Tools list

0d1n	1:263.2d723ae	Web security tool to make fuzzing at HTTP inputs, made in C with libCurl.
0trace	1.5	A hop enumeration tool.
3proxy	0.9.4	Tiny free proxy server.
3proxy-win32	0.8.13	Tiny free proxy server.
42zip	1:42	Recursive Zip archive bomb.
a2sv	140.cb24c4e	Auto Scanning to SSL Vulnerability (HeartBleed, CCS Injection, SSLv3 POODLE, FREAK, LOGJAM Attack, SSLv2 DROWN etc).
abcd	4.2738809	ActionScript ByteCode Disassembler.
abuse-ssl-bypass-waf	7.c28f98e	Bypassing WAF by abusing SSL/TLS Ciphers.
acccheck	0.2.1	A password dictionary attack tool that targets windows authentication via the SMB protocol.
ace	1.10	Automated Corporate Enumerator. A simple yet powerful VoIP Corporate Directory enumeration tool that mimics the behavior of an IP Phone in order to download the name and extension entries that a given phone can display on its screen interface
aclpwn	4.81480cc	Active Directory ACL exploitation with BloodHound.
activedirectoryenum	1:0.5.0	Enumerate AD through LDAP.
ad-ldap-enum	88.60bc5bb	An LDAP based Active Directory user and group enumeration tool.
adape-script	43.4d0b9ff	Active Directory Assessment and Privilege Escalation Script.
adenum	36.fbbe14d	A pentesting tool that allows to find misconfiguration through the the protocol LDAP and exploit some of those weaknesses with kerberos.
adfind	31.9808cb7	Admin Panel Finder.
adfspray	6.3d7745d	Python3 tool to perform password spraying against Microsoft Online service using various methods.
adidnsdump	24.65169b2	Active Directory Integrated DNS dumping by any authenticated user.
admid-pack	1:0.1	ADM DNS spoofing tools - Uses a variety of active and passive methods to spoof DNS packets. Very powerful.

adminpagefinder	0.1	This python script looks for a large amount of possible administrative interfaces on a given site.
admsnmp	0.1	ADM SNMP audit scanner.
aesfix	1.0.1	A tool to find AES key in RAM
aeskeyfind	1.0	A tool to find AES key in RAM
aespipe	2.4f	Reads data from stdin and outputs encrypted or decrypted results to stdout.
aesshell	0.7	A backconnect shell for Windows and Unix written in python and uses AES in CBC mode in conjunction with HMAC-SHA256 for secure transport.
afflib	3.7.19	An extensible open format for the storage of disk images and related forensic information.
afl	2.57b	Security-oriented fuzzer using compile-time instrumentation and genetic algorithms
aflplusplus	4.06c.r45.g74be9ab5	American Fuzzing Lop fuzzer with community patches and additional features.
afpfs-ng	0.8.2	A client for the Apple Filing Protocol (AFP)
agafi	1:1.1	A gadget finder and a ROP-Chainer tool for x86 platforms.
against	1:0.2	A very fast ssh attacking script which includes a multithreaded port scanning module (tcp connect) for discovering possible targets and a multithreaded brute-forcing module which attacks parallel all discovered hosts or given ip addresses from a list.
aggroargs	51.c032446	Bruteforce commandline buffer overflows, linux, aggressive arguments.
aiengine	1:2.0.1	A packet inspection engine with capabilities of learning without any human intervention.
aimage	3.2.5	A program to create aff-images.
aiodnsbrute	38.e773a4c	Python 3 DNS asynchronous brute force utility.
air	2.0.0	A GUI front-end to dd/dc3dd designed for easily creating forensic images.
aircrack-ng	1.7	Key cracker for the 802.11 WEP and WPA-PSK protocols
airflood	0.1	A modification of aireplay that allows for a DoS of the AP. This program fills the table of clients of the AP with random MACs doing impossible new connections.
airgeddon	1:v11.11.r0.g3d95621	Multi-use bash script for Linux systems to audit wireless networks.
airgraph-ng	2:2.0.2	Graphing tool for the aircrack suite.

airopy	5.b83f11d	Get (wireless) clients and access points.
airoscript	2:45.0a122ee	A script to simplify the use of aircrack-ng tools.
airpwn	1.4	A tool for generic packet injection on an 802.11 network.
ajpfuzzer	0.6	A command-line fuzzer for the Apache JServ Protocol (ajp13).
albatar	34.4e63f22	A SQLi exploitation framework in Python.
allthevhosts	1.0	A vhost discovery tool that scrapes various web applications.
altdns	76.8c1de0f	Generates permutations, alterations and mutations of subdomains and then resolves them.
amass	2:2052.b8f8520c	In-depth subdomain enumeration written in Go.
amber	254.a331b34	Reflective PE packer.
amoco	1:v2.4.1.r307.ged579ea	Yet another tool for analysing binaries.
analyzemft	130.16d1282	Parse the MFT file from an NTFS filesystem.
analyzepesig	0.0.0.5	Analyze digital signature of PE file.
androbugs	1.7fd3a2c	An efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications.
androguard	2:2118.8d091cbb	Reverse engineering, Malware and goodware analysis of Android applications and more.
androick	8.522cfb4	A python tool to help in forensics analysis on android.
android-apktool	2.7.0	A tool for reengineering Android apk files.
android-ndk	2:r23.b	Android C/C++ developer kit.
android-sdk	26.1.1	Google Android SDK.
android-sdk-platform-tools	r23.0.1	Platform-Tools for Google Android SDK (adb and fastboot).
android-udev-rules	1:471.b4d81e6	Android udev rules.
androidpincrack	2.ddaf307	Bruteforce the Android Passcode given the hash and salt.
androidsniffer	0.1	A perl script that lets you search for 3rd party passwords, dump the call log, dump contacts, dump wireless configuration, and more.
androwarn	135.626c02d	Yet another static code analyzer for malicious Android applications.
angr	1:9.1.11752	The next-generation binary analysis platform from UC Santa Barbara's Seclab.

angr-management	9.1.11752	This is the GUI for angr.
angr-py2	1:7.8.9.26	The next-generation binary analysis platform from UC Santa Barbaras Seclab.
angrop	251.1391ca4	A rop gadget finder and chain builder.
anontwi	1.1b	A free software python client designed to navigate anonymously on social networks. It supports Identi.ca and Twitter.com.
anti-xss	166.2725dc9	A XSS vulnerability scanner.
antiransom	5	A tool capable of detect and stop attacks of Ransomware using honeypots.
apache-users	2.1	This perl script will enumerate the usernames on a unix system that use the apache module UserDir.
apachetomcatscanner	3.2	Apache Tomcat vulnerability scanner.
apacket	374.16e7036	Sniffer syn and backscatter packets.
aphopper	0.3	AP Hopper is a program that automatically hops between access points of different wireless networks.
api-dnsdumpster	59.eda15d6	Unofficial Python API for http://dnsdumpster.com/.
apkid	2:2.1.4	Android Application Identifier for Packers, Protectors, Obfuscators and Oddities.
apkleaks	v2.6.1.r5.g1fd6f3c	Scanning APK file for URIs, endpoints & secrets.
apkstat	18.81cdad3	Automated Information Retrieval From APKs For Initial Analysis.
apkstudio	100.9e114ca	An IDE for decompiling/editing & then recompiling of android application binaries.
apnbf	0.1	A small python script designed for enumerating valid APNs (Access Point Name) on a GTP-C speaking device.
appmon	177.f753c4d	A runtime security testing & profiling framework for native apps on macOS, iOS & android and it is built using Frida.
apt2	183.8075cdc	Automated penetration toolkit.
aquatone	142.2daa022	a set of tools for performing reconnaissance on domain names.
arachni	1.6.1.3	A feature-full, modular, high-performance Ruby framework aimed towards helping penetration testers and administrators evaluate the security of web applications.

aranea	6.469b9ee	A fast and clean dns spoofing tool.
arcane	2.750cb9f	Backdoor iOS packages and create the necessary resources for APT repositories.
archivebox	903.59da482	The open source self-hosted web archive. Takes browser history/bookmarks/Pocket/Pinboard/etc., saves HTML, JS, PDFs, media, and more.
arduino	1:1.8.19	Arduino prototyping platform SDK
argon2	20190702	The password hash Argon2, winner of PHC.
argus	3.0.8.2	Network monitoring tool with flow control.
argus-clients	3.0.8.2	Network monitoring client for Argus.
arjun	214.70b5b28	HTTP parameter discovery suite.
armitage	4:150813	A graphical cyber attack management tool for Metasploit.
armor	5.bae27a6	A simple Bash script designed to create encrypted macOS payloads capable of evading antivirus scanners.
armscgen	98.c51b7d6	ARM Shellcode Generator (Mostly Thumb Mode).
arp-scan	1.10.0	A tool that uses ARP to discover and fingerprint IP hosts on the local network
arpalert	1:2.0.12	Monitor ARP changes in ethernet networks.
arpoison	0.7	The UNIX arp cache update utility
arpon	2.7	A portable handler daemon that make ARP protocol secure in order to avoid the Man In The Middle (MITM) attack through ARP Spoofing, ARP Cache Poisoning or ARP Poison Routing (APR) attacks.
arpstraw	27.ab40e13	Arp spoof detection tool.
arptools	13.41cdb23	A simple tool about ARP broadcast, ARP attack, and data transmission.
arpwner	26.f300fdf	GUI-based python tool for arp posioning and dns poisoning attacks.
artillery	1:357.805a5d8	A combination of a honeypot, file-system monitoring, system hardening, and overall health of a server to create a comprehensive way to secure a system.
artlas	154.e5fdd8d	Apache Real Time Logs Analyzer System.
arybo	65.89d9a42	Manipulation, canonicalization and identification of mixed boolean-arithmetic symbolic expressions.
asleap	2.2	Actively recover LEAP/PPTP passwords.
asnmap	v1.0.2.r0.g4bff	Map organization network ranges using ASN information.

	fc3	
asp-audit	2BETA	An ASP fingerprinting tool and vulnerability scanner.
assetfinder	19.4e95d87	Find domains and subdomains potentially related to a given domain.
astra	487.57c1e41	Automated Security Testing For REST API's.
atear	139.245ec8d	Wireless Hacking, WiFi Security, Vulnerability Analyzer, Pentestration.
atftp	0.8.0	Client/server implementation of the TFTP protocol that implements RFCs 1350, 2090, 2347, 2348, and 2349
athena-ssl-scanner	0.6.2	a SSL cipher scanner that checks all cipher codes. It can identify about 150 different ciphers.
atlas	7.77bd6c8	Open source tool that can suggest sqlmap tampers to bypass WAF/IDS/IPS.
atscan	2454.b1b241e	Server, Site and Dork Scanner.
atstaketools	0.1	This is an archive of various @Stake tools that help perform vulnerability scanning and analysis, information gathering, password auditing, and forensics.
attacksurfacemapper	45.0a2e408	Tool that aims to automate the reconnaissance process.
attk	2.0.1023	Trend Micro Anti-Threat Toolkit.
aurebeshjs	77.75a8fc6	Translate JavaScript to Other Alphabets.
auto-eap	18.ee36d37	Automated Brute-Force Login Attacks Against EAP Networks.
auto-xor-decryptor	7.2eb176d	Automatic XOR decryptor tool.
automato	33.0561b59	Should help with automating some of the user-focused enumeration tasks during an internal penetration test.
autonessus	24.7933022	This script communicates with the Nessus API in an attempt to help with automating scans.
autonse	25.7c87f4c	Massive NSE (Nmap Scripting Engine) AutoSploit and AutoScanner.
autopsy	1:4.20.0	A GUI for The Sleuth Kit.
autopwn	190.fc80cef	Specify targets and run sets of tools against them.
autorecon	277.b4567a2	A multi-threaded network reconnaissance tool which performs automated enumeration of services.
autosint	234.e1f4937	Tool to automate common osint tasks.
autosploit	281.9a6a5ef	Automate the exploitation of remote hosts.

autovpn	18.28b1a87	Easily connect to a VPN in a country of your choice.
avaloniailspy	1:v7.2.rc.r1.ge6562c2	.NET Decompiler (port of ILSpy)
avet	133.2f1d882	AntiVirus Evasion Tool
avml	1:v0.6.1.r11.g155f084	A portable volatile memory acquisition tool for Linux.
aws-extender-cli	17.a351154	Script to test S3 buckets as well as Google Storage buckets and Azure Storage containers for common misconfiguration issues.
aws-inventory	19.9a2fa8e	Discover resources created in an AWS account.
awsbucketdump	82.4684670	A tool to quickly enumerate AWS S3 buckets to look for loot.
azazel	15.a41fbb5	A userland rootkit based off of the original LD_PRELOAD technique from Jynx rootkit.
aztarna	1.2.1	A footprinting tool for ROS and SROS systems.
ba-testpkg	8.8	BlackArch Linux Test Package.
backcookie	51.6dabc38	Small backdoor using cookie.
backdoor-apk	141.2710126	Shell script that simplifies the process of adding a backdoor to any Android APK file
backdoor-factory	1:208.9972ac6	Patch win32/64 binaries with shellcode.
backdoorme	308.f9755ca	A powerful utility capable of backdooring Unix machines with a slew of backdoors.
backdoorppt	88.d0e7f91	Transform your payload.exe into one fake word doc (.ppt).
backfuzz	1:1.b0648de	A network protocol fuzzing toolkit.
backhack	39.561ec86	Tool to perform Android app analysis by backing up and extracting apps, allowing you to analyze and modify file system contents for apps.
backoori	55.988e507	Tool aided persistence via Windows URI schemes abuse.
backorifice	1.0	A remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application.
bad-pdf	61.a8149ee	Steal NTLM Hashes with Bad-PDF.
badkarma	85.2c46334	Advanced network reconnaissance toolkit.
badministration	16.69e4ec2	A tool which interfaces with management or administration applications from an offensive standpoint.
bagbak	160.b0633a4	Yet another frida based App decryptor.

balbuzard	67.d6349ef1bc55	A package of malware analysis tools in python to extract patterns of interest from suspicious files (IP addresses, domain names, known file headers, interesting strings, etc).
bamf-framework	35.30d2b4b	A modular framework designed to be a platform to launch attacks against botnets.
bandicoot	0.6.0	A toolbox to analyze mobile phone metadata.
barf	923.9547ef8	A multiplatform open source Binary Analysis and Reverse engineering Framework.
barmie	1.01	Java RMI enumeration and attack tool.
barq	35.6f1a68c	An AWS Cloud Post Exploitation framework.
base64dump	0.0.14	Extract and decode base64 strings from files.
basedomainname	0.1	Tool that can extract TLD (Top Level Domain), domain extensions (Second Level Domain + TLD), domain name, and hostname from fully qualified domain names.
bashfuscator	338.7487348	Fully configurable and extendable Bash obfuscation framework.
bashscan	94.80c066c	A port scanner built to utilize /dev/tcp for network and service discovery.
batctl	2023.0	B.A.T.M.A.N. advanced control and management tool
batman-adv	2019.2	Batman kernel module, (included upstream since .38)
batman-alfred	2022.0	Almighty Lightweight Fact Remote Exchange Daemon
bbqsql	261.b9859d2	SQL injection exploit tool.
bbscan	48.43c1088	A tiny Batch weB vulnerability Scanner.
bdfproxy	107.276c367	Patch Binaries via MITM: BackdoorFactory + mitmProxy
bdlogparser	2	This is a utility to parse a Bit Defender log file, in order to sort them into a malware archive for easier maintanence of your malware collection.
bed	0.5	Collection of scripts to test for buffer overflows, format string vulnerabilities.
beebug	25.cddb375	A tool for checking exploitability.
beef	1:4191.82e4d364	The Browser Exploitation Framework that focuses on the web browser
beeswarm	1183.db51ea0	Honeypot deployment made easy http://www.beeswarm-ids.org/
beholder	0.8.10	A wireless intrusion detection tool that looks for anomalies in a wifi environment.
belati	72.49577a1	The Traditional Swiss Army Knife for OSINT.

beleth	36.0963699	A Multi-threaded Dictionary based SSH cracker.
bettercap	2.32.0	A complete, modular, portable and easily extensible MITM framework.
bettercap-ui	1.3.0	Official Bettercap's Web UI.
bfac	53.18fb0b5	An automated tool that checks for backup artifacts that may disclose the web-application's source code.
bfbtester	2.0.1	Performs checks of single and multiple argument command line overflows and environment variable overflows
bfuzz	60.fdaefc0	Input based fuzzer tool for browsers.
bgp-md5crack	0.1	RFC2385 password cracker
bgrep	24.28029c9	Binary grep.
billcipher	32.97fba59	Information Gathering tool for a Website or IP address.
binaryninja-demo	3.3.3996	A new kind of reversing platform (demo version).
binaryninja-python	13.83f59f7	Binary Ninja prototype written in Python.
bind	9.18.14	The ISC DNS Server
bind-tools	9.16.5	The ISC DNS tools
bindead	4504.67019b97b	A static analysis tool for binaries
bindiff	6.0.0	A comparison tool for binary files, that assists vulnerability researchers and engineers to quickly find differences and similarities in disassembled code.
binex	1.0	Format String exploit building tool.
binflow	5.7fb02a9	POSIX function tracing. Much better and faster than ftrace.
bing-ip2hosts	1.0.5	Enumerates all hostnames which Bing has indexed for a specific IP address.
bing-lfi-rfi	0.1	This is a python script for searching Bing for sites that may have local and remote file inclusion vulnerabilities.
bingoo	3.698132f	A Linux bash based Bing and Google Dorking Tool.
binnavi	6.1.0	A binary analysis IDE that allows to inspect, navigate, edit and annotate control flow graphs and call graphs of disassembled code.
binproxy	8.d02fce9	A proxy for arbitrary TCP connections.
binwalk	2.3.4	A tool for searching a given binary image for embedded files

binwally	4.0aabd8b	Binary and Directory tree comparison tool using the Fuzzy Hashing concept (ssdeep).
bios_memimage	1.2	A tool to dump RAM contents to disk (aka cold boot attack).
birp	65.b2e108a	A tool that will assist in the security assessment of mainframe applications served over TN3270.
bitdump	34.6a5cbd8	A tool to extract database data from a blind SQL injection vulnerability.
bittwist	2.0	A simple yet powerful libpcap-based Ethernet packet generator. It is designed to complement tcpdump, which by itself has done a great job at capturing network traffic.
bkcrack	v1.5.0.r3.g27a9f22	Crack legacy zip encryption with Biham and Kocher known plaintext attack.
bkhive	1.1.1	Program for dumping the syskey bootkey from a Windows NT/2K/XP system hive.
BlackArch Linux	2023.04.01	BlackArch Linux is an Arch Linux-based penetration testing distribution for penetration testers and security researchers. You can install tools individually or in groups. BlackArch Linux is compatible with existing Arch installs.
blackbox-scanner	4:1.7a25220	Dork scanner & bruteforcing & hash cracker tool with blackbox penetration testing framework.
blackeye	1:v2.0.r0.g27a3f04	The most complete Phishing Tool, with 32 templates +1 customizable.
blackhash	0.2	Creates a filter from system hashes
blacknurse	9.d2a2b23	A low bandwidth ICMP attack that is capable of doing denial of service to well known firewalls.
bleah	53.6a2fd3a	A BLE scanner for "smart" devices hacking.
bless	0.6.3	Gtk# Hex Editor.
bletchley	0.0.1	A collection of practical application cryptanalysis tools.
blind-sql-bitshifting	54.5bbc183	A blind SQL injection module that uses bitshfting to calculate characters.
blindelephant	7	A web application fingerprinter. Attempts to discover the version of a (known) web application by comparing static files at known locations
blindsql	1.0	Set of bash scripts for blind SQL injection attacks.
blindy	12.59de8f2	Simple script to automate brutforcing blind sql injection vulnerabilities.
blisqy	20.e9995fc	Exploit Time-based blind-SQL injection in HTTP-Headers

		(MySQL/MariaDB).
bloodhound	1534.69786fa	Six Degrees of Domain Admin
bloodhound-python	v1.0.1.r104.g760e6ee	Bloodhound python data collector
bloodyad	158.b0cee6b	An Active Directory Privilege Escalation Framework.
blue-hydra	710.1c2372d	A Bluetooth device discovery service built on top of the bluez library.
bluebox-ng	1:1.1.0	A GPL VoIP/UC vulnerability scanner.
bluebugger	0.1	An implementation of the bluebug technique which was discovered by Martin Herfurt.
bluediving	0.9	A Bluetooth penetration testing suite.
bluefog	0.0.4	A tool that can generate an essentially unlimited number of phantom Bluetooth devices.
bluelog	1.1.2	A Bluetooth scanner and sniffer written to do a single task, log devices that are in discoverable mode.
bluepot	0.2	A Bluetooth Honeypot written in Java, it runs on Linux
blueprint	0.1_3	A perl tool to identify Bluetooth devices.
blueranger	1.0	A simple Bash script which uses Link Quality to locate Bluetooth device radios.
bluescan	1.0.6	A Bluetooth Device Scanner.
bluesnarfer	0.1	A bluetooth attacking tool
bluffy	47.180ed5b	Convert shellcode into different formats.
bluphish	9.a7200bd	Bluetooth device and service discovery tool that can be used for security assessment and penetration testing.
bluto	1:142.25cad7a	Recon, Subdomain Bruting, Zone Transfers.
bmap-tools	3.6	Tool for copying largely sparse files using information from a block map file.
bmc-tools	25.c66a657	RDP Bitmap Cache parser.
bob-the-butcher	0.7.1	A distributed password cracker package.
bof-detector	19.e08367d	A simple detector of BOF vulnerabilities by source-code-level check.
bokken	1:1.8	GUI for radare2 and pyew.
bonesi	12.733c9e9	The DDoS Botnet Simulator.
boofuzz	v0.4.1.r42.gb23f270	

boopsuite	170.16c902f	A Suite of Tools written in Python for wireless auditing and security testing.
bopscrk	1:v2.4.5.r9.g5fdb5bb	bopscrk (Before Outset PaSsword CRacKing) is a tool to generate smart and powerful wordlists for targeted attacks.
botb	69.6d33aae	A container analysis and exploitation tool for pentesters and engineers.
bowcaster	230.17d69c1	A framework intended to aid those developing exploits.
box-js	509.bdca8ea	A tool for studying JavaScript malware.
bqm	v1.3.0.r3.g055f66f	Download BloudHound query lists, deduplicate entries and merge them in one file.
braa	0.82	A mass snmp scanner
braces	0.4	A Bluetooth Tracking Utility.
brakeman	1:v5.4.1.r0.g0bc31d9fd	A static analysis security vulnerability scanner for Ruby on Rails applications
bridgekeeper	57.55c390c	Scrape employee names from search engine LinkedIn profiles. Convert employee names to a specified username format.
bro	2.6.4	A powerful network analysis framework that is much different from the typical IDS you may know.
bro-aux	451.a98acb8	Handy auxiliary programs related to the use of the Bro Network Security Monitor (https://www.bro.org/).
brosec	278.c51164f	An interactive reference tool to help security professionals utilize useful payloads and commands.
browselist	1.4	Retrieves the browse list ; the output list contains computer names, and the roles they play in the network.
browser-fuzzer	3	Browser Fuzzer 3
brut3k1t	104.793821f	Brute-force attack that supports multiple protocols and services.
brute-force	52.78d1d8e	Brute-Force attack tool for Gmail, Hotmail, Twitter, Facebook, Netflix.
brute12	1	A tool designed for auditing the cryptography container security in PKCS12 format.
bruteforce-luks	46.a18694a	Try to find the password of a LUKS encrypted volume.
bruteforce-salted-openssl	55.23e3a72	Try to find the password of a file that was encrypted with the 'openssl' command.
bruteforce-wallet	39.f6d8cc5	Try to find the password of an encrypted Peercoin (or Bitcoin,Litecoin, etc...) wallet file.

brutemap	65.da4b303	Penetration testing tool that automates testing accounts to the site's login page.
brutespray	203.f282627	Brute-Forcing from Nmap output - Automatically attempts default creds on found services.
brutessh	0.6	A simple sshd password bruteforcer using a wordlist, it's very fast for internal networks. It's multithreads.
brutex	112.23f511c	Automatically brute force all services running on a target.
brutexss	54.ba753df	Cross-Site Scripting Bruteforcer.
brutus	2	One of the fastest, most flexible remote password crackers you can get your hands on.
bsdiff	4.3	bsdiff and bspatch are tools for building and applying patches to binary files.
bsqlbf	2.7	Blind SQL Injection Brute Forcer.
bsqlinjector	13.027184f	Blind SQL injection exploitation tool written in ruby.
bss	0.8	Bluetooth stack smasher / fuzzer
bt_audit	0.1.1	Bluetooth audit
btcrack	1.1	The world's first Bluetooth Pass phrase (PIN) bruteforce tool. Bruteforces the Passkey and the Link key from captured Pairing exchanges.
btlejack	87.d0dd2df	Bluetooth Low Energy Swiss-army knife.
btproxy-mitm	71.cd1c906	Man in the Middle analysis tool for Bluetooth.
btscanner	2.1	Bluetooth device scanner.
bulk-extractor	1562.1c67a75	Bulk Email and URL extraction tool.
bully	1.1.12.g04185d7	A wifi-protected-setup (WPS) brute force attack tool.
bunny	0.93	A closed loop, high-performance, general purpose protocol-blind fuzzer for C programs.
burpsuite	1:2023.2.3	An integrated platform for attacking web applications (free edition).
buster	92.131437e	Find emails of a person and return info associated with them.
buttinsky	138.1a2a1b2	Provide an open source framework for automated botnet monitoring.
bvi	1.4.1	A display-oriented editor for binary files operate like "vi" editor.
byepass	213.8cbfd9b	Automates password cracking tasks using optimized dictionaries and mangling rules.
bypass-firewall-	33.c55b7ce	Firewall bypass script based on DNS history records.

dns-history		
bytecode-viewer	1:2.9.22	A Java 8/Android APK Reverse Engineering Suite.
c5scan	30.be8845c	Vulnerability scanner and information gatherer for the Concrete5 CMS.
cachedump	1.1	A tool that demonstrates how to recover cache entry information: username and hashed password (called MSCASH).
cadaver	0.24	Command-line WebDAV client for Unix
cafebabe	0.1.2	Java bytecode editor & decompiler.
cameradar	195.1b91e54	Hacks its way into RTSP videosurveillance cameras.
camover	73.abcded1	A camera exploitation tool that allows to disclosure network camera admin password.
camscan	1.0057215	A tool which will analyze the CAM table of Cisco switches to look for anamolies.
can-utils	946.cfe4196	Linux-CAN / SocketCAN user space applications.
canalyzat0r	41.6bc251e	Security analysis toolkit for proprietary car protocols.
canari	3.3.10	A transform framework for maltego
cangibrina	123.6de0165	Dashboard Finder.
cansina	2:59.67c6301	A python-based Web Content Discovery Tool.
cantoolz	1:425.82d330b	Framework for black-box CAN network analysis https://asintsov.blogspot.de/.
capfuzz	34.97ac312	Capture, fuzz and intercept web traffic.
capstone	4.0.2	A lightweight multi-platform, multi-architecture disassembly framework
captipper	74.3fb2836	Malicious HTTP traffic explorer tool.
cardpwn	32.166abf9	OSINT Tool to find Breached Credit Cards Information.
carwhisperer	0.2	Intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys.
casefile	1.0.1	The little brother to Maltego without transforms, but combines graph and link analysis to examine links between manually added data to mind map your information
catana	31.9ea1f0d	Filter your wordlist according to the specified password policy.
catnthecanary	7.e9184fe	An application to query the canary.pw data set for leaked data.
catphish	44.768d213	For phishing and corporate espionage.

ccrawldns	6.92525b6	Retrieves from the CommonCrawl data set unique subdomains for a given domain name.
cdpsnarf	0.1.6	Cisco discovery protocol sniffer.
cecster	5.15544cb	A tool to perform security testing against the HDMI CEC (Consumer Electronics Control) and HEC (HDMI Ethernet Channel) protocols.
centry	72.6de2868	Cold boot & DMA protection
cero	v1.3.0.r17.gcf826d0	Scrape domain names from SSL certificates of arbitrary hosts.
certgraph	172.465bddc	Crawl the graph of certificate Alternate Names.
certipy	4.4.0.r2.g74dcd97	Active Directory Certificate Services enumeration and abuse.
cewl	146.1c741bb	A custom word list generator
cflow	1.7	A C program flow analyzer.
cfr	0.152	Another Java decompiler.
chainsaw	v2.5.0.r1.gf8ef669	A powerful ‘first-response’ capability to quickly identify threats within Windows event logs.
chameleon	27.a2f0cf1	A tool for evading Proxy categorisation.
chameleonmini	606.791720c	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.
changeme	266.89f59d4	A default credential scanner.
chankro	21.7b6e844	Tool that generates a PHP capable of run a custom binary (like a meterpreter) or a bash script (p.e. reverse shell) bypassing disable_functions & open_basedir).
chaos-client	245.24dc2bf	Go client to communicate with Chaos dataset API.
chaosmap	1.3	An information gathering tool and dns / whois / web server scanner
chaosreader	0.94	A freeware tool to trace tcp, udp etc. sessions and fetch application data from snoop or tcpdump logs.
chapcrack	17.ae2827f	A tool for parsing and decrypting MS-CHAPv2 network handshakes.
cheat-sh	6	The only cheat sheet you need.
check-weak-dh-ssh	0.1	Debian OpenSSL weak client Diffie-Hellman Exchange checker.
checkiban	0.2	Checks the validity of an International Bank Account Number (IBAN).

checkpwd	1.23	Oracle Password Checker (Cracker).
checksec	2.6.0	Tool designed to test which standard Linux OS and PaX security features are being used
cheetah-suite	21.2364713	Complete penetration testing suite (port scanning, brute force attacks, services discovery, common vulnerabilities searching, reporting etc.)
chiasm-shell	33.e20ed9f	Python-based interactive assembler/disassembler CLI, powered byKeystone/Capstone.
chipsec	4:1743.505170ae	Framework for analyzing the security of PC platforms including hardware, system firmware (BIOS/UEFI), and platform components.
chiron	48.524abe1	An all-in-one IPv6 Penetration Testing Framework.
chisel	230.ce307e5	A fast TCP tunnel over HTTP.
chkrootkit	0.57	Checks for rootkits on a system
chntpw	140201	Offline NT Password Editor - reset passwords in a Windows NT SAM user database file
chopshop	444.8bdd393	Protocol Analysis/Decoder Framework.
choronzon	4.d702c31	An evolutionary knowledge-based fuzzer.
chownat	0.08b	Allows two peers behind two separate NATs with no port forwarding and no DMZ setup on their routers to directly communicate with each other
chrome-decode	0.1	Chrome web browser decoder tool that demonstrates recovering passwords.
chromefreak	24.12745b1	A Cross-Platform Forensic Framework for Google Chrome
chromensics	1.0	A Google chrome forensics tool.
chw00t	39.1fd1016	Unices chroot breaking tool.
cidr2range	1.0	Script for listing the IP addresses contained in a CIDR netblock
cintruder	14.f8a3f12	An automatic pentesting tool to bypass captchas.
cipherscan	419.c67f3ee	A very simple way to find out which SSL ciphersuites are supported by a target.
ciphertest	22.e33eb4a	A better SSL cipher checker using gnutls.
ciphr	127.5da7137	A CLI tool for encoding, decoding, encryption, decryption, and hashing streams of data.
cirt-fuzzer	1.0	A simple TCP/UDP protocol fuzzer.
cisco-auditing-tool	1	Perl script which scans cisco routers for common vulnerabilities. Checks for default passwords, easily guessable community names, and the IOS

		history bug. Includes support for plugins and scanning multiple hosts.
cisco-global-exploiter	1.3	A perl script that targets multiple vulnerabilities in the Cisco Internetwork Operating System (IOS) and Catalyst products.
cisco-ocs	0.2	Cisco Router Default Password Scanner.
cisco-router-config	1.1	copy-router-config and merge-router-config to copy and merge Cisco Routers Configuration
cisco-scanner	0.2	Multithreaded Cisco HTTP vulnerability scanner. Tested on Linux, OpenBSD and Solaris.
cisco-snmp-enumeration	10.ad06f57	Automated Cisco SNMP Enumeration, Brute Force, Configuration Download and Password Cracking.
cisco-snmp-slap	5.daf0589	IP address spoofing tool in order to bypass an ACL protecting an SNMP service on Cisco IOS devices.
cisco-torch	0.4b	Cisco Torch mass scanning, fingerprinting, and exploitation tool.
cisco5crack	2.c4b228c	Crypt and decrypt the cisco enable 5 passwords.
cisco7crack	2.f1c21dd	Crypt and decrypt the cisco enable 7 passwords.
ciscos	1.3	Сканирует сети классов A, B и C в поисках роутеров cisco с открытым портом telnet и неизменённым заводским паролем от cisco.
citadel	95.3b1adbc	A library of OSINT tools.
cjexploiter	6.72b08d8	Drag and Drop ClickJacking exploit development assistance tool.
clair	1638.d726e157	Vulnerability Static Analysis for Containers.
clairvoyance	2.0.6	Obtain GraphQL API Schema even if the introspection is not enabled.
clamscanlogparser	1	This is a utility to parse a Clam Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your malware collection.
clash	1.15.1	A rule-based tunnel in Go.
climber	30.5530a78	Check UNIX/Linux systems for privilege escalation.
cloakify	117.f45c3b3	Data Exfiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of Analysts; Evade AV Detection.
cloud-buster	194.b55e4a1	A tool that checks Cloudflare enabled sites for origin IP leaks.
cloudfail	79.7982c7d	Utilize misconfigured DNS and old database records to find hidden IP's behind the CloudFlare network.
cloudflare-enum	10.412387f	Cloudflare DNS Enumeration Tool for Pentesters.
cloudget	64.cba10b1	Python script to bypass cloudflare from command line. Built upon

		cfscrape module.
cloudlist	342.29bacea	A tool for listing Assets from multiple Cloud Providers.
cloudmare	102.032a1ab	A simple tool to find origin servers of websites protected by CloudFlare with a misconfiguration DNS.
cloudsploit	3790.3d5f72d4	AWS security scanning checks.
cloudunflare	14.b91a8a7	Reconnaissance Real IP address for Cloudflare Bypass.
clusterd	143.d190b2c	Automates the fingerprinting, reconnaissance, and exploitation phases of an application server attack.
cminer	25.d766f7e	A tool for enumerating the code caves in PE files.
cmospwd	5.1	Decrypts password stored in CMOS used to access BIOS setup.
cms-explorer	15.23b58cd	Designed to reveal the specific modules, plugins, components and themes that various cms driven websites are running
cms-few	0.1	Joomla, Mambo, PHP-Nuke, and XOOPS CMS SQL injection vulnerability scanning tool written in Python.
cmseek	362.5992739	CMS (Content Management Systems) Detection and Exploitation suite.
cmsfuzz	5.6be5a98	Fuzzer for wordpress, cold fusion, drupal, joomla, and phpnuke.
cmsmap	1:8.59dd0e2	A python open source Content Management System scanner that automates the process of detecting security flaws of the most popular CMSs.
cmsscan	43.f060b4b	CMS scanner to identify and find vulnerabilities for Wordpress, Drupal, Joomla, vBulletin.
cmsscanner	0.13.8.26.g12775a6	CMS Scanner Framework.
cnamulator	5.4667c68	A phone CNAM lookup utility using the OpenCNAM API.
cntlm	4.b35d55c	An NTLM, NTLM2SR, and NTLMv2 authenticating HTTP proxy.
codeql	1:2.8.1	The CLI tool for GitHub CodeQL
codetective	45.52b91f1	A tool to determine the crypto/encoding algorithm used according to traces of its representation.
coercer	1.6	Coerce a Windows server to authenticate on an arbitrary machine through 9 methods.
comission	203.67b890e	WhiteBox CMS analysis.
commentor	19.d81a660	Extract all comments from the specified URL resource.
commix	1965.ae94360c	Automated All-in-One OS Command Injection and Exploitation Tool.

