, scans WebDAV. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| davtest | 3.a282c58 | 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. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dawnscanner | v2.0.0.rc3.r23.gf6a18fa | A static analysis security scanner for ruby written web applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dbd | 61.8cf5350 | A Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| dbpwaudit | 0.8 | A Java tool that allows you to perform online audits of password quality for several database engines. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| dbusmap | 16.6bb2831 | Simple utility for enumerating D-Bus endpoints, an nmap for D-Bus. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dc3dd | 7.2.646 | A patched version of dd that includes a number of features useful for computer forensics. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dcfldd | 1.7 | DCFL (DoD Computer Forensics Lab) dd replacement with hashing. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dcrawl | 7.3273c35 | Simple, but smart, multi-threaded web crawler for randomly gathering huge lists of unique domain names. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ddrescue | 1.25 | GNU data recovery tool | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| de4dot | 3.1.41592 | .NET deobfuscator and unpacker. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| deathstar | 51.86f9cda | Automate getting Domain Admin using Empire. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| debinject | 40.88b7824 | Inject malicious code into \*.debs. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| deblaze | 1.0608dc3 | Performs method enumeration and interrogation against flash remoting end points. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| decodify | 50.76a0801 | Tool that can detect and decode encoded strings, recursively. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| deen | 595.b1a5e25 | Generic data encoding/decoding application built with PyQt5. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| delldrac | 0.1a | DellDRAC and Dell Chassis Discovery and Brute Forcer. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| delorean | 15.ccc39c2 | NTP Main-in-the-Middle tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| demiguise | 9.0293989 | HTA encryption tool for RedTeams. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| depant | 0.3a | Check network for services with default passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| depdep | 2.0 | A merciless sentinel which will seek sensitive files containing critical info leaking through your network. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| depix | 35.6ec05c9 | A tool for recovering passwords from pixelized screenshots. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| det | 31.417cbce | (extensible) Data Exfiltration Toolkit. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| detect-it-easy | 3.01 | A program for determining types of files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| detect-secrets | v1.0.3.r76.ga7dfa01 | An enterprise friendly way of detecting and preventing secrets in code. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| detect-sniffer | 151.63f0d7f | Tool that detects sniffers in the network. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| detectem | 276.bc5f073 | Detect software and its version on websites. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| devaudit | 803.ca0a68e | An open-source, cross-platform, multi-purpose security auditing tool targeted at developers and teams. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| device-pharmer | 40.b06a460 | Opens 1K+ IPs or Shodan search results and attempts to login. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| dex2jar | 2.1 | A tool for converting Android's .dex format to Java's .class format | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| dexpatcher | 1.7.0 | Modify Android DEX/APK files at source-level using Java. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| dff-scanner | 1.1 | Tool for finding path of predictable resource locations. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dfir-ntfs | 1.0.9 | An NTFS parser for digital forensics & incident response. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dga-detection | 78.0a3186e | DGA Domain Detection using Bigram Frequency Analysis. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dharma | 95.c0fc274 | Generation-based, context-free grammar fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| dhcdrop | 0.5 | Remove illegal dhcp servers with IP-pool underflow. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| dhcpf | 3.a770b20 | Passive DHCP fingerprinting implementation. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| dhcpig | 92.9fd8df5 | Enhanced DHCPv4 and DHCPv6 exhaustion and fuzzing script written in python using scapy network library. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dhcpoptinj | 123.58a12c6 | DHCP option injector. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| didier-stevens-suite | 275.dfcbfa7 | Didier Stevens Suite. |  |  |
| dinouml | 0.9.5 | A network simulation tool, based on UML (User Mode Linux) that can simulate big Linux networks on a single PC | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dirb | 2.22 | A web content scanner, brute forceing for hidden files. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dirble | 1.4.2 | Fast directory scanning and scraping tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dirbuster | 1.0\_RC1 | An application designed to brute force directories and files names on web/application servers | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dirbuster-ng | 9.0c34920 | C CLI implementation of the Java dirbuster tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| directorytraversalscan | 1.0.1.0 | Detect directory traversal vulnerabilities in HTTP servers and web applications. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| dirhunt | 266.30e98e4 | Find web directories without bruteforce. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dirscanner | 0.1 | This is a python script that scans webservers looking for administrative directories, php shells, and more. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dirscraper | 16.e752450 | OSINT Scanning tool which discovers and maps directories found in javascript files hosted on a website. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dirsearch | 1577.62a032a | HTTP(S) directory/file brute forcer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dirstalk | 1.3.2 | Modern alternative to dirbuster/dirb. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| disitool | 0.3 | Tool to work with Windows executables digital signatures. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dislocker | 549.ad87d02 | Read BitLocker encrypted volumes under Linux. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| dissector | 1 | This code dissects the internal data structures in ELF files. It supports x86 and x86\_64 archs and runs under Linux. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| distorm | 3.5.2 | Powerful disassembler library for x86/AMD64 | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| dizzy | 2.0 | A Python based fuzzing framework with many features. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| dkmc | 56.3c238f0 | Dont kill my cat - Malicious payload evasion tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| dmde | 3.6.0.770 | Disk Editor and Data Recovery Software. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dmg2img | 1.6.7 | A CLI tool to uncompress Apple's compressed DMG files to the HFS+ IMG format | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dmitry | 1.3a | Deepmagic Information Gathering Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnmap | 0.6 | The distributed nmap framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dns-parallel-prober | 56.99a7b83 | PoC for an adaptive parallelised DNS prober. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dns-reverse-proxy | 32.a5ccda3 | A reverse DNS proxy written in Go. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| dns-spoof | 13.81ba29f | Yet another DNS spoof utility. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| dns2geoip | 0.1 | A simple python script that brute forces DNS and subsequently geolocates the found subdomains. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dns2tcp | 0.5.2 | A tool for relaying TCP connections over DNS. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| dnsa | 0.6 | A dns security swiss army knife. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnsbf | 0.3 | Search for available domain names in an IP range. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnsbrute | 2.b1dc84a | Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnschef | 17.a395411 | A highly configurable DNS proxy for pentesters. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| dnscobra | 1.0 | DNS subdomain bruteforcing tool with Tor support through torsocks | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsdiag | 259.ba9102b | DNS Diagnostics and Performance Measurement Tools. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dnsdrdos | 0.1 | Proof of concept code for distributed DNS reflection DoS. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| dnsenum | 1.2.4.2 | Script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsfilexfer | 24.126edcd | File transfer via DNS. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dnsgoblin | 0.1 | Nasty creature constantly searching for DNS servers. It uses standard dns querys and waits for the replies. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnsgrep | 14.3f4fa7c | A utility for quickly searching presorted DNS names. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsmap | 0.30 | Passive DNS network mapper | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| dnspredict | 0.0.2 | DNS prediction. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnsprobe | 56.7120008 | Allows you to perform multiple dns queries of your choice with a list of user supplied resolvers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnspy | 6.1.7 | .NET debugger and assembly editor. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| dnsrecon | 0.10.1 | Python script for enumeration of hosts, subdomains and emails from a given domain using google. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnssearch | 20.e4ea439 | A subdomain enumeration tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsspider | 1.3 | A fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsteal | 26.8b5ed85 | DNS Exfiltration tool for stealthily sending files over DNS requests.. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dnstracer | 1.10 | Determines where a given DNS server gets its information from, and follows the chain of DNS servers | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnstwist | 395.89fee06 | Domain name permutation engine for detecting typo squatting, phishing and corporate espionage. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dnsvalidator | 67.b12acc0 | Maintains a list of IPv4 DNS servers by verifying them against baseline servers, and ensuring accurate responses. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dnswalk | 2.0.2 | A DNS debugger and zone-transfer utility. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dnsx | 112.6688056 | Fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| docem | 20.b0ddd87 | Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML\_XEE on steroids). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dockerscan | 59.590a844 | Docker security analysis & hacking tools. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| domain-analyzer | 0.8.1 | Finds all the security information for a given domain name. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| domain-stats | 160.2119e16 | A web API to deliver domain information from whois and alexa. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| domainhunter | 38.c185116 | Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| domato | 92.8320455 | DOM fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| domi-owned | 41.583d0a5 | A tool used for compromising IBM/Lotus Domino servers. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| domlink | 37.1cabd5d | A tool to link a domain with registered organisation names and emails, to other domains. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| donut | 368.dafea17 | Generates x86, x64 or AMD64+x86 P.I. shellcode loading .NET Assemblies from memory. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| doona | 143.bb03dad | A fork of the Bruteforce Exploit Detector Tool (BED). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| doork | 6.90c7260 | Passive Vulnerability Auditor. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| doozer | 9.5cfc8f8 | A Password cracking utility. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| dorkbot | 157.b5d7e7d | Command-line tool to scan Google search results for vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dorkme | 56.73305d6 | Tool designed with the purpose of making easier the searching of vulnerabilities with Google Dorks, such as SQL Injection vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dorknet | 58.419d6a2 | Selenium powered Python script to automate searching for vulnerable web apps. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dotdotpwn | 3.0.2 | The Transversal Directory Fuzzer. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| dotpeek | 2020.2.1 | Free .NET Decompiler and Assembly Browser. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| dpeparser | beta002 | Default password enumeration project | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| dpscan | 0.1 | Drupal Vulnerability Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dr-checker | 137.d742943 | A Soundy Vulnerability Detection Tool for Linux Kernel Drivers. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| dr0p1t-framework | 44.db9bc2d | A framework that creates a dropper that bypass most AVs, some sandboxes and have some tricks. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| dracnmap | 69.09d3945 | Tool to exploit the network and gathering information with nmap help. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| dradis-ce | 4033.13d9d682 | An open source framework to enable effective information sharing. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| dragon-backdoor | 7.c7416b7 | A sniffing, non binding, reverse down/exec, portknocking service Based on cd00r.c. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| driftnet | v1.3.0.r5.g9ad8da4 | Listens to network traffic and picks out images from TCP streams it observes. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| drinkme | 19.acf1a14 | A shellcode testing harness. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| dripcap | 0.6.15 | Caffeinated Packet Analyzer. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dripper | v1.r1.gc9bb0c9 | A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| droopescan | 1.44.1 | A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| drozer | 2.4.4 | A security testing framework for Android - Precompiled binary from official repository. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| drupal-module-enum | 11.525543c | Enumerate on drupal modules. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| drupalscan | 0.5.2 | Simple non-intrusive Drupal scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| drupwn | 59.8186732 | Drupal enumeration & exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dscanner | 0.11.0 | Swiss-army knife for D source code | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| dsd | 91.7ee04e5 | Digital Speech Decoder | [blackarch-misc](http://docs.google.com/misc.html) |  |
| dsfs | 36.8e9f8e9 | A fully functional File inclusion vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dshell | 142.695c891 | A network forensic analysis framework. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| dsjs | 32.26287d0 | A fully functional JavaScript library vulnerability scanner written in under 100 lines of code. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dsniff | 2.4b1 | Collection of tools for network auditing and penetration testing | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| dsss | 123.84ddd33 | A fully functional SQL injection vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dsstore-crawler | 4.9e003a3 | A parser + crawler for .DS\_Store files exposed publically. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dsxs | 130.3e628b6 | A fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| dtp-spoof | 4.4b2df1b | Python script/security tool to test Dynamic Trunking Protocol configuration on a switch. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dublin-traceroute | 331.06d4c88 | NAT-aware multipath tracerouting tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ducktoolkit | 35.7f1e19c | Encoding Tools for Rubber Ducky. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| dumb0 | 19.1493e74 | A simple tool to dump users in popular forums and CMS. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| dump1090 | 386.bff92c4 | A simple Mode S decoder for RTLSDR devices. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| dumpacl | 0.1 | Dumps NTs ACLs and audit settings. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| dumpusers | 1.0 | Dumps account names and information even though RestrictAnonymous has been set to 1. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| dumpzilla | 03152013 | A forensic tool for firefox. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| duplicut | 2.2 | Remove duplicates from massive wordlist, without sorting it (for dictionnary-based password cracking). | [blackarch-misc](http://docs.google.com/misc.html) |  |
| dutas | 10.37fa3ab | Analysis PE file or Shellcode. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| dvcs-ripper | 54.2c1bbc6 | Rip web accessible (distributed) version control systems: SVN/GIT/BZR/CVS/HG. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| dwarf | 1070.d418234 | Full featured multi arch/os debugger built on top of PyQt5 and frida. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| dynamorio | 8.0.18655 | A dynamic binary instrumentation framework. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| eapeak | 130.9550d1c | Analysis Suite For EAP Enabled Wireless Networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| eaphammer | 266.a5f2bdf | Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| eapmd5pass | 3.3d5551f | An implementation of an offline dictionary attack against the EAP-MD5 protocol. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| easy-creds | 45.bf9f00c | A bash script that leverages ettercap and other tools to obtain credentials. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| easyda | 7.0867f9b | Easy Windows Domain Access Script. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| easyfuzzer | 3.6 | A flexible fuzzer, not only for web, has a CSV output for efficient output analysis (platform independent). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| eazy | 0.1 | This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ecfs | 305.1758063 | Extended core file snapshot format. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| edb | 3230.39925b68 | A cross platform AArch32/x86/x86 debugger. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| eggshell | 157.eaeeea7 | iOS/macOS/Linux Remote Administration Tool. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| eigrp-tools | 0.1 | This is a custom EIGRP packet generator and sniffer developed to test the security and overall operation quality of this brilliant Cisco routing protocol. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| eindeutig | 20050628\_1 | Examine the contents of Outlook Express DBX email repository files (forensic purposes) | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| electric-fence | 2.2.5 | A malloc(3) debugger that uses virtual memory hardware to detect illegal memory accesses. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| elettra | 1.0 | Encryption utility by Julia Identity | [blackarch-misc](http://docs.google.com/misc.html) |  |
| elettra-gui | 1.0 | Gui for the elettra crypto application. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| elfkickers | 3.1.a | Collection of ELF utilities (includes sstrip) | [blackarch-binary](http://docs.google.com/binary.html) |  |
| elfparser | 7.39d21ca | Cross Platform ELF analysis. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| elfutils | 0.183 | Handle ELF object files and DWARF debugging information (utilities) | [blackarch-binary](http://docs.google.com/binary.html) |  |
| elidecode | 48.38fa5ba | A tool to decode obfuscated shellcodes using the unicorn-engine for the emulation and the capstone-engine to print the asm code. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| elite-proxy-finder | 51.1ced3be | Finds public elite anonymity proxies and concurrently tests them. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| email2phonenumber | 19.d097c07 | A OSINT tool to obtain a target's phone number just by having his email address. | [blackarch-social](http://docs.google.com/social.html) |  |
| emldump | 0.0.10 | Analyze MIME files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| empire | 2289.9259e510 | A PowerShell and Python post-exploitation agent. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| enabler | 1 | Attempts to find the enable password on a cisco system via brute force. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| encodeshellcode | 0.1b | This is an encoding tool for 32-bit x86 shellcode that assists a researcher when dealing with character filter or byte restrictions in a buffer overflow vulnerability or some kind of IDS/IPS/AV blocking your code. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ent | 1.0 | Pseudorandom number sequence test. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| enteletaor | 66.e8e4daa | Message Queue & Broker Injection tool that implements attacks to Redis, RabbitMQ and ZeroMQ. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| entropy | 702.13aac50 | A set of tools to exploit Netwave and GoAhead IP Webcams. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| enum-shares | 7.97cba5a | Tool that enumerates shared folders across the network and under a custom user account. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| enum4linux | 0.8.9 | A tool for enumerating information from Windows and Samba systems. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| enum4linux-ng | 264.d37b7ef | A next generation version of enum4linux. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| enumerate-iam | 14.4529114 | Enumerate the permissions associated with an AWS credential set. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| enumerid | 27.c106f05 | Enumerate RIDs using pure Python. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| enumiax | 1.0 | An IAX enumerator. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| enyelkm | 1.2 | Rootkit for Linux x86 kernels v2.6. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| eos | 10.7f0cc9f | Enemies Of Symfony - Debug mode Symfony looter. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| epicwebhoneypot | 2.0a | Tool which aims to lure attackers using various types of web vulnerability scanners by tricking them into believing that they have found a vulnerability on a host. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| erase-registrations | 1.0 | An IAX flooder. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| eraser | 6.2.0.2986 | Windows tool which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| eresi | 1291.4769c175 | The ERESI Reverse Engineering Software Interface. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| erl-matter | 43.7958385 | Tool to exploit epmd related services such ass rabbitmp, ejabberd and couchdb by bruteforcing the cookie and gaining RCE afterwards. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| espionage | 39.790e519 | A Network Packet and Traffic Interceptor For Linux. Sniff All Data Sent Through a Network. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| eternal-scanner | 90.510be17 | An internet scanner for exploit CVE-0144 (Eternal Blue). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| etherape | 0.9.19 | Graphical network monitor for various OSI layers and protocols | [blackarch-networking](http://docs.google.com/networking.html) |  |
| etherchange | 1.1 | Can change the Ethernet address of the network adapters in Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| etherflood | 1.1 | Floods a switched network with Ethernet frames with random hardware addresses. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ettercap | 0.8.3.1 | Network sniffer/interceptor/logger for ethernet LANs - console | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| evil-ssdp | 94.ee76fb0 | Spoof SSDP replies to phish for NetNTLM challenge/response on a network. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| evil-winrm | 267.3c318f1 | The ultimate WinRM shell for hacking/pentesting. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| evilclippy | 62.fa610c6 | A cross-platform assistant for creating malicious MS Office documents. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| evilginx | 2.4.0 | Man-in-the-middle attack framework used for phishing login credentials | [blackarch-social](http://docs.google.com/social.html) |  |
| evilgrade | 2.0.9 | Modular framework that takes advantage of poor upgrade implementations by injecting fake updates. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| evilize | 0.2 | Tool to create MD5 colliding binaries. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| evillimiter | 36.46d2033 | Tool that limits bandwidth of devices on the same network without access. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| evilmaid | 1.01 | TrueCrypt loader backdoor to sniff volume password | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| evilpdf | 5.43696a8 | Embedding executable files in PDF Documents. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| evine | 38.1643204 | Interactive CLI Web Crawler. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| evtkit | 8.af06db3 | Fix acquired .evt - Windows Event Log files (Forensics). | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| exabgp | 4699.0fcaf2ca | The BGP swiss army knife of networking. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| exe2image | 1.1 | A simple utility to convert EXE files to JPEG images and vice versa. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| exescan | 1.ad993e3 | A tool to detect anomalies in PE (Portable Executable) files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| exitmap | 369.172e763 | A fast and modular scanner for Tor exit relays. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| expimp-lookup | 4.79a96c7 | Looks for all export and import names that contain a specified string in all Portable Executable in a directory tree. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| exploit-db | 1.6 | The Exploit Database (EDB) – an ultimate archive of exploits and vulnerable software - A collection of hacks | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| exploitdb | 20210316 | Offensive Security’s Exploit Database Archive | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| exploitpack | 139.e565c47 | Exploit Pack - The next generation exploit framework. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| expose | 1110.30264af | A Dynamic Symbolic Execution (DSE) engine for JavaScript | [blackarch-binary](http://docs.google.com/binary.html) |  |
| exrex | 142.fd1e21f | Irregular methods on regular expressions. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| extended-ssrf-search | 28.680f815 | Smart ssrf scanner using different methods like parameter brute forcing in post and get. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| extracthosts | 17.8fdff9e | Extracts hosts (IP/Hostnames) from files. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| extractusnjrnl | 7.362d4290 | Tool to extract the $UsnJrnl from an NTFS volume. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| eyeballer | 127.c50eae4 | Convolutional neural network for analyzing pentest screenshots. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| eyepwn | 1.0 | Exploit for Eye-Fi Helper directory traversal vulnerability | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| eyewitness | 900.b4866e6 | Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| f-scrack | 19.9a00357 | A single file bruteforcer supports multi-protocol. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| facebash | 17.95c3c25 | Facebook Brute Forcer in shellscript using TOR. | [blackarch-social](http://docs.google.com/social.html) |  |
| facebookosint | 21.656a04a | OSINT tool to replace facebook graph search. | [blackarch-social](http://docs.google.com/social.html) |  |
| facebot | 23.57f6025 | A facebook profile and reconnaissance system. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| facebrok | 33.0f6fe8d | Social Engineering Tool Oriented to facebook. | [blackarch-social](http://docs.google.com/social.html) |  |
| facebrute | 7.ece355b | This script tries to guess passwords for a given facebook account using a list of passwords (dictionary). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| factordb-pycli | 1.3.0 | CLI for factordb and Python API Client. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| fakeap | 0.3.2 | Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| fakedns | 118.39609da | A regular-expression based python MITM DNS server with correct DNS request passthrough and "Not Found" responses. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| fakemail | 1.0 | Fake mail server that captures e-mails as files for acceptance testing. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| fakenet-ng | 299.596bb13 | Next Generation Dynamic Network Analysis Tool. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| fakenetbios | 7.b83701e | A family of tools designed to simulate Windows hosts (NetBIOS) on a LAN. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| fang | 22.4f94552 | A multi service threaded MD5 cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| faradaysec | 10226.58906c92d | Collaborative Penetration Test and Vulnerability Management Platform. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fastnetmon | v1.1.4.r62.g780aff3 | High performance DoS/DDoS load analyzer built on top of multiple packet capture engines. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| favfreak | 25.b85ebde | Weaponizing favicon.ico for BugBounties , OSINT and what not. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| fbht | 70.d75ae93 | A Facebook Hacking Tool | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| fbi | 28.0f94e99 | An accurate facebook account information gathering. | [blackarch-social](http://docs.google.com/social.html) |  |
| fbid | 16.1b35eb9 | Show info about the author by facebook photo url. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| fcrackzip | 1.0 | Zip file password cracker | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| fdsploit | 26.4522f53 | A File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| featherduster | 185.76954f2 | An automated, modular cryptanalysis tool. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| fern-wifi-cracker | 289.0da03ab | WEP, WPA wifi cracker for wireless penetration testing | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| fernflower | 485.e19aab6 | An analytical decompiler for Java. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| fernmelder | 6.c6d4ebe | Asynchronous mass DNS scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| feroxbuster | v2.2.3.r14.gef195bd | A fast, simple, recursive content discovery tool written in Rust. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ffuf | 174.8a9a075 | Fast web fuzzer written in Go. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ffuf-scripts | 1.2192bf7 | Scripts and snippets for ffuf payloads. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| fgscanner | 11.893372c | An advanced, opensource URL scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fhttp | 1.3 | This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| fi6s | 170.5073aee | IPv6 network scanner designed to be fast. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fierce | 126.2ef6794 | A DNS reconnaissance tool for locating non-contiguous IP space. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| fiked | 0.0.5 | Fake IDE daemon | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| filebuster | 73.2d1749f | An extremely fast and flexible web fuzzer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| filefuzz | 1.0 | A binary file fuzzer for Windows with several options. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| filegps | 90.03cbc75 | A tool that help you to guess how your shell was renamed after the server-side script of the file uploader saved it. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| fileintel | 33.a0bff38 | A modular Python application to pull intelligence about malicious files. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| filibuster | 167.c54ac80 | A Egress filter mapping application with additional functionality. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| fimap | 1.00 | A little tool for local and remote file inclusion auditing and exploitation | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| finalrecon | 58.55e7c60 | OSINT Tool for All-In-One Web Reconnaissance. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| find-dns | 0.1 | A tool that scans networks looking for DNS servers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| findmyhash | 1.1.2 | Crack different types of hashes using free online services. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| findmyiphone | 19.aef3ac8 | Locates all devices associated with an iCloud account | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| findomain | 4.0.1 | The fastest and cross-platform subdomain enumerator, do not waste your time | [blackarch-recon](http://docs.google.com/recon.html) |  |
| findsploit | 84.1107a48 | Find exploits in local and online databases instantly. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| fingerprinter | 464.6be23a8 | CMS/LMS/Library etc Versions Fingerprinter. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| firecat | 6.b5205c8 | A penetration testing tool that allows you to punch reverse TCP tunnels out of a compromised network. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| firefox-security-toolkit | 16.31dacf0 | A tool that transforms Firefox browsers into a penetration testing suite. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| firewalk | 5.0 | An active reconnaissance network security tool | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| firmwalker | 101.23ff299 | Script for searching the extracted firmware file system for goodies. | [blackarch-firmware](http://docs.google.com/firmware.html) |  |
| firmware-mod-kit | 145.104c821 | Modify firmware images without recompiling. | [blackarch-firmware](http://docs.google.com/firmware.html) |  |
| firstexecution | 6.a275793 | A Collection of different ways to execute code outside of the expected entry points. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| firstorder | 8.107eb6a | A traffic analyzer to evade Empire communication from Anomaly-Based IDS. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| fl0p | 0.1 | A passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| flamerobin | 2370.c75f8618 | A tool to handle Firebird database management. | [blackarch-database](http://docs.google.com/database.html) |  |
| flare | 0.6 | Flare processes an SWF and extracts all scripts from it. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| flare-floss | 1.7.0 | Obfuscated String Solver - Automatically extract obfuscated strings from malware. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| flashlight | 109.90d1dc5 | Automated Information Gathering Tool for Penetration Testers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| flashscanner | 11.6815b02 | Flash XSS Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| flashsploit | 23.c465a6d | Exploitation Framework for ATtiny85 Based HID Attacks. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| flask-session-cookie-manager2 | v1.2.1.1.r6.g86197c4 | Decode and encode Flask session cookie. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| flask-session-cookie-manager3 | v1.2.1.1.r6.g86197c4 | Decode and encode Flask session cookie. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| flasm | 1.62 | Disassembler tool for SWF bytecode | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| flawfinder | 2.0.11 | Searches through source code for potential security flaws | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| flowinspect | 97.34759ed | A network traffic inspection tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| flunym0us | 2.0 | A Vulnerability Scanner for Wordpress and Moodle. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fluxion | 1538.48c3953 | A security auditing and social-engineering research tool. | [blackarch-social](http://docs.google.com/social.html) |  |
| flyr | 76.4926ecc | Block-based software vulnerability fuzzing framework. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fockcache | 10.3e7efa9 | Tool to make cache poisoning by trying X-Forwarded-Host and X-Forwarded-Scheme headers on web pages. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| forager | 115.7439b0a | Multithreaded threat Intelligence gathering utilizing. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| foremost | 1.5.7 | A console program to recover files based on their headers, footers, and internal data structures | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| foresight | 57.6f48984 | A tool for predicting the output of random number generators. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| forkingportscanner | 1 | Simple and fast forking port scanner written in perl. Can only scan on host at a time, the forking is done on the specified port range. Or on the default range of 1. Has the ability to scan UDP or TCP, defaults to tcp. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| formatstringexploiter | 29.8d64a56 | Helper script for working with format string bugs. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| fpdns | 108.2a898bf | Program that remotely determines DNS server versions. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| fping | 5.0 | Utility to ping multiple hosts at once | [blackarch-networking](http://docs.google.com/networking.html) |  |
