

Red Teaming Toolkit

Table of Contents

[Reconnaissance](#)

[Initial Access](#)

[Delivery](#)

[Situational Awareness](#)

[Credential Dumping](#)

[Privilege Escalation](#)

[Defense Evasion](#)

[Persistence](#)

[Lateral Movement](#)

[Exfiltration](#)

[Miscellaneous](#)

Reconnaissance

| Name | Description | URL |
|------------|--|---|
| RustScan | The Modern Port Scanner. Find ports quickly (3 seconds at its fastest). Run scripts through our scripting engine (Python, Lua, Shell supported). | https://github.com/RustScan/RustScan |
| Amass | In-depth Attack Surface Mapping and Asset Discovery | https://github.com/OWASP/Amass |
| gitleaks | Gitleaks is a SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos. | https://github.com/zricethezav/gitleaks |
| S3Scanner | Scan for open S3 buckets and dump the contents | https://github.com/sa7mon/S3Scanner |
| cloud_enum | Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud. | https://github.com/initstring/cloud_enum |

| Name | Description | URL |
|---------------------|--|---|
| Recon-ng | Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources. | https://github.com/lanmaster53/recon-ng |
| buster | An advanced tool for email reconnaissance | https://github.com/sham00n/buster |
| linkedin2username | OSINT Tool: Generate username lists for companies on LinkedIn | https://github.com/initstring/linkedin2username |
| WitnessMe | Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier. | https://github.com/byt3bl33d3r/WitnessMe |
| pagodo | pagodo (Passive Google Dork) - Automate Google Hacking Database scraping and searching | https://github.com/opsdisk/pagodo |
| AttackSurfaceMapper | AttackSurfaceMapper is a tool that aims to automate the reconnaissance process. | https://github.com/superhedgy/AttackSurfaceMapper |
| SpiderFoot | SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilises a range of methods for data analysis, making that data easy to navigate. | https://github.com/smicallef/spiderfoot |
| dnscan | dnscan is a python wordlist-based DNS subdomain scanner. | https://github.com/rbsec/dnscan |
| spooftcheck | A program that checks if a | https://github.com/BishopFox/spooftcheck |

| Name | Description | URL |
|-----------|--|---|
| | domain can be spoofed from. The program checks SPF and DMARC records for weak configurations that allow spoofing. | |
| LinkedInt | LinkedIn Recon Tool | https://github.com/vysecurity/LinkedInt |

Initial Access

Brute Force

| Name | Description | URL |
|-----------------|---|---|
| | Scripts to make password spraying attacks against Lync/S4B, OWA & O365 a lot quicker, less painful and more efficient | |
| SprayingToolkit | | https://github.com/byt3bl33d3r/SprayingToolkit |
| o365recon | Retrieve information via O365 with a valid cred | https://github.com/nyxgeek/o365recon |
| CredMaster | Refactored & improved CredKing password spraying tool, uses FireProx APIs to rotate IP addresses, stay anonymous, and beat throttling | https://github.com/knavesec/CredMaster |

Payload Development

| Name | Description | URL |
|-----------------|---|---|
| Ivy | Ivy is a payload creation framework for the execution of arbitrary VBA (macro) source code directly in memory. | https://github.com/optiv/Ivy |
| PEzor | Open-Source PE Packer | https://github.com/phra/PEzor |
| GadgetToJScript | A tool for generating .NET serialized gadgets that can trigger .NET assembly load/execution when deserialized using | https://github.com/med0x2e/GadgetToJScript |

| Name | Description | URL |
|------------------------------------|--|---|
| | BinaryFormatter from JS/VBS/VBA scripts. | |
| ScareCrow | Payload creation framework designed around EDR bypass. | https://github.com/optiv/ScareCrow |
| Donut | Donut is a position-independent code that enables in-memory execution of VBScript, JScript, EXE, DLL files and dotNET assemblies. | https://github.com/TheWover/donut |
| Mystikal | macOS Initial Access Payload Generator | https://github.com/D00MFist/Mystikal |
| charlotte | c++ fully undetected shellcode launcher ;) | https://github.com/9emin1/charlotte |
| InvisibilityCloak | Proof-of-concept obfuscation toolkit for C# post-exploitation tools. This will perform the below actions for a C# visual studio project. | https://github.com/xforcered/InvisibilityCloak |
| Dendrobate | Dendrobate is a framework that facilitates the development of payloads that hook unmanaged code through managed .NET code. | https://github.com/FuzzySecurity/Dendrobate |
| Offensive VBA and XLS Entanglement | This repo provides examples of how VBA can be used for offensive purposes beyond a simple dropper or shell injector. As we develop more use cases, the repo will be updated. | https://github.com/BC-SECURITY/Offensive-VBA-and-XLS-Entanglement |
| xlsGen | Tiny Excel BIFF8 Generator, to Embedded 4.0 Macros in *.xls | https://github.com/aaaddress1/xlsGen |
| darkarmour | Windows AV Evasion | https://github.com/bats3c/darkarmour |
| InlineWhispers | Tool for working with Direct System Calls in Cobalt Strike's | https://github.com/outflanknl/InlineWhispers |

