**Red-Team-Operation-Tools**

**Powershell Scripts**

* <https://github.com/S3cur3Th1sSh1t/WinPwn>
* <https://github.com/dafthack/MailSniper>
* <https://github.com/putterpanda/mimikittenz>
* <https://github.com/dafthack/DomainPasswordSpray>
* <https://github.com/mdavis332/DomainPasswordSpray>
* <https://github.com/jnqpblc/SharpSpray>
* <https://github.com/Arvanaghi/SessionGopher>
* <https://github.com/samratashok/nishang>
* <https://github.com/PowerShellMafia/PowerSploit>
* <https://github.com/fdiskyou/PowerOPS>
* <https://github.com/giMini/PowerMemory>
* <https://github.com/Kevin-Robertson/Inveigh>
* <https://github.com/MichaelGrafnetter/DSInternals>
* <https://github.com/PowerShellEmpire/PowerTools>
* <https://github.com/FuzzySecurity/PowerShell-Suite>
* <https://github.com/hlldz/Invoke-Phant0m>
* <https://github.com/leoloobeek/LAPSToolkit>
* <https://github.com/n00py/LAPSDumper>
* <https://github.com/sense-of-security/ADRecon>
* <https://github.com/adrecon/ADRecon>
* <https://github.com/S3cur3Th1sSh1t/Grouper>
* <https://github.com/l0ss/Grouper2>
* <https://github.com/NetSPI/PowerShell>
* <https://github.com/NetSPI/PowerUpSQL>
* <https://github.com/GhostPack>
* <https://github.com/Kevin-Robertson/Powermad>

**AMSI Bypass**

* <https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell>
* <https://github.com/Flangvik/AMSI.fail>
* <https://github.com/p3nt4/PowerShdll>
* <https://github.com/jaredhaight/PSAttack>
* <https://github.com/Cn33liz/p0wnedShell>
* <https://github.com/cobbr/InsecurePowerShell>
* <https://github.com/bitsadmin/nopowershell>
* <https://github.com/Mr-Un1k0d3r/PowerLessShell>
* <https://github.com/OmerYa/Invisi-Shell>
* <https://github.com/Hackplayers/Salsa-tools>
* <https://github.com/padovah4ck/PSByPassCLM>
* <https://github.com/rasta-mouse/AmsiScanBufferBypass>
* <https://github.com/itm4n/VBA-RunPE>
* <https://github.com/cfalta/PowerShellArmoury>
* <https://github.com/Mr-B0b/SpaceRunner>
* <https://github.com/RythmStick/AMSITrigger>
* <https://github.com/rmdavy/AMSI_Ordinal_Bypass>
* <https://github.com/mgeeky/Stracciatella>
* <https://github.com/med0x2e/NoAmci>
* <https://github.com/rvrsh3ll/NoMSBuild>
* <https://github.com/bohops/UltimateWDACBypassList>
* <https://github.com/jxy-s/herpaderping>
* <https://github.com/Cn33liz/MSBuildShell>

**Payload Hosting**

* <https://github.com/kgretzky/pwndrop>
* <https://github.com/sc0tfree/updog>

**Network Share Scanner**

* <https://github.com/SnaffCon/Snaffler>
* <https://github.com/djhohnstein/SharpShares>
* <https://github.com/vivami/SauronEye>
* <https://github.com/leftp/VmdkReader>

**Reverse Shellz**

* <https://github.com/xct/xc>
* <https://github.com/cytopia/pwncat>
* <https://github.com/Kudaes/LOLBITS>

**Backdoor Finder**

* <https://github.com/linuz/Sticky-Keys-Slayer>
* <https://github.com/ztgrace/sticky_keys_hunter>
* <https://github.com/countercept/doublepulsar-detection-script>

