RVCTF Training

Non-exhaustive compilation of resources/tools.

Whatsapp Aaron(+65 8719 1734) if you have any suggestions/find any errors.

FLAGS UP, GAME ON.

[**Absolute Beginner's Guide 2**](#_rn51kvwhu24i)

[**TROUBLESHOOTING AND DEBUGGING 3**](#_n8q790pe4mti)

[**Coding (good to learn) 5**](#_op6l2calxcku)

[Youtube 5](#_qt4qrgooaty)

[Documentations 5](#_jbu0h7tqs1kj)

[**Courses (ay Sec4s gap month hehe) 6**](#_59v1azbzr0o8)

[Self-paced courses 6](#_btntp6f8nwuv)

[Instructor-paced courses 6](#_ba2jrwe3a8zu)

[Certificate assessments 6](#_j0op7udda0hv)

[**Youtube 7**](#_ry4lt28xrihq)

[CTF youtube channels 7](#_o69s0910bucy)

[**Documentations 8**](#_x6femttns8cw)

[GENERAL DOCUMENTATION PLATFORMS 8](#_h85cel6vuczi)

[Cryptography 8](#_ns39j0skv01m)

[Forensics 8](#_yyaqci3apmp1)

[Web exploitation 8](#_i2i1v5l5yocx)

[Binary exploitation 8](#_7g7olcgqwgq)

[Reverse Engineering 8](#_3b6uokg4maxu)

[OSINT (not commonly found in CTFs) 8](#_n382cgh8xvvq)

[Data science (Cyberthon only) 9](#_cxu9z7fhztw1)

[**CTF Tools and Tutorials 10**](#_7ujco68t9a6g)

[Cryptography 10](#_eebomz8leqnr)

[Forensics 11](#_81otp8i1pshx)

[Web exploitation 11](#_no5zflg1wohk)

[Binary Exploitation 11](#_imn7nwsmuveb)

[Reverse engineering 11](#_oxzd1vxj5rrm)

[OSINT 11](#_9qaxfdqexigv)

[Data science 12](#_zb10qpiljdoc)

[**CTF Practice Websites 13**](#_dh6j9wegzj92)

[General (all topics) 13](#_1td2f999ix7i)

[Web Exploitation 13](#_9xfj9hxw4u4n)

[Box Pentesting 13](#_k2g7anx8ch6v)

# 

# Absolute Beginner's Guide

[Beginner’s Guide to Capture the Flag (CTF) | by The Hackers Meetup | Medium](https://thehackersmeetup.medium.com/beginners-guide-to-capture-the-flag-ctf-71a1cbd9d27c)

[The ctf playbook](https://fareedfauzi.gitbook.io/ctf-playbook/web)

Some RVCTF session documentations you may find helpful :

[004 RESOURCES](https://drive.google.com/drive/folders/1lM9M7ZKHPRgFiOCJhFq4Qm0nUUOzpAxH?usp=sharing) (OUR CCA RESOURCE DRIVE !!)

# TROUBLESHOOTING AND DEBUGGING

We highly recommend you to Google around and use ChatGPT for troubleshooting and debugging, it will be very effective for your learning :D If all fails you, feel free to DM our instagram (rv.ctf) or our ExCos (allocated to different categories) ! Don’t be shy, and happy CTFing :3

Troubleshooting tips :

* Stuck on a CTF practice question ? Google <CTF practice site name> <challenge name> writeup. E.g. CTFlearn my blog writeup
* Don’t understand source code from question >> chatgpt it (can try the google ai Bard now that its out)

**Coding :**

ChatGPT

**Cryptography :**

Charles

+65 9335 3150 (Whatsapp)

@p0pet\_t (Instagram)

Zhumo

+65 9640 2658 (Whatsapp)

Zian

+65 9712 5966 (Whatsapp)

**Forensics :**

*Zian*

*+65 9712 5966 (Whatsapp)*

**Web exploitation :**

*Charles*

*+65 9335 3150 (Whatsapp)*

*@p0pet\_t (Instagram)*

**Binary Exploitation :**

*Zhumo*

+65 9640 2658 (Whatsapp)

**Reverse engineering :**

**OSINT :**

*Zian*

+65 9712 5966 (Whatsapp)

*Aaron*

+65 8719 1734 (Whatsapp)

# Coding (good to learn)

## Youtube

FreeCodeCamp

CodingTrain

## Documentations

[Python Tutorial](https://www.w3schools.com/python/default.asp) (personal recommendation)

[C Tutorial](https://www.w3schools.com/c/index.php) (if you really like things the hard way)

# 

# Courses (ay Sec4s gap month hehe)

Courses that introduce you to the fundamental theory of cybersecurity. CTF applications not included.

