Red Teaming Toolkit

This repository contains cutting-edge open-source security tools (OST) that will help you during adversary simulation and as information intended for threat hunter can make detection and prevention control easier. The list of tools below that could be potentially misused by threat actors such as APT and Human-Operated Ransomware (HumOR). If you want to contribute to this list send me a pull request.

Table of Contents

- 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://tinyurl.com/yzm7jdhz
Amass	In-depth Attack Surface Mapping and Asset Discovery	https://tinyurl.com/y5ndjozr
gitleaks	Gitleaks is a SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos.	https://tinyurl.com/y3bwm7nn
S3Scanner	Scan for open S3 buckets and dump the contents	https://tinyurl.com/y5snjrqp
cloud_enum	Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud.	https://tinyurl.com/2olyguyl
Recon-ng	Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.	https://tinyurl.com/yxj3nmhh
buster	An advanced tool for email reconnaissance	https://tinyurl.com/2dljxosh
linkedin2username	OSINT Tool: Generate username lists for companies on LinkedIn	https://tinyurl.com/2cnnegek
WitnessMe	Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless	https://tinyurl.com/26mq7ogl

	Chrome/Chromium) and provides some extra bells & whistles to make life easier.	
pagodo	pagodo (Passive Google Dork) - Automate Google Hacking Database scraping and searching	https://tinyurl.com/2n8gdxz4
AttackSurfaceMapper	AttackSurfaceMapper is a tool that aims to automate the reconnaissance process.	https://tinyurl.com/yxmn4wbt
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://tinyurl.com/krg6svm
dnscan	dnscan is a python wordlist-based DNS subdomain scanner.	https://tinyurl.com/27pqj6rc
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://tinyurl.com/2b39ch7f
LinkedInt	LinkedIn Recon Tool	https://tinyurl.com/29qhcae6

Initial Access

Brute Force

Name	Description	URL
SprayingToolkit	Scripts to make password spraying attacks against Lync/S4B, OWA & O365 a lot quicker, less painful and more efficient	https://tinyurl.com/2yzbkw8x

o365recon	Retrieve information via O365 with a valid cred	https://tinyurl.com/2yeuf5l4
CredMaster	Refactored & improved CredKing password spraying tool, uses FireProx APIs to rotate IP addresses, stay anonymous, and beat throttling	https://tinyurl.com/2d9th2aa

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://tinyurl.com/2azxbnbh
PEzor	Open-Source PE Packer	https://tinyurl.com/26qzxmlt
GadgetToJScript	A tool for generating .NET serialized gadgets that can trigger .NET assembly load/execution when deserialized using BinaryFormatter from JS/VBS/VBA scripts.	https://tinyurl.com/26jmm2f4
ScareCrow	Payload creation framework designed around EDR bypass.	https://tinyurl.com/y2467n9h
Donut	Donut is a position-independent code that enables in-memory execution of VBScript, JScript, EXE, DLL files and dotNET assemblies.	https://tinyurl.com/26tw6g8p
Mystikal	macOS Initial Access Payload Generator	https://tinyurl.com/24khapxe
charlotte	c++ fully undetected shellcode launcher ;)	https://tinyurl.com/23ev367q
InvisibilityCloak	Proof-of-concept obfuscation toolkit for C# post-exploitation tools. This will perform the below actions for a C# visual studio project.	https://tinyurl.com/25ocvug4
	Dendrobate is a framework that	