| Name | Description | URL |
|--------------|---|---|
| | Beacon Object Files (BOF) | |
| EvilClippy | A cross-platform assistant for creating malicious MS Office documents. Can hide VBA macros, stomp VBA code (via P-Code) and confuse macro analysis tools. Runs on Linux, OSX and Windows. | https://github.com/outflanknl/EvilClippy |
| OfficePurge | VBA purge your Office documents with OfficePurge. VBA purging removes P-code from module streams within Office documents. | https://github.com/fireeye/OfficePurge |
| ThreatCheck | Identifies the bytes that Microsoft Defender / AMSI Consumer flags on. | https://github.com/rasta-mouse/ThreatCheck |
| CrossC2 | Generate CobaltStrike's cross-platform payload | https://github.com/gloxec/CrossC2 |
| Ruler | 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 |
| DueDLLigence | Shellcode runner framework for application whitelisting bypasses and DLL side-loading. The shellcode included in this project spawns calc.exe. | https://github.com/fireeye/DueDLLigence |
| RuralBishop | RuralBishop is practically a carbon copy of UrbanBishop by b33f, but all P/Invoke calls have been replaced with D/Invoke. | https://github.com/rasta-mouse/RuralBishop |
| TikiTorch | TikiTorch was named in homage to CACTUSTORCH by Vincent | https://github.com/rasta-mouse/TikiTorch |

| Name | Description | URL |
|------------------|--|---|
| | Yiu. The basic concept of CACTUSTORCH is that it spawns a new process, allocates a region of memory, then uses CreateRemoteThread to run the desired shellcode within that target process. Both the process and shellcode are specified by the user. | |
| SharpShooter | SharpShooter is a payload creation framework for the retrieval and execution of arbitrary CSharp source code. SharpShooter is capable of creating payloads in a variety of formats, including HTA, JS, VBS and WSF. | https://github.com/mdsecactivebreach/SharpShooter |
| SharpSploit | SharpSploit is a .NET post-exploitation library written in C# | https://github.com/cobbr/SharpSploit |
| MSBuildAPICaller | MSBuild Without MSBuild.exe | https://github.com/rvrsh3ll/MSBuildAPICaller |
| macro_pack | 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 |
| inceptor | Template-Driven AV/EDR Evasion Framework | https://github.com/klezVirus/inceptor |
| mortar | evasion technique to defeat and divert detection and prevention of security products (AV/EDR/XDR) | https://github.com/0xsp-SRD/mortar |
| ProtectMyTooling | Multi-Packer wrapper letting us | https://github.com/mgeeky/ProtectMyTooling |

| Name | Description | URL |
|--------|---|---|
| | daisy-chain various packers, obfuscators and other Red Team oriented weaponry. Featured with artifacts watermarking, IOCs collection & PE Backdooring. You feed it with your implant, it does a lot of sneaky things and spits out obfuscated executable. | |
| Freeze | Freeze is a payload toolkit for bypassing EDRs using suspended processes, direct syscalls, and alternative execution methods | https://github.com/optiv/Freeze |

Delivery

Phishing

| Name | Description | URL |
|---------------------|---|---|
| o365-attack-toolkit | A toolkit to attack Office365 | https://github.com/mdsecactivebreach/o365-attack-toolkit |
| Evilginx2 | Evilginx2 is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service. | https://github.com/kgretzky/evilginx2 |
| Gophish | 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 |
| PwnAuth | PwnAuth a web application framework for launching and managing OAuth abuse campaigns. | https://github.com/fireeye/PwnAuth |
| Modlishka | Modlishka is a flexible and powerful reverse proxy, that will take your ethical phishing | https://github.com/drklwi/Modlishka |

| Name | Description | URL |
|------|-------------|-----|
|------|-------------|-----|

campaigns to the next level.

Watering Hole Attack

| Name | Description | URL |
|------|-------------|-----|
|------|-------------|-----|

| | | |
|------|--|---|
| BeEF | 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 |
|------|--|---|

