<https://exploit.courses/#/challenges>

<https://github.com/ChrisTruncer/PenTestScripts>

<https://realpython.com/blog/python/primer-on-jinja-templating/>

<https://github.com/Bash-it/bash-it>

**Awesome:**

<https://github.com/jivoi/junk>

<https://dhavalkapil.com/blogs/Shellcode-Injection/>

<https://rich0gentoo.wordpress.com/2012/01/21/a-quick-dracut-module/>

<https://github.com/rhinstaller/anaconda/blob/master/dracut/README>

<https://samsclass.info/126/proj/127-p0_Jasmin.htm>

<http://www.jasonbernier.com/oscp-review/>

<https://www.avarx.io/tag/kioptrix/>

<https://www.theweakestlink.es/index.php/2016/04/18/from-metasploit-module-to-pyhton-standalone-with-the-help-of-wireshark/>

**awesome**

**https://roguesecurity.in/2017/12/16/hack-the-box-nineveh-writeup/**

<https://forums.offensive-security.com/search.php?searchid=643579>

<https://github.com/infoslack/awesome-web-hacking>

<http://bxi.es/Reversing-Exploiting/LinuxExploitWritingTutorial(by%20Sickness)/>

<https://support.offensive-security.com/#!pwk-kali-vm.md>

<https://support.offensive-security.com/#!pwk-connectivity-guide.md>

<https://support.offensive-security.com/#!pwk-connectivity-guide.md>

<https://the.earth.li/~sgtatham/putty/0.58/htmldoc/Chapter9.html>

<https://unix.stackexchange.com/questions/65745/command-scripts-to-check-the-reverse-dns-lookup-time>

<https://samsclass.info/127/127_S18.shtml#lecture>

<https://canvas.instructure.com/courses/1271494/assignments/7856085?module_item_id=15734619>

<https://manybutfinite.com/post/anatomy-of-a-program-in-memory/>

<https://www.youtube.com/watch?v=y7SWXTyXF0E>

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

<http://zempirians.com/ebooks/>

<https://doc.lagout.org/network/>

windows Privilleges

<http://toshellandback.com/2015/11/24/ms-priv-esc/>

 vulnhub

https://www.vulnhub.com/lab/reading/

OSCP Video

file:///G:/OSCP/pwk-35719-370111/index.html#module=Passive Info Gathering&sub-module=Overview&time-offset=63

<https://github.com/EbookFoundation/free-programming-books/blob/master/free-programming-books.md#assembly-language>

<https://chortle.ccsu.edu/AssemblyTutorial/Chapter-01/ass01_3.html>

<http://www.securitytube.net/video/208>  
-or-  
<https://www.youtube.com/watch?v=-ECNMxZBLa0>

<https://forums.offensive-security.com/forumdisplay.php?f=39>

<http://www.irongeek.com/i.php?page=videos/ncat-nmap-netcat>

Download

<http://www.mrjoeyjohnson.com/Documents/Cryptography/>

<https://github.com/laramies/theHarvester>

<http://www.r00tsec.com/2012/11/howto-manual-pentest-windows-cheatsheet.html>

<http://0daysecurity.com/articles/hping3_examples.html>

<https://danwin1210.me/>

<https://www.slideshare.net/chrisgates/devoops-attacks-and-defenses-for-devops-toolchains>

<https://pen-testing.sans.org/blog/2013/07/24/plundering-windows-account-info-via-authenticated-smb-sessions>

https://gist.github.com/jivoi

<https://www.samba.org/samba/docs/current/man-html/rpcclient.1.html>

<https://raw.githubusercontent.com/portcullislabs/enum4linux/master/enum4linux.pl>

#### Security Courses

* **ComputerSecurityStudent**: <https://www.computersecuritystudent.com/>
* **eLearn Security**: <http://www.elearnsecurity.com/>
* **Hacking Dojo**: <http://hackingdojo.com/>
* **MDSec**: <http://mdsec.net/>
* **Offensive Security**: <https://www.offensive-security.com/>
* **Security Tube Training**: [http://securitytube-training.com/](http://www.securitytube-training.com/)
* **The Hacker Academy**: <http://www.thehackeracademy.com/>

