



Curated list of awesome lists

Awesome CTF Build Status

A curated list of [Capture The Flag](#) (CTF) frameworks, libraries, resources, softwares and tutorials. This list aims to help starters as well as seasoned CTF players to find everything related to CTFs at one place.

Contributing

Please take a quick look at the [contribution guidelines](#) first.

If you know a tool that isn't present here, feel free to open a pull request.

Why?

It takes time to build up collection of tools used in CTF and remember them all. This repo helps to keep all these scattered tools at one place.

Contents

- [Awesome CTF](#)
 - [Create](#)
 - [Forensics](#)
 - [Platforms](#)
 - [Steganography](#)
 - [Web](#)
 - [Solve](#)
 - [Attacks](#)
 - [Bruteforcers](#)
 - [Cryptography](#)
 - [Exploits](#)
 - [Forensics](#)
 - [Networking](#)
 - [Reversing](#)
 - [Services](#)
 - [Steganography](#)
 - [Web](#)
 - [Resources](#)
 - [Operating Systems](#)
 - [Starter Packs](#)
 - [Tutorials](#)
 - [Wargames](#)
 - [Websites](#)
 - [Wikis](#)
 - [Writeups Collections](#)

Create

Tools used for creating CTF challenges

- [Kali Linux CTF Blueprints](#) - Online book on building, testing, and customizing your own Capture the Flag challenges.

Forensics

Tools used for creating Forensics challenges

- [Dnscat2](#) - Hosts communication through DNS.
- [Kroll Artifact Parser and Extractor \(KAPE\)](#) - Triage program.
- [Magnet AXIOM](#) - Artifact-centric DFIR tool.
- [Registry Dumper](#) - Dump your registry.

Platforms

Projects that can be used to host a CTF

- [CTFd](#) - Platform to host jeopardy style CTFs from ISISLab, NYU Tandon.
- [echoCTF:RED](#) - Develop, deploy and maintain your own CTF infrastructure.
- [FBCTF](#) - Platform to host Capture the Flag competitions from Facebook.
- [Hauukins](#) - A Highly Accessible and Automated Virtualization Platform for Security Education.
- [HackTheArch](#) - CTF scoring platform.
- [Mellivora](#) - A CTF engine written in PHP.
- [MotherFucking-CTF](#) - Badass lightweight platform to host CTFs. No JS involved.
- [NightShade](#) - A simple security CTF framework.
- [OpenCTF](#) - CTF in a box. Minimal setup required.
- [PicoCTF](#) - The platform used to run picoCTF. A great framework to host any CTF.
- [PyChallFactory](#) - Small framework to create/manage/package jeopardy CTF challenges.
- [RootTheBox](#) - A Game of Hackers (CTF Scoreboard & Game Manager).
- [Scorebot](#) - Platform for CTFs by Legitbs (Defcon).
- [SecGen](#) - Security Scenario Generator. Creates randomly vulnerable virtual machines.

Steganography

Tools used to create stego challenges

Check solve section for steganography.

Web

Tools used for creating Web challenges

JavaScript Obfuscators

- [Metasploit JavaScript Obfuscator](#)
- [Uglify](#)

Solve

Tools used for solving CTF challenges

Attacks

Tools used for performing various kinds of attacks

- [Bettercap](#) - Framework to perform MITM (Man in the Middle) attacks.
- [Yersinia](#) - Attack various protocols on layer 2.

Crypto

Tools used for solving Crypto challenges

- [CyberChef](#) - Web app for analysing and decoding data.
- [FeatherDuster](#) - An automated, modular cryptanalysis tool.
- [Hash Extender](#) - A utility tool for performing hash length extension attacks.
- [padding-oracle-attacker](#) - A CLI tool to execute padding oracle attacks.
- [PkCrack](#) - A tool for Breaking PKZip-encryption.
- [QuipQuip](#) - An online tool for breaking substitution ciphers or vigenere ciphers (without key).
- [RSACTFTool](#) - A tool for recovering RSA private key with various attack.
- [RSATool](#) - Generate private key with knowledge of p and q.
- [XORTool](#) - A tool to analyze multi-byte xor cipher.

Bruteforcers

Tools used for various kind of bruteforcing (passwords etc.)

