RECOMMENDED TOOLS FOR CTF

CyberSecurity CTF Tools

In addition a knowledge of basic Linux commands, access to the following tools (or equivalent tools) are recommended as preparation for an entry level Capture-the-Flag (CTF) competition. Use what ever works for you!

1. **General Competition Tools:**
   - **Basic Linux Commands**
   - **Kali Linux**
   - **Google Chrome SSH** – Lightweight SSH Browser addon:
   - **Number / Text Conversion Tools:**
     - Number Converter (Binary, Octal, Decimal, Hex)
     - Hex to ASCII (text)
     - Binary to Text
     - Text to Numbers (Hex, Decimal, Binary)
     - Base64 (Text, Hex, Video, Audio, etc.)
     - Base2-Base36 – Base2 to Base36 Converter
2. **Open Source Intelligence**:
   - Google, Google Maps, Google Dorks (operators)
   - whois.domaintools.com – Domain owners, name servers info, IP addresses
   - www.robtex.com – Host name, IP , DNS and registry information
   - Jeffrey's Image Meta Data Viewer – Image Meta Data info
3. **Steganography Tools:**
   - **StegOnline** – web-based open-source port of StegSolve.
   - **Hex Editor** – browser based hex editor
   - '***strings***' – Linux command to view visible text characters
   - '***binwalk***' – Linux command to extract embedded files and executables
   - **Digital Invisible Ink Toolkit** – hide/extract files from inside an image
   - **Steghide** – open source steganography software (Linux)
   - **Stegosuite** – a free steganography tool written in Java (Linux).
   - **pngcheck** – look for/correct broken chunks.
   - **GeorgeOM.net** – Geo Explore Colour & Bit Planes (Go to "Browse Bit Planes")
4. **Crytography Decoders:**
   - **XOR Decorder** – Calculate exclusive 'OR' operation
   - **Caesar Cipher** – Shift Cipher
   - **ROT13** – Shift Cipher
   - **A1Z26** – Replace Letters with Numbers
   - **Vigenere Cipher** (requires a key)
   - **Atbash Cipher (simple)**
   - **Vernan (One-time Pad)**
   - **Rail Fence Cipher (ZigZag)**
5. **Password Cracking:**
   1. **Hash-Identifier** – Identifies hash type (Kali)
   2. **Hashcat** – HASH cracking tool (Kali)
   3. **Crackstation** – Browser based Hash Cracker: (https://crackstation.net/)
   4. **md5sum** – calculates/verifies 128-bit MD5 hashes,
   5. **John the Ripper** – Detect and crack weak PWs (Kali).
   6. **Rockyou.txt WordList** (download) – contains 14m unique PWs (Kali).
6. **Web Exploitation**:
   1. **/robots.txt –** lists pages or files that search engines can't request,
   2. **Dirbuster –** brute force discovery of **hidden** directories/files (Kali)
   3. **Development Tools –** Browser option use to inspect source and cookies.
   4. **User Agent Extension** – allows browser to switch user agent .
7. **Log Analysis:**
   - See Basic Linux Commands
8. **Scanning:**
   1. **Nmap** – utility for network discovery and auditing
   2. **Dirbuster** – Scan web sites for hidden web pages
   3. **Metasploit Framework** – scan for known vulnerabilities (Kali)
   4. **Recon-ng** – perform recon on remote targets (Kali).
   5. **W3bin.com** – Info on who is hosting a website
9. **Network Traffic Analysis:**
   1. **Wireshark** – GUI based traffic capture and analysis tool (Kali, Windows or Mac OS).
   2. **tcpdump** – packet analyzer utility for Linux command line
   3. **WinDump** – Windows version on tcpdump.
   4. **ngrep** – search for strings in network packets
10. **Enumeration and Exploitation:**
    1. **'File' Command** – determine a file type (including executables)
    2. **'Strings' Command** – Display text comments in an executable.
    3. **Hex Editor** – view executable for visible text stings
    4. **'*xxd* -r' Command** – convert a hex dump back to its original binary form
    5. **Ghidra** – reverse engineering tool developed by the NSA
    6. ***Objdump -d*** – Linux command line dis-assembler
    7. **Netcat** – utility that reads and writes data across network
    8. **uncompyle6 –** translates Python bytecode back into source
    9. **GDB** – Inspect memory w/in the code being debugged
    10. **Pwntools** – a CTF framework and exploit development library.
11. **Wireless Exploitation**:
    1. **Wigle.Net** – Wifi info database for hotspots from around the world
    2. **Kali Linux** – Linux suite of cybersecurity tools
    3. **Wireshark** – network packet analysis
    4. **Aircrack- ng** – tools to assess WiFi network security
    5. '***ifconfig***' command – configure and query TCP/IP network interface parameters
    6. **Stumbler** (set SSID to ANY) active mode (Windows)
    7. **Kismet** : both war-drive and sniffer. Uses passive mode (Linux)

