Adversary Emulation and Cracking The Bridge – Overview PT.1

Joas Antonio

Details

- This is an ebook overview of Adversary Emulation and my Cracking The Bridge Framework
- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

Adversary Emulation: Concepts

- https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3
- https://attack.mitre.org/resources/adversary-emulation-plans/
- https://www.youtube.com/watch?v=tvQbh0bawEM
- https://www.youtube.com/watch?v=wAonnM-AkQE
- https://www.youtube.com/watch?v=nZF3JjPyjNo
- https://www.cybereason.com/blog/what-are-adversary-emulation-plans
- https://www.scythe.io/library/introduction-to-adversary-emulation
- https://www.scythe.io/adversary-emulation
- https://www.crowdstrike.com/services/am-i-ready/adversary-emulation-exercise/
- https://www.nviso.eu/en/service/21/adversary-emulation

Cracking The Bridge

- https://github.com/CyberSecurityUP/Cracking-The-Perimeter-Framework

Adversary Emulation: In Practice

- https://medium.com/mitre-engenuity/introducing-the-all-new-adversary-emulation-plan-library-234b1d543f6b
- https://pt.slideshare.net/erikvanbuggenhout/adversary-emulation-using-caldera
- https://pt.slideshare.net/erikvanbuggenhout/adversary-emulation-using-caldera-232232038
- https://www.youtube.com/watch?v=fx3635hLewg
- https://www.youtube.com/watch?v=xjDrWStR68E
- https://www.youtube.com/watch?v=iXGF6GHEQps
- https://www.youtube.com/watch?v=qy6RqCPLV8Y
- https://www.youtube.com/watch?v=3tNrlutqazQ
- https://www.youtube.com/watch?v=gOS1c375Hbg
- https://www.youtube.com/watch?v=5CRSh5V0s-A
- https://www.youtube.com/watch?v=r_PMfojuXLo
- https://www.youtube.com/watch?v=d6AueWjUHfA
- https://www.youtube.com/watch?v=Fa4GHF_OVVc

Adversary Emulation: In Practice

- https://www.youtube.com/watch?v=YMTlrjkbZHM
- https://www.youtube.com/watch?v=isYotlCFxf8
- https://www.youtube.com/watch?v=RSMJsyACSm8
- https://www.youtube.com/watch?v=igikBwKImWA
- https://www.youtube.com/watch?v=7WUDnFleC5Y
- https://www.youtube.com/watch?v=bEzxyijPkSI
- https://www.youtube.com/watch?v=6elZxGmXxH4
- https://www.youtube.com/watch?v=hIGbgm-HlZA
- https://www.youtube.com/watch?v=0lE5oHqZV0s
- https://blog.reconinfosec.com/adversary-emulation-mapping/

Adversary Emulation: In Practice

- https://medium.com/@jorgeorchilles/purple-team-exercise-tools-a85187ce341
- https://twitter.com/jorgeorchilles
- https://orchilles.com/
- https://www.youtube.com/jorgeorchilles
- https://www.youtube.com/watch?v=BDzw9cGEJos
- https://www.youtube.com/watch?v=YkgBNkh_wtw
- https://www.youtube.com/watch?v=qPqlz75lzwo
- https://www.youtube.com/watch?v=sRaLleKghrE
- https://www.youtube.com/watch?v=TelqSCdwi10
- https://github.com/jorgeorchilles

Adversary Emulation: Purple Team

- https://www.youtube.com/watch?v=iE0CgG0MAH4
- https://www.youtube.com/watch?v=rwOh9MC0M7E
- https://www.youtube.com/watch?v=WOf2U01RhCk
- https://www.youtube.com/watch?v=SA-HeOnOi2A
- https://www.youtube.com/watch?v=GRTa7HfJC6w
- https://www.youtube.com/watch?v=jvXRAbYYE0U
- https://www.youtube.com/watch?v=o3Qb_0clIpg
- https://www.youtube.com/watch?v=0CdFK0qBZZc
- https://www.youtube.com/watch?v=m3mpnUcSpa4
- https://danielmiessler.com/study/red-blue-purple-teams/
- https://www.sans.org/purple-team
- https://github.com/praetorian-inc/purple-team-attack-automation
- https://www.packetlabs.net/mitre-attack/