- [Hashcat](#) - Password Cracker
- [Hydra](#) - A parallelized login cracker which supports numerous protocols to attack
- [John The Jumbo](#) - Community enhanced version of John the Ripper.
- [John The Ripper](#) - Password Cracker.
- [Nozzlr](#) - Nozzlr is a bruteforce framework, truly modular and script-friendly.
- [Ophcrack](#) - Windows password cracker based on rainbow tables.
- [Patator](#) - Patator is a multi-purpose brute-forcer, with a modular design.
- [Turbo Intruder](#) - Burp Suite extension for sending large numbers of HTTP requests

Exploits

Tools used for solving Exploits challenges

- [DLLInjector](#) - Inject dlls in processes.
- [libformatstr](#) - Simplify format string exploitation.
- [Metasploit](#) - Penetration testing software.
 - [Cheatsheet](#)
- [one_gadget](#) - A tool to find the one gadget `execve('/bin/sh', NULL, NULL)` call.
 - `gem install one_gadget`
- [PwnTools](#) - CTF Framework for writing exploits.
- [Qira](#) - QEMU Interactive Runtime Analyser.
- [ROP Gadget](#) - Framework for ROP exploitation.
- [V0it](#) - Security CTF Toolkit.

Forensics

Tools used for solving Forensics challenges

- [Aircrack-ng](#) - Crack 802.11 WEP and WPA-PSK keys.
 - `apt-get install aircrack-ng`
- [Audacity](#) - Analyze sound files (mp3, m4a, whatever).
 - `apt-get install audacity`
- [Bkhive](#) and [Sandmump2](#) - Dump SYSTEM and SAM files.
 - `apt-get install sandmump2 bkhive`
- [CFF Explorer](#) - PE Editor.
- [CredDump](#) - Dump windows credentials.
- [DVCS Ripper](#) - Rips web accessible (distributed) version control systems.
- [Exif Tool](#) - Read, write and edit file metadata.
- [Exiftooldelete](#) - Used for recovering lost data from mountable images.
- [Fibratus](#) - Tool for exploration and tracing of the Windows kernel.
- [Foremost](#) - Extract particular kind of files using headers.
 - `apt-get install foremost`
- [Fskck.ext4](#) - Used to fix corrupt filesystems.
- [Malzilla](#) - Malware hunting tool.
- [NetworkMiner](#) - Network Forensic Analysis Tool.
- [PDF Streams Inflator](#) - Find and extract zlib files compressed in PDF files.
- [Pngcheck](#) - Verifies the integrity of PNG and dump all of the chunk-level information in human-readable form.
 - `apt-get install pngcheck`
- [ResourcesExtract](#) - Extract various filetypes from exes.
- [Shellbags](#) - Investigate NT_USER.dat files.
- [Snow](#) - A Whitespace Steganography Tool.
- [USBrip](#) - Simple CLI forensics tool for tracking USB device artifacts (history of USB events) on GNU/Linux.
- [Volatility](#) - To investigate memory dumps.
- [Wireshark](#) - Used to analyze pcap or pcapng files

Registry Viewers

- [OfflineRegistryView](#) - Simple tool for Windows that allows you to read offline Registry files from external drive and view the desired Registry key in .reg file format.
- [Registry Viewer®](#) - Used to view Windows registries.

Networking

Tools used for solving Networking challenges

- [Masscan](#) - Mass IP port scanner, TCP port scanner.
- [Monit](#) - A linux tool to check a host on the network (and other non-network activities).
- [Nipe](#) - Nipe is a script to make Tor Network your default gateway.
- [Nmap](#) - An open source utility for network discovery and security auditing.
- [Wireshark](#) - Analyze the network dumps.
 - `apt-get install wireshark`
- [Zeek](#) - An open-source network security monitor.
- [Zmap](#) - An open-source network scanner.

Reversing

Tools used for solving Reversing challenges

- [Androguard](#) - Reverse engineer Android applications.
- [Angr](#) - platform-agnostic binary analysis framework.
- [Apk2Gold](#) - Yet another Android decompiler.
- [ApkTool](#) - Android Decompiler.
- [Barf](#) - Binary Analysis and Reverse engineering Framework.
- [Binary Ninja](#) - Binary analysis framework.
- [BinUtils](#) - Collection of binary tools.
- [BinWaik](#) - Analyze, reverse engineer, and extract firmware images.
- [Boomerang](#) - Decompile x86/SPARC/PowerPC/ST-20 binaries to C.
- [ctf_import](#) - run basic functions from poweredPC binaries cross platform.
- [cwe_checker](#) - cwe_checker finds vulnerable patterns in binary executables.
- [demovfuscator](#) - A work-in-progress deobfuscator for movfuscated binaries.
- [Frida](#) - Dynamic Code Injection.
- [GDB](#) - The GNU project debugger.
- [GEF](#) - GDB plugin.
- [Ghidra](#) - Open Source suite of reverse engineering tools. Similar to IDA Pro.
- [Hopper](#) - Reverse engineering tool (disassembler) for OSX and Linux.
- [IDA Pro](#) - Most used Reversing software.
- [Jadx](#) - Decompile Android files.
- [Java Decompilers](#) - An online decompiler for Java and Android APKs.
- [Krakatau](#) - Java decompiler and disassembler.
- [Objection](#) - Runtime Mobile Exploration.
- [PEDA](#) - GDB plugin (only python2.7).
- [Pin](#) - A dynamic binary instrumentation tool by Intel.
- [PINCE](#) - GDB front-end/reverse engineering tool, focused on game-hacking and automation.
- [PnCTF](#) - A tool which uses intel pin for Side Channel Analysis.
- [Plasma](#) - An interactive disassembler for x86/ARM/MIPS which can generate indented pseudo-code with colored syntax.
- [Pwndbg](#) - A GDB plugin that provides a suite of utilities to hack around GDB easily.
- [radare2](#) - A portable reversing framework.
- [Triton](#) - Dynamic Binary Analysis (DBA) framework.
- [Uncompyle](#) - Decompile Python 2.7 binaries (.pyc).
- [WinDbg](#) - Windows debugger distributed by Microsoft.
- [Xocopy](#) - Program that can copy executables with execute, but no read permission.
- [Z3](#) - A theorem prover from Microsoft Research.

