**Privilege Escalation**

[Linux Privilege Escalation · OSCP - Useful Resources](https://backdoorshell.gitbooks.io/oscp-useful-links/content/linux-privilege-escalation.html)

[Privilege Escalation - Windows · Total OSCP Guide](https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html)

[Linux Privilege Escalation using Sudo Rights](https://www.hackingarticles.in/linux-privilege-escalation-using-exploiting-sudo-rights/)

[Abusing SUDO (Linux Privilege Escalation) - Touhid M.Shaikh](https://touhidshaikh.com/blog/?p=790)

[Basic Linux Privilege Escalation](https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/)

[rebootuser/LinEnum: Scripted Local Linux Enumeration & Privilege Escalation Checks](https://github.com/rebootuser/LinEnum)

[Windows Privilege Escalation · OSCP - Useful Resources](https://backdoorshell.gitbooks.io/oscp-useful-links/content/windows-privilege-escalation.html)

[Spawning a TTY Shell](https://netsec.ws/?p=337)

[Linux Privilege Escalation Using PATH Variable](https://www.hackingarticles.in/linux-privilege-escalation-using-path-variable/)

**Windows**

[Weak Service Permissions | Penetration Testing Lab](https://pentestlab.blog/2017/03/30/weak-service-permissions/)

[Windows elevation of privileges](https://guif.re/windowseop#EoP%200:%20System%20info)

[Windows Privilege Escalation - AwanSec](https://awansec.com/windows-priv-esc.html)

[OSCP Notes – Privilege Escalation (Windows) – Securism](https://securism.wordpress.com/oscp-notes-privilege-escalation-windows/)

[FuzzySecurity | Windows Privilege Escalation Fundamentals](http://www.fuzzysecurity.com/tutorials/16.html)

[Start or stop Windows service from command line (CMD)](https://www.windows-commandline.com/start-stop-service-command-line/)

**Reverse Shell**

[php-reverse-shell | pentestmonkey](http://pentestmonkey.net/tools/web-shells/php-reverse-shell)

[Reverse Shell Cheat Sheet | pentestmonkey](http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet)

[jondonas/linux-exploit-suggester-2: Next-Generation Linux Kernel Exploit Suggester](https://github.com/jondonas/linux-exploit-suggester-2)

[OSCP-PwK/check-exploits.py at master · so87/OSCP-PwK](https://github.com/so87/OSCP-PwK/blob/master/check-exploits.py)

[OSCP-PwK/Penetration Testing Tools.docx at master · so87/OSCP-PwK](https://github.com/so87/OSCP-PwK/blob/master/Penetration%20Testing%20Tools.docx)

<https://raw.githubusercontent.com/so87/OSCP-PwK/master/linux-local-enum.sh>

[OSCP/Bookmark List.pdf at master · ihack4falafel/OSCP](https://github.com/ihack4falafel/OSCP/blob/master/Documents/Bookmark%20List.pdf)

[dostoevskylabs/dostoevsky-pentest-notes: Notes for taking the OSCP in 2097. Read in book form on GitBook](https://github.com/dostoevskylabs/dostoevsky-pentest-notes)

[abatchy's blog | Posts Tagged “OSCP Prep”](https://www.abatchy.com/tag/OSCP%20Prep/)

[35 Practical Examples of Linux Find Command](https://www.tecmint.com/35-practical-examples-of-linux-find-command/)

[Character Code, HEX, ASCII](http://www.techdictionary.com/ascii.html)

[Md5 Decrypt & Encrypt - More than 10.000.000.000 hashes](https://md5decrypt.net/en/)

[Best MD5 & SHA1 Password Hash Decrypter - Hash Toolkit](https://hashtoolkit.com/)

[(87) Mr Frauenhofer - YouTube](https://www.youtube.com/channel/UCm8uTQnrzoBOmw50yRlzYhQ)

