Red Team and PENTEST

@ANHKWAR

knowledge requirements

These are the basic competencies expected (and tested for during the 1st in person interview) by a large, very visible InfoSec company I think it is a good base competency list for anyone looking to get into an InfoSec career (with specialization plus and some programming /scripting ability) or learn cybersecurity/hacking as a hobby:

Networking:

1. Good understanding of OSI layer model
2. Understating of communication flow through each layer
3. Good understanding of functions of each layer
4. Understanding of major protocols in each layer
5. In-depth understanding Layer 3 & Layer 4 protocols, IP, ICMP (layer 3) TCP, UDP Protocols (layer 4).

Overview of TCP/IP Layer model:

1. ARP / Understanding of Client & Server communication model
2. Ports common services run on Ephemeral port vs Well known ports.

Understanding of major (everyday Layer 7) services/protocols:

1. DNS
2. DHCP
3. HTTP
4. HTTP Header
5. Fields HTTP Status Codes
6. HTTP maintains state
7. HTTPS vs HTTP o FTP.

Active vs Passive data transfer:

1. SSH / SSH handshake
2. Telnet /Telnet Handshake
3. SMTP / SMTP handshake (Mail from/ rcpt to) / How attachments are handled Network.

Troubleshooting Methodology:

1. Understanding of Network Address Translation (NAT)
2. Understanding of Port Address Translation (PAT)
3. Understanding of Proxies / Overview of Virtual Private Networks (VPNs)

Understand which device operates at which OSI layer:

1. Hub - Switch Managed
2. Unmanaged - Firewall - IDS/IPS

Ability to read devices logs:

1. IDS/IPS
2. Firewall
3. Windows

Advanced Concepts (Possible Self Study Topics):

1. Content Delivery Networks (CDNs)
2. HTTP Pipelining
3. IPv4 vs IPv6 addressing scheme
4. IPv4 and IPv6 differences(cont'd) Security

Security Device Operations:

1. Understanding of IDS/IPS technologies
2. Signature vs Anomaly based
3. HIDS vs NIDS
4. How Snort works / How IPS systems prevent attacks
5. Drop packets o TCP reset

Security Attacks:

1. Detailed understanding of common web attacks
2. SQL Injection / Blind o Cross Site Scripting, Stored, Reflected, DOM
3. Cross Site Request Forgery
4. Local File Inclusion
5. Remote File Inclusion
6. Basic understanding of buffer overflow
7. Denial of Service
8. Remote Code Execution / PHP attacks
9. Heartbleed
10. Shellshock
11. Brute Force attacks

Understanding of the Malware Kill Chain:

1. Worm vs Trojan
2. Phishing email/Landing redirect page
3. Exploit Kit
4. Malware Download

5. Malware Install
6. Phone Home
7. Data Exfiltration/Command and Control

Linux Overview of file structure:

1. Knowledge of file systems used NTFS, FAT vs ext2/3/4
2. Overview of a journaling file system

The Shell:

1. Executing commands and command options
2. Interactive features: job control, history
3. File Utilities (cp, mv, rm, etc.)
4. Editors: vi/vim vimtutor (Homework) / Process Utilities (PS, kill, wait, sleep)
5. Filters: cat, head, tail, sort, uniq

Basic Training

General/Basic Exploitation:

1. http://www.pentest-standard.org/index.php/Main_Page
2. https://www.offensive-security.com/metasploit-unleashed/
3. http://null-byte.wonderhowto.com/how-to/metasploit-basics/
4. https://www.owasp.org/index.php/Main_Page
5. https://github.com/nixawk/pentest-wiki
6. https://github.com/beefproject/beef
7. https://portswigger.net/burp/
8. https://www.metasploit.com/
9. http://exploitpack.com/
10. https://github.com/commixproject/commix
11. https://github.com/reverse-shell/routersploit

Distros:

1. https://www.kali.org/
2. https://www.blackarch.org/
3. https://www.parrotsec.org/

Vulnscanner/Sniffer/Tools/Web Exploitation

1. http://www.askapache.com/security/computer-security-toolbox-2/#common_security_programs
2. https://pastebin.com/kP04r4PM
3. http://www.irongeek.com/i.php?page=backtrack-r1-man-pages/netdiscover
4. http://www.tenable.com/products/nessus-vulnerability-scanner
5. https://www.rapid7.com/products/nexpose/

6. https://cirt.net/nikto2
7. https://nmap.org/
8. https://github.com/netsniff-ng/netsniff-ng
9. https://www.wireshark.org/
10. https://github.com/fwaeytens/dnsenum/
11. https://github.com/makefu/dnsmap/
12. http://www.tcpdump.org/
13. http://sqlmap.org/
14. https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project
15. https://wpscan.org/
16. http://networksecuritytoolkit.org/nst/index.html
17. https://github.com/droope/droopescan
18. https://github.com/andresriancho/w3af
19. https://www.netsparker.com/

Password Cracker

1. http://www.openwall.com/john/
2. http://hashcat.net/hashcat/

Online Tools

1. http://crackstation.net
2. http://www.tcpiputils.com/
3. https://shodan.io

Exploits (Exploit/Vulnerability Databases)

1. https://exploit-db.com/
2. http://kernel-exploits.com
3. https://github.com/PenturaLabs/Linux_Exploit_Suggester
4. https://nvd.nist.gov/
5. https://www.us-cert.gov/
6. https://blog.osvdb.org/
7. http://www.securityfocus.com/
8. http://seclists.org/fulldisclosure/
9. https://technet.microsoft.com/en-us/security/bulletins
10. https://technet.microsoft.com/en-us/security/advisories
11. https://packetstormsecurity.com/
12. http://www.securiteam.com/
13. http://cxsecurity.com/
14. https://www.vulnerability-lab.com/

Payloads/Reverse Shells

1. https://www.veil-framework.com/framework/veil-evasion/
2. http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
3. https://highon.coffee/blog/reverse-shell-cheat-sheet/

CTF

1. https://www.vulnhub.com/
2. https://www.wechall.net/about_wechall
3. https://picoctf.org/
4. https://tryhackme.com/
5. https://www.hackthissite.org/
6. https://www.hackthebox.com/
7. https://pwnable.tw/challenge/
8. https://overthewire.org/wargames/
9. https://w3challs.com/challenges/list/web
10. https://ringzer0ctf.com/challenges
11. https://ctf.komodosec.com/rules.php
12. https://www.root-me.org/?lang=en
13. https://hacking-lab.com/index.html
14. https://pwnable.tw/challenge/
15. https://halls-of-valhalla.org/beta/challenges
16. https://redtiger.labs.overthewire.org/

Info/Blogs/Techniques/etc.

1. http://wiki.bash-hackers.org/scripting/style
2. https://www.corelan.be/index.php/articles/
3. https://www.veracode.com/security/xss
4. http://www.thegeekstuff.com/2012/02/xss-attack-examples/
5. https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
6. https://thehackernews.com/
7. http://securityidiots.com/Web-Pentest/SQL-Injection/Basic-Union-Based-SQL-Injection.html
8. https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/
9. https://hakin9.org/voip-hacking-techniques/

Lists

1. https://code.google.com/archive/p/hacktooldepot/downloads
2. http://tools.kali.org/tools-listing
3. http://sectools.org/
4. https://github.com/fffaraz/awesome-cpp
5. https://github.com/alebcay/awesome-shell
6. https://github.com/dreikanter/ruby-bookmarks
7. https://github.com/sorrycc/awesome-javascript
8. https://github.com/sindresorhus/awesome-nodejs
9. https://github.com/dloss/python-pentest-tools
10. https://github.com/ashishb/android-security-awesome
11. https://github.com/bayandin/awesome-awesomeness
12. https://github.com/paragonie/awesome-appsec
13. https://github.com/apsdehal/awesome-ctf
14. https://github.com/carpedm20/awesome-hacking
15. https://github.com/paralax/awesome-honeypots
16. https://github.com/clowwindy/Awesome-Networking

17. https://github.com/onlurking/awesome-infosec
18. https://github.com/rshipp/awesome-malware-analysis
19. https://github.com/caesar0301/awesome-pcaptools
20. https://github.com/sbilly/awesome-security
21. https://github.com/sindresorhus/awesome
22. https://github.com/danielmiessler/SecLists
23. https://github.com/PaulSec/awesome-sec-talks

Red Teaming

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.

Reconnaissance

Name	Description	URL
RustScan	The Modern Port Scanner. Find ports quickly (3 seconds at its fastest). Run scripts through our scripting engine (Python, Lua, Shell supported).	https://github.com/RustScan/RustScan
Amass	In-depth Attack Surface Mapping and Asset Discovery	https://github.com/OWASP/Amass
gitleaks	Gitleaks is a SAST tool for detecting hardcoded secrets like passwords, api keys, and tokens in git repos.	https://github.com/zricethezav/gitleaks
S3Scanner	Scan for open S3 buckets and dump the contents	https://github.com/sa7mon/S3Scanner
cloud_enum	Multi-cloud OSINT tool. Enumerate public resources in AWS, Azure, and Google Cloud.	https://github.com/initstring/cloud_enum
Recon-ng	Open Source Intelligence gathering tool aimed at reducing the time spent harvesting information from open sources.	https://github.com/lanmaster53/recon-ng
buster	An advanced tool for email reconnaissance	https://github.com/sham00n/buster
linkedin2username	OSINT Tool: Generate username lists for companies on LinkedIn	https://github.com/initstring/linkedin2username

Name	Description	URL
WitnessMe	Web Inventory tool, takes screenshots of webpages using Pyppeteer (headless Chrome/Chromium) and provides some extra bells & whistles to make life easier.	https://github.com/byt3bl33d3r/WitnessMe
pagodo	pagodo (Passive Google Dork) - Automate Google Hacking Database scraping and searching	https://github.com/opsdisk/pagodo
AttackSurfaceMapper	AttackSurfaceMapper is a tool that aims to automate the reconnaissance process.	https://github.com/superhedgy/AttackSurfaceMapper
SpiderFoot	SpiderFoot is an open source intelligence (OSINT) automation tool. It integrates with just about every data source available and utilises a range of methods for data analysis, making that data easy to navigate.	https://github.com/smicallef/spiderfoot
dnscan	dnscan is a python wordlist-based DNS subdomain scanner.	https://github.com/rbsec/dnscan
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
LinkedInt	LinkedIn Recon Tool	https://github.com/vysecurity/LinkedInt

