‹ ›

Over 2900 tools

Tools

Hacking Tools List

Home (index.html) / 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: 2905 ()

Input tool name

BlackArch Linux Complete Tools List

Name	**Description**	**Website**
0d1n	Web security tool to make fuzzing at HTTP inputs, made in C with libCurl.	(https://github.com/CoolerVoid/0d1n)
0trace	A hop enumeration tool.	(http://jon.oberheide.org/0trace/)
3proxy	Tiny free proxy server.	(https://github.com/3proxy/3proxy)
3proxy-win32	Tiny free proxy server.	(http://3proxy.ru/)
42zip	Recursive Zip archive bomb.	(http://blog.fefe.de/?ts=b6cea88d)
a2sv	Auto Scanning to SSL Vulnerability.	(https://github.com/hahwul/a2sv)
abcd	ActionScript ByteCode Disassembler.	(https://github.com/MITRECND/abcd)

Name	Description	Website
abuse-ssl-bypass-waf	Bypassing WAF by abusing SSL/TLS Ciphers.	↗ (https://github.com/LandGrey/abuse-ssl-bypass-waf)
acccheck	A password dictionary attack tool that targets windows authentication via the SMB protocol.	↗ (http://labs.portcullis.co.uk/tools/acccheck/)
ace	Automated Corporate Enumerator. A simple yet powerful VoIP Corporate Directory enumeration tool that mimics the behavior of an IP Phone in order to download the name and extension entries that a given phone can display on its screen interface	↗ (http://ucsniff.sourceforge.net/ace.html)
aclpwn	Active Directory ACL exploitation with BloodHound.	↗ (https://github.com/fox-it/aclpwn.py)
activedirectoryenum	Enumerate AD through LDAP.	↗ (https://github.com/CasperGN/ActiveDirectoryEnumeration)
ad-ldap-enum	An LDAP based Active Directory user and group enumeration tool.	↗ (https://github.com/CroweCybersecurity/ad-ldap-enum)
ad-miner	Active Directory audit tool that extract data from Bloodhound to uncover security weaknesses and generate an HTML report	↗ (https://github.com/Mazars-Tech/AD_Miner)
adape-script	Active Directory Assessment and Privilege Escalation Script.	↗ (https://github.com/hausec/ADAPE-Script)
adenum	A pentesting tool that allows to find misconfiguration through the the protocol LDAP and exploit some of those weaknesses with kerberos.	↗ (https://github.com/SecuProject/ADenum)
adfind	Simple admin panel finder for php,js,cgi,asp and aspx admin panels.	↗ (https://github.com/sahakkhotsanyan/adfind)
adfspray	Python3 tool to perform password spraying against Microsoft Online service using various methods.	↗ (https://github.com/xFreed0m/ADFSpray)
adidnsdump	Active Directory Integrated DNS dumping by any authenticated user.	↗ (https://github.com/dirkjanm/adidnsdump)
admid-pack	ADM DNS spoofing tools - Uses a variety of active and passive methods to spoof DNS packets. Very powerful.	↗ (http://packetstormsecurity.com/files/10080/ADMid-pkg.tgz.html)
adminpagefinder	This python script looks for a large amount of possible administrative interfaces on a given site.	↗ (http://packetstormsecurity.com/files/112855/Admin-Page-Finder-Script.html)
admsnmp	ADM SNMP audit scanner.	↗ ()
aesfix	A tool to find AES key in RAM.	↗ (http://citp.princeton.edu/memory/code/)
aeskeyfind	A tool to find AES key in RAM.	↗ (http://citp.princeton.edu/memory/code/)
aespipe	Reads data from stdin and outputs encrypted or decrypted results to stdout.	↗ (http://loop-aes.sourceforge.net/aespipe/)
aesshell	A backconnect shell for Windows and Unix written in python and uses AES in CBC mode in conjunction with HMAC-SHA256 for secure transport.	↗ (https://packetstormsecurity.com/files/132438/AESshell.7.html)
afflib	An extensible open format for the storage of disk images and related forensic information.	↗ (https://github.com/sshock/AFFLIBv3)
afl++	instrumentation-driven fuzzer for binary format	↗ (https://aflplus.plus/)
afpfs-ng	A client for the Apple Filing Protocol (AFP)	↗ (http://alexthepuffin.googlepages.com/)
agafi	A gadget finder and a ROP-Chainer tool for x86 platforms.	↗ (https://github.com/CoreSecurity/Agafi)
against	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.	↗ (http://nullsecurity.net/tools/cracker.html)
aggroargs	Bruteforce commandline buffer overflows, linux, aggressive arguments.	↗ (https://github.com/tintinweb/aggroArgs)
aiengine	A packet inspection engine with capabilities of learning without any human intervention.	↗ (https://bitbucket.org/camp0/aiengine/downloads/)
aimage	A program to create aff-images.	↗ (http://www.afflib.org)
aiodnsbrute	Python 3 DNS asynchronous brute force utility.	↗ (https://github.com/blark/aiodnsbrute)
air	A GUI front-end to dd/dc3dd designed for easily creating forensic images.	↗ (https://sourceforge.net/projects/air-imager/)
aircrack-ng	Key cracker for the 802.11 WEP and WPA-PSK protocols	↗ (https://www.aircrack-ng.org)
airflood	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]	↗ (http://packetstormsecurity.com/files/51127/airflood.1.tar.gz.html)
airgeddon	Multi-use bash script for Linux systems to audit wireless networks.	↗ (https://github.com/v1s1t0r1sh3r3/airgeddon)
airopy	Get (wireless) clients and access points.	↗ (https://github.com/Josue87/Airopy)
airoscript	A script to simplify the use of aircrack-ng tools.	↗ (http://midnightresearch.com/projects/wicrawl/)
airpwn	A tool for generic packet injection on an 802.11 network.	↗ (http://airpwn.sourceforge.net)
ajpfuzzer	A command-line fuzzer for the Apache JServ Protocol (ajp13).	↗ (https://github.com/doyensec/ajpfuzzer)
albatar	A SQLi exploitation framework in Python.	↗ (https://github.com/lanjelot/albatar)
allthevhosts	A vhost discovery tool that scrapes various web applications.	↗ (http://labs.portcullis.co.uk/tools/finding-all-the-vhosts/)
altdns	Generates permutations, alterations and mutations of subdomains and then resolves them.	↗ (https://github.com/infosec-au/altdns)
amass	In-depth subdomain enumeration written in Go.	↗ (https://github.com/OWASP/Amass)
amber	Reflective PE packer.	↗ (https://github.com/EgeBalci/Amber)
amoco	Yet another tool for analysing binaries.	↗ (https://github.com/bdcht/amoco)
analyzemft	Parse the MFT file from an NTFS filesystem.	↗ (https://github.com/dkovar/analyzeMFT)
analyzepesig	Analyze digital signature of PE file.	↗ (https://blog.didierstevens.com/my-software/#AnalyzePESig)
androbugs	An efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications.	↗ (https://github.com/AndroBugs/AndroBugs_Framework)
androguard	Reverse engineering, Malware and goodware analysis of Android applications and more.	↗ (https://github.com/androguard/androguard)
androick	A python tool to help in forensics analysis on android.	↗ (https://github.com/Flo354/Androick)
android-apktool	A tool for reverse engineering Android apk files.	↗ (https://github.com/iBotPeaches/Apktool/releases)
android-ndk	Android C/C++ developer kit	↗ (https://developer.android.com/sdk/ndk/index.html)
android-sdk	Google Android SDK	↗ (https://developer.android.com/studio/releases/sdk-tools.html)
android-udev-rules	Android udev rules.	↗ (https://github.com/bbqlinux/android-udev-rules)
androidpincrack	Bruteforce the Android Passcode given the hash and salt.	↗ (https://github.com/PentesterES/AndroidPINCrack)
androidsniffer	A perl script that lets you search for 3rd party passwords, dump the call log, dump contacts, dump wireless configuration, and more.	↗ (http://packetstormsecurity.com/files/97464/Andr01d-Magic-Dumper.1.html)
androwarn	Yet another static code analyzer for malicious Android applications.	↗ (https://github.com/maaaaz/androwarn)
angr	The next-generation binary analysis platform from UC Santa Barbaras Seclab.	↗ (https://pypi.org/project/angr/#files)
angr-management	This is the GUI for angr.	↗ (https://pypi.org/project/angr-management/#files)

Name	Description	Website
angr-py2	The next-generation binary analysis platform from UC Santa Barbaras Seclab.	(https://pypi.org/project/angr/#files)
angrop	A rop gadget finder and chain builder.	(https://github.com/salls/angrop)
anontwi	A free software python client designed to navigate anonymously on social networks. It supports Identi.ca and Twitter.com.	(http://anontwi.sourceforge.net/)
anti-xss	A XSS vulnerability scanner.	(https://github.com/lewangbtcc/anti-XSS)
antiransom	A tool capable of detect and stop attacks of Ransomware using honeypots.	(http://www.security-projects.com/?Anti_Ransom___Download)
anubis	Subdomain enumeration and information gathering tool.	(https://github.com/jonluca/anubis)
apache-users	This perl script will enumerate the usernames on a unix system that use the apache module UserDir.	(https://labs.portcullis.co.uk/downloads/)
apachetomcatscanner	Apache Tomcat vulnerability scanner.	(https://github.com/p0dalirius/ApacheTomcatScanner)
apacket	Sniffer syn and backscatter packets.	(https://github.com/Acey9/apacket)
aphopper	A program that automatically hops between access points of different wireless networks.	(http://aphopper.sourceforge.net/)
apkid	Android Application Identifier for Packers, Protectors, Obfuscators and Oddities.	(https://github.com/rednaga/APKiD)
apkleaks	Scanning APK file for URIs, endpoints & secrets.	(https://github.com/dwisiswant0/apkleaks)
apkstat	Automated Information Retrieval From APKs For Initial Analysis.	(https://github.com/hexabin/APKStat)
apkstudio	An IDE for decompiling/editing & then recompiling of android application binaries.	(http://www.vaibhavpandey.com/apkstudio/)
apkurlgrep	Extract endpoints from APK files.	(https://github.com/ndelphit/apkurlgrep)
apnbf	A small python script designed for enumerating valid APNs (Access Point Name) on a GTP-C speaking device.	(http://www.c0decafe.de/)
appmon	A runtime security testing & profiling framework for native apps on macOS, iOS & android and it is built using Frida.	(https://github.com/dpnishant/appmon)
apt2	Automated penetration toolkit.	(https://github.com/MooseDojo/apt2)
aquatone	A Tool for Domain Flyovers.	(https://github.com/shelld3v/aquatone)
arachni	A feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications.	(https://www.arachni-scanner.com)
aranea	A fast and clean dns spoofing tool.	(https://github.com/TigerSecurity)
arcane	Backdoor iOS packages and create the necessary resources for APT repositories.	(https://github.com/tokyoneon/Arcane)
archivebox	The open source self-hosted web archive. Takes browser history/bookmarks/Pocket/Pinboard/etc., saves HTML, JS, PDFs, media, and more.	(https://github.com/pirate/ArchiveBox)
ares	Automated decoding of encrypted text without knowing the key or ciphers used.	(https://github.com/bee-san/Ares)
argon2	A password-hashing function (reference C implementation)	(https://github.com/P-H-C/phc-winner-argon2)
argus	Network monitoring tool with flow control.	(http://qosient.com/argus/)
argus-clients	Network monitoring client for Argus.	(http://qosient.com/argus/)
arjun	HTTP parameter discovery suite.	(https://github.com/s0md3v/Arjun)
armitage	A graphical cyber attack management tool for Metasploit.	(http://www.fastandeasyhacking.com/)
armor	A simple Bash script designed to create encrypted macOS payloads capable of evading antivirus scanners.	(https://github.com/tokyoneon/Armor)
armscgen	ARM Shellcode Generator (Mostly Thumb Mode).	(https://github.com/alexpark07/ARMSCGen)
arp-scan	A tool that uses ARP to discover and fingerprint IP hosts on the local network	(https://github.com/royhills/arp-scan)
arpalert	Monitor ARP changes in ethernet networks.	(http://www.arpalert.org/)
arpoison	The UNIX arp cache update utility	(http://www.arpoison.net)
arpon	A portable handler daemon that make ARP protocol secure in order to avoid the Man In The Middle (MITM) attack through ARP Spoofing, ARP Cache Poisoning or ARP Poison Routing (APR) attacks.	(http://arpon.sourceforge.net/)
arpstraw	Arp spoof detection tool.	(https://github.com/he2ss/arpstraw)
arptools	A simple tool about ARP broadcast, ARP attack, and data transmission.	(https://github.com/Lab-Zjt/ARPTools)
arpwner	GUI-based python tool for arp poisoning and dns poisoning attacks.	(https://github.com/ntrippar/ARPwner)
artillery	A combination of a honeypot, file-system monitoring, system hardening, and overall health of a server to create a comprehensive way to secure a system.	(https://www.trustedsec.com/downloads/artillery/)
artlas	Apache Real Time Logs Analyzer System.	(https://github.com/mthbernardes/ARTLAS)
arybo	Manipulation, canonicalization and identification of mixed boolean-arithmetic symbolic expressions.	(https://github.com/quarkslab/arybo)
asleap	Actively recover LEAP/PPTP passwords.	(http://www.willhackforsushi.com/Asleap.html)
asnmap	Map organization network ranges using ASN information.	(https://github.com/projectdiscovery/asnmap)
asp-audit	An ASP fingerprinting tool and vulnerability scanner.	(http://seclists.org/basics/2006/Sep/128)
assetfinder	Find domains and subdomains potentially related to a given domain.	(https://github.com/tomnomnom/assetfinder)
astra	Automated Security Testing For REST API's.	(https://github.com/flipkart-incubator/astra)
atear	Wireless Hacking, WiFi Security, Vulnerability Analyzer, Pentestration.	(https://github.com/NORMA-Inc/AtEar)
atftp	Client/server implementation of the TFTP protocol that implements RFCs 1350, 2090, 2347, 2348, and 2349	(https://sourceforge.net/projects/atftp/)
athena-ssl-scanner	A SSL cipher scanner that checks all cipher codes. It can identify about 150 different ciphers.	(http://packetstormsecurity.com/files/93062/Athena-SSL-Cipher-Scanner.html)
atlas	Open source tool that can suggest sqlmap tampers to bypass WAF/IDS/IPS.	(https://github.com/m4ll0k/Atlas)
atscan	Server, Site and Dork Scanner.	(https://github.com/AlisamTechnology/ATSCAN-V3.1)
atstaketools	This is an archive of various @Stake tools that help perform vulnerability scanning and analysis, information gathering, password auditing, and forensics.	(http://packetstormsecurity.com/files/50718/AtStakeTools.zip.html)
attacksurfacemapper	Tool that aims to automate the reconnaissance process.	(https://github.com/superhedgy/AttackSurfaceMapper)
attk	Trend Micro Anti-Threat Toolkit.	(https://spnsupport.trendmicro.com/)
aurebeshjs	Translate JavaScript to Other Alphabets.	(https://github.com/aemkei/aurebesh.js)
auto-eap	Automated Brute-Force Login Attacks Against EAP Networks.	(https://github.com/Tylous/Auto_EAP)
auto-xor-decryptor	Automatic XOR decryptor tool.	(https://github.com/MRGEffitas/scripts)
automato	Should help with automating some of the user-focused enumeration tasks during an internal penetration test.	(https://github.com/skahwah/automato)
autonessus	This script communicates with the Nessus API in an attempt to help with automating scans.	(https://github.com/redteamsecurity/AutoNessus)
autonse	Massive NSE (Nmap Scripting Engine) AutoSploit and AutoScanner.	(https://github.com/m4ll0k/AutoNSE)

Name	Description	Website
autopsy	The forensic browser. A GUI for the Sleuth Kit.	(https://github.com/sleuthkit/autopsy)
autopwn	Specify targets and run sets of tools against them.	(https://github.com/nccgroup/autopwn)
autorecon	A multi-threaded network reconnaissance tool which performs automated enumeration of services.	(https://github.com/Tib3rius/AutoRecon)
autosint	Tool to automate common osint tasks.	(https://github.com/bharshbarger/AutOSINT)
autosploit	Automate the exploitation of remote hosts.	(https://github.com/NullArray/AutoSploit)
autovpn	Easily connect to a VPN in a country of your choice.	(https://github.com/adtac/autovpn)
avaloniailspy	.NET Decompiler (port of ILSpy)	(https://github.com/icsharpcode/AvaloniaILSpy)
avet	AntiVirus Evasion Tool	(https://github.com/govolution/avet)
avml	A portable volatile memory acquisition tool for Linux.	(https://github.com/microsoft/avml)
aws-extender-cli	Script to test S3 buckets as well as Google Storage buckets and Azure Storage containers for common misconfiguration issues.	(https://github.com/VirtueSecurity/aws-extender-cli)
aws-iam-privesc	AWS IAM policy scanner that helps determine where privilege escalation can be achieved.	(https://github.com/cyberqueenmeg/aws_iam_privesc)
aws-inventory	Discover resources created in an AWS account.	(https://github.com/nccgroup/aws-inventory)
awsbucketdump	A tool to quickly enumerate AWS S3 buckets to look for loot.	(https://github.com/jordanpotti/AWSBucketDump)
azazel	A userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit.	(https://github.com/chokepoint/azazel)
aztarna	A footprinting tool for ROS and SROS systems.	(https://github.com/aliasrobotics/aztarna)
backcookie	Small backdoor using cookie.	(https://github.com/mrjopino/backcookie)
backdoor-apk	Shell script that simplifies the process of adding a backdoor to any Android APK file	(https://github.com/dana-at-cp/backdoor-apk)
backdoor-factory	Patch win32/64 binaries with shellcode.	(https://github.com/secretsquirrel/the-backdoor-factory)
backdoorme	A powerful utility capable of backdooring Unix machines with a slew of backdoors.	(https://github.com/Kkevsterrr/backdoorme)
backdoorppt	Transform your payload.exe into one fake word doc (.ppt).	(https://github.com/r00txp10it/backdoorppt)
backfuzz	A network protocol fuzzing toolkit.	(https://github.com/localh0t/backfuzz)
backhack	Tool to perform Android app analysis by backing up and extracting apps, allowing you to analyze and modify file system contents for apps.	(https://github.com/l0gan/backHack)
backoori	Tool aided persistence via Windows URI schemes abuse.	(https://github.com/giuliocomi/backoori)
backorifice	A remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application.	(http://www.cultdeadcow.com/tools/bo.html)
bad-pdf	Steal NTLM Hashes with Bad-PDF.	(https://github.com/deepzec/Bad-Pdf)
badkarma	Advanced network reconnaissance toolkit.	(https://github.com/r3vn/badKarma)
badministration	A tool which interfaces with management or administration applications from an offensive standpoint.	(https://github.com/ThunderGunExpress/BADministration)
bagbak	Yet another frida based App decryptor.	(https://github.com/ChiChou/bagbak)
balbuzard	A package of malware analysis tools in python to extract patterns of interest from suspicious files (IP addresses, domain names, known file headers, interesting strings, etc).	(https://bitbucket.org/decalage/balbuzard/)
bamf-framework	A modular framework designed to be a platform to launch attacks against botnets.	(https://github.com/bwall/BAMF)
bandicoot	A toolbox to analyze mobile phone metadata.	(https://pypi.org/project/bandicoot/#files)
bandit	Python security linter from OpenStack Security	(https://github.com/PyCQA/bandit)
barf	A multiplatform open source Binary Analysis and Reverse engineering Framework.	(https://github.com/programa-stic/barf-project)
barmie	Java RMI enumeration and attack tool.	(https://github.com/NickstaDB/BaRMIe)
barq	An AWS Cloud Post Exploitation framework.	(https://github.com/Voulnet/barq)
base64dump	Extract and decode base64 strings from files.	(https://blog.didierstevens.com/my-software/#base64dump)
basedomainname	Tool that can extract TLD (Top Level Domain), domain extensions (Second Level Domain + TLD), domain name, and hostname from fully qualified domain names.	(http://www.morningstarsecurity.com/research)
bashfuscator	Fully configurable and extendable Bash obfuscation framework.	(https://github.com/Bashfuscator/Bashfuscator)
bashscan	A port scanner built to utilize /dev/tcp for network and service discovery.	(https://github.com/astryzia/BashScan)
batctl	B.A.T.M.A.N. advanced control and management tool	(http://www.open-mesh.net/)
batman-adv	Batman kernel module, (included upstream since .38)	(http://www.open-mesh.net/)
batman-alfred	Almighty Lightweight Fact Remote Exchange Daemon.	(http://www.open-mesh.org/)
bbqsql	SQL injection exploit tool.	(https://github.com/neohapsis/bbqsql)
bbscan	A tiny Batch web vulnerability Scanner.	(https://github.com/lijiejie/bbscan)
bdfproxy	Patch Binaries via MITM: BackdoorFactory + mitmProxy	(https://github.com/secretsquirrel/BDFProxy)
bdlogparser	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.	(http://magikh0e.xyz/)
bed	Collection of scripts to test for buffer overflows, format string vulnerabilities.	(http://www.aldeid.com/wiki/Bed)
beebug	A tool for checking exploitability.	(https://github.com/invictus1306/beebug)
beef	The Browser Exploitation Framework that focuses on the web browser.	(http://beefproject.com/)
beeswarm	Honeypot deployment made easy http://www.beeswarm-ids.org/	(https://github.com/honeynet/beeswarm/)
beholder	A wireless intrusion detection tool that looks for anomalies in a wifi environment.	(http://www.beholderwireless.org/)
belati	The Traditional Swiss Army Knife for OSINT.	(https://github.com/aancw/Belati)
beleth	A Multi-threaded Dictionary based SSH cracker.	(https://github.com/chokepoint/Beleth)
bettercap	Swiss army knife for network attacks and monitoring	(https://github.com/bettercap/bettercap)
bettercap-ui	Official Bettercap's Web UI.	(https://github.com/bettercap/ui)
bfac	An automated tool that checks for backup artifacts that may disclose the web-application's source code.	(https://github.com/mazen160/bfac)
bfbtester	Performs checks of single and multiple argument command line overflows and environment variable overflows	(http://sourceforge.net/projects/bfbtester/)
bfuzz	Input based fuzzer tool for browsers.	(https://github.com/RootUp/BFuzz)
bgp-md5crack	RFC2385 password cracker	(http://www.c0decafe.de/)
bgrep	Binary grep.	(https://github.com/tmbinc/bgrep)
billcipher	Information Gathering tool for a Website or IP address.	(https://github.com/GitHackTools/BillCipher)
binaryninja-demo	A new kind of reversing platform (demo version).	(http://binary.ninja/demo.html)
binaryninja-python	Binary Ninja prototype written in Python.	(https://github.com/Vector35/binaryninja-python)

Name	Description	Website
bind	A complete, highly portable implementation of the DNS protocol	(https://www.isc.org/software/bind/)
bindead	A static analysis tool for binaries	(https://bitbucket.org/mihaila/bindead)
bindiff	A comparison tool for binary files, that assists vulnerability researchers and engineers to quickly find differences and similarities in disassembled code.	(http://www.zynamics.com/bindiff.html)
binex	Format String exploit building tool.	(http://www.morxploit.com/morxtool)
binflow	POSIX function tracing. Much better and faster than ftrace.	(https://github.com/elfmaster/binflow)
bing-ip2hosts	Enumerates all hostnames which Bing has indexed for a specific IP address.	(http://www.morningstarsecurity.com/research/bing-ip2hosts)
bing-lfi-rfi	Python script for searching Bing for sites that may have local and remote file inclusion vulnerabilities.	(http://packetstormsecurity.com/files/121590/Bing-LFI-RFI-Scanner.html)
bingoo	A Linux bash based Bing and Google Dorking Tool.	(https://github.com/Hood3dRob1n/BinGoo)
binnavi	A binary analysis IDE that allows to inspect, navigate, edit and annotate control flow graphs and call graphs of disassembled code.	(https://github.com/google/binnavi)
binproxy	A proxy for arbitrary TCP connections.	(https://github.com/nccgroup/BinProxy/)
binwalk	Tool for searching a given binary image for embedded files	(https://github.com/OSPG/binwalk)
binwally	Binary and Directory tree comparison tool using the Fuzzy Hashing concept (ssdeep).	(https://github.com/bmaia/binwally)
bios_memimage	A tool to dump RAM contents to disk (aka cold boot attack).	(http://citp.princeton.edu/memory/code/)
birp	A tool that will assist in the security assessment of mainframe applications served over TN3270.	(https://github.com/sensepost/birp)
bitdump	A tool to extract database data from a blind SQL injection vulnerability.	(https://github.com/nbshelton/bitdump)
bittwist	A simple yet powerful libpcap-based Ethernet packet generator. It is designed to complement tcpdump, which by itself has done a great job at capturing network traffic.	(http://bittwist.sourceforge.net/)
bkcrack	Crack legacy zip encryption with Biham and Kocher known plaintext attack.	(https://github.com/kimci86/bkcrack)
bkhive	Program for dumping the syskey bootkey from a Windows NT/2K/XP system hive.	(http://sourceforge.net/projects/ophcrack)
blackbox-scanner	Dork scanner & bruteforcing & hash cracker with blackbox framework.	(https://github.com/sepehrdaddev/blackbox)
blackeye	Ultimate phishing tool with ngrok and serveo.	(https://github.com/Git-Ankitraj/blackeye-im)
blackhash	Creates a filter from system hashes.	(http://16s.us/blackhash/)
blacknurse	A low bandwidth ICMP attack that is capable of doing denial of service to well known firewalls.	(https://github.com/jedisct1/blacknurse)
bleah	A BLE scanner for "smart" devices hacking.	(https://github.com/evilsocket/bleah)
bless	High-quality, full-featured hex editor	(https://github.com/afrantzis/bless)
bletchley	A collection of practical application cryptanalysis tools.	(https://code.google.com/p/bletchley/)
blind-sql-bitshifting	A blind SQL injection module that uses bitshfting to calculate characters.	(https://github.com/libeclipse/blind-sql-bitshifting)
blindelephant	A web application fingerprinter. Attempts to discover the version of a (known) web application by comparing static files at known locations	(http://blindelephant.sourceforge.net/)
blindsql	Set of bash scripts for blind SQL injection attacks.	(http://www.enye-sec.org/programas.html)
blindy	Simple script to automate brutforcing blind sql injection vulnerabilities.	(https://github.com/missDronio/blindy)
blisqy	Exploit Time-based blind-SQL injection in HTTP-Headers (MySQL/MariaDB).	(https://github.com/JohnTroony/Blisqy)
bloodhound	Six Degrees of Domain Admin	(https://github.com/BloodHoundAD/BloodHound)
bloodhound-python	Bloodhound python data collector	(https://github.com/fox-it/BloodHound.py)
bloodyad	An Active Directory Privilege Escalation Framework.	(https://github.com/CravateRouge/bloodyAD)
blue-hydra	A Bluetooth device discovery service built on top of the bluez library.	(https://github.com/pwnieexpress/blue_hydra)
bluebox-ng	A GPL VoIP/UC vulnerability scanner.	(https://github.com/jesusprubio/bluebox-ng)
bluebugger	An implementation of the bluebug technique which was discovered by Martin Herfurt.	(http://packetstormsecurity.com/files/54024/bluebugger.1.tar.gz.html)
bluediving	A Bluetooth penetration testing suite.	(http://bluediving.sourceforge.net/)
bluefog	A tool that can generate an essentially unlimited number of phantom Bluetooth devices.	()
bluelog	A Bluetooth scanner and sniffer written to do a single task, log devices that are in discoverable mode.	(http://www.digifail.com/software/bluelog.shtml)
bluepot	A Bluetooth Honeypot written in Java, it runs on Linux.	(https://github.com/andrewmichaelsmith/bluepot)
blueprint	A perl tool to identify Bluetooth devices.	(https://trifinite.org/trifinite_stuff_blueprinting.html)
blueranger	A simple Bash script which uses Link Quality to locate Bluetooth device radios.	(http://www.hackfromacave.com/projects/blueranger.html)
bluescan	A Bluetooth Device Scanner.	(http://www.darknet.org.uk/2015/01/bluescan-bluetooth-device-scanner/)
bluesnarfer	A bluetooth attacking tool.	(http://www.alighieri.org/project.html)
bluffy	Convert shellcode into different formats.	(https://github.com/ad/bluffy)
bluphish	Bluetooth device and service discovery tool that can be used for security assessment and penetration testing.	(https://github.com/olivo/BluPhish)
bluto	Recon, Subdomain Bruting, Zone Transfers.	(https://github.com/RandomStorm/Bluto)
bmap-tools	Tool for copying largely sparse files using information from a block map file.	(http://git.infradead.org/users/dedekind/bmap-tools.git)
bmc-tools	RDP Bitmap Cache parser.	(https://github.com/ANSSI-FR/bmc-tools)
bob-the-butcher	A distributed password cracker package.	(http://btb.banquise.net/)
bof-detector	A simple detector of BOF vulnerabilities by source-code-level check.	(https://github.com/st9140927/BOF_Detector)
bonesi	The DDoS Botnet Simulator.	(https://github.com/Markus-Go/bonesi)
boofuzz		(https://github.com/jtpereyda/boofuzz)
boopsuite	A Suite of Tools written in Python for wireless auditing and security testing.	(https://github.com/M1ND-B3ND3R/BoopSuite)
bopscrk	Tool to generate smart wordlists, eg. based on lyrics.	(https://github.com/R3nt0n/bopscrk)
botb	A container analysis and exploitation tool for pentesters and engineers.	(https://github.com/brompwnie/botb)
bowcaster	A framework intended to aid those developing exploits.	(https://github.com/zcutlip/bowcaster)
box-js	A tool for studying JavaScript malware.	(https://github.com/CapacitorSet/box-js)
bqm	Download BloudHound query lists, deduplicate entries and merge them in one file.	(https://github.com/Acceis/bqm)
braa	A mass snmp scanner	(http://s-tech.elsat.net.pl/braa/)
braces	A Bluetooth Tracking Utility.	(http://braces.shmoo.com/)
brakeman	A static analysis security vulnerability scanner for Ruby on Rails applications.	(https://brakemanscanner.org/)

Name	Description	Website
bridgekeeper	Scrape employee names from search engine LinkedIn profiles. Convert employee names to a specified username format.	(https://github.com/0xZDH/BridgeKeeper)
brosec	An interactive reference tool to help security professionals utilize useful payloads and commands.	(https://github.com/gabemarshall/Brosec)
browselist	Retrieves the browse list ; the output list contains computer names, and the roles they play in the network.	(http://ntsecurity.nu/toolbox/browselist/)
browser-fuzzer	Browser Fuzzer 3	(http://www.krakowlabs.com/dev.html)
brute-force	Brute-Force attack tool for Gmail Hotmail Twitter Facebook Netflix.	(https://github.com/Matrix07ksa/Brute_Force)
brute12	A tool designed for auditing the cryptography container security in PKCS12 format.	(http://www.security-projects.com/?Brute12)
bruteforce-luks	Try to find the password of a LUKS encrypted volume.	(https://github.com/glv2/bruteforce-luks)
bruteforce-salted-openssl	Try to find the password of a file that was encrypted with the 'openssl' command.	(https://github.com/glv2/bruteforce-salted-openssl)
bruteforce-wallet	Try to find the password of an encrypted Peercoin (or Bitcoin,Litecoin, etc...) wallet file.	(https://github.com/glv2/bruteforce-wallet)
brutemap	Penetration testing tool that automates testing accounts to the site's login page.	(https://github.com/brutemap-dev/brutemap)
brutespray	Brute-Forcing from Nmap output - Automatically attempts default creds on found services.	(https://github.com/x90skysn3k/brutespray)
brutessh	A simple sshd password bruteforcer using a wordlist, it's very fast for internal networks. It's multithreads.	(http://www.edge-security.com/edge-soft.php)
brutex	Automatically brute force all services running on a target.	(https://github.com/1N3/BruteX)
brutexss	Cross-Site Scripting Bruteforcer.	(https://github.com/shawarkhanethicalhacker/BruteXSS)
brutus	One of the fastest, most flexible remote password crackers you can get your hands on.	(http://www.hoobie.net/brutus/)
bsdiff	Tools for building and applying patches to binary files.	(https://www.daemonology.net/bsdiff/)
bsqlbf	Blind SQL Injection Brute Forcer.	(http://code.google.com/p/bsqlbf-v2/)
bsqlinjector	Blind SQL injection exploitation tool written in ruby.	(https://github.com/enjoiz/BSQLinjector)
bss	Bluetooth stack smasher / fuzzer.	(http://www.secuobs.com/news/15022006-bss_0_8.shtml)
bt_audit	Bluetooth audit	(http://www.betaversion.net/btdsd/download/)
btcrack	The world's first Bluetooth Pass phrase (PIN) bruteforce tool. Bruteforces the Passkey and the Link key from captured Pairing exchanges.	(http://www.nruns.com/_en/security_tools_btcrack.php)
btlejack	Bluetooth Low Energy Swiss-army knife.	(https://github.com/virtualabs/btlejack)
btproxy-mitm	Man in the Middle analysis tool for Bluetooth.	(https://github.com/conorpp/btproxy)
btscanner	Bluetooth device scanner.	(http://www.pentest.co.uk)
bulk-extractor	Bulk Email and URL extraction tool.	(https://github.com/simsong/bulk_extractor)
bully	Retrieve WPA/WPA2 passphrase from a WPS enabled access point	(https://github.com/kimocoder/bully)
bunny	A closed loop, high-performance, general purpose protocol-blind fuzzer for C programs.	(https://code.google.com/p/bunny-the-fuzzer/)
burpsuite	An integrated platform for attacking web applications (community edition) + SHELLING plugin.	(https://portswigger.net/burp/releases)
buster	Find emails of a person and return info associated with them.	(https://github.com/sham00n/buster)
buttinsky	Provide an open source framework for automated botnet monitoring.	(https://github.com/buttinsky/buttinsky)
bvi	A display-oriented editor for binary files operate like "vi" editor.	(http://bvi.sourceforge.net/)
byepass	Automates password cracking tasks using optimized dictionaries and mangling rules.	(https://github.com/webpwnized/byepass)
bypass-firewall-dns-history	Firewall bypass script based on DNS history records.	(https://github.com/vincentcox/bypass-firewalls-by-DNS-history)
bytecode-viewer	A Java 8/Android APK Reverse Engineering Suite.	(https://github.com/Konloch/bytecode-viewer)
c5scan	Vulnerability scanner and information gatherer for the Concrete5 CMS.	(https://github.com/auraltension/c5scan)
c7decrypt	Cisco password type encryptor and decryptor.	(https://github.com/claudijd/c7decrypt)
cachedump	A tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH).	(https://packetstormsecurity.com/files/36781/cachedump.1.zip.html)
cadaver	Command-line WebDAV client for Unix	(https://notroj.github.io/cadaver/)
cafebabe	Java bytecode editor & decompiler.	(https://grax.info/)
cameradar	Hacks its way into RTSP videosurveillance cameras.	(https://github.com/Ullaakut/cameradar)
camover	A camera exploitation tool that allows to disclosure network camera admin password.	(https://github.com/EntySec/camover)
camscan	A tool which will analyze the CAM table of Cisco switches to look for anamolies.	(https://github.com/securestate/camscan)
can-utils	Linux-CAN / SocketCAN user space applications.	(https://github.com/linux-can/can-utils)
canalyzat0r	Security analysis toolkit for proprietary car protocols.	(https://github.com/schutzwerk/CANalyzat0r)
canari	Maltego rapid transform development and execution framework.	(https://pypi.org/project/canari/#files)
cangibrina	Dashboard Finder.	(https://github.com/fnk0c/cangibrina)
cansina	A python-based Web Content Discovery Tool.	(https://github.com/deibit/cansina)
cantoolz	Framework for black-box CAN network analysis.	(https://github.com/CANToolz/CANToolz)
capfuzz	Capture, fuzz and intercept web traffic.	(https://github.com/MobSF/CapFuzz)
capstone	Lightweight multi-platform, multi-architecture disassembly framework	(https://www.capstone-engine.org/index.html)
captipper	Malicious HTTP traffic explorer tool.	(http://www.omriher.com/2015/01/captipper-malicious-http-traffic.html)
cardpwn	OSINT Tool to find Breached Credit Cards Information.	(https://github.com/itsmehacker/CardPwn)
cariddi	Take a list of domains, crawl urls and scan for endpoints, secrets, api keys, file extensions, token.	(https://github.com/edoardottt/cariddi)
carwhisperer	Intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys.	(http://trifinite.org/trifinite_stuff_carwhisperer.html)
casefile	The little brother to Maltego without transforms, but combines graph and link analysis to examine links between manually added data to mind map your information	(http://www.paterva.com/web6/products/casefile.php)
catana	Filter your wordlist according to the specified password policy.	(https://github.com/D3vil0p3r/catana)
catnthecanary	An application to query the canary.pw data set for leaked data.	(https://github.com/packetassailant/catnthecanary)
catphish	For phishing and corporate espionage.	(https://github.com/ring0lab/catphish)
ccrawldns	Retrieves from the CommonCrawl data set unique subdomains for a given domain name.	(https://github.com/lgandx/CCrawlDNS)
cdpsnarf	Cisco discovery protocol sniffer.	(https://github.com/Zapotek/cdpsnarf)

Name	Description	Website
cecster	A tool to perform security testing against the HDMI CEC (Consumer Electronics Control) and HEC (HDMI Ethernet Channel) protocols.	(https://github.com/nccgroup/CECster)
cent	Community edition nuclei templates.	(https://github.com/xm1k3/cent)
centry	Cold boot & DMA protection	(https://github.com/0xPoly/Centry)
cero	Scrape domain names from SSL certificates of arbitrary hosts.	(https://github.com/glebarez/cero)
certgraph	Crawl the graph of certificate Alternate Names.	(https://github.com/lanrat/certgraph)
certipy	Active Directory Certificate Services enumeration and abuse.	(https://github.com/ly4k/Certipy)
certsync	Dump NTDS remotely without DRSUAPI: using golden certificate and UnPAC the hash.	(https://github.com/zblurx/certsync)
cewl	A custom word list generator.	(http://www.digininja.org/projects/cewl.php)
cflow	A C program flow analyzer.	(http://www.gnu.org/software/cflow/)
cfr	Another Java decompiler	(https://www.benf.org/other/cfr/)
chainsaw	A powerful 'first-response' capability to quickly identify threats within Windows event logs.	(https://github.com/countercept/chainsaw)
chameleon	A tool for evading Proxy categorisation.	(https://github.com/mdsecactivebreach/Chameleon)
chameleonmini	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.	(https://github.com/emsec/ChameleonMini)
changeme	A default credential scanner.	(https://github.com/ztgrace/changeme)
chankro	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).	(https://github.com/TarlogicSecurity/Chankro)
chaos-client	Go client to communicate with Chaos dataset API.	(https://github.com/projectdiscovery/chaos-client)
chaosmap	An information gathering tool and dns / whois / web server scanner	(http://freecode.com/projects/chaosmap)
chaosreader	A freeware tool to trace tcp, udp etc. sessions and fetch application data from snoop or tcpdump logs.	(http://chaosreader.sourceforge.net/)
chapcrack	A tool for parsing and decrypting MS-CHAPv2 network handshakes.	(https://github.com/moxie0/chapcrack)
cheat-sh	The only cheat sheet you need.	(https://cheat.sh)
check-weak-dh-ssh	Debian OpenSSL weak client Diffie-Hellman Exchange checker.	(http://packetstormsecurity.com/files/66683/check_weak_dh_ssh.pl.bz2.html)
checkiban	Checks the validity of an International Bank Account Number (IBAN).	(http://kernel.embedromix.ro/us/)
checkov	Prevent cloud misconfigurations and find vulnerabilities during build-time in infrastructure as code, container images and open source packages.	(https://github.com/bridgecrewio/checkov)
checksec	Tool designed to test which standard Linux OS and PaX security features are being used	(https://github.com/slimm609/checksec.sh)
chiasm-shell	Python-based interactive assembler/disassembler CLI, powered byKeystone/Capstone.	(https://github.com/0xbc/chiasm-shell)
chipsec	Platform Security Assessment Framework.	(https://github.com/chipsec/chipsec)
chiron	An all-in-one IPv6 Penetration Testing Framework.	(http://www.secfu.net/tools-scripts/)
chisel	A fast TCP tunnel over HTTP.	(https://github.com/jpillora/chisel)
chkrootkit	Checks for rootkits on a system.	(http://www.chkrootkit.org/)
chntpw	Offline NT Password Editor - reset passwords in a Windows NT SAM user database file	(https://pogostick.net/~pnh/ntpasswd/)
chopshop	Protocol Analysis/Decoder Framework.	(https://github.com/MITRECND/chopshop)
choronzon	An evolutionary knowledge-based fuzzer.	(https://github.com/CENSUS/choronzon)
chownat	Allows two peers behind two separate NATs with no port forwarding and no DMZ setup on their routers to directly communicate with each other	(http://samy.pl/chownat/)
chrome-decode	Chrome web browser decoder tool that demonstrates recovering passwords.	(http://packetstormsecurity.com/files/119153/Chrome-Web-Browser-Decoder.html)
chromefreak	A Cross-Platform Forensic Framework for Google Chrome	(http://osandamalith.github.io/ChromeFreak/)
chromensics	A Google chrome forensics tool.	(https://sourceforge.net/projects/chromensics/)
chw00t	Unices chroot breaking tool.	(https://github.com/earthquake/chw00t)
cidr2range	Script for listing the IP addresses contained in a CIDR netblock.	(http://www.cpan.org/authors/id/R/RA/RAYNERLUC)
cintruder	An automatic pentesting tool to bypass captchas.	(https://github.com/epsylon/cintruder)
cipherscan	A very simple way to find out which SSL ciphersuites are supported by a target.	(https://github.com/jvehent/cipherscan)
ciphertest	A better SSL cipher checker using gnutls.	(https://github.com/OpenSecurityResearch/ciphertest)
ciphr	A CLI tool for encoding, decoding, encryption, decryption, and hashing streams of data.	(https://github.com/frohoff/ciphr)
cirt-fuzzer	A simple TCP/UDP protocol fuzzer.	(http://www.cirt.dk/)
cisco-auditing-tool	Perl script which scans cisco routers for common vulnerabilities. Checks for default passwords, easily guessable community names, and the IOS history bug. Includes support for plugins and scanning multiple hosts.	(http://www.scrypt.net)
cisco-global-exploiter	A perl script that targets multiple vulnerabilities in the Cisco Internetwork Operating System (IOS) and Catalyst products.	(http://www.blackangels.it)
cisco-ocs	Cisco Router Default Password Scanner.	(http://www.question-defense.com/2013/01/11/ocs-version-2-release-ocs-cisco-router-default-password-scanner)
cisco-router-config	Tools to copy and merge Cisco Routers Configuration.	()
cisco-scanner	Multithreaded Cisco HTTP vulnerability scanner. Tested on Linux, OpenBSD and Solaris.	(http://wayreth.eu.org/old_page/)
cisco-snmp-enumeration	Automated Cisco SNMP Enumeration, Brute Force, Configuration Download and Password Cracking.	(https://github.com/nccgroup/cisco-snmp-enumeration)
cisco-snmp-slap	IP address spoofing tool in order to bypass an ACL protecting an SNMP service on Cisco IOS devices.	(https://github.com/nccgroup/cisco-snmp-slap)
cisco-torch	Cisco Torch mass scanning, fingerprinting, and exploitation tool.	(https://github.com/foreni-packages/cisco-torch/)
cisco5crack	Crypt and decrypt the cisco enable 5 passwords.	(https://github.com/madrisan/cisco5crack)
cisco7crack	Crypt and decrypt the cisco enable 7 passwords.	(https://github.com/madrisan/cisco7crack)
ciscos	Scans class A, B, and C networks for cisco routers which have telnet open and have not changed the default password from cisco.	()
citadel	A library of OSINT tools.	(https://github.com/jakecreps/Citadel)
cjexploiter	Drag and Drop ClickJacking exploit development assistance tool.	(https://github.com/enddo/CJExploiter)
clair	Vulnerability Static Analysis for Containers.	(https://github.com/quay/clair)
clairvoyance	Obtain GraphQL API Schema even if the introspection is not enabled.	(https://github.com/nikitastupin/clairvoyance)