[GitHub - qazbnm456/awesome-cve-poc: ✍️ A curated list of CVE PoCs.](https://github.com/qazbnm456/awesome-cve-poc)

[Awesome Search](https://awesomelists.top/#/repos/qazbnm456/awesome-cve-poc)

[(131) Study Music Alpha Waves: Relaxing Studying Music, Brain Power, Focus Concentration Music, ☯161 - YouTube](https://www.youtube.com/watch?v=WPni755-Krg&t=4716s)

[unix-privesc-check | pentestmonkey](http://pentestmonkey.net/tools/audit/unix-privesc-check)

[linpostexp/linprivchecker.py at master · reider-roque/linpostexp](https://github.com/reider-roque/linpostexp/blob/master/linprivchecker.py)

[reider-roque/linpostexp: Linux post exploitation enumeration and exploit checking tools](https://github.com/reider-roque/linpostexp)

[lanmaster53.com](https://www.lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/)

[scanning port wihout nmap](https://www.lanmaster53.com/2010/04/16/no-nmap-no-permissions-no-problem/)

[A guide to Linux Privilege Escalation - payatu](https://payatu.com/guide-linux-privilege-escalation/)

**Converter**

[Best Base64 Decode Online tool to Decodes base64 String, URL, File.](https://codebeautify.org/base64-decode)

[More with smbclient, smbget, enum4linux Carnal0wnage - Attack Research Blog Carnal0wnage & Attack Research Blog](http://carnal0wnage.attackresearch.com/2015/12/more-with-smbclient-smbget-enum4linux.html)

[Resource: The how to pass an exam/certification and study guide Wiki by Peerlyst - OSCP, peerlyst wiki, guides](https://www.peerlyst.com/posts/resource-the-how-to-pass-an-exam-certification-and-study-guide-wiki-peerlyst)

[P0cL4bs/Kadimus: Kadimus is a tool to check sites to lfi vulnerability , and also exploit it...](https://github.com/P0cL4bs/Kadimus)

**type of encoding**

[Hash Type Checker - Check and validate your hash string](https://md5hashing.net/hash_type_checker)

[LFI Cheat Sheet](https://highon.coffee/blog/lfi-cheat-sheet/)

[31 days of OSCP Experience - ScriptDotSh](https://scriptdotsh.com/index.php/2018/04/17/31-days-of-oscp-experience/)

[Pentester Academy: Learn Pentesting Online](https://www.pentesteracademy.com/)

**Buffer Overflow**

[Exploiting Simple Buffer Overflows on Win32](https://www.pentesteracademy.com/course?id=13)

[Simple Buffer Overflows](http://netsec.ws/?p=180)

[Buffer Overflow: Lesson 1: PCMan's FTP Server 2.0.7 Buffer Overflow Explained](https://www.computersecuritystudent.com/SECURITY_TOOLS/BUFFER_OVERFLOW/WINDOWS_APPS/lesson1/index.html)

[Exploting Buffer Overflow Minishare 1.4.1 – mosunit](https://mosunit.wordpress.com/2016/03/15/exploting-buffer-overflow-minishare-1-4-1/)

[Exploit writing tutorial part 1 : Stack Based Overflows | Corelan Team](https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/)

[How to use msfvenom · rapid7/metasploit-framework Wiki](https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom)

[A Virgil's Guide to Pentest: Enumeration is the KEY](http://virgil-cj.blogspot.com/2018/02/enumeration-is-key_6.html?m=1)

[Welcome to SecurityTube.net](http://www.securitytube.net/)

[Offensive Security Student Support](https://support.offensive-security.com/#!oscp-exam-guide.md)

[Passing OSCP - scund00r](https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html)

[LazySysAdmin: 1 ~ VulnHub](https://www.vulnhub.com/entry/lazysysadmin-1,205/)

[(231) HackTheBox - Waldo - YouTube](https://www.youtube.com/watch?v=1klneIHECqY&list=PL18XzHJvd28QkiWFGAKTyaa7EU8BJv2dA)