Adversary Emulation: Purple Team

- https://academy.attackiq.com/learning-paths/purple-teaming
- https://www.pluralsight.com/courses/pentesting-red-blue-purple-teams-exec-briefing?aid=7010a000002BWqBAAW&promo=&utm_source=non_branded&utm_medium=digital_paid_search_google&utm_campaign=NASA_Dynamic&utm_content=&cq_cmp=846117097&gclid=Cj0KCQjwnueFBhChARIsAPu3YkRUH91lmOHgEeWIUVhqApeu9XggRuS0KKLj3qW_s3_CmyA1bg_NaRgaAr4eEALw_wcB
- https://resources.infosecinstitute.com/topic/purple-team-cyber-ranges-hands-on-training-for-red-and-blue-teams/
- https://www.blackhillsinfosec.com/training/applied-purple-teaming-training/
- https://academy.picussecurity.com/
- https://cyberwarfare.live/certified-purple-team-analyst

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Domain Escalation

- PowerView is a PowerShell tool to gain network situational awareness on Windows domains. https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- Get-GPPPassword Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences. https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Get-GPPPassword.ps1
- Invoke-ACLpwn is a tool that automates the discovery and pwnage of ACLs in Active Directory that are unsafe configured. https://github.com/fox-it/Invoke-ACLPwn
- BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. https://github.com/BloodHoundAD/BloodHound
- PyKEK (Python Kerberos Exploitation Kit), a python library to manipulate KRB5-related data. https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS14-068/pykek
- Grouper a PowerShell script for helping to find vulnerable settings in AD Group Policy. https://github.com/l0ss/Grouper
- 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

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- ADACLScanner one script for ACL's in Active Directory. https://github.com/canix1/ADACLScanner
- ACLight a useful script for advanced discovery of Domain Privileged Accounts that could be targeted - including Shadow Admins. https://github.com/cyberark/ACLight
- LAPSToolkit a tool to audit and attack LAPS environments. https://github.com/leoloobeek/LAPSToolkit
- PingCastle is a free, Windows-based utility to audit the risk level of your AD infrastructure and check for vulnerable practices. https://www.pingcastle.com/download
- RiskySPNs is a collection of PowerShell scripts focused on detecting and abusing accounts associated with SPNs (Service Principal Name). https://github.com/cyberark/RiskySPN
- Mystique is a PowerShell tool to play with Kerberos S4U extensions, this module can assist blue teams to identify risky Kerberos delegation configurations as well as red teams to impersonate arbitrary users by leveraging KCD with Protocol Transition. https://github.com/machosec/Mystique
- Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project. https://github.com/GhostPack/Rubeus
- kekeo is a little toolbox I have started to manipulate Microsoft Kerberos in C (and for fun). https://github.com/gentilkiwi/kekeo

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Local Escalation

- 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/blob/master/Privesc/PowerUp.ps1
- 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
- Tokenvator a tool to elevate privilege with Windows Tokens. https://github.com/0xbadjuju/Tokenvator

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Recon and Planning

- https://osintframework.com/
- https://en.wikipedia.org/wiki/Doxing
- https://github.com/HackingEnVivo/Doxing
- https://www.maltego.com/blog/investigating-ta413-threat-actor-group-using-opencti-in-maltego/