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://github.com/byt3bl33d3r/SprayingToolkit
o365recon	Retrieve information via O365 with a valid cred	https://github.com/nyxgeek/o365recon

Payload Development

Name	Description	URL
PEzor	Open-Source PE Packer	https://github.com/phra/PEzor
GadgetToJScript	A tool for generating .NET serialized gadgets that can trigger .NET assembly load/execution when deserialized using BinaryFormatter from JS/VBS/VBA scripts.	https://github.com/med0x2e/GadgetToJScript
ScareCrow	Payload creation framework designed around EDR bypass.	https://github.com/optiv/ScareCrow
Donut	Donut is a position-independent code that enables in-memory execution of VBScript, JScript, EXE, DLL files and dotNET assemblies.	https://github.com/TheWover/donut
Mystikal	macOS Initial Access Payload Generator	https://github.com/D00MFist/Mystikal
charlotte	c++ fully undetected shellcode launcher ;)	https://github.com/9emin1/charlotte
InvisibilityCloak	Proof-of-concept obfuscation toolkit for C# post-exploitation tools. This will perform the below actions for a C# visual studio project.	https://github.com/xforcered/InvisibilityCloak
Dendrobate	Dendrobate is a framework that facilitates the development of payloads that hook unmanaged code through managed .NET code.	https://github.com/FuzzySecurity/Dendrobate
Offensive VBA and XLS Entanglement	This repo provides examples of how VBA can be used for offensive purposes beyond a simple dropper or shell injector. As we develop more use cases, the repo will be updated.	https://github.com/BC-SECURITY/Offensive-VBA-and-XLS-Entanglement
xlsGen	Tiny Excel BIFF8 Generator, to Embedded 4.0 Macros in *.xls	https://github.com/aaaddress1/xlsGen
darkarmour	Windows AV Evasion	https://github.com/bats3c/darkarmour

Name	Description	URL
InlineWhispers	Tool for working with Direct System Calls in Cobalt Strike's Beacon Object Files (BOF)	https://github.com/outflanknl/InlineWhispers
EvilClippy	A cross-platform assistant for creating malicious MS Office documents. Can hide VBA macros, stomp VBA code (via P-Code) and confuse macro analysis tools. Runs on Linux, OSX and Windows.	https://github.com/outflanknl/EvilClippy
OfficePurge	VBA purge your Office documents with OfficePurge. VBA purging removes P-code from module streams within Office documents.	https://github.com/fireeye/OfficePurge
ThreatCheck	Identifies the bytes that Microsoft Defender / AMSI Consumer flags on.	https://github.com/rasta-mouse/ThreatCheck
CrossC2	Generate CobaltStrike's cross-platform payload	https://github.com/gloxec/CrossC2
Ruler	Ruler is a tool that allows you to interact with Exchange servers remotely, through either the MAPI/HTTP or RPC/HTTP protocol.	https://github.com/sensepost/ruler
DueDLLigence	Shellcode runner framework for application whitelisting bypasses and DLL side-loading. The shellcode included in this project spawns calc.exe.	https://github.com/fireeye/DueDLLigence
RuralBishop	RuralBishop is practically a carbon copy of UrbanBishop by b33f, but all P/Invoke calls have been replaced with D/Invoke.	https://github.com/rasta-mouse/RuralBishop
TikiTorch	TikiTorch was named in homage to CACTUSTORCH by Vincent Yiu. The basic concept of CACTUSTORCH is that it spawns a new process, allocates a region of memory, then uses CreateRemoteThread to run the	https://github.com/rasta-mouse/TikiTorch

Name	Description	URL
	desired shellcode within that target process. Both the process and shellcode are specified by the user.	
SharpShooter	SharpShooter is a payload creation framework for the retrieval and execution of arbitrary CSharp source code. SharpShooter is capable of creating payloads in a variety of formats, including HTA, JS, VBS and WSF.	https://github.com/mdsecactivebreach/SharpShooter
SharpSploit	SharpSploit is a .NET post-exploitation library written in C#	https://github.com/cobbr/SharpSploit
MSBuildAPICaller	MSBuild Without MSBuild.exe	https://github.com/rvrsh3ll/MSBuildAPICaller
macro_pack	macro_pack is a tool by @EmericNasi used to automatize obfuscation and generation of MS Office documents, VB scripts, and other formats for pentest, demo, and social engineering assessments.	https://github.com/sevagas/macro_pack
inceptor	Template-Driven AV/EDR Evasion Framework	https://github.com/klezVirus/inceptor

Delivery Phishing

Name	Description	URL
o365-attack-toolkit	A toolkit to attack Office365	https://github.com/mdsecactivebreach/o365-attack-toolkit
Evilginx2	Evilginx2 is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service.	https://github.com/kgretzky/evilginx2
Gophish	Gophish is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly	https://github.com/gophish/gophish

Name	Description	URL
	and easily setup and execute phishing engagements and security awareness training.	
PwnAuth	PwnAuth a web application framework for launching and managing OAuth abuse campaigns.	https://github.com/fireeye/PwnAuth
Modlishka	Modlishka is a flexible and powerful reverse proxy, that will take your ethical phishing campaigns to the next level.	https://github.com/drk1wi/Modlishka

Watering Hole Attack

Name	Description	URL
BeEF	BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser	https://github.com/beefproject/beef

Command and Control Remote Access Tools (RAT)

Name	Description	URL
Cobalt Strike	Cobalt Strike is software for Adversary Simulations and Red Team Operations.	https://cobaltstrike.com/
Empire	Empire 3 is a post-exploitation framework that includes a pure-PowerShell Windows agent, and compatibility with Python 3.x Linux/OS X agents.	https://github.com/BC-SECURITY/Empire
PoshC2	PoshC2 is a proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement.	https://github.com/nettitude/PoshC2

Name	Description	URL
Koadic	Koadic C3 COM Command & Control - JScript RAT	https://github.com/zerosum0x0/koadic
merlin	Merlin is a cross-platform post-exploitation Command & Control server and agent written in Go.	https://github.com/Ne0nd0g/merlin
Mythic	A cross-platform, post-exploit, red teaming framework built with python3, docker, docker-compose, and a web browser UI.	https://github.com/its-a-feature/Mythic
Covenant	Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.	https://github.com/cobbr/Covenant
shad0w	A post exploitation framework designed to operate covertly on heavily monitored environments	https://github.com/bats3c/shad0w
Sliver	Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS.	https://github.com/BishopFox/sliver
SILENTTRINITY	An asynchronous, collaborative post-exploitation agent powered by Python and .NET's DLR	https://github.com/byt3bl33d3r/SILENTTRINITY
Pupy	Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python	https://github.com/n1nj4sec/pupy

Staging

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

Name	Description	URL
Cobalt Strike Malleable C2 Design and Reference Guide	Cobalt Strike Malleable C2 Design and Reference Guide	https://github.com/threatexpress/malleable-c2/
redirect.rules	Quick and dirty dynamic redirect.rules generator	https://github.com/0xZDH/redirect.rules

Log Aggregation

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

Situational Awareness Host Situational Awareness

Name	Description	URL
AggressiveProxy	AggressiveProxy is a combination of a .NET 3.5 binary (LetMeOutSharp) and a Cobalt Strike aggressor script (AggressiveProxy.cna). Once LetMeOutSharp is executed on a workstation, it will try to enumerate all available proxy configurations and try to communicate with the Cobalt Strike server over HTTP(s) using the identified proxy configurations.	https://github.com/EncodeGroup/AggressiveProxy
Gopher	C# tool to discover low hanging fruits	https://github.com/EncodeGroup/Gopher

Name	Description	URL
SharpEDRChecker	Checks running processes, process metadata, Dlls loaded into your current process and the each DLLs metadata, common install directories, installed services and each service binaries metadata, installed drivers and each drivers metadata, all for the presence of known defensive products such as AV's, EDR's and logging tools.	https://github.com/PwnDexter/SharpEDRChecker
Situational Awareness BOF	This Repo intends to serve two purposes. First it provides a nice set of basic situational awareness commands implemented in BOF.	https://github.com/trustedsec/CS-Situational-Awareness-BOF
Seatbelt	Seatbelt is a C# project that performs a number of security oriented host-survey "safety checks" relevant from both offensive and defensive security perspectives.	https://github.com/GhostPack/Seatbelt
SauronEye	SauronEye is a search tool built to aid red teams in finding files containing specific keywords.	https://github.com/vivami/SauronEye
SharpShares	Multithreaded C# .NET Assembly to enumerate accessible network shares in a domain	https://github.com/mitchmoser/SharpShares
SharpAppLocker	C# port of the Get-AppLockerPolicy PowerShell cmdlet with extended features. Includes the ability to filter and search for a specific type of rules and actions.	https://github.com/Flangvik/SharpAppLocker/
SharpPrinter	Printer is a modified and console version of ListNetworks	https://github.com/rvrsh3ll/SharpPrinter

Domain Situational Awareness

Name	Description	URL
StandIn	StandIn is a small AD post-compromise toolkit. StandIn came about because recently at xforcered we needed a .NET native solution to perform resource based constrained delegation.	https://github.com/FuzzySecurity/StandIn
Recon-AD	An AD recon tool based on ADSI and reflective DLL's	https://github.com/outflanknl/Recon-AD
BloodHound	Six Degrees of Domain Admin	https://github.com/BloodHoundAD/BloodHound
PSPKIAudit	PowerShell toolkit for auditing Active Directory Certificate Services (AD CS).	https://github.com/GhostPack/PSPKIAudit
SharpView	C# implementation of harmj0y's PowerView	https://github.com/tevora-threat/SharpView
Rubeus	Rubeus is a C# toolset for raw Kerberos interaction and abuses. It is heavily adapted from Benjamin Delpy's Kekeo project (CC BY-NC-SA 4.0 license) and Vincent LE TOUX's MakeMeEnterpriseAdmin project (GPL v3.0 license).	https://github.com/GhostPack/Rubeus
Grouper	A PowerShell script for helping to find vulnerable settings in AD Group Policy. (deprecated, use Grouper2 instead!)	https://github.com/l0ss/Grouper
ImproHound	Identify the attack paths in BloodHound breaking your AD tiering	https://github.com/improsec/ImproHound
ADRecon	ADRecon is a tool which gathers information about the Active Directory and generates a report which can provide a holistic picture of the current state of the target AD environment.	https://github.com/adrecon/ADRecon
ADCSPwn	A tool to escalate privileges in an active directory network by coercing authenticate from machine accounts (Petitpotam) and relaying to the certificate service.	https://github.com/bats3c/ADCSPwn