Name	Description	Website
clamscanlogparser	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.	(http://magikh0e.xyz/)
clash	A rule based proxy in Go	(https://github.com/Dreamacro/clash)
climber	Check UNIX/Linux systems for privilege escalation.	(https://github.com/raffaele-forte/climber)
cloakify	Data Exfiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of Analysts; Evade AV Detection.	(https://github.com/trycatchhcf/cloakify)
cloud-buster	A tool that checks Cloudflare enabled sites for origin IP leaks.	(https://github.com/SageHack/cloud-buster)
cloudfail	Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network.	(https://github.com/m0rtem/CloudFail)
cloudflare-enum	Cloudflare DNS Enumeration Tool for Pentesters.	(https://github.com/mandatoryprogrammer/cloudflare_enum)
cloudget	Python script to bypass cloudflare from command line. Built upon cfscrape module.	(https://github.com/eudemonics/cloudget)
cloudlist	A tool for listing Assets from multiple Cloud Providers.	(https://github.com/projectdiscovery/cloudlist)
cloudmare	A simple tool to find origin servers of websites protected by CloudFlare with a misconfiguration DNS.	(https://github.com/MrH0wl/Cloudmare)
cloudsploit	AWS security scanning checks.	(https://github.com/cloudsploit/scans)
cloudunflare	Reconnaissance Real IP address for Cloudflare Bypass.	(https://github.com/greycatz/CloudUnflare)
clusterd	Automates the fingerprinting, reconnaissance, and exploitation phases of an application server attack.	(https://github.com/hatRiot/clusterd)
cminer	A tool for enumerating the code caves in PE files.	(https://github.com/EgeBalci/Cminer/)
cmospwd	Decrypts password stored in CMOS used to access BIOS setup.	(http://www.cgsecurity.org/wiki/CmosPwd)
cms-explorer	Designed to reveal the specific modules, plugins, components and themes that various cms driven websites are running.	(https://github.com/FlorianHeigl/cms-explorer)
cms-few	Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python.	(http://packetstormsecurity.com/files/64722/cms_few.py.txt.html)
cmseek	CMS (Content Management Systems) Detection and Exploitation suite.	(https://github.com/Tuhinshubhra/CMSeeK)
cmsfuzz	Fuzzer for wordpress, cold fusion, drupal, joomla, and phpnuke.	(https://github.com/nahamsec/CMSFuzz)
cmsmap	A python open source Content Management System scanner that automates the process of detecting security flaws of the most popular CMSs.	(https://www.dionach.com/blog/cmsmap-%E2%80%93-a-simple-cms-vulnerability-scanner)
cmsscan	CMS scanner to identify and find vulnerabilities for Wordpress, Drupal, Joomla, vBulletin.	(https://github.com/ajinabraham/CMSScan)
cmsscanner	CMS Scanner Framework.	(https://github.com/wpscanteam/CMSScanner)
cnamulator	A phone CNAM lookup utility using the OpenCNAM API.	(https://github.com/packetassailant/cnamulator)
cntlm	An NTLM, NTLM2SR, and NTLMv2 authenticating HTTP proxy.	(https://github.com/bseb/cntlm)
codeql	The CLI tool for GitHub CodeQL	(https://github.com/codeql)
codetective	A tool to determine the crypto/encoding algorithm used according to traces of its representation.	(https://www.digitalloft.org/init/plugin_wiki/page/codetective)
coercer	Coerce a Windows server to authenticate on an arbitrary machine through 15 methods.	(https://github.com/p0dalirius/Coercer)
comission	WhiteBox CMS analysis.	(https://github.com/Intrinsec/comission)
commentor	Extract all comments from the specified URL resource.	(https://github.com/D3vil0p3r/comMENTOR)
commix	Automated All-in-One OS Command Injection and Exploitation Tool.	(https://github.com/commixproject/commix)
commonspeak	Leverages publicly available datasets from Google BigQuery to generate wordlists.	(https://github.com/assetnote/commonspeak2)
complemento	A collection of tools for pentester: LetDown is a powerful tcp flooder ReverseRaider is a domain scanner that use wordlist scanning or reverse resolution scanning Httsquash is an http server scanner, banner grabber and data retriever	(http://complemento.sourceforge.net)
compp	Company Passwords Profiler helps making a bruteforce wordlist for a targeted company.	(https://github.com/sec-it/ComPP)
configpush	This is a tool to span /8-sized networks quickly sending snmpset requests with default or otherwise specified community string to Cisco devices.	(http://packetstormsecurity.com/files/126621/Config-Push-snmpset-Utility.html)
conpass	Password spraying in AD environment avoing account locking.	(https://github.com/login-securite/conpass)
conpot	ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting industrial control systems.	(https://pypi.org/project/Conpot/)
conscan	A blackbox vulnerability scanner for the Concre5 CMS.	(http://nullsecurity.net/tools/scanner.html)
cook	Easily create word's permutation and combination to generate complex wordlists and passwords.	(https://github.com/giteshnxtlvl/cook)
cookie-cadger	An auditing tool for Wi-Fi or wired Ethernet connections.	(https://cookiecadger.com/)
corkscrew	A tool for tunneling SSH through HTTP proxies	(https://github.com/patpadgett/corkscrew)
corscanner	Fast CORS misconfiguration vulnerabilities scanner.	(https://github.com/chenjj/CORScanner)
corstest	A simple CORS misconfigurations checker.	(https://github.com/RUB-NDS/CORStest)
corsy	CORS Misconfiguration Scanner.	(https://github.com/s0md3v/Corsy)
cottontail	Capture all RabbitMQ messages being sent through a broker.	(https://github.com/QKaiser/cottontail)
cowpatty	Wireless WPA/WPA2 PSK handshake cracking utility	(https://github.com/joswr1ght/cowpatty)
cpfinder	Simple script that looks for administrative web interfaces.	(http://packetstormsecurity.com/files/118851/Control-Panel-Finder-Script.html)
cpp2il	A tool to reverse unity's IL2PP toolchain	(https://github.com/SamboyCoding/Cpp2IL)
cppcheck	A tool for static C/C++ code analysis	(http://cppcheck.sourceforge.net/)
cpptest	A portable and powerful, yet simple, unit testing framework for handling automated tests in C++.	(https://github.com/cpptest/cpptest/releases)
cr3dov3r	Search for public leaks for email addresses + check creds against 16 websites.	(https://github.com/D4Vinci/Cr3dOv3r)
crabstick	Automatic remote/local file inclusion vulnerability analysis and exploit tool.	(https://github.com/Hack-Hut/CrabStick)
cracken	A ast password wordlist generator, Smartlist creation and password hybrid-mask analysis tool written in pure safe Rust.	(https://github.com/shmuelamar/cracken)
crackhor	A Password cracking utility.	(https://github.com/CoalfireLabs/crackHOR)
crackle	Crack and decrypt BLE encryption.	(https://github.com/mikeryan/crackle/)
crackmapexec	A swiss army knife for pentesting Windows/Active Directory environments.	(https://github.com/Porchetta-Industries/CrackMapExec)
crackmapexec-pingcastle	NetExec & CrackMapExec module that execute PingCastle on a remote machine.	(https://github.com/TRIKKSS/CrackMapExec-PingCastle)
crackpkcs12	A multithreaded program to crack PKCS#12 files (p12 and pfx extensions).	(https://github.com/crackpkcs12/crackpkcs12)

Name	Description	Website
crackq	Hashcrack.org GPU-accelerated password cracker.	(https://github.com/vnik5287/Crackq)
crackql	GraphQL password brute-force and fuzzing utility	(https://github.com/nicholasaleks/CrackQL)
crackserver	An XMLRPC server for password cracking.	(https://github.com/averagesecurityguy/crack)
crawlic	Web recon tool (find temporary files, parse robots.txt, search folders, google dorks and search domains hosted on same server).	(https://github.com/Ganapati/Crawlic)
creak	Poison, reset, spoof, redirect MITM script.	(https://github.com/codepr/creak)
create_ap	A shell script to create a NATed/Bridged Software Access Point.	(https://github.com/oblique/create_ap)
creddump	A python tool to extract various credentials and secrets from Windows registry hives.	(https://github.com/moyix/creddump)
credmap	The Credential mapper - Tool that was created to bring awareness to the dangers of credential reuse.	(https://github.com/lightos/credmap)
credmaster	Refactored & improved CredKing password spraying tool, uses FireProx APIs to rotate IP addresses, stay anonymous, and beat throttling.	(https://github.com/knavesec/CredMaster)
creds	Harvest FTP/POP/IMAP/HTTP/IRC credentials along with interesting data from each of the protocols.	(https://github.com/DanMcInerney/creds.py)
credsniper	Phishing framework written with the Python micro-framework Flask and Jinja2 templating which supports capturing 2FA tokens.	(https://github.com/ustayready/CredSniper)
creepy	A geolocation information gatherer. Offers geolocation information gathering through social networking platforms.	(http://github.com/ilektrojohn/creepy.git)
cribdrag	An interactive crib dragging tool for cryptanalysis on ciphertext generated with reused or predictable stream cipher keys.	(https://github.com/SpiderLabs/cribdrag)
crlf-injector	A python script for testing CRLF injecting issues.	(https://github.com/rudSarkar/crlf-injector)
crlfuzz	A fast tool to scan CRLF vulnerability written in Go.	(https://github.com/dwisiswant0/crlfuzz)
crosslinked	LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping.	(https://github.com/m8r0wn/crosslinked)
crosstool-ng	A versatile (cross-)toolchain generator	(https://crosstool-ng.github.io/)
crowbar	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.	(https://github.com/galkan/crowbar)
crozono	A modular framework designed to automate the penetration testing of wireless networks from drones and such unconventional devices.	(https://github.com/crozono/crozono-free)
crunch	A wordlist generator for all combinations/permutations of a given character set.	(http://sourceforge.net/projects/crunch-wordlist/)
crypthook	TCP/UDP symmetric encryption tunnel wrapper.	(https://github.com/chokepoint/CryptHook)
cryptohazemultiforcer	High performance multihash brute forcer with CUDA support.	(http://www.cryptohaze.com/multiforcer.php)
cryptonark	SSL security checker.	(http://blog.techstacks.com/cryptonark.html)
csrftester	The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws.	(http://www.owasp.org/index.php/Category:OWASP_CSRFTester_Project)
ct-exposer	An OSINT tool that discovers sub-domains by searching Certificate Transparency logs.	(https://github.com/chris408/ct-exposer)
ctf-party	A CLI tool & library to enhance and speed up script/exploit writing for CTF players.	(https://noraj.github.io/ctf-party/)
ctunnel	Tunnel and/or proxy TCP or UDP connections via a cryptographic tunnel.	(http://nardcore.org/ctunnel)
ctypes-sh	Allows you to call routines in shared libraries from within bash.	(https://github.com/taviso/ctypes.sh)
cuckoo	Automated malware analysis system.	(http://cuckoosandbox.org/)
cudahashcat	Worlds fastest WPA cracker with dictionary mutation engine.	(http://hashcat.net/oclhashcat/)
cupp	Common User Password Profiler	(http://www.remote-exploit.org/?page_id=418)
cutycapt	A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page.	(http://cutycapt.sourceforge.net/)
cve-api	Unofficial api for cve.mitre.org.	(https://github.com/Beyarz/Cve-api)
cve-search	A tool to perform local searches for known vulnerabilities.	(http://cve-search.github.io/cve-search)
cvechecker	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.	(https://github.com/sjvermeu/cvechecker)
cvemap	CLI tool designed to provide a structured and easily navigable interface to various vulnerability databases.	(https://github.com/projectdiscovery/cvemap)
cybercrowl	A Python Web path scanner tool.	(https://github.com/chamli/CyberCrowl)
cyberscan	A Network Pentesting Tool	(https://github.com/medbenali/CyberScan)
cymothoa	A stealth backdooring tool, that inject backdoor's shellcode into an existing process.	(http://cymothoa.sourceforge.net/)
d-tect	Pentesting the Modern Web.	(https://github.com/shawarkhanethicalhacker/D-TECT)
dagon	Advanced Hash Manipulation.	(https://github.com/Ekultek/Dagon)
dalfox	Parameter Analysis and XSS Scanning tool.	(https://github.com/hahwul/dalfox)
damm	Differential Analysis of Malware in Memory.	(https://github.com/504ensicsLabs/DAMM)
daredevil	A tool to perform (higher-order) correlation power analysis attacks (CPA).	(https://github.com/SideChannelMarvels/Daredevil)
dark-dork-searcher	Dark-Dork Searcher.	(http://rafale.org/~mattoufoutu/darkc0de.com/c0de/c/)
darkarmour	Store and execute an encrypted windows binary from inside memory, without a single bit touching disk.	(https://github.com/bats3c/darkarmour)
darkbing	A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection.	(http://packetstormsecurity.com/files/111510/darkBing-SQL-Scanner.1.html)
darkd0rk3r	Python script that performs dork searching and searches for local file inclusion and SQL injection errors.	(http://packetstormsecurity.com/files/117403/Dark-D0rk3r.0.html)
darkdump	Search The Deep Web Straight From Your Terminal.	(https://github.com/josh0xA/darkdump)
darkjumper	This tool will try to find every website that host at the same server at your target.	(http://sourceforge.net/projects/darkjumper/)
darkmysqli	Multi-Purpose MySQL Injection Tool	(https://github.com/BlackArch/darkmysqli)
darkscrape	OSINT Tool For Scraping Dark Websites.	(https://github.com/itsmehacker/DarkScrape)
darkspiritz	A penetration testing framework for Linux, MacOS, and Windows systems.	(https://github.com/M4cs/DarkSpiritz)
darkstat	Network statistics gatherer (packet sniffer)	(https://unix4lyfe.org/darkstat/)
datajackproxy	A proxy which allows you to intercept TLS traffic in native x86 applications across platform.	(https://github.com/nccgroup/DatajackProxy)
datasploit	Performs automated OSINT and more.	(https://github.com/upgoingstar/datasploit)
davoset	A tool for using Abuse of Functionality and XML External Entities vulnerabilities on some websites to attack other websites.	(http://websecurity.com.ua/davoset/)

Name	Description	Website
davscan	Fingerprints servers, finds exploits, scans WebDAV.	(https://github.com/Graph-X/davscan)
davtest	Tests WebDAV enabled servers by uploading test executable files, and then (optionally) uploading files which allow for command execution or other actions directly on the target.	(http://code.google.com/p/davtest/)
dawnscanner	A static analysis security scanner for ruby written web applications.	(https://github.com/thesp0nge/dawnscanner)
dbd	A Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32.	(https://github.com/gitdurandal/dbd)
dbpwaudit	A Java tool that allows you to perform online audits of password quality for several database engines.	(http://www.cqure.net/wp/dbpwaudit/)
dbusmap	Simple utility for enumerating D-Bus endpoints, an nmap for D-Bus.	(https://github.com/taviso/dbusmap)
dc3dd	A patched version of dd that includes a number of features useful for computer forensics.	(http://sourceforge.net/projects/dc3dd)
dcdetector	Spot all domain controllers in a Microsoft Active Directory environment. Find computer name, FQDN, and IP address(es) of all DCs.	(https://github.com/noraj/DCDetector)
dcfldd	DCFL (DoD Computer Forensics Lab) dd replacement with hashing.	(https://github.com/resurrecting-open-source-projects/dcfldd/)
dcrawl	Simple, but smart, multi-threaded web crawler for randomly gathering huge lists of unique domain names.	(https://github.com/kgretzky/dcrawl)
ddosify	High-performance load testing tool, written in Golang.	(https://github.com/ddosify/ddosify)
ddrescue	GNU data recovery tool	(https://www.gnu.org/software/ddrescue/ddrescue.html)
de4dot	.NET deobfuscator and unpacker.	(https://github.com/0xd4d/de4dot/)
deathstar	Automate getting Domain Admin using Empire.	(https://github.com/byt3bl33d3r/DeathStar)
debinject	Inject malicious code into *.debs.	(https://github.com/UndeadSec/Debinject)
deblaze	Performs method enumeration and interrogation against flash remoting end points.	(https://github.com/SpiderLabs/deblaze)
decodify	Tool that can detect and decode encoded strings, recursively.	(https://github.com/UltimateHackers/Decodify)
deen	Generic data encoding/decoding application built with PyQt5.	(https://github.com/takeshixx/deen)
deepce	Docker Enumeration, Escalation of Privileges and Container Escapes.	(https://github.com/stealthcopter/deepce)
delldrac	DellDRAC and Dell Chassis Discovery and Brute Forcer.	(https://www.trustedsec.com/september/owning-dell-drac-awesome-hack/)
delorean	NTP Main-in-the-Middle tool.	(https://github.com/PentesterES/Delorean)
demiguise	HTA encryption tool for RedTeams.	(https://github.com/nccgroup/demiguise)
densityscout	Calculates density for files of any file-system-path to finally output an accordingly descending ordered list.	(https://www.cert.at/en/downloads/software/software-densityscout)
depant	Check network for services with default passwords.	(http://midnightresearch.com/projects/depant/)
depdep	A merciless sentinel which will seek sensitive files containing critical info leaking through your network.	(https://github.com/galkan/depdep)
dependency-check	A tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies.	(https://github.com/jeremylong/DependencyCheck/releases/)
depix	A tool for recovering passwords from pixelized screenshots.	(https://github.com/beurtschipper/Depix)
der-ascii	A reversible DER and BER pretty-printer.	(https://github.com/google/der-ascii)
det	(extensible) Data Exfiltration Toolkit.	(https://github.com/sensepost/det)
detect-it-easy	A program for determining types of files.	(https://github.com/horsicq/DIE-engine/releases)
detect-secrets	An enterprise friendly way of detecting and preventing secrets in code.	(https://github.com/Yelp/detect-secrets)
detect-sniffer	Tool that detects sniffers in the network.	(https://github.com/galkan/tools/tree/master/detect_sniffer)
detectem	Detect software and its version on websites.	(https://github.com/spectresearch/detectem)
devaudit	An open-source, cross-platform, multi-purpose security auditing tool targeted at developers and teams.	(https://github.com/sonatype-nexus-community/DevAudit)
device-pharmer	Opens 1K+ IPs or Shodan search results and attempts to login.	(https://github.com/DanMcInerney/device-pharmer)
dex2jar	A tool for converting Android's .dex format to Java's .class format	(http://code.google.com/p/dex2jar)
dexpatcher	Modify Android DEX/APK files at source-level using Java.	(https://github.com/DexPatcher/dexpatcher-tool)
dff-scanner	Tool for finding path of predictable resource locations.	(http://netsec.rs/70/tools.html)
dfir-ntfs	An NTFS parser for digital forensics & incident response.	(https://github.com/msuhanov/dfir_ntfs)
dftimewolf	Framework for orchestrating forensic collection, processing and data export.	(https://github.com/log2timeline/dftimewolf)
dga-detection	DGA Domain Detection using Bigram Frequency Analysis.	(https://github.com/philarkwright/DGA-Detection)
dharma	Generation-based, context-free grammar fuzzer.	(https://github.com/MozillaSecurity/dharma)
dhcdrop	Remove illegal dhcp servers with IP-pool underflow.	(http://www.netpatch.ru/dhcdrop.html)
dhcpf	Passive DHCP fingerprinting implementation.	(https://github.com/elceef/dhcpf)
dhcpig	Enhanced DHCPv4 and DHCPv6 exhaustion and fuzzing script written in python using scapy network library.	(https://github.com/kamorin/DHCPig)
dhcpoptinj	DHCP option injector.	(https://github.com/misje/dhcpoptinj)
didier-stevens-suite	Didier Stevens Suite.	(https://github.com/DidierStevens/DidierStevensSuite)
dinouml	A network simulation tool, based on UML (User Mode Linux) that can simulate big Linux networks on a single PC	(http://kernel.embedromix.ro/us/)
dirb	A web content scanner, brute forceing for hidden files.	(http://dirb.sourceforge.net/)
dirble	Fast directory scanning and scraping tool.	(https://github.com/nccgroup/dirble)
dirbuster	An application designed to brute force directories and files names on web/application servers	(http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
dirbuster-ng	C CLI implementation of the Java dirbuster tool.	(https://github.com/digination/dirbuster-ng)
directorytraversalscan	Detect directory traversal vulnerabilities in HTTP servers and web applications.	(http://sourceforge.net/projects/httpdirscan/)
dirhunt	Find web directories without bruteforce.	(https://github.com/hahwul/dirhunt)
dirscanner	This is a python script that scans webservers looking for administrative directories, php shells, and more.	(http://packetstormsecurity.com/files/117773/Directory-Scanner-Tool.html)
dirscraper	OSINT Scanning tool which discovers and maps directories found in javascript files hosted on a website.	(https://github.com/Cillian-Collins/dirscraper)
dirsearch	HTTP(S) directory/file brute forcer.	(https://github.com/maurosoria/dirsearch)
dirstalk	Modern alternative to dirbuster/dirb.	(https://github.com/stefanoj3/dirstalk)

Name	Description	Website
disitool	Tool to work with Windows executables digital signatures.	(https://blog.didierstevens.com/my-software/#disitool)
dislocker	Read BitLocker encrypted volumes under Linux.	(http://www.hsc.fr/ressources/outils/dislocker)
dissector	This code dissects the internal data structures in ELF files. It supports x86 and x86_64 archs and runs under Linux.	(http://packetstormsecurity.com/files/125972/Coloured-ELF-File-Dissector.html)
distorm	Powerful disassembler library for x86/AMD64	(https://github.com/gdabah/distorm)
dive	A tool for exploring layers in a docker image	(https://github.com/wagoodman/dive)
dizzy	A Python based fuzzing framework with many features.	(http://www.c0decafe.de/)
dkmc	Dont kill my cat - Malicious payload evasion tool.	(https://github.com/Mr-Un1k0d3r/DKMC)
dmde	Disk Editor and Data Recovery Software.	(https://dmde.com/download.html)
dmg2img	A CLI tool to uncompress Apple's compressed DMG files to the HFS+ IMG format.	(http://vu1tur.eu.org/tools/)
dmitry	Deepmagic Information Gathering Tool.	(http://www.mor-pah.net/)
dnmap	The distributed nmap framework.	(http://sourceforge.net/projects/dnmap/)
dns-parallel-prober	PoC for an adaptive parallelised DNS prober.	(https://github.com/lorenzog/dns-parallel-prober)
dns-reverse-proxy	A reverse DNS proxy written in Go.	(https://github.com/StalkR/dns-reverse-proxy)
dns-spoof	Yet another DNS spoof utility.	(https://github.com/maurotfilho/dns-spoof)
dns2geoip	A simple python script that brute forces DNS and subsequently geolocates the found subdomains.	(http://packetstormsecurity.com/files/118036/DNS-GeoIP.html)
dns2tcp	A tool for relaying TCP connections over DNS.	(http://www.hsc.fr/ressources/outils/dns2tcp/index.html.en)
dnsa	A dns security swiss army knife.	(http://packetfactory.openwall.net/projects/dnsa/index.html)
dnsbf	Search for available domain names in an IP range.	(http://code.google.com/p/dnsbf)
dnsbrute	Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads.	(https://github.com/d4rkcat/dnsbrute)
dnscan	A python wordlist-based DNS subdomain scanner.	(https://github.com/rbsec/dnscan)
dnschef	A highly configurable DNS proxy for pentesters.	(http://thesprawl.org/projects/dnschef/)
dnscobra	DNS subdomain bruteforcing tool with Tor support through torsocks.	(https://github.com/dmitescu/dnscobra)
dnsdiag	DNS Diagnostics and Performance Measurement Tools.	(https://dnsdiag.org/)
dnsdrdos	Proof of concept code for distributed DNS reflection DoS.	(http://nullsecurity.net/tools/dos.html)
dnsenum	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.	(https://github.com/fwaeytens/dnsenum/)
dnsfilexfer	File transfer via DNS.	(https://github.com/leonjza/dnsfilexfer)
dnsgoblin	Nasty creature constantly searching for DNS servers. It uses standard dns querys and waits for the replies.	(http://nullsecurity.net/tools/scanner.html)
dnsgrep	A utility for quickly searching presorted DNS names.	(https://github.com/erbbysam/DNSGrep)
dnsmap	Passive DNS network mapper	(http://dnsmap.googlecode.com)
dnsobserver	A handy DNS service written in Go to aid in the detection of several types of blind vulnerabilities.	(https://github.com/allyomalley/dnsobserver)
dnspredict	DNS prediction.	(http://johnny.ihackstuff.com/)
dnsprobe	Allows you to perform multiple dns queries of your choice with a list of user supplied resolvers.	(https://github.com/projectdiscovery/dnsprobe)
dnspy	.NET debugger and assembly editor.	(https://github.com/0xd4d/dnSpy/)
dnsrecon	Python script for enumeration of hosts, subdomains and emails from a given domain using google.	(https://github.com/darkoperator/dnsrecon)
dnssearch	A subdomain enumeration tool.	(https://github.com/evilsocket/dnssearch)
dnsspider	A fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation.	(http://nullsecurity.net/tools/scanner.html)
dnsteal	DNS Exfiltration tool for stealthily sending files over DNS requests..	(https://github.com/m57/dnsteal)
dnstracer	Determines where a given DNS server gets its information from, and follows the chain of DNS servers	(https://www.mavetju.org/unix/dnstracer.php)
dnstwist	Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.	(https://github.com/elceef/dnstwist)
dnsvalidator	Maintains a list of IPv4 DNS servers by verifying them against baseline servers, and ensuring accurate responses.	(https://github.com/vortexau/dnsvalidator)
dnswalk	A DNS debugger and zone-transfer utility.	(http://sourceforge.net/projects/dnswalk/)
dnsx	Fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers.	(https://github.com/projectdiscovery/dnsx)
docem	Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids).	(https://github.com/whitel1st/docem)
dockerscan	Docker security analysis & hacking tools.	(https://github.com/cr0hn/dockerscan)
domain-analyzer	Finds all the security information for a given domain name.	(http://sourceforge.net/projects/domainanalyzer/)
domain-stats	A web API to deliver domain information from whois and alexa.	(https://github.com/MarkBaggett/domain_stats)
domained	Multi Tool Subdomain Enumeration.	(https://github.com/TypeError/domained)
domainhunter	Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names.	(https://github.com/threatexpress/domainhunter)
domato	DOM fuzzer.	(https://github.com/googleprojectzero/domato)
domi-owned	A tool used for compromising IBM/Lotus Domino servers.	(https://github.com/coldfusion39/domi-owned)
domlink	A tool to link a domain with registered organisation names and emails, to other domains.	(https://github.com/vysecurity/DomLink)
donpapi	Dumping revelant information on compromised targets without AV detection with DPAPI.	(https://github.com/login-securite/DonPAPI)
dontgo403	Tool to bypass 40X response codes..	(https://github.com/devploit/dontgo403)
donut	Generates x86, x64 or AMD64+x86 P.I. shellcode loading .NET Assemblies from memory.	(https://github.com/TheWover/donut)
doona	A fork of the Bruteforce Exploit Detector Tool (BED).	(https://github.com/wireghoul/doona)
doork	Passive Vulnerability Auditor.	(https://github.com/AeonDave/doork)
doozer	A Password cracking utility.	(https://github.com/CoalfireLabs/crackHOR)
dorkbot	Command-line tool to scan Google search results for vulnerabilities.	(https://github.com/utiso/dorkbot)
dorkme	Tool designed with the purpose of making easier the searching of vulnerabilities with Google Dorks, such as SQL Injection vulnerabilities.	(https://github.com/blueudp/DorkMe)

Name	Description	Website
dorknet	Selenium powered Python script to automate searching for vulnerable web apps.	(https://github.com/NullArray/DorkNet)
dorkscout	Golang tool to automate google dork scan against the entire internet or specific targets.	(https://github.com/R4yGM/dorkscout)
dotdotpwn	The Transversal Directory Fuzzer.	(http://dotdotpwn.blogspot.com)
dotpeek	Free .NET Decompiler and Assembly Browser.	(https://www.jetbrains.com/decompiler/)
dpeparser	Default password enumeration project	(http://www.toolswatch.org/dpe/)
dpscan	Drupal Vulnerability Scanner.	(https://github.com/insaneisnotfree/Blue-Sky-Information-Security)
dr-checker	A Soundy Vulnerability Detection Tool for Linux Kernel Drivers.	(https://github.com/ucsb-seclab/dr_checker)
dr0p1t-framework	A framework that creates a dropper that bypass most AVs, some sandboxes and have some tricks.	(https://github.com/D4Vinci/Dr0p1t-Framework)
dracnmap	Tool to exploit the network and gathering information with nmap help.	(https://github.com/screetsec/Dracnmap)
dradis-ce	An open source framework to enable effective information sharing.	(http://dradisframework.org/)
dragon-backdoor	A sniffing, non binding, reverse down/exec, portknocking service Based on cd00r.c.	(https://github.com/Shellntel/backdoors)
driftnet	Listens to network traffic and picks out images from TCP streams it observes.	(http://www.ex-parrot.com/~chris/driftnet/)
drinkme	A shellcode testing harness.	(https://github.com/emptymonkey/drinkme)
dripcap	Caffeinated Packet Analyzer.	(https://github.com/dripcap/dripcap)
dripper	A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS.	(http://www.blackhatlibrary.net/Dripper)
droopescan	A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe.	(https://github.com/droope/droopescan)
drozer	A security testing framework for Android - Precompiled binary from official repository.	(https://github.com/mwrlabs/drozer)
drupal-module-enum	Enumerate on drupal modules.	(https://github.com/Tethik/drupal-module-enumeration)
drupalscan	Simple non-intrusive Drupal scanner.	(https://rubygems.org/gems/DrupalScan/)
drupwn	Drupal enumeration & exploitation tool.	(https://github.com/immunIT/drupwn)
dscanner	Swiss-army knife for D source code	(https://github.com/dlang-community/D-Scanner)
dsd	Digital Speech Decoder	(https://github.com/szechyjs/dsd)
dsfs	A fully functional File inclusion vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	(https://github.com/stamparm/DSFS)
dshell	A network forensic analysis framework.	(https://github.com/USArmyResearchLab/Dshell)
dsjs	A fully functional JavaScript library vulnerability scanner written in under 100 lines of code.	(https://github.com/stamparm/DSJS)
dsniff	Collection of tools for network auditing and penetration testing	(https://www.monkey.org/~dugsong/dsniff/)
dsss	A fully functional SQL injection vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	(https://github.com/stamparm/DSSS)
dsstore-crawler	A parser + crawler for .DS_Store files exposed publically.	(https://github.com/anantshri/DS_Store_crawler_parser)
dsxs	A fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.	(https://github.com/stamparm/DSXS)
dtp-spoof	Python script/security tool to test Dynamic Trunking Protocol configuration on a switch.	(https://github.com/fleetcaptain/dtp-spoof)
dublin-traceroute	NAT-aware multipath tracerouting tool.	(https://github.com/insomniacslk/dublin-traceroute)
ducktoolkit	Encoding Tools for Rubber Ducky.	(https://github.com/kevthehermit/DuckToolkit)
dumb0	A simple tool to dump users in popular forums and CMS.	(https://github.com/0verl0ad/Dumb0)
dump1090	A simple Mode S decoder for RTLSDR devices.	(https://github.com/MalcolmRobb/dump1090)
dumpacl	Dumps NTs ACLs and audit settings.	(http://www.systemtools.com/cgi-bin/download.pl?DumpAcl)
dumpsmbshare	A script to dump files and folders remotely from a Windows SMB share.	(https://github.com/p0dalirius/DumpSMBShare)
dumpusers	Dumps account names and information even though RestrictAnonymous has been set to 1.	(http://ntsecurity.nu/toolbox/dumpusers/)
dumpzilla	A forensic tool for firefox.	(http://www.dumpzilla.org/)
duplicut	Remove duplicates from massive wordlist, without sorting it (for dictionnary-based password cracking).	(https://github.com/nil0x42/duplicut)
dutas	Analysis PE file or Shellcode.	(https://github.com/dungtv543/Dutas)
dvcs-ripper	Rip web accessible (distributed) version control systems: SVN/GIT/BZR/CVS/HG.	(https://github.com/kost/dvcs-ripper)
dwarf	Full featured multi arch/os debugger built on top of PyQt5 and frida.	(https://github.com/iGio90/Dwarf)
dynamorio	A dynamic binary instrumentation framework.	(https://github.com/DynamoRIO/dynamorio)
eapeak	Analysis Suite For EAP Enabled Wireless Networks.	(https://github.com/securestate/eapeak)
eaphammer	Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks.	(https://github.com/s0lst1c3/eaphammer)
eapmd5pass	An implementation of an offline dictionary attack against the EAP-MD5 protocol.	(http://www.willhackforsushi.com/?page_id=67)
easy-creds	A bash script that leverages ettercap and other tools to obtain credentials.	(https://github.com/brav0hax/easy-creds)
easyda	Easy Windows Domain Access Script.	(https://github.com/nccgroup/easyda)
easyfuzzer	A flexible fuzzer, not only for web, has a CSV output for efficient output analysis (platform independent).	(http://www.mh-sec.de/downloads.html.en)
eazy	This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more.	(http://packetstormsecurity.com/files/117572/EAZY-Web-Scanner.html)
ecfs	Extended core file snapshot format.	(https://github.com/elfmaster/ecfs)
edb	A cross platform AArch32/x86/x86 debugger.	(https://github.com/eteran/edb-debugger/)
eggshell	iOS/macOS/Linux Remote Administration Tool.	(https://github.com/neoneggplant/EggShell)
eigrp-tools	This is a custom EIGRP packet generator and sniffer developed to test the security and overall operation quality of this brilliant Cisco routing protocol.	(http://www.hackingciscoexposed.com/?link=tools)
eindeutig	Examine the contents of Outlook Express DBX email repository files (forensic purposes)	(http://www.jonesdykstra.com/)
electric-fence	A malloc(3) debugger that uses virtual memory hardware to detect illegal memory accesses.	(https://packages.debian.org/sid/electric-fence)
elettra	Encryption utility by Julia Identity	(http://www.winstonsmith.info/julia/elettra/)
elettra-gui	Gui for the elettra crypto application.	(http://www.winstonsmith.info/julia/elettra/)
elevate	Horizontal domain discovery tool you can use to discover other domains owned by a given company.	(https://github.com/Healdb/Elevate)

Name	Description	Website
elfkickers	Collection of ELF utilities (includes sstrip)	(https://www.muppetlabs.com/~breadbox/software/elfkickers.html)
elfparser	Cross Platform ELF analysis.	(https://github.com/jacob-baines/elfparser)
elfutils	Handle ELF object files and DWARF debugging information (utilities)	(https://sourceware.org/elfutils/)
elidecode	A tool to decode obfuscated shellcodes using the unicorn-engine for the emulation and the capstone-engine to print the asm code.	(https://github.com/DeveloppSoft/EliDecode)
elite-proxy-finder	Finds public elite anonymity proxies and concurrently tests them.	(https://github.com/DanMcInerney/elite-proxy-finder)
email2phonenumber	A OSINT tool to obtain a target's phone number just by having his email address.	(https://github.com/martinvigo/email2phonenumber/)
emldump	Analyze MIME files.	(https://blog.didierstevens.com/my-software/#emldump)
emp3r0r	Linux post-exploitation framework made by linux user.	(https://github.com/jm33-m0/emp3r0r)
empire	A PowerShell and Python post-exploitation agent.	(https://github.com/BC-SECURITY/Empire)
enabler	Attempts to find the enable password on a cisco system via brute force.	(http://packetstormsecurity.org/cisco/enabler.c)
encodeshellcode	This is an encoding tool for 32-bit x86 shellcode that assists a researcher when dealing with character filter or byte restrictions in a buffer overflow vulnerability or some kind of IDS/IPS/AV blocking your code.	(http://packetstormsecurity.com/files/119904/Encode-Shellcode.1b.html)
ent	Pseudorandom number sequence test.	(http://www.fourmilab.ch/random)
enteletaor	Message Queue & Broker Injection tool that implements attacks to Redis, RabbitMQ and ZeroMQ.	(https://github.com/cr0hn/enteletaor)
entropy	A set of tools to exploit Netwave and GoAhead IP Webcams.	(https://github.com/entynetproject/entropy)
enum-shares	Tool that enumerates shared folders across the network and under a custom user account.	(https://github.com/dejanlevaja/enum_shares)
enum4linux	A tool for enumerating information from Windows and Samba systems.	(http://labs.portcullis.co.uk/application/enum4linux/)
enum4linux-ng	A next generation version of enum4linux.	(https://github.com/cddmp/enum4linux-ng)
enumerate-iam	Enumerate the permissions associated with an AWS credential set.	(https://github.com/andresriancho/enumerate-iam)
enumerid	Enumerate RIDs using pure Python.	(https://github.com/Gilks/enumerid)
enumiax	An IAX enumerator.	(http://sourceforge.net/projects/enumiax/)
enyelkm	Rootkit for Linux x86 kernels v2.6.	(http://www.enye-sec.org/programas.html)
eos	Enemies Of Symfony - Debug mode Symfony looter.	(https://github.com/synacktiv/eos)
epicwebhoneypot	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.	(http://sourceforge.net/projects/epicwebhoneypot/)
erase-registrations	An IAX flooder.	(http://www.hackingexposedvoip.com/)
eraser	Windows tool which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.	(https://eraser.heidi.ie/download/)
eresi	The ERESI Reverse Engineering Software Interface.	(https://github.com/thorkill/eresi)
erl-matter	Tool to exploit epmd related services such as rabbitmq, ejabberd and couchdb by bruteforcing the cookie and gaining RCE afterwards.	(https://github.com/gteissier/erl-matter)
espionage	A Network Packet and Traffic Interceptor For Linux. Sniff All Data Sent Through a Network.	(https://github.com/josh0xA/Espionage)
eternal-scanner	An internet scanner for exploit CVE-0144 (Eternal Blue).	(https://github.com/peterpt/eternal_scanner)
etherape	Graphical network monitor for various OSI layers and protocols	(http://etherape.sourceforge.net/)
etherchange	Can change the Ethernet address of the network adapters in Windows.	(http://ntsecurity.nu/toolbox/etherchange/)
etherflood	Floods a switched network with Ethernet frames with random hardware addresses.	(http://ntsecurity.nu/toolbox/etherflood/)
ettercap	Network sniffer/interceptor/logger for ethernet LANs - console	(https://www.ettercap-project.org/)
evil-ssdp	Spoof SSDP replies to phish for NetNTLM challenge/response on a network.	(https://gitlab.com/initstring/evil-ssdp)
evil-winrm	The ultimate WinRM shell for hacking/pentesting.	(https://github.com/Hackplayers/evil-winrm)
evilclippy	A cross-platform assistant for creating malicious MS Office documents.	(https://github.com/outflanknl/EvilClippy)
evilginx	Man-in-the-middle attack framework used for phishing login credentials	(https://github.com/kgretzky/evilginx2)
evilgrade	Modular framework that takes advantage of poor upgrade implementations by injecting fake updates.	(https://github.com/infobyte/evilgrade)
evilize	Tool to create MD5 colliding binaries.	(http://www.mathstat.dal.ca/~selinger/md5collision/)
evillimiter	Tool that limits bandwidth of devices on the same network without access.	(https://github.com/bitbrute/evillimiter)
evilmaid	TrueCrypt loader backdoor to sniff volume password	(http://theinvisiblethings.blogspot.com)
evilpdf	Embedding executable files in PDF Documents.	(https://github.com/thelinuxchoice/evilpdf)
evine	Interactive CLI Web Crawler.	(https://github.com/saeeddhqan/evine.git)
evtkit	Fix acquired .evt - Windows Event Log files (Forensics).	(https://github.com/yarox24/evtkit)
exabgp	The BGP swiss army knife of networking.	(https://github.com/Exa-Networks/exabgp)
exe2hex	Inline file transfer using in-built Windows tools (DEBUG.exe or PowerShell).	(https://github.com/g0tmi1k/exe2hex)
exe2image	A simple utility to convert EXE files to JPEG images and vice versa.	(https://github.com/OsandaMalith/Exe2Image)
exescan	A tool to detect anomalies in PE (Portable Executable) files.	(https://github.com/cysinfo/Execscan)
exiflooter	Find geolocation on all image urls and directories also integrates with OpenStreetMap.	(https://github.com/aydinnyunus/exifLooter)
exitmap	A fast and modular scanner for Tor exit relays.	(https://github.com/NullHypothesis/exitmap)
expimp-lookup	Looks for all export and import names that contain a specified string in all Portable Executable in a directory tree.	(https://github.com/tr3w/ExpImp-Lookup)
exploit-db	The Exploit Database (EDB) – an ultimate archive of exploits and vulnerable software - A collection of hacks	(http://www.exploit-db.com)
exploitdb	Offensive Security’s Exploit Database Archive	(https://www.exploit-db.com/)
exploitpack	Exploit Pack - The next generation exploit framework.	(https://github.com/juansacco/exploitpack)
expose	A Dynamic Symbolic Execution (DSE) engine for JavaScript	(https://github.com/ExpoSEJS/ExpoSE)
exrex	Irregular methods on regular expressions.	(https://github.com/asciimoo/exrex)
extended-ssrf-search	Smart ssrf scanner using different methods like parameter brute forcing in post and get.	(https://github.com/Damian89/extended-ssrf-search)
extracthosts	Extracts hosts (IP/Hostnames) from files.	(https://github.com/bwall/ExtractHosts)
extractusnjrnl	Tool to extract the $UsnJrnl from an NTFS volume.	(https://github.com/jschicht/ExtractUsnJrnl)
eyeballer	Convolutional neural network for analyzing pentest screenshots.	(https://github.com/BishopFox/eyeballer)
eyepwn	Exploit for Eye-Fi Helper directory traversal vulnerability	(http://www.pentest.co.uk)
eyewitness	Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.	(https://github.com/ChrisTruncer/EyeWitness)