Active Intelligence Gathering

- EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible. https://github.com/ChrisTruncer/EyeWitness
- AWSBucketDump is a tool to quickly enumerate AWS S3 buckets to look for loot. https://github.com/jordanpotti/AWSBucketDump
- 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
- Nmap is used to discover hosts and services on a computer network, thus building a "map" of the network. https://github.com/nmap/nmap
- dnsrecon a tool DNS Enumeration Script. https://github.com/darkoperator/dnsrecon
- dirsearch is a simple command line tool designed to brute force directories and files in websites. https://github.com/maurosoria/dirsearch
- Sn1per automated pentest recon scanner. https://github.com/1N3/Sn1per

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Passive Intelligence Gathering

- Social Mapper OSINT Social Media Mapping Tool, takes a list of names & images (or LinkedIn company name) and performs automated target searching on a huge scale across multiple social media sites. Not restricted by APIs as it instruments a browser using Selenium. Outputs reports to aid in correlating targets across sites. https://github.com/SpiderLabs/social_mapper
- skiptracer OSINT scraping framework, utilizes some basic python webscraping (BeautifulSoup) of PII paywall sites to compile passive information on a target on a ramen noodle budget. https://github.com/xillwillx/skiptracer
- 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
- 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
- truffleHog searches through git repositories for secrets, digging deep into commit history and branches. https://github.com/dxa4481/truffleHog
- Just-Metadata is a tool that gathers and analyzes metadata about IP addresses. It attempts to find relationships between systems within a large dataset. https://github.com/ChrisTruncer/Just-Metadata
- typofinder a finder of domain typos showing country of IP address. https://github.com/nccgroup/typofinder

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- pwnedOrNot is a python script which checks if the email account has been compromised in a data breach, if the email account is compromised it proceeds to find passwords for the compromised account. https://github.com/thewhiteh4t/pwnedOrNot
- GitHarvester This tool is used for harvesting information from GitHub like google dork. https://github.com/metac0rtex/GitHarvester
- pwndb is a python command-line tool for searching leaked credentials using the Onion service with the same name. https://github.com/davidtavarez/pwndb/
- LinkedInt LinkedIn Recon Tool. https://github.com/vysecurity/LinkedInt
- CrossLinked LinkedIn enumeration tool to extract valid employee names from an organization through search engine scraping. https://github.com/m8r0wn/CrossLinked
- findomain is a fast domain enumeration tool that uses Certificate Transparency logs and a selection of APIs. https://github.com/Edu4rdSHL/findomain

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- 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
- 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
- Recon-ng is a full-featured Web Reconnaissance framework written in Python. https://bitbucket.org/LaNMaSteR53/recon-ng

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Weaponization

- **WinRAR Remote Code Execution Proof of Concept exploit for CVE-2018-20250. https://github.com/WyAtu/CVE-2018-20250**
- **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**

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- Invoke-Obfuscation PowerShell Obfuscator. https://github.com/danielbohannon/Invoke-Obfuscation
- Invoke-CradleCrafter PowerShell remote download cradle generator and obfuscator. https://github.com/danielbohannon/Invoke-CradleCrafter
- Invoke-DOSfuscation cmd.exe Command Obfuscation Generator & Detection Test Harness. https://github.com/danielbohannon/Invoke-DOSfuscation
- morphHTA Morphing Cobalt Strike's evil.HTA. https://github.com/vysec/morphHTA
- Unicorn is a simple tool for using a PowerShell downgrade attack and inject shellcode straight into memory. https://github.com/trustedsec/unicorn
- Shellter is a dynamic shellcode injection tool, and the first truly dynamic PE infector ever created. https://www.shellterproject.com/
- EmbedInHTML Embed and hide any file in an HTML file. https://github.com/Arno0x/EmbedInHTML
- 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

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- 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
- SocialEngineeringPayloads a collection of social engineering tricks and payloads being used for credential theft and spear phishing attacks. https://github.com/bhdresh/SocialEngineeringPayloads
- The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. https://github.com/trustedsec/social-engineer-toolkit
- 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

