<https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-exact-location-any-ip-address-0161964/>

[~~http://kmb.ufoctf.ru/stego/stegsolve/main.html~~](http://kmb.ufoctf.ru/stego/stegsolve/main.html)

[~~https://github.com/zardus/ctf-tools/blob/master/stegsolve/install~~](https://github.com/zardus/ctf-tools/blob/master/stegsolve/install) ~~- Have in another one~~

<https://wargame.whitehat.vn/Challenges/ChallengesContest/38>

Redteams.net

~~How to break into Toyota canyon~~

Program that removes systemfiles (They screw up copying data) and maybe add on finding duplicate files and rid of invalid url and empty folders

~~Eggshell cracking (iPhone/IOS)~~

* [~~https://www.youtube.com/watch?v=3hITafnHgJs~~](https://www.youtube.com/watch?v=3hITafnHgJs)

<http://www.computersecuritystudent.com/UNIX/FEDORA/lesson1/index.html>

<https://null-byte.wonderhowto.com/forum/use-null-byte-study-become-professional-hacker-0159816/>

~~KOplayer to emulate an android~~

Jailbreaking iPhone

<https://gist.github.com/heiswayi/502fd1dd79c985a58c58>

[~~https://pythonprogramming.net/image-recognition-python/~~](https://pythonprogramming.net/image-recognition-python/) ~~- already know this and don’t really need it~~

[~~https://www.pyimagesearch.com/2017/07/10/using-tesseract-ocr-python/~~](https://www.pyimagesearch.com/2017/07/10/using-tesseract-ocr-python/) ~~- Need to write program for this~~

<https://www.endgame.com/blog/technical-blog/how-get-started-ctf>

[~~https://github.com/apsdehal/awesome-ctf~~](https://github.com/apsdehal/awesome-ctf)

More Hacking Tools

[~~https://www.youtube.com/watch?v=oBpo5sElrMY~~](https://www.youtube.com/watch?v=oBpo5sElrMY)

[~~https://www.youtube.com/watch?v=Q8hAjEaAgE8~~](https://www.youtube.com/watch?v=Q8hAjEaAgE8)

[~~https://www.youtube.com/watch?v=kCSu9gLx6Lw~~](https://www.youtube.com/watch?v=kCSu9gLx6Lw)

Shell code

[~~https://github.com/MunGell/awesome-for-beginners~~](https://github.com/MunGell/awesome-for-beginners)

Look into Snort

How to get past NC Challenges

LLVM – OSX disassembler

Ocfa for forensics

Build Sudoku Code again

Morse code decoder based on prediction and not reading it straight through

PHP Vulnerabilities

SQLmap

~~What is the requirement to speak at Def Con~~

<http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html>

Payloads  
https://pentestbox.org

Over the wire

DEEP image search: <https://www.pyimagesearch.com/2014/11/10/histogram-oriented-gradients-object-detection/>

Things to look at

Arp cache capturing

~~Defcon.com~~

<https://captf.com/practice-ctf/>

<https://trailofbits.github.io/ctf/>

<https://www.youtube.com/watch?v=BcDbKlz06no>

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

<https://www.youtube.com/watch?v=P2_2ArKPzds&list=PLt_Hvzh8oeR5S27UaoKDx2qqYZcpokGL5&index=4>

Smash the Stack

<https://developer.nvidia.com/how-to-cuda-python>

<https://www.anaconda.com/distribution/>

Parallel Computing

Read website hacking book

List of hacking websites

Scan website for vulnerabilities (Firewall)

Reverse engineering books

~~Learn php and MySql – Tough but going to because have a class on it~~

Metasploit and Wireshark , zero day book

~~Make more videos – Taking a break because I have done almost all of the ones possible to me.~~

Enterprise security risk management

<https://www.hackthis.co.uk/>

Investigating browser history

Pen Test Book

copying partition images, and netcat instances

Get into hacking communities

Involved in oswpa derbycon

Black hat.com

NSA.gov/ia/acedemic\_outreach/

Nat\_cae/index.html

We.penetration-standard.org

Areas

Ethical hacking

Web application security

System security

Reverse engineering

Tool development

Malware analysis

Defense security

Software security

Digital forensics

Wireless security

Owasp top ten projects

Metasploit unleashed

De-Ice

Heorot.net/livecds

Hacker defender and 3 files

Pass the hash?

Practice websites?

What is zone transfer?

What is lst filetype?

Movie swordfish

**Research The Stuff in the Pen Testing Notes**

Look into maintaining a permeant backdoor

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

[~~https://www.youtube.com/watch?v=EnlDejocu3o~~](https://www.youtube.com/watch?v=EnlDejocu3o)

<https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/>

<https://null-byte.wonderhowto.com/how-to/seize-control-router-with-routersploit-0177774/>

<http://gifcreator.me/>

[~~https://github.com/Hack-with-Github/Awesome-Hacking~~](https://github.com/Hack-with-Github/Awesome-Hacking)

Metadata Extrator

[~~https://github.com/drewnoakes/metadata-extractor~~](https://github.com/drewnoakes/metadata-extractor)

~~Vulnerability scanning – Already have this added~~

How to get ports open on a website

~~Downloading steogo magic. – Cannot find~~

Advance cookie manager to manipulate cookies on firefox (Log into someones account)

Steal cookies through XSS or packet sniffin

Popular attack: DNS changer

Hacking websites from book 2 (Not the best)

Hellbound hackers

How to wipe IE history

Viewing IE history

SANS & Rob lee

How does checking archives work on 7z

<https://www.vulnhub.com/resources/>

How does Bluetooth pairing work

Termineter

Questions

Automated XSS scripting

SQL injections

Cookies

Session id

Manipulating what variables

Webshells

***(Executing a file in CMD)***

OSSTM and PTES methodologies

Configure and starting Nessus (pg 29)

~~Nikto (pg 32)~~

~~Update : perl nikto.pl -update~~

Metasploit vm

Sharingmyip.com – gets information for websites (ip, dns, services ip, etc)

Burp as a proxy

Intercept turn off if not loading

Prompt for guidance

Contact us and forms problems (automated)

Linux add admin

Windows add admin

Net local group administrators username /add

(Use is to escalate power or cat etc/passwd)

Networking

Creating a zeroday

File signatures

Encrypting executables

Guarantee authentication (on infected machines)

Tcp connection creation

Pgp & ssl