commonspeak	36.f0aad23	Leverages publicly available datasets from Google BigQuery to generate wordlists.
complemento	0.7.6	A collection of tools for pentester: LetDown is a powerful tcp flooder ReverseRaider is a domain scanner that use wordlist scanning or reverse resolution scanning Httsquash is an http server scanner, banner grabber and data retriever
compp	1.0.5	Company Passwords Profiler helps making a bruteforce wordlist for a targeted company.
configpush	0.8.5	This is a tool to span /8-sized networks quickly sending snmpset requests with default or otherwise specified community string to Cisco devices.
conpot	0.6.0	ICS honeypot with the goal to collect intelligence about the motives and methods of adversaries targeting industrial control systems url="http://conpot.org"
conscan	1.2	A blackbox vulnerability scanner for the Concre5 CMS.
cook	238.8f8b958	Easily create word's permutation and combination to generate complex wordlists and passwords.
cookie-cadger	1.08	An auditing tool for Wi-Fi or wired Ethernet connections.
corkscrew	2.0	A tool for tunneling SSH through HTTP proxies
corscanner	99.593043f	Fast CORS misconfiguration vulnerabilities scanner.
corstest	10.beffd0b	A simple CORS misconfigurations checker.
corsy	69.2985ae2	CORS Misconfiguration Scanner.
cottontail	93.b7f5222	Capture all RabbitMQ messages being sent through a broker.
cowpatty	4.8	Wireless WPA/WPA2 PSK handshake cracking utility
cpfinder	0.1	This is a simple script that looks for administrative web interfaces.
cpp2il	1:2022.0.7.r11.gdc9dcd9	A tool to reverse unity's IL2PP toolchain
cppcheck	2.10.3	A tool for static C/C++ code analysis
cpptest	2.0.0	A portable and powerful, yet simple, unit testing framework for handling automated tests in C++.
cr3dov3r	46.99a1660	Search for public leaks for email addresses + check creds against 16 websites.
crabstick	47.bb7827f	Automatic remote/local file inclusion vulnerability analysis and exploit tool.
cracken	v1.0.1.r0.g7a3	A ast password wordlist generator, Smartlist creation and password

	25ff	hybrid-mask analysis tool written in pure safe Rust.
crackhor	2.ae7d83f	A Password cracking utility.
crackle	111.d83b4b6	Crack and decrypt BLE encryption
crackmapexec	2:v5.4.0.r30.gd2ea13f	A swiss army knife for pentesting Windows/Active Directory environments.
crackq	48.89b7318	Hashcrack.org GPU-accelerated password cracker.
crackql	1.0.r51.ge96af25	GraphQL password brute-force and fuzzing utility
crackserver	33.e5763ab	An XMLRPC server for password cracking.
crawlic	51.739fe2b	Web recon tool (find temporary files, parse robots.txt, search folders, google dorks and search domains hosted on same server).
creak	40.52b0d74	Poison, reset, spoof, redirect MITM script.
create_ap	265.462c09f	A shell script to create a NATed/Bridged Software Access Point
creddump	3.ed95e1a	A python tool to extract various credentials and secrets from Windows registry hives.
credmap	116.d862247	The Credential mapper - Tool that was created to bring awareness to the dangers of credential reuse.
creds	1:17.1ec8297	Harvest FTP/POP/IMAP/HTTP/IRC credentials along with interesting data from each of the protocols.
credsniper	21.f52461b	Phishing framework written with the Python micro-framework Flask and Jinja2 templating which supports capturing 2FA tokens.
creepy	1:137.9f60449	A geolocation information gatherer. Offers geolocation information gathering through social networking platforms.
cribdrag	5.2d27dbf	An interactive crib dragging tool for cryptanalysis on ciphertext generated with reused or predictable stream cipher keys.
crlf-injector	9.bd6db06	A python script for testing CRLF injecting issues.
crlfuzz	62.7a442bb	A fast tool to scan CRLF vulnerability written in Go.
crosslinked	1:19.786ad1c	LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping.
crosstool-ng	1.25.0	Versatile (cross-)toolchain generator.
crowbar	111.4b563dc	A brute forcing tool that can be used during penetration tests. It is developed to support protocols that are not currently supported by thc-hydra and other popular brute forcing tools.

crozono	1:5.6a51669	A modular framework designed to automate the penetration testing of wireless networks from drones and such unconventional devices.
crunch	3.6	A wordlist generator for all combinations/permutations of a given character set.
crypthook	18.690dcae	TCP/UDP symmetric encryption tunnel wrapper.
cryptonark	0.5.7	SSL security checker.
csrftester	1.0	The OWASP CSRFTester Project attempts to give developers the ability to test their applications for CSRF flaws.
ct-exposer	24.71252ac	An OSINT tool that discovers sub-domains by searching Certificate Transparency logs
ctf-party	v2.3.0.r22.ga5be46a	A CLI tool & library to enhance and speed up script/exploit writing for CTF players.
ctunnel	0.7	Tunnel and/or proxy TCP or UDP connections via a cryptographic tunnel.
ctypes-sh	153.6982e6c	Allows you to call routines in shared libraries from within bash.
cuckoo	2.0.7	A malware analysis system.
cupp	77.56547fd	Common User Password Profiler
cutycapt	3:10	A Qt and WebKit based command-line utility that captures WebKit's rendering of a web page.
cve-api	170.8e9c247	Unofficial api for cve.mitre.org.
cve-search	v4.2.1.r31.g1f0b50a	A tool to perform local searches for known vulnerabilities.
cvechecker	4.0	The goal of cvechecker is to report about possible vulnerabilities on your system, by scanning the installed software and matching the results with the CVE database.
cybercrowl	111.f7cac52	A Python Web path scanner tool.
cyberscan	75.ca85794	A Network Pentesting Tool
cymothoa	1	A stealth backdooring tool, that inject backdoor's shellcode into an existing process.
d-tect	13.9555c25	Pentesting the Modern Web.
dagon	244.f065d7b	Advanced Hash Manipulation.
dalfox	1251.a953704	Parameter Analysis and XSS Scanning tool.
damm	32.60e7ec7	Differential Analysis of Malware in Memory.
Damn	v1.9	Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application

Vulnerable Web App (DVWA)		that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
daredevil	42.81cb57f	A tool to perform (higher-order) correlation power analysis attacks (CPA).
dark-dork-searcher	1.0	Dark-Dork Searcher.
darkarmour	4.f10228a	Store and execute an encrypted windows binary from inside memory, without a single bit touching disk.
darkbing	0.1	A tool written in python that leverages bing for mining data on systems that may be susceptible to SQL injection.
darkd0rk3r	1.0	Python script that performs dork searching and searches for local file inclusion and SQL injection errors.
darkdump	43.40abd92	Search The Deep Web Straight From Your Terminal.
darkjumper	5.8	This tool will try to find every website that host at the same server at your target.
darkmysqli	1.6	Multi-Purpose MySQL Injection Tool
darkscrape	68.2ca0e37	OSINT Tool For Scraping Dark Websites.
darkspiritz	1:6.4d23e94	A penetration testing framework for Linux, MacOS, and Windows systems.
darkstat	3.0.721	Network statistics gatherer (packet sniffer)
dartspylru	7.5ef01b1	Simple dictionary with LRU behaviour.
datajackproxy	42.f75f3a3	A proxy which allows you to intercept TLS traffic in native x86 applications across platform.
datasploit	1:367.a270d50	A tool to perform various OSINT techniques, aggregate all the raw data, visualize it on a dashboard, and facilitate alerting and monitoring on the data.
davoset	1.3.7	A tool for using Abuse of Functionality and XML External Entities vulnerabilities on some websites to attack other websites.
davscan	30.701f967	Fingerprints servers, finds exploits, scans WebDAV.
davtest	3.a282c58	Tests WebDAV enabled servers by uploading test executable files, and then (optionally) uploading files which allow for command execution or other actions directly on the target

dawnscanner	1:v2.0.0.rc4.r0.gd6150be	A static analysis security scanner for ruby written web applications.
dbd	61.8cf5350	A Netcat-clone, designed to be portable and offer strong encryption. It runs on Unix-like operating systems and on Microsoft Win32.
dbpwaudit	0.8	A Java tool that allows you to perform online audits of password quality for several database engines.
dbusmap	16.6bb2831	This is a simple utility for enumerating D-Bus endpoints, an nmap for D-Bus.
dc3dd	7.2.646	A patched version of dd that includes a number of features useful for computer forensics.
dcdetector	0.0.1.r7.g7b859c5	Spot all domain controllers in a Microsoft Active Directory environment. Find computer name, FQDN, and IP address(es) of all DCs.
dcfldd	1.7.1	DCFL (DoD Computer Forensics Lab) dd replacement with hashing
dcrawl	7.3273c35	Simple, but smart, multi-threaded web crawler for randomly gathering huge lists of unique domain names.
ddosify	v0.15.1.r0.ga24fcf9	High-performance load testing tool, written in Golang.
ddrescue	1.27	A data recovery tool. It copies data from one file or block device (hard disc, cdrom, etc) to another, trying to rescue the good parts first in case of read errors.
de4dot	3.1.41592	.NET deobfuscator and unpacker.
deathstar	59.f10fdbf	Automate getting Domain Admin using Empire.
debinject	43.d884309	Inject malicious code into *.debs.
deblaze	1:1.0608dc3	A remote method enumeration tool for flex servers
decodify	50.76a0801	Tool that can detect and decode encoded strings, recursively.
deen	601.fd9aebe	Generic data encoding/decoding application built with PyQt5.
deepce	108.934a991	Docker Enumeration, Escalation of Privileges and Container Escapes.
delldrac	0.1a	DellDRAC and Dell Chassis Discovery and Brute Forcer.
delorean	16.0291151	NTP Main-in-the-Middle tool.
demiguise	11.58d5681	HTA encryption tool for RedTeams.
densityscout	45	Calculates density for files of any file-system-path to finally output an accordingly descending ordered list.
depant	0.3a	Check network for services with default passwords.

depdep	2.0	A merciless sentinel which will seek sensitive files containing critical info leaking through your network.
dependency-check	6.5.3	A tool that attempts to detect publicly disclosed vulnerabilities contained within a project's dependencies.
depix	38.f7d1850	A tool for recovering passwords from pixelized screenshots.
der-ascii	84.031bca8	A reversible DER and BER pretty-printer.
det	31.417cbce	(extensible) Data Exfiltration Toolkit.
detect-it-easy	1:3.02	A program for determining types of files.
detect-secrets	v1.4.0.r10.g4495a0	An enterprise friendly way of detecting and preventing secrets in code.
detect-sniffer	151.63f0d7f	Tool that detects sniffers in the network.
detectem	276.bc5f073	Detect software and its version on websites.
devaudit	803.ca0a68e	An open-source, cross-platform, multi-purpose security auditing tool targeted at developers and teams.
device-pharmer	40.b06a460	Opens 1K+ IPs or Shodan search results and attempts to login.
dex2jar	2.1	A tool for converting Android's .dex format to Java's .class format
dexpatcher	1.7.0	Modify Android DEX/APK files at source-level using Java.
dff	183.d40d46b	A Forensics Framework coming with command line and graphical interfaces.
dff-scanner	1.1	Tool for finding path of predictable resource locations.
dfir-ntfs	1.1.13	An NTFS parser for digital forensics & incident response.
dftimewolf	585.c4241a78	Framework for orchestrating forensic collection, processing and data export .
dga-detection	78.0a3186e	DGA Domain Detection using Bigram Frequency Analysis.
dharma	98.6b1e511	Generation-based, context-free grammar fuzzer.
dhcdrop	0.5	Remove illegal dhcp servers with IP-pool underflow.
dhcpf	3.a770b20	Passive DHCP fingerprinting implementation.
dhcpig	2:92.9fd8df5	Enhanced DHCPv4 and DHCPv6 exhaustion and fuzzing script written in python using scapy network library.
dhcpoptinj	123.58a12c6	DHCP option injector.
didier-stevens-suite	361.a03e58e	Didier Stevens Suite.
dinouml	0.9.5	A network simulation tool, based on UML (User Mode Linux) that can

		simulate big Linux networks on a single PC
dirb	2.22	A web content scanner, brute forceing for hidden files.
dirble	1:1.4.2	Fast directory scanning and scraping tool.
dirbuster	1.0_RC1	An application designed to brute force directories and files names on web/application servers
dirbuster-ng	9.0c34920	C CLI implementation of the Java dirbuster tool.
directorytraversalscan	1.0.1.0	Detect directory traversal vulnerabilities in HTTP servers and web applications.
dirhunt	298.57bfd58	Find web directories without bruteforce.
dirscanner	0.1	This is a python script that scans webservers looking for administrative directories, php shells, and more.
dirscraper	16.e752450	OSINT Scanning tool which discovers and maps directories found in javascript files hosted on a website.
dirsearch	2288.0a18692	HTTP(S) directory/file brute forcer.
dirstalk	1.3.3	Dirstalk is a multi threaded application designed to brute force paths on web servers. The tool contains functionalities similar to the ones offered by dirbuster and dirb.
disitool	0.4	Tool to work with Windows executables digital signatures.
dislocker	564.3a8f757	A tool to exploit the hash length extension attack in various hashing algorithms. With FUSE capabilities built in.
dissector	1	This code dissects the internal data structures in ELF files. It supports x86 and x86_64 archs and runs under Linux.
distorm	3.5.2.b	Powerful disassembler library for x86/AMD64
dive	0.10.0	A tool for exploring each layer in a docker image.
dizzy	2.0	A Python based fuzzing framework with many features.
dkmc	56.3c238f0	Dont kill my cat - Malicious payload evasion tool.
dmde	3.8.0.790	Disk Editor and Data Recovery Software.
dmg2img	1.6.7	Convert a (compressed) Apple Disk Images. A CLI tool to uncompress Apple's compressed DMG files to the HFS+ IMG format A CLI tool to uncompress Apple's compressed DMG files to the HFS+ IMG format
dmitry	1.3a	Deepmagic Information Gathering Tool. Gathers information about hosts. It is able to gather possible subdomains, email addresses, and uptime information and run tcp port scans, whois lookups, and more.

dnmap	0.6	The distributed nmap framework
dns-parallel-prober	68.422db61	PoC for an adaptive parallelised DNS prober.
dns-reverse-proxy	36.937d3d2	A reverse DNS proxy written in Go.
dns-spoof	13.81ba29f	Yet another DNS spoof utility.
dns2geoip	0.1	A simple python script that brute forces DNS and subsequently geolocates the found subdomains.
dns2tcp	0.5.2	A tool for relaying TCP connections over DNS.
dnsa	0.6	DNSA is a dns security swiss army knife
dnsbf	0.3	Search for available domain names in an IP range.
dnsbrute	2.b1dc84a	Multi-theaded DNS bruteforcing, average speed 80 lookups/second with 40 threads.
dnscan	208.2e23323	A python wordlist-based DNS subdomain scanner.
dnschef	17.a395411	A highly configurable DNS proxy for pentesters.
dnscobra	1.0	DNS subdomain bruteforcing tool with Tor support through torsocks
dnsdiag	292.1f94ad7	DNS Diagnostics and Performance Measurement Tools.
dnsdrdos	0.1	Proof of concept code for distributed DNS reflection DoS.
dnsenum	1.2.4.2	Script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
dnsfilexfer	24.126edcd	File transfer via DNS.
dnsgoblin	1:0.1	Nasty creature constantly searching for DNS servers. It uses standard dns queries and waits for the replies.
dnsgrep	14.3f4fa7c	A utility for quickly searching presorted DNS names.
dnsmap	0.30	Passive DNS network mapper
dnsobserver	5.f331482	A handy DNS service written in Go to aid in the detection of several types of blind vulnerabilities.
dnspredict	0.0.2	DNS prediction.
dnsprobe	56.7120008	Allows you to perform multiple dns queries of your choice with a list of user supplied resolvers.
dnspy	6.1.8	.NET debugger and assembly editor.
dnsrecon	2:1.1.4	Python script for enumeration of hosts, subdomains and emails from a

		given domain using google.
dnssearch	20.e4ea439	A subdomain enumeration tool.
dnsspider	1.3	A very fast multithreaded bruteforcer of subdomains that leverages a wordlist and/or character permutation.
dnsteal	28.1b09d21	DNS Exfiltration tool for stealthily sending files over DNS requests..
dnstracer	1.10	Determines where a given DNS server gets its information from, and follows the chain of DNS servers
dnstwist	574.dbe2b56	Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
dnsvalidator	82.146c9b0	Maintains a list of IPv4 DNS servers by verifying them against baseline servers, and ensuring accurate responses.
dnswalk	2.0.2	A DNS debugger.
dnsx	474.1ed65d8	Fast and multi-purpose DNS toolkit allow to run multiple DNS queries of your choice with a list of user-supplied resolvers.
docem	20.b0ddd87	Uility to embed XXE and XSS payloads in docx,odt,pptx,etc (OXML_XEE on steroids).
dockerscan	59.590a844	Docker security analysis & hacking tools.
domain-analyzer	0.8.1	Finds all the security information for a given domain name.
domain-stats	165.1cf05bf	A web API to deliver domain information from whois and alexa.
domained	80.d9d079c	Multi Tool Subdomain Enumeration.
domainhunter	51.38cb7ef	Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names.
domato	123.8083920	DOM fuzzer.
domi-owned	41.583d0a5	A tool used for compromising IBM/Lotus Domino servers.
domlink	37.1cabd5d	A tool to link a domain with registered organisation names and emails, to other domains.
dontgo403	0.7.r12.g9b6f590	Tool to bypass 40X response codes..
donut	501.61af8cc	Generates x86, x64 or AMD64+x86 P.I. shellcode loading .NET Assemblies from memory.
doona	145.7a4796c	A fork of the Bruteforce Exploit Detector Tool (BED).
doork	6.90c7260	Passive Vulnerability Auditor.

doozer	9.5cfc8f8	A Password cracking utility.
dorkbot	186.8d9df3c	Command-line tool to scan Google search results for vulnerabilities.
dorkme	57.0a7017a	Tool designed with the purpose of making easier the searching of vulnerabilities with Google Dorks, such as SQL Injection vulnerabilities.
dorknet	58.419d6a2	Selenium powered Python script to automate searching for vulnerable web apps.
dorkscout	1.0.r13.gdd87daf	Golang tool to automate google dork scan against the entire internet or specific targets.
dotdotpwn	3.0.2	The Transversal Directory Fuzzer
dotpeek	2021.3.3	Free .NET Decompiler and Assembly Browser.
dpeparser	1:beta002	Default password enumeration project
dpscan	0.1	Drupal Vulnerabilty Scanner.
dr-checker	140.ea63c0f	A Soundy Vulnerability Detection Tool for Linux Kernel Drivers.
dr0p1t-framework	44.db9bc2d	A framework that creates a dropper that bypass most AVs, some sandboxes and have some tricks.
dracnmap	69.09d3945	Tool to exploit the network and gathering information with nmap help.
dradis	3.0.0.rc1	An open source framework to enable effective information sharing.
dradis-ce	5575.ed72071c	An open source framework to enable effective information sharing.
dragon-backdoor	7.c7416b7	A sniffing, non binding, reverse down/exec, portknocking service Based on cd00r.c.
driftnet	1:v1.3.0.r13.ge492335	Listens to network traffic and picks out images from TCP streams it observes.
drinkme	19.acf1a14	A shellcode testing harness.
dripcap	0.6.15	Caffeinated Packet Analyzer.
dripper	v1.r1.gc9bb0c9	A fast, asynchronous DNS scanner; it can be used for enumerating subdomains and enumerating boxes via reverse DNS.
droopescan	1.45.1	A plugin-based scanner that aids security researchers in identifying issues with several CMSs, mainly Drupal & Silverstripe.
drozer	2.4.4	A security testing framework for Android - Precompiled binary from official repository.
drupal-module-enum	11.525543c	Enumerate on drupal modules.

drupalscan	0.5.2	Simple non-intrusive Drupal scanner.
drupwn	1:59.8186732	Drupal enumeration & exploitation tool.
dscanner	0.14.0	Swiss-army knife for D source code.
dsd	91.7ee04e5	Digital Speech Decoder
dsfs	36.8e9f8e9	A fully functional File inclusion vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.
dshell	142.695c891	A network forensic analysis framework.
dsjs	32.26287d0	A fully functional JavaScript library vulnerability scanner written in under 100 lines of code.
dsniff	2.4b1	Collection of tools for network auditing and penetration testing
dsss	123.84ddd33	A fully functional SQL injection vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.
dsstore-crawler	6.524117b	A parser + crawler for .DS_Store files exposed publically.
dsxs	130.3e628b6	A fully functional Cross-site scripting vulnerability scanner (supporting GET and POST parameters) written in under 100 lines of code.
dtp-spoof	5.3ae05fc	Python script/security tool to test Dynamic Trunking Protocol configuration on a switch.
dublin-traceroute	338.600c6ea	NAT-aware multipath tracerouting tool.
ducktoolkit	37.42da733	Encoding Tools for Rubber Ducky.
dudley	16.ea14ca6	Block-based vulnerability fuzzing framework.
dumb0	19.1493e74	A simple tool to dump users in popular forums and CMS.
dump1090	386.bff92c4	A simple Mode S decoder for RTLSDR devices.
dumpacl	1:0.1	Dumps NTs ACLs and audit settings.
dumpsmbshare	21.9fd4d5b	A script to dump files and folders remotely from a Windows SMB share.
dumpusers	1.0	Dumps account names and information even though RestrictAnonymous has been set to 1.
dumpzilla	03152013	A forensic tool for firefox.
duplicut	2.2	Remove duplicates from massive wordlist, without sorting it (for dictionnary-based password cracking).
dutas	10.37fa3ab	Analysis PE file or Shellcode.
dvcs-ripper	54.2c1bbc6	Rip web accessible (distributed) version control systems: SVN/GIT/...
dwarf	1082.cdf85f4	Full featured multi arch/os debugger built on top of PyQt5 and frida.

dynamorio	9.0.19046	DynamoRIO is a runtime code manipulation system that supports code transformations on any part of a program, while it executes.
eapeak	130.9550d1c	Analysis Suite For EAP Enabled Wireless Networks.
eaphammer	273.e8d1ff8	Targeted evil twin attacks against WPA2-Enterprise networks. Indirect wireless pivots using hostile portal attacks.
eapmd5pass	3.3d5551f	An implementation of an offline dictionary attack against the EAP-MD5 protocol
easy-creds	45.bf9f00c	A bash script that leverages ettercap and other tools to obtain credentials.
easyda	7.0867f9b	Easy Windows Domain Access Script.
easyfuzzer	3.6	A flexible fuzzer, not only for web, has a CSV output for efficient output analysis (platform independant).
eazy	0.1	This is a small python tool that scans websites to look for PHP shells, backups, admin panels, and more.
ecfs	305.1758063	Extended core file snapshot format.
edb	3247.4c824664	A QT4-based binary mode debugger with the goal of having usability on par with OllyDbg.
eggshell	157.eaeeea7	iOS/macOS/Linux Remote Administration Tool.
eigrp-tools	0.1	This is a custom EIGRP packet generator and sniffer developed to test the security and overall operation quality of this brilliant Cisco routing protocol.
eindeutig	20050628_1	Examine the contents of Outlook Express DBX email repository files (forensic purposes)
electric-fence	2.2.5	A malloc(3) debugger that uses virtual memory hardware to detect illegal memory accesses.
elettra	1.0	Encryption utility by Julia Identity
elettra-gui	1.0	Gui for the elettra crypto application.
elevate	27.1272d51	Horizontal domain discovery tool you can use to discover other domains owned by a given company.
elfkickers	3.2	Collection of ELF utilities (includes sstrip)
elfparser	7.39d21ca	Cross Platform ELF analysis.
elfutils	0.189	Utilities to handle ELF object files and DWARF debugging information.
elidecode	48.38fa5ba	A tool to decode obfuscated shellcodes using the unicorn-engine for the emulation and the capstone-engine to print the asm code.

elite-proxy-finder	51.1ced3be	Finds public elite anonymity proxies and concurrently tests them.
email2phonenumber	29.9df9dbe	A OSINT tool to obtain a target's phone number just by having his email address.
emldump	0.0.11	Analyze MIME files.
emp3r0r	v1.23.0.r1.g3621842	Linux post-exploitation framework made by linux user.
empire	2:3086.ce3fdeca	A PowerShell and Python post-exploitation agent.
enabler	1	Attempts to find the enable password on a cisco system via brute force.
encodeshellcode	0.1b	This is an encoding tool for 32-bit x86 shellcode that assists a researcher when dealing with character filter or byte restrictions in a buffer overflow vulnerability or some kind of IDS/IPS/AV blocking your code.
ent	1.0	Pseudorandom number sequence test.
enteletaor	66.e8e4daa	Message Queue & Broker Injection tool that implements attacks to Redis, RabbitMQ and ZeroMQ.
entropy	702.13aac50	A set of tools to exploit Netwave and GoAhead IP Webcams.
enum-shares	7.97cba5a	Tool that enumerates shared folders across the network and under a custom user account.
enum4linux	0.9.1	A tool for enumerating information from Windows and Samba systems.
enum4linux-ng	400.5729ab8	A next generation version of enum4linux.
enumerate-iam	14.4529114	Enumerate the permissions associated with an AWS credential set.
enumerid	30.5311fd8	Enumerate RIDs using pure Python.
enumiax	1.0	An IAX enumerator.
enyelkm	1.2	Rootkit for Linux x86 kernels v2.6.
eos	14.0127319	Enemies Of Symfony - Debug mode Symfony looter.
epicwebhoneypot	2.0a	Tool which aims to lure attackers using various types of web vulnerability scanners by tricking them into believing that they have found a vulnerability on a host.
erase-registrations	1.0	An IAX flooder.
eraser	6.2.0.2992	Windows tool which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns.

eresi	1291.4769c175	The ERESI Reverse Engineering Software Interface.
erl-matter	51.a8bb204	Tool to exploit epmd related services such ass rabbitmp, ejabberd and couchdb by bruteforcing the cookie and gaining RCE afterwards.
espionage	1:45.1926d8a	A Network Packet and Traffic Interceptor For Linux. Sniff All Data Sent Through a Network.
eternal-scanner	91.4ba62ff	An internet scanner for exploit CVE-2017-0144 (Eternal Blue).
etherape	0.9.20	A graphical network monitor for various OSI layers and protocols
etherchange	1.1	Can change the Ethernet address of the network adapters in Windows.
etherflood	1.1	Floods a switched network with Ethernet frames with random hardware addresses.
ettercap	0.8.3.1	Ettercap is a comprehensive suite for man in the middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.
evil-ssdp	94.ee76fb0	Spoof SSDP replies to phish for NetNTLM challenge/response on a network.
evil-winrm	1:v3.4.r0.g381b126	The ultimate WinRM shell for hacking/pentesting.
evilclippy	62.fa610c6	A cross-platform assistant for creating malicious MS Office documents.
evilginx	2.4.0	Man-in-the-middle attack framework used for phishing credentials and session cookies of any web service.
evilginx2	59.5a477f7	Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication.
evilgrade	2.0.9	Modular framework that takes advantage of poor upgrade implementations by injecting fake updates
evilize	0.2	Tool to create MD5 colliding binaries.
evillimiter	36.46d2033	Tool that monitors, analyzes and limits the bandwidth of devices on the local network without administrative access.
evilmaid	1.01	TrueCrypt loader backdoor to sniff volume password
evilpdf	5.43696a8	Embedding executable files in PDF Documents.
evine	42.46051de	Interactive CLI Web Crawler.
evtkit	8.af06db3	Fix acquired .evt - Windows Event Log files (Forensics).

exabgp	5000.13314356	The BGP swiss army knife of networking.
exe2image	1.1	A simple utility to convert EXE files to JPEG images and vice versa.
exescan	1.ad993e3	A tool to detect anomalies in PE (Portable Executable) files.
exiflooter	33.a92e697	Find geolocation on all image urls and directories also integrates with OpenStreetMap.
exitmap	369.172e763	A fast and modular scanner for Tor exit relays.
exiv2	0.27.2	Exif, Iptc and XMP metadata manipulation library and tools
expimp-lookup	4.79a96c7	Looks for all export and import names that contain a specified string in all Portable Executable in a directory tree.
exploit-db	1.6	The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software - A collection of hacks
exploitdb	20221122	Offensive Security's Exploit Database Archive
exploitpack	139.e565c47	Exploit Pack - Project.
expose	1110.30264af	A Dynamic Symbolic Execution (DSE) engine for JavaScript
exrex	146.239e4da	Irregular methods on regular expressions. Exrex is a command line tool and python module that generates all - or random - matching strings to a given regular expression and more. It's pure python, without external dependencies.
extended-ssrf-search	28.680f815	Smart ssrf scanner using different methods like parameter brute forcing in post and get.
extracthosts	17.8fdff9e	Extracts hosts (IP/Hostnames) from files.
extractusnjrnl	7.362d4290	Tool to extract the $UsnJrnl from an NTFS volume.
extundelete	0.2.4	Utility for recovering deleted files from ext2, ext3 or ext4 partitions by parsing the journal
eyeballer	140.5b15ce7	Convolutional neural network for analyzing pentest screenshots.
eyepwn	1.0	Exploit for Eye-Fi Helper directory traversal vulnerability
eyewitness	1018.18a80a4	Designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
f-scrack	19.9a00357	A single file bruteforcer supports multi-protocol.
facebash	17.95c3c25	Facebook Brute Forcer in shellscript using TOR.
facebookosint	21.656a04a	OSINT tool to replace facebook graph search.
facebot	23.57f6025	A facebook profile and reconnaissance system.

facebrok	33.0f6fe8d	Social Engineering Tool Oriented to facebook.
facebrute	7.ece355b	This script tries to guess passwords for a given facebook account using a list of passwords (dictionary).
factordb-pycli	1.3.0	CLI for factordb and Python API Client.
fakeap	0.3.2	Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames.
fakedns	118.39609da	A regular-expression based python MITM DNS server with correct DNS request passthrough and "Not Found" responses.
fakemail	1.0	Fake mail server that captures e-mails as files for acceptance testing.
fakenet-ng	300.68da2d7	Next Generation Dynamic Network Analysis Tool.
fakenetbios	7.b83701e	A family of tools designed to simulate Windows hosts (NetBIOS) on a LAN.
fang	22.4f94552	A multi service threaded MD5 cracker.
faraday	9269.4625bd369	A new concept (IPE) Integrated Penetration-Test Environment a multiuser Penetration test IDE. Designed for distribution, indexation and analyze of the generated data during the process of a security audit.
faradaysec	11910.f56dfca36	Collaborative Penetration Test and Vulnerability Management Platform.
fastnetmon	v1.1.4.r62.g780aff3	High performance DoS/DDoS load analyzer built on top of multiple packet capture engines.
fav-up	54.089aa11	IP lookup by favicon using Shodan.
favfreak	26.a1ecf3b	Weaponizing favicon.ico for BugBounties , OSINT and what not.
fbht	1:70.d75ae93	A Facebook Hacking Tool
fbi	28.0f94e99	An accurate facebook account information gathering.
fbid	16.1b35eb9	Show info about the author by facebook photo url.
fcrackzip	1.0	Zip file password cracker
fdsploit	26.4522f53	A File Inclusion & Directory Traversal fuzzing, enumeration & exploitation tool.
featherduster	191.9229158	An automated, modular cryptanalysis tool.
fern-wifi-cracker	295.76c64b3	WEP, WPA wifi cracker for wireless penetration testing
fernflower	485.e19aab6	An analytical decompiler for Java.