References:

- Basic Cyber Competition Skill Domains
- Cybersecurity Capture-the-flag (CTF) Competition Tips
- CTF101 – Cryptography
- CTF101 – Forensics
- CTF101 – Web Exploitation
- CTF101 – Reverse Engineering
- CTF101 – Binary Exploitation

Home
Articles
Books
CTF Challenges
Gaming
Linux
Money Making
Online Tools
Q&A
SEO
Tech Articles
Tech News
Tech Offers
Tools
Tutorials

Home > Tech Articles > Top 10 Essential CTF Tools for Solving Reversing Challenges

Top 10 Essential CTF Tools for Solving Reversing Challenges

TECH ARTICLES By Sarcastic Writer · June 16, 2019 · Comments off

Top 10 Essential CTF Tools for Solving Reversing Challenges

1. Androguard

Androguard is a full python tool to play with android files. You can either use the command line or graphical frontend for androguard, or use androguard purely as a library for your own tools and scripts. There are so many open source projects are there which uses androguard like Droidbot, Cuckoo Sandbox, MobSF etc.

For especially malware analysis of android apps, Androguard is one of the best tool.

Download Link – https://github.com/androguard/androguard

2. ApkTool

Apktool is another reverse engineering tool to decompile Android APKs. It can easily decode resources to nearly original form and can even rebuild them after making some modifications.

It's the go-to tool for most independent developers looking to mod apps or uncover their secrets. The developer behind the tool recently announced an update to version 2.4.0, bringing lots of bug fixes and changes.

Download Link – https://github.com/iBotPeaches/Apktool

3. BinUtils

The GNU Binary Utilities, or Binutils, are a set of programming tools for creating and managing binary programs, object files, libraries, profile data, and assembly source code.

But, if you are a developer who is working on Linux / UNIX platform, it is essential to understand the various commands that are available as part of GNU development tools. The below commands of BinUtils will help you to manipulate your binary, object and library files effectively.

- as – GNU Assembler Command
- ld – GNU Linker Command
- ar – GNU Archive Command
- nm – List Object File Symbols
- objcopy – Copy and Translate Object Files
- objdump – Display Object File Information
- size – List Section Size and Toal Size
- strings – Display Printable Characters from a File
- strip – Discard Symbols from Object File

Download Link – http://www.gnu.org/software/binutils/binutils.html

4. GDB

GDB, the GNU Project debugger, allows you to see what is going on 'inside' another program while it executes — or what another program was doing at the moment it crashed. GDB supports various programming languages such as C, C++, Fortran, Pascal, Assembly, Go etc.

The latest version of GDB is v8.3 which was released on May 11th, 2019 and is now available for download.

Download Link – https://www.gnu.org/software/gdb/

5. IDA Pro

IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features. IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger and augmented by a complete plugin programming environment.

As a disassembler, IDA Pro explores binary programs, for which source code isn't always available, to create maps of their execution.

Download Link – https://www.hex-rays.com/products/ida/

6. WinDbg

WinDbg is a multipurpose debugger for the Microsoft Windows computer operating system, distributed by Microsoft.

WinDbg can automatically load debugging symbol files (e.g., PDB files) from a server by matching various criteria like timestamp via SymSrv (SymSrv.dll). To begin using Windbg, you need to create a dump (.dmp) file that you can load and look at.

Download Link – http://www.windbg.org/

7. Radare2

Radare2 or r2 is a rewrite from scratch of radare in order to provide a set of libraries and tools to work with binary files.

Radare project started as a forensics tool, a scriptable command-line hexadecimal editor able to open disk files, but later added support for analyzing binaries, disassembling code, debugging programs, attaching to remote gdb servers.

Download Link – https://github.com/radare/radare2

8. Detox

Detox is of the most popular JS malware analysis tool which works on most Linux distributions. The development is currently done on Linux with the latest chrome browser.

JSDetox is a Javascript malware analysis tool using static analysis / deobfuscation techniques and an execution engine featuring HTML DOM emulation.