Credential Dumping

Name	Description	URL
Mimikatz	Mimikatz is an open-source application that allows users to view and save authentication credentials like Kerberos tickets.	https://github.com/gentilkiwi/mimikatz
Dumpert	LSASS memory dumper using direct system calls and API unhooking.	https://github.com/outflanknl/Dumpert
CredBandit	CredBandit is a proof of concept Beacon Object File (BOF) that uses static x64 syscalls to perform a complete in memory dump of a process and send that back through your already existing Beacon communication channel.	https://github.com/xforcered/CredBandit
CloneVault	CloneVault allows a red team operator to export and import entries including attributes from Windows Credential Manager.	https://github.com/mdsecactivebreach/CloneVault
SharpLAPS	Retrieve LAPS password from LDAP	https://github.com/swisskyrepo/SharpLAPS
SharpDPAPI	SharpDPAPI is a C# port of some DPAPI functionality from @gentilkiwi's Mimikatz project.	https://github.com/GhostPack/SharpDPAPI
KeeThief	Allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system.	https://github.com/GhostPack/KeeThief
SafetyKatz	SafetyKatz is a combination of slightly modified version of @gentilkiwi's Mimikatz project and @subtee's .NET PE Loader.	https://github.com/GhostPack/SafetyKatz

Name	Description	URL
forkatz	credential dump using forshaw technique using SeTrustedCredmanAccessPrivilege	https://github.com/Barbarisch/forkatz
PPLKiller	Tool to bypass LSA Protection (aka Protected Process Light)	https://github.com/RedCursorSecurityConsulting/PPLKiller
LaZagne	The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer.	https://github.com/AlessandroZ/LaZagne
AndrewSpecial	AndrewSpecial, dumping lsass' memory stealthily and bypassing "Cilence" since 2019.	https://github.com/hoangprod/AndrewSpecial
Net-GPPPassword	.NET implementation of Get-GPPPassword. Retrieves the plaintext password and other information for accounts pushed through Group Policy Preferences.	https://github.com/outflanknl/Net-GPPPassword
SharpChromium	.NET 4.0 CLR Project to retrieve Chromium data, such as cookies, history and saved logins.	https://github.com/djhohnstein/SharpChromium
Chlonium	Chlonium is an application designed for cloning Chromium Cookies.	https://github.com/rxwx/chlonium
SharpCloud	SharpCloud is a simple C# utility for checking for the existence of credential files related to Amazon Web Services, Microsoft Azure, and Google Compute.	https://github.com/chrismaddalena/SharpCloud
pypykatz	Mimikatz implementation in pure Python. At least a part of it :)	https://github.com/skelsec/pypykatz

Privilege Escalation

Name	Description	URL
ElevateKit	The Elevate Kit demonstrates how to use third-party privilege escalation attacks with Cobalt Strike's Beacon payload.	https://github.com/rsmudge/ElevateKit
Watson	Watson is a .NET tool designed to enumerate missing KBs and suggest exploits for Privilege Escalation vulnerabilities.	https://github.com/rasta-mouse/Watson
SharpUp	SharpUp is a C# port of various PowerUp functionality. Currently, only the most common checks have been ported; no weaponization functions have yet been implemented.	https://github.com/GhostPack/SharpUp
dazzleUP	A tool that detects the privilege escalation vulnerabilities caused by misconfigurations and missing updates in the Windows operating systems. dazzleUP detects the following vulnerabilities.	https://github.com/hlldz/dazzleUP
PEASS	Privilege Escalation Awesome Scripts SUITE (with colors)	https://github.com/carlospolop/PEASS-ng
SweetPotato	A collection of various native Windows privilege escalation techniques from service accounts to SYSTEM	https://github.com/CCob/SweetPotato

Defense Evasion

Name	Description	URL
unDefender	Killing your preferred antimalware by abusing native symbolic links and NT paths.	https://github.com/APTortellini/unDefender
Backstab	A tool to kill antimalware protected processes	https://github.com/Yaxser/Backstab
SPAWN - Cobalt Strike BOF	Cobalt Strike BOF that spawns a sacrificial process, injects it with shellcode, and executes payload. Built to evade EDR/UserLand hooks by spawning sacrificial	https://github.com/boku7/spawn

Name	Description	URL
	process with Arbitrary Code Guard (ACG), BlockDll, and PPID spoofing.	
BOF.NET - A .NET Runtime for Cobalt Strike's Beacon Object Files	BOF.NET is a small native BOF object combined with the BOF.NET managed runtime that 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://github.com/CCob/BOF.NET
NetLoader	Loads any C# binary from filepath or url, patching AMSI and bypassing Windows Defender on runtime	https://github.com/Flangvik/NetLoader
FindObjects-BOF	A Cobalt Strike Beacon Object File (BOF) project which uses direct system calls to enumerate processes for specific modules or process handles.	https://github.com/outflanknl/FindObjects-BOF
SharpUnhooker	C# Based Universal API Unhooker - Automatically Unhook API Hives (ntdll.dll,kernel32.dll,user32.dll,advapi32.dll, and kernelbase.dll).	https://github.com/GetRektBoy724/SharpUnhooker
EvtMute	Apply a filter to the events being reported by windows event logging	https://github.com/bats3c/EvtMute
InlineExecute-Assembly	InlineExecute-Assembly is a proof of concept Beacon Object File (BOF) that allows security professionals to perform in process .NET assembly execution as an alternative to Cobalt Strikes traditional fork and run execute-assembly module	https://github.com/xforcered/InlineExecute-Assembly
Phant0m	Windows Event Log Killer	https://github.com/hlldz/Phant0m
SharpBlock	A method of bypassing EDR's active projection DLL's by preventing entry point execution.	https://github.com/CCob/SharpBlock
NtdllUnpatcher	Example code for EDR bypassing, please use this for testing blue team detection	https://github.com/Kharos102/NtdllUnpatcher

Name	Description	URL
	capabilities against this type of malware that will bypass EDR's userland hooks.	
DarkLoadLibrary	LoadLibrary for offensive operations.	https://github.com/bats3c/DarkLoadLibrary
BlockETW	.Net 3.5 / 4.5 Assembly to block ETW telemetry in a process	https://github.com/Soledge/BlockEtw
firewalker	This repo contains a simple library which can be used to add FireWalker hook bypass capabilities to existing code	https://github.com/mdsecactivebreach/firewalker

Persistence

Name	Description	URL
SharpStay	.NET project for installing Persistence	https://github.com/0xthirteen/SharpStay
SharPersist	Windows persistence toolkit written in C#.	https://github.com/fireeye/SharPersist
SharpHide	Tool to create hidden registry keys.	https://github.com/outflanknl/SharpHide
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://github.com/Ben0xA/DoUCMe
A Black Path Toward The Sun	(TCP tunneling over HTTP for web application servers)	https://github.com/nccgroup/ABPTTS
pivotnacci	A tool to make socks connections through HTTP agents	https://github.com/blackarrowsec/pivotnacci
reGeorg	The successor to reDuh, pwn a bastion webserver and create SOCKS proxies through the DMZ. Pivot and pwn.	https://github.com/sensepost/reGeorg
DAMP	The Discretionary ACL Modification Project: Persistence Through Host-based Security Descriptor Modification.	https://github.com/HarmJ0y/DAMP

Name	Description	URL
IIS-Raid	A native backdoor module for Microsoft IIS (Internet Information Services)	https://github.com/0x09AL/IIS-Raid
SharPyShell	tiny and obfuscated ASP.NET webshell for C# web applications	https://github.com/antonioCoco/SharPyShell

Lateral Movement

Name	Description	URL
Liquid Snake	LiquidSnake is a tool that allows operators to perform fileless lateral movement using WMI Event Subscriptions and GadgetToJScript	https://github.com/RiccardoAncarani/LiquidSnake
PowerUpSQL	A PowerShell Toolkit for Attacking SQL Server	https://github.com/NetSPI/PowerUpSQL
SharpRDP	Remote Desktop Protocol Console Application for Authenticated Command Execution	https://github.com/0xthirteen/SharpRDP
MoveKit	Movekit is an extension of built in Cobalt Strike lateral movement by leveraging the execute_assembly function with the SharpMove and SharpRDP .NET assemblies.	https://github.com/0xthirteen/MoveKit
SharpNoPSExec	File less command execution for lateral movement.	https://github.com/juliourena/SharpNoPSExec
Responder/MultiRelay	LLMNR/NBT-NS/mDNS Poisoner and NTLMv1/2 Relay.	https://github.com/lgandx/Responder
impacket	Impacket is a collection of Python classes for working with network protocols. Impacket is focused on providing low-level programmatic access to the packets and for some protocols (e.g. SMB1-3 and MSRPC) the protocol implementation itself.	https://github.com/SecureAuthCorp/impacket

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

Name	Description	URL
	LDAP and is compatible with Cobalt Strike.	
CrackMapExec	A swiss army knife for pentesting networks	https://github.com/byt3bl33d3r/CrackMapExec
SharpAllowedToAct	A C# implementation of a computer object takeover through Resource-Based Constrained Delegation (msDS-AllowedToActOnBehalfOfOtherIdentity) based on the research by @elad_shamir.	https://github.com/pkb1s/SharpAllowedToAct
SharpRDPHijack	Sharp RDP Hijack is a proof-of-concept .NET/C# Remote Desktop Protocol (RDP) session hijack utility for disconnected sessions	https://github.com/bohops/SharpRDPHijack
CheeseTools	This repository has been made basing onto the already existing MiscTool, so big shout-out to rasta-mouse for releasing them and for giving me the right motivation to work on them.	https://github.com/klezVirus/CheeseTools
SharpSpray	SharpSpray is a Windows domain password spraying tool written in .NET C#.	https://github.com/iomoath/SharpSpray

Exfiltration

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

Miscellaneous Cloud Amazon Web Services (AWS)

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

Azure

Name	Description	URL
Azure AD Connect password extraction	This toolkit offers several ways to extract and decrypt stored Azure AD and Active Directory credentials from Azure AD Connect servers.	https://github.com/fox-it/adconnectdump
Storm Spotter	Azure Red Team tool for graphing Azure and Azure Active Directory objects	https://github.com/Azure/Stormspotter
ROADtools	The Azure AD exploration framework.	https://github.com/dirkjanm/ROADtools
MicroBurst: A PowerShell Toolkit for Attacking Azure	A collection of scripts for assessing Microsoft Azure security	https://github.com/NetSPI/MicroBurst
AADInternals	AADInternals PowerShell module for administering Azure AD and Office 365	https://github.com/Gerenios/AADInternals

