infosecn1nja / Red-Teaming-Toolkit

A collection of open source and commercial tools that aid in red team operations.

red-team hacking infosec pentesting

55 commits **1** branch **0** releases **2** contributors GPL-3.0

Branch: **master** New pull request Find file Clone or download

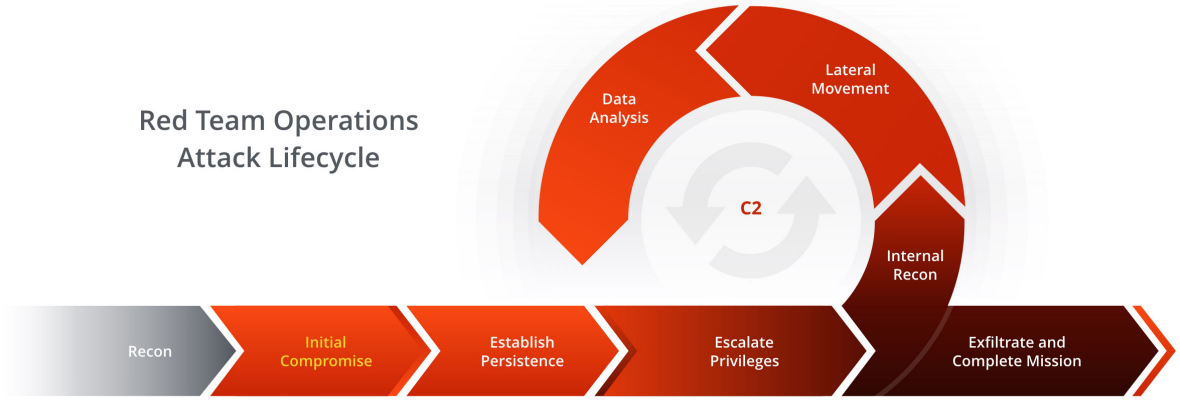
infosecn1nja Update README.md Latest commit e271a3b 6 days ago

LICENSE	Initial commit	17 days ago

README.md

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. If you want to contribute to this list send me a pull request.



Contents

Reconnaissance

- **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
- **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
- **ScrapedIn** a tool to scrape LinkedIn without API restrictions for data reconnaissance. https://github.com/dchrastil/ScrapedIn
- **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
- **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
- **SimplyEmail** Email recon made fast and easy, with a framework to build on. https://github.com/killswitch-GUI/SimplyEmail
- **Recon-ng** is a full-featured Web Reconnaissance framework written in Python. https://bitbucket.org/LaNMaSteR53/recon-ng

- **PowerMeta** searches for publicly available files hosted on various websites for a particular domain by using specially crafted Google, and Bing searches. https://github.com/dafthack/PowerMeta
- **raven** is a Linkedin information gathering tool that can be used by pentesters to gather information about an organization employees using Linkedin. https://github.com/0x09AL/raven
- **AWSBucketDump** is a tool to quickly enumerate AWS S3 buckets to look for loot. https://github.com/jordanpotti/AWSBucketDump
- **SpiderFoot** the open source footprinting and intelligence-gathering tool. 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
- **EyeWitness** is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. https://github.com/ChrisTruncer/EyeWitness
- **AQUATONE** is a set of tools for performing reconnaissance on domain names. 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
- **Probable Wordlists** sorted by probability originally created for password generation and testing. https://github.com/berzerk0/Probable-Wordlists
- **Nmap** is used to discover hosts and services on a computer network, thus building a "map" of the network. https://github.com/nmap/nmap
- **typofinder** a finder of domain typos showing country of IP address. https://github.com/nccgroup/typofinder

Weaponization

- **Composite Moniker** Proof of Concept exploit for 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

- **CVE-2017-11882 Exploit** accepts over 17k bytes long command/code in maximum. https://github.com/unamer/CVE-2017-11882
- **Adobe Flash Exploit** 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
- **demiguise** is a HTA encryption tool for RedTeams. 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
- **CACTUSTORCH** Payload Generation for Adversary Simulations. 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
- **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
- **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
- **SCT Obfuscator** Cobalt Strike SCT payload obfuscator. https://github.com/Mr-Un1k0d3r/SCT-obfuscator
- **Invoke-Obfuscation** PowerShell Obfuscator. https://github.com/danielbohannon/Invoke-Obfuscation
- **Invoke-DOSfuscation** cmd.exe Command Obfuscation Generator & Detection Test Harness. https://github.com/danielbohannon/Invoke-DOSfuscation
- **Unicorn** is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. 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/
- **SigThief** Stealing Signatures and Making One Invalid Signature at a Time. 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
- **CheckPlease** Sandbox evasion modules written in PowerShell, Python, Go, Ruby, C, C#, Perl, and Rust. 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
- **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
- **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
- **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
- **StarFighters** a JavaScript and VBScript Based Empire Launcher. 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
- **Social Engineering Payloads** is a collection of generic payloads for red team and social engineering assessments. https://github.com/t3ntman/Social-Engineering-Payloads
- **The Social-Engineer Toolkit** is an open-source penetration testing framework designed for social engineering. 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
- **PowerShdll** run PowerShell with rundll32. Bypass software restrictions. 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