Name	Description	Website
f-scrack	A single file bruteforcer supports multi-protocol.	(https://github.com/ysrc/F-Scrack)
facebash	Facebook Brute Forcer in shellscript using TOR.	(https://github.com/thelinuxchoice/facebash)
facebookosint	OSINT tool to replace facebook graph search.	(https://github.com/tomoneill19/facebookOSINT)
facebot	A facebook profile and reconnaissance system.	(https://github.com/pun1sh3r/facebot)
facebrok	Social Engineering Tool Oriented to facebook.	(https://github.com/PowerScript/facebrok)
facebrute	This script tries to guess passwords for a given facebook account using a list of passwords (dictionary).	(https://github.com/emerinohdz/FaceBrute)
factordb-pycli	CLI for factordb and Python API Client.	(https://github.com/ryosan/factordb-pycli)
fakeap	Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames.	(http://www.blackalchemy.to/project/fakeap/)
fakedns	A regular-expression based python MITM DNS server with correct DNS request passthrough and "Not Found" responses.	(https://github.com/Crypt0s/FakeDns)
fakemail	Fake mail server that captures e-mails as files for acceptance testing.	(http://sourceforge.net/projects/fakemail/)
fakenet-ng	Next Generation Dynamic Network Analysis Tool.	(https://github.com/fireeye/flare-fakenet-ng)
fakenetbios	A family of tools designed to simulate Windows hosts (NetBIOS) on a LAN.	(https://github.com/mubix/FakeNetBIOS)
fang	A multi service threaded MD5 cracker.	(https://github.com/evilsocket/fang)
faradaysec	Collaborative Penetration Test and Vulnerability Management Platform.	(http://www.faradaysec.com/)
fastnetmon	High performance DoS/DDoS load analyzer built on top of multiple packet capture engines.	(https://github.com/pavel-odintsov/fastnetmon)
fav-up	IP lookup by favicon using Shodan.	(https://github.com/pielco11/fav-up)
favfreak	Weaponizing favicon.ico for BugBounties , OSINT and what not.	(https://github.com/devanshbatham/FavFreak)
fbht	A Facebook Hacking Tool	(https://github.com/chinoogawa/fbht)
fbi	An accurate facebook account information gathering.	(https://github.com/xHak9x/fbi)
fbid	Show info about the author by facebook photo url.	(https://github.com/guelfoweb/fbid)
fcrackzip	Zip file password cracker	(http://oldhome.schmorp.de/marc/fcrackzip.html)
fdsploit	A File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool.	(https://github.com/chrispetrou/FDsploit)
featherduster	An automated, modular cryptanalysis tool.	(https://github.com/nccgroup/featherduster)
fern-wifi-cracker	WEP, WPA wifi cracker for wireless penetration testing.	(http://code.google.com/p/fern-wifi-cracker/)
fernflower	An analytical decompiler for Java.	(https://github.com/fesh0r/fernflower)
fernmelder	Asynchronous mass DNS scanner.	(https://github.com/stealth/fernmelder)
feroxbuster	A fast, simple, recursive content discovery tool written in Rust.	(https://github.com/epi052/feroxbuster)
ffm	A hacking harness that you can use during the post-exploitation phase of a red-teaming engagement.	(https://github.com/JusticeRage/FFM)
ffuf	Fast web fuzzer written in Go.	(https://github.com/ffuf/ffuf)
ffuf-scripts	Scripts and snippets for ffuf payloads.	(https://github.com/ffuf/ffuf-scripts)
fgscanner	An advanced, opensource URL scanner.	(http://www.fantaghost.com/fgscanner)
fhttp	This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more.	(http://packetstormsecurity.com/files/104315/FHTTP-Attack-Tool.3.html)
fi6s	IPv6 network scanner designed to be fast.	(https://github.com/sfan5/fi6s)
fierce	A DNS reconnaissance tool for locating non-contiguous IP space.	(https://github.com/mschwager/fierce)
fiked	Fake IDE daemon	(http://www.roe.ch/FakeIKEd)
filebuster	An extremely fast and flexible web fuzzer.	(https://github.com/henshin/filebuster)
filefuzz	A binary file fuzzer for Windows with several options.	(http://www.fuzzing.org/)
filegps	A tool that help you to guess how your shell was renamed after the server-side script of the file uploader saved it.	(https://github.com/0blio/fileGPS)
fileintel	A modular Python application to pull intelligence about malicious files.	(https://github.com/keithjjones/fileintel)
filibuster	A Egress filter mapping application with additional functionality.	(https://github.com/subinacls/Filibuster)
fimap	A little tool for local and remote file inclusion auditing and exploitation	(http://code.google.com/p/fimap/)
finalrecon	OSINT Tool for All-In-One Web Reconnaissance.	(https://github.com/thewhiteh4t/FinalRecon)
find-dns	A tool that scans networks looking for DNS servers.	(https://packetstormsecurity.com/files/132449/Find-DNS-Scanner.html)
find3	High-precision indoor positioning framework.	(https://github.com/schollz/find3)
findmyhash	Crack different types of hashes using free online services.	(https://code.google.com/archive/p/findmyhash/)
findmyiphone	Locates all devices associated with an iCloud account	(https://github.com/manwhoami/findmyiphone)
findomain	The fastest and cross-platform subdomain enumerator, do not waste your time	(https://github.com/Findomain/Findomain)
findsploit	Find exploits in local and online databases instantly.	(https://github.com/1N3/findsploit)
fingerprinter	CMS/LMS/Library etc Versions Fingerprinter.	(https://github.com/erwanlr/Fingerprinter)
firecat	A penetration testing tool that allows you to punch reverse TCP tunnels out of a compromised network.	(https://github.com/BishopFox/firecat)
firefox-decrypt	Extract passwords from Mozilla Firefox, Waterfox, Thunderbird, SeaMonkey profiles.	(https://github.com/unode/firefox_decrypt)
firefox-security-toolkit	A tool that transforms Firefox browsers into a penetration testing suite.	(https://github.com/mazen160/Firefox-Security-Toolkit)
firewalk	An active reconnaissance network security tool.	(http://packetfactory.openwall.net/projects/firewalk/)
firmwalker	Script for searching the extracted firmware file system for goodies.	(https://github.com/craigz28/firmwalker)
firmware-mod-kit	Modify firmware images without recompiling.	(https://github.com/rampageX/firmware-mod-kit)
firstexecution	A Collection of different ways to execute code outside of the expected entry points.	(https://github.com/nccgroup/firstexecution)
firstorder	A traffic analyzer to evade Empire communication from Anomaly-Based IDS.	(https://github.com/tearsecurity/firstorder)
fl0p	A passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks.	(http://lcamtuf.coredump.cx/)
flare	Flare processes an SWF and extracts all scripts from it.	(http://www.nowrap.de/flare.html)
flare-floss	Obfuscated String Solver - Automatically extract obfuscated strings from malware.	(https://github.com/mandiant/flare-floss)
flashlight	Automated Information Gathering Tool for Penetration Testers.	(https://github.com/galkan/flashlight)
flashscanner	Flash XSS Scanner.	(https://github.com/riusksk/FlashScanner)
flashsploit	Exploitation Framework for ATtiny85 Based HID Attacks.	(https://github.com/thewhiteh4t/flashsploit)
flask-session-cookie-manager2	Decode and encode Flask session cookie.	(https://noraj.github.io/flask-session-cookie-manager/)

Name	Description	Website
flask-session-cookie-manager3	Decode and encode Flask session cookie.	(https://noraj.github.io/flask-session-cookie-manager/)
flask-unsign	Decode, encode and brute-force Flask session cookie.	(https://github.com/Paradoxis/Flask-Unsign)
flasm	Disassembler tool for SWF bytecode	(http://www.nowrap.de/flasm.html)
flawfinder	Searches through source code for potential security flaws	(https://dwheeler.com/flawfinder/)
flowinspect	A network traffic inspection tool.	(https://github.com/7h3rAm/flowinspect)
flunym0us	A Vulnerability Scanner for Wordpress and Moodle.	(http://code.google.com/p/flunym0us/)
fluxion	A security auditing and social-engineering research tool.	(https://github.com/FluxionNetwork/fluxion)
flyr	Block-based software vulnerability fuzzing framework.	(https://github.com/zznop/flyr)
fockcache	Tool to make cache poisoning by trying X-Forwarded-Host and X-Forwarded-Scheme headers on web pages.	(https://github.com/tismayil/fockcache)
forager	Multithreaded threat Intelligence gathering utilizing.	(https://github.com/byt3smith/Forager)
foremost	A console program to recover files based on their headers, footers, and internal data structures	(http://foremost.sourceforge.net/)
foresight	A tool for predicting the output of random number generators.	(https://github.com/ALSchwalm/foresight)
forkingportscanner	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.	(http://magikh0e.xyz/)
formatstringexploiter	Helper script for working with format string bugs.	(https://github.com/Owlz/formatStringExploiter)
fortiscan	A high performance FortiGate SSL-VPN vulnerability scanning and exploitation tool.	(https://github.com/anasbousselham/fortiscan)
fpdns	Program that remotely determines DNS server versions.	(https://github.com/kirei/fpdns)
fping	Utility to ping multiple hosts at once	(https://www.fping.org/)
fport	Identify unknown open ports and their associated applications.	(http://www.foundstone.com/us/resources/proddesc/fport.htm)
fprotlogparser	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.	(http://magikh0e.xyz/)
fraud-bridge	ICMP and DNS tunneling via IPv4 and IPv6.	(https://github.com/stealth/fraud-bridge)
fred	Cross-platform M$ registry hive editor.	(https://www.pinguin.lu/fred)
freeipmi	IPMI remote console and system management software	(https://www.gnu.org/software/freeipmi)
freeradius	The premier open source RADIUS server	(https://freeradius.org/)
freewifi	How to get free wifi.	(https://github.com/kylemcdonald/FreeWifi)
frida	Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.	(https://pypi.org/project/frida/#files)
frida-extract	Frida.re based RunPE (and MapViewOfSection) extraction tool.	(https://github.com/OALabs/frida-extract)
frida-ios-dump	Pull decrypted ipa from jailbreak device.	(https://github.com/AloneMonkey/frida-ios-dump)
fridump	A universal memory dumper using Frida.	(https://github.com/Nightbringer21/fridump)
frisbeelite	A GUI-based USB device fuzzer.	(https://github.com/nccgroup/FrisbeeLite)
fs-exploit	Format string exploit generation.	(https://github.com/miaouPlop/fs)
fs-nyarl	A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit.	(http://www.fulgursecurity.com/en/content/fs-nyarl)
fscan	A Security Auditing Tool.	(https://github.com/shadow1ng/fscan)
fsnoop	A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods").	(http://vladz.devzero.fr/fsnoop.php)
fssb	A low-level filesystem sandbox for Linux using syscall intercepts.	(https://github.com/adtac/fssb)
fstealer	Automates file system mirroring through remote file disclosure vulnerabilities on Linux machines.	(http://packetstormsecurity.com/files/106450/FStealer-Filesystem-Mirroring-Tool.html)
ftester	A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities.	(http://www.inversepath.com/ftester.html)
ftp-fuzz	The master of all master fuzzing scripts specifically targeted towards FTP server software.	(http://nullsecurity.net/tools/fuzzer.html)
ftp-scanner	Multithreaded ftp scanner/brute forcer. Tested on Linux, OpenBSD and Solaris.	(http://wayreth.eu.org/old_page/)
ftp-spider	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.	(http://packetstormsecurity.com/files/35120/ftp-spider.pl.html)
ftpmap	Scans remote FTP servers to identify what software and what versions they are running.	(http://wcoserver.googlecode.com/files/)
ftpscout	Scans ftps for anonymous access.	(https://github.com/RubenRocha/ftpscout)
fuddly	Fuzzing and Data Manipulation Framework (for GNU/Linux).	(https://github.com/k0retux/fuddly)
fusil	A Python library used to write fuzzing programs.	(http://bitbucket.org/haypo/fusil/wiki/Home)
fuxploider	Tool that automates the process of detecting and exploiting file upload forms flaws.	(https://github.com/almandin/fuxploider)
fuzzap	A python script for obfuscating wireless networks.	(https://github.com/lostincynicism/FuzzAP)
fuzzball2	A little fuzzer for TCP and IP options. It sends a bunch of more or less bogus packets to the host of your choice.	(http://nologin.org/)
fuzzbunch	NSA Exploit framework	(https://github.com/mdiazcl/fuzzbunch-debian)
fuzzdb	Attack and Discovery Pattern Dictionary for Application Fault Injection Testing.	(https://github.com/fuzzdb-project/fuzzdb)
fuzzdiff	A simple tool designed to help out with crash analysis during fuzz testing. It selectively 'un-fuzzes' portions of a fuzzed file that is known to cause a crash, re-launches the targeted application, and sees if it still crashes.	(http://vsecurity.com/resources/tool)
fuzzowski	A Network Protocol Fuzzer made by NCCGroup based on Sulley and BooFuzz.	(https://github.com/nccgroup/fuzzowski)
fuzztalk	An XML driven fuzz testing framework that emphasizes easy extensibility and reusability.	(https://code.google.com/p/fuzztalk)
g72x++	Decoder for the g72x++ codec.	(http://www.ps-auxw.de/)
gadgetinspector	A byte code analyzer for finding deserialization gadget chains in Java applications.	(https://github.com/JackOfMostTrades/gadgetinspector)
gadgettojscript	.NET serialized gadgets that can trigger .NET assembly from JS/VBS/VBA based scripts.	(https://github.com/med0x2e/GadgetToJScript)
galleta	Examine the contents of the IE's cookie files for forensic purposes	(http://www.jonesdykstra.com/)
gasmask	All in one Information gathering tool - OSINT.	(https://github.com/twelvesec/gasmask)

Name	Description	Website
gatecrasher	Network auditing and analysis tool developed in Python.	↗ (https://github.com/michaeltelford/gatecrasher)
gau	Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.	↗ (https://github.com/lc/gau/)
gcat	A fully featured backdoor that uses Gmail as a C&C server.	↗ (https://github.com/byt3bl33d3r/gcat)
gcpbucketbrute	A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated.	↗ (https://github.com/RhinoSecurityLabs/GCPBucketBrute)
gcrypt	Simple, secure and performance file encryption tool written in C	↗ (https://gitlab.com/GasparVardanyan/gcrypt)
gdb	The GNU Debugger	↗ (https://www.gnu.org/software/gdb/)
gdb-common	The GNU Debugger	↗ (https://www.gnu.org/software/gdb/)
gdbgui	Browser-based gdb frontend using Flask and JavaScript to visually debug C, C++, Go, or Rust.	↗ (https://github.com/cs01/gdbgui)
gene	Signature Engine for Windows Event Logs.	↗ (https://github.com/0xrawsec/gene)
genisys	Powerful Telegram Members Scraping and Adding Toolkit.	↗ (https://github.com/ahayder/Genisys)
genlist	Generates lists of IP addresses.	↗ ()
geoedge	This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool).	↗ ()
geoip	Non-DNS IP-to-country resolver C library & utils	↗ (https://www.maxmind.com/app/c)
geoipgen	GeoIPgen is a country to IP addresses generator.	↗ (http://code.google.com/p/geoipgen/)
gerix-wifi-cracker	A graphical user interface for aircrack-ng and pyrit.	↗ (https://github.com/TigerSecurity)
gethsploit	Finding Ethereum nodes which are vulnerable to RPC-attacks.	↗ (https://github.com/KarmaHostage/gethspoit)
getsids	Getsids tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener. Like doing ‘lsnrctl service’.	↗ (http://www.cqure.net/wp/getsids/)
getsploit	Command line utility for searching and downloading exploits.	↗ (https://github.com/vulnersCom/getsploit)
gf	A wrapper around grep, to help you grep for things.	↗ (https://github.com/tomnomnom/gf)
gg-images	The application was created to allow anyone to easily download profile pictures from GG.	↗ (https://codeberg.org/nanoory/gg_images)
gggooglescan	A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames.	↗ (http://www.morningstarsecurity.com/research/gggooglescan)
gh-dork	Github dorking tool.	↗ (https://github.com/molly/gh-dork)
ghauri	An advanced cross-platform tool that automates the process of detecting and exploiting SQL injection security flaws.	↗ (https://github.com/r0oth3x49/ghauri)
ghettotooth	Ghettodriving for bluetooth.	↗ (http://www.oldskoolphreak.com/tfiles/ghettotooth.txt)
ghidra	Software reverse engineering framework	↗ (https://ghidra-sre.org/)
ghost-phisher	GUI suite for phishing and penetration attacks	↗ (http://code.google.com/p/ghost-phisher)
ghost-py	Webkit based webclient (relies on PyQT).	↗ (http://jeanphix.github.com/Ghost.py/)
ghostdelivery	Python script to generate obfuscated .vbs script that delivers payload (payload dropper) with persistence and windows antivirus disabling functions.	↗ (https://github.com/s1egesystems/GhostDelivery)
gibberish-detector	Train a model and detect gibberish strings with it.	↗ (https://github.com/domanchi/gibberish-detector)
girsh	Automatically spawn a reverse shell fully interactive for Linux or Windows victim.	↗ (https://github.com/nodauf/Girsh)
giskismet	A program to visually represent the Kismet data in a flexible manner.	↗ (http://www.giskismet.org)
git-dump	Dump the contents of a remote git repository without directory listing enabled.	↗ (https://github.com/bahamas10/node-git-dump)
git-dumper	A tool to dump a git repository from a website.	↗ (https://github.com/arthaud/git-dumper)
git-hound	Pinpoints exposed API keys on GitHub. A batch-catching, pattern-matching, patch-attacking secret snatcher.	↗ (https://github.com/tillson/git-hound)
git-wild-hunt	A tool to hunt for credentials in github wild AKA git*hunt.	↗ (https://github.com/d1vious/git-wild-hunt)
gitdorker	Python program to scrape secrets from GitHub through usage of a large repository of dorks.	↗ (https://github.com/obheda12/GitDorker)
gitdump	A pentesting tool that dumps the source code from .git even when the directory traversal is disabled.	↗ (https://github.com/Ebryx/GitDump)
gitem	A Github organization reconnaissance tool.	↗ (https://github.com/mschwager/gitem)
gitgraber	Monitor GitHub to search and find sensitive data in real time for different online services.	↗ (https://github.com/hisxo/gitGraber)
githack	A `.git` folder disclosure exploit.	↗ (https://github.com/lijiejie/githack)
githound	Find secret information in git repositories.	↗ (https://github.com/tillson/git-hound)
github-dorks	Collection of github dorks and helper tool to automate the process of checking dorks.	↗ (https://github.com/techgaun/github-dorks)
githubcloner	A script that clones Github repositories of users and organizations automatically.	↗ (https://github.com/mazen160/GithubCloner)
gitleaks	Audit Git repos for secrets and keys	↗ (https://github.com/gitleaks/gitleaks)
gitmails	An information gathering tool to collect git commit emails in version control host services.	↗ (https://github.com/giovanifss/gitmails)
gitminer	Tool for advanced mining for content on Github.	↗ (https://github.com/danilovazb/GitMiner)
gitrecon	OSINT tool to get information from a Github and Gitlab profile and find user's email addresses leaked on commits.	↗ (https://github.com/GONZOsint/gitrecon)
gitrob	Reconnaissance tool for GitHub organizations.	↗ (http://michenriksen.com/blog/gitrob-putting-the-open-source-in-osint/)
gittools	A repository with 3 tools for pwn'ing websites with .git repositories available'.	↗ (https://github.com/internetwache/GitTools)
gloom	Linux Penetration Testing Framework.	↗ (https://github.com/StreetSec/Gloom-Framework)
glue	A framework for running a series of tools.	↗ (https://github.com/OWASP/glue)
gmsadumper	A tool that Reads any gMSA password blobs the user can access and parses the values.	↗ (https://github.com/micahvandeusen/gMSADumper)
gnuradio	General purpose DSP and SDR toolkit with drivers for usrp and fcd.	↗ (https://gnuradio.org)
gnutls2	A library which provides a secure layer over a reliable transport layer (Version 2)	↗ (http://gnutls.org/)
go-windapsearch	Utility to enumerate users, groups and computers from a Windows domain through LDAP queries.	↗ (https://github.com/ropnop/go-windapsearch)
gobd	A Golang covert backdoor.	↗ (https://github.com/razc411/GoBD)
gobuster	Directory/file & DNS busting tool written in Go.	↗ (https://github.com/OJ/gobuster)
gocabrito	Super organized and flexible script for sending phishing campaigns.	↗ (https://github.com/KINGSABRI/goCabrito)
goddi	Dumps Active Directory domain information.	↗ (https://github.com/NetSPI/goddi)
goldeneye	A HTTP DoS test tool. Attack Vector exploited: HTTP Keep Alive + NoCache.	↗ (https://github.com/jseidl/GoldenEye)

Name	Description	Website
golismero	Opensource web security testing framework.	(https://github.com/golismero/golismero)
gomapenum	User enumeration and password bruteforce on Azure, ADFS, OWA, O365, Teams and gather emails on Linkedin.	(https://github.com/nodauf/GoMapEnum)
goodork	A python script designed to allow you to leverage the power of google dorking straight from the comfort of your command line.	(http://goo-dork.blogspot.com/)
goofile	Command line filetype search	(https://code.google.com/p/goofile/)
goofuzz	A Bash script that uses advanced Google search techniques to obtain sensitive information in files or directories without making requests to the web server.	(https://github.com/m3n0sd0n4ld/GooFuzz)
goog-mail	Enumerate domain emails from google.	(http://www.darkc0de.com/others/goog-mail.py)
google-explorer	Google mass exploit robot - Make a google search, and parse the results for a especific exploit you define.	(https://github.com/anarcoder/google_explorer)
googlesub	A python script to find domains by using google dorks.	(https://github.com/zombiesam/googlesub)
goohak	Automatically Launch Google Hacking Queries Against A Target Domain.	(https://github.com/1N3/Goohak)
goop	Perform google searches without being blocked by the CAPTCHA or hitting any rate limits.	(https://github.com/s0md3v/goop)
goop-dump	Tool to dump a git repository from a website, focused on as-complete-as-possible dumps and handling weird edge-cases.	(https://github.com/nyancrimew/goop)
gooscan	A tool that automates queries against Google search appliances, but with a twist.	(http://johnny.ihackstuff.com/downloads/task,doc_details&Itemid=/gid,28/)
gopherus	Tool generates gopher link for exploiting SSRF and gaining RCE in various servers.	(https://github.com/tarunkant/Gopherus)
gophish	Open-Source Phishing Framework.	(https://github.com/gophish/gophish)
goshs	A SimpleHTTPServer written in Go, enhanced with features and with a nice design.	(https://github.com/patrickhener/goshs)
gosint	OSINT framework in Go.	(https://github.com/Nhoya/gOSINT)
gospider	Fast web spider written in Go.	(https://github.com/jaeles-project/gospider)
gostringsr2	Extract strings from a Go binary using radare2.	(https://github.com/CarveSystems/gostringsr2)
gowitness	A golang, web screenshot utility using Chrome Headless.	(https://github.com/sensepost/gowitness)
gplist	Lists information about the applied Group Policies.	(http://ntsecurity.nu/toolbox/gplist/)
gpocrack	Active Directory Group Policy Preferences cpassword cracker/decrypter.	(https://github.com/MartinIngesen/gpocrack)
gpredict	A real-time satellite tracking and orbit prediction application.	(http://gpredict.oz9aec.net/)
gps-sdr-sim	Software-Defined GPS Signal Simulator.	(https://github.com/osqzss/gps-sdr-sim)
gqrx	Interactive SDR receiver waterfall for many devices.	(http://gqrx.dk/)
gr-air-modes	Gnuradio tools for receiving Mode S transponder signals, including ADS-B.	(https://github.com/bistromath/gr-air-modes)
gr-gsm	Gnuradio blocks and tools for receiving GSM transmissions.	(https://github.com/ptrkrysik/gr-gsm)
gr-paint	An OFDM Spectrum Painter for GNU Radio.	(https://github.com/drmpeg/gr-paint)
grabbb	Clean, functional, and fast banner scanner.	(https://packetstormsecurity.com/files/11372/grabbb.0.7.tar.gz.html)
grabber	A web application scanner. Basically it detects some kind of vulnerabilities in your website.	(http://rgaucher.info/beta/grabber/)
grabing	Counts all the hostnames for an IP adress	(https://github.com/black-brain/graBing)
grabitall	Performs traffic redirection by sending spoofed ARP replies.	(http://ntsecurity.nu/toolbox/grabitall/)
graffiti	A tool to generate obfuscated one liners to aid in penetration testing.	(https://github.com/Ekultek/Graffiti)
grammarinator	A random test generator / fuzzer that creates test cases according to an input ANTLR v4 grammar.	(https://github.com/renatahodovan/grammarinator)
graphinder	GraphQL endpoints finder using subdomain enumeration, scripts analysis and bruteforce.	(https://github.com/Escape-Technologies/graphinder)
graphql-cop	GraphQL vulnerability scanner.	(https://github.com/dolevf/graphql-cop)
graphql-path-enum	Tool that lists the different ways of reaching a given type in a GraphQL schema.	(https://gitlab.com/dee-see/graphql-path-enum)
graphqlmap	Scripting engine to interact with a graphql endpoint for pentesting purposes.	(https://github.com/swisskyrepo/GraphQLmap)
graphw00f	GraphQL endpoint detection and engine fingerprinting.	(https://github.com/dolevf/graphw00f)
graudit	Grep rough source code auditing tool.	(https://github.com/wireghoul/graudit)
grepforrfi	Simple script for parsing web logs for RFIs and Webshells v1.2	(http://www.irongeek.com/downloads/grepforrfi.txt)
grokevt	A collection of scripts built for reading Windows® NT/2K/XP/2K eventlog files.	(http://code.google.com/p/grokevt/)
grr	High-throughput fuzzer and emulator of DECREE binaries.	(https://github.com/trailofbits/grr)
grype	A vulnerability scanner for container images and filesystems.	(https://github.com/anchore/grype)
gsd	Gives you the Discretionary Access Control List of any Windows NT service you specify as a command line option.	(http://ntsecurity.nu/toolbox/gsd/)
gsocket	Global Socket moving data from here to there securely, fast and trough NAT/Firewalls	(https://www.gsocket.io/)
gspoof	A simple GTK/command line TCP/IP packet generator.	(http://gspoof.sourceforge.net/)
gtalk-decode	Google Talk decoder tool that demonstrates recovering passwords from accounts.	(http://packetstormsecurity.com/files/119154/Google-Talk-Decoder.html)
gtfo	Search gtfobins and lolbas files from your terminal.	(https://github.com/mzfr/gtfo)
gtfoblookup	Offline command line lookup utility for GTFOBins and LOLBAS.	(https://github.com/nccgroup/GTFOBLookup)
gtp-scan	A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts.	(http://www.c0decafe.de/)
guymager	A forensic imager for media acquisition.	(http://guymager.sourceforge.net/)
gwcheck	A simple program that checks if a host in an ethernet network is a gateway to Internet.	(http://packetstormsecurity.com/files/62047/gwcheck.c.html)
gwtenum	Enumeration of GWT-RCP method calls.	(http://www.gdssecurity.com/l/t/d.php?k=GwtEnum)
h2buster	A threaded, recursive, web directory brute-force scanner over HTTP/2.	(https://github.com/00xc/h2buster)
h2csmuggler	HTTP Request Smuggling over HTTP/2 Cleartext (h2c).	(https://github.com/BishopFox/h2csmuggler)
h2spec	A conformance testing tool for HTTP/2 implementation.	(https://github.com/summerwind/h2spec)
h2t	Scans a website and suggests security headers to apply.	(https://github.com/gildasio/h2t)
h8mail	Email OSINT and password breach hunting.	(https://github.com/khast3x/h8mail)
habu	Python Network Hacking Toolkit.	(https://github.com/portantier/habu)
hackersh	A shell for with Pythonect-like syntax, including wrappers for commonly used security tools.	(http://www.hackersh.org/)
hackredis	A simple tool to scan and exploit redis servers.	(https://github.com/Ridter/hackredis)

Name	Description	Website
hackrf	Driver for HackRF, allowing general purpose software defined radio (SDR).	(https://github.com/mossmann/hackrf)
haiti	Hash type identifier (CLI & lib).	(https://noraj.github.io/haiti/)
haka	A collection of tool that allows capturing TCP/IP packets and filtering them based on Lua policy files.	(https://github.com/haka-security/haka)
hakku	Simple framework that has been made for penetration testing tools.	(https://github.com/4shadoww/hakkuframework)
hakrawler	Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application.	(https://github.com/hakluke/hakrawler)
hakrevdns	Small, fast tool for performing reverse DNS lookups en masse.	(https://github.com/hakluke/hakrevdns)
halberd	Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing.	(http://halberd.superadditive.com/)
halcyon	A repository crawler that runs checksums for static files found within a given git repository.	(http://www.blackhatlibrary.net/Halcyon)
halcyon-ide	First IDE for Nmap Script (NSE) Development.	(https://halcyon-ide.org/)
hamster	Tool for HTTP session sidejacking.	(http://hamster.erratasec.com/)
handle	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,..	(http://www.tarasco.org/security/handle/index.html)
harness	Interactive remote PowerShell Payload.	(https://github.com/Rich5/Harness)
harpoon	CLI tool for open source and threat intelligence.	(https://github.com/Te-k/harpoon)
hasere	Discover the vhosts using google and bing.	(https://github.com/galkan/hasere)
hash-buster	A python script which scraps online hash crackers to find cleartext of a hash.	(https://github.com/UltimateHackers/Hash-Buster/)
hash-extender	A hash length extension attack tool.	(https://github.com/iagox86/hash_extender)
hash-identifier	Software to identify the different types of hashes used to encrypt data and especially passwords.	(https://github.com/blackploit/hash-identifier)
hashcat	Multithreaded advanced password recovery utility	(https://hashcat.net/hashcat)
hashcat-utils	Set of small utilities that are useful in advanced password cracking	(https://github.com/hashcat/hashcat-utils)
hashcatch	Capture handshakes of nearby WiFi networks automatically.	(https://github.com/staz0t/hashcatch/releases)
hashcheck	Search for leaked passwords while maintaining a high level of privacy using the k-anonymity method.	(https://github.com/Telefonica/HashCheck)
hashdb	A block hash toolkit.	(https://github.com/NPS-DEEP/hashdb/)
hashdeep	Cross-platform tools to message digests for any number of files.	(https://github.com/jessek/hashdeep)
hasher	A tool that allows you to quickly hash plaintext strings, or compare hashed values with a plaintext locally.	(https://github.com/ChrisTruncer/Hasher)
hashfind	A tool to search files for matching password hash types and other interesting data.	(https://github.com/rurapenthe/hashfind)
hashid	Software to identify the different types of hashes used to encrypt data.	(https://github.com/psypanda/hashID)
hashpump	A tool to exploit the hash length extension attack in various hashing algorithms.	(https://github.com/bwall/HashPump)
hashrat	Hashing tool supporting MD5, SHA1, SHA256, SHA512, Whirlpool, JH and their HMAC.	(https://github.com/ColumPaget/Hashrat)
hashtag	A python script written to parse and identify password hashes.	(https://github.com/SmeegeSec/HashTag)
hatcloud	Bypass CloudFlare with Ruby.	(https://github.com/HatBashBR/HatCloud)
hate-crack	A tool for automating cracking methodologies through Hashcat.	(https://github.com/trustedsec/hate_crack)
haystack	A Python framework for finding C structures from process memory - heap analysis - Memory structures forensics.	(https://github.com/trolldbois/python-haystack)
hbad	This tool allows you to test clients on the heartbleed bug.	(http://www.curesec.com/)
hcraft	HTTP Vuln Request Crafter	(http://sourceforge.net/projects/hcraft/)
hcxdumptool	Small tool to capture packets from wlan devices	(https://github.com/ZerBea/hcxdumptool)
hcxkeys	Set of tools to generate plainmasterkeys (rainbowtables) and hashes for hashcat and John the Ripper	(https://github.com/ZerBea/hcxkeys)
hcxtools	Portable solution for capturing wlan traffic and conversion to hashcat and John the Ripper formats	(https://github.com/ZerBea/hcxtools)
hdcp-genkey	Generate HDCP source and sink keys from the leaked master key.	(https://github.com/rjw57/hdcp-genkey)
hdmi-sniff	HDMI DDC (I2C) inspection tool. It is designed to demonstrate just how easy it is to recover HDCP crypto keys from HDMI devices.	(https://github.com/ApertureLabsLtd/hdmi-sniff)
heaptrace	Helps visualize heap operations for pwn and debugging.	(https://github.com/Arinerron/heaptrace)
heartbleed-honeypot	Script that listens on TCP port 443 and responds with completely bogus SSL heartbeat responses, unless it detects the start of a byte pattern similar to that used in Jared Stafford's	(http://packetstormsecurity.com/files/126068/hb_honeypot.pl.txt)
heartleech	Scans for systems vulnerable to the heartbleed bug, and then download them.	(https://github.com/robertdavidgraham/heartleech)
hekatomb	Extract and decrypt all credentials from all domain computers using DPAPI.	(https://github.com/ProcessusT/HEKATOMB)
hellraiser	Vulnerability Scanner.	(https://github.com/m0nad/HellRaiser)
hemingway	A simple and easy to use spear phishing helper.	(https://github.com/ytisf/hemingway)
hercules-payload	A special payload generator that can bypass all antivirus software.	(https://github.com/EgeBalci/HERCULES)
hetty	HTTP toolkit for security research. Aims to become an open source alternative to commercial software like Burp Suite Pro.	(https://github.com/dstotijn/hetty)
hex2bin	Converts Motorola and Intel hex files to binary.	(http://hex2bin.sourceforge.net/)
hexinject	A very versatile packet injector and sniffer that provides a command-line framework for raw network access.	(http://hexinject.sourceforge.net)
hexorbase	A database application designed for administering and auditing multiple database servers simultaneously from a centralized location. It is capable of performing SQL queries and bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL).	(https://code.google.com/p/hexorbase/)
hexyl	Colored command-line hex viewer	(https://github.com/sharkdp/hexyl)
hharp	This tool can perform man-in-the-middle and switch flooding attacks. It has 4 major functions, 3 of which attempt to man-in-the-middle one or more computers on a network with a passive method or flood type method.	(http://packetstormsecurity.com/files/81368/Hackers-Hideaway-ARP-Attack-Tool.html)
hidattack	HID Attack (attacking HID host implementations)	(http://mulliner.org/bluetooth/hidattack.php)
hiddeneye	Modern phishing tool with advanced functionality.	(https://github.com/DarkSecDevelopers/HiddenEye)

Name	Description	Website
hiddeneye-legacy	Modern Phishing Tool With Advanced Functionality.	(https://github.com/DarkSecDevelopers/HiddenEye-Legacy)
hikpwn	A simple scanner for Hikvision devices with basic vulnerability scanning capabilities written in Python 3.8.	(https://github.com/4n4nk3/HikPwn)
hlextend	Pure Python hash length extension module.	(https://github.com/stephenbradshaw/hlextend)
hodor	A general-use fuzzer that can be configured to use known-good input and delimiters in order to fuzz specific locations.	(https://github.com/nccgroup/hodor)
holehe	A tool for Efficiently finding registered accounts from emails.	(https://github.com/megadose/holehe)
hollows-hunter	Scans all running processes. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches).	(https://github.com/hasherezade/hollows_hunter)
homepwn	Swiss Army Knife for Pentesting of IoT Devices.	(https://github.com/ElevenPaths/HomePWN)
honeycreds	Network credential injection to detect responder and other network poisoners.	(https://github.com/Ben0xA/HoneyCreds)
honeyd	A small daemon that creates virtual hosts on a network.	(https://github.com/DataSoft/Honeyd/)
honeypy	A low interaction Honeypot.	(https://github.com/foospidy/HoneyPy)
honggfuzz	A general-purpose fuzzer with simple, command-line interface.	(https://code.google.com/p/honggfuzz/)
honssh	A high-interaction Honey Pot solution designed to log all SSH communications between a client and server.	(https://code.google.com/p/honssh/)
hookanalyser	A hook tool which can be potentially helpful in reversing applications and analyzing malware. It can hook to an API in a process and search for a pattern in memory or dump the buffer.	(http://hookanalyser.blogspot.de/)
hookshot	Integrated web scraper and email account data breach comparison tool.	(https://github.com/andrew-vii/hookshot/)
hoover	Wireless Probe Requests Sniffer.	(https://github.com/xme/hoover/)
hoper	Trace URL's jumps across the rel links to obtain the last URL.	(https://github.com/gabamnml/hoper)
hopper	Reverse engineering tool that lets you disassemble, decompile and debug your applications.	(https://www.hopperapp.com/download.html?)
hoppy	A python script which tests http methods for configuration issues leaking information or just to see if they are enabled.	(https://labs.portcullis.co.uk/downloads/)
horusec	Static code analysis to identify security flaws for many languages.	(https://github.com/ZupIT/horusec)
host-extract	Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL.	(https://code.google.com/p/host-extract/)
hostapd-wpe	Modified hostapd to facilitate AP impersonation attacks.	(https://w1.fi/hostapd/)
hostbox-ssh	A ssh password/account scanner.	(http://stridsmanit.wordpress.com/2012/12/02/brute-forcing-passwords-with-hostbox-ssh-1-1/)
hosthunter	A recon tool for discovering hostnames using OSINT techniques.	(https://github.com/SpiderLabs/HostHunter)
hotpatch	Hot patches executables on Linux using .so file injection.	(http://www.selectiveintellect.com/hotpatch.html)
hotspotter	Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names.	(http://www.remote-exploit.org/?page_id=418)
howmanypeoplearearound	Count the number of people around you by monitoring wifi signals.	(https://github.com/schollz/howmanypeoplearearound)
hpfeeds	Honeynet Project generic authenticated datafeed protocol.	(https://github.com/rep/hpfeeds)
hping	A command-line oriented TCP/IP packet assembler/analyzer.	(http://www.hping.org)
hqlmap	A tool to exploit HQL Injections.	(https://github.com/PaulSec/HQLmap)
hsecscan	A security scanner for HTTP response headers.	(https://github.com/riramar/hsecscan)
htcap	A web application analysis tool for detecting communications between javascript and the server.	(https://github.com/segment-srl/htcap)
htexploit	A Python script that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process	(http://www.mkit.com.ar/labs/htexploit/)
htpwdscan	A python HTTP weak pass scanner.	(https://github.com/lijiejie/htpwdScan)
htrosbif	Active HTTP server fingerprinting and recon tool.	(https://github.com/lkarsten/htrosbif)
htshells	Self contained web shells and other attacks via .htaccess files.	(https://github.com/wireghoul/htshells)
http-enum	A tool to enumerate the enabled HTTP methods supported on a webserver.	(https://www.thexero.co.uk/tools/http-enum/)
http-fuzz	A simple http fuzzer.	(none)
http-put	Simple http put perl script.	()
http-traceroute	This is a python script that uses the Max-Forwards header in HTTP and SIP to perform a traceroute-like scanning functionality.	(http://packetstormsecurity.com/files/107167/Traceroute-Like-HTTP-Scanner.html)
http2smugl	Http2Smugl - Tool to detect and exploit HTTP request smuggling in cases it can be achieved via HTTP/2 -> HTTP/1.1 conversion.	(https://github.com/neex/http2smugl)
httpbog	A slow HTTP denial-of-service tool that works similarly to other attacks, but rather than leveraging request headers or POST data Bog consumes sockets by slowly reading responses.	(http://sourceforge.net/projects/httpbog/)
httpforge	A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the security of Web servers, apps, and sites. An accompanying Python library is available for extensions.	(http://packetstormsecurity.com/files/98109/HTTPForge.02.01.html)
httpgrep	A python tool which scans for HTTP servers and finds given strings in HTTP body and HTTP response headers.	(https://nullsecurity.net/tools/scanner.html)
httping	A ping-like tool for HTTP requests	(https://www.vanheusden.com/httping/)
httppwnly	"Repeater" style XSS post-exploitation tool for mass browser control.	(https://github.com/Danladi/HttpPwnly)
httprecon	Tool for web server fingerprinting, also known as http fingerprinting.	(http://www.computec.ch/projekte/httprecon/?s=download)
httprint	A web server fingerprinting tool.	(http://www.net-square.com/httprint.html)
httprint-win32	A web server fingerprinting tool (Windows binaries).	(http://net-square.com/httprint)
httprobe	Take a list of domains and probe for working HTTP and HTTPS servers	(https://github.com/tomnomnom/httprobe)
httpry	A specialized packet sniffer designed for displaying and logging HTTP traffic.	(http://dumpsterventures.com/jason/httpry/)
httpscreenshot	A tool for grabbing screenshots and HTML of large numbers of websites.	(https://github.com/breenmachine/httpscreenshot)
httpsniff	Tool to sniff HTTP responses from TCP/IP based networks and save contained files locally for later review.	(http://www.sump.org/projects/httpsniff/)

Name	Description	Website
httpsscanner	A tool to test the strength of a SSL web server.	↗ (https://code.google.com/p/libre-tools/)
httptunnel	Creates a bidirectional virtual data connection tunnelled in HTTP requests	↗ (https://github.com/larsbrinkhoff/httptunnel)
httpx	A fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library.	↗ (https://github.com/projectdiscovery/httpx)
httrack	An easy-to-use offline browser utility	↗ (https://www.httrack.com/)
hubbit-sniffer	Simple application that listens for WIFI-frames and records the mac-address of the sender and posts them to a REST-api.	↗ (https://github.com/cthit/hubbIT-sniffer)
hulk	A webserver DoS tool (Http Unbearable Load King) ported to Go with some additional features.	↗ (https://github.com/grafov/hulk)
hungry-interceptor	Intercepts data, does something with it, stores it.	↗ (https://github.com/nbuechler/hungry-interceptor)
hurl-encoder	Hexadecimal & URL (en/de)coder.	↗ (https://github.com/fnord0/hURL)
hwk	Collection of packet crafting and wireless network flooding tools	↗ (http://www.nullsecurity.net/)
hxd	Freeware Hex Editor and Disk Editor.	↗ (https://mh-nexus.de/en/hxd/)
hyde	Just another tool in C to do DDoS (with spoofing).	↗ (https://github.com/CoolerVoid/Hyde)
hydra	Very fast network logon cracker which support many different services	↗ (https://github.com/vanhauser-thc/thc-hydra)
hyenae	Flexible platform independent packet generator.	↗ (http://sourceforge.net/projects/hyenae/)
hyperfox	A security tool for proxying and recording HTTP and HTTPs traffic.	↗ (https://github.com/xiam/hyperfox)
hyperion-crypter	A runtime encrypter for 32-bit and 64-bit portable executables.	↗ (http://nullsecurity.net/tools/binary.html)
i2pd	A full-featured C++ implementation of the I2P router	↗ (https://i2pd.website/)
iaito	Qt and C++ GUI for radare2 reverse engineering framework	↗ (https://github.com/radareorg/iaito)
iaxflood	IAX flooder.	↗ (http://www.hackingexposedvoip.com/)
iaxscan	A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts.	↗ (http://code.google.com/p/iaxscan/)
ibrute	An AppleID password bruteforce tool. It uses Find My Iphone service API, where bruteforce protection was not implemented.	↗ (https://github.com/hackappcom/ibrute/)
icloudbrutter	Tool for AppleID Bruteforce.	↗ (https://github.com/m4ll0k/iCloudBrutter)
icmpquery	Send and receive ICMP queries for address mask and current time.	↗ (http://www.angio.net/security/)
icmpsh	Simple reverse ICMP shell.	↗ (https://github.com/inquisb/icmpsh)
icmptx	IP over ICMP tunnel.	↗ (http://thomer.com/icmptx/)
id-entify	Search for information related to a domain: Emails - IP addresses - Domains - Information on WEB technology - Type of Firewall - NS and MX records.	↗ (https://github.com/BillyV4/ID-entify)
ida-free	Freeware version of the world's smartest and most feature-full disassembler.	↗ (https://www.hex-rays.com/products/ida/)
idb	A tool to simplify some common tasks for iOS pentesting and research.	↗ (https://rubygems.org/gems/idb)
identywaf	Blind WAF identification tool.	↗ (https://github.com/stamparm/identYwaf)
idswakeup	A collection of tools that allows to test network intrusion detection systems.	↗ (http://www.hsc.fr/ressources/outils/idswakeup/index.html.en)
ifchk	A network interface promiscuous mode detection tool.	↗ (http://www.noorg.org/ifchk/)
ifuzz	A binary file fuzzer with several options.	↗ (http://www.fuzzing.org/)
iheartxor	A tool for bruteforcing encoded strings within a boundary defined by a regular expression. It will bruteforce the key value range of 0x1 through 0x255.	↗ (http://hooked-on-mnemonics.blogspot.com.es/p/iheartxor.html)
iis-shortname-scanner	An IIS shortname Scanner.	↗ (https://github.com/lijiejie/IIS_shortname_Scanner)
iisbruteforcer	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.	↗ (http://www.open-labs.org/)
ike-scan	A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers.	↗ (http://www.nta-monitor.com/tools/ike-scan/)
ikecrack	An IKE/IPSec crack tool designed to perform Pre-Shared-Key analysis of RFC compliant aggressive mode authentication	↗ (http://sourceforge.net/projects/ikecrack/)
ikeforce	A command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.	↗ (https://github.com/SpiderLabs/ikeforce)
ikeprobe	Determine vulnerabilities in the PSK implementation of the VPN server.	↗ (http://www.ernw.de/download/ikeprobe.zip)
ikeprober	Tool crafting IKE initiator packets and allowing many options to be manually set. Useful to find overflows, error conditions and identifiyng vendors	↗ (http://ikecrack.sourceforge.net/)
ilo4-toolbox	Toolbox for HPE iLO4 analysis.	↗ (https://github.com/airbus-seclab/ilo4_toolbox)
ilty	An interception phone system for VoIP network.	↗ (http://chdir.org/~nico/ilty/)
imagegrep	Grep word in pdf or image based on OCR.	↗ (https://github.com/coderofsalvation/imagegrep-bash)
imagejs	Small tool to package javascript into a valid image file.	↗ (https://github.com/jklmnn/imagejs)
imagemounter	Command line utility and Python package to ease the (un)mounting of forensic disk images.	↗ (https://github.com/ralphje/imagemounter)
imhex	A Hex Editor for Reverse Engineers, Programmers and people that value their eye sight when working at 3 AM.	↗ (https://github.com/WerWolv/ImHex)
impacket-ba	Collection of classes for working with network protocols.	↗ (https://github.com/fortra/impacket)
impulse	Modern Denial-of-service ToolKit.	↗ (https://github.com/LimerBoy/Impulse)
inception	A FireWire physical memory manipulation and hacking tool exploiting IEEE 1394 SBP DMA.	↗ (http://www.breaknenter.org/projects/inception/)
indx2csv	An advanced parser for INDX records.	↗ (https://github.com/jschicht/Indx2Csv)
indxcarver	Carve INDX records from a chunk of data.	↗ (https://github.com/jschicht/IndxCarver)
indxparse	A Tool suite for inspecting NTFS artifacts.	↗ (http://www.williballenthin.com/forensics/mft/indxparse/)
inetsim	A software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.	↗ (http://www.inetsim.org/)
infection-monkey	Automated security testing tool for networks.	↗ (https://github.com/guardicore/monkey)
infip	A python script that checks output from netstat against RBLs from Spamhaus.	↗ (http://packetstormsecurity.com/files/104927/infIP.1-Blacklist-Checker.html)
infoga	Tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers).	↗ (https://github.com/m4ll0k/infoga)
inguma	A free penetration testing and vulnerability discovery toolkit entirely written in python. Framework includes modules to discover hosts, gather information about, fuzz targets, brute force usernames and passwords, exploits, and a disassembler.	↗ (http://inguma.sourceforge.net)
injectus	CRLF and open redirect fuzzer.	↗ (https://github.com/BountyStrike/Injectus)