Adversary Emulation

Name	Description	URL
Prelude Operator	A Platform for Developer-first advanced security· Defend your organization by mimicking real adversarial attacks.	https://www.prelude.org/
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

Red Team Scripts

Name	Description	URL
RedTeamCCode	Red Team C code repo	https://github.com/Mr-Un1k0d3r/RedTeamCCode

Name	Description	URL
EDRs	This repo contains information about EDRs that can be useful during red team exercise.	https://github.com/Mr-Un1k0d3r/EDRs
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://cobalt-strike.github.io/community_kit/

Web application and network Pentest

Initial Access

- The Hitchhiker's Guide To Initial Access
- How To: Empire's Cross Platform Office Macro
- Phishing with PowerPoint
- PHISHING WITH EMPIRE
- Bash Bunny
- OWASP Presentation of Social Engineering - OWASP
- USB Drop Attacks: The Danger of "Lost And Found" Thumb Drives
- Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter - Defcon 24
- Cobalt Strike - Spear Phishing documentation
- Cobalt Strike Blog - What's the go-to phishing technique or exploit?
- Spear phishing with Cobalt Strike - Raphael Mudge
- EMAIL RECONNAISSANCE AND PHISHING TEMPLATE GENERATION MADE SIMPLE
- Phishing for access
- Excel macros with PowerShell
- PowerPoint and Custom Actions
- Macro-less Code Exec in MSWord
- Multi-Platform Macro Phishing Payloads
- Abusing Microsoft Word Features for Phishing: "subDoc"
- Phishing Against Protected View
- POWERSHELL EMPIRE STAGERS 1: PHISHING WITH AN OFFICE MACRO AND EVADING AVS

- The PlugBot: Hardware Botnet Research Project
- Luckystrike: An Evil Office Document Generator
- The Absurdly Underestimated Dangers of CSV Injection
- Macroless DOC malware that avoids detection with Yara rule
- Phishing between the app whitelists
- Executing Metasploit & Empire Payloads from MS Office Document Properties (part 1 of 2)
- Executing Metasploit & Empire Payloads from MS Office Document Properties (part 2 of 2)
- Social Engineer Portal
- 7 Best social Engineering attack
- Using Social Engineering Tactics For Big Data Espionage - RSA Conference Europe 2012
- USING THE DDE ATTACK WITH POWERSHELL EMPIRE
- Phishing on Twitter - POT
- Microsoft Office – NTLM Hashes via Frameset
- Defense-In-Depth write-up
- Spear Phishing 101

Execution

- Research on CMSTP.exe,
- Windows oneliners to download remote payload and execute arbitrary code
- Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts
- WSH Injection: A Case Study
- Gscript Dropper

Persistence

- A View of Persistence
- hiding registry keys with psreflect
- Persistence using RunOnceEx – Hidden from Autoruns.exe
- Persistence using GlobalFlags in Image File Execution Options – Hidden from Autoruns.exe
- Putting data in Alternate data streams and how to execute it – part 2
- WMI Persistence with Cobalt Strike
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence
- Leveraging INF-SCT Fetch & Execute Techniques For Bypass, Evasion, & Persistence (Part 2)

- Vshadow: Abusing the Volume Shadow Service for Evasion, Persistence, and Active Directory Database Extraction

Privilege Escalation

User Account Control Bypass

- First entry: Welcome and fileless UAC bypass,
- Exploiting Environment Variables in Scheduled Tasks for UAC Bypass,
- Reading Your Way Around UAC in 3 parts: Part 1. Part 2. Part 3.
- Bypassing UAC using App Paths,
- "Fileless" UAC Bypass using sdclt.exe,
- UAC Bypass or story about three escalations,
- "Fileless" UAC Bypass Using eventvwr.exe and Registry Hijacking,
- Bypassing UAC on Windows 10 using Disk Cleanup,
- Using IARPUninstallStringLauncher COM interface to bypass UAC,
- Fileless UAC Bypass using sdclt
- Eventvwr File-less UAC Bypass CNA
- Windows 7 UAC whitelist

Escalation

- Windows Privilege Escalation Checklist
- From Patch Tuesday to DA
- A Path for Privilege Escalation

Defense Evasion

- Window 10 Device Guard Bypass
- App Locker ByPass List
- Window Signed Binary
- Bypass Application Whitelisting Script Protections - Regsvr32.exe & COM Scriptlets (.sct files)
- Bypassing Application Whitelisting using MSBuild.exe - Device Guard Example and Mitigations
- Empire without powershell
- Powershell without Powershell to bypass app whitelist
- MS Signed mimikatz in just 3 steps
- Hiding your process from sysinternals
- code signing certificate cloning attacks and defenses

- userland api monitoring and code injection detection
- In memory evasion
- Bypassing AMSI via COM Server Hijacking
- process doppelganging
- Week of Evading Microsoft ATA - Announcement and Day 1 to Day 5
- VEIL-EVASION AES ENCRYPTED HTTPKEY REQUEST: SAND-BOX EVASION
- Putting data in Alternate data streams and how to execute it
- AppLocker – Case study – How insecure is it really? – Part 1
- AppLocker – Case study – How insecure is it really? – Part 2
- Harden Windows with AppLocker – based on Case study part 2
- Harden Windows with AppLocker – based on Case study part 2
- Office 365 Safe links bypass
- Windows Defender Attack Surface Reduction Rules bypass
- Bypassing Device guard UMCI using CHM – CVE-2017-8625
- Bypassing Application Whitelisting with BGInfo
- Cloning and Hosting Evil Captive Portals using a Wifi PineApple
- https://bohops.com/2018/01/23/loading-alternate-data-stream-ads-dll-cpl-binaries-to-bypass-applocker/
- Executing Commands and Bypassing AppLocker with PowerShell Diagnostic Scripts
- mavinject.exe Functionality Deconstructed

Credential Access

- Windows Access Tokens and Alternate credentials
- Bringing the hashes home with reGeorg & Empire
- Intercepting passwords with Empire and winning
- Local Administrator Password Solution (LAPS) Part 1
- Local Administrator Password Solution (LAPS) Part 2
- USING A SCF FILE TO GATHER HASHES
- Remote Hash Extraction On Demand Via Host Security Descriptor Modification
- Offensive Encrypted Data Storage
- Practical guide to NTLM Relaying
- Dump Clear-Text Passwords for All Admins in the Domain Using Mimikatz DCSync
- Dumping Domain Password Hashes

Discovery

- Red Team Operating in a Modern Environment
- My First Go with BloodHound
- Introducing BloodHound
- A Red Teamer's Guide to GPOs and OUs
- Automated Derivative Administrator Search
- A Pentester's Guide to Group Scoping
- Local Group Enumeration
- The PowerView PowerUsage Series #1 - Mass User Profile Enumeration
- The PowerView PowerUsage Series #2 – Mapping Computer Shortnames With the Global Catalog
- The PowerView PowerUsage Series #3 – Enumerating GPO edit rights in a foreign domain
- The PowerView PowerUsage Series #4 – Finding cross-trust ACEs
- Aggressor PowerView
- Lay of the Land with BloodHound
- Scanning for Active Directory Privileges & Privileged Accounts
- Microsoft LAPS Security & Active Directory LAPS Configuration Recon
- Trust Direction: An Enabler for Active Directory Enumeration and Trust Exploitation
- SPN Discovery

Lateral Movement

- A Citrix Story
- Jumping Network Segregation with RDP
- Pass hash pass ticket no pain
- Abusing DNSAdmins privilege for escalation in Active Directory
- Using SQL Server for attacking a Forest Trust
- Extending BloodHound for Red Teamers
- OPSEC Considerations for beacon commands
- My First Go with BloodHound
- Kerberos Party Tricks: Weaponizing Kerberos Protocol Flaws
- Lateral movement using excel application and dcom
- Lay of the Land with BloodHound
- The Most Dangerous User Right You (Probably) Have Never Heard Of

- Agentless Post Exploitation
- A Guide to Attacking Domain Trusts
- Pass-the-Hash Is Dead: Long Live LocalAccountTokenFilterPolicy
- Targeted Kerberoasting
- Kerberoasting Without Mimikatz
- Abusing GPO Permissions
- Abusing Active Directory Permissions with PowerView
- Roasting AS-REPs
- Getting the goods with CrackMapExec: Part 1
- Getting the goods with CrackMapExec: Part 2
- DiskShadow: The Return of VSS Evasion, Persistence, and Active Directory Database Extraction
- Abusing Exported Functions and Exposed DCOM Interfaces for Pass-Thru Command Execution and Lateral Movement
- a guide to attacking domain trusts
- Outlook Home Page – Another Ruler Vector
- Outlook Forms and Shells
- Abusing the COM Registry Structure: CLSID, LocalServer32, & InprocServer32
- LethalHTA - A new lateral movement technique using DCOM and HTA
- Abusing DCOM For Yet Another Lateral Movement Technique

Collection

- Accessing clipboard from the lock screen in Windows 10 Part 1
- Accessing clipboard from the lock screen in Windows 10 Part 2

Exfiltration

- DNS Data exfiltration — What is this and How to use?
- DNS Tunnelling
- sg1: swiss army knife for data encryption, exfiltration & covert communication
- Data Exfiltration over DNS Request Covert Channel: DNSExfiltrator
- DET (extensible) Data Exfiltration Toolkit
- Data Exfiltration via Formula Injection Part1

Command and Control

Domain Fronting

- Empre Domain Fronting
- Escape and Evasion Egressing Restricted Networks - Tom Steele and Chris Patten
- Finding Frontable Domain
- TOR Fronting – Utilising Hidden Services for Privacy
- Simple domain fronting PoC with GAE C2 server
- Domain Fronting Via Cloudfront Alternate Domains
- Finding Domain frontable Azure domains - thoth / Fionnbharr (@a_profligate)
- Google Groups: Blog post on finding 2000+ Azure domains using Censys
- Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike
- SSL Domain Fronting 101
- How I Identified 93k Domain-Frontable CloudFront Domains
- Validated CloudFront SSL Domains
- CloudFront Hijacking
- CloudFrunt GitHub Repo