[Hack The Box :: Dashboard](https://www.hackthebox.eu/home)

[Pwk kali vm - Offensive Security](https://support.offensive-security.com/pwk-kali-vm/)

[Pwk connectivity guide - Offensive Security](https://support.offensive-security.com/pwk-connectivity-guide/)

[Status - freenode Web IRC](https://webchat.freenode.net/)

[PWK Resources and Downloads](https://forums.offensive-security.com/forumdisplay.php?87-PWK-Resources-and-Downloads)

[Penetration Testing with Kali Linux](file:///D:\OSCP_Rishabh\pwk-45208-490249\pwk-45208-490249\index.html#module=Welcome&sub-module=Overview&time-offset=0)

[Week 1 - OSCP Preparation / LAB Setup](https://www.jpsecnetworks.com/week-1-oscp-preparation-lab-setup/)

[PWB General Conversation](https://forums.offensive-security.com/forumdisplay.php?29-PWB-General-Conversation)

[OSCP Survival Guide · xxooxxooxx/xxooxxooxx.github.io Wiki](https://github.com/xxooxxooxx/xxooxxooxx.github.io/wiki/OSCP-Survival-Guide#networking-pivoting-and-tunneling)

[SSH Tunneling Magic – Reznok](http://reznok.com/ssh-tunneling-magic/)

[Local Port Forwarding (SSH)](https://netsec.ws/?p=287)

[Go-For-OSCP | Hacking and security](https://hackingandsecurity.blogspot.com/2017/08/go-for-oscp.html)

[My OSCP Experience - The Coffeegist](https://coffeegist.com/security/my-oscp-experience/)

[Higgsx's Journey to OSCP — TechExams Community](https://community.infosecinstitute.com/discussion/131070/higgsxs-journey-to-oscp)

[scipag/vulscan: Advanced vulnerability scanning with Nmap NSE](https://github.com/scipag/vulscan)

[pentest-notes/OSCP-Survival-Guide.md at master · wwong99/pentest-notes](https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md)

[Pentesting Cheatsheet – root@Hausec](https://hausec.com/pentesting-cheatsheet/#_Toc475368986)

[44592-linux-restricted-shell-bypass-guide.pdf](https://www.exploit-db.com/docs/english/44592-linux-restricted-shell-bypass-guide.pdf)

[OSCP - Windows Priviledge Escalation | Hacking and security](https://hackingandsecurity.blogspot.com/2017/09/oscp-windows-priviledge-escalation.html)

[Pentestit Lab v11 - RDP Token (3/12) - Jack Hacks](https://jhalon.github.io/pentestit-lab-11-rdp-token/)

[tms4a/failed-stuff: stuff that was never worth finishing. mostly junk programs](https://github.com/tms4a/failed-stuff)

[OSCP course review | Hacking and security](https://hackingandsecurity.blogspot.com/2015/04/blog-post.html)

[Offensive Security's Complete Guide to Alpha](https://forums.offensive-security.com/showthread.php?4689-Offensive-Security-s-Complete-Guide-to-Alpha)

[Offensive Security's Complete Guide to Alpha](https://forums.offensive-security.com/showthread.php?4689-Offensive-Security-s-Complete-Guide-to-Alpha&p=20532#post20532)

[Paste · Slexy.org Pastebin](https://slexy.org/view/s20koEbsBP)

[OSCP notes](https://blog.propriacausa.de/wp-content/uploads/2016/07/oscp_notes.html)

[[PentesterLab]](https://pentesterlab.com/exercises/php_include_and_post_exploitation/course)

<https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh>

[linuxprivchecker/linuxprivchecker.py at master · sleventyeleven/linuxprivchecker](https://github.com/sleventyeleven/linuxprivchecker/blob/master/linuxprivchecker.py)

