Helpful Software:

Windows:

<https://github.com/SpiderLabs/Responder>

<https://github.com/EmpireProject/Empire>

<https://github.com/Hackplayers/evil-winrm>

<https://github.com/PowerShellMafia/PowerSploit>

<https://github.com/coreb1t/awesome-pentest-cheat-sheets>

Guides:

[https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md#eop---runas)

<https://byt3bl33d3r.github.io/practical-guide-to-ntlm-relaying-in-2017-aka-getting-a-foothold-in-under-5-minutes.html>

<https://mez0.cc/posts/ntlm-relaying.html>

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#powershell>

<https://www.hackingarticles.in/post-exploitation-using-wmic-system-command/>

Win-Defender/Applocker bypass:

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Powershell Limited Language Mode Bypass:

<https://github.com/padovah4ck/PSByPassCLM>

[https://github.com/MinatoTW/CLMBypassBlogpost](https://github.com/MinatoTW/CLMBypassBlogpost/blob/master/Msbuild/pwn.csproj)

LFI:

<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/File%20Inclusion>

Ethereum:

<https://web3py.readthedocs.io/en/stable/contracts.html#contract-deployment-example>

<https://web3py.readthedocs.io/en/stable/web3.eth.html#contracts>

<https://eth-account.readthedocs.io/en/stable/eth_account.html>

<https://solidity.readthedocs.io/en/latest/using-the-compiler.html#commandline-compiler>