Connection Proxy

- Redirecting Cobalt Strike DNS Beacons
- Apache2Mod Rewrite Setup
- Cobalt Strike HTTP C2 Redirectors with Apache mod_rewrite
- High-reputation Redirectors and Domain Fronting
- Cloud-based Redirectors for Distributed Hacking
- Combatting Incident Responders with Apache mod_rewrite
- Operating System Based Redirection with Apache mod_rewrite
- Invalid URI Redirection with Apache mod_rewrite
- Strengthen Your Phishing with Apache mod_rewrite and Mobile User Redirection
- mod_rewrite rule to evade vendor sandboxes
- Expire Phishing Links with Apache RewriteMap
- Serving random payloads with NGINX
- Mod_Rewrite Automatic Setup
- Hybrid Cobalt Strike Redirectors
- Expand Your Horizon Red Team – Modern SAAS C2

- RTOps: Automating Redirector Deployment With Ansible

Web Services

- C2 with Dropbox
- C2 with gmail
- C2 with twitter
- Office 365 for Cobalt Strike C2
- Red Team Insights on HTTPS Domain Fronting Google Hosts Using Cobalt Strike
- A stealthy Python based Windows backdoor that uses Github as a C&C server
- External C2 (Third-Party Command and Control)
- Cobalt Strike over external C2 – beacon home in the most obscure ways
- External C2 for Cobalt Strike
- External C2 framework for Cobalt Strike
- External C2 framework - GitHub Repo
- Hiding in the Cloud: Cobalt Strike Beacon C2 using Amazon APIs
- Exploring Cobalt Strike's ExternalC2 framework

Application Layer Protocol

- C2 WebSocket
- C2 WMI
- C2 Website
- C2 Image
- C2 Javascript
- C2 WebInterface
- C2 with DNS
- C2 with https
- C2 with webdav
- Introducing Merlin — A cross-platform post-exploitation HTTP/2 Command & Control Tool
- InternetExplorer.Application for C2

Infrastructure

- Automated Red Team Infrastructure Deployment with Terraform - Part 1
- Automated Red Team Infrastructure Deployment with Terraform - Part 2

- Red Team Infrastructure - AWS Encrypted EBS
- 6 RED TEAM INFRASTRUCTURE TIPS
- How to Build a C2 Infrastructure with Digital Ocean – Part 1
- Infrastructure for Ongoing Red Team Operations
- Attack Infrastructure Log Aggregation and Monitoring
- Randomized Malleable C2 Profiles Made Easy
- Migrating Your infrastructure
- ICMP C2
- Using WebDAV features as a covert channel
- Safe Red Team Infrastructure
- EGRESSING BLUECOAT WITH COBALTSTIKE & LET'S ENCRYPT
- Command and Control Using Active Directory
- A Vision for Distributed Red Team Operations
- Designing Effective Covert Red Team Attack Infrastructure
- Serving Random Payloads with Apache mod_rewrite
- Mail Servers Made Easy
- Securing your Empire C2 with Apache mod_rewrite
- Automating Gophish Releases With Ansible and Docker
- How to Write Malleable C2 Profiles for Cobalt Strike
- How to Make Communication Profiles for Empire
- A Brave New World: Malleable C2
- Malleable Command and Control

Embedded and Peripheral Devices Hacking

- Gettting in with the Proxmark3 & ProxBrute
- Practical Guide to RFID Badge copying
- Contents of a Physical Pentester Backpack
- MagSpoof - credit card/magstripe spoofer
- Wireless Keyboard Sniffer
- RFID Hacking with The Proxmark 3
- Swiss Army Knife for RFID

- Exploring NFC Attack Surface
- Outsmarting smartcards
- Reverse engineering HID iClass Master keys
- Android Open Pwn Project (AOPP)

Misc.

- Red Tips of Vysec
- Cobalt Strike Tips for 2016 ccde red teams
- Models for Red Team Operations
- Planning a Red Team exercise
- Raphael Mudge - Dirty Red Team tricks
- introducing the adversary resilience methodology part 1
- introducing the adversary resilience methodology part 2
- Responsible red team
- Red Teaming for Pacific Rim CCDC 2017
- How I Prepared to Red Team at PRCCDC 2015
- Red Teaming for Pacific Rim CCDC 2016
- Responsible Red Teams
- Awesome-CobaltStrike
- Red Teaming from Zero to One Part-1 Part-2

Red Team Gadgets

Network Implants

- LAN Tap Pro
- LAN Turtle
- Bash Bunny
- Key Croc
- Packet Squirrel
- Shark Jack

Wifi Auditing

- WiFi Pineapple
- Alpha Long range Wireless USB

- Wifi-Deauth Monster
- Crazy PA
- Signal Owl

IoT

- BLE Key
- Proxmark3
- Zigbee Sniffer
- Attify IoT Exploit kit

Software Defined Radio - SDR

- HackRF One Bundle
- RTL-SDR
- YARD stick one Bundle
- Ubertooth

Misc.

- Key Grabber
- Magspoof
- Poison tap
- keysweeper
- USB Rubber Ducky
- Screen Crab
- O.MG Cable
- Keysy

EBooks

- Next Generation Red Teaming
- Targeted Cyber Attack
- Advanced Penetration Testing: Hacking the World's Most Secure Networks
- Social Engineers' Playbook Practical Pretexting
- The Hacker Playbook 3: Practical Guide To Penetration Testing
- How to Hack Like a PORNSTAR: A step by step process for breaking into a BANK

Training (Free)

- Tradecraft - a course on red team operations
- Advanced Threat Tactics Course & Notes
- FireEye - a whiteboard session on red team operations

Home Lab

- Building an Effective Active Directory Lab Environment for Testing
- Setting up DetectionLab
- vulnerable-AD - Script to make your home AD Lab vulnerable

Multi-paradigm Frameworks

- Armitage - Java-based GUI front-end for the Metasploit Framework.
- AutoSploit - Automated mass exploiter, which collects target by employing the Shodan.io API and programmatically chooses Metasploit exploit modules based on the Shodan query.
- Decker - Penetration testing orchestration and automation framework, which allows writing declarative, reusable configurations capable of ingesting variables and using outputs of tools it has run as inputs to others.
- Faraday - Multiuser integrated pentesting environment for red teams performing cooperative penetration tests, security audits, and risk assessments.
- Metasploit - Software for offensive security teams to help verify vulnerabilities and manage security assessments.
- Pupy - Cross-platform (Windows, Linux, macOS, Android) remote administration and post-exploitation tool.

Network Tools

- CrackMapExec - Swiss army knife for pentesting networks.
- IKEForce - Command line IPSEC VPN brute forcing tool for Linux that allows group name/ID enumeration and XAUTH brute forcing capabilities.
- Intercepter-NG - Multifunctional network toolkit.
- Legion - Graphical semi-automated discovery and reconnaissance framework based on Python 3 and forked from SPARTA.
- Network-Tools.com - Website offering an interface to numerous basic network utilities like ping, traceroute, whois, and more.
- Ncrack - High-speed network authentication cracking tool built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.
- Praeda - Automated multi-function printer data harvester for gathering usable data during security assessments.
- Printer Exploitation Toolkit (PRET) - Tool for printer security testing capable of IP and USB connectivity, fuzzing, and exploitation of PostScript, PJL, and PCL printer language features.

- SPARTA - Graphical interface offering scriptable, configurable access to existing network infrastructure scanning and enumeration tools.
- SigPloit - Signaling security testing framework dedicated to telecom security for researching vulnerabilites in the signaling protocols used in mobile (cellular phone) operators.
- Smart Install Exploitation Tool (SIET) - Scripts for identifying Cisco Smart Install-enabled switches on a network and then manipulating them.
- THC Hydra - Online password cracking tool with built-in support for many network protocols, including HTTP, SMB, FTP, telnet, ICQ, MySQL, LDAP, IMAP, VNC, and more.
- Tsunami - General purpose network security scanner with an extensible plugin system for detecting high severity vulnerabilities with high confidence.
- Zarp - Network attack tool centered around the exploitation of local networks.
- dnstwist - Domain name permutation engine for detecting typo squatting, phishing and corporate espionage.
- dsniff - Collection of tools for network auditing and pentesting.
- impacket - Collection of Python classes for working with network protocols.
- pivotsuite - Portable, platform independent and powerful network pivoting toolkit.
- routersploit - Open source exploitation framework similar to Metasploit but dedicated to embedded devices.
- rshijack - TCP connection hijacker, Rust rewrite of shijack.

DDoS Tools

- Anevicon - Powerful UDP-based load generator, written in Rust.
- HOIC - Updated version of Low Orbit Ion Cannon, has 'boosters' to get around common counter measures.
- Low Orbit Ion Canon (LOIC) - Open source network stress tool written for Windows.
- Memcrashed - DDoS attack tool for sending forged UDP packets to vulnerable Memcached servers obtained using Shodan API.
- SlowLoris - DoS tool that uses low bandwidth on the attacking side.
- T50 - Faster network stress tool.
- UFONet - Abuses OSI layer 7 HTTP to create/manage 'zombies' and to conduct different attacks using; GET/POST, multithreading, proxies, origin spoofing methods, cache evasion techniques, etc.

Network Reconnaissance Tools

- ACLight - Script for advanced discovery of sensitive Privileged Accounts - includes Shadow Admins.
- AQUATONE - Subdomain discovery tool utilizing various open sources producing a report that can be used as input to other tools.
- CloudFail - Unmask server IP addresses hidden behind Cloudflare by searching old database records and detecting misconfigured DNS.

- DNSDumpster - Online DNS recon and search service.
- Mass Scan - TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes.
- OWASP Amass - Subdomain enumeration via scraping, web archives, brute forcing, permutations, reverse DNS sweeping, TLS certificates, passive DNS data sources, etc.
- ScanCannon - Python script to quickly enumerate large networks by calling masscan to quickly identify open ports and then nmap to gain details on the systems/services on those ports.
- XRay - Network (sub)domain discovery and reconnaissance automation tool.
- dnsenum - Perl script that enumerates DNS information from a domain, attempts zone transfers, performs a brute force dictionary style attack, and then performs reverse look-ups on the results.
- dnsmap - Passive DNS network mapper.
- dnsrecon - DNS enumeration script.
- dnstracer - Determines where a given DNS server gets its information from, and follows the chain of DNS servers.
- fierce - Python3 port of the original fierce.pl DNS reconnaissance tool for locating non-contiguous IP space.
- nmap - Free security scanner for network exploration & security audits.
- passivedns-client - Library and query tool for querying several passive DNS providers.
- passivedns - Network sniffer that logs all DNS server replies for use in a passive DNS setup.
- RustScan - Lightweight and quick open-source port scanner designed to automatically pipe open ports into Nmap.
- scanless - Utility for using websites to perform port scans on your behalf so as not to reveal your own IP.
- smbmap - Handy SMB enumeration tool.
- subbrute - DNS meta-query spider that enumerates DNS records, and subdomains.
- zmap - Open source network scanner that enables researchers to easily perform Internet-wide network studies.