Name	Description	Website
innounp	Inno Setup Unpacker.	(https://sourceforge.net/projects/innounp/files/innounp/)
inquisitor	OSINT Gathering Tool for Companies and Organizations.	(https://github.com/penafieljlm/inquisitor)
insanity	Generate Payloads and Control Remote Machines .	(https://github.com/4w4k3/Insanity-Framework)
instagramosint	An Instagram Open Source Intelligence Tool.	(https://github.com/sc1341/InstagramOSINT/)
instashell	Multi-threaded Instagram Brute Forcer without password limit.	(https://github.com/thelinuxchoice/instashell)
intelmq	A tool for collecting and processing security feeds using a message queuing protocol.	(https://github.com/certtools/intelmq)
intelplot	OSINT Tool to Mark Points on Offline Map.	(https://github.com/itsmehacker/IntelPlot)
intensio-obfuscator	Obfuscate a python code 2 and 3.	(https://github.com/Hnfull/Intensio-Obfuscator)
interactsh-client	Open-Source Solution for Out of band Data Extraction.	(https://github.com/projectdiscovery/interactsh)
intercepter-ng	A next generation sniffer including a lot of features: capturing passwords/hashes, sniffing chat messages, performing man-in-the-middle attacks, etc.	(http://sniff.su/download.html)
interlace	Easily turn single threaded command line applications into a fast, multi-threaded application with CIDR and glob support.	(https://github.com/codingo/Interlace/releases)
interrogate	A proof-of-concept tool for identification of cryptographic keys in binary material (regardless of target operating system), first and foremost for memory dump analysis and forensic usage.	(https://github.com/carmaa/interrogate)
intersect	Post-exploitation framework.	(https://github.com/ohdae/Intersect.5)
intrace	Traceroute-like application piggybacking on existing TCP connections	(http://intrace.googlecode.com)
inundator	An ids evasion tool, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real attack.	(http://inundator.sourceforge.net/)
inurlbr	Advanced search in the search engines - Inurl scanner, dorker, exploiter.	(https://code.google.com/p/inurlbr/)
inviteflood	Flood a device with INVITE requests	(https://launchpad.net/~wagungs/+archive/kali-linux/+build/4386635)
invoke-cradlecrafter	PowerShell Remote Download Cradle Generator & Obfuscator.	(https://github.com/danielbohannon/Invoke-CradleCrafter)
invoke-dosfuscation	Cmd.exe Command Obfuscation Generator & Detection Test Harness.	(https://github.com/danielbohannon/Invoke-DOSfuscation)
invoke-obfuscation	PowerShell Obfuscator.	(https://github.com/danielbohannon/Invoke-Obfuscation)
inzider	This is a tool that lists processes in your Windows system and the ports each one listen on.	(http://ntsecurity.nu/toolbox/inzider/)
iodine	Tunnel IPv4 data through a DNS server	(https://code.kryo.se/iodine)
iosforensic	iOS forensic tool https://www.owasp.org/index.php/Projects/OWASP_iOSForensic	(https://github.com/Flo354/iOSForensic)
ip-https-tools	Tools for the IP over HTTPS (IP-HTTPS) Tunneling Protocol.	(https://github.com/takeshixx/ip-https-tools)
ip-tracer	Track and retrieve any ip address information.	(https://github.com/Rajkumrdusad/IP-Tracer)
ip2clue	A small memory/CPU footprint daemon to lookup country (and other info) based on IP (v4 and v6).	(http://kernel.embedromix.ro/us/)
ipaudit	Monitors network activity on a network.	(http://ipaudit.sourceforge.net)
ipba2	IOS Backup Analyzer.	(http://www.ipbackupanalyzer.com/)
ipcountry	Fetches IPv4 ranges of given country in host and cidr format.	(https://nullsecurity.net/tools/misc.html)
ipdecap	Can decapsulate traffic encapsulated within GRE, IPIP, 6in4, ESP (ipsec) protocols, and can also remove IEEE 802.1Q (virtual lan) header.	(http://www.loicp.eu/ipdecap#dependances)
iphoneanalyzer	Allows you to forensically examine or recover date from in iOS device.	(http://www.crypticbit.com/zen/products/iphoneanalyzer)
ipmipwn	IPMI cipher 0 attack tool.	(https://github.com/AnarchyAngel/IPMIPWN)
ipmitool	Command-line interface to IPMI-enabled devices	(https://github.com/ipmitool/ipmitool)
ipobfuscator	A simple tool to convert the IP to a DWORD IP.	(https://github.com/OsandaMalith/IPObfuscator)
ipscan	A very fast IP address and port scanner.	(https://github.com/angryip/ipscan)
ipsourcebypass	This Python script can be used to bypass IP source restrictions using HTTP headers.	(https://github.com/p0dalirius/ipsourcebypass)
iptodomain	This tool extract domains from IP address based in the information saved in virustotal.	(https://github.com/Hackplayers/iptodomain)
iptv	Search and brute force illegal iptv server.	(https://github.com/Pinperepette/IPTV)
iputils	Network monitoring tools, including ping	(https://github.com/iputils/iputils)
ipv4bypass	Using IPv6 to Bypass Security.	(https://github.com/milo2012/ipv4Bypass)
ipv666	Golang IPv6 address enumeration.	(https://github.com/lavalamp-/ipv666)
ipv6toolkit	SI6 Networks' IPv6 Toolkit.	(http://www.si6networks.com/tools/ipv6toolkit/)
ircsnapshot	Tool to gather information from IRC servers.	(https://github.com/bwall/ircsnapshot)
irpas	Internetwork Routing Protocol Attack Suite.	(http://phenoelit-us.org/irpas)
isf	An exploitation framework based on Python.	(https://github.com/dark-lbp/isf)
isip	Interactive sip toolkit for packet manipulations, sniffing, man in the middle attacks, fuzzing, simulating of dos attacks.	(https://github.com/halitalptekin/isip)
isme	Scans a VOIP environment, adapts to enterprise VOIP, and exploits the possibilities of being connected directly to an IP Phone VLAN.	(https://packetstormsecurity.com/files/123534/IP-Phone-Scanning-Made-Easy.12.html)
isr-form	Simple html parsing tool that extracts all form related information and generates reports of the data. Allows for quick analyzing of data.	(http://www.infobyte.com.ar/)
issniff	Internet Session Sniffer.	(https://github.com/juphoff/issniff)
ivre	Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,...	(https://ivre.rocks/)
ivre-docs	Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (documentation)	(https://ivre.rocks/)
ivre-web	Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (web application)	(https://ivre.rocks/)
ja3	Standard for creating SSL client fingerprints in an easy to produce and shareable way.	(https://github.com/salesforce/ja3)
jaadas	Joint Advanced Defect assEsment for android applications.	(https://github.com/flankerhqd/JAADAS/)
jackdaw	Collect all information in your domain, show you graphs on how domain objects interact with each-other and how to exploit these interactions.	(https://github.com/skelsec/jackdaw)
jad	Java decompiler	(https://varaneckas.com/jad)
jadx	Command line and GUI tools to produce Java source code from Android Dex and APK files	(https://github.com/skylot/jadx)
jaeles	The Swiss Army knife for automated Web Application Testing.	(https://github.com/jaeles-project/jaeles)

Name	Description	Website
jaidam	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.	(https://github.com/stasinopoulos/jaidam)
jast	Just Another Screenshot Tool.	(https://github.com/mikehacksthings/jast)
javasnoop	A tool that lets you intercept methods, alter data and otherwise hack Java applications running on your computer	(https://code.google.com/p/javasnoop/)
jboss-autopwn	A JBoss script for obtaining remote shell access.	(https://github.com/SpiderLabs/jboss-autopwn)
jbrofuzz	Web application protocol fuzzer that emerged from the needs of penetration testing.	(http://sourceforge.net/projects/jbrofuzz/)
jbrute	Open Source Security tool to audit hashed passwords.	(http://sourceforge.net/projects/jbrute/)
jcrack	A utility to create dictionary files that will crack the default passwords of select wireless gateways	(http://www.thedrahos.net/jcrack/)
jd-cli	Command line Java Decompiler.	(https://github.com/kwart/jd-cli)
jd-gui	A standalone graphical utility that displays Java source codes of .class files.	(https://github.com/java-decompiler/jd-gui)
jdeserialize	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.	(https://github.com/frohoff/jdeserialize/)
jeangrey	A tool to perform differential fault analysis attacks (DFA).	(https://github.com/SideChannelMarvels/JeanGrey)
jeb-android	Android decompiler.	(https://www.pnfsoftware.com/jeb/android)
jeb-arm	Arm decompiler.	(https://www.pnfsoftware.com/jeb/arm)
jeb-intel	Intel decompiler.	(https://www.pnfsoftware.com/jeb/intel)
jeb-mips	Mips decompiler.	(https://www.pnfsoftware.com/jeb/mips)
jeb-webasm	WebAssembly decompiler.	(https://www.pnfsoftware.com/jeb/#wasm)
jeopardize	A low(zero) cost threat intelligence & response tool against phishing domains.	(https://github.com/utkusen/jeopardize)
jexboss	Jboss verify and Exploitation Tool.	(https://github.com/joaomatosf/jexboss)
jhead	EXIF JPEG info parser and thumbnail remover	(http://www.sentex.net/~mwandel/jhead/)
jira-scan	A simple remote scanner for Atlassian Jira	(https://github.com/bcoles/jira_scan)
jndi-injection-exploit	A tool which generates JNDI links can start several servers to exploit JNDI Injection vulnerability, like Jackson, Fastjson, etc.	(https://github.com/welk1n/JNDI-Injection-Exploit)
jnetmap	A network monitor of sorts.	(https://sourceforge.net/projects/jnetmap/files/jNetMap%200.5.5-RC2/)
john	John the Ripper password cracker	(https://www.openwall.com/john)
johnny	GUI for John the Ripper.	(http://openwall.info/wiki/john/johnny)
jok3r	Network and Web Pentest Framework.	(https://github.com/koutto/jok3r)
jomplug	This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components.	(http://packetstormsecurity.com/files/121390/Janissaries-Joomla-Fingerprint-Tool.html)
jondo	Redirects internet traffic trough a mix of proxy servers to hide the origin of the requests.	(https://anonymous-proxy-servers.net/)
jooforce	A Joomla password brute force tester.	(https://github.com/rastating/jooforce)
joomlascan	Joomla scanner scans for known vulnerable remote file inclusion paths and files.	(http://packetstormsecurity.com/files/62126/joomlascan.2.py.txt.html)
joomlavs	A black box, Ruby powered, Joomla vulnerability scanner.	(https://github.com/rastating/joomlavs)
joomscan	Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site.	(http://joomscan.sourceforge.net/)
jpegdump	Tool to analyzse JPEG images Reads binary files and parses the JPEG markers inside them.	(https://blog.didierstevens.com/2019/04/28/update-jpegdump-py-version-0-7/)
jpexs-decompiler	JPEXS Free Flash Decompiler.	(https://github.com/jindrapetrik/jpexs-decompiler)
jsearch	Simple script that grep infos from javascript files.	(https://github.com/incogbyte/jsearch)
jsfuck	Write any JavaScript with 6 Characters: []()!+.	(https://github.com/aemkei/jsfuck)
jshell	Get a JavaScript shell with XSS.	(https://github.com/s0md3v/JShell)
jsonbee	A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP).	(https://github.com/zigoo0/JSONBee)
jsparser	Parse javascript using Tornado and JSBeautifier to discover interesting enpoints.	(https://github.com/nahamsec/JSParser)
jsql-injection	A Java application for automatic SQL database injection.	(https://github.com/ron190/jsql-injection)
jstillery	Advanced JavaScript Deobfuscation via Partial Evaluation.	(https://github.com/mindedsecurity/JStillery)
juicy-potato	A sugared version of RottenPotatoNG, with a bit of juice.	(https://github.com/ohpe/juicy-potato)
junkie	A modular packet sniffer and analyzer.	(https://github.com/securactive/junkie)
justdecompile	The decompilation engine of JustDecompile.	(https://github.com/telerik/JustDecompileEngine/releases)
juumla	Python tool created to identify Joomla version, scan for vulnerabilities and search for config files.	(https://github.com/oppsec/juumla)
jwscan	Scanner for Jar to EXE wrapper like Launch4j, Exe4j, JSmooth, Jar2Exe.	(https://github.com/katjahahn/JWScan)
jwt-cracker	JWT brute force cracker written in C.	(https://github.com/brendan-rius/c-jwt-cracker)
jwt-hack	A tool for hacking / security testing to JWT.	(https://github.com/hahwul/jwt-hack)
jwt-key-recovery	Recovers the public key used to sign JWT tokens.	(https://github.com/FlorianPicca/JWT-Key-Recovery)
jwt-tool	Toolkit for validating, forging and cracking JWTs (JSON Web Tokens).	(https://github.com/ticarpi/jwt_tool)
jwtcat	Script performs offline brute-force attacks against JSON Web Token (JWT)	(https://github.com/aress31/jwtcat)
jynx2	An expansion of the original Jynx LD_PRELOAD rootkit	(http://www.blackhatlibrary.net/Jynx2)
k55	Linux x86_64 Process Injection Utility.	(https://github.com/josh0xA/K55)
kacak	Tools for penetration testers that can enumerate which users logged on windows system.	(https://github.com/galkan/kacak)
kadimus	LFI Scan & Exploit Tool.	(https://github.com/P0cL4bs/Kadimus)
kalibrate-rtl	Fork of http://thre.at/kalibrate/ for use with rtl-sdr devices.	(https://github.com/steve-m/kalibrate-rtl)
kamerka	Build interactive map of cameras from Shodan.	(https://github.com/woj-ciech/kamerka)
katana-framework	A framework that seekss to unite general auditing tools, which are general pentesting tools (Network,Web,Desktop and others).	(https://github.com/PowerScript/KatanaFramework)
katana-pd	Crawling and spidering framework.	(https://github.com/projectdiscovery/katana)
katsnoop	Utility that sniffs HTTP Basic Authentication information and prints the base64 decoded form.	(http://packetstormsecurity.com/files/52514/katsnoop.tbz2.html)

Name	Description	Website
kautilya	Pwnage with Human Interface Devices using Teensy++2.0 and Teensy 3.0 devices.	(https://github.com/samratashok/Kautilya/releases)
kcptun	A Secure Tunnel Based On KCP with N:M Multiplexing	(https://github.com/xtaci/kcptun)
keimpx	Tool to verify the usefulness of credentials across a network over SMB.	(http://code.google.com/p/keimpx/)
kekeo	A little toolbox to play with Microsoft Kerberos in C.	(https://github.com/gentilkiwi/kekeo)
kerbcrack	Kerberos sniffer and cracker for Windows.	(http://ntsecurity.nu/toolbox/kerbcrack/)
kerberoast	Kerberoast attack -pure python-.	(https://github.com/skelsec/kerberoast)
kerbrute	A tool to perform Kerberos pre-auth bruteforcing.	(https://github.com/ropnop/kerbrute)
kernelpop	Kernel privilege escalation enumeration and exploitation framework.	(https://github.com/spencerdodd/kernelpop)
keye	Recon tool detecting changes of websites based on content-length differences.	(https://github.com/clirimemini/Keye)
kh2hc	Convert OpenSSH known_hosts file hashed with HashKnownHosts to hashes crackable by Hashcat.	(https://github.com/noraj/kh2hc)
khc	A small tool designed to recover hashed known_hosts fiels back to their plain-text equivalents.	(http://packetstormsecurity.com/files/87003/Known-Host-Cracker.2.html)
kickthemout	Kick devices off your network by performing an ARP Spoof attack.	(https://github.com/k4m4/kickthemout)
killcast	Manipulate Chromecast Devices in your Network.	(https://github.com/thewhiteh4t/killcast)
killerbee	Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks.	(https://github.com/riverloopsec/killerbee)
kimi	Script to generate malicious debian packages (debain trojans).	(https://github.com/ChaitanyaHaritash/kimi)
kippo	A medium interaction SSH honeypot designed to log brute force attacks and most importantly, the entire shell interaction by the attacker.	(https://github.com/desaster/kippo)
kismet	802.11 layer2 wireless network detector, sniffer, and intrusion detection system	(https://www.kismetwireless.net/)
kismet-earth	Various scripts to convert kismet logs to kml file to be used in Google Earth.	(https://www.blackarch.org/)
kismet2earth	A set of utilities that convert from Kismet logs to Google Earth .kml format	(http://code.google.com/p/kismet2earth/)
kismon	GUI client for kismet (wireless scanner/sniffer/monitor).	(https://www.salecker.org/software/kismon.html)
kiterunner	Contextual Content Discovery Tool.	(https://github.com/assetnote/kiterunner)
kitty-framework	Fuzzing framework written in python.	(https://github.com/cisco-sas/kitty)
klar	Integration of Clair and Docker Registry.	(https://github.com/optiopay/klar)
klee	A symbolic virtual machine built on top of the LLVM compiler infrastructure.	(https://github.com/klee/klee)
klogger	A keystroke logger for the NT-series of Windows.	(http://ntsecurity.nu/toolbox/klogger/)
knock	Subdomain scanner.	(https://github.com/guelfoweb/knock)
knxmap	KNXnet/IP scanning and auditing tool for KNX home automation installations.	(https://github.com/ernw/knxmap)
koadic	A Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire.	(https://github.com/zerosum0x0/koadic)
kolkata	A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion.	(http://www.blackhatlibrary.net/Kolkata)
konan	Advanced Web Application Dir Scanner.	(https://github.com/m4ll0k/Konan)
kraken	A project to encrypt A5/1 GSM signaling using a Time/Memory Tradeoff Attack.	(http://opensource.srlabs.de/projects/a51-decrypt)
krbjack	DNS dynamic update abuse in ADIDNS and MitM attack using Kerberos AP-REQ hijacking.	(https://github.com/almandin/krbjack)
krbrelayx	Kerberos unconstrained delegation abuse toolkit.	(https://github.com/dirkjanm/krbrelayx)
kube-hunter	Hunt for security weaknesses in Kubernetes clusters.	(https://github.com/aquasecurity/kube-hunter)
kubesploit	Cross-platform post-exploitation HTTP/2 Command & Control server.	(https://github.com/cyberark/kubesploit)
kubestriker	A Blazing fast Security Auditing tool for Kubernetes.	(https://github.com/vchinnipilli/kubestriker)
kubolt	Utility for scanning public kubernetes clusters.	(https://github.com/averonesis/kubolt)
kwetza	Python script to inject existing Android applications with a Meterpreter payload.	(https://github.com/sensepost/kwetza)
l0l	The Exploit Development Kit.	(https://github.com/roissy/l0l)
laf	Login Area Finder: scans host/s for login panels.	(https://github.com/takeshixx/laf)
lanmap2	Passive network mapping tool.	(http://github.com/rflynn/lanmap2)
lans	A Multithreaded asynchronous packet parsing/injecting arp spoofer.	(https://github.com/DanMcInerney/LANs.py)
latd	A LAT terminal daemon for Linux and BSD.	(http://sourceforge.net/projects/linux-decnet/files/latd/1.31/)
laudanum	A collection of injectable files, designed to be used in a pentest when SQL injection flaws are found and are in multiple languages for different environments.	(http://laudanum.inguardians.com/#)
lazagne	An open source application used to retrieve lots of passwords stored on a local computer.	(https://github.com/AlessandroZ/LaZagne)
lazydroid	Tool written as a bash script to facilitate some aspects of an Android Assessment	(https://github.com/nccgroup/LazyDroid)
lbd	Load Balancing detector,	(http://ge.mine.nu/code/lbd)
lbmap	Proof of concept scripts for advanced web application fingerprinting, presented at OWASP AppSecAsia 2012.	(https://github.com/wireghoul/lbmap)
ld-shatner	ld-linux code injector.	(https://github.com/sduverger/ld-shatner)
ldap-brute	A semi fast tool to bruteforce values of LDAP injections over HTTP.	(https://github.com/droope/ldap-brute)
ldapdomaindump	Active Directory information dumper via LDAP.	(https://pypi.org/project/ldapdomaindump/#files)
ldapenum	Enumerate domain controllers using LDAP.	(https://gobag.googlecode.com/svn-history/r2/trunk/ldap/ldapenum/)
ldapscripts	Simple shell scripts to handle POSIX entries in an LDAP directory.	(https://sourceforge.net/projects/ldapscripts)
ldeep	In-depth ldap enumeration utility.	(https://github.com/franc-pentest/ldeep)
ldsview	Offline search tool for LDAP directory dumps in LDIF format.	(https://github.com/kgoins/ldsview)
leaklooker	Find open databases with Shodan.	(https://github.com/woj-ciech/LeakLooker)
leena	Symbolic execution engine for JavaScript	(https://github.com/mmicu/leena)
legion	Automatic Enumeration Tool based in Open Source tools.	(https://github.com/carlospolop/legion)
leo	Literate programmer's editor, outliner, and project manager.	(https://github.com/leo-editor/leo-editor/)
leroy-jenkins	A python tool that will allow remote execution of commands on a Jenkins server and its nodes.	(https://github.com/captainhooligan/Leroy-Jenkins)
lethalhta	Lateral Movement technique using DCOM and HTA.	(https://github.com/codewhitesec/LethalHTA)
letmefuckit-scanner	Scanner and Exploit Magento.	(https://github.com/onthefrontline/LetMeFuckIt-Scanner)
leviathan	A mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities.	(https://github.com/leviathan-framework/leviathan)

Name	Description	Website
levye	A brute force tool which is support sshkey, vnckey, rdp, openvpn.	(https://github.com/galkan/levye)
lfi-autopwn	A Perl script to try to gain code execution on a remote server via LFI	(http://www.blackhatlibrary.net/Lfi_autopwn.pl)
lfi-exploiter	This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability..	(http://packetstormsecurity.com/files/124332/LFI-Exploiter.1.html)
lfi-fuzzploit	A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications.	(http://packetstormsecurity.com/files/106912/LFI-Fuzzploit-Tool.1.html)
lfi-image-helper	A simple script to infect images with PHP Backdoors for local file inclusion attacks.	(http://packetstormsecurity.com/files/129871/LFI-Image-Helper.8.html)
lfi-scanner	This is a simple perl script that enumerates local file inclusion attempts when given a specific target.	(http://packetstormsecurity.com/files/102848/LFI-Scanner.0.html)
lfi-sploiter	This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities.	(http://packetstormsecurity.com/files/96056/Simple-Local-File-Inclusion-Exploiter.0.html)
lfifreak	A unique automated LFi Exploiter with Bind/Reverse Shells.	(https://github.com/OsandaMalith/LFiFreak/)
lfimap	Local file inclusion discovery and exploitation tool.	(https://github.com/hansmach1ne/lfimap)
lfisuite	Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner.	(https://github.com/D35m0nd142/LFISuite)
lfle	Recover event log entries from an image by heurisitically looking for record structures.	(https://github.com/williballenthin/LfLe)
lft	A layer four traceroute implementing numerous other features.	(http://pwhois.org/lft/)
lhf	A modular recon tool for pentesting.	(https://github.com/blindfuzzy/LHF)
libbde	A library to access the BitLocker Drive Encryption (BDE) format.	(https://github.com/libyal/libbde)
libc-database	Database of libc offsets to simplify exploitation.	(https://github.com/niklasb/libc-database)
libdisasm	A disassembler library.	(http://bastard.sourceforge.net/libdisasm.html)
libfvde	Library and tools to access FileVault Drive Encryption (FVDE) encrypted volumes.	(https://github.com/libyal/libfvde)
libosmocore	Collection of common code used in various sub-projects inside the Osmocom family of projects.	(https://osmocom.org/projects/libosmocore/wiki/Libosmocore)
libparistraceroute	A library written in C dedicated to active network measurements with examples, such as paris-ping and paris-traceroute.	(https://github.com/libparistraceroute/libparistraceroute)
libpst	Outlook .pst file converter	(https://www.five-ten-sg.com/libpst/)
libtins	High-level, multiplatform C++ network packet sniffing and crafting library.	(https://github.com/mfontanini/libtins)
lief	Library to Instrument Executable Formats.	(https://github.com/lief-project/LIEF/)
liffy	A Local File Inclusion Exploitation tool.	(https://github.com/mzfr/liffy/)
lightbulb	Python framework for auditing web applications firewalls.	(https://github.com/lightbulb-framework/lightbulb-framework)
ligolo-ng	An advanced, yet simple, tunneling tool that uses a TUN interface.	(https://github.com/nicocha30/ligolo-ng/releases)
limeaide	Remotely dump RAM of a Linux client and create a volatility profile for later analysis on your local host.	(https://github.com/kd8bny/LiMEaide)
limelighter	A tool for generating fake code signing certificates or signing real ones.	(https://github.com/Tylous/Limelighter)
linenum	Scripted Local Linux Enumeration & Privilege Escalation Checks	(https://github.com/rebootuser/LinEnum)
linikatz	Tool to attack AD on UNIX.	(https://github.com/portcullislabs/linikatz)
linkedin2username	OSINT Tool: Generate username lists for companies on LinkedIn.	(https://github.com/initstring/linkedin2username)
linkfinder	Discovers endpoint and their parameters in JavaScript files.	(https://github.com/GerbenJavado/LinkFinder)
linset	Evil Twin Attack Bash script - An automated WPA/WPA2 hacker.	(https://github.com/vk496/linset)
linux-exploit-suggester	A Perl script that tries to suggest exploits based OS version number.	(https://github.com/PenturaLabs/Linux_Exploit_Suggester)
linux-exploit-suggester.sh	Linux privilege escalation auditing tool.	(https://github.com/mzet-/linux-exploit-suggester)
linux-inject	Tool for injecting a shared object into a Linux process.	(https://github.com/gaffe23/linux-inject)
linux-smart-enumeration	Linux enumeration tool for pentesting and CTFs with verbosity levels.	(https://github.com/diego-treitos/linux-smart-enumeration)
lisa.py	An Exploit Dev Swiss Army Knife.	(https://github.com/ant4g0nist/lisa.py)
list-urls	Extracts links from webpage.	(http://www.whoppix.net/)
littleblackbox	Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices.	(http://code.google.com/p/littleblackbox/wiki/FAQ)
littlebrother	OSINT tool to get informations on French, Belgian and Swizerland people.	(https://github.com/lulz3xploit/LittleBrother)
lldb	Next generation, high-performance debugger	(https://lldb.llvm.org/)
loadlibrary	Porting Windows Dynamic Link Libraries to Linux.	(https://github.com/taviso/loadlibrary)
local-php-security-checker	A command line tool that checks your PHP application packages with known security vulnerabilities.	(https://github.com/fabpot/local-php-security-checker)
locasploit	Local enumeration and exploitation framework.	(https://github.com/lightfaith/locasploit)
lodowep	Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver system.	(http://www.cqure.net/wp/lodowep/)
log-file-parser	Parser for $LogFile on NTFS.	(https://github.com/jschicht/LogFileParser)
log4j-bypass	Log4j web app tester that includes WAF bypasses.	(https://github.com/cyberqueen-meg/log4j-bypass)
log4j-scan	A fully automated, accurate, and extensive scanner for finding log4j RCE CVE-44228.	(https://github.com/fullhunt/log4j-scan)
logkeys	A GNU/Linux keylogger that worked.	(https://github.com/kernc/logkeys)
logmepwn	A fully automated, reliable, super-fast, mass scanning and validation toolkit for the Log4J RCE CVE-44228 vulnerability.	(https://github.com/0xInfection/LogMePwn)
loic	An open source network stress tool for Windows.	(https://github.com/NewEraCracker/LOIC)
loki-scanner	Simple IOC and Incident Response Scanner.	(https://github.com/Neo23x0/Loki)
lolbas	Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts).	(https://github.com/api0cradle/LOLBAS)
loot	Sensitive information extraction tool.	(https://github.com/GuerrillaWarfare/Loot)
lorcon	Generic library for injecting 802.11 frames	(https://github.com/kismetwireless/lorcon)
lorg	Apache Logfile Security Analyzer.	(https://github.com/jensvoid/lorg)
lorsrf	Find the parameters that can be used to find SSRF or Out-of-band resource load.	(https://github.com/knassar702/lorsrf)
lotophagi	a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases.	(http://packetstormsecurity.com/files/55250/lotophagi.rar.html)
lsrtunnel	Spoofs connections using source routed packets.	(http://www.synacklabs.net/projects/lsrtunnel/)

Name	Description	Website
lte-cell-scanner	LTE SDR cell scanner optimized to work with very low performance RF front ends (8bit A/D, 20dB noise figure).	(https://github.com/Evrytania/LTE-Cell-Scanner)
ltrace	Tracks runtime library calls in dynamically linked programs	(https://www.ltrace.org/)
luksipc	A tool to convert unencrypted block devices to encrypted LUKS devices in-place.	(http://www.johannes-bauer.com/linux/luksipc)
lulzbuster	A very fast and smart web directory and file enumeration tool written in C.	(http://www.nullsecurity.net/tools/scanner.html)
lunar	A UNIX security auditing tool based on several security frameworks.	(https://github.com/lateralblast/lunar)
luyten	An Open Source Java Decompiler Gui for Procyon.	(https://github.com/deathmarine/Luyten)
lynis	Security and system auditing tool to harden Unix/Linux systems	(https://cisofy.com/lynis/)
lyricpass	Tool to generate wordlists based on lyrics.	(https://github.com/initstring/lyricpass)
m3-gen	Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass, this tool intended for adversary simulation and red teaming purpose.	(https://github.com/infosecn1nja/MaliciousMacroMSBuild)
mac-robber	A digital investigation tool that collects data from allocated files in a mounted file system.	(http://www.sleuthkit.org/mac-robber/download.php)
macchanger	A small utility to change your NIC's MAC address	(https://www.gnu.org/software/macchanger)
machinae	A tool for collecting intelligence from public sites/feeds about various security-related pieces of data.	(https://github.com/HurricaneLabs/machinae)
maclookup	Lookup MAC addresses in the IEEE MA-L/OUI public listing.	(https://github.com/paraxor/maclookup)
magescan	Scan a Magento site for information.	(https://github.com/steverobbins/magescan)
magicrescue	Find and recover deleted files on block devices	(http://freshmeat.net/projects/magicrescue/)
magictree	A penetration tester productivity tool designed to allow easy and straightforward data consolidation, querying, external command execution and report generation	(http://www.gremwell.com)
maigret	OSINT username checker. Collect a dossier on a person by username from a huge number of sites.	(https://github.com/soxoj/maigret)
mail-crawl	Tool to harvest emails from website.	(https://raw.githubusercontent.com/galkan/tools/master/mail-crawl/)
mailsend-go	A multi-platform command line tool to send mail via SMTP protocol.	(https://github.com/muquit/mailsend-go)
make-pdf	This tool will embed javascript inside a PDF document.	(http://blog.didierstevens.com/programs/pdf-tools/)
maketh	A packet generator that supports forging ARP, IP, TCP, UDP, ICMP and the ethernet header as well.	(https://packetstormsecurity.com/files/83892/Maketh-Packet-Generator.2.0.html)
malboxes	Builds malware analysis Windows VMs so that you don't have to.	(https://github.com/GoSecure/malboxes)
malcom	Analyze a system's network communication using graphical representations of network traffic.	(https://github.com/tomchop/malcom)
malheur	A tool for the automatic analyze of malware behavior.	(http://www.mlsec.org/malheur/)
malice	VirusTotal Wanna Be - Now with 100% more Hipster.	(https://github.com/maliceio/malice)
maligno	An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS.	(http://www.encripto.no/tools/)
mallory	HTTP/HTTPS proxy over SSH.	(https://github.com/justmao945/mallory)
malmon	Hosting exploit/backdoor detection daemon.	(http://sourceforge.net/projects/malmon/)
malscan	A Simple PE File Heuristics Scanner.	(https://github.com/Ice3man543/MalScan)
maltego	An open source intelligence and forensics application, enabling to easily gather information about DNS, domains, IP addresses, websites, persons, etc.	(https://www.maltego.com/downloads/)
maltrail	Malicious traffic detection system.	(https://github.com/stamparm/maltrail)
maltrieve	Originated as a fork of mwcrawler. It retrieves malware directly from the sources as listed at a number of sites.	(https://github.com/technoskald/maltrieve)
malware-check-tool	Python script that detects malicious files via checking md5 hashes from an offline set or via the virustotal site. It has http proxy support and an update feature.	(http://packetstormsecurity.com/files/93518/Malware-Check-Tool.2.html)
malwareanalyser	A freeware tool to perform static and dynamic analysis on malware.	(http://malwareanalyser.blogspot.de/2011/10/malware-analyser.html)
malwaredetect	Submits a file's SHA1 sum to VirusTotal to determine whether it is a known piece of malware	(http://www.virustotal.com)
malwasm	Offline debugger for malware's reverse engineering.	(https://code.google.com/p/malwasm/)
malybuzz	A Python tool focused in discovering programming faults in network software.	(http://eternal-todo.com/tools/malybuzz-network-fuzzer)
mana	A toolkit for rogue access point (evilAP) attacks first presented at Defcon 22.	(https://github.com/sensepost/mana)
mando.me	Web Command Injection Tool.	(https://github.com/z0noxz/mando.me)
manspider	Spider entire networks for juicy files sitting on SMB shares. Search filenames or file content - regex supported!	(https://github.com/blacklanternsecurity/MANSPIDER)
manticore	Symbolic execution tool.	(https://github.com/trailofbits/manticore)
mantra	Hunt down API key leaks in JS files and pages.	(https://github.com/MrEmpy/mantra)
manul	A coverage-guided parallel fuzzer for open-source and blackbox binaries on Windows, Linux and MacOS.	(https://github.com/mxmssh/manul)
mapcidr	Utility program to perform multiple operations for a given subnet/CIDR ranges.	(https://github.com/projectdiscovery/mapcidr)
mara-framework	A Mobile Application Reverse engineering and Analysis Framework.	(https://github.com/xtiankisutsa/MARA_Framework)
marc4dasm	This python-based tool is a disassembler for the Atmel MARC4 (a 4 bit Harvard micro).	(https://github.com/ApertureLabsLtd/marc4dasm)
marshalsec	Java Unmarshaller Security - Turning your data into code execution.	(https://github.com/mbechler/marshalsec/)
maryam	Full-featured Web Identification framework written in Python.	(https://github.com/saeeddhqan/Maryam)
maskprocessor	A High-Performance word generator with a per-position configurable charset.	(http://hashcat.net/wiki/doku.php?id=maskprocessor)
massbleed	SSL Vulnerability Scanner.	(https://github.com/1N3/Sn1per)
masscan	TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes	(https://github.com/robertdavidgraham/masscan)
masscan-automation	Masscan integrated with Shodan API.	(https://github.com/trevordavenport/MasscanAutomation)
massdns	A high-performance DNS stub resolver in C.	(https://github.com/blechschmidt/massdns)
massexpconsole	A collection of tools and exploits with a cli ui for mass exploitation.	(https://github.com/jm33-m0/massExpConsole)
mat	Metadata Anonymisation Toolkit composed of a GUI application, a CLI application and a library.	(https://mat.boum.org/)
mat2	Metadata removal tool, supporting a wide range of commonly used file formats	(https://0xacab.org/jvoisin/mat2)
matahari	A reverse HTTP shell to execute commands on remote machines behind firewalls.	(http://matahari.sourceforge.net/)
matroschka	Python steganography tool to hide images or text in images.	(https://github.com/fgrimme/Matroschka)

Name	Description	Website
mausezahn	A free fast traffic generator written in C which allows you to send nearly every possible and impossible packet.	(http://www.perihel.at/sec/mz/)
mbenum	Queries the master browser for whatever information it has registered.	(http://www.cqure.net/wp/mbenum/)
mboxgrep	A small, non-interactive utility that scans mail folders for messages matching regular expressions. It does matching against basic and extended POSIX regular expressions, and reads and writes a variety of mailbox formats.	(http://mboxgrep.sourceforge.net)
mdbtools	Utilities for viewing data and exporting schema from Microsoft Access Database files.	(https://github.com/evanmiller/mdbtools)
mdcrack	MD4/MD5/NTLM1 hash cracker	(http://c3rb3r.openwall.net/mdcrack/)
mdk3	WLAN penetration tool.	(https://aspj.aircrack-ng.org/)
mdk4	A tool to exploit common IEEE 802.11 protocol weaknesses	(https://github.com/aircrack-ng/mdk4)
mdns-recon	An mDNS recon tool written in Python.	(https://github.com/chadillac/mdns_recon)
meanalyzer	Intel Engine Firmware Analysis Tool.	(https://github.com/platomav/MEAnalyzer)
medusa	Speedy, massively parallel and modular login brute-forcer for network	(http://www.foofus.net/jmk/medusa/medusa.html)
meg	Fetch many paths for many hosts - without killing the hosts.	(https://github.com/tomnomnom/meg)
melkor	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).	(http://packetstormsecurity.com/files/127924/Melkor-ELF-Fuzzer.0.html)
memdump	Dumps system memory to stdout, skipping over holes in memory maps.	(http://www.porcupine.org/forensics/tct.html)
memfetch	Dumps any userspace process memory without affecting its execution.	(http://lcamtuf.coredump.cx/)
memimager	Performs a memory dump using NtSystemDebugControl.	(http://ntsecurity.nu/toolbox/memimager/)
mentalist	Graphical tool for custom wordlist generation.	(https://github.com/sc0tfree/mentalist)
merlin-server	Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.	(https://github.com/Ne0nd0g/merlin)
metabigor	Intelligence Tool but without API key.	(https://github.com/j3ssie/metabigor)
metacoretex	MetaCoretex is an entirely JAVA vulnerability scanning framework for databases.	(http://metacoretex.sourceforge.net/)
metafinder	Search for documents in a domain through Search Engines (Google, Bing and Baidu). The objective is to extract metadata.	(https://github.com/Josue87/MetaFinder)
metaforge	Auto Scanning to SSL Vulnerability.	(https://github.com/chriswmorris/Metaforge)
metagoofil	An information gathering tool designed for extracting metadata of public documents.	(http://www.edge-security.com/metagoofil.php)
metame	A simple metamorphic code engine for arbitrary executables.	(https://github.com/a0rtega/metame)
metasploit	Advanced open-source platform for developing, testing, and using exploit code	(https://www.metasploit.com/)
metasploit-autopwn	db_autopwn plugin of metasploit.	(https://github.com/hahwul/metasploit-autopwn)
meterssh	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.	(https://github.com/trustedsec/meterssh)
metoscan	Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests.	(http://www.open-labs.org/)
mfcuk	MIFARE Classic Universal toolKit.	(http://code.google.com/p/mfcuk/)
mfoc	MiFare Classic Universal toolKit	(http://nfc-tools.org/)
mfsniffer	A python script for capturing unencrypted TSO login credentials.	(http://packetstormsecurity.com/files/120802/MF-Sniffer-TN3270-Password-Grabber.html)
mft2csv	Extract $MFT record info and log it to a csv file.	(https://github.com/jschicht/Mft2Csv)
mftcarver	Carve $MFT records from a chunk of data (for instance a memory dump).	(https://github.com/jschicht/MftCarver)
mftrcrd	Command line $MFT record decoder.	(https://github.com/jschicht/MftRcrd)
mftref2name	Resolve file index number to name or vice versa on NTFS.	(https://github.com/jschicht/MftRef2Name)
mibble	An open-source SNMP MIB parser (or SMI parser) written in Java. It can be used to read SNMP MIB files as well as simple ASN.1 files.	(http://www.mibble.org/)
microsploit	Fast and easy create backdoor office exploitation using module metasploit packet, Microsoft Office, Open Office, Macro attack, Buffer Overflow.	(https://github.com/Screetsec/Microsploit)
middler	A Man in the Middle tool to demonstrate protocol middling attacks.	(http://code.google.com/p/middler/)
mikrotik-npk	Python tools for manipulating Mikrotik NPK format.	(https://github.com/kost/mikrotik-npk)
mildew	Dotmil subdomain discovery tool that scrapes domains from official DoD website directories and certificate transparency logs.	(https://github.com/daehee/mildew)
mimikatz	A little tool to play with Windows security.	(https://github.com/gentilkiwi/mimikatz)
mimipenguin	A tool to dump the login password from the current linux user.	(https://github.com/huntergregal/mimipenguin)
mingsweeper	A network reconnaissance tool designed to facilitate large address space,high speed node discovery and identification.	(http://www.hoobie.net/mingsweeper/)
minimodem	A command-line program which decodes (or generates) audio modem tones at any specified baud rate, using various framing protocols.	(https://github.com/kamalmostafa/minimodem)
minimysqlator	A multi-platform application used to audit web sites in order to discover and exploit SQL injection vulnerabilities.	(http://www.scrt.ch/en/attack/downloads/mini-mysqlat0r)
miranda-upnp	A Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices	(http://code.google.com/p/miranda-upnp/)
missidentify	A program to find Win32 applications.	(http://missidentify.sourceforge.net/)
missionplanner	A GroundControl Station for Ardupilot.	(https://firmware.ardupilot.org/Tools/MissionPlanner/)
mitm	A simple yet effective python3 script to perform DNS spoofing via ARP poisoning.	(https://github.com/Th3Hurrican3/mitm)
mitm-relay	Hackish way to intercept and modify non-HTTP protocols through Burp & others.	(https://github.com/jrmdev/mitm_relay)
mitm6	Pwning IPv4 via IPv6.	(https://github.com/fox-it/mitm6)
mitmap	A python program to create a fake AP and sniff data.	(https://github.com/xdavidhu/mitmAP)
mitmap-old	Shell Script for launching a Fake AP with karma functionality and launches ettercap for packet capture and traffic manipulation.	(http://www.darkoperator.com/tools-and-scripts/)
mitmer	A man-in-the-middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.	(https://github.com/husam212/MITMer)
mitmf	A Framework for Man-In-The-Middle attacks written in Python.	(https://github.com/byt3bl33d3r/MITMf)
mitmproxy	SSL-capable man-in-the-middle HTTP proxy	(https://mitmproxy.org)
mkbrutus	Password bruteforcer for MikroTik devices or boxes running RouterOS.	(http://mkbrutusproject.github.io/MKBRUTUS/)
mkyara	Tool to generate YARA rules based on binary code.	(https://github.com/fox-it/mkYARA)

