Pentesting Use Cases

Reconnaissance: Whois, Nslookup/Dig, theHarvester, Shodan, Recon-NG, Censys, Aircrack-NG, Kismet, WiFite2, Wireshark, Hping, SET, nmap, Metasploit framework, Maltego, WiGLE, Fierce

Enumeration: Nslookup/Dig, Wireshark, Hping, nmap, DirBuster, FOCA, GoBuster, Burp Suite, mitm6, CloudBrute, Cloud Custodian, Metagoofil, WitnessMe, nmap-boostrap-xsl

Vulnerability scanning: Nikto, OpenVAS, SQLmap, Nessus, W3AF, OWASP ZAP, nmap, Metasploit framework, Wapiti, WPScan, Brakeman, Pacu, SearchSploit, Sharp Collection, Bloodhound

Credential Attacks

- Offline Password Cracking: Hashcat, HateCrack, John the Ripper, Cain, Mimikatz, Aircrack-NG, CeWL, PCredz
- Brute-Forcing Services: SQLmap (for database accounts), Medusa, Hydra, Cain, Mimikatz, Patator, W3AF, Aircrack-NG, EAPHammer, mdk4, Spooftoof, Reaver, CrackMapExec, Fern, Trufflehog, Responder, Rubeus, lsassy

Persistence: SET, BeEF, SSH, NCAT, NETCAT, Drozer, Powersploit, Empire, Metasploit framework, Covenant, Pacu, Sharp Collection

Configuration Compliance: Nikto, OpenVAS, SQLmap, Nessus, nmap, Scout Suite, Impacket Tools, Online SSL checkers

Evasion: Proxychains, SET, Metasploit framework, Openstego, Steghide, Snow, Coagula, Sonic Visualiser, TinEye, Sharp Collection

Decompilation: Immunity debugger, APKX, APK studio

Forensics: Immunity debugger

Debugging: OLLYDBG, Immunity debugger, GDB, WinDBG, IDA

Software Assurance: Findbugs/Findsecbugs, SonarQube, YASCA, Peach, AFL, SAST, DAST

Pentesting Tools

OSINT

- **WHOIS - For querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an AS**
  https://whois.icann.org/en

- **Nslookup / Dig - For querying the DNS to obtain the mapping between domain name and IP address, or other DNS records**

- **Fingerprinting Organization with Collected Archives (FOCA) – Find metadata and hidden information in documents**
  https://www.elevenpaths.com/labstools/foca/

- **theHarvester - OSINT gathering to determine a company's external threat landscape on the internet (gathers emails, names, subdomains, IPs and URLs)**
  https://github.com/laramies/theHarvester

- **Shodan – Search engine for internet connected devices**
  https://www.shodan.io/

- **Maltego - OSINT and graphical link analysis tool for gathering and connecting information for investigative tasks for security professionals, forensic investigators, investigative journalists, and researchers**
  https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

- **Recon-ng - Framework for open source web-based reconnaissance**
  https://github.com/lanmaster53/recon-ng

- **Censys - Finding, monitoring, and understanding a target's internet-facing assets**
  https://censys.io/

- **Metagoofil – Google search to identify and download documents from a target website**
  https://www.kali.org/tools/metagoofil/

Scanners

- **Nikto – Web Server Scanner**
  https://github.com/sullo/nikto

- **Open Vulnerability Assessment Scanner (OpenVAS) – Full-feature Vulnerability Scanner**
  http://www.openvas.org/

- **SQLmap – Automated SQL Injection**
  https://github.com/sqlmapproject/sqlmap

- **Nessus – Professional Vulnerability Scanner (proprietary branch-off from OpenVAS)**
  https://www.tenable.com/products/nessus/nessus-professional

- **Open Security Content Automation Protocol (SCAP) - format by which security content is communicated with the industry**
  https://csrc.nist.gov/projects/security-content-automation-protocol

- **Wapiti – Web Application Vulnerability Scanner**
  https://wapiti-scanner.github.io/

- **WPScan – Word Press Security Scanner**
  https://wpscan.com/wordpress-security-scanner

- **Brakeman – Ruby on Rails Vulnerability Scanner**
  https://brakemanscanner.org/

- **Nmap – Network discovery and security auditing**
  https://nmap.org/

- **nmap-boostrap-xsl – Interface for checking results of nmap scans**
  https://github.com/honze-net/nmap-bootstrap-xsl