**Pivoting**

* <https://github.com/0x36/VPNPivot>
* <https://github.com/securesocketfunneling/ssf>
* <https://github.com/p3nt4/Invoke-SocksProxy>
* <https://github.com/sensepost/reGeorg>
* <https://github.com/hayasec/reGeorg-Weblogic>
* <https://github.com/nccgroup/ABPTTS>
* <https://github.com/RedTeamOperations/PivotSuite>
* <https://github.com/trustedsec/egressbuster>
* <https://github.com/vincentcox/bypass-firewalls-by-DNS-history>
* <https://github.com/shantanu561993/SharpChisel>
* <https://github.com/jpillora/chisel>
* <https://github.com/esrrhs/pingtunnel>
* <https://github.com/sysdream/ligolo>
* <https://github.com/nccgroup/SocksOverRDP>
* <https://github.com/blackarrowsec/mssqlproxy>

**Persistence on Windows**

* <https://github.com/fireeye/SharPersist>
* <https://github.com/outflanknl/SharpHide>
* <https://github.com/HarmJ0y/DAMP>

**Framework Discovery**

* <https://github.com/Tuhinshubhra/CMSeeK>
* <https://github.com/Dionach/CMSmap> - Wordpress, Joomla, Drupal Scanner
* <https://github.com/wpscanteam/wpscan>
* <https://github.com/Ekultek/WhatWaf>
* <https://github.com/KingOfBugbounty/KingOfBugBountyTips>

**Framework Scanner / Exploitation**

* <https://github.com/wpscanteam/wpscan> - wordpress
* <https://github.com/n00py/WPForce>
* <https://github.com/m4ll0k/WPSeku> <https://github.com/swisskyrepo/Wordpresscan>
* <https://github.com/rastating/wordpress-exploit-framework>
* <https://github.com/coldfusion39/domi-owned> - lotus domino
* <https://github.com/droope/droopescan> - Drupal
* <https://github.com/whoot/Typo-Enumerator> - Typo3
* <https://github.com/rezasp/joomscan> - Joomla

**File / Directory / Parameter discovery**

* <https://github.com/OJ/gobuster>
* <https://github.com/nccgroup/dirble>
* <https://github.com/maK-/parameth>
* <https://github.com/devanshbatham/ParamSpider> - Mining parameters from dark corners of Web Archives
* <https://github.com/s0md3v/Arjun> - 💗
* <https://github.com/Cillian-Collins/dirscraper> - Directory lookup from Javascript files
* <https://github.com/hannob/snallygaster>
* <https://github.com/maurosoria/dirsearch>
* <https://github.com/s0md3v/Breacher> - Admin Panel Finder
* <https://github.com/mazen160/server-status_PWN>
* <https://github.com/helviojunior/turbosearch>

**Rest API Audit**

* <https://github.com/microsoft/restler-fuzzer> - RESTler is the first stateful REST API fuzzing tool for automatically testing cloud services through their REST APIs and finding security and reliability bugs in these services.
* <https://github.com/flipkart-incubator/Astra>

**Windows Privilege Escalation / Audit**

* <https://github.com/itm4n/PrivescCheck> - Privilege Escalation Enumeration Script for Windows
* <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS> - powerfull Privilege Escalation Check Script with nice output
* <https://github.com/AlessandroZ/BeRoot>
* <https://github.com/rasta-mouse/Sherlock>
* <https://github.com/hfiref0x/UACME> - UAC
* <https://github.com/rootm0s/WinPwnage> - UAC
* <https://github.com/abatchy17/WindowsExploits>
* <https://github.com/dafthack/HostRecon>
* <https://github.com/sensepost/rattler> - find vulnerable dlls for preloading attack
* <https://github.com/WindowsExploits/Exploits>
* <https://github.com/Cybereason/siofra> - dll hijack scanner
* <https://github.com/0xbadjuju/Tokenvator> - admin to system
* <https://github.com/MojtabaTajik/Robber>
* <https://github.com/411Hall/JAWS>
* <https://github.com/GhostPack/SharpUp>
* <https://github.com/GhostPack/Seatbelt>
* <https://github.com/A-mIn3/WINspect>
* <https://github.com/hausec/ADAPE-Script>
* <https://github.com/SecWiki/windows-kernel-exploits>
* <https://github.com/bitsadmin/wesng>
* <https://github.com/rasta-mouse/Watson>

