# Red Teaming/Adversary Simulation Toolkit

A collection of open source and commercial tools that aid in red team operations. This repository will help you during red team engagement.

## Contents

## Reconnaissance

### Active Intelligence Gathering

- **EyeWitness** is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. https://github.com/ChrisTruncer/EyeWitness (https://github.com/ChrisTruncer/EyeWitness)
- **AWSBucketDump** is a tool to quickly enumerate AWS S3 buckets to look for loot. https://github.com/jordanpotti/AWSBucketDump (https://github.com/jordanpotti/AWSBucketDump)
- **AQUATONE** is a set of tools for performing reconnaissance on domain names. https://github.com/michenriksen/aquatone (https://github.com/michenriksen/aquatone)
- **spoofcheck** a program that checks if a domain can be spoofed from. The program checks SPF and DMARC records for weak configurations that allow spoofing. https://github.com/BishopFox/spoofcheck (https://github.com/BishopFox/spoofcheck)
- **Nmap** is used to discover hosts and services on a computer network, thus building a "map" of the network. https://github.com/nmap/nmap (https://github.com/nmap/nmap)
- **dnsrecon** a tool DNS Enumeration Script. https://github.com/darkoperator/dnsrecon (https://github.com/darkoperator/dnsrecon)

### Passive Intelligence Gathering

- **Social Mapper** OSINT Social Media Mapping Tool, takes a list of names & images (or LinkedIn company name) and performs automated target searching on a huge scale across multiple social media sites. Not restricted by APIs as it instruments a browser using Selenium. Outputs reports to aid in correlating targets across sites. https://github.com/SpiderLabs/social_mapper (https://github.com/SpiderLabs/social_mapper)
- **skiptracer** OSINT scraping framework, utilizes some basic python webscraping (BeautifulSoup) of PII paywall sites to compile passive information on a target on a ramen noodle budget. https://github.com/xillwillx/skiptracer (https://github.com/xillwillx/skiptracer)
- **ScrapedIn** a tool to scrape LinkedIn without API restrictions for data reconnaissance. https://github.com/dchrastil/ScrapedIn (https://github.com/dchrastil/ScrapedIn)
- **linkScrape** A LinkedIn user/company enumeration tool. https://github.com/NickSanzotta/linkScrape (https://github.com/NickSanzotta/linkScrape)
- **FOCA** (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans. https://github.com/ElevenPaths/FOCA (https://github.com/ElevenPaths/FOCA)
- **theHarvester** is a tool for gathering subdomain names, e-mail addresses, virtual hosts, open ports/ banners, and employee names from different public sources. https://github.com/laramies/theHarvester (https://github.com/laramies/theHarvester)
- **Metagoofil** is a tool for extracting metadata of public documents (pdf,doc,xls,ppt,etc) availables in the target websites. https://github.com/laramies/metagoofil (https://github.com/laramies/metagoofil)
- **SimplyEmail** Email recon made fast and easy, with a framework to build on. https://github.com/killswitch-GUI/SimplyEmail (https://github.com/killswitch-GUI/SimplyEmail)
- **truffleHog** searches through git repositories for secrets, digging deep into commit history and branches. https://github.com/dxa4481/truffleHog (https://github.com/dxa4481/truffleHog)
- **Just-Metadata** is a tool that gathers and analyzes metadata about IP addresses. It attempts to find relationships between systems within a large dataset. https://github.com/ChrisTruncer/Just-Metadata (https://github.com/ChrisTruncer/Just-Metadata)
- **typofinder** a finder of domain typos showing country of IP address. https://github.com/nccgroup/typofinder (https://github.com/nccgroup/typofinder)
- **pwnedOrNot** is a python script which checks if the email account has been compromised in a data breach, if the email account is compromised it proceeds to find passwords for the compromised account. https://github.com/thewhiteh4t/pwnedOrNot (https://github.com/thewhiteh4t/pwnedOrNot)
- **GitHarvester** This tool is used for harvesting information from GitHub like google dork. https://github.com/metac0rtex/GitHarvester (https://github.com/metac0rtex/GitHarvester)
- **pwndb** is a python command-line tool for searching leaked credentials using the Onion service with the same name. https://github.com/davidtavarez/pwndb/ (https://github.com/davidtavarez/pwndb/)