- **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
- **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
- **Malicious Macro MSBuild Generator** Generates Malicious Macro and Execute Powershell or Shellcode via MSBuild Application Whitelisting Bypass. 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
- **Malicious file maker/sender** to create and send malicious attachments to test your email filter/alerting. https://github.com/carnal0wnage/malicious_file_maker
- **DotNetToJScript** a tool to create a JScript file which loads a .NET v2 assembly from memory. https://github.com/tyranid/DotNetToJScript
- **PSAmsi** is a tool for auditing and defeating AMSI signatures. 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
- **ps1encode** use to generate and encode a powershell based metasploit payloads. 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
- **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
- **Great SCT** 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
- **nps** running powershell without powershell. https://github.com/Ben0xA/nps

Delivery

- **King Phisher** is a tool for testing and promoting user awareness by simulating real world phishing attacks. 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
- **ReelPhish** is a Real-Time Two-Factor Phishing Tool. 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/chrismaddalena/GoReport
- **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
- **Phishing Frenzy** Ruby on Rails Phishing Framework. https://github.com/pentestgeek/phishing-frenzy
- **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
- **Wifiphisher** is a security tool that performs Wi-Fi automatic association attacks to force wireless clients to unknowingly connect to an attacker-controlled Access Point. https://github.com/wifiphisher/wifiphisher
- **Evilginx** is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service. https://github.com/kgretzky/evilginx

Command and Control

Remote Access Tools

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

- **Empire** is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. https://github.com/EmpireProject/Empire
- **Pupy** is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python. https://github.com/n1nj4sec/pupy
- **Koadic** or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. https://github.com/zerosum0x0/koadic
- **PoshC2** is a proxy aware C2 framework written completely in PowerShell to aid penetration testers with red teaming, post-exploitation and lateral movement. https://github.com/nettitude/PoshC2
- **Gcat** a stealthy Python based backdoor that uses Gmail as a command and control server. https://github.com/byt3bl33d3r/gcat
- **TrevorC2** is a legitimate website (browsable) that tunnels client/server communications for covert command execution. https://github.com/trustedsec/trevorc2
- **Merlin** is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang. https://github.com/Ne0nd0g/merlin

Staging

- **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/Coalfire-Research/Red-Baron
- **EvilURL** generate unicode evil domains for IDN Homograph Attack and detect them. https://github.com/UndeadSec/EvilURL
- **Domain Hunter** checks expired domains, bluecoat categorization, and Archive.org history to determine good candidates for phishing and C2 domain names. https://github.com/threatexpress/domainhunter
- **PowerDNS** is a simple proof of concept to demonstrate the execution of PowerShell script using DNS only. https://github.com/mdsecactivebreach/PowerDNS
- **Chameleon** a tool for evading Proxy categorisation. https://github.com/mdsecactivebreach/Chameleon