| fport | 2.0 | Identify unknown open ports and their associated applications. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| fprotlogparser | 1 | This is a utility to parse a F-Prot Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your collection. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| fraud-bridge | 10.775c563 | ICMP and DNS tunneling via IPv4 and IPv6. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| fred | 0.1.1 | Cross-platform M$ registry hive editor. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| freeipmi | 1.6.7 | Sensor monitoring, system event monitoring, power control, and serial-over-LAN (SOL). | [blackarch-networking](http://docs.google.com/networking.html) |  |
| freeradius | 3.0.21 | The premier open source RADIUS server | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| freewifi | 30.1cb752b | How to get free wifi. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| frida | 12.6.8 | Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| frida-extract | 13.abb3f14 | Frida.re based RunPE (and MapViewOfSection) extraction tool. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| frida-ios-dump | 53.56e99b2 | Pull decrypted ipa from jailbreak device. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| frida-push | 1.0.8 | Wrapper tool to identify the remote device and push device specific frida-server binary | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| fridump | 23.3e64ee0 | A universal memory dumper using Frida. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| frisbeelite | 1.2 | A GUI-based USB device fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fs-exploit | 3.28bb9bb | Format string exploit generation. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| fs-nyarl | 1.0 | A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fsnoop | 3.4 | A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods"). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fssb | 73.51d2ac2 | A low-level filesystem sandbox for Linux using syscall intercepts. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| fstealer | 0.1 | Automates file system mirroring through remote file disclosure vulnerabilities on Linux machines. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| ftester | 1.0 | A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| ftp-fuzz | 1337 | The master of all master fuzzing scripts specifically targeted towards FTP server software. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| ftp-scanner | 0.2.5 | Multithreaded ftp scanner/brute forcer. Tested on Linux, OpenBSD and Solaris. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ftp-spider | 1.0 | FTP investigation tool - Scans ftp server for the following: reveal entire directory tree structures, detect anonymous access, detect directories with write permissions, find user specified data within repository. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ftpmap | 52.cbeabbe | Scans remote FTP servers to identify what software and what versions they are running. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| ftpscout | 12.cf1dff1 | Scans ftps for anonymous access. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| fuddly | 569.fd2c4d0 | Fuzzing and Data Manipulation Framework (for GNU/Linux). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fusil | 1.5 | A Python library used to write fuzzing programs. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fuxploider | 140.ec8742b | Tool that automates the process of detecting and exploiting file upload forms flaws. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| fuzzap | 17.057002b | A python script for obfuscating wireless networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| fuzzball2 | 0.7 | A little fuzzer for TCP and IP options. It sends a bunch of more or less bogus packets to the host of your choice. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fuzzbunch | 32.2b76c22 | NSA Exploit framework | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| fuzzdb | 475.5656ab2 | Attack and Discovery Pattern Dictionary for Application Fault Injection Testing. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fuzzdiff | 1.0 | A simple tool designed to help out with crash analysis during fuzz testing. It selectively 'un-fuzzes' portions of a fuzzed file that is known to cause a crash, re-launches the targeted application, and sees if it still crashes. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fuzzowski | 38.e042c62 | A Network Protocol Fuzzer made by NCCGroup based on Sulley and BooFuzz. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| fuzztalk | 1.0.0.0 | An XML driven fuzz testing framework that emphasizes easy extensibility and reusability. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| g72x++ | 1 | Decoder for the g72x++ codec. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| gadgetinspector | 6.ac7832d | A byte code analyzer for finding deserialization gadget chains in Java applications. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| gadgettojscript | 20.005cb8b | .NET serialized gadgets that can trigger .NET assembly from JS/VBS/VBA based scripts. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| galleta | 20040505\_1 | Examine the contents of the IE's cookie files for forensic purposes | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| gasmask | 170.e0d0f0a | All in one Information gathering tool - OSINT. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gatecrasher | 2.3ad5225 | Network auditing and analysis tool developed in Python. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gau | 64.4f1ba3c | Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| gcat | 29.39b266c | A fully featured backdoor that uses Gmail as a C&C server. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| gcpbucketbrute | 16.5fe33df | A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| gcrypt | 13.4d9a9ce | Simple, secure and performance file encryption tool written in C | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| gdb | 10.1 | The GNU Debugger | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| gdb-common | 10.1 | The GNU Debugger | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| gdbgui | 420.e53b7f4 | Browser-based gdb frontend using Flask and JavaScript to visually debug C, C++, Go, or Rust. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| gef | 1946.3b7a97c | Multi-Architecture GDB Enhanced Features for Exploiters & Reverse-Engineers. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| gene | 57.bd12ed4 | Signature Engine for Windows Event Logs. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| genisys | 24.bc2a27a | Powerful Telegram Members Scraping and Adding Toolkit. | [blackarch-social](http://docs.google.com/social.html) |  |
| genlist | 0.1 | Generates lists of IP addresses. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| geoedge | 0.2 | This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| geoip | 1.6.12 | Non-DNS IP-to-country resolver C library & utils | [blackarch-networking](http://docs.google.com/networking.html) |  |
| geoipgen | 0.4 | GeoIPgen is a country to IP addresses generator. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| gerix-wifi-cracker | 1.1c3cd73 | A graphical user interface for aircrack-ng and pyrit. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| gethsploit | 3.144778b | Finding Ethereum nodes which are vulnerable to RPC-attacks. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| getsids | 0.0.1 | Getsids tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener. Like doing ‘lsnrctl service’. | [blackarch-database](http://docs.google.com/database.html) |  |
| getsploit | 33.5993293 | Command line utility for searching and downloading exploits. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| gggooglescan | 0.4 | A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ghettotooth | 1.0 | Ghettodriving for bluetooth | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| ghidra | 9.2.2 | Software reverse engineering framework | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| ghost-phisher | 1.62 | GUI suite for phishing and penetration attacks | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ghost-py | 2.0.0 | Webkit based webclient (relies on PyQT). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ghostdelivery | 32.a23ed5a | Python script to generate obfuscated .vbs script that delivers payload (payload dropper) with persistence and windows antivirus disabling functions. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| gibberish-detector | v0.1.1.r0.gca47133 | Train a model and detect gibberish strings with it. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| girsh | v0.27.r0.g83ef5ca | Automatically spawn a reverse shell fully interactive for Linux or Windows victim. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| giskismet | 20110805 | A program to visually represent the Kismet data in a flexible manner. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| git-dump | 7.4c9a2a9 | Dump the contents of a remote git repository without directory listing enabled. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| git-dumper | 42.1f784ff | A tool to dump a git repository from a website. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| git-hound | 116.f1528c0 | Pinpoints exposed API keys on GitHub. A batch-catching, pattern-matching, patch-attacking secret snatcher. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitdorker | 109.50db967 | Python program to scrape secrets from GitHub through usage of a large repository of dorks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitem | 104.d40a1c9 | A Github organization reconnaissance tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitgraber | 67.72e5850 | Monitor GitHub to search and find sensitive data in real time for different online services. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| githack | 10.1fed62c | A `.git` folder disclosure exploit. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| github-dorks | 63.38ee335 | Collection of github dorks and helper tool to automate the process of checking dorks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| githubcloner | 34.26d03ae | A script that clones Github repositories of users and organizations automatically. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| gitleaks | 633.a2019a4 | Audit Git repos for secrets and keys. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitmails | 71.8aa8411 | An information gathering tool to collect git commit emails in version control host services. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitminer | 54.16ada58 | Tool for advanced mining for content on Github. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitrecon | 30.6467e78 | OSINT tool to get information from a Github and Gitlab profile and find user's email addresses leaked on commits. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gitrob | 7.7be4c53 | Reconnaissance tool for GitHub organizations. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| gittools | 65.24eaef0 | A repository with 3 tools for pwn'ing websites with .git repositories available'. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| gloom | 93.cd6e927 | Linux Penetration Testing Framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| glue | 380.8703380 | A framework for running a series of tools. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| gnuradio | 3.8.2.0 | General purpose DSP and SDR toolkit. With drivers for usrp and fcd. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| gnutls2 | 2.12.23 | A library which provides a secure layer over a reliable transport layer (Version 2) | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| gobd | 82.3bbd17c | A Golang covert backdoor. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| gobuster | 341.f278731 | Directory/file & DNS busting tool written in Go. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| goddi | 1.2 | Dumps Active Directory domain information. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| goldeneye | 28.792862f | A HTTP DoS test tool. Attack Vector exploited: HTTP Keep Alive + NoCache. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| golismero | 73.7d605b9 | Opensource web security testing framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| goodork | 2.2 | A python script designed to allow you to leverage the power of google dorking straight from the comfort of your command line. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| goofile | 1.5 | Command line filetype search | [blackarch-recon](http://docs.google.com/recon.html) |  |
| goog-mail | 1.0 | Enumerate domain emails from google. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| google-explorer | 140.0b21b57 | Google mass exploit robot - Make a google search, and parse the results for a especific exploit you define. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| googlesub | 14.a7a3cc7 | A python script to find domains by using google dorks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| goohak | 30.576ca53 | Automatically Launch Google Hacking Queries Against A Target Domain. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| goop | 12.39b34eb | Perform google searches without being blocked by the CAPTCHA or hitting any rate limits. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gooscan | 1.0.9 | A tool that automates queries against Google search appliances, but with a twist. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| gopherus | 31.9ca94b8 | Tool generates gopher link for exploiting SSRF and gaining RCE in various servers. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| gophish | 766.db63ee9 | Open-Source Phishing Framework. | [blackarch-social](http://docs.google.com/social.html) |  |
| gosint | 196.9c86ed2 | OSINT framework in Go. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| gospider | 86.fe1d58b | Fast web spider written in Go. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| gostringsr2 | 1.1.2 | Extract strings from a Go binary using radare2. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| gowitness | 170.c168591 | A golang, web screenshot utility using Chrome Headless. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| gplist | 1.0 | Lists information about the applied Group Policies. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| gpocrack | 3.cf63c86 | Active Directory Group Policy Preferences cpassword cracker/decrypter. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| gpredict | 1617.aa57710 | A real-time satellite tracking and orbit prediction application. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| gps-sdr-sim | 183.bf998ab | Software-Defined GPS Signal Simulator. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| gqrx | 2.14.4 | Interactive SDR receiver waterfall for many devices. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| gr-air-modes | 396.0b6c383 | Gnuradio tools for receiving Mode S transponder signals, including ADS-B. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| gr-gsm | 1151.2efaa49 | Gnuradio blocks and tools for receiving GSM transmissions. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| gr-paint | 34.0aad1fc | An OFDM Spectrum Painter for GNU Radio. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| grabbb | 0.0.7 | Clean, functional, and fast banner scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| grabber | 0.1 | A web application scanner. Basically it detects some kind of vulnerabilities in your website. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| grabing | 11.9c1aa6c | Counts all the hostnames for an IP adress | [blackarch-recon](http://docs.google.com/recon.html) |  |
| grabitall | 1.1 | Performs traffic redirection by sending spoofed ARP replies. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| graffiti | 24.4af61b4 | A tool to generate obfuscated one liners to aid in penetration testing. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| grammarinator | 146.86d348e | A random test generator / fuzzer that creates test cases according to an input ANTLR v4 grammar. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| graphql-path-enum | 14.aed4346 | Tool that lists the different ways of reaching a given type in a GraphQL schema. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| graphqlmap | 45.b77bf73 | Scripting engine to interact with a graphql endpoint for pentesting purposes. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| graudit | 507.4e4ff33 | Grep rough source code auditing tool. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| greenbone-security-assistant | 9.0.1 | Greenbone Security Assistant (gsa) - OpenVAS web frontend | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| grepforrfi | 0.1 | Simple script for parsing web logs for RFIs and Webshells v1.2 | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| grokevt | 0.5.0 | A collection of scripts built for reading Windows® NT/2K/XP/2K eventlog files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| grr | 17.791ed5a | High-throughput fuzzer and emulator of DECREE binaries. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| grype | 0.5.0 | A vulnerability scanner for container images and filesystems. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| gsd | 1.1 | Gives you the Discretionary Access Control List of any Windows NT service you specify as a command line option. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| gsocket | 396.a3155dc | Global Socket. Moving data from here to there. Securely, Fast and trough NAT/Firewalls. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| gspoof | 3.2 | A simple GTK/command line TCP/IP packet generator. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| gtalk-decode | 0.1 | Google Talk decoder tool that demonstrates recovering passwords from accounts. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| gtfo | 16.2296edf | Search gtfobins and lolbas files from your terminal. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| gtfoblookup | 52.949a9c1 | Offline command line lookup utility for GTFOBins and LOLBAS. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| gtp-scan | 0.7 | A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| guymager | 0.8.12 | A forensic imager for media acquisition. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| gvmd | 8.0.1 | greenbone-vulnerability-manager | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| gwcheck | 0.1 | A simple program that checks if a host in an ethernet network is a gateway to Internet. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| gwtenum | 7.f27a5aa | Enumeration of GWT-RCP method calls. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| h2buster | 79.6c4dd1c | A threaded, recursive, web directory brute-force scanner over HTTP/2. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| h2csmuggler | 7.7ea573a | HTTP Request Smuggling over HTTP/2 Cleartext (h2c). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| h2spec | 2.6.0 | A conformance testing tool for HTTP/2 implementation. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| h2t | 36.9183a30 | Scans a website and suggests security headers to apply. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| h8mail | 330.0a371eb | Email OSINT and password breach hunting. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| habu | 352.cda99c8 | Python Network Hacking Toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hackersh | 0.2.0 | A shell for with Pythonect-like syntax, including wrappers for commonly used security tools. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| hackredis | 3.fbae1bc | A simple tool to scan and exploit redis servers. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| hackrf | 2018.01.1 | Driver for HackRF, allowing general purpose software defined radio (SDR). | [blackarch-radio](http://docs.google.com/radio.html) |  |
| haiti | v1.0.1.r40.g46e197e | A CLI tool to identify the hash type of a given hash. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| haka | 0.2.2 | A collection of tool that allows capturing TCP/IP packets and filtering them based on Lua policy files. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hakku | 384.bbb434d | Simple framework that has been made for penetration testing tools. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hakrawler | 134.bd3d30a | Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| hakrevdns | 37.9fa2d59 | Small, fast tool for performing reverse DNS lookups en masse. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| halberd | 0.2.4 | Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| halcyon | 0.1 | A repository crawler that runs checksums for static files found within a given git repository. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| halcyon-ide | 2.0.2 | First IDE for Nmap Script (NSE) Development. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hamster | 2.0.0 | Tool for HTTP session sidejacking. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| handle | 0.1 | An small application designed to analyze your system searching for global objects related to running process and display information for every found object, like tokens, semaphores, ports, files,.. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| harness | 19.ed2a6aa | Interactive remote PowerShell Payload. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| harpoon | 284.ab607b9 | CLI tool for open source and threat intelligence. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| hasere | 1.0 | Discover the vhosts using google and bing. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| hash-buster | 48.3f1d7c9 | A python script which scraps online hash crackers to find cleartext of a hash. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hash-extender | 149.3c3bcf1 | A hash length extension attack tool. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hash-identifier | 6.0e08a97 | Software to identify the different types of hashes used to encrypt data and especially passwords. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hashcat | 6.1.1 | Multithreaded advanced password recovery utility | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| hashcat-utils | 1.9 | Set of small utilities that are useful in advanced password cracking | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hashcatch | 52.8145660 | Capture handshakes of nearby WiFi networks automatically. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| hashdb | 1089.1da1b9f | A block hash toolkit. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hashdeep | 4.4 | cross-platform tools to message digests for any number of files | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hasher | 48.40173c5 | A tool that allows you to quickly hash plaintext strings, or compare hashed values with a plaintext locally. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| hashfind | 8.e9a9a14 | A tool to search files for matching password hash types and other interesting data. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hashid | 397.7e8473a | Software to identify the different types of hashes used to encrypt data. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hashpump | 49.314268e | A tool to exploit the hash length extension attack in various hashing algorithms. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hashtag | 0.41 | A python script written to parse and identify password hashes. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| hatcloud | 33.3012ad6 | Bypass CloudFlare with Ruby. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| hate-crack | 179.4b1d76a | A tool for automating cracking methodologies through Hashcat. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| haystack | 1823.c178b5a | A Python framework for finding C structures from process memory - heap analysis - Memory structures forensics. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| hbad | 1.0 | This tool allows you to test clients on the heartbleed bug. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hcraft | 1.0.0 | HTTP Vuln Request Crafter | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| hcxdumptool | 6.1.6 | Small tool to capture packets from wlan devices | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| hcxkeys | 6.0.0 | Set of tools to generate plainmasterkeys (rainbowtables) and hashes for hashcat and John the Ripper | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hcxtools | 6.1.6 | Portable solution for capturing wlan traffic and conversion to hashcat and John the Ripper formats | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| hdcp-genkey | 18.e8d342d | Generate HDCP source and sink keys from the leaked master key. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hdmi-sniff | 5.f7fbc0e | HDMI DDC (I2C) inspection tool. It is designed to demonstrate just how easy it is to recover HDCP crypto keys from HDMI devices. | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| heartbleed-honeypot | 0.1 | Script that listens on TCP port 443 and responds with completely bogus SSL heartbeat responses, unless it detects the start of a byte pattern similar to that used in Jared Stafford's | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| heartleech | 116.3ab1d60 | Scans for systems vulnerable to the heartbleed bug, and then download them. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| hellraiser | 221.b4fadd2 | Vulnerability Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hemingway | 8.9c70a13 | A simple and easy to use spear phishing helper. | [blackarch-social](http://docs.google.com/social.html) |  |
| hercules-payload | 220.958541e | A special payload generator that can bypass all antivirus software. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| hetty | 64.98dacbe | HTTP toolkit for security research. It aims to become an open source alternative to commercial software like Burp Suite Pro, with powerful features tailored to the needs of the infosec and bug bounty community. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| hex2bin | 2.5 | Converts Motorola and Intel hex files to binary. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| hexinject | 1.6 | A very versatile packet injector and sniffer that provides a command-line framework for raw network access. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| hexorbase | 6 | A database application designed for administering and auditing multiple database servers simultaneously from a centralized location. It is capable of performing SQL queries and bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| hexyl | 0.8.0 | Colored command-line hex viewer | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hharp | 1beta | This tool can perform man-in-the-middle and switch flooding attacks. It has 4 major functions, 3 of which attempt to man-in-the-middle one or more computers on a network with a passive method or flood type method. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hidattack | 0.1 | HID Attack (attacking HID host implementations) | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| hiddeneye | 1228.7a3deaf | Modern phishing tool with advanced functionality. | [blackarch-social](http://docs.google.com/social.html) |  |
| hikpwn | 7.7fc1465 | A simple scanner for Hikvision devices with basic vulnerability scanning capabilities written in Python 3.8. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hlextend | 5.c9e8ff9 | Pure Python hash length extension module. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| hodor | 1.01be107 | A general-use fuzzer that can be configured to use known-good input and delimiters in order to fuzz specific locations. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| hollows-hunter | 0.2.9 | Scans all running processes. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| homepwn | 30.6bf431e | Swiss Army Knife for Pentesting of IoT Devices. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| honeyd | 337.a0f3d64 | A small daemon that creates virtual hosts on a network. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| honeypy | 599.feccab5 | A low interaction Honeypot. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| honggfuzz | 3872.8eea2e7a | A general-purpose fuzzer with simple, command-line interface. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| honssh | 202.7adbf1b | A high-interaction Honey Pot solution designed to log all SSH communications between a client and server. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| hookanalyser | 3.4 | A hook tool which can be potentially helpful in reversing applications and analyzing malware. It can hook to an API in a process and search for a pattern in memory or dump the buffer. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| hoover | 4.9bda860 | Wireless Probe Requests Sniffer. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| hoper | 12.3951159 | Trace URL's jumps across the rel links to obtain the last URL. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| hopper | 4.5.29 | Reverse engineering tool that lets you disassemble, decompile and debug your applications. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| hoppy | 1.8.1 | A python script which tests http methods for configuration issues leaking information or just to see if they are enabled. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| host-extract | 8.0134ad7 | Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| hostapd-wpe | 2.9.1 | Modified hostapd to facilitate AP impersonation attacks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| hostbox-ssh | 0.1.1 | A ssh password/account scanner. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| hosthunter | 106.0924314 | A recon tool for discovering hostnames using OSINT techniques. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| hotpatch | 90.fd2baf1 | Hot patches executables on Linux using .so file injection. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| hotspotter | 0.4 | Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| howmanypeoplearearound | 123.b05e06a | Count the number of people around you by monitoring wifi signals. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| hpfeeds | 411.539e738 | Honeynet Project generic authenticated datafeed protocol. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| hping | 3.0.0 | A command-line oriented TCP/IP packet assembler/analyzer. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hqlmap | 38.bb6ab46 | A tool to exploit HQL Injections. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| hsecscan | 64.3089ac2 | A security scanner for HTTP response headers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| htcap | 154.e4535f0 | A web application analysis tool for detecting communications between javascript and the server. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| htexploit | 0.77 | A Python script that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| htpwdscan | 18.d334e02 | A python HTTP weak pass scanner. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| htrosbif | 134.9dc3f86 | Active HTTP server fingerprinting and recon tool. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| htshells | 88.eb895ac | Self contained web shells and other attacks via .htaccess files. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| http-enum | 0.4 | A tool to enumerate the enabled HTTP methods supported on a webserver. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| http-fuzz | 0.1 | A simple http fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| http-put | 1.0 | Simple http put perl script. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| http-traceroute | 0.5 | This is a python script that uses the Max-Forwards header in HTTP and SIP to perform a traceroute-like scanning functionality. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| httpbog | 1.0.0.0 | A slow HTTP denial-of-service tool that works similarly to other attacks, but rather than leveraging request headers or POST data Bog consumes sockets by slowly reading responses. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| httpforge | 11.02.01 | A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the security of Web servers, apps, and sites. An accompanying Python library is available for extensions. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| httpgrep | 1.8 | A python tool which scans for HTTP servers and finds given strings in URIs. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| httping | 2.5 | A ping-like tool for http-requests | [blackarch-networking](http://docs.google.com/networking.html) |  |
| httppwnly | 47.528a664 | "Repeater" style XSS post-exploitation tool for mass browser control. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| httprecon | 7.3 | Tool for web server fingerprinting, also known as http fingerprinting. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| httprint | 301 | A web server fingerprinting tool. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| httprint-win32 | 301 | A web server fingerprinting tool (Windows binaries). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| httprobe | 22.5555984 | Take a list of domains and probe for working HTTP and HTTPS servers | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| httpry | 0.1.8 | A specialized packet sniffer designed for displaying and logging HTTP traffic. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| httpscreenshot | 60.510b318 | A tool for grabbing screenshots and HTML of large numbers of websites. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| httpsniff | 0.4 | Tool to sniff HTTP responses from TCP/IP based networks and save contained files locally for later review. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| httpsscanner | 1.2 | A tool to test the strength of a SSL web server. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| httptunnel | 3.3 | Creates a bidirectional virtual data connection tunnelled in HTTP requests | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| httpx | 352.dc89316 | A fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| httrack | 3.49.2 | An easy-to-use offline browser utility | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hubbit-sniffer | 74.460ecf8 | Simple application that listens for WIFI-frames and records the mac-address of the sender and posts them to a REST-api. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| hulk | 25.9670699 | A webserver DoS tool (Http Unbearable Load King) ported to Go with some additional features. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| hungry-interceptor | 391.1aea7f3 | Intercepts data, does something with it, stores it. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| hurl | 20.afca9c5 | Hexadecimal & URL (en/de)coder. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hwk | 0.4 | Collection of packet crafting and wireless network flooding tools | [blackarch-dos](http://docs.google.com/dos.html) |  |
| hxd | 2.4.0.0 | Freeware Hex Editor and Disk Editor. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| hyde | 11.ec09462 | Just another tool in C to do DDoS (with spoofing). | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hydra | 9.2 | Very fast network logon cracker which support many different services | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| hyenae | 0.36\_1 | Flexible platform independent packet generator. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hyperfox | 121.1a8c26f | A security tool for proxying and recording HTTP and HTTPs traffic. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| hyperion-crypter | 2.3.1 | A runtime encrypter for 32-bit and 64-bit portable executables. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| i2pd | 2.37.0 | A full-featured C++ implementation of the I2P router | [blackarch-networking](http://docs.google.com/networking.html) |  |