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- WePWNise generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software. https://github.com/mwrlabs/wePWNise
- 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
- GreatSCT is an open source project to generate application white list bypasses. This tool is intended for BOTH red and blue team. https://github.com/GreatSCT/GreatSCT
- nps running powershell without powershell. https://github.com/Ben0xA/nps
- Meterpreter_Paranoid_Mode.sh allows users to secure your staged/stageless connection for Meterpreter by having it check the certificate of the handler it is connecting to. https://github.com/r00t-3xp10it/Meterpreter_Paranoid_Mode-SSL
- The Backdoor Factory (BDF) is to patch executable binaries with user desired shellcode and continue normal execution of the prepatched state. https://github.com/secretsquirrel/the-backdoor-factory
- MacroShop a collection of scripts to aid in delivering payloads via Office Macros. https://github.com/khr0x40sh/MacroShop
- UnmanagedPowerShell Executes PowerShell from an unmanaged process. https://github.com/leechristensen/UnmanagedPowerShell
- evil-ssdp Spoof SSDP replies to phish for NTLM hashes on a network. Creates a fake UPNP device, tricking users into visiting a malicious phishing page. https://gitlab.com/initstring/evil-ssdp
- Ebowla Framework for Making Environmental Keyed Payloads. https://github.com/Genetic-Malware/Ebowla

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- **make-pdf-embedded a tool to create a PDF document with an embedded file. https://github.com/DidierStevens/DidierStevensSuite/blob/master/make-pdf-embedded.py**
- **avet (AntiVirusEvasionTool) is targeting windows machines with executable files using different evasion techniques. https://github.com/govolution/avet**
- **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**
- **CallObfuscator Obfuscate windows apis from static analysis tools and debuggers. https://github.com/d35ha/CallObfuscator**
- **Donut is a shellcode generation tool that creates position-independant shellcode payloads from .NET Assemblies. This shellcode may be used to inject the Assembly into arbitrary Windows processes. https://github.com/TheWover/donut**

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Phishing

- 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
- 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
- PwnAuth a web application framework for launching and managing OAuth abuse campaigns. https://github.com/fireeye/PwnAuth
- Phishing Frenzy Ruby on Rails Phishing Framework. https://github.com/pentestgeek/phishing-frenzy
- Phishing Pretexts a library of pretexts to use on offensive phishing engagements. https://github.com/L4bF0x/PhishingPretexts
- Modlishka is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level. https://github.com/drk1wi/Modlishka
- 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
- 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

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- **Command and Control**
- Cobalt Strike is software for Adversary Simulations and Red Team Operations. https://cobaltstrike.com/
- Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. https://github.com/EmpireProject/Empire
- Metasploit Framework is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. https://github.com/rapid7/metasploit-framework
- SILENTTRINITY A post-exploitation agent powered by Python, IronPython, C#/.NET. https://github.com/byt3bl33d3r/SILENTTRINITY
- Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python. https://github.com/n1nj4sec/pupy
- Koadic or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. https://github.com/zerosum0x0/koadic
- PoshC2 is a proxy aware C2 framework written completely in PowerShell to aid penetration testers with red teaming, post-exploitation and lateral movement. https://github.com/nettitude/PoshC2_Python

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Command and Control

- Gcat a stealthy Python based backdoor that uses Gmail as a command and control server. https://github.com/byt3bl33d3r/gcat
- TrevorC2 is a legitimate website (browsable) that tunnels client/server communications for covert command execution. https://github.com/trustedsec/trevorc2
- Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang. https://github.com/Ne0nd0g/merlin
- Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you. https://github.com/quasar/QuasarRAT
- Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers. https://github.com/cobbr/Covenant
- FactionC2 is a C2 framework which use websockets based API that allows for interacting with agents and transports. https://github.com/FactionC2/
- DNScat2 is a tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol. https://github.com/iagox86/dnscat2
- Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. https://github.com/BishopFox/sliver
- EvilOSX An evil RAT (Remote Administration Tool) for macOS / OS X. https://github.com/Marten4n6/EvilOSX
- EggShell is a post exploitation surveillance tool written in Python. It gives you a command line session with extra functionality between you and a target machine. https://github.com/neoneggplant/EggShell
- https://github.com/CyberSecurityUP/Trevorfuscation