Name	Description	Website
mobiusft	An open-source forensic framework written in Python/GTK that manages cases and case items, providing an abstract interface for developing extensions.	(http://savannah.nongnu.org/projects/mobiusft)
mobsf	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.	(https://github.com/MobSF/Mobile-Security-Framework-MobSF)
modifycerttemplate	Aid operators in modifying ADCS certificate templates so that a created vulnerable state can be leveraged for privilege escalation.	(https://github.com/fortalice/modifyCertTemplate)
modlishka	A powerful and flexible HTTP reverse proxy.	(https://github.com/drk1wi/Modlishka)
modscan	A new tool designed to map a SCADA MODBUS TCP based network.	(https://code.google.com/p/modscan/)
moloch	An open source large scale IPv4 full PCAP capturing, indexing and database system.	(https://github.com/aol/moloch)
mongoaudit	A powerful MongoDB auditing and pentesting tool .	(https://github.com/stampery/mongoaudit)
monocle	A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network.	(http://packetstormsecurity.com/files/99823/Monocle-Host-Discovery-Tool.0.html)
monsoon	A fast HTTP enumerator that allows you to execute a large number of HTTP requests.	(https://github.com/RedTeamPentesting/monsoon)
moonwalk	Cover your tracks during Linux Exploitation by leaving zero traces on system logs and filesystem timestamps.	(https://github.com/mufeedvh/moonwalk)
mooscan	A scanner for Moodle LMS.	(https://github.com/vortexau/mooscan)
morpheus	Automated Ettercap TCP/IP Hijacking Tool.	(https://github.com/r00txp10it/morpheus)
morxbook	A password cracking tool written in perl to perform a dictionary-based attack on a specific Facebook user through HTTPS.	(http://www.morxploit.com/)
morxbrute	A customizable HTTP dictionary-based password cracking tool written in Perl.	(http://www.morxploit.com/morxbrute/)
morxbtcrack	Single Bitcoin private key cracking tool released.	(http://www.morxploit.com/tools/)
morxcoinpwn	Mass Bitcoin private keys brute forcing/Take over tool released.	(http://www.morxploit.com/tools/)
morxcrack	A cracking tool written in Perl to perform a dictionary-based attack on various hashing algorithm and CMS salted-passwords.	(http://www.morxploit.com/morxcrack/)
morxkeyfmt	Read a private key from stdin and output formatted data values.	(http://www.morxploit.com/tools/)
morxtraversal	Path Traversal checking tool.	(http://www.morxploit.com/tools/)
morxtunel	Network Tunneling using TUN/TAP interfaces over TCP tool.	(http://www.morxploit.com/tools/)
mosca	Static analysis tool to find bugs like a grep unix command.	(https://github.com/CoolerVoid/Mosca)
mosquito	XSS exploitation tool - access victims through HTTP proxy.	(https://github.com/koto/mosquito)
mots	Man on the Side Attack - experimental packet injection and detection.	(https://github.com/kevinkoo001/MotS)
motsa-dns-spoofing	ManOnTheSideAttack-DNS Spoofing.	(https://github.com/waytoalpit/ManOnTheSideAttack-DNS-Spoofing)
mousejack	Wireless mouse/keyboard attack with replay/transmit poc.	(https://github.com/iamckn/mousejack_transmit)
mp3nema	A tool aimed at analyzing and capturing data that is hidden between frames in an MP3 file or stream, otherwise noted as "out of band" data.	(http://packetstormsecurity.com/files/76432/MP3nema-Forensic-Analysis-Tool.html)
mptcp	A tool for manipulation of raw packets that allows a large number of options.	(http://packetstormsecurity.com/files/119132/Mptcp-Packet-Manipulator.9.0.html)
mptcp-abuse	A collection of tools and resources to explore MPTCP on your network. Initially released at Black Hat USA 2014.	(https://github.com/Neohapsis/mptcp-abuse)
mqtt-pwn	A one-stop-shop for IoT Broker penetration-testing and security assessment operations.	(https://github.com/akamai-threat-research/mqtt-pwn)
mrkaplan	Help red teamers to stay hidden by clearing evidence of execution.	(https://github.com/Idov31/MrKaplan)
mrsip	SIP-Based Audit and Attack Tool.	(https://github.com/meliht/mr.sip)
mrtparse	A module to read and analyze the MRT format data.	(https://github.com/YoshiyukiYamauchi/mrtparse)
ms-sys	A tool to write Win9x- master boot records (mbr) under linux - RTM!	(http://ms-sys.sourceforge.net/)
msf-mpc	Msfvenom payload creator.	(https://github.com/g0tmi1k/mpc)
msfdb	Manage the metasploit framework database.	(https://github.com/BlackArch/msfdb)
msfenum	A Metasploit auto auxiliary script.	(https://github.com/wez3/msfenum)
msmailprobe	Office 365 and Exchange Enumeration tool.	(https://github.com/busterb/msmailprobe)
mssqlscan	A small multi-threaded tool that scans for Microsoft SQL Servers.	(http://www.cqure.net/wp/mssqlscan/)
msvpwn	Bypass Windows' authentication via binary patching.	(https://bitbucket.org/mrabault/msvpwn)
mtr	Combines the functionality of traceroute and ping into one tool (CLI version)	(https://www.bitwizard.nl/mtr/)
mtscan	Mikrotik RouterOS wireless scanner.	(https://github.com/kkonradpl/mtscan)
mubeng	An incredibly fast proxy checker & IP rotator with ease.	(https://github.com/kitabisa/mubeng)
multiinjector	Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation.	(http://chaptersinwebsecurity.blogspot.de/2008/11/multiinjector-v03-released.html)
multimac	Multiple MACs on an adapter	(http://sourceforge.net/projects/multimac/)
multimon-ng	An sdr decoder, supports pocsag, ufsk, clipfsk, afsk, hapn, fsk, dtmf, zvei.	(https://github.com/EliasOenal/multimon-ng)
multiscanner	Modular file scanning/analysis framework.	(https://github.com/mitre/multiscanner)
multitun	Tunnel arbitrary traffic through an innocuous WebSocket.	(https://github.com/covertcodes/multitun)
munin-hashchecker	Online hash checker for Virustotal and other services	(https://github.com/Neo23x0/munin)
muraena	Almost-transparent reverse proxy to automate phishing and post-phishing activities.	(https://github.com/muraenateam/muraena)
mutator	This project aims to be a wordlist mutator with hormones, which means that some mutations will be applied to the result of the ones that have been already done, resulting in something like: corporation -> C0rp0r4t10n_2012	(https://bitbucket.org/alone/mutator/)
mwebfp	Mass Web Fingerprinter.	(https://github.com/falcon-lnhg/mwebfp)
mxtract	Memory Extractor & Analyzer.	(https://github.com/rek7/mXtract)
mybff	A Brute Force Framework.	(https://github.com/MooseDojo/myBFF)
myjwt	This cli is for pentesters, CTF players, or dev. You can modify your jwt, sign, inject, etc.	(https://github.com/mBouamama/MyJWT)
mylg	Network Diagnostic Tool.	(https://github.com/mehrdadrad/mylg)
myrescue	A hard disk recovery tool that reads undamaged regions first.	(http://myrescue.sourceforge.net)
mysql2sqlite	Converts a mysqldump file into a Sqlite 3 compatible file.	(https://gist.github.com/esperlu/943776)
n1qlmap	An N1QL exploitation tool.	(https://github.com/FSecureLABS/N1QLMap)
naabu	A fast port scanner written in go with focus on reliability and simplicity.	(https://github.com/projectdiscovery/naabu)
nacker	A tool to circumvent 802.1x Network Access Control on a wired LAN.	(https://github.com/carmaa/nacker)
naft	Network Appliance Forensic Toolkit.	(https://blog.didierstevens.com/my-software/#NAFT)

Name	Description	Website
narthex	Modular personalized dictionary generator.	(https://github.com/MichaelDim02/Narthex)
nasnum	Script to enumerate network attached storages.	(https://github.com/tcstool/nasnum.git)
nbname	Decodes and displays all NetBIOS name packets it receives on UDP port 137 and more!	(http://www.cultdeadcow.com/tools/bo.html)
nbnspoof	NetBIOS Name Service Spoofer	(http://www.mcgrewsecurity.com/tools/nbnspoof/)
nbtenum	A utility for Windows that can be used to enumerate NetBIOS information from one host or a range of hosts.	(http://reedarvin.thearvins.com/)
nbtool	Some tools for NetBIOS and DNS investigation, attacks, and communication.	(http://wiki.skullsecurity.org/Nbtool)
nbtscan	Scan networks searching for NetBIOS information	(https://github.com/resurrecting-open-source-projects/nbtscan)
ncpfs	Allows you to mount volumes of NetWare servers under Linux.	(http://www.novell.com/)
ncrack	High-speed network authentication cracking tool	(https://nmap.org/ncrack/)
necromant	Python Script that search unused Virtual Hosts in Web Servers.	(https://github.com/PentesterES/Necromant)
needle	The iOS Security Testing Framework.	(https://github.com/mwrlabs/needle)
neglected	Facebook CDN Photo Resolver.	(https://github.com/GuerrillaWarfare/neglected)
neighbor-cache-fingerprinter	An ARP based Operating System version scanner.	(https://github.com/PherricOxide/Neighbor-Cache-Fingerprinter)
nemesis	A command-line network packet crafting and injection utility.	(https://github.com/troglobit/nemesis)
neo-regeorg	Improved version of reGeorg, HTTP tunneling pivot tool	(https://github.com/L-codes/Neo-reGeorg)
net-creds	Sniffs sensitive data from interface or pcap.	(https://github.com/DanMcInerney/net-creds)
netactview	A graphical network connections viewer similar in functionality to netstat.	(http://netactview.sourceforge.net/index.html)
netattack	Python script to scan and attack wireless networks.	(https://github.com/chrizator/netattack2)
netbios-share-scanner	This tool could be used to check windows workstations and servers if they have accessible shared resources.	(http://www.secpoint.com/netbios-share-scanner.html)
netbus	NetBus remote administration tool	(https://packetstormsecurity.com/files/10320/nb16_p04.zip.html)
netcommander	An easy-to-use arp spoofing tool.	(https://github.com/evilsocket/netcommander)
netcon	A network connection establishment and management script.	(http://www.paramecium.org/~leendert/)
netdiscover	An active/passive address reconnaissance tool, mainly developed for those wireless networks without dhcp server, when you are wardriving. It can be also used on hub/switched networks.	(http://nixgeneration.com/~jaime/netdiscover/)
netexec-pingcastle	NetExec & CrackMapExec module that execute PingCastle on a remote machine.	(https://github.com/TRIKKSS/CrackMapExec-PingCastle)
netexec	A Windows / Active Directory environments pentest tool.	(https://netexec.wiki/)
netkit-bsd-finger	BSD-finger ported to Linux.	(http://ftp.linux.org.uk/pub/linux/Networking/netkit)
netkit-rusers	Logged in users; Displays who is logged in to machines on local network.	(https://packages.debian.org/source/sid/net/netkit-rusers)
netkit-rwho	Remote who client and server (with Debian patches).	(http://packages.qa.debian.org/n/netkit-rwho.html)
netmap	Can be used to make a graphical representation of the surrounding network.	(http://netmap.sourceforge.net/)
netmask	Helps determine network masks	(http://packages.qa.debian.org/n/netmask.html)
netreconn	A collection of network scan/recon tools that are relatively small compared to their larger cousins.	(http://packetstormsecurity.com/files/86076/NetReconn-Scanning-Tool-Collection.76.html)
netripper	Smart traffic sniffing for penetration testers.	(https://github.com/NytroRST/NetRipper)
netscan	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).	(http://packetstormsecurity.com/files/125569/Netscan-Port-Scanner.0.html)
netscan2	Active / passive network scanner.	(https://github.com/walchko/netscan2)
netsed	Small and handful utility design to alter the contents of packets forwarded thru network in real time.	(http://silicone.homelinux.org/projects/netsed/)
netsniff-ng	High performance Linux network sniffer for packet inspection	(http://netsniff-ng.org/)
netstumbler	Well-known wireless AP scanner and sniffer.	(http://www.netstumbler.com/downloads/)
nettacker	Automated Penetration Testing Framework.	(https://github.com/OWASP/Nettacker)
network-app-stress-tester	Network Application Stress Testing Yammer.	(https://github.com/PherricOxide/Network-App-Stress-Tester)
networkmap	Post-exploitation network mapper.	(https://github.com/lorenzog/NetworkMap)
networkminer	A Network Forensic Analysis Tool for advanced Network Traffic Analysis, sniffer and packet analyzer.	(http://www.netresec.com/)
netz	Discover internet-wide misconfigurations while drinking coffee.	(https://github.com/spectralops/netz)
netzob	An open source tool for reverse engineering, traffic generation and fuzzing of communication protocols.	(https://github.com/netzob/netzob/)
nexfil	OSINT tool for finding profiles by username.	(https://github.com/thewhiteh4t/nexfil)
nextnet	Pivot point discovery tool.	(https://github.com/hdm/nextnet)
nfcutils	Provides a simple 'lsnfc' command that list tags which are in your NFC device field	(http://code.google.com/p/nfc-tools)
nfdump	A set of tools to collect and process netflow data.	(https://github.com/phaag/nfdump)
nfex	A tool for extracting files from the network in real-time or post-capture from an offline tcpdump pcap savefile.	(https://code.google.com/p/nfex/)
nfspy	A Python library for automating the falsification of NFS credentials when mounting an NFS share.	(https://github.com/bonsaiviking/NfSpy)
nfsshell	Userland NFS command tool.	(http://www.paramecium.org/~leendert/)
ngrep	A grep-like utility that allows you to search for network packets on an interface.	(https://github.com/jpr5/ngrep/)
ngrok	A tunneling, reverse proxy for developing and understanding networked, HTTP services.	(https://ngrok.com/)
nield	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.	(http://nield.sourceforge.net/)
nikto	A web server scanner which performs comprehensive tests against web servers for multiple items	(https://github.com/sullo/nikto)
nili	Tool for Network Scan, Man in the Middle, Protocol Reverse Engineering and Fuzzing.	(https://github.com/niloofarkheirkhah/nili)
nimbostratus	Tools for fingerprintinging and exploiting Amazon cloud infrastructures.	(https://github.com/andresriancho/nimbostratus)
nipe	A script to make Tor Network your default gateway.	(https://github.com/GouveaHeitor/nipe)
nipper	Network Infrastructure Parser	(https://www.titania-security.com/)

Name	Description	Website
nirsoft	Unique collection of small and useful freeware utilities.	(https://www.nirsoft.net)
nishang	Using PowerShell for Penetration Testing.	(https://code.google.com/p/nishang/)
njsscan	A static application testing (SAST) tool that can find insecure code patterns in your node.js applications.	(https://pypi.org/project/njsscan/#files)
nkiller2	A TCP exhaustion/stressing tool.	(http://sock-raw.org/projects.html)
nmap	Utility for network discovery and security auditing	(https://nmap.org/)
nmap-parse-output	Converts/manipulates/extracts data from a nmap scan output.	(https://github.com/hahwul/nmap-parse-output)
nmbscan	Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols.	(http://nmbscan.gbarbier.org/)
nohidy	The system admins best friend, multi platform auditing tool.	(https://github.com/flipchan/Nohidy)
nomorexor	Tool to help guess a files 256 byte XOR key by using frequency analysis.	(https://github.com/hiddenillusion/NoMoreXOR)
noriben	Portable, Simple, Malware Analysis Sandbox.	(https://github.com/Rurik/Noriben)
nosqlattack	Python tool to automate exploit MongoDB server IP on Internet anddisclose the database data by MongoDB default configuration weaknesses and injection attacks.	(https://github.com/youngyangyang04/NoSQLAttack)
nosqli	NoSQL scanner and injector.	(https://github.com/Charlie-belmer/nosqli)
nosqli-user-pass-enum	Script to enumerate usernames and passwords from vulnerable web applications running MongoDB.	(https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration)
nosqlmap	Automated Mongo database and NoSQL web application exploitation tool	(https://github.com/tcstool/NoSQLMap)
notspikefile	A Linux based file format fuzzing tool	(http://packetstormsecurity.com/files/39627/notSPIKEfile.tgz.html)
novahot	A webshell framework for penetration testers.	(https://github.com/chrisallenlane/novahot)
nray	Distributed port scanner.	(https://github.com/nray-scanner/nray)
nsdtool	A netgear switch discovery tool. It contains some extra features like bruteoforce and setting a new password.	(http://www.curesec.com/en/publications/tools.html)
nsearch	Minimal script to help find script into the nse database.	(https://github.com/JKO/nsearch)
nsec3map	A tool to enumerate the resource records of a DNS zone using its DNSSEC NSEC or NSEC3 chain.	(https://github.com/anonion0/nsec3map)
nsec3walker	Enumerates domain names using DNSSEC	(http://dnscurve.org/nsec3walker.html)
nsntrace	Perform network trace of a single process by using network namespaces.	(https://github.com/jonasdn/nsntrace)
nsoq	A Network Security Tool for packet manipulation that allows a large number of options.	(http://www.nsoq.org/)
ntds-decode	This application dumps LM and NTLM hashes from active accounts stored in an Active Directory database.	(http://packetstormsecurity.com/files/121543/NTDS-Hash-Decoder.b.html)
ntdsxtract	Active Directory forensic framework.	(https://github.com/csababarta/ntdsxtract)
ntfs-file-extractor	Extract files off NTFS.	(https://github.com/jschicht/NtfsFileExtractor)
ntfs-log-tracker	This tool can parse $LogFile, $UsnJrnl of NTFS.	(https://sites.google.com/site/forensicnote/ntfs-log-tracker)
ntlm-challenger	Parse NTLM over HTTP challenge messages.	(https://github.com/b17zr/ntlm_challenger)
ntlm-scanner	A simple python tool based on Impacket that tests servers for various known NTLM vulnerabilities.	(https://github.com/preempt/ntlm-scanner)
ntlm-theft	A tool for generating multiple types of NTLMv2 hash theft files.	(https://github.com/Greenwolf/ntlm_theft)
ntlmrecon	A tool to enumerate information from NTLM authentication enabled web endpoints.	(https://github.com/sachinkamath/ntlmrecon)
ntp-fingerprint	An active fingerprinting utility specifically designed to identify the OS the NTP server is running on.	(http://www.hackingciscoexposed.com/?link=tools)
ntp-ip-enum	Script to pull addresses from a NTP server using the monlist command. Can also output Maltego resultset.	(http://www.securepla.net/)
ntpdos	PoC for distributed NTP reflection DoS (CVE-5211)	(https://github.com/sepehrdaddev/ntpdos)
nuclei	A fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.	(https://github.com/projectdiscovery/nuclei)
nuclei-templates	Community curated list of template files for the nuclei engine.	(https://github.com/projectdiscovery/nuclei-templates)
nullinux	Tool that can be used to enumerate OS information, domain information, shares, directories, and users through SMB null sessions.	(https://github.com/m8r0wn/nullinux)
nullscan	A modular framework designed to chain and automate security tests.	(http://www.nullsecurity.net/tools/automation.html)
nxcrypt	Python backdoor framework.	(https://github.com/Hadi999/NXcrypt)
nzyme	WiFi defense system.	(https://www.nzyme.org/download)
o-saft	A tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations.	(https://www.owasp.org/index.php/O-Saft)
o365enum	Username enumeration and password enuming tool aimed at Microsoft O365.	(https://github.com/gremwell/o365enum)
o365spray	Username enumeration and password spraying tool aimed at Microsoft O365.	(https://github.com/0xZDH/o365spray)
oat	A toolkit that could be used to audit security within Oracle database servers.	(http://www.cqure.net/wp/test/)
obevilion	Another archive cracker created in python, cracking [zip/7z/rar].	(https://github.com/BL4CKvGHOST/Ob3vil1on)
obexstress	Script for testing remote OBEX service for some potential vulnerabilities.	(http://bluetooth-pentest.narod.ru/)
obfs4proxy	A pluggable transport proxy written in Go.	(https://gitlab.com/yawning/obfs4)
objdump2shellcode	A tool I have found incredibly useful whenever creating custom shellcode.	(https://github.com/wetw0rk/objdump2shellcode)
objection	Instrumented Mobile Pentest Framework.	(https://pypi.org/project/objection/#files)
oclhashcat	Worlds fastest WPA cracker with dictionary mutation engine.	(http://hashcat.net/oclhashcat/)
ocs	Compact mass scanner for Cisco routers with default telnet/enable passwords.	(http://packetstormsecurity.com/files/119462/OCS-Cisco-Scanner.2.html)
octopwnweb	Internal pentest framework running in your browser via WebAssembly, powerd by Pyodide	(https://github.com/skelsec/octopwnweb)
office-dde-payloads	Collection of scripts and templates to generate Office documents embedded with the DDE, macro-less command execution technique.	(https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads)
ofp-sniffer	An OpenFlow sniffer to help network troubleshooting in production networks.	(https://github.com/amlight/ofp_sniffer)
ohrwurm	A small and simple RTP fuzzer.	(http://mazzoo.de/)
okadminfinder	Tool to find admin panels / admin login pages.	(https://github.com/mIcHyAmRaNe/okadminfinder3)
oledump	Analyze OLE files (Compound File Binary Format). These files contain streams of data. This tool allows you to analyze these streams.	(http://blog.didierstevens.com/programs/oledump-py/)
ollydbg	A 32-bit assembler-level analysing debugger.	(http://www.ollydbg.de)

Name	Description	Website
omen	Ordered Markov ENumerator - Password Guesser.	(https://github.com/RUB-SysSec/OMEN)
omnibus	OSINT tool for intelligence collection, research and artifact management.	(https://github.com/InQuest/omnibus)
omnihash	Hash files, strings, input streams and network resources in various common algorithms simultaneously.	(https://github.com/Miserlou/omnihash)
one-lin3r	Gives you one-liners that aids in penetration testing and more.	(https://github.com/D4Vinci/One-Lin3r)
onesixtyone	An SNMP scanner that sends multiple SNMP requests to multiple IP addresses	(http://labs.portcullis.co.uk/application/onesixtyone/)
onetwopunch	Use unicornscan to quickly scan all open ports, and then pass the open ports to nmap for detailed scans.	(https://github.com/superkojiman/onetwopunch)
onioff	An onion url inspector for inspecting deep web links.	(https://github.com/k4m4/onioff)
oniongrok	Onion addresses for anything.	(https://github.com/cmars/oniongrok)
onionscan	Scan Onion Services for Security Issues.	(https://github.com/s-rah/onionscan)
onionsearch	Script that scrapes urls on different ".onion" search engines.	(https://github.com/megadose/OnionSearch)
onionshare	Share a file over Tor Hidden Services anonymously and securely	(https://github.com/onionshare/onionshare)
open-iscsi	iSCSI userland tools	(https://www.open-iscsi.com/)
opendoor	OWASP WEB Directory Scanner.	(https://github.com/stanislav-web/OpenDoor)
openpuff	Yet not another steganography SW.	(https://embeddedsw.net/OpenPuff_Steganography_Home.html)
openrisk	Generates a risk score based on the results of a Nuclei scan using OpenAI's GPT model.	(https://github.com/projectdiscovery/openrisk)
openscap	Open Source Security Compliance Solution.	(https://www.open-scap.org/)
openstego	A tool implemented in Java for generic steganography, with support for password-based encryption of the data.	(https://github.com/syvaidya/openstego/releases)
opensvp	A security tool implementing "attacks" to be able to the resistance of firewall to protocol level attack.	(https://github.com/regit/opensvp)
openvas-scanner	The OpenVAS scanning Daemon.	(https://github.com/greenbone/openvas-scanner/)
operative	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 ...).	(https://github.com/graniet/operative-framework)
ophcrack	Windows password cracker based on rainbow tables	(http://ophcrack.sourceforge.net)
orakelcrackert	This tool can crack passwords which are encrypted using Oracle's latest SHA1 based password protection algorithm.	(http://freeworld.thc.org/thc-orakelcrackert11g/)
origami	Aims at providing a scripting tool to generate and analyze malicious PDF files.	(https://github.com/gdelugre/origami)
orjail	A more secure way to force programs to exclusively use tor network.	(https://github.com/orjail/orjail)
oscanner	An Oracle assessment framework developed in Java.	(http://www.cqure.net/wp/oscanner/)
osert	Markdown Templates for Offensive Security exam reports.	(https://github.com/noraj/OSCP-Exam-Report-Template-Markdown)
osfooler-ng	Prevents remote active/passive OS fingerprinting by tools like nmap or p0f.	(https://github.com/segofensiva/OSfooler-ng)
osi.ig	Instagram OSINT Tool gets a range of information from an Instagram account.	(https://github.com/th3unkn0n/osi.ig)
osint-spy	Performs OSINT scan on email/domain/ip_address/organization.	(https://github.com/SharadKumar97/OSINT-SPY)
osinterator	Open Source Toolkit for Open Source Intelligence Gathering.	(https://github.com/guitarmanj/OSINTerator)
osintgram	OSINT tool offering an interactive shell to perform analysis on Instagram account of any users by its nickname.	(https://github.com/Datalux/Osintgram)
osrframework	A project focused on providing API and tools to perform more accurate online researches.	(https://github.com/i3visio/osrframework)
osslsigncode	A small tool that implements part of the functionality of the Microsoft tool signtool.exe.	(https://github.com/mtrojnar/osslsigncode)
ostinato	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.	(https://github.com/pstavirs/ostinato/)
osueta	A simple Python script to exploit the OpenSSH User Enumeration Timing Attack.	(https://github.com/c0r3dump3d/osueta)
otori	A python-based toolbox intended to allow useful exploitation of XML external entity ("XXE") vulnerabilities.	(http://www.beneaththewaves.net/Software/On_The_Outside_Reaching_In.html)
outguess	A universal steganographic tool.	(https://github.com/resurrecting-open-source-projects/outguess)
outlook-webapp-brute	Microsoft Outlook WebAPP Brute.	(https://github.com/lijiejie/OutLook_WebAPP_Brute)
owabf	Outlook Web Access bruteforcer tool.	(http://netsec.rs/70/tools.html)
owasp-bywaf	A web application penetration testing framework (WAPTF).	(https://github.com/depasonico/OWASP-ByWaf)
owasp-zsc	Shellcode/Obfuscate Code Generator.	(https://github.com/zscproject/OWASP-ZSC)
owtf	The Offensive (Web) Testing Framework.	(https://www.owasp.org/index.php/OWASP_OWTF)
p0f	Purely passive TCP/IP traffic fingerprinting tool	(http://lcamtuf.coredump.cx/p0f3/)
pack	Password Analysis and Cracking Kit	(http://thesprawl.org/projects/pack/)
packer	tool for creating identical machine images for multiple platforms from a single source configuration	(https://github.com/hashicorp/packer)
packerid	Script which uses a PEiD database to identify which packer (if any) is being used by a binary.	(http://handlers.sans.org/jclausing/)
packet-o-matic	A real time packet processor. Reads the packet from an input module, match the packet using rules and connection tracking information and then send it to a target module.	(http://www.packet-o-matic.org/)
packeth	Linux GUI packet generator tool for ethernet	(http://packeth.sourceforge.net/)
packetq	A tool that provides a basic SQL-frontend to PCAP-files.	(https://github.com/DNS-OARC/PacketQ)
packetsender	An open source utility to allow sending and receiving TCP and UDP packets.	(https://github.com/dannagle/PacketSender)
packit	A network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic.	(http://packit.sourceforge.net/)
pacu	The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.	(https://github.com/RhinoSecurityLabs/pacu)
pacumen	Packet Acumen - Analyse encrypted network traffic and more (side-channel attacks).	(https://github.com/bniemczyk/pacumen)
padbuster	Automated script for performing Padding Oracle attacks.	(http://www.gdssecurity.com/l/t.php)
padoracle	Padding Oracle Attack with Node.js.	(https://github.com/imyelo/padoracle)
pafish	A demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do.	(http://www.hoobie.net/pafish/)

Name	Description	Website
pagodo	Google dork script to collect potentially vulnerable web pages and applications on the Internet.	↗ (https://github.com/opsdisk/pagodo)
paketto	Advanced TCP/IP Toolkit.	↗ (http://www.doxpara.com/paketto)
panhunt	Searches for credit card numbers (PANs) in directories.	↗ (https://github.com/Dionach/PANhunt)
panoptic	A tool that automates the process of search and retrieval of content for common log and config files through LFI vulnerability.	↗ (https://github.com/lightos/Panoptic)
pappy-proxy	An intercepting proxy for web application testing.	↗ (https://github.com/roglew/pappy-proxy)
parameth	This tool can be used to brute discover GET and POST parameters.	↗ (https://github.com/mak-/parameth)
parampampam	This tool for brute discover GET and POST parameters.	↗ (https://github.com/Bo0oM/ParamPamPam)
paranoic	A simple vulnerability scanner written in Perl.	↗ (http://packetstormsecurity.com/files/128065/Paranoic-Scan.7.html)
paros	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.	↗ (http://www.parosproxy.org)
parse-evtx	A tool to parse the Windows XML Event Log (EVTX) format.	↗ (https://github.com/KasperskyLab/ForensicsTools)
parsero	A robots.txt audit tool.	↗ (https://github.com/behindthefirewalls/Parsero)
pasco	Examines the contents of Internet Explorer's cache files for forensic purposes	↗ (http://www.jonesdykstra.com/)
pass-station	CLI & library to search for default credentials among thousands of Products / Vendors.	↗ (https://noraj.github.io/pass-station/)
passcracking	A little python script for sending hashes to passcracking.com and milw0rm	↗ (http://github.com/jensp/passcracking)
passdetective	Scans shell command history to detect mistakenly written passwords, API keys, and secrets.	↗ (https://github.com/aydinnyunus/PassDetective)
passe-partout	Tool to extract RSA and DSA private keys from any process linked with OpenSSL. The target memory is scanned to lookup specific OpenSSL patterns.	↗ (http://www.hsc.fr/ressources/outils/passe-partout/index.html.en)
passgan	A Deep Learning Approach for Password Guessing.	↗ (https://github.com/D3vil0p3r/PassGAN)
passhunt	Search drives for documents containing passwords.	↗ (https://github.com/Dionach/PassHunt)
passivedns	A network sniffer that logs all DNS server replies for use in a passive DNS setup.	↗ (https://github.com/gamelinux/passivedns)
pastejacker	Hacking systems with the automation of PasteJacking attacks.	↗ (https://github.com/D4Vinci/PasteJacker)
pastemonitor	Scrape Pastebin API to collect daily pastes, setup a wordlist and be alerted by email when you have a match..	↗ (https://github.com/pixelbubble/PasteMonitor)
pasv-agrsv	Passive recon / OSINT automation script.	↗ (https://github.com/isaudits/pasv-agrsv)
patator	A multi-purpose bruteforcer.	↗ (https://github.com/lanjelot/patator)
patchkit	Powerful binary patching from Python.	↗ (https://github.com/lunixbochs/patchkit)
pathzuzu	Checks for PATH substitution vulnerabilities and logs the commands executed by the vulnerable executables.	↗ (https://github.com/ShotokanZH/Pa-th-zuzu)
pax-oracle	CLI tool for PKCS7 padding oracle attacks.	↗ (https://github.com/liamg/pax)
payloadmask	Web Payload list editor to use techniques to try bypass web application firewall.	↗ (https://github.com/CoolerVoid/payloadmask)
payloadsallthethings	A list of useful payloads and bypass for Web Application Security and Pentest/CTF.	↗ (https://github.com/swisskyrepo/PayloadsAllTheThings/)
pblind	Little utility to help exploiting blind sql injection vulnerabilities.	↗ (http://www.edge-security.com/pblind.php)
pbscan	Faster and more efficient stateless SYN scanner and banner grabber due to userland TCP/IP stack usage.	↗ (https://github.com/gvb84/pbscan)
pcapfex	Packet CAPture Forensic Evidence eXtractor.	↗ (https://github.com/vikwin/pcapfex)
pcapfix	Tries to repair your broken pcap and pcapng files.	↗ (http://f00l.de/pcapfix/)
pcapsipdump	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).	↗ (http://pcapsipdump.sourceforge.net/)
pcapteller	A tool designed for traffic manipulation and replay.	↗ (https://www.encripto.no/nb/downloads/tools/)
pcapxray	A Network Forensics Tool - To visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction.	↗ (https://github.com/Srinivas11789/PcapXray)
pcileech	Tool, which uses PCIe hardware devices to read and write from the target system memory.	↗ (https://github.com/ufrisk/pcileech/releases)
pcode2code	VBA p-code decompiler.	↗ (https://github.com/Big5-sec/pcode2code)
pcredz	A tool that extracts credit card numbers and more from a pcap file or from a live interface.	↗ (https://github.com/lgandx/PCredz)
pdblaster	Extract PDB file paths from large sample sets of executable files.	↗ (https://github.com/SecurityRiskAdvisors/PDBlaster)
pdf-parser	Parses a PDF document to identify the fundamental elements used in the analyzed file.	↗ (http://blog.didierstevens.com/programs/pdf-tools/)
pdfbook-analyzer	Utility for facebook memory forensics.	↗ (http://sourceforge.net/projects/pdfbook/)
pdfcrack	Password recovery tool for PDF-files	↗ (https://pdfcrack.sourceforge.net/)
pdfgrab	Tool for searching pdfs withthin google and extracting pdf metadata.	↗ (https://github.com/c0decave/pdfgrab)
pdfid	Scan a file to look for certain PDF keywords.	↗ (http://blog.didierstevens.com/programs/pdf-tools/)
pdfresurrect	A tool aimed at analyzing PDF documents.	↗ (http://packetstormsecurity.com/files/118459/PDFResurrect-PDF-Analyzer.12.html)
pdfwalker	Frontend to explore the internals of a PDF document with Origami	↗ (https://github.com/gdelugre/pdfwalker)
pdgmail	A password dictionary attack tool that targets windows authentication via the SMB protocol.	↗ (http://www.jeffbryner.com/code/pdgmail)
pe-bear	A freeware reversing tool for PE files.	↗ (https://github.com/hasherezade/pe-bear)
pe-sieve	Scans a given process. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches).	↗ (https://github.com/hasherezade/pe-sieve)
peach	A SmartFuzzer that is capable of performing both generation and mutation based fuzzing.	↗ (http://peachfuzzer.com/)
peach-fuzz	Simple vulnerability scanning framework.	↗ (https://github.com/Caleb1994/peach)
peass	Privilege Escalation Awesome Scripts SUITE (with colors).	↗ (https://github.com/carlospolop/PEASS-ng)
peda	Python Exploit Development Assistance for GDB	↗ (https://github.com/longld/peda)
peepdf	A Python tool to explore PDF files in order to find out if the file can be harmful or not.	↗ (http://eternal-todo.com/tools/peepdf-pdf-analysis-tool)
peepingtom	A tool to take screenshots of websites. Much like eyewitness.	↗ (https://bitbucket.org/LaNMaSteR53/peepingtom)
peframe	Tool to perform static analysis on (portable executable) malware.	↗ (https://github.com/guelfoweb/peframe)
pemcrack	Cracks SSL PEM files that hold encrypted private keys. Brute forces or dictionary cracks.	↗ (https://github.com/robertdavidgraham/pemcrack)

Name	Description	Website
pemcracker	Tool to crack encrypted PEM files.	(https://github.com/bwall/pemcracker.git)
penbox	A Penetration Testing Framework - The Tool With All The Tools.	(https://github.com/x3omdax/PenBox)
pencode	Complex payload encoder.	(https://github.com/ffuf/pencode)
pentbox	A security suite that packs security and stability testing oriented tools for networks and systems.	(http://www.pentbox.net)
pentestgpt	A penetration testing tool empowered by ChatGPT. It is designed to automate the penetration testing process.	(https://github.com/GreyDGL/PentestGPT)
pentestly	Python and Powershell internal penetration testing framework.	(https://github.com/praetorian-inc/pentestly)
pentmenu	A bash script for recon and DOS attacks.	(https://github.com/GinjaChris/pentmenu)
pepe	Collect information about email addresses from Pastebin.	(https://github.com/woj-ciech/pepe)
pepper	An open source script to perform malware static analysis on Portable Executable.	(https://github.com/Th3Hurrican3/PEpper)
periscope	A PE file inspection tool.	(http://ntsecurity.nu/toolbox/periscope/)
perl-image-exiftool	Reader and rewriter of EXIF information that supports raw files	(https://exiftool.org/)
persistencesniper	Hunt persistences implanted in Windows machines.	(https://github.com/last-byte/PersistenceSniper)
petools	Portable executable (PE) manipulation toolkit.	(https://github.com/petoolse/petools)
pev	Command line based tool for PE32/PE32+ file analysis.	(http://pev.sourceforge.net/)
pextractor	A forensics tool that can extract all files from an executable file created by a joiner or similar.	(http://packetstormsecurity.com/files/62977/PExtractor_v0.18b_binary_and_src.rar.html)
pftriage	Python tool and library to help analyze files during malware triage and analysis.	(https://github.com/idiom/pftriage)
pgdbf	Convert XBase / FoxPro databases to PostgreSQL	(https://github.com/kstrauser/pgdbf)
phantap	An 'invisible' network tap aimed at red teams.	(https://github.com/nccgroup/phantap)
phantom-evasion	Antivirus evasion tool written in python.	(https://github.com/oddcod3/Phantom-Evasion)
phemail	A python open source phishing email tool that automates the process of sending phishing emails as part of a social engineering test.	(https://github.com/Dionach/PhEmail)
phishery	An SSL Enabled Basic Auth Credential Harvester with a Word Document Template URL Injector.	(https://github.com/ryhanson/phishery)
phishingkithunter	Find phishing kits which use your brand/organization's files and image'.	(https://github.com/t4d/PhishingKitHunter)
phoneinfoga	Information gathering & OSINT framework for phone numbers.	(https://github.com/sundowndev/PhoneInfoga)
phonesploit	Adb exploiting tools.	(https://github.com/metachar/PhoneSploit)
phonia	Advanced toolkits to scan phone numbers using only free resources.	(https://github.com/entynetproject/phonia)
phoss	Sniffer designed to find HTTP, FTP, LDAP, Telnet, IMAP4, VNC and POP3 logins.	(http://www.phenoelit.org/fr/tools.html)
photon	Incredibly fast crawler which extracts urls, emails, files, website accounts and much more.	(https://github.com/s0md3v/Photon)
php-findsock-shell	A Findsock Shell implementation in PHP + C.	(https://github.com/pentestmonkey/php-findsock-shell)
php-malware-finder	Detect potentially malicious PHP files.	(https://github.com/jvoisin/php-malware-finder)
php-mt-seed	PHP mt_rand() seed cracker.	(http://www.openwall.com/php_mt_seed/)
php-rfi-payload-decoder	Decode and analyze RFI payloads developed in PHP.	(https://github.com/bwall/PHP-RFI-Payload-Decoder)
php-vulnerability-hunter	An whitebox fuzz testing tool capable of detected several classes of vulnerabilities in PHP web applications.	(https://phpvulnhunter.codeplex.com/)
phpggc	A library of PHP unserialize() payloads along with a tool to generate them, from command line or programmatically.	(https://github.com/ambionics/phpggc)
phpsploit	Stealth post-exploitation framework.	(https://github.com/nil0x42/phpsploit)
phpstan	PHP Static Analysis Tool - discover bugs in your code without running it.	(https://github.com/phpstan/phpstan)
phpstress	A PHP denial of service / stress test for Web Servers running PHP-FPM or PHP-CGI.	(https://github.com/nightlionsecurity/phpstress)
phrasendrescher	A modular and multi processing pass phrase cracking tool.	(http://www.leidecker.info/projects/phrasendrescher/)
pidense	Monitor illegal wireless network activities. (Fake Access Points)	(https://github.com/WiPi-Hunter/PiDense)
pin	A dynamic binary instrumentation tool.	(https://software.intel.com/en-us/articles/pin-a-binary-instrumentation-tool-downloads)
pingcastle	Active Directory scanning tool.	(https://www.pingcastle.com)
pinkerton	JavaScript file crawler and secret finder.	(https://github.com/oppsec/Pinkerton)
pintool	This tool can be useful for solving some reversing challenges in CTFs events.	(https://github.com/wagiro/pintool)
pintool2	Improved version of pintool.	(https://github.com/sebastiendamaye/pintool2)
pip3line	The Swiss army knife of byte manipulation.	(https://github.com/nccgroup/pip3line)
pipal	A password analyser.	(https://github.com/digininja/pipal)
pipeline	Designed to aid in targeted brute force password cracking attacks.	(https://github.com/hirnschallsebastian/Pipeline2)
pirana	Exploitation framework that tests the security of a email content filter.	(http://www.guay-leroux.com/projects.html)
pivotsuite	A portable, platform independent and powerful network pivoting toolkit.	(https://github.com/RedTeamOperations/PivotSuite)
pixd	Colourful visualization tool for binary files.	(https://github.com/FireyFly/pixd)
pixiewps	Offline bruteforce of the WPS pin exploiting the low or non-existing entropy of some APs	(https://github.com/wiire/pixiewps)
pixload	Image Payload Creating/Injecting tools.	(https://github.com/chinarulezzz/pixload)
pkcrack	A PkZip encryption cracker.	(https://www.unix-ag.uni-kl.de/~conrad/krypto/pkcrack/download1.html)
pkinittools	Tools for Kerberos PKINIT and relaying to AD CS.	(https://github.com/dirkjanm/PKINITtools)
pkt2flow	A simple utility to classify packets into flows.	(https://github.com/caesar0301/pkt2flow)
plasma-disasm	An interactive disassembler for x86/ARM/MIPS. It can generates indented pseudo-code with colored syntax.	(https://github.com/joelpx/plasma)
plcscan	This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols.	(http://packetstormsecurity.com/files/119726/PLC-Device-Scanner.html)
plecost	Wordpress finger printer Tool.	(https://github.com/iniqua/plecost)
plown	A security scanner for Plone CMS.	(https://github.com/unweb/plown)
plumber.py	A python implementation of a grep friendly ftrace wrapper.	(https://github.com/cybereason/linux_plumber)
plutil	Converts .plist files between binary and UTF (editable) text formats.	(http://scw.us/iPhone/plutil/)
pmacct	Small set of multi-purpose passive network monitoring tools [NetFlow IPFIX sFlow libpcap BGP BMP IGP Streaming Telemetry].	(https://github.com/pmacct/pmacct)