| iaxflood | 0.1 | IAX flooder. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| iaxscan | 0.02 | A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ibrute | 12.3a6a11e | An AppleID password bruteforce tool. It uses Find My Iphone service API, where bruteforce protection was not implemented. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| icloudbrutter | 15.1f64f19 | Tool for AppleID Bruteforce. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| icmpquery | 1.0 | Send and receive ICMP queries for address mask and current time. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| icmpsh | 12.82caf34 | Simple reverse ICMP shell. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| icmptx | 17.52df90f | IP over ICMP tunnel. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| id-entify | 34.dd064a5 | Search for information related to a domain: Emails - IP addresses - Domains - Information on WEB technology - Type of Firewall - NS and MX records. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| idb | 2.10.3 | A tool to simplify some common tasks for iOS pentesting and research. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| identywaf | 204.c623194 | Blind WAF identification tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| idswakeup | 1.0 | A collection of tools that allows to test network intrusion detection systems. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ifchk | 1.1.2 | A network interface promiscuous mode detection tool. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| ifuzz | 1.0 | A binary file fuzzer with several options. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| iheartxor | 0.01 | A tool for bruteforcing encoded strings within a boundary defined by a regular expression. It will bruteforce the key value range of 0x1 through 0x255. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| iis-shortname-scanner | 5.4ad4937 | An IIS shortname Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| iisbruteforcer | 15 | HTTP authentication cracker. It's a tool that launchs an online dictionary attack to test for weak or simple passwords against protected areas on an IIS Web server. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ike-scan | 1.9 | A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ikecrack | 1.00 | An IKE/IPSec crack tool designed to perform Pre-Shared-Key analysis of RFC compliant aggressive mode authentication | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ikeforce | 30.575af15 | A command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ikeprobe | 0.1 | Determine vulnerabilities in the PSK implementation of the VPN server. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ikeprober | 1.12 | Tool crafting IKE initiator packets and allowing many options to be manually set. Useful to find overflows, error conditions and identifiyng vendors | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| ilo4-toolbox | 33.a08e718 | Toolbox for HPE iLO4 analysis. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ilty | 1.0 | An interception phone system for VoIP network. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| imagegrep | 8.1f14af2 | Grep word in pdf or image based on OCR. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| imagejs | 55.f926663 | Small tool to package javascript into a valid image file. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| imagemounter | 385.5d8ba6f | Command line utility and Python package to ease the (un)mounting of forensic disk images. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| imhex | 1.5.0.r29.gb71a9b7 | A Hex Editor for Reverse Engineers, Programmers and people that value their eye sight when working at 3 AM. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| impacket | 0.9.22 | Collection of classes for working with network protocols | [blackarch-networking](http://docs.google.com/networking.html) |  |
| impulse | 77.6939ea2 | Modern Denial-of-service ToolKit. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| inception | 450.ffe83ee | A FireWire physical memory manipulation and hacking tool exploiting IEEE 1394 SBP DMA. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| indx2csv | 17.129a411e | An advanced parser for INDX records. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| indxcarver | 5.dee36608 | Carve INDX records from a chunk of data. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| indxparse | 170.ca08236 | A Tool suite for inspecting NTFS artifacts. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| inetsim | 1.3.2 | A software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| infip | 0.1 | A python script that checks output from netstat against RBLs from Spamhaus. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| infoga | 26.963663b | Tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| inguma | 0.1.1 | A free penetration testing and vulnerability discovery toolkit entirely written in python. Framework includes modules to discover hosts, gather information about, fuzz targets, brute force usernames and passwords, exploits, and a disassembler. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| injectus | 11.f63590c | CRLF and open redirect fuzzer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| innounp | 0.49 | Inno Setup Unpacker. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| inquisitor | 28.12a9ec1 | OSINT Gathering Tool for Companies and Organizations. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| insanity | 117.cf51ff3 | Generate Payloads and Control Remote Machines . | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| instagramosint | 20.94213fd | An Instagram Open Source Intelligence Tool. | [blackarch-social](http://docs.google.com/social.html) |  |
| instashell | 56.49b6b4f | Multi-threaded Instagram Brute Forcer without password limit. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| intelplot | 12.4dd9fc0 | OSINT Tool to Mark Points on Offline Map. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| intensio-obfuscator | 280.f66a22b | Obfuscate a python code 2 and 3. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| intercepter-ng | 1.0 | A next generation sniffer including a lot of features: capturing passwords/hashes, sniffing chat messages, performing man-in-the-middle attacks, etc. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| interlace | 324.068a991 | Easily turn single threaded command line applications into a fast, multi-threaded application with CIDR and glob support. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| interrogate | 5.eb5f071 | A proof-of-concept tool for identification of cryptographic keys in binary material (regardless of target operating system), first and foremost for memory dump analysis and forensic usage. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| intersect | 2.5 | Post-exploitation framework | [blackarch-automation](http://docs.google.com/automation.html) |  |
| intrace | 1.5 | Traceroute-like application piggybacking on existing TCP connections | [blackarch-recon](http://docs.google.com/recon.html) |  |
| inundator | 0.5 | An ids evasion tool, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real attack. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| inurlbr | 34.dbf9773 | Advanced search in the search engines - Inurl scanner, dorker, exploiter. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| inviteflood | 2.0 | Flood a device with INVITE requests | [blackarch-dos](http://docs.google.com/dos.html) |  |
| invoke-cradlecrafter | 19.3ff8bac | PowerShell Remote Download Cradle Generator & Obfuscator. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| invoke-dosfuscation | 7.6260f5b | Cmd.exe Command Obfuscation Generator & Detection Test Harness. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| invoke-obfuscation | 45.f20e7f8 | PowerShell Obfuscator. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| inzider | 1.2 | This is a tool that lists processes in your Windows system and the ports each one listen on. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| iodine | 0.7.0 | Tunnel IPv4 data through a DNS server | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| iosforensic | 1.0 | iOS forensic tool https://www.owasp.org/index.php/Projects/OWASP\_iOSForensic | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ip-https-tools | 7.170691f | Tools for the IP over HTTPS (IP-HTTPS) Tunneling Protocol. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| ip-tracer | 88.28c5c49 | Track and retrieve any ip address information. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ip2clue | 0.0.95 | A small memory/CPU footprint daemon to lookup country (and other info) based on IP (v4 and v6). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ipaudit | 1.1 | Monitors network activity on a network. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ipba2 | 95.c03bd85 | IOS Backup Analyzer. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ipcountry | 1.2 | Fetches IPv4 ranges of given country in host and cidr format. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ipdecap | 96.45d2a7d | Can decapsulate traffic encapsulated within GRE, IPIP, 6in4, ESP (ipsec) protocols, and can also remove IEEE 802.1Q (virtual lan) header. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| iphoneanalyzer | 2.1.0 | Allows you to forensically examine or recover date from in iOS device. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ipmipwn | 6.74a08a8 | IPMI cipher 0 attack tool. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ipmitool | 1.8.18 | Command-line interface to IPMI-enabled devices | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ipobfuscator | 26.0a7f802 | A simple tool to convert the IP to a DWORD IP. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ipscan | 3.7.4 | A very fast IP address and port scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| iptodomain | 18.f1afcd7 | This tool extract domains from IP address based in the information saved in virustotal. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| iptv | 136.de37822 | Search and brute force illegal iptv server. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| iputils | 20200821 | Network monitoring tools, including ping | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ipv4bypass | 21.99bb285 | Using IPv6 to Bypass Security. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ipv666 | 182.ad45ae8 | Golang IPv6 address enumeration. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ipv6toolkit | 805.babee5e | SI6 Networks' IPv6 Toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ircsnapshot | 94.cb02a85 | Tool to gather information from IRC servers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| irpas | 0.10 | Internetwork Routing Protocol Attack Suite. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| isf | 68.5228865 | An exploitation framework based on Python. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| isip | 2.fad1f10 | Interactive sip toolkit for packet manipulations, sniffing, man in the middle attacks, fuzzing, simulating of dos attacks. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| isme | 0.12 | Scans a VOIP environment, adapts to enterprise VOIP, and exploits the possibilities of being connected directly to an IP Phone VLAN. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| isr-form | 1.0 | Simple html parsing tool that extracts all form related information and generates reports of the data. Allows for quick analyzing of data. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| issniff | 294.79c6c2a | Internet Session Sniffer. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| ivre | 0.9.16.dev163 | Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ivre-docs | 0.9.16.dev163 | Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (documentation) | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ivre-web | 0.9.16.dev163 | Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (web application) | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ja3 | 117.cb29184 | Standard for creating SSL client fingerprints in an easy to produce and shareable way. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| jaadas | 0.1 | Joint Advanced Defect assEsment for android applications. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| jackdaw | 340.3876298 | Collect all information in your domain, show you graphs on how domain objects interact with each-other and how to exploit these interactions | [blackarch-recon](http://docs.google.com/recon.html) |  |
| jad | 1.5.8e | Java decompiler | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jadx | 1.2.0 | Command line and GUI tools to produce Java source code from Android Dex and APK files | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| jaeles | 214.e1c3839 | The Swiss Army knife for automated Web Application Testing. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jaidam | 18.15e0fec | Penetration testing tool that would take as input a list of domain names, scan them, determine if wordpress or joomla platform was used and finally check them automatically, for web vulnerabilities using two well-known open source tools, WPScan and Joomscan. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jast | 17.361ecde | Just Another Screenshot Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| javasnoop | 1.1 | A tool that lets you intercept methods, alter data and otherwise hack Java applications running on your computer | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jboss-autopwn | 1.3bc2d29 | A JBoss script for obtaining remote shell access. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| jbrofuzz | 2.5 | Web application protocol fuzzer that emerged from the needs of penetration testing. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| jbrute | 0.99 | Open Source Security tool to audit hashed passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jcrack | 0.3.6 | A utility to create dictionary files that will crack the default passwords of select wireless gateways | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| jd-cli | 1.1.0 | Command line Java Decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| jd-gui | 1.6.6 | A standalone graphical utility that displays Java source codes of .class files. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| jdeserialize | 31.20635ba | A library that interprets Java serialized objects. It also comes with a command-line tool that can generate compilable class declarations, extract block data, and print textual representations of instance values. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jeangrey | 29.46aa996 | A tool to perform differential fault analysis attacks (DFA). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jeb-android | 3.7.0.201909272058 | Android decompiler. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jeb-arm | 3.7.0.201909272058 | Arm decompiler. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jeb-intel | 3.7.0.201909272058 | Intel decompiler. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jeb-mips | 3.7.0.201909272058 | Mips decompiler. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jeb-webasm | 3.7.0.201909272058 | WebAssembly decompiler. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jeopardize | 5.34f1d07 | A low(zero) cost threat intelligence & response tool against phishing domains. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| jexboss | 86.338b531 | Jboss verify and Exploitation Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jhead | 3.04 | EXIF JPEG info parser and thumbnail remover | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| jnetmap | 0.5.4 | A network monitor of sorts. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| john | 1.9.0.jumbo1 | John the Ripper password cracker | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| johnny | 20120424 | GUI for John the Ripper. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jok3r | 447.0761996 | Network and Web Pentest Framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jomplug | 0.1 | This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jondo | 00.20.001 | Redirects internet traffic trough a mix of proxy servers to hide the origin of the requests. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| jooforce | 11.43c21ad | A Joomla password brute force tester. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| joomlascan | 1.2 | Joomla scanner scans for known vulnerable remote file inclusion paths and files. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| joomlavs | 254.eea7500 | A black box, Ruby powered, Joomla vulnerability scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| joomscan | 71.4192949 | Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jpegdump | 0.0.7 | Tool to analyzse JPEG images Reads binary files and parses the JPEG markers inside them. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| jpexs-decompiler | 12.0.1 | JPEXS Free Flash Decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| jsearch | 34.15a5285 | Simple script that grep infos from javascript files. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| jsfuck | 222.94c3835 | Write any JavaScript with 6 Characters: []()!+. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| jshell | 7.ee3c92d | Get a JavaScript shell with XSS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jsonbee | 24.1a518dd | A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jsparser | 31.ccd3ab6 | Parse javascript using Tornado and JSBeautifier to discover interesting enpoints. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jsql-injection | 0.84 | A Java application for automatic SQL database injection. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| jstillery | 65.512e9af | Advanced JavaScript Deobfuscation via Partial Evaluation. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| juicy-potato | 53.744d321 | A sugared version of RottenPotatoNG, with a bit of juice. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| junkie | 1365.70a83d6 | A modular packet sniffer and analyzer. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| justdecompile | 22018 | The decompilation engine of JustDecompile. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| jwscan | 7.874b3a5 | Scanner for Jar to EXE wrapper like Launch4j, Exe4j, JSmooth, Jar2Exe. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| jwt-cracker | 23.8130879 | JWT brute force cracker written in C. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jwt-tool | 54.0565d56 | Toolkit for validating, forging and cracking JWTs (JSON Web Tokens). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jwtcat | 63.64dde89 | Script performs offline brute-force attacks against JSON Web Token (JWT) | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| jynx2 | 2.0 | An expansion of the original Jynx LD\_PRELOAD rootkit | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| k55 | 86.b3c4aa9 | Linux x86\_64 Process Injection Utility. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| kacak | 1.0 | Tools for penetration testers that can enumerate which users logged on windows system. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| kadimus | 113.b036a7f | LFI Scan & Exploit Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| kalibrate-rtl | 65.66074b8 | Fork of http://thre.at/kalibrate/ for use with rtl-sdr devices. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| kamerka | 40.be17620 | Build interactive map of cameras from Shodan. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| katana | 1.0.0.1 | A framework that seekss to unite general auditing tools, which are general pentesting tools (Network,Web,Desktop and others). | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| katsnoop | 0.1 | Utility that sniffs HTTP Basic Authentication information and prints the base64 decoded form. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| kautilya | 52.1c9d5b0 | Pwnage with Human Interface Devices using Teensy++2.0 and Teensy 3.0 devices. | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| kcptun | 20210103 | A Secure Tunnel Based On KCP with N:M Multiplexing | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| keimpx | 298.8521412 | Tool to verify the usefulness of credentials across a network over SMB. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| kekeo | 2.2.0\_20200718 | A little toolbox to play with Microsoft Kerberos in C. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| kerbcrack | 1.3d3 | Kerberos sniffer and cracker for Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| kerbrute | 90.9cfb81e | A tool to perform Kerberos pre-auth bruteforcing. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| kernelpop | 238.b3467d3 | Kernel privilege escalation enumeration and exploitation framework. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| keye | 29.d44a578 | Recon tool detecting changes of websites based on content-length differences. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| khc | 0.2 | A small tool designed to recover hashed known\_hosts fiels back to their plain-text equivalents. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| kickthemout | 212.861aea2 | Kick devices off your network by performing an ARP Spoof attack. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| killcast | 30.ee81cfa | Manipulate Chromecast Devices in your Network. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| killerbee | 313.9bfe694 | Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| kimi | 28.e7cafda | Script to generate malicious debian packages (debain trojans). | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| kippo | 285.0d03635 | A medium interaction SSH honeypot designed to log brute force attacks and most importantly, the entire shell interaction by the attacker. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| kismet | 2020\_12\_R3 | 802.11 layer2 wireless network detector, sniffer, and intrusion detection system | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| kismet-earth | 0.1 | Various scripts to convert kismet logs to kml file to be used in Google Earth. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| kismet2earth | 1.0 | A set of utilities that convert from Kismet logs to Google Earth .kml format | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| kismon | 1.0.2 | GUI client for kismet (wireless scanner/sniffer/monitor). | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| kiterunner | 11.e7a7fa6 | Contextual Content Discovery Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| kitty-framework | 352.cb07609 | Fuzzing framework written in python. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| klar | 2.4.0 | Integration of Clair and Docker Registry. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| klee | 2.1 | A symbolic virtual machine built on top of the LLVM compiler infrastructure. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| klogger | 1.0 | A keystroke logger for the NT-series of Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| knock | 281.14dc079 | Subdomain scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| knxmap | 243.2d6f622 | KNXnet/IP scanning and auditing tool for KNX home automation installations. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| koadic | 635.ba83d9c | A Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| kolkata | 3.0 | A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| konan | 23.7b5ac80 | Advanced Web Application Dir Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| kraken | 32.368a837 | A project to encrypt A5/1 GSM signaling using a Time/Memory Tradeoff Attack. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| krbrelayx | 21.d6a2738 | Kerberos unconstrained delegation abuse toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| kube-hunter | 666.99678f3 | Hunt for security weaknesses in Kubernetes clusters. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| kubolt | 22.0be200d | Utility for scanning public kubernetes clusters. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| kwetza | 26.0e50272 | Python script to inject existing Android applications with a Meterpreter payload. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| l0l | 322.1319ea7 | The Exploit Development Kit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| laf | 12.7a456b3 | Login Area Finder: scans host/s for login panels. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lanmap2 | 127.1197999 | Passive network mapping tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| lans | 148.9f8ef2d | A Multithreaded asynchronous packet parsing/injecting arp spoofer. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| latd | 1.31 | A LAT terminal daemon for Linux and BSD. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| laudanum | 1.0 | A collection of injectable files, designed to be used in a pentest when SQL injection flaws are found and are in multiple languages for different environments. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| lazagne | 784.ab1e140 | An open source application used to retrieve lots of passwords stored on a local computer. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| lazydroid | 25.0f559ec | Tool written as a bash script to facilitate some aspects of an Android Assessment | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| lbd | 20130719 | Load Balancing detector, | [blackarch-recon](http://docs.google.com/recon.html) |  |
| lbmap | 147.2d15ace | Proof of concept scripts for advanced web application fingerprinting, presented at OWASP AppSecAsia 2012. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| ld-shatner | 4.5c215c4 | ld-linux code injector. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| ldap-brute | 21.acc06e3 | A semi fast tool to bruteforce values of LDAP injections over HTTP. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ldapdomaindump | 0.9.3 | Active Directory information dumper via LDAP. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ldapenum | 0.1 | Enumerate domain controllers using LDAP. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ldapscripts | 2.0.8 | Simple shell scripts to handle POSIX entries in an LDAP directory. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| ldeep | 103.74dcf81 | In-depth ldap enumeration utility. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| leaklooker | 5.0d2b9fc | Find open databases with Shodan. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| leena | 2.5119f56 | Symbolic execution engine for JavaScript | [blackarch-binary](http://docs.google.com/binary.html) |  |
| legion | 55.df23a34 | Automatic Enumeration Tool based in Open Source tools. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| leo | 23486.e46e9315f | Literate programmer's editor, outliner, and project manager. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| leroy-jenkins | 3.bdc3965 | A python tool that will allow remote execution of commands on a Jenkins server and its nodes. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| lethalhta | 1.a8d772a | Lateral Movement technique using DCOM and HTA. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| letmefuckit-scanner | 3.f3be22b | Scanner and Exploit Magento. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| leviathan | 35.a1a1d8c | A mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| levye | 84.5406303 | A brute force tool which is support sshkey, vnckey, rdp, openvpn. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| lfi-autopwn | 3.0 | A Perl script to try to gain code execution on a remote server via LFI | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| lfi-exploiter | 1.1 | This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability.. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfi-fuzzploit | 1.1 | A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfi-image-helper | 0.8 | A simple script to infect images with PHP Backdoors for local file inclusion attacks. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfi-scanner | 4.0 | This is a simple perl script that enumerates local file inclusion attempts when given a specific target. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lfi-sploiter | 1.0 | This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfifreak | 21.0c6adef | A unique automated LFi Exploiter with Bind/Reverse Shells. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfimap | 7.99877ec | This script is used to take the highest beneficts of the local file include vulnerability in a webserver. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lfisuite | 85.470e01f | Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lfle | 24.f28592c | Recover event log entries from an image by heurisitically looking for record structures. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| lft | 3.91 | A layer four traceroute implementing numerous other features. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| lhf | 40.51568ee | A modular recon tool for pentesting. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| libbde | 294.b5695e0 | A library to access the BitLocker Drive Encryption (BDE) format. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| libc-database | 45.69815cd | Database of libc offsets to simplify exploitation. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| libdisasm | 0.23 | A disassembler library. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| libfvde | 151.8b8b55a | Library and tools to access FileVault Drive Encryption (FVDE) encrypted volumes. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| libosmocore | 3247.3a6bedf1 | Collection of common code used in various sub-projects inside the Osmocom family of projects. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| libparistraceroute | 378.6fb8f48 | A library written in C dedicated to active network measurements with examples, such as paris-ping and paris-traceroute. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| libpst | 0.6.75 | Outlook .pst file converter | [blackarch-misc](http://docs.google.com/misc.html) |  |
| libtins | 1268.e90e377 | High-level, multiplatform C++ network packet sniffing and crafting library. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| lief | 0.11.3 | Library to Instrument Executable Formats. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| liffy | 27.f9948aa | A Local File Inclusion Exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lightbulb | 88.9e8d6f3 | Python framework for auditing web applications firewalls. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| limeaide | 305.ce3c9b7 | Remotely dump RAM of a Linux client and create a volatility profile for later analysis on your local host. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| limelighter | 16.c808c3c | A tool for generating fake code signing certificates or signing real ones. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| linenum | 75.c47f9b2 | Scripted Local Linux Enumeration & Privilege Escalation Checks | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| linikatz | 27.bfa0d50 | Tool to attack AD on UNIX. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| linkedin2username | 108.4b52b0c | OSINT Tool: Generate username lists for companies on LinkedIn. | [blackarch-social](http://docs.google.com/social.html) |  |
| linkfinder | 162.095bb62 | Discovers endpoint and their parameters in JavaScript files. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| linset | 9.8746b1f | Evil Twin Attack Bash script - An automated WPA/WPA2 hacker. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| linux-exploit-suggester | 32.9db2f5a | A Perl script that tries to suggest exploits based OS version number. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| linux-exploit-suggester.sh | 159.a1b33c8 | Linux privilege escalation auditing tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| linux-inject | 100.268d4e4 | Tool for injecting a shared object into a Linux process. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| linux-smart-enumeration | 160.c721f31 | Linux enumeration tool for pentesting and CTFs with verbosity levels. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lisa.py | 42.dc4e241 | An Exploit Dev Swiss Army Knife. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| list-urls | 0.1 | Extracts links from webpage. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| littleblackbox | 0.1.3 | Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| littlebrother | 112.338cf82 | OSINT tool to get informations on French, Belgian and Swizerland people. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| lldb | 11.1.0 | Next generation, high-performance debugger | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| loadlibrary | 101.19c7819 | Porting Windows Dynamic Link Libraries to Linux. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| locasploit | 117.fa48151 | Local enumeration and exploitation framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lodowep | 1.2.1 | Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver system. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| log-file-parser | 60.c7a0ae7e | Parser for $LogFile on NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| logkeys | 96.2539ccb | A GNU/Linux keylogger that worked. | [blackarch-keylogger](http://docs.google.com/keylogger.html) |  |
| loic | 2.9.9.99 | An open source network stress tool for Windows. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| loki-scanner | 1096.8f7f2bf | Simple IOC and Incident Response Scanner. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| lolbas | 192.d148d27 | Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| loot | 51.656fb85 | Sensitive information extraction tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| lorcon | 2020.06.06 | Generic library for injecting 802.11 frames | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| lorg | 98.aa4f1a3 | Apache Logfile Security Analyzer. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| lotophagi | 0.1 | a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lsrtunnel | 0.2 | Spoofs connections using source routed packets. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| lte-cell-scanner | 57.5fa3df8 | LTE SDR cell scanner optimized to work with very low performance RF front ends (8bit A/D, 20dB noise figure). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ltrace | 0.7.3 | Tracks runtime library calls in dynamically linked programs | [blackarch-binary](http://docs.google.com/binary.html) |  |
| luksipc | 0.01 | A tool to convert unencrypted block devices to encrypted LUKS devices in-place. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| lulzbuster | 1.3.2 | A very fast and smart web directory and file enumeration tool written in C. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| lunar | 677.42406f2 | A UNIX security auditing tool based on several security frameworks. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| luyten | 0.5.4 | An Open Source Java Decompiler Gui for Procyon. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| lynis | 2.7.5 | Security and system auditing tool to harden Unix/Linux systems | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| lyricpass | 44.b1c8a6a | Tool to generate wordlists based on lyrics. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| m3-gen | 7.7c656cc | Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass, this tool intended for adversary simulation and red teaming purpose. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| mac-robber | 1.02 | A digital investigation tool that collects data from allocated files in a mounted file system. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| macchanger | 1.7.0 | A small utility to change your NIC's MAC address | [blackarch-networking](http://docs.google.com/networking.html) |  |
| machinae | 192.d1c78b8 | A tool for collecting intelligence from public sites/feeds about various security-related pieces of data. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| maclookup | 0.4 | Lookup MAC addresses in the IEEE MA-L/OUI public listing. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| magescan | 1.12.9 | Scan a Magento site for information. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| magicrescue | 1.1.9 | Find and recover deleted files on block devices | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| magictree | 1.3 | A penetration tester productivity tool designed to allow easy and straightforward data consolidation, querying, external command execution and report generation | [blackarch-misc](http://docs.google.com/misc.html) |  |
| mail-crawl | 0.1 | Tool to harvest emails from website. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| make-pdf | 0.1.7 | This tool will embed javascript inside a PDF document. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| maketh | 0.2.0 | A packet generator that supports forging ARP, IP, TCP, UDP, ICMP and the ethernet header as well. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| malboxes | 446.32d358f | Builds malware analysis Windows VMs so that you don't have to. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| malcom | 708.02e55b9 | Analyze a system's network communication using graphical representations of network traffic. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| malheur | 0.5.4 | A tool for the automatic analyze of malware behavior. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| malice | 0.3.28 | VirusTotal Wanna Be - Now with 100% more Hipster. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| maligno | 2.5 | An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| mallory | 132.8db35b9 | HTTP/HTTPS proxy over SSH. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| malmon | 0.3 | Hosting exploit/backdoor detection daemon. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| malscan | 5.773505a | A Simple PE File Heuristics Scanner. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| maltego | 4.2.15.13632 | An open source intelligence and forensics application, enabling to easily gather information about DNS, domains, IP addresses, websites, persons, etc. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| maltrail | 56866.ffb2d190f6 | Malicious traffic detection system. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| maltrieve | 342.b9e7560 | Originated as a fork of mwcrawler. It retrieves malware directly from the sources as listed at a number of sites. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| malware-check-tool | 1.2 | Python script that detects malicious files via checking md5 hashes from an offline set or via the virustotal site. It has http proxy support and an update feature. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| malwareanalyser | 3.3 | A freeware tool to perform static and dynamic analysis on malware. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| malwaredetect | 0.1 | Submits a file's SHA1 sum to VirusTotal to determine whether it is a known piece of malware | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| malwasm | 0.2 | Offline debugger for malware's reverse engineering. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| malybuzz | 1.0 | A Python tool focused in discovering programming faults in network software. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| mana | 68.56bcfcd | A toolkit for rogue access point (evilAP) attacks first presented at Defcon 22. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mando.me | 9.8b34f1a | Web Command Injection Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| manticore | 0.2.4.r292.gb4d129f8 | Symbolic execution tool. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| manul | 197.f525df9 | A coverage-guided parallel fuzzer for open-source and blackbox binaries on Windows, Linux and MacOS. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| mara-framework | 176.ac4ac88 | A Mobile Application Reverse engineering and Analysis Framework. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| marc4dasm | 6.f11860f | This python-based tool is a disassembler for the Atmel MARC4 (a 4 bit Harvard micro). | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| maryam | 462.473f218 | Full-featured Web Identification framework written in Python. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| maskprocessor | 0.73 | A High-Performance word generator with a per-position configurable charset. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| massbleed | 20.44b7e85 | SSL Vulnerability Scanner. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| masscan | 1.3.2 | TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| masscan-automation | 26.a170abc | Masscan integrated with Shodan API. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| massdns | 221.df86e6f | A high-performance DNS stub resolver in C. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| massexpconsole | 410.d9cef9e | A collection of tools and exploits with a cli ui for mass exploitation. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| mat | 0.6.1 | Metadata Anonymisation Toolkit composed of a GUI application, a CLI application and a library. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| mat2 | 0.12.1 | Metadata removal tool, supporting a wide range of commonly used file formats | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| matahari | 0.1.30 | A reverse HTTP shell to execute commands on remote machines behind firewalls. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| matroschka | 58.2f026a4 | Python steganography tool to hide images or text in images. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| mausezahn | 0.40 | A free fast traffic generator written in C which allows you to send nearly every possible and impossible packet. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| mbenum | 1.5.0 | Queries the master browser for whatever information it has registered. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| mboxgrep | 0.7.9 | A small, non-interactive utility that scans mail folders for messages matching regular expressions. It does matching against basic and extended POSIX regular expressions, and reads and writes a variety of mailbox formats. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mdbtools | 738.823b32f | Utilities for viewing data and exporting schema from Microsoft Access Database files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mdcrack | 1.2 | MD4/MD5/NTLM1 hash cracker | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| mdk3 | v6 | WLAN penetration tool | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mdk4 | 29.002f64a | Proof-of-Concept tool to exploit common IEEE 802.11 protocol weaknesses. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mdns-recon | 10.81ecf94 | An mDNS recon tool written in Python. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| meanalyzer | 1.186.2 | Intel Engine Firmware Analysis Tool. | [blackarch-firmware](http://docs.google.com/firmware.html) |  |