Command and Control

Remote Access Tools (RAT)

| Name | Description | URL |
|------|-------------|-----|
|------|-------------|-----|

| | | |
|---------------|--|---|
| Cobalt Strike | Cobalt Strike is software for Adversary Simulations and Red Team Operations. | https://cobaltstrike.com/ |
|---------------|--|---|

| | | |
|----------------|---|---|
| Brute Ratel C4 | Brute Ratel is the most advanced Red Team & Adversary Simulation Software in the current C2 Market. | https://bruteratel.com/ |
|----------------|---|---|

| | | |
|--------|---|---|
| Empire | Empire 5 is a post-exploitation framework that includes a pure-PowerShell Windows agent, and compatibility with Python 3.x Linux/OS X agents. | https://github.com/BC-SECURITY/Empire |
|--------|---|---|

| | | |
|--------|--|---|
| PoshC2 | PoshC2 is a proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement. | https://github.com/nettitude/PoshC2 |
|--------|--|---|

| | | |
|--------|---|---|
| Koadic | Koadic C3 COM Command & Control - JScript RAT | https://github.com/zerosum0x0/koadic |
|--------|---|---|

| | | |
|--------|--|---|
| merlin | Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go. | https://github.com/Ne0nd0g/merlin |
|--------|--|---|

| | | |
|--------|---|---|
| Mythic | A cross-platform, post-exploit, red teaming framework built with python3, docker, docker-compose, | https://github.com/its-a-feature/Mythic |
|--------|---|---|

| Name | Description | URL |
|---------------|--|---|
| | and a web browser UI. | |
| Covenant | 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 |
| shad0w | A post exploitation framework designed to operate covertly on heavily monitored environments | https://github.com/bats3c/shad0w |
| Sliver | Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. | https://github.com/BishopFox/sliver |
| SILENTTRINITY | An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR | https://github.com/byt3bl33d3r/SILENTTRINITY |
| Pupy | 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 |
| Havoc | Havoc is a modern and malleable post-exploitation command and control framework, created by @C5pider. | https://github.com/HavocFramework/Havoc |
| NimPlant | A light first-stage C2 implant written in Nim and Python | https://github.com/chvancooten/NimPlant |
| SharpC2 | SharpC2 is a Command & Control (C2) framework written in C#. It consists of an ASP.NET Core Team Server, a .NET Framework implant, and a .NET MAUI client. | https://github.com/rasta-mouse/SharpC2 |

Staging

| Name | Description | URL |
|----------------------|--|---|
| pwndrop | Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV. | https://github.com/kgretzky/pwndrop |
| C2concealer | A command line tool that generates randomized C2 malleable profiles for use in Cobalt Strike. | https://github.com/FortyNorthSecurity/C2concealer |
| FindFrontableDomains | Search for potential frontable domains | https://github.com/rvrsh3ll/FindFrontableDomains |
| Domain Hunter | Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names | https://github.com/threatexpress/domainhunter |
| RedWarden | Flexible CobaltStrike Malleable Redirector | https://github.com/mgeeky/RedWarden |
| AzureC2Relay | AzureC2Relay is an Azure Function that validates and relays Cobalt Strike beacon traffic by verifying the incoming requests based on a Cobalt Strike Malleable C2 profile. | https://github.com/Flangvik/AzureC2Relay |
| C3 | C3 (Custom Command and Control) is a tool that allows Red Teams to rapidly develop and utilise esoteric command and control channels (C2). | https://github.com/FSecureLABS/C3 |

| Name | Description | URL |
|---|---|---|
| Chameleon | A tool for evading Proxy categorisation | https://github.com/mdsecactivebreach/Chameleon |
| Cobalt Strike Malleable C2 Design and Reference Guide | Cobalt Strike Malleable C2 Design and Reference Guide | https://github.com/threatexpress/malleable-c2/ |
| redirect.rules | Quick and dirty dynamic redirect.rules generator | https://github.com/0xZDH/redirect.rules |
| CobaltBus | Cobalt Strike External C2 Integration With Azure Servicebus, C2 traffic via Azure Servicebus | https://github.com/Flangvik/CobaltBus |
| SourcePoint | SourcePoint is a C2 profile generator for Cobalt Strike command and control servers designed to ensure evasion. | https://github.com/Tylous/SourcePoint |
| RedGuard | RedGuard is a C2 front flow control tool, Can avoid Blue Teams, AVs, EDRs check. | https://github.com/wikiZ/RedGuard |

Log Aggregation

| Name | Description | URL |
|-------------------------|---|---|
| RedELK | Red Team's SIEM - tool for Red Teams used for tracking and alarming about Blue Team activities as well as better usability in long term operations. | https://github.com/outflanknl/RedELK |
| Elastic for Red Teaming | Repository of resources for configuring a Red Team SIEM using Elastic. | https://github.com/SecurityRiskAdvisors/RedTeamSIEM |
| RedEye | RedEye is a visual analytic tool supporting Red & Blue Team operations | https://github.com/cisagov/RedEye |