Name	Description	Website
pmap	Passively discover, scan, and fingerprint link-local peers by the background noise they generate (i.e. their broadcast and multicast traffic).	↗ (http://www.hellfiresecurity.com/tools.htm)
pmapper	A tool for quickly evaluating IAM permissions in AWS.	↗ (https://github.com/nccgroup/PMapper)
pmcma	Automated exploitation of invalid memory writes (being them the consequences of an overflow in a writable section, of a missing format string, integer overflow, variable misuse, or any other type of memory corruption).	↗ (http://packetstormsecurity.com/files/104724/Post-Memory-Corruption-Memory-Analyzer.00.html)
pmdump	A tool that lets you dump the memory contents of a process to a file without stopping the process.	↗ (http://ntsecurity.nu/toolbox/pmdump/)
pngcheck	Verifies the integrity of PNG, JNG and MNG files by checking the CRCs and decompressing the image data.	↗ (http://www.libpng.org/pub/png/apps/pngcheck.html)
pnscan	A parallel network scanner that can be used to survey TCP network services.	↗ (http://www.lysator.liu.se/~pen/pnscan/)
pocsuite	An open-sourced remote vulnerability testing framework developed by the Knownsec Security Team.	↗ (https://github.com/knownsec/Pocsuite)
poison	A fast, asynchronous syn and udp scanner.	↗ (http://nologin.org/main.pl?action=codeList&)
poly	Polymorphic webshells.	↗ (https://github.com/grCod/poly)
polyswarm	An interface to the public and private PolySwarm APIs.	↗ (https://github.com/polyswarm/polyswarm-api)
pompem	A python exploit tool finder.	↗ (https://github.com/rfunix/Pompem)
poracle	A tool for demonstrating padding oracle attacks.	↗ (https://github.com/iagox86/poracle)
portia	Automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised.	↗ (https://github.com/SpiderLabs/portia)
portmanteau	An experimental unix driver IOCTL security tool that is useful for fuzzing and discovering device driver attack surface.	↗ (https://packetstormsecurity.com/files/134230/Portmanteau-Unix-Driver-IOCTL-Security-Tool.html)
portspoof	This program's primary goal is to enhance OS security through a set of new techniques.	↗ (https://drk1wi.github.io/portspoof/)
postenum	Clean, nice and easy tool for basic/advanced privilege escalation techniques.	↗ (https://github.com/mbahadou/postenum)
posttester	A jar file that will send POST requests to servers in order to test for the hash collision vulnerability discussed at the Chaos Communication Congress in Berlin.	↗ (http://packetstormsecurity.com/files/109010/MagicHash-Collision-Testing-Tool.html)
powercloud	Deliver powershell payloads via DNS TXT via CloudFlare using PowerShell.	↗ (https://github.com/mantvydasb/Invoke-PowerCloud)
powerfuzzer	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.	↗ (http://www.powerfuzzer.com)
powerlessshell	Run PowerShell command without invoking powershell.exe.	↗ (https://github.com/Mr-Un1k0d3r/PowerLessShell)
powermft	Powerful commandline $MFT record editor.	↗ (https://github.com/jschicht/PowerMft)
powerops	PowerShell Runspace Portable Post Exploitation Tool aimed at making Penetration Testing with PowerShell "easier".	↗ (https://github.com/fdiskyou/PowerOPS)
powershdll	Run PowerShell with rundll32. Bypass software restrictions.	↗ (https://github.com/p3nt4/PowerShdll)
powersploit	A PowerShell Post-Exploitation Framework.	↗ (https://github.com/mattifestation/PowerSploit)
powerstager	A payload stager using PowerShell.	↗ (https://github.com/z0noxz/powerstager)
pown	Security testing and exploitation toolkit built on top of Node.js and NPM.	↗ (https://github.com/pownjs/pown)
ppee	A Professional PE file Explorer for reversers, malware researchers and those who want to statically inspect PE files in more details.	↗ (https://www.mzrst.com/)
ppfuzz	A fast tool to scan client-side prototype pollution vulnerability written in Rust.	↗ (https://github.com/dwisiswant0/ppfuzz)
ppmap	A scanner/exploitation tool written in GO, which leverages client-side Prototype Pollution to XSS by exploiting known gadgets.	↗ (https://github.com/kleiton0x00/ppmap)
ppscan	Yet another port scanner with HTTP and FTP tunneling support.	↗ (https://packetstormsecurity.com/files/82897/PPScan-Portscanner.3.html)
pr0cks	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.	↗ (https://github.com/n1nj4sec/pr0cks)
prads	A "Passive Real-time Asset Detection System".	↗ (http://gamelinux.github.io/prads/)
praeda	An automated data/information harvesting tool designed to gather critical information from various embedded devices.	↗ (https://github.com/percx/Praeda)
preeny	Some helpful preload libraries for pwning stuff.	↗ (https://github.com/zardus/preeny)
pret	Printer Exploitation Toolkit - The tool that made dumpster diving obsolete.	↗ (https://github.com/RUB-NDS/PRET)
princeprocessor	Standalone password candidate generator using the PRINCE algorithm.	↗ (https://github.com/jsteube/princeprocessor/)
procdump	Generate coredumps based off performance triggers.	↗ (https://github.com/Microsoft/ProcDump-for-Linux)
proctal	Provides a command line interface and a C library to manipulate the address space of a running program on Linux.	↗ (https://github.com/daniel-araujo/proctal)
procyon	A suite of Java metaprogramming tools focused on code generation and analysis.	↗ (https://github.com/mstrobel/procyon)
profuzz	Simple PROFINET fuzzer based on Scapy.	↗ (https://github.com/HSASec/ProFuzz)
prometheus-firewall	A Firewall analyzer written in ruby	↗ (https://github.com/averagesecurityguy/prometheus)
promiscdetect	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.	↗ (http://ntsecurity.nu/toolbox/promisdetect/)
propecia	A fast class scanner that scans for a specified open port with banner grabbing	↗ (http://www.redlevel.org)
protos-sip	SIP test suite.	↗ (https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c07-sip)
protosint	Python script that helps you investigate Protonmail accounts and ProtonVPN IP addresses.	↗ (https://github.com/pixelbubble/ProtOSINT)
prowler	Tool for AWS security assessment, auditing and hardening.	↗ (https://github.com/alfresco/prowler)
proxenet	THE REAL hacker friendly proxy for web application pentests.	↗ (https://github.com/hugsy/proxenet)
proxify	Swiss Army knife Proxy tool for HTTP/HTTPS traffic capture, manipulation, and replay on the go.	↗ (https://github.com/projectdiscovery/proxify)
proxmark	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.	↗ (https://github.com/Proxmark/proxmark3)
proxmark3	Software for the the Proxmark3, an RFID swiss-army tool	↗ (https://github.com/RfidResearchGroup/proxmark3)
proxybroker2	Proxy [Finder	↗ (Server]. HTTP(S) & SOCKS.| blackarch-proxy |https://github.com/bluet/proxybroker2)

Name	Description	Website
proxychains-ng	A hook preloader that allows to redirect TCP traffic of existing dynamically linked programs through one or more SOCKS or HTTP proxies	↗ (https://github.com/rofl0r/proxychains-ng)
proxycheck	This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver.	↗ (http://packetstormsecurity.com/files/61864/proxycheck.pl.txt.html)
proxyp	Small multithreaded Perl script written to enumerate latency, port numbers, server names, & geolocations of proxy IP addresses.	↗ (http://sourceforge.net/projects/proxyp/)
proxyscan	A security penetration testing tool to scan for hosts and ports through a Web proxy server.	↗ (http://packetstormsecurity.com/files/69778/proxyScan.3.tgz.html)
proxytunnel	Creates tunnels through HTTP(S) proxies for any TCP based protocol	↗ (https://github.com/proxytunnel/proxytunnel)
ps1encode	A tool to generate and encode a PowerShell based Metasploit payloads.	↗ (https://github.com/CroweCybersecurity/ps1encode)
pscan	A limited problem scanner for C source files	↗ (http://deployingradius.com/pscan/)
pshitt	A lightweight fake SSH server designed to collect authentication data sent by intruders.	↗ (https://github.com/regit/pshitt)
pspy	Monitor linux processes without root permissions.	↗ (https://github.com/DominicBreuker/pspy)
pstoreview	Lists the contents of the Protected Storage.	↗ (http://www.ntsecurity.nu/toolbox/pstoreview/)
ptf	The Penetration Testers Framework: Way for modular support for up-to-date tools.	↗ (https://github.com/trustedsec/ptf)
pth-toolkit	Modified version of the passing-the-hash tool collection made to work straight out of the box.	↗ (https://github.com/byt3bl33d3r/pth-toolkit)
ptunnel	A tool for reliably tunneling TCP connections over ICMP echo request and reply packets	↗ (https://www.cs.uit.no/~daniels/PingTunnel)
pulledpork	Snort rule management.	↗ (https://github.com/shirkdog/pulledpork)
pulsar	Protocol Learning and Stateful Fuzzing.	↗ (https://github.com/hgascon/pulsar)
punk	A post-exploitation tool meant to help network pivoting from a compromised unix box.	↗ (https://github.com/r3vn/punk.py)
punter	Hunt domain names using DNSDumpster, WHOIS, Reverse WHOIS, Shodan, Crimeflare.	↗ (https://github.com/nethunteros/punter)
pupy	Opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.	↗ (https://github.com/n1nj4sec/pupy)
pureblood	A Penetration Testing Framework created for Hackers / Pentester / Bug Hunter.	↗ (https://github.com/cr4shcod3/pureblood)
puredns	Fast domain resolver and subdomain bruteforcing with accurate wildcard filtering.	↗ (https://github.com/d3mondev/puredns)
pwcrack	Password hash automatic cracking framework.	↗ (https://github.com/L-codes/pwcrack-framework)
pwd-hash	A password hashing tool that use the crypt function to generate the hash of a string given on standard input.	↗ (http://vladz.devzero.fr/pwd-hash.php)
pwdlogy	A target specific wordlist generating tool for social engineers and security researchers.	↗ (https://github.com/tch1001/pwdlogy)
pwdlyser	Python-based CLI Password Analyser (Reporting Tool).	↗ (https://github.com/ins1gn1a/pwdlyser)
pwdump	Extracts the binary SAM and SYSTEM file from the filesystem and then the hashes.	↗ (http://www.tarasco.org/security/pwdump_7/index.html)
pwfuzz-rs	Rust-based password mutator for brute force attacks.	↗ (https://github.com/mttaggart/pwfuzz-rs)
pwnat	A tool that allows any number of clients behind NATs to communicate with a server behind a separate NAT with *no* port forwarding and *no* DMZ setup on any routers in order to directly communicate with each other.	↗ (http://samy.pl/pwnat/)
pwncat	Bind and reverse shell handler with FW/IDS/IPS evasion, self-inject and port-scanning.	↗ (https://github.com/cytopia/pwncat)
pwncat-caleb	A post-exploitation platform.	↗ (https://github.com/calebstewart/pwncat)
pwndbg	Makes debugging with GDB suck less	↗ (https://github.com/pwndbg/pwndbg)
pwndora	Massive IPv4 scanner, find and analyze internet-connected devices in minutes, create your own IoT search engine at home.	↗ (https://github.com/alechilczenko/pwndora)
pwndrop	Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV.	↗ (https://github.com/kgretzky/pwndrop)
pwned	A command-line tool for querying the 'Have I been pwned?' service.	↗ (https://github.com/wKovacs64/pwned)
pwned-search	Pwned Password API lookup.	↗ (https://github.com/mikepound/pwned-search)
pwnedornot	Tool to find passwords for compromised email addresses.	↗ (https://github.com/thewhiteh4t/pwnedOrNot)
pwnedpasswords	Generate and verify pwnedpasswords check digits.	↗ (https://github.com/lionheart/pwnedpasswords)
pwnloris	An improved slowloris DOS tool which keeps attacking until the server starts getting exhausted.	↗ (https://github.com/h0ussni/pwnloris)
pyaxmlparser	A simple parser to parse Android XML file.	↗ (https://github.com/appknox/pyaxmlparser)
pybozocrack	A silly & effective MD5 cracker in Python.	↗ (https://github.com/ikkebr/PyBozoCrack)
pydictor	A useful hacker dictionary builder for a brute-force attack.	↗ (https://github.com/LandGrey/pydictor)
pyersinia	Network attack tool like yersinia but written in Python.	↗ (https://github.com/nottinghamprisateam/pyersinia)
pyew	A python tool to analyse malware.	↗ (https://code.google.com/p/pyew/)
pyexfil	A couple of beta stage tools for data exfiltration.	↗ (https://github.com/ytisf/PyExfil)
pyfiscan	Free web-application vulnerability and version scanner.	↗ (https://github.com/fgeek/pyfiscan)
pyfuscation	Obfuscate powershell scripts by replacing Function names, Variables and Parameters.	↗ (https://github.com/CBHue/PyFuscation)
pyinstaller	A program that converts (packages) Python programs into stand-alone executables, under Windows, Linux, Mac OS X, Solaris and AIX.	↗ (http://www.pyinstaller.org/downloads.html)
pyjfuzz	Python JSON Fuzzer.	↗ (https://github.com/mseclab/PyJFuzz)
pykek	Kerberos Exploitation Kit.	↗ (https://github.com/bidord/pykek)
pymeta	Auto Scanning to SSL Vulnerability.	↗ (https://github.com/m8r0wn/pymeta)
pyminifakedns	Minimal DNS server written in Python; it always replies with a 127.0.0.1 A-record.	↗ (http://code.activestate.com/recipes/491264/)
pyrasite	Code injection and introspection of running Python processes.	↗ (https://pypi.org/project/pyrasite/#files)
pyrdp	Python 3 RDP MITM and library.	↗ (https://github.com/GoSecure/pyrdp)
pyrit	The famous WPA precomputed cracker.	↗ (https://github.com/JPaulMora/Pyrit)
pyssltest	A python multithreaded script to make use of Qualys ssllabs api to test SSL flaws.	↗ (https://github.com/moheshmohan/pyssltest)
pytacle	Automates the task of sniffing GSM frames	↗ (http://packetstormsecurity.com/files/124299/pytacle-alpha2.tar.gz)
pytbull	Next generation of pytbull, IDS/IPS testing framework.	↗ (https://github.com/netrunn3r/pytbull-ng)
pythem	Python2 penetration testing framework.	↗ (https://github.com/m4n3dw0lf/PytheM)
python-api-dnsdumpster	Unofficial Python API for http://dnsdumpster.com/.	↗ (https://github.com/PaulSec/API-dnsdumpster.com)
python-arsenic	Async WebDriver implementation for asyncio and asyncio-compatible frameworks.	↗ (https://github.com/HDE/arsenic/releases)
python-capstone	Lightweight multi-platform, multi-architecture disassembly framework	↗ (https://www.capstone-engine.org/index.html)

Name	Description	Website
python-cymruwhois	Python client for the whois.cymru.com service	↗ (https://pypi.org/project/cymruwhois/#files)
python-frida	Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.	↗ (https://pypi.org/project/frida/#files)
python-frida-tools	Frida CLI tools.	↗ (https://pypi.org/project/frida-tools/#files)
python-google-streetview	A command line tool and module for Google Street View Image API.	↗ (https://pypi.org/project/google-streetview/#files)
python-ivre	Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (library)	↗ (https://ivre.rocks/)
python-jsbeautifier	JavaScript unobfuscator and beautifier	↗ (https://github.com/beautify-web/js-beautify)
python-keylogger	Simple keystroke logger.	↗ (https://github.com/GiacomoLaw/Keylogger)
python-mmbot	Powerful malicious file triage tool for cyber responders.	↗ (https://github.com/egaus/MaliciousMacroBot)
python-oletools	Tools to analyze Microsoft OLE2 files.	↗ (https://pypi.org/project/oletools/)
python-pcodedmp	A VBA p-code disassembler.	↗ (https://pypi.org/project/pcodedmp/#files)
python-peid	Python implementation of the Packed Executable iDentifier (PEiD).	↗ ()
python-pwntools	CTF framework and exploit development library	↗ (https://github.com/Gallopsled/pwntools)
python-search-engine-parser	Scrapes search engine pages for query titles, descriptions and links.	↗ (https://pypi.org/project/search-engine-parser/#files)
python-shodan	The official Python library and CLI for Shodan	↗ (https://shodan.readthedocs.io/)
python-ssh-mitm	SSH mitm server for security audits supporting public key authentication, session hijacking and file manipulation.	↗ (https://pypi.org/project/ssh-mitm/#files)
python-trackerjacker	Finds and tracks wifi devices through raw 802.11 monitoring.	↗ (https://github.com/calebmadrigal/trackerjacker)
python-uncompyle6	A Python cross-version decompiler.	↗ (https://pypi.org/project/uncompyle6/#files)
python-utidylib	Python bindings for Tidy HTML parser/cleaner.	↗ (http://utidylib.berlios.de)
python-witnessme	Web Inventory tool, takes screenshots of webpages using Pyppeteer.	↗ (https://pypi.org/project/witnessme/#files)
python-yara-rednaga	The Python interface for YARA.	↗ (https://github.com/rednaga/yara-python)
python2-api-dnsdumpster	Unofficial Python API for http://dnsdumpster.com/.	↗ (https://github.com/PaulSec/API-dnsdumpster.com)
python2-capstone	A disassembly framework with the target of becoming the ultimate disasm engine for binary analysis and reversing in the security community.	↗ (https://github.com/aquynh/capstone)
python2-cymruwhois	Python client for the whois.cymru.com service	↗ (https://pypi.org/project/cymruwhois/#files)
python2-darts.util.lru	Simple dictionary with LRU behaviour.	↗ (https://pypi.python.org/pypi/darts.util.lru)
python2-exrex	Irregular methods on regular expressions.	↗ (https://github.com/asciimoo/exrex)
python2-frida	Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.	↗ (https://pypi.org/project/frida/#files)
python2-frida-tools	Frida CLI tools.	↗ (https://pypi.org/project/frida-tools/#files)
python2-google-streetview	A command line tool and module for Google Street View Image API.	↗ (https://pypi.org/project/google-streetview/#files)
python2-hpfeeds	Honeynet Project generic authenticated datafeed protocol.	↗ (https://github.com/rep/hpfeeds)
python2-ivre	Network recon framework based on Nmap, Masscan, Zeek (Bro), Argus, Netflow,... (library)	↗ (https://ivre.rocks/)
python2-jsbeautifier	JavaScript unobfuscator and beautifier.	↗ (https://github.com/beautify-web/js-beautify)
python2-ldapdomaindump	Active Directory information dumper via LDAP.	↗ (https://pypi.org/project/ldapdomaindump/#files)
python2-minidump	Python library to parse and read Microsoft minidump file format.	↗ (https://github.com/skelsec/minidump)
python2-minikerberos	Kerberos manipulation library in pure Python.	↗ (https://github.com/skelsec/minikerberos)
python2-oletools	Tools to analyze Microsoft OLE2 files.	↗ (https://pypi.org/project/oletools/)
python2-pcodedmp	A VBA p-code disassembler.	↗ (https://pypi.org/project/pcodedmp/#files)
python2-peepdf	A Python tool to explore PDF files in order to find out if the file can be harmful or not.	↗ (http://eternal-todo.com/tools/peepdf-pdf-analysis-tool)
python2-ropgadget	Pythonic argument parser, that will make you smile.	↗ (https://pypi.org/project/ropgadget/#files)
python2-shodan	Python library and command-line utility for Shodan (https://developer.shodan.io).	↗ (https://pypi.org/project/shodan/#files)
python2-yara	Python interface for YARA.	↗ (https://pypi.org/project/yara-python/#files)
qark	Tool to look for several security related Android application vulnerabilities.	↗ (https://github.com/linkedin/qark)
qrgen	Simple script for generating Malformed QRCodes.	↗ (https://github.com/h0nus/QRGen)
qrljacker	QRLJacker is a highly customizable exploitation framework to demonstrate "QRLJacking Attack Vector".	↗ (https://github.com/OWASP/QRLJacking/tree/master/QRLJacker)
qsreplace	Accept URLs on stdin, replace all query string values with a user-supplied value, only output each combination of query string parameters once per host and path.	↗ (https://github.com/tomnomnom/qsreplace)
quark-engine	An Obfuscation-Neglect Android Malware Scoring System.	↗ (https://github.com/quark-engine/quark-engine)
quickrecon	A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing.	↗ (http://packetstormsecurity.com/files/104314/QuickRecon.3.2.html)
quicksand-lite	Command line tool for scanning streams within office documents plus xor db attack.	↗ (https://github.com/tylabs/quicksand_lite)
quickscope	Statically analyze windows, linux, osx, executables and also APK files.	↗ (https://github.com/CYB3RMX/Qu1cksc0pe)
r2ghidra	Deep ghidra decompiler integration for radare2 and iaito	↗ (https://github.com/radareorg/r2ghidra)
rabid	A CLI tool and library allowing to simply decode all kind of BigIP cookies	↗ (https://noraj.github.io/rabid/)
raccoon	A high performance offensive security tool for reconnaissance and vulnerability scanning.	↗ (https://github.com/evyatarmeged/Raccoon)
radamsa	General purpose mutation based fuzzer	↗ (https://gitlab.com/akihe/radamsa)
radare2	Open-source tools to disasm, debug, analyze and manipulate binary files	↗ (https://radare.org)
radare2-keystone	Keystone assembler plugins for radare2.	↗ (https://github.com/radare/radare2-extras/tree/master/unicorn)
radare2-unicorn	Unicorn Emulator Plugin for radare2.	↗ (https://github.com/radare/radare2-extras/tree/master/unicorn)
radiography	A forensic tool which grabs as much information as possible from a Windows system.	↗ (http://www.security-projects.com/?RadioGraPhy)
rainbowcrack	Password cracker based on the faster time-memory trade-off. With MySQL and Cisco PIX Algorithm patches.	↗ (http://project-rainbowcrack.com/)
ranger-scanner	A tool to support security professionals to access and interact with remote Microsoft Windows based systems.	↗ (https://github.com/funkandwagnalls/ranger)

Name	Description	Website
rapidscan	The Multi-Tool Web Vulnerability Scanner.	↗ (https://github.com/skavngr/rapidscan)
rarcrack	Bruteforce password cracker for rar, 7z, zip archives	↗ (https://github.com/ziman/rarcrack)
rasenum	A small program which lists the information for all of the entries in any phonebook file (.pbk).	↗ (http://www.cultdeadcow.com/tools/rasenum.html)
rathole	A reverse proxy for NAT traversal	↗ (https://github.com/rapiz1/rathole)
ratproxy	A passive web application security assessment tool	↗ (http://code.google.com/p/ratproxy/)
rats	A rough auditing tool for security in source code files.	↗ (https://github.com/andrew-d/rough-auditing-tool-for-security)
raven	A Linkedin information gathering tool that can be used by pentesters to gather information about an organization employees using Linkedin.	↗ (https://github.com/0x09AL/raven)
rawr	Rapid Assessment of Web Resources. A web enumerator.	↗ (https://bitbucket.org/al14s/rawr/wiki/Home)
rawsec-cli	Rawsec Inventory search CLI to find security tools and resources.	↗ (https://github.com/mBouamama/rawsec_cli)
rbac-lookup	A CLI that allows you to easily find Kubernetes roles and cluster roles bound to any user.	↗ (https://github.com/FairwindsOps/rbac-lookup)
rbasefind	A firmware base address search tool.	↗ (https://github.com/sgayou/rbasefind)
rbkb	A miscellaneous collection of command-line tools related to pen-testing and reversing.	↗ (https://github.com/emonti/rbkb)
rbndr	Simple DNS Rebinding Service.	↗ (https://github.com/taviso/rbndr)
rcracki-mt	A tool to perform rainbow table attacks on password hashes. It is intended for indexed/ perfected rainbow tables, mainly generated by the distributed project www.freerainbowtables.com	↗ (http://rcracki.sourceforge.net/)
rcrdcarver	Carve RCRD records ($LogFile) from a chunk of data..	↗ (https://github.com/jschicht/RcrdCarver)
rdesktop-brute	It connects to windows terminal servers - Bruteforce patch included.	↗ (http://www.rdesktop.org/)
rdp-cipher-checker	Enumerate the encryption protocols supported by the server and the cipher strengths supported using native RDP encryption.	↗ (https://labs.f-secure.com/tools/rdp-cipher-checker/)
rdp-sec-check	Script to enumerate security settings of an RDP Service.	↗ (https://github.com/portcullislabs/rdp-sec-check)
rdpassspray	Python3 tool to perform password spraying using RDP.	↗ (https://github.com/xFreed0m/RDPassSpray)
rdwarecon	A python script to extract information from a Microsoft Remote Desktop Web Access (RDWA) application.	↗ (https://github.com/p0dalirius/RDWArecon)
reaver	Brute force attack against Wifi Protected Setup	↗ (https://github.com/t6x/reaver-wps-fork-t6x)
rebind	DNS Rebinding Tool	↗ (http://code.google.com/p/rebind/)
recaf	Modern Java bytecode editor.	↗ (https://github.com/Col-E/Recaf)
recentfilecache-parser	Python parser for the RecentFileCache.bcf on Windows.	↗ (https://github.com/prolsen/recentfilecache-parser)
recomposer	Randomly changes Win32/64 PE Files for 'safer' uploading to malware and sandbox sites.	↗ (https://github.com/secretsquirrel/recomposer)
recon-ng	A full-featured Web Reconnaissance framework written in Python.	↗ (https://github.com/lanmaster53/recon-ng)
reconnoitre	A security tool for multithreaded information gathering and service enumeration.	↗ (https://github.com/codingo/Reconnoitre)
reconscan	Network reconnaissance and vulnerability assessment tools.	↗ (https://github.com/RoliSoft/ReconScan)
recoverdm	Recover damaged CD DVD and disks with bad sectors.	↗ (http://www.vanheusden.com/recoverdm/)
recoverjpeg	Recover jpegs from damaged devices.	↗ (https://github.com/samueltardieu/recoverjpeg)
recsech	Tool for doing Footprinting and Reconnaissance on the target web.	↗ (https://github.com/radenvodka/Recsech)
recstudio	Cross platform interactive decompiler.	↗ (http://www.backerstreet.com/rec/rec.htm)
recuperabit	A tool for forensic file system reconstruction.	↗ (https://github.com/Lazza/RecuperaBit)
red-hawk	All in one tool for Information Gathering, Vulnerability Scanning and Crawling.	↗ (https://github.com/Tuhinshubhra/RED_HAWK)
redasm	Interactive, multiarchitecture disassembler written in C++ using Qt5 as UI Framework.	↗ (https://github.com/REDasmOrg/REDasm)
redfang	Finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the devices' Bluetooth addresses and calling read_remote_name().	↗ (http://packetstormsecurity.com/files/31864/redfang.2.5.tar.gz.html)
redirectpoison	A tool to poison a targeted issuer of SIP INVITE requests with 301 (i.e. Moved Permanently) redirection responses.	↗ (http://www.hackingexposedvoip.com/)
redpoint	Digital Bond's ICS Enumeration Tools.	↗ (https://github.com/digitalbond/Redpoint3)
redress	A tool for analyzing stripped Go binaries.	↗ (https://github.com/goretk/redress)
redsocks	Transparent redirector of any TCP connection to proxy.	↗ (https://github.com/darkk/redsocks)
reelphish	A Real-Time Two-Factor Phishing Tool.	↗ (https://github.com/fireeye/ReelPhish)
regeorg	The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.	↗ (https://github.com/sensepost/reGeorg)
regipy	Library for parsing offline registry hives.	↗ (https://github.com/mkorman90/regipy)
reglookup	Command line utility for reading and querying Windows NT registries	↗ (http://projects.sentinelchicken.org/reglookup)
regreport	Windows registry forensic analysis tool.	↗ (https://www.gaijin.at/dlregreport.php)
regripper	Open source forensic software used as a Windows Registry data extraction command line or GUI tool.	↗ (https://github.com/keydet89/RegRipper3.0)
regrippy	Framework for reading and extracting useful forensics data from Windows registry hives.	↗ (https://pypi.org/project/regrippy/#files)
regview	Open raw Windows NT 5 Registry files (Windows 2000 or higher).	↗ (https://www.gaijin.at/en/dlregview.php)
rekall	Memory Forensic Framework.	↗ (https://github.com/google/rekall)
relay-scanner	An SMTP relay scanner.	↗ (http://www.cirt.dk)
remot3d	An Simple Exploit for PHP Language.	↗ (https://github.com/KeepWannabe/Remot3d)
replayproxy	Forensic tool to replay web-based attacks (and also general HTTP traffic) that were captured in a pcap file.	↗ (https://code.google.com/p/replayproxy/)
reptor	CLI tool to automate pentest reporting with SysReptor.	↗ (https://github.com/Syslifters/reptor)
resourcehacker	Resource compiler and decompiler for Windows® applications.	↗ (http://www.angusj.com/resourcehacker/)
responder	A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2 (multirelay version).	↗ (https://github.com/lgandx/Responder)
restler-fuzzer	First stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services.	↗ (https://github.com/microsoft/restler-fuzzer)
retdec	Retargetable machine-code decompiler based on LLVM.	↗ (https://retdec.com/)
retire	Scanner detecting the use of JavaScript libraries with known vulnerabilities.	↗ (http://retirejs.github.io/retire.js/)
reverseip	Ruby based reverse IP-lookup tool.	↗ (https://github.com/lolwaleet/ReverseIP)
revipd	A simple reverse IP domain scanner.	↗ (https://github.com/PypeRanger/revipd)
revsh	A reverse shell with terminal support, data tunneling, and advanced pivoting capabilities.	↗ (https://github.com/emptymonkey/revsh/)

Name	Description	Website
rex	Shellphish's automated exploitation engine, originally created for the Cyber Grand Challenge.	(https://github.com/shellphish/rex)
rext	Router EXploitation Toolkit - small toolkit for easy creation and usage of various python scripts that work with embedded devices.	(https://github.com/j91321/rext)
rfcat	RF ChipCon-based Attack Toolset.	(http://code.google.com/p/rfcat)
rfdump	Tool to detect RFID-Tags and show their meta information	(http://www.rfdump.org)
rfidiot	An open source python library for exploring RFID devices.	(http://rfidiot.org/)
rfidtool	A opensource tool to read / write rfid tags	(http://www.bindshell.net/tools/rfidtool.html)
rhodiola	Personalized wordlist generator with NLP, by analyzing tweets (A.K.A crunch2049).	(https://github.com/utkusen/rhodiola)
richsploit	Exploitation toolkit for RichFaces.	(https://github.com/redtimmy/Richsploit)
ridenum	A null session RID cycle attack for brute forcing domain controllers.	(https://github.com/trustedsec/ridenum)
ridrelay	Enumerate usernames on a domain where you have no creds by using SMB Relay with low priv.	(https://github.com/skorov/ridrelay)
rifiuti2	A rewrite of rifiuti, a great tool from Foundstone folks for analyzing Windows Recycle Bin INFO2 file.	(https://github.com/abelcheung/rifiuti2)
rinetd	Internet redirection server.	(http://www.boutell.com/rinetd)
ripdc	A script which maps domains related to an given ip address or domainname.	(http://nullsecurity.net/tools/scanner)
rita	Real Intelligence Threat Analytics.	(https://github.com/activecm/rita)
riwifshell	Web backdoor - infector - explorer.	(https://github.com/graniet/riwifshell)
rkhunter	Checks machines for the presence of rootkits and other unwanted tools.	(http://rkhunter.sourceforge.net/)
rlogin-scanner	Multithreaded rlogin scanner. Tested on Linux, OpenBSD and Solaris.	(http://wayreth.eu.org/old_page/)
rmiscout	Enumerate Java RMI functions and exploit RMI parameter unmarshalling vulnerabilities.	(https://github.com/BishopFox/rmiscout)
rogue-mysql-server	A rogue MySQL server written in Python.	(https://github.com/Gifts/Rogue-MySql-Server)
roguehostapd	Hostapd fork including Wi-Fi attacks and providing Python bindings with ctypes.	(https://github.com/wifiphisher/roguehostapd)
rombuster	A router exploitation tool that allows to disclosure network router admin password.	(https://github.com/EntySec/RomBuster)
rootbrute	Local root account bruteforcer.	(http://www.packetstormsecurity.org/)
ropeadope	A linux log cleaner.	(http://www.highhacksociety.com/)
ropeme	A set of python scripts to generate ROP gadgets and payload.	(http://www.vnsecurity.net/2010/08/ropeme-rop-exploit-made-easy/)
ropgadget	Search gadgets in binaries to facilitate ROP exploitation for several file formats and architectures	(http://www.shell-storm.org/project/ROPgadget)
ropper	Show information about binary files and find gadgets to build rop chains for different architectures	(https://github.com/sashs/Ropper)
roputils	A Return-oriented Programming toolkit.	(https://github.com/inaz2/roputils)
routerhunter	Tool used to find vulnerable routers and devices on the Internet and perform tests.	(https://github.com/jh00nbr/Routerhunter.0)
routersploit	Open-source exploitation framework dedicated to embedded devices	(https://github.com/threat9/routersploit)
rp	A full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O x86/x64 binaries.	(https://github.com/0vercl0k/rp)
rpak	A collection of tools that can be useful for doing attacks on routing protocols.	(http://ntsecurity.nu/toolbox/promisdetect/)
rpcsniffer	Sniffs WINDOWS RPC messages in a given RPC server process.	(https://github.com/AdiKo/RPCSniffer)
rpctools	Contains three separate tools for obtaining information from a system that is running RPC services	(https://packetstormsecurity.com/files/31879/rpctools.0.zip.html)
rpdscan	Remmina Password Decoder and scanner.	(https://github.com/freakyclown/RPDscan)
rpivot	Socks4 reverse proxy for penetration testing.	(https://github.com/artkond/rpivot)
rr	A Record and Replay Framework.	(https://github.com/mozilla/rr)
rrs	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.	(http://www.cycom.se/dl/rrs)
rsactftool	RSA tool for ctf - retrieve private key from weak public key and/or uncipher data.	(https://github.com/Ganapati/RsaCtfTool)
rsakeyfind	A tool to find RSA key in RAM.	(http://citp.princeton.edu/memory/code/)
rsatool	Tool that can be used to calculate RSA and RSA-CRT parameters.	(https://github.com/ius/rsatool)
rshack	Python tool which allows to carry out some attacks on RSA, and offer a few tools to manipulate RSA keys.	(https://github.com/zweisamkeit/RSHack)
rsmangler	rsmangler takes a wordlist and mangle it	(http://www.randomstorm.com/rsmangler-security-tool.php)
rspet	A Python based reverse shell equipped with functionalities that assist in a post exploitation scenario.	(https://github.com/panagiks/RSPET)
rtfm	A database of common, interesting or useful commands, in one handy referable form.	(https://github.com/leostat/rtfm)
rtlamr	An rtl-sdr receiver for smart meters operating in the 900MHz ISM band.	(https://github.com/bemasher/rtlamr/)
rtlizer	Simple spectrum analyzer.	(https://github.com/csete/rtlizer)
rtlsdr-scanner	A cross platform Python frequency scanning GUI for the OsmoSDR rtl-sdr library.	(https://github.com/EarToEarOak/RTLSDR-Scanner)
rtp-flood	RTP flooder	(http://www.hackingexposedvoip.com/)
rtpbreak	Detects, reconstructs and analyzes any RTP session	(http://xenion.antifork.org/rtpbreak/)
rubilyn	64bit Mac OS-X kernel rootkit that uses no hardcoded address to hook the BSD subsystem in all OS-X Lion & below. It uses a combination of syscall hooking and DKOM to hide activity on a host.	(http://nullsecurity.net/tools/backdoor.html)
ruler	A tool to abuse Exchange services.	(https://github.com/sensepost/ruler)
rulesfinder	Machine-learn password mangling rules.	(https://github.com/synacktiv/rulesfinder)
rupture	A framework for BREACH and other compression-based crypto attacks.	(https://github.com/decrypto-org/rupture)
rustbuster	DirBuster for Rust.	(https://github.com/phra/rustbuster)
rustcat	A modern port listener and reverse shell.	(https://github.com/robiot/rustcat)
rusthound	Active Directory data collector for BloodHound.	(https://github.com/OPENCYBER-FR/RustHound)
rustpad	Multi-threaded Padding Oracle attacks against any service.	(https://github.com/Kibouo/rustpad)
rustscan	A modern port scanner	(https://github.com/rustscan/RustScan)
rvi-capture	Capture packets sent or received by iOS devices.	(https://github.com/gh2o/rvi_capture)
rww-attack	Performs a dictionary attack against a live Microsoft Windows Small Business Server.	(http://packetstormsecurity.com/files/79021/Remote-Web-Workplace-Attack-Tool.html)

Name	Description	Website
rz-cutter	Qt and C++ GUI for rizin reverse engineering framework	(https://github.com/rizinorg/cutter)
rz-ghidra	Deep ghidra decompiler integration for rizin and rz-cutter	(https://github.com/rizinorg/rz-ghidra)
s3-fuzzer	A concurrent, command-line AWS S3 Fuzzer.	(https://github.com/petermbenjamin/s3-fuzzer)
s3enum	Amazon S3 bucket enumeration.	(https://github.com/koenrh/s3enum)
s3scanner	A tool to find open S3 buckets in AWS or other cloud providers.	(https://github.com/sa7mon/S3Scanner)
safecopy	A disk data recovery tool to extract data from damaged media.	(http://safecopy.sourceforge.net/)
sagan	A snort-like log analysis engine.	(https://quadrantsec.com/sagan_log_analysis_engine/)
sakis3g	An all-in-one script for connecting with 3G.	(http://www.sakis3g.org/)
saleae-logic	Debug happy.	(https://www.saleae.com/downloads)
sambascan	Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds.	(http://sourceforge.net/projects/sambascan2/)
samdump2	Dump password hashes from a Windows NT/2k/XP installation	(http://sourceforge.net/projects/ophcrack/files/samdump2/)
samesame	Command line tool to generate crafty homograph strings.	(https://github.com/TheTarquin/samesame)
samplicator	Send copies of (UDP) datagrams to multiple receivers, with optional sampling and spoofing.	(https://github.com/sleinen/samplicator)
samydeluxe	Automatic samdump creation script.	(http://github.com/jensp/samydeluxe)
sandcastle	A Python script for AWS S3 bucket enumeration.	(https://github.com/0xSearches/sandcastle)
sandmap	Simple CLI with the ability to run pure Nmap engine, 31 modules with 459 scan profiles.	(https://github.com/trimstray/sandmap)
sandsifter	The x86 processor fuzzer.	(https://github.com/xoreaxeaxeax/sandsifter)
sandy	An open-source Samsung phone encryption assessment framework	(https://github.com/donctl/sandy)
saruman	ELF anti-forensics exec, for injecting full dynamic executables into process image (With thread injection).	(https://github.com/elfmaster/saruman)
sasm	A simple crossplatform IDE for NASM, MASM, GAS and FASM assembly languages.	(https://github.com/Dman95/SASM)
sawef	Send Attack Web Forms.	(https://github.com/danilovazb/sawef)
sb0x	A simple and Lightweight framework for Penetration testing.	(https://github.com/levi0x0/sb0x-project)
sbd	Netcat-clone, portable, offers strong encryption - features AES-CBC + HMAC-SHA1 encryption, program execution (-e), choosing source port, continuous reconnection with delay + more	(http://www2.packetstormsecurity.org/cgi-bin/search/search.cgi?searchvalue=sbd)
sc-make	Tool for automating shellcode creation.	(https://github.com/t00sh/sc-make)
scalpel	A frugal, high performance file carver.	(http://www.digitalforensicssolutions.com/Scalpel/)
scamper	A tool that actively probes the Internet in order to analyze topology and performance.	(http://www.caida.org/tools/measurement/scamper/)
scanless	Utility for using websites that can perform port scans on your behalf.	(https://github.com/vesche/scanless)
scanmem	Memory scanner designed to isolate the address of an arbitrary variable in an executing process	(https://github.com/scanmem/scanmem)
scannerl	The modular distributed fingerprinting engine.	(https://github.com/kudelskisecurity/scannerl)
scanqli	SQLi scanner to detect SQL vulns.	(https://github.com/bambish/ScanQLi)
scansploit	Exploit using barcodes, QRcodes, earn13, datamatrix.	(https://github.com/huntergregal/scansploit)
scanssh	Fast SSH server and open proxy scanner.	(http://www.monkey.org/~provos/scanssh/)
scap-security-guide	Security compliance content in SCAP, Bash, Ansible, and other formats.	(https://www.open-scap.org/security-policies/scap-security-guide/)
scap-workbench	SCAP Scanner And Tailoring Graphical User Interface.	(https://www.open-scap.org/tools/scap-workbench/)
scapy	Powerful interactive packet manipulation program written in Python (tools)	(http://www.secdev.org/projects/scapy/)
scavenger	Crawler (Bot) searching for credential leaks on different paste sites.	(https://github.com/rndinfosecguy/Scavenger)
schnappi-dhcp	Can fuck network with no DHCP.	(http://www.emanuelegentili.eu/)
scout2	Security auditing tool for AWS environments.	(http://isecpartners.github.io/Scout2/)
scoutsuite	Multi-Cloud Security Auditing Tool.	(https://github.com/nccgroup/ScoutSuite)
scrape-dns	Searches for interesting cached DNS entries.	(https://github.com/304GEEK/Scrape-DNS)
scrapy	A fast high-level scraping and web crawling framework.	(https://scrapy.org)
scratchabit	Easily retargetable and hackable interactive disassembler with IDAPython-compatible plugin API.	(https://github.com/pfalcon/ScratchABit)
scrounge-ntfs	Data recovery program for NTFS file systems	(http://memberwebs.com/stef/software/scrounge/)
scrying	Collect RDP, web, and VNC screenshots smartly.	(https://github.com/nccgroup/scrying)
sctpscan	A network scanner for discovery and security.	(http://www.p1sec.com/)
scylla	Find Advanced Information on a Username, Website, Phone Number, etc.	(https://github.com/josh0xA/Scylla)
sdn-toolkit	Discover, Identify, and Manipulate SDN-Based Networks	(http://www.hellfiresecurity.com/tools.htm)
sdnpwn	An SDN penetration testing toolkit.	(https://github.com/smythtech/sdnpwn)
sea	A tool to help to create exploits of binary programs.	(https://github.com/neuromancer/SEA)
search1337	1337Day Online Exploit Scanner.	(https://github.com/b3mb4m/Search1337)
seat	Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities.	(http://thesprawl.org/projects/search-engine-assessment-tool/)
seclists	A collection of multiple types of lists used during security assessments.	(https://github.com/danielmiessler/SecLists/)
second-order	Second-order subdomain takeover scanner.	(https://github.com/mhmdiaa/second-order)
secretfinder	A python script to find sensitive data (apikeys, accesstoken, jwt,..) in javascript files.	(https://github.com/m4ll0k/SecretFinder)
secscan	Web Apps Scanner and Much more utilities.	(http://code.google.com/p/secscan-py/)
secure-delete	Secure file, disk, swap, memory erasure utilities.	(http://www.thc.org/)
secure2csv	Decode security descriptors in $Secure on NTFS.	(https://github.com/jschicht/Secure2Csv)
see-surf	A Python based scanner to find potential SSRF parameters in a web application.	(https://github.com/In3tinct/See-SURF)
seeker	Accurately Locate People using Social Engineering.	(https://github.com/thewhiteh4t/seeker)
sees	Increase the success rate of phishing attacks by sending emails to company users as if they are coming from the very same company's domain.	(https://github.com/galkan/sees/)
semgrep	Lightweight static analysis for many languages.	(https://pypi.org/project/semgrep/#files)
sensepost-xrdp	A rudimentary remote desktop tool for the X11 protocol exploiting unauthenticated x11 sessions.	(https://github.com/sensepost/xrdp)
sentrypeer	Protect SIP Servers from bad actors.	(https://github.com/SentryPeer/SentryPeer)

