**Note:** This is a copy of the content found on the CyberHawks Discord server #resources channel.

# Your #1 Resources by Category

## Binary Exploitation (Exploit Development)

Software vulnerabilities/exploits on the lowest level, how to develop 0-days, bug bounty

• [Pwn College](https://pwn.college/) - Also check out their [YouTube channel](https://www.youtube.com/c/pwncollege/playlists)

• [Protostar](https://exploit.education/protostar/) - Also check out [this videoseries](https://www.youtube.com/watch?v=iyAyN3GFM7A&list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN)

## Pen Testing

Conducting network scans, locating vulnerabilities, modifying premade exploits to gain access

Learn: TryHackMe or Zero to Hero Pentesting → Practice: HackTheBox and VulnHub

• [TryHackMe](https://tryhackme.com/) - Check out the Offensive Pentesting and Jr Penetration Tester paths

• [Zero to Hero Pentesting](https://www.youtube.com/watch?v=qlK174d_uu8&list=PLLKT__MCUeiwBa7d7F_vN1GUwz_2TmVQj)

• [HackTheBox](https://www.hackthebox.com/)

• [VulnHub](https://www.vulnhub.com/)

## Social Engineering

Man in the Middle, phishing, credential harvesting, bad USB, OSINT, email spoofing

• [Videos on social engineering topics](https://www.youtube.com/watch?v=A7TGrEPIZ_0&list=PLSpsCUl2cY8Zo3nVE3FmeJ0XR0DS2demz)

‣ [Presentations from videos](https://drive.google.com/drive/folders/1OiF-Aq5wiW9E3YgpCBn-LWkDuHqnAs6I/)

• [Fall 2021 assignments](https://docs.google.com/document/d/1zgdOtgy5sf1MujpCmZL0bDgBLMvwTKXONt3H3xShdK4) (good for practice and individual learning)

## Malware Development/Analysis

Developing and detecting files that perform unauthorized activity when run

Free:

• [Intro to DOT NET malware](https://www.youtube.com/watch?v=8lk6VhmlhoI)

• [TryHackMe (on malware analysis)](https://tryhackme.com/module/malware-analysis)

• [Pwn College (on reversing)](https://pwn.college/modules/reversing)

AV Evasion

• <https://www.ired.team/offensive-security/defense-evasion/>

• <https://wikileaks.org/ciav7p1/cms/files/BypassAVDynamics.pdf>

Paid:

• [Udemy beginner course (development)](https://www.udemy.com/course/malware-development-beginner-level/)

• [TCM course (analysis)](https://academy.tcm-sec.com/p/practical-malware-analysis-triage)

## Defense

Hardening (securing), realtime monitoring, applying corrective actions in the event of an attack

Resources are poor, mostly because the industry uses existing paid software like Splunk, so I kind of learned this on my own. Also check out my Linux cheat sheets in the cheat sheets section. Honestly though, my specialty is offense so my knowledge here is lacking.

• [TryHackMe](https://tryhackme.com/)

• It may also be worth going the book route for this - read through some Linux/Windows fundamentals books, forensics books, or take the ITM forensics course. Check out the Books section!

## CTF

Capture-the-Flag style challenges: codebreaking, reverse engineering, crypto, binary exploits, capture analysis, etc.

I'm not that interested in CTFs specifically because they tend to not be applicable to real-world scenarios. Most of my CTF knowledge comes from exploit development and pen testing, so if there's a specific area within CTFs you want to get better at, let me know because I'll likely have resources for it. The best way to get better at CTFs is to participate in them. I've attempted PicoCTF and NCL. But I was also recommended RootMe (by Sarah) specifically for CTFs and OverTheWire (by Michael) for cybersecurity concepts in general.

• [RootMe](https://www.root-me.org/)  
 • [OverTheWire](https://overthewire.org/)

## Physical Security

Breaking-and-entering, under the door, bypass, keycard cloning

If you have any questions about or want a demo of my break-in tools, let me know.

• [TheNotSoCivilEngr on YouTube](https://www.youtube.com/channel/UCd6KUzV7wcdm3Nc85Xa-tUw) - especially check out [this video](https://www.youtube.com/watch?v=7FullVIDj9o) for tools and [this one](https://www.youtube.com/watch?v=jcVIruSqI6w) for an example break-in scenario

• For lockpicking, check out [LockPickingLawyer](https://www.youtube.com/channel/UCm9K6rby98W8JigLoZOh6FQ)

# Job Preparation

[Cybersecurity Certifications List](https://docs.google.com/document/d/1BbYJhduq0b3pEWsuWsqqtoMPlYH-SASrU8kwzdT9yeI/)

[Cybersecurity Careers List](https://docs.google.com/document/d/100O1KszmoTufqHwHxY_ZKux4JfejieIM_kQ8tMUzfmM/)

# Cheat Sheets

[Kali Linux (offensive)](https://docs.google.com/document/d/1MYIUJ-HvIDI1A8RPldMEcrVAOQzABeT_E0yaaN8rKKs/)

[Linux Commands](https://docs.google.com/document/d/1vJxoHrjW607NJDLC1Zln1llrEIqrS6Ea3j9ihJTdblg/)

[Linux Defense Checklist](https://docs.google.com/document/d/1clHbKElHkmNRgSKz21c-2q4R1rMhVodCm_NZV_upWhY/)

[Linux Defense and Services Cheat Sheet](https://docs.google.com/document/d/1DikLS0jAhuflCj3bOlbh5ZIJE6Ou4WkyIxMN0t2ZqU0/)

[Linux Defense Scripts](https://github.com/TheCatLover/Linux-Defense-Scripts)

# CyberHawks Video Channels

• [YouTube Channel](https://www.youtube.com/channel/UCuYP-AZUcHEZMmUyb1MpZyw) - managed by me and Przemek (but mostly me)

• [Official Video Content](http://cyberhawks.iit.edu/videos.html) - managed by David and Grace

# Additional Resources

• <https://www.youtube.com/c/PowerCertAnimatedVideos> - easy to follow videos on networking and computer concepts relevant to cybersecurity

• \*\*\* <https://overthewire.org/> - fantastic set of challenges in cybersecurity topics (especially recon and exploitation) and good place to start for beginners (check out Bandit)

• <https://github.com/swisskyrepo/PayloadsAllTheThings> - nice cheatsheets

• <https://daviscybersec.org/resources> - great PowerPoints on a bunch of topics

• <https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA> - security channel

• <https://www.youtube.com/channel/UC0ZTPkdxlAKf-V33tqXwi3Q> - another security channel

• <https://www.youtube.com/user/NetSecNow> - another security channel

• <https://www.offensive-security.com/pwk-oscp/> - OSCP pen testing course

• <https://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob> - blog with OSCP prep/pentesting stuff

• \*\*\* <https://docs.google.com/document/d/1USipV0CtxLibqxJ3xJL2-5_yuJXb-q_CUnL6N4cKt3g/> - the original doc with all these resources - has a good overview of various cybersecurity topics

## Books

Thanks to Przemek, I have access to the following book PDFs:

• The Art of Memory Forensics

• Malware Analyst's Cookbook and DVD

• Practical Reverse Engineering

• Cryptography Engineering

• Advanced Penetration Testing

• Threat Modeling: Designing for Security

• Security Engineering (2nd ed)

• Windows Operating System Fundamentals

There are some additional hardcover books available upon request.

## Discord Servers

Thanks to Ty, I have access to the following Discords:

• OnlyFeet

• The Alh4z-R3d Team

• n00b\_Sec

• The Taggart Institute for Cybering Good

• TCM Security

• HackTheBox

• pwn.college

• CFC red team village