

# Periodic Table of Offensive Security

v1.1.2

															1 <b>PT</b> PTES									
2 <b>Sh</b> Shodan															3 <b>Sli</b> sliver	4 <b>Sb</b> Seatbelt	5 <b>Au</b> Autorunsc	6 <b>REx</b> RemoteExec	7 <b>Py</b> pspy	8 <b>Ak</b> AccessChk	9 <b>Rt</b> ROADtools	10 <b>Ma</b> MITRE ATT&CK	11 <b>RTo</b> Red Team Ops	12 <b>MM</b> OSSTMM
13 <b>Wi</b> WHOIS	14 <b>Dg</b> dig				15 <b>MS</b> Metasploit	16 <b>Sq</b> SQLmap	17 <b>XS</b> XSSStrike	18 <b>BS</b> Burp Suite	19 <b>Ne</b> NetExec	20 <b>Mi</b> Mimikatz	21 <b>Pe</b> PEASS-ng	22 <b>Ke</b> KeeThief	23 <b>BL</b> BloodHound	24 <b>EM</b> Empire	25 <b>PS</b> PowerSploit	26 <b>SC</b> SharpCradle	27 <b>OW</b> OWASP Top 10	28 <b>IF</b> ISSAF						
29 <b>Ff</b> FOFA	30 <b>Wy</b> WaybckMachine	31 <b>NM</b> Nmap	32 <b>Nu</b> Nuclei	33 <b>ff</b> ffuf	34 <b>Gb</b> Gobuster	35 <b>Hx</b> HTTPX	36 <b>Re</b> Responder	37 <b>SCg</b> ShellCodeGen	38 <b>Ex<sup>2</sup></b> evilginx2	39 <b>Ve</b> Veil	40 <b>UC</b> unicorn	41 <b>Su</b> Supernova	42 <b>Ru</b> Rubeus	43 <b>Co</b> Covenant	44 <b>Cd</b> creddump	45 <b>Ri</b> Risk Assessment	46 <b>Re</b> Reporting Stndrs							
47 <b>Hu</b> hunter.io	48 <b>Vt</b> VirusTotal	49 <b>Us</b> URLScan	50 <b>Dx</b> DNSX	51 <b>Am</b> Amass	52 <b>Su</b> Sublist3r	53 <b>Mc</b> Masscan	54 <b>Pw</b> pwntools	55 <b>Ro</b> ropper	56 <b>Be</b> BeEF	57 <b>Tx</b> toxssin	58 <b>Hv</b> Havoc	59 <b>sd</b> srum-dump	60 <b>Fi</b> fileless-xec	61 <b>Ke</b> kerbrute	62 <b>Lz</b> LaZagne	63 <b>TM</b> Threat Modeling	64 <b>VA</b> Vuln Assessment							
65 <b>Ma</b> Maltego	66 <b>Fo</b> FOCA	67 <b>ng</b> recon-ng	68 <b>Zp</b> ZAP	69 <b>Dum</b> dnsenum	70 <b>na</b> Naabu	71 <b>Ar</b> arp-scan	72 <b>ZM</b> ZMap	73 <b>Iv</b> Invicti	74 <b>Ni</b> nishang	75 <b>SL</b> SecLists	76 <b>Hy</b> Hydra	77 <b>Rev</b> revshells.com	78 <b>Li</b> ligolo-ng	79 <b>Ce</b> Certipy	80 <b>dS</b> dnsteal	81 <b>SDLi</b> SecDevLifecycle	82 <b>Ca</b> CREST							
83 <b>TH</b> theHarvester	84 <b>Cn</b> Cencys	85 <b>Wpp</b> Wappalyzer	86 <b>mt</b> Metagoofil	87 <b>rs</b> reconspider	88 <b>Ru</b> RustScan	89 <b>nk</b> Nikto	90 <b>Ss</b> sslscan	91 <b>Ne</b> Nessus	92 <b>ix</b> commix	93 <b>pP</b> PetitPotam	94 <b>Def</b> dnschef	95 <b>Im</b> impacket	96 <b>Ps</b> PsExec	97 <b>WMI</b> wmiexec	98 <b>Cs</b> CobaltStrike	99 <b>AR</b> Audit Ready	100 <b>Ti</b> TIBER-EU							
101 <b>Ct</b> crt.sh	102 <b>Ho</b> Holehe	103 <b>SH</b> Sherlock	104 <b>Sf</b> spiderfoot	105 <b>Ww</b> WhatWeb	106 <b>Sw</b> SnmpWalk	107 <b>E4x</b> enum4linux	108 <b>fx</b> dalfox	109 <b>GD</b> GitDorker	110 <b>Ew</b> Evil-WinRM	111 <b>X-er</b> xsser	112 <b>UAC</b> UACME	113 <b>JW</b> jwt_tool	114 <b>RC</b> RunasCs	115 <b>CDk</b> CDK	116 <b>Vi</b> Villain	117 <b>Ki</b> Cyber Kill Chain	118 <b>CAf</b> CAF NCSC UK							

Reconnaissance

Enumeration &  
Fuzzing

Exploitation

Post-  
Exploitation

Frameworks &  
Standards



Need a print-quality file?  
SCAN here for GitHub repo!

Created by ILIAS MAVROPOULOS  
[linkedin.com/in/imavropoulos](https://www.linkedin.com/in/imavropoulos)

