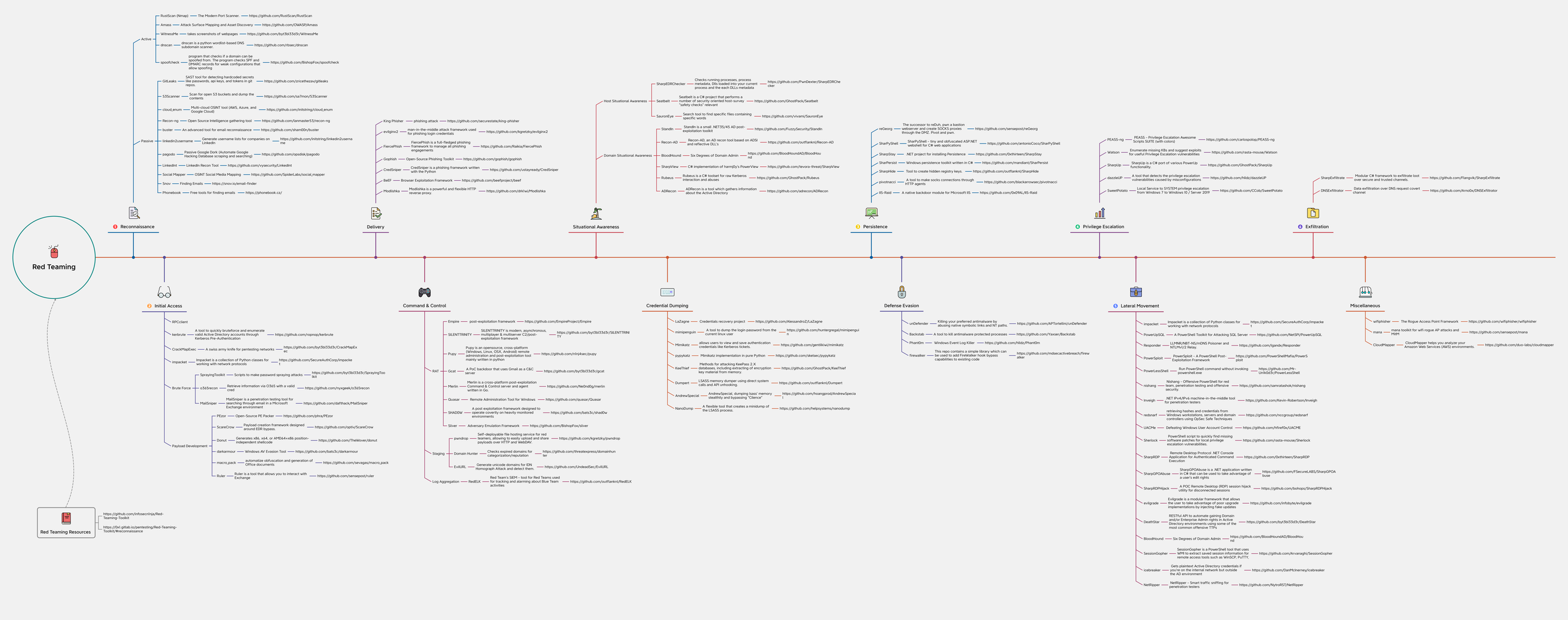
Red Teaming
1 Reconnaissance
Active
RustScan (Nmap) — The Modern Port Scanner. — https://github.com/RustScan/RustScan
Amass — Attack Surface Mapping and Asset Discovery — https://github.com/OWASP/Amass
WitnessMe — takes screenshots of webpages — https://github.com/byt3bl33d3r/WitnessMe
dnscan — dnscan is a python wordlist-based DNS subdomain scanner. — https://github.com/rbsec/dnscan
spoofcheck — 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
Passive
GitLeaks — SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos. — https://github.com/zricethezav/gitleaks
S3Scanner — Scan for open S3 buckets and dump the contents — https://github.com/sa7mon/S3Scanner
cloud_enum — Multi-cloud OSINT tool (AWS, Azure, and Google Cloud) — https://github.com/initstring/cloud_enum
Recon-ng — Open Source Intelligence gathering tool — https://github.com/lanmaster53/recon-ng
buster — An advanced tool for email reconnaissance — https://github.com/sham00n/buster
linkedin2username — Generate username lists for companies on LinkedIn — https://github.com/initstring/linkedin2username
pagodo — Passive Google Dork (Automate Google Hacking Database scraping and searching) — https://github.com/opsdisk/pagodo
LinkedInt — LinkedIn Recon Tool — https://github.com/vysecurity/LinkedInt
Social Mapper — OSINT Social Media Mapping — https://github.com/SpiderLabs/social_mapper
Snov — Finding Emails — https://snov.io/email-finder
Phonebook — Free tools for finding emails — https://phonebook.cz/
Delivery
King Phisher — phishing attack — https://github.com/securestate/king-phisher
evilginx2 — man-in-the-middle attack framework used for phishing login credentials — https://github.com/kgretzky/evilginx2
FiercePhish — FiercePhish is a full-fledged phishing framework to manage all phishing engagements — https://github.com/Raikia/FiercePhish
Gophish — Open-Source Phishing Toolkit — https://github.com/gophish/gophish
CredSniper — CredSniper is a phishing framework written with the Python — https://github.com/ustayready/CredSniper
BeEF — Browser Exploitation Framework — https://github.com/beefproject/beef
Modlishka — Modlishka is a powerful and flexible HTTP reverse proxy. — https://github.com/drk1wi/Modlishka
Situational Awareness
Host Situational Awareness
SharpEDRChecker — Checks running processes, process metadata, Dlls loaded into your current process and the each DLLs metadata — https://github.com/PwnDexter/SharpEDRChecker
Seatbelt — Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant — https://github.com/GhostPack/Seatbelt
SauronEye — Search tool to find specific files containing specific words — https://github.com/vivami/SauronEye
Domain Situational Awareness
Standin — Standin is a small .NET35/45 AD post-exploitation toolkit — https://github.com/FuzzySecurity/Standin
Recon-AD — Recon-AD, an AD recon tool based on ADSI and reflective DLL's — https://github.com/outflanknl/Recon-AD
BloodHound — Six Degrees of Domain Admin — https://github.com/BloodHoundAD/BloodHound