**LinkedIn**

* <https://www.linkedin.com/in/joas-antonio-dos-santos>

**Windows Privilege Abuse (Privilege Escalation)**

* <https://github.com/gtworek/Priv2Admin> - Abuse Windows Privileges
* <https://github.com/itm4n/UsoDllLoader> - load malicious dlls from system32
* <https://github.com/TsukiCTF/Lovely-Potato> - Exploit potatoes with automation
* <https://github.com/antonioCoco/RogueWinRM> - from Service Account to System
* <https://github.com/antonioCoco/RoguePotato> - Another Windows Local Privilege Escalation from Service Account to System
* <https://github.com/itm4n/PrintSpoofer> - Abusing Impersonation Privileges on Windows 10 and Server 2019
* <https://github.com/BeichenDream/BadPotato> - itm4ns Printspoofer in C#
* <https://github.com/itm4n/FullPowers> - Recover the default privilege set of a LOCAL/NETWORK SERVICE account

**Exfiltration**

* <https://github.com/gentilkiwi/mimikatz>
* <https://github.com/GhostPack/SafetyKatz>
* <https://github.com/Flangvik/BetterSafetyKatz> - Fork of SafetyKatz that dynamically fetches the latest pre-compiled release of Mimikatz directly from gentilkiwi GitHub repo, runtime patches signatures and uses SharpSploit DInvoke to PE-Load into memory.
* <https://github.com/GhostPack/Rubeus>
* <https://github.com/Arvanaghi/SessionGopher>
* <https://github.com/peewpw/Invoke-WCMDump>
* <https://github.com/tiagorlampert/sAINT>
* <https://github.com/AlessandroZ/LaZagneForensic> - remote lazagne
* <https://github.com/eladshamir/Internal-Monologue>
* <https://github.com/djhohnstein/SharpWeb> - Browser Creds gathering
* <https://github.com/moonD4rk/HackBrowserData> - hack-browser-data is an open-source tool that could help you decrypt data[passwords|bookmarks|cookies|history] from the browser.
* <https://github.com/mwrlabs/SharpClipHistory> - ClipHistory feature get the last 25 copy paste actions
* <https://github.com/outflanknl/Dumpert> - dump lsass using direct system calls and API unhooking
* <https://github.com/b4rtik/SharpMiniDump> - Create a minidump of the LSASS process from memory - using Dumpert
* <https://github.com/b4rtik/ATPMiniDump> - Evade WinDefender ATP credential-theft
* <https://github.com/aas-n/spraykatz> - remote procdump.exe, copy dump file to local system and pypykatz for analysis/extraction
* <https://github.com/0x09AL/RdpThief> - extract live rdp logins
* <https://github.com/chrismaddalena/SharpCloud> - Simple C# for checking for the existence of credential files related to AWS, Microsoft Azure, and Google Compute.
* <https://github.com/djhohnstein/SharpChromium> - .NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins.
* <https://github.com/jfmaes/SharpHandler> - This project reuses open handles to lsass to parse or minidump lsass
* <https://github.com/V1V1/SharpScribbles> - ThunderFox for Firefox Credentials, SitkyNotesExtract for "Notes as passwords"
* <https://github.com/securesean/DecryptAutoLogon> - Command line tool to extract/decrypt the password that was stored in the LSA by SysInternals AutoLogon
* <https://github.com/G0ldenGunSec/SharpSecDump> - .Net port of the remote SAM + LSA Secrets dumping functionality of impacket's secretsdump.py
* <https://github.com/EncodeGroup/Gopher> - C# tool to discover low hanging fruits like SessionGopher
* <https://github.com/GhostPack/SharpDPAPI> - DPAPI Creds via C#
* LSASS Dump Without Mimikatz
* <https://github.com/Hackndo/lsassy>
* <https://github.com/aas-n/spraykatz>
* <https://github.com/b4rtik/SharpKatz> - C# porting of mimikatz sekurlsa::logonpasswords, sekurlsa::ekeys and lsadump::dcsync commands
* Credential harvesting Linux Specific
* <https://github.com/huntergregal/mimipenguin>
* <https://github.com/n1nj4sec/mimipy>
* <https://github.com/dirtycow/dirtycow.github.io>
* <https://github.com/mthbernardes/sshLooterC> - SSH Credential loot
* <https://github.com/blendin/3snake> - SSH / Sudo / SU Credential loot
* <https://github.com/0xmitsurugi/gimmecredz>
* <https://github.com/TarlogicSecurity/tickey> - Tool to extract Kerberos tickets from Linux kernel keys.
* Data Exfiltration - DNS/ICMP/Wifi Exfiltration
* <https://github.com/FortyNorthSecurity/Egress-Assess>
* <https://github.com/p3nt4/Invoke-TmpDavFS>
* <https://github.com/DhavalKapil/icmptunnel>
* <https://github.com/iagox86/dnscat2>
* <https://github.com/Arno0x/DNSExfiltrator>
* <https://github.com/spieglt/FlyingCarpet> - Wifi Exfiltration
* <https://github.com/SECFORCE/Tunna> - Tunna is a set of tools which will wrap and tunnel any TCP communication over HTTP
* <https://github.com/sysdream/chashell>
* <https://github.com/no0be/DNSlivery> - Easy files and payloads delivery over DNS