# Frameworks

- **Maltego** is a unique platform developed to deliver a clear threat picture to the environment that an organization owns and operates. https://www.paterva.com/web7/downloads.php (https://www.paterva.com/web7/downloads.php)
- **SpiderFoot** the open source footprinting and intelligence-gathering tool. https://github.com/smicallef/spiderfoot (https://github.com/smicallef/spiderfoot)

- **datasploit** is an OSINT Framework to perform various recon techniques on Companies, People, Phone Number, Bitcoin Addresses, etc., aggregate all the raw data, and give data in multiple formats. https://github.com/DataSploit/datasploit (https://github.com/DataSploit/datasploit)
- **Recon-ng** is a full-featured Web Reconnaissance framework written in Python. https://bitbucket.org/LaNMaSteR53/recon-ng (https://bitbucket.org/LaNMaSteR53/recon-ng)

# Weaponization

- **Composite Moniker** Proof of Concept exploit for CVE-2017-8570. https://github.com/rxwx/CVE-2017-8570 (https://github.com/rxwx/CVE-2017-8570)
- **Exploit toolkit CVE-2017-8759** is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft .NET Framework RCE. https://github.com/bhdresh/CVE-2017-8759 (https://github.com/bhdresh/CVE-2017-8759)
- **CVE-2017-11882 Exploit** accepts over 17k bytes long command/code in maximum. https://github.com/unamer/CVE-2017-11882 (https://github.com/unamer/CVE-2017-11882)
- **Adobe Flash Exploit** CVE-2018-4878. https://github.com/anbai-inc/CVE-2018-4878 (https://github.com/anbai-inc/CVE-2018-4878)
- **Exploit toolkit CVE-2017-0199** is a handy python script which provides pentesters and security researchers a quick and effective way to test Microsoft Office RCE. https://github.com/bhdresh/CVE-2017-0199 (https://github.com/bhdresh/CVE-2017-0199)
- **demiguise** is a HTA encryption tool for RedTeams. https://github.com/nccgroup/demiguise (https://github.com/nccgroup/demiguise)
- **Office-DDE-Payloads** collection of scripts and templates to generate Office documents embedded with the DDE, macro-less command execution technique. https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads (https://github.com/0xdeadbeefJERKY/Office-DDE-Payloads)
- **CACTUSTORCH** Payload Generation for Adversary Simulations. https://github.com/mdsecactivebreach/CACTUSTORCH (https://github.com/mdsecactivebreach/CACTUSTORCH)
- **SharpShooter** is a payload creation framework for the retrieval and execution of arbitrary CSharp source code. https://github.com/mdsecactivebreach/SharpShooter (https://github.com/mdsecactivebreach/SharpShooter)
- **Don't kill my cat** is a tool that generates obfuscated shellcode that is stored inside of polyglot images. The image is 100% valid and also 100% valid shellcode. https://github.com/Mr-Un1k0d3r/DKMC (https://github.com/Mr-Un1k0d3r/DKMC)
- **Malicious Macro Generator Utility** Simple utility design to generate obfuscated macro that also include a AV / Sandboxes escape mechanism. https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator (https://github.com/Mr-Un1k0d3r/MaliciousMacroGenerator)
- **SCT Obfuscator** Cobalt Strike SCT payload obfuscator. https://github.com/Mr-Un1k0d3r/SCT-obfuscator (https://github.com/Mr-Un1k0d3r/SCT-obfuscator)
- **Invoke-Obfuscation** PowerShell Obfuscator. https://github.com/danielbohannon/Invoke-Obfuscation (https://github.com/danielbohannon/Invoke-Obfuscation)
- **Invoke-CradleCrafter** PowerShell remote download cradle generator and obfuscator. https://github.com/danielbohannon/Invoke-CradleCrafter (https://github.com/danielbohannon/Invoke-CradleCrafter)