[SecLists/Passwords/Default-Credentials at master · danielmiessler/SecLists](https://github.com/danielmiessler/SecLists/tree/master/Passwords/Default-Credentials)

[How to Perform Local Privilege Escalation Using a Linux Kernel Exploit « Null Byte :: WonderHowTo](https://null-byte.wonderhowto.com/how-to/perform-local-privilege-escalation-using-linux-kernel-exploit-0186317/)

[milo2012/pathbrute: Pathbrute](https://github.com/milo2012/pathbrute)

[Hakluke’s Ultimate OSCP Guide: Part 3 — Practical hacking tips and tricks](https://medium.com/@hakluke/haklukes-ultimate-oscp-guide-part-3-practical-hacking-tips-and-tricks-c38486f5fc97)

[Jump ESP, jump!: Attacking Adobe ColdFusion](https://jumpespjump.blogspot.com/2014/03/attacking-adobe-coldfusion.html)

[PayloadsAllTheThings/Reverse Shell Cheatsheet.md at master · swisskyrepo/PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md)

[How to Remotely Enable and Disable (RDP) Remote Desktop](https://www.interfacett.com/blogs/how-to-remotely-enable-and-disable-rdp-remote-desktop/)

[Window-Tools/Simple Reverse Shell at master · infoskirmish/Window-Tools](https://github.com/infoskirmish/Window-Tools/tree/master/Simple%20Reverse%20Shell)

[pentest-tools/shells at master · reider-roque/pentest-tools](https://github.com/reider-roque/pentest-tools/tree/master/shells)

[Port Scanning · Total OSCP Guide](https://sushant747.gitbooks.io/total-oscp-guide/port_scanning.html)

[Creating Metasploit Payloads](https://netsec.ws/?p=331)

[Windows and Unix command line equivalents](https://www.lemoda.net/windows/windows2unix/windows2unix.html)

[Pashkela/Cfm\_Shell\_v3.0\_edition: Cfm Shell v3.0 edition](https://github.com/Pashkela/Cfm_Shell_v3.0_edition)

[1N3/BruteX: Automatically brute force all services running on a target.](https://github.com/1N3/BruteX)

[Penetration Testing Methodology - 0DAYsecurity.com](http://www.0daysecurity.com/penetration-testing/enumeration.html)

[Local File Inclusion · Total OSCP Guide](https://sushant747.gitbooks.io/total-oscp-guide/local_file_inclusion.html)

[Get Reverse-shell via Windows one-liner](https://www.hackingarticles.in/get-reverse-shell-via-windows-one-liner/?unapproved=95442&moderation-hash=f48ddc834c552c7283784e82c563c6eb#comment-95442)

[Transferring files from Kali to Windows (post exploitation)](https://blog.ropnop.com/transferring-files-from-kali-to-windows/)

[How to use the Linux ftp command to up- and download files on the shell](https://www.howtoforge.com/tutorial/how-to-use-ftp-on-the-linux-shell/)

[Payload netcat FTP download and reverse shell · hak5darren/USB-Rubber-Ducky Wiki](https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload-netcat-FTP-download-and-reverse-shell)

[Windows elevation of privileges](https://guif.re/windowseop)

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

[Testing a POP3 server via telnet or OpenSSL – The Sarth Repository](https://blog.yimingliu.com/2009/01/23/testing-a-pop3-server-via-telnet-or-openssl/)

[Samba 2.2.x - 'call\_trans2open' Remote Buffer Overflow (2)](https://www.exploit-db.com/exploits/22469)

[A Little Guide to SMB Enumeration](https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/)

[OSCPRepo/scripts/recon\_enum at master · rewardone/OSCPRepo](https://github.com/rewardone/OSCPRepo/tree/master/scripts/recon_enum)