JavaScript Deobfuscators

- [Detox](#) - A Javascript malware analysis tool.
- [Revelo](#) - Analyze obfuscated Javascript code.

SWF Analyzers

- [RABCDAsm](#) - Collection of utilities including an ActionScript 3 assembler/disassembler.
- [SwfTools](#) - Collection of utilities to work with SWF files.
- [Xxxswf](#) - A Python script for analyzing Flash files.

Services

Various kind of useful services available around the internet

- [CSWSH](#) - Cross-Site WebSocket Hijacking Tester.
- [Request Bin](#) - Lets you inspect http requests to a particular url.

Steganography

Tools used for solving Steganography challenges

- [AperiSolve](#) - AperiSolve is a platform which performs layer analysis on image (open-source).
- [Convert](#) - Convert images blw formats and apply filters.
- [Exif](#) - Shows EXIF information in JPEG files.
- [Exiftool](#) - Read and write meta information in files.
- [Exiv2](#) - Image metadata manipulation tool.
- [Image Steganography](#) - Embeds text and files in images with optional encryption. Easy-to-use UI.
- [Image Steganography Online](#) - This is a client-side Javascript tool to steganographically hide images inside the lower "bits" of other images
- [ImageMagick](#) - Tool for manipulating images.
- [Outguess](#) - Universal steganographic tool.
- [Pngtools](#) - For various analysis related to PNGs.
 - `apt-get install pngtools`
- [SmartDeblur](#) - Used to deblur and fix defocused images.
- [Steganabara](#) - Tool for stegano analysis written in Java.
- [SteganographyOnline](#) - Online steganography encoder and decoder.
- [Stegbreak](#) - Launches brute-force dictionary attacks on JPG image.
- [StegCracker](#) - Steganography brute-force utility to uncover hidden data inside files.
- [stegextract](#) - Detect hidden files and text in images.
- [Steghide](#) - Hide data in various kind of images.
- [StegOnline](#) - Conduct a wide range of image steganography operations, such as concealing/revealing files hidden within bits (open-source).
- [Stegsolve](#) - Apply various steganography techniques to images.
- [Zsteg](#) - PNG/BMP analysis.

Web

Tools used for solving Web challenges

- [BurpSuite](#) - A graphical tool to testing website security.
- [Comixit](#) - Automated All-in-One OS Command Injection and Exploitation Tool.
- [Hackbar](#) - Firefox addon for easy web exploitation.
- [OWASP ZAP](#) - Intercepting proxy to replay, debug, and fuzz HTTP requests and responses
- [Raccoon](#) - Add on for chrome for debugging network requests.
- [Raccoon](#) - A high performance offensive security tool for reconnaissance and vulnerability scanning.
- [SQLMap](#) - Automatic SQL injection and database takeover tool. `pip install sqlmap`
- [W3af](#) - Web Application Attack and Audit Framework.
- [XSSer](#) - Automated XSS tester.

Resources

Where to discover about CTF

Operating Systems

Penetration testing and security lab Operating Systems

- [Android Tamer](#) - Based on Debian.
- [BackBox](#) - Based on Ubuntu.
- [BlackArch Linux](#) - Based on Arch Linux.
- [Fedora Security Lab](#) - Based on Fedora.
- [Kali Linux](#) - Based on Debian.
- [Parrot Security OS](#) - Based on Debian.
- [Pentoo](#) - Based on Gentoo.
- [UNIX OS](#) - Based on openSUSE.
- [WiFislax](#) - Based on Slackware.

Malware analysts and reverse-engineering

- [Flare VM](#) - Based on Windows.
- [REMnux](#) - Based on Debian.

Starter Packs

Collections of installer scripts, useful tools

- [CTF Tools](#) - Collection of setup scripts to install various security research tools.
- [LazyKali](#) - A 2016 refresh of LazyKali which simplifies install of tools and configuration.