- **Invoke-DOSfuscation** cmd.exe Command Obfuscation Generator & Detection Test Harness. https://github.com/danielbohannon/Invoke-DOSfuscation (https://github.com/danielbohannon/Invoke-DOSfuscation)
- **morphHTA** Morphing Cobalt Strike's evil.HTA. https://github.com/vysec/morphHTA (https://github.com/vysec/morphHTA)
- **Unicorn** is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. https://github.com/trustedsec/unicorn (https://github.com/trustedsec/unicorn)
- **Shellter** is a dynamic shellcode injection tool, and the first truly dynamic PE infector ever created. https://www.shellterproject.com/ (https://www.shellterproject.com/)
- **EmbedInHTML** Embed and hide any file in an HTML file. https://github.com/Arno0x/EmbedInHTML (https://github.com/Arno0x/EmbedInHTML)
- **SigThief** Stealing Signatures and Making One Invalid Signature at a Time. https://github.com/secretsquirrel/SigThief (https://github.com/secretsquirrel/SigThief)
- **Veil** is a tool designed to generate metasploit payloads that bypass common anti-virus solutions. https://github.com/Veil-Framework/Veil (https://github.com/Veil-Framework/Veil)
- **CheckPlease** Sandbox evasion modules written in PowerShell, Python, Go, Ruby, C, C#, Perl, and Rust. https://github.com/Arvanaghi/CheckPlease (https://github.com/Arvanaghi/CheckPlease)
- **Invoke-PSImage** is a tool to embeded a PowerShell script in the pixels of a PNG file and generates a oneliner to execute. https://github.com/peewpw/Invoke-PSImage (https://github.com/peewpw/Invoke-PSImage)
- **LuckyStrike** a PowerShell based utility for the creation of malicious Office macro documents. To be used for pentesting or educational purposes only. https://github.com/curi0usJack/luckystrike (https://github.com/curi0usJack/luckystrike)
- **ClickOnceGenerator** Quick Malicious ClickOnceGenerator for Red Team. The default application a simple WebBrowser widget that point to a website of your choice. https://github.com/Mr-Un1k0d3r/ClickOnceGenerator (https://github.com/Mr-Un1k0d3r/ClickOnceGenerator)
- **macro_pack** is a tool by @EmericNasi used to automatize obfuscation and generation of MS Office documents, VB scripts, and other formats for pentest, demo, and social engineering assessments. https://github.com/sevagas/macro_pack (https://github.com/sevagas/macro_pack)
- **StarFighters** a JavaScript and VBScript Based Empire Launcher. https://github.com/Cn33liz/StarFighters (https://github.com/Cn33liz/StarFighters)
- **nps_payload** this script will generate payloads for basic intrusion detection avoidance. It utilizes publicly demonstrated techniques from several different sources. https://github.com/trustedsec/nps_payload (https://github.com/trustedsec/nps_payload)
- **SocialEngineeringPayloads** a collection of social engineering tricks and payloads being used for credential theft and spear phishing attacks. https://github.com/bhdresh/SocialEngineeringPayloads (https://github.com/bhdresh/SocialEngineeringPayloads)
- **The Social-Engineer Toolkit** is an open-source penetration testing framework designed for social engineering. https://github.com/trustedsec/social-engineer-toolkit (https://github.com/trustedsec/social-engineer-toolkit)
- **Phishery** is a Simple SSL Enabled HTTP server with the primary purpose of phishing credentials via Basic Authentication. https://github.com/ryhanson/phishery (https://github.com/ryhanson/phishery)
- **PowerShdll** run PowerShell with rundll32. Bypass software restrictions. https://github.com/p3nt4/PowerShdll (https://github.com/p3nt4/PowerShdll)
- **Ultimate AppLocker ByPass List** The goal of this repository is to document the most common techniques to bypass AppLocker. https://github.com/api0cradle/UltimateAppLockerByPassList

(https://github.com/api0cradle/UltimateAppLockerByPassList)