fernmelder	6.c6d4ebe	Asynchronous mass DNS scanner.
feroxbuster	2.7.1.r11.g53e3420	A fast, simple, recursive content discovery tool written in Rust.
ffdec	11.0.0	Open source Flash SWF decompiler and editor.
ffm	60.ad691d4	A hacking harness that you can use during the post-exploitation phase of a red-teaming engagement.
ffuf	1:v2.0.0.r1.gb2c1f94	Fast web fuzzer written in Go.
ffuf-scripts	1.2192bf7	Scripts and snippets for ffuf payloads.
fgscanner	11.893372c	An advanced, opensource URL scanner.
fhttp	1.3	This is a framework for HTTP related attacks. It is written in Perl with a GTK interface, has a proxy for debugging and manipulation, proxy chaining, evasion rules, and more.
fi6s	172.8d5ddba	IPv6 network scanner designed to be fast.
fierce	134.99eca52	A DNS reconnaissance tool for locating non-contiguous IP space. A DNS scanner.
fiked	0.0.5	FakeIKEd, or fiked for short, is a fake IKE daemon supporting just enough of the standards and Cisco extensions to attack commonly found insecure Cisco VPN PSK+XAUTH based IPsec authentication setups in what could be described as a semi MitM attack. Fiked can impersonate a VPN gateway's IKE responder in order to capture XAUTH login credentials; it doesn't currently do the client part of full MitM.
filebuster	95.f2b04c7	An extremely fast and flexible web fuzzer.
filefuzz	1.0	A binary file fuzzer for Windows with several options.
filegps	90.03cbc75	A tool that help you to guess how your shell was renamed after the server-side script of the file uploader saved it.
fileintel	33.a0bff38	A modular Python application to pull intelligence about malicious files.
filibuster	167.c54ac80	A Egress filter mapping application with additional functionality.
fimap	2:1.00	A little tool for local and remote file inclusion auditing and exploitation. fimap is a little python tool which can find, prepare, audit, exploit and even google automaticly for local and remote file inclusion bugs in webapps.
finalrecon	123.2f64052	OSINT Tool for All-In-One Web Reconnaissance.
find-dns	0.1	A tool that scans networks looking for DNS servers.

find3	604.5964026	High-precision indoor positioning framework.
findmyhash	1.1.2	Crack different types of hashes using free online services
findmyiphone	19.aef3ac8	Locates all devices associated with an iCloud account
findomain	9.0.0	A tool that use Certificate Transparency logs to find subdomains.
findsploit	87.3e61d8d	Find exploits in local and online databases instantly.
fingerprinter	480.105ab04	CMS/LMS/Library etc Versions Fingerprinter.
firecat	6.b5205c8	A penetration testing tool that allows you to punch reverse TCP tunnels out of a compromised network.
firefox-decrypt	1.0.0.r40.gb4ecc96	Extract passwords from Mozilla Firefox, Waterfox, Thunderbird, SeaMonkey profiles.
firefox-security-toolkit	16.31dacf0	A tool that transforms Firefox browsers into a penetration testing suite.
firewalk	5.0	An active reconnaissance network security tool
firmwalker	101.23ff299	A simple bash script for searching the extracted or mounted firmware file system.
firmware-mod-kit	149.8403a17	Modify firmware images without recompiling.
firstexecution	6.a275793	A Collection of different ways to execute code outside of the expected entry points.
firstorder	8.107eb6a	A traffic analyzer to evade Empire communication from Anomaly-Based IDS.
fl0p	0.1	A passive L7 flow fingerprinter that examines TCP/UDP/ICMP packet sequences, can peek into cryptographic tunnels, can tell human beings and robots apart, and performs a couple of other infosec-related tricks.
flamerobin	2370.c75f8618	A tool to handle Firebird database management.
flare	0.6	Flare processes an SWF and extracts all scripts from it.
flare-floss	860.7138b61	Obfuscated String Solver - Automatically extract obfuscated strings from malware.
flashlight	109.90d1dc5	Automated Information Gathering Tool for Penetration Testers.
flashscanner	11.6815b02	Flash XSS Scanner.
flashsploit	23.c465a6d	Exploitation Framework for ATtiny85 Based HID Attacks.
flask-session-cookie-	v1.2.1.1.r11.g821b80c	Decode and encode Flask session cookie.

manager2		
flask-session-cookie-manager3	v1.2.1.1.r11.g821b80c	Decode and encode Flask session cookie.
flasm	1.62	Disassembler tool for SWF bytecode
flawfinder	2.0.19	Searches through source code for potential security flaws.
flowinspect	97.34759ed	A network traffic inspection tool.
flunym0us	2.0	A Vulnerability Scanner for Wordpress and Moodle.
fluxion	3:1568.081254b	A security auditing and social-engineering research tool.
flyr	76.4926ecc	Block-based software vulnerability fuzzing framework.
fockcache	10.3e7efa9	Tool to make cache poisoning by trying X-Forwarded-Host and X-Forwarded-Scheme headers on web pages.
forager	115.7439b0a	Multithreaded threat Intelligence gathering utilizing.
foremost	1.5.7	A console program to recover files based on their headers, footers, and internal data structures
foresight	57.6f48984	A tool for predicting the output of random number generators.
forkingportscanner	1	Simple and fast forking port scanner written in perl. Can only scan one host at a time, the forking is done on the specified port range. Or on the default range of 1-65535. Has the ability to scan UDP or TCP, defaults to tcp.
formatstringexploiter	29.8d64a56	Helper script for working with format string bugs.
fortiscan	0.7.r7.gd54faa0	A high performance FortiGate SSL-VPN vulnerability scanning and exploitation tool.
fpdns	2:108.2a898bf	Program that remotely determines DNS server versions.
fping	5.1	A utility to ping multiple hosts at once
fport	2.0	Identify unknown open ports and their associated applications.
fprotlogparser	1	This is a utility to parse a F-Prot Anti Virus log file, in order to sort them into a malware archive for easier maintanence of your collection.
fraud-bridge	10.775c563	ICMP and DNS tunneling via IPv4 and IPv6.
fred	0.1.1	Cross-platform M$ registry hive editor.
freeipmi	1.6.10	Sensor monitoring, system event monitoring, power control, and serial-

		over-LAN (SOL).
freeradius	3.2.2	The premier open source RADIUS server
freewifi	30.1cb752b	How to get free wifi.
frida	12.6.8	An interactive disassembler based on LLVM and Qt.
frida-extract	13.abb3f14	Frida.re based RunPE (and MapViewOfSection) extraction tool.
frida-ios-dump	53.56e99b2	Pull decrypted ipa from jailbreak device.
frida-ipa-dump	1:117.b9dcb91	Yet another frida based iOS dumpdecrypted.
frida-push	1.0.8	Wrapper tool to identify the remote device and push device specific frida-server binary
fridump	23.3e64ee0	A universal memory dumper using Frida.
frisbeelite	1.2	A GUI-based USB device fuzzer.
fs-exploit	3.28bb9bb	Format string exploit generation.
fs-nyarl	1.0	A network takeover & forensic analysis tool - useful to advanced PenTest tasks & for fun and profit.
fscan	1.8.1.r18.g38e48ba	A Security Auditing Tool.
fsnoop	3.4	A tool to monitor file operations on GNU/Linux systems by using the Inotify mechanism. Its primary purpose is to help detecting file race condition vulnerabilities and since version 3, to exploit them with loadable DSO modules (also called "payload modules" or "paymods").
fssb	73.51d2ac2	A low-level filesystem sandbox for Linux using syscall intercepts.
fstealer	0.1	Automates file system mirroring through remote file disclosure vulnerabilities on Linux machines.
ftester	1.0	A tool designed for testing firewall filtering policies and Intrusion Detection System (IDS) capabilities.
ftp-fuzz	1:1337	The master of all master fuzzing scripts specifically targeted towards FTP server sofware.
ftp-scanner	0.2.5	Multithreaded ftp scanner/brute forcer. Tested on Linux, OpenBSD and Solaris.
ftp-spider	1.0	FTP investigation tool - Scans ftp server for the following: reveal entire directory tree structures, detect anonymous access, detect directories with write permissions, find user specified data within repository.
ftpmap	52.cbeabbe	Scans remote FTP servers to identify what software and what versions they are running.

ftpscout	12.cf1dff1	Scans ftps for anonymous access.
fuddly	569.fd2c4d0	Fuzzing and Data Manipulation Framework (for GNU/Linux).
fusil	1.5	A Python library used to write fuzzing programs.
fuxploider	140.ec8742b	Tool that automates the process of detecting and exploiting file upload forms flaws.
fuzzap	17.057002b	A python script for obfuscating wireless networks.
fuzzball2	0.7	A little fuzzer for TCP and IP options. It sends a bunch of more or less bogus packets to the host of your choice.
fuzzbunch	32.2b76c22	NSA Exploit framework
fuzzdb	475.5656ab2	Attack and Discovery Pattern Dictionary for Application Fault Injection Testing
fuzzdiff	1.0	A simple tool designed to help out with crash analysis during fuzz testing. It selectively 'un-fuzzes' portions of a fuzzed file that is known to cause a crash, re-launches the targeted application, and sees if it still crashes.
fuzzowski	41.e39f665	A Network Protocol Fuzzer made by NCCGroup based on Sulley and BooFuzz.
fuzztalk	1.0.0.0	An XML driven fuzz testing framework that emphasizes easy extensibility and reusability.
g72x++		Decoder for the g72x++ codec.
gadgetinspector	6.ac7832d	A byte code analyzer for finding deserialization gadget chains in Java applications.
gadgettojscript	20.005cb8b	.NET serialized gadgets that can trigger .NET assembly from JS/VBS/VBA based scripts.
galleta	20040505_1	Examine the contents of the IE's cookie files for forensic purposes
gasmask	172.2527371	All in one Information gathering tool - OSINT.
gatecrasher	2.3ad5225	Network auditing and analysis tool developed in Python.
gau	127.e75ad3d	Fetch known URLs from AlienVault's Open Threat Exchange, the Wayback Machine, and Common Crawl.
gcat	29.39b266c	A fully featured backdoor that uses Gmail as a C&C server.
gcpbucketbrute	16.5fe33df	A script to enumerate Google Storage buckets, determine what access you have to them, and determine if they can be privilege escalated.
gcrypt	1:30.7c2fd05	Simple file encryption tool written in C++.
gdb	13.1	The GNU Debugger

gdb-common	13.1	The GNU Debugger
gdbgui	1:431.9138473	Browser-based gdb frontend using Flask and JavaScript to visually debug C, C++, Go, or Rust.
gef	2308.2830670	Multi-Architecture GDB Enhanced Features for Exploiters & Reverse-Engineers.
gene	78.faf8cc0	Signature Engine for Windows Event Logs.
genisys	53.d53bb0c	Powerful Telegram Members Scraping and Adding Toolkit.
genlist	1:0.1	Generates lists of IP addresses.
geoedge	0.2	This little tools is designed to get geolocalization information of a host, it get the information from two sources (maxmind and geoiptool).
geoip	1.6.12	Non-DNS IP-to-country resolver C library & utils
geoipgen	0.4	GeoIPgen is a country to IP addresses generator.
gerix-wifi-cracker	1.1c3cd73	A graphical user interface for aircrack-ng and pyrit.
gethsploit	3.144778b	Finding Ethereum nodes which are vulnerable to RPC-attacks.
getsids	0.0.1	Getsids tries to enumerate Oracle Sids by sending the services command to the Oracle TNS listener. Like doing 'lsnrctl service'.
getsploit	37.bcab2ee	Command line utility for searching and downloading exploits.
gf	39.dcd4c36	A wrapper around grep, to help you grep for things.
gg-images	35.b2dd863	The application was created to allow anyone to easily download profile pictures from GG.
gggooglescan	0.4	A Google scraper which performs automated searches and returns results of search queries in the form of URLs or hostnames.
gh-dork	3.799f86f	Github dorking tool.
ghauri	1.1.9.r3.gbb22483	An advanced cross-platform tool that automates the process of detecting and exploiting SQL injection security flaws.
ghettotooth	1.0	Ghettodriving for bluetooth
ghidra	10.2.3	A software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate in support of the Cybersecurity mission.
ghost-phisher	1.62	GUI suite for phishing and penetration attacks
ghost-py	2.0.0	Webkit based webclient (relies on PyQT).
ghostdelivery	32.a23ed5a	Python script to generate obfuscated .vbs script that delivers payload (payload dropper) with persistence and windows antivirus disabling

		functions.
gibberish-detector	v0.1.1.r2.gecac969	Train a model and detect gibberish strings with it.
girsh	v0.40.r2.g0fa6870	Automatically spawn a reverse shell fully interactive for Linux or Windows victim.
giskismet	20110805	A program to visually represent the Kismet data in a flexible manner.
git-dump	7.4c9a2a9	Dump the contents of a remote git repository without directory listing enabled.
git-dumper	1:1.0.6.r0.g32d47a2	A tool to dump a git repository from a website.
git-hound	148.c8daed6	Pinpoints exposed API keys on GitHub. A batch-catching, pattern-matching, patch-attacking secret snatcher.
git-wild-hunt	16.6495672	A tool to hunt for credentials in github wild AKA git*hunt.
gitdorker	113.8199375	Python program to scrape secrets from GitHub through usage of a large repository of dorks.
gitdump	1.682fa37	A pentesting tool that dumps the source code from .git even when the directory traversal is disabled.
gitem	104.d40a1c9	A Github organization reconnaissance tool.
gitgraber	67.72e5850	Monitor GitHub to search and find sensitive data in real time for different online services.
githack	16.a3d70b1	A `.git` folder disclosure exploit.
githound	v1.6.2.r0.gc8daed6	Find secret information in git repositories.
github-dorks	79.bc65a29	Collection of github dorks and helper tool to automate the process of checking dorks.
githubcloner	35.2bcb9c2	A script that clones Github repositories of users and organizations automatically.
gitleaks	907.8a31f4a	Audit Git repos for secrets and keys.
gitmails	71.8aa8411	An information gathering tool to collect git commit emails in version control host services.
gitminer	54.16ada58	Tool for advanced mining for content on Github.
gitrecon	30.6467e78	OSINT tool to get information from a Github and Gitlab profile and find user's email addresses leaked on commits.
gitrob	7.7be4c53	Scan Github For Sensitive Files.

gittools	70.7cac63a	A repository with 3 tools for pwn'ing websites with .git repositories available'.
gloom	1:93.cd6e927	Linux Penetration Testing Framework.
glue	380.8703380	A framework for running a series of tools.
gmsadumper	16.cbc13e0	A tool that Reads any gMSA password blobs the user can access and parses the values.
gnuradio	3.10.6.0	General purpose DSP and SDR toolkit. With drivers for usrp and fcd.
gnutls2	2.12.23	A library which provides a secure layer over a reliable transport layer (Version 2)
gobd	82.3bbd17c	A Golang covert backdoor.
gobuster	2:358.c3fed5e	Directory/file & DNS busting tool written in Go.
gocabrito	4.33ac59a	Super organized and flexible script for sending phishing campaigns.
goddi	1.2	Dumps Active Directory domain information.
goldeneye	28.792862f	A HTTP DoS test tool. Attack Vector exploited: HTTP Keep Alive + NoCache.
golismero	73.7d605b9	Opensource web security testing framework.
gomapenum	v1.1.0.r95.g23ecc54	User enumeration and password bruteforce on Azure, ADFS, OWA, O365, Teams and gather emails on Linkedin.
goodork	2.2	A python script designed to allow you to leverage the power of google dorking straight from the comfort of your command line.
goofile	1.5	Command line filetype search
goog-mail	1.0	Enumerate domain emails from google.
google_streetview	1.2.9	A command line tool and module for Google Street View Image API.
google-explorer	140.0b21b57	Google mass exploit robot - Make a google search, and parse the results for a especific exploit you define.
googlesub	14.a7a3cc7	A python script to find domains by using google dorks.
goohak	31.815a31e	Automatically Launch Google Hacking Queries Against A Target Domain.
goop	12.39b34eb	Perform google searches without being blocked by the CAPTCHA or hitting any rate limits. Note: It no longer works.
gooscan	1.0.9	A tool that automates queries against Google search appliances, but with a twist.

gopherus	33.90a2fd5	Tool generates gopher link for exploiting SSRF and gaining RCE in various servers.
gophish	810.d2efb18	Open-Source Phishing Framework.
gosint	196.9c86ed2	OSINT framework in Go.
gospider	106.721e78c	Fast web spider written in Go.
gostringsr2	1.1.2	Extract strings from a Go binary using radare2.
gowitness	270.9e88f8c	A golang, web screenshot utility using Chrome Headless.
gplist	1.0	Lists information about the applied Group Policies.
gpocrack	3.cf63c86	Active Directory Group Policy Preferences cpassword cracker/decrypter.
gpredict	1629.0f3beb6	A real-time satellite tracking and orbit prediction application.
gps-sdr-sim	203.dc403c8	Software-Defined GPS Signal Simulator.
gqrx	2.16	Interactive SDR receiver waterfall for many devices.
gr-air-modes	396.0b6c383	Gnuradio tools for receiving Mode S transponder signals, including ADS-B.
gr-gsm	1151.2efaa49	Gnuradio blocks and tools for receiving GSM transmissions
gr-paint	42.24765f9	An OFDM Spectrum Painter for GNU Radio.
grabbb	0.0.7	Clean, functional, and fast banner scanner.
grabber	0.1	A web application scanner. Basically it detects some kind of vulnerabilities in your website.
grabing	11.9c1aa6c	Counts all the hostnames for an IP adress
grabitall	1.1	Performs traffic redirection by sending spoofed ARP replies.
graffiti	24.4af61b4	A tool to generate obfuscated one liners to aid in penetration testing.
grammarinator	153.7dace54	A random test generator / fuzzer that creates test cases according to an input ANTLR v4 grammar.
graphinder	1.11.6	GraphQL endpoints finder using subdomain enumeration, scripts analysis and bruteforce.
graphql-cop	1.12.r5.g6deb322	GraphQL vulnerability scanner.
graphql-path-enum	16.1a44883	Tool that lists the different ways of reaching a given type in a GraphQL schema.
graphqlmap	63.59305d7	Scripting engine to interact with a graphql endpoint for pentesting purposes.
graphw00f	1.1.8.r8.g2321	GraphQL endpoint detection and engine fingerprinting.

	1eb	
graudit	606.44111c8	Grep rough source code auditing tool.
greenbone-security-assistant	9.0.1	Greenbone Security Assistant (gsa) - OpenVAS web frontend
grepforrfi	0.1	Simple script for parsing web logs for RFIs and Webshells v1.2
grokevt	0.5.0	A collection of scripts built for reading Windows NT/2K/XP/2K eventlog files.
grr	17.791ed5a	High-throughput fuzzer and emulator of DECREE binaries.
grype	1:0.33.1	A vulnerability scanner for container images and filesystems.
gsd	1.1	Gives you the Discretionary Access Control List of any Windows NT service you specify as a command line option.
gsocket	1.4.40	Global Socket. Moving data from here to there. Securely, Fast and trough NAT/Firewalls.
gspoof	3.2	A simple GTK/command line TCP/IP packet generator.
gtalk-decode	0.1	Google Talk decoder tool that demonstrates recovering passwords from accounts.
gtfo	17.873d862	Search gtfobins and lolbas files from your terminal.
gtfoblookup	66.6b8f4a5	Offline command line lookup utility for GTFOBins and LOLBAS.
gtp-scan	0.7	A small python script that scans for GTP (GPRS tunneling protocol) speaking hosts.
guymager	0.8.13	A forensic imager for media acquisition.
gvmd	8.0.1	Greenbone Vulnerability Manager - The database backend for the Greenbone Vulnerability Management (GVM) framework
gwcheck	0.1	A simple program that checks if a host in an ethernet network is a gateway to Internet.
gwtenum	1:7.f27a5aa	A command line tool that analyzes the obfuscated Javascript produced by Google Web Toolkit (GWT) applications in order to enumerate all services and method calls.
h2buster	79.6c4dd1c	A threaded, recursive, web directory brute-force scanner over HTTP/2.
h2csmuggler	7.7ea573a	HTTP Request Smuggling over HTTP/2 Cleartext (h2c).
h2spec	2.6.0	A conformance testing tool for HTTP/2 implementation.
h2t	36.9183a30	Scans a website and suggests security headers to apply.

h8mail	344.ee31c8f	Email OSINT and password breach hunting.
habu	359.8326936	Python Network Hacking Toolkit.
hackersh	0.2.0	A shell for with Pythonect-like syntax, including wrappers for commonly used security tools.
hackredis	3.fbae1bc	A simple tool to scan and exploit redis servers.
hackrf	2023.01.1	Driver for HackRF, allowing general purpose software defined radio (SDR).
haiti	v1.5.0.r13.gf9e20c7	A CLI tool to identify the hash type of a given hash.
haka	0.2.2	A collection of tool that allows capturing TCP/IP packets and filtering them based on Lua policy files.
hakku	384.bbb434d	Simple framework that has been made for penetration testing tools.
hakrawler	234.14e240b	Simple, fast web crawler designed for easy, quick discovery of endpoints and assets within a web application.
hakrevdns	41.8b638e4	Small, fast tool for performing reverse DNS lookups en masse.
halberd	0.2.4	Halberd discovers HTTP load balancers. It is useful for web application security auditing and for load balancer configuration testing.
halcyon	0.1	A repository crawler that runs checksums for static files found within a given git repository.
halcyon-ide	2.0.2	First IDE for Nmap Script (NSE) Development.
hamster	2.0.0	Tool for HTTP session sidejacking.
handle	1:0.1	An small application designed to analyze your system searching for global objects related to running proccess and display information for every found object, like tokens, semaphores, ports, files,..
harness	19.ed2a6aa	Interactive remote PowerShell Payload.
harpoon	380.0bd1f34	CLI tool for open source and threat intelligence.
hasere	1.0	Discover the vhosts using google and bing.
hash-buster	49.0d6ebb4	A python script which scraps online hash crackers to find cleartext of a hash.
hash-extender	157.1f29520	A hash length extension attack tool.
hash-identifier	6.0e08a97	Software to identify the different types of hashes used to encrypt data and especially passwords.
hashcat	1:6.2.6	Multithreaded advanced password recovery utility

hashcat-utils	1.9	Utilites for Hashcat
hashcatch	52.8145660	Hashcatch deauthenticates clients connected to all nearby WiFi networks and tries to capture the handshakes. It can be used in any linux device including Raspberry Pi and Nethunter devices so that you can capture handshakes while walking your dog.
hashcheck	2.72b0c6e	Search for leaked passwords while maintaining a high level of privacy using the k-anonymity method.
hashdb	1089.1da1b9f	A block hash toolkit.
hashdeep	4.4	Advanced checksum hashing tool.
hasher	48.40173c5	A tool that allows you to quickly hash plaintext strings, or compare hashed values with a plaintext locally.
hashfind	8.e9a9a14	A tool to search files for matching password hash types and other interesting data.
hashid	1:397.7e8473a	Software to identify the different types of hashes used to encrypt data.
hashpump	49.314268e	A tool to exploit the hash length extension attack in various hashing algorithms.
hashtag	0.41	A python script written to parse and identify password hashes.
hatcloud	33.3012ad6	Bypass CloudFlare with Ruby.
hate-crack	187.b1d7e39	A tool for automating cracking methodologies through Hashcat.
haystack	1823.c178b5a	A Python framework for finding C structures from process memory - heap analysis - Memory structures forensics.
hbad	1.0	This tool allows you to test clients on the heartbleed bug.
hcraft	1.0.0	HTTP Vuln Request Crafter
hcxdumptool	6.2.7	Small tool to capture packets from wlan devices
hcxkeys	6.2.1	Set of tools to generate plainmasterkeys (rainbowtables) and hashes for hashcat and John the Ripper
hcxtools	6.2.7	Small set of tools to capture and convert packets from wlan devices for the use with hashcat.
hdcp-genkey	18.e8d342d	Generate HDCP source and sink keys from the leaked master key.
hdmi-sniff	5.f7fbc0e	HDMI DDC (I2C) inspection tool. It is designed to demonstrate just how easy it is to recover HDCP crypto keys from HDMI devices.
heaptrace	2.2.8.2.r20.g06f43fc	Helps visualize heap operations for pwn and debugging.

heartbleed-honeypot	0.1	Script that listens on TCP port 443 and responds with completely bogus SSL heartbeat responses, unless it detects the start of a byte pattern similar to that used in Jared Stafford's
heartleech	116.3ab1d60	Scans for systems vulnerable to the heartbleed bug, and then download them.
hellraiser	279.bea43e2	Vulnerability Scanner.
hemingway	8.9c70a13	A simple and easy to use spear phishing helper.
hercules-payload	222.2607a3a	A special payload generator that can bypass all antivirus software.
hetty	134.f60202e	HTTP toolkit for security research. It aims to become an open source alternative to commercial software like Burp Suite Pro, with powerful features tailored to the needs of the infosec and bug bounty community.
hex2bin	2.5	Converts Motorola and Intel hex files to binary.
hexinject	1.6	A very versatile packet injector and sniffer that provides a command-line framework for raw network access.
hexorbase	2:6	A database application designed for administering and auditing multiple database servers simultaneously from a centralized location. It is capable of performing SQL queries and bruteforce attacks against common database servers (MySQL, SQLite, Microsoft SQL Server, Oracle, PostgreSQL).
hexyl	0.12.0	A command-line hex viewer.
hharp	1beta	This tool can perform man-in-the-middle and switch flooding attacks. It has 4 major functions, 3 of which attempt to man-in-the-middle one or more computers on a network with a passive method or flood type method.
hidattack	0.1	HID Attack (attacking HID host implementations)
hiddeneye	1228.7a3deaf	Modern phishing tool with advanced functionality.
hiddeneye-legacy	RC1.r226.g7a3deaf	Modern Phishing Tool With Advanced Functionality.
hikpwn	8.5a7d69c	A simple scanner for Hikvision devices with basic vulnerability scanning capabilities written in Python 3.8.
hlextend	17.be21920	Pure Python hash length extension module.
hodor	1.01be107	A general-use fuzzer that can be configured to use known-good input and delimiters in order to fuzz specific locations.
holehe	421.2158f87	A tool for Efficiently finding registered accounts from emails.

hollows-hunter	0.3.5	Scans all running processes. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches).
homepwn	31.0803981	Swiss Army Knife for Pentesting of IoT Devices.
honeycreds	26.eaeb401	Network credential injection to detect responder and other network poisoners.
honeyd	337.a0f3d64	A small daemon that creates virtual hosts on a network.
honeypy	599.feccab5	A low interaction Honeypot.
honggfuzz	4055.3a8f2ae4	A general-purpose fuzzer with simple, command-line interface.
honssh	204.821ce87	A high-interaction Honey Pot solution designed to log all SSH communications between a client and server.
hookanalyser	3.4	A hook tool which can be potentially helpful in reversing applications and analyzing malware. It can hook to an API in a process and search for a pattern in memory or dump the buffer.
hookshot	199.3258c3e	Integrated web scraper and email account data breach comparison tool.
hoover	4.9bda860	Wireless Probe Requests Sniffer.
hoper	15.8d5dbd9	Trace URL's jumps across the rel links to obtain the last URL.
hopper	5.8.6	Reverse engineering tool that lets you disassemble, decompile and debug your applications.
hoppy	1.8.1	A python script which tests http methods for configuration issues leaking information or just to see if they are enabled.
host-extract	1:8.0134ad7	Ruby script tries to extract all IP/Host patterns in page response of a given URL and JavaScript/CSS files of that URL.
hostapd-wpe	2.9.1	IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator - Wireless Pwnage Edition.
hostbox-ssh	0.1.1	A ssh password/account scanner.
hosthunter	158.553f1c7	A recon tool for discovering hostnames using OSINT techniques.
hotpatch	90.fd2baf1	Hot patches executables on Linux using .so file injection.
hotspotter	0.4	Hotspotter passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names.
howmanypeoplearearound	123.b05e06a	Count the number of people around you by monitoring wifi signals.
hpfeeds	411.539e738	Honeynet Project generic authenticated datafeed protocol.

hping	3.0.0	A command-line oriented TCP/IP packet assembler/analyzer.
hqlmap	38.bb6ab46	A tool to exploit HQL Injections.
hsecscan	66.7b8fa71	A security scanner for HTTP response headers.
htcap	1:155.a59c592	A web application analysis tool for detecting communications between javascript and the server.
htexploit	0.77	A Python script that exploits a weakness in the way that .htaccess files can be configured to protect a web directory with an authentication process
htpwdscan	23.e995d6f	A python HTTP weak pass scanner.
htrosbif	134.9dc3f86	Active HTTP server fingerprinting and recon tool.
htshells	2:89.3216523	Self contained web shells and other attacks via .htaccess files.
http-enum	0.4	A tool to enumerate the enabled HTTP methods supported on a webserver.
http-fuzz	1:0.1	A simple http fuzzer.
http-put	1.0	Simple http put perl script.
http-traceroute	0.5	This is a python script that uses the Max-Forwards header in HTTP and SIP to perform a traceroute-like scanning functionality.
http2smugl	36.78abc09	Http2Smugl - Tool to detect and exploit HTTP request smuggling in cases it can be achieved via HTTP/2 -больше HTTP/1.1 conversion.
httpbog	1.0.0.0	A slow HTTP denial-of-service tool that works similarly to other attacks, but rather than leveraging request headers or POST data Bog consumes sockets by slowly reading responses.
httpforge	11.02.01	A set of shell tools that let you manipulate, send, receive, and analyze HTTP messages. These tools can be used to test, discover, and assert the security of Web servers, apps, and sites. An accompanying Python library is available for extensions.
httpgrep	2.3	A python tool which scans for HTTP servers and finds given strings in URIs.
httping	2.9	A ping-like tool for http-requests
httppwnly	47.528a664	"Repeater" style XSS post-exploitation tool for mass browser control.
httprecon	7.3	Tool for web server fingerprinting, also known as http fingerprinting.
httprint	301	A web server fingerprinting tool.
httprint-win32	301	A web server fingerprinting tool (Windows binaries).
httprobe	22.5555984	Take a list of domains and probe for working HTTP and HTTPS servers
httpry	0.1.8	A specialized packet sniffer designed for displaying and logging HTTP

		traffic.
httpscreenshot	69.0ef8f8f	A tool for grabbing screenshots and HTML of large numbers of websites.
httpsniff	0.4	Tool to sniff HTTP responses from TCP/IP based networks and save contained files locally for later review.
httpsscanner	1.2	A tool to test the strength of a SSL web server.
httptunnel	3.3	Creates a bidirectional virtual data connection tunnelled in HTTP requests
httpx	1272.344c54a	A fast and multi-purpose HTTP toolkit allow to run multiple probers using retryablehttp library.
httrack	3.49.2	An easy-to-use offline browser utility
hubbit-sniffer	74.460ecf8	Simple application that listens for WIFI-frames and records the mac-address of the sender and posts them to a REST-api.
hulk	27.ed2b11c	A webserver DoS tool (Http Unbearable Load King) ported to Go with some additional features.
hungry-interceptor	391.1aea7f3	Intercepts data, does something with it, stores it.
hurl	20.afca9c5	Hexadecimal & URL (en/de)coder.
hwk	0.4	Collection of packet crafting and wireless network flooding tools
hxd	2.5.0.0	Freeware Hex Editor and Disk Editor.
hyde	11.ec09462	Just another tool in C to do DDoS (with spoofing).
hydra	9.4	Very fast network logon cracker which support many different services
hyenae	0.36_1	flexible platform independent packet generator
hyperfox	121.1a8c26f	A security tool for proxying and recording HTTP and HTTPs traffic.
hyperion-crypter	2.3.1	A runtime encrypter for 32-bit portable executables.
i2pd	2.47.0	A full-featured C++ implementation of the I2P router
iaito	5.8.4	Qt and C++ GUI for radare2 reverse engineering framework
iaxflood	3:0.1	IAX flooder.
iaxscan	0.02	A Python based scanner for detecting live IAX/2 hosts and then enumerating (by bruteforce) users on those hosts.
ibrute	12.3a6a11e	An AppleID password bruteforce tool. It uses Find My Iphone service API, where bruteforce protection was not implemented.
icloudbrutter	15.1f64f19	Tool for AppleID Bruteforce.
icmpquery	1.0	Send and receive ICMP queries for address mask and current time.

icmpsh	12.82caf34	Simple reverse ICMP shell.
icmptx	17.52df90f	IP over ICMP tunnel.
id-entify	34.dd064a5	Search for information related to a domain: Emails - IP addresses - Domains - Information on WEB technology - Type of Firewall - NS and MX records.
ida-free	8.2	Freeware version of the world's smartest and most feature-full disassembler.
idb	2.10.3	A tool to simplify some common tasks for iOS pentesting and research.
identywaf	206.aa670df	Blind WAF identification tool.
idswakeup	1.0	A collection of tools that allows to test network intrusion detection systems.
ifchk	1.1.2	A network interface promiscuous mode detection tool.
ifuzz	1.0	A binary file fuzzer with several options.
iheartxor	0.01	A tool for bruteforcing encoded strings within a boundary defined by a regular expression. It will bruteforce the key value range of 0x1 through 0x255.
iis-shortname-scanner	5.4ad4937	An IIS shortname Scanner.
iisbruteforcer	15	HTTP authentication cracker. It's a tool that launchs an online dictionary attack to test for weak or simple passwords against protected areas on an IIS Web server.
ike-scan	1.9.5	A tool that uses IKE protocol to discover, fingerprint and test IPSec VPN servers
ikecrack	1.00	An IKE/IPSec crack tool designed to perform Pre-Shared-Key analysis of RFC compliant aggressive mode authentication
ikeforce	30.575af15	A command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.
ikeprobe	2:0.1	Determine vulnerabilities in the PSK implementation of the VPN server.
ikeprober	1.12	Tool crafting IKE initiator packets and allowing many options to be manually set. Useful to find overflows, error conditions and identifiyng vendors
ilo4-toolbox	43.6a494fe	Toolbox for HPE iLO4 analysis.
ilty	1.0	An interception phone system for VoIP network.
imagegrep	8.1f14af2	Grep word in pdf or image based on OCR.