**Staging**

* Rapid Attack Infrastructure (RAI) Red Team Infrastructure... Quick... Fast... Simplified One of the most tedious phases of a Red Team Operation is usually the infrastructure setup. This usually entails a teamserver or controller, domains, redirectors, and a Phishing server. <https://github.com/obscuritylabs/RAI>
* Red Baron is a set of modules and custom/third-party providers for Terraform which tries to automate creating resilient, disposable, secure and agile infrastructure for Red Teams. <https://github.com/byt3bl33d3r/Red-Baron>
* EvilURL generate unicode evil domains for IDN Homograph Attack and detect them. <https://github.com/UndeadSec/EvilURL>
* Domain Hunter checks expired domains, bluecoat categorization, and Archive.org history to determine good candidates for phishing and C2 domain names. <https://github.com/threatexpress/domainhunter>
* PowerDNS is a simple proof of concept to demonstrate the execution of PowerShell script using DNS only. <https://github.com/mdsecactivebreach/PowerDNS>
* Chameleon a tool for evading Proxy categorisation. <https://github.com/mdsecactivebreach/Chameleon>
* CatMyFish Search for categorized domain that can be used during red teaming engagement. Perfect to setup whitelisted domain for your Cobalt Strike beacon C&C. <https://github.com/Mr-Un1k0d3r/CatMyFish>
* Malleable C2 is a domain specific language to redefine indicators in Beacon's communication. <https://github.com/rsmudge/Malleable-C2-Profiles>
* Malleable-C2-Randomizer This script randomizes Cobalt Strike Malleable C2 profiles through the use of a metalanguage, hopefully reducing the chances of flagging signature-based detection controls. <https://github.com/bluscreenofjeff/Malleable-C2-Randomizer>
* FindFrontableDomains search for potential frontable domains. <https://github.com/rvrsh3ll/FindFrontableDomains>
* Postfix-Server-Setup Setting up a phishing server is a very long and tedious process. It can take hours to setup, and can be compromised in minutes. <https://github.com/n0pe-sled/Postfix-Server-Setup>
* DomainFrontingLists a list of Domain Frontable Domains by CDN. <https://github.com/vysec/DomainFrontingLists>
* Apache2-Mod-Rewrite-Setup Quickly Implement Mod-Rewrite in your infastructure. <https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup>
* mod\_rewrite rule to evade vendor sandboxes. <https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10>
* external\_c2 framework a python framework for usage with Cobalt Strike's External C2. <https://github.com/Und3rf10w/external_c2_framework>
* Malleable-C2-Profiles A collection of profiles used in different projects using Cobalt Strike <https://www.cobaltstrike.com/>. <https://github.com/xx0hcd/Malleable-C2-Profiles>
* ExternalC2 a library for integrating communication channels with the Cobalt Strike External C2 server. <https://github.com/ryhanson/ExternalC2>
* cs2modrewrite a tools for convert Cobalt Strike profiles to modrewrite scripts. <https://github.com/threatexpress/cs2modrewrite>
* e2modrewrite a tools for convert Empire profiles to Apache modrewrite scripts. <https://github.com/infosecn1nja/e2modrewrite>
* redi automated script for setting up CobaltStrike redirectors (nginx reverse proxy, letsencrypt). <https://github.com/taherio/redi>
* cat-sites Library of sites for categorization. <https://github.com/audrummer15/cat-sites>
* ycsm is a quick script installation for resilient redirector using nginx reverse proxy and letsencrypt compatible with some popular Post-Ex Tools (Cobalt Strike, Empire, Metasploit, PoshC2). <https://github.com/infosecn1nja/ycsm>
* Domain Fronting Google App Engine. <https://github.com/redteam-cyberark/Google-Domain-fronting>
* DomainFrontDiscover Scripts and results for finding domain frontable CloudFront domains. <https://github.com/peewpw/DomainFrontDiscover>
* Automated Empire Infrastructure <https://github.com/bneg/RedTeam-Automation>
* Serving Random Payloads with NGINX. <https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9>
* meek is a blocking-resistant pluggable transport for Tor. It encodes a data stream as a sequence of HTTPS requests and responses. <https://github.com/arlolra/meek>
* CobaltStrike-ToolKit Some useful scripts for CobaltStrike. <https://github.com/killswitch-GUI/CobaltStrike-ToolKit>
* mkhtaccess\_red Auto-generate an HTaccess for payload delivery -- automatically pulls ips/nets/etc from known sandbox companies/sources that have been seen before, and redirects them to a benign payload. <https://github.com/violentlydave/mkhtaccess_red>
* RedFile a flask wsgi application that serves files with intelligence, good for serving conditional RedTeam payloads. <https://github.com/outflanknl/RedFile>
* keyserver Easily serve HTTP and DNS keys for proper payload protection. <https://github.com/leoloobeek/keyserver>
* DoHC2 allows the ExternalC2 library from Ryan Hanson (<https://github.com/ryhanson/ExternalC2>) to be leveraged for command and control (C2) via DNS over HTTPS (DoH). This is built for the popular Adversary Simulation and Red Team Operations Software Cobalt Strike ([https://www.cobaltstrike.com](https://www.cobaltstrike.com/)). <https://github.com/SpiderLabs/DoHC2>
* HTran is a connection bouncer, a kind of proxy server. A “listener” program is hacked stealthily onto an unsuspecting host anywhere on the Internet. <https://github.com/HiwinCN/HTran>