| medusa | 2.2 | Speedy, massively parallel and modular login brute-forcer for network | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| meg | 87.9daab00 | Fetch many paths for many hosts - without killing the hosts. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| melkor | 1.0 | An ELF fuzzer that mutates the existing data in an ELF sample given to create orcs (malformed ELFs), however, it does not change values randomly (dumb fuzzing), instead, it fuzzes certain metadata with semi-valid values through the use of fuzzing rules (knowledge base). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| memdump | 1.01 | Dumps system memory to stdout, skipping over holes in memory maps. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| memfetch | 0.05b | Dumps any userspace process memory without affecting its execution. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| memimager | 1.0 | Performs a memory dump using NtSystemDebugControl. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| mentalist | 6.953a07b | Graphical tool for custom wordlist generation. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| merlin-server | 0.9.1 | Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| metabigor | 43.f669f18 | Intelligence Tool but without API key. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| metacoretex | 0.8.0 | MetaCoretex is an entirely JAVA vulnerability scanning framework for databases. | [blackarch-database](http://docs.google.com/database.html) |  |
| metagoofil | 12.823b114 | An information gathering tool designed for extracting metadata of public documents. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| metame | 14.8d583a0 | A simple metamorphic code engine for arbitrary executables. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| metasploit | 6.0.34 | Advanced open-source platform for developing, testing, and using exploit code | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| metasploit-autopwn | 12.09320cc | db\_autopwn plugin of metasploit. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| meterssh | 18.9a5ed19 | A way to take shellcode, inject it into memory then tunnel whatever port you want to over SSH to mask any type of communications as a normal SSH connection. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| metoscan | 05 | Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| mfcuk | 0.3.8 | MIFARE Classic Universal toolKit. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mfoc | 0.10.7+38+gba072f1 | MiFare Classic Universal toolKit | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| mfsniffer | 0.1 | A python script for capturing unencrypted TSO login credentials. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| mft2csv | 40.164eb224 | Extract $MFT record info and log it to a csv file. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mftcarver | 9.7bfcc0a2 | Carve $MFT records from a chunk of data (for instance a memory dump). | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mftrcrd | 16.35c3ac2f | Command line $MFT record decoder. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mftref2name | 6.7df9eebb | Resolve file index number to name or vice versa on NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mibble | 2.10.1 | An open-source SNMP MIB parser (or SMI parser) written in Java. It can be used to read SNMP MIB files as well as simple ASN.1 files. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| microsploit | 9.441e132 | Fast and easy create backdoor office exploitation using module metasploit packet, Microsoft Office, Open Office, Macro attack, Buffer Overflow. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| middler | 1.0 | A Man in the Middle tool to demonstrate protocol middling attacks. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mikrotik-npk | 11.d54e97c | Python tools for manipulating Mikrotik NPK format. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| mildew | 9.9130e5a | Dotmil subdomain discovery tool that scrapes domains from official DoD website directories and certificate transparency logs. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| mimikatz | 2.2.0\_20200918 | A little tool to play with Windows security. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| mimipenguin | 150.eb2fe50 | A tool to dump the login password from the current linux user. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mingsweeper | 1.00 | A network reconnaissance tool designed to facilitate large address space,high speed node discovery and identification. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| minimodem | 352.ac63965 | A command-line program which decodes (or generates) audio modem tones at any specified baud rate, using various framing protocols. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| minimysqlator | 0.5 | A multi-platform application used to audit web sites in order to discover and exploit SQL injection vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| miranda-upnp | 1.3 | A Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| missidentify | 1.0 | A program to find Win32 applications. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| missionplanner | 1.3.74 | A GroundControl Station for Ardupilot. | [blackarch-drone](http://docs.google.com/drone.html) |  |
| mitm | 8.bd2b351 | A simple yet effective python3 script to perform DNS spoofing via ARP poisoning. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mitm-relay | 29.9f34e23 | Hackish way to intercept and modify non-HTTP protocols through Burp & others. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| mitm6 | 24.a4842cb | Pwning IPv4 via IPv6. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| mitmap | 89.b590f9a | A python program to create a fake AP and sniff data. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mitmap-old | 0.1 | Shell Script for launching a Fake AP with karma functionality and launches ettercap for packet capture and traffic manipulation. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| mitmer | 22.b01c7fe | A man-in-the-middle and phishing attack tool that steals the victim's credentials of some web services like Facebook. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| mitmf | 467.0458300 | A Framework for Man-In-The-Middle attacks written in Python. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| mitmproxy | 6.0.2 | SSL-capable man-in-the-middle HTTP proxy | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| mkbrutus | 27.ddd5f8e | Password bruteforcer for MikroTik devices or boxes running RouterOS. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| mkyara | 3.8147f91 | Tool to generate YARA rules based on binary code. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| mobiusft | 1.12 | An open-source forensic framework written in Python/GTK that manages cases and case items, providing an abstract interface for developing extensions. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mobsf | 1603.68bdcd15 | An intelligent, all-in-one open source mobile application (Android/iOS) automated pen-testing framework capable of performing static, dynamic analysis and web API testing. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| modscan | 0.1 | A new tool designed to map a SCADA MODBUS TCP based network. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| moloch | 0.11.3 | An open source large scale IPv4 full PCAP capturing, indexing and database system. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mongoaudit | 222.70b83e8 | A powerful MongoDB auditing and pentesting tool . | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| monocle | 1.0 | A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| monsoon | 261.f4f9852 | A fast HTTP enumerator that allows you to execute a large number of HTTP requests. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| mooscan | 10.82963b0 | A scanner for Moodle LMS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| morpheus | 165.5d81c9e | Automated Ettercap TCP/IP Hijacking Tool. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| morxbook | 1.0 | A password cracking tool written in perl to perform a dictionary-based attack on a specific Facebook user through HTTPS. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| morxbrute | 1.01 | A customizable HTTP dictionary-based password cracking tool written in Perl. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| morxbtcrack | 1.0 | Single Bitcoin private key cracking tool released. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| morxcoinpwn | 1.0 | Mass Bitcoin private keys brute forcing/Take over tool released. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| morxcrack | 1.2 | A cracking tool written in Perl to perform a dictionary-based attack on various hashing algorithm and CMS salted-passwords. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| morxkeyfmt | 1.0 | Read a private key from stdin and output formatted data values. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| morxtraversal | 1.0 | Path Traversal checking tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| morxtunel | 1.0 | Network Tunneling using TUN/TAP interfaces over TCP tool. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| mosca | 112.7d33611 | Static analysis tool to find bugs like a grep unix command. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| mosquito | 39.fe54831 | XSS exploitation tool - access victims through HTTP proxy. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| mots | 5.34017ca | Man on the Side Attack - experimental packet injection and detection. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| motsa-dns-spoofing | 2.6ac6980 | ManOnTheSideAttack-DNS Spoofing. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| mousejack | 5.58b69c1 | Wireless mouse/keyboard attack with replay/transmit poc. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mp3nema | 0.4 | A tool aimed at analyzing and capturing data that is hidden between frames in an MP3 file or stream, otherwise noted as "out of band" data. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mptcp | 1.9.0 | A tool for manipulation of raw packets that allows a large number of options. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mptcp-abuse | 6.b0eeb27 | A collection of tools and resources to explore MPTCP on your network. Initially released at Black Hat USA 2014. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mrsip | 110.bdd98ad | SIP-Based Audit and Attack Tool. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| mrtparse | 505.3dfd9a4 | A module to read and analyze the MRT format data. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ms-sys | 2.6.0 | A tool to write Win9x-.. master boot records (mbr) under linux - RTM! | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| msf-mpc | 35.8007ef2 | Msfvenom payload creator. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| msfdb | 16.09c603b | Manage the metasploit framework database. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| msfenum | 33.17bd3ee | A Metasploit auto auxiliary script. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| mssqlscan | 0.8.4 | A small multi-threaded tool that scans for Microsoft SQL Servers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| msvpwn | 65.328921b | Bypass Windows' authentication via binary patching. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| mtr | 0.94 | Combines the functionality of traceroute and ping into one tool (CLI version) | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mtscan | 107.fb82be7 | Mikrotik RouterOS wireless scanner. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| mubeng | 47.71a372a | An incredibly fast proxy checker & IP rotator with ease. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| multiinjector | 0.4 | Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| multimac | 1.0.3 | Multiple MACs on an adapter | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| multimon-ng | 1.1.9 | An sdr decoder, supports pocsag, ufsk, clipfsk, afsk, hapn, fsk, dtmf, zvei. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| multiscanner | 1559.86e0145 | Modular file scanning/analysis framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| multitun | 1.319a134 | Tunnel arbitrary traffic through an innocuous WebSocket. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| munin-hashchecker | 205.dcaa01d | Online hash checker for Virustotal and other services | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| muraena | 130.fe5b89e | Almost-transparent reverse proxy to automate phishing and post-phishing activities. | [blackarch-social](http://docs.google.com/social.html) |  |
| mutator | 51.164132d | This project aims to be a wordlist mutator with hormones, which means that some mutations will be applied to the result of the ones that have been already done, resulting in something like: corporation -> C0rp0r4t10n\_2012 | [blackarch-automation](http://docs.google.com/automation.html) |  |
| mwebfp | 16.a800b98 | Mass Web Fingerprinter. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| mxtract | 89.ed5198b | Memory Extractor & Analyzer. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| mybff | 94.6547c51 | A Brute Force Framework. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| myjwt | 176.41602da | This cli is for pentesters, CTF players, or dev. You can modify your jwt, sign, inject, etc. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| mylg | 656.616fd53 | Network Diagnostic Tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| mysql2sqlite | 14.e5b2c31 | Converts a mysqldump file into a Sqlite 3 compatible file. | [blackarch-database](http://docs.google.com/database.html) |  |
| n1qlmap | 2.5365444 | An N1QL exploitation tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| naabu | 291.ce92dec | A fast port scanner written in go with focus on reliability and simplicity. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nacker | 23.b67bb39 | A tool to circumvent 802.1x Network Access Control on a wired LAN. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| naft | 0.0.9 | Network Appliance Forensic Toolkit. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| nasnum | 5.df5df19 | Script to enumerate network attached storages. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| nbname | 1.0 | Decodes and displays all NetBIOS name packets it receives on UDP port 137 and more! | [blackarch-windows](http://docs.google.com/windows.html) |  |
| nbnspoof | 1.0 | NetBIOS Name Service Spoofer | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| nbtenum | 3.3 | A utility for Windows that can be used to enumerate NetBIOS information from one host or a range of hosts. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| nbtool | 2.bf90c76 | Some tools for NetBIOS and DNS investigation, attacks, and communication. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nbtscan | 36.8ab6a70 | Scan networks for NetBIOS name information. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ncpfs | 2.2.6 | Allows you to mount volumes of NetWare servers under Linux. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ncrack | 0.7 | High-speed network authentication cracking tool | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| necromant | 3.acbc448 | Python Script that search unused Virtual Hosts in Web Servers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| needle | 579.891b660 | The iOS Security Testing Framework. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| neglected | 8.68d02b3 | Facebook CDN Photo Resolver. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| neighbor-cache-fingerprinter | 83.f1e596f | An ARP based Operating System version scanner. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| nemesis | 233.7aab64a | A command-line network packet crafting and injection utility. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| neo-regeorg | 108.b6239c1 | Improved version of reGeorg, HTTP tunneling pivot tool | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| net-creds | 87.07a25e1 | Sniffs sensitive data from interface or pcap. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| netactview | 0.6.4 | A graphical network connections viewer similar in functionality to netstat. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| netattack | 24.230b856 | Python script to scan and attack wireless networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| netbios-share-scanner | 1.0 | This tool could be used to check windows workstations and servers if they have accessible shared resources. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| netbus | 1.6 | NetBus remote administration tool | [blackarch-windows](http://docs.google.com/windows.html) |  |
| netcommander | 1.3 | An easy-to-use arp spoofing tool. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| netcon | 0.1 | A network connection establishment and management script. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| netdiscover | 162.e3c3331 | An active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| netkit-bsd-finger | 0.17 | BSD-finger ported to Linux. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| netkit-rusers | 0.17 | Logged in users; Displays who is logged in to machines on local network. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| netkit-rwho | 0.17 | Remote who client and server (with Debian patches). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| netmap | 0.1.3 | Can be used to make a graphical representation of the surrounding network. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| netmask | 2.4.4 | Helps determine network masks | [blackarch-recon](http://docs.google.com/recon.html) |  |
| netreconn | 1.78 | A collection of network scan/recon tools that are relatively small compared to their larger cousins. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| netripper | 79.683ef1b | Smart traffic sniffing for penetration testers. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| netscan | 1.0 | Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| netscan2 | 58.a1db723 | Active / passive network scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| netsed | 1.3 | Small and handful utility design to alter the contents of packets forwarded thru network in real time. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| netsniff-ng | 0.6.8 | High performance Linux network sniffer for packet inspection | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| netstumbler | 0.4.0 | Well-known wireless AP scanner and sniffer. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| network-app-stress-tester | 19.df75391 | Network Application Stress Testing Yammer. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| networkmap | 58.f5faf17 | Post-exploitation network mapper. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| networkminer | 2.6 | A Network Forensic Analysis Tool for advanced Network Traffic Analysis, sniffer and packet analyzer. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| netzob | 1.0.2 | An open source tool for reverse engineering, traffic generation and fuzzing of communication protocols. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| nextnet | 3.c8dc7a6 | Pivot point discovery tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nfcutils | 0.3.2 | Provides a simple 'lsnfc' command that list tags which are in your NFC device field | [blackarch-nfc](http://docs.google.com/nfc.html) |  |
| nfdump | 1.6.13 | A set of tools to collect and process netflow data. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nfex | 2.5 | A tool for extracting files from the network in real-time or post-capture from an offline tcpdump pcap savefile. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| nfspy | 1.0 | A Python library for automating the falsification of NFS credentials when mounting an NFS share. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| nfsshell | 19980519 | Userland NFS command tool. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| ngrep | 1.47 | A grep-like utility that allows you to search for network packets on an interface. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ngrok | 2.3.35 | A tunneling, reverse proxy for developing and understanding networked, HTTP services. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| nield | 38.0c0848d | A tool to receive notifications from kernel through netlink socket, and generate logs related to interfaces, neighbor cache(ARP,NDP), IP address(IPv4,IPv6), routing, FIB rules, traffic control. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nikto | 2.1.6 | A web server scanner which performs comprehensive tests against web servers for multiple items | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nili | 39.285220a | Tool for Network Scan, Man in the Middle, Protocol Reverse Engineering and Fuzzing. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nimbostratus | 54.c7c206f | Tools for fingerprintinging and exploiting Amazon cloud infrastructures. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| nipe | 302.9e628df | A script to make Tor Network your default gateway. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| nipper | 0.11.7 | Network Infrastructure Parser | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nirsoft | 1.23.30 | Unique collection of small and useful freeware utilities. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| nishang | 0.7.6 | Using PowerShell for Penetration Testing. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| njsscan | 0.2.0 | A static application testing (SAST) tool that can find insecure code patterns in your node.js applications. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| nkiller2 | 2.0 | A TCP exhaustion/stressing tool. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| nmap | 7.91 | Utility for network discovery and security auditing | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nmap-parse-output | 23.6405abf | Converts/manipulates/extracts data from a nmap scan output. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| nmbscan | 1.2.6 | Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nohidy | 67.22c1283 | The system admins best friend, multi platform auditing tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| nomorexor | 2.84489f9 | Tool to help guess a files 256 byte XOR key by using frequency analysis. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| noriben | 147.d128833 | Portable, Simple, Malware Analysis Sandbox. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| nosqlattack | 98.a5b0329 | Python tool to automate exploit MongoDB server IP on Internet anddisclose the database data by MongoDB default configuration weaknesses and injection attacks. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| nosqli | 33.214d14f | NoSQL scanner and injector. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| nosqli-user-pass-enum | 18.1b3713a | Script to enumerate usernames and passwords from vulnerable web applications running MongoDB. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| nosqlmap | 238.ae0b461 | Automated Mongo database and NoSQL web application exploitation tool | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| notspikefile | 0.1 | A Linux based file format fuzzing tool | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| novahot | 23.69857bb | A webshell framework for penetration testers. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| nray | 59.30517fd | Distributed port scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nsdtool | 0.1 | A netgear switch discovery tool. It contains some extra features like bruteoforce and setting a new password. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| nsearch | 353.bd8205b | Minimal script to help find script into the nse database. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| nsec3map | 20.1263537 | A tool to enumerate the resource records of a DNS zone using its DNSSEC NSEC or NSEC3 chain. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nsec3walker | 20101223 | Enumerates domain names using DNSSEC | [blackarch-recon](http://docs.google.com/recon.html) |  |
| nsia | 1.0.6 | A website scanner that monitors websites in realtime in order to detect defacements, compliance violations, exploits, sensitive information disclosure and other issues. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nsntrace | 81.4d02e74 | Perform network trace of a single process by using network namespaces. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| nsoq | 1.9.5 | A Network Security Tool for packet manipulation that allows a large number of options. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ntds-decode | 0.1 | This application dumps LM and NTLM hashes from active accounts stored in an Active Directory database. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ntdsxtract | 34.7fa1c8c | Active Directory forensic framework. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ntfs-file-extractor | 6.f2b23d72 | Extract files off NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ntfs-log-tracker | 1.6 | This tool can parse $LogFile, $UsnJrnl of NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| ntlm-challenger | 3.e7d3ba8 | Parse NTLM over HTTP challenge messages. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ntlm-scanner | 6.4b29329 | A simple python tool based on Impacket that tests servers for various known NTLM vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ntlm-theft | 20.81589ea | A tool for generating multiple types of NTLMv2 hash theft files. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ntlmrecon | 69.d72d96b | A tool to enumerate information from NTLM authentication enabled web endpoints. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ntp-fingerprint | 0.1 | An active fingerprinting utility specifically designed to identify the OS the NTP server is running on. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| ntp-ip-enum | 0.1 | Script to pull addresses from a NTP server using the monlist command. Can also output Maltego resultset. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ntpdos | 4.3fe389b | PoC for distributed NTP reflection DoS (CVE-5211) | [blackarch-dos](http://docs.google.com/dos.html) |  |
| nuclei | 1125.781a71e | A fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| nuclei-templates | 4061.b36ec072 | Community curated list of template files for the nuclei engine. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| nullinux | 117.04ca542 | Tool that can be used to enumerate OS information, domain information, shares, directories, and users through SMB null sessions. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| nullscan | 1.0.1 | A modular framework designed to chain and automate security tests. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| nxcrypt | 32.6ae06b5 | NXcrypt - python backdoor framework. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| o-saft | 4293.e41eb2f | A tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| o365spray | 96.e235abd | Username enumeration and password spraying tool aimed at Microsoft O365. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| oat | 1.3.1 | A toolkit that could be used to audit security within Oracle database servers. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| obevilion | 409.29fbe9d | Another archive cracker created in python | cracking [zip/7z/rar]. |  |
| obexstress | 0.1 | Script for testing remote OBEX service for some potential vulnerabilities. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| obfs4proxy | 0.0.11 | A pluggable transport proxy written in Go. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| objdump2shellcode | 28.c2d6120 | A tool I have found incredibly useful whenever creating custom shellcode. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| objection | 1.11.0 | Instrumented Mobile Pentest Framework. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| oclhashcat | 2.01 | Worlds fastest WPA cracker with dictionary mutation engine. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ocs | 0.2 | Compact mass scanner for Cisco routers with default telnet/enable passwords. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| office-dde-payloads | 34.53291f9 | Collection of scripts and templates to generate Office documents embedded with the DDE, macro-less command execution technique. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ofp-sniffer | 189.3898088 | An OpenFlow sniffer to help network troubleshooting in production networks. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| ohrwurm | 1.7a1182a | A small and simple RTP fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| okadminfinder | 78.3f0e226 | Tool to find admin panels / admin login pages. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| oledump | 0.0.57 | Analyze OLE files (Compound File Binary Format). These files contain streams of data. This tool allows you to analyze these streams. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| ollydbg | 201g | A 32-bit assembler-level analysing debugger. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| omen | 19.10aa99e | Ordered Markov ENumerator - Password Guesser. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| omnibus | 129.88dbf5d | OSINT tool for intelligence collection, research and artifact management. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| omnihash | 70.870e9ae | Hash files, strings, input streams and network resources in various common algorithms simultaneously. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| one-lin3r | 63.9fdfa5f | Gives you one-liners that aids in penetration testing and more. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| onesixtyone | 0.7 | An SNMP scanner that sends multiple SNMP requests to multiple IP addresses | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| onetwopunch | v1.0.0.r2.gd4ab4e8 | Use unicornscan to quickly scan all open ports, and then pass the open ports to nmap for detailed scans. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| onioff | 84.34dc309 | An onion url inspector for inspecting deep web links. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| onionscan | 130.da42865 | Scan Onion Services for Security Issues. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| onionsearch | 33.274af4f | Script that scrapes urls on different ".onion" search engines. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| onionshare | 2.2 | Share a file over Tor Hidden Services anonymously and securely | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| open-iscsi | 2.1.4 | iSCSI userland tools | [blackarch-misc](http://docs.google.com/misc.html) |  |
| opendoor | 420.fbdffd1 | OWASP WEB Directory Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| openpuff | 4.01 | Yet not another steganography SW. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| openscap | 1.3.4.r256.g2e804671d | Open Source Security Compliance Solution. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| openstego | 0.8.0 | A tool implemented in Java for generic steganography, with support for password-based encryption of the data. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| opensvp | 65.df54ed8 | A security tool implementing "attacks" to be able to the resistance of firewall to protocol level attack. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| openvas | 6.0.1 | The OpenVAS scanning Daemon. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| operative | 107.6a08245 | Framework based on fingerprint action, this tool is used for get information on a website or a enterprise target with multiple modules (Viadeo search,Linkedin search, Reverse email whois, Reverse ip whois, SQL file forensics ...). | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| ophcrack | 3.8.0 | Windows password cracker based on rainbow tables | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| orakelcrackert | 1.00 | This tool can crack passwords which are encrypted using Oracle's latest SHA1 based password protection algorithm. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| origami | 2.1.0 | Aims at providing a scripting tool to generate and analyze malicious PDF files. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| orjail | 194.a0b9e6c | A more secure way to force programs to exclusively use tor network. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| oscanner | 1.0.6 | An Oracle assessment framework developed in Java. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| osfooler-ng | 2.c0b20d6 | Prevents remote active/passive OS fingerprinting by tools like nmap or p0f. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| osi.ig | 99.1568b65 | Instagram OSINT Tool gets a range of information from an Instagram account. | [blackarch-social](http://docs.google.com/social.html) |  |
| osint-spy | 25.03dcf48 | Performs OSINT scan on email/domain/ip\_address/organization. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| osinterator | 3.8447f58 | Open Source Toolkit for Open Source Intelligence Gathering. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| osrframework | 830.82f9e46 | A project focused on providing API and tools to perform more accurate online researches. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| osslsigncode | 243.315357f | A small tool that implements part of the functionality of the Microsoft tool signtool.exe. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ostinato | 0.9 | An open-source, cross-platform packet/traffic generator and analyzer with a friendly GUI. It aims to be "Wireshark in Reverse" and thus become complementary to Wireshark. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| osueta | 82.2ee8068 | A simple Python script to exploit the OpenSSH User Enumeration Timing Attack. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| otori | 0.3 | A python-based toolbox intended to allow useful exploitation of XML external entity ("XXE") vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| outguess | 0.2 | A universal steganographic tool. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| outlook-webapp-brute | 1.61d7177 | Microsoft Outlook WebAPP Brute. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| owabf | 1.3 | Outlook Web Access bruteforcer tool. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| owasp-bywaf | 26.e730d1b | A web application penetration testing framework (WAPTF). | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| owasp-zsc | 315.5bb9fed | Shellcode/Obfuscate Code Generator. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| owtf | 2133.30f8e409 | The Offensive (Web) Testing Framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| p0f | 3.09b | Purely passive TCP/IP traffic fingerprinting tool | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| pack | 0.0.4 | Password Analysis and Cracking Kit | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| packer | 1.6.5 | tool for creating identical machine images for multiple platforms from a single source configuration | [blackarch-binary](http://docs.google.com/binary.html) |  |
| packerid | 1.4 | Script which uses a PEiD database to identify which packer (if any) is being used by a binary. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| packet-o-matic | 351 | A real time packet processor. Reads the packet from an input module, match the packet using rules and connection tracking information and then send it to a target module. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| packeth | 2.1 | Linux GUI packet generator tool for ethernet | [blackarch-networking](http://docs.google.com/networking.html) |  |