Dendrobate	facilitates the development of payloads that hook unmanaged code through managed .NET code.	https://tinyurl.com/2849xfbb
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://tinyurl.com/26t3tq3q
xlsGen	Tiny Excel BIFF8 Generator, to Embedded 4.0 Macros in *.xls	https://tinyurl.com/2axx5w65
darkarmour	Windows AV Evasion	https://tinyurl.com/2xjkpxm4
InlineWhispers	Tool for working with Direct System Calls in Cobalt Strike's Beacon Object Files (BOF)	https://tinyurl.com/27ewc7e4
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://tinyurl.com/22yl7a3e
OfficePurge	VBA purge your Office documents with OfficePurge. VBA purging removes P-code from module streams within Office documents.	https://tinyurl.com/263d2ojn
ThreatCheck	Identifies the bytes that Microsoft Defender / AMSI Consumer flags on.	https://tinyurl.com/25frxtwe
CrossC2	Generate CobaltStrike's cross-platform payload	https://tinyurl.com/298zqfth
Ruler	Ruler is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol.	https://tinyurl.com/hcq6kqc
	Shellcode runner framework for application whitelisting bypasses and	

DueDLLigence	DLL side-loading. The shellcode included in this project spawns calc.exe.	https://tinyurl.com/229qxfhl
RuralBishop	RuralBishop is practically a carbon copy of UrbanBishop by b33f, but all P/Invoke calls have been replaced with D/Invoke.	https://tinyurl.com/2ym6vkuc
TikiTorch	TikiTorch was named in homage to CACTUSTORCH by Vincent 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.	https://tinyurl.com/25dm9lkx
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://tinyurl.com/2aw56prh
SharpSploit	SharpSploit is a .NET post-exploitation library written in C#	https://tinyurl.com/2bjo8keq
MSBuildAPICaller	MSBuild Without MSBuild.exe	https://tinyurl.com/2yh26exz
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://tinyurl.com/ydb277y6
inceptor	Template-Driven AV/EDR Evasion Framework	https://tinyurl.com/2afxaor4
mortar	evasion technique to defeat and divert detection and prevention of security	https://tinyurl.com/27kz99de

	products (AV/EDR/XDR)	
ProtectMyTooling	Multi-Packer wrapper letting us 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.	https://tinyurl.com/29g9eq88
Freeze	Freeze is a payload toolkit for bypassing EDRs using suspended processes, direct syscalls, and alternative execution methods	https://tinyurl.com/2djf5w9d

Delivery

Phishing

Name	Description	URL
o365-attack-toolkit	A toolkit to attack Office365	https://tinyurl.com/25xqt4bf
Evilginx2	Evilginx2 is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service.	https://tinyurl.com/y8a84894
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://tinyurl.com/h5qdqxu
PwnAuth	PwnAuth a web application framework for launching and managing OAuth abuse campaigns.	https://tinyurl.com/27pnyga8
	Modlishka is a flexible and powerful reverse	

Modlishka	proxy, that will take your ethical phishing campaigns to the next level.	https://tinyurl.com/ydycmr5h

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://tinyurl.com/bwmgtk3

Command and Control

Remote Access Tools (RAT)

Name	Description	URL
Cobalt Strike	Cobalt Strike is software for Adversary Simulations and Red Team Operations.	https://tinyurl.com/2yw9dkmp
Brute Ratel C4	Brute Ratel is the most advanced Red Team & Adversary Simulation Software in the current C2 Market.	https://tinyurl.com/2ycmheog
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://tinyurl.com/yckfweyv
PoshC2	PoshC2 is a proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement.	https://tinyurl.com/2xwn7vvu
Koadic	Koadic C3 COM Command & Control - JScript RAT	https://tinyurl.com/y86l7rk6
merlin	Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go.	https://tinyurl.com/yd3836u8
	A cross-platform, post-exploit, red	

Mythic	teaming framework built with python3, docker, docker-compose, and a web browser UI.	https://tinyurl.com/26u68uax
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://tinyurl.com/2ytak3ya
shad0w	A post exploitation framework designed to operate covertly on heavily monitored environments	https://tinyurl.com/25l8hwyz
Sliver	Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS.	https://tinyurl.com/y52ghpgo
SILENTTRINITY	An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR	https://tinyurl.com/yyr8vcrf
Pupy	Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python	https://tinyurl.com/p8zvzdo
Havoc	Havoc is a modern and malleable post-exploitation command and control framework, created by @C5pider.	https://tinyurl.com/2d99h72h
NimPlant	A light first-stage C2 implant written in Nim and Python	https://tinyurl.com/2xutf34p
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://tinyurl.com/25qakora