#### Training Material

* **nets.ec** (used to be called "Blackhat Library"): <https://nets.ec/Main_Page>
* **Codecademy**: <http://www.codecademy.com/>
* **Corelan**: <https://www.corelan.be/index.php/articles/>
* **End Game (How to Get Started in CTF)**: <http://www.endgame.com/>
* **Hacking Cisco**: <http://hackingcisco.blogspot.com/>
* **Metasploit Unleashed**: <http://www.offensive-security.com/metasploit-unleashed/>
* **N00b pentesting**: [http://n00bpentesting.com/lessons/](https://web.archive.org/web/20120412031808/http:/n00bpentesting.com/lessons)
* **Open Security Training**: <http://opensecuritytraining.info/>
* **Pentest Standard**: <http://www.pentest-standard.org/index.php/Main_Page>
* **Router Gods**: <http://www.routergods.com/>
* **SWEET (Secure WEb dEvelopment Teaching)**: <http://www.csis.pace.edu/~lchen/sweet/>
* **SEED: Vulnerability and Attack Labs**: [http://www.cis.syr.edu/~wedu/seed/all\_labs.html/](http://www.cis.syr.edu/~wedu/seed/all_labs.html)
* **Security Tube**: <http://www.securitytube.net/>

## Recommended Reading

* [How to set up a penetration testing lab](https://community.rapid7.com/docs/DOC-2196)
* [Portable (secure) (pen)test virtual lab](https://diablohorn.wordpress.com/2012/12/08/portable-secure-pentest-virtual-lab/)
* [Set up your Pen Testing/Hacking Lab Network using a Single System](http://securityxploded.com/setup-your-pentest-hacker-network.php)
* [Setting up your Windows XP SP2](http://web-beta.archive.org/web/20120815030857/http:/www.offensive-security.com/metasploit-unleashed/Windows_XP_SP2_Setup)

<https://securityonline.info/aircrack-ng-cheatsheet/>

<http://www.weaknetlabs.com/>

<https://github.com/weaknetlabs/debian-custom-iso-scripts>

<http://www.weaknetlabs.com/p/weakerthan-linux-6.html>

<https://github.com/c9/node-gnu-tools/tree/master/grep-src/src>

<https://tools.kali.org/reverse-engineering/ollydbg>

<https://github.com/magnetikonline/linuxmicrosoftievirtualmachines>

<https://www.osboxes.org/vmware-images/>

https://www.reddit.com/r/jailbreak/comments/7vrl1q/discussion\_iboot\_source\_code\_leaked/dtul55j/?context=0

<https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md>

<https://github.com/cokebottle/oscp-tools>

<https://github.com/ferreirasc/oscp>

[http://superuser.com/questions/890383/kali-linux-update-fails](https://superuser.com/questions/890383/kali-linux-update-fails)

<https://samsclass.info/127/127_S18.shtml>

<https://www.hackingtutorials.org/exploit-tutorials/mingw-w64-how-to-compile-windows-exploits-on-kali-linux/>

<https://canvas.instructure.com/courses/1271494>

<http://svn.code.sf.net/p/mingw-w64/code/experimental/tools/jParserC/src/Proc/funct.java>

<https://sourceforge.net/p/mingw-w64/discussion/723797/thread/391024c0/>

<https://gist.github.com/P7h/9fcccc54596ad05764128dec6f6cf78d>

yum search mingw

<https://github.com/iamthad/base16-mintty/tree/master/mintty>

<http://www.blogcompiler.com/2010/07/11/compile-for-windows-on-linux/>

<https://centos.pkgs.org/7/epel-x86_64/mingw64-gcc-4.9.3-1.el7.x86_64.rpm.html>

<http://mingw-cross.sourceforge.net/howto.html>

<https://github.com/opinkerfi/winexe-waf/issues/5>

<https://sourceforge.net/p/winexe/bugs/64/>

<https://github.com/devzero2000/violentpython>

**Powershell**

<https://github.com/wg135/pentest/blob/master/wget.ps1>

<https://github.com/wg135/pentest>

**assignments OSCP**

<https://github.com/wg135/pentest/tree/master/assigment>

**assembiy**

<https://github.com/wg135/shellcode>

<https://gist.github.com/Sinkmanu>

**OSCP notes**

<http://www.lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/><http://bernardodamele.blogspot.in/2011/09/reverse-shells-one-liners.html>

**https://piter0ff.wordpress.com/wget/**

**Need to work on it today**

<https://www.whitehatters.academy/assembly-language-and-shellcoding-on-linux-part-2/>