**Buffer Overflow and Exploit Development**

* <https://github.com/CyberSecurityUP/Buffer-Overflow-Labs>
* <https://github.com/gh0x0st/Buffer_Overflow>
* <https://github.com/freddiebarrsmith/Buffer-Overflow-Exploit-Development-Practice>
* <https://github.com/21y4d/Windows_BufferOverflowx32>
* <https://github.com/johnjhacking/Buffer-Overflow-Guide>
* <https://github.com/npapernot/buffer-overflow-attack>
* <https://github.com/V1n1v131r4/OSCP-Buffer-Overflow>
* <https://github.com/KINGSABRI/BufferOverflow-Kit>
* <https://github.com/FabioBaroni/awesome-exploit-development>
* <https://github.com/Gallopsled/pwntools>
* <https://github.com/hardenedlinux/linux-exploit-development-tutorial>
* <https://github.com/Billy-Ellis/Exploit-Challenges>
* <https://github.com/wtsxDev/Exploit-Development>

**MindMaps by Joas**

* <https://www.mindmeister.com/pt/1746180947/web-attacks-bug-bounty-and-appsec-by-joas-antonio>
* <https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio>
* <https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest>
* <https://www.mindmeister.com/pt/1760781948/information-security-certifications-by-joas-antonio>
* <https://www.mindmeister.com/pt/1746187693/cyber-security-career-knowledge-by-joas-antonio>

