```
acccheck   +++   Password dictionary attack tool for SMB
ace-voip   +++   A simple VoIP corporate directory enumeration tool
aircrack-ng   +++   wireless WEP/WPA cracking utilities
amap   +++   next-generation scanning tool for pentesters
android-sdk   +++   Android software development kit
apache-users   +++   Enumerate usernames on systems with Apache UserDir module
arduino   +++   AVR development board IDE and built-in libraries
armitage   +++   Cyber attack management for Metasploit
asleap   +++   A tool for exploiting Cisco LEAP networks
augeas-lenses   +++   Set of lenses needed by libaugeas0 to parse config files
automater   +++   A IP and URL analysis tool.
bbqsql   +++   SQL Injection Exploitation Tool
bed   +++   A network protocol fuzzer
beef-xss   +++   Browser Exploitation Framework (BeEF)
binwalk   +++   tool for searching binary images for embedded files and executable
blindelephant   +++   A generic web application fingerprinter
bluelog   +++   Bluetooth scanner and logger
bluemaho   +++   GUI interface for testing Bluetooth devices
bluepot   +++   Bluetooth honeypot
blueranger   +++   Simple Bash script to locate Bluetooth devices
bluesnarfer   +++   A Bluesnarfing Utility
bluez-hcidump   +++   Analyses Bluetooth HCI packets
braa   +++   Mass SNMP scanner
bulk-extractor   +++   Extracts information without parsing filesystem
bully   +++   Bully is a new implementation of the WPS brute force
busybox   +++   Tiny utilities for small and embedded systems
cabextract   +++   Microsoft Cabinet file unpacker
casefile   +++   Offline intelligence tool
cdpsnarf   +++   Network sniffer to extract CDP information
cewl   +++   Custom wordlist generator
chntpw   +++   NT SAM password recovery utility
cisco-auditing-tool   +++   Scans Cisco routers for vulnerabilities
cisco-global-exploiter   +++   Simple and fast Cisco exploitation tool
cisco-ocs   +++   Mass Cisco scanner
cisco-torch   +++   Cisco device scanner
cmospwd   +++   decrypt BIOS passwords from CMOS
copy-router-config   +++   Copies Cisco configs via SNMP
cowpatty   +++   Brute-force WPA dictionary attack
creddump   +++   Extracts credentials from Windows registry hives
crunch   +++   Password wordlist generator
cryptcat   +++   A lightweight version netcat extended with twofish encryption
cutycapt   +++   utility to capture WebKit's rendering of a web page
cymothoa   +++   Stealth backdooring tool
davtest   +++   Testing tool for WebDAV servers
dbd   +++   Netcat clone with encryption
dbpwaudit   +++   Does online password audits of DB engines
dc3dd   +++   patched version of GNU dd with forensic features
ddrescue   +++   Copies data from one file or block device to another.
deblaze   +++   Performs testing against flash remoting endpoints
dex2jar   +++   Tools to work with android .dex and java .class files
dff   +++   Powerful, efficient and modular digital forensic framework
dhcpig   +++   DHCP exhaustion script
dirb   +++   URL bruteforcing tool
dirbuster   +++   Web server directory brute-forcer
dmitry   +++   Deepmagic Information Gathering Tool
dnmap   +++   Distributed nmap framework
dns2tcp   +++   TCP over DNS tunnel client and server
dnschef   +++   DNS proxy for penetration testers
dnsenum   +++   Tool to enumerate domain DNS information
dnsmap   +++   DNS domain name brute forcing tool
dnsrecon   +++   A powerful DNS enumeration script
dnstracer   +++   trace DNS queries to the source
dnswalk   +++   Checks dns zone information using nameserver lookups
dos2unix   +++   convert text file line endings between CRLF and LF
dotdotpwn   +++   DotDotPwn - The Directory Traversal Fuzzer.