## Self-paced courses

[HarvardX: CS50's Introduction to Cybersecurity | edX](https://www.edx.org/learn/cybersecurity/harvard-university-cs50-s-introduction-to-cybersecurity?index=product&objectID=course-88391405-e329-495d-bf72-5de13bbf1846&webview=false&campaign=CS50%27s+Introduction+to+Cybersecurity&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (10-30 hours)

[IBM Cybersecurity Basics](https://www.edx.org/learn/cybersecurity/ibm-cybersecurity-basics?index=product&objectID=course-53e0b3db-0712-495f-9ce6-f12045373a5b&webview=false&campaign=Cybersecurity+Basics&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (16-32 hours)

[IBM Beginner's Guide to Cybersecurity](https://www.edx.org/learn/cybersecurity/ibm-beginners-guide-to-cybersecurity?index=product&objectID=course-cc2b4496-bccb-4ddc-b6d9-a6ad7d05d28f&webview=false&campaign=Beginners+Guide+to+Cybersecurity&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (12-20 hours)

[UWashingtonX: Introduction to Cybersecurity | edX](https://www.edx.org/learn/cybersecurity/university-of-washington-introduction-to-cybersecurity?index=product&objectID=course-db4c2a32-da56-48c1-b33e-d4924d855510&webview=false&campaign=Introduction+to+Cybersecurity&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (12-30 hours)

[EDx Ethical Hacking](https://www.edx.org/learn/computer-programming/edx-try-it-ethical-hacking?index=product&objectID=course-8776d574-3bd3-4670-80a0-3a369bb18696&webview=false&campaign=Try+It%3A+Ethical+Hacking&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (1-2 hours per week)

[IBM Penetration Testing and Incident Response](https://www.edx.org/learn/penetration-testing/ibm-penetration-testing-and-incident-response?index=product&objectID=course-030f3b32-99e9-460e-a1d0-dc8cb61de5e0&webview=false&campaign=Penetration+Testing+and+Incident+Response&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (16-20 hours)

[EDx Cybersecurity Basics](https://www.edx.org/learn/cybersecurity/edx-try-it-cybersecurity-basics?index=product&objectID=course-ada7a9ec-3cfa-48db-86d0-16b11fc262a6&webview=false&campaign=Try+It%3A+Cybersecurity+Basics&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (1-2 hours)

## Instructor-paced courses

[Rochester Institute of Technology - Cybersecurity Fundamentals](https://www.edx.org/learn/cybersecurity/rochester-institute-of-technology-cybersecurity-fundamentals?index=product&objectID=course-bb90d02a-a562-4632-a0af-e72987f27fea&webview=false&campaign=Cybersecurity+Fundamentals&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (2024 Jan8-Mar4, 80-96 hours)

[Rochester Institute of Technology - Network Security](https://www.edx.org/learn/network-security/rochester-institute-of-technology-network-security?index=product&objectID=course-9ff9b63d-f504-424c-978a-be0b6fab8e96&webview=false&campaign=Network+Security&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (2024 Jan8-Mar4, 80-96 hours)

[Rochester Institute of Technology - Computer Forensics](https://www.edx.org/learn/computer-forensics/rochester-institute-of-technology-computer-forensics?index=product&objectID=course-d2fb4b76-e398-42d8-9835-970a49678fa3&webview=false&campaign=Computer+Forensics&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (2024 Jan8-Mar4, 80-96 hours)