| packetq | 240.965b6e1 | A tool that provides a basic SQL-frontend to PCAP-files. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| packetsender | 591.0d88d7d | An open source utility to allow sending and receiving TCP and UDP packets. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| packit | 1.0 | A network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pacu | 993.795ad34 | The AWS exploitation framework, designed for testing the security of Amazon Web Services environments. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pacumen | 1.92a0884 | Packet Acumen - Analyse encrypted network traffic and more (side-channel attacks). | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| padbuster | 10.320a020 | Automated script for performing Padding Oracle attacks. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pafish | 166.6c1fabd | A demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| paketto | 1.10 | Advanced TCP/IP Toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| panhunt | 63.ec87e88 | Searches for credit card numbers (PANs) in directories. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| panoptic | 185.df35a6c | A tool that automates the process of search and retrieval of content for common log and config files through LFI vulnerability. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pappy-proxy | 77.e1bb049 | An intercepting proxy for web application testing. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| parameth | 56.8da6f27 | This tool can be used to brute discover GET and POST parameters. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| parampampam | 32.9a10782 | This tool for brute discover GET and POST parameters. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| paranoic | 1.7 | A simple vulnerability scanner written in Perl. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| paros | 3.2.13 | Java-based HTTP/HTTPS proxy for assessing web app vulnerabilities. Supports editing/viewing HTTP messages on-the-fly, spiders, client certificates, proxy-chaining, intelligent scanning for XSS and SQLi, etc. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| parse-evtx | 3.a4b02b9 | A tool to parse the Windows XML Event Log (EVTX) format. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| parsero | 81.e5b585a | A robots.txt audit tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pasco | 20040505\_1 | Examines the contents of Internet Explorer's cache files for forensic purposes | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pass-station | v1.2.0.r0.g487f224 | CLI & library to search for default credentials among thousands of Products / Vendors. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| passcracking | 20131214 | A little python script for sending hashes to passcracking.com and milw0rm | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| passe-partout | 0.1 | Tool to extract RSA and DSA private keys from any process linked with OpenSSL. The target memory is scanned to lookup specific OpenSSL patterns. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| passhunt | 5.332f374 | Search drives for documents containing passwords. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| passivedns | 287.d757713 | A network sniffer that logs all DNS server replies for use in a passive DNS setup. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| pastejacker | 12.ed9f153 | Hacking systems with the automation of PasteJacking attacks. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pasv-agrsv | 57.6bb54f7 | Passive recon / OSINT automation script. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| patator | 199.5947f5f | A multi-purpose bruteforcer. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| patchkit | 37.95dc699 | Powerful binary patching from Python. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| pathzuzu | 64.4f4533c | Checks for PATH substitution vulnerabilities and logs the commands executed by the vulnerable executables. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| payloadmask | 16.ff38964 | Web Payload list editor to use techniques to try bypass web application firewall. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| payloadsallthethings | 1040.2b43fa8 | A list of useful payloads and bypass for Web Application Security and Pentest/CTF. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pblind | 1.0 | Little utility to help exploiting blind sql injection vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pbscan | 10.566c3d7 | Faster and more efficient stateless SYN scanner and banner grabber due to userland TCP/IP stack usage. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pcapfex | 60.c51055a | Packet CAPture Forensic Evidence eXtractor. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pcapfix | 1.1.5 | Tries to repair your broken pcap and pcapng files. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pcapsipdump | 0.2 | A tool for dumping SIP sessions (+RTP traffic, if available) to disk in a fashion similar to 'tcpdump -w' (format is exactly the same), but one file per sip session (even if there is thousands of concurrent SIP sessions). | [blackarch-voip](http://docs.google.com/voip.html) |  |
| pcapteller | 1.1 | A tool designed for traffic manipulation and replay. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| pcapxray | 271.dc2bd65 | A Network Forensics Tool - To visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pcileech | 4.8 | Tool, which uses PCIe hardware devices to read and write from the target system memory. | [blackarch-hardware](http://docs.google.com/hardware.html) |  |
| pcode2code | 4.4de2193 | VBA p-code decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| pcredz | 66.0b6df2b | A tool that extracts credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, and more from a pcap file or from a live interface. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pdblaster | 4.fc8abb3 | Extract PDB file paths from large sample sets of executable files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pdf-parser | 0.7.4 | Parses a PDF document to identify the fundamental elements used in the analyzed file. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pdfbook-analyzer | 2 | Utility for facebook memory forensics. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pdfcrack | 0.19 | Password recovery tool for PDF-files | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pdfgrab | 15.1327508 | Tool for searching pdfs withthin google and extracting pdf metadata. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pdfid | 0.2.7 | Scan a file to look for certain PDF keywords. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pdfresurrect | 0.12 | A tool aimed at analyzing PDF documents. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pdfwalker | 7.64c17f0 | Frontend to explore the internals of a PDF document with Origami | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pdgmail | 1.0 | A password dictionary attack tool that targets windows authentication via the SMB protocol. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pe-bear | 0.5.3.1 | A freeware reversing tool for PE files. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pe-sieve | 0.2.9 | Scans a given process. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| peach | 3.0.202 | A SmartFuzzer that is capable of performing both generation and mutation based fuzzing. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| peach-fuzz | 55.404e8ee | Simple vulnerability scanning framework. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| peass | 557.6e09137 | Privilege Escalation Awesome Scripts SUITE (with colors). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| peda | 1.1 | Python Exploit Development Assistance for GDB | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| peepdf | 0.4.2 | A Python tool to explore PDF files in order to find out if the file can be harmful or not. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| peepingtom | 56.bc6f4d8 | A tool to take screenshots of websites. Much like eyewitness. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| peframe | 134.ad02a17 | Tool to perform static analysis on (portable executable) malware. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| pemcrack | 12.66e02b8 | Cracks SSL PEM files that hold encrypted private keys. Brute forces or dictionary cracks. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pemcracker | 9.a741c93 | Tool to crack encrypted PEM files. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| penbox | 81.3b77c69 | A Penetration Testing Framework - The Tool With All The Tools. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pencode | 23.937072d | Complex payload encoder. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pentbox | 1.8 | A security suite that packs security and stability testing oriented tools for networks and systems. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| pentestly | 1798.93d1b39 | Python and Powershell internal penetration testing framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pentmenu | 205.9cc5733 | A bash script for recon and DOS attacks. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pepe | 13.b81889b | Collect information about email addresses from Pastebin. | [blackarch-social](http://docs.google.com/social.html) |  |
| pepper | 8.c35aaa8 | An open source script to perform malware static analysis on Portable Executable. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| periscope | 3.2 | A PE file inspection tool. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| perl-image-exiftool | 12.16 | Reader and rewriter of EXIF informations that supports raw files | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| petools | 1.9.762 | Portable executable (PE) manipulation toolkit. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pev | 0.70 | Command line based tool for PE32/PE32+ file analysis. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| pextractor | 0.18b | A forensics tool that can extract all files from an executable file created by a joiner or similar. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pfff | 0.29 | Tools and APIs for code analysis, visualization and transformation | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| pftriage | 79.d7ad183 | Python tool and library to help analyze files during malware triage and analysis. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| pgdbf | 113.4e84775 | Convert XBase / FoxPro databases to PostgreSQL | [blackarch-database](http://docs.google.com/database.html) |  |
| phantap | 58.a717723 | An 'invisible' network tap aimed at red teams. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| phantom-evasion | 103.2cd0673 | Antivirus evasion tool written in python. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| phemail | 28.302b24d | A python open source phishing email tool that automates the process of sending phishing emails as part of a social engineering test. | [blackarch-social](http://docs.google.com/social.html) |  |
| phishery | 14.5743953 | An SSL Enabled Basic Auth Credential Harvester with a Word Document Template URL Injector. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| phishingkithunter | 20.ac9bd1e | Find phishing kits which use your brand/organization's files and image'. | [blackarch-social](http://docs.google.com/social.html) |  |
| phonesploit | 51.0193f9e | Adb exploiting tools. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| phonia | 593.8ae14ff | Advanced toolkits to scan phone numbers using only free resources. | [blackarch-social](http://docs.google.com/social.html) |  |
| phoss | 0.1.13 | Sniffer designed to find HTTP, FTP, LDAP, Telnet, IMAP4, VNC and POP3 logins. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| photon | 324.198deac | Incredibly fast crawler which extracts urls, emails, files, website accounts and much more. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| php-findsock-shell | 2.b8a984f | A Findsock Shell implementation in PHP + C. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| php-mt-seed | 4.0 | PHP mt\_rand() seed cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| php-rfi-payload-decoder | 30.bd42caa | Decode and analyze RFI payloads developed in PHP. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| php-vulnerability-hunter | 1.4.0.20 | An whitebox fuzz testing tool capable of detected several classes of vulnerabilities in PHP web applications. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| phpggc | 296.7b33d9d | A library of PHP unserialize() payloads along with a tool to generate them, from command line or programmatically. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| phpsploit | 971.5e4eabf | Stealth post-exploitation framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| phpstan | 5512.893b68fc | PHP Static Analysis Tool - discover bugs in your code without running it. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| phpstress | 5.f987a7e | A PHP denial of service / stress test for Web Servers running PHP-FPM or PHP-CGI. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| phrasendrescher | 1.2.2c | A modular and multi processing pass phrase cracking tool. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pidense | 29.ef26704 | Monitor illegal wireless network activities. (Fake Access Points) | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| pin | 3.11.r97998 | A dynamic binary instrumentation tool. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pingcastle | 2.9.1.0 | Active Directory scanning tool. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pintool | 24.d538a79 | This tool can be useful for solving some reversing challenges in CTFs events. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| pintool2 | 5.1c1af91 | Improved version of pintool. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| pip3line | 92.5e27195 | The Swiss army knife of byte manipulation. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| pipal | 1.1 | A password analyser. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pipeline | 18.d90fc65 | Designed to aid in targeted brute force password cracking attacks. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pirana | 0.3.1 | Exploitation framework that tests the security of a email content filter. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pivotsuite | 19.9078d1e | A portable, platform independent and powerful network pivoting toolkit. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pixd | 7.873db72 | Colourful visualization tool for binary files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| pixiewps | 1.4.2 | Offline bruteforce of the WPS pin exploiting the low or non-existing entropy of some APs | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| pixload | 27.3035bab | Image Payload Creating/Injecting tools. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| pkcrack | 1.2.2 | A PkZip encryption cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pkt2flow | 69.868a2e8 | A simple utility to classify packets into flows. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| plasma | 922.ec7df9b | An interactive disassembler for x86/ARM/MIPS. It can generates indented pseudo-code with colored syntax. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| plcscan | 0.1 | This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| plecost | 98.1a4a11b | Wordpress finger printer Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| plown | 13.ccf998c | A security scanner for Plone CMS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| plumber | 18.3f1be68 | A python implementation of a grep friendly ftrace wrapper. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| plutil | 1.6 | Converts .plist files between binary and UTF (editable) text formats. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pmacct | 3947.f202e528 | Small set of multi-purpose passive network monitoring tools [NetFlow IPFIX sFlow libpcap BGP BMP IGP Streaming Telemetry]. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pmap | 1.10 | Passively discover, scan, and fingerprint link-local peers by the background noise they generate (i.e. their broadcast and multicast traffic). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pmapper | 70.f047d19 | A tool for quickly evaluating IAM permissions in AWS. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pmcma | 1.00 | Automated exploitation of invalid memory writes (being them the consequences of an overflow in a writable section, of a missing format string, integer overflow, variable misuse, or any other type of memory corruption). | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pmdump | 1.2 | A tool that lets you dump the memory contents of a process to a file without stopping the process. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pngcheck | 2.3.0 | Verifies the integrity of PNG, JNG and MNG files by checking the CRCs and decompressing the image data. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| pnscan | 1.11 | A parallel network scanner that can be used to survey TCP network services. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pocsuite | 430.877d1b1 | An open-sourced remote vulnerability testing framework developed by the Knownsec Security Team. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| poison | 1.5.41 | A fast, asynchronous syn and udp scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| poly | 52.4e6f189 | Polymorphic webshells. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| polyswarm | 2.7.0 | An interface to the public and private PolySwarm APIs. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| pompem | 141.3ebe768 | A python exploit tool finder. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| poracle | 68.dcc00b0 | A tool for demonstrating padding oracle attacks. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| portia | 39.2e6e608 | Automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| portmanteau | 1.0 | An experimental unix driver IOCTL security tool that is useful for fuzzing and discovering device driver attack surface. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| portspoof | 128.8b5596a | This program's primary goal is to enhance OS security through a set of new techniques. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| postenum | 115.542bde9 | Clean, nice and easy tool for basic/advanced privilege escalation techniques. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| posttester | 0.1 | A jar file that will send POST requests to servers in order to test for the hash collision vulnerability discussed at the Chaos Communication Congress in Berlin. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| powercloud | 21.0928303 | Deliver powershell payloads via DNS TXT via CloudFlare using PowerShell. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| powerfuzzer | 1\_beta | Powerfuzzer is a highly automated web fuzzer based on many other Open Source fuzzers available (incl. cfuzzer, fuzzled, fuzzer.pl, jbrofuzz, webscarab, wapiti, Socket Fuzzer). It can detect XSS, Injections (SQL, LDAP, commands, code, XPATH) and others. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| powerlessshell | 110.17705f8 | Run PowerShell command without invoking powershell.exe. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| powermft | 5.76574543 | Powerful commandline $MFT record editor. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| powerops | 32.13fe55b | PowerShell Runspace Portable Post Exploitation Tool aimed at making Penetration Testing with PowerShell "easier". | [blackarch-windows](http://docs.google.com/windows.html) |  |
| powershdll | 72.62cfa17 | Run PowerShell with rundll32. Bypass software restrictions. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| powersploit | 591.d943001 | A PowerShell Post-Exploitation Framework. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| powerstager | 14.0149dc9 | A payload stager using PowerShell. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| pown | 144.8bf21d3 | Security testing and exploitation toolkit built on top of Node.js and NPM. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ppee | 1.12 | A Professional PE file Explorer for reversers, malware researchers and those who want to statically inspect PE files in more details. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ppscan | 0.3 | Yet another port scanner with HTTP and FTP tunneling support. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pr0cks | 20.c98188b | python script setting up a transparent proxy to forward all TCP and DNS traffic through a SOCKS / SOCKS5 or HTTP(CONNECT) proxy using iptables -j REDIRECT target. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| prads | 1132.e631f4f | A "Passive Real-time Asset Detection System". | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| praeda | 48.1dc2220 | An automated data/information harvesting tool designed to gather critical information from various embedded devices. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| preeny | 110.aaef77f | Some helpful preload libraries for pwning stuff. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pret | 81.4f3820a | Printer Exploitation Toolkit - The tool that made dumpster diving obsolete. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| princeprocessor | 132.bffda8c | Standalone password candidate generator using the PRINCE algorithm. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| procdump | 35.2ec3090 | Generate coredumps based off performance triggers. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| proctal | 482.67bf7e8 | Provides a command line interface and a C library to manipulate the address space of a running program on Linux. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| procyon | 0.5.36 | A suite of Java metaprogramming tools focused on code generation and analysis. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| profuzz | 9.aa6dded | Simple PROFINET fuzzer based on Scapy. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| prometheus-firewall | 176.a316d66 | A Firewall analyzer written in ruby | [blackarch-networking](http://docs.google.com/networking.html) |  |
| promiscdetect | 1.0 | Checks if your network adapter(s) is running in promiscuous mode, which may be a sign that you have a sniffer running on your computer. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| propecia | 2 | A fast class scanner that scans for a specified open port with banner grabbing | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| protos-sip | 2 | SIP test suite. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| prowler | 1518.b0fd6ce | Tool for AWS security assessment, auditing and hardening. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| proxenet | 712.67fc6b5 | THE REAL hacker friendly proxy for web application pentests. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| proxify | 18.6252e3f | Swiss Army knife Proxy tool for HTTP/HTTPS traffic capture, manipulation, and replay on the go. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| proxmark | 2413.61163344 | A powerful general purpose RFID tool, the size of a deck of cards, designed to snoop, listen and emulate everything from Low Frequency (125kHz) to High Frequency (13.56MHz) tags. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| proxychains-ng | 4.14 | A hook preloader that allows to redirect TCP traffic of existing dynamically linked programs through one or more SOCKS or HTTP proxies | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| proxycheck | 0.1 | This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| proxyp | 2013 | Small multithreaded Perl script written to enumerate latency, port numbers, server names, & geolocations of proxy IP addresses. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| proxyscan | 0.3 | A security penetration testing tool to scan for hosts and ports through a Web proxy server. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| proxytunnel | 1.9.0.253 | a program that connects stdin and stdout to a server somewhere on the network, through a standard HTTPS proxy | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| ps1encode | 41.68d7778 | A tool to generate and encode a PowerShell based Metasploit payloads. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pscan | 1.3 | A limited problem scanner for C source files | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| pshitt | 23.dae7931 | A lightweight fake SSH server designed to collect authentication data sent by intruders. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| pspy | 159.2312eed | Monitor linux processes without root permissions. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pstoreview | 1.0 | Lists the contents of the Protected Storage. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ptf | 1455.f17f506 | The Penetration Testers Framework: Way for modular support for up-to-date tools. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pth-toolkit | 7.3641cdc | Modified version of the passing-the-hash tool collection made to work straight out of the box. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| ptunnel | 0.72 | A tool for reliably tunneling TCP connections over ICMP echo request and reply packets | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| pulledpork | 392.764d980 | Snort rule management. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pulsar | 51.357dd0f | Protocol Learning and Stateful Fuzzing. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| punter | 45.97b7bed | Hunt domain names using DNSDumpster, WHOIS, Reverse WHOIS, Shodan, Crimeflare. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pupy | 2988.4b78dc58 | Opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pureblood | 37.2c5ce07 | A Penetration Testing Framework created for Hackers / Pentester / Bug Hunter. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pwd-hash | 2.0 | A password hashing tool that use the crypt function to generate the hash of a string given on standard input. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| pwdlogy | 14.8b92bcf | A target specific wordlist generating tool for social engineers and security researchers. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pwdlyser | 136.483b9bc | Python-based CLI Password Analyser (Reporting Tool). | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| pwdump | 7.1 | Extracts the binary SAM and SYSTEM file from the filesystem and then the hashes. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| pwnat | 13.5de412c | 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. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pwncat | 0.1.1 | Bind and reverse shell handler with FW/IDS/IPS evasion, self-inject and port-scanning. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| pwndbg | 2020.07.23 | Makes debugging with GDB suck less | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| pwndrop | 18.385ba70 | Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| pwned | 1303.df45f3a | A command-line tool for querying the 'Have I been pwned?' service. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pwned-search | 40.04c1439 | Pwned Password API lookup. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pwnedornot | 137.4707b81 | Tool to find passwords for compromised email addresses. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pwnloris | 10.5b79eff | An improved slowloris DOS tool which keeps attacking until the server starts getting exhausted. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| pwntools | 4.3.1 | CTF framework and exploit development library. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| pybozocrack | 87.ceb0cd9 | A silly & effective MD5 cracker in Python. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pydictor | 87.a054a4d | A useful hacker dictionary builder for a brute-force attack. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pyersinia | 49.73f4056 | Network attack tool like yersinia but written in Python. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pyew | 109.8eb3e49 | A python tool to analyse malware. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| pyexfil | 81.2ef1b8c | A couple of beta stage tools for data exfiltration. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pyfiscan | 2561.a27a348 | Free web-application vulnerability and version scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| pyfuscation | 17.6d8d53f | Obfuscate powershell scripts by replacing Function names, Variables and Parameters. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| pyinstaller | 3.3.1 | A program that converts (packages) Python programs into stand-alone executables, under Windows, Linux, Mac OS X, Solaris and AIX. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| pyjfuzz | 157.f777067 | Python JSON Fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| pykek | 12.651b9ba | Kerberos Exploitation Kit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| pymeta | 13.fa74e64 | Auto Scanning to SSL Vulnerability. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| pyminifakedns | 0.1 | Minimal DNS server written in Python; it always replies with a 127.0.0.1 A-record. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| pyrasite | 2.0 | Code injection and introspection of running Python processes. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| pyrdp | 1681.ef7b669 | Python 3 RDP MITM and library. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| pyrit | 0.5.0 | The famous WPA precomputed cracker | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| pyssltest | 9.d7703f0 | A python multithreaded script to make use of Qualys ssllabs api to test SSL flaws. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pytacle | alpha2 | Automates the task of sniffing GSM frames | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| pytbull | 2.1 | A python based flexible IDS/IPS testing framework shipped with more than 300 tests. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| pythem | 454.e4fcb8a | Python2 penetration testing framework. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| python-api-dnsdumpster | 69.eddcc18 | Unofficial Python API for http://dnsdumpster.com/. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python-arsenic | 19.1 | Async WebDriver implementation for asyncio and asyncio-compatible frameworks. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| python-capstone | 4.0.2 | Lightweight multi-platform, multi-architecture disassembly framework | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| python-cymruwhois | 1.6 | Python client for the whois.cymru.com service | [blackarch-networking](http://docs.google.com/networking.html) |  |
| python-frida | 14.2.14 | Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| python-frida-tools | 9.2.3 | Frida CLI tools. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| python-google-streetview | 1.2.9 | A command line tool and module for Google Street View Image API. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| python-ivre | 0.9.16.dev163 | Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (library) | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python-jsbeautifier | 1.13.6 | JavaScript unobfuscator and beautifier | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| python-keylogger | 2.7.3 | Simple keystroke logger. | [blackarch-keylogger](http://docs.google.com/keylogger.html) |  |
| python-minidump | 0.0.17 | Python library to parse and read Microsoft minidump file format. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| python-mmbot | 78.f5f5478 | Powerful malicious file triage tool for cyber responders. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| python-oletools | 0.56 | Tools to analyze Microsoft OLE2 files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| python-pcodedmp | 1.2.6 | A VBA p-code disassembler. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| python-search-engine-parser | 0.6.2 | Scrapes search engine pages for query titles, descriptions and links. |  |  |
| python-shodan | 1.25.0 | Python library and command-line utility for Shodan (https://developer.shodan.io). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python-ssh-mitm | 0.5.0 | SSH mitm server for security audits supporting public key authentication, session hijacking and file manipulation. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| python-trackerjacker | 1.9.0 | Finds and tracks wifi devices through raw 802.11 monitoring. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| python-uncompyle6 | 3.7.4 | A Python cross-version decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| python-utidylib | 0.2 | Python bindings for Tidy HTML parser/cleaner. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| python-witnessme | 1.5.0 | Web Inventory tool, takes screenshots of webpages using Pyppeteer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| python-yara-rednaga | 279.32b6a74 | The Python interface for YARA. |  |  |
| python2-api-dnsdumpster | 69.eddcc18 | Unofficial Python API for http://dnsdumpster.com/. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python2-capstone | 4.0.1 | A disassembly framework with the target of becoming the ultimate disasm engine for binary analysis and reversing in the security community. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| python2-cymruwhois | 1.6 | Python client for the whois.cymru.com service | [blackarch-networking](http://docs.google.com/networking.html) |  |
| python2-darts.util.lru | 7.5ef01b1 | Simple dictionary with LRU behaviour. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| python2-exrex | 142.fd1e21f | Irregular methods on regular expressions. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| python2-frida | 14.2.14 | Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| python2-frida-tools | 9.2.3 | Frida CLI tools. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| python2-google-streetview | 1.2.9 | A command line tool and module for Google Street View Image API. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| python2-hpfeeds | 411.539e738 | Honeynet Project generic authenticated datafeed protocol. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| python2-ivre | 0.9.16.dev26 | Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (library) | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python2-jsbeautifier | 1.13.4 | JavaScript unobfuscator and beautifier. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| python2-ldapdomaindump | 0.9.3 | Active Directory information dumper via LDAP. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| python2-minidump | 19.749e6da | Python library to parse and read Microsoft minidump file format. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| python2-minikerberos | 17.e7e8d0a | Kerberos manipulation library in pure Python. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| python2-oletools | 0.56 | Tools to analyze Microsoft OLE2 files. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| python2-pcodedmp | 1.2.6 | A VBA p-code disassembler. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| python2-ropgadget | 5.9 | Pythonic argument parser, that will make you smile. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| python2-shodan | 1.25.0 | Python library and command-line utility for Shodan (https://developer.shodan.io). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| python2-webtech | 1.2.8 | Identify technologies used on websites. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| python2-yara | 4.0.5 | Python interface for YARA. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| qark | 301.ba1b265 | Tool to look for several security related Android application vulnerabilities. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| qrgen | 37.82a015b | Simple script for generating Malformed QRCodes. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| qrljacker | 209.102173f | QRLJacker is a highly customizable exploitation framework to demonstrate "QRLJacking Attack Vector". | [blackarch-social](http://docs.google.com/social.html) |  |
| quark-engine | 21.01.6 | An Obfuscation-Neglect Android Malware Scoring System. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| quickrecon | 0.3.2 | A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| quicksand-lite | 32.42af152 | Command line tool for scanning streams within office documents plus xor db attack. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| r2cutter | 1.12.0 | Qt and C++ GUI for radare2 reverse engineering framework | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| r2ghidra | 5.1.1 | Deep ghidra decompiler integration for radare2 and r2cutter | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| rabid | v0.0.6.r24.ga64f002 | A CLI tool and library allowing to simply decode all kind of BigIP cookies | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| raccoon | 184.a77dae5 | A high performance offensive security tool for reconnaissance and vulnerability scanning. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| radamsa | 0.6 | General purpose mutation based fuzzer | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| radare2 | 5.1.1 | Open-source tools to disasm, debug, analyze and manipulate binary files | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| radare2-keystone | 631.ac57ab3 | Keystone assembler plugins for radare2. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| radare2-unicorn | 631.ac57ab3 | Unicorn Emulator Plugin for radare2. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| radiography | 2 | A forensic tool which grabs as much information as possible from a Windows system. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| rainbowcrack | 1.8 | Password cracker based on the faster time-memory trade-off. With MySQL and Cisco PIX Algorithm patches. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ranger-scanner | 149.3aae5dd | A tool to support security professionals to access and interact with remote Microsoft Windows based systems. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rapidscan | 172.e9ed81e | The Multi-Tool Web Vulnerability Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| rarcrack | 0.2 | This program uses bruteforce algorithm to find correct password (rar, 7z, zip). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rasenum | 1.0 | A small program which lists the information for all of the entries in any phonebook file (.pbk). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| ratproxy | 1.58 | A passive web application security assessment tool | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| rats | 6.4ba54ce | A rough auditing tool for security in source code files. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| raven | 0.3 | A Linkedin information gathering tool that can be used by pentesters to gather information about an organization employees using Linkedin. | [blackarch-social](http://docs.google.com/social.html) |  |