Download Link – https://github.com/svent/jsdetox

9. BinWalk

Binwalk is a simple linux tool for analysing binary files for embedded files and executable code. It is mostly used to extract the content of firmware images.

On kali linux, binwalk is already installed. On Ubuntu you can do apt-get install binwalk or you can go to https://github.com/ReFirmLabs/binwalk and follow the instructions.

Download Link – https://github.com/ReFirmLabs/binwalk

10. Barf

BARF is an open source binary analysis framework that aims to support a wide range of binary code analysis tasks that are common in the information security discipline.

It is a scriptable platform that supports instruction lifting from multiple architectures, binary translation to an intermediate representation, an extensible framework for code analysis plugins and interoperation with external tools such as debuggers, SMT solvers and instrumentation tools.

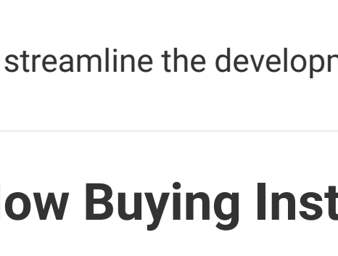
Download Link – https://github.com/programa-stic/barf-project

CTF Challenge Tools
CTF challenges
CTF Opensource Tools
CTF Solutions
CTF Tools
CTF Tools Checklist
CTF Yeahhub
essential CTF tools
Reverse Engineering
Reverse Engineering CTF Tools
Reverse Engineering tools
Reversing Challenges
Solve Reverse Engineering
Top CTF Tools
Yeahhub Tools

Related Posts

Various Python Libraries for developing RESTful APIs

TECH ARTICLES By Sarcastic Writer · July 2, 2023 · Comments off



RESTful APIs (Application Programming Interfaces) have become a popular choice for building web applications and services. They allow different systems to communicate and exchange data using the HTTP protocol. Python, being a versatile programming language, offers several libraries and frameworks... Read more

Top 7 NodeJS Frameworks You Need To Know

TECH ARTICLES By Sarcastic Writer · June 18, 2023 · Comments off

Node.js has gained immense popularity in the web development community due to its ability to build highly scalable and efficient applications. It provides a runtime environment that allows developers to write server-side applications in JavaScript. However, to streamline the development... Read more

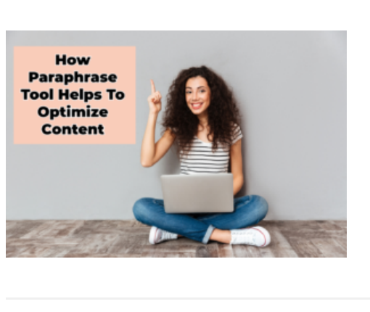
How Buying Instagram Followers Can Help Businesses Soar

TECH ARTICLES By Sarcastic Writer · February 25, 2023 · Comments off

With social media becoming more popular by the year, a growing number of businesses are looking for more ways to cash in on the phenomenon. Not long after the current craze started taking shape, companies realized they needed to establish... Read more

How To Find Gaps In Your Cybersecurity And How To Address Them

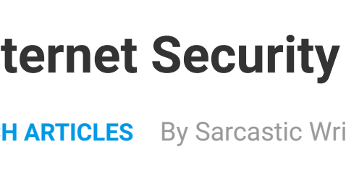
TECH ARTICLES By Sarcastic Writer · January 26, 2023 · Comments off



Cybersecurity has become a significant issue in today's digital world. Cases of phishing attacks, ransomware attacks, and data breaches have become increasingly common. In 2023, experts estimate the cost of cybercrime to cross the USD$8-trillion mark. This rise in cybercrime... Read more

How Paraphrase Tool Helps To Optimize Content

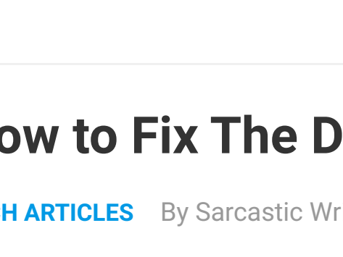
TOOLS By Sarcastic Writer · December 23, 2022 · Comments off



Content optimization is necessary to rank higher in search engine page results, especially if it is about promoting a blog post or online business. The readability and uniqueness of content significantly impact the ranking factor. Readability is good for the... Read more