- **Ruler** is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol. https://github.com/sensepost/ruler (https://github.com/sensepost/ruler)
- **Generate-Macro** is a standalone PowerShell script that will generate a malicious Microsoft Office document with a specified payload and persistence method. https://github.com/enigma0x3/Generate-Macro (https://github.com/enigma0x3/Generate-Macro)
- **Malicious Macro MSBuild Generator** Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass. https://github.com/infosecn1nja/MaliciousMacroMSBuild (https://github.com/infosecn1nja/MaliciousMacroMSBuild)
- **Meta Twin** is designed as a file resource cloner. Metadata, including digital signature, is extracted from one file and injected into another. https://github.com/threatexpress/metatwin (https://github.com/threatexpress/metatwin)
- **WePWNise** generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software. https://github.com/mwrlabs/wePWNise (https://github.com/mwrlabs/wePWNise)
- **DotNetToJScript** a tool to create a JScript file which loads a .NET v2 assembly from memory. https://github.com/tyranid/DotNetToJScript (https://github.com/tyranid/DotNetToJScript)
- **PSAmsi** is a tool for auditing and defeating AMSI signatures. https://github.com/cobbr/PSAmsi (https://github.com/cobbr/PSAmsi)
- **Reflective DLL injection** is a library injection technique in which the concept of reflective programming is employed to perform the loading of a library from memory into a host process. https://github.com/stephenfewer/ReflectiveDLLInjection (https://github.com/stephenfewer/ReflectiveDLLInjection)
- **ps1encode** use to generate and encode a powershell based metasploit payloads. https://github.com/CroweCybersecurity/ps1encode (https://github.com/CroweCybersecurity/ps1encode)
- **Worse PDF** turn a normal PDF file into malicious. Use to steal Net-NTLM Hashes from windows machines. https://github.com/3gstudent/Worse-PDF (https://github.com/3gstudent/Worse-PDF)
- **SpookFlare** has a different perspective to bypass security measures and it gives you the opportunity to bypass the endpoint countermeasures at the client-side detection and network-side detection. https://github.com/hlldz/SpookFlare (https://github.com/hlldz/SpookFlare)
- **GreatSCT** is an open source project to generate application white list bypasses. This tool is intended for BOTH red and blue team. https://github.com/GreatSCT/GreatSCT (https://github.com/GreatSCT/GreatSCT)
- **nps** running powershell without powershell. https://github.com/Ben0xA/nps (https://github.com/Ben0xA/nps)
- **Meterpreter_Paranoid_Mode.sh** allows users to secure your staged/stageless connection for Meterpreter by having it check the certificate of the handler it is connecting to. https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL (https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL)
- **The Backdoor Factory (BDF)** is to patch executable binaries with user desired shellcode and continue normal execution of the prepatched state. https://github.com/secretsquirrel/the-backdoor-factory (https://github.com/secretsquirrel/the-backdoor-factory)
- **MacroShop** a collection of scripts to aid in delivering payloads via Office Macros. https://github.com/khr0x40sh/MacroShop (https://github.com/khr0x40sh/MacroShop)
- **UnmanagedPowerShell** Executes PowerShell from an unmanaged process. https://github.com/leechristensen/UnmanagedPowerShell (https://github.com/leechristensen/UnmanagedPowerShell)
- **evil-ssdp** Spoof SSDP replies to phish for NTLM hashes on a network. Creates a fake UPNP device, tricking users into visiting a malicious phishing page. https://gitlab.com/initstring/evil-ssdp (https://gitlab.com/initstring/evil-

ssdp)

- **Ebowla** Framework for Making Environmental Keyed Payloads. https://github.com/Genetic-Malware/Ebowla (https://github.com/Genetic-Malware/Ebowla)
- **make-pdf-embedded** a tool to create a PDF document with an embedded file. https://github.com/DidierStevens/DidierStevensSuite/blob/master/make-pdf-embedded.py (https://github.com/DidierStevens/DidierStevensSuite/blob/master/make-pdf-embedded.py)
- **avet** (AntiVirusEvasionTool) is targeting windows machines with executable files using different evasion techniques. https://github.com/govolution/avet (https://github.com/govolution/avet)