| rawr | 74.544dd75 | Rapid Assessment of Web Resources. A web enumerator. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rawsec-cli | 1.1.1.r7.g217adc4 | Rawsec Inventory search CLI to find security tools and resources. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| rbndr | 9.a189ffd | Simple DNS Rebinding Service. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| rcracki-mt | 0.7.0 | A tool to perform rainbow table attacks on password hashes. It is intended for indexed/perfected rainbow tables, mainly generated by the distributed project www.freerainbowtables.com | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rcrdcarver | 5.54507d21 | Carve RCRD records ($LogFile) from a chunk of data.. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| rdesktop-brute | 1.5.0 | It connects to windows terminal servers - Bruteforce patch included. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rdp-sec-check | 11.d0cc143 | Script to enumerate security settings of an RDP Service. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rdpassspray | 21.23c7b31 | Python3 tool to perform password spraying using RDP. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| reaver | 1.6.6 | Brute force attack against Wifi Protected Setup | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| rebind | 0.3.4 | DNS Rebinding Tool | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| recaf | 2.18.3.2136.419925d9 | Modern Java bytecode editor. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| recentfilecache-parser | 2.5e22518 | Python parser for the RecentFileCache.bcf on Windows. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| recomposer | 2.90f85ed | Randomly changes Win32/64 PE Files for 'safer' uploading to malware and sandbox sites. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| recon-ng | 1017.093a9e6 | A full-featured Web Reconnaissance framework written in Python. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| reconnoitre | 441.f62afba | A security tool for multithreaded information gathering and service enumeration. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| reconscan | 37.d321842 | Network reconnaissance and vulnerability assessment tools. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| recoverjpeg | 2.6.3 | Recover jpegs from damaged devices. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| recsech | 123.1fc298a | Tool for doing Footprinting and Reconnaissance on the target web. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| recstudio | 4.1 | Cross platform interactive decompiler. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| recuperabit | 65.0d3232f | A tool for forensic file system reconstruction. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| red-hawk | 36.fa54e23 | All in one tool for Information Gathering, Vulnerability Scanning and Crawling. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| redasm | 1667.5ab6be9 | Interactive, multiarchitecture disassembler written in C++ using Qt5 as UI Framework. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| redfang | 2.5 | Finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the devices' Bluetooth addresses and calling read\_remote\_name(). | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| redirectpoison | 1.1 | A tool to poison a targeted issuer of SIP INVITE requests with 301 (i.e. Moved Permanently) redirection responses. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| redpoint | 123.23ef36b | Digital Bond's ICS Enumeration Tools. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| redsocks | 211.19b822e | Transparent redirector of any TCP connection to proxy. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| reelphish | 5.dc1be33 | A Real-Time Two-Factor Phishing Tool. | [blackarch-social](http://docs.google.com/social.html) |  |
| regeorg | 30.1ca54c2 | The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| regipy | 1.8.0 | Library for parsing offline registry hives. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| reglookup | 1.0.1 | Command line utility for reading and querying Windows NT registries | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| regreport | 1.6 | Windows registry forensic analysis tool. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| regrippy | 1.0.1 | Framework for reading and extracting useful forensics data from Windows registry hives. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| regview | 1.3 | Open raw Windows NT 5 Registry files (Windows 2000 or higher). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| rekall | 1409.55d1925f | Memory Forensic Framework. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| relay-scanner | 1.7 | An SMTP relay scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| remot3d | 38.a707ef7 | An Simple Exploit for PHP Language. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| replayproxy | 1.1 | Forensic tool to replay web-based attacks (and also general HTTP traffic) that were captured in a pcap file. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| resourcehacker | 5.1.7 | Resource compiler and decompiler for Windows® applications. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| responder | 377.d01bbaa | A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2 (multirelay version). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| restler-fuzzer | v7.3.0.r8.gdd3e1ca | First stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| retdec | 1917.dca4d73f | Retargetable machine-code decompiler based on LLVM. | [blackarch-decompiler](http://docs.google.com/decompiler.html) |  |
| retire | 2.2.1.r26.ga3c8a65 | Scanner detecting the use of JavaScript libraries with known vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| reverseip | 13.42cc9c3 | Ruby based reverse IP-lookup tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| revipd | 5.2aaacfb | A simple reverse IP domain scanner. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| revsh | 215.174e309 | A reverse shell with terminal support, data tunneling, and advanced pivoting capabilities. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| rex | 640.6fa9eef | Shellphish's automated exploitation engine, originally created for the Cyber Grand Challenge. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rext | 63.5f0f626 | Router EXploitation Toolkit - small toolkit for easy creation and usage of various python scripts that work with embedded devices. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rfcat | 170508 | RF ChipCon-based Attack Toolset. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rfdump | 1.6 | Tool to detect RFID-Tags and show their meta information | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| rfidiot | 107.88f2ef9 | An open source python library for exploring RFID devices. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| rfidtool | 0.01 | A opensource tool to read / write rfid tags | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| rhodiola | 4.8bc08a0 | Personalized wordlist generator with NLP, by analyzing tweets (A.K.A crunch2049). | [blackarch-automation](http://docs.google.com/automation.html) |  |
| richsploit | 2.583f553 | Exploitation toolkit for RichFaces. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ridenum | 75.9e3b89b | A null session RID cycle attack for brute forcing domain controllers. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ridrelay | 34.f2fa99c | Enumerate usernames on a domain where you have no creds by using SMB Relay with low priv. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| rifiuti2 | 0.7.0 | A rewrite of rifiuti, a great tool from Foundstone folks for analyzing Windows Recycle Bin INFO2 file. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| rinetd | 0.62 | internet redirection server | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ripdc | 0.3 | A script which maps domains related to an given ip address or domainname. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| rita | 763.ce2efdc | Real Intelligence Threat Analytics. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| riwifshell | 38.40075d5 | Web backdoor - infector - explorer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| rkhunter | 1.4.6 | Checks machines for the presence of rootkits and other unwanted tools. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| rlogin-scanner | 0.2 | Multithreaded rlogin scanner. Tested on Linux, OpenBSD and Solaris. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rogue-mysql-server | 2.78ebbfc | A rogue MySQL server written in Python. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| roguehostapd | 78.381b373 | Hostapd fork including Wi-Fi attacks and providing Python bindings with ctypes. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| rootbrute | 0.1 | Local root account bruteforcer. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ropeadope | 1.1 | A linux log cleaner. | [blackarch-anti-forensic](http://docs.google.com/anti-forensic.html) |  |
| ropeme | 4.9b3a8fd | A set of python scripts to generate ROP gadgets and payload. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ropgadget | 6.5 | Search gadgets in binaries to facilitate ROP exploitation for several file formats and architectures | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ropper | 1.13.5 | Show information about binary files and find gadgets to build rop chains for different architectures | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| roputils | 195.ae7ed20 | A Return-oriented Programming toolkit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| routerhunter | 21.4da257c | Tool used to find vulnerable routers and devices on the Internet and perform tests. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| routersploit | 3.4.0 | Open-source exploitation framework dedicated to embedded devices | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rp | 138.3a54a7c | A full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O x86/x64 binaries. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rpak | 1.0 | A collection of tools that can be useful for doing attacks on routing protocols. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| rpcsniffer | 7.9fab095 | Sniffs WINDOWS RPC messages in a given RPC server process. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| rpctools | 1.0 | Contains three separate tools for obtaining information from a system that is running RPC services | [blackarch-windows](http://docs.google.com/windows.html) |  |
| rpdscan | 2.a71b0f3 | Remmina Password Decoder and scanner. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rpivot | 5.4963487 | Socks4 reverse proxy for penetration testing. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| rr | 5520.e6a476b1 | A Record and Replay Framework. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| rrs | 1.70 | A reverse (connecting) remote shell. Instead of listening for incoming connections it will connect out to a listener (rrs in listen mode). With tty support and more. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| rsactftool | 414.ccc6560 | RSA tool for ctf - retrieve private key from weak public key and/or uncipher data. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| rsakeyfind | 1.0 | A tool to find RSA key in RAM. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| rsatool | 14.7dab6bc | Tool that can be used to calculate RSA and RSA-CRT parameters. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| rshack | 64.cf197e3 | Python tool which allows to carry out some attacks on RSA, and offer a few tools to manipulate RSA keys. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| rsmangler | 1.4 | rsmangler takes a wordlist and mangle it | [blackarch-automation](http://docs.google.com/automation.html) |  |
| rspet | 263.de4356e | A Python based reverse shell equipped with functionalities that assist in a post exploitation scenario. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| rtfm | 93.02f6432 | A database of common, interesting or useful commands, in one handy referable form. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| rtlamr | 197.03369d1 | An rtl-sdr receiver for smart meters operating in the 900MHz ISM band. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| rtlizer | 35.5614163 | Simple spectrum analyzer. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rtlsdr-scanner | 1013.3c032de | A cross platform Python frequency scanning GUI for the OsmoSDR rtl-sdr library. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rtp-flood | 1.0 | RTP flooder | [blackarch-voip](http://docs.google.com/voip.html) |  |
| rtpbreak | 1.3a | Detects, reconstructs and analyzes any RTP session | [blackarch-networking](http://docs.google.com/networking.html) |  |
| rubilyn | 0.0.1 | 64bit Mac OS-X kernel rootkit that uses no hardcoded address to hook the BSD subsystem in all OS-X Lion & below. It uses a combination of syscall hooking and DKOM to hide activity on a host. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| ruler | 301.1e5ee2d | A tool to abuse Exchange services. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| rulesfinder | 30.da36b09 | Machine-learn password mangling rules. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| rupture | 1383.131c61a | A framework for BREACH and other compression-based crypto attacks. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| rustbuster | 300.d3735cb | DirBuster for Rust. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| rustscan | 647.3085635 | Faster Nmap Scanning with Rust. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| rvi-capture | 14.a2e129b | Capture packets sent or received by iOS devices. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| rww-attack | 0.9.2 | The Remote Web Workplace Attack tool will perform a dictionary attack against a live Microsoft Windows Small Business Server's 'Remote Web Workplace' portal. It currently supports both SBS 2003 and SBS 2008 and includes features to avoid account lock out. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| s3-fuzzer | 4.0a2a6f0 | A concurrent, command-line AWS S3 Fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| s3scanner | 265.c064f42 | Scan for open S3 buckets and dump. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| safecopy | 1.7 | A disk data recovery tool to extract data from damaged media. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| sagan | 1.2.2 | A snort-like log analysis engine. | [blackarch-ids](http://docs.google.com/ids.html) |  |
| sakis3g | 0.2.0e | An all-in-one script for connecting with 3G. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| saleae-logic | 2.3.19 | Debug happy. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| sambascan | 0.5.0 | Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| samdump2 | 3.0.0 | Dump password hashes from a Windows NT/2k/XP installation | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| samesame | 67.5c20983 | Command line tool to generate crafty homograph strings. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| samplicator | 172.4230b82 | Send copies of (UDP) datagrams to multiple receivers, with optional sampling and spoofing. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| samydeluxe | 2.2ed1bac | Automatic samdump creation script. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sandcastle | 73.10af7c7 | A Python script for AWS S3 bucket enumeration. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sandmap | 579.a7c4860 | Simple CLI with the ability to run pure Nmap engine, 31 modules with 459 scan profiles. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sandsifter | 2.8375e61 | The x86 processor fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| sandy | 6.531ab16 | An open-source Samsung phone encryption assessment framework | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| saruman | 2.4be8db5 | ELF anti-forensics exec, for injecting full dynamic executables into process image (With thread injection). | [blackarch-binary](http://docs.google.com/binary.html) |  |
| sasm | 3.2.0 | A simple crossplatform IDE for NASM, MASM, GAS and FASM assembly languages. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| sawef | 29.8580d55 | Send Attack Web Forms. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sb0x | 19.04f40fe | A simple and Lightweight framework for Penetration testing. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sbd | 1.36 | Netcat-clone, portable, offers strong encryption - features AES-CBC + HMAC-SHA1 encryption, program execution (-e), choosing source port, continuous reconnection with delay + more | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| sc-make | 12.7e39718 | Tool for automating shellcode creation. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| scalpel | 1.1687261 | A frugal, high performance file carver. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| scamper | 20200923 | A tool that actively probes the Internet in order to analyze topology and performance. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scanless | 85.d775b0c | Utility for using websites that can perform port scans on your behalf. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scanmem | 0.17 | Memory scanner designed to isolate the address of an arbitrary variable in an executing process | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| scannerl | 15.e52c46b | The modular distributed fingerprinting engine. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| scanqli | 26.40a028d | SQLi scanner to detect SQL vulns. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| scansploit | 9.a0890af | Exploit using barcodes, QRcodes, earn13, datamatrix. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| scanssh | 2.1 | Fast SSH server and open proxy scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scap-security-guide | 0.1.53 | Security compliance content in SCAP, Bash, Ansible, and other formats. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| scap-workbench | 1.2.1 | SCAP Scanner And Tailoring Graphical User Interface. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| scapy | 2.4.3 | Powerful interactive packet manipulation program written in Python (tools) | [blackarch-networking](http://docs.google.com/networking.html) |  |
| scavenger | 94.334bdd1 | Crawler (Bot) searching for credential leaks on different paste sites. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| schnappi-dhcp | 0.1 | Can fuck network with no DHCP. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| scout2 | 1182.5d86d46 | Security auditing tool for AWS environments. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scoutsuite | 5496.db827e3d | Multi-Cloud Security Auditing Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scrape-dns | 58.3df392f | Searches for interesting cached DNS entries. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| scrapy | 2.4.1 | A fast high-level scraping and web crawling framework. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| scratchabit | 565.d93d759 | Easily retargetable and hackable interactive disassembler with IDAPython-compatible plugin API. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| scrounge-ntfs | 0.9 | Data recovery program for NTFS file systems | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| sctpscan | 34.4d44706 | A network scanner for discovery and security. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sdn-toolkit | 1.21 | Discover, Identify, and Manipulate SDN-Based Networks | [blackarch-networking](http://docs.google.com/networking.html) |  |
| sdnpwn | 58.b1db5b9 | An SDN penetration testing toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sea | 103.9aca1c8 | A tool to help to create exploits of binary programs. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| search1337 | 13.c69937e | 1337Day Online Exploit Scanner. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| seat | 0.3 | Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| seclists | 1094.7693c73 | A collection of multiple types of lists used during security assessments. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| secretfinder | 12.d936681 | A python script to find sensitive data (apikeys, accesstoken, jwt,..) in javascript files. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| secscan | 1.5 | Web Apps Scanner and Much more utilities. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| secure-delete | 1.b63d814 | Secure file, disk, swap, memory erasure utilities. | [blackarch-anti-forensic](http://docs.google.com/anti-forensic.html) |  |
| secure2csv | 10.119eefb0 | Decode security descriptors in $Secure on NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| seeker | 192.0dcb8f0 | Accurately Locate People using Social Engineering. | [blackarch-social](http://docs.google.com/social.html) |  |
| sees | 67.cd741aa | Increase the success rate of phishing attacks by sending emails to company users as if they are coming from the very same company's domain. | [blackarch-social](http://docs.google.com/social.html) |  |
| sensepost-xrdp | 16.46d6c19 | A rudimentary remote desktop tool for the X11 protocol exploiting unauthenticated x11 sessions. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sergio-proxy | 20.8a91bb4 | A multi-threaded transparent HTTP proxy for manipulating web traffic. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| serialbrute | 3.111c217 | Java serialization brute force attack tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| serializationdumper | 26.49dbece | A tool to dump Java serialization streams in a more human readable form. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| server-status-pwn | 7.0c02af0 | A script that monitors and extracts requested URLs and clients connected to the service by exploiting publicly accessible Apache server-status instances. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sessionlist | 6.3efc3b2 | Sniffer that intents to sniff HTTP packets and attempts to reconstruct interesting authentication data from websites that do not employ proper secure cookie auth. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| set | 8.0.3 | Social-engineer toolkit. Aimed at penetration testing around Social-Engineering. | [blackarch-social](http://docs.google.com/social.html) |  |
| seth | 98.327ba73 | Perform a MitM attack and extract clear text credentials from RDP connections. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| setowner | 1.1 | Allows you to set file ownership to any account, as long as you have the "Restore files and directories" user right. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sfuzz | 198.3bf135b | A simple fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| sgn | 22.686e60d | Shikata ga nai encoder ported into go with several improvements. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| sh00t | 207.25e5d3d | A Testing Environment for Manual Security Testers. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| sha1collisiondetection | 105.b4a7b0b | Library and command line tool to detect SHA collision in a file | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| shad0w | 375.bfc3437 | A modular C2 framework designed to successfully operate on mature environments. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| shadowexplorer | 0.9 | Browse the Shadow Copies created by the Windows Vista / 7 / 8 / 10 Volume Shadow Copy Service. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| shard | 1.5 | A command line tool to detect shared passwords. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| shareenum | 46.3bfa81d | Tool to enumerate shares from Windows hosts. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sharesniffer | 52.7f8a372 | Network share sniffer and auto-mounter for crawling remote file systems. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| shed | 2.0.0 | .NET runtime inspector. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| shellcheck | 0.7.1 | Shell script analysis tool | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| shellcode-compiler | 24.e8edc8e | Compiles C/C++ style code into a small, position-independent and NULL-free shellcode for Windows & Linux. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellcode-factory | 96.07ae857 | Tool to create and test shellcodes from custom assembly sources. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellcodecs | 0.1 | A collection of shellcode, loaders, sources, and generators provided with documentation designed to ease the exploitation and shellcode programming process. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellen | 66.c0c5f83 | Interactive shellcoding environment to easily craft shellcodes. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellerator | 31.60c5032 | Simple command-line tool aimed to help pentesters quickly generate one-liner reverse/bind shells in multiple languages. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| shellinabox | 428.98e6eeb | Implements a web server that can export arbitrary command line tools to a web based terminal emulator. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| shellme | 5.d5206f0 | Because sometimes you just need shellcode and opcodes quickly. This essentially just wraps some nasm/objdump calls into a neat script. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellnoob | 30.c923d5e | A toolkit that eases the writing and debugging of shellcode. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| shellpop | 148.a145349 | Generate easy and sophisticated reverse or bind shell commands. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| shellsploit-framework | 273.a16d22f | New Generation Exploit Development Kit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shellter | 7.2 | A dynamic shellcode injection tool, and the first truly dynamic PE infector ever created. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sherlock | 1505.253ffa8 | Find usernames across social networks. | [blackarch-social](http://docs.google.com/social.html) |  |
| sherlocked | 1.f190c2b | Universal script packer-- transforms any type of script into a protected ELF executable, encrypted with anti-debugging. | [blackarch-packer](http://docs.google.com/packer.html) |  |
| shhgit | 65.65351a7 | Find committed secrets and sensitive files across GitHub, Gists, GitLab and BitBucket or your local repositories in real time. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| shitflood | 14.e74fc42 | A Socks5 clone flooder for the Internet Relay Chat (IRC) protocol. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| shocker | 63.0380a73 | A tool to find and exploit servers vulnerable to Shellshock. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| shodanhat | 13.e5e7e68 | Search for hosts info with shodan. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| shootback | 83.cab462c | A reverse TCP tunnel let you access target behind NAT or firewall. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| shortfuzzy | 0.1 | A web fuzzing script written in perl. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| shuffledns | 89.eda49bb | A wrapper around massdns written in GO. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sickle | 73.e14c0bb | A shellcode development tool, created to speed up the various steps needed to create functioning shellcode. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sidguesser | 1.0.5 | Guesses sids/instances against an Oracle database according to a predefined dictionary file. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| siege | 4.0.8 | An http regression testing and benchmarking utility | [blackarch-dos](http://docs.google.com/dos.html) |  |
| sigma | 0.18.1 | Generic Signature Format for SIEM Systems | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| sign | 10.2dc4018 | Automatically signs an apk with the Android test certificate. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| sigploit | 786.0e52072 | Telecom Signaling Exploitation Framework - SS7, GTP, Diameter & SIP. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sigspotter | 1.0 | A tool that search in your HD to find which publishers has been signed binaries in your PC. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sigthief | 22.6620cac | Stealing Signatures and Making One Invalid Signature at a Time. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| silenteye | 20.9319304 | A cross-platform application design for an easy use of steganography. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| silenttrinity | 291.84663d5 | An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| silk | 3.19.1 | A collection of traffic analysis tools developed by the CERT NetSA to facilitate security analysis of large networks. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| simple-ducky | 20.f15079e | A payload generator. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| simple-lan-scan | 1.0 | A simple python script that leverages scapy for discovering live hosts on a network. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| simpleemailspoofer | 53.c6a7ec3 | A simple Python CLI to spoof emails. | [blackarch-social](http://docs.google.com/social.html) |  |
| simplify | 1.3.0 | Generic Android Deobfuscator. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| simplyemail | 1.4.10.r7.6a42d37 | Email recon made fast and easy, with a framework to build on CyberSyndicates | [blackarch-recon](http://docs.google.com/recon.html) |  |
| simtrace2 | 907.a124c17 | Host utilities to communicate with SIMtrace2 USB Devices. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| sinfp | 1.24 | A full operating system stack fingerprinting suite. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| siparmyknife | 11232011 | A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| sipbrute | 11.5be2fdd | A utility to perform dictionary attacks against the VoIP SIP Register hash. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| sipcrack | 0.2 | A SIP protocol login cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sipffer | 29.efc3ff1 | SIP protocol command line sniffer. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| sipi | 13.58f0dcc | Simple IP Information Tools for Reputation Data Analysis. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sipp | 1265.0262353 | A free Open Source test tool / traffic generator for the SIP protocol. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| sippts | 127.3da2878 | Set of tools to audit SIP based VoIP Systems. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| sipsak | 0.9.7 | A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| sipscan | 0.1 | A sip scanner. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sipshock | 7.6ab5591 | A scanner for SIP proxies vulnerable to Shellshock. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sipvicious | 415.fc5d9ba | Tools for auditing SIP devices. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| sireprat | 34.b8ef60b | Remote Command Execution as SYSTEM on Windows IoT Core. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sitadel | 121.0a0e475 | Web Application Security Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sitediff | 3.1383935 | Fingerprint a web app using local files as the fingerprint sources. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sjet | 27.2d52f0c | Siberas JMX exploitation toolkit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| skipfish | 2.10b | A fully automated, active web application security reconnaissance tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| skiptracer | 123.ca40957 | OSINT python2 webscraping framework. Skipping the needs of API keys. | [blackarch-social](http://docs.google.com/social.html) |  |
| skul | 27.7bd83f1 | A PoC to bruteforce the Cryptsetup implementation of Linux Unified Key Setup (LUKS). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| skyjack | 16.24e3878 | Takes over Parrot drones, deauthenticating their true owner and taking over control, turning them into zombie drones under your own control. | [blackarch-drone](http://docs.google.com/drone.html) |  |
| skype-dump | 0.1 | This is a tool that demonstrates dumping MD5 password hashes from the configuration file in Skype. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| skypefreak | 33.9347a65 | A Cross Platform Forensic Framework for Skype. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| slackpirate | 142.9788be6 | Slack Enumeration and Extraction Tool - extract sensitive information from a Slack Workspace. | [blackarch-social](http://docs.google.com/social.html) |  |
| sleuthkit | 4.10.2 | File system and media management forensic analysis tools | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| sleuthql | 9.29fc878 | Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| slither | 2166.e45f24fc | Solidity static analysis framework written in Python 3. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| sloth-fuzzer | 39.9f7f59a | A smart file fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| slowhttptest | 1.8.2 | Highly configurable tool that simulates some Application Layer Denial of Service (DoS) attacks | [blackarch-dos](http://docs.google.com/dos.html) |  |
| slowloris | 0.7 | A tool which is written in perl to test http-server vulnerabilities for connection exhaustion denial of service (DoS) attacks so you can enhance the security of your webserver. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| slowloris-py | 30.eb7f632 | Low bandwidth DoS tool. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| slurp-scanner | 90.6a4eaaf | Evaluate the security of S3 buckets. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smali | 2.4.0 | Assembler/disassembler for Android's dex format | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| smali-cfgs | 6.4450418 | Smali Control Flow Graph's. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| smalisca | 58.1aa7a16 | Static Code Analysis for Smali files. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| smap | 24.3ed1ac7 | Shellcode mapper - Handy tool for shellcode analysis. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| smartphone-pentest-framework | 104.fc45347 | Repository for the Smartphone Pentest Framework (SPF). | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| smbbf | 0.9.1 | SMB password bruteforcer. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| smbcrunch | 12.313400e | 3 tools that work together to simplify reconnaissance of Windows File Shares. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| smbexec | 59.a54fc14 | A rapid psexec style attack with samba tools. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smbmap | 145.5c98c5f | A handy SMB enumeration tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smbrelay | 3 | SMB / HTTP to SMB replay attack toolkit. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| smbspider | 10.7db9323 | A lightweight python utility for searching SMB/CIFS/Samba file shares. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smikims-arpspoof | 25.244d9ee | Performs an ARP spoofing attack using the Linux kernel's raw sockets. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| smod | 53.7eb8423 | A modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smplshllctrlr | 9.2baf390 | PHP Command Injection exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| smtp-fuzz | 1.0 | Simple smtp fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| smtp-test | 5.d8d8598 | Automated testing of SMTP servers for penetration testing. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smtp-user-enum | 1.2 | Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| smtp-vrfy | 1.0 | An SMTP Protocol Hacker. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smtpmap | 0.8.234\_BETA | Tool to identify the running smtp software on a given host. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| smtpscan | 0.5 | An SMTP scanner | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| smtptester | 13.634e1ee | Small python3 tool to check common vulnerabilities in SMTP servers. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| smtptx | 1.0 | A very simple tool used for sending simple email and do some basic email testing from a pentester perspective. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| smuggler | 21.7084d63 | An HTTP Request Smuggling / Desync testing tool written in Python 3. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| smuggler-py | 1.0 | Python tool used to test for HTTP Desync/Request Smuggling attacks. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sn00p | 0.8 | A modular tool written in bourne shell and designed to chain and automate security tools and tests. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| sn1per | 509.c2f4b66 | Automated Pentest Recon Scanner. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| snallygaster | 164.bfe8914 | Tool to scan for secret files on HTTP servers. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| snapception | 8.c156f9e | Intercept and decrypt all snapchats received over your network. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| snare | 175.5af7675 | Super Next generation Advanced Reactive honEypot | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| snarf-mitm | 41.bada142 | SMB Man in the Middle Attack Engine / relay suite. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sniff-probe-req | 362.cf34b91 | Wi-Fi Probe Requests Sniffer. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| sniffer | 4.688854e | Packet Trace Parser for TCP, SMTP Emails, and HTTP Cookies. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| sniffglue | 0.12.0 | Secure multithreaded packet sniffer | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| sniffjoke | 772.434bfb1 | Injects packets in the transmission flow that are able to seriously disturb passive analysis like sniffing, interception and low level information theft. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| sniffles | 469.118e93f | A Packet Capture Generator for IDS and Regular Expression Evaluation. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| snitch | 1.2 | Turn back the asterisks in password fields to plaintext passwords. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| snmp-brute | 15.64ec0ce | SNMP brute force, enumeration, CISCO config downloader and password cracking script. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| snmp-fuzzer | 0.1.1 | SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| snmpattack | 1.8 | SNMP scanner and attacking tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| snmpcheck | 1.9 | A free open source utility to get information via SNMP protocols. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| snmpenum | 1.7 | An snmp enumerator. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| snmpscan | 0.1 | A free, multi-processes SNMP scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| snoopbrute | 17.589fbe6 | Multithreaded DNS recursive host brute-force tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| snoopy-ng | 128.eac73f5 | A distributed, sensor, data collection, interception, analysis, and visualization framework. | [blackarch-drone](http://docs.google.com/drone.html) |  |