imagejs	56.a442f94	Small tool to package javascript into a valid image file.
imagemounter	413.383b30b	Command line utility and Python package to ease the (un)mounting of forensic disk images.
imhex	1.28.0.r79.gbec655a8	A Hex Editor for Reverse Engineers, Programmers and people that value their eye sight when working at 3 AM.
impacket	0.9.24	Impacket is a collection of Python classes for working with network protocols.
impulse	77.6939ea2	Modern Denial-of-service ToolKit.
inception	453.e2aed33	A FireWire physical memory manipulation and hacking tool exploiting IEEE 1394 SBP-2 DMA.
indx2csv	17.129a411e	An advanced parser for INDX records.
indxcarver	5.dee36608	Carve INDX records from a chunk of data.
indxparse	176.4e1e293	A Tool suite for inspecting NTFS artifacts.
inetsim	1.3.2	A software suite for simulating common internet services in a lab environment, e.g. for analyzing the network behaviour of unknown malware samples.
infection-monkey	v1.13.0.r9113.g1d713513f	Automated security testing tool for networks.
infip	0.1	A python script that checks output from netstat against RBLs from Spamhaus.
infoga	3:33.79a1c03	Tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers).
inguma	0.1.1	A free penetration testing and vulnerability discovery toolkit entirely written in python. Framework includes modules to discover hosts, gather information about, fuzz targets, brute force usernames and passwords, exploits, and a disassembler.
injectus	12.3c01fa0	Simple python tool that goes through a list of URLs trying CRLF and open redirect payloads.
innounp	0.50	Inno Setup Unpacker.
inquisitor	1:28.12a9ec1	OSINT Gathering Tool for Companies and Organizations.
insanity	117.cf51ff3	Generate Payloads and Control Remote Machines .
instagramosint	20.94213fd	An Instagram Open Source Intelligence Tool.
instashell	56.49b6b4f	Multi-threaded Instagram Brute Forcer without password limit.
intelmq	3.1.0.rc1.r17.g	A tool for collecting and processing security feeds using a message

	122e3a386	queuing protocol.
intelplot	12.4dd9fc0	OSINT Tool to Mark Points on Offline Map.
intensio-obfuscator	280.f66a22b	Obfuscate a python code 2 and 3.
interactsh-client	v1.1.1.r0.g14231ab	Open-Source Solution for Out of band Data Extraction.
intercepter-ng	1.0	A next generation sniffer including a lot of features: capturing passwords/hashes, sniffing chat messages, performing man-in-the-middle attacks, etc.
interlace	348.7823e42	Easily turn single threaded command line applications into a fast, multi-threaded application with CIDR and glob support.
interrogate	5.eb5f071	A proof-of-concept tool for identification of cryptographic keys in binary material (regardless of target operating system), first and foremost for memory dump analysis and forensic usage.
intersect	2.5	Post-exploitation framework
intrace	1.5	Traceroute-like application piggybacking on existing TCP connections
inundator	0.5	An ids evasion tool, used to anonymously inundate intrusion detection logs with false positives in order to obfuscate a real attack.
inurlbr	34.dbf9773	Advanced search in the search engines - Inurl scanner, dorker, exploiter.
inviteflood	2.0	Flood a device with INVITE requests
invoke-cradlecrafter	19.3ff8bac	PowerShell Remote Download Cradle Generator & Obfuscator.
invoke-dosfuscation	7.6260f5b	Cmd.exe Command Obfuscation Generator & Detection Test Harness.
invoke-obfuscation	45.f20e7f8	PowerShell Obfuscator.
inzider	1.2	This is a tool that lists processes in your Windows system and the ports each one listen on.
iodine	0.7.0	Tunnel IPv4 data through a DNS server
iosforensic	1.0	iOS forensic tool https://www.owasp.org/index.php/Projects/OWASP_iOSForensic
ip-https-tools	7.170691f	Tools for the IP over HTTPS (IP-HTTPS) Tunneling Protocol.
ip-tracer	91.8e2e3dd	Track and retrieve any ip address information.
ip2clue	0.0.95	A small memory/CPU footprint daemon to lookup country (and other info)

		based on IP (v4 and v6).
ipaudit	1.1	Monitors network activity on a network.
ipba2	1:95.c03bd85	IOS Backup Analyzer
ipcountry	1.2	
ipdecap	96.45d2a7d	Can decapsulate traffic encapsulated within GRE, IPIP, 6in4, ESP (ipsec) protocols, and can also remove IEEE 802.1Q (virtual lan) header.
iphoneanalyzer	2.1.0	Allows you to forensically examine or recover date from in iOS device.
ipmipwn	6.74a08a8	IPMI cipher 0 attack tool.
ipmitool	1.8.19	Command-line interface to IPMI-enabled devices
ipobfuscator	27.f005262	A simple tool to convert the IP to a DWORD IP.
ipscan	3.9.1	Angry IP scanner is a very fast IP address and port scanner.
ipsourcebypass	1.2.r12.g91b16ad	This Python script can be used to bypass IP source restrictions using HTTP headers.
iptodomain	18.f1afcd7	This tool extract domains from IP address based in the information saved in virustotal.
iptv	138.ae6457b	Search and brute force illegal iptv server.
iputils	20221126	Network monitoring tools, including ping
ipv4bypass	21.99bb285	Using IPv6 to Bypass Security.
ipv666	182.ad45ae8	Golang IPv6 address enumeration. ipv666 is a set of tools that enables the discovery of IPv6 addresses both in the global IPv6 address space and in more narrow IPv6 network ranges. These tools are designed to work out of the box with minimal knowledge of their workings.
ipv6toolkit	819.367bbe6	SI6 Networks' IPv6 Toolkit
ipython-genutils	0.2.0	Vestigial utilities from IPython.
ircsnapshot	94.cb02a85	Tool to gather information from IRC servers.
irpas	0.10	Internetwork Routing Protocol Attack Suite.
isf	68.5228865	Industrial Exploitation Framework is an exploitation framework based on Python.
isip	2.fad1f10	Interactive sip toolkit for packet manipulations, sniffing, man in the middle attacks, fuzzing, simulating of dos attacks.
isme	0.12	Scans a VOIP environment, adapts to enterprise VOIP, and exploits the possibilities of being connected directly to an IP Phone VLAN.
isr-form	1.0	Simple html parsing tool that extracts all form related information and

		generates reports of the data. Allows for quick analyzing of data.
issniff	294.79c6c2a	Internet Session Sniffer.
ivre	0.9.20.dev64	Network recon framework.
ivre-docs	0.9.20.dev64	Network recon framework (documentation)
ivre-web	0.9.20.dev64	Network recon framework (web application)
ja3	117.cb29184	Standard for creating SSL client fingerprints in an easy to produce and shareable way.
jaadas	0.1	Joint Advanced Defect assEsment for android applications.
jackdaw	410.5b8c35c	Collect all information in your domain, show you graphs on how domain objects interact with each-other and how to exploit these interactions
jad	1.5.8e	Java decompiler
jadx	1.4.7	Command line and GUI tools to produce Java source code from Android Dex and APK files
jaeles	220.f2032a5	The Swiss Army knife for automated Web Application Testing.
jaidam	18.15e0fec	Penetration testing tool that would take as input a list of domain names, scan them, determine if wordpress or joomla platform was used and finally check them automatically, for web vulnerabilities using two well-known open source tools, WPScan and Joomscan.
jast	17.361ecde	Just Another Screenshot Tool.
javasnoop	1.1	A tool that lets you intercept methods, alter data and otherwise hack Java applications running on your computer
jboss-autopwn	1.3bc2d29	A JBoss script for obtaining remote shell access.
jbrofuzz	2.5	Web application protocol fuzzer that emerged from the needs of penetration testing.
jbrute	1:0.99	Open Source Security tool to audit hashed passwords.
jcrack	0.3.6	A utility to create dictionary files that will crack the default passwords of select wireless gateways
jd-cli	1.2.0	Command line Java Decompiler.
jd-gui	1.6.6	A standalone graphical utility that displays Java source codes of .class files.
jdeserialize	31.20635ba	A library that interprets Java serialized objects. It also comes with a command-line tool that can generate compilable class declarations, extract block data, and print textual representations of instance values.

jeangrey	40.01aef30	A tool to perform differential fault analysis attacks (DFA).
jeb-android	3.7.0.201909272058	Android decompiler.
jeb-arm	3.7.0.201909272058	Arm decompiler.
jeb-intel	1:3.7.0.201909272058	Intel decompiler.
jeb-mips	1:3.7.0.201909272058	Mips decompiler.
jeb-webasm	3.7.0.201909272058	WebAssembly decompiler.
jeopardize	5.34f1d07	A low(zero) cost threat intelligence & response tool against phishing domains.
jexboss	86.338b531	Jboss verify and Exploitation Tool.
jhead	3.06.0.1	EXIF JPEG info parser and thumbnail remover
jira-scan	7.447d0ec	A simple remote scanner for Atlassian Jira
jndi-injection-exploit	10.2dc4018	A tool which generates JNDI links can start several servers to exploit JNDI Injection vulnerability, like Jackson, Fastjson, etc.
jnetmap	0.5.5	jNetMap helps you to keep an eye on your network. You can draw a graphical representation of your network, and jNetMap will periodically check if the devices are still up or a service is still running. You can also set up E-mail notifications or let jNetMap execute a script when a device goes down or comes up again. Additionally, you may attach notes to a device, initiate an RDP/VNC/SSH connection to a device and much more.
john	1.9.0.jumbo1	John the Ripper password cracker
johnny	20120424	GUI for John the Ripper.
jok3r	447.0761996	Network and Web Pentest Framework.
jomplug	0.1	This php script fingerprints a given Joomla system and then uses Packet Storm's archive to check for bugs related to the installed components.
jondo	00.20.001	Redirects internet traffic trough a mix of proxy servers to hide the origin of the requests.
jooforce	11.43c21ad	A Joomla password brute force tester.
joomlascan	1.2	Joomla scanner scans for known vulnerable remote file inclusion paths and files.

joomlavs	254.eea7500	A black box, Ruby powered, Joomla vulnerability scanner.
joomscan	1:82.7931539	Detects file inclusion, sql injection, command execution vulnerabilities of a target Joomla! web site.
jpegdump	0.0.7	Tool to analyzse JPEG images Reads binary files and parses the JPEG markers inside them.
jpexs-decompiler	15.1.0	JPEXS Free Flash Decompiler.
jsearch	44.87cf9c1	Simple script that grep infos from javascript files.
jsfuck	228.1f02651	Write any JavaScript with 6 Characters: []()!+.
jshell	7.ee3c92d	Get a JavaScript shell with XSS.
jsonbee	26.e106db2	A ready to use JSONP endpoints/payloads to help bypass content security policy (CSP).
jsparser	31.ccd3ab6	A python 2.7 script using Tornado and JSBeautifier to parse relative URLs from JavaScript files. Useful for easily discovering AJAX requests.
jsql	0.81	A lightweight application used to find database information from a distant server.
jsql-injection	0.85	A Java application for automatic SQL database injection.
jstillery	65.512e9af	Advanced JavaScript Deobfuscation via Partial Evaluation.
juicy-potato	53.744d321	A sugared version of RottenPotatoNG, with a bit of juice.
junkie	1365.70a83d6	A modular packet sniffer and analyzer.
justdecompile	22018	The decompilation engine of JustDecompile.
juumla	94.1661231	Python tool created to identify Joomla version, scan for vulnerabilities and search for config files.
jwscan	7.874b3a5	Scanner for Jar to EXE wrapper like Launch4j, Exe4j, JSmooth, Jar2Exe.
jwt-cracker	23.8130879	JWT brute force cracker written in C.
jwt-hack	v1.1.2.r8.g06fb757	A tool for hacking / security testing to JWT.
jwt-key-recovery	10.d3b8ad4	Recovers the public key used to sign JWT tokens.
jwt-tool	69.6c7d430	Toolkit for validating, forging and cracking JWTs (JSON Web Tokens).
jwtcat	77.f80f3d9	Script performs offline brute-force attacks against JSON Web Token (JWT)
jynx2	2.0	An expansion of the original Jynx LD_PRELOAD rootkit

k55	86.b3c4aa9	Linux x86_64 Process Injection Utility.
kacak	1.0	Tools for penetration testers that can enumerate which users logged on windows system.
kadimus	183.ac5f438	LFI Scan & Exploit Tool.
Kali Linux	2023.1	Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering.
kalibrate-rtl	69.340003e	Fork of http://thre.at/kalibrate/ for use with rtl-sdr devices.
kamerka	40.be17620	Build interactive map of cameras from Shodan.
katana	1.0.0.1	A framework that seeks to unite general auditing tools, which are general pentesting tools (Network,Web,Desktop and others).
katana-framework	1.0.0.1	A framework that seekss to unite general auditing tools, which are general pentesting tools (Network,Web,Desktop and others).
katana-pd	v0.0.3.r7.gdb629bb	Crawling and spidering framework.
katsnoop	0.1	Utility that sniffs HTTP Basic Authentication information and prints the base64 decoded form.
kautilya	52.1c9d5b0	Pwnage with Human Interface Devices using Teensy++2.0 and Teensy 3.0 devices.
kcptun	20230214	A Secure Tunnel Based On KCP with N:M Multiplexing
keimpx	3:300.37190f4	Tool to verify the usefulness of credentials across a network over SMB.
kekeo	2.2.0_20211214	A little toolbox to play with Microsoft Kerberos in C.
kerbcrack	1.3d3	Kerberos sniffer and cracker for Windows.
kerberoast	1:0.2.0.r7.g025fe39	Kerberoast attack -pure python-.
kerbrute	90.9cfb81e	A tool to perform Kerberos pre-auth bruteforcing.
kernelpop	238.b3467d3	Kernel privilege escalation enumeration and exploitation framework.
keye	29.d44a578	Recon tool detecting changes of websites based on content-length differences.
kh2hc	0.0.1.r0.g7d62c18	Convert OpenSSH known_hosts file hashed with HashKnownHosts to hashes crackable by Hashcat.

khc	0.2	A small tool designed to recover hashed known_hosts fields back to their plain-text equivalents.
kickthemout	212.861aea2	Kick devices off your network by performing an ARP Spoof attack.
killcast	30.ee81cfa	Manipulate Chromecast Devices in your Network.
killerbee	398.748740d	Framework and tools for exploiting ZigBee and IEEE 802.15.4 networks.
kimi	28.e7cafda	Script to generate malicious debian packages (debain trojans).
kippo	285.0d03635	A medium interaction SSH honeypot designed to log brute force attacks and most importantly, the entire shell interaction by the attacker.
kismet	2022_08_R1	802.11 layer2 wireless network detector, sniffer, and intrusion detection system
kismet-earth	1:0.1	Various scripts to convert kismet logs to kml file to be used in Google Earth.
kismet2earth	1.0	A set of utilities that convert from Kismet logs to Google Earth .kml format
kismon	1.0.3	GUI client for kismet (wireless scanner/sniffer/monitor).
kiterunner	19.7d5824c	Contextual Content Discovery Tool.
kitty	321.f19e811	Fuzzing framework written in python.
kitty-framework	352.cb07609	Fuzzing framework written in python.
klar	2.4.0	Integration of Clair and Docker Registry.
klee	2.1	A symbolic virtual machine built on top of the LLVM compiler infrastructure.
klogger	1.0	A keystroke logger for the NT-series of Windows.
knock	2:78.3e7d95d	Subdomain scanner.
knxmap	252.6f40dd1	KNXnet/IP scanning and auditing tool for KNX home automation installations.
koadic	1:637.ac46c44	A Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire.
kolkata	3.0	A web application fingerprinting engine written in Perl that combines cryptography with IDS evasion.
konan	23.7b5ac80	Advanced Web Application Dir Scanner.
kraken	32.368a837	A project to encrypt A5/1 GSM signaling using a Time/Memory Tradeoff Attack.
krbrelayx	43.8269af0	Kerberos unconstrained delegation abuse toolkit.

kube-hunter	699.ff9f2c5	Hunt for security weaknesses in Kubernetes clusters.
kubesploit	86.2de2f12	Cross-platform post-exploitation HTTP/2 Command & Control server.
kubestriker	39.e1776ea	A Blazing fast Security Auditing tool for Kubernetes.
kubolt	28.0027239	Utility for scanning public kubernetes clusters.
kwetza	26.0e50272	Python script to inject existing Android applications with a Meterpreter payload.
l0l	322.1319ea7	The Exploit Development Kit.
laf	12.7a456b3	Login Area Finder: scans host/s for login panels.
lanmap2	1:127.1197999	Passive network mapping tool.
lans	1:148.9f8ef2d	A Multithreaded asynchronous packet parsing/injecting arp spoofer.
latd	1.31	A LAT terminal daemon for Linux and BSD.
laudanum	1.0	A collection of injectable files, designed to be used in a pentest when SQL injection flaws are found and are in multiple languages for different environments.
lazagne	845.8c9f962	An open source application used to retrieve lots of passwords stored on a local computer.
lazydroid	25.0f559ec	Tool written as a bash script to facilitate some aspects of an Android Assessment
lbd	20130719	Load Balancing detector
lbmap	147.2d15ace	Proof of concept scripts for advanced web application fingerprinting, presented at OWASP AppSecAsia 2012.
ld-shatner	4.5c215c4	ld-linux code injector.
ldap-brute	21.acc06e3	A semi fast tool to bruteforce values of LDAP injections over HTTP.
ldapdomaindump	0.9.4	Active Directory information dumper via LDAP.
ldapenum	1:0.1	Enumerate domain controllers using LDAP.
ldapscripts	2.0.8	Simple shell scripts to handle POSIX entries in an LDAP directory.
ldeep	199.a2c0edf	In-depth ldap enumeration utility.
ldsview	47.d8bfcaa	Offline search tool for LDAP directory dumps in LDIF format.
leaklooker	5.0d2b9fc	Find open databases with Shodan.
leena	2.5119f56	Symbolic execution engine for JavaScript
legion	59.3c08884	Automatic Enumeration Tool based in Open Source tools.
leo	30696.f739f40	Literate programmer's editor, outliner, and project manager.

	65	
leroy-jenkins	3.bdc3965	A python tool that will allow remote execution of commands on a Jenkins server and its nodes.
lethalhta	2.5602402	Lateral Movement technique using DCOM and HTA.
letmefuckit-scanner	3.f3be22b	Scanner and Exploit Magento.
leviathan	35.a1a1d8c	A mass audit toolkit which has wide range service discovery, brute force, SQL injection detection and running custom exploit capabilities.
levye	1:84.5406303	A brute force tool which is support sshkey, vnckey, rdp, openvpn.
lfi-autopwn	3.0	A Perl script to try to gain code execution on a remote server via LFI
lfi-exploiter	1.1	This perl script leverages /proc/self/environ to attempt getting code execution out of a local file inclusion vulnerability.
lfi-fuzzploit	1.1	A simple tool to help in the fuzzing for, finding, and exploiting of local file inclusion vulnerabilities in Linux-based PHP applications.
lfi-image-helper	0.8	A simple script to infect images with PHP Backdoors for local file inclusion attacks.
lfi-scanner	4.0	This is a simple perl script that enumerates local file inclusion attempts when given a specific target.
lfi-sploiter	1.0	This tool helps you exploit LFI (Local File Inclusion) vulnerabilities. Post discovery, simply pass the affected URL and vulnerable parameter to this tool. You can also use this tool to scan a URL for LFI vulnerabilities.
lfifreak	21.0c6adef	A unique automated LFi Exploiter with Bind/Reverse Shells.
lfimap	155.436ea01	This script is used to take the highest beneficts of the local file include vulnerability in a webserver.
lfisuite	85.470e01f	Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner.
lfle	24.f28592c	Recover event log entries from an image by heurisitically looking for record structures.
lft	1:3.91	A layer four traceroute implementing numerous other features.
lhf	40.51568ee	A modular recon tool for pentesting.
libbde	318.8805b43	A library to access the BitLocker Drive Encryption (BDE) format.
libc-database	45.69815cd	Database of libc offsets to simplify exploitation.
libdisasm	0.23	A disassembler library.
libfvde	191.df72aae	Library and tools to access FileVault Drive Encryption (FVDE) encrypted

		volumes.
libosmocore	1:4248.2d10ff20	Collection of common code used in various sub-projects inside the Osmocom family of projects.
libparistraceroute	378.6fb8f48	A library written in C dedicated to active network measurements with examples, such as paris-ping and paris-traceroute.
libpst	0.6.76	Outlook .pst file converter
libtins	1292.fa87e1b	High-level, multiplatform C++ network packet sniffing and crafting library.
lief	0.12.1	Library to Instrument Executable Formats.
liffy	1:33.89dd4f8	A Local File Inclusion Exploitation tool.
lightbulb	88.9e8d6f3	Python framework for auditing web applications firewalls.
ligolo-ng	v0.4.1.r0.gabb7e8a	An advanced, yet simple, tunneling tool that uses a TUN interface.
limeaide	305.ce3c9b7	Remotely dump RAM of a Linux client and create a volatility profile for later analysis on your local host.
limelighter	17.d119dc7	A tool for generating fake code signing certificates or signing real ones.
linenum	75.c47f9b2	Scripted Local Linux Enumeration & Privilege Escalation Checks
linikatz	46.113bab7	Tool to attack Active Directory on UNIX.
linkedin2username	1:124.8196968	OSINT Tool: Generate username lists for companies on LinkedIn.
linkfinder	162.095bb62	Discovers endpoint and their parameters in JavaScript files.
linset	9.8746b1f	Evil Twin Attack Bash script - An automated WPA/WPA2 hacker.
linux-exploit-suggester	32.9db2f5a	A Perl script that tries to suggest exploits based OS version number.
linux-exploit-suggester.sh	167.b6a730b	Linux privilege escalation auditing tool.
linux-inject	100.268d4e4	Tool for injecting a shared object into a Linux process.
linux-smart-enumeration	272.d69e353	Linux enumeration tool for pentesting and CTFs with verbosity levels.
LionSec Linux	5.0	LionSec Linux is a Linux Penetration Testing Operating system based on Ubuntu . It is a stable OS for security professional. It was built in order to perform Computer Forensics , Penetration Tests , Wireless Analysis . With the "Anonymous Mode" , you can browse the internet or send packets anonymously . There are lots of inbuilt tools like netool ,websploit ,

		burpsuite , web analysis tools , social engineering tools and other pentesting tools.
lisa.py	61.2d1f81a	An Exploit Dev Swiss Army Knife.
list-urls	0.1	Extracts links from webpage
littleblackbox	0.1.3	Penetration testing tool, search in a collection of thousands of private SSL keys extracted from various embedded devices.
littlebrother	112.338cf82	OSINT tool to get informations on French, Belgian and Swizerland people.
lldb	15.0.7	Next generation, high-performance debugger
loadlibrary	104.c40033b	Porting Windows Dynamic Link Libraries to Linux.
local-php-security-checker	v2.0.6.r2.gef59356	A command line tool that checks your PHP application packages with known security vulnerabilities.
locasploit	117.fa48151	Local enumeration and exploitation framework.
lodowep	1.2.1	Lodowep is a tool for analyzing password strength of accounts on a Lotus Domino webserver system.
log-file-parser	60.c7a0ae7e	Parser for $LogFile on NTFS.
log4j-bypass	33.f5c92f9	Log4j web app tester that includes WAF bypasses.
log4j-scan	88.07f7e32	A fully automated, accurate, and extensive scanner for finding log4j RCE CVE-2021-44228.
logkeys	97.98aac72	Simple keylogger supporting also USB keyboards.
logmepwn	22.a8882bd	A fully automated, reliable, super-fast, mass scanning and validation toolkit for the Log4J RCE CVE-2021-44228 vulnerability.
loic	2.9.9.99	An open source network stress tool for Windows.
loki-scanner	1189.2f0f824	Simple IOC and Incident Response Scanner.
lolbas	192.d148d27	Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts).
loot	51.656fb85	Sensitive information extraction tool.
lorcon	2:2020.06.06	Generic library for injecting 802.11 frames
lorg	98.aa4f1a3	Apache Logfile Security Analyzer.
lorsrf	bbb.r0.g91c26ec	Find the parameters that can be used to find SSRF or Out-of-band resource load.
lotophagi	0.1	a relatively compact Perl script designed to scan remote hosts for default (or common) Lotus NSF and BOX databases.
lsrtunnel	0.2	Spoofs connections using source routed packets.

lte-cell-scanner	57.5fa3df8	LTE SDR cell scanner optimized to work with very low performance RF front ends (8bit A/D, 20dB noise figure).
ltrace	0.7.3	Tracks runtime library calls in dynamically linked programs
luksipc	0.01	A tool to convert unencrypted block devices to encrypted LUKS devices in-place.
lulzbuster	1.3.2	A very fast and smart web-dir/file enumeration tool written in C.
lunar	722.a9c64db	A UNIX security auditing tool based on several security frameworks.
luyten	0.5.4	An Open Source Java Decompiler Gui for Procyon.
lynis	3.0.8	Security and system auditing tool to harden Unix/Linux systems
lyricpass	44.b1c8a6a	Tool to generate wordlists based on lyrics.
m3-gen	7.7c656cc	Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass. This tool intended for adversary simulation and red teaming purpose.
mac-robber	1.02	A digital investigation tool that collects data from allocated files in a mounted file system.
macchanger	1.7.0	A small utility to change your NIC's MAC address
machinae	195.360bb07	A tool for collecting intelligence from public sites/feeds about various security-related pieces of data.
maclookup	1:0.4	Lookup MAC addresses in the IEEE MA-L/OUI public listing.
magescan	1.12.9	Scan a Magento site for information.
magicrescue	1.1.9	Find and recover deleted files on block devices
magictree	1.3	A penetration tester productivity tool designed to allow easy and straightforward data consolidation, querying, external command execution and report generation
maigret	866.9f2f4d5	Collect a dossier on a person by username from a huge number of sites.
mail-crawl	0.1	Tool to harvest emails from website.
mailsend-go	108.cb4c77b	A multi-platform command line tool to send mail via SMTP protocol.
make-pdf	0.1.7	This tool will embed javascript inside a PDF document.
maketh	0.2.0	A packet generator that supports forging ARP, IP, TCP, UDP, ICMP and the ethernet header as well.
malcom	708.02e55b9	Analyze a system's network communication using graphical representations of network traffic.
malheur	0.5.4	A tool for the automatic analyze of malware behavior.

malice	0.3.28	VirusTotal Wanna Be - Now with 100% more Hipster.
maligno	2.5	An open source penetration testing tool written in python, that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS.
mallory	134.47094fb	HTTP/HTTPS proxy over SSH.
malmon	0.3	Hosting exploit/backdoor detection daemon. It's written in python, and uses inotify (pyinotify) to monitor file system activity. It checks files smaller then some size, compares their md5sum and hex signatures against DBs with known exploits/backdoor.
malscan	5.773505a	A Simple PE File Heuristics Scanner.
maltego	4.3.1	An open source intelligence and forensics application, enabling to easily gather information about DNS, domains, IP addresses, websites, persons, etc.
maltrail	89611.b14c176866	Malicious traffic detection system.
maltrieve	342.b9e7560	Originated as a fork of mwcrawler. It retrieves malware directly from the sources as listed at a number of sites.
malware-check-tool	1.2	Python script that detects malicious files via checking md5 hashes from an offline set or via the virustotal site. It has http proxy support and an update feature.
malwareanalyser	3.3	A freeware tool to perform static and dynamic analysis on malware.
malwaredetect	0.1	Submits a file's SHA1 sum to VirusTotal to determine whether it is a known piece of malware
malwasm	0.2	Offline debugger for malware's reverse engineering.
malybuzz	1.0	A Python tool focused in discovering programming faults in network software.
mana	68.56bcfcd	A toolkit for rogue access point (evilAP) attacks first presented at Defcon 22.
mando.me	9.8b34f1a	Web Command Injection Tool.
manspider	56.e10bb6a	Spider entire networks for juicy files sitting on SMB shares. Search filenames or file content - regex supported!
manticore	0.3.7.r71.g7f629c94	Symbolic execution tool.

manul	197.f525df9	A coverage-guided parallel fuzzer for open-source and blackbox binaries on Windows, Linux and MacOS.
mapcidr	v1.1.1.r0.g72a8d97	Utility program to perform multiple operations for a given subnet/CIDR ranges.
mara-framework	176.ac4ac88	A Mobile Application Reverse engineering and Analysis Framework.
marc4dasm	6.f11860f	This python-based tool is a disassembler for the Atmel MARC4 (a 4 bit Harvard micro).
marshalsec	10.2dc4018	Java Unmarshaller Security - Turning your data into code execution.
maryam	2:819.99ae85a	Tool to scan Web application and networks and easily and complete the information gathering process.
maskprocessor	0.73	A High-Performance word generator with a per-position configurable charset.
massbleed	20.44b7e85	Automated Pentest Recon Scanner.
masscan	1.3.2	TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes
masscan-automation	26.a170abc	Masscan integrated with Shodan API.
massdns	290.164fd41	A high-performance DNS stub resolver in C.
massexpconsole	1:v2.3.5.r1.g530c880	A collection of tools and exploits with a cli ui for mass exploitation.
mat	0.6.1	Metadata Anonymisation Toolkit composed of a GUI application, a CLI application and a library.
mat2	0.13.3	A metadata removal tool, supporting a wide range of commonly used file formats.
matahari	0.1.30	A reverse HTTP shell to execute commands on remote machines behind firewalls.
matroschka	58.2f026a4	Python steganography tool to hide images or text in images.
mausezahn	0.40	A free fast traffic generator written in C which allows you to send nearly every possible and impossible packet.
mbenum	1.5.0	Queries the master browser for whatever information it has registered.
mboxgrep	0.7.9	A small, non-interactive utility that scans mail folders for messages matching regular expressions. It does matching against basic and extended POSIX regular expressions, and reads and writes a variety of mailbox

		formats.
mdbtools	738.823b32f	Utilities for viewing data and exporting schema from Microsoft Access Database files.
mdcrack	1.2	MD4/MD5/NTLM1 hash cracker
mdk3	v6	WLAN penetration tool
mdk4	4.2	Proof-of-Concept tool to exploit common IEEE 802.11 protocol weaknesses.
mdns-recon	11.69b864e	An mDNS recon tool written in Python.
mdns-scan	0.5	Scan mDNS/DNS-SD published services on the local network.
meanalyzer	1.273.0	Intel Engine Firmware Analysis Tool.
medusa	2.2	Speedy, massively parallel and modular login brute-forcer for network
meg	87.9daab00	Fetch many paths for many hosts - without killing the hosts.
melkor	1.0	An ELF fuzzer that mutates the existing data in an ELF sample given to create orcs (malformed ELFs), however, it does not change values randomly (dumb fuzzing), instead, it fuzzes certain metadata with semi-valid values through the use of fuzzing rules (knowledge base).
memdump	1.01	Dumps system memory to stdout, skipping over holes in memory maps.
memfetch	0.05b	Dumps any userspace process memory without affecting its execution.
memimager	1.0	Performs a memory dump using NtSystemDebugControl.
mentalist	6.953a07b	Mentalist is a graphical tool for custom wordlist generation. It utilizes common human paradigms for constructing passwords and can output the full wordlist as well as rules compatible with Hashcat and John the Ripper.
merlin-server	1.3.0	Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang.
metabigor	59.f012781	Intelligence Tool but without API key.
metacoretex	0.8.0	MetaCoretex is an entirely JAVA vulnerability scanning framework for databases.
metafinder	v1.2.r0.g2caed73	Search for documents in a domain through Search Engines (Google, Bing and Baidu). The objective is to extract metadata.
metaforge	115.7b32693	Auto Scanning to SSL Vulnerability.
metagoofil	78.d1e00fe	An information gathering tool designed for extracting metadata of public documents.
metame	14.8d583a0	A simple metamorphic code engine for arbitrary executables.

metasploit	6.3.15	Advanced open-source platform for developing, testing, and using exploit code
metasploit-autopwn	12.09320cc	db_autopwn plugin of metasploit.
meterssh	18.9a5ed19	A way to take shellcode, inject it into memory then tunnel whatever port you want to over SSH to mask any type of communications as a normal SSH connection.
metoscan	05	Tool for scanning the HTTP methods supported by a webserver. It works by testing a URL and checking the responses for the different requests.
mfcuk	0.3.8	MIFARE Classic Universal toolKit
mfoc	0.10.7+38+gba072f1	Mifare Classic Offline Cracker
mfsniffer	0.1	A python script for capturing unencrypted TSO login credentials.
mft2csv	40.164eb224	Extract $MFT record info and log it to a csv file.
mftcarver	9.7bfcc0a2	Carve $MFT records from a chunk of data (for instance a memory dump).
mftrcrd	16.35c3ac2f	Command line $MFT record decoder.
mftref2name	6.7df9eebb	Resolve file index number to name or vice versa on NTFS. A simple tool that just converts MFT reference number to file name and path, or the other way around.
mibble	2.10.1	An open-source SNMP MIB parser (or SMI parser) written in Java. It can be used to read SNMP MIB files as well as simple ASN.1 files.
microsploit	9.441e132	Fast and easy create backdoor office exploitation using module metasploit packet, Microsoft Office, Open Office, Macro attack, Buffer Overflow.
middler	1.0	A Man in the Middle tool to demonstrate protocol middling attacks.
mikrotik-npk	11.d54e97c	Python tools for manipulating Mikrotik NPK format.
mildew	11.df49c23	Dotmil subdomain discovery tool that scrapes domains from official DoD website directories and certificate transparency logs.
mimikatz	2.2.0_20210810	A little tool to play with Windows security.
mimipenguin	152.880a427	A tool to dump the login password from the current linux user.
mingsweeper	1.00	A network reconnaissance tool designed to facilitate large address space,high speed node discovery and identification.
minimodem	353.bb2f34c	A command-line program which decodes (or generates) audio modem tones at any specified baud rate, using various framing protocols.

minimysqlator	0.5	A multi-platform application used to audit web sites in order to discover and exploit SQL injection vulnerabilities.
miranda-upnp	1.3	A Python-based Universal Plug-N-Play client application designed to discover, query and interact with UPNP devices
miredo	1.2.6	Teredo client and server.
missidentify	1.0	A program to find Win32 applications.
missionplanner	1.3.76	A GroundControl Station for Ardupilot.
mitm	8.bd2b351	A simple yet effective python3 script to perform DNS spoofing via ARP poisoning.
mitm-relay	40.1b74741	Hackish way to intercept and modify non-HTTP protocols through Burp & others.
mitm6	33.8e75884	Pwning IPv4 via IPv6.
mitmap	89.b590f9a	A python program to create a fake AP and sniff data.
mitmap-old	1:0.1	Shell Script for launching a Fake AP with karma functionality and launches ettercap for packet capture and traffic manipulation.
mitmer	22.b01c7fe	A man-in-the-middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.
mitmf	467.0458300	A Framework for Man-In-The-Middle attacks written in Python.
mitmproxy	9.0.1	SSL-capable man-in-the-middle HTTP proxy
mkbrutus	27.ddd5f8e	Password bruteforcer for MikroTik devices or boxes running RouterOS.
mkyara	3.8147f91	Tool to generate YARA rules based on binary code.
mobiusft	1.12	An open-source forensic framework written in Python/GTK that manages cases and case items, providing an abstract interface for developing extensions.
mobsf	1:1833.b43b561a	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.
modlishka	v.1.1.0.r47.gfb7f111	A powerful and flexible HTTP reverse proxy.
modscan	0.1	A new tool designed to map a SCADA MODBUS TCP based network.
moloch	0.11.3	An open source large scale IPv4 full PCAP capturing, indexing and database system.
mongoaudit	222.70b83e8	A powerful MongoDB auditing and pentesting tool .

monocle	1.0	A local network host discovery tool. In passive mode, it will listen for ARP request and reply packets. In active mode, it will send ARP requests to the specific IP range. The results are a list of IP and MAC addresses present on the local network.
monsoon	261.f4f9852	A fast HTTP enumerator that allows you to execute a large number of HTTP requests.
moonwalk	v1.0.0.r18.g68d5be1	Cover your tracks during Linux Exploitation by leaving zero traces on system logs and filesystem timestamps.
mooscan	1:10.82963b0	A scanner for Moodle LMS.
morpheus	165.5d81c9e	Automated Ettercap TCP/IP Hijacking Tool.
morxbook	1.0	A password cracking tool written in perl to perform a dictionary-based attack on a specific Facebook user through HTTPS.
morxbrute	1.01	A customizable HTTP dictionary-based password cracking tool written in Perl
morxbtcrack	1.0	Single Bitcoin private key cracking tool released.
morxcoinpwn	1.0	Mass Bitcoin private keys brute forcing/Take over tool released.
morxcrack	1.2	A cracking tool written in Perl to perform a dictionary-based attack on various hashing algorithm and CMS salted-passwords.
morxkeyfmt	1.0	Read a private key from stdin and output formatted data values.
morxtraversal	1.0	Path Traversal checking tool.
morxtunel	1.0	Network Tunneling using TUN/TAP interfaces over TCP tool.
morxtunnel	1.0	Network Tunneling using TUN/TAP interfaces over TCP tool.
mosca	130.a7e725d	Static analysis tool to find bugs like a grep unix command.
mosquito	39.fe54831	XSS exploitation tool - access victims through HTTP proxy.
mots	5.34017ca	Man on the Side Attack - experimental packet injection and detection.
motsa-dns-spoofing	2.6ac6980	ManOnTheSideAttack-DNS Spoofing.
mousejack	5.58b69c1	Wireless mouse/keyboard attack with replay/transmit poc.
mp3nema	0.4	A tool aimed at analyzing and capturing data that is hidden between frames in an MP3 file or stream, otherwise noted as "out of band" data.
mptcp	1.9.0	A tool for manipulation of raw packets that allows a large number of options.
mptcp-abuse	6.b0eeb27	A collection of tools and resources to explore MPTCP on your network.