Protocol Analyzers and Sniffers

See also awesome-pcaptools.

- Debookee - Simple and powerful network traffic analyzer for macOS.
- Dshell - Network forensic analysis framework.
- Netzob - Reverse engineering, traffic generation and fuzzing of communication protocols.
- Wireshark - Widely-used graphical, cross-platform network protocol analyzer.
- netsniff-ng - Swiss army knife for network sniffing.
- sniffglue - Secure multithreaded packet sniffer.
- tcpdump/libpcap - Common packet analyzer that runs under the command line.

Network Traffic Replay and Editing Tools

- TraceWrangler - Network capture file toolkit that can edit and merge pcap or pcapng files with batch editing features.
- WireEdit - Full stack WYSIWYG pcap editor (requires a free license to edit packets).
- bittwist - Simple yet powerful libpcap-based Ethernet packet generator useful in simulating networking traffic or scenario, testing firewall, IDS, and IPS, and troubleshooting various network problems.
- hping3 - Network tool able to send custom TCP/IP packets.
- pig - GNU/Linux packet crafting tool.
- scapy - Python-based interactive packet manipulation program and library.
- tcpreplay - Suite of free Open Source utilities for editing and replaying previously captured network traffic.

Proxies and Machine-in-the-Middle (MITM) Tools

See also *Intercepting Web proxies*.

- BetterCAP - Modular, portable and easily extensible MITM framework.
- Ettercap - Comprehensive, mature suite for machine-in-the-middle attacks.
- Habu - Python utility implementing a variety of network attacks, such as ARP poisoning, DHCP starvation, and more.
- Lambda-Proxy - Utility for testing SQL Injection vulnerabilities on AWS Lambda serverless functions.
- MITMf - Framework for Man-In-The-Middle attacks.
- Morpheus - Automated ettercap TCP/IP Hijacking tool.
- SSH MITM - Intercept SSH connections with a proxy; all plaintext passwords and sessions are logged to disk.
- dnschef - Highly configurable DNS proxy for pentesters.
- evilgrade - Modular framework to take advantage of poor upgrade implementations by injecting fake updates.
- mallory - HTTP/HTTPS proxy over SSH.
- oregano - Python module that runs as a machine-in-the-middle (MITM) accepting Tor client requests.
- sylkie - Command line tool and library for testing networks for common address spoofing security vulnerabilities in IPv6 networks using the Neighbor Discovery Protocol.

Transport Layer Security Tools

- SSLyze - Fast and comprehensive TLS/SSL configuration analyzer to help identify security mis-configurations.
- crackpkcs12 - Multithreaded program to crack PKCS#12 files (.p12 and .pfx extensions), such as TLS/SSL certificates.
- testssl.sh - Command line tool which checks a server's service on any port for the support of TLS/SSL ciphers, protocols as well as some cryptographic flaws.
- tls_prober - Fingerprint a server's SSL/TLS implementation.

Wireless Network Tools

- Aircrack-ng - Set of tools for auditing wireless networks.
- Airgeddon - Multi-use bash script for Linux systems to audit wireless networks.
- BoopSuite - Suite of tools written in Python for wireless auditing.
- Bully - Implementation of the WPS brute force attack, written in C.
- Cowpatty - Brute-force dictionary attack against WPA-PSK.
- Fluxion - Suite of automated social engineering based WPA attacks.
- KRACK Detector - Detect and prevent KRACK attacks in your network.
- Kismet - Wireless network detector, sniffer, and IDS.
- PSKracker - Collection of WPA/WPA2/WPS default algorithms, password generators, and PIN generators written in C.
- Reaver - Brute force attack against WiFi Protected Setup.
- WiFi Pineapple - Wireless auditing and penetration testing platform.
- WiFi-Pumpkin - Framework for rogue Wi-Fi access point attack.
- Wifite - Automated wireless attack tool.
- infernal-twin - Automated wireless hacking tool.
- krackattacks-scripts - WPA2 Krack attack scripts.
- pwnagotchi - Deep reinforcement learning based AI that learns from the Wi-Fi environment and instruments BetterCAP in order to maximize the WPA key material captured.
- wifi-arsenal - Resources for Wi-Fi Pentesting.

Network Vulnerability Scanners

- celerystalk - Asynchronous enumeration and vulnerability scanner that "runs all the tools on all the hosts" in a configurable manner.
- kube-hunter - Open-source tool that runs a set of tests ("hunters") for security issues in Kubernetes clusters from either outside ("attacker's view") or inside a cluster.
- Nessus - Commercial vulnerability management, configuration, and compliance assessment platform, sold by Tenable.
- Netsparker Application Security Scanner - Application security scanner to automatically find security flaws.
- Nexpose - Commercial vulnerability and risk management assessment engine that integrates with Metasploit, sold by Rapid7.
- OpenVAS - Free software implementation of the popular Nessus vulnerability assessment system.
- Vuls - Agentless vulnerability scanner for GNU/Linux and FreeBSD, written in Go.

Web Vulnerability Scanners

- ACSTIS - Automated client-side template injection (sandbox escape/bypass) detection for AngularJS.
- Arachni - Scriptable framework for evaluating the security of web applications.
- JCS - Joomla Vulnerability Component Scanner with automatic database updater from exploitdb and packetstorm.
- Nikto - Noisy but fast black box web server and web application vulnerability scanner.
- SQLmate - Friend of sqlmap that identifies SQLi vulnerabilities based on a given dork and (optional) website.
- SecApps - In-browser web application security testing suite.
- WPScan - Black box WordPress vulnerability scanner.
- Wapiti - Black box web application vulnerability scanner with built-in fuzzer.
- WebReaver - Commercial, graphical web application vulnerability scanner designed for macOS.
- cms-explorer - Reveal the specific modules, plugins, components and themes that various websites powered by content management systems are running.
- joomscan - Joomla vulnerability scanner.
- w3af - Web application attack and audit framework.

Online Resources

Online Operating Systems Resources

- DistroWatch.com's Security Category - Website dedicated to talking about, reviewing, and keeping up to date with open source operating systems.

Online Penetration Testing Resources

- MITRE's Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) - Curated knowledge base and model for cyber adversary behavior.
- Metasploit Unleashed - Free Offensive Security Metasploit course.
- Open Web Application Security Project (OWASP) - Worldwide not-for-profit charitable organization focused on improving the security of especially Web-based and Application-layer software.
- PENTEST-WIKI - Free online security knowledge library for pentesters and researchers.
- Penetration Testing Execution Standard (PTES) - Documentation designed to provide a common language and scope for performing and reporting the results of a penetration test.
- Penetration Testing Framework (PTF) - Outline for performing penetration tests compiled as a general framework usable by vulnerability analysts and penetration testers alike.
- XSS-Payloads - Resource dedicated to all things XSS (cross-site), including payloads, tools, games, and documentation.

Other Lists Online

- .NET Programming - Software framework for Microsoft Windows platform development.
- Infosec/hacking videos recorded by cooper - Collection of security conferences recorded by Cooper.
- Android Exploits - Guide on Android Exploitation and Hacks.
- Android Security - Collection of Android security related resources.
- AppSec - Resources for learning about application security.
- Awesome Awesomness - The List of the Lists.
- Awesome Malware - Curated collection of awesome malware, botnets, and other post-exploitation tools.
- Awesome Shodan Queries - Awesome list of useful, funny, and depressing search queries for Shodan.
- AWS Tool Arsenal - List of tools for testing and securing AWS environments.
- Blue Team - Awesome resources, tools, and other shiny things for cybersecurity blue teams.
- C/C++ Programming - One of the main language for open source security tools.
- CTFs - Capture The Flag frameworks, libraries, etc.
- Forensics - Free (mostly open source) forensic analysis tools and resources.
- Hacking - Tutorials, tools, and resources.
- Honeypots - Honeypots, tools, components, and more.
- InfoSec § Hacking challenges - Comprehensive directory of CTFs, wargames, hacking challenge websites, pentest practice lab exercises, and more.
- Infosec - Information security resources for pentesting, forensics, and more.
- JavaScript Programming - In-browser development and scripting.
- Kali Linux Tools - List of tools present in Kali Linux.
- Node.js Programming by @sindresorhus - Curated list of delightful Node.js packages and resources.
- Pentest Cheat Sheets - Awesome Pentest Cheat Sheets.
- Python Programming by @svaksha - General Python programming.
- Python Programming by @vinta - General Python programming.
- Python tools for penetration testers - Lots of pentesting tools are written in Python.
- Red Teaming - List of Awesome Red Teaming Resources.
- Ruby Programming by @Sdogruyol - The de-facto language for writing exploits.
- Ruby Programming by @dreikanter - The de-facto language for writing exploits.
- Ruby Programming by @markets - The de-facto language for writing exploits.
- SecLists - Collection of multiple types of lists used during security assessments.
- SecTools - Top 125 Network Security Tools.

- Security Talks - Curated list of security conferences.
- Security - Software, libraries, documents, and other resources.
- Serverless Security - Curated list of awesome serverless security resources such as (e)books, articles, whitepapers, blogs and research papers.
- Shell Scripting - Command line frameworks, toolkits, guides and gizmos.
- YARA - YARA rules, tools, and people.

Penetration Testing Report Templates

- Public Pentesting Reports - Curated list of public penetration test reports released by several consulting firms and academic security groups.
- T&VS Pentesting Report Template - Pentest report template provided by Test and Verification Services, Ltd.
- Web Application Security Assessment Report Template - Sample Web application security assessment reporting template provided by Lucideus.

Open Sources Intelligence (OSINT)

See also awesome-osint.

