

Hacking & Penetesting Tools

Exploitation Tools

- Crackmapexec
- Metasploit Framework
- msf-payload creator
- searchsploit
- social engineering toolkit (root)
- sqlmap
- Empire

Sniffing & Spoofing

- Network Sniffers
 - dnschef
 - netsniff-ng
 - wireshark
- Spoofing & MITM
 - ettercap
 - dnschef
 - rebind
 - sslsplit
 - tcpreplay
- ettercap-graphical
- macchanger
- minicom
- mitmproxy
- netsniff-ng
- responder
- wireshark

Post Exploitation

- OS Backdoors
 - dbd
 - powersploit
 - sbd
- Tunneling & Exfiltration
 - dns2tcp
 - exe2hex
 - dns2tcpd
 - exe2hex
 - iodine
 - miredo
 - proxychains4
 - proxytunnel
 - ptunnel
 - pwnat
 - sslh
 - stunnel4
 - udptunnel
- Web Backdoors
 - laudanum
 - weeveily
- evil-winrm
- exe2hex
- mimikatz
- powershell empire
- powersploit
- proxychains4
- weeveily

Forensics

- Forensic Carving Tools
 - magisrescue
 - scalpel
 - scrounge-ntfs
- Forensic Imaging Tools
 - guymager (root)
- Sleuth Kit Suite
 - autopsy (root)
 - blkcalc
 - blkcat
 - blkls
 - blkstat
 - ffind
 - fsstat
 - fls
 - hfind
 - icat-sleuthkit
 - ifind
 - ils-sleuthkit
 - img_cat
 - istat
 - jls
 - jcat
 - mactime-sleuthkit
 - mmcat
 - mmis
 - mmstat
 - sigfind
 - sorter
 - srch_strings
 - tsk_comparedir
 - tsk_gettimes
 - tsk_recover
 - tsk_loaddb
- binwalk
- bulk_extractor
- hashdeep
- PDF Forensic Tools
 - pdfid
 - pdf-parser

Reporting Tools

- cutycapt
- faraday start
- pipal
- Subtopic
- recordmydesktop

Social Engineering Tools

- msf payload creator
- social engineering toolkit (root)

Information Gathering

- DNS Analysis
 - dnsenum
 - dnsrecon
 - fierce
- IDS/IPS Identification
 - lbd
 - wafw00f
- Live Host Identification
 - arping
 - fping
 - hping3
 - thcping6
 - masscan
- Network & Port Scanners
 - masscan
 - nmap
- OSINT Analysis
 - spiderfoot
 - spiderfoot-cli
 - thehravester
- Route Analysis
 - netdiscover
 - netmask
 - enum4linux
- SMB Analysis
 - smbmap
 - nbtscan
- SMTP Analysis
 - swaks
- SNMP Analysis
 - snmp-check
 - onesixtyone
- SSL Analysis
 - ssldump
 - ssllh
 - sslyze
 - ssllcan
- dmitry
- ike-scan
- legion (root)
- recon-ng

Vulnerability Analysis

- Fuzzing Tools
 - spike-generic_chunked
 - spike-generic_listen_tcp
 - spike-generic_send_tcp
 - spike-generic_send_udp
- VoIP Tools
 - voiphopper
- legion (root)
- nikto
- nmap
- unix-privesc-check
- Linpeas
- Winpeas

Web Application Analysis

- CMS & Framework Identification
 - wpscan
- Web Application Proxies
 - burpsuite
- Web Crawlers & Directory Bruteforce
 - cutycapt
 - dirb
 - ffuf
 - dirbuster
 - wfuzz
- Web Vulnerability Scanners
 - cadaver
 - davtest
 - nikto
 - skipfish
 - wapiti
 - whatweb
 - wpscan
- commix
- sqlmap

Database Assessment

- SQLite database browser
- sqlmap
- PowerUpSQL

Password Attacks

- Offline Attacks
 - chntpw
 - hashcat
 - hashid
 - hash-identifier
 - ophcarck-cli
 - samdmp2
 - John the Ripper
 - onesixtyone
- Online Attacks
 - hydra
 - patator
 - thc-pptp-bruter
 - Medusa
 - Ncrack
 - Crowbar
- Passing the Hash Tools
 - mimikatz
 - smbmap
 - pth-curl
 - pth-net
 - pth-winexe
 - pth-rpcclient
 - pth-smbclient
 - pth-smbget
 - pth-wmic
 - pth-wmis
 - pth-xfreerdp
- Password Profiling & Wordlists
 - crunch
 - cewl
 - rsmangler
 - wordlists
 - cUPP
 - Pydictor

Wireless Attacks

- 802.11 Wireless Tools
 - bully
 - Fluxion
 - Airgeddon
 - Fern
 - Wifite
 - Kismet
 - Reaver
- Bluetooth Tools
 - spooftooth

Reverse Engineering

- clang
- clang++
- NASM shell
- radare2