		Initially released at Black Hat USA 2014.
mqtt-pwn	43.40368e5	A one-stop-shop for IoT Broker penetration-testing and security assessment operations.
mrkaplan	1:1.1.1	Help red teamers to stay hidden by clearing evidence of execution.
mrsip	110.bdd98ad	SIP-Based Audit and Attack Tool.
mrtparse	521.23e569c	A module to read and analyze the MRT format data.
ms-sys	2.7.0	A tool to write Win9x-.. master boot records (mbr) under linux - RTM!
msf-mpc	35.8007ef2	Msfvenom payload creator.
msfdb	16.09c603b	Manage the metasploit framework database.
msfenum	36.6c6b77e	A Metasploit auto auxiliary script.
msmailprobe	1.c01c8bf	Office 365 and Exchange Enumeration tool.
mssqlscan	0.8.4	A small multi-threaded tool that scans for Microsoft SQL Servers.
msvpwn	1:65.328921b	Bypass Windows' authentication via binary patching.
mtr	0.95	Combines the functionality of traceroute and ping into one tool (CLI version)
mtscan	153.185d099	Mikrotik RouterOS wireless scanner.
mubeng	160.05461a5	An incredibly fast proxy checker & IP rotator with ease.
multiinjector	0.4	Automatic SQL injection utility using a lsit of URI addresses to test parameter manipulation.
multimac	1.0.3	Multiple MACs on an adapter
multimon-ng	1.2.0	An sdr decoder, supports pocsag, ufsk, clipfsk, afsk, hapn, fsk, dtmf, zvei.
multiscanner	1559.86e0145	Modular file scanning/analysis framework.
multitun	1:1.319a134	Tunnel arbitrary traffic through an innocuous WebSocket.
munin-hashchecker	237.3b5558e	Online hash checker for Virustotal and other services
muraena	178.cec3b66	Almost-transparent reverse proxy to automate phishing and post-phishing activities.
mutator	51.164132d	This project aims to be a wordlist mutator with hormones, which means that some mutations will be applied to the result of the ones that have been already done, resulting in something like: corporation -> C0rp0r4t10n_2012
mwebfp	16.a800b98	Mass Web Fingerprinter.
mxtract	90.0b34376	Memory Extractor & Analyzer.

mybff	94.6547c51	A Brute Force Framework.
myjwt	195.73c4d58	This cli is for pentesters, CTF players, or dev. You can modify your jwt, sign, inject, etc.
mylg	659.faba867	Network Diagnostic Tool.
mysql2sqlite	1:14.e5b2c31	Converts a mysqldump file into a Sqlite 3 compatible file.
n1qlmap	2.5365444	An N1QL exploitation tool.
naabu	781.7e27650	A fast port scanner written in go with focus on reliability and simplicity.
nacker	23.b67bb39	A tool to circumvent 802.1x Network Access Control on a wired LAN.
naft	0.0.9	Network Appliance Forensic Toolkit.
narthex	v1.2.r7.g8b78746	Modular personalized dictionary generator.
nasnum	5.df5df19	Script to enumerate network attached storages.
nbname	1.0	Decodes and displays all NetBIOS name packets it receives on UDP port 137 and more!
nbnspoof	1.0	NBNSpoof - NetBIOS Name Service Spoofer
nbtenum	3.3	A utility for Windows that can be used to enumerate NetBIOS information from one host or a range of hosts.
nbtool	1:2.bf90c76	Some tools for NetBIOS and DNS investigation, attacks, and communication.
nbtscan	1.7.2	NBTscan is a program for scanning IP networks for NetBIOS name information.
ncpfs	2.2.6	Allows you to mount volumes of NetWare servers under Linux.
ncrack	0.7	A high-speed network authentication cracking tool
necromant	4.53930c2	Python Script that search unused Virtual Hosts in Web Servers.
needle	579.891b660	The iOS Security Testing Framework.
neglected	1:8.68d02b3	Facebook CDN Photo Resolver.
neighbor-cache-fingerprinter	83.f1e596f	An ARP based Operating System version scanner.
nemesis	329.b1d398c	command-line network packet crafting and injection utility
neo-regeorg	1:v5.0.1.r7.g6bd94c6	Improved version of reGeorg, HTTP tunneling pivot tool
net-creds	87.07a25e1	Sniffs sensitive data from interface or pcap.
netactview	0.6.4	A graphical network connections viewer similar in functionality to netstat

netattack	2:24.230b856	Python script to scan and attack wireless networks.
netbios-share-scanner	1.0	This tool could be used to check windows workstations and servers if they have accessible shared resources.
netbus	1.6	NetBus remote adminsitration tool
netcommander	1.3	An easy-to-use arp spoofing tool.
netcon	0.1	A network connection establishment and management script.
netdiscover	218.ff28964	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.
netkit-bsd-finger	0.17	BSD-finger ported to Linux.
netkit-rusers	0.17	Logged in users; Displays who is logged in to machines on local network.
netkit-rwho	0.17	Remote who client and server (with Debian patches).
netmap	0.1.3	Can be used to make a graphical representation of the surounding network.
netmask	2.4.4	Helps determine network masks
netreconn	1.78	A collection of network scan/recon tools that are relatively small compared to their larger cousins.
netripper	84.c763bd0	Smart traffic sniffing for penetration testers.
netscan	1.0	Tcp/Udp/Tor port scanner with: synpacket, connect TCP/UDP and socks5 (tor connection).
netscan2	1:58.a1db723	Active / passive network scanner.
netsed	1.3	Small and handful utility design to alter the contents of packets forwarded thru network in real time.
netsniff-ng	0.6.8	A high performance Linux network sniffer for packet inspection.
netstumbler	0.4.0	Well-known wireless AP scanner and sniffer.
nettacker	0.0.3.6.r128.gd2ae55a3	Automated Penetration Testing Framework.
network-app-stress-tester	19.df75391	Network Application Stress Testing Yammer.
networkmap	58.f5faf17	Post-exploitation network mapper.
networkminer	2.7.3	A Network Forensic Analysis Tool for advanced Network Traffic Analysis, sniffer and packet analyzer.
netz	v0.1.0.r8.g375	Discover internet-wide misconfigurations while drinking coffee.

	4e56	
netzob	1.0.2	An open source tool for reverse engineering, traffic generation and fuzzing of communication protocols.
nexfil	43.4d93c57	OSINT tool for finding profiles by username.
nextnet	3.c8dc7a6	Pivot point discovery tool.
nfcutils	0.3.2	Provides a simple 'lsnfc' command that list tags which are in your NFC device field
nfdump	1.6.23	A set of tools to collect and process netflow data.
nfex	2.5	A tool for extracting files from the network in real-time or post-capture from an offline tcpdump pcap savefile.
nfspy	1.0	A Python library for automating the falsification of NFS credentials when mounting an NFS share.
nfsshell	19980519	Userland NFS command tool.
ngrep	1.47	A grep-like utility that allows you to search for network packets on an interface.
ngrok	3.2.2	A tunneling, reverse proxy for developing and understanding networked, HTTP services.
nield	38.0c0848d	A tool to receive notifications from kernel through netlink socket, and generate logs related to interfaces, neighbor cache(ARP,NDP), IP address(IPv4,IPv6), routing, FIB rules, traffic control.
nikto	2.1.6	A web server scanner which performs comprehensive tests against web servers for multiple items
nili	39.285220a	Tool for Network Scan, Man in the Middle, Protocol Reverse Engineering and Fuzzing.
nimbostratus	54.c7c206f	Tools for fingerprintinging and exploiting Amazon cloud infrastructures.
nipe	302.9e628df	A script to make Tor Network your default gateway.
nipper	0.11.7	Network Infrastructure Parser
nirsoft	1.23.30	Unique collection of small and useful freeware utilities.
nishang	0.7.6	Using PowerShell for Penetration Testing.
njsscan	0.3.1	A static application testing (SAST) tool that can find insecure code patterns in your node.js applications.
nkiller2	2.0	A TCP exhaustion/stressing tool.
nmap	7.93	Utility for network discovery and security auditing

nmap-parse-output	23.6405abf	Converts/manipulates/extracts data from a nmap scan output.
nmbscan	1.2.6	Tool to scan the shares of a SMB/NetBIOS network, using the NMB/SMB/NetBIOS protocols.
nohidy	67.22c1283	The system admins best friend, multi platform auditing tool.
nomorexor	2.84489f9	Tool to help guess a files 256 byte XOR key by using frequency analysis
noriben	171.2855a5e	Portable, Simple, Malware Analysis Sandbox.
nosqlattack	98.a5b0329	Python tool to automate exploit MongoDB server IP on Internet and disclose the database data by MongoDB default configuration weaknesses and injection attacks.
nosqli	37.6fce3eb	NoSQL scanner and injector.
nosqli-user-pass-enum	18.1b3713a	Script to enumerate usernames and passwords from vulnerable web applications running MongoDB.
nosqlmap	296.9502b8c	Automated Mongo database and NoSQL web application exploitation tool
notspikefile	1:0.1	A Linux based file format fuzzing tool
novahot	23.69857bb	A webshell framework for penetration testers.
nray	59.30517fd	Distributed port scanner.
nsdtool	0.1	A netgear switch discovery tool. It contains some extra features like bruteoforce and setting a new password.
nsearch	353.bd8205b	Minimal script to help find script into the nse database.
nsec3map	20.1263537	A tool to enumerate the resource records of a DNS zone using its DNSSEC NSEC or NSEC3 chain.
nsec3walker	20101223	Enumerates domain names using DNSSEC
nsia	1.0.6	A website scanner that monitors websites in realtime in order to detect defacements, compliance violations, exploits, sensitive information disclosure and other issues.
nsntrace	81.4d02e74	Perform network trace of a single process by using network namespaces.
nsoq	1.9.5	A Network Security Tool for packet manipulation that allows a large number of options.
ntds-decode	0.1	This application dumps LM and NTLM hashes from active accounts stored in an Active Directory database.
ntdsxtract	34.7fa1c8c	Active Directory forensic framework.
ntfs-file-	6.f2b23d72	Extract files off NTFS.

extractor		
ntfs-log-tracker	1:1.6	This tool can parse $LogFile, $UsnJrnl of NTFS.
ntlm-challenger	8.bd61ef6	Parse NTLM over HTTP challenge messages.
ntlm-scanner	6.4b29329	A simple python tool based on Impacket that tests servers for various known NTLM vulnerabilities.
ntlm-theft	20.81589ea	A tool for generating multiple types of NTLMv2 hash theft files.
ntlmrecon	75.da150d6	A tool to enumerate information from NTLM authentication enabled web endpoints.
ntp-fingerprint	0.1	An active fingerprinting utility specifically designed to identify the OS the NTP server is running on.
ntp-ip-enum	0.1	Script to pull addresses from a NTP server using the monlist command. Can also output Maltego resultset.
ntpdos	1:4.3fe389b	Create a DDOS attack using NTP servers.
nuclei	1:v2.9.1.r0.g5b22ca84	Nuclei is a fast tool for configurable targeted scanning based on templates offering massive extensibility and ease of use.
nullinux	123.a647159	Tool that can be used to enumerate OS information, domain information, shares, directories, and users through SMB null sessions.
nullscan	1.0.1	A modular framework designed to chain and automate security tests.
nxcrypt	32.6ae06b5	NXcrypt - python backdoor framework.
nzyme	1.2.2	WiFi defense system.
o-saft	5211.eff0a006	A tool to show informations about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations.
o365enum	17.2d4f99c	Username enumeration and password enuming tool aimed at Microsoft O365.
o365spray	146.a794c97	Auto Scanning to SSL Vulnerability.
oat	1.3.1	A toolkit that could be used to audit security within Oracle database servers.
obevilion	409.29fbe9d	Another archive cracker created in python | cracking [zip/7z/rar].
obexstress	0.1	Script for testing remote OBEX service for some potential vulnerabilities.
obfs4proxy	0.0.13	A pluggable transport proxy written in Go.
obfsproxy	0.2.13	A pluggable transport proxy written in Python
objdump2shellcode	28.c2d6120	A tool I have found incredibly useful whenever creating custom shellcode.

objection	1.11.0	Instrumented Mobile Pentest Framework.
oclhashcat	1:2.01	Worlds fastest WPA cracker with dictionary mutation engine.
ocs	0.2	Compact mass scanner for Cisco routers with default telnet/enable passwords.
octopwnweb	14.e0f83ee	Internal pentest framework running in your browser via WebAssembly, powerd by Pyodide
office-dde-payloads	34.53291f9	Collection of scripts and templates to generate Office documents embedded with the DDE, macro-less command execution technique.
ofp-sniffer	230.4b79b6c	An OpenFlow sniffer to help network troubleshooting in production networks.
ohrwurm	1.7a1182a	A small and simple RTP fuzzer.
okadminfinder	80.b367ec7	Tool to find admin panels / admin login pages.
oledump	0.0.69	Analyze OLE files (Compound File Binary Format). These files contain streams of data. This tool allows you to analyze these streams.
oletools	1:0.54.1	Tools to analyze Microsoft OLE2 files.
ollydbg	201g	A 32-bit assembler-level analysing debugger
omen	19.10aa99e	Ordered Markov ENumerator - Password Guesser.
omnibus	129.88dbf5d	OSINT tool for intelligence collection, research and artifact management.
omnihash	70.870e9ae	Hash files, strings, input streams and network resources in various common algorithms simultaneously.
one-lin3r	63.9fdfa5f	Gives you one-liners that aids in penetration testing and more.
onesixtyone	0.7	An SNMP scanner that sends multiple SNMP requests to multiple IP addresses
onetwopunch	v1.0.0.r2.gd4ab4e8	Use unicornscan to quickly scan all open ports, and then pass the open ports to nmap for detailed scans.
onioff	84.34dc309	An onion url inspector for inspecting deep web links.
oniongrok	v1.0.13.r1.g1a01be8	Onion addresses for anything.
onionscan	130.da42865	Scan Onion Services for Security Issues.
onionsearch	43.ab4095c	Script that scrapes urls on different ".onion" search engines.
onionshare	2.6	Securely and anonymously share a file of any size.
open-iscsi	2.1.8	iSCSI userland tools
opendoor	422.d1ed311	OWASP Directory Access scanner.

openpuff	4.01	Yet not another steganography SW.
openrisk	v0.0.1.r7.g218de01	Generates a risk score based on the results of a Nuclei scan using OpenAI's GPT-3 model.
openscap	1.3.7.r48.ga6d6753f1	Open Source Security Compliance Solution.
openstego	0.8.4	A tool implemented in Java for generic steganography, with support for password-based encryption of the data.
opensvp	65.df54ed8	A security tool implementing "attacks" to be able to the resistance of firewall to protocol level attack.
openvas	6.0.1	The OpenVAS scanning Daemon
openvas-cli	1.4.5	The OpenVAS Command-Line Interface
openvas-libraries	9.0.2	The OpenVAS libraries
openvas-manager	7.0.3	A layer between the OpenVAS Scanner and various client applications
openvas-scanner	22.4.0	The OpenVAS scanning Daemon
operative	1:148.163acdf	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 ...).
ophcrack	3.8.0	Windows password cracker based on rainbow tables
orakelcrackert	1.00	This tool can crack passwords which are encrypted using Oracle's latest SHA1 based password protection algorithm.
origami	2.1.0	Aims at providing a scripting tool to generate and analyze malicious PDF files.
orjail	200.ae38ba2	A more secure way to force programs to exclusively use tor network.
oscanner	1.0.6	An Oracle assessment framework developed in Java.
osert	80.f6cef2d	Markdown Templates for Offensive Security exam reports.
osfooler-ng	2.c0b20d6	Prevents remote active/passive OS fingerprinting by tools like nmap or p0f.
osi.ig	101.4debaa2	Instagram OSINT Tool gets a range of information from an Instagram account.
osint-spy	25.03dcf48	Performs OSINT scan on email/domain/ip_address/organization.

osinterator	3.8447f58	Open Source Toolkit for Open Source Intelligence Gathering.
osintgram	1.3.r5.g50d44fd	OSINT tool offering an interactive shell to perform analysis on Instagram account of any users by its nickname.
osrframework	840.e02a6e9	A project focused on providing API and tools to perform more accurate online researches.
osslsigncode	333.b967175	A small tool that implements part of the functionality of the Microsoft tool signtool.exe.
ostinato	0.9	An open-source, cross-platform packet/traffic generator and analyzer with a friendly GUI. It aims to be "Wireshark in Reverse" and thus become complementary to Wireshark.
osueta	82.2ee8068	A simple Python script to exploit the OpenSSH User Enumeration Timing Attack.
otori	0.3	A python-based toolbox intended to allow useful exploitation of XML external entity ("XXE") vulnerabilities.
outguess	0.2	A universal steganographic tool.
outlook-webapp-brute	1.61d7177	Microsoft Outlook WebAPP Brute.
owabf	1.3	Outlook Web Access bruteforcer tool.
OWASP Broken Web Applications Project	1.2	OWASP Broken Web Applications Project is a collection of vulnerable web applications that is distributed on a Virtual Machine. The Broken Web Applications (BWA) Project produces a Virtual Machine running a variety of applications with known vulnerabilities for those interested in: learning about web application security; testing manual assessment techniques; testing automated tools; testing source code analysis tools; observing web attacks; testing WAFs and similar code technologies.
OWASP Mutillidae II	2.6.67	OWASP Mutillidae II is a free, open source, deliberately vulnerable web-application providing a target for web-security enthusiast. Mutillidae can be installed on Linux and Windows using LAMP, WAMP, and XAMMP. It is pre-installed on SamuraiWTF and OWASP BWA. The existing version can be updated on these platforms. With dozens of vulns and hints to help the user; this is an easy-to-use web hacking environment designed for labs, security enthusiast, classrooms, CTF, and vulnerability assessment tool targets. Mutillidae has been used in graduate security courses, corporate web sec training courses, and as an "assess the assessor" target for vulnerability assessment software.

owasp-bywaf	26.e730d1b	A web application penetration testing framework (WAPTF).
owasp-zsc	315.5bb9fed	Shellcode/Obfuscate Code Generator.
owtf	2187.af993ecb	The Offensive (Web) Testing Framework.
p0f	3.09b	Purely passive TCP/IP traffic fingerprinting tool
pacaur	4.7.10	An AUR helper that minimizes user interaction.
pack	0.0.4	Password Analysis and Cracking Kit
packer	1.8.7	tool for creating identical machine images for multiple platforms from a single source configuration
packer-io	1.2.4	tool for creating identical machine images for multiple platforms from a single source configuration
packerid	1.4	Script which uses a PEiD database to identify which packer (if any) is being used by a binary.
packet-o-matic	351	A real time packet processor. Reads the packet from an input module, match the packet using rules and connection tracking information and then send it to a target module.
packeth	2.1	A Linux GUI packet generator tool for ethernet.
packetq	280.740a99e	A tool that provides a basic SQL-frontend to PCAP-files.
packetsender	877.d548e7e	An open source utility to allow sending and receiving TCP and UDP packets.
packit	1.0	A network auditing tool. Its value is derived from its ability to customize, inject, monitor, and manipulate IP traffic.
pacu	1166.76d4474	The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.
pacumen	1.92a0884	Packet Acumen - Analyse encrypted network traffic and more (side-channel attacks).
padbuster	11.50e4a3e	Automated script for performing Padding Oracle attacks.
pafish	193.b497899	A demonstration tool that employs several techniques to detect sandboxes and analysis environments in the same way as malware families do.
pagodo	127.3fa6cfb	Google dork script to collect potentially vulnerable web pages and applications on the Internet.
paketto	1.10	Advanced TCP/IP Toolkit.
panhunt	63.ec87e88	Searches for credit card numbers (PANs) in directories.
panoptic	185.df35a6c	A tool that automates the process of search and retrieval of content for

		common log and config files through LFI vulnerability.
pappy-proxy	77.e1bb049	An intercepting proxy for web application testing.
parameth	56.8da6f27	This tool can be used to brute discover GET and POST parameters.
parampampam	45.9171018	This tool for brute discover GET and POST parameters.
paranoic	1.7	A simple vulnerability scanner written in Perl.
paros	3.2.13	Java-based HTTP/HTTPS proxy for assessing web app vulnerabilities. Supports editing/viewing HTTP messages on-the-fly, spiders, client certificates, proxy-chaining, intelligent scanning for XSS and SQLi, etc.
Parrot Security OS	4.6	Security GNU/Linux distribution designed with cloud pentesting and IoT security in mind. It includes a full portable laboratory for security and digital forensics experts, but it also includes all you need to develop your own softwares or protect your privacy with anonymity and crypto tools.
parse-evtx	3.a4b02b9	A tool to parse the Windows XML Event Log (EVTX) format.
parsero	81.e5b585a	A robots.txt audit tool.
pasco	20040505_1	Examines the contents of Internet Explorer's cache files for forensic purposes
pass-station	v1.4.0.r24.gd6b481c	CLI & library to search for default credentials among thousands of Products / Vendors.
passcracking	20131214	A little python script for sending hashes to passcracking.com and milw0rm
passe-partout	0.1	Tool to extract RSA and DSA private keys from any process linked with OpenSSL. The target memory is scanned to lookup specific OpenSSL patterns.
passhunt	5.332f374	Search drives for documents containing passwords.
passivedns	292.c411c46	A network sniffer that logs all DNS server replies for use in a passive DNS setup.
pastejacker	12.ed9f153	Hacking systems with the automation of PasteJacking attacks.
pastemonitor	8.b3551f1	Scrape Pastebin API to collect daily pastes, setup a wordlist and be alerted by email when you have a match..
pasv-agrsv	57.6bb54f7	Passive recon / OSINT automation script.
patator	1:214.b97f8b2	A multi-purpose bruteforcer.
patchkit	37.95dc699	Powerful binary patching from Python.
pathzuzu	64.4f4533c	Checks for PATH substitution vulnerabilities and logs the commands executed by the vulnerable executables.

payloadmask	17.58e0525	Web Payload list editor to use techniques to try bypass web application firewall.
payloadsalltheth ings	1715.579207a	A list of useful payloads and bypass for Web Application Security and Pentest/CTF.
pblind	1.0	Little utility to help exploiting blind sql injection vulnerabilities.
pbscan	10.566c3d7	Faster and more efficient stateless SYN scanner and banner grabber due to userland TCP/IP stack usage.
pcapfex	60.c51055a	Packet CAPture Forensic Evidence eXtractor.
pcapfix	1.1.7	Tries to repair your broken pcap and pcapng files.
pcapsipdump	0.2	A tool for dumping SIP sessions (+RTP traffic, if available) to disk in a fashion similar to 'tcpdump -w' (format is exactly the same), but one file per sip session (even if there is thousands of concurrect SIP sessions).
pcapteller	1.1	A tool designed for traffic manipulation and replay.
pcapxray	274.1721645	A Network Forensics Tool - To visualize a Packet Capture offline as a Network Diagram including device identification, highlight important communication and file extraction.
pcileech	4.15	Tool, which uses PCIe hardware devices to read and write from the target system memory.
pcode2code	6.65ae983	VBA p-code decompiler.
pcredz	81.4565195	A tool that extracts credit card numbers, NTLM(DCE-RPC, HTTP, SQL, LDAP, etc), Kerberos (AS-REQ Pre-Auth etype 23), HTTP Basic, SNMP, POP, SMTP, FTP, IMAP, and more from a pcap file or from a live interface.
pdblaster	4.fc8abb3	Extract PDB file paths from large sample sets of executable files.
pdf-parser	0.7.6	Parses a PDF document to identify the fundamental elements used in the analyzed file.
pdfbook-analyzer	1:2	Utility for facebook memory forensics.
pdfcrack	0.20	Password recovery tool for PDF-files.
pdfgrab	15.1327508	Tool for searching pdfs withthin google and extracting pdf metadata.
pdfid	0.2.8	Scan a file to look for certain PDF keywords.
pdfresurrect	0.12	A tool aimed at analyzing PDF documents.
pdfwalker	1:7.64c17f0	Frontend to explore the internals of a PDF document with Origami
pdgmail	1.0	A password dictionary attack tool that targets windows authentication via

		the SMB protocol.
pe-bear	0.5.5.7	A freeware reversing tool for PE files.
pe-sieve	0.3.5	Scans a given process. Recognizes and dumps a variety of potentially malicious implants (replaced/injected PEs, shellcodes, hooks, in-memory patches).
peach	3.0.202	A SmartFuzzer that is capable of performing both generation and mutation based fuzzing.
peach-fuzz	55.404e8ee	Simple vulnerability scanning framework.
peass	20230425.bd7331ea.r7.g2963e47	Privilege Escalation Awesome Scripts SUITE (with colors).
peda	1.2	Python Exploit Development Assistance for GDB
peepdf	0.4.2	A Python tool to explore PDF files in order to find out if the file can be harmful or not
peepingtom	1:56.bc6f4d8	A tool to take screenshots of websites. Much like eyewitness.
peframe	135.70683b6	Tool to perform static analysis on (portable executable) malware.
pemcrack	12.66e02b8	Cracks SSL PEM files that hold encrypted private keys. Brute forces or dictionary cracks.
pemcracker	9.a741c93	Tool to crack encrypted PEM files.
penbox	81.3b77c69	A Penetration Testing Framework - The Tool With All The Tools.
pencode	32.47e5784	Complex payload encoder.
pentbox	1.8	A security suite that packs security and stability testing oriented tools for networks and systems.
pentestly	1798.93d1b39	Python and Powershell internal penetration testing framework.
pentmenu	218.2e45233	A bash script for recon and DOS attacks.
pepe	13.b81889b	Collect information about email addresses from Pastebin.
pepper	18.9dfcade	An open source script to perform malware static analysis on Portable Executable.
periscope	3.2	A PE file inspection tool.
perl-image-exiftool	12.60	Reader and rewriter of EXIF informations that supports raw files
petools	1.9.762	Portable executable (PE) manipulation toolkit.
pev	0.81	Command line based tool for PE32/PE32+ file analysis.

pextractor	0.18b	A forensics tool that can extract all files from an executable file created by a joiner or similar.
pfff	0.29	Tools and APIs for code analysis, visualization and transformation
pftriage	79.d7ad183	Python tool and library to help analyze files during malware triage and analysis.
pgdbf	113.4e84775	Convert XBase / FoxPro databases to PostgreSQL
phantap	64.815c312	An 'invisible' network tap aimed at red teams.
phantom-evasion	103.2cd0673	Antivirus evasion tool written in python.
phemail	28.302b24d	A python open source phishing email tool that automates the process of sending phishing emails as part of a social engineering test.
phishery	14.5743953	An SSL Enabled Basic Auth Credential Harvester with a Word Document Template URL Injector.
phishingkithunter	20.ac9bd1e	Find phishing kits which use your brand/organization's files and image.
phoneinfoga	v2.10.3.r1.gf6a458d	Information gathering & OSINT framework for phone numbers.
phonesploit	51.0193f9e	Adb exploiting tools.
phonia	593.8ae14ff	Advanced toolkits to scan phone numbers using only free resources.
phoss	0.1.13	Sniffer designed to find HTTP, FTP, LDAP, Telnet, IMAP4, VNC and POP3 logins.
photon	326.d4af460	Incredibly fast crawler which extracts urls, emails, files, website accounts and much more.
php-findsock-shell	2.b8a984f	A Findsock Shell implementation in PHP + C.
php-malware-finder	0.3.4.r81.g1b85a73	Detect potentially malicious PHP files.
php-mt-seed	4.0	PHP mt_rand() seed cracker
php-rfi-payload-decoder	30.bd42caa	Decode and analyze RFI payloads developed in PHP.
php-vulnerability-hunter	1.4.0.20	An whitebox fuzz testing tool capable of detected several classes of vulnerabilities in PHP web applications.
phpggc	508.bb22d2a	A library of PHP unserialize() payloads along with a tool to generate them,

		from command line or programmatically.
phpsploit	1011.7b262f6	Stealth post-exploitation framework.
phpstan	9076.01ce76a20	PHP Static Analysis Tool - discover bugs in your code without running it.
phpstress	5.f987a7e	A PHP denial of service / stress test for Web Servers running PHP-FPM or PHP-CGI.
phrasendrescher	1:1.2.2c	A modular and multi processing pass phrase cracking tool
pidense	29.ef26704	Monitor illegal wireless network activities. (Fake Access Points)
pin	3.11.r97998	A dynamic binary instrumentation tool.
pingcastle	2.10.1.1	Active Directory scanning tool.
pintool	24.d538a79	This tool can be useful for solving some reversing challenges in CTFs events.
pintool2	5.1c1af91	Improved version of pintool.
pip3line	2:92.5e27195	The Swiss army knife of byte manipulation.
pipal	3.3.2.r16.g3b9950d	A password analyser.
pipeline	19.f4935c9	Designed to aid in targeted brute force password cracking attacks.
pirana	0.3.1	Exploitation framework that tests the security of a email content filter.
pivotsuite	19.9078d1e	A portable, platform independent and powerful network pivoting toolkit.
pixd	7.873db72	Colourful visualization tool for binary files.
pixiewps	1.4.2	An offline WPS bruteforce utility.
pixload	79.85077e1	Set of tools for creating/injecting payload into images (hiding backdoors). The following image types are currently supported: BMP, GIF, JPG, PNG, WebP.
pkcrack	1.2.2	A PkZip encryption cracker.
pkinittools	8.0f7f9a5	Tools for Kerberos PKINIT and relaying to AD CS.
pkt2flow	69.868a2e8	A simple utility to classify packets into flows.
plasma	922.ec7df9b	An interactive disassembler for x86/ARM/MIPS. It can generates indented pseudo-code with colored syntax.
plasma-disasm	922.ec7df9b	An interactive disassembler for x86/ARM/MIPS. It can generates indented pseudo-code with colored syntax.
plcscan	0.1	This is a tool written in Python that will scan for PLC devices over s7comm or modbus protocols.