dradis   +++   Collaboration tools for penetration testing
dumpzilla   +++   Mozilla browser forensic tool
eapmd5pass   +++   Tool for extracting and cracking EAP-MD5
edb-debugger   +++   Linux equivalent of OllyDbg
enum4linux   +++   Enumerates info from Windows and Samba systems
enumiax   +++   IAX protocol username enumerator
```

```
exploitdb   +++   Searchable Exploit Database archive
extundelete   +++   utility to recover deleted files from ext3/ext4 partition
fierce   +++   Domain DNS scanner
fiked   +++   Cisco VPN attack tool
fimap   +++   LFI and RFI exploitation tool
findmyhash   +++   Crack hashes with online services
foremost   +++   forensic program to recover lost files
fping   +++   sends ICMP ECHO_REQUEST packets to network hosts
fragroute   +++   Test a NIDS by attempting to evade using fragmented packets
fragrouter   +++   IDS evasion toolkit
funkload   +++   web testing tool
galleta   +++   An Internet Explorer cookie forensic analysis tool
giskismet   +++   Wireless recon visualization tool
golismero   +++   Web application mapper
goofile   +++   Command line filetype search
gpp-decrypt   +++   Group Policy Preferences decrypter
gr-scan   +++   Scans a range of frequencies and prints a list of
grabber   +++   Web application vulnerability scanner
greenbone-security-assistant   +++   The Greenbone Security Assistant
guymager   +++   Forensic imaging tool based on Qt
hackrf-tools   +++   transitional dummy package
hamster-sidejack   +++   Sidejacking tool
hash-identifier   +++   Tool to identify hash types
hexinject   +++   Versatile packet injector and sniffer
hexorbase   +++   Multiple database management and audit application
hping3   +++   Active Network Smashing Tool
i2c-tools   +++   heterogeneous set of I2C tools for Linux
iaxflood   +++   VoIP flooder tool
icedtea6-plugin   +++   web browser plugin to execute Java applets (dependency package)
intersect   +++   Post-exploitation framework
intrace   +++   Traceroute-like application piggybacking on existing TCP connections
inundator   +++   Multi-threaded IDS false positive generator
inviteflood   +++   SIP/SDP INVITE message flooding over UDP/IP
isr-evilgrade   +++   Evilgrade framework
jad   +++   Java decompiler
javasnoop   +++   Intercept Java applications locally
jboss-autopwn   +++   JBoss script for obtaining remote shell access
johnny   +++   GUI for John the Ripper
joomscan   +++   OWASP Joomla Vulnerability Scanner Project
jsql   +++   Java tool for automatic database injection
kalibrate-rtl   +++   Calculate local oscillator frequency offset using GSM base stations
keepnote   +++   cross-platform note-taking and organization application
keimpx   +++   Check for valid credentials across a network over SMB
killerbee   +++   Framwork for ZigBee exploitation
kismet   +++   wireless sniffer and monitor - core
lbd   +++   Load balancer detector
ldb-tools   +++   LDAP-like embedded database - tools
lynis   +++   security auditing tool for Unix based systems
magictree   +++   Penetration tester productivity tool
maltego-teeth   +++   Set of offensive Maltego transforms
maskprocessor   +++   High-performance word generator
mdk3   +++   Wireless attack tool for IEEE 802.11 networks
metagoofil   +++   Tool designed for extracting metadata of public documents
mfcuk   +++   MFCUK - MiFare Classic Universal toolKit
mfoc   +++   MIFARE Classic offline cracker
miranda   +++   UPNP administration tool
mitmproxy   +++   SSL-capable man-in-the-middle HTTP proxy
multiforcer   +++   GPU accelerated password cracking tool
ncrack   +++   High-speed network authentication cracking tool
netsed   +++   network packet-altering stream editor
netsniff-ng   +++   packet sniffing beast
nipper-ng   +++   Device security configuration review tool
nmap   +++   The Network Mapper
ohrwurm   +++   RTP fuzzer
openvas-administrator   +++   Administrator Module of OpenVAS
openvas-cli   +++   Command Line Tools for OpenVAS
openvas-manager   +++   Manager Module of OpenVAS
openvas-scanner   +++   remote network security auditor - scanner
os-prober   +++   utility to detect other OSes on a set of drives
oscanner   +++   Oracle assessment framework
p0f   +++   Passive OS fingerprinting tool
```

pack +++ Password analysis and cracking kit
padbuster +++ Script for performing Padding Oracle attacks
paros +++ Web application proxy
patator +++ Multi-purpose brute-forcer
pdf-parser +++ Parses PDF files to identify fundamental elements
pdfid +++ Scans PDF files for certain PDF keywords
pdgmail +++ Extracts gmail artifacts from a pd dump
peepdf +++ PDF analysis tool
phrasendrescher +++ Passphrase cracking tool
pipal +++ Statistical analysis on password dumps
pixiewps +++ An offline the WPS bruteforce tool.