[rewardone/OSCPRepo: A list of commands, scripts, resources, and more that I have gathered and attempted to consolidate for use as OSCP (and more) study material. Commands in 'Usefulcommands' Keepnote. Bookmarks and reading material in 'BookmarkList' Keepn](https://github.com/rewardone/OSCPRepo)

[PWK Notes: SMB Enumeration Checklist [Updated] | 0xdf hacks stuff](https://0xdf.gitlab.io/2018/12/02/pwk-notes-smb-enumeration-checklist-update1.html)

[areyou1or0/OSCP: OSCP](https://github.com/areyou1or0/OSCP)

[skywind3000/terminal: Open Terminal Window to execute command in Windows / Cygwin / Ubuntu / OS X](https://github.com/skywind3000/terminal)

[epinna/tplmap: Server-Side Template Injection and Code Injection Detection and Exploitation Tool](https://github.com/epinna/tplmap)

[ch4inrulz: 1.0.1 | Vulnhub Walkthrough – egghunter – Medium](https://medium.com/egghunter/ch4inrulz-1-0-1-vulnhub-walkthrough-d5f48e8ae187)

[r57.txt - c99.txt - r57 shell - c99 shell - r57shell - c99shell - r57 - c99 - shell archive - php shells - php exploits - bypass shell - safe mode bypass - sosyete safe mode bypass shell - Evil Shells - exploit - root - localshell.net](http://www.r57.gen.tr/)

[Insert PHP Backdoor Files into JPG Image Files](https://exploit.linuxsec.org/menyisipkan-file-backdoor-php-ke-jpg/)

[web application - Malicious code in image. Harmful? - Information Security Stack Exchange](https://security.stackexchange.com/questions/53958/malicious-code-in-image-harmful)

[Microsoft Word - File Upload Vulnerability in FCKEditor.doc](https://secureyes.net/nw/assets/File-Upload-Vulnerability-in-FCKEditor.pdf)

[Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE\_POKEDATA' Race Condition Privilege Escalation (/etc/passwd Method)](https://www.exploit-db.com/exploits/40839)

[45074-file-upload-restrictions-bypass.pdf](https://www.exploit-db.com/docs/english/45074-file-upload-restrictions-bypass.pdf)

[Dashboard](https://www.shodan.io/home)

[DVWA - Main Login Page - Brute Force HTTP POST Form With CSRF Tokens](https://blog.g0tmi1k.com/dvwa/login/)

[Moham3dRiahi/XBruteForcer: X Brute Forcer Tool 🔓 WordPress , Joomla , DruPal , OpenCart , Magento](https://github.com/Moham3dRiahi/XBruteForcer)

[Penetration Testing on Remote Desktop (Port 3389)](https://www.hackingarticles.in/penetration-testing-remote-desktop-port-3389/)

[How to Crack Shadow Hashes After Getting Root on a Linux System « Null Byte :: WonderHowTo](https://null-byte.wonderhowto.com/how-to/crack-shadow-hashes-after-getting-root-linux-system-0186386/)

[worawit/MS17-010: MS17-010](https://github.com/worawit/MS17-010)

[danielmiessler/SecLists: SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing pa](https://github.com/danielmiessler/SecLists)

[Lateral Movement with SMBRelayx.py | Breaking Applications](https://ramnathshenoy.wordpress.com/2017/03/19/lateral-movement-with-smbrelayx-py/)

[Bash get exit code of command on a Linux / Unix - nixCraft](https://www.cyberciti.biz/faq/bash-get-exit-code-of-command/)

[8 Ways To Mount SMBfs (SAMBA FILE SYSTEM) In Linux. - The Linux Juggernaut](https://www.linuxnix.com/8-ways-to-mount-smbfs-samba-file-system-in-linux/)

[Hack The Box Write-up - Active | text/plain](https://dominicbreuker.com/post/htb_active/)

[Pentesting Cheatsheet – root@Hausec](https://hausec.com/pentesting-cheatsheet/)