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

Staging

- Rapid Attack Infrastructure (RAI) Red Team Infrastructure... Quick... Fast... Simplified One of the most tedious phases of a Red Team Operation is usually the infrastructure setup. This usually entails a teamserver or controller, domains, redirectors, and a Phishing server. https://github.com/obscuritylabs/RAI
- Red Baron is a set of modules and custom/third-party providers for Terraform which tries to automate creating resilient, disposable, secure and agile infrastructure for Red Teams. https://github.com/byt3bl33d3r/Red-Baron
- EvilURL generate unicode evil domains for IDN Homograph Attack and detect them. https://github.com/UndeadSec/EvilURL
- Domain Hunter checks expired domains, bluecoat categorization, and Archive.org history to determine good candidates for phishing and C2 domain names. https://github.com/threatexpress/domainhunter
- PowerDNS is a simple proof of concept to demonstrate the execution of PowerShell script using DNS only. https://github.com/mdsecactivebreach/PowerDNS
- Chameleon a tool for evading Proxy categorisation. https://github.com/mdsecactivebreach/Chameleon
- CatMyFish Search for categorized domain that can be used during red teaming engagement. Perfect to setup whitelisted domain for your Cobalt Strike beacon C&C. https://github.com/Mr-Un1k0d3r/CatMyFish
- Malleable C2 is a domain specific language to redefine indicators in Beacon's communication. https://github.com/rsmudge/Malleable-C2-Profiles
- Malleable-C2-Randomizer This script randomizes Cobalt Strike Malleable C2 profiles through the use of a metalanguage, hopefully reducing the chances of flagging signature-based detection controls. https://github.com/bluscreenofjeff/Malleable-C2-Randomizer
- FindFrontableDomains search for potential frontable domains. https://github.com/rvrsh3ll/FindFrontableDomains
- Postfix-Server-Setup Setting up a phishing server is a very long and tedious process. It can take hours to setup, and can be compromised in minutes. https://github.com/n0pe-sled/Postfix-Server-Setup

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- DomainFrontingLists a list of Domain Frontable Domains by CDN. https://github.com/vysec/DomainFrontingLists
- Apache2-Mod-Rewrite-Setup Quickly Implement Mod-Rewrite in your infastructure. https://github.com/n0pe-sled/Apache2-Mod-Rewrite-Setup
- mod_rewrite rule to evade vendor sandboxes. https://gist.github.com/curi0usJack/971385e8334e189d93a6cb4671238b10
- external_c2 framework a python framework for usage with Cobalt Strike's External C2. https://github.com/Und3rf10w/external_c2_framework
- Malleable-C2-Profiles A collection of profiles used in different projects using Cobalt Strike https://www.cobaltstrike.com/. https://github.com/xx0hcd/Malleable-C2-Profiles
- ExternalC2 a library for integrating communication channels with the Cobalt Strike External C2 server. https://github.com/ryhanson/ExternalC2