Name	Description	Website
sergio-proxy	A multi-threaded transparent HTTP proxy for manipulating web traffic.	(https://github.com/supernothing/sergio-proxy)
serialbrute	Java serialization brute force attack tool.	(https://github.com/NickstaDB/SerialBrute)
serializationdumper	A tool to dump Java serialization streams in a more human readable form.	(https://github.com/NickstaDB/SerializationDumper/)
server-status-pwn	A script that monitors and extracts requested URLs and clients connected to the service by exploiting publicly accessible Apache server-status instances.	(https://github.com/mazen160/server-status_PWN)
sessionlist	Sniffer that intents to sniff HTTP packets and attempts to reconstruct interesting authentication data from websites that do not employ proper secure cookie auth.	(http://www.0xrage.com/)
set	Social-engineer toolkit. Aimed at penetration testing around Social-Engineering.	(https://github.com/trustedsec/social-engineer-toolkit/tags)
seth	Perform a MitM attack and extract clear text credentials from RDP connections.	(https://github.com/SySS-Research/Seth)
setowner	Allows you to set file ownership to any account, as long as you have the "Restore files and directories" user right.	(http://ntsecurity.nu/toolbox/setowner/)
sfuzz	A simple fuzzer.	(http://aconole.brad-x.com/programs/sfuzz.html)
sgn	Shikata ga nai encoder ported into go with several improvements.	(https://github.com/EgeBalci/sgn)
sh00t	A Testing Environment for Manual Security Testers.	(https://github.com/pavanw3b/sh00t)
sha1collisiondetection	Library and command line tool to detect SHA collision in a file	(https://github.com/cr-marcstevens/sha1collisiondetection)
shad0w	A modular C2 framework designed to successfully operate on mature environments.	(https://github.com/bats3c/shad0w)
shadowexplorer	Browse the Shadow Copies created by the Windows Vista / 7 / 8 / 10 Volume Shadow Copy Service.	(https://www.shadowexplorer.com/downloads.html)
shard	A command line tool to detect shared passwords.	(https://github.com/philwantsfish/shard)
shareenum	Tool to enumerate shares from Windows hosts.	(https://github.com/CroweCybersecurity/shareenum)
sharesniffer	Network share sniffer and auto-mounter for crawling remote file systems.	(https://github.com/shirosaidev/sharesniffer)
shed	.NET runtime inspector.	(https://github.com/enkomio/shed)
shellcheck	Shell script analysis tool	(https://www.shellcheck.net)
shellcode-compiler	Compiles C/C++ style code into a small, position-independent and NULL-free shellcode for Windows & Linux.	(https://github.com/NytroRST/ShellcodeCompiler)
shellcode-factory	Tool to create and test shellcodes from custom assembly sources.	(https://github.com/danielhenrymantilla/shellcode-factory)
shellcodecs	A collection of shellcode, loaders, sources, and generators provided with documentation designed to ease the exploitation and shellcode programming process.	(http://www.blackhatlibrary.net/Shellcodecs)
shellen	Interactive shellcoding environment to easily craft shellcodes.	(https://github.com/merrychap/shellen)
shellerator	Simple command-line tool aimed to help pentesters quickly generate one-liner reverse/bind shells in multiple languages.	(https://github.com/ShutdownRepo/shellerator)
shellinabox	Implements a web server that can export arbitrary command line tools to a web based terminal emulator.	(https://github.com/shellinabox/shellinabox)
shelling	An offensive approach to the anatomy of improperly written OS command injection sanitisers.	(https://github.com/ewilded/shelling)
shellme	Because sometimes you just need shellcode and opcodes quickly. This essentially just wraps some nasm/objdump calls into a neat script.	(https://github.com/hatRiot/shellme)
shellnoob	A toolkit that eases the writing and debugging of shellcode.	(https://github.com/reyammer/shellnoob)
shellpop	Generate easy and sophisticated reverse or bind shell commands.	(https://github.com/0x00x00/ShellPop)
shellsploit-framework	New Generation Exploit Development Kit.	(https://github.com/b3mb4m/shellsploit-framework)
shellter	A dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.	(https://www.shellterproject.com/download/)
shellz	A script for generating common revshells fast and easy.	(https://github.com/4ndr34z/shells)
sherlock	Find usernames across social networks.	(https://github.com/sherlock-project/sherlock)
sherlocked	Universal script packer-- transforms any type of script into a protected ELF executable, encrypted with anti-debugging.	(https://github.com/elfmaster/sherlocked)
shhgit	Find committed secrets and sensitive files across GitHub, Gists, GitLab and BitBucket or your local repositories in real time.	(https://github.com/eth0izzle/shhgit)
shitflood	A Socks5 clone flooder for the Internet Relay Chat (IRC) protocol.	(https://github.com/acidvegas/shitflood)
shocker	A tool to find and exploit servers vulnerable to Shellshock.	(https://github.com/nccgroup/shocker)
shodanhat	Search for hosts info with shodan.	(https://github.com/HatBashBR/ShodanHat)
shootback	A reverse TCP tunnel let you access target behind NAT or firewall.	(https://github.com/aploium/shootback)
shortfuzzy	A web fuzzing script written in perl.	(http://packetstormsecurity.com/files/104872/Short-Fuzzy-Rat-Scanner.html)
shosubgo	Small tool to Grab subdomains using Shodan API.	(https://github.com/incogbyte/shosubgo)
shreder	A powerful multi-threaded SSH protocol password bruteforce tool.	(https://github.com/EntySec/Shreder)
shuffledns	A wrapper around massdns written in GO.	(https://github.com/projectdiscovery/shuffledns.git)
sickle	A shellcode development tool, created to speed up the various steps needed to create functioning shellcode.	(https://github.com/wetw0rk/Sickle)
sidguesser	Guesses sids/instances against an Oracle database according to a predefined dictionary file.	(http://www.cqure.net/wp/tools/database/sidguesser/)
siege	An http regression testing and benchmarking utility	(https://www.joedog.org/siege-home/)
sigma	Generic Signature Format for SIEM Systems	(https://github.com/SigmaHQ/sigma/releases)
sign	Automatically signs an apk with the Android test certificate.	(https://github.com/appium/sign)
sigploit	Telecom Signaling Exploitation Framework - SS7, GTP, Diameter & SIP.	(https://github.com/SigPloiter/SigPloit)
sigspotter	A tool that search in your HD to find which publishers has been signed binaries in your PC.	(http://www.security-projects.com/?SigSpotter)
sigthief	Stealing Signatures and Making One Invalid Signature at a Time.	(https://github.com/secretsquirrel/SigThief)
silenteye	A cross-platform application design for an easy use of steganography.	(https://github.com/achorein/silenteye/)
silenttrinity	An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR.	(https://github.com/byt3bl33d3r/SILENTTRINITY)
silk	A collection of traffic analysis tools developed by the CERT NetSA to facilitate security analysis of large networks.	(https://tools.netsa.cert.org/silk/download.html)
simple-ducky	A payload generator.	(https://code.google.com/p/simple-ducky-payload-generator)

Name	Description	Website
simple-lan-scan	A simple python script that leverages scapy for discovering live hosts on a network.	(http://packetstormsecurity.com/files/97353/Simple-LAN-Scanner.0.html)
simpleemailspoofer	A simple Python CLI to spoof emails.	(https://github.com/lunarca/SimpleEmailSpoofer)
simplify	Generic Android Deobfuscator.	(https://github.com/CalebFenton/simplify)
simplyemail	Email recon made fast and easy, with a framework to build on CyberSyndicates	(https://github.com/killswitch-GUI/SimplyEmail)
simtrace2	Host utilities to communicate with SIMtrace2 USB Devices.	(https://osmocom.org/projects/simtrace2/wiki)
sinfp	A full operating system stack fingerprinting suite.	(https://cpan.metacpan.org/authors/id/G/GO/GOMOR/)
siparmyknife	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.	(http://packetstormsecurity.com/files/107301/sipArmyKnife_11232011.pl.txt)
sipbrute	A utility to perform dictionary attacks against the VoIP SIP Register hash.	(https://github.com/packetassailant/sipbrute)
sipcrack	A SIP protocol login cracker.	(http://www.remote-exploit.org/codes_sipcrack.html)
sipffer	SIP protocol command line sniffer.	(https://github.com/xenomuta/SIPffer)
sipi	Simple IP Information Tools for Reputation Data Analysis.	(https://github.com/ST2Labs/SIPI)
sipp	A free Open Source test tool / traffic generator for the SIP protocol.	(http://sipp.sourceforge.net/)
sippts	Set of tools to audit SIP based VoIP Systems.	(https://github.com/Pepelux/sippts)
sipsak	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.	(https://github.com/nils-ohlmeier/sipsak/releases)
sipscan	A sip scanner.	(http://www.hackingvoip.com/sec_tools.html)
sipshock	A scanner for SIP proxies vulnerable to Shellshock.	(https://github.com/zaf/sipshock)
sipvicious	Tools for auditing SIP devices.	(http://blog.sipvicious.org/)
sireprat	Remote Command Execution as SYSTEM on Windows IoT Core.	(https://github.com/SafeBreach-Labs/SirepRAT)
sitadel	Web Application Security Scanner.	(https://github.com/shenril/Sitadel)
sitediff	Fingerprint a web app using local files as the fingerprint sources.	(https://github.com/digininja/sitediff)
sjet	Siberas JMX exploitation toolkit.	(https://github.com/h0ng10/sjet)
skipfish	A fully automated, active web application security reconnaissance tool.	(http://code.google.com/p/skipfish/)
skiptracer	OSINT python2 webscraping framework. Skipping the needs of API keys.	(https://github.com/84KaliPleXon3/skiptracer)
skul	A PoC to bruteforce the Cryptsetup implementation of Linux Unified Key Setup (LUKS).	(https://github.com/cryptcoffee/skul)
skydive	An open source real-time network topology and protocols analyzer.	(https://github.com/skydive-project/skydive)
skyjack	Takes over Parrot drones, deauthenticating their true owner and taking over control, turning them into zombie drones under your own control.	(https://github.com/samyk/skyjack)
skype-dump	This is a tool that demonstrates dumping MD5 password hashes from the configuration file in Skype.	(http://packetstormsecurity.com/files/119155/Skype-Hash-Dumper.0.html)
skypefreak	A Cross Platform Forensic Framework for Skype.	(http://osandamalith.github.io/SkypeFreak/)
slackpirate	Slack Enumeration and Extraction Tool - extract sensitive information from a Slack Workspace.	(https://github.com/emtunc/SlackPirate)
sleuthkit	File system and media management forensic analysis tools	(https://www.sleuthkit.org/sleuthkit)
sleuthql	Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap.	(https://github.com/RhinoSecurityLabs/SleuthQL)
slither	Solidity static analysis framework written in Python 3.	(https://github.com/crytic/slither)
sloth-fuzzer	A smart file fuzzer.	(https://github.com/mfontanini/sloth-fuzzer)
slowhttptest	Highly configurable tool that simulates some Application Layer Denial of Service (DoS) attacks	(https://github.com/shekyan/slowhttptest)
slowloris	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.	(http://ha.ckers.org/slowloris/)
slowloris-py	Low bandwidth DoS tool.	(https://github.com/gkbrk/slowloris)
slurp-scanner	Evaluate the security of S3 buckets.	(https://github.com/0xbharath/slurp)
smali	Assembler/disassembler for Android's dex format	(https://github.com/JesusFreke/smali)
smali-cfgs	Smali Control Flow Graph's.	(https://github.com/ch0psticks/Smali-CFGs)
smalisca	Static Code Analysis for Smali files.	(https://github.com/dorneanu/smalisca)
smap	Shellcode mapper - Handy tool for shellcode analysis.	(https://github.com/suraj-root/smap)
smap-scanner	Passive port scanner built with shodan free API.	(https://github.com/s0md3v/Smap)
smartphone-pentest-framework	Repository for the Smartphone Pentest Framework (SPF).	(https://github.com/georgiaw/Smartphone-Pentest-Framework)
smbbf	SMB password bruteforcer.	(http://packetstormsecurity.com/files/25381/smbbf.9.1.tar.gz.html)
smbcrunch	3 tools that work together to simplify reconnaissance of Windows File Shares.	(https://github.com/Raikia/SMBCrunch)
smbexec	A rapid psexec style attack with samba tools.	(https://github.com/pentestgeek/smbexec)
smbmap	A handy SMB enumeration tool.	(https://github.com/ShawnDEvans/smbmap)
smbrelay	SMB / HTTP to SMB replay attack toolkit.	(http://www.tarasco.org/security/smbrelay/)
smbspider	A lightweight python utility for searching SMB/CIFS/Samba file shares.	(https://github.com/T-S-A/smbspider)
smbsr	Lookup for interesting stuff in SMB shares.	(https://github.com/oldboy21/SMBSR)
smikims-arpspoof	Performs an ARP spoofing attack using the Linux kernel's raw sockets.	(https://github.com/smikims/arpspoof)
smod	A modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol.	(https://github.com/enddo/smod)
smplshllctrlr	PHP Command Injection exploitation tool.	(https://github.com/z0noxz/smplshllctrlr)
smtp-fuzz	Simple smtp fuzzer.	(none)
smtp-test	Automated testing of SMTP servers for penetration testing.	(https://github.com/isaudits/smtp-test)
smtp-user-enum	Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.	(http://pentestmonkey.net/tools/user-enumeration/smtp-user-enum)
smtp-vrfy	An SMTP Protocol Hacker.	()
smtpmap	Tool to identify the running smtp software on a given host.	(http://www.projectiwear.org/~plasmahh/software.html)
smtpscan	An SMTP scanner	(http://packetstormsecurity.com/files/31102/smtpscan.5.tar.gz.html)
smtptester	Small python3 tool to check common vulnerabilities in SMTP servers.	(https://github.com/xFreed0m/SMTPTester)
smtptx	A very simple tool used for sending simple email and do some basic email testing from a pentester perspective.	(http://www.0x90.se/)

Name	Description	Website
smuggler	An HTTP Request Smuggling / Desync testing tool written in Python 3.	(https://github.com/defparam/smuggler)
smuggler-py	Python tool used to test for HTTP Desync/Request Smuggling attacks.	(https://github.com/gwen001/pentest-tools/blob/master/smuggler.py)
sn00p	A modular tool written in bourne shell and designed to chain and automate security tools and tests.	(http://www.nullsecurity.net/tools/automation.html)
sn1per	Automated Pentest Recon Scanner.	(https://github.com/1N3/Sn1per)
snallygaster	Tool to scan for secret files on HTTP servers.	(https://github.com/hannob/snallygaster)
snapception	Intercept and decrypt all snapchats received over your network.	(https://github.com/thebradbain/snapception)
snare	Super Next generation Advanced Reactive honeypot.	(https://github.com/mushorg/snare)
snarf-mitm	SMB Man in the Middle Attack Engine / relay suite.	(https://github.com/purpleteam/snarf)
sniff-probe-req	Wi-Fi Probe Requests Sniffer.	(https://github.com/SkypLabs/sniff-probe-req)
sniffer	Packet Trace Parser for TCP, SMTP Emails, and HTTP Cookies.	(https://github.com/julioreynaga/sniffer)
sniffglue	Secure multithreaded packet sniffer	(https://github.com/kpcyrd/sniffglue)
sniffjoke	Injects packets in the transmission flow that are able to seriously disturb passive analysis like sniffing, interception and low level information theft.	(http://www.delirandom.net/sniffjoke/)
sniffles	A Packet Capture Generator for IDS and Regular Expression Evaluation.	(https://github.com/petabi/sniffles)
snitch	Turn back the asterisks in password fields to plaintext passwords.	(http://ntsecurity.nu/toolbox/snitch/)
snmp-brute	SNMP brute force, enumeration, CISCO config downloader and password cracking script.	(https://github.com/SECFORCE/SNMP-Brute)
snmp-fuzzer	SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl.	(http://www.arhont.com/en/category/resources/tools-utilities/)
snmpattack	SNMP scanner and attacking tool.	(http://www.c0decafe.de/)
snmpcheck	A free open source utility to get information via SNMP protocols.	(http://www.nothink.org/perl/snmpcheck/)
snmpenum	An snmp enumerator.	(http://www.filip.waeytens.easynet.be/)
snmpscan	A free, multi-processes SNMP scanner.	(http://www.nothink.org/perl/snmpscan/index.php)
snoopbrute	Multithreaded DNS recursive host brute-force tool.	(https://github.com/m57/snoopbrute)
snoopy-ng	A distributed, sensor, data collection, interception, analysis, and visualization framework.	(https://github.com/sensepost/snoopy-ng)
snort	A lightweight network intrusion detection system.	(http://www.snort.org/)
snow	Steganography program for concealing messages in text files.	(http://darkside.com.au/snow/index.html)
snowman	A native code to C/C++ decompiler, see the examples of generated code.	(http://derevenets.com/)
snscan	A Windows based SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network.	(http://www.mcafee.com/uk/downloads/free-tools/snscan.aspx)
snscrape	A social networking service scraper in Python.	(https://github.com/JustAnotherArchivist/snscrape)
snuck	Automatic XSS filter bypass.	(https://github.com/mauro-g/snuck)
snyk	CLI and build-time tool to find and fix known vulnerabilities in open-source dependencies.	(https://github.com/snyk/cli)
soapui	The Swiss-Army Knife for SOAP Testing.	(https://www.soapui.org/downloads/soapui/source-forge.html)
socat	Multipurpose relay	(http://www.dest-unreach.org/socat/)
social-analyzer	Analyzing & finding a person's profile across social media websites.	(https://pypi.org/project/social-analyzer/)
social-mapper	A social media enumeration and correlation tool.	(https://github.com/SpiderLabs/social_mapper)
social-vuln-scanner	Gathers public information on companies to highlight social engineering risk.	(https://github.com/Betawolf/social-vuln-scanner)
socialfish	Ultimate phishing tool with Ngrok integrated.	(https://github.com/UndeadSec/SocialFish)
socialpwned	OSINT tool that allows to get the emails, from a target, published in social networks.	(https://github.com/MrTuxx/SocialPwned)
socialscan	Check email address and username availability on online platforms.	(https://github.com/iojw/socialscan)
socketfuzz	Simple socket fuzzer.	(https://github.com/landw1re/socketfuzz)
sockstat	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.	(https://packages.debian.org/unstable/main/sockstat)
sonar-scanner	Generic CLI tool to launch project analysis on SonarQube servers.	(https://docs.sonarqube.org/latest/analysis/scan/sonarscanner/)
soot	A Java Bytecode Analysis and Transformation Framework.	(http://www.sable.mcgill.ca/soot)
sooty	The SOC Analysts all-in-one CLI tool to automate and speed up workflow.	(https://github.com/TheresAFewConors/Sooty)
sourcemapper	Extract JavaScript source trees from Sourcemap files.	(https://github.com/denandz/sourcemapper)
spade	A general-purpose Internet utility package, with some extra features to help in tracing the source of spam and other forms of Internet harassment.	(http://www.hoobie.net/brutus/)
spaf	Static Php Analysis and Fuzzer.	(https://github.com/Ganapati/spaf)
sparta	Python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase.	(http://sparta.secforce.com/)
spartan	Frontpage and Sharepoint fingerprinting and attack tool.	(https://github.com/sensepost/SPartan)
sparty	An open source tool written in python to audit web applications using sharepoint and frontpage architecture.	(http://sparty.secniche.org/)
spectools	Spectrum-Tools is a set of utilities for using the Wi-Spy USB spectrum analyzer hardware. Stable version.	(http://www.kismetwireless.net/spectools/)
speedpwn	An active WPA/2 Bruteforcer, original created to prove weak standard key generation in different ISP labeled routers without a client is connected.	(https://gitorious.org/speedpwn/)
spf	A python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.	(https://github.com/tatanus/SPF)
spfmap	A program to map out SPF and DKIM records for a large number of domains.	(https://github.com/BishopFox/spfmap)
spiderfoot	The Open Source Footprinting Tool.	(https://github.com/smicallef/spiderfoot)
spiderpig-pdffuzzer	A javascript pdf fuzzer.	(https://code.google.com/p/spiderpig-pdffuzzer/)
spiga	Configurable web resource scanner.	(https://github.com/getdual/scripts-n-tools/blob/master/spiga.py)
spike-fuzzer	IMMUNITYsec's fuzzer creation kit in C.	(http://www.immunitysec.com/resources-freesoftware.shtml)
spike-proxy	A Proxy for detecting vulnerabilities in web applications	(http://www.immunitysec.com/resources-freesoftware.shtml)

Name	Description	Website
spiped	Secure pipe daemon	(http://www.tarsnap.com/spiped.html)
spipscan	SPIP (CMS) scanner for penetration testing purpose written in Python.	(https://github.com/PaulSec/SPIPScan)
splint	A tool for statically checking C programs for security vulnerabilities and coding mistakes	(https://repo.or.cz/splint-patched.git)
sploitctl	Fetch, install and search exploit archives from exploit sites like exploit-db and packetstorm.	(https://github.com/BlackArch/sploitctl)
sploitego	Maltego Penetration Testing Transforms.	(https://github.com/allfro/sploitego)
spoofcheck	Simple script that checks a domain for email protections.	(https://github.com/bishopfox/spoofcheck)
spooftooph	Designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain sight.	(http://www.hackfromacave.com/projects/spooftooph.html)
spookflare	Loader, dropper generator with multiple features for bypassing client-side and network-side countermeasures.	(https://github.com/hlldz/SpookFlare)
spotbugs	A tool for static analysis to look for bugs in Java code.	(https://github.com/spotbugs/spotbugs)
spray365	Makes spraying Microsoft accounts (Office 365 / Azure AD) easy through its customizable two-step password spraying approach.	(https://github.com/MarkoH17/Spray365)
spraycharles	Low and slow password spraying tool, designed to spray on an interval over a long period of time.	(https://github.com/Tw1sm/spraycharles)
sprayhound	Password spraying tool and Bloodhound integration.	(https://github.com/Hackndo/sprayhound)
sprayingtoolkit	Scripts to make password spraying attacks against Lync/S4B & OWA a lot quicker, less painful and more efficient.	(https://github.com/byt3bl33d3r/SprayingToolkit)
spraykatz	Credentials gathering tool automating remote procdump and parse of lsass process.	(https://github.com/aas-n/spraykatz)
sps	A Linux packet crafting tool. Supports IPv4, IPv6 including extension headers, and tunneling IPv6 over IPv4.	(https://sites.google.com/site/simplepacketsender/)
spyse	Python API wrapper and command-line client for the tools hosted on spyse.com.	(https://github.com/zeropwn/spyse.py)
sqid	A SQL injection digger.	(http://sqid.rubyforge.org/)
sqlbrute	Brute forces data out of databases using blind SQL injection.	(http://www.justinclarke.com/archives/2006/03/sqlbrute.html)
sqldict	A dictionary attack tool for SQL Server.	(http://ntsecurity.nu/toolbox/sqldict/)
sqlivulscan	This will give you the SQLi Vulnerable Website Just by Adding the Dork.	(https://github.com/Hadesy2k/sqlivulscan)
sqlmap	Automatic SQL injection and database takeover tool	(https://sqlmap.org)
sqlninja	A tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.	(http://sqlninja.sourceforge.net/)
sqlpat	This tool should be used to audit the strength of Microsoft SQL Server passwords offline.	(http://www.cqure.net/wp/sqlpat/)
sqlping	SQL Server scanning tool that also checks for weak passwords using wordlists.	(http://www.sqlsecurity.com/downloads)
sqlpowerinjector	Application created in .Net 1.1 that helps the penetration tester to find and exploit SQL injections on a web page.	(http://www.sqlpowerinjector.com/download.htm)
sqlsus	An open source MySQL injection and takeover tool.	(http://sqlsus.sourceforge.net/)
ssdeep	A program for computing context triggered piecewise hashes	(https://ssdeep-project.github.io/ssdeep/)
ssdp-scanner	SSDP amplification scanner written in Python. Makes use of Scapy.	(http://packetstormsecurity.com/files/127994/SSDP-Amplification-Scanner.html)
ssh-audit	SSH configuration auditing	(https://github.com/jtesta/ssh-audit)
ssh-honeypot	Fake sshd that logs ip addresses, usernames, and passwords.	(https://github.com/droberson/ssh-honeypot)
ssh-mitm	SSH man-in-the-middle tool.	(https://github.com/jtesta/ssh-mitm)
ssh-privkey-crack	A SSH private key cracker.	(https://code.google.com/p/lusas/)
ssh-user-enum	SSH User Enumeration Script in Python Using The Timing Attack.	(https://github.com/nccgroup/ssh-user-enum)
sshatter	Password bruteforcer for SSH.	(http://www.nth-dimension.org.uk/downloads.php?id=34)
sshfuzz	A SSH Fuzzing utility written in Perl that uses Net::SSH2.	(https://packetstormsecurity.com/fuzzer/sshfuzz.txt)
sshprank	A fast SSH mass-scanner, login cracker and banner grabber tool using the python-masscan and shodan module.	(https://nullsecurity.net/tools/cracker.html)
sshscan	A horizontal SSH scanner that scans large swaths of IPv4 space for a single SSH user and pass.	(https://github.com/getdual/scripts-n-tools/blob/master/sshscan.py)
sshtrix	A very fast multithreaded SSH login cracker.	(http://nullsecurity.net/tools/cracker.html)
sshtunnel	Pure python SSH tunnels (CLI)	(https://github.com/pahaz/sshtunnel)
sshuttle	Transparent proxy server that forwards all TCP packets over ssh	(https://github.com/sshuttle/sshuttle)
ssl-hostname-resolver	CN (Common Name) grabber on X.509 Certificates over HTTPS.	(http://packetstormsecurity.com/files/120634/Common-Name-Grabber-Script.html)
ssl-phuck3r	All in one script for Man-In-The-Middle attacks.	(https://github.com/zombiesam/ssl_phuck3r)
sslcat	SSLCat is a simple Unix utility that reads and writes data across an SSL enable network connection.	(http://www.bindshell.net/tools/sslcat)
sslcaudit	Utility to perform security audits of SSL/TLS clients.	(https://github.com/grwl/sslcaudit)
ssldump	An SSLv3/TLS network protocol analyzer.	(http://www.rtfm.com/ssldump/)
sslh	SSL/SSH/OpenVPN/XMPP/tinc port multiplexer	(https://www.rutschle.net/tech/sslh/README.html)
ssllabs-scan	Command-line client for the SSL Labs APIs	(https://github.com/ssllabs/ssllabs-scan)
sslmap	A lightweight TLS/SSL cipher suite scanner.	(http://thesprawl.org/projects/latest/)
sslnuke	Transparent proxy that decrypts SSL traffic and prints out IRC messages.	(https://github.com/jtripper/sslnuke)
sslscan	Fast tool to scan SSL services such as HTTPS to determine supported ciphers	(https://github.com/rbsec/sslscan)
sslscan2	Tests SSL/TLS enabled services to discover supported cipher suites.	(https://github.com/rbsec/sslscan)
sslsniff	A tool to MITM all SSL connections on a LAN and dynamically generate certs for the domains that are being accessed on the fly	(http://www.thoughtcrime.org/software/sslsniff/)
sslstrip	Python tool to hijack HTTPS connections during a MITM attack.	(https://github.com/moxie0/sslstrip)
sslyze	Python tool for analyzing the configuration of SSL servers and for identifying misconfigurations.	(https://github.com/nabla-c0d3/sslyze)
ssma	Simple Static Malware Analyzer.	(https://github.com/secrary/SSMA)
ssrf-proxy	Facilitates tunneling HTTP communications through servers vulnerable to Server-Side Request Forgery.	(https://github.com/bcoles/ssrf_proxy)
ssrf-sheriff	A simple SSRF-testing sheriff written in Go.	(https://github.com/teknogeek/ssrf-sheriff)
ssrfmap	Automatic SSRF fuzzer and exploitation tool.	(https://github.com/swisskyrepo/SSRFmap)
stackflow	Universal stack-based buffer overfow exploitation tool.	(https://github.com/d4rkcat/stackflow)

Name	Description	Website
stacoan	Crossplatform tool which aids developers, bugbounty hunters and ethical hackers performing static code analysis on mobile applications.	(https://github.com/vincentcox/StaCoAn)
stacs	Static Token And Credential Scanner.	(https://github.com/stacscan/stacs)
staekka	This plugin extends Metasploit for some missing features and modules allowing interaction with other/custom exploits/ways of getting shell access.	(https://github.com/j-t/staekka)
stardox	Github stargazers information gathering tool.	(https://github.com/0xPrateek/Stardox)
starttls-mitm	A mitm proxy that will transparently proxy and dump both plaintext and TLS traffic.	(https://github.com/ipopov/starttls-mitm)
statsprocessor	A high-performance word-generator based on per-position Markov-attack.	(http://hashcat.net/wiki/doku.php?id=statsprocessor)
stegcracker	Steganography brute-force utility to uncover hidden data inside files.	(https://github.com/Paradoxis/StegCracker/tags)
stegdetect	An automated tool for detecting steganographic content in images.	(https://github.com/redNixon/stegdetect)
steghide	Embeds a message in a file by replacing some of the least significant bits.	(http://steghide.sourceforge.net/)
stegolego	Simple program for using stegonography to hide data within BMP images.	(https://github.com/razc411/StegoLeggo)
stegosip	TCP tunnel over RTP/SIP.	(https://github.com/epinna/Stegosip)
stegoveritas	Automatic image steganography analysis tool.	(https://github.com/bannsec/stegoVeritas/)
stegseek	Lightning fast steghide cracker.	(https://github.com/RickdeJager/stegseek)
stegsolve	Steganography Solver.	(https://github.com/zardus/ctf-tools/blob/master/stegsolve/install)
stenographer	A packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets.	(https://github.com/google/stenographer)
stepic	A python image steganography tool.	(http://domnit.org/stepic/doc/)
stews	A Security Tool for Enumerating WebSockets.	(https://github.com/PalindromeLabs/STEWS)
sticky-keys-hunter	Script to test an RDP host for sticky keys and utilman backdoor.	(https://github.com/ztgrace/sticky_keys_hunter)
stig-viewer	XCCDF formatted SRGs and STIGs files viewer for SCAP validation tools.	(https://www.stig-viewer.com)
stompy	An advanced utility to test the quality of WWW session identifiers and other tokens that are meant to be unpredictable.	(http://lcamtuf.coredump.cx/)
stoq	An open source framework for enterprise level automated analysis.	(https://github.com/PUNCH-Cyber/stoq)
storm-ring	This simple tool is useful to test a PABX with "allow guest" parameter set to "yes" (in this scenario an anonymous caller could place a call).	(http://packetstormsecurity.com/files/115852/Storm-Ringing-PABX-Test-Tool.html)
stowaway	A Multi-hop proxy tool for security researchers and pentesters.	(https://github.com/ph4ntonn/Stowaway)
strace	A diagnostic, debugging and instructional userspace tracer	(https://strace.io/)
streamfinder	Searches for Alternate Data Streams (ADS).	(https://www.gaijin.at/en/dlstreamfind.php)
striker	An offensive information and vulnerability scanner.	(https://github.com/UltimateHackers/Striker)
stringsifter	Machine learning tool that automatically ranks strings based on their relevance for malware analysis.	(https://github.com/fireeye/stringsifter)
striptls	Proxy PoC implementation of STARTTLS stripping attacks.	(https://github.com/tintinweb/striptls)
strutscan	Apache Struts2 vulnerability scanner written in Perl.	(https://github.com/riusksk/StrutScan)
stunnel	A program that allows you to encrypt arbitrary TCP connections inside SSL	(https://www.stunnel.org/)
sub7	A remote administration tool. No further comments ;-)	(https://dl.packetstormsecurity.net/trojans/Subseven.2.2.zip)
subbrute	A DNS meta-query spider that enumerates DNS records and subdomains	(https://github.com/TheRook/subbrute)
subdomainer	A tool designed for obtaining subdomain names from public sources.	(http://www.edge-security.com/subdomainer.php)
subfinder	Modular subdomain discovery tool that can discover massive amounts of valid subdomains for any target.	(https://github.com/projectdiscovery/subfinder)
subjack	Subdomain Takeover tool written in Go.	(https://github.com/haccer/subjack)
subjs	Fetches javascript file from a list of URLS or subdomains.	(https://github.com/lc/subjs)
sublert	A security and reconnaissance tool which leverages certificate transparency to automatically monitor new subdomains deployed by specific organizations and issued TLS/SSL certificate.	(https://github.com/yassineaboukir/sublert)
sublist3r	A Fast subdomains enumeration tool for penetration testers.	(https://github.com/aboul3la/Sublist3r)
subover	A Powerful Subdomain Takeover Tool.	(https://github.com/Ice3man543/SubOver)
subscraper	Tool that performs subdomain enumeration through various techniques.	(https://github.com/m8r0wn/subscraper)
subterfuge	Automated Man-in-the-Middle Attack Framework.	(https://github.com/Subterfuge-Framework/Subterfuge)
sucrack	A multi-threaded Linux/UNIX tool for brute-force cracking local user accounts via su.	(http://labs.portcullis.co.uk/application/sucrack)
suid3num	Python script which utilizes python's built-in modules to enumerate SUID binaries.	(https://github.com/Anon-Exploiter/SUID3NUM)
sulley	A pure-python fully automated and unattended fuzzing framework.	(https://github.com/OpenRCE/sulley/)
superscan	Powerful TCP port scanner, pinger, resolver.	(http://www.foundstone.com/us/resources/proddesc/superscan.htm)
suricata	An Open Source Next Generation Intrusion Detection and Prevention Engine.	(https://suricata.io/download/)
suricata-verify	Suricata Verification Tests - Testing Suricata Output.	(https://github.com/OISF/suricata-verify)
svn-extractor	A simple script to extract all web resources by means of .SVN folder exposed over network.	(https://github.com/anantshri/svn-extractor)
swaks	Swiss Army Knife SMTP; Command line SMTP testing, including TLS and AUTH	(https://jetmore.org/john/code/swaks/)
swamp	An OSINT tool for discovering associated sites through Google Analytics Tracking IDs.	(https://github.com/jakecreps/swamp)
swap-digger	A tool used to automate Linux swap analysis during post-exploitation or forensics.	(https://github.com/sevagas/swap_digger)
swarm	A distributed penetration testing tool.	(https://github.com/Arvin-X/swarm)
swfintruder	First tool for testing security in Flash movies. A runtime analyzer for SWF external movies. It helps to find flaws in Flash.	(http://code.google.com/p/swfintruder/)
swftools	A collection of SWF manipulation and creation utilities.	(http://www.swftools.org/)
syborg	Recursive DNS Subdomain Enumerator with dead-end avoidance system.	(https://github.com/MilindPurswani/Syborg)
sylkie	IPv6 address spoofing with the Neighbor Discovery Protocol.	(https://github.com/dlrobertson/sylkie)
syms2elf	A plugin for Hex-Ray's IDA Pro and radare2 to export the symbols recognized to the ELF symbol table.	(https://github.com/danigargu/syms2elf)
synflood	A very simply script to illustrate DoS SYN Flooding attack.	(http://thesprawl.org/projects/syn-flooder/)
synner	A custom eth->ip->tcp packet generator (spoofer) for testing firewalls and dos attacks.	(http://packetstormsecurity.com/files/69802/synner.c.html)
synscan	fast asynchronous half-open TCP portscanner	(http://www.digit-labs.org/files/tools/synscan/)

Name	Description	Website
syringe	A General Purpose DLL & Code Injection Utility.	(https://github.com/securestate/syringe)
sysdig	Open source system-level exploration and troubleshooting tool	(https://www.sysdig.com/)
sysinternals-suite	Sysinternals tools suite.	(http://sysinternals.com/)
t50	Experimental Multi-protocol Packet Injector Tool.	(https://gitlab.com/fredericopissarra/t50/tags)
tabi	BGP Hijack Detection.	(https://github.com/ANSSI-FR/tabi)
tachyon-scanner	Fast Multi-Threaded Web Discovery Tool.	(https://github.com/delvelabs/tachyon)
tactical-exploitation	Modern tactical exploitation toolkit.	(https://github.com/0xdea/tactical-exploitation)
taipan	Web application security scanner.	(https://github.com/enkomio/Taipan)
takeover	Sub-Domain TakeOver Vulnerability Scanner.	(https://github.com/m4ll0k/takeover)
talon	A password guessing tool that targets the Kerberos and LDAP services within the Windows Active Directory environment.	(https://github.com/optiv/Talon)
taof	A GUI cross-platform Python generic network protocol fuzzer.	(http://taof.sf.net/)
tbear	Transient Bluetooth Environment Auditor includes an ncurses-based Bluetooth scanner (a bit similar to kismet), a Bluetooth DoS tool, and a Bluetooth hidden device locator.	(http://freshmeat.net/projects/t-bear)
tcgetkey	A set of tools that deal with acquiring physical memory dumps via FireWire and then scan the memory dump to locate TrueCrypt keys and finally decrypt the encrypted TrueCrypt container using the keys.	(http://packetstormsecurity.com/files/119146/tcgetkey.1.html)
tchunt-ng	Reveal encrypted files stored on a filesystem.	(https://github.com/antagon/TCHunt-ng)
tcpcontrol-fuzzer	2^6 TCP control bit fuzzer (no ECN or CWR).	(https://www.ee.oulu.fi/research/ouspg/tcpcontrol-fuzzer)
tcpcopy	A TCP stream replay tool to support real testing of Internet server applications.	(https://github.com/session-replay-tools/tcpcopy)
tcpdstat	Get protocol statistics from tcpdump pcap files.	(https://github.com/netik/tcpdstat)
tcpdump	Powerful command-line packet analyzer	(https://www.tcpdump.org/)
tcpextract	Extracts files from captured TCP sessions. Support live streams and pcap files.	(https://pypi.python.org/pypi/tcpextract/)
tcpflow	Captures data transmitted as part of TCP connections then stores the data conveniently	(https://github.com/simsong/tcpflow)
tcpick	TCP stream sniffer and connection tracker	(http://tcpick.sourceforge.net/)
tcpjunk	A general tcp protocols testing and hacking utility.	(http://code.google.com/p/tcpjunk)
tcpreplay	Gives the ability to replay previously captured traffic in a libpcap format	(https://tcpreplay.appneta.com)
tcptrace	A TCP dump file analysis tool.	(http://tcptrace.org/)
tcptraceroute	A traceroute implementation using TCP packets.	(http://michael.toren.net/code/tcptraceroute/)
tcpwatch	A utility written in Python that lets you monitor forwarded TCP connections or HTTP proxy connections.	(http://hathawaymix.org/Software/TCPWatch)
tcpxtract	A tool for extracting files from network traffic.	(http://tcpxtract.sourceforge.net)
teamsuserenum	User enumeration with Microsoft Teams API	(https://github.com/immunIT/TeamsUserEnum)
teardown	Command line tool to send a BYE request to tear down a call.	(http://www.hackingexposedvoip.com/)
tekdefense-automater	IP URL and MD5 OSINT Analysis	(https://github.com/1aN0rmus/TekDefense-Automater)
tell-me-your-secrets	Find secrets on any machine from over 120 Different Signatures.	(https://github.com/valayDave/tell-me-your-secrets)
tempomail	Tool to create a temporary email address in 1 Second and receive emails.	(https://github.com/kavishgr/tempomail)
termineter	Smart meter testing framework.	(https://code.google.com/p/termineter/)
testdisk	Checks and undeletes partitions + PhotoRec, signature based recovery tool	(https://www.cgsecurity.org/index.html?testdisk.html)
testssl.sh	Testing TLS/SSL encryption	(https://github.com/drwetter/testssl.sh)
tfsec	Security scanner for your Terraform code.	(https://github.com/aquasecurity/tfsec)
tftp-bruteforce	A fast TFTP filename bruteforcer written in perl.	(http://www.hackingexposedcisco.com/)
tftp-fuzz	Master TFTP fuzzing script as part of the ftools series of fuzzers.	(http://nullsecurity.net/tools/fuzzer.html)
tftp-proxy	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.	(http://www.c0decafe.de/)
tgcd	TCP/IP Gender Changer Daemon utility.	(http://tgcd.sourceforge.net/)
thc-ipv6	Complete tool set to attack the inherent protocol weaknesses of IPv6 and ICMP6	(https://github.com/vanhauser-thc/thc-ipv6)
thc-keyfinder	Finds crypto keys, encrypted data and compressed data in files by analyzing the entropy of parts of the file.	(https://www.thc.org/releases.php)
thc-pptp-bruter	A brute force program that works against pptp vpn endpoints (tcp port 1723).	(http://www.thc.org)
thc-smartbrute	This tool finds undocumented and secret commands implemented in a smartcard.	(https://www.thc.org/thc-smartbrute/)
thc-ssl-dos	A tool to verify the performance of SSL. To be used in your authorized and legitimate area ONLY. You need to accept this to make use of it, no use for bad intentions, you have been warned!	(http://www.thc.org/thc-ssl-dos/)
thcrut	Network discovery and OS Fingerprinting tool.	(https://github.com/vanhauser-thc/THC-Archive/)
thedorkbox	Comprehensive collection of Google Dorks & OSINT techniques to find Confidential Data.	(https://github.com/cybersafeblr/thedorkbox)
thefatrat	TheFatRat a massive exploiting tool: easy tool to generate backdoor and easy tool to post exploitation attack.	(https://github.com/Screetsec/TheFatRat)
thefuzz	CLI fuzzing tool.	(https://github.com/droberson/thefuzz)
theharvester	Python tool for gathering e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).	(http://www.edge-security.com/theHarvester.php)
themole	Automatic SQL injection exploitation tool.	(http://sourceforge.net/projects/themole/)
thezoo	A project created to make the possibility of malware analysis open and available to the public.	(https://github.com/ytisf/theZoo)
threatspec	Project to integrate threat modelling into development process.	(https://github.com/threatspec/threatspec)
thumbcacheviewer	Extract Windows thumbcache database files.	(https://github.com/thumbcacheviewer/thumbcacheviewer)
tidos-framework	Offensive Web Application Penetration Testing Framework.	(https://github.com/0xInfection/TIDoS-Framework)
tiger	A security scanner, that checks computer for known problems. Can also use tripwire, aide and chkrootkit.	(http://www.nongnu.org/tiger/)
tilt	An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup.	(https://github.com/AeonDave/tilt)
timegen	This program generates a *.wav file to "send" an own time signal to DCF77 compatible devices.	(http://bastianborn.de/radio-clock-hack/)
timeverter	Bruteforce time-based tokens and to convert several time domains.	(https://github.com/D3vil0p3r/timeverter)