**Lateral Movement**

* <https://github.com/0xthirteen/SharpRDP>
* <https://github.com/0xthirteen/MoveKit>
* <https://github.com/0xthirteen/SharpMove>
* <https://github.com/rvrsh3ll/SharpCOM>
* <https://github.com/malcomvetter/CSExec>
* <https://github.com/byt3bl33d3r/CrackMapExec>
* <https://github.com/cube0x0/SharpMapExec>
* <https://github.com/nccgroup/WMIcmd>
* <https://github.com/rasta-mouse/MiscTools>
* <https://github.com/byt3bl33d3r/DeathStar>
* <https://github.com/SpiderLabs/portia>
* <https://github.com/Screetsec/Vegile>
* <https://github.com/DanMcInerney/icebreaker>
* <https://github.com/MooseDojo/apt2>
* <https://github.com/hdm/nextnet>
* <https://github.com/mubix/IOXIDResolver>
* <https://github.com/Hackplayers/evil-winrm>
* <https://github.com/bohops/WSMan-WinRM>
* <https://github.com/dirkjanm/krbrelayx>
* <https://github.com/Mr-Un1k0d3r/SCShell>
* <https://github.com/rvazarkar/GMSAPasswordReader>
* <https://github.com/fdiskyou/hunter>
* <https://github.com/360-Linton-Lab/WMIHACKER>
* <https://github.com/leechristensen/SpoolSample>
* <https://github.com/leftp/SpoolSamplerNET>
* <https://github.com/lexfo/rpc2socks>
* <https://github.com/checkymander/sshiva>
* <https://github.com/dev-2null/ADCollector>

**POST Exploitation**

* <https://github.com/mubix/post-exploitation>
* <https://github.com/emilyanncr/Windows-Post-Exploitation>
* <https://github.com/nettitude/Invoke-PowerThIEf>
* <https://github.com/ThunderGunExpress/BADministration>
* <https://github.com/bohops/SharpRDPHijack>
* <https://github.com/antonioCoco/RunasCs>
* <https://github.com/klsecservices/Invoke-Vnc>
* <https://github.com/mandatoryprogrammer/CursedChrome>
* <https://github.com/djhohnstein/WireTap>
* <https://github.com/GhostPack/Lockless>
* <https://github.com/infosecn1nja/SharpDoor>
* Phishing Tools
* <https://github.com/hlldz/pickl3>
* <https://github.com/shantanu561993/SharpLoginPrompt>
* <https://github.com/Dviros/CredsLeaker>
* <https://github.com/bitsadmin/fakelogonscreen>
* <https://github.com/CCob/PinSwipe>

**Wrapper for various tools**

* <https://github.com/bohops/GhostBuild>
* <https://github.com/S3cur3Th1sSh1t/PowerSharpPack>
* <https://github.com/rvrsh3ll/Rubeus-Rundll32>
* <https://github.com/checkymander/Zolom>

**Active Directory Audit and exploit tools**

* <https://github.com/mwrlabs/SharpGPOAbuse>
* <https://github.com/BloodHoundAD/BloodHound>
* <https://github.com/BloodHoundAD/SharpHound3>
* <https://github.com/chryzsh/awesome-bloodhound>
* <https://github.com/hausec/Bloodhound-Custom-Queries>
* <https://github.com/CompassSecurity/BloodHoundQueries>
* <https://github.com/vletoux/pingcastle>
* <https://github.com/cyberark/ACLight>
* <https://github.com/canix1/ADACLScanner>
* <https://github.com/fox-it/Invoke-ACLPwn>
* <https://github.com/NinjaStyle82/rbcd_permissions>
* <https://github.com/NotMedic/NetNTLMtoSilverTicket>
* <https://github.com/dirkjanm/ldapdomaindump>

**Web Vulnerability Scanner / Burp Plugins**

* <https://github.com/m4ll0k/WAScan> - all in one scanner
* <https://github.com/s0md3v/XSStrike> - XSS discovery
* <https://github.com/federicodotta/Java-Deserialization-Scanner>
* <https://github.com/d3vilbug/HackBar>
* <https://github.com/gyoisamurai/GyoiThon>
* <https://github.com/snoopysecurity/awesome-burp-extensions>
* <https://github.com/sting8k/BurpSuite_403Bypasser> - Burpsuite Extension to bypass 403 restricted directory
* <https://github.com/BishopFox/GadgetProbe>

