1. **OSCP wargames/boxes**

<https://overthewire.org/wargames/> [SUPER INTERESTING, CAN GIVE IT A TRY] (For a start, try Natas lab path)

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

<https://tryhackme.com/>

<https://www.hackthebox.eu/>

<https://www.hacker101.com/>

1. **HackTheBox Writeups**

<https://medium.com/@hussaini.faisal/hackthebox-writeup-networked-63681c68dfba>

<https://hackso.me/> [Recommended to read, if you are bored and looking for something to do]

<https://github.com/Hackplayers/hackthebox-writeups>

1. **Enumeration Scripts / Priv Escalation / Tools / Scripts / Cheatsheets**

<https://book.hacktricks.xyz/pentesting-methodology>

<http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet>

<https://guif.re/windowseop>

<https://github.com/wwong99/pentest-notes>

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

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md>

[probably u will need these two links]

<https://github.com/swisskyrepo/PayloadsAllTheThings>

<https://github.com/robertdavidgraham/masscan>

[Alternate portscan tool other than nmap 🡪 "hping3 -S --scan 1-65535 <IP>"]

<https://github.com/Tib3rius/AutoRecon>

<https://github.com/itm4n/PrivescCheck>

<https://github.com/FuzzySecurity/PowerShell-Suite.git>

<https://github.com/cmoras/linux-exploit-suggester>

<https://gtfobins.github.io/>

<https://github.com/danielmiessler/SecLists> [your all in one stop for dictionary lists/fuzz payload]

<https://github.com/pgaijin66/XSS-Payloads/blob/master/payload.txt>

<https://medium.com/@mucomplex/reproduce-and-study-proof-of-concept-poc-with-nessus-nasl-eb8cd30d620b>

<https://www.hackingarticles.in/web-shells-penetration-testing/>

<https://github.com/tennc/webshell/tree/master/fuzzdb-webshell/php>

<https://www.tecmint.com/calculate-ip-subnet-address-with-ipcalc-tool/> [ip subnet calculator]

<https://github.com/buftas/Active-Directory-Exploitation-Cheat-Sheet>

<https://hackingpassion.com/shodan-eye-getting-started-with-shodan/>

<https://github.com/odedshimon/BruteShark>

<https://ceso.github.io/posts/2020/04/hacking/oscp-cheatsheet/>

<https://www.kitploit.com/2020/05/invoker-penetration-testing-utility.html>

<https://hakin9.org/ptf-pentest-tools-framework-exploits-scanner-password/>

<https://github.com/AngelSecurityTeam/RapidPayload>

<https://github.com/trimstray/the-book-of-secret-knowledge>

<https://github.com/m4ll0k/Awesome-Hacking-Tools>

<https://guide.offsecnewbie.com/privilege-escalation/windows-pe#acesschk-exe>

<https://github.com/ankh2054/windows-pentest>

<https://www.fuzzysecurity.com/tutorials/16.html>

<https://gist.github.com/henrik/1967800>

<https://pentest.tonyng.net/timo-sablowskis-oscp-note/>

<https://medium.com/@simonsulyma/hack-the-box-legacy-penetration-testing-without-metasploit-44b628fe870f>

1. **OSCP Preparation Videos (Recommended)**

<https://www.youtube.com/playlist?list=PLidcsTyj9JXK-fnabFLVEvHinQ14Jy5tf> @IppSec (37 Videos) **\*SUPER IMPORTANT IN FACT HIS WHOLE CHANNEL IS IMPORTANT TOO\***

<https://www.youtube.com/playlist?list=PLZOToVAK85MqxEPGXA80NPMZEczZfA9ej> @webpwnized (282 Videos)

<https://www.youtube.com/playlist?list=PLqM63j87R5p4Mp4NP-Oa1kLV6o22RDfex&app=desktop>

@Motasem Hamdan (44 Videos)

1. **Resources for OSCP Prep on every topic (MUST READ UP EVERY SINGLE LINK)**

<https://github.com/burntmybagel/OSCP-Prep>

<https://github.com/security-prince/PWK-OSCP-Preparation-Roadmap>

<https://www.tripwire.com/state-of-security/security-awareness/oscp-journey/>

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

<https://github.com/moshekaplan/pentesting_notes/blob/master/OSCP_prep.md>

<https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md>

<https://www.linkedin.com/pulse/penultimate-guide-defeat-oscp-corey-ball-oscp-cissp-cism>

<https://github.com/s0wr0b1ndef/OSCP-note>

<https://medium.com/@tom.business/an-oscp-journey-without-using-metasploit-htb-nibbles-2-ab62bb706a84>

<https://www.facebook.com/bugbounty.hackerone/>

1. **Miscellaneous Reads on non-OSCP related resources**

<https://shells.systems/introducing-ninja-c2-the-c2-built-for-stealth-red-team-operations/?fbclid=IwAR1-NObteookkaYqoOgpsUsaZaPc2lCyow9rt3cboVufJOzoqBv1rePGVW8>

<https://cuckoosandbox.org/>

<https://github.com/ExtremeHacking/infinityhacks-botnet>

<https://github.com/D3VL/L3MON>

<https://hakin9.org/tool-x-is-a-kali-linux-hacking-tools-installer-for-termux-and-linux-system/>

1. **Cybersecurity News / Podcasts**

<https://www.facebook.com/ExWareLabs/>

<https://darknetdiaries.com/>

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

8) **Some notes**

* when you face some issues like a web server you not sure how to attack try to find CTFs write-ups on the webserver framework. Save tons of time

**Unofficial OSCP Approved Tools**

<https://medium.com/@falconspy/oscp-approved-tools-b2b4e889e707>

**Report**

Serpico - <https://github.com/SerpicoProject/Serpico>

Serpico template for OSCP - <https://www.reddit.com/r/oscp/comments/dzwca6/serpico_template_for_the_oscp_now_available/>

**Infosec Prep Discord channel** - https://discord.gg/eG6Nt4x