Situational Awareness

Host Situational Awareness

| Name | Description | URL |
|---------------------------|---|---|
| AggressiveProxy | AggressiveProxy is a combination of a .NET 3.5 binary (LetMeOutSharp) and a Cobalt Strike aggressor script (AggressiveProxy.cna). Once LetMeOutSharp is executed on a workstation, it will try to enumerate all available proxy configurations and try to communicate with the Cobalt Strike server over HTTP(s) using the identified proxy configurations. | https://github.com/EncodeGroup/AggressiveProxy |
| Gopher | C# tool to discover low hanging fruits | https://github.com/EncodeGroup/Gopher |
| SharpEDRChecker | Checks running processes, process metadata, Dlls loaded into your current process and the each DLLs metadata, common install directories, installed services and each service binaries metadata, installed drivers and each drivers metadata, all for the presence of known defensive products such as AV's, EDR's and logging tools. | https://github.com/PwnDexter/SharpEDRChecker |
| Situational Awareness BOF | This Repo intends to serve two purposes. First it provides a nice set of basic situational awareness commands implemented in BOF. | https://github.com/trustedsec/CS-Situational-Awareness-BOF |
| Seatbelt | Seatbelt is a C# project that performs a number of security | https://github.com/GhostPack/Seatbelt |

| Name | Description | URL |
|----------------|--|---|
| | oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives. | |
| SauronEye | SauronEye is a search tool built to aid red teams in finding files containing specific keywords. | https://github.com/vivami/SauronEye |
| SharpShares | Multithreaded C# .NET Assembly to enumerate accessible network shares in a domain | https://github.com/mitchmoser/SharpShares |
| SharpAppLocker | C# port of the Get-AppLockerPolicy PowerShell cmdlet with extended features. Includes the ability to filter and search for a specific type of rules and actions. | https://github.com/Flangvik/SharpAppLocker/ |
| SharpPrinter | Printer is a modified and console version of ListNetworks | https://github.com/rvrsh3ll/SharpPrinter |

Domain Situational Awareness

| Name | Description | URL |
|------------|---|---|
| StandIn | StandIn is a small AD post-compromise toolkit. StandIn came about because recently at xforcerd we needed a .NET native solution to perform resource based constrained delegation. | https://github.com/FuzzySecurity/StandIn |
| Recon-AD | An AD recon tool based on ADSI and reflective DLL's | https://github.com/outflanknl/Recon-AD |
| BloodHound | Six Degrees of Domain Admin | https://github.com/BloodHoundAD/BloodHound |
| PSPKIAudit | PowerShell toolkit for auditing Active Directory Certificate Services (AD CS). | https://github.com/GhostPack/PSPKIAudit |
| SharpView | C# implementation of harmj0y's PowerView | https://github.com/tevora-threat/SharpView |
| Rubeus | Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project (CC | https://github.com/GhostPack/Rubeus |

| Name | Description | URL |
|------------|---|---|
| | BY-NC-SA 4.0 license) and Vincent LE TOUX's MakeMeEnterpriseAdmin project (GPL v3.0 license). | |
| Grouper | A PowerShell script for helping to find vulnerable settings in AD Group Policy. (deprecated, use Grouper2 instead!) | https://github.com/l0ss/Grouper |
| ImproHound | Identify the attack paths in BloodHound breaking your AD tiering | https://github.com/improsec/ImproHound |
| ADRecon | ADRecon is a tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD environment. | https://github.com/adrecon/ADRecon |
| ADCSPwn | A tool to escalate privileges in an active directory network by coercing authenticate from machine accounts (Petitpotam) and relaying to the certificate service. | https://github.com/bats3c/ADCSPwn |

Credential Dumping

| Name | Description | URL |
|------------|---|---|
| Mimikatz | Mimikatz is an open-source application that allows users to view and save authentication credentials like Kerberos tickets. | https://github.com/gentilkiwi/mimikatz |
| Dumpert | LSASS memory dumper using direct system calls and API unhooking. | https://github.com/outflanknl/Dumpert |
| CredBandit | CredBandit is a proof of concept Beacon Object File (BOF) that uses static x64 syscalls to perform a complete in memory dump of a process and send that back through your already | https://github.com/xforced/CredBandit |

| Name | Description | URL |
|---------------|--|---|
| | existing Beacon communication channel. | |
| CloneVault | CloneVault allows a red team operator to export and import entries including attributes from Windows Credential Manager. | https://github.com/mdsecactivebreach/CloneVault |
| SharpLAPS | Retrieve LAPS password from LDAP | https://github.com/swisskyrepo/SharpLAPS |
| SharpDPAPI | SharpDPAPI is a C# port of some DPAPI functionality from @gentilkiwi's Mimikatz project. | https://github.com/GhostPack/SharpDPAPI |
| 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/GhostPack/KeeThief |
| SafetyKatz | SafetyKatz is a combination of slightly modified version of @gentilkiwi's Mimikatz project and @subtee's .NET PE Loader. | https://github.com/GhostPack/SafetyKatz |
| forkatz | credential dump using forshaw technique using SeTrustedCredmanAccessPrivilege | https://github.com/Barbarisch/forkatz |
| PPLKiller | Tool to bypass LSA Protection (aka Protected Process Light) | https://github.com/RedCursorSecurityConsulting/PPLKiller |
| LaZagne | The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer. | https://github.com/AlessandroZ/LaZagne |
| AndrewSpecial | AndrewSpecial, dumping lsass' memory stealthily and bypassing "Cilence" since 2019. | https://github.com/hoangprod/AndrewSpecial |
| Net- | .NET implementation of Get- | https://github.com/outflanknl/Net-GPPPassword |