**Web Exploitation Tools**

* <https://github.com/OsandaMalith/LFiFreak> - lfi
* <https://github.com/enjoiz/XXEinjector> - xxe
* <https://github.com/tennc/webshell> - shellz
* <https://github.com/flozz/p0wny-shell>
* <https://github.com/epinna/tplmap> - ssti
* <https://github.com/orf/xcat> - xpath injection
* <https://github.com/almandin/fuxploider> - File Uploads
* <https://github.com/nccgroup/freddy> - deserialization
* <https://github.com/irsdl/IIS-ShortName-Scanner> - IIS Short Filename Vuln. exploitation
* <https://github.com/frohoff/ysoserial> - Deserialize Java Exploitation
* <https://github.com/pwntester/ysoserial.net> - Deserialize .NET Exploitation
* <https://github.com/internetwache/GitTools> - Exploit .git Folder Existence
* <https://github.com/cujanovic/SSRF-Testing> - SSRF Tutorials
* <https://github.com/ambionics/phpggc> - PHP Unserialize Payload generator
* <https://github.com/BuffaloWill/oxml_xxe> - Malicious Office XXE payload generator
* <https://github.com/tijme/angularjs-csti-scanner> - Angularjs Csti Scanner
* <https://github.com/0xacb/viewgen> - Deserialize .NET Viewstates
* <https://github.com/Illuminopi/RCEvil.NET> - Deserialize .NET Viewstates

**Linux Privilege Escalation / Audit**

* <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS> - powerfull Privilege Escalation Check Script with nice output
* <https://github.com/mzet-/linux-exploit-suggester>
* <https://github.com/rebootuser/LinEnum>
* <https://github.com/diego-treitos/linux-smart-enumeration>
* <https://github.com/CISOfy/lynis>
* <https://github.com/AlessandroZ/BeRoot>
* <https://github.com/future-architect/vuls>
* <https://github.com/ngalongc/AutoLocalPrivilegeEscalation>
* <https://github.com/b3rito/yodo>
* <https://github.com/belane/linux-soft-exploit-suggester> - lookup vulnerable installed software
* <https://github.com/sevagas/swap_digger>
* <https://github.com/NullArray/RootHelper>
* <https://github.com/NullArray/MIDA-Multitool>
* <https://github.com/initstring/dirty_sock>
* <https://github.com/jondonas/linux-exploit-suggester-2>
* <https://github.com/sosdave/KeyTabExtract>
* <https://github.com/DominicBreuker/pspy>
* <https://github.com/itsKindred/modDetective>
* <https://github.com/nongiach/sudo_inject>
* <https://github.com/Anon-Exploiter/SUID3NUM> - find suid bins and look them up under gtfobins / exploitable or not
* <https://github.com/nccgroup/GTFOBLookup> - Offline GTFOBins
* <https://github.com/TH3xACE/SUDO_KILLER> - sudo misconfiguration exploitation
* <https://raw.githubusercontent.com/sleventyeleven/linuxprivchecker/master/linuxprivchecker.py>
* <https://github.com/inquisb/unix-privesc-check>
* <https://github.com/hc0d3r/tas> - easily manipulate the tty and create fake binaries
* <https://github.com/SecWiki/linux-kernel-exploits>
* <https://github.com/initstring/uptux>
* <https://github.com/andrew-d/static-binaries> - not really privesc but helpfull