SharpView — C# implementation of harmj0y's PowerView — https://github.com/tevora-threat/SharpView
Rubeus — Rubeus is a C# toolset for raw Kerberos interaction and abuses — https://github.com/GhostPack/Rubeus
ADRecon — ADRecon is a tool which gathers information about the Active Directory — https://github.com/adrecon/ADRecon
3 Persistence
reGeorg — The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn. — https://github.com/sensepost/reGeorg
SharPyShell — SharPyShell - tiny and obfuscated ASP.NET webshell for C# web applications — https://github.com/antonioCoco/SharPyShell
SharpStay — .NET project for installing Persistence — https://github.com/0xthirteen/SharpStay
SharPersist — Windows persistence toolkit written in C# — https://github.com/mandiant/SharPersist
SharpHide — Tool to create hidden registry keys. — https://github.com/outflanknl/SharpHide
pivotnacci — A tool to make socks connections through HTTP agents — https://github.com/blackarrowsec/pivotnacci
IIS-Raid — A native backdoor module for Microsoft IIS — https://github.com/0x09AL/IIS-Raid
4 Privilege Escalation
PEASS-ng — PEASS - Privilege Escalation Awesome Scripts SUITE (with colors) — https://github.com/carlospolop/PEASS-ng
Watson — Enumerate missing KBs and suggest exploits for useful Privilege Escalation vulnerabilities — https://github.com/rasta-mouse/Watson
SharpUp — SharpUp is a C# port of various PowerUp functionality. — https://github.com/GhostPack/SharpUp
dazzleUP — A tool that detects the privilege escalation vulnerabilities caused by misconfigurations — https://github.com/hlldz/dazzleUP
SweetPotato — Local Service to SYSTEM privilege escalation from Windows 7 to Windows 10 / Server 2019 — https://github.com/CCob/SweetPotato
5 Exfiltration
SharpExfiltrate — Modular C# framework to exfiltrate loot over secure and trusted channels. — https://github.com/Flangvik/SharpExfiltrate
DNSExfiltrator — Data exfiltration over DNS request covert channel — https://github.com/Arno0x/DNSExfiltrator
2 Initial Access
RPCclient
kerbrute — A tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication — https://github.com/ropnop/kerbrute
CrackMapExec — A swiss army knife for pentesting networks — https://github.com/byt3bl33d3r/CrackMapExec
impacket — Impacket is a collection of Python classes for working with network protocols — https://github.com/SecureAuthCorp/impacket
Brute Force
o365recon — Retrieve information via O365 with a valid cred — https://github.com/nyxgeek/o365recon
MailSniper — MailSniper is a penetration testing tool for searching through email in a Microsoft Exchange environment — https://github.com/dafthack/MailSniper
SprayingToolkit — Scripts to make password spraying attacks — https://github.com/byt3bl33d3r/SprayingToolkit
Payload Development
PEzor — Open-Source PE Packer — https://github.com/phra/PEzor
ScareCrow — Payload creation framework designed around EDR bypass. — https://github.com/optiv/ScareCrow
Donut — Generates x86, x64, or AMD64+x86 position-independent shellcode — https://github.com/TheWover/donut