[pentest-notes/OSCP-Survival-Guide.md at master · wwong99/pentest-notes](https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md#file-transfers)

[15 Ways to Download a File](https://blog.netspi.com/15-ways-to-download-a-file/)

[OSCP/Documents at master · ihack4falafel/OSCP](https://github.com/ihack4falafel/OSCP/tree/master/Documents)

[oscp/reconscan.py at master · xapax/oscp](https://github.com/xapax/oscp/blob/master/recon_enum/reconscan.py)

[Passing OSCP - scund00r](https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html#file-transfers)

[Pen Testing SQL Servers With Nmap | Penetration Testing Lab](https://pentestlab.blog/2013/04/21/pen-testing-sql-servers-with-nmap/)

[SMB Share – SCF File Attacks | Penetration Testing Lab](https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/)

[HackingDatabases.ppt](https://www.blackhat.com/presentations/bh-europe-07/Cerrudo/Presentation/bh-eu-07-Cerrudo-ppt-Apr14.pdf)

[Hand Guide To Local File Inclusion(LFI)](http://www.securityidiots.com/Web-Pentest/LFI/guide-to-lfi.html)

[Local File Inclusion · Security - My notepad](https://xapax.gitbooks.io/security/content/local_file_inclusion.html)

[CVV #1: Local File Inclusion – InfoSec Write-ups – Medium](https://medium.com/bugbountywriteup/cvv-1-local-file-inclusion-ebc48e0e479a)

[D35m0nd142/LFISuite: Totally Automatic LFI Exploiter (+ Reverse Shell) and Scanner](https://github.com/D35m0nd142/LFISuite)

[fuzzdb/dict/BURP-PayLoad at master · tennc/fuzzdb](https://github.com/tennc/fuzzdb/tree/master/dict/BURP-PayLoad)

[Basics of Linux · Security - My notepad](https://xapax.gitbooks.io/security/content/basics_of_linux.html)

[Public Network](https://forums.offensive-security.com/forumdisplay.php?138-Public-Network)

[Local Linux Enumeration & Privilege Escalation Cheatsheet – Rebootuser](https://www.rebootuser.com/?p=1623)

[Editing /etc/passwd File for Privilege Escalation](https://www.hackingarticles.in/editing-etc-passwd-file-for-privilege-escalation/)

[Linux Privilege Escalation using SUID Binaries](https://www.hackingarticles.in/linux-privilege-escalation-using-suid-binaries/)

[Linux Privilege Escalation via Automated Script](https://www.hackingarticles.in/linux-privilege-escalation-via-automated-script/)

<https://gist.githubusercontent.com/sckalath/ec7af6a1786e3de6c309/raw/206505282d0d0261cbc2bce8c33d55fe6ac6b7fd/wget_vbs>

[Windows Kernel Exploits | Penetration Testing Lab](https://pentestlab.blog/2017/04/24/windows-kernel-exploits/)

[GitHub - Arvanaghi/SessionGopher: SessionGopher is a PowerShell tool that uses WMI to extract saved session information for remote access tools such as WinSCP, PuTTY, SuperPuTTY, FileZilla, and Microsoft Remote Desktop. It can be run remotely or locally.](https://github.com/Arvanaghi/SessionGopher)

[Windows Privilege Escalation Scripts & Techniques – Rahmat Nurfauzi – Medium](https://medium.com/@rahmatnurfauzi/windows-privilege-escalation-scripts-techniques-30fa37bd194)

[GitHub - 411Hall/JAWS: JAWS - Just Another Windows (Enum) Script](https://github.com/411Hall/JAWS)

[MS16-032 | Penetration Testing Lab](https://pentestlab.blog/tag/ms16-032/)

[Windows - Pentest Notes](https://guide.offsecnewbie.com/privilege-escalation/windows-pe)

[Unquoted Service Path | Penetration Testing Lab](https://pentestlab.blog/2017/03/09/unquoted-service-path/)