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://tinyurl.com/29xl2ogz
C2concealer	A command line tool that generates randomized C2 malleable profiles for use in Cobalt Strike.	https://tinyurl.com/252ad3k5
FindFrontableDomains	Search for potential frontable domains	https://tinyurl.com/2aguwj5a
Domain Hunter	Checks expired domains for categorization/reputation and Archive.org history to determine good candidates for phishing and C2 domain names	https://tinyurl.com/yao3e538
RedWarden	Flexible CobaltStrike Malleable Redirector	https://tinyurl.com/25o5tget
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://tinyurl.com/2ywnzfp8
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://tinyurl.com/y7noysve
Chameleon	A tool for evading Proxy categorisation	https://tinyurl.com/27gft6mr
Cobalt Strike Malleable C2 Design and Reference Guide	Cobalt Strike Malleable C2 Design and Reference Guide	https://tinyurl.com/27u6je3b

redirect.rules	Quick and dirty dynamic redirect.rules generator	https://tinyurl.com/26dfhoc3
CobaltBus	Cobalt Strike External C2 Integration With Azure Servicebus, C2 traffic via Azure Servicebus	https://tinyurl.com/22f4s3fn
SourcePoint	SourcePoint is a C2 profile generator for Cobalt Strike command and control servers designed to ensure evasion.	https://tinyurl.com/22ye4t26
RedGuard	RedGuard is a C2 front flow control tool,Can avoid Blue Teams,AVs,EDRs check.	https://tinyurl.com/24ea6dud
skyhook	A round-trip obfuscated HTTP file transfer setup built to bypass IDS detections.	https://tinyurl.com/25talnbn

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://tinyurl.com/y4xsacbw
Elastic for Red Teaming	Repository of resources for configuring a Red Team SIEM using Elastic.	https://tinyurl.com/26c4v6fx
RedEye	RedEye is a visual analytic tool supporting Red & Blue Team operations	https://tinyurl.com/27rknale

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://tinyurl.com/284u7of2
Gopher	C# tool to discover low hanging fruits	https://tinyurl.com/257ta5jf
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://tinyurl.com/2cu7xwdc
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://tinyurl.com/2xk8w9ps
Seatbelt	Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.	https://tinyurl.com/2cy2y49d
SauronEye	SauronEye is a search tool built to aid red teams in finding files containing specific keywords.	https://tinyurl.com/2cf8y6fy
SharpShares	Multithreaded C# .NET Assembly to enumerate accessible network shares in a domain	https://tinyurl.com/24yeptls

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://tinyurl.com/2b3lonkk
SharpPrinter	Printer is a modified and console version of ListNetworks	https://tinyurl.com/24mxro94

Domain Situational Awareness

Name	Description	URL
StandIn	StandIn is a small AD post-compromise toolkit. StandIn came about because recently at xforcered we needed a .NET native solution to perform resource based constrained delegation.	https://tinyurl.com/2c53qruj
Recon-AD	An AD recon tool based on ADSI and reflective DLL's	https://tinyurl.com/2982t9yw
BloodHound	Six Degrees of Domain Admin	https://tinyurl.com/y2s37jeg
PSPKIAudit	PowerShell toolkit for auditing Active Directory Certificate Services (AD CS).	https://tinyurl.com/24faq6bz
SharpView	C# implementation of harmj0y's PowerView	https://tinyurl.com/26vlxhql
Rubeus	Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project (CC BY-NC-SA 4.0 license) and Vincent LE TOUX's MakeMeEnterpriseAdmin project (GPL v3.0 license).	https://tinyurl.com/2a6ka5my
nanorobeus	A minimalistic tool for managing Kerberos tickets. Supports redteam frameworks	https://tinyurl.com/22g5ests
Grouper	A PowerShell script for helping to find vulnerable settings in AD Group Policy.	https://tinyurl.com/28nvx8yj