- **Fierce – DNS reconnaissance/zone transfer tool**
  https://github.com/mschwager/fierce

- **Bloodhound – analysis of AD rights and exploitable relations**
  https://github.com/GhostPack/Rubeus

Cloud Tools/Scanners

- **Scout Suite - Security posture assessment of cloud environments**
  https://github.com/nccgroup/ScoutSuite

- **CloudBrute – finds infrastructure, files, and apps on the top cloud providers (Amazon, Google, Microsoft, DigitalOcean, Alibaba, Vultr, Linode)**
  https://github.com/0xsha/CloudBrute

- **Pacu – AWS Exploitation Framework**
  https://rhinosecuritylabs.com/aws/pacu-open-source-aws-exploitation-framework/

- **Cloud Custodian – AWS Cloud Security, Governance, and Management**
  https://cloudcustodian.io/

Credential Testing Tools

- **Hashcat – Advanced Password Recovery**
  https://hashcat.net/hashcat/

- **Hatecrack – Automating cracking methodologies through Hashcat**
  https://github.com/trustedsec/hate_crack

- **Medusa – Login Brute Forcer**
  http://foofus.net/goons/jmk/medusa/medusa.html

- **Hydra - Brute force crack a remote authentication service**
  http://sectools.org/tool/hydra/

- **CeWL - Returns a list of words which can then be used for password crackers**
  https://digi.ninja/projects/cewl.php

- **John the Ripper - Password security auditing and password recovery tool**
  http://www.openwall.com/john/

- **Cain – Windows password recovery tool**
  http://www.oxid.it/cain.html
  https://github.com/xchwarze/Cain

- **Mimikatz - Extract plaintext passwords, hash, PIN code and kerberos tickets, perform pass-the-hash, pass-the-ticket or build Golden tickets**
  https://github.com/gentilkiwi/mimikatz

- **Patator – Multi-purpose brute forcer**
  https://github.com/lanjelot/patator
  https://www.kali.org/tools/patator/

- **DirBuster - Brute force directories and file names on web/application servers**
  https://www.kali.org/tools/dirbuster/

- **w3af – Web Application Attack and Audit Framework**
  http://w3af.org/

- **Rubeus - C# toolset for raw Kerberos interaction and abuses**
  https://github.com/GhostPack/Rubeus

- **lsassy - Python tool to remotely extract credentials on a set of host**
  https://github.com/Hackndo/lsassy

Wireless

- **Aircrack-ng suite – Tools to assess WiFi network security**
  https://www.aircrack-ng.org/

- **Kismet - Wireless network and device detector, sniffer, wardriving tool, and WIDS (wireless intrusion detection) framework**
  https://www.kismetwireless.net/

- **WiFite2 – WAP password recovery tool**
  https://github.com/derv82/wifite2

- **Rogue access point – AP installed on a network without the network owner's permission**

- **EAPHammer - Toolkit for performing targeted evil twin attacks against WPA2-Enterprise networks**
  https://github.com/s0lst1c3/eaphammer

- **mdk4 - tool to exploit common IEEE 802.11 protocol weaknesses**
  https://github.com/aircrack-ng/mdk4

- **Spooftooph - automate spoofing or cloning Bluetooth device Name, Class, and Address**
  https://www.kali.org/tools/spooftooph/

- **Reaver - Brute force attack against WiFi Protected Setup to get WPA PSK**
  https://www.kali.org/tools/reaver/

- **Wireless Geographic Logging Engine (WiGLE) – All Networks. Found by everyone**
  https://www.wigle.net/

- **Fern – WiFi cracker**
  https://www.kali.org/tools/fern-wifi-cracker/

Networking Tools

- **Wireshark – Network protocol analyzer**
  https://www.wireshark.org/

- **Hping – CLI oriented TCP/IP packet assembler/analyzer**
  http://www.hping.org/

- **PCredz - 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, etc from a pcap file or from a live interface**
  https://github.com/lgandx/PCredz

- **WitnessMe – Skim targets for web interfaces on popular ports**
  https://github.com/byt3bl33d3r/WitnessMe

Mobile Tools

- **Drozer – Deprecated rouge application simulator**
  https://github.com/mwrlabs/drozer

- **APKX – Android APK Decompilation**
  https://github.com/b-mueller/apkx

- **APK studio – Reverse engineering Android application packages**
  http://vaibhavpandey.com/apkstudio/

Web Application Tools

- **OWASP ZAP – Web App scanner and proxy**
  https://www.zaproxy.org/

- **Burp Suite – Vulnerability finder and intercepting proxy**
  https://portswigger.net/burp

