

## Coleção de links para estudos futuros

Pentest:

<https://www.youtube.com/watch?v=8JJUTQWI7Io>

[https://www.youtube.com/watch?v=keFx6yYA\\_WY](https://www.youtube.com/watch?v=keFx6yYA_WY)

<https://www.youtube.com/watch?v=pL9q2lOZ1Fw>

Kali Linux:

<https://www.cybrary.it/0p3n/kali-linux-commands-list/>

<https://www.offensive-security.com/kali-linux/top-10-post-install-tips/>

Obtendo Informações:

<http://www.nanoshots.com.br/2016/02/encontrando-e-acessando-cameras-e.html>

<https://spreadsecurity.github.io/2016/07/25/information-gathering-with-shodan.html>

<https://null-byte.wonderhowto.com/how-to/hack-like-pro-reconnaissance-with-recon-ng-part-1-getting-started-0169854/>

<https://securityonline.info/category/penetration-testing/network-pentest/information-gathering/>

Identificação de Vulnerabilidade:

<https://www.youtube.com/watch?v=oqGg6QXaoWQ>

<https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux>

<https://codingsec.net/2016/05/use-proxychains-evade-detection-kali-linux/>

<https://securityonline.info/category/penetration-testing/network-pentest/vulnerability-analysis/>

Captura de Tráfego:

<https://null-byte.wonderhowto.com/how-to/tutorial-dns-spoofing-0167796/>

<https://securityonline.info/category/penetration-testing/network-pentest/sniffing-spoofing/>

Exploits:

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

Exploração:

<https://github.com/Screetsec/TheFatRat>

<https://securityonline.info/detect-ms17-010-smb-vulnerability-using-metasploit/>

<https://forum.fsocietybrasil.org/topic/658-ferramenta-explora%C3%A7%C3%A3o-de-vulnerabilidades-em-modem/>

<https://securityonline.info/roxysploit-a-hackers-framework/>

<https://github.com/NullArray/AutoSploit>

<https://securityonline.info/category/penetration-testing/network-pentest/exploitation/>

Ataques a Senhas:

<https://fossbytes.com/windows-safe-mode-can-exploited-steal-pc-passwords/>

<https://securityonline.info/category/password-attacks/>

Engenharia social:

<https://www.youtube.com/watch?v=My-SizcEJok>

[https://medium.com/@pedrorafael\\_90498/clonando-p%C3%A1gina-da-web-e-capturando-informa%C3%A7%C3%B5es-funcionando-em-rede-externa-e0bc3fbdfdd1](https://medium.com/@pedrorafael_90498/clonando-p%C3%A1gina-da-web-e-capturando-informa%C3%A7%C3%B5es-funcionando-em-rede-externa-e0bc3fbdfdd1)

Evitando Antivírus:

<https://www.linkedin.com/pulse/bypass-all-anti-viruses-encrypted-payloads-c-damon-mohammadbagher?trk=hp-feed-article-title-like>

Pós-Exploração e Manutenção de Acesso:

<https://www.kitploit.com/2016/09/winpirate-automated-sticky-keys-hack.html>

<https://www.youtube.com/watch?v=kEsshExn7aE>

<https://techviral.net/hacker-cracks-windows-account-less-1-minute/>

<https://securityonline.info/category/penetration-testing/network-pentest/post-exploitation/>

<https://securityonline.info/category/penetration-testing/network-pentest/maintaining-access/>

Ataques para Web:

<http://www.100security.com.br/sqlmap/>

<https://www.youtube.com/watch?v=WtLTtbe5JcM>

<http://www.hackingarticles.in/manual-sql-injection-exploitation-step-step/>

<http://www.hackingarticles.in/beginner-guide-sql-injection-part-1/>

[https://www.youtube.com/watch?v=5BG6iq\\_AUvM](https://www.youtube.com/watch?v=5BG6iq_AUvM)

<https://www.youtube.com/playlist?list=PLZUQcQP4Xtlp64Q6tzw8GdLsOweBsKDSs>

<https://wpvulndb.com/wordpresses>

<https://securityintelligence.com/the-10-most-common-application-attacks-in-action/>

<https://hackingvision.com/2017/04/14/sqlmap-tutorial-sql-injection-hack-website-database-kali-linux/>

<http://www.hackingarticles.in/xss-exploitation-dvwa-bypass-security/>

<http://www.hackingarticles.in/csrf-attack-in-dvwa/>

<https://seleniumbycharan.wordpress.com/2017/03/17/set-up-your-penetration-testing-lab/>

<https://seleniumbycharan.wordpress.com/2017/03/17/html-injection-introduction/>

<https://securityonline.info/category/penetration-testing/webapp-pentest/>

Cobertura de Rastros:

<https://www.kitploit.com/2017/05/freedom-fighting-collection-of-scripts.html>

Redes Sem Fio:

<https://www.drungston.com/wifite-hacking-wifi-easy-way-kali-linux/>

<https://en.kali.tools/?p=90>

<https://www.youtube.com/watch?v=4XLUVfoJqo8>

<https://securityonline.info/wireless-penetration-testing-tool/>

<https://github.com/v1s1t0r1sh3r3/airgeddon>

<https://securityonline.info/category/penetration-testing/network-pentest/wireless/>

Desenvolvimento de Exploits:

<https://www.youtube.com/watch?v=H2ZTTQX-ma4>

<https://exploit-exercises.com/>

Dispositivos Móveis:

<https://github.com/payatu/diva-android>

<https://securityonline.info/category/penetration-testing/network-pentest/smartphone-pentest/>

Conteúdo Extra de Pentest:

<https://medium.com/hack-with-github/black-hat-arsenal-usa-2017-3fb5bd9b5cf2>

<https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/>

<https://github.com/Hack-with-Github/Awesome-Hacking/blob/master/README.md>

<http://www.hackingarticles.in/penetration-testing/>

<https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/>

<http://www.amanhardikar.com/mindmaps/Practice.html>

Exercícios e CTF's:

<https://www.checkmarx.com/2016/12/04/15-vulnerable-sites-legally-practice-hacking-skills-2016-update/>

<https://ctf-br.org/docs/>

<https://github.com/facebook/fbctf>

<http://www.hackingarticles.in/hack-freshly-vm-ctf-challenge/>

<https://exploit-exercises.com/>

<https://www.vulnhub.com/entry/bwapp-bee-box-v16,53/>

<https://xss-game.appspot.com/>

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

<https://github.com/apsdehal/awesome-ctf>