plecost	104.4895e34	Wordpress finger printer Tool.
plown	13.ccf998c	A security scanner for Plone CMS.
plumber	18.3f1be68	A python implementation of a grep friendly ftrace wrapper.
plumber.py	18.3f1be68	A python implementation of a grep friendly ftrace wrapper.
plutil	1.6	Converts .plist files between binary and UTF-8 (editable) text formats.
pmacct	4281.db67590d	Small set of multi-purpose passive network monitoring tools [NetFlow IPFIX sFlow libpcap BGP BMP IGP Streaming Telemetry].
pmap	1.10	Passively discover, scan, and fingerprint link-local peers by the background noise they generate (i.e. their broadcast and multicast traffic).
pmapper	82.91d2e60	A tool for quickly evaluating IAM permissions in AWS.
pmcma	1.00	Automated exploitation of invalid memory writes (being them the consequences of an overflow in a writable section, of a missing format string, integer overflow, variable misuse, or any other type of memory corruption).
pmdump	1.2	A tool that lets you dump the memory contents of a process to a file without stopping the process.
pngcheck	3.0.3	Verifies the integrity of PNG, JNG and MNG files by checking the CRCs and decompressing the image data.
pnscan	1.14.1	A parallel network scanner that can be used to survey TCP network services.
pocsuite	430.877d1b1	An open-sourced remote vulnerability testing framework developed by the Knownsec Security Team.
poison	1.5.41	A fast, asynchronous syn and udp scanner.
poly	52.4e6f189	A python script that generates polymorphic webshells. Use it to encode your favourite shell and make it practically undetectable.
polyswarm	2.9.2	An interface to the public and private PolySwarm APIs.
polyswarm-api	0.5.3	An interface to the public and private PolySwarm APIs.
pompem	141.3ebe768	A python exploit tool finder.
poracle	68.dcc00b0	A tool for demonstrating padding oracle attacks.
portia	39.2e6e608	Automate a number of techniques commonly performed on internal network penetration tests after a low privileged account has been compromised.
portmanteau	1.0	An experimental unix driver IOCTL security tool that is useful for fuzzing and discovering device driver attack surface.

portspoof	128.8b5596a	This program's primary goal is to enhance OS security through a set of new techniques.
postenum	116.9cd9d7e	Clean, nice and easy tool for basic/advanced privilege escalation techniques.
posttester	0.1	A jar file that will send POST requests to servers in order to test for the hash collision vulnerability discussed at the Chaos Communication Congress in Berlin.
powercloud	21.0928303	Deliver powershell payloads via DNS TXT via CloudFlare using PowerShell.
powerfuzzer	1_beta	Powerfuzzer is a highly automated web fuzzer based on many other Open Source fuzzers available (incl. cfuzzer, fuzzled, fuzzer.pl, jbrofuzz, webscarab, wapiti, Socket Fuzzer). It can detect XSS, Injections (SQL, LDAP, commands, code, XPATH) and others.
powerlessshell	113.7159552	PowerLessShell rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe. You can also execute raw shellcode using the same approach.
powermft	5.76574543	Powerful commandline $MFT record editor.
powerops	32.13fe55b	PowerShell Runspace Portable Post Exploitation Tool aimed at making Penetration Testing with PowerShell "easier".
powershdll	72.62cfa17	Run PowerShell with rundll32. Bypass software restrictions.
powersploit	591.d943001	A PowerShell Post-Exploitation Framework.
powerstager	14.0149dc9	A payload stager using PowerShell.
pown	332.0e32edf	Security testing and exploitation toolkit built on top of Node.js and NPM.
ppee	1.12	A Professional PE file Explorer for reversers, malware researchers and those who want to statically inspect PE files in more details.
ppfuzz	31.80982ec	A fast tool to scan client-side prototype pollution vulnerability written in Rust.
ppmap	v1.2.0.r15.g9426af6	A scanner/exploitation tool written in GO, which leverages client-side Prototype Pollution to XSS by exploiting known gadgets.
ppscan	0.3	Yet another port scanner with HTTP and FTP tunneling support.
pr0cks	1:20.bcfcf2d	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.
prads	1132.e631f4f	Is a "Passive Real-time Asset Detection System".

praeda	48.1dc2220	An automated data/information harvesting tool designed to gather critical information from various embedded devices.
preeny	110.aaef77f	Some helpful preload libraries for pwning stuff.
pret	106.8ae5210	Printer Exploitation Toolkit - The tool that made dumpster diving obsolete.
princeprocessor	1:132.bffda8c	Standalone password candidate generator using the PRINCE algorithm.
procdump	63.5f23548	Generate coredumps based off performance triggers.
proctal	482.67bf7e8	Provides a command line interface and a C library to manipulate the address space of a running program on Linux.
procyon	0.6	A suite of Java metaprogramming tools focused on code generation and analysis.
profuzz	9.aa6dded	Simple PROFINET fuzzer based on Scapy.
prometheus	176.a316d66	A Firewall analyzer written in ruby
prometheus-firewall	176.a316d66	A Firewall analyzer written in ruby
promiscdetect	1.0	Checks if your network adapter(s) is running in promiscuous mode, which may be a sign that you have a sniffer running on your computer.
propecia	2	A fast class scanner that scans for a specified open port with banner grabbing
protos-sip	2	SIP test suite.
protosint	26.1ee6ee4	Python script that helps you investigate Protonmail accounts and ProtonVPN IP addresses.
prowler	2505.848122b0	Tool for AWS security assessment, auditing and hardening.
proxenet	712.67fc6b5	THE REAL hacker friendly proxy for web application pentests.
proxify	250.afcc2fa	Swiss Army knife Proxy tool for HTTP/HTTPS traffic capture, manipulation, and replay on the go.
proxmark	2413.61163344	A powerful general purpose RFID tool, the size of a deck of cards, designed to snoop, listen and emulate everything from Low Frequency (125kHz) to High Frequency (13.56MHz) tags.
proxmark3	4.16191	A general purpose RFID tool for Proxmark3 hardware.
proxybroker	152.d21aae8	Proxy [Finder | Checker | Server]. HTTP(S) & SOCKS.
proxybroker2	373.d7dfd10	Proxy [Finder | Checker | Server]. HTTP(S) & SOCKS.

proxychains-ng	4.16	A hook preloader that allows to redirect TCP traffic of existing dynamically linked programs through one or more SOCKS or HTTP proxies
proxycheck	0.1	This is a simple proxy tool that checks for the HTTP CONNECT method and grabs verbose output from a webserver.
proxyp	2013	Small multithreaded Perl script written to enumerate latency, port numbers, server names, & geolocations of proxy IP addresses.
proxyscan	0.3	A security penetration testing tool to scan for hosts and ports through a Web proxy server.
proxytunnel	1.10.20210604	a program that connects stdin and stdout to a server somewhere on the network, through a standard HTTPS proxy
ps1encode	41.68d7778	A tool to generate and encode a PowerShell based Metasploit payloads.
pscan	1.3	A limited problem scanner for C source files
pshitt	23.dae7931	A lightweight fake SSH server designed to collect authentication data sent by intruders.
pspy	159.2312eed	Monitor linux processes without root permissions.
pstoreview	1.0	Lists the contents of the Protected Storage.
ptf	1491.f87dfa8	The Penetration Testers Framework is a way for modular support for up-to-date tools.
pth-toolkit	7.3641cdc	Modified version of the passing-the-hash tool collection made to work straight out of the box.
ptunnel	0.72	A tool for reliably tunneling TCP connections over ICMP echo request and reply packets
pulledpork	397.5ccf5c5	Snort rule management
pulsar	55.3c61178	Protocol Learning and Stateful Fuzzing.
punk	9.c2bc420	A post-exploitation tool meant to help network pivoting from a compromised unix box.
punter	45.97b7bed	Hunt domain names using DNSDumpster, WHOIS, Reverse WHOIS, Shodan, Crimeflare.
pupy	2988.4b78dc58	Opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python.
pureblood	37.2c5ce07	A Penetration Testing Framework created for Hackers / Pentester / Bug Hunter.
pwcrack	352.e824657	Password hash automatic cracking framework.

pwd-hash	2.0	A password hashing tool that use the crypt function to generate the hash of a string given on standard input.
pwdlogy	14.8b92bcf	A target specific wordlist generating tool for social engineers and security researchers.
pwdlyser	136.483b9bc	Python-based CLI Password Analyser (Reporting Tool).
pwdump	7.1	Extracts the binary SAM and SYSTEM file from the filesystem and then the hashes.
pwfuzz-rs	v0.1.1.r1.g169cd32	Rust-based password mutator for brute force attacks.
pwnat	14.d3c2b05	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.
pwncat	0.1.2	Bind and reverse shell handler with FW/IDS/IPS evasion, self-inject and port-scanning.
pwncat-caleb	v0.5.4.r11.g37f04d4	A post-exploitation platform.
pwndbg	2023.03.19	Makes debugging with GDB suck less.
pwndora	248.d3f676a	Massive IPv4 scanner, find and analyze internet-connected devices in minutes, create your own IoT search engine at home.
pwndrop	18.385ba70	Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV.
pwned	2003.f6ca8d5	A command-line tool for querying the 'Have I been pwned?' service.
pwned-search	40.04c1439	Pwned Password API lookup.
pwnedornot	147.5053c7f	Tool to find passwords for compromised email addresses.
pwnedpasswords	2.0.0.r0.g717702e	Generate and verify pwnedpasswords check digits.
pwnloris	10.5b79eff	An improved slowloris DOS tool which keeps attacking until the server starts getting exhausted.
pwntools	4.8.0	CTF framework and exploit development library.
pyaxmlparser	v0.3.28.r0.g9ba2165	A simple parser to parse Android XML file.
pybozocrack	87.ceb0cd9	A silly & effective MD5 cracker in Python.
pydictor	98.e48ee88	A useful hacker dictionary builder for a brute-force attack.

pyersinia	49.73f4056	Network attack tool like yersinia but written in Python.
pyew	109.8eb3e49	A python tool to analyse malware.
pyexfil	81.2ef1b8c	A couple of beta stage tools for data exfiltration.
pyfiscan	2948.bfed6c3	Free web-application vulnerability and version scanner.
pyfuscation	17.6d8d53f	Obfuscate powershell scripts by replacing Function names, Variables and Parameters.
pyinstaller	2:3.6	A program that converts (packages) Python programs into stand-alone executables, under Windows, Linux, Mac OS X, Solaris and AIX.
pyjfuzz	157.f777067	Python JSON Fuzzer.
pykek	12.651b9ba	Kerberos Exploitation Kit.
pymeta	13.fa74e64	Auto Scanning to SSL Vulnerability.
pyminifakedns	0.1	Minimal DNS server written in Python; it always replies with a 127.0.0.1 A-record.
pyrasite	2.0	Code injection and introspection of running Python processes.
pyrdp	1973.da7982a	RDP man-in-the-middle (mitm) and library for Python with the ability to watch connections live or after the fact.
pyrit	0.5.0	The famous WPA precomputed cracker
pyssltest	9.d7703f0	A python multithreaded script to make use of Qualys ssllabs api to test SSL flaws.
pytacle	alpha2	Automates the task of sniffing GSM frames
pytbull	19.3d82a54	A python based flexible IDS/IPS testing framework shipped with more than 300 tests.
pythem	454.e4fcb8a	Python penetration testing framework.
python-api-dnsdumpster	76.fa952c6	Unofficial Python API for http://dnsdumpster.com/.
python-arsenic	21.8	Async WebDriver implementation for asyncio and asyncio-compatible frameworks.
python-capstone	4.0.2	A lightweight multi-platform, multi-architecture disassembly framework
python-crontab	2.5.1	Crontab module for reading and writing crontab files and accessing the system cron automatically and simply using a direct API.
python-cymruwhois	1.6	Python client for the whois.cymru.com service
python-frida	15.2.2	Dynamic instrumentation toolkit for developers, reverse-engineers, and

		security researchers.
python-frida-tools	11.0.0	Frida CLI tools.
python-google-streetview	1.2.9	A command line tool and module for Google Street View Image API.
python-ivre	0.9.20.dev64	Network recon framework (library)
python-jsbeautifier	1.14.7	JavaScript unobfuscator and beautifier
python-keylogger	2.7.3	Simple keystroke logger.
python-libesedb-python	20181229	Library and tools to access the Extensible Storage Engine (ESE) Database File (EDB) format.
python-minidump	1:0.0.21	Python library to parse and read Microsoft minidump file format.
python-minikerberos	1:0.2.1	Kerberos manipulation library in pure Python.
python-mmbot	78.f5f5478	Powerful malicious file triage tool for cyber responders.
python-oletools	1:0.60.1	Tools to analyze Microsoft OLE2 files.
python-pcodedmp	1.2.6	A VBA p-code disassembler.
python-python-cymruwhois	30.022e16d	Python client for the whois.cymru.com service
python-rekall	1396.041d6964	Memory Forensic Framework.
python-search-engine-parser	0.6.8	Scrapes search engine pages for query titles, descriptions and links.
python-shodan	1.28.0	Python library for Shodan (https://developer.shodan.io).
python-ssh-mitm	3.0.2	SSH mitm server for security audits supporting public key authentication, session hijacking and file manipulation.
python-trackerjacker	1.9.0	Finds and tracks wifi devices through raw 802.11 monitoring.
python-uncompyle6	3.9.0	A Python cross-version decompiler.
python-utidylib	0.2	Python bindings for Tidy HTML parser/cleaner.

python-winsspi	0.0.9	Windows SSPI library in pure Python.
python-witnessme	1:1.5.0	Web Inventory tool, takes screenshots of webpages using Pyppeteer.
python-yara	3.8.1	Tool aimed at helping malware researchers to identify and classify malware samples
python-yara-rednaga	279.32b6a74	The Python interface for YARA.
python2-api-dnsdumpster	76.fa952c6	Unofficial Python API for http://dnsdumpster.com/.
python2-capstone	4.0.1	A lightweight multi-platform, multi-architecture disassembly framework
python2-cymruwhois	1.6	Python client for the whois.cymru.com service
python2-darts.util.lru	7.5ef01b1	Simple dictionary with LRU behaviour.
python2-exrex	146.239e4da	Irregular methods on regular expressions. Exrex is a command line tool and python module that generates all - or random - matching strings to a given regular expression and more.
python2-frida	15.2.2	Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.
python2-frida-tools	11.0.0	Frida CLI tools.
python2-google_streetview	1.2.9	A command line tool and module for Google Street View Image API.
python2-google-streetview	1.2.9	A command line tool and module for Google Street View Image API.
python2-hpfeeds	411.539e738	Honeynet Project generic authenticated datafeed protocol.
python2-ivre	0.9.16.dev26	Network recon framework (library)
python2-jsbeautifier	1.13.4	JavaScript unobfuscator and beautifier
python2-	0.9.4	Active Directory information dumper via LDAP.

ldapdomaindump		
python2-libesedb	20181229	Library and tools to access the Extensible Storage Engine (ESE) Database File (EDB) format. The ESE database format is used in may different applications like Windows Search, Windows Mail, Exchange, Active Directory, etc.
python2-libesedb-python	20181229	Library and tools to access the Extensible Storage Engine (ESE) Database File (EDB) format.
python2-minidump	19.749e6da	Python library to parse and read Microsoft minidump file format.
python2-minikerberos	17.e7e8d0a	Kerberos manipulation library in pure Python.
python2-oletools	1:0.60.1	Tools to analyze Microsoft OLE2 files.
python2-pcodedmp	1.2.6	A VBA p-code disassembler.
python2-peepdf	0.4.2	A Python tool to explore PDF files in order to find out if the file can be harmful or not.
python2-rekall	1396.041d6964	Memory Forensic Framework.
python2-ropgadget	5.9	ROPgadget supports ELF, PE and Mach-O format on x86, x64, ARM, ARM64, PowerPC, SPARC and MIPS architectures.
python2-shodan	1.28.0	Python library and command-line utility for Shodan (https://developer.shodan.io).
python2-webtech	1.2.12	Identify technologies used on websites.
python2-winsspi	0.0.9	Windows SSPI library in pure Python.
python2-yara	4.0.5	Tool aimed at helping malware researchers to identify and classify malware samples
qark	301.ba1b265	Tool to look for several security related Android application vulnerabilities.
qrgen	37.82a015b	Simple script for generating Malformed QRCodes.
qrljacker	218.1b0a4e2	QRLJacker is a highly customizable exploitation framework to

		demonstrate "QRLJacking Attack Vector".
qsreplace	3.0b053d2	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.
quark-engine	21.6.2	Android Malware (Analysis | Scoring) System
quickrecon	0.3.2	A python script for simple information gathering. It attempts to find subdomain names, perform zone transfers and gathers emails from Google and Bing.
quicksand-lite	32.42af152	Command line tool for scanning streams within office documents plus xor db attack.
quickscope	383.d46c407	Statically analyze windows, linux, osx, executables and also APK files.
r2cutter	1:1.12.0	Qt and C++ GUI for radare2 reverse engineering framework
r2ghidra	5.8.4	Deep ghidra decompiler integration for radare2 and r2cutter
rabid	1:v0.1.0.r53.gff1475d	A CLI tool and library allowing to simply decode all kind of BigIP cookies.
raccoon	187.9cf6c11	A high performance offensive security tool for reconnaissance and vulnerability scanning.
radamsa	0.6	General purpose mutation based fuzzer
radare2	5.8.6	Open-source tools to disasm, debug, analyze and manipulate binary files
radare2-cutter	1:1.12.0	Qt and C++ GUI for radare2 reverse engineering framework.
radare2-keystone	720.d034b27	Keystone assembler plugins for radare2.
radare2-unicorn	743.4235786	Unicorn Emulator Plugin for radare2.
radiography	2	A forensic tool which grabs as much information as possible from a Windows system.
rainbowcrack	1.8	Password cracker based on the faster time-memory trade-off. With MySQL and Cisco PIX Algorithm patches.
ranger-scanner	149.3aae5dd	A tool to support security professionals to access and interact with remote Microsoft Windows based systems.
rapidscan	218.cb5ea0e	The Multi-Tool Web Vulnerability Scanner.
rarcrack	0.2	This program uses bruteforce algorithm to find correct password (rar, 7z, zip).
rasenum	1.0	A small program which lists the information for all of the entries in any phonebook file (.pbk).

rathole	0.4.7	A reverse proxy for NAT traversal
ratproxy	1.58	A passive web application security assessment tool
rats	6.4ba54ce	A rough auditing tool for security in source code files. It is a tool for scanning C, C++, Perl, PHP, Python and Ruby source code and flagging common security related programming errors such as buffer overflows and TOCTOU (Time Of Check, Time Of Use) race conditions. As its name implies, the tool performs only a rough analysis of source code. It will not find every error and will also find things that are not errors. Manual inspection of your code is still necessary, but greatly aided with this tool.
raven	1:33.8646a58	A Linkedin information gathering tool used to gather information.
rawr	74.544dd75	Rapid Assessment of Web Resources. A web enumerator.
rawsec-cli	1.2.0.r7.gf7a08c6	Rawsec Inventory search CLI to find security tools and resources.
rbasefind	41.a661118	A firmware base address search tool.
rbkb	v0.7.2.r0.ga6d35c0	A miscellaneous collection of command-line tools related to pen-testing and reversing.
rbndr	9.a189ffd	Simple DNS Rebinding Service.
rcracki-mt	0.7.0	A tool to perform rainbow table attacks on password hashes. It is intended for indexed/perfected rainbow tables, mainly generated by the distributed project www.freerainbowtables.com
rcrdcarver	5.54507d21	Carve RCRD records ($LogFile) from a chunk of data..
rdesktop-brute	1.5.0	It connects to windows terminal servers - Bruteforce patch included.
rdp-cipher-checker	0.1	Enumerate the encryption protocols supported by the server and the cipher strengths supported using native RDP encryption.
rdp-sec-check	11.d0cc143	Script to enumerate security settings of an RDP Service.
rdpasspray	25.6aaeb60	Python3 tool to perform password spraying using RDP.
rdwarecon	1.2.r0.g9675200	A python script to extract information from a Microsoft Remote Desktop Web Access (RDWA) application.
reaver	1.6.6	Brute force attack against Wifi Protected Setup
rebind	0.3.4	DNS Rebinding Tool
recaf	2.21.8.2224.c8a3cf8b	Modern Java bytecode editor.
recentfilecache-parser	2.5e22518	Python parser for the RecentFileCache.bcf on Windows.

recomposer	2.90f85ed	Randomly changes Win32/64 PE Files for 'safer' uploading to malware and sandbox sites.
recon-ng	1:1021.9e907df	A full-featured Web Reconnaissance framework written in Python.
reconnoitre	441.f62afba	A security tool for multithreaded information gathering and service enumeration.
reconscan	61.afbcfc0	Network reconnaissance and vulnerability assessment tools.
recoverjpeg	2.6.3	Recover jpegs from damaged devices.
recsech	123.1fc298a	Tool for doing Footprinting and Reconnaissance on the target web.
recstudio	4.1	Cross platform interactive decompiler
recuperabit	69.8e77cde	A tool for forensic file system reconstruction.
red-hawk	36.fa54e23	All in one tool for Information Gathering, Vulnerability Scanning and Crawling.
redasm	1667.5ab6be9	Interactive, multiarchitecture disassembler written in C++ using Qt5 as UI Framework.
redfang	2.5	Finds non-discoverable Bluetooth devices by brute-forcing the last six bytes of the devices' Bluetooth addresses and calling read_remote_name().
redirectpoison	1.1	A tool to poison a targeted issuer of SIP INVITE requests with 301 (i.e. Moved Permanently) redirection responses.
redpoint	123.23ef36b	Digital Bond's ICS Enumeration Tools.
redress	v0.8.0.alpha4.r6.g28a8814	A tool for analyzing stripped Go binaries.
redsocks	211.19b822e	Transparent redirector of any TCP connection to proxy.
reelphish	5.dc1be33	A Real-Time Two-Factor Phishing Tool.
regeorg	30.1ca54c2	The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.
regipy	2.2.2	Library for parsing offline registry hives.
reglookup	1.0.1	Command line utility for reading and querying Windows NT registries
regreport	1.6	Windows registry forensic analysis tool.
regrippy	2.0.0	Framework for reading and extracting useful forensics data from Windows registry hives.
regview	1.3	Open raw Windows NT 5 Registry files (Windows 2000 or higher).
rekall	1409.55d1925f	Memory Forensic Framework.

relay-scanner	1.7	An SMTP relay scanner.
remot3d	38.a707ef7	An Simple Exploit for PHP Language.
replayproxy	1.1	Forensic tool to replay web-based attacks (and also general HTTP traffic) that were captured in a pcap file.
resourcehacker	5.1.8	Resource compiler and decompiler for WindowsB® applications.
responder	4:v3.1.3.0.r25.g07c963f	A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.
responder-multirelay	1:360.24e7b7c	A LLMNR and NBT-NS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2 (multirelay version),
restler-fuzzer	4:latest.main.r3.g9507f4b	First stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services.
retdec	2118.407f290c	Retargetable machine-code decompiler based on LLVM.
retire	3.2.3.r10.g2fa6f21	Scanner detecting the use of JavaScript libraries with known vulnerabilities.
reverseip	13.42cc9c3	ReverseIP is a ruby-based reverse IP-lookup tool, which finds all domains hosted on a web server and returns the HTTP status code of those domains.
revipd	5.2aaacfb	A simple reverse IP domain scanner.
revsh	215.174e309	A reverse shell with terminal support, data tunneling, and advanced pivoting capabilities.
rex	684.1907878	Shellphish's automated exploitation engine, originally created for the Cyber Grand Challenge.
rext	63.5f0f626	Router EXploitation Toolkit - small toolkit for easy creation and usage of various python scripts that work with embedded devices.
rfcat	170508	RF ChipCon-based Attack Toolset.
rfdump	1.6	A back-end GPL tool to directly inter-operate with any RFID ISO-Reader to make the contents stored on RFID tags accessible
rfidiot	107.88f2ef9	An open source python library for exploring RFID devices.
rfidtool	0.01	A opensource tool to read / write rfid tags
rhodiola	4.8bc08a0	Personalized wordlist generator with NLP, by analyzing tweets (A.K.A

		crunch2049).
richsploit	3.6b15e0f	Exploitation toolkit for RichFaces.
ridenum	75.9e3b89b	A null session RID cycle attack for brute forcing domain controllers.
ridrelay	34.f2fa99c	Enumerate usernames on a domain where you have no creds by using SMB Relay with low priv.
rifiuti2	1:0.7.0	A rewrite of rifiuti, a great tool from Foundstone folks for analyzing Windows Recycle Bin INFO2 file.
rinetd	0.62	internet redirection server
ripdc	0.3	A script which maps domains related to an given ip address or domainname.
rita	827.974db68	Real Intelligence Threat Analytics (RITA) is a framework for detecting command and control communication through network traffic analysis.
riwifshell	38.40075d5	Web backdoor - infector - explorer.
rkhunter	1.4.6	Checks machines for the presence of rootkits and other unwanted tools.
rlogin-scanner	0.2	Multithreaded rlogin scanner. Tested on Linux, OpenBSD and Solaris.
rmiscout	1.4	Enumerate Java RMI functions and exploit RMI parameter unmarshalling vulnerabilities.
rogue-mysql-server	2.78ebbfc	A rogue MySQL server written in Python.
roguehostapd	78.381b373	Hostapd fork including Wi-Fi attacks and providing Python bindings with ctypes.
rombuster	204.b0b12d1	A router exploitation tool that allows to disclosure network router admin password.
rootbrute	1:0.1	Local root account bruteforcer.
ropeadope	1.1	A linux log cleaner.
ropeme	4.9b3a8fd	ROPME is a set of python scripts to generate ROP gadgets and payload.
ropgadget	7.1	Lets you search your gadgets on your binaries (ELF format) to facilitate your ROP exploitation.
ropgadget2	5.4	Search gadgets in binaries to facilitate ROP exploitation for several file formats and architectures
ropper	1.13.8	Show information about binary files and find gadgets to build rop chains for different architectures
roputils	195.ae7ed20	A Return-oriented Programming toolkit.

Router Scan	v2.60 Beta	Router Scan is able to find and identify a variety of devices from large number of known routers and that the most important thing is to get from them useful information, in particular the characteristics of the wireless network: a method of protecting the access point (encryption), access point name (SSID) and access point key (passphrase). Also it receives information about the WAN connection (useful when scanning a local network) and show the model of router. Getting information occurs in two possible ways: 1. The program will try to guess a pair of username/password to the router from a list of standard passwords, thereby get access. 2. Or the vulnerabilities (bugs) will be used against the router model, allowing to get the necessary information and/or bypass the authorization process.
routerhunter	21.4da257c	Tool used to find vulnerable routers and devices on the Internet and perform tests.
routersploit	3.4.0	The Router Exploitation Framework.
rp	138.3a54a7c	A full-cpp written tool that aims to find ROP sequences in PE/Elf/Mach-O x86/x64 binaries.
rpak	1.0	A collection of tools that can be useful for doing attacks on routing protocols.
rpcsniffer	7.9fab095	Sniffs WINDOWS RPC messages in a given RPC server process.
rpctools	1.0	Contains three separate tools for obtaining information from a system that is running RPC services
rpdscan	2.a71b0f3	Remmina Password Decoder and scanner.
rpivot	5.4963487	Socks4 reverse proxy for penetration testing.
rr	6345.91cfc7c1	A Record and Replay Framework.
rrs	100:1.70	A reverse (connecting) remote shell. Instead of listening for incoming connections it will connect out to a listener (rrs in listen mode). With tty support and more.
rsactftool	946.079ba2e	RSA tool for ctf - retreive private key from weak public key and/or uncipher data.
rsakeyfind	1.0	A tool to find RSA key in RAM.
rsatool	29.b5f56da	Tool that can be used to calculate RSA and RSA-CRT parameters.
rshack	64.cf197e3	Python tool which allows to carry out some attacks on RSA, and offer a few tools to manipulate RSA keys.

rsmangler	1.4	rsmangler takes a wordlist and mangle it
rspet	263.de4356e	A Python based reverse shell equipped with functionalities that assist in a post exploitation scenario.
rtfm	93.02f6432	A database of common, interesting or useful commands, in one handy referable form.
rtlamr	197.03369d1	An rtl-sdr receiver for smart meters operating in the 900MHz ISM band.
rtlizer	35.5614163	Simple spectrum analyzer.
rtlsdr-scanner	1013.3c032de	A cross platform Python frequency scanning GUI for the OsmoSDR rtl-sdr library.
rtp-flood	1.0	RTP flooder
rtpbreak	1:1.3a	Detects, reconstructs and analyzes any RTP session
rubilyn	0.0.1	64bit Mac OS-X kernel rootkit that uses no hardcoded address to hook the BSD subsystem in all OS-X Lion & below. It uses a combination of syscall hooking and DKOM to hide activity on a host.
ruler	301.1e5ee2d	A tool to abuse Exchange services.
rulesfinder	38.38313f3	Machine-learn password mangling rules.
rupture	1383.131c61a	A framework for BREACH and other compression-based crypto attacks.
rustbuster	302.4a243d4	DirBuster for Rust.
rustcat	v3.0.0.r4.g245c791	A Modern Port Listener & Reverse Shell.
rusthound	55.6d7b945	Active Directory data collector for BloodHound.
rustpad	v1.8.1.r1.g11ce343	Multi-threaded Padding Oracle attacks against any service.
rustscan	2.1.1	Faster Nmap Scanning with Rust.
rvi-capture	14.a2e129b	Capture packets sent or received by iOS devices.
rww-attack	0.9.2	The Remote Web Workplace Attack tool will perform a dictionary attack against a live Microsoft Windows Small Business Server's 'Remote Web Workplace' portal. It currently supports both SBS 2003 and SBS 2008 and includes features to avoid account lock out.
rz-cutter	2.2.0	Qt and C++ GUI for rizin reverse engineering framework
rz-ghidra	0.5.0	Deep ghidra decompiler integration for rizin and rz-cutter
s3-fuzzer	4.0a2a6f0	A concurrent, command-line AWS S3 Fuzzer.
s3scanner	419.6a67603	Scan for open S3 buckets and dump.

safecopy	1.7	A disk data recovery tool to extract data from damaged media.
sagan	2.0.2	A snort-like log analysis engine.
sakis3g	0.2.0e	An all-in-one script for connecting with 3G.
saleae-logic	2.3.47	Debug happy.
sambascan	0.5.0	Allows you to search an entire network or a number of hosts for SMB shares. It will also list the contents of all public shares that it finds.
samdump2	3.0.0	Dump password hashes from a Windows NT/2k/XP installation
samesame	68.a9bcd7b	Command line tool to generate crafty homograph strings.
samplicator	175.ceeb1d2	Send copies of (UDP) datagrams to multiple receivers, with optional sampling and spoofing.
samydeluxe	1:2.2ed1bac	Automatic samdump creation script.
sandcastle	73.10af7c7	A Python script for AWS S3 bucket enumeration.
sandmap	579.a7c4860	Nmap on steroids! Simple CLI with the ability to run pure Nmap engine, 31 modules with 459 scan profiles.
sandsifter	2.8375e61	The x86 processor fuzzer.
sandy	6.531ab16	An open-source Samsung phone encryption assessment framework
saruman	2.4be8db5	ELF anti-forensics exec, for injecting full dynamic executables into process image (With thread injection).
sasm	3.2.0	A simple crossplatform IDE for NASM, MASM, GAS and FASM assembly languages.
sawef	32.e5ce862	Send Attack Web Forms.
sb0x	19.04f40fe	A simple and Lightweight framework for Penetration testing.
sbd	1.36	Netcat-clone, portable, offers strong encryption - features AES-128-CBC + HMAC-SHA1 encryption, program execution (-e), choosing source port, continuous reconnection with delay + more
sc-make	12.7e39718	Tool for automating shellcode creation.
scalpel	1:1.1687261	A frugal, high performance file carver
scamper	20230323	A tool that actively probes the Internet in order to analyze topology and performance.
scanless	89.725110c	Utility for using websites that can perform port scans on your behalf.
scanmem	0.17	Memory scanner designed to isolate the address of an arbitrary variable in an executing process
scannerl	15.e52c46b	The modular distributed fingerprinting engine.

scanqli	26.40a028d	SQLi scanner to detect SQL vulns.
scansploit	9.a0890af	Exploit using barcodes, QRcodes, earn13, datamatrix.
scanssh	2.1	Fast SSH server and open proxy scanner.
scap-security-guide	0.1.60	Security compliance content in SCAP, Bash, Ansible, and other formats.
scap-workbench	1.2.1	SCAP Scanner And Tailoring Graphical User Interface.
scapy	2.5.0	A powerful interactive packet manipulation program written in Python
scapy3k	0.23	Powerful interactive packet manipulation program written in Python 3
scavenger	103.75907e8	Crawler (Bot) searching for credential leaks on different paste sites.
schnappi-dhcp	0.1	Can test network with no DHCP.
scout2	1182.5d86d46	Security auditing tool for AWS environments.
scoutsuite	1:5.12.0.r0.g6b8debb1c	Multi-Cloud Security Auditing Tool.
scrape-dns	58.3df392f	Searches for interesting cached DNS entries.
scrapy	2.8.0	A fast high-level scraping and web crawling framework.
scratchabit	571.e52ba4b	Easily retargetable and hackable interactive disassembler with IDAPython-compatible plugin API.
scrounge-ntfs	0.9	Data recovery program for NTFS file systems
scrying	234.caa233c	Collect RDP, web, and VNC screenshots smartly.
sctpscan	34.4d44706	A network scanner for discovery and security.
scylla	76.34cb51c	The Simplistic Information Gathering Engine | Find Advanced Information on a Username, Website, Phone Number, etc
sdn-toolkit	1.21	Discover, Identify, and Manipulate SDN-Based Networks
sdnpwn	67.c4809da	An SDN penetration testing toolkit.
sea	103.9aca1c8	A tool to help to create exploits of binary programs.
search1337	1:11.bf03ec9	Online, lightweight exploit scanner and downloader.
searchsploit	1:1828.2ae6cf2b7	The official Exploit Database search tool.
seat	0.3	Next generation information digging application geared toward the needs of security professionals. It uses information stored in search engine databases, cache repositories, and other public resources to scan web sites for potential vulnerabilities.
second-order	v3.2.r0.g24256	Second-order subdomain takeover scanner.