How to close the site from indexing using robots.txt

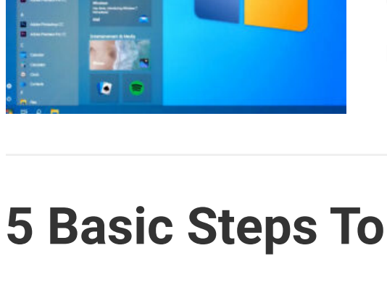
TECH ARTICLES By Sarcastic Writer · June 13, 2021 · Comments off



In this article, we answered five frequently asked questions about closing the site from search engines. Search engine crawlers scan all data on the Internet. Nevertheless, website owners can limit or deny access to their resource. This requires closing the... Read more

Internet Security With VPN – Why Do You Need It

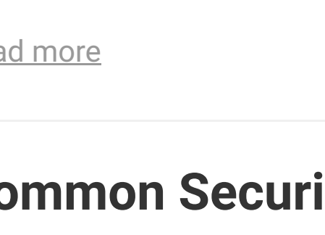
TECH ARTICLES By Sarcastic Writer · April 21, 2021 · Comments off



With growing numbers of individuals working remotely in pandemic of Covid-19, telecommuting or traveling with increasing frequency, the traditional business security model continues to evolve. With the advent of widely available high-speed Internet access coupled with VPN technologies; the secure,... Read more

How to Fix The DLL Missing Error in Windows 7?

TECH ARTICLES By Sarcastic Writer · April 16, 2021 · Comments off



DLL stands for Dynamic Link Library, and it is a file format that contains various codes and procedures that Windows programs can use to perform several tasks. It is also helpful in sharing data and resources since DLL allows programs... Read more

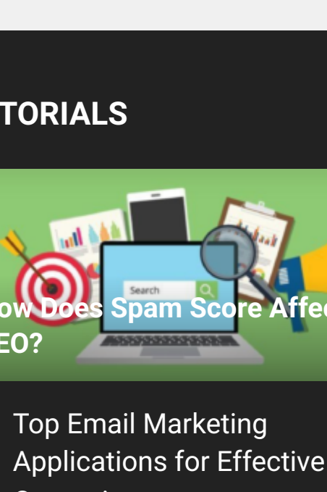
5 Basic Steps To Protect Your Personal Data Online

TECH ARTICLES By Sarcastic Writer · March 26, 2021 · Comments off

Even though news about another celebrity's hacked cloud storage – from Jennifer Lawrence to Hilary Clinton – appear regularly, many people think their personal information is not attractive to cyber criminals. However, practice shows that fame does not affect the... Read more

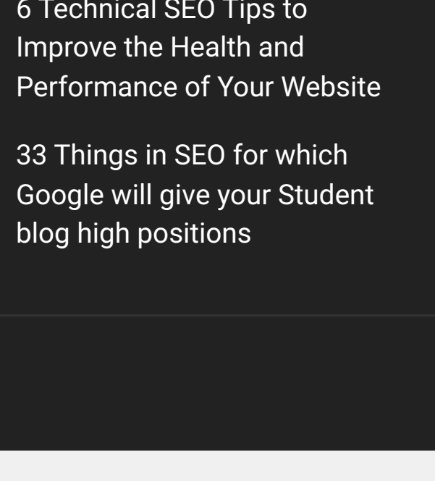
Common Security Threats and How to Secure your Windows PC

TECH ARTICLES By Sarcastic Writer · March 5, 2021 · Comments off



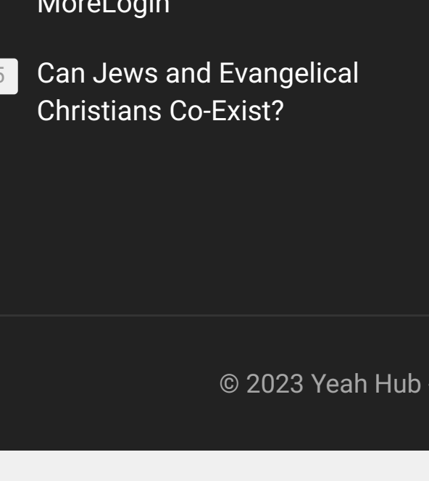
As technology continues to advance, hackers enhance their skills in using advanced malware and viruses. Cybersecurity threats have become more dangerous over the past few years, making it more difficult for computer users to keep up with data protection methods.... Read more