**Command and Control**

* Cobalt Strike is software for Adversary Simulations and Red Team Operations. <https://cobaltstrike.com/>
* Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. <https://github.com/EmpireProject/Empire>
* Metasploit Framework is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. <https://github.com/rapid7/metasploit-framework>
* SILENTTRINITY A post-exploitation agent powered by Python, IronPython, C#/.NET. <https://github.com/byt3bl33d3r/SILENTTRINITY>
* Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python. <https://github.com/n1nj4sec/pupy>
* Koadic or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. <https://github.com/zerosum0x0/koadic>
* PoshC2 is a proxy aware C2 framework written completely in PowerShell to aid penetration testers with red teaming, post-exploitation and lateral movement. <https://github.com/nettitude/PoshC2_Python>
* Gcat a stealthy Python based backdoor that uses Gmail as a command and control server. <https://github.com/byt3bl33d3r/gcat>
* TrevorC2 is a legitimate website (browsable) that tunnels client/server communications for covert command execution. <https://github.com/trustedsec/trevorc2>
* Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang. <https://github.com/Ne0nd0g/merlin>
* Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you. <https://github.com/quasar/QuasarRAT>
* Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers. <https://github.com/cobbr/Covenant>
* FactionC2 is a C2 framework which use websockets based API that allows for interacting with agents and transports. <https://github.com/FactionC2/>
* DNScat2 is a tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol. <https://github.com/iagox86/dnscat2>
* Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. <https://github.com/BishopFox/sliver>
* EvilOSX An evil RAT (Remote Administration Tool) for macOS / OS X. <https://github.com/Marten4n6/EvilOSX>
* EggShell is a post exploitation surveillance tool written in Python. It gives you a command line session with extra functionality between you and a target machine. <https://github.com/neoneggplant/EggShell>

**Adversary Emulation**

* MITRE CALDERA - An automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks. <https://github.com/mitre/caldera>
* APTSimulator - A Windows Batch script that uses a set of tools and output files to make a system look as if it was compromised. <https://github.com/NextronSystems/APTSimulator>
* Atomic Red Team - Small and highly portable detection tests mapped to the Mitre ATT&CK Framework. <https://github.com/redcanaryco/atomic-red-team>
* Network Flight Simulator - flightsim is a lightweight utility used to generate malicious network traffic and help security teams to evaluate security controls and network visibility. <https://github.com/alphasoc/flightsim>
* Metta - A security preparedness tool to do adversarial simulation. <https://github.com/uber-common/metta>
* Red Team Automation (RTA) - RTA provides a framework of scripts designed to allow blue teams to test their detection capabilities against malicious tradecraft, modeled after MITRE ATT&CK. <https://github.com/endgameinc/RTA>

**Repositores**

* <https://github.com/infosecn1nja/Red-Teaming-Toolkit>
* <https://github.com/S3cur3Th1sSh1t/Pentest-Tools>
* <https://github.com/yeyintminthuhtut/Awesome-Red-Teaming>
* <https://github.com/enaqx/awesome-pentest>
* <https://github.com/Muhammd/Awesome-Pentest>
* <https://github.com/CyberSecurityUP/Awesome-PenTest-Practice>
* <https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU>
* <https://github.com/0x4D31/awesome-oscp>
* <https://github.com/six2dez/OSCP-Human-Guide>
* <https://github.com/RustyShackleford221/OSCP-Prep>
* <https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md>

**Malware Analysis and Reverse Engineering**

* <https://github.com/rshipp/awesome-malware-analysis>
* <https://github.com/topics/malware-analysis>
* <https://github.com/Apress/malware-analysis-detection-engineering>
* <https://github.com/SpiderLabs/malware-analysis>
* <https://github.com/ytisf/theZoo>
* <https://github.com/arxlan786/Malware-Analysis>
* <https://github.com/nheijmans/malzoo>
* <https://github.com/mikesiko/PracticalMalwareAnalysis-Labs>
* <https://github.com/secrary/SSMA>
* <https://github.com/merces/aleph>
* <https://github.com/mentebinaria/retoolkit>
* <https://github.com/mytechnotalent/Reverse-Engineering>
* <https://github.com/wtsxDev/reverse-engineering>
* <https://github.com/mentebinaria/retoolkit>
* <https://github.com/topics/reverse-engineering>
* <https://github.com/0xZ0F/Z0FCourse_ReverseEngineering>
* <https://github.com/NationalSecurityAgency/ghidra>
* <https://github.com/hax0rtahm1d/Reverse-Engineering>
* <https://github.com/tylerha97/awesome-reversing>