PENTESTING TOOL	DESCRIPTION	OPEN / PAID / BOTH
Reconnaissance:		
WHOIS	public records about domain	open
Nslookup	identify IP addresses associated with organization	open
theHarvester	email harvesting from domains and search engines	open
Recon-ng	OSINT framework	open
Censys	probes IP addresses using search engine	paid
FOCA	metadata from office docs, PDF and other files	both
Shodan	Vulnerable IoT devices that are public facing	both
Maltego	OSINT visualization	both
Vulnerability Scanners:		
Nessus	vulnerability scanning tool	paid
OpenVAS	vulnerability scanning tool	open
Sqlmap	SQL injections	open
Nikto	web application testing	open
Wapiti	web application testing	open
W3AF	web application testing	open
SCAP	compliance tool	
Social Engineering:		
SET	spear phishing, fake websites, collecting credentials	open
BeEF	web browser attacks/takeovers	open
Credential Testing/Password Cracking:		
Hashcat	cracking hashed passwords	open
John the Ripper	cracking hashed passwords	open
Hydra	password brute forcing	open
Medusa	password brute forcing	open
Patator	cracking passwords	open
Cain	cracking hashed passwords	open
CeWL	wordlist generator for dictionary attacks	open
Mimikatz/kiwi	retrives credentials from Windows memory	open
DirBuster	web server directory brute forcing	open
Debuggers:		
Immunity Debugger	reverse engineering of malware	
GDB	debugger for Linux	open
OllyDbg	Windows debugger	
WinDbg	Windows debugger	
IDA	Windows, Mac, Linux debugger	paid
Brakeman	static software analysis	
Covenant	used for .NET applications	
TruffleHog	scan code repositories for accidentally published secrets	
Network Testing:		
Wireshark	eavesdrop on wired or wireless traffic	both
Hping	manipulate traffic/packets	open
Aircrack-ng	wireless attacks	open
WiFite	wireless attacks	open
mdk4	wireless attacks	open
Fern	wireless attacks	open
Kismet	wireless attacks	open
Rogue AP (hardware)	used to lure victims to join so traffic can be visible (Man-in-middle)	paid
EAPHammer	evil twin attacks vs WPA2-Enterprise networks	
Reaver	attacks WPS (Wi-Fi Protected Setup)	
Spooftooph	attacks bluetooth devices	
WiGLE	database of wireless network information	
Online SSL checkers	website TLS/SSL vulnerabilities	
Remote Access:		
SSH	encrypted connection	open
Ncat/Netcat	bind and reverse shells	open
Proxychains	proxy servers	open
RDP/Anydesk/Teamviewer/No Machine	if the port is listening you can attempt connections to these	open
Telnet	unencrypted connection (will show user/password in clear text if traffic is sniffed)	open

Exploitation:		
Metasploit	exploit console	open
Searchsploit	seaches exploit database	open
Powersploit	windows powershell scripts	
Empire	windows powershell scripts	
Responder	netBIOS attacks	
Impacket	low-level access network protocols	
Mitm6	attacks IPv6 networks	
CrackMapExec	attacks Acrive Directory	
Steganography:		
Open Steg	hide text within images	
Steghide	hide text within images	
Coagula	hide text within audio	
Snow	hide info within whitespace of documents	
tinEye	reverse image engineering	
Metagoofil	extract metadata	
Cloud Tools:		
ScoutSuite	general purpose auditing tool	
CloudBrute	scanner to identify cloud components	
Pacu	attacks AWS hosts	
Cloud Custodian	engine that allows consistent application of security policies	