SEO



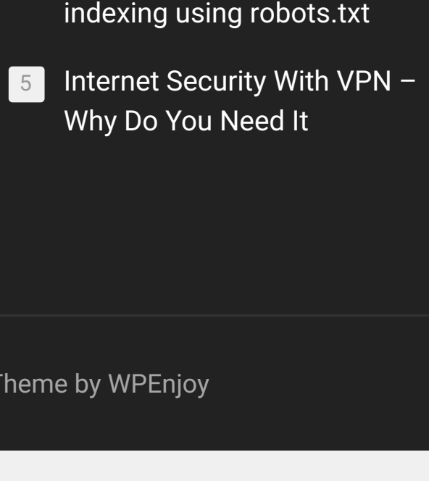
1. Local SEO: Must-Know Content Strategy for Every Business
2. 13 Tips To Optimize Your WordPress Site to Rank Better in SERP
3. Benefits of SEO in e-learning
4. 6 Technical SEO Tips to Improve the Health and Performance of Your Website
5. 33 Things in SEO for which Google will give your Student blog high positions

TUTORIALS



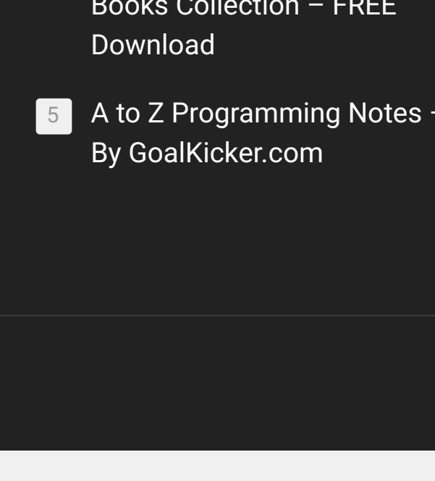
1. Top Email Marketing Applications for Effective Campaigns
2. Edit and Compile Code with the Best 5 Code Editors
3. 50+ Top DevSecOps Tools You Need To Know
4. Learn How to Add Proxy and Multiple Accounts in MoreLogin
5. Can Jews and Evangelical Christians Co-Exist?

TECH



1. Top 7 NodeJS Frameworks You Need To Know
2. How Buying Instagram Followers Can Help Businesses Soar
3. How To Find Gaps In Your Cybersecurity And How To Address Them
4. How to close the site from indexing using robots.txt
5. Internet Security With VPN – Why Do You Need It

BOOKS



1. Must Buy Python Books Collection – 2019 Update
2. Top 20 Hacking Books To Read Before You Die
3. Learn JavaScript with 50+ Resources/Ebooks
4. Biggest Hacking & Security E-Books Collection – FREE Download
5. A to Z Programming Notes – By GoalKicker.com

alexandre-lavoie / **ctf-tools** Public

Notifications Fork 0 Star 2

Code Issues Pull requests Actions Projects Security Insights

master 1 branch 0 tags Go to file Code

Alexandre Lavoie Added a few tools from iHack CTF. `60bb247` on Jun 23, 2020 **17** commits

README.md Added a few tools from iHack CTF. 3 years ago

README.md

CTF Tools

List of tools and resources for Pentesting and CTFs.

Table of Content

- General Tools
- Cryptography
- Forensics
- Pentesting
- Programming
- Network Exploitation
- Reverse Engineering
- Virtual Machines
- Web Exploitation
- Write-Ups and Tutorials

General Tools

- Visual Studio Code - IDE, Programming, text/binary, etc - it can do it all.

Cryptography

Resources

- XOR Cypher - Explains the algorithm (understand XOR is always useful - not only in cybersecurity)

Tools

- gchq CyberChef - Encryption, encoding, compression, data analysis tool.
- hashcat - Hash bruteforcing.
- John the Ripper - Hash bruteforcing.
- password-removal - Online ZIP password removal (uses john)

Forensics

Tools

- binwalk - Extracts hidden files in files.
- HxD - Hex Editor.
- gzip - Linux .gz decompressing.
- WinRAR - Decompression on Windows.
- minimodem - Decodes modem audio file or audio source to data.

Pentesting

Resources

- GTFOBins - List of base Linux vulnerable binaries.
- netcat - Simple reverse shell server.
- Reverse Shell Cheat Sheet - Reverse shell commands for various programs.
- ssh - Understanding the SSH protocol.
- DNS - Get information from DNS server.
- SMTP - Writeup for SMTP.

Programming

Languages

- Python - Useful for basically all CTF challenges (Recommend pwntools).