	9b	
secretfinder	1:14.a0283cb	A python script to find sensitive data (apikeys, accesstoken, jwt,..) in javascript files.
secscan	1.5	Web Apps Scanner and Much more utilities.
secure-delete	1:1.b63d814	Secure file, disk, swap, memory erasure utilities.
secure2csv	10.119eefb0	Decode security descriptors in $Secure on NTFS.
see-surf	v2.0.r40.gbe79a31	A Python based scanner to find potential SSRF parameters in a web application.
seeker	1:304.b21f28c	Accurately Locate People using Social Engineering.
sees	67.cd741aa	Increase the success rate of phishing attacks by sending emails to company users as if they are coming from the very same company's domain.
semgrep	1.17.1	Lightweight static analysis for many languages.
sensepost-xrdp	16.46d6c19	A rudimentary remote desktop tool for the X11 protocol exploiting unauthenticated x11 sessions.
sergio-proxy	20.8a91bb4	A multi-threaded transparent HTTP proxy for manipulating web traffic
serialbrute	3.111c217	Java serialization brute force attack tool.
serializationdumper	31.69ea9ba	A tool to dump Java serialization streams in a more human readable form.
server-status-pwn	12.841d55d	A script that monitors and extracts requested URLs and clients connected to the service by exploiting publicly accessible Apache server-status instances.
sessionlist	6.3efc3b2	Sniffer that intents to sniff HTTP packets and attempts to reconstruct interesting authentication data from websites that do not employ proper secure cookie auth.
set	1:8.0.3	Social-engineer toolkit. Aimed at penetration testing around Social-Engineering.
seth	103.8b6e36c	Perform a MitM attack and extract clear text credentials from RDP connections.
setowner	1.1	Allows you to set file ownership to any account, as long as you have the "Restore files and directories" user right.
sfuzz	198.3bf135b	A simple fuzzer.
sgn	26.2dfae64	Shikata ga nai encoder ported into go with several improvements.
sh00t	209.46c734d	A Testing Environment for Manual Security Testers.

sha1collisiondetection	105.b4a7b0b	Library and command line tool to detect SHA-1 collision in a file
shad0w	387.d35b9dc	A modular C2 framework designed to successfully operate on mature environments.
shadowexplorer	0.9	Browse the Shadow Copies created by the Windows Vista / 7 / 8 / 10 Volume Shadow Copy Service.
shard	1.5	A command line tool to detect shared passwords.
shareenum	48.db728dd	Tool to enumerate shares from Windows hosts.
sharesniffer	58.a0c5ed6	Network share sniffer and auto-mounter for crawling remote file systems.
shed	2.0.0	.NET runtime inspector.
shellcheck	0.9.0	Shell script analysis tool
shellcode-compiler	24.e8edc8e	Compiles C/C++ style code into a small, position-independent and NULL-free shellcode for Windows & Linux.
shellcode-factory	96.07ae857	Tool to create and test shellcodes from custom assembly sources.
shellcodecs	0.1	A collection of shellcode, loaders, sources, and generators provided with documentation designed to ease the exploitation and shellcode programming process.
shellen	66.c0c5f83	Interactive shellcoding environment to easily craft shellcodes.
shellerator	32.0ed6571	Simple command-line tool aimed to help pentesters quickly generate one-liner reverse/bind shells in multiple languages.
shellinabox	428.98e6eeb	Implements a web server that can export arbitrary command line tools to a web based terminal emulator.
shelling	227.0a6c135	An offensive approach to the anatomy of improperly written OS command injection sanitisers.
shellme	5.d5206f0	Because sometimes you just need shellcode and opcodes quickly. This essentially just wraps some nasm/objdump calls into a neat script.
shellnoob	35.72cf498	A toolkit that eases the writing and debugging of shellcode
shellpop	148.a145349	Generate easy and sophisticated reverse or bind shell commands.
shellsploit-framework	273.a16d22f	New Generation Exploit Development Kit.
shellter	7.2	A dynamic shellcode injection tool, and the first truly dynamic PE infector ever created.
shellz	161.0ed068f	A script for generating common revshells fast and easy.

sherlock	2097.b7cd7ab	Find usernames across social networks.
sherlocked	1.f190c2b	Universal script packer-- transforms any type of script into a protected ELF executable, encrypted with anti-debugging.
shhgit	66.53e656c	Find committed secrets and sensitive files across GitHub, Gists, GitLab and BitBucket or your local repositories in real time.
shitflood	14.e74fc42	A Socks5 clone flooder for the Internet Relay Chat (IRC) protocol.
shocker	64.d3f7603	A tool to find and exploit servers vulnerable to Shellshock.
shodan	1.13.0	Python library for Shodan (https://developer.shodan.io).
shodanhat	13.e5e7e68	Search for hosts info with shodan.
shootback	83.cab462c	A reverse TCP tunnel let you access target behind NAT or firewall.
shortfuzzy	0.1	A web fuzzing script written in perl.
shosubgo	2.0.r19.g6e8d48c	Small tool to Grab subdomains using Shodan API.
shreder	87.814adb4	A powerful multi-threaded SSH protocol password bruteforce tool.
shuffledns	227.a2ae07f	A wrapper around massdns written in go that allows you to enumerate valid subdomains.
sickle	73.e14c0bb	A shellcode development tool, created to speed up the various steps needed to create functioning shellcode.
sidguesser	1.0.5	Guesses sids/instances against an Oracle database according to a predefined dictionary file.
siege	4.1.6	An http regression testing and benchmarking utility
sigma	0.20	Generic Signature Format for SIEM Systems
sign	10.2dc4018	Automatically signs an apk with the Android test certificate.
sigploit	786.0e52072	Telecom Signaling Exploitation Framework - SS7, GTP, Diameter & SIP.
sigspotter	1.0	A tool that search in your HD to find wich publishers has been signed binaries in your PC.
sigthief	25.ffb501b	Stealing Signatures and Making One Invalid Signature at a Time.
silenteye	21.a53a7ff	A cross-platform application design for an easy use of steganography.
silenttrinity	292.cd9416d	An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR.
silk	3.19.2	A collection of traffic analysis tools developed by the CERT NetSA to facilitate security analysis of large networks.
simple-ducky	20.f15079e	A payload generator.

simple-lan-scan	1.0	A simple python script that leverages scapy for discovering live hosts on a network.
simpleemailspoofer	54.7075f0c	A simple Python CLI to spoof emails.
simplify	1.3.0	Generic Android Deobfuscator.
simplyemail	1:1.4.10.r7.6a42d37	Email recon made fast and easy, with a framework to build on http://CyberSyndicates.com.
simtrace2	1071.773d314	Host utilities to communicate with SIMtrace2 USB Devices.
sinfp	1.24	A full operating system stack fingerprinting suite.
siparmyknife	11232011	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.
sipbrute	11.5be2fdd	A utility to perform dictionary attacks against the VoIP SIP Register hash.
sipcrack	0.2	A SIP protocol login cracker.
sipffer	1:29.efc3ff1	SIP protocol command line sniffer.
sipi	13.58f0dcc	Simple IP Information Tools for Reputation Data Analysis.
sipp	1331.f44d0cf	A free Open Source test tool / traffic generator for the SIP protocol.
sippts	492.72c87f3	Set of tools to audit SIP based VoIP Systems.
sipsak	1:0.9.8.1	A small command line tool for developers and administrators of Session Initiation Protocol (SIP) applications.
sipscan	1:0.1	A sip scanner.
sipshock	7.6ab5591	A scanner for SIP proxies vulnerable to Shellshock.
sipvicious	462.fd3e7c7	Tools for auditing SIP devices
sireprat	34.b8ef60b	Remote Command Execution as SYSTEM on Windows IoT Core.
sitadel	121.0a0e475	Web Application Security Scanner.
sitediff	3.1383935	Fingerprint a web app using local files as the fingerprint sources.
sjet	103.dd2a4e6	Siberas JMX exploitation toolkit.
skipfish	2.10b	A fully automated, active web application security reconnaissance tool
skiptracer	1:123.ca40957	OSINT python2 webscraping framework. Skipping the needs of API keys.
skul	27.7bd83f1	A PoC to bruteforce the Cryptsetup implementation of Linux Unified Key Setup (LUKS).
skydive	0.28.0	An open source real-time network topology and protocols analyzer.
skyjack	16.24e3878	Takes over Parrot drones, deauthenticating their true owner and taking over control, turning them into zombie drones under your own control.

skype-dump	0.1	This is a tool that demonstrates dumping MD5 password hashes from the configuration file in Skype.
skypefreak	33.9347a65	A Cross Platform Forensic Framework for Skype.
slackpirate	142.9788be6	Slack Enumeration and Extraction Tool - extract sensitive information from a Slack Workspace.
sleuthkit	4.11.1	File system and media management forensic analysis tools
sleuthql	9.29fc878	Python3 Burp History parsing tool to discover potential SQL injection points. To be used in tandem with SQLmap.
slither	1:3367.0ec487460	Solidity static analysis framework written in Python 3.
sloth-fuzzer	39.9f7f59a	A smart file fuzzer.
slowhttptest	1.9.0	A highly configurable tool that simulates application layer denial of service attacks.
slowloris	0.7	A tool which is written in perl to test http-server vulnerabilites for connection exhaustion denial of service (DoS) attacks so you can enhance the security of your webserver.
slowloris-py	30.eb7f632	Low bandwidth DoS tool.
slurp	90.6a4eaaf	S3 bucket enumerator
slurp-scanner	90.6a4eaaf	Evaluate the security of S3 buckets.
smali	2.5.2	An assembler/disassembler for Android's dex format
smali-cfgs	6.4450418	Smali Control Flow Graph's.
smalisca	58.1aa7a16	Static Code Analysis for Smali files.
smap	24.3ed1ac7	Shellcode mapper - Handy tool for shellcode analysis.
smartphone-pentest-framework	104.fc45347	Repository for the Smartphone Pentest Framework (SPF).
smbbf	0.9.1	SMB password bruteforcer.
smbcrunch	12.313400e	3 tools that work together to simplify reconaissance of Windows File Shares.
smbexec	2:59.a54fc14	A rapid psexec style attack with samba tools.
smbmap	147.a771476	A handy SMB enumeration tool.
smbrelay	3	SMB / HTTP to SMB replay attack toolkit.
smbspider	10.7db9323	A lightweight python utility for searching SMB/CIFS/Samba file shares.

smbsr	49.a44ced7	Lookup for interesting stuff in SMB shares.
smikims-arpspoof	25.244d9ee	Performs an ARP spoofing attack using the Linux kernel's raw sockets.
smod	53.7eb8423	A modular framework with every kind of diagnostic and offensive feature you could need in order to pentest modbus protocol.
smplshllctrlr	9.2baf390	PHP Command Injection exploitation tool.
smtp-fuzz	1.0	Simple smtp fuzzer.
smtp-test	5.d8d8598	Automated testing of SMTP servers for penetration testing.
smtp-user-enum	1.2	Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.
smtp-vrfy	1.0	An SMTP Protocol Hacker.
smtpmap	0.8.234_BETA	Tool to identify the running smtp software on a given host.
smtpscan	0.5	An SMTP scanner
smtptester	13.634e1ee	Small python3 tool to check common vulnerabilities in SMTP servers.
smtptx	1.0	A very simple tool used for sending simple email and do some basic email testing from a pentester perspective.
smuggler	23.2be871e	Python tool used to test for HTTP Desync/Request Smuggling attacks.
smuggler-py	1.0	Python tool used to test for HTTP Desync/Request Smuggling attacks.
sn00p	0.8	A modular tool written in bourne shell and designed to chain and automate security tools and tests.
sn1per	1:563.9deac2b	Automated Pentest Recon Scanner.
snallygaster	225.4c5a9b5	Tool to scan for secret files on HTTP servers.
snapception	8.c156f9e	Intercept and decrypt all snapchats received over your network.
snare	183.0919a80	Super Next generation Advanced Reactive honEypot. SNARE is a web application honeypot sensor attracting all sort of maliciousness from the Internet.
snarf-mitm	41.bada142	SMB Man in the Middle Attack Engine / relay suite.
sniff-probe-req	379.8a02dbd	Wi-Fi Probe Requests Sniffer.
sniffer	4.688854e	Packet Trace Parser for TCP, SMTP Emails, and HTTP Cookies.
sniffglue	0.15.0	Secure multithreaded packet sniffer
sniffjoke	772.434bfb1	Injects packets in the transmission flow that are able to seriously disturb passive analysis like sniffing, interception and low level information theft.
sniffles	469.118e93f	A Packet Capture Generator for IDS and Regular Expression Evaluation.

snitch	1.2	Turn back the asterisks in password fields to plaintext passwords.
snmp-brute	19.830bb0a	SNMP brute force, enumeration, CISCO config downloader and password cracking script.
snmp-fuzzer	0.1.1	SNMP fuzzer uses Protos test cases with an entirely new engine written in Perl.
snmpattack	1.8	SNMP scanner and attacking tool.
snmpcheck	1.9	A free open source utility to get information via SNMP protocols.
snmpenum	1.7	snmp enumerator
snmpscan	0.1	A free, multi-processes SNMP scanner.
snoopbrute	17.589fbe6	Multithreaded DNS recursive host brute-force tool.
snoopy-ng	128.eac73f5	A distributed, sensor, data collection, interception, analysis, and visualization framework.
snort	2.9.20	A lightweight network intrusion detection system.
snow	20130616	Steganography program for concealing messages in text files.
snowman	0.1.3	A native code to C/C++ decompiler, see the examples of generated code.
snscan	1.05	A Windows based SNMP detection utility that can quickly and accurately identify SNMP enabled devices on a network.
snscrape	0.4.3.20220106	A social networking service scraper in Python.
snuck	6.76196b6	Automatic XSS filter bypass.
snyk	1.878.0	CLI and build-time tool to find and fix known vulnerabilities in open-source dependencies.
soapui	5.7.0	The Swiss-Army Knife for SOAP Testing.
socat	1.7.4.4	Multipurpose relay
social-analyzer	0.42	Analyzing & finding a person's profile across social media websites.
social-mapper	190.92be8da	A social media enumeration and correlation tool.
social-vuln-scanner	11.91794c6	Gathers public information on companies to highlight social engineering risk.
socialfish	242.3167ab8	Ultimate phishing tool with Ngrok integrated.
socialpwned	v2.0.0.r2.gc7845c3	OSINT tool that allows to get the emails, from a target, published in social networks.
socialscan	123.9f68539	Check email address and username availability on online platforms.
socketfuzz	26.089add2	Simple socket fuzzer.

sockstat	0.4.1	A tool to let you view information about open connections. It is similar to the tool of the same name that is included in FreeBSD, trying to faithfully reproduce as much functionality as is possible.
sonar-scanner	4.8.0.2856	Generic CLI tool to launch project analysis on SonarQube servers.
soot	3.4.0	A Java Bytecode Analysis and Transformation Framework.
sooty	326.e1e86e5	The SOC Analysts all-in-one CLI tool to automate and speed up workflow.
spade	114	A general-purpose Internet utility package, with some extra features to help in tracing the source of spam and other forms of Internet harassment.
spaf	11.671a976	Static Php Analysis and Fuzzer.
spaghetti	4:9.df39a11	Web Application Security Scanner.
sparta	21.b0a4514	Python GUI application which simplifies network infrastructure penetration testing by aiding the penetration tester in the scanning and enumeration phase.
spartan	23.babdd7d	TCHunt-ng attempts to reveal encrypted files stored on a filesystem. The program is successful in finding TrueCrypt, VeraCrypt, CipherShed containers, EncFS encrypted files, PGP/GPG encrypted messages, OpenSSH and PEM private keys, password databases, and files made up of random data.
sparty	0.1	An open source tool written in python to audit web applications using sharepoint and frontpage architecture.
spectools	2010_04_R1	Spectrum-Tools is a set of utilities for using the Wi-Spy USB spectrum analyzer hardware. Stable version.
speedpwn	8.3dd2793	An active WPA/2 Bruteforcer, original created to prove weak standard key generation in different ISP labeled routers without a client is connected.
spf	85.344ac2f	A python tool designed to allow for quick recon and deployment of simple social engineering phishing exercises.
spfmap	8.a42d15a	A program to map out SPF and DKIM records for a large number of domains.
spiderfoot	4.0	The Open Source Footprinting Tool.
spiderpig-pdffuzzer	0.1	A javascript pdf fuzzer
spiga	2:623.8bc1ddc	Configurable web resource scanner.
spike	2.9	IMMUNITYsec's fuzzer creation kit in C

spike-fuzzer	2.9	IMMUNITYsec's fuzzer creation kit in C.
spike-proxy	148	A Proxy for detecting vulnerabilities in web applications
spiped	1.6.2	A utility for creating symmetrically encrypted and authenticated pipes between socket addresses.
spipscan	1:69.4ad3235	SPIP (CMS) scanner for penetration testing purpose written in Python.
splint	3.1.2.git20180129	A tool for statically checking C programs for security vulnerabilities and coding mistakes
sploitctl	1:3.0.3	Fetch, install and search exploit archives from exploit sites like exploit-db and packetstorm.
sploitego	153.d9568dc	Maltego Penetration Testing Transforms.
spoofcheck	16.8cce591	Simple script that checks a domain for email protections.
spooftooph	0.5.2	Designed to automate spoofing or cloning Bluetooth device Name, Class, and Address. Cloning this information effectively allows Bluetooth device to hide in plain sight
spookflare	24.19491b5	Loader, dropper generator with multiple features for bypassing client-side and network-side countermeasures.
spotbugs	16957.73d952249	A tool for static analysis to look for bugs in Java code.
spray365	42.58fd193	Makes spraying Microsoft accounts (Office 365 / Azure AD) easy through its customizable two-step password spraying approach.
spraycharles	198.041a598	Low and slow password spraying tool, designed to spray on an interval over a long period of time.
sprayhound	0.0.3	Password spraying tool and Bloodhound integration.
sprayingtoolkit	60.82e2ec8	Scripts to make password spraying attacks against Lync/S4B & OWA a lot quicker, less painful and more efficient.
spraykatz	62.1fb3aa7	Credentials gathering tool automating remote procdump and parse of lsass process.
sps	4.3	A Linux packet crafting tool. Supports IPv4, IPv6 including extension headers, and tunneling IPv6 over IPv4.
spyse	47.cd11ba9	Python API wrapper and command-line client for the tools hosted on spyse.com.
sqid	0.3	A SQL injection digger.
sqlbrute	1.0	Brute forces data out of databases using blind SQL injection.
sqldict	2.1	A dictionary attack tool for SQL Server.

sqlivulscan	249.cc8e657	This will give you the SQLi Vulnerable Website Just by Adding the Dork.
sqlmap	1.7	Automatic SQL injection and database takeover tool
sqlninja	0.2.999	A tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.
sqlpat	1.0.1	This tool should be used to audit the strength of Microsoft SQL Server passwords offline.
sqlping	4	SQL Server scanning tool that also checks for weak passwords using wordlists.
sqlpowerinjector	1.2	Application created in .Net 1.1 that helps the penetration tester to find and exploit SQL injections on a web page.
sqlsus	0.7.2	An open source MySQL injection and takeover tool, written in perl
ssdeep	2.14.1	A program for computing context triggered piecewise hashes
ssdp-scanner	1.0	SSDP amplification scanner written in Python. Makes use of Scapy.
ssh-audit	2.5.0	SSH server auditing (banner, key exchange, encryption, mac, compression, compatbility, etc).
ssh-honeypot	109.6307259	Fake sshd that logs ip addresses, usernames, and passwords.
ssh-mitm	140.70998ba	SSH man-in-the-middle tool.
ssh-privkey-crack	0.4	A SSH private key cracker.
ssh-user-enum	7.ae453c1	SSH User Enumeration Script in Python Using The Timing Attack.
sshatter	1.2	Password bruteforcer for SSH.
sshfuzz	1.0	A SSH Fuzzing utility written in Perl that uses Net::SSH2.
sshprank	1.4.2	A fast SSH mass-scanner, login cracker and banner grabber tool using the python-masscan module.
sshscan	1:1.0	A horizontal SSH scanner that scans large swaths of IPv4 space for a single SSH user and pass.
sshtrix	0.0.3	A very fast multithreaded SSH login cracker.
sshtunnel	0.4.0	Pure python SSH tunnels.
sshuttle	1.1.1	Transparent proxy server that forwards all TCP packets over ssh
ssl-hostname-resolver	1	CN (Common Name) grabber on X.509 Certificates over HTTPS.
ssl-phuck3r	2.0	All in one script for Man-In-The-Middle attacks.
sslcat	1.0	SSLCat is a simple Unix utility that reads and writes data across an SSL

		enable network connection.
sslcaudit	524.f218b9b	Utility to perform security audits of SSL/TLS clients.
ssldump	1.7	an SSLv3/TLS network protocol analyzer
sslh	1.22.c	SSL/SSH/OpenVPN/XMPP/tinc port multiplexer
ssllabs-scan	250.7a9f44e	Command-line client for the SSL Labs APIs
sslmap	0.2.0	A lightweight TLS/SSL cipher suite scanner.
sslnuke	5.c5faeaa	Transparent proxy that decrypts SSL traffic and prints out IRC messages.
sslscan	2.0.16	A fast tools to scan SSL services, such as HTTPS to determine the ciphers that are supported
sslscan2	649.bc46606	Tests SSL/TLS enabled services to discover supported cipher suites.
sslsniff	0.8	A tool to MITM all SSL connections on a LAN and dynamically generate certs for the domains that are being accessed on the fly
sslstrip	0.9	Python tool to hijack HTTPS connections during a MITM attack.
sslyze	5.0.6	Python tool for analyzing the configuration of SSL servers and for identifying misconfigurations.
ssma	215.2a2b6bd	Simple Static Malware Analyzer.
ssrf-proxy	293.e79da7a	Facilitates tunneling HTTP communications through servers vulnerable to Server-Side Request Forgery.
ssrf-sheriff	2.f95d691	A simple SSRF-testing sheriff written in Go.
ssrfmap	101.cd7536e	Automatic SSRF fuzzer and exploitation tool.
stackflow	2.2af525d	Universal stack-based buffer overfow exploitation tool.
stacoan	0.90	Crossplatform tool which aids developers, bugbounty hunters and ethical hackers performing static code analysis on mobile applications.
stacs	0.4.15.r0.gd6f71cf	Static Token And Credential Scanner.
staekka	9.57787ca	This plugin extends Metasploit for some missing features and modules allowing interaction with other/custom exploits/ways of getting shell access.
stardox	41.95b0a97	Github stargazers information gathering tool.
starttls-mitm	7.b257756	A mitm proxy that will transparently proxy and dump both plaintext and TLS traffic.
statsprocessor	5:0.11	A high-performance word-generator based on per-position Markov-attack.
stegcracker	2.1.0	Steganography brute-force utility to uncover hidden data inside files.

stegdetect	19.ac1df7a	An automated tool for detecting steganographic content in images.
steghide	0.5.1	Embeds a message in a file by replacing some of the least significant bits
stegolego	8.85354f6	Simple program for using stegonography to hide data within BMP images.
stegosip	11.5cda6d6	TCP tunnel over RTP/SIP.
stegoveritas	1.9	Automatic image steganography analysis tool.
stegseek	104.ff677b9	Lightning fast steghide cracker.
stegsolve	1.3	Steganography Solver.
stenographer	486.355604b	A packet capture solution which aims to quickly spool all packets to disk, then provide simple, fast access to subsets of those packets.
stepic	0.4	A python image steganography tool.
stews	1.0.0.r7.gc7bba5a	A Security Tool for Enumerating WebSockets.
sticky-keys-hunter	15.c816fc9	Script to test an RDP host for sticky keys and utilman backdoor.
stig-viewer	2.8	XCCDF formatted SRGs and STIGs files viewer for SCAP validation tools.
stompy	0.0.4	An advanced utility to test the quality of WWW session identifiers and other tokens that are meant to be unpredictable.
stoq	769.8bfc78b	An open source framework for enterprise level automated analysis.
storm-ring	0.1	This simple tool is useful to test a PABX with "allow guest" parameter set to "yes" (in this scenario an anonymous caller could place a call).
stowaway	v2.1.r1.g366d6a5	A Multi-hop proxy tool for security researchers and pentesters.
strace	6.2	A diagnostic, debugging and instructional userspace tracer
streamfinder	1.2	Searches for Alternate Data Streams (ADS).
striker	85.87c184d	An offensive information and vulnerability scanner.
stringsifter	29.3cb284a	Machine learning tool that automatically ranks strings based on their relevance for malware analysis.
striptls	55.5ec712c	Proxy PoC implementation of STARTTLS stripping attacks.
strutscan	4.8712c12	Apache Struts2 vulnerability scanner written in Perl.
stunnel	5.69	A program that allows you to encrypt arbitrary TCP connections inside SSL
sub7	2.2	A remote administration tool. No further comments ;-)

subbrute	1.2.1	A DNS meta-query spider that enumerates DNS records and subdomains
subdomainer	1.2	A tool designed for obtaining subdomain names from public sources.
subfinder	1257.bf74523	Modular subdomain discovery tool that can discover massive amounts of valid subdomains for any target.
subjack	182.49c51e5	Subdomain Takeover tool written in Go.
subjs	45.76ce9ec	Fetches javascript file from a list of URLS or subdomains.
sublert	67.56d2a12	A security and reconnaissance tool which leverages certificate transparency to automatically monitor new subdomains deployed by specific organizations and issued TLS/SSL certificate.
sublist3r	138.729d649	A Fast subdomains enumeration tool for penetration testers.
subover	71.3d258e2	A Powerful Subdomain Takeover Tool.
subscraper	2:12.b736b01	Tool that performs subdomain enumeration through various techniques.
subterfuge	2:64.69dda99	Automated Man-in-the-Middle Attack Framework
sucrack	1.2.3	A multi-threaded Linux/UNIX tool for brute-force cracking local user accounts via su
suid3num	60.2241c9c	Python script which utilizes python's built-in modules to enumerate SUID binaries.
sulley	4:1.0.bff0dd1	A pure-python fully automated and unattended fuzzing framework.
superscan	4.1	Powerful TCP port scanner, pinger, resolver.
suricata	6.0.10	An Open Source Next Generation Intrusion Detection and Prevention Engine.
suricata-verify	958.494b9d59	Suricata Verification Tests - Testing Suricata Output.
svn-extractor	43.1de6adb	A simple script to extract all web resources by means of .SVN folder exposed over network.
swaks	20201014.0	Swiss Army Knife SMTP; Command line SMTP testing, including TLS and AUTH
swamp	59.3c8be65	An OSINT tool for discovering associated sites through Google Analytics Tracking IDs.
swap-digger	51.4d18ce0	A tool used to automate Linux swap analysis during post-exploitation or forensics.
swarm	1:41.1713c1e	A distributed penetration testing tool.
swfintruder	0.9.1	First tool for testing security in Flash movies. A runtime analyzer for SWF external movies. It helps to find flaws in Flash.

swftools	0.9.2	A collection of SWF manipulation and creation utilities
syborg	36.5cd010b	Recursive DNS Subdomain Enumerator with dead-end avoidance system.
syft	814.5e5312c	A CLI tool and go library for generating a Software Bill of Materials (SBOM) from container images and filesystems.
sylkie	1:0.0.4.r3.g1cf170f	IPv6 address spoofing with the Neighbor Discovery Protocol.
syms2elf	12.329c2ce	A plugin for Hex-Ray's IDA Pro and radare2 to export the symbols recognized to the ELF symbol table.
synflood	0.1	A very simply script to illustrate DoS SYN Flooding attack.
synner	1.1	A custom eth->ip->tcp packet generator (spoofer) for testing firewalls and dos attacks.
synscan	5.02	fast asynchronous half-open TCP portscanner
syringe	12.79a703e	A General Purpose DLL & Code Injection Utility.
sysdig	0.31.5	Open source system-level exploration and troubleshooting tool
sysinternals-suite	1:5.9	Sysinternals tools suite.
t50	5.8.7	Experimental Multi-protocol Packet Injector Tool.
tabi	13.068a406	BGP Hijack Detection.
tachyon-scanner	461.6a0900e	Fast Multi-Threaded Web Discovery Tool.
tactical-exploitation	90.0df0bd2	Modern tactical exploitation toolkit.
Tails	5.4	It aims at preserving your privacy and anonymity, and helps you to: use the Internet anonymously and circumvent censorship; all connections to the Internet are forced to go through the Tor network; leave no trace on the computer you are using unless you ask it explicitly; use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.
taipan	1:2.9.498.18	Web application security scanner.
takeover	98.a058647	Sub-Domain TakeOver Vulnerability Scanner.
talon	v3.1.r0.gbee8aa4	A password guessing tool that targets the Kerberos and LDAP services within the Windows Active Directory environment.
taof	0.3.2	Taof is a GUI cross-platform Python generic network protocol fuzzer.
tbear	1.5	Transient Bluetooth Environment Auditor includes an ncurses-based Bluetooth scanner (a bit similar to kismet), a Bluetooth DoS tool, and a Bluetooth hidden device locator.

tcgetkey	0.1	A set of tools that deal with acquiring physical memory dumps via FireWire and then scan the memory dump to locate TrueCrypt keys and finally decrypt the encrypted TrueCrypt container using the keys.
tchunt-ng	208.b8cf7fc	Reveal encrypted files stored on a filesystem.
tckfc	23.911e92e	TrueCrypt key file cracker.
tcpcontrol-fuzzer	2:0.1	2^6 TCP control bit fuzzer (no ECN or CWR).
tcpcopy	1244.9a5406a	A TCP stream replay tool to support real testing of Internet server applications.
tcpdstat	4.be5bd28	Get protocol statistics from tcpdump pcap files.
tcpdump	4.99.4	A tool for network monitoring and data acquisition
tcpextract	1.1	Extracts files from captured TCP sessions. Support live streams and pcap files.
tcpflow	1.6.1	Captures data transmitted as part of TCP connections then stores the data conveniently
tcpick	0.2.1	TCP stream sniffer and connection tracker
tcpjunk	2.9.03	A general tcp protocols testing and hacking utility.
tcpreplay	4.4.3	Gives the ability to replay previously captured traffic in a libpcap format
tcptrace	6.6.7	A TCP dump file analysis tool
tcptraceroute	1.5beta7	A traceroute implementation using TCP packets.
tcpwatch	1.3.1	A utility written in Python that lets you monitor forwarded TCP connections or HTTP proxy connections.
tcpxtract	1.0.1	A tool for extracting files from network traffic.
teamsuserenum	v1.0.r1.g0c8b6c2	User enumeration with Microsoft Teams API
teardown	1.0	Command line tool to send a BYE request to tear down a call.
tekdefense-automater	88.42548cf	IP URL and MD5 OSINT Analysis
tell-me-your-secrets	1:v2.4.1.r0.g8d59fe3	Find secrets on any machine from over 120 Different Signatures.
tempomail	25.3ca0fcf	Tool to create a temporary email address in 1 Second and receive emails.
termineter	203.9311d6d	Smart meter testing framework
terminus-font-	4.47.0	Monospaced bitmap font designed for long work with computers (TTF

ttf		version, mainly for Java applications).
testdisk	7.1	Checks and undeletes partitions + PhotoRec, signature based recovery tool
testssl	1:2.9.5	Testing TLS/SSL encryption.
testssl.sh	3.0.8	Testing TLS/SSL encryption
tfsec	v0.63.1.r380.gfbca9334c	Security scanner for your Terraform code.
tftp-bruteforce	0.1	TFTP-bruteforcer is a fast TFTP filename bruteforcer written in perl.
tftp-fuzz	1:1337	Master TFTP fuzzing script as part of the ftools series of fuzzers.
tftp-proxy	0.1	This tool accepts connection on tftp and reloads requested content from an upstream tftp server. Meanwhile modifications to the content can be done by pluggable modules. So this one's nice if your mitm with some embedded devices.
tgcd	1.1.1	TCP/IP Gender Changer Daemon utility.
thc-ipv6	3.8	Complete tool set to attack the inherent protocol weaknesses of IPv6 and ICMP6
thc-keyfinder	1.0	Finds crypto keys, encrypted data and compressed data in files by analyzing the entropy of parts of the file.
thc-pptp-bruter	0.1.4	A brute force program that works against pptp vpn endpoints (tcp port 1723).
thc-smartbrute	1.0	This tool finds undocumented and secret commands implemented in a smartcard.
thc-ssl-dos	1.4	A tool to verify the performance of SSL. To be used in your authorized and legitimate area ONLY. You need to accept this to make use of it, no use for bad intentions, you have been warned!
thcrut	1.2.5	Network discovery and OS Fingerprinting tool.
thedorkbox	7.43852d3	Comprehensive collection of Google Dorks & OSINT techniques to find Confidential Data.
thefatrat	813.b0586d0	TheFatRat a massive exploiting tool: easy tool to generate backdoor and easy tool to post exploitation attack.
thefuzz	160.b4c2c80	CLI fuzzing tool.
theharvester	3231.caf21cb	Python tool for gathering e-mail accounts and subdomain names from different public sources (search engines, pgp key servers).
themole	0.3	Automatic SQL injection exploitation tool.
thezoo	156.d4404c8	A project created to make the possibility of malware analysis open and

		available to the public.
threatspec	0.5.0	Project to integrate threat modelling into development process.
thumbcacheviewer	1.0.3.7	Extract Windows thumbcache database files.
tidos-framework	v2.0.beta2.r22.g4098187	Offensive Web Application Penetration Testing Framework.
tiger	3.2.3	A security scanner, that checks computer for known problems. Can also use tripwire, aide and chkrootkit.
tilt	90.2bc2ef2	An easy and simple tool implemented in Python for ip reconnaissance, with reverse ip lookup.
timegen	0.4	This program generates a *.wav file to "send" an own time signal to DCF77 compatible devices.
timeverter	83.24b715e	Bruteforce time-based tokens and to convert several time domains.
tinc	1.0.36	VPN (Virtual Private Network) daemon
tinfoleak	3.6469eb3	Get detailed information about a Twitter user activity.
tinfoleak2	41.c45c33e	Get detailed information about a Twitter user activity.
tinyproxy	1.11.1	A light-weight HTTP proxy daemon for POSIX operating systems.
tls-attacker	1:6653.742394f9b	A Java-based framework for analyzing TLS libraries.
tls-fingerprinting	257.4b6e878	Tool and scripts to perform TLS Fingerprinting.
tls-map	v2.1.0.r54.g13b6ecf	CLI & library for mapping TLS cipher algorithm names: IANA, OpenSSL, GnUTLS, NSS.
tls-prober	286.72b1029	A tool to fingerprint SSL/TLS servers.
tlsenum	78.787c88b	A command line tool to enumerate TLS cipher-suites supported by a server.
tlsfuzzer	1427.d0d14c2	SSL and TLS protocol test suite and fuzzer.
tlshelpers	21.6e422be	A collection of shell scripts that help handling X.509 certificate and TLS issues.
tlspretense	1:v0.6.2.r22.g0a5faf4	SSL/TLS client testing framework
tlssled	1.3	A Linux shell script whose purpose is to evaluate the security of a target SSL/TLS (HTTPS) web server implementation.