| Name | Description | URL |
|---------------|---|---|
| GPPPassword | GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences. | |
| SharpChromium | .NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins. | https://github.com/djhohnstein/SharpChromium |
| Chlonium | Chlonium is an application designed for cloning Chromium Cookies. | https://github.com/rxwx/chlonium |
| SharpCloud | SharpCloud is a simple C# utility for checking for the existence of credential files related to Amazon Web Services, Microsoft Azure, and Google Compute. | https://github.com/chrismaddalena/SharpCloud |
| pypykatz | Mimikatz implementation in pure Python. At least a part of it :) | https://github.com/skelsec/pypykatz |
| nanodump | A Beacon Object File that creates a minidump of the LSASS process. | https://github.com/helpsystems/nanodump |
| Koh | Koh is a C# and Beacon Object File (BOF) toolset that allows for the capture of user credential material via purposeful token/logon session leakage. | https://github.com/GhostPack/Koh |

Privilege Escalation

| Name | Description | URL |
|------------|---|---|
| ElevateKit | The Elevate Kit demonstrates how to use third-party privilege escalation attacks with Cobalt Strike's Beacon payload. | https://github.com/rsmudge/ElevateKit |
| Watson | Watson is a .NET tool designed to enumerate | https://github.com/rasta-mouse/Watson |

| Name | Description | URL |
|-------------|--|---|
| | missing KBs and suggest exploits for Privilege Escalation vulnerabilities. | |
| SharpUp | SharpUp is a C# port of various PowerUp functionality. Currently, only the most common checks have been ported; no weaponization functions have yet been implemented. | https://github.com/GhostPack/SharpUp |
| dazzleUP | A tool that detects the privilege escalation vulnerabilities caused by misconfigurations and missing updates in the Windows operating systems. dazzleUP detects the following vulnerabilities. | https://github.com/hlldz/dazzleUP |
| PEASS | Privilege Escalation Awesome Scripts SUITE (with colors) | https://github.com/carlospolop/PEASS-ng |
| SweetPotato | A collection of various native Windows privilege escalation techniques from service accounts to SYSTEM | https://github.com/CCob/SweetPotato |
| MultiPotato | Another Potato to get SYSTEM via SeImpersonate privileges | https://github.com/S3cur3Th1sSh1t/MultiPotato |
| KrbRelayUp | a universal no-fix local privilege escalation in windows domain environments where LDAP signing is not enforced (the default settings). | https://github.com/Dec0ne/KrbRelayUp |

Defense Evasion

| Name | Description | URL |
|--------------|---|---|
| RefleXXion | RefleXXion is a utility designed to aid in bypassing user-mode hooks utilised by AV/EPP/EDR etc. | https://github.com/hlldz/RefleXXion |
| EDRSandBlast | EDRSandBlast is a tool written in C that weaponize a vulnerable signed driver to bypass EDR detections (Kernel callbacks and ETW TI provider) and LSASS | https://github.com/wavestone-cdt/EDRSandblast |

| Name | Description | URL |
|------------------------------|---|---|
| | protections. | |
| unDefender | Killing your preferred antimalware by abusing native symbolic links and NT paths. | https://github.com/APTortellini/unDefender |
| Backstab | A tool to kill antimalware protected processes | https://github.com/Yaxser/Backstab |
| SPAWN | Cobalt Strike BOF that spawns a sacrificial process, injects it with shellcode, and - executes payload. Built to evade | |
| Cobalt Strike BOF | EDR/UserLand hooks by spawning sacrificial process with Arbitrary Code Guard (ACG), BlockDll, and PPID spoofing. | https://github.com/boku7/spawn |
| BOF.NET | BOF.NET is a small native BOF object | |
| BOF.NET | - A combined with the BOF.NET managed .NET Runtime runtime that enables the development of for Cobalt Strike BOFs directly in .NET. | https://github.com/CCob/BOF.NET |
| Strike's Beacon Object Files | BOF.NET removes the complexity of native compilation along with the headaches of manually importing native API. | |
| NetLoader | Loads any C# binary from filepath or url, patching AMSI and bypassing Windows Defender on runtime | https://github.com/Flangvik/NetLoader |
| FindObjects-BOF | A Cobalt Strike Beacon Object File (BOF) project which uses direct system calls to enumerate processes for specific modules or process handles. | https://github.com/outflanknl/FindObjects-BOF |
| SharpUnhooker | C# Based Universal API Unhooker - Automatically Unhook API Hives (ntdll.dll, kernel32.dll, user32.dll, advapi32.dll, and kernelbase.dll). | https://github.com/GetRektBoy724/SharpUnhooker |
| EvtMute | Apply a filter to the events being reported by windows event logging | https://github.com/bats3c/EvtMute |
| InlineExecute-Assembly | InlineExecute-Assembly is a proof of concept Beacon Object File (BOF) that | https://github.com/xforced/InlineExecute-Assembly |