	(deprecated, use Grouper2 instead!)	
ImproHound	Identify the attack paths in BloodHound breaking your AD tiering	https://tinyurl.com/25zb4lm9
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://tinyurl.com/y58q9ta2
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://tinyurl.com/2bqqh3vo

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://tinyurl.com/qdf539r
Dumpert	LSASS memory dumper using direct system calls and API unhooking.	https://tinyurl.com/25skm2fu
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 existing Beacon communication channel.	https://tinyurl.com/2xzh7tq9
CloneVault	CloneVault allows a red team operator to export and import entries including attributes from Windows Credential Manager.	https://tinyurl.com/2aehdhwj
SharpLAPS	Retrieve LAPS password from LDAP	https://tinyurl.com/2bbhn38h

SharpDPAPI	SharpDPAPI is a C# port of some DPAPI functionality from @gentilkiwi's Mimikatz project.	https://tinyurl.com/287ldu65
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://tinyurl.com/2xl9j27x
SafetyKatz	SafetyKatz is a combination of slightly modified version of @gentilkiwi's Mimikatz project and @subtee's .NET PE Loader.	https://tinyurl.com/26fbe6v7
forkatz	credential dump using forshaw technique using SeTrustedCredmanAccessPrivilege	https://tinyurl.com/29wvdke3
PPLKiller	Tool to bypass LSA Protection (aka Protected Process Light)	https://tinyurl.com/ya2ej9r7
LaZagne	The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer.	https://tinyurl.com/m9k4zzr
AndrewSpecial	AndrewSpecial, dumping lsass' memory stealthily and bypassing "Cilence" since 2019.	https://tinyurl.com/27eujsm2
Net-GPPPassword	.NET implementation of Get-GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.	https://tinyurl.com/2abvhehm
SharpChromium	.NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins.	https://tinyurl.com/2bfknzyz
Chlonium	Chlonium is an application designed for cloning Chromium Cookies.	https://tinyurl.com/27w2ftmf
SharpCloud	SharpCloud is a simple C# utility for checking for the existence of credential	https://tinyurl.com/274l2ese

	files related to Amazon Web Services, Microsoft Azure, and Google Compute.	
pypykatz	Mimikatz implementation in pure Python. At least a part of it :)	https://tinyurl.com/yxp3rds4
nanodump	A Beacon Object File that creates a minidump of the LSASS process.	https://tinyurl.com/29kwh76f
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://tinyurl.com/23lahjkx

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://tinyurl.com/256p5ml6
Watson	Watson is a .NET tool designed to enumerate missing KBs and suggest exploits for Privilege Escalation vulnerabilities.	https://tinyurl.com/25vcv3qu
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://tinyurl.com/2c9e5rfo
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://tinyurl.com/26d6mvzq
PEASS	Privilege Escalation Awesome Scripts SUITE (with colors)	https://tinyurl.com/27s758x3

SweetPotato	A collection of various native Windows privilege escalation techniques from service accounts to SYSTEM	https://tinyurl.com/26gksp5m
MultiPotato	Another Potato to get SYSTEM via SeImpersonate privileges	https://tinyurl.com/25ykdfoc
KrbRelayUp	a universal no-fix local privilege escalation in windows domain environments where LDAP signing is not enforced (the default settings).	https://tinyurl.com/2746ujpv
GodPotato	As Long as You Have the ImpersonatePrivilege Permission, Then You are the SYSTEM!	https://tinyurl.com/2a3qo93f

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://tinyurl.com/2y5
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 protections.	https://tinyurl.com/yxpt
unDefender	Killing your preferred antimalware by abusing native symbolic links and NT paths.	https://tinyurl.com/2cg
Backstab	A tool to kill antimalware protected processes	https://tinyurl.com/268
SPAWN - Cobalt Strike BOF	Cobalt Strike BOF that spawns a sacrificial process, injects it with shellcode, and executes payload. Built to evade EDR/UserLand hooks by spawning sacrificial process with Arbitrary Code Guard (ACG), BlockDll, and PPID spoofing.	https://tinyurl.com/23u
BOF.NET - A	BOF.NET is a small native BOF object combined with the BOF.NET managed runtime that	