[Rochester Institute of Technology - Cybersecurity Risk Management](https://www.edx.org/learn/risk-management/rochester-institute-of-technology-cybersecurity-risk-management?index=product&objectID=course-c913261b-8081-4f28-9c10-0079b616ab39&webview=false&campaign=Cybersecurity+Risk+Management&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (2024 Jan8-Mar4, 80-96 hours)

## Certificate assessments

[IBM Cybersecurity Analyst Assessment](https://www.edx.org/learn/cybersecurity/ibm-cybersecurity-analyst-assessment?index=product&objectID=course-236ea439-1b6a-42c8-ad87-eef0d779aa4f&webview=false&campaign=Cybersecurity+Analyst+Assessment&source=edX&product_category=course&placement_url=https%3A%2F%2Fwww.edx.org%2Flearn%2Fcybersecurity) (3-4 hours)

# 

# 

# Youtube

## CTF youtube channels

[0: Intro/Basics/Setup - Buffer Overflows - Intro to Binary Exploitation (Pwn)](https://www.youtube.com/watch?v=wa3sMSdLyHw&t=125s&ab_channel=CryptoCat)

[Top 10 Cyber-Security Youtube Channels To Follow | Learn CTF | Learn To Hack](https://www.youtube.com/watch?v=QcOnhf1KJdU)

[Top 10 Cybersec / Hacking Youtube Channels (2021)](https://www.youtube.com/watch?v=azndMJjXDQ4)

[Liveoverflow](https://www.youtube.com/channel/UClcE-kVhqyiHCcjYwcpfj9w)

# Documentations

## GENERAL DOCUMENTATION PLATFORMS

[Cycubix Docs](https://docs.cycubix.com/)

[CTF 101](https://ctf101.org/)

## Cryptography

[Category:Classical ciphers - Wikipedia](https://en.wikipedia.org/wiki/Category:Classical_ciphers) (list of ciphers, not full)

[Category:Cryptographic algorithms - Wikipedia](https://en.wikipedia.org/wiki/Category:Cryptographic_algorithms) (list of crypto algorithms, not full)

[Practical Cryptography](http://practicalcryptography.com/)

[Cryptography concepts - IBM i](https://www.ibm.com/docs/en/i/7.5?topic=cryptography-concepts)

[Cryptography Tutorial](https://www.geeksforgeeks.org/cryptography-tutorial/?ref=lbp)

[Cryptography](https://ctf101.org/cryptography/overview/) (personal recommendation)

[Cryptool](https://www.cryptool.org/assets/ct1/presentations/CrypTool1-Presentation-en.pdf) (wow)

## Forensics

[Forensics](https://ctf101.org/forensics/overview/) (personal recommendation)

[Chapter 1. Introduction](https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html) (wireshark tutorial)

[Forensics – SANReN Cyber Security Challenge](https://www.csc.ac.za/?page_id=249)

[List of file signatures - Wikipedia](https://en.wikipedia.org/wiki/List_of_file_signatures)

[GCK'S File Signatures Table](https://www.garykessler.net/library/file_sigs.html) (seniors recommendation)

[Forensics · CTF Field Guide](https://trailofbits.github.io/ctf/forensics/)

## Web exploitation

[SQL Tutorial](https://www.w3schools.com/sql/default.asp) (good to understand SQL injection in-depth)

[Burpsuite Academy](https://portswigger.net/web-security/dashboard) (learn almost all CTF web topics)

## Binary exploitation

[Binary Exploitation](https://ctf101.org/binary-exploitation/overview/) (understanding binary exploitation)

[GitHub - Bretley/how2exploit\_binary: An in depth tutorial on how to do binary exploitation](https://github.com/Bretley/how2exploit_binary) (in-depth + practices)

## Reverse Engineering

[Reverse Engineering Resources-Beginners to intermediate Guide/Links | by Bbinfosec](https://bbinfosec.medium.com/reverse-engineering-resources-beginners-to-intermediate-guide-links-f64c207505ed) (intro)

[Reverse Engineering](https://0xinfection.github.io/reversing/reversing-for-everyone.pdf) (op form)

## OSINT (not commonly found in CTFs)

[OSINT Framework](https://osintframework.com/) (USE RESPONSIBLY. VERY RESPONSIBLY. )