darkarmour — Windows AV Evasion Tool — https://github.com/bats3c/darkarmour
macro_pack — automatize obfuscation and generation of Office documents — https://github.com/sevagas/macro_pack
Ruler — Ruler is a tool that allows you to interact with Exchange — https://github.com/sensepost/ruler
Command & Control
RAT
Empire — post-exploitation framework — https://github.com/EmpireProject/Empire
SILENTTRINITY — SILENTTRINITY is modern, asynchronous, multiplayer & multiserver C2/post-exploitation framework — https://github.com/byt3bl33d3r/SILENTTRINITY
Pupy — Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python — https://github.com/n1nj4sec/pupy
Gcat — A PoC backdoor that uses Gmail as a C&C server — https://github.com/byt3bl33d3r/gcat
Merlin — Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go. — https://github.com/Ne0nd0g/merlin
Quasar — Remote Administration Tool for Windows — https://github.com/quasar/Quasar
SHADOW — A post exploitation framework designed to operate covertly on heavily monitored environments — https://github.com/bats3c/shadow
Sliver — Adversary Emulation Framework — https://github.com/BishopFox/sliver
Staging
pwndrop — Self-deployable file hosting service for red teamers, allowing to easily upload and share payloads over HTTP and WebDAV. — https://github.com/kgretzky/pwndrop
Domain Hunter — Checks expired domains for categorization/reputation — https://github.com/threatexpress/domainhunter
EvilURL — Generate unicode domains for IDN Homograph Attack and detect them. — https://github.com/UndeadSec/EvilURL
Log Aggregation
RedELK — Red Team's SIEM - tool for Red Teams used for tracking and alarming about Blue Team activities — https://github.com/outflanknl/RedELK
Credential Dumping
LaZagne — Credentials recovery project — https://github.com/AlessandroZ/LaZagne
mimipenguin — A tool to dump the login password from the current linux user — https://github.com/huntergregal/mimipenguin
Mimikatz — allows users to view and save authentication credentials like Kerberos tickets. — https://github.com/gentilkiwi/mimikatz
pypykatz — Mimikatz implementation in pure Python — https://github.com/skelsec/pypykatz
KeeThief — Methods for attacking KeePass 2.X databases, including extracting of encryption key material from memory. — https://github.com/GhostPack/KeeThief
Dumpert — LSASS memory dumper using direct system calls and API unhooking. — https://github.com/outflanknl/Dumpert
AndrewSpecial — AndrewSpecial, dumping lsass' memory stealthily and bypassing "Clience" — https://github.com/hoangprod/AndrewSpecial
NanoDump — A flexible tool that creates a minidump of the LSASS process. — https://github.com/helpsystems/nanodump
Defense Evasion
unDefender — Killing your preferred antimalware by abusing native symbolic links and NT paths. — https://github.com/APTortellini/unDefender
Backstab — A tool to kill antimalware protected processes — https://github.com/Yaxser/Backstab
PhantDm — Windows Event Log Killer — https://github.com/hlldz/PhantDm