Tutorials

Tutorials to learn how to play CTFs

- [CTF Field Guide](#) - Field Guide by Trails of Bits.
- [CTF Resources](#) - Start Guide maintained by community.
- [How to Get Started in CTF](#) - Short guideline for CTF beginners by Endgame
- [Intro. to CTF Course](#) - A free course that teaches beginners the basics of forensics, crypto, and web-ex.
- [IppSec](#) - Video tutorials and walkthroughs of popular CTF platforms.
- [LiveOverflow](#) - Video tutorials on Exploitation.
- [MIPT CTF](#) - A small course for beginners in CTFs (in Russian).

Wargames

Always online CTFs

- [Backdoor](#) - Security Platform by SDSLabs.
- [Crackmes](#) - Reverse Engineering Challenges.
- [CryptoHack](#) - Fun cryptography challenges.
- [echoCTF:REDs](#) - Online CTF with a variety of targets to attack.
- [Exploit Exercises](#) - Variety of VMs to learn variety of computer security issues.
- [Exploit.Education](#) - Variety of VMs to learn variety of computer security issues.
- [Gracker](#) - Binary challenges having a slow learning curve, and write-ups for each level.
- [Hack The Box](#) - Weekly CTFs for all types of security enthusiasts.
- [Hack This Site](#) - Training ground for hackers.
- [Hacker101](#) - CTF from HackerOne
- [Hacking-Lab](#) - Ethical hacking, computer network and security challenge platform.
- [Hone Your Ninja Skills](#) - Web challenges starting from basic ones.
- [IO](#) - Wargame for binary challenges.
- [Microcorruption](#) - Embedded security CTF.
- [Over The Wire](#) - Wargame maintained by OverTheWire Community.
- [PentesterLab](#) - Variety of VM and online challenges (paid).
- [PicoCTF](#) - All year round ctf game. Questions from the yearly picoCTF competition.
- [PwnChallenge](#) - Binary Exploitation Wargame.
- [Pwnable.kr](#) - Pwn Game.
- [Pwnable.tw](#) - Binary wargame.
- [Pwnable.xyz](#) - Binary Exploitation Wargame.
- [Reversin.kr](#) - Reversing challenge.
- [Ringzer0Team](#) - Ringzer0 Team Online CTF.
- [Root-Me](#) - Hacking and Information Security learning platform.
- [ROP Wargames](#) - ROP Wargames.
- [SANS HHC](#) - Challenges with a holiday theme released annually and maintained by SANS.
- [SmashTheStack](#) - A variety of wargames maintained by the SmashTheStack Community.
- [Vb10 CTF](#) - Various amazing CTF challenges, in many different categories. Has both Practice mode and Contest mode.
- [VulnHubs](#) - VM-based for practical in digital security, computer application & network administration.
- [W3Cthalls](#) - A penetration testing training platform, which offers various computer challenges, in various categories.
- [WebHacking](#) - Hacking challenges for web.

Self-hosted CTFs

- [Damn Vulnerable Web Application](#) - PHP/MySQL web application that is damn vulnerable.
- [Juice Shop CTF](#) - Scripts and tools for hosting a CTF on [OWASP Juice Shop](#) easily.

Websites

Various general websites about and on CTF

- [Awesome CTF Cheatsheet](#) - CTF Cheatsheet.
- [CTF Time](#) - General information on CTF occurring around the worlds.
- [Reddit Security CTF](#) - Reddit CTF category.

Wikis

Various Wikis available for learning about CTFs

- [Bamboofox](#) - Chinese resources to learn CTF.
- [b0ts Wiki](#) - Wiki from team b0ts.
- [CTF Cheatsheet](#) - CTF tips and tricks.
- [ISIS Lab](#) - CTF Wiki by Isis lab.
- [OpenToAll](#) - CTF tips by OTA CTF team members.

Writeups Collections

Collections of CTF write-ups

- [0e85dc6eaf](#) - Write-ups for CTF challenges by 0e85dc6eaf
- [CapT](#) - Dumped CTF challenges and materials by psifertex.
- [CTF write-ups \(community\)](#) - CTF challenges + write-ups archive maintained by the community.
- [CTFTime Scrapper](#) - Scraps all writeup from CTF Time and organize which to read first.
- [HackThisSite](#) - CTF write-ups repo maintained by HackThisSite team.
- [Mzfr](#) - CTF competition write-ups by mzfr
- [pwnTools writeups](#) - A collection of CTF write-ups all using pwnTools.
- [SababaSec](#) - A collection of CTF write-ups by the SababaSec team.
- [Shell Storm](#) - CTF challenge archive maintained by Jonathan Salwan.
- [Smoke Leet Everyday](#) - CTF write-ups repo maintained by SmokeLeetEveryday team.

LICENSE

CC0.0