[How to modify exploits for Windows](https://zero-day.io/modifyexploits/)

[ms16-032 one-liners – Will Genovese](http://willgenovese.com/ms16-032-one-liners/)

[GitHub - samratashok/nishang: Nishang - Offensive PowerShell for red team, penetration testing and offensive security.](https://github.com/samratashok/nishang)

[Window Privilege Escalation via Automated Script](https://www.hackingarticles.in/window-privilege-escalation-via-automated-script/)

[GitHub - gammathc/oscp\_material: Material i gathered for the Offensive Security Certified Professional OSCP](https://github.com/gammathc/oscp_material)

[Offensive Security’s PWK & OSCP Review - Jack Hacks](https://jhalon.github.io/OSCP-Review/)

[GitHub - SecWiki/windows-kernel-exploits: windows-kernel-exploits Windows平台提权漏洞集合](https://github.com/SecWiki/windows-kernel-exploits)

[Lab of a Penetration Tester: Using PowerShell for Client Side Attacks](http://www.labofapenetrationtester.com/2014/11/powershell-for-client-side-attacks.html)

[PJRC: Electronic Projects](https://www.pjrc.com/)

[Lab of a Penetration Tester: Fun with DNS TXT Records and PowerShell](http://www.labofapenetrationtester.com/2015/01/fun-with-dns-txt-records-and-powershell.html)

[Mad With PowerShell: 64-bit vs 32-bit PowerShell](https://www.madwithpowershell.com/2015/06/64-bit-vs-32-bit-powershell.html)

[optimum on hackthebox.eu](http://road2oscp.blogspot.com/2018/01/optimum-on-hacktheboxeu.html)

[Empire/Invoke-MS16032.ps1 at master · EmpireProject/Empire · GitHub](https://github.com/EmpireProject/Empire/blob/master/data/module_source/privesc/Invoke-MS16032.ps1)

[GitHub - rasta-mouse/Sherlock: PowerShell script to quickly find missing software patches for local privilege escalation vulnerabilities.](https://github.com/rasta-mouse/Sherlock)

[GitHub - frizb/Windows-Privilege-Escalation: Windows Privilege Escalation Techniques and Scripts](https://github.com/frizb/Windows-Privilege-Escalation)

[MS16-032提权正确方法](https://paper.tuisec.win/detail/e88e7fc75b82cc7)

[GitHub - togie6/Windows-Privesc: Basics of Windows privilege escalation](https://github.com/togie6/Windows-Privesc)

[Run a command as a different user in Powershell - IT Droplets](https://www.itdroplets.com/run-a-command-as-a-different-user-in-powershell/)

[OSCP - JollyFrogs' tale - { Anas Aboureada }](https://anasaboureada.github.io/oscp/2017/12/02/jolly_frog.html)

[Privilege Escalation | Penetration Testing Lab | Page 3](https://pentestlab.blog/tag/privilege-escalation/page/3/)

[Post Exploitation — Ptest Method 1 documentation](https://ptestmethod.readthedocs.io/en/latest/LFF-IPS-P4-PostExploitation.html)

[MySQL SQL Injection Cheat Sheet | pentestmonkey](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet)

[Basic Shellshock Exploitation - Knapsy’s brain dump](https://blog.knapsy.com/blog/2014/10/07/basic-shellshock-exploitation/)

[HowTo: Grant Root Access to User - Root Privileges - Linux - ShellHacks](https://www.shellhacks.com/how-to-grant-root-access-user-root-privileges-linux/)

[Filesystem Hierarchy Standard](http://www.pathname.com/fhs/pub/fhs-2.3.html)

[Post-Exploitation Without A TTY | pentestmonkey](http://pentestmonkey.net/blog/post-exploitation-without-a-tty)

[Escaping Restricted Shell | SecureBean](http://securebean.blogspot.com/2014/05/escaping-restricted-shell_3.html)