Name	Description	Website
tinc	VPN (Virtual Private Network) daemon	(https://www.tinc-vpn.org/)
tinfoleak	Get detailed information about a Twitter user activity.	(https://github.com/technoskald/tinfoleak/)
tinfoleak2	The most complete open-source tool for Twitter intelligence analysis.	(http://www.vicenteaguileradiaz.com/tools/)
tinyproxy	A light-weight HTTP proxy daemon for POSIX operating systems	(https://tinyproxy.github.io/)
tls-attacker	A Java-based framework for analyzing TLS libraries.	(https://github.com/RUB-NDS/TLS-Attacker)
tls-fingerprinting	Tool and scripts to perform TLS Fingerprinting.	(https://github.com/LeeBrotherston/tls-fingerprinting)
tls-map	CLI & library for TLS cipher suites manipulation.	(https://noraj.github.io/tls-map/)
tls-prober	A tool to fingerprint SSL/TLS servers.	(https://github.com/WestpointLtd/tls_prober)
tlsenum	A command line tool to enumerate TLS cipher-suites supported by a server.	(https://github.com/Ayrx/tlsenum)
tlsfuzzer	SSL and TLS protocol test suite and fuzzer.	(https://github.com/tomato42/tlsfuzzer)
tlshelpers	A collection of shell scripts that help handling X.509 certificate and TLS issues.	(https://github.com/hannob/tlshelpers)
tlspretense	SSL/TLS client testing framework.	(https://github.com/iSECPartners/tlspretense)
tlssled	A Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation.	(http://blog.taddong.com/2011/05/tlssled-v10.html)
tlsx	TLS grabber focused on TLS based data collection.	(https://github.com/projectdiscovery/tlsx)
tnscmd	A lame tool to prod the oracle tnslsnr process (1521/tcp).	(http://www.jammed.com/~jwa/hacks/security/tnscmd/)
token-hunter	OSINT Tool - Search the group and group members' snippets, issues, and issue discussions for sensitive data that may be included in these assets.	(https://github.com/GitLab-Red-Team/token-hunter)
token-reverser	Word list generator to crack security tokens.	(https://github.com/dariusztytko/token-reverser)
tomcatwardeployer	Apache Tomcat auto WAR deployment & pwning penetration testing tool.	(https://github.com/mgeeky/tomcatWarDeployer)
topera	An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort.	(https://github.com/toperaproject/topera)
tor	Anonymizing overlay network.	(https://www.torproject.org/download/tor/)
tor-autocircuit	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.	(http://www.thesprawl.org/projects/tor-autocircuit/)
tor-browser	Tor Browser Bundle: anonymous browsing using Firefox and Tor.	(https://www.torproject.org/projects/torbrowser.html)
tor-router	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.	(https://github.com/Edu4rdSHL/tor-router)
torcrawl	Crawl and extract (regular or onion) webpages through TOR network.	(https://github.com/MikeMeliz/TorCrawl.py)
torctl	Script to redirect all traffic through tor network including dns queries for anonymizing entire system.	(https://github.com/BlackArch/torctl)
torpy	Pure python Tor client implementation.	(https://github.com/torpyorg/torpy)
torshammer	A slow POST Denial of Service testing tool written in Python.	(http://sourceforge.net/projects/torshammer/)
torsocks	Wrapper to safely torify applications	(https://gitlab.torproject.org/tpo/core/torsocks)
tpcat	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.	(http://sourceforge.net/projects/tpcat/)
tplmap	Automatic Server-Side Template Injection Detection and Exploitation Tool.	(https://github.com/epinna/tplmap)
traceroute	Tracks the route taken by packets over an IP network	(http://traceroute.sourceforge.net/)
trape	People tracker on the Internet: OSINT analysis and research tool by Jose Pino.	(https://github.com/jofpin/trape)
traxss	Automated XSS Vulnerability Scanner.	(https://github.com/M4cs/traxss)
treasure	Hunt for sensitive information through githubs code search.	(https://github.com/GuerrillaWarfare/Treasure)
trevorproxy	A SOCKS proxy written in Python that randomizes your source IP address.	(https://github.com/blacklanternsecurity/TREVORproxy)
trevorspray	A modular password sprayer with threading, clever proxying, loot modules, and more!	(https://github.com/blacklanternsecurity/TREVORspray)
trid	An utility designed to identify file types from their binary signatures.	(http://mark0.net/soft-trid-e.html)
trinity	A Linux System call fuzzer.	(http://codemonkey.org.uk/projects/trinity/)
triton	A Dynamic Binary Analysis (DBA) framework.	(https://github.com/JonathanSalwan/Triton)
trivy	A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI	(https://github.com/aquasecurity/trivy)
trixd00r	An advanced and invisible userland backdoor based on TCP/IP for UNIX systems.	(http://nullsecurity.net/tools/backdoor.html)
truecrack	Password cracking for truecrypt(c) volumes.	(http://code.google.com/p/truecrack/)
truegaze	Static analysis tool for Android/iOS apps focusing on security issues outside the source code.	(https://github.com/nightwatchcybersecurity/truegaze)
truehunter	Detect TrueCrypt containers using a fast and memory efficient approach.	(https://github.com/adoreste/truehunter)
trufflehog	Searches through git repositories for high entropy strings, digging deep into commit history.	(https://github.com/dxa4481/truffleHog)
trusttrees	A Tool for DNS Delegation Trust Graphing.	(https://github.com/mandatoryprogrammer/TrustTrees)
tsh	An open-source UNIX backdoor that compiles on all variants, has full pty support, and uses strong crypto for communication.	(http://packetstormsecurity.com/search/?q=tsh)
tsh-sctp	An open-source UNIX backdoor.	(https://github.com/infodox/tsh-sctp)
ttpassgen	Highly flexible and scriptable password dictionary generator based on Python.	(https://github.com/tp7309/TTPassGen)
tunna	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.	(https://github.com/SECFORCE/Tunna)
turner	Tunnels HTTP over a permissive/open TURN server; supports HTTP and SOCKS5 proxy.	(https://github.com/staaldraad/turner)
tweets-analyzer	Tweets metadata scraper & activity analyzer.	(https://github.com/x0rz/tweets_analyzer)
tweetshell	Multi-thread Twitter BruteForcer in Shell Script.	(https://github.com/thelinuxchoice/tweetshell)
twint	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.	(https://github.com/twintproject/twint)
twofi	Twitter Words of Interest.	(http://www.digininja.org/projects/twofi.php)
typo3scan	Enumerate Typo3 version and extensions.	(https://github.com/whoot/Typo3Scan)
tyton	Kernel-Mode Rootkit Hunter.	(https://github.com/nbulischeck/tyton)
u3-pwn	A tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install.	(http://www.nullsecurity.net/tools/backdoor.html)
uacme	Defeating Windows User Account Control.	(https://github.com/hfiref0x/UACME)

Name	Description	Website
uatester	User Agent String Tester	(http://code.google.com/p/ua-tester/)
uberfile	CLI tool for the generation of downloader oneliners for UNIX-like or Windows systems.	(https://github.com/ShutdownRepo/uberfile)
ubertooth	A 2.4 GHz wireless development board suitable for Bluetooth experimentation. Open source hardware and software. Tools only.	(https://github.com/greatscottgadgets/ubertooth/releases)
ubiquiti-probing	A Ubiquiti device discovery tool.	(https://github.com/headlesszeke/ubiquiti-probing)
ubitack	Tool, which automates some of the tasks you might need on a (wireless) penetration test or while you are on the go.	(https://code.google.com/p/ubitack/)
udis86	A minimalistic disassembler library.	(http://udis86.sourceforge.net/)
udork	Bash script that uses advanced Google search techniques to obtain sensitive information in files or directories, find IoT devices, detect versions of web applications.	(https://github.com/m3n0sd0n4ld/uDork)
udp-hunter	Network assessment tool for various UDP Services covering both IPv4 and IPv6 protocols.	(https://github.com/NotSoSecure/udp-hunter)
udp2raw	A Tunnel which Turns UDP Traffic into Encrypted UDP/FakeTCP/ICMP Traffic by using Raw Socket	(https://github.com/wangyu-/udp2raw)
udpastcp	This program hides UDP traffic as TCP traffic in order to bypass certain firewalls.	(https://github.com/Hello71/udpastcp)
udptunnel	Tunnels TCP over UDP packets.	(http://code.google.com/p/udptunnel/)
udsim	A graphical simulator that can emulate different modules in a vehicle and respond to UDS request.	(https://github.com/zombieCraig/UDSim/)
uefi-firmware-parser	Parse BIOS/Intel ME/UEFI firmware related structures: Volumes, FileSystems, Files, etc.	(https://github.com/theopolis/uefi-firmware-parser)
ufo-wardriving	Allows you to test the security of wireless networks by detecting their passwords based on the router model.	(http://www.ufo-wardriving.com/)
ufonet	A tool designed to launch DDoS attacks against a target, using 'Open Redirect' vectors on third party web applications, like botnet.	(https://github.com/epsylon/ufonet)
uhoh365	Script to enumerate Office 365 users without performing login attempts	(https://github.com/Raikia/UhOh365)
ultimate-facebook-scraper	A bot which scrapes almost everything about a Facebook user's profile.	(https://github.com/harismuneer/Ultimate-Facebook-Scraper)
umap	The USB host security assessment tool.	(https://github.com/nccgroup/umap)
umit	A powerful nmap frontend.	(http://www.umitproject.org/)
uncaptcha2	Defeating the latest version of ReCaptcha with 91% accuracy.	(http://uncaptcha.cs.umd.edu/)
uncover	Discover exposed hosts on the internet using multiple search engines.	(https://github.com/projectdiscovery/uncover)
undbx	Extract e-mail messages from Outlook Express DBX files.	(https://github.com/ZungBang/undbx)
unfurl	Pull out bits of URLs provided on stdin.	(https://github.com/tomnomnom/unfurl)
unhide	A forensic tool to find processes hidden by rootkits, LKMs or by other techniques.	(https://github.com/YJesus/Unhide/)
unibrute	Multithreaded SQL union bruteforcer.	(https://github.com/GDSSecurity/Unibrute)
unicorn-powershell	A simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory.	(https://github.com/trustedsec/unicorn)
unicornscan	A new information gathering and correlation engine.	(http://www.unicornscan.org/)
unifuzzer	A fuzzing tool for closed-source binaries based on Unicorn and LibFuzzer.	(https://github.com/rk700/uniFuzzer)
uniofuzz	The universal fuzzing tool for browsers, web services, files, programs and network services/ports	(http://nullsecurity.net/tools/fuzzer.html)
uniscan	A simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.	(http://sourceforge.net/projects/uniscan/)
unisec	Unicode Security Toolkit.	(https://acceis.github.io/unisec)
unix-privesc-check	Tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases).	(http://pentestmonkey.net/tools/audit/unix-privesc-check)
unsecure	Bruteforces network login masks.	(http://www.sniperx.net/)
unstrip	ELF Unstrip Tool.	(https://github.com/pzread/unstrip)
untwister	Seed recovery tool for PRNGs.	(https://github.com/altf4/untwister)
upnp-pentest-toolkit	UPnP Pentest Toolkit for Windows.	(https://github.com/nccgroup/UPnP-Pentest-Toolkit)
upnpscan	Scans the LAN or a given address range for UPnP capable devices.	(http://www.cqure.net/wp/upnpscan/)
uppwn	A script that automates detection of security flaws on websites' file upload systems'.	(https://github.com/ferrery1/UpPwn)
uptux	Linux privilege escalation checks (systemd, dbus, socket fun, etc).	(https://github.com/initstring/uptux)
upx	Extendable, high-performance executable packer for several executable formats	(https://github.com/upx/upx)
urh	Universal Radio Hacker: investigate wireless protocols like a boss	(https://github.com/jopohl/urh)
urlcrazy	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage.	(http://www.morningstarsecurity.com/research/urlcrazy)
urldigger	A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code	(https://code.google.com/p/urldigger/)
urlextractor	Information gathering & website reconnaissance.	(https://github.com/eschultze/URLextractor)
urlview	A curses URL parser for text files.	(http://packages.qa.debian.org/u/urlview.html)
usb-canary	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.	(https://github.com/errbufferoverfl/usb-canary)
usbrip	USB device artifacts tracker.	(https://github.com/snovvcrash/usbrip)
username-anarchy	Tools for generating usernames when penetration testing.	(http://www.morningstarsecurity.com/research/username-anarchy)
usernamer	Pentest Tool to generate usernames/logins based on supplied names.	(https://github.com/jseidl/usernamer)
userrecon	Find usernames across over 75 social networks.	(https://github.com/thelinuxchoice/userrecon)
userrecon-py	Recognition usernames in 187 social networks.	(https://github.com/lucmski/userrecon-py)
usnjrnl2csv	Parser for $UsnJrnl on NTFS.	(https://github.com/jschicht/UsnJrnl2Csv)
usnparser	A Python script to parse the NTFS USN journal.	(https://pypi.org/project/usnparser/#files)
uw-loveimap	Multi threaded imap bounce scanner.	(http://uberwall.org/bin/download/45/UWloveimap.tgz)
uw-offish	Clear-text protocol simulator.	(http://uberwall.org/bin/download/42/UW_offish.1.tar.gz)
uw-udpscan	Multi threaded udp scanner.	(http://uberwall.org/bin/download/44/UWudpscan.tar.gz)
uw-zone	Multi threaded, randomized IP zoner.	(http://uberwall.org/bin/download/43/UWzone.tgz)
v3n0m	Offensive Security Tool for Vulnerability Scanning & Pentesting	(https://github.com/v3n0m-Scanner/V3n0M-Scanner)
vais	SWF Vulnerability & Information Scanner.	(https://github.com/hahwul/vais)

Name	Description	Website
valabind	Tool to parse vala or vapi files to transform them into swig interface files, C++, NodeJS-ffi or GIR	(https://github.com/radare/valabind)
valgrind	Tool to help find memory-management problems in programs	(https://valgrind.org/)
valhalla	Valhalla API Client.	(https://github.com/NextronSystems/valhallaAPI)
vane	A vulnerability scanner which checks the security of WordPress installations using a black box approach.	(https://github.com/delvelabs/vane)
vanguard	A comprehensive web penetration testing tool written in Perl thatidentifies vulnerabilities in web applications.	(http://packetstormsecurity.com/files/110603/Vanguard-Pentesting-Scanner.html)
vault-scanner	Swiss army knife for hackers.	(https://github.com/abhisharma404/vault)
vba2graph	Generate call graphs from VBA code, for easier analysis of malicious documents.	(https://github.com/MalwareCantFly/Vba2Graph)
vbrute	Virtual hosts brute forcer.	(https://github.com/nccgroup/vbrute)
vbscan	A black box vBulletin vulnerability scanner written in perl.	(https://github.com/rezasp/vbscan)
vbsmin	VBScript minifier.	(https://noraj.github.io/vbsmin/)
vcsmap	A plugin-based tool to scan public version control systems for sensitive information.	(https://github.com/melvinsh/vcsmap)
vega	An open source platform to test the security of web applications.	(https://github.com/subgraph/Vega/wiki)
veil	A tool designed to generate metasploit payloads that bypass common anti-virus solutions.	(https://github.com/Veil-Framework/Veil)
veles	New open source tool for binary data analysis.	(https://codisec.com/veles/)
venom	A Multi-hop Proxy for Penetration Testers.	(https://github.com/Dliv3/Venom)
veracrypt	Disk encryption with strong security based on TrueCrypt	(https://www.veracrypt.fr/)
verinice	Tool for managing information security.	(https://github.com/SerNet/verinice)
vfeed	Open Source Cross Linked and Aggregated Local Vulnerability Database main repository.	(http://www.toolswatch.org/vfeed)
vhostscan	A virtual host scanner that can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.	(https://github.com/codingo/VHostScan)
videosnarf	A new security assessment tool for pcap analysis	(http://ucsniff.sourceforge.net/videosnarf.html)
vinetto	A forensics tool to examine Thumbs.db files	(http://vinetto.sourceforge.net)
viper	A Binary analysis framework.	(https://github.com/botherder/viper)
vipermonkey	A VBA parser and emulation engine to analyze malicious macros.	(https://github.com/decalage2/ViperMonkey)
viproy-voipkit	VoIP Pen-Test Kit for Metasploit Framework.	(http://viproy.com/)
virustotal	Command-line utility to automatically lookup on VirusTotal all files recursively contained in a directory.	(https://github.com/botherder/virustotal)
visql	Scan SQL vulnerability on target site and sites of on server.	(https://github.com/blackvkng/viSQL)
visualize-logs	A Python library and command line tools to provide interactive log visualization.	(https://github.com/keithjjones/visualize_logs)
vivisect	A Python based static analysis and reverse engineering framework.	(https://github.com/vivisect/vivisect)
vlan-hopping	Easy 802.1Q VLAN Hopping	(https://github.com/nccgroup/vlan-hopping)
vlany	Linux LD_PRELOAD rootkit (x86 and x86_64 architectures).	(https://github.com/mempodippy/vlany)
vmap	A Vulnerability-Exploit desktop finder.	(https://github.com/git-rep/vmap)
vmcloak	Automated Virtual Machine Generation and Cloaking for Cuckoo Sandbox.	(https://github.com/jbremer/vmcloak)
vnak	Aim is to be the one tool a user needs to attack multiple VoIP protocols.	(https://www.isecpartners.com/vnak.html)
vnc-bypauth	Multi-threaded bypass authentication scanner for VNC smaller than v4.1.1 servers.	(http://pentester.fr/resources/tools/techno/VNC/VNC_bypauth/)
vncrack	What it looks like: crack VNC.	(http://phenoelit-us.org/vncrack)
voiper	A VoIP security testing toolkit incorporating several VoIP fuzzers and auxiliary tools to assist the auditor.	(http://voiper.sourceforge.net/)
voiphopper	A security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN.	(http://voiphopper.sourceforge.net/)
voipong	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.	(http://www.enderunix.org/voipong/)
volafox	Mac OS X Memory Analysis Toolkit.	(https://github.com/n0fate/volafox)
volatility-extra	Volatility plugins developed and maintained by the community.	(https://github.com/volatilityfoundation/community)
volatility3	Advanced memory forensics framework	(https://github.com/volatilityfoundation/volatility3/wiki)
voltron	UI for GDB, LLDB and Vivisect's VDB.	(https://github.com/snare/voltron)
vpnpivot	Explore the network using this tool.	(https://github.com/0x36/VPNPivot)
vsaudit	VOIP Security Audit Framework.	(https://github.com/sanvil/vsaudit)
vscan	HTTPS / Vulnerability scanner.	(https://github.com/pasjtene/Vscan)
vstt	VSTT is a multi-protocol tunneling tool. It accepts input by TCP stream sockets and FIFOs, and can send data via TCP, POP3, and ICMP tunneling.	(http://www.wendzel.de/dr.org/files/Projects/vstt/)
vsvbp	Black box tool for Vulnerability detection in web applications.	(https://github.com/varunjammula/VSVBP)
vt-cli	VirusTotal Command Line Interface.	(https://github.com/VirusTotal/vt-cli)
vulmap	Vulmap Online Local Vulnerability Scanners Project	(https://github.com/vulmon/Vulmap)
vulnerabilities-spider	A tool to scan for web vulnerabilities.	(https://github.com/muhammad-bouabid/Vulnerabilities-spider)
vulnx	Cms and vulnerabilites detector & An intelligent bot auto shell injector.	(https://github.com/anouarbensaad/vulnx)
vuls	Vulnerability scanner for Linux/FreeBSD, agentless, written in Go.	(https://github.com/future-architect/vuls)
vulscan	A module which enhances nmap to a vulnerability scanner	(https://www.computec.ch/projekte/vulscan/)
w13scan	Passive Security Scanner.	(https://github.com/boy-hack/w13scan)
w3af	Web Application Attack and Audit Framework.	(https://github.com/andresriancho/w3af/releases)
wafninja	A tool which contains two functions to attack Web Application Firewalls.	(https://github.com/khalilbijjou/WAFNinja)
wafp	An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints.	(http://packetstormsecurity.com/files/84468/Web-Application-Finger-Printer.01-26c3.html)
wafpass	Analysing parameters with all payloads' bypass methods, aiming at benchmarking security solutions like WAF.	(https://github.com/wafpassproject/wafpass)
wafw00f	Identify and fingerprint Web Application Firewall (WAF) products protecting a website.	(https://github.com/EnableSecurity/wafw00f)
waidps	Wireless Auditing, Intrusion Detection & Prevention System.	(https://github.com/SYWorks/waidps)

Name	Description	Website
waldo	A lightweight and multithreaded directory and subdomain bruteforcer implemented in Python.	(https://github.com/red-team-labs/waldo)
wapiti	A vulnerability scanner for web applications.	(https://github.com/wapiti-scanner/wapiti)
wascan	Web Application Scanner.	(https://github.com/m4ll0k/WAScan)
wavemon	Ncurses-based monitoring application for wireless network devices	(https://github.com/uoaerg/wavemon)
waybackpack	Download the entire Wayback Machine archive for a given URL.	(https://github.com/jsvine/waybackpack)
waybackurls	Fetch all the URLs that the Wayback Machine knows about for a domain.	(https://github.com/tomnomnom/waybackurls)
wcc	The Witchcraft Compiler Collection.	(https://github.com/endrazine/wcc)
wce	A security tool to list logon sessions and add, change, list and delete associated credentials (ex.: LM/NT hashes, plaintext passwords and Kerberos tickets).	(http://www.hoobie.net/wce/)
wcvs	Web Cache Vulnerability Scanner is a Go-based CLI tool for testing for web cache poisoning.	(https://github.com/Hackmanit/Web-Cache-Vulnerability-Scanner)
web-soul	A plugin based scanner for attacking and data mining web sites written in Perl.	(http://packetstormsecurity.com/files/122064/Web-Soul-Scanner.html)
web2ldap	Full-featured LDAP client running as web application.	(https://web2ldap.de/)
webacoo	Web Backdoor Cookie Script-Kit.	(https://bechtsoudis.com/webacoo/)
webanalyze	Port of Wappalyzer (uncovers technologies used on websites) in go to automate scanning.	(https://github.com/rverton/webanalyze)
webborer	A directory-enumeration tool written in Go.	(https://github.com/Matir/webborer)
webenum	Tool to enumerate http responses using dynamically generated queries and more.	(https://github.com/sarthakpandit/webenum)
webexploitationtool	A cross platform web exploitation toolkit.	(https://github.com/AutoSecTools/WebExploitationTool)
webfixy	On-the-fly decryption proxy for MikroTik RouterOS WebFig sessions.	(https://github.com/takeshixx/webfixy)
webhandler	A handler for PHP system functions & also an alternative 'netcat' handler.	(https://github.com/lnxg33k/webhandler)
webhunter	Tool for scanning web applications and networks and easily completing the process of collecting knowledge.	(https://github.com/peedcorp/WebHunter)
webkiller	Tool Information Gathering Write By Python.	(https://github.com/ultrasecurity/webkiller)
webpwn3r	A python based Web Applications Security Scanner.	(https://github.com/zigoo0/webpwn3r)
webrute	Web server directory brute forcer.	(https://github.com/BlackArch/webrute)
webscarab	Framework for analysing applications that communicate using the HTTP and HTTPS protocols	(http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)
websearch	Search vhost names given a host range. Powered by Bing..	(https://github.com/PentesterES/WebSearch)
webshag	A multi-threaded, multi-platform web server audit tool.	(http://www.scrt.ch/en/attack/downloads/webshag)
webshells	Web Backdoors.	(https://github.com/BlackArch/webshells)
webslayer	A tool designed for brute forcing Web Applications.	(https://code.google.com/p/webslayer/)
websockify	WebSocket to TCP proxy/bridge.	(http://github.com/kanaka/websockify)
webspa	A web knocking tool, sending a single HTTP/S to run O/S commands.	(http://sourceforge.net/projects/webspa/)
websploit	An Open Source Project For, Social Engineering Works, Scan, Crawler & Analysis Web, Automatic Exploiter, Support Network Attacks	(https://github.com/f4rih/websploit)
webtech	Identify technologies used on websites.	(https://pypi.org/project/webtech/#files)
webxploiter	An OWASP Top 10 Security scanner.	(https://github.com/xionsec/WebXploiter)
weebdns	DNS Enumeration with Asynchronicity.	(https://github.com/WeebSec/weebdns)
weeman	HTTP Server for phishing in python.	(https://github.com/Hypsurus/weeman)
weevely	Weaponized web shell.	(http://epinna.github.io/Weevely/)
weirdaal	AWS Attack Library.	(https://github.com/carnal0wnage/weirdAAL)
wepbuster	script for automating aircrack-ng	(http://code.google.com/p/wepbuster/)
wesng	Windows Exploit Suggester - Next Generation.	(https://github.com/bitsadmin/wesng)
wfuzz	Utility to bruteforce web applications to find their not linked resources.	(https://github.com/xmendez/wfuzz)
whapa	WhatsApp Parser Tool.	(https://github.com/B16f00t/whapa)
whatbreach	OSINT tool to find breached emails and databases.	(https://github.com/ekultek/whatbreach)
whatportis	A command to search port names and numbers.	(https://github.com/ncrocfer/whatportis)
whatsmyname	Tool to perform user and username enumeration on various websites.	(https://github.com/WebBreacher/WhatsMyName)
whatwaf	Detect and bypass web application firewalls and protection systems.	(https://github.com/Ekultek/WhatWaf)
whatweb	Next generation web scanner that identifies what websites are running.	(http://www.morningstarsecurity.com/research/whatweb)
whichcdn	Tool to detect if a given website is protected by a Content Delivery Network.	(https://github.com/Nitr4x/whichCDN)
whispers	Identify hardcoded secrets in static structured text.	(https://github.com/adeptex/whispers/)
whitewidow	SQL Vulnerability Scanner.	(https://github.com/Ekultek/whitewidow)
whoxyrm	A reverse whois tool based on Whoxy API.	(https://github.com/MilindPurswani/whoxyrm)
wi-feye	An automated wireless penetration testing tool written in python, its designed to simplify common attacks that can be performed on wifi networks so that they can be executed quickly and easily.	(http://wi-feye.za1d.com/download.php)
wifi-autopwner	Script to automate searching and auditing Wi-Fi networks with weak security.	(https://github.com/Mi-Al/WiFi-autopwner)
wifi-honey	A management tool for wifi honeypots.	(http://www.digininja.org/projects/wifi_honey.php)
wifi-monitor	Prints the IPs on your local network that're sending the most packets.	(https://github.com/DanMcInerney/wifi-monitor)
wifi-pumpkin	Framework for Rogue Wi-Fi Access Point Attack.	(https://github.com/P0cL4bs/wifipumpkin3)
wifibroot	A WiFi Pentest Cracking tool for WPA/WPA2 (Handshake, PMKID, Cracking, EAPOL, Deauthentication).	(https://github.com/hash3liZer/WiFiBroot)
wifichannelmonitor	A utility for Windows that captures wifi traffic on the channel you choose, using Microsoft Network Monitor capture driver.	(https://www.nirsoft.net/utils/wifi_channel_monitor.html)
wificurse	WiFi jamming tool.	(https://github.com/oblique/wificurse)
wifijammer	A python script to continuously jam all wifi clients within range.	(https://github.com/DanMcInerney/wifijammer)
wifiphisher	Fast automated phishing attacks against WPA networks.	(https://github.com/wifiphisher/wifiphisher)
wifiscanmap	Another wifi mapping tool.	(https://github.com/mehdilauters/wifiScanMap)
wifitap	WiFi injection tool through tun/tap device.	(https://github.com/GDSSecurity/wifitap)
wifite	Tool to attack multiple WEP and WPA encrypted networks at the same time	(https://github.com/kimocoder/wifite2)
wig	WebApp Information Gatherer.	(https://github.com/jekyc/wig)
wikigen	A script to generate wordlists out of wikipedia pages.	(https://github.com/zombiesam/wikigen)

Name	Description	Website
wildpwn	Unix wildcard attacks.	(https://github.com/localh0t/wildpwn)
windapsearch	Script to enumerate users, groups and computers from a Windows domain through LDAP queries.	(https://github.com/ropnop/windapsearch)
windivert	A user-mode packet capture-and-divert package for Windows.	(https://github.com/basil00/Divert)
windows-binaries	A colleciton of pentesting Windows binaries.	(https://github.com/BlackArch/windows-binaries)
windows-exploit-suggester	This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target.	(https://github.com/GDSSecurity/Windows-Exploit-Suggester)
windows-prefetch-parser	Parse Windows Prefetch files.	(https://github.com/PoorBillionaire/Windows-Prefetch-Parser)
windows-privesc-check	Standalone Executable to Check for Simple Privilege Escalation Vectors on Windows Systems.	(https://github.com/pentestmonkey/windows-privesc-check)
windowsspyblocker	Block spying and tracking on Windows.	(https://github.com/crazy-max/WindowsSpyBlocker/)
winexe	Remotely execute commands on Windows NT/2000/XP/2003 systems.	(http://sourceforge.net/projects/winexe/)
winfo	Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP.	(http://www.ntsecurity.nu/toolbox/winfo/)
winhex	Hex Editor and Disk Editor.	(https://www.x-ways.net/winhex/)
winpwn	Automation for internal Windows Penetrationtest / AD-Security.	(https://github.com/S3cur3Th1sSh1t/WinPwn)
winregfs	Windows Registry FUSE filesystem.	(https://github.com/jbruchon/winregfs)
winrelay	A TCP/UDP forwarder/redirector that works with both IPv4 and IPv6.	(http://ntsecurity.nu/toolbox/winrelay/)
wireless-ids	Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets.	(https://github.com/SYWorks/wireless-ids)
wireshark-cli	Network traffic and protocol analyzer/sniffer - CLI tools and data files	(https://www.wireshark.org/)
wireshark-qt	Network traffic and protocol analyzer/sniffer - Qt GUI	(https://www.wireshark.org/)
wirouter-keyrec	A platform independent software to recover the default WPA passphrases of the supported router models	(http://www.salvatorefresta.net/tools/)
witchxtool	A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner.	(http://packetstormsecurity.com/files/97465/Witchxtool-Port-LFI-SQL-Scanner-And-MD5-Bruteforcing-Tool.1.html)
wlan2eth	Re-writes 802.11 captures into standard Ethernet frames.	(http://www.willhackforsushi.com/?page_id=79)
wmat	Automatic tool for testing webmail accounts.	(http://netsec.rs/70/tools.html)
wmd	Python framework for IT security tools.	(https://github.com/ThomasTJdev/WMD)
wmi-forensics	Scripts used to find evidence in WMI repositories.	(https://github.com/davidpany/WMI_Forensics)
wnmap	A shell script written with the purpose to automate and chain scans via nmap.	(http://nullsecurity.net/tools/automation.html)
wol-e	A suite of tools for the Wake on LAN feature of network attached computers.	(http://code.google.com/p/wol-e/)
wolpertinger	A distributed portscanner.	(https://github.com/Crapworks/wolpertinger)
wondershaper	Limit the bandwidth of one or more network adapters.	(https://github.com/magnific0/wondershaper)
wordbrutepress	Python script that performs brute forcing against WordPress installs using a wordlist.	(http://www.homelab.it/index.php/2014/11/03/wordpress-brute-force-multithreading/)
wordlistctl	Fetch, install and search wordlist archives from websites.	(https://github.com/BlackArch/wordlistctl)
wordlister	A simple wordlist generator and mangler written in python.	(https://github.com/4n4nk3/Wordlister)
wordpot	A Wordpress Honeypot.	(https://github.com/gbrindisi/wordpot)
wordpress-exploit-framework	A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.	(https://github.com/rastating/wordpress-exploit-framework)
wordpresscan	WPScan rewritten in Python + some WPSeku ideas.	(https://github.com/swisskyrepo/Wordpresscan)
wpa-bruteforcer	Attacking WPA/WPA encrypted access point without client.	(https://github.com/SYWorks/wpa-bruteforcer)
wpa2-halfhandshake-crack	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.	(https://github.com/dxa4481/WPA2-HalfHandshake-Crack)
wpbf	Multithreaded WordPress brute forcer.	(https://github.com/dejanlevaja/wpbf)
wpbrute-rpc	Tool for amplified bruteforce attacks on wordpress based website via xmlrcp API.	(https://github.com/zendoctor/wpbrute-rpc)
wpbullet	A static code analysis for WordPress (and PHP).	(https://github.com/webarx-security/wpbullet)
wpforce	Wordpress Attack Suite.	(https://github.com/n00py/WPForce)
wpintel	Chrome extension designed for WordPress Vulnerability Scanning and information gathering.	(https://github.com/Tuhinshubhra/WPintel)
wpscan	Black box WordPress vulnerability scanner	(https://wpscan.org)
wpseku	Simple Wordpress Security Scanner.	(https://github.com/m4ll0k/WPSeku)
wpsik	WPS scan and pwn tool.	(https://github.com/0x90/wpsik)
wpsweep	A simple ping sweeper, that is, it pings a range of IP addresses and lists the ones that reply.	(http://ntsecurity.nu/toolbox/wpsweep/)
wreckuests	Yet another one hard-hitting tool to run DDoS attacks with HTTP-flood.	(https://github.com/JamesJGoodwin/wreckuests)
ws-attacker	A modular framework for web services penetration testing.	(http://ws-attacker.sourceforge.net/)
wscript	Emulator/tracer of the Windows Script Host functionality.	(https://github.com/mrpapercut/wscript)
wsfuzzer	A Python tool written to automate SOAP pentesting of web services.	(https://www.owasp.org/index.php/Category:OWASP_WSFuzzer_Project)
wssip	Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa.	(https://github.com/nccgroup/wssip)
wsuspect-proxy	A tool for MITM'ing insecure WSUS connections.	(https://github.com/ctxis/wsuspect-proxy)
wups	An UDP port scanner for Windows.	(http://ntsecurity.nu/toolbox/wups/)
wuzz	Interactive cli tool for HTTP inspection.	(https://github.com/asciimoo/wuzz)
wxhexeditor	A free hex editor / disk editor for Linux, Windows and MacOSX.	(http://wxhexeditor.sourceforge.net/)
wyd	Gets keywords from personal files. IT security/forensic tool.	(http://www.remote-exploit.org/?page_id=418)
x-rsa	Contains a many of attack types in RSA such as Hasted, Common Modulus, Chinese Remainder Theorem.	(https://github.com/X-Vector/X-RSA)
x-scan	A general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable.	(http://www.xfocus.org/)
x64dbg	An open-source x64/x32 debugger for windows.	(https://github.com/x64dbg/x64dbg/releases)
x8	Hidden parameters discovery suite.	(https://github.com/Sh1Yo/x8)

Name	Description	Website
xcat	A command line tool to automate the exploitation of blind XPath injection vulnerabilities.	(https://github.com/orf/xcat)
xcavator	Man-In-The-Middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.	(https://github.com/nccgroup/xcavator)
xcname	A tool for enumerating expired domains in CNAME records.	(https://github.com/mandatoryprogrammer/xcname)
xerosploit	Efficient and advanced man in the middle framework.	(https://github.com/LionSec/xerosploit)
xfltreat	Tunnelling framework.	(https://github.com/earthquake/xfltreat/)
xmlrpc-bruteforcer	An XMLRPC brute forcer targeting Wordpress written in Python 3.	(https://github.com/kavishgr/xmlrpc-bruteforcer)
xorbruteforcer	Script that implements a XOR bruteforcing of a given file, although a specific key can be used too.	(http://eternal-todo.com/category/bruteforce)
xorsearch	Program to search for a given string in an XOR, ROL or ROT encoded binary file.	(http://blog.didierstevens.com/programs/xorsearch/)
xortool	Tool to analyze multi-byte XOR cipher	(https://github.com/hellman/xortool)
xpire-crossdomain-scanner	Scans crossdomain.xml policies for expired domain names.	(https://github.com/mandatoryprogrammer/xpire-crossdomain-scanner)
xpl-search	Search exploits in multiple exploit databases!.	(https://github.com/CoderPirata/XPL-SEARCH)
xplico	Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT).	(http://www.xplico.org/)
xprobe2	An active OS fingerprinting tool.	(http://sourceforge.net/apps/mediawiki/xprobe/index.php?title=Main_Page)
xray	A tool for recon, mapping and OSINT gathering from public networks.	(https://github.com/evilsocket/xray)
xrop	Tool to generate ROP gadgets for ARM, AARCH64, x86, MIPS, PPC, RISCV, SH4 and SPARC.	(https://github.com/acama/xrop)
xspear	Powerful XSS Scanning and Parameter analysis tool&gem.	(https://github.com/hahwul/XSpear)
xspy	A utility for monitoring keypresses on remote X servers	(http://www.freshports.org/security/xspy/)
xsrfprobe	The Prime Cross Site Request Forgery Audit and Exploitation Toolkit.	(https://github.com/0xInfection/XSRFProbe)
xss-freak	An XSS scanner fully written in Python3 from scratch.	(https://github.com/hacker900123/XSS-Freak)
xsscon	Simple XSS Scanner tool.	(https://github.com/menkrep1337/XSSCon)
xsscrapy	XSS spider - 66/66 wavsep XSS detected.	(https://github.com/DanMcInerney/xsscrapy)
xsser	A penetration testing tool for detecting and exploiting XSS vulnerabilites.	(https://xsser.03c8.net/)
xssless	An automated XSS payload generator written in python.	(https://github.com/mandatoryprogrammer/xssless)
xsspy	Web Application XSS Scanner.	(https://github.com/faizann24/XssPy)
xsss	A brute force cross site scripting scanner.	(http://www.sven.de/xsss/)
xssscan	Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS.	(https://github.com/gwroblew/detectXSSlib)
xsssniper	An automatic XSS discovery tool	(https://github.com/gbrindisi/xsssniper)
xsstracer	Python script that checks remote web servers for Clickjacking, Cross-Frame Scripting, Cross-Site Tracing and Host Header Injection.	(https://github.com/1N3/XSSTracer)
xsstrike	An advanced XSS detection and exploitation suite.	(https://github.com/UltimateHackers/XSStrike)
xssya	A Cross Site Scripting Scanner & Vulnerability Confirmation.	(https://github.com/yehia-mamdouh/XSSYA)
xwaf	Automatic WAF bypass tool.	(https://github.com/3xp10it/bypass_waf)
xxeinjector	Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods.	(https://github.com/enjoiz/XXEinjector)
xxeserv	A mini webserver with FTP support for XXE payloads.	(https://github.com/staaldraad/xxeserv)
xxexploiter	It generates the XML payloads, and automatically starts a server to serve the needed DTD's or to do data exfiltration.	(https://github.com/luisfontes19/xxexploiter)
xxxpwn	A tool Designed for blind optimized XPath 1 injection attacks.	(https://github.com/feakk/xxxpwn)
xxxpwn-smart	A fork of xxxpwn adding further optimizations and tweaks.	(https://github.com/aayla-secura/xxxpwn_smart)
yaaf	Yet Another Admin Finder.	(https://github.com/RomeuG/YAAF)
yaf	Yet Another Flowmeter.	(https://tools.netsa.cert.org/yaf/download.html)
yara	Tool aimed at helping malware researchers to identify and classify malware samples	(https://github.com/VirusTotal/yara)
yasat	Yet Another Stupid Audit Tool.	(http://yasat.sourceforge.net/)
yasca	Multi-Language Static Analysis Toolset.	(http://www.scovetta.com/yasca.html)
yasuo	A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network.	(https://github.com/0xsauby/yasuo)
yate-bts	An open source GSM Base Station software.	(https://yatebts.com/)
yawast	The YAWAST Antecedent Web Application Security Toolkit.	(https://github.com/adamcaudill/yawast)
yay	Yet another yogurt. Pacman wrapper and AUR helper written in go.	(https://github.com/Jguer/yay)
ycrawler	A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support.	(http://packetstormsecurity.com/files/98546/yCrawler-Web-Crawling-Utility.html)
yersinia	A network tool designed to take advantage of some weakness in different network protocols.	(http://www.yersinia.net/)
yeti	A platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository.	(https://github.com/yeti-platform/yeti)
yinjector	A MySQL injection penetration tool. It has multiple features, proxy support, and multiple exploitation methods.	(http://packetstormsecurity.com/files/98359/yInjector-MySQL-Injection-Tool.html)
ysoserial	A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.	(https://github.com/frohoff/ysoserial)
zackattack	A new tool set to do NTLM Authentication relaying unlike any other tool currently out there.	(https://github.com/urbanesec/ZackAttack/)
zaproxy	Integrated penetration testing tool for finding vulnerabilities in web applications	(https://www.zaproxy.org/)
zarp	A network attack tool centered around the exploitation of local networks.	(https://defense.ballastsecurity.net/wiki/index.php/Zarp)
zdns	Fast CLI DNS Lookup Tool.	(https://github.com/zmap/zdns)
zeek	A powerful network analysis framework that is much different from the typical IDS you may know.	(https://github.com/zeek/zeek)
zeek-aux	Handy auxiliary programs related to the use of the Zeek Network Security Monitor.	(https://github.com/zeek/zeek-aux)
zelos	A comprehensive binary emulation and instrumentation platform.	(https://github.com/zeropointdynamics/zelos)
zeratool	Automatic Exploit Generation (AEG) and remote flag capture for exploitable CTF problems.	(https://github.com/ChrisTheCoolHut/Zeratool)

Name	Description	Website
zerowine	Malware Analysis Tool - research project to dynamically analyze the behavior of malware	(http://zerowine.sf.net/)
zeus	AWS Auditing & Hardening Tool.	(https://github.com/DenizParlak/Zeus)
zeus-scanner	Advanced dork searching utility.	(https://github.com/Ekultek/Zeus-Scanner)
zgrab	Grab banners (optionally over TLS).	(https://github.com/zmap/zgrab)
zgrab2	Go Application Layer Scanner.	(https://github.com/zmap/zgrab2)
zipdump	ZIP dump utility.	(https://blog.didierstevens.com/my-software/#zipdump)
zipexec	A unique technique to execute binaries from a password protected zip.	(https://github.com/Tylous/ZipExec)
zirikatu	Fud Payload generator script.	(https://github.com/pasahitz/zirikatu)
zizzania	Automated DeAuth attack.	(https://github.com/cyrus-and/zizzania)
zmap	Fast network scanner designed for Internet-wide network surveys	(https://zmap.io/)
zssh	SSH and Telnet client with ZMODEM file transfer capability	(http://zssh.sourceforge.net/)
zsteg	Detect stegano-hidden data in PNG and BMP.	(https://github.com/zedxff/zsteg)
zulu	A light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks.	(http://sourceforge.net/projects/zulu-wireless/)
zulucrypt	Front end to cryptsetup and tcplay and it allows easy management of encrypted block devices.	(https://github.com/mhogomchungu/zuluCrypt)
zykeys	Demonstrates how default wireless settings are derived on some models of ZyXEL routers.	(http://packetstormsecurity.com/files/119156/Zykeys-Wireless-Tool.html)
zzuf	Transparent application input fuzzer	(https://github.com/samhocevar/zzuf)

(https://github.com/BlackArch) (https://twitter.com/blackarchlinux) (https://matrix.to/#/#BlackArch:matrix.org) (https://blackarch.org/news.html) (https://blackarch.org/rss.xml)