| Name | Description | URL |
|-------------------|--|---|
| | allows security professionals to perform in process .NET assembly execution as an alternative to Cobalt Strikes traditional fork and run execute-assembly module | |
| Phant0m | Windows Event Log Killer | https://github.com/hlldz/Phant0m |
| SharpBlock | A method of bypassing EDR's active projection DLL's by preventing entry point execution. | https://github.com/CCob/SharpBlock |
| NtdllUnpatcher | Example code for EDR bypassing, please use this for testing blue team detection capabilities against this type of malware that will bypass EDR's userland hooks. | https://github.com/Kharos102/NtdllUnpatcher |
| DarkLoadLibrary | LoadLibrary for offensive operations. | https://github.com/bats3c/DarkLoadLibrary |
| BlockETW | .Net 3.5 / 4.5 Assembly to block ETW telemetry in a process | https://github.com/Soledge/BlockEtw |
| firewalker | This repo contains a simple library which can be used to add FireWalker hook bypass capabilities to existing code | https://github.com/mdsecactivebreach/firewalker |
| KillDefenderBOF | Beacon Object File PoC implementation of KillDefender | https://github.com/Cerbersec/KillDefenderBOF |
| Mangle | Mangle is a tool that manipulates aspects of compiled executables (.exe or DLL) to avoid detection from EDRs | https://github.com/optiv/Mangle |
| AceLdr | Cobalt Strike UDRL for memory scanner evasion. | https://github.com/kyleavery/AceLdr |
| AtomLdr | CA DLL loader with advanced evasive features | https://github.com/NUL0x4C/AtomLdr |
| Inline-Execute-PE | Execute unmanaged Windows executables in CobaltStrike Beacons | https://github.com/Octoberfest7/Inline-Execute-PE |

Persistence

| Name | Description | URL |
|-----------------------------|---|---|
| SharpStay | .NET project for installing Persistence | https://github.com/0xthirteen/SharpStay |
| SharPersist | Windows persistence toolkit written in C#. | https://github.com/fireeye/SharPersist |
| SharpHide | Tool to create hidden registry keys. This leverages the NetUserAdd Win32 | https://github.com/outflanknl/SharpHide |
| DoUCMe | API to create a new computer account. This is done by setting the usr1_priv of the USER_INFO_1 type to 0x1000. | https://github.com/Ben0xA/DoUCMe |
| A Black Path Toward The Sun | (TCP tunneling over HTTP for web application servers) | https://github.com/nccgroup/ABPTTS |
| pivotnacci | A tool to make socks connections through HTTP agents | https://github.com/blackarrowsec/pivotnacci |
| reGeorg | The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. | https://github.com/sensepost/reGeorg |
| DAMP | The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification. | https://github.com/HarmJ0y/DAMP |
| IIS-Raid | A native backdoor module for Microsoft IIS (Internet Information Services) | https://github.com/0x09AL/IIS-Raid |
| SharPyShell | tiny and obfuscated ASP.NET webshell for C# web applications | https://github.com/antonioCoco/SharPyShell |
| ScheduleRunner | A C# tool with more flexibility to customize scheduled task for both persistence and lateral movement in red team operation | https://github.com/netero1010/ScheduleRunner |
| SharpEventPersist | Persistence by writing/reading shellcode from Event Log | https://github.com/improsec/SharpEventPersist |
| Kraken | Kraken, a modular multi-language webshell coded by @secu_x11. | https://github.com/kraken-ng/Kraken |

Lateral Movement

| Name | Description | URL |
|----------------------|---|---|
| Liquid Snake | LiquidSnake is a tool that allows operators to perform fileless lateral movement using WMI Event Subscriptions and GadgetToJScript | https://github.com/RiccardoAncarani/LiquidSnake |
| PowerUpSQL | A PowerShell Toolkit for Attacking SQL Server | https://github.com/NetSPI/PowerUpSQL |
| SQLRecon | A C# MS SQL toolkit designed for offensive reconnaissance and post-exploitation. | https://github.com/skawah/SQLRecon |
| SCShell | Fileless lateral movement tool that relies on ChangeServiceConfigA to run command | https://github.com/Mr-Un1k0d3r/SCShell |
| SharpRDP | Remote Desktop Protocol Console Application for Authenticated Command Execution | https://github.com/0xthirteen/SharpRDP |
| MoveKit | Movekit is an extension of built in Cobalt Strike lateral movement by leveraging the execute_assembly function with the SharpMove and SharpRDP .NET assemblies. | https://github.com/0xthirteen/MoveKit |
| SharpNoPSExec | File less command execution for lateral movement. | https://github.com/juliourena/SharpNoPSExec |
| Responder/MultiRelay | LLMNR/NBT-NS/mDNS Poisoner and NTLMv1/2 Relay. | https://github.com/lgandx/Responder |
| impacket | 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 (e.g. SMB1-3 and MSRPC) the protocol implementation itself. | https://github.com/SecureAuthCorp/impacket |