.NET Runtime for Cobalt Strike's Beacon Object Files	enables the development of Cobalt Strike BOFs directly in .NET. BOF.NET removes the complexity of native compilation along with the headaches of manually importing native API.	https://tinyurl.com/26x
NetLoader	Loads any C# binary from filepath or url, patching AMSI and bypassing Windows Defender on runtime	https://tinyurl.com/y82
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://tinyurl.com/267
SharpUnhooker	C# Based Universal API Unhooker - Automatically Unhook API Hives (ntdll.dll,kernel32.dll,user32.dll,advapi32.dll,and kernelbase.dll).	https://tinyurl.com/29x
EvtMute	Apply a filter to the events being reported by windows event logging	https://tinyurl.com/2cp
InlineExecute-Assembly	InlineExecute-Assembly is a proof of concept Beacon Object File (BOF) that allows security professionals to perform in process .NET assembly execution as an alternative to Cobalt Strikes traditional fork and run execute-assembly module	https://tinyurl.com/24lc
Phant0m	Windows Event Log Killer	https://tinyurl.com/2ag
SharpBlock	A method of bypassing EDR's active projection DLL's by preventing entry point execution.	https://tinyurl.com/2xrl
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://tinyurl.com/2cc
DarkLoadLibrary	LoadLibrary for offensive operations.	https://tinyurl.com/29f5
BlockETW	.Net 3.5 / 4.5 Assembly to block ETW telemetry in a process	https://tinyurl.com/28h
	This repo contains a simple library which can	

firewalker	be used to add FireWalker hook bypass capabilities to existing code	https://tinyurl.com/24z
KillDefenderBOF	Beacon Object File PoC implementation of KillDefender	https://tinyurl.com/254
Mangle	Mangle is a tool that manipulates aspects of compiled executables (.exe or DLL) to avoid detection from EDRs	https://tinyurl.com/25g
AceLdr	Cobalt Strike UDRL for memory scanner evasion.	https://tinyurl.com/25lv
AtomLdr	CA DLL loader with advanced evasive features	https://tinyurl.com/27v
Inline-Execute-PE	Execute unmanaged Windows executables in CobaltStrike Beacons	https://tinyurl.com/28s
SigFlip	SigFlip is a tool for patching authenticode signed PE files (exe, dll, sys ..etc) without invalidating or breaking the existing signature.	https://tinyurl.com/yelp
Blackout	kill anti-malware protected processes (BYOVD)	https://tinyurl.com/2cq

Persistence

Name	Description	URL
SharpStay	.NET project for installing Persistence	https://tinyurl.com/234qsrnb
SharPersist	Windows persistence toolkit written in C#.	https://tinyurl.com/24jrb44l
SharpHide	Tool to create hidden registry keys.	https://tinyurl.com/24ow3byf
DoUCMe	This leverages the NetUserAdd Win32 API to create a new computer account. This is done by setting the usri1_priv of the USER_INFO_1 type to 0x1000.	https://tinyurl.com/24vrev87
A Black Path Toward The Sun	(TCP tunneling over HTTP for web application servers)	https://tinyurl.com/2ac5jszu

pivotnacci	A tool to make socks connections through HTTP agents	https://tinyurl.com/29sxnrzh
reGeorg	The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.	https://tinyurl.com/2edz9l8v
DAMP	The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification.	https://tinyurl.com/26o4elg5
IIS-Raid	A native backdoor module for Microsoft IIS (Internet Information Services)	https://tinyurl.com/29meqpj7
SharPyShell	tiny and obfuscated ASP.NET webshell for C# web applications	https://tinyurl.com/yyqc93m8
ScheduleRunner	A C# tool with more flexibility to customize scheduled task for both persistence and lateral movement in red team operation	https://tinyurl.com/2bvtmgrz
SharpEventPersist	Persistence by writing/reading shellcode from Event Log	https://tinyurl.com/28hnstvz
Kraken	Kraken, a modular multi-language webshell coded by @secu_x11.	https://tinyurl.com/2cgyzhrv
HiddenDesktop	HVNC for Cobalt Strike	https://tinyurl.com/28tnwo24