<https://www.whitehatters.academy/>

**https://github.com/ferreirasc/oscp/tree/master/payloads/one-liners**

<https://www.sploitspren.com/2018-01-26-Windows-Privilege-Escalation-Guide/>

<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

**https://github.com/mthbernardes/rsg**

<https://www.sploitspren.com/2017-12-29-HackTheBox-Arctic-Writeup/>

<https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

<https://git.zx2c4.com/CVE-2012-0056/tree/mempodipper.c>

<https://gnahackteam.wordpress.com/2012/07/20/mempodipper/>

<https://www.exploit-db.com/exploits/18411/>

<https://www.youtube.com/watch?v=n9OXaQxx06E>

<https://asciinema.org/a/14258>

<http://blog.weetech.co/2014/08/cve-2012-0056-mempodipper.html>

<https://eromang.zataz.com/2012/01/23/cve-2012-0056-mempodipper-linux-local-root-exploit-demo/>

**http://hackmysystems.tumblr.com/post/91788882301/cve-2012-0056-memwrite-mempodipperc**

<https://securism.wordpress.com/oscp-notes-shells/>

<https://securism.wordpress.com/oscp-notes-privilege-escalation-windows/>

<https://0day.today/author/26182>

<https://packetstormsecurity.com/files/author/11947/>

**https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS11-046**

<https://github.com/SecWiki/windows-kernel-exploits>

<https://github.com/SecWiki/linux-kernel-exploits>

<https://github.com/abatchy17/WindowsExploits/blob/master/MS11-046/40564.c>

<https://github.com/abatchy17/SLAE>

<http://www.abatchy.com/>

<https://null-byte.wonderhowto.com/how-to/writing-64-bit-shellcode-part-1-beginner-assembly-0161593/>

<https://blogs.technet.microsoft.com/askds/2008/10/22/getting-a-cmd-prompt-as-system-in-windows-vista-and-windows-server-2008/><http://carnal0wnage.attackresearch.com/2013/07/admin-to-system-win7-with-remoteexe.html>

**USEFUL RESOURCES**

<http://it-ovid.blogspot.in/2012/02/windows-privilege-escalation.html><http://toshellandback.com/2015/11/24/ms-priv-esc/>

**WATCH YOU TUBE VIDEOS**

<http://www.youtube.com/watch?v=kMG8IsCohHA><http://www.youtube.com/watch?v=_8xJaaQlpBo><http://www.greyhathacker.net/?p=738>

<https://github.com/GDSSecurity/Windows-Exploit-Suggester>

<https://www.exploit-db.com/docs/26000.pdf>

#### (Free) Virtual Networks (VPNs)

* **ChaosVPN**: <http://wiki.hamburg.ccc.de/ChaosVPN>
* **Gh0st Networks**: <http://www.gh0st.net/>
* **Hacking Lab**: <https://www.hacking-lab.com/>
* **p0wnlabs**: <http://p0wnlabs.com/>
* **pwn0**: <https://pwn0.com/>
* **PentestIT**: <https://lab.pentestit.ru/>

#### Custom Personal Targets

* **Hack A Server**: <https://hackaserver.com/>
* **Hack Me**: <http://hack.me/>
* **Hack This**: [https://www.hackthis.co.uk/](https://www.hackthis.co.uk/levels/)
* **Smash The Stack**: <http://smashthestack.org/>
* **Hack The Box**: <https://www.hackthebox.gr/>
* **SecAdvise**: <https://labs.secadvise.com/>
* **DarkHive**: <http://darkhive.net/>
* **Avatao**: <https://avatao.com/>
* **Root-Me**: <https://www.root-me.org/>

<https://www.abatchy.com/2017/02/oscp-like-vulnhub-vms>

PASSWORD RECOVERY TOOLS

<http://www.nirsoft.net/>

SHATTER ATTACK

For windows NT4.0, Win2000, WinXP  
<https://en.wikipedia.org/wiki/Shatter_attack>  
<http://www.hpl.hp.com/techreports/2005/HPL-2005-87.pdf>

<http://labs.portcullis.co.uk/application/enum4linux/>

<https://labs.portcullis.co.uk/tools/enum4linux/>

<https://labs.portcullis.co.uk/>

<https://www.itworld.com/article/2988289/linux/how-to-install-and-use-rdesktop-the-remote-desktop-client-for-linux.html>

<https://www.exploit-db.com/google-hacking-database/>

<https://twitter.com/zerosum0x0>

<https://github.com/drwetter/testssl.sh.git>

https://tails.boum.org/doc/index.en.html

<http://cdimage.kali.org/kali-weekly/>

https://github.com/corelan/mona/blob/master/mona.py