## Data science (Cyberthon only)

<https://www.kaggle.com/> (covered in 2023 Cyberthon training)

# CTF Tools and Tutorials

( Seniors version : [Training Platforms and Tools](https://docs.google.com/document/d/1tiQ6H24kFv2PZOONLnsWJuDv3muN3Z7jn9wxiCvgli8/edit?usp=sharing)  )

## Cryptography

Online tools (for beginner challenges)

<https://www.dcode.fr/en> - useful cipher identifier

<https://www.boxentriq.com/>

<https://rumkin.com/tools/cipher/>

++ other misc cryptography tools online. You can find one thats easiest for you to use :D

Tools on Kali Linux :

hashcat - password cracker

<https://resources.infosecinstitute.com/topics/hacking/hashcat-tutorial-beginners/>

<https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/>

<https://youtu.be/5fy6Lq1vgZk?si=STTNa6Q-T0ckUx-G>

<https://www.youtube.com/watch?v=irQlWaH0LPQ>

<https://www.stationx.net/how-to-use-hashcat/>

John The Ripper - password cracker

<https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/>

<https://www.varonis.com/blog/john-the-ripper>

<https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-John-the-Ripper-password-cracker>

<https://www.stationx.net/how-to-use-john-the-ripper/>

hydra - password cracker

<https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/>

<https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-Hydra-password-cracking-tool>

RsaCtfTool - designed for RSA decryption

<https://github.com/RsaCtfTool/RsaCtfTool>

## 

## Forensics

Online tools (for beginner challenges) :

<https://cyberchef.org/> - forensics section

<https://www.aperisolve.com/> - for steganography

<https://hexed.it/> - HEX editing

Tools on Kali Linux :

binwalk - file extractions

<https://allabouttesting.org/short-tutorial-firmware-analysis-tool-binwalk/>

<https://fr3ak-hacks.medium.com/analysing-and-extracting-firmware-using-binwalk-982012281ff6>

Wireshark - network forensics

<https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html>

<https://www.varonis.com/blog/how-to-use-wireshark>

## Web exploitation

WebGoat - training platform to be installed on Kali Linux

sqlmap - SQL injections (USE RESPONSIBLY)

<https://medium.com/@cuncis/the-ultimate-sqlmap-tutorial-master-sql-injection-and-vulnerability-assessment-4babdc978e7d>

<https://hackertarget.com/sqlmap-tutorial/>

Burp Suite - network analysis

<https://portswigger.net/burp/documentation/desktop/getting-started>

## Binary Exploitation

Python

## Reverse engineering

Ghidra

<https://www.varonis.com/blog/how-to-use-ghidra>

Clang (already installed in Kali Linux)

<https://kevinaboos.wordpress.com/2013/07/23/clang-tutorial-part-i-introduction/>

radare2 (pre-installed in Kali Linux)

[How to Reverse Engineering with Radare2 (A Quick Introduction) « Null Byte](https://null-byte.wonderhowto.com/how-to/reverse-engineering-with-radare2-a-quick-introduction-0165996/)

## OSINT

NIL, just google around for flag lol

## 

## Data science

Kaggle (+python)

<https://www.kaggle.com/>

## 

# 

# CTF Practice Websites

## 

## General (all topics)

[Imaginary CTF](https://imaginaryctf.org) (most realistic for practice)

[PicoCTF](https://play.picoctf.org/practice) (relatively easy)

[CTFLearn](https://ctflearn.com) (easier-best for starters)

[Cryptohack](https://cryptohack.org/) (CTF questions for cryptography)

## Web Exploitation

[XSS Game](https://xss-game.appspot.com)

[LordOfSQL](https://los.rubiya.kr)

[Burpsuite Labs](https://portswigger.net/web-security/all-labs)

[Hacker 101](https://www.hacker101.com/) (practical bug bounty)

## Box Pentesting

[OverTheWire](https://overthewire.org/wargames/)

[SmashTheStack](https://www.smashthestack.org/main.html#wargames)

[Exploit.Education](https://exploit.education)