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://tinyurl.com/27cwd3
PowerUpSQL	A PowerShell Toolkit for Attacking SQL Server	https://tinyurl.com/2cxk8u

SQLRecon	A C# MS SQL toolkit designed for offensive reconnaissance and post-exploitation.	https://tinyurl.com/225yh7
SCShell	Fileless lateral movement tool that relies on ChangeServiceConfigA to run command	https://tinyurl.com/yzwwln
SharpRDP	Remote Desktop Protocol Console Application for Authenticated Command Execution	https://tinyurl.com/2ayeujn
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://tinyurl.com/274exx
SharpNoPSExec	File less command execution for lateral movement.	https://tinyurl.com/2dyyo9
Responder/MultiRelay	LLMNR/NBT-NS/mDNS Poisoner and NTLMv1/2 Relay.	https://tinyurl.com/zue3sty
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://tinyurl.com/yysqx7
Farmer	Farmer is a project for collecting NetNTLM hashes in a Windows domain.	https://tinyurl.com/2yqphw
CIMplant	C# port of WMImplant which uses either CIM or WMI to query remote systems. It can use provided credentials or the current user's session.	https://tinyurl.com/2asyyb
	PowerLessShell rely on MSBuild.exe to	

PowerLessShell	remotely execute PowerShell scripts and commands without spawning powershell.exe. You can also execute raw shellcode using the same approach.	https://tinyurl.com/y7x3j6g
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://tinyurl.com/2y2ql3
kerbrute	A tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication	https://tinyurl.com/y66kz8
mssqlproxy	mssqlproxy is a toolkit aimed to perform lateral movement in restricted environments through a compromised Microsoft SQL Server via socket reuse	https://tinyurl.com/2227m7
Invoke-TheHash	PowerShell Pass The Hash Utils	https://tinyurl.com/27c4lb5
InveighZero	.NET IPv4/IPv6 machine-in-the-middle tool for penetration testers	https://tinyurl.com/28plsny
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://tinyurl.com/2bafaw
CrackMapExec	A swiss army knife for pentesting networks	https://tinyurl.com/ngzqxs
SharpAllowedToAct	A C# implementation of a computer object takeover through Resource-Based Constrained Delegation (msDS-AllowedToActOnBehalfOfOtherIdentity) based on the research by @elad_shamir.	https://tinyurl.com/29yb2c

SharpRDPHijack	Sharp RDP Hijack is a proof-of-concept .NET/C# Remote Desktop Protocol (RDP) session hijack utility for disconnected sessions	https://tinyurl.com/2cpqdd
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://tinyurl.com/24oanh
SharpSpray	SharpSpray is a Windows domain password spraying tool written in .NET C#.	https://tinyurl.com/29w6lk
MalSCCM	This tool allows you to abuse local or remote SCCM servers to deploy malicious applications to hosts they manage.	https://tinyurl.com/2c8aom
Coercer	A python script to automatically coerce a Windows server to authenticate on an arbitrary machine through 9 methods.	https://tinyurl.com/2bgpf2
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://tinyurl.com/2bjo8ke
orpheus	Bypassing Kerberoast Detections with Modified KDC Options and Encryption Types	https://tinyurl.com/27xf4lk
Chisel	Chisel is a fast TCP/UDP tunnel, transported over HTTP, secured via SSH. Single executable including both client and server.	https://tinyurl.com/z6yl32k
frp	frp is a fast reverse proxy that allows you to expose a local server located behind a NAT or firewall to the Internet.	https://tinyurl.com/joc488