firewalker — This repo contains a simple library which can be used to add FireWalker hook bypass capabilities to existing code — https://github.com/mdsecactivebreach/firewalker
6 Lateral Movement
impacket — Impacket is a collection of Python classes for working with network protocols — https://github.com/SecureAuthCorp/impacket
PowerUpSQL — A PowerShell Toolkit for Attacking SQL Server — https://github.com/NetSPI/PowerUpSQL
Responder — LLMNR/NBT-NS/mDNS Poisoner and NTLMv1/2 Relay. — https://github.com/lgandx/Responder
PowerSploit — PowerSploit - A PowerShell Post-Exploitation Framework — https://github.com/PowerShellMafia/PowerSploit
PowerLessShell — Run PowerShell command without invoking powershell.exe — https://github.com/Mr-Un1k0d3r/PowerLessShell
nishang — Nishang - Offensive PowerShell for red team, penetration testing and offensive security. — https://github.com/samratashok/nishang
Inveigh — .NET IPv4/IPv6 machine-in-the-middle tool for penetration testers — https://github.com/Kevin-Robertson/Inveigh
rednarf — retrieving hashes and credentials from Windows workstations, servers and domain controllers using OpSec Safe Techniques — https://github.com/nccgroup/rednarf
UACMe — Defeating Windows User Account Control — https://github.com/hfiref0x/UACME
Sherlock — PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities. — https://github.com/rasta-mouse/Sherlock
SharpRDP — Remote Desktop Protocol .NET Console Application for Authenticated Command Execution — https://github.com/0xthirteen/SharpRDP
SharpGPOAbuse — SharpGPOAbuse is a .NET application written in C# that can be used to take advantage of a user's edit rights — https://github.com/FSecureLABS/SharpGPOAbuse
SharpRDPHijack — A POC Remote Desktop (RDP) session hijack utility for disconnected sessions — https://github.com/bohops/SharpRDPHijack
evilgrade — Evilgrade is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates — https://github.com/infobyte/evilgrade
DeathStar — RESTful API to automate gaining Domain and/or Enterprise Admin rights in Active Directory environments using some of the most common offensive TTPs — https://github.com/byt3bl33d3r/DeathStar
BloodHound — Six Degrees of Domain Admin — https://github.com/BloodHoundAD/BloodHound
SessionGopher — SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY. — https://github.com/Arvanaghi/SessionGopher
icebreaker — Gets plaintext Active Directory credentials if you're on the internal network but outside the AD environment — https://github.com/DanMcInerney/icebreaker
NetRipper — NetRipper - Smart traffic sniffing for penetration testers — https://github.com/NytroRST/NetRipper
Miscellaneous
wifiphisher — The Rogue Access Point Framework — https://github.com/wifiphisher/wifiphisher
mana — mana toolkit for wifi rogue AP attacks and MitM — https://github.com/sensepost/mana
CloudMapper — CloudMapper helps you analyze your Amazon Web Services (AWS) environments. — https://github.com/duo-labs/cloudmapper
Red Teaming Resources
https://github.com/infosecn/pa/Red-Teaming-Toolkit
https://0x1.gitlab.io/pentesting/Red-Teaming-Toolkit/#reconnaissance