| Name | Description | URL |
|----------------|---|---|
| Farmer | Farmer is a project for collecting NetNTLM hashes in a Windows domain. | https://github.com/mdsecactivebreach/Farmer |
| CIMplant | C# port of WMIImplant which uses either CIM or WMI to query remote systems. It can use provided credentials or the current user's session. | https://github.com/FortyNorthSecurity/CIMplant |
| PowerLessShell | PowerLessShell rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe. You can also execute raw shellcode using the same approach. | https://github.com/Mr-Un1k0d3r/PowerLessShell |
| SharpGPOAbuse | SharpGPOAbuse is a .NET application written in C# that can be used to take advantage of a user's edit rights on a Group Policy Object (GPO) in order to compromise the objects that are controlled by that GPO. | https://github.com/FSecureLABS/SharpGPOAbuse |
| kerbrute | A tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication | https://github.com/ropnop/kerbrute |
| mssqlproxy | mssqlproxy is a toolkit aimed to perform lateral movement in restricted environments through a compromised Microsoft SQL Server via socket reuse | https://github.com/blackarrowsec/mssqlproxy |
| Invoke-TheHash | PowerShell Pass The Hash Utils | https://github.com/Kevin-Robertson/Invoke-TheHash |
| InveighZero | .NET IPv4/IPv6 machine-in-the-middle tool for penetration testers | https://github.com/Kevin-Robertson/InveighZero |

| Name | Description | URL |
|-------------------|---|---|
| SharpSpray | SharpSpray a simple code set to perform a password spraying attack against all users of a domain using LDAP and is compatible with Cobalt Strike. | https://github.com/jnqpbld/SharpSpray |
| CrackMapExec | A swiss army knife for pentesting networks | https://github.com/byt3bl33d3r/CrackMapExec |
| SharpAllowedToAct | A C# implementation of a computer object takeover through Resource-Based Constrained Delegation (msDS-AllowedToActOnBehalfOfOtherIdentity) based on the research by @elad_shamir. | https://github.com/pkb1s/SharpAllowedToAct |
| SharpRDPHijack | Sharp RDP Hijack is a proof-of-concept .NET/C# Remote Desktop Protocol (RDP) session hijack utility for disconnected sessions | https://github.com/bohops/SharpRDPHijack |
| CheeseTools | This repository has been made basing onto the already existing MiscTool, so big shout-out to rasta-mouse for releasing them and for giving me the right motivation to work on them. | https://github.com/klezVirus/CheeseTools |
| SharpSpray | SharpSpray is a Windows domain password spraying tool written in .NET C#. | https://github.com/iomoath/SharpSpray |
| MalSCCM | This tool allows you to abuse local or remote SCCM servers to deploy malicious applications to hosts they manage. | https://github.com/nettitude/MalSCCM |
| Coercer | A python script to automatically coerce a Windows server to authenticate on an arbitrary machine through 9 methods. | https://github.com/p0dalirius/Coercer |

| Name | Description | URL |
|-------------|--|---|
| SharpSploit | SharpSploit is a .NET post-exploitation library written in C# that aims to highlight the attack surface of .NET and make the use of offensive .NET easier for red teamers. | https://github.com/cobbr/SharpSploit |
| orpheus | Bypassing Kerberoast Detections with Modified KDC Options and Encryption Types | https://github.com/trustedsec/orpheus |

Exfiltration

| Name | Description | URL |
|-----------------|---|---|
| SharpExfiltrate | Modular C# framework to exfiltrate loot over secure and trusted channels. | https://github.com/Flangvik/SharpExfiltrate |
| DNSExfiltrator | Data exfiltration over DNS request covert channel | https://github.com/Arno0x/DNSExfiltrator |
| Egress-Assess | Egress-Assess is a tool used to test egress data detection capabilities. | https://github.com/FortyNorthSecurity/Egress-Assess |

Miscellaneous

Threat-informed Defense

| Name | Description | URL |
|----------------------------|--|---|
| Tidal Cyber | Tidal Cyber helps enterprise organizations to define, measure, and improve their defenses to address the adversary behaviors that are most important to them. | https://app.tidalcyber.com |
| Control Validation Compass | Threat modeling aide & purple team content repository, pointing security & intelligence teams to 10,000+ publicly-accessible technical and policy controls and 2,100+ offensive security tests, aligned with nearly 600 common attacker techniques | https://controlcompass.github.io |