- **CatMyFish** Search for categorized domain that can be used during red teaming engagement. Perfect to setup whitelisted domain for your Cobalt Strike beacon C&C. https://github.com/Mr-Un1k0d3r/CatMyFish
- **Malleable C2** is a domain specific language to redefine indicators in Beacon's communication. https://github.com/rsmudge/Malleable-C2-Profiles
- **FindFrontableDomains** search for potential frontable domains. https://github.com/rvrsh3ll/FindFrontableDomains
- **Postfix-Server-Setup** Setting up a phishing server is a very long and tedious process. It can take hours to setup, and can be compromised in minutes. https://github.com/n0pe-sled/Postfix-Server-Setup
- **DomainFrontingLists** a list of Domain Frontable Domains by CDN. https://github.com/vysec/DomainFrontingLists
- **Apache2-Mod-Rewrite-Setup** Quickly Implement Mod-Rewrite in your infastructure. https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup
- **mod_rewrite rule** to evade vendor sandboxes. https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10
- **external_c2 framework** a python framework for usage with Cobalt Strike's External C2. https://github.com/Und3rf10w/external_c2_framework
- **ExternalC2** a library for integrating communication channels with the Cobalt Strike External C2 server. https://github.com/ryhanson/ExternalC2
- **cs2modrewrite** a tools for convert Cobalt Strike profiles to modrewrite scripts. https://github.com/threatexpress/cs2modrewrite
- **e2modrewrite** a tools for convert Empire profiles to Apache modrewrite scripts. https://github.com/infosecn1nja/e2modrewrite
- **redi** automated script for setting up CobaltStrike redirectors (nginx reverse proxy, letsencrypt). https://github.com/taherio/redi
- **Domain Fronting Google App Engine**. https://github.com/redteam-cyberark/Google-Domain-fronting
- **DomainFrontDiscover** Scripts and results for finding domain frontable CloudFront domains. https://github.com/peewpw/DomainFrontDiscover

- **Automated Empire Infrastructure** https://github.com/bneg/RedTeam-Automation
- **Serving Random Payloads** with NGINX. https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9
- **meek** is a blocking-resistant pluggable transport for Tor. It encodes a data stream as a sequence of HTTPS requests and responses. https://github.com/arlolra/meek

Lateral Movement

- **CrackMapExec** is a swiss army knife for pentesting networks. https://github.com/byt3bl33d3r/CrackMapExec
- **BloodHound** uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. https://github.com/BloodHoundAD/BloodHound
- **PowerLessShell** rely on MSBuild.exe to remotely execute PowerShell scripts and commands without spawning powershell.exe. 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
- **ANGRYPUPPY** a bloodhound attack path automation in CobaltStrike. 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
- **SharpHound** C# Rewrite of the BloodHound Ingestor. https://github.com/BloodHoundAD/SharpHound
- **BloodHound.py** is a Python based ingestor for BloodHound, based on Impacket. 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
- **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

- **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
- **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
- **Inveigh** is a Windows PowerShell LLMNR/mDNS/NBNS spoofer/man-in-the-middle tool. https://github.com/Kevin-Robertson/Inveigh
- **PowerUpSQL** a PowerShell Toolkit for Attacking SQL Server. 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
- **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
- **Mimikatz** is an open-source utility that enables the viewing of credential information from the Windows lsass. 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
- **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
- **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
- **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
- **PSAttack** combines some of the best projects in the infosec powershell community into a self contained custom PowerShell console. https://github.com/jaredhaight/PSAttack

- **Internal Monologue Attack** Retrieving NTLM Hashes without Touching LSASS. 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
- **ADRecon** is a tool which extracts various artifacts (as highlighted below) out of an AD environment in a specially formatted Microsoft Excel report that includes summary views with metrics to facilitate analysis. https://github.com/sense-of-security/ADRecon
- **icebreaker** gets plaintext Active Directory credentials if you're on the internal network but outside the AD environment. 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

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
- **reGeorg** the successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. 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
- **TinyShell** Web Shell Framework. https://github.com/threatexpress/tinyshell
- **PowerLurk** is a PowerShell toolset for building malicious WMI Event Subsriptions. https://github.com/Sw4mpf0x/PowerLurk

Escalate Privileges

- **UACMe** is an open source assessment tool that contains many methods for bypassing Windows User Account Control on multiple versions of the operating system. https://github.com/hfiref0x/UACME
- **windows-kernel-exploits** a collection windows kernel exploit. https://github.com/SecWiki/windows-kernel-exploits
- **PowerUp** aims to be a clearinghouse of common Windows privilege escalation vectors that rely on misconfigurations. https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc
- **The Elevate Kit** demonstrates how to use third-party privilege escalation attacks with Cobalt Strike's Beacon payload. https://github.com/rsmudge/ElevateKit
- **Sherlock** a powerShell script to quickly find missing software patches for local privilege escalation vulnerabilities. https://github.com/rasta-mouse/Sherlock