- DataSploit - OSINT visualizer utilizing Shodan, Censys, Clearbit, EmailHunter, FullContact, and Zoomeye behind the scenes.
- Depix - Tool for recovering passwords from pixelized screenshots (by de-pixelating text).
- GyoiThon - GyoiThon is an Intelligence Gathering tool using Machine Learning.
- Intrigue - Automated OSINT & Attack Surface discovery framework with powerful API, UI and CLI.
- Maltego - Proprietary software for open sources intelligence and forensics.
- PacketTotal - Simple, free, high-quality packet capture file analysis facilitating the quick detection of network-borne malware (using Zeek and Suricata IDS signatures under the hood).
- Skiptracer - OSINT scraping framework that utilizes basic Python webscraping (BeautifulSoup) of PII paywall sites to compile passive information on a target on a ramen noodle budget.
- Sn1per - Automated Pentest Recon Scanner.
- Spiderfoot - Multi-source OSINT automation tool with a Web UI and report visualizations.
- creepy - Geolocation OSINT tool.
- gOSINT - OSINT tool with multiple modules and a telegram scraper.
- image-match - Quickly search over billions of images.
- recon-ng - Full-featured Web Reconnaissance framework written in Python.
- sn0int - Semi-automatic OSINT framework and package manager.

Data Broker and Search Engine Services

- Hunter.io - Data broker providing a Web search interface for discovering the email addresses and other organizational details of a company.
- Threat Crowd - Search engine for threats.
- Virus Total - Free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.
- surfraw - Fast UNIX command line interface to a variety of popular WWW search engines.

Dorking tools

- BinGoo - GNU/Linux bash based Bing and Google Dorking Tool.
- dorkbot - Command-line tool to scan Google (or other) search results for vulnerabilities.
- github-dorks - CLI tool to scan GitHub repos/organizations for potential sensitive information leaks.
- GooDork - Command line Google dorking tool.
- Google Hacking Database - Database of Google dorks; can be used for recon.
- dork-cli - Command line Google dork tool.
- dorks - Google hack database automation tool.
- fast-recon - Perform Google dorks against a domain.
- pagodo - Automate Google Hacking Database scraping.
- snitch - Information gathering via dorks.

Email search and analysis tools

- SimplyEmail - Email recon made fast and easy.
- WhatBreach - Search email addresses and discover all known breaches that this email has been seen in, and download the breached database if it is publicly available.

Metadata harvesting and analysis

- FOCA (Fingerprinting Organizations with Collected Archives) - Automated document harvester that searches Google, Bing, and DuckDuckGo to find and extrapolate internal company organizational structures.
- metagoofil - Metadata harvester.
- theHarvester - E-mail, subdomain and people names harvester.

Network device discovery tools

- Censys - Collects data on hosts and websites through daily ZMap and ZGrab scans.
- Shodan - World's first search engine for Internet-connected devices.
- ZoomEye - Search engine for cyberspace that lets the user find specific network components.

OSINT Online Resources

- CertGraph - Crawls a domain's SSL/TLS certificates for its certificate alternative names.
- GhostProject - Searchable database of billions of cleartext passwords, partially visible for free.
- NetBootcamp OSINT Tools - Collection of OSINT links and custom Web interfaces to other services.
- OSINT Framework - Collection of various OSINT tools broken out by category.
- WiGLE.net - Information about wireless networks world-wide, with user-friendly desktop and web applications.

Source code repository searching tools

See also *Web-accessible source code ripping tools*.

- vcsmap - Plugin-based tool to scan public version control systems for sensitive information.
- Yar - Clone git repositories to search through the whole commit history in order of commit time for secrets, tokens, or passwords.

Web application and resource analysis tools

- BlindElephant - Web application fingerprinter.
- EyeWitness - Tool to take screenshots of websites, provide some server header info, and identify default credentials if possible.
- VHostScan - Virtual host scanner that performs reverse lookups, can be used with pivot tools, detect catch-all scenarios, aliases and dynamic default pages.
- Wappalyzer - Wappalyzer uncovers the technologies used on websites.
- WhatWaf - Detect and bypass web application firewalls and protection systems.
- WhatWeb - Website fingerprinter.
- wafw00f - Identifies and fingerprints Web Application Firewall (WAF) products.
- webscreenshot - Simple script to take screenshots of websites from a list of sites.

Operating System Distributions

- Android Tamer - Distribution built for Android security professionals that includes tools required for Android security testing.
- ArchStrike - Arch GNU/Linux repository for security professionals and enthusiasts.
- AttifyOS - GNU/Linux distribution focused on tools useful during Internet of Things (IoT) security assessments.
- BlackArch - Arch GNU/Linux-based distribution for penetration testers and security researchers.
- Buscador - GNU/Linux virtual machine that is pre-configured for online investigators.
- Kali - Rolling Debian-based GNU/Linux distribution designed for penetration testing and digital forensics.
- Network Security Toolkit (NST) - Fedora-based GNU/Linux bootable live Operating System designed to provide easy access to best-of-breed open source network security applications.
- Parrot - Distribution similar to Kali, with support for multiple hardware architectures.

- PentestBox - Open source pre-configured portable penetration testing environment for the Windows Operating System.
- The Pentesters Framework - Distro organized around the Penetration Testing Execution Standard (PTES), providing a curated collection of utilities that omits less frequently used utilities.

Periodicals

- 2600: The Hacker Quarterly - American publication about technology and computer "underground" culture.
- Phrack Magazine - By far the longest running hacker zine.

Physical Access Tools

- AT Commands - Use AT commands over an Android device's USB port to rewrite device firmware, bypass security mechanisms, exfiltrate sensitive information, perform screen unlocks, and inject touch events.
- Bash Bunny - Local exploit delivery tool in the form of a USB thumbdrive in which you write payloads in a DSL called BunnyScript.
- LAN Turtle - Covert "USB Ethernet Adapter" that provides remote access, network intelligence gathering, and MITM capabilities when installed in a local network.
- PCILeech - Uses PCIe hardware devices to read and write from the target system memory via Direct Memory Access (DMA) over PCIe.
- Packet Squirrel - Ethernet multi-tool designed to enable covert remote access, painless packet captures, and secure VPN connections with the flip of a switch.
- Poisontap - Siphons cookies, exposes internal (LAN-side) router and installs web backdoor on locked computers.
- Proxmark3 - RFID/NFC cloning, replay, and spoofing toolkit often used for analyzing and attacking proximity cards/readers, wireless keys/keyfobs, and more.
- Thunderclap - Open source I/O security research platform for auditing physical DMA-enabled hardware peripheral ports.
- USB Rubber Ducky - Customizable keystroke injection attack platform masquerading as a USB thumbdrive.

Privilege Escalation Tools

- Active Directory and Privilege Escalation (ADAPE) - Umbrella script that automates numerous useful PowerShell modules to discover security misconfigurations and attempt privilege escalation against Active Directory.
- GTFOBins - Curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.
- LinEnum - Scripted local Linux enumeration and privilege escalation checker useful for auditing a host and during CTF gaming.
- Postenum - Shell script used for enumerating possible privilege escalation opportunities on a local GNU/Linux system.
- unix-privesc-check - Shell script to check for simple privilege escalation vectors on UNIX systems.

Password Spraying Tools

- DomainPasswordSpray - Tool written in PowerShell to perform a password spray attack against users of a domain.
- SprayingToolkit - Scripts to make password spraying attacks against Lync/S4B, Outlook Web Access (OWA) and Office 365 (O365) a lot quicker, less painful and more efficient.

Reverse Engineering

See also awesome-reversing, *Exploit Development Tools*.

Reverse Engineering Books

- Gray Hat Hacking The Ethical Hacker's Handbook by Daniel Regalado et al., 2015
- Hacking the Xbox by Andrew Huang, 2003
- Practical Reverse Engineering by Bruce Dang et al., 2014
- Reverse Engineering for Beginners by Dennis Yurichev
- The IDA Pro Book by Chris Eagle, 2011

Reverse Engineering Tools

- angr - Platform-agnostic binary analysis framework.
- Capstone - Lightweight multi-platform, multi-architecture disassembly framework.
- Detect It Easy(DiE) - Program for determining types of files for Windows, Linux and MacOS.
- Evan's Debugger - OllyDbg-like debugger for GNU/Linux.
- Frida - Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers.
- Fridax - Read variables and intercept/hook functions in Xamarin/Mono JIT and AOT compiled iOS/Android applications.
- Ghidra - Suite of free software reverse engineering tools developed by NSA's Research Directorate originally exposed in WikiLeaks's "Vault 7" publication and now maintained as open source software.
- Immunity Debugger - Powerful way to write exploits and analyze malware.
- Interactive Disassembler (IDA Pro) - Proprietary multi-processor disassembler and debugger for Windows, GNU/Linux, or macOS; also has a free version, IDA Free.
- Medusa - Open source, cross-platform interactive disassembler.
- OllyDbg - x86 debugger for Windows binaries that emphasizes binary code analysis.
- PyREBox - Python scriptable Reverse Engineering sandbox by Cisco-Talos.
- Radare2 - Open source, crossplatform reverse engineering framework.
- UEFITool - UEFI firmware image viewer and editor.

- Voltron - Extensible debugger UI toolkit written in Python.
- WDK/WinDbg - Windows Driver Kit and WinDbg.
- binwalk - Fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images.
- boxxy - Linkable sandbox explorer.
- dnSpy - Tool to reverse engineer .NET assemblies.
- plasma - Interactive disassembler for x86/ARM/MIPS. Generates indented pseudo-code with colored syntax code.
- pwndbg - GDB plug-in that eases debugging with GDB, with a focus on features needed by low-level software developers, hardware hackers, reverse-engineers, and exploit developers.
- rVMI - Debugger on steroids; inspect userspace processes, kernel drivers, and preboot environments in a single tool.
- x64dbg - Open source x64/x32 debugger for windows.

Security Education Courses

- ARIZONA CYBER WARFARE RANGE - 24x7 live fire exercises for beginners through real world operations; capability for upward progression into the real world of cyber warfare.
- Cybrary - Free courses in ethical hacking and advanced penetration testing. Advanced penetration testing courses are based on the book 'Penetration Testing for Highly Secured Environments'.
- European Union Agency for Network and Information Security - ENISA Cyber Security Training material.
- Offensive Security Training - Training from BackTrack/Kali developers.
- Open Security Training - Training material for computer security classes.
- SANS Security Training - Computer Security Training & Certification.

Shellcoding Guides and Tutorials

- Exploit Writing Tutorials - Tutorials on how to develop exploits.
- Shellcode Examples - Shellcodes database.
- Shellcode Tutorial - Tutorial on how to write shellcode.
- The Shellcoder's Handbook by Chris Anley et al., 2007

Side-channel Tools

- ChipWhisperer - Complete open-source toolchain for side-channel power analysis and glitching attacks.
- SGX-Step - Open-source framework to facilitate side-channel attack research on Intel x86 processors in general and Intel SGX (Software Guard Extensions) platforms in particular.
- TRRespass - Many-sided rowhammer tool suite able to reverse engineer the contents of DDR3 and DDR4 memory chips protected by Target Row Refresh mitigations.