Cloud

Amazon Web Services (AWS)

| Name | Description | URL |
|-----------------------|--|---|
| Pacu | The AWS exploitation framework, designed for testing the security of Amazon Web Services environments. | https://github.com/RhinoSecurityLabs/pacu |
| CloudMapper | CloudMapper helps you analyze your Amazon Web Services (AWS) environments. | https://github.com/duo-labs/cloudmapper |
| Enumerate permissions | IAM Enumerate the permissions associated with AWS credential set | https://github.com/andresriancho/enumerate-iam |

Azure

| Name | Description | URL |
|--|---|---|
| Azure AD Connect password extraction | This toolkit offers several ways to extract and decrypt stored Azure AD and Active Directory credentials from Azure AD Connect servers. | https://github.com/fox-it/adconnectdump |
| Storm Spotter | Azure Red Team tool for graphing Azure and Azure Active Directory objects | https://github.com/Azure/Stormspotter |
| ROADtools | The Azure AD exploration framework. | https://github.com/dirkjanm/ROADtools |
| MicroBurst: PowerShell Toolkit for Attacking Azure | A collection of scripts for assessing Microsoft Azure security | https://github.com/NetSPI/MicroBurst |
| AADInternals | AADInternals PowerShell module for administering Azure AD and Office 365 | https://github.com/Gerenios/AADInternals |
| TeamFiltration | TeamFiltration is a cross-platform framework for enumerating, spraying, exfiltrating, and backdooring O365 AAD accounts. | https://github.com/Flangvik/TeamFiltration |
| MAAD Framework | An attack tool for simple, fast & effective security testing of M365 & Azure AD. | https://github.com/vectra-ai-research/MAAD-AF |

Adversary Emulation

| Name | Description | URL |
|---------------------------|---|---|
| Stratus Red Team | Stratus Red Team is "Atomic Red Team™" for the cloud, allowing to emulate offensive attack techniques in a granular and self-contained manner. | https://github.com/DataDog/stratus-red-team |
| Prelude Operator | A Platform for Developer-first advanced security. Defend your organization by mimicking real adversarial attacks. | https://www.preludesecurity.com/products/operator |
| Prelude Build | An open source IDE for authoring, testing, and verifying production-ready security tests.. | https://www.preludesecurity.com/products/build |
| 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 | https://github.com/endgameinc/RTA |

| Name | Description | URL |
|---|--|---|
| | MITRE ATT&CK. | |
| Living Off the Living Off the Land | | |
| Name | Description | URL |
| Living Off The Land Drivers | Living Off The Land Drivers is a curated list of Windows drivers used by adversaries to bypass security controls and carry out attacks | https://www.loldrivers.io/ |
| GTFOBins | GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems | https://gtfobins.github.io |
| LOLBAS | The goal of the LOLBAS project is to document every binary, script, and library that can be used for Living Off The Land techniques | https://lolbas-project.github.io/ |
| Living Off Trusted Sites (LOTS) Project | Attackers are using popular legitimate domains when conducting phishing, C&C, exfiltration and downloading tools to evade detection. The list of websites below allow attackers to use their domain or subdomain | https://lots-project.com |
| Filesec | Stay up-to-date with the latest file extensions being used by attackers. | https://filesec.io/ |
| LOOBins | Living Off the Orchard: macOS Binaries (LOOBins) is designed to provide detailed information on various built-in macOS binaries and how they can be used by threat actors for malicious purposes. | https://www.loobins.io/ |
| WTFBins | WTFBin(n): a binary that behaves exactly like malware, except, somehow, it's not? This project aims to catalogue benign applications that exhibit suspicious behavior. These binaries can emit noise and false positives in threat hunting and automated detections. | https://wtfbins.wtf/ |
| Hijack Libs | This project provides an curated list of DLL Hijacking candidates | https://hijacklibs.net |

Red Team Scripts

| Name | Description | URL |
|--------------|----------------------|---|
| RedTeamCCode | Red Team C code repo | https://github.com/Mr- |

| Name | Description | URL |
|-----------------------------|--|--|
| | | <u>Un1k0d3r/RedTeamCCode</u> |
| EDRs | This repo contains information about EDRs that can be useful during red team exercise. | <u>https://github.com/Mr-Un1k0d3r/EDRs</u> |
| Cobalt Strike Community Kit | Community Kit is a central repository of extensions written by the user community to extend the capabilities of Cobalt Strike. | <u>https://cobalt-strike.github.io/community_kit/</u> |

Red Team Infrastructure

| Name | Description | URL |
|---------------|--|--|
| Red Team Wiki | to collect Red Team infrastructure hardening resources | <u>https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki</u> |