All Applications (covered)

1) information Gathering
   - DNS analysis
     - dnsenum
     - dnsmap
     - dnsrecon
     - fierce
   - IDS/IPS Identification
     - lbd
     - wafw00f
   - Live Host Identification
     - arping
     - fping
     - hping3
     - masscan
     - netcat
     - thcping6
     - unicornscan
   - Network & Port Scanners
     - masscan
     - nmap
     - unicornscan
   - OSINT Analysis
     - maltego (installer)
     - spiderfoot
     - spiderfoot-cli
     - theharvester
   - Route Analysis

        - netdiscover
        - netmask
    - SMB Analysis
        - enum4linux
        - nbtscan
        - smbmap
    - SMTP Analysis
        - smtp-user-enum
        - swaks
    - SNMP Analysis
        - onesixtyone
        - snmp-check
    - SSL Analysis
        - ssldump
        - sslh
        - sslscan
        - sslyze

- amass
- dmitry
- ike-scan
- legion (Root)
- maltego (installer)
- netdiscover
- nmap
- recon-ng
- spiderfoot

2) Vulnerability Analysis
   - Fuzzing Tools
     - spike-generic_chunked
     - spike-generic_listen_tcp
     - spike-generic_send_tcp
     - spike-generic_send_udp
   - volP Tools
     - voiphopper

- legion (root)
- nikto
- nmap
- unix-privesc-check

3) Web Application Analysis
   - CMS & Framework Identification
     - wpscan
   - Web Application Proxies
     - burpsuite
   - Web Crawlers & Directory Brut…
     - cutycapt
     - dirb
     - dirbuster
     - ffuf
     - wfuzz
   - Web Vulnerability Scanners
     - cadaver
     - davtest
     - nikto
     - skipfish
     - wapiti
     - whatweb
     - wpscan

- burpsuite
- commix
- skipfish
- sqlmap
- webshells
- wpscan

4) Database Assessment
    - SQLite database browser
    - Sqlmap

5) Password Attacks
   - Offline Attacks
     - chntpw
     - hashcat
     - hashid
     - hash-identifier
     - john
     - ophcrack-cli
     - samdump2
   - Online Attacks
     - hydra
     - hydra-graphical
     - medusa
     - ncrack
     - onesixtyone
     - patator
     - thc-pptp-bruter
   - Passing the Hash Tools
     - Crackmapexec
     - evil-winrm
     - impacket
     - mimikatz
     - pth-curl
     - pth-net
     - pth-rpcclient
     - pth-smbclient
     - pth-smbget

        - pth-sqsh
        - pth-winexe
        - pth-wmic
        - pth-wmis
        - pth-xfreerdp
        - smbmap
- Password Profiling & Wordlists
        - cewl
        - crunch
        - rsmangler
        - worlists

- cewl
- crunch
- hashcat
- hydra
- john
- medusa
- ncrack
- ophcrack
- wordlists

6) Wireless Attacks
   - 802.11 wireless Tools
     - bully
     - fern wifi cracker (root)
   - Bluetooth Toola
     - spooftooph

   - aircrack-ng
   - fern wifi cracker (root)
   - kismet
   - pixiewps
   - reaver
   - wifite

7) Reverse Engineering
   - clang
   - clang++
   - NASM shell
   - radare2

8) Exploitation Tools
   - crackmapexec
   - metasploit framework
   - msf payload creator
   - searchsploit
   - social engineering toolkit (root)
   - sqimap

9) Sniffing & Spoofing
   - Network Sniffers
     - dnschef
     - netsniffi-ng
   - Spoofing & MITH
     - dnschef
     - rebind
     - sslsplit
     - tcpreplay

- ettercap-graphical
- macchanger
- minicom
- mitmproxy
- netsniff-ng
- responder
- scapy
- tcpdump
- wireshark

10) Post Exploitation

- OS backdoors
    - dbd
    - powersploit
    - sbd
- Tunneling & Exfiltration
    - dbd
    - dns2tcpc
    - dns2tcpd
    - exe2hex
    - iodine
    - miredo
    - proxychains4
    - proxytunnel
    - ptunnel
    - pwnat
    - sslh
    - stunnel4
    - udptunnel
- Web Backdoors
    - laudanum
    - weevely

- evil-winrm
- exe2hex
- impacket
- mimikatz
- netcat
- powershell empire
- powersploit

- proxychains4
- starkiller
- weevely

11) Forensics

- Forensic Carving Tools
- Forensic Imaging Tools
- PDF Forensics Tools
- Sleuth Kit Suite
- autopsy (root)
- binwalk
- bulk_extractor
- hashdeep

12) Reporting Tools

- cherryTree
- cutycapt
- faraday start
- maltego (installer)
- pipal
- recordmydesktop

13) Social Engineering Tools

- Maltego (installer)
- msf payload creator
- social engineering toolkit (root)

Kali & Offsec Links

- Exploit Database
- Kali Bugs
- Kali Docs
- Kali Forums
- Kali Linux
- Kali Tools
- NetHunter
- OffSec Training
- VulnHu