| snort | 2.9.17.1 | A lightweight network intrusion detection system. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| snow | 20130616 | Steganography program for concealing messages in text files. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| snowman | 0.1.3 | A native code to C/C++ decompiler, see the examples of generated code. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| snscan | 1.05 | A Windows based SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| snuck | 6.76196b6 | Automatic XSS filter bypass. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| snyk | 1.393.0 | CLI and build-time tool to find and fix known vulnerabilities in open-source dependencies. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| soapui | 5.6.0 | The Swiss-Army Knife for SOAP Testing. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| socat | 1.7.4.1 | Multipurpose relay | [blackarch-networking](http://docs.google.com/networking.html) |  |
| social-mapper | 185.8055805 | A social media enumeration and correlation tool. | [blackarch-social](http://docs.google.com/social.html) |  |
| social-vuln-scanner | 11.91794c6 | Gathers public information on companies to highlight social engineering risk. | [blackarch-social](http://docs.google.com/social.html) |  |
| socialfish | 230.9fad9bd | Ultimate phishing tool with Ngrok integrated. | [blackarch-social](http://docs.google.com/social.html) |  |
| socialscan | 106.95a413e | Check email address and username availability on online platforms. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| socketfuzz | 26.089add2 | Simple socket fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| sockstat | 0.4.1 | A tool to let you view information about open connections. It is similar to the tool of the same name that is included in FreeBSD, trying to faithfully reproduce as much functionality as is possible. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| soot | 3.4.0 | A Java Bytecode Analysis and Transformation Framework. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| sooty | 314.894dbd6 | The SOC Analysts all-in-one CLI tool to automate and speed up workflow. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| spade | 114 | A general-purpose Internet utility package, with some extra features to help in tracing the source of spam and other forms of Internet harassment. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| spaf | 11.671a976 | Static Php Analysis and Fuzzer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sparta | 21.b0a4514 | Python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| spartan | 23.babdd7d | Frontpage and Sharepoint fingerprinting and attack tool. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| sparty | 0.1 | An open source tool written in python to audit web applications using sharepoint and frontpage architecture. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| spectools | 2010\_04\_R1 | Spectrum-Tools is a set of utilities for using the Wi-Spy USB spectrum analyzer hardware. Stable version. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| speedpwn | 8.3dd2793 | An active WPA/2 Bruteforcer, original created to prove weak standard key generation in different ISP labeled routers without a client is connected. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| spf | 85.344ac2f | A python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises. | [blackarch-social](http://docs.google.com/social.html) |  |
| spfmap | 8.a42d15a | A program to map out SPF and DKIM records for a large number of domains. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| spiderfoot | 3.3 | The Open Source Footprinting Tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| spiderpig-pdffuzzer | 0.1 | A javascript pdf fuzzer | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| spiga | 623.8bc1ddc | Configurable web resource scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| spike-fuzzer | 2.9 | IMMUNITYsec's fuzzer creation kit in C. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| spike-proxy | 148 | A Proxy for detecting vulnerabilities in web applications | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| spiped | 1.6.1 | A utility for creating symmetrically encrypted and authenticated pipes between socket addresses. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| spipscan | 69.4ad3235 | SPIP (CMS) scanner for penetration testing purpose written in Python. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| splint | 3.1.2.git20180129 | A tool for statically checking C programs for security vulnerabilities and coding mistakes | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| sploitctl | 3.0.3 | Fetch, install and search exploit archives from exploit sites like exploit-db and packetstorm. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| sploitego | 153.d9568dc | Maltego Penetration Testing Transforms. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| spoofcheck | 16.8cce591 | Simple script that checks a domain for email protections. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| spooftooph | 0.5.2 | Designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain sight. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| spookflare | 24.19491b5 | Loader, dropper generator with multiple features for bypassing client-side and network-side countermeasures. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| spotbugs | 16468.0a34d96f8 | A tool for static analysis to look for bugs in Java code. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| sprayingtoolkit | 58.68f295d | Scripts to make password spraying attacks against Lync/S4B & OWA a lot quicker, less painful and more efficient. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| spraykatz | 62.1fb3aa7 | Credentials gathering tool automating remote procdump and parse of lsass process. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sps | 4.3 | A Linux packet crafting tool. Supports IPv4, IPv6 including extension headers, and tunneling IPv6 over IPv4. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| spyse | 47.cd11ba9 | Python API wrapper and command-line client for the tools hosted on spyse.com. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sqid | 0.3 | A SQL injection digger. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sqlbrute | 1.0 | Brute forces data out of databases using blind SQL injection. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| sqldict | 2.1 | A dictionary attack tool for SQL Server. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sqlivulscan | 249.cc8e657 | This will give you the SQLi Vulnerable Website Just by Adding the Dork. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sqlmap | 1.5.2 | Automatic SQL injection and database takeover tool | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sqlninja | 0.2.999 | A tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sqlpat | 1.0.1 | This tool should be used to audit the strength of Microsoft SQL Server passwords offline. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sqlping | 4 | SQL Server scanning tool that also checks for weak passwords using wordlists. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sqlpowerinjector | 1.2 | Application created in .Net 1.1 that helps the penetration tester to find and exploit SQL injections on a web page. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| sqlsus | 0.7.2 | An open source MySQL injection and takeover tool, written in perl | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ssdeep | 2.14.1 | A program for computing context triggered piecewise hashes | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| ssdp-scanner | 1.0 | SSDP amplification scanner written in Python. Makes use of Scapy. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ssh-audit | v2.4.0.r6.g2f1a2a6 | SSH server auditing (banner, key exchange, encryption, mac, compression, compatbility, etc). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ssh-honeypot | 86.1f72fa6 | Fake sshd that logs ip addresses, usernames, and passwords. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| ssh-mitm | 118.6f042a1 | SSH man-in-the-middle tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ssh-privkey-crack | 0.4 | A SSH private key cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ssh-user-enum | 7.ae453c1 | SSH User Enumeration Script in Python Using The Timing Attack. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sshatter | 1.2 | Password bruteforcer for SSH. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sshfuzz | 1.0 | A SSH Fuzzing utility written in Perl that uses Net::SSH2. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| sshprank | 1.3.5 | A fast SSH mass-scanner, login cracker and banner grabber tool using the python-masscan and shodan module. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sshscan | 1.0 | A horizontal SSH scanner that scans large swaths of IPv4 space for a single SSH user and pass. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sshtrix | 0.0.3 | A very fast multithreaded SSH login cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sshtunnel | 0.1.5 | Pure python SSH tunnels (CLI) | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| sshuttle | 1.0.5 | Transparent proxy server that forwards all TCP packets over ssh | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| ssl-hostname-resolver | 1 | CN (Common Name) grabber on X.509 Certificates over HTTPS. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ssl-phuck3r | 2.0 | All in one script for Man-In-The-Middle attacks. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| sslcat | 1.0 | SSLCat is a simple Unix utility that reads and writes data across an SSL enable network connection. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| sslcaudit | 524.f218b9b | Utility to perform security audits of SSL/TLS clients. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| ssldump | 0.9b3 | An SSLv3/TLS network protocol analyzer. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| sslh | 1.21c | SSL/SSH/OpenVPN/XMPP/tinc port multiplexer | [blackarch-networking](http://docs.google.com/networking.html) |  |
| ssllabs-scan | 249.a7f3d49 | Command-line client for the SSL Labs APIs | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sslmap | 0.2.0 | A lightweight TLS/SSL cipher suite scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sslnuke | 5.c5faeaa | Transparent proxy that decrypts SSL traffic and prints out IRC messages. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| sslscan | 1.10.2 | A fast tools to scan SSL services, such as HTTPS to determine the ciphers that are supported | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sslscan2 | 613.cf0437f | Tests SSL/TLS enabled services to discover supported cipher suites. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| sslsniff | 0.8 | A tool to MITM all SSL connections on a LAN and dynamically generate certs for the domains that are being accessed on the fly | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| sslstrip | 0.9 | Python tool to hijack HTTPS connections during a MITM attack. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| sslyze | 4.0.2 | Python tool for analyzing the configuration of SSL servers and for identifying misconfigurations. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| ssma | 215.2a2b6bd | Simple Static Malware Analyzer. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| ssrf-proxy | 293.e79da7a | Facilitates tunneling HTTP communications through servers vulnerable to Server-Side Request Forgery. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| ssrf-sheriff | 2.f95d691 | A simple SSRF-testing sheriff written in Go. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| ssrfmap | 89.c7922ba | Automatic SSRF fuzzer and exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| stackflow | 2.2af525d | Universal stack-based buffer overfow exploitation tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| stacoan | 0.90 | Crossplatform tool which aids developers, bugbounty hunters and ethical hackers performing static code analysis on mobile applications. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| staekka | 9.57787ca | This plugin extends Metasploit for some missing features and modules allowing interaction with other/custom exploits/ways of getting shell access. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| stardox | 41.95b0a97 | Github stargazers information gathering tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| starttls-mitm | 7.b257756 | A mitm proxy that will transparently proxy and dump both plaintext and TLS traffic. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| statsprocessor | 0.11 | A high-performance word-generator based on per-position Markov-attack. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| stegcracker | 2.0.9 | Steganography brute-force utility to uncover hidden data inside files. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| stegdetect | 19.ac1df7a | An automated tool for detecting steganographic content in images. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| steghide | 0.5.1 | Embeds a message in a file by replacing some of the least significant bits. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| stegolego | 8.85354f6 | Simple program for using stegonography to hide data within BMP images. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| stegosip | 11.5cda6d6 | TCP tunnel over RTP/SIP. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| stegoveritas | 1.8 | Automatic image steganography analysis tool. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| stegsolve | 1.3 | Steganography Solver. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| stenographer | 486.355604b | A packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| stepic | 0.4 | A python image steganography tool. | [blackarch-stego](http://docs.google.com/stego.html) |  |
| sticky-keys-hunter | 15.c816fc9 | Script to test an RDP host for sticky keys and utilman backdoor. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| stig-viewer | 2.8 | XCCDF formatted SRGs and STIGs files viewer for SCAP validation tools. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| stompy | 0.0.4 | An advanced utility to test the quality of WWW session identifiers and other tokens that are meant to be unpredictable. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| stoq | 764.6763957 | An open source framework for enterprise level automated analysis. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| storm-ring | 0.1 | This simple tool is useful to test a PABX with "allow guest" parameter set to "yes" (in this scenario an anonymous caller could place a call). | [blackarch-voip](http://docs.google.com/voip.html) |  |
| strace | 5.11 | A diagnostic, debugging and instructional userspace tracer | [blackarch-binary](http://docs.google.com/binary.html) |  |
| streamfinder | 1.2 | Searches for Alternate Data Streams (ADS). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| striker | 85.87c184d | An offensive information and vulnerability scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| stringsifter | 29.3cb284a | Machine learning tool that automatically ranks strings based on their relevance for malware analysis. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| striptls | 53.eff1d59 | Proxy PoC implementation of STARTTLS stripping attacks. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| strutscan | 4.8712c12 | Apache Struts2 vulnerability scanner written in Perl. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| stunnel | 5.57 | A program that allows you to encrypt arbitrary TCP connections inside SSL | [blackarch-networking](http://docs.google.com/networking.html) |  |
| sub7 | 2.2 | A remote administration tool. No further comments ;-) | [blackarch-windows](http://docs.google.com/windows.html) |  |
| subbrute | 1.2.1 | A DNS meta-query spider that enumerates DNS records and subdomains | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| subdomainer | 1.2 | A tool designed for obtaining subdomain names from public sources. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| subfinder | 898.cc5f017 | Modular subdomain discovery tool that can discover massive amounts of valid subdomains for any target. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| subjack | 182.49c51e5 | Subdomain Takeover tool written in Go. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| subjs | 32.2aeaa83 | Fetches javascript file from a list of URLS or subdomains. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| sublert | 67.56d2a12 | A security and reconnaissance tool which leverages certificate transparency to automatically monitor new subdomains deployed by specific organizations and issued TLS/SSL certificate. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sublist3r | 138.729d649 | A Fast subdomains enumeration tool for penetration testers. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| subover | 71.3d258e2 | A Powerful Subdomain Takeover Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| subscraper | 38.5602e41 | Tool that performs subdomain enumeration through various techniques. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| subterfuge | 64.69dda99 | Automated Man-in-the-Middle Attack Framework. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sucrack | 1.2.3 | A multi-threaded Linux/UNIX tool for brute-force cracking local user accounts via su | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| suid3num | 43.df2c7b9 | Python script which utilizes python's built-in modules to enumerate SUID binaries. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| sulley | 1.0.bff0dd1 | A pure-python fully automated and unattended fuzzing framework. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| superscan | 4.1 | Powerful TCP port scanner, pinger, resolver. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| suricata | 6.0.2 | An Open Source Next Generation Intrusion Detection and Prevention Engine. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| suricata-verify | 546.87e0dca | Suricata Verification Tests - Testing Suricata Output. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| svn-extractor | 42.c27831c | A simple script to extract all web resources by means of .SVN folder exposed over network. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| swaks | 20201014.0 | Swiss Army Knife SMTP; Command line SMTP testing, including TLS and AUTH | [blackarch-networking](http://docs.google.com/networking.html) |  |
| swamp | 59.3c8be65 | An OSINT tool for discovering associated sites through Google Analytics Tracking IDs. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| swap-digger | 43.3570eb3 | A tool used to automate Linux swap analysis during post-exploitation or forensics. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| swarm | 41.1713c1e | A distributed penetration testing tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| swfintruder | 0.9.1 | First tool for testing security in Flash movies. A runtime analyzer for SWF external movies. It helps to find flaws in Flash. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| swftools | 0.9.2 | A collection of SWF manipulation and creation utilities. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| syborg | 36.5cd010b | Recursive DNS Subdomain Enumerator with dead-end avoidance system. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| syft | 572.7a10cba | A CLI tool and go library for generating a Software Bill of Materials (SBOM) from container images and filesystems. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| sylkie | 0.0.4.r3.g1cf170f | IPv6 address spoofing with the Neighbor Discovery Protocol. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| syms2elf | 10.692867b | A plugin for Hex-Ray's IDA Pro and radare2 to export the symbols recognized to the ELF symbol table. | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| synflood | 0.1 | A very simply script to illustrate DoS SYN Flooding attack. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| synner | 1.1 | A custom eth->ip->tcp packet generator (spoofer) for testing firewalls and dos attacks. | [blackarch-spoof](http://docs.google.com/spoof.html) |  |
| synscan | 5.02 | fast asynchronous half-open TCP portscanner | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| syringe | 12.79a703e | A General Purpose DLL & Code Injection Utility. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| sysdig | 0.27.1 | Open source system-level exploration and troubleshooting tool | [blackarch-recon](http://docs.google.com/recon.html) |  |
| sysinternals-suite | 4.8 | Sysinternals tools suite. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| t50 | 5.8.7 | Experimental Multi-protocol Packet Injector Tool. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| tabi | 13.068a406 | BGP Hijack Detection. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| tachyon-scanner | 456.428a7c5 | Fast Multi-Threaded Web Discovery Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| tactical-exploitation | 83.ebf3603 | Modern tactical exploitation toolkit. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| taipan | 2.7 | Web application security scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| takeover | 98.a058647 | Sub-Domain TakeOver Vulnerability Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| taof | 0.3.2 | A GUI cross-platform Python generic network protocol fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| tbear | 1.5 | Transient Bluetooth Environment Auditor includes an ncurses-based Bluetooth scanner (a bit similar to kismet), a Bluetooth DoS tool, and a Bluetooth hidden device locator. | [blackarch-bluetooth](http://docs.google.com/bluetooth.html) |  |
| tcgetkey | 0.1 | A set of tools that deal with acquiring physical memory dumps via FireWire and then scan the memory dump to locate TrueCrypt keys and finally decrypt the encrypted TrueCrypt container using the keys. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| tchunt-ng | 208.b8cf7fc | Reveal encrypted files stored on a filesystem. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| tckfc | 23.911e92e | TrueCrypt key file cracker. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| tcpcontrol-fuzzer | 0.1 | 2^6 TCP control bit fuzzer (no ECN or CWR). | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| tcpcopy | 1243.2365b36 | A TCP stream replay tool to support real testing of Internet server applications. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpdstat | 4.be5bd28 | Get protocol statistics from tcpdump pcap files. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpdump | 4.99.0 | Powerful command-line packet analyzer | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpextract | 1.1 | Extracts files from captured TCP sessions. Support live streams and pcap files. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpflow | 1.6.1 | Captures data transmitted as part of TCP connections then stores the data conveniently | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpick | 0.2.1 | TCP stream sniffer and connection tracker | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| tcpjunk | 2.9.03 | A general tcp protocols testing and hacking utility. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| tcpreplay | 4.3.3 | Gives the ability to replay previously captured traffic in a libpcap format | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcptrace | 6.6.7 | A TCP dump file analysis tool | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcptraceroute | 1.5beta7 | A traceroute implementation using TCP packets. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpwatch | 1.3.1 | A utility written in Python that lets you monitor forwarded TCP connections or HTTP proxy connections. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tcpxtract | 1.0.1 | A tool for extracting files from network traffic. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| teardown | 1.0 | Command line tool to send a BYE request to tear down a call. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| tekdefense-automater | 88.42548cf | IP URL and MD5 OSINT Analysis | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| tell-me-your-secrets | v2.2.1.r3.g7f0674c | Find secrets on any machine from over 120 Different Signatures. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| tempomail | 25.3ca0fcf | Tool to create a temporary email address in 1 Second and receive emails. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| termineter | 199.ba06b3e | Smart meter testing framework. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| testdisk | 7.1 | Checks and undeletes partitions + PhotoRec, signature based recovery tool | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| testssl.sh | 3.0.4 | Testing TLS/SSL encryption | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| tftp-bruteforce | 0.1 | A fast TFTP filename bruteforcer written in perl. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| tftp-fuzz | 1337 | Master TFTP fuzzing script as part of the ftools series of fuzzers. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| tftp-proxy | 0.1 | This tool accepts connection on tftp and reloads requested content from an upstream tftp server. Meanwhile modifications to the content can be done by pluggable modules. So this one's nice if your mitm with some embedded devices. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| tgcd | 1.1.1 | TCP/IP Gender Changer Daemon utility. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| thc-ipv6 | 3.8 | Complete tool set to attack the inherent protocol weaknesses of IPv6 and ICMP6 | [blackarch-networking](http://docs.google.com/networking.html) |  |
| thc-keyfinder | 1.0 | Finds crypto keys, encrypted data and compressed data in files by analyzing the entropy of parts of the file. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| thc-pptp-bruter | 0.1.4 | A brute force program that works against pptp vpn endpoints (tcp port 1723). | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| thc-smartbrute | 1.0 | This tool finds undocumented and secret commands implemented in a smartcard. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| thc-ssl-dos | 1.4 | A tool to verify the performance of SSL. To be used in your authorized and legitimate area ONLY. You need to accept this to make use of it, no use for bad intentions, you have been warned! | [blackarch-dos](http://docs.google.com/dos.html) |  |
| thedorkbox | 7.43852d3 | Comprehensive collection of Google Dorks & OSINT techniques to find Confidential Data. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| thefatrat | 785.9927123 | TheFatRat a massive exploiting tool: easy tool to generate backdoor and easy tool to post exploitation attack. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| thefuzz | 160.b4c2c80 | CLI fuzzing tool. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| theharvester | 2311.ae63bd7 | Python tool for gathering e-mail accounts and subdomain names from different public sources (search engines, pgp key servers). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| themole | 0.3 | Automatic SQL injection exploitation tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| thezoo | 208.5def214 | A project created to make the possibility of malware analysis open and available to the public. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| threatspec | 0.5.0 | Project to integrate threat modelling into development process. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| thumbcacheviewer | 1.0.3.6 | Extract Windows thumbcache database files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| tiger | 3.2.3 | A security scanner, that checks computer for known problems. Can also use tripwire, aide and chkrootkit. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| tilt | 90.2bc2ef2 | An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| timegen | 0.4 | This program generates a \*.wav file to "send" an own time signal to DCF77 compatible devices. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| tinc | 1.0.36 | VPN (Virtual Private Network) daemon | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tinfoleak | 3.6469eb3 | Get detailed information about a Twitter user activity. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| tinfoleak2 | 41.c45c33e | The most complete open-source tool for Twitter intelligence analysis. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| tinyproxy | 1.10.0 | A light-weight HTTP proxy daemon for POSIX operating systems. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| tls-attacker | 5082.a5e9b78b0 | A Java-based framework for analyzing TLS libraries. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| tls-fingerprinting | 257.4b6e878 | Tool and scripts to perform TLS Fingerprinting. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| tls-prober | 284.4d5c1f2 | A tool to fingerprint SSL/TLS servers. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| tlsenum | 78.787c88b | A command line tool to enumerate TLS cipher-suites supported by a server. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| tlsfuzzer | 1280.309fe03 | SSL and TLS protocol test suite and fuzzer. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| tlspretense | v0.6.2.r22.g0a5faf4 | SSL/TLS client testing framework. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| tlssled | 1.3 | A Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| tnscmd | 1.3 | a lame tool to prod the oracle tnslsnr process (1521/tcp) | [blackarch-misc](http://docs.google.com/misc.html) |  |
| token-reverser | 10.cbb4528 | Word list generator to crack security tokens. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| tomcatwardeployer | 91.a1a4453 | Apache Tomcat auto WAR deployment & pwning penetration testing tool. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| topera | 19.3e230fd | An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| tor | 0.4.5.7 | Anonymizing overlay network. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| tor-autocircuit | 0.2 | Tor Autocircuit was developed to give users a finer control over Tor circuit creation. The tool exposes the functionality of TorCtl library which allows its users to control circuit length, speed, geolocation, and other parameters. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| tor-browser-en | 10.0.15 | Tor Browser Bundle: anonymous browsing using Firefox and Tor. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| tor-router | 4.001a510 | A tool that allow you to make TOR your default gateway and send all internet connections under TOR (as transparent proxy) for increase privacy/anonymity without extra unnecessary code. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| torcrawl | 65.6944a0a | Crawl and extract (regular or onion) webpages through TOR network. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| torctl | 0.5.7 | Script to redirect all traffic through tor network including dns queries for anonymizing entire system. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| torshammer | 1.0 | A slow POST Denial of Service testing tool written in Python. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| torsocks | 2.3.0 | Wrapper to safely torify applications | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| tpcat | latest | Tool based upon pcapdiff by the EFF. It will analyze two packet captures (taken on each side of the firewall as an example) and report any packets that were seen on the source capture but didn’t make it to the dest. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| tplmap | 714.1d63156 | Automatic Server-Side Template Injection Detection and Exploitation Tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| traceroute | 2.1.0 | Tracks the route taken by packets over an IP network | [blackarch-recon](http://docs.google.com/recon.html) |  |
| trape | 126.b2810f7 | People tracker on the Internet: OSINT analysis and research tool by Jose Pino. | [blackarch-social](http://docs.google.com/social.html) |  |
| traxss | 81.48dee2e | Automated XSS Vulnerability Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| treasure | 2.b3249be | Hunt for sensitive information through githubs code search. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| trid | 2.24 | An utility designed to identify file types from their binary signatures. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| trinity | 5167.03f10b67 | A Linux System call fuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| triton | 0.8.1 | A Dynamic Binary Analysis (DBA) framework. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| trivy | 475.0518d27 | A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| trixd00r | 0.0.1 | An advanced and invisible userland backdoor based on TCP/IP for UNIX systems. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| truecrack | 35 | Password cracking for truecrypt(c) volumes. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| truecrypt | 7.1a | Free open-source cross-platform disk encryption software | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| truegaze | 108.ae1d1f7 | Static analysis tool for Android/iOS apps focusing on security issues outside the source code. | [blackarch-mobile](http://docs.google.com/mobile.html) |  |
| truehunter | 14.0a2895d | Detect TrueCrypt containers using a fast and memory efficient approach. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| trufflehog | 199.0f22322 | Searches through git repositories for high entropy strings, digging deep into commit history. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| trusttrees | 102.a9b7399 | A Tool for DNS Delegation Trust Graphing. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| tsh | 0.6 | An open-source UNIX backdoor that compiles on all variants, has full pty support, and uses strong crypto for communication. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| tsh-sctp | 2.850a2da | An open-source UNIX backdoor. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| ttpassgen | 133.a06d99d | Highly flexible and scriptable password dictionary generator based on Python. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| tunna | 41.cba006d | a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| tweets-analyzer | 55.8d6bd3c | Tweets metadata scraper & activity analyzer. | [blackarch-social](http://docs.google.com/social.html) |  |
| tweetshell | 21.47a415c | Multi-thread Twitter BruteForcer in Shell Script. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| twint | 845.e7c8a0c | An advanced Twitter scraping & OSINT tool written in Python that doesn't use Twitter's API, allowing you to scrape a user's followers, following, Tweets and more while evading most API limitations. | [blackarch-social](http://docs.google.com/social.html) |  |
| twofi | 2.0 | Twitter Words of Interest. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| typo-enumerator | 117.7fb4fa0 | Enumerate Typo3 version and extensions. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| tyton | 80.56494f3 | Kernel-Mode Rootkit Hunter. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| u3-pwn | 2.0 | A tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| uacme | 243.1eb514e | Defeating Windows User Account Control. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| uatester | 1.06 | User Agent String Tester | [blackarch-misc](http://docs.google.com/misc.html) |  |
| uberfile | 14.4414c2a | CLI tool for the generation of downloader oneliners for UNIX-like or Windows systems. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ubiquiti-probing | 5.c28f4c1 | A Ubiquiti device discovery tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ubitack | 0.3 | Tool, which automates some of the tasks you might need on a (wireless) penetration test or while you are on the go. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| udis86 | 1.7.2 | A minimalistic disassembler library | [blackarch-reversing](http://docs.google.com/reversing.html) |  |
| udork | 94.5c31877 | Python script that uses advanced Google search techniques to obtain sensitive information in files or directories, find IoT devices, detect versions of web applications. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| udp2raw-tunnel | 20200818.0 | An Encrypted, Anti-Replay, Multiplexed UdP Tunnel, tunnels udp traffic through fake-tcp or icmp by using raw socket | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| udpastcp | 29.683b5e3 | This program hides UDP traffic as TCP traffic in order to bypass certain firewalls. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| udptunnel | 19 | Tunnels TCP over UDP packets. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| udsim | 25.df19f07 | A graphical simulator that can emulate different modules in a vehicle and respond to UDS request. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| uefi-firmware-parser | 170.2af7e41 | Parse BIOS/Intel ME/UEFI firmware related structures: Volumes, FileSystems, Files, etc. | [blackarch-firmware](http://docs.google.com/firmware.html) |  |