Adversary Emulation and Cracking The Perimeter: Auxiliary Tools

- cs2modrewrite a tools for convert Cobalt Strike profiles to modrewrite scripts. https://github.com/threatexpress/cs2modrewrite
- e2modrewrite a tools for convert Empire profiles to Apache modrewrite scripts. https://github.com/infosecn1nja/e2modrewrite
- redi automated script for setting up CobaltStrike redirectors (nginx reverse proxy, letsencrypt). https://github.com/taherio/redi
- cat-sites Library of sites for categorization. https://github.com/audrummer15/cat-sites
- ycsm is a quick script installation for resilient redirector using nginx reverse proxy and letsencrypt compatible with some popular Post-Ex Tools (Cobalt Strike, Empire, Metasploit, PoshC2). https://github.com/infosecn1nja/ycsm
- Domain Fronting Google App Engine. https://github.com/redteam-cyberark/Google-Domain-fronting
- DomainFrontDiscover Scripts and results for finding domain frontable CloudFront domains. https://github.com/peewpw/DomainFrontDiscover
- Automated Empire Infrastructure https://github.com/bneg/RedTeam-Automation
- Serving Random Payloads with NGINX. https://gist.github.com/jivoi/a33ace2e25515a31aa2ffbae246d98c9
- meek is a blocking-resistant pluggable transport for Tor. It encodes a data stream as a sequence of HTTPS requests and responses. https://github.com/arlolra/meek
- CobaltStrike-ToolKit Some useful scripts for CobaltStrike. https://github.com/killswitch-GUI/CobaltStrike-ToolKit
- mkhtaccess_red Auto-generate an HTaccess for payload delivery -- automatically pulls ips/nets/etc from known sandbox companies/sources that have been seen before, and redirects them to a benign payload. https://github.com/violentlydave/mkhtaccess_red
- RedFile a flask wsgi application that serves files with intelligence, good for serving conditional RedTeam payloads. https://github.com/outflanknl/RedFile
- keyserver Easily serve HTTP and DNS keys for proper payload protection. https://github.com/leoloobeek/keyserver
- DoHC2 allows the ExternalC2 library from Ryan Hanson (https://github.com/ryhanson/ExternalC2) to be leveraged for command and control (C2) via DNS over HTTPS (DoH). This is built for the popular Adversary Simulation and Red Team Operations Software Cobalt Strike (https://www.cobaltstrike.com). https://github.com/SpiderLabs/DoHC2
- HTran is a connection bouncer, a kind of proxy server. A “listener” program is hacked stealthily onto an unsuspecting host anywhere on the Internet. https://github.com/HiwinCN/HTran

Adversary Emulation Tools

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

C2 Matrix

- Ares
- AsyncRAT-C#
- BabyShark
- BlackMamba
- Brute Ratel
- C3
- CALDERA
- Callidus
- CHAOS
- Cobalt Strike
- Covenant
- Dali
- DarkFinger
- DBC2
- DeimosC2
- Eggshell
- Empire
- EvilOSX
- Faction C2
- FlyingAFalseFlag
- FudgeC2
- godoh
- GRAT2
- HARS
- HTTP-RevShell
- ibombshell
- INNUENDO
- Koadic C3
- MacC2
- MacShellSwift
- Merlin
- Metasploit
- Meterpeter
- MicroBackdoor
- MikeC2
- Mistica
- Mythic
- Ninja
- NorthStarC2
- Nuages
- Octopus
- Oyabun C2
- PetaQ
- PoshC2
- PowerHub
- Prelude
- Prismatica
- Proton
- Pupy
- QuasarRAT
- RATel
- Red Team Toolkit
- redViper
- ReverseTCPShell
- sak1to-shell
- SCYTHE
- Serpentine
- Shad0w
- Shadow Workers
- SharpC2
- SilentTrinity
- SK8PARK/RAT
- Slack-C2Bot
- Slackor
- Sliver
- Throwback
- ThunderShell
- Trevor C2
- Void-RAT
- Voodoo
- WEASEL

Adversary Emulation Training

- https://www.sans.org/cyber-security-courses/red-team-exercises-adversary-emulation/
- https://specterops.io/what-we-do/adversary-simulation
- https://training.teamares.io/
- https://adversaryemulation.com/course-red-team-adversary-emulation-101
- https://www.mdsec.co.uk/training/adversary-simulation-red-team-tactics/
- https://obscuritylabs.com/adversary-emulation/
- https://www.loopsec.com.au/solutions/offensive-security-services/adversary-simulation-training
- https://attackiq.com/