Data Exfiltration

- **CloakifyFactory** & the Cloakify Toolset - Data Exfiltration & Infiltration In Plain Sight; Evade DLP/MLS Devices; Social Engineering of Analysts; Defeat Data Whitelisting Controls; Evade AV Detection. https://github.com/TryCatchHCF/Cloakify
- **DET** (is provided AS IS), is a proof of concept to perform Data Exfiltration using either single or multiple channel(s) at the same time. https://github.com/sensepost/DET
- **DNSExfiltrator** allows for transfering (exfiltrate) a file over a DNS request covert channel. This is basically a data leak testing tool allowing to exfiltrate data over a covert channel. https://github.com/Arno0x/DNSExfiltrator
- **PyExfil** a Python Package for Data Exfiltration. https://github.com/ytisf/PyExfil
- **Egress-Assess** is a tool used to test egress data detection capabilities. https://github.com/ChrisTruncer/Egress-Assess
- **Powershell RAT** python based backdoor that uses Gmail to exfiltrate data as an e-mail attachment. https://github.com/Viralmaniar/Powershell-RAT

Misc

Embedded & Peripheral Devices Hacking

- **magspoof** a portable device that can spoof/emulate any magnetic stripe, credit card or hotel card "wirelessly", even on standard magstripe (non-NFC/RFID) readers. https://github.com/samyk/magspoof

Scripts

- **Aggressor Scripts** is a scripting language for red team operations and adversary simulations inspired by scriptable IRC clients and bots.
  - https://github.com/invokethreatguy/CSASC
  - https://github.com/secgroundzero/CS-Aggressor-Scripts
  - https://github.com/Und3rf10w/Aggressor-scripts
  - https://github.com/harleyQu1nn/AggressorScripts
  - https://github.com/rasta-mouse/Aggressor-Script
  - https://github.com/RhinoSecurityLabs/Aggressor-Scripts
  - https://github.com/bluscreenofjeff/AggressorScripts
  - https://github.com/001SPARTaN/aggressor_scripts
- A collection scripts useful for red teaming and pentesting
  - https://github.com/FuzzySecurity/PowerShell-Suite
  - https://github.com/threatexpress/red-team-scripts
  - https://github.com/SadProcessor/SomeStuff
  - https://github.com/rvrsh3ll/Misc-Powershell-Scripts
  - https://github.com/enigma0x3/Misc-PowerShell-Stuff
  - https://github.com/ChrisTruncer/PenTestScripts

- https://github.com/bluscreenofjeff/Scripts
- https://github.com/xorrior/RandomPS-Scripts
- https://github.com/xorrior/Random-CSharpTools
- https://github.com/mgeeky/Penetration-Testing-Tools/tree/master/social-engineering

References

- **Cheat Sheets** for various projects (Beacon/Cobalt Strike,PowerView, PowerUp, Empire, and PowerSploit). https://github.com/HarmJ0y/CheatSheets
- **PRE-ATT&CK** Adversarial Tactics, Techniques & Common Knowledge for Left-of-Exploit. https://attack.mitre.org/pre-attack/index.php/Main_Page
- **Adversary OPSEC** consists of the use of various technologies or 3rd party services to obfuscate, hide, or blend in with accepted network traffic or system behavior. https://attack.mitre.org/pre-attack/index.php/Adversary_OPSEC
- **Adversary Emulation Plans** To showcase the practical use of ATT&CK for offensive operators and defenders, MITRE created Adversary Emulation Plans. https://attack.mitre.org/wiki/Adversary_Emulation_Plans
- **Red-Team-Infrastructure-Wiki** Wiki to collect Red Team infrastructure hardening resources. https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
- **Advanced Threat Tactics – Course and Notes** This is a course on red team operations and adversary simulations. https://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes
- **Red Team Tips** as posted by @vysecurity on Twitter. https://vincentyiu.co.uk/red-team-tips
- **Awesome Red Teaming** List of Awesome Red Team / Red Teaming Resources. https://github.com/yeyintminthuhtut/Awesome-Red-Teaming
- **ATT&CK for Enterprise Software** is a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK. https://attack.mitre.org/wiki/Software
- **Planning a Red Team exercise** This document helps inform red team planning by contrasting against the very specific red team style described in Red Teams. https://github.com/magoo/redteam-plan

- **Awesome Lockpicking** a curated list of awesome guides, tools, and other resources related to the security and compromise of locks, safes, and keys. https://github.com/meitar/awesome-lockpicking
- **Awesome Threat Intelligence** a curated list of awesome Threat Intelligence resources. https://github.com/hslatman/awesome-threat-intelligence
- **APT Notes** Need some scenario? APTnotes is a repository of publicly-available papers and blogs (sorted by year) related to malicious campaigns/activity/software that have been associated with vendor-defined APT (Advanced Persistent Threat) groups and/or tool-sets. https://github.com/aptnotes/data