# Delivery

## Phishing

- **King Phisher** is a tool for testing and promoting user awareness by simulating real world phishing attacks. https://github.com/securestate/king-phisher (https://github.com/securestate/king-phisher)
- **FiercePhish** is a full-fledged phishing framework to manage all phishing engagements. It allows you to track separate phishing campaigns, schedule sending of emails, and much more. https://github.com/Raikia/FiercePhish (https://github.com/Raikia/FiercePhish)
- **ReelPhish** is a Real-Time Two-Factor Phishing Tool. https://github.com/fireeye/ReelPhish/ (https://github.com/fireeye/ReelPhish/)
- **Gophish** is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly and easily setup and execute phishing engagements and security awareness training. https://github.com/gophish/gophish (https://github.com/gophish/gophish)
- **CredSniper** is a phishing framework written with the Python micro-framework Flask and Jinja2 templating which supports capturing 2FA tokens. https://github.com/ustayready/CredSniper (https://github.com/ustayready/CredSniper)
- **PwnAuth** a web application framework for launching and managing OAuth abuse campaigns. https://github.com/fireeye/PwnAuth (https://github.com/fireeye/PwnAuth)
- **Phishing Frenzy** Ruby on Rails Phishing Framework. https://github.com/pentestgeek/phishing-frenzy (https://github.com/pentestgeek/phishing-frenzy)
- **Phishing Pretexts** a library of pretexts to use on offensive phishing engagements. https://github.com/L4bF0x/PhishingPretexts (https://github.com/L4bF0x/PhishingPretexts)
- *__Modlishka__ is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level. https://github.com/drk1wi/Modlishka (https://github.com/drk1wi/Modlishka)

## Watering Hole Attack

- **BeEF** is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. https://github.com/beefproject/beef (https://github.com/beefproject/beef)

# Command and Control

# Remote Access Tools

- **Cobalt Strike** is software for Adversary Simulations and Red Team Operations. https://cobaltstrike.com/ (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 (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 (https://github.com/rapid7/metasploit-framework)
- **SILENTTRINITY** A post-exploitation agent powered by Python, IronPython, C#/.NET. https://github.com/byt3bl33d3r/SILENTTRINITY (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 (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 (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 (https://github.com/nettitude/PoshC2)
- **Gcat** a stealthy Python based backdoor that uses Gmail as a command and control server. https://github.com/byt3bl33d3r/gcat (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 (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 (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 (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 (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/ (https://github.com/FactionC2/)

# 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 (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 (https://github.com/byt3bl33d3r/Red-Baron)

- **EvilURL** generate unicode evil domains for IDN Homograph Attack and detect them. https://github.com/UndeadSec/EvilURL (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 (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 (https://github.com/mdsecactivebreach/PowerDNS)
- **Chameleon** a tool for evading Proxy categorisation. https://github.com/mdsecactivebreach/Chameleon (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 (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 (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 (https://github.com/bluscreenofjeff/Malleable-C2-Randomizer)
- **FindFrontableDomains** search for potential frontable domains. https://github.com/rvrsh3ll/FindFrontableDomains (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 (https://github.com/n0pe-sled/Postfix-Server-Setup)
- **DomainFrontingLists** a list of Domain Frontable Domains by CDN. https://github.com/vysec/DomainFrontingLists (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 (https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup)
- **mod_rewrite rule** to evade vendor sandboxes. https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10 (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 (https://github.com/Und3rf10w/external_c2_framework)
- **ExternalC2** a library for integrating communication channels with the Cobalt Strike External C2 server. https://github.com/ryhanson/ExternalC2 (https://github.com/ryhanson/ExternalC2)
- **cs2modrewrite** a tools for convert Cobalt Strike profiles to modrewrite scripts. https://github.com/threatexpress/cs2modrewrite (https://github.com/threatexpress/cs2modrewrite)
- **e2modrewrite** a tools for convert Empire profiles to Apache modrewrite scripts. https://github.com/infosecn1nja/e2modrewrite (https://github.com/infosecn1nja/e2modrewrite)
- **redi** automated script for setting up CobaltStrike redirectors (nginx reverse proxy, letsencrypt). https://github.com/taherio/redi (https://github.com/taherio/redi)
- **cat-sites** Library of sites for categorization. https://github.com/audrummer15/cat-sites (https://github.com/audrummer15/cat-sites)
- **now-you-see-me** Pass-thru web server for traffic redirection. https://github.com/audrummer15/now-you-see-me (https://github.com/audrummer15/now-you-see-me)