tlsx	v1.0.6.r3.g55ee7ec	TLS grabber focused on TLS based data collection.
tnscmd	1.3	a lame tool to prod the oracle tnslsnr process (1521/tcp)
token-hunter	343.3358a33	OSINT Tool - Search the group and group members' snippets, issues, and issue discussions for sensitive data that may be included in these assets.
token-reverser	10.cbb4528	Word list generator to crack security tokens.
tomcatwardeployer	98.4535e64	Apache Tomcat auto WAR deployment & pwning penetration testing tool.
topera	19.3e230fd	An IPv6 security analysis toolkit, with the particularity that their attacks can't be detected by Snort.
tor	0.4.7.13	Anonymizing overlay network.
tor-autocircuit	0.2	Tor Autocircuit was developed to give users a finer control over Tor circuit creation. The tool exposes the functionality of TorCtl library which allows its users to control circuit length, speed, geolocation, and other parameters.
tor-browser	12.0.4	Tor Browser Bundle: anonymous browsing using Firefox and Tor.
tor-browser-en	11.5.6	Tor Browser Bundle: Anonymous browsing using firefox and tor
tor-router	4.001a510	A tool that allow you to make TOR your default gateway and send all internet connections under TOR (as transparent proxy) for increase privacy/anonymity without extra unnecessary code.
torcrawl	81.3241834	Crawl and extract (regular or onion) webpages through TOR network.
torctl	1:0.5.7	Script to redirect all traffic through tor network.
torpy	60.ebf000c	Pure python Tor client implementation.
torshammer	1.0	A slow POST Denial of Service testing tool written in Python.
torsocks	2.4.0	Wrapper to safely torify applications
tpcat	latest	TPCAT is based upon pcapdiff by the EFF. TPCAT will analyze two packet captures (taken on each side of the firewall as an example) and report any packets that were seen on the source capture but did not make it to the dest.
tplmap	719.616b0e5	Automatic Server-Side Template Injection Detection and Exploitation Tool.
traceroute	2.1.2	Tracks the route taken by packets over an IP network
trape	132.6baae24	People tracker on the Internet: OSINT analysis and research tool by Jose Pino.

traxss	81.48dee2e	Automated XSS Vulnerability Scanner.
treasure	1:2.b3249be	Hunt for sensitive information through githubs code search.
trevorspray	111.70aca7b	A modular password sprayer with threading, clever proxying, loot modules, and more!
trid	2.24	An utility designed to identify file types from their binary signatures.
trinity	5188.ca07c86b	A Linux System call fuzzer.
triton	1:4080.c344d782	A Dynamic Binary Analysis (DBA) framework.
trivy	0.41.0	A Simple and Comprehensive Vulnerability Scanner for Containers, Suitable for CI.
trixd00r	0.0.1	An advanced and invisible userland backdoor based on TCP/IP for UNIX systems.
trizen	1.52	Trizen AUR Package Manager: A lightweight wrapper for AUR.
truecrypt	1:7.1a	Free open-source cross-platform disk encryption software
truegaze	117.c3f26bc	Static analysis tool for Android/iOS apps focusing on security issues outside the source code.
truehunter	14.0a2895d	Detect TrueCrypt containers using a fast and memory efficient approach.
trufflehog	213.e9ac138	Searches through git repositories for high entropy strings, digging deep into commit history.
trusttrees	102.a9b7399	A Tool for DNS Delegation Trust Graphing.
tsh	0.6	An open-source UNIX backdoor that compiles on all variants, has full pty support, and uses strong crypto for communication.
tsh-sctp	2.850a2da	An open-source UNIX backdoor.
ttpassgen	133.a06d99d	Highly flexible and scriptable password dictionary generator based on Python.
tunna	41.cba006d	a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments.
turner	29.f57ebb9	Tunnels HTTP over a permissive/open TURN server; supports HTTP and SOCKS5 proxy.
tuxcut	1:3.77cd151	Netcut-like program for Linux written in PyQt.
tweets-analyzer	55.8d6bd3c	Tweets metadata scraper & activity analyzer.
tweetshell	21.47a415c	Multi-thread Twitter BruteForcer in Shell Script.

twint	1:845.e7c8a0c7	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.
twofi	2.0	Twitter Words of Interest.
typo-enumerator	1:14.295f103	Enumerate Typo3 version and extensions.
typo3scan	v1.1.2.r3.g330d71b	Enumerate Typo3 version and extensions.
tyton	1:80.56494f3	Kernel-Mode Rootkit Hunter.
u3-pwn	2.0	A tool designed to automate injecting executables to Sandisk smart usb devices with default U3 software install.
uacme	271.dbbcc71	Defeating Windows User Account Control.
uatester	1.06	User Agent String Tester
uberfile	14.4414c2a	CLI tool for the generation of downloader oneliners for UNIX-like or Windows systems.
ubertooth	2020.12.R1	A 2.4 GHz wireless development board suitable for Bluetooth experimentation. Open source hardware and software. Tools only.
ubiquiti-probing	5.c28f4c1	A Ubiquiti device discovery tool.
ubitack	0.3	Tool, which automates some of the tasks you might need on a (wireless) penetration test or while you are on the go.
udis86	1.7.2	A minimalistic disassembler library
udork	102.1a0aab0	Python script that uses advanced Google search techniques to obtain sensitive information in files or directories, find IoT devices, detect versions of web applications.
udp-hunter	4.b95cce5	Network assessment tool for various UDP Services covering both IPv4 and IPv6 protocols.
udp2raw	20230206.0	A Tunnel which Turns UDP Traffic into Encrypted UDP/FakeTCP/ICMP Traffic by using Raw Socket
udp2raw-tunnel	20200818.0	An Encrpyted, Anti-Replay, Multiplexed Udp Tunnel, tunnels udp traffic through fake-tcp or icmp by using raw socket.
udpastcp	29.683b5e3	This program hides UDP traffic as TCP traffic in order to bypass certain firewalls.
udptunnel	2:19	Tunnels TCP over UDP packets.
udsim	33.b379464	A graphical simulator that can emulate different modules in a vehicle and

		respond to UDS request.
uefi-firmware-parser	181.dfb15b0	Parse BIOS/Intel ME/UEFI firmware related structures: Volumes, FileSystems, Files, etc
ufo-wardriving	4	Allows you to test the security of wireless networks by detecting their passwords based on the router model.
ufonet	83.e5d4014	A tool designed to launch DDoS attacks against a target, using 'Open Redirect' vectors on third party web applications, like botnet.
uhoh365	26.110277a	Script to enumerate Office 365 users without performing login attempts
ultimate-facebook-scraper	236.5661bdc	A bot which scrapes almost everything about a Facebook user's profile.
umap	25.3ad8121	The USB host security assessment tool.
umit	1.0	A powerful nmap frontend.
uncaptcha2	7.473f33d	Defeating the latest version of ReCaptcha with 91% accuracy.
uncover	v1.0.2.r2.g4b929e0	Discover exposed hosts on the internet using multiple search engines.
unfurl	16.99ad735	Pull out bits of URLs provided on stdin.
unhide	20220611	A forensic tool to find processes hidden by rootkits, LKMs or by other techniques.
unibrute	1.b3fb4b7	Multithreaded SQL union bruteforcer.
unicorn-powershell	202.80a37eb	A simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory.
unicornscan	0.4.7	A new information gathering and correlation engine.
unifuzzer	5.3385a3b	A fuzzing tool for closed-source binaries based on Unicorn and LibFuzzer.
uniofuzz	2:1337	The universal fuzzing tool for browsers, web services, files, programs and network services/ports
uniscan	6.3	A simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.
unix-privesc-check	1.4	Tries to find misconfigurations that could allow local unprivilged users to escalate privileges to other users or to access local apps (e.g. databases).
unsecure	1.2	Bruteforces network login masks.
unstrip	13.05e00c2	ELF Unstrip Tool.
untwister	119.a42b8f8	Seed recovery tool for PRNGs.

upnp-pentest-toolkit	1.1	UPnP Pentest Toolkit for Windows.
upnpscan	0.4	Scans the LAN or a given address range for UPnP capable devices.
uppwn	9.f69dec4	A script that automates detection of security flaws on websites' file upload systems'.
uptux	33.85ccfd0	Linux privilege escalation checks (systemd, dbus, socket fun, etc).
upx	4.0.2	Ultimate executable compressor.
urh	2.9.4	Universal Radio Hacker: investigate wireless protocols like a boss.
urlcrazy	0.5	Generate and test domain typos and variations to detect and perform typo squatting, URL hijacking, phishing, and corporate espionage.
urldigger	02c	A python tool to extract URL addresses from different HOT sources and/or detect SPAM and malicious code
urlextractor	19.739864d	Information gathering & website reconnaissance.
urlview	0.9	A curses URL parser for text files.
usb-canary	31.bb23552	A Linux or OSX tool that uses psutil to monitor devices while your computer is locked. In the case it detects someone plugging in or unplugging devices it can be configured to send you an SMS or alert you via Slack or Pushover.
usbrip	291.5093c84	USB device artifacts tracker.
username-anarchy	54.d5e653f	Tools for generating usernames when penetration testing.
usernamer	20.12983f8	Pentest Tool to generate usernames/logins based on supplied names.
userrecon	10.3b56891	Find usernames across over 75 social networks.
userrecon-py	1:15.eebd422	Recognition usernames in 187 social networks.
usnjrnl2csv	29.1ecbddc	Parser for $UsnJrnl on NTFS.
usnparser	4.1.5	A Python script to parse the NTFS USN journal.
uw-loveimap	0.1	Multi threaded imap bounce scanner.
uw-offish	0.1	Clear-text protocol simulator.
uw-udpscan	0.1	Multi threaded udp scanner.
uw-zone	0.1	Multi threaded, randomized IP zoner.
v3n0m	532.1e2c9dd	A tool to automate mass SQLi d0rk scans and Metasploit Vulns.
vais	17.5c35c3a	SWF Vulnerability & Information Scanner.
valabind	1.8.0	Tool to parse vala or vapi files to transform them into swig interface files,

		C++, NodeJS-ffi or GIR
valgrind	3.20.0	A tool to help find memory-management problems in programs
valhalla	87.c010a48	Valhalla API Client.
vane	1899.48f9ab5	A vulnerability scanner which checks the security of WordPress installations using a black box approach.
vanguard	0.1	A comprehensive web penetration testing tool written in Perl that identifies vulnerabilities in web applications.
vault	297.593e046	Secure, store and tightly control access to tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data using a UI, CLI, or HTTP API.
vault-scanner	299.0303cf4	Swiss army knife for hackers.
vba2graph	29.fcf96ef	Generate call graphs from VBA code, for easier analysis of malicious documents.
vbrute	1.11dda8b	Virtual hosts brute forcer.
vbscan	1:39.2b1ce48	A black box vBulletin vulnerability scanner written in perl.
vbsmin	v1.1.0.r50.g2aa5c92	VBScript minifier.
vcsmap	47.3889964	A plugin-based tool to scan public version control systems for sensitive information.
vega	1.0	An open source platform to test the security of web applications.
veil	5:297.d8acd4c	A tool designed to generate metasploit payloads that bypass common anti-virus solutions.
veles	1:637.e65de5a	New open source tool for binary data analysis.
venom	135.2b84e68	A Multi-hop Proxy for Penetration Testers.
veracrypt	1.25.9	Disk encryption with strong security based on TrueCrypt
verinice	1.19.1.r1.gf82b192a6	Tool for managing information security.
vfeed	3:81.fad17ae	Open Source Cross Linked and Aggregated Local Vulnerability Database main repository.
vhostscan	338.4a3a1ee	A virtual host scanner that can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.
videosnarf	0.63	A new security assessment tool for pcap analysis
vinetto	0.07beta	A forensics tool to examine Thumbs.db files

viper	2091.cd532ca	A Binary analysis framework.
vipermonkey	1160.511ecd5	A VBA parser and emulation engine to analyze malicious macros.
viproy-voipkit	1:82.52b27db	VoIP Pen-Test Kit for Metasploit Framework
virustotal	4.9aea023	Command-line utility to automatically lookup on VirusTotal all files recursively contained in a directory.
visql	49.3082e30	Scan SQL vulnerability on target site and sites of on server.
visualize-logs	118.d2e370e	A Python library and command line tools to provide interactive log visualization.
vivisect	2:1705.d3b3d869	A Python based static analysis and reverse engineering framework, Vdb is a Python based research/reversing focused debugger and programatic debugging API by invisigoth of kenshoto
vlan-hopping	21.a37ba4e	Easy 802.1Q VLAN Hopping
vlany	255.9ef014a	Linux LD_PRELOAD rootkit (x86 and x86_64 architectures).
vmap	0.3	A Vulnerability-Exploit desktop finder.
vnak	1:1.cf0fda7	Aim is to be the one tool a user needs to attack multiple VoIP protocols.
vnc-bypauth	0.0.1	Multi-threaded bypass authentication scanner for VNC servers <= 4.1.1.
vncrack	1.21	What it looks like: crack VNC.
voiper	0.07	A VoIP security testing toolkit incorporating several VoIP fuzzers and auxilliary tools to assist the auditor.
voiphopper	2.04	A security validation tool that tests to see if a PC can mimic the behavior of an IP Phone. It rapidly automates a VLAN Hop into the Voice VLAN.
voipong	2.0	A utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to seperate wave files.
volafox	143.5b42987	Mac OS X Memory Analysis Toolkit.
volatility	2.6.1	Advanced memory forensics framework
volatility-extra	92.d9fc072	Volatility plugins developed and maintained by the community.
volatility3	2.4.1	Advanced memory forensics framework
voltron	627.d9fef0b	UI for GDB, LLDB and Vivisect's VDB.
vpnpivot	22.37bbde0	Explore the network using this tool.
vsaudit	21.2cbc47b	VOIP Security Audit Framework.
vscan	10.da4e47e	HTTPS / Vulnerability scanner.
vstt	0.5.3	VSTT is a multi-protocol tunneling tool. It accepts input by TCP stream

		sockets and FIFOs, and can send data via TCP, POP3, and ICMP tunneling.
vsvbp	6.241a7ab	Black box tool for Vulnerability detection in web applications.
vt-cli	0.13.0	VirusTotal Command Line Interface.
vulmap	95.a167c47	Vulmap Online Local Vulnerability Scanners Project
vulnerabilities-spider	1.426e70f	A tool to scan for web vulnerabilities.
vulnx	321.bcf451d	Cms and vulnerabilites detector & An intelligent bot auto shell injector.
vuls	1106.e3c27e1	Vulnerability scanner for Linux/FreeBSD, agentless, written in Go.
vulscan	2.0	A module which enhances nmap to a vulnerability scanner
w13scan	430.432b835	Passive Security Scanner.
w3af	1.6.49	Web Application Attack and Audit Framework.
waffit	202.d28dc3d	Identify and fingerprint Web Application Firewall (WAF) products protecting a website.
wafninja	25.379cd98	A tool which contains two functions to attack Web Application Firewalls.
wafp	0.01_26c3	An easy to use Web Application Finger Printing tool written in ruby using sqlite3 databases for storing the fingerprints.
wafpass	48.c3ea1b9	Analysing parameters with all payloads' bypass methods, aiming at benchmarking security solutions like WAF.
wafw00f	840.28ec94a	Identify and fingerprint Web Application Firewall (WAF) products protecting a website.
waidps	16.ff8d270	Wireless Auditing, Intrusion Detection & Prevention System.
waldo	29.ee4f960	A lightweight and multithreaded directory and subdomain bruteforcer implemented in Python.
wapiti	3.1.6.r1.g90a86e8	A vulnerability scanner for web applications. It currently search vulnerabilities like XSS, SQL and XPath injections, file inclusions, command execution, LDAP injections, CRLF injections...
wascan	1:37.6926338	Web Application Scanner.
wavemon	0.9.4	Ncurses-based monitoring application for wireless network devices
waybackpack	91.58b3d0f	Download the entire Wayback Machine archive for a given URL.
waybackurls	11.89da10c	Fetch all the URLs that the Wayback Machine knows about for a domain.
wcc	83.8254480	The Witchcraft Compiler Collection.
wce	1.41beta	A security tool to list logon sessions and add, change, list and delete

		associated credentials (ex.: LM/NT hashes, plaintext passwords and Kerberos tickets).
wcvs	1.1.0.r0.ga9ae886	Web Cache Vulnerability Scanner is a Go-based CLI tool for testing for web cache poisoning.
Web Security Dojo	3.4.1	A free open-source self-contained training environment for Web Application Security penetration testing. Tools + Targets = Dojo. Various web application security testing tools and vulnerable web applications were added to a clean install of Ubuntu v12.04LTS, which is patched with the appropriate updates and VM additions for easy use. The Web Security Dojo is for learning and practicing web app security testing techniques. It is ideal for self-teaching and skill assessment, as well as training classes and conferences since it does not need a network connection. The Dojo contains everything needed to get started - tools, targets, and documentation.
web-soul	2	A plugin based scanner for attacking and data mining web sites written in Perl.
web2ldap	1.7.6	Full-featured LDAP client running as web application.
webacoo	0.2.3	Web Backdoor Cookie Script-Kit.
webanalyze	108.6a48cd0	Port of Wappalyzer (uncovers technologies used on websites) in go to automate scanning.
webborer	173.b323cf4	A directory-enumeration tool written in Go.
webenum	21.24b43b4	Tool to enumerate http responses using dynamically generated queries and more. Useful for penetration tests against web servers.
webexploitation tool	155.85bcf0e	A cross platform web exploitation toolkit.
webfixy	25.5d477b0	On-the-fly decryption proxy for MikroTik RouterOS WebFig sessions.
webhandler	348.1bd971e	A handler for PHP system functions & also an alternative 'netcat' handler.
webhunter	12.918b606	Tool for scanning web applications and networks and easily completing the process of collecting knowledge.
webkiller	42.d680598	Tool Information Gathering Write By Python.
webpwn3r	38.3d75e76	A python based Web Applications Security Scanner.
webrute	3.3	Web server directory brute forcer.
webscarab	20120422.001828	Framework for analysing applications that communicate using the HTTP and HTTPS protocols

websearch	4.cb7ef8e	Search vhost names given a host range. Powered by Bing..
webshag	1.10	A multi-threaded, multi-platform web server audit tool.
webshells	46.e8e1a37	Web Backdoors.
webslayer	5	A tool designed for brute forcing Web Applications.
websockify	925.a134655	WebSocket to TCP proxy/bridge.
webspa	0.8	A web knocking tool, sending a single HTTP/S to run O/S commands.
websploit	4.0.4	An Open Source Project For, Social Engineering Works, Scan, Crawler & Analysis Web, Automatic Exploiter, Support Network Attacks
webtech	1.3.1	Identify technologies used on websites.
webxploiter	56.c03fe6b	An OWASP Top 10 Security scanner.
weebdns	14.c01c04f	DNS Enumeration with Asynchronicity.
weeman	91.53c2efa	HTTP Server for phishing in python.
weevely	883.0bae932	Weaponized web shell.
weirdaal	331.c14e36d	AWS Attack Library.
wepbuster	1.0_beta_0.7	script for automating aircrack-ng
wesng	283.13851e9	Windows Exploit Suggester - Next Generation.
wfuzz	1155.1b695ee	Utility to bruteforce web applications to find their not linked resources.
whapa	361.248b6e8	WhatsApp Parser Tool.
whatbreach	42.dad6b9f	OSINT tool to find breached emails and databases.
whatportis	54.59a1718	A command to search port names and numbers.
whatsmyname	2034.7e6ac66	Tool to perform user and username enumeration on various websites.
whatwaf	392.b14e866	Detect and bypass web application firewalls and protection systems.
whatweb	4910.efee4d80	Next generation web scanner that identifies what websites are running.
whichcdn	22.5fc6ddd	Tool to detect if a given website is protected by a Content Delivery Network.
whispers	2.1.5.r38.g1ef441f	Identify hardcoded secrets and dangerous behaviours.
whitewidow	605.4f27bfe	SQL Vulnerability Scanner.
wi-feye	1.1	An automated wireless penetration testing tool written in python, its designed to simplify common attacks that can be performed on wifi networks so that they can be executed quickly and easily.
wifi-autopwner	36.faa4d01	Script to automate searching and auditing Wi-Fi networks with weak security.

wifi-honey	1.0	A management tool for wifi honeypots.
wifi-monitor	30.0657e48	Prints the IPs on your local network that're sending the most packets.
wifi-pumpkin	2:v1.0.9R2.r0.g47d79c3	Framework for Rogue Wi-Fi Access Point Attack.
wifibroot	84.d0cd2cc	A WiFi Pentest Cracking tool for WPA/WPA2 (Handshake, PMKID, Cracking, EAPOL, Deauthentication).
wifichannelmonitor	1.70	A utility for Windows that captures wifi traffic on the channel you choose, using Microsoft Network Monitor capture driver.
wificurse	0.3.9	WiFi jamming tool.
wifijammer	96.9add021	A python script to continuosly jam all wifi clients within range.
wifiphisher	1:798.bc4a077	Fast automated phishing attacks against WPA networks.
wifiscanmap	135.9adcd08	Another wifi mapping tool.
wifitap	2b16088	WiFi injection tool through tun/tap device.
wifite	2:2.6.8	A tool to attack multiple WEP and WPA encrypted networks at the same time.
wig	574.d5ddd91	WebApp Information Gatherer.
wikigen	8.348aa99	A script to generate wordlists out of wikipedia pages.
wildpwn	11.4623714	Unix wildcard attacks.
windapsearch	28.7724ec4	Script to enumerate users, groups and computers from a Windows domain through LDAP queries.
windivert	2.2.0	A user-mode packet capture-and-divert package for Windows.
windows-binaries	20.7d272da	A colleciton of pentesting Windows binaries.
windows-exploit-suggester	41.776bd91	This tool compares a targets patch levels against the Microsoft vulnerability database in order to detect potential missing patches on the target.
windows-prefetch-parser	88.bc1fa58	Parse Windows Prefetch files.
windows-privesc-check	181.9f304fd	Standalone Executable to Check for Simple Privilege Escalation Vectors on Windows Systems.
windowsspyblocker	4.38.0	Block spying and tracking on Windows.
winexe	1.00	Remotely execute commands on Windows NT/2000/XP/2003 systems.

winfo	2.0	Uses null sessions to remotely try to retrieve lists of and information about user accounts, workstation/interdomain/server trust accounts, shares (also hidden), sessions, logged in users, and password/lockout policy, from Windows NT/2000/XP.
winhex	20.4	Hex Editor and Disk Editor.
winpwn	402.1c71a13	Automation for internal Windows Penetrationtest / AD-Security.
winregfs	153.7567c83	Windows Registry FUSE filesystem.
winrelay	2.0	A TCP/UDP forwarder/redirector that works with both IPv4 and IPv6.
wireless-ids	24.b132071	Ability to detect suspicious activity such as (WEP/WPA/WPS) attack by sniffing the air for wireless packets.
wireshark-cli	4.0.5	a free network protocol analyzer for Unix/Linux and Windows - CLI version
wireshark-gtk	2.6.6	a free network protocol analyzer for Unix/Linux and Windows - GTK frontend
wireshark-qt	4.0.5	Network traffic and protocol analyzer/sniffer - Qt GUI
wirouter-keyrec	1.1.2	A powerful and platform independent software to recover the default WPA passphrases of the supported router models (Telecom Italia Alice AGPF, Fastweb Pirelli, Fastweb Tesley, Eircom Netopia, Pirelli TeleTu/Tele 2).
witchxtool	1.1	A perl script that consists of a port scanner, LFI scanner, MD5 bruteforcer, dork SQL injection scanner, fresh proxy scanner, and a dork LFI scanner.
wlan2eth	1.3	Re-writes 802.11 captures into standard Ethernet frames.
wmat	3:0.1	Automatic tool for testing webmail accounts.
wmd	30.32e249a	Python framework for IT security tools.
wmi-forensics	11.0ab08dc	Scripts used to find evidence in WMI repositories.
wnmap	0.1	A shell script written with the purpose to automate and chain scans via nmap. You can run nmap with a custom mode written by user and create directories for every mode with the xml/nmap files inside.
wol-e	2.0	A suite of tools for the Wake on LAN feature of network attached computers.
wolpertinger	2.58ef8e2	A distributed portscanner.
wondershaper	48.98792b5	Limit the bandwidth of one or more network adapters.
wordbrutepress	30.5165648	Python script that performs brute forcing against WordPress installs using a wordlist.
wordlistctl	0.9.3	Fetch, install and search wordlist archives from websites and torrent peers.

wordlister	56.7457c21	A simple wordlist generator and mangler written in python.
wordpot	44.e96889b	A Wordpress Honeypot.
wordpress-exploit-framework	907.e55ded4	A Ruby framework for developing and using modules which aid in the penetration testing of WordPress powered websites and systems.
wordpresscan	76.f810c1c	WPScan rewritten in Python + some WPSeku ideas.
wpa-bruteforcer	4.d5f8586	Attacking WPA/WPA encrypted access point without client.
wpa2-halfhandshake-crack	29.3f42124	A POC to show it is possible to capture enough of a handshake with a user from a fake AP to crack a WPA2 network without knowing the passphrase of the actual AP.
wpbf	7.11b6ac1	Multithreaded WordPress brute forcer.
wpbrute-rpc	3.e7d8145	Tool for amplified bruteforce attacks on wordpress based website via xmlrcp API.
wpbullet	34.6185112	A static code analysis for WordPress (and PHP).
wpforce	88.b72ec64	Wordpress Attack Suite.
wpintel	6.741c0c9	Chrome extension designed for WordPress Vulnerability Scanning and information gathering.
wpscan	1:3.8.22	Black box WordPress vulnerability scanner
wpseku	2:39.862fb2c	Simple Wordpress Security Scanner.
wpsik	8.8d3856b	WPS scan and pwn tool.
wpsweep	1.0	A simple ping sweeper, that is, it pings a range of IP addresses and lists the ones that reply.
wreckuests	75.69b6c27	Yet another one hard-hitting tool to run DDoS atacks with HTTP-flood.
ws-attacker	1.7	A modular framework for web services penetration testing.
wscript	201.0410be2	Emulator/tracer of the Windows Script Host functionality.
wsfuzzer	1.9.5	A Python tool written to automate SOAP pentesting of web services.
wssip	75.56d0d2c	Application for capturing, modifying and sending custom WebSocket data from client to server and vice versa.
wsuspect-proxy	24.89f9375	A tool for MITM'ing insecure WSUS connections.
wups	1.4	An UDP port scanner for Windows.
wuzz	229.66176b6	Interactive cli tool for HTTP inspection.
wxhexeditor	722.c22ce20	A free hex editor / disk editor for Linux, Windows and MacOSX.
wyd	0.2	Gets keywords from personal files. IT security/forensic tool.

x-rsa	165.ec75d15	Contains a many of attack types in RSA such as Hasted, Common Modulus, Chinese Remainder Theorem.
x-scan	3.3	A general network vulnerabilities scanner for scanning network vulnerabilities for specific IP address scope or stand-alone computer by multi-threading method, plug-ins are supportable.
x64dbg	2023.03.04	An open-source x64/x32 debugger for windows.
x8	1:v4.1.0.r2.g6ee4532	Hidden parameters discovery suite.
xattacker	122.72f9f8e	Website Vulnerability Scanner & Auto Exploiter.
xcat	266.faaf8fe	A command line tool to automate the exploitation of blind XPath injection vulnerabilities.
xcavator	5.bd9e2d8	Man-In-The-Middle and phishing attack tool that steals the victim's credentials of some web services like Facebook.
xcname	11.9c475a1	A tool for enumerating expired domains in CNAME records.
xerosploit	38.e2c3c7b	Efficient and advanced man in the middle framework.
xfltreat	270.17d4ec8	Tunnelling framework.
xmlrpc-bruteforcer	35.6023237	An XMLRPC brute forcer targeting Wordpress written in Python 3.
xorbruteforcer	0.1	Script that implements a XOR bruteforcing of a given file, although a specific key can be used too.
xorsearch	1.11.4	Program to search for a given string in an XOR, ROL or ROT encoded binary file.
xortool	0.99	A tool to analyze multi-byte xor cipher.
xpire-crossdomain-scanner	1.0cb8d3b	Scans crossdomain.xml policies for expired domain names.
xpl-search	42.d4dbc97	Search exploits in multiple exploit databases!.
xplico	1:1.2.2	Internet Traffic Decoder. Network Forensic Analysis Tool (NFAT).
xprobe2	0.3	An active OS fingerprinting tool.
xray	91.ca50a32	A tool for recon, mapping and OSINT gathering from public networks.
xrop	83.4af7452	Tool to generate ROP gadgets for ARM, AARCH64, x86, MIPS, PPC, RISCV, SH4 and SPARC.
xspear	1:144.57bb7b4	Powerfull XSS Scanning and Parameter analysis tool&gem.

xspy	1.0c	A utility for monitoring keypresses on remote X servers
xsrfprobe	523.ce04111	The Prime Cross Site Request Forgery Audit and Exploitation Toolkit.
xss-freak	17.e361766	An XSS scanner fully written in Python3 from scratch.
xsscon	45.ce91fd6	Simple XSS Scanner tool.
xsscrapy	153.4966255	XSS spider - 66/66 wavsep XSS detected.
xsser	2:1.8	A penetration testing tool for detecting and exploiting XSS vulnerabilites.
xssless	45.8e7ebe1	An automated XSS payload generator written in python.
xsspy	60.b10d336	Web Application XSS Scanner.
xsss	0.40b	A brute force cross site scripting scanner.
xssscan	1:17.7f1ea90	Command line tool for detection of XSS attacks in URLs. Based on ModSecurity rules from OWASP CRS.
xsssniper	79.02b59af	An automatic XSS discovery tool
xsstracer	5.f2ed21a	Python script that checks remote web servers for Clickjacking, Cross-Frame Scripting, Cross-Site Tracing and Host Header Injection.
xsstrike	467.f292787	An advanced XSS detection and exploitation suite.
xssya	1:13.cd62817	A Cross Site Scripting Scanner & Vulnerability Confirmation.
xwaf	162.c6f6bb7	Automatic WAF bypass tool.
xxeinjector	55.604c39a	Tool for automatic exploitation of XXE vulnerability using direct and different out of band methods.
xxeserv	12.046c559	A mini webserver with FTP support for XXE payloads.
xxexploiter	103.c1f0f41	It generates the XML payloads, and automatically starts a server to serve the needed DTD's or to do data exfiltration.
xxxpwn	10.27a2d27	A tool Designed for blind optimized XPath 1 injection attacks.
xxxpwn-smart	6.b11b95b	A fork of xxxpwn adding further optimizations and tweaks.
yaaf	7.4d6273a	Yet Another Admin Finder.
yaf	2.12.2	Yet Another Flowmeter.
yara	4.3.0	Tool aimed at helping malware researchers to identify and classify malware samples
yasat	848	Yet Another Stupid Audit Tool.
yasca	2.1	Multi-Language Static Analysis Toolset.
yasuo	121.994dcb1	A ruby script that scans for vulnerable & exploitable 3rd-party web applications on a network.
yate-bts	6.1.0	An open source GSM Base Station software.

yawast	1072.5e9e7a3	The YAWAST Antecedent Web Application Security Toolkit.
yay	12.0.4	Yet another yogurt. Pacman wrapper and AUR helper written in go.
ycrawler	0.1	A web crawler that is useful for grabbing all user supplied input related to a given website and will save the output. It has proxy and log file support.
yersinia	0.8.2	A network tool designed to take advantage of some weakness in different network protocols.
yeti	2483.753adfbf	A platform meant to organize observables, indicators of compromise, TTPs, and knowledge on threats in a single, unified repository.
yinjector	0.1	A MySQL injection penetration tool. It has multiple features, proxy support, and multiple exploitation methods.
ysoserial	0.0.6	A proof-of-concept tool for generating payloads that exploit unsafe Java object deserialization.
zackattack	5.1f96c14	A new tool set to do NTLM Authentication relaying unlike any other tool currently out there.
zaproxy	2.11.1	Integrated penetration testing tool for finding vulnerabilities in web applications
zarp	0.1.8	A network attack tool centered around the exploitation of local networks.
zdns	249.bfbfae2	Fast CLI DNS Lookup Tool.
zeek	14921.2044cf661	Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.
zeek-aux	555.444a6fb	Handy auxiliary programs related to the use of the Zeek Network Security Monitor.
zelos	272.506554d	A comprehensive binary emulation and instrumentation platform.
zeratool	46.cb70d53	Automatic Exploit Generation (AEG) and remote flag capture for exploitable CTF problems.
zerowine	0.0.2	Malware Analysis Tool - research project to dynamically analyze the behavior of malware
zeus	111.97db152	AWS Auditing & Hardening Tool.
zeus-scanner	414.21b8756	Advanced dork searching utility.
zgrab	804.59a517f	Grab banners (optionally over TLS).
zgrab2	583.d5532ce	Go Application Layer Scanner.
zipdump	0.0.21	ZIP dump utility.
zipexec	19.f8d661f	A unique technique to execute binaries from a password protected zip.

zirikatu	7.afe1d9c	Fud Payload generator script.
zizzania	124.8f2062f	Automated DeAuth attack.
zmap	2.1.1	Fast network scanner designed for Internet-wide network surveys
zssh	1.5c	SSH and Telnet client with ZMODEM file transfer capability
zsteg	v0.2.13.r1.gc8d2508	Detect stegano-hidden data in PNG and BMP.
zulu	0.1	A light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks.
zulucrypt	6.2.0	Front end to cryptsetup and tcplay and it allows easy management of encrypted block devices.
zykeys	0.1	Demonstrates how default wireless settings are derived on some models of ZyXEL routers.
zzuf	0.15	Transparent application input fuzzer.