



Features Business Explore Marketplace Pricing

This repository

Search

Sign in or Sign up

apsdehal / awesome-ctf

Watch

138

★ Star

2,112

🍴 Fork

418

<> Code

! Issues 2

🔗 Pull requests 1

📁 Projects 0

📊 Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

A curated list of CTF frameworks, libraries, resources and softwares <https://apsdehal.in/awesome-ctf/>

ctf

awesome

security

penetration

📄 180 commits

🔗 1 branch

📦 0 releases

👤 38 contributors

📄 CC0-1.0

Branch: master ▾

New pull request

Find file

Clone or download ▾










apsdehal Set theme jekyll-theme-slate

Latest commit dae55f1 14 days ago

📁 tests

Complete tests for the repo

3 years ago

 .gitignore	Add gitignore, test.js	3 years ago
 .travis.yml	Add travis file	3 years ago
 CONTRIBUTING.md	Update instructions in Contributing to include testing information	3 years ago
 LICENSE	Change LICENSE to CC0	2 years ago
 README.md	Fix Bettercap repository (#77)	2 months ago
 _config.yml	Set theme jekyll-theme-slate	14 days ago
 package.json	Change name to awesome-ctf	3 years ago

README.md

Awesome CTF build passing awesome

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

Forensics

Tools used for creating Forensics challenges

- [Dnscat](#) - Hosts communication through DNS
- [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
- [FBCTF](#) - Platform to host Capture the Flag competitions from Facebook
- [HackTheArch](#) - CTF scoring platform
- [Mellivora](#) - A CTF engine written in PHP
- [NightShade](#) - A simple security CTF framework
- [OpenCTF](#) - CTF in a box. Minimal setup required

- [PicoCTF Platform 2](#) - A genericized version of picoCTF 2014 that can be easily adapted to host CTF or programming competitions.
- [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.
- [Layer 2 attacks](#) - Attack various protocols on layer 2

Crypto

Tools used for solving Crypto challenges

- [FeatherDuster](#) - An automated, modular cryptanalysis tool
- [Hash Extender](#) - A utility tool for performing hash length extension attacks
- [PkCrack](#) - A tool for Breaking PkZip-encryption
- [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
- [John The Jumbo](#) - Community enhanced version of John the Ripper
- [John The Ripper](#) - Password Cracker
- [Nozzlr](#) - Nozzlr is a bruteforce framework, trully modular and script-friendly.

- [Ophcrack](#) - Windows password cracker based on rainbow tables.
- [Patator](#) - Patator is a multi-purpose brute-forcer, with a modular design.

Exploits

Tools used for solving Exploits challenges

- [DLLInjector](#) - Inject dlls in processes
- [libformatstr](#) - Simplify format string exploitation.
- [Metasploit](#) - Penetration testing software
- [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
- [V0lt](#) - 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 Samdump2](#) - Dump SYSTEM and SAM files

- `apt-get install samdump2 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
- [Extundelete](#) - 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`
- [Fsck.ext4](#) - Used to fix corrupt filesystems
- [Malzilla](#) - Malware hunting tool
- [NetworkMiner](#) - Network Forensic Analysis Tool
- [PDF Streams Inflater](#) - Find and extract zlib files compressed in PDF files
- [ResourcesExtract](#) - Extract various filetypes from exes
- [Shellbags](#) - Investigate NT_USER.dat files
- [UsbForensics](#) - Contains many tools for usb forensics
- [Volatility](#) - To investigate memory dumps

Registry Viewers

- [RegistryViewer](#) - Used to view windows registries
- [Windows Registry Viewers](#) - More registry viewers

Networking

Tools used for solving Networking challenges

- [Bro](#) - An open-source network security monitor.
- [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`
- [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
- [BinWalk](#) - Analyze, reverse engineer, and extract firmware images.
- [Boomerang](#) - Decompile x86 binaries to C
- [ctf_import](#) – run basic functions from stripped binaries cross platform
- [GDB](#) - The GNU project debugger
- [GEF](#) - GDB plugin

- [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
- [PEDA](#) - GDB plugin (only python2.7)
- [Pin](#) A dynamic binary instrumentation tool by Intel
- [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
- [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

- [Convert](#) - Convert images b/w formats and apply filters
- [Exif](#) - Shows EXIF information in JPEG files
- [Exiftool](#) - Read and write meta information in files
- [Exiv2](#) - Image metadata manipulation tool
- [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
- [Stegbreak](#) - Launches brute-force dictionary attacks on JPG image
- [Steghide](#) - Hide data in various kind of images
- [Stegsolve](#) - Apply various steganography techniques to images

Web

Tools used for solving Web challenges

- [BurpSuite](#) - A graphical tool to testing website security.
- [Commix](#) - 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
- [Postman](#) - Add on for chrome for debugging network requests
- [SQLMap](#) - Automatic SQL injection and database takeover tool
- [W3af](#) - Web Application Attack and Audit Framework.
- [XSSer](#) - Automated XSS testor

Resources

Where to discover about CTF

Operating Systems

Penetration testing and security lab Operating Systems

- [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

- [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
- [Damn Vulnerable Web Application](#) PHP/MySQL web application that is damn vulnerable
- [How to Get Started in CTF](#) - Short guideline for CTF beginners by Endgame
- [MIPT CTF](#) - A small course for beginners in CTFs (in Russian)

Wargames

Always online CTFs

- [Backdoor](#) - Security Platform by SDSLabs.
- [Ctfs.me](#) - CTF All the time
- [Exploit Exercises](#) - 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.
- [IO](#) - Wargame for binary challenges.
- [Over The Wire](#) - Wargame maintained by OvertheWire Community
- [Pwnable.kr](#) - Pwn Game
- [Ringzer0Team](#) - Ringzer0 Team Online CTF
- [Root-Me](#) - Hacking and Information Security learning platform.
- [ROP Wargames](#) - ROP Wargames
- [SmashTheStack](#) - A variety of wargames maintained by the SmashTheStack Community.
- [VulnHub](#) - VM-based for practical in digital security, computer application & network administration.
- [W3Challs](#) - A penetration testing training platform, which offers various computer challenges, in various categories.
- [WebHacking](#) - Hacking challenges for web.
- [WeChall](#) - Always online challenge site.
- [WTHack OnlineCTF](#) - CTF Practice platform for every level of cyber security enthusiasts.

Self-hosted CTFs

- [Juice Shop CTF](#) - Scripts and tools for hosting a CTF on [OWASP Juice Shop](#) easily.

Websites

Various general websites about and on ctf

- [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
- [ISIS Lab](#) - CTF Wiki by Isis lab
- [OpenToAll](#) - Open To All Knowledge Base

Writeups Collections

Collections of CTF write-ups

- [Captf](#) - 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
- [pwntools writeups](#) - A collection of CTF write-ups all using pwntools
- [Shell Storm](#) - CTF challenge archive maintained by Jonathan Salwan
- [Smoke Leet Everyday](#) - CTF write-ups repo maintained by SmokeLeetEveryday team.

LICENSE

CC0 :)