Resources

- Esoteric Languages - Obscure programming languages.

Network Explotation

Tools

- aircrack-ng - Tools to analyze network traffic.
- ipconfig / ifconfig - Get information about computer network.
- Wireshark - Network traffic monitoring.
- nmap - Port analysis.

Reverse Engineering

Resources

- ROP - Reference for Return-Oriented Programming.
- trailofbits Forensics - Reference for forensics challenges in CTF.

Tools

- Android Emulator - Android Emulator.
- Cheat Engine - Data debugger for Windows.
- dex2jar - APK to JAR.
- edb - Visual debugger for Linux.
- gdb - Standard debugger for Linux.
- Ghidra - Universal decompiler with C integrated.
- IDA Freeware - Universal decompiler with Visual Graphs.
- ILSpy - Decompiler for C# DLL and Executables.
- JD-GUI - Visual Decompiler for Java.
- ollydbg - Visual debugger cross platform (usually for Windows).

Virtual Machines

Images

- CTF-Env - Linux CTF Image for Docker.
- LiveOverflow Dockerfile - Dockerfile VM.
- Kali Linux - Robust Linux Cybersecurity Image.

Tools

- Docker - Lightweight linux virtualization.
- Hyper-V - Windows 10 virtualization.
- VirutalBox - Full OS virutalization.

Web Exploitation

Resources

- OWASP Top Ten - Common security vulnerabilities.
- PayloadsAllTheThings - Reference for most web exploits.
- SQL Injection - Understanding an SQL Injection Attack.
- XSS Scenarios - Scenarios / demonstration for typical XSS attacks.
- XXE Injection - Understanding an XXE Injection Attack.

Tools

- BurpSuite Community - HTTP and HTTPS traffic editing and monitoring
- Firefox - Browser with built-in proxy (easy to use with BurpSuite).
- Flask - Customize API with Python.
- gobuster - Website URL fuzzing.
- PostBin - GET and POST endpoint for testing requests.
- Postman - Customize web request.
- wfuzz - Website fuzzing.
- Flask Session Decoder - Decoder for `base64(payload).base64(time).base64(crypto)` .

Write-Ups and Tutorials

- LiveOverflow - Tutorials on many cybersecurity topics and write-ups for CTFs.
- IppSec - Write-ups on HackTheBox VMs.

About

List of tools for CTFs

Readme
Activity
2 stars
3 watching
0 forks
Report repository

Releases

No releases published

Packages

No packages published

apsdehal / **awesome-ctf** Public

proditis Minor updates and fixes (#141) … `eb504b2` on May 18, 2020 **232** commits

tests	Complete tests for the repo	8 years ago
.gitignore	Add gitignore, test.js	8 years ago
.travis.yml	Add travis file	8 years ago
CONTRIBUTING.md	Update instructions in Contributing to include testing information	8 years ago
LICENSE	Change LICENSE to CC0	7 years ago
README.md	Minor updates and fixes (#141)	3 years ago
_config.yml	Set theme jekyll-theme-slate	5 years ago
package.json	Change name to awesome-ctf	8 years ago

README.md

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

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.
- Haaukins- 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 plaform 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 Obfustcators

- 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, 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.
- 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.
- 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.
- 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.
- BinWalk - Analyze, reverse engineer, and extract firmware images.
- Boomerang - Decompile x86/SPARC/PowerPC/ST-20 binaries to C.
- ctf_import – run basic functions from stripped 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 instrumentaion tool by Intel.
- PINCE - GDB front-end/reverse engineering tool, focused on game-hacking and automation.
- PinCTF - 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 - Aperi'Solve is a platform which performs layer analysis on image (open-source).
- 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.
- 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.
- 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.
- 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 testor.

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.
- URIX 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.RED - 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.
- PWN Challenge - 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.
- Viblo CTF - Various amazing CTF challenges, in many different categories. Has both Practice mode and Contest mode.
- 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.

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 occuring around the worlds.
- Reddit Security CTF - Reddit CTF category.

Wikis

Various Wikis available for learning about CTFs

- Bamboofox - Chinese resources to learn CTF.
- bi0s Wiki - Wiki from team bi0s.
- 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
- 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.
- 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 :)

About

A curated list of CTF frameworks, libraries, resources and softwares

apsdehal.in/awesome-ctf/

Releases

No releases published

Packages

No packages published

Used by 8

Contributors 74

+ 63 contributors

Languages

JavaScript 100.0%