Social Engineering

See also awesome-social-engineering.

Social Engineering Books

- Ghost in the Wires by Kevin D. Mitnick & William L. Simon, 2011
- No Tech Hacking by Johnny Long & Jack Wiles, 2008
- Social Engineering in IT Security: Tools, Tactics, and Techniques by Sharon Conheady, 2014
- The Art of Deception by Kevin D. Mitnick & William L. Simon, 2002
- The Art of Intrusion by Kevin D. Mitnick & William L. Simon, 2005
- Unmasking the Social Engineer: The Human Element of Security by Christopher Hadnagy, 2014

Social Engineering Online Resources

- Social Engineering Framework - Information resource for social engineers.

Social Engineering Tools

- Beelogger - Tool for generating keylooger.
- Catphish - Tool for phishing and corporate espionage written in Ruby.
- Evilginx2 - Standalone Machine-in-the-Middle (MitM) reverse proxy attack framework for setting up phishing pages capable of defeating most forms of 2FA security schemes.
- FiercePhish - Full-fledged phishing framework to manage all phishing engagements.
- Gophish - Open-source phishing framework.
- King Phisher - Phishing campaign toolkit used for creating and managing multiple simultaneous phishing attacks with custom email and server content.
- Modlishka - Flexible and powerful reverse proxy with real-time two-factor authentication.
- ReelPhish - Real-time two-factor phishing tool.
- Social Engineer Toolkit (SET) - Open source pentesting framework designed for social engineering featuring a number of custom attack vectors to make believable attacks quickly.
- SocialFish - Social media phishing framework that can run on an Android phone or in a Docker container.
- phishery - TLS/SSL enabled Basic Auth credential harvester.
- wifiphisher - Automated phishing attacks against WiFi networks.

Static Analyzers

- Brakeman - Static analysis security vulnerability scanner for Ruby on Rails applications.
- FindBugs - Free software static analyzer to look for bugs in Java code.
- Progpilot - Static security analysis tool for PHP code.

- RegEx-DoS - Analyzes source code for Regular Expressions susceptible to Denial of Service attacks.
- bandit - Security oriented static analyser for Python code.
- cppcheck - Extensible C/C++ static analyzer focused on finding bugs.
- sobelow - Security-focused static analysis for the Phoenix Framework.
- cwe_checker - Suite of tools built atop the Binary Analysis Platform (BAP) to heuristically detect CWEs in compiled binaries and firmware.

Steganography Tools

- Cloakify - Textual steganography toolkit that converts any filetype into lists of everyday strings.
- StegOnline - Web-based, enhanced, and open-source port of StegSolve.
- StegCracker - Steganography brute-force utility to uncover hidden data inside files.

Vulnerability Databases

- Bugtraq (BID) - Software security bug identification database compiled from submissions to the SecurityFocus mailing list and other sources, operated by Symantec, Inc.
- CXSecurity - Archive of published CVE and Bugtraq software vulnerabilities cross-referenced with a Google dork database for discovering the listed vulnerability.
- China National Vulnerability Database (CNNVD) - Chinese government-run vulnerability database analoguous to the United States's CVE database hosted by Mitre Corporation.
- Common Vulnerabilities and Exposures (CVE) - Dictionary of common names (i.e., CVE Identifiers) for publicly known security vulnerabilities.
- Exploit-DB - Non-profit project hosting exploits for software vulnerabilities, provided as a public service by Offensive Security.
- Full-Disclosure - Public, vendor-neutral forum for detailed discussion of vulnerabilities, often publishes details before many other sources.
- GitHub Advisories - Public vulnerability advisories published by or affecting codebases hosted by GitHub, including open source projects.
- HPI-VDB - Aggregator of cross-referenced software vulnerabilities offering free-of-charge API access, provided by the Hasso-Plattner Institute, Potsdam.
- Inj3ct0r - Exploit marketplace and vulnerability information aggregator. (Onion service.)
- Microsoft Security Advisories and Bulletins - Archive and announcements of security advisories impacting Microsoft software, published by the Microsoft Security Response Center (MSRC).
- Mozilla Foundation Security Advisories - Archive of security advisories impacting Mozilla software, including the Firefox Web Browser.
- National Vulnerability Database (NVD) - United States government's National Vulnerability Database provides additional meta-data (CPE, CVSS scoring) of the standard CVE List along with a fine-grained search engine.

- Open Source Vulnerabilities (OSV) - Database of vulnerabilities affecting open source software, queryable by project, Git commit, or version.
- Packet Storm - Compendium of exploits, advisories, tools, and other security-related resources aggregated from across the industry.
- SecuriTeam - Independent source of software vulnerability information.
- Snyk Vulnerability DB - Detailed information and remediation guidance for vulnerabilities known by Snyk.
- US-CERT Vulnerability Notes Database - Summaries, technical details, remediation information, and lists of vendors affected by software vulnerabilities, aggregated by the United States Computer Emergency Response Team (US-CERT).
- Vulnerability Lab - Open forum for security advisories organized by category of exploit target.
- Vulners - Security database of software vulnerabilities.
- Vulmon - Vulnerability search engine with vulnerability intelligence features that conducts full text searches in its database.
- Zero Day Initiative - Bug bounty program with publicly accessible archive of published security advisories, operated by TippingPoint.

Web Exploitation

- FuzzDB - Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.
- Offensive Web Testing Framework (OWTF) - Python-based framework for pentesting Web applications based on the OWASP Testing Guide.
- Raccoon - High performance offensive security tool for reconnaissance and vulnerability scanning.
- WPSploit - Exploit WordPress-powered websites with Metasploit.
- autochrome - Chrome browser profile preconfigured with appropriate settings needed for web application testing.
- badtouch - Scriptable network authentication cracker.
- sslstrip2 - SSLStrip version to defeat HSTS.
- sslstrip - Demonstration of the HTTPS stripping attacks.

Intercepting Web proxies

See also *Proxies and Machine-in-the-Middle (MITM) Tools*.

- Burp Suite - Integrated platform for performing security testing of web applications.
- Fiddler - Free cross-platform web debugging proxy with user-friendly companion tools.
- OWASP Zed Attack Proxy (ZAP) - Feature-rich, scriptable HTTP intercepting proxy and fuzzer for penetration testing web applications.
- mitmproxy - Interactive TLS-capable intercepting HTTP proxy for penetration testers and software developers.

Web file inclusion tools

- Kadimus - LFI scan and exploit tool.
- LFISuite - Automatic LFI scanner and exploiter.
- fimap - Find, prepare, audit, exploit and even Google automatically for LFI/RFI bugs.
- liffy - LFI exploitation tool.

Web injection tools

- Commix - Automated all-in-one operating system command injection and exploitation tool.
- NoSQLmap - Automatic NoSQL injection and database takeover tool.
- SQLmap - Automatic SQL injection and database takeover tool.
- tplmap - Automatic server-side template injection and Web server takeover tool.

Web path discovery and bruteforcing tools

- dirsearch - Web path scanner.
- recursebuster - Content discovery tool to perform directory and file bruteforcing.

Web shells and C2 frameworks

- Browser Exploitation Framework (BeEF) - Command and control server for delivering exploits to commandeered Web browsers.
- DAws - Advanced Web shell.
- SharPyShell - Tiny and obfuscated ASP.NET webshell for C# web applications.
- PhpSploit - Full-featured C2 framework which silently persists on webserver via evil PHP oneliner.
- weevely3 - Weaponized PHP-based web shell.

Web-accessible source code ripping tools

- DVCS Ripper - Rip web accessible (distributed) version control systems: SVN/GIT/HG/BZR.
- GitTools - Automatically find and download Web-accessible .git repositories.
- git-dumper - Tool to dump a git repository from a website.
- git-scanner - Tool for bug hunting or pentesting websites that have open .git repositories available in public.

Web Exploitation Books

- The Browser Hacker's Handbook by Wade Alcorn et al., 2014
- The Web Application Hacker's Handbook by D. Stuttard, M. Pinto, 2011

Windows Utilities

- Bloodhound - Graphical Active Directory trust relationship explorer.
- Commando VM - Automated installation of over 140 Windows software packages for penetration testing and red teaming.
- Covenant - ASP.NET Core application that serves as a collaborative command and control platform for red teamers.
- ctftool - Interactive Collaborative Translation Framework (CTF) exploration tool capable of launching cross-session edit session attacks.
- DeathStar - Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.
- Empire - Pure PowerShell post-exploitation agent.
- Fibratus - Tool for exploration and tracing of the Windows kernel.
- Inveigh - Windows PowerShell ADIDNS/LLMNR/mDNS/NBNS spoofer/machine-in-the-middle tool.
- LaZagne - Credentials recovery project.
- MailSniper - Modular tool for searching through email in a Microsoft Exchange environment, gathering the Global Address List from Outlook Web Access (OWA) and Exchange Web Services (EWS), and more.
- PowerSploit - PowerShell Post-Exploitation Framework.
- RID_ENUM - Python script that can enumerate all users from a Windows Domain Controller and crack those user's passwords using brute-force.
- Responder - Link-Local Multicast Name Resolution (LLMNR), NBT-NS, and mDNS poisoner.
- Rubeus - Toolset for raw Kerberos interaction and abuses.
- Ruler - Abuses client-side Outlook features to gain a remote shell on a Microsoft Exchange server.
- SCOMDecrypt - Retrieve and decrypt RunAs credentials stored within Microsoft System Center Operations Manager (SCOM) databases.
- Sysinternals Suite - The Sysinternals Troubleshooting Utilities.
- Windows Credentials Editor - Inspect logon sessions and add, change, list, and delete associated credentials, including Kerberos tickets.
- Windows Exploit Suggester - Detects potential missing patches on the target.
- mimikatz - Credentials extraction tool for Windows operating system.
- redsnarf - Post-exploitation tool for retrieving password hashes and credentials from Windows workstations, servers, and domain controllers.
- wePWNise - Generates architecture independent VBA code to be used in Office documents or templates and automates bypassing application control and exploit mitigation software.
- WinPwn - Internal penetration test script to perform local and domain reconnaissance, privilege escalation and exploitation.