plecost +++ Wordpress fingerprinting tool
polenum +++ Extracts the password policy from a Windows system
powerfuzzer +++ Highly automated and fully customizable web fuzzer
powersploit +++ PowerShell Post-Exploitation Framework
protos-sip +++ SIP test suite
proxystrike +++ Active web application proxy
ptunnel +++ Tunnel TCP connections over ICMP packets
pwnat +++ NAT to NAT client-server communication
rainbowcrack +++ Rainbow table password cracker
rcracki-mt +++ Version of rcrack that supports hybrid and indexed tables
reaver +++ brute force attack tool against Wifi Protected Setup PIN number
rebind +++ DNS rebinding tool
recon-ng +++ Web Reconnaissance framework written in Python
redfang +++ Locates non-discoverable bluetooth devices
responder +++ NBT-NS/LLMNR Responder
rsmangler +++ Wordlist mangling tool
rtpbreak +++ Detects, reconstructs, and analyzes RTP sessions
rtpflood +++ Tool to flood any RTP device
sakis3g +++ Tool for establishing 3G connections
sbd +++ Secure backdoor for linux and windows
sctpscan +++ SCTP network scanner for discovery and security
set +++ Social-Engineer Toolkit
sfuzz +++ Black Box testing utilities
sidguesser +++ Guesses sids against an Oracle database
siparmyknife +++ SIP fuzzing tool
sipp +++ Traffic generator for the SIP protocol
sipvicious +++ Tools for auditing SIP based VoIP systems
skipfish +++ fully automated, active web application security reconnaissance tool
smali +++ Assembler/disassembler for Android's dex format
sniffjoke +++ Transparent TCP connection scrambler
snmpcheck +++ SNMP service enumeration tool
spooftooph +++ Automates spoofing or cloning Bluetooth devices
sqlmap +++ automatic SQL injection tool
sqlninja +++ SQL server injection and takeover tool
sqlsus +++ MySQL injection tool
sslcaudit +++ Tests SSL/TLS clients susceptibility to MITM attacks
sslsplit +++ Transparent and scalable SSL/TLS interception
sslstrip +++ SSL/TLS man-in-the-middle attack tool
sslyze +++ Fast and full-featured SSL scanner
statsprocessor +++ High-performance word-generator
t50 +++ Multi-protocol packet injector tool
termineter +++ Smart meter testing framework
thc-ipv6 +++ IPv6 attack suite
thc-pptp-bruter +++ THC PPTP Brute Force
thc-ssl-dos +++ Stress tester for the SSL handshake
theharvester +++ theHarvester is a tool for gathering e-mail accounts and subdomain
tlssled +++ Evaluates the security of a target SSL/TLS (HTTPS) server
traceroute +++ Traces the route taken by packets over an IPv4/IPv6 network
truecrack +++ Bruteforce password cracker for TrueCrypt volumes.
twofi +++ Twitter words of interest
u3-pwn +++ Injects executables onto U3 USB devices
ua-tester +++ User agent string tester
udptunnel +++ tunnel UDP packets over a TCP connection
uniscan +++ LFI, RFI, and RCE vulnerability scanner
unix-privesc-check +++ Script to check for simple privilege escalation vectors
urlcrazy +++ Domain typo generator
vega +++ Platform to test the security of web applications
voiphopper +++ Runs a VLAN hop security test
volatility +++ advanced memory forensics framework
volatility-tools +++ generate profiles to Volatility Framework

w3af +++ framework to find and exploit web application vulnerabilities
webscarab +++ Web application review tool
webshag +++ Multi-threaded web server audit tool
webshells +++ Collection of webshells
webslayer +++ Web application bruteforcer
websploit +++ Web exploitation framework
weevely +++ Stealth tiny web shell
wfuzz +++ Web application bruteforcer
wicd +++ wired and wireless network manager - metapackage
wifitap +++ WiFi injection via a tun/tap device
wifite +++ Automated wireless auditor
winetricks +++ package manager for WINE to install software easily
winexe +++ Remote Windows-command executor
wireshark +++ network traffic analyzer - GTK+ version
wol-e +++ Wake on LAN Explorer
wordlists +++ Contains the rockyou wordlist
wpscan +++ Black box WordPress vulnerability scanner
xspy +++ X server sniffer
xsser +++ XSS testing framework
yersinia +++ Network vulnerabilities check software
zaproxy +++ Testing tool for finding vulnerabilities in web applications.
zenmap +++ The Network Mapper Front End