- **Domain Fronting Google App Engine**. https://github.com/redteam-cyberark/Google-Domain-fronting (https://github.com/redteam-cyberark/Google-Domain-fronting)
- **DomainFrontDiscover** Scripts and results for finding domain frontable CloudFront domains. https://github.com/peewpw/DomainFrontDiscover (https://github.com/peewpw/DomainFrontDiscover)
- **Automated Empire Infrastructure** https://github.com/bneg/RedTeam-Automation (https://github.com/bneg/RedTeam-Automation)
- **Serving Random Payloads** with NGINX. https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9 (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 (https://github.com/arlolra/meek)
- **CobaltStrike-ToolKit** Some useful scripts for CobaltStrike. https://github.com/killswitch-GUI/CobaltStrike-ToolKit (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 (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 (https://github.com/outflanknl/RedFile)
- **keyserver** Easily serve HTTP and DNS keys for proper payload protection. https://github.com/leoloobeek/keyserver (https://github.com/leoloobeek/keyserver)
- **DoHC2** allows the ExternalC2 library from Ryan Hanson (https://github.com/ryhanson/ExternalC2 (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 (https://github.com/SpiderLabs/DoHC2)

# Lateral Movement

- **CrackMapExec** is a swiss army knife for pentesting networks. https://github.com/byt3bl33d3r/CrackMapExec (https://github.com/byt3bl33d3r/CrackMapExec)
- **PowerLessShell** rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe. https://github.com/Mr-Un1k0d3r/PowerLessShell (https://github.com/Mr-Un1k0d3r/PowerLessShell)
- **GoFetch** is a tool to automatically exercise an attack plan generated by the BloodHound application. https://github.com/GoFetchAD/GoFetch (https://github.com/GoFetchAD/GoFetch)
- **ANGRYPUPPY** a bloodhound attack path automation in CobaltStrike. https://github.com/vysec/ANGRYPUPPY (https://github.com/vysec/ANGRYPUPPY)
- **DeathStar** is a Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments using a variety of techinques. https://github.com/byt3bl33d3r/DeathStar (https://github.com/byt3bl33d3r/DeathStar)
- **SharpHound** C# Rewrite of the BloodHound Ingestor. https://github.com/BloodHoundAD/SharpHound (https://github.com/BloodHoundAD/SharpHound)
- **BloodHound.py** is a Python based ingestor for BloodHound, based on Impacket. https://github.com/fox-it/BloodHound.py (https://github.com/fox-it/BloodHound.py)

- **Responder** is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication. https://github.com/SpiderLabs/Responder (https://github.com/SpiderLabs/Responder)
- **SessionGopher** is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally. https://github.com/fireeye/SessionGopher (https://github.com/fireeye/SessionGopher)
- **PowerSploit** is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment. https://github.com/PowerShellMafia/PowerSploit (https://github.com/PowerShellMafia/PowerSploit)
- **Nishang** is a framework and collection of scripts and payloads which enables usage of PowerShell for offensive security, penetration testing and red teaming. Nishang is useful during all phases of penetration testing. https://github.com/samratashok/nishang (https://github.com/samratashok/nishang)
- **Inveigh** is a Windows PowerShell LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool. https://github.com/Kevin-Robertson/Inveigh (https://github.com/Kevin-Robertson/Inveigh)
- **PowerUpSQL** a PowerShell Toolkit for Attacking SQL Server. https://github.com/NetSPI/PowerUpSQL (https://github.com/NetSPI/PowerUpSQL)
- **MailSniper** is a penetration testing tool for searching through email in a Microsoft Exchange environment for specific terms (passwords, insider intel, network architecture information, etc.). https://github.com/dafthack/MailSniper (https://github.com/dafthack/MailSniper)
- **WMIOps** is a powershell script that uses WMI to perform a variety of actions on hosts, local or remote, within a Windows environment. It's designed primarily for use on penetration tests or red team engagements. https://github.com/ChrisTruncer/WMIOps (https://github.com/ChrisTruncer/WMIOps)
- **Mimikatz** is an open-source utility that enables the viewing of credential information from the Windows lsass. https://github.com/gentilkiwi/mimikatz (https://github.com/gentilkiwi/mimikatz)
- **LaZagne** project is an open source application used to retrieve lots of passwords stored on a local computer. https://github.com/AlessandroZ/LaZagne (https://github.com/AlessandroZ/LaZagne)
- **mimipenguin** a tool to dump the login password from the current linux desktop user. Adapted from the idea behind the popular Windows tool mimikatz. https://github.com/huntergregal/mimipenguin (https://github.com/huntergregal/mimipenguin)
- **PsExec** is a light-weight telnet-replacement that lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. https://docs.microsoft.com/en-us/sysinternals/downloads/psexec (https://docs.microsoft.com/en-us/sysinternals/downloads/psexec)
- **KeeThief** allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system. https://github.com/HarmJ0y/KeeThief (https://github.com/HarmJ0y/KeeThief)
- **PSAttack** combines some of the best projects in the infosec powershell community into a self contained custom PowerShell console. https://github.com/jaredhaight/PSAttack (https://github.com/jaredhaight/PSAttack)
- **Internal Monologue Attack** Retrieving NTLM Hashes without Touching LSASS. https://github.com/eladshamir/Internal-Monologue (https://github.com/eladshamir/Internal-Monologue)
- **Impacket** is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (for instance NMB, SMB1-3 and MS-DCERPC) the protocol implementation itself. https://github.com/CoreSecurity/impacket (https://github.com/CoreSecurity/impacket)