- **Gobuster – Enumerate hidden directories and files by brute-force attack**
  https://www.kali.org/tools/gobuster/

Social Engineering Tools

- **Social Engineering Toolkit (SET) – Testing framework for social engineering**
  https://github.com/trustedsec/social-engineer-toolkit

- **BeEF – Web browser testing tool**
  https://github.com/beefproject/beef

Remote Access Tools

- **Secure Shell (SSH)**

- **Netcat – Reads and writes data across TCP or UDP connections**
  https://sectools.org/tool/netcat/

- **Ncat – CLI tool, written by nmap team to update/replace Netcat**
  https://nmap.org/ncat/

- **ProxyChains - Hooks network-related libc functions in dynamically linked programs via a preloaded DLL and redirects connections through SOCKS4a/5 or HTTP proxies**
  https://github.com/haad/proxychains

Software Assurance

- **Findbugs/findsecbugs – Security audits of Java web applications**
  https://find-sec-bugs.github.io/

- **Peach – Fuzzing framework**
  https://gitlab.com/gitlab-org/security-products/protocol-fuzzer-ce

- **AFL (American Fuzzy Lop) – Software brute-force fuzzer**
  http://lcamtuf.coredump.cx/afl/

- **SonarQube – Static code analysis**
  https://www.sonarqube.org/

- **YASCA (Yet Another Source Code Analyzer) – Deprecated**
  https://github.com/scovetta/yasca

- **SAST (Static Application Security Testing) – Examine code to find software flaws, white box**

- **DAST (Dynamic Application Security Testing) – Find vulnerabilities in a running application, black box**

Debuggers

- **OllyDbg – Windows assembler level analyzing debugger**
  http://www.ollydbg.de/

- **Immunity Debugger - Write exploits, analyze malware, and reverse engineer binary files**
  https://www.immunityinc.com/products/debugger/

- **GNU Debugger (GDB) – Source level debugging package**
  https://www.gnu.org/software/gdb/

- **WinDbg - Debug kernel-mode and user-mode code, analyze crash dumps, and examine the CPU registers while the code executes**
  https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debugger-download-tools

- **Interactive Disassembler (IDA) – Disassembler and debugger**
  https://www.hex-rays.com/products/ida/debugger/index.shtml

- **Covenant - .NET C2 framework that highlights the attack surface of .NET**
  https://github.com/cobbr/Covenant/blob/master/README.md

Steganography Tools

- **Openstego – Data hiding and Watermarking**
  https://www.openstego.com/

- **Steghide – hide data in image and audio files**
  http://steghide.sourceforge.net/

- **Snow – Text-based steganography that uses whitespace to hide information**
  https://github.com/mattkwan-zz/snow

- **Coagula – Turns images into sound**
  https://www.abc.se/~re/Coagula/Coagula.html

- **Sonic Visualiser – Viewing and analyzing music audio files**
  https://www.sonicvisualiser.org/

- **TinEye – Image recognition and reverse image search product**
  https://tineye.com/

Misc.

- **SearchSploit – CLI search tool for Exploit-DB**
  https://www.exploit-db.com/searchsploit/

- **Responder – LLMNR, NBT-NS and MDNS poisoner**
  https://github.com/SpiderLabs/Responder

- **Impacket tools – Python3 classes for crafting/decoding network packets**
  https://github.com/CoreSecurity/impacket
  https://www.kali.org/tools/impacket/

- **Empire - PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent for post-exploitation modules**
  https://github.com/EmpireProject/Empire

- **Metasploit Framework – Penetration testing framework**
  https://www.metasploit.com/

- **Sharp Collection - common C# offensive tools, fresh from their respective master branches built and released in a CDI fashion using Azure DevOps release pipelines**
  https://github.com/Flangvik/SharpCollection

- **mitm6 - Exploits the default configuration of Windows to take over the default DNS server**
  https://github.com/dirkjanm/mitm6

- **CrackMapExec – Pentesting Windows/Active Directory environments**
  https://www.kali.org/tools/crackmapexec/

- **TruffleHog - Searches through git repositories for secrets, digging deep into commit history and branches**
  https://github.com/trufflesecurity/truffleHog

- **Powersploit – Penetration testing PowerShell modules**
  https://github.com/PowerShellMafia/PowerSploit

- **Online SSL checkers – diagnose problems with an SSL certificate**