Exfiltration

Name	Description	URL
SharpExfiltrate	Modular C# framework to exfiltrate loot over secure and trusted channels.	https://tinyurl.com/2b92bnao
DNSExfiltrator	Data exfiltration over DNS request covert channel	https://tinyurl.com/ybeyldvg
Egress-Assess	Egress-Assess is a tool used to test egress data detection capabilities.	https://tinyurl.com/y6zkl93s

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://tinyurl.com/22a8umc6
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://tinyurl.com/26t5m4ss

Cloud

Amazon Web Services (AWS)

Name	Description	URL
pacu	The AWS exploitation framework, designed for testing the security of Amazon Web Services environments.	https://tinyurl.com/y7yo3rtg

CloudMapper	CloudMapper helps you analyze your Amazon Web Services (AWS) environments.	https://tinyurl.com/y9wjhuue
Enumerate IAM permissions	Enumerate the permissions associated with AWS credential set	https://tinyurl.com/yy86zgea

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://tinyurl.com/23gnev9q
Storm Spotter	Azure Red Team tool for graphing Azure and Azure Active Directory objects	https://tinyurl.com/25cekf4k
ROADtools	The Azure AD exploration framework.	https://tinyurl.com/2y3rddej
MicroBurst: A PowerShell Toolkit for Attacking Azure	A collection of scripts for assessing Microsoft Azure security	https://tinyurl.com/27zfacq2
AADInternals	AADInternals PowerShell module for administering Azure AD and Office 365	https://tinyurl.com/28rtsk82
TeamFiltration	TeamFiltration is a cross-platform framework for enumerating, spraying, exfiltrating, and backdooring O365 AAD accounts.	https://tinyurl.com/26pabg6g
MAAD Attack Framework	An attack tool for simple, fast & effective security testing of M365 & Azure AD.	https://tinyurl.com/2y53rvmy

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://tinyurl.com/2d5om4mg
Prelude Operator	A Platform for Developer-first advanced security· Defend your organization by mimicking real adversarial attacks.	https://tinyurl.com/2cmqcehj
Prelude Build	An open source IDE for authoring, testing, and verifying production-ready security tests..	https://tinyurl.com/27uy9br5
Caldera	An automated adversary emulation system that performs post-compromise adversarial behavior within Windows Enterprise networks.	https://tinyurl.com/y8jw9jc4
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://tinyurl.com/24hj2583
Atomic Red Team	Small and highly portable detection tests mapped to the Mitre ATT&CK Framework.	https://tinyurl.com/yc7zduf8
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://tinyurl.com/2af233j6
Metta	A security preparedness tool to do adversarial simulation.	https://tinyurl.com/2agjmveq
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://tinyurl.com/24uefmgl

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://tinyurl.com/24d9jlg8
GTFOBins	GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems	https://tinyurl.com/yccgv6ks
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://tinyurl.com/y6ct9yf9
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://tinyurl.com/2yez2man
Filesec	Stay up-to-date with the latest file extensions being used by attackers.	https://tinyurl.com/248sbkdm
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://tinyurl.com/29zyqza8
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://tinyurl.com/24snt96n
Hijack Libs	This project provides an curated list of DLL Hijacking candidates	https://tinyurl.com/259ejgk7

Red Team Scripts

Name	Description	URL
RedTeamCCode	Red Team C code repo	https://tinyurl.com/27wk5f92
EDRs	This repo contains information about EDRs that can be useful during red team exercise.	https://tinyurl.com/2agzk2rt
Cobalt Strike Community Kit	Community Kit is a central repository of extensions written by the user community to extend the capabilities of Cobalt Strike.	https://tinyurl.com/27jhmgw9

Red Team Infrastructure

Name	Description	URL
Red Team Infrastructure Wiki	Wiki to collect Red Team infrastructure hardening resources	https://tinyurl.com/hha9dyk

License