| ufo-wardriving | 4 | Allows you to test the security of wireless networks by detecting their passwords based on the router model. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| ufonet | 71.ed3dd2a | A tool designed to launch DDoS attacks against a target, using 'Open Redirect' vectors on third party web applications, like botnet. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| uhoh365 | 26.110277a | Script to enumerate Office 365 users without performing login attempts | [blackarch-recon](http://docs.google.com/recon.html) |  |
| ultimate-facebook-scraper | 236.5661bdc | A bot which scrapes almost everything about a Facebook user's profile. | [blackarch-social](http://docs.google.com/social.html) |  |
| umap | 25.3ad8121 | The USB host security assessment tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| umit | 1.0 | A powerful nmap frontend. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| uncaptcha2 | 7.473f33d | Defeating the latest version of ReCaptcha with 91% accuracy. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| unfurl | 16.99ad735 | Pull out bits of URLs provided on stdin. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| unhide | 20130526 | A forensic tool to find processes hidden by rootkits, LKMs or by other techniques. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| unibrute | 1.b3fb4b7 | Multithreaded SQL union bruteforcer. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| unicorn-powershell | 198.22f94cc | A simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| unicornscan | 0.4.7 | A new information gathering and correlation engine. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| unifuzzer | 5.3385a3b | A fuzzing tool for closed-source binaries based on Unicorn and LibFuzzer. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| uniofuzz | 1337 | The universal fuzzing tool for browsers, web services, files, programs and network services/ports | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| uniscan | 6.3 | A simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| unix-privesc-check | 1.4 | Tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases). | [blackarch-automation](http://docs.google.com/automation.html) |  |
| unsecure | 1.2 | Bruteforces network login masks. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| unstrip | 13.05e00c2 | ELF Unstrip Tool. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| untwister | 119.a42b8f8 | Seed recovery tool for PRNGs. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| upnp-pentest-toolkit | 1.1 | UPnP Pentest Toolkit for Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| upnpscan | 0.4 | Scans the LAN or a given address range for UPnP capable devices. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| uppwn | 9.f69dec4 | A script that automates detection of security flaws on websites' file upload systems'. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| uptux | 33.85ccfd0 | Linux privilege escalation checks (systemd, dbus, socket fun, etc). | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| upx | 3.96 | Extendable, high-performance executable packer for several executable formats | [blackarch-binary](http://docs.google.com/binary.html) |  |
| urh | 2.9.1 | Universal Radio Hacker: investigate wireless protocols like a boss | [blackarch-radio](http://docs.google.com/radio.html) |  |
| urlcrazy | 0.5 | Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| urldigger | 02c | A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| urlextractor | 19.739864d | Information gathering & website reconnaissance. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| urlview | 0.9 | A curses URL parser for text files. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| usb-canary | 31.bb23552 | A Linux or OSX tool that uses psutil to monitor devices while your computer is locked. In the case it detects someone plugging in or unplugging devices it can be configured to send you an SMS or alert you via Slack or Pushover. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| usbrip | 282.77a5f79 | USB device artifacts tracker. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| username-anarchy | 54.d5e653f | Tools for generating usernames when penetration testing. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| usernamer | 20.12983f8 | Pentest Tool to generate usernames/logins based on supplied names. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| userrecon | 10.3b56891 | Find usernames across over 75 social networks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| userrecon-py | 15.eebd422 | Recognition usernames in 187 social networks. | [blackarch-social](http://docs.google.com/social.html) |  |
| usnjrnl2csv | 28.e99844d | Parser for $UsnJrnl on NTFS. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| usnparser | 4.1.4 | A Python script to parse the NTFS USN journal. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| uw-loveimap | 0.1 | Multi threaded imap bounce scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| uw-offish | 0.1 | Clear-text protocol simulator. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| uw-udpscan | 0.1 | Multi threaded udp scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| uw-zone | 0.1 | Multi threaded, randomized IP zoner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| v3n0m | 340.c3ea4e2 | A tool to automate mass SQLi d0rk scans and Metasploit Vulns. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vais | 17.5c35c3a | SWF Vulnerability & Information Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| valabind | 1.8.0 | Tool to parse vala or vapi files to transform them into swig interface files, C++, NodeJS-ffi or GIR | [blackarch-misc](http://docs.google.com/misc.html) |  |
| valgrind | 3.16.1 | Tool to help find memory-management problems in programs | [blackarch-binary](http://docs.google.com/binary.html) |  |
| valhalla | 87.c010a48 | Valhalla API Client. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| vane | 1899.48f9ab5 | A vulnerability scanner which checks the security of WordPress installations using a black box approach. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vanguard | 0.1 | A comprehensive web penetration testing tool written in Perl thatidentifies vulnerabilities in web applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vault-scanner | 299.0303cf4 | Swiss army knife for hackers. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vba2graph | 29.fcf96ef | Generate call graphs from VBA code, for easier analysis of malicious documents. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| vbrute | 1.11dda8b | Virtual hosts brute forcer. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| vbscan | 39.2b1ce48 | A black box vBulletin vulnerability scanner written in perl. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vbsmin | v1.0.0.r25.g5b2fd93 | VBScript minifier. | [blackarch-packer](http://docs.google.com/packer.html) |  |
| vcsmap | 47.3889964 | A plugin-based tool to scan public version control systems for sensitive information. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vega | 1.0 | An open source platform to test the security of web applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| veil | 285.c825577 | A tool designed to generate metasploit payloads that bypass common anti-virus solutions. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| veles | 637.e65de5a | New open source tool for binary data analysis. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| venom | 135.2b84e68 | A Multi-hop Proxy for Penetration Testers. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| veracrypt | 1.24.update7 | Disk encryption with strong security based on TrueCrypt | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| verinice | 1.19.1.r1.gf82b192a6 | Tool for managing information security. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| vfeed | 79.46d8aa9 | Open Source Cross Linked and Aggregated Local Vulnerability Database main repository. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| vhostscan | 338.4a3a1ee | A virtual host scanner that can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| videosnarf | 0.63 | A new security assessment tool for pcap analysis | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vinetto | 0.07beta | A forensics tool to examine Thumbs.db files | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| viper | 2087.92aa4e5 | A Binary analysis framework. | [blackarch-disassembler](http://docs.google.com/disassembler.html) |  |
| vipermonkey | 1160.511ecd5 | A VBA parser and emulation engine to analyze malicious macros. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| viproy-voipkit | 81.427f26e | VoIP Pen-Test Kit for Metasploit Framework | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| virustotal | 4.9aea023 | Command-line utility to automatically lookup on VirusTotal all files recursively contained in a directory. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| visql | 49.3082e30 | Scan SQL vulnerability on target site and sites of on server. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| visualize-logs | 118.d2e370e | A Python library and command line tools to provide interactive log visualization. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| vivisect | 1593.6b214526 | A Python based static analysis and reverse engineering framework. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| vlan-hopping | 21.a37ba4e | Easy 802.1Q VLAN Hopping | [blackarch-automation](http://docs.google.com/automation.html) |  |
| vlany | 255.9ef014a | Linux LD\_PRELOAD rootkit (x86 and x86\_64 architectures). | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| vmap | 0.3 | A Vulnerability-Exploit desktop finder. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| vmcloak | 912.13853ff | Automated Virtual Machine Generation and Cloaking for Cuckoo Sandbox. | [blackarch-malware](http://docs.google.com/malware.html) |  |
| vnak | 1.cf0fda7 | Aim is to be the one tool a user needs to attack multiple VoIP protocols. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| vnc-bypauth | 0.0.1 | Multi-threaded bypass authentication scanner for VNC smaller than v4.1.1 servers. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| vncrack | 1.21 | What it looks like: crack VNC. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| voiper | 0.07 | A VoIP security testing toolkit incorporating several VoIP fuzzers and auxiliary tools to assist the auditor. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| voiphopper | 2.04 | A security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| voipong | 2.0 | A utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| volafox | 143.5b42987 | Mac OS X Memory Analysis Toolkit. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| volatility-extra | 92.d9fc072 | Volatility plugins developed and maintained by the community. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| volatility3 | 1.0.1 | Advanced memory forensics framework | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| voltron | 627.d9fef0b | UI for GDB, LLDB and Vivisect's VDB. | [blackarch-debugger](http://docs.google.com/debugger.html) |  |
| vpnpivot | 22.37bbde0 | Explore the network using this tool. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| vsaudit | 21.2cbc47b | VOIP Security Audit Framework. | [blackarch-voip](http://docs.google.com/voip.html) |  |
| vscan | 10.da4e47e | HTTPS / Vulnerability scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vstt | 0.5.3 | VSTT is a multi-protocol tunneling tool. It accepts input by TCP stream sockets and FIFOs, and can send data via TCP, POP3, and ICMP tunneling. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| vsvbp | 6.241a7ab | Black box tool for Vulnerability detection in web applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vulmap | 95.a167c47 | Vulmap Online Local Vulnerability Scanners Project | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vulnerabilities-spider | 1.426e70f | A tool to scan for web vulnerabilities. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vulnx | 314.e200aa2 | Cms and vulnerabilites detector & An intelligent bot auto shell injector. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| vuls | 1106.e3c27e1 | Vulnerability scanner for Linux/FreeBSD, agentless, written in Go. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| vulscan | 2.0 | A module which enhances nmap to a vulnerability scanner | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| w13scan | 413.cd69357 | Passive Security Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| w3af | 1.6.49 | Web Application Attack and Audit Framework. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| wafninja | 25.379cd98 | A tool which contains two functions to attack Web Application Firewalls. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wafp | 0.01\_26c3 | An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wafpass | 48.c3ea1b9 | Analysing parameters with all payloads' bypass methods, aiming at benchmarking security solutions like WAF. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wafw00f | 816.e3e6147 | Identify and fingerprint Web Application Firewall (WAF) products protecting a website. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| waidps | 16.ff8d270 | Wireless Auditing, Intrusion Detection & Prevention System. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| waldo | 29.ee4f960 | A lightweight and multithreaded directory and subdomain bruteforcer implemented in Python. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| wapiti | 3.0.4 | A vulnerability scanner for web applications. It currently search vulnerabilities like XSS, SQL and XPath injections, file inclusions, command execution, LDAP injections, CRLF injections... | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| wascan | 37.6926338 | Web Application Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wavemon | 0.9.3 | Ncurses-based monitoring application for wireless network devices | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| waybackpack | 56.b6e8ec7 | Download the entire Wayback Machine archive for a given URL. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| waybackurls | 9.58bbafe | Fetch all the URLs that the Wayback Machine knows about for a domain. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| wcc | 55.f141963 | The Witchcraft Compiler Collection. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| wce | 1.41beta | A security tool to list logon sessions and add, change, list and delete associated credentials (ex.: LM/NT hashes, plaintext passwords and Kerberos tickets). | [blackarch-windows](http://docs.google.com/windows.html) |  |
| web-soul | 2 | A plugin based scanner for attacking and data mining web sites written in Perl. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| web2ldap | 1.5.112 | Full-featured LDAP client running as web application. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| webacoo | 0.2.3 | Web Backdoor Cookie Script-Kit. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| webanalyze | 91.4b7ed27 | Port of Wappalyzer (uncovers technologies used on websites) in go to automate scanning. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| webborer | 170.c20d51c | A directory-enumeration tool written in Go. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| webenum | 21.24b43b4 | Tool to enumerate http responses using dynamically generated queries and more. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| webexploitationtool | 155.85bcf0e | A cross platform web exploitation toolkit. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| webfixy | 25.5d477b0 | On-the-fly decryption proxy for MikroTik RouterOS WebFig sessions. | [blackarch-proxy](http://docs.google.com/proxy.html) |  |
| webhandler | 348.1bd971e | A handler for PHP system functions & also an alternative 'netcat' handler. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| webhunter | 12.918b606 | Tool for scanning web applications and networks and easily completing the process of collecting knowledge. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| webkiller | 36.7ad72d3 | Tool Information Gathering Write By Python. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| webpwn3r | 35.3fb27bb | A python based Web Applications Security Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| webrute | 3.3 | Web server directory brute forcer. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| webscarab | 20120422.001828 | Framework for analysing applications that communicate using the HTTP and HTTPS protocols | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| websearch | 3.09935a5 | Search vhost names given a host range. Powered by Bing.. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| webshag | 1.10 | A multi-threaded, multi-platform web server audit tool. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| webshells | 36.ea3a60d | Web Backdoors. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| webslayer | 5 | A tool designed for brute forcing Web Applications. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| websockify | 879.c5d365d | WebSocket to TCP proxy/bridge. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| webspa | 0.8 | A web knocking tool, sending a single HTTP/S to run O/S commands. | [blackarch-backdoor](http://docs.google.com/backdoor.html) |  |
| websploit | 4.0.4 | An Open Source Project For, Social Engineering Works, Scan, Crawler & Analysis Web, Automatic Exploiter, Support Network Attacks | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| webtech | 1.2.8 | Identify technologies used on websites. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| webxploiter | 56.c03fe6b | An OWASP Top 10 Security scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| weebdns | 14.c01c04f | DNS Enumeration with Asynchronicity. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| weeman | 91.53c2efa | HTTP Server for phishing in python. | [blackarch-social](http://docs.google.com/social.html) |  |
| weevely | 880.6332b46 | Weaponized web shell. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| weirdaal | 331.c14e36d | AWS Attack Library. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wepbuster | 1.0\_beta\_0.7 | script for automating aircrack-ng | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wesng | 156.3f3acab | Windows Exploit Suggester - Next Generation. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| wfuzz | 1155.1b695ee | Utility to bruteforce web applications to find their not linked resources. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| whapa | 278.0b7ebc4 | WhatsApp Parser Tool. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| whatbreach | 42.dad6b9f | OSINT tool to find breached emails and databases. | [blackarch-social](http://docs.google.com/social.html) |  |
| whatportis | 48.e8e1665 | A command to search port names and numbers. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| whatsmyname | 663.5f44d5f | Tool to perform user and username enumeration on various websites. | [blackarch-social](http://docs.google.com/social.html) |  |
| whatwaf | 392.b14e866 | Detect and bypass web application firewalls and protection systems. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| whatweb | 4908.eeca4cd3 | Next generation web scanner that identifies what websites are running. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| whichcdn | 22.5fc6ddd | Tool to detect if a given website is protected by a Content Delivery Network. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| whitewidow | 605.4f27bfe | SQL Vulnerability Scanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| wi-feye | 1.1 | An automated wireless penetration testing tool written in python, its designed to simplify common attacks that can be performed on wifi networks so that they can be executed quickly and easily. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifi-autopwner | 36.faa4d01 | Script to automate searching and auditing Wi-Fi networks with weak security. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| wifi-honey | 1.0 | A management tool for wifi honeypots. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| wifi-monitor | 24.33b682e | Prints the IPs on your local network that're sending the most packets. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| wifi-pumpkin | v1.0.8R1.r1.g7aef4d2 | Framework for Rogue Wi-Fi Access Point Attack. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifibroot | 84.d0cd2cc | A WiFi Pentest Cracking tool for WPA/WPA2 (Handshake, PMKID, Cracking, EAPOL, Deauthentication). | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifichannelmonitor | 1.42 | A utility for Windows that captures wifi traffic on the channel you choose, using Microsoft Network Monitor capture driver. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| wificurse | 0.3.9 | WiFi jamming tool. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifijammer | 92.5f69529 | A python script to continuously jam all wifi clients within range. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifiphisher | 787.f0be783 | Fast automated phishing attacks against WPA networks. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifiscanmap | 135.9adcd08 | Another wifi mapping tool. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifitap | 2b16088 | WiFi injection tool through tun/tap device. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wifite | 87.r139.918a499 | Tool to attack multiple WEP and WPA encrypted networks at the same time | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wig | 574.d5ddd91 | WebApp Information Gatherer. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wikigen | 8.348aa99 | A script to generate wordlists out of wikipedia pages. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| wildpwn | 11.4623714 | Unix wildcard attacks. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| windapsearch | 28.7724ec4 | Script to enumerate users, groups and computers from a Windows domain through LDAP queries. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| windivert | 2.2.0 | A user-mode packet capture-and-divert package for Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| windows-binaries | 20.7d272da | A colleciton of pentesting Windows binaries. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| windows-exploit-suggester | 41.776bd91 | This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| windows-prefetch-parser | 81.f593a8c | Parse Windows Prefetch files. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| windows-privesc-check | 181.9f304fd | Standalone Executable to Check for Simple Privilege Escalation Vectors on Windows Systems. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| windowsspyblocker | 4.33.1 | Block spying and tracking on Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| winexe | 1.00 | Remotely execute commands on Windows NT/2000/XP/2003 systems. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| winfo | 2.0 | Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| winhex | 20.0 | Hex Editor and Disk Editor. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| winpwn | 320.86a8568 | Automation for internal Windows Penetrationtest / AD-Security. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| winregfs | 145.6f29498 | Windows Registry FUSE filesystem. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| winrelay | 2.0 | A TCP/UDP forwarder/redirector that works with both IPv4 and IPv6. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| wireless-ids | 24.b132071 | Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wireshark-cli | 3.4.4 | Network traffic and protocol analyzer/sniffer - CLI tools and data files | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| wireshark-qt | 3.4.4 | Network traffic and protocol analyzer/sniffer - Qt GUI | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| wirouter-keyrec | 1.1.2 | A platform independent software to recover the default WPA passphrases of the supported router models | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| witchxtool | 1.1 | A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wlan2eth | 1.3 | Re-writes 802.11 captures into standard Ethernet frames. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wmat | 0.1 | Automatic tool for testing webmail accounts. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| wmd | 30.32e249a | Python framework for IT security tools. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| wmi-forensics | 11.0ab08dc | Scripts used to find evidence in WMI repositories. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| wnmap | 0.1 | A shell script written with the purpose to automate and chain scans via nmap. You can run nmap with a custom mode written by user and create directories for every mode with the xml/nmap files inside. | [blackarch-automation](http://docs.google.com/automation.html) |  |
| wol-e | 2.0 | A suite of tools for the Wake on LAN feature of network attached computers. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| wolpertinger | 2.58ef8e2 | A distributed portscanner. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| wondershaper | 42.b0663cb | Limit the bandwidth of one or more network adapters. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| wordbrutepress | 30.5165648 | Python script that performs brute forcing against WordPress installs using a wordlist. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| wordlistctl | 0.9.1 | Fetch, install and search wordlist archives from websites. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| wordlister | 48.d63f5ab | A simple wordlist generator and mangler written in python. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| wordpot | 44.e96889b | A Wordpress Honeypot. | [blackarch-honeypot](http://docs.google.com/honeypot.html) |  |
| wordpress-exploit-framework | 907.e55ded4 | A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wordpresscan | 72.5558c1a | WPScan rewritten in Python + some WPSeku ideas. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| wpa-bruteforcer | 4.d5f8586 | Attacking WPA/WPA encrypted access point without client. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wpa2-halfhandshake-crack | 29.3f42124 | A POC to show it is possible to capture enough of a handshake with a user from a fake AP to crack a WPA2 network without knowing the passphrase of the actual AP. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wpbf | 7.11b6ac1 | Multithreaded WordPress brute forcer. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| wpbrute-rpc | 3.e7d8145 | Tool for amplified bruteforce attacks on wordpress based website via xmlrcp API. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| wpbullet | 34.6185112 | A static code analysis for WordPress (and PHP). | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| wpforce | 88.b72ec64 | Wordpress Attack Suite. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wpintel | 6.741c0c9 | Chrome extension designed for WordPress Vulnerability Scanning and information gathering. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wpscan | 3.8.16 | Black box WordPress vulnerability scanner | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wpseku | 39.862fb2c | Simple Wordpress Security Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wpsik | 8.8d3856b | WPS scan and pwn tool. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| wpsweep | 1.0 | A simple ping sweeper, that is, it pings a range of IP addresses and lists the ones that reply. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| wreckuests | 75.69b6c27 | Yet another one hard-hitting tool to run DDoS attacks with HTTP-flood. | [blackarch-dos](http://docs.google.com/dos.html) |  |
| ws-attacker | 1.7 | A modular framework for web services penetration testing. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wscript | 201.0410be2 | Emulator/tracer of the Windows Script Host functionality. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| wsfuzzer | 1.9.5 | A Python tool written to automate SOAP pentesting of web services. | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |
| wssip | 75.56d0d2c | Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wsuspect-proxy | 24.89f9375 | A tool for MITM'ing insecure WSUS connections. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| wups | 1.4 | An UDP port scanner for Windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| wuzz | 229.66176b6 | Interactive cli tool for HTTP inspection. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| wxhexeditor | 722.c22ce20 | A free hex editor / disk editor for Linux, Windows and MacOSX. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| wyd | 0.2 | Gets keywords from personal files. IT security/forensic tool. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| x-rsa | 163.f39358f | Contains a many of attack types in RSA such as Hasted, Common Modulus, Chinese Remainder Theorem. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| x-scan | 3.3 | A general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| x64dbg | 2021.04.03 | An open-source x64/x32 debugger for windows. | [blackarch-windows](http://docs.google.com/windows.html) |  |
| xcat | 266.faaf8fe | A command line tool to automate the exploitation of blind XPath injection vulnerabilities. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| xcavator | 5.bd9e2d8 | Man-In-The-Middle and phishing attack tool that steals the victim's credentials of some web services like Facebook. | [blackarch-sniffer](http://docs.google.com/sniffer.html) |  |
| xcname | 11.9c475a1 | A tool for enumerating expired domains in CNAME records. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| xerosploit | 33.2a65f3d | Efficient and advanced man in the middle framework. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| xfltreat | 270.17d4ec8 | Tunnelling framework. | [blackarch-tunnel](http://docs.google.com/tunnel.html) |  |
| xmlrpc-bruteforcer | 35.6023237 | An XMLRPC brute forcer targeting Wordpress written in Python 3. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xorbruteforcer | 0.1 | Script that implements a XOR bruteforcing of a given file, although a specific key can be used too. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| xorsearch | 1.11.4 | Program to search for a given string in an XOR, ROL or ROT encoded binary file. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| xortool | 0.99 | Tool to analyze multi-byte XOR cipher | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| xpire-crossdomain-scanner | 1.0cb8d3b | Scans crossdomain.xml policies for expired domain names. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| xpl-search | 42.d4dbc97 | Search exploits in multiple exploit databases!. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| xplico | 1.2.2 | Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT). | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| xprobe2 | 0.3 | An active OS fingerprinting tool. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| xray | 91.ca50a32 | A tool for recon, mapping and OSINT gathering from public networks. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| xrop | 83.4af7452 | Tool to generate ROP gadgets for ARM, AARCH64, x86, MIPS, PPC, RISCV, SH4 and SPARC. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| xspear | 141.5fe0a29 | Powerful XSS Scanning and Parameter analysis tool&gem. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xspy | 1.0c | A utility for monitoring keypresses on remote X servers | [blackarch-keylogger](http://docs.google.com/keylogger.html) |  |
| xsrfprobe | 523.ce04111 | The Prime Cross Site Request Forgery Audit and Exploitation Toolkit. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xss-freak | 17.e361766 | An XSS scanner fully written in Python3 from scratch. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsscon | 45.ce91fd6 | Simple XSS Scanner tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsscrapy | 143.f6e65c0 | XSS spider - 66/66 wavsep XSS detected. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsser | 1.8 | A penetration testing tool for detecting and exploiting XSS vulnerabilites. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xssless | 45.8e7ebe1 | An automated XSS payload generator written in python. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsspy | 60.b10d336 | Web Application XSS Scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsss | 0.40b | A brute force cross site scripting scanner. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xssscan | 17.7f1ea90 | Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsssniper | 79.02b59af | An automatic XSS discovery tool | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xsstracer | 5.f2ed21a | Python script that checks remote web servers for Clickjacking, Cross-Frame Scripting, Cross-Site Tracing and Host Header Injection. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| xsstrike | 448.0ecedc1 | An advanced XSS detection and exploitation suite. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xssya | 13.cd62817 | A Cross Site Scripting Scanner & Vulnerability Confirmation. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xwaf | 159.cfde8e0 | Automatic WAF bypass tool. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| xxeinjector | 55.604c39a | Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| xxeserv | 12.046c559 | A mini webserver with FTP support for XXE payloads. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| xxexploiter | 88.7576a79 | It generates the XML payloads, and automatically starts a server to serve the needed DTD's or to do data exfiltration. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| yaaf | 7.4d6273a | Yet Another Admin Finder. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| yaf | 2.12.1 | Yet Another Flowmeter. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| yara | 4.0.5 | Tool aimed at helping malware researchers to identify and classify malware samples | [blackarch-malware](http://docs.google.com/malware.html) |  |
| yasat | 848 | Yet Another Stupid Audit Tool. | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| yasca | 2.1 | Multi-Language Static Analysis Toolset. | [blackarch-code-audit](http://docs.google.com/code-audit.html) |  |
| yasuo | 121.994dcb1 | A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| yate-bts | 6.1.0 | An open source GSM Base Station software. | [blackarch-radio](http://docs.google.com/radio.html) |  |
| yawast | 1072.5e9e7a3 | The YAWAST Antecedent Web Application Security Toolkit. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| yay | 10.2.0 | Yet another yogurt. Pacman wrapper and AUR helper written in go. | [blackarch-misc](http://docs.google.com/misc.html) |  |
| ycrawler | 0.1 | A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| yersinia | 0.8.2 | A network tool designed to take advantage of some weakness in different network protocols. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| yeti | 2339.c6bd7246 | A platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| yinjector | 0.1 | A MySQL injection penetration tool. It has multiple features, proxy support, and multiple exploitation methods. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| ysoserial | 0.0.5 | A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization. | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| zackattack | 5.1f96c14 | A new tool set to do NTLM Authentication relaying unlike any other tool currently out there. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| zaproxy | 2.10.0 | Integrated penetration testing tool for finding vulnerabilities in web applications | [blackarch-webapp](http://docs.google.com/webapp.html) |  |
| zarp | 0.1.8 | A network attack tool centered around the exploitation of local networks. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| zdns | 237.8c53210 | Fast CLI DNS Lookup Tool. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| zeek | 11716.0c93e2fcb | A powerful network analysis framework that is much different from the typical IDS you may know. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| zeek-aux | 478.b2ce33b | Handy auxiliary programs related to the use of the Zeek Network Security Monitor. | [blackarch-networking](http://docs.google.com/networking.html) |  |
| zelos | 270.0c5bd57 | A comprehensive binary emulation and instrumentation platform. | [blackarch-binary](http://docs.google.com/binary.html) |  |
| zeratool | 16.157d9fd | Automatic Exploit Generation (AEG) and remote flag capture for exploitable CTF problems. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| zerowine | 0.0.2 | Malware Analysis Tool - research project to dynamically analyze the behavior of malware | [blackarch-malware](http://docs.google.com/malware.html) |  |
| zeus | 111.97db152 | AWS Auditing & Hardening Tool. | [blackarch-defensive](http://docs.google.com/defensive.html) |  |
| zeus-scanner | 414.21b8756 | Advanced dork searching utility. | [blackarch-recon](http://docs.google.com/recon.html) |  |
| zgrab | 803.031475e | Grab banners (optionally over TLS). | [blackarch-recon](http://docs.google.com/recon.html) |  |
| zgrab2 | 552.5e9507c | Go Application Layer Scanner. | [blackarch-fingerprint](http://docs.google.com/fingerprint.html) |  |
| zipdump | 0.0.20 | ZIP dump utility. | [blackarch-forensic](http://docs.google.com/forensic.html) |  |
| zirikatu | 7.afe1d9c | Fud Payload generator script. | [blackarch-exploitation](http://docs.google.com/exploitation.html) |  |
| zizzania | 124.8f2062f | Automated DeAuth attack. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| zmap | 2.1.1 | Fast network scanner designed for Internet-wide network surveys | [blackarch-scanner](http://docs.google.com/scanner.html) |  |
| zssh | 1.5c | SSH and Telnet client with ZMODEM file transfer capability | [blackarch-networking](http://docs.google.com/networking.html) |  |
| zulu | 0.1 | A light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks. | [blackarch-cracker](http://docs.google.com/cracker.html) |  |
| zulucrypt | 6.0.0 | Front end to cryptsetup and tcplay and it allows easy management of encrypted block devices. | [blackarch-crypto](http://docs.google.com/crypto.html) |  |
| zykeys | 0.1 | Demonstrates how default wireless settings are derived on some models of ZyXEL routers. | [blackarch-wireless](http://docs.google.com/wireless.html) |  |
| zzuf | 0.15 | Transparent application input fuzzer | [blackarch-fuzzer](http://docs.google.com/fuzzer.html) |  |

BlackArch Linux 2013-2021