- **icebreaker** gets plaintext Active Directory credentials if you're on the internal network but outside the AD environment. https://github.com/DanMcInerney/icebreaker (https://github.com/DanMcInerney/icebreaker)
- **Living Off The Land Binaries and Scripts (and now also Libraries)** The goal of these lists are to document every binary, script and library that can be used for other purposes than they are designed to. https://github.com/api0cradle/LOLBAS (https://github.com/api0cradle/LOLBAS)
- **WSUSpendu** for compromised WSUS server to extend the compromise to clients. https://github.com/AlsidOfficial/WSUSpendu (https://github.com/AlsidOfficial/WSUSpendu)
- **Evilgrade** is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates. https://github.com/infobyte/evilgrade (https://github.com/infobyte/evilgrade)
- **NetRipper** is a post exploitation tool targeting Windows systems which uses API hooking in order to intercept network traffic and encryption related functions from a low privileged user, being able to capture both plain-text traffic and encrypted traffic before encryption/after decryption. https://github.com/NytroRST/NetRipper (https://github.com/NytroRST/NetRipper)
- **LethalHTA** Lateral Movement technique using DCOM and HTA. https://github.com/codewhitesec/LethalHTA (https://github.com/codewhitesec/LethalHTA)
- **Invoke-PowerThIEf** an Internet Explorer Post Exploitation library. https://github.com/nettitude/Invoke-PowerThIEf (https://github.com/nettitude/Invoke-PowerThIEf)
- **RedSnarf** is a pen-testing / red-teaming tool for Windows environments. https://github.com/nccgroup/redsnarf (https://github.com/nccgroup/redsnarf)
- **HoneypotBuster** Microsoft PowerShell module designed for red teams that can be used to find honeypots and honeytokens in the network or at the host. https://github.com/JavelinNetworks/HoneypotBuster (https://github.com/JavelinNetworks/HoneypotBuster)

# Establish Foothold

- **Tunna** is a set of tools which will wrap and tunnel any TCP communication over HTTP. It can be used to bypass network restrictions in fully firewalled environments. https://github.com/SECFORCE/Tunna (https://github.com/SECFORCE/Tunna)
- **reGeorg** the successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. https://github.com/sensepost/reGeorg (https://github.com/sensepost/reGeorg)
- **Blade** is a webshell connection tool based on console, currently under development and aims to be a choice of replacement of Chooper. https://github.com/wonderqs/Blade (https://github.com/wonderqs/Blade)
- **TinyShell** Web Shell Framework. https://github.com/threatexpress/tinyshell (https://github.com/threatexpress/tinyshell)
- **PowerLurk** is a PowerShell toolset for building malicious WMI Event Subsriptions. https://github.com/Sw4mpf0x/PowerLurk (https://github.com/Sw4mpf0x/PowerLurk)
- **DAMP** The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification. https://github.com/HarmJ0y/DAMP (https://github.com/HarmJ0y/DAMP)

# Escalate Privileges

## Domain Escalation