[Restricted Linux Shell Escaping Techniques | FireShell Security Team](https://fireshellsecurity.team/restricted-linux-shell-escaping-techniques/)

[How do I find out what shell I am using on Linux/Unix? - nixCraft](https://www.cyberciti.biz/tips/how-do-i-find-out-what-shell-im-using.html)

[GitHub - peterpt/fuzzbunch: Shadow Brokers NSA fuzzbunch tool leak . With windows auto instalation script](https://github.com/peterpt/fuzzbunch)

[Wizard Labs: Dummy | 0xdf hacks stuff](https://0xdf.gitlab.io/2019/02/22/wl-dummy.html)

[GitHub - amonsec/exploit: Collection of different exploits](https://github.com/amonsec/exploit)

[Get Reverse-shell via Windows one-liner](https://www.hackingarticles.in/get-reverse-shell-via-windows-one-liner/)

[Windows oneliners to download remote payload and execute arbitrary code – arno0x0x](https://arno0x0x.wordpress.com/2017/11/20/windows-oneliners-to-download-remote-payload-and-execute-arbitrary-code/)

[GreatSCT/GreatSCT: The project is called Great SCT (Great Scott). Great SCT is an open source project to generate application white list bypasses. This tool is intended for BOTH red and blue team.](https://github.com/GreatSCT/GreatSCT)

[Femitter FTP Server 1.04 - Directory Traversal](https://www.exploit-db.com/exploits/15445)

[wireghoul/dotdotpwn: DotDotPwn - The Directory Traversal Fuzzer](https://github.com/wireghoul/dotdotpwn)

[fingerprinting - How to find Windows version from the file on a remote system - Information Security Stack Exchange](https://security.stackexchange.com/questions/110673/how-to-find-windows-version-from-the-file-on-a-remote-system)

[OSCP-2/Exploits at master · codingo/OSCP-2](https://github.com/codingo/OSCP-2/tree/master/Exploits)

[List of FTP commands - Wikipedia](https://en.wikipedia.org/wiki/List_of_FTP_commands)

[Manually Exploiting MS17-010 - LMG Security](https://lmgsecurity.com/manually-exploiting-ms17-010/)

[pentest/exploit\_win at master · jivoi/pentest](https://github.com/jivoi/pentest/tree/master/exploit_win)

[exploitdb/exploits at master · offensive-security/exploitdb](https://github.com/offensive-security/exploitdb/tree/master/exploits)

[Hack The Box (HTB): Blue – Travis – Medium](https://medium.com/@sdgeek/hack-the-box-htb-blue-115b3f563125)

[Exploiting Eternalblue for shell with Empire & Msfconsole - Hacking Tutorials](https://www.hackingtutorials.org/exploit-tutorials/exploiting-eternalblue-for-shell-with-empire-msfconsole/)

[Tags | 0xdf hacks stuff](https://0xdf.gitlab.io/tags.html)

[mez0cc/MS17-010-Python: MS17-010: Python and Meterpreter](https://github.com/mez0cc/MS17-010-Python)

[EternalBlue7 Crashing Server 2008 · Issue #3 · worawit/MS17-010](https://github.com/worawit/MS17-010/issues/3)

[A Guide to Exploiting MS17-010 With Metasploit — Secure Network Technologies | Penetration Testers & Ethical Hackers](https://www.securenetworkinc.com/news/2017/9/7/a-guide-to-exploiting-ms17-010-with-metasploit)

[Hacking Windows with Meterpreter](https://www.coengoedegebure.com/hacking-windows-with-meterpreter/)

[exploiting-ebdp-en.pdf](https://dl.packetstormsecurity.net/papers/attack/exploiting-ebdp-en.pdf)

[System | Init Se7en](https://initse7en.github.io/system/)

[Metasploit Console: my own cheatsheet | So Long, and Thanks for All the Fish](https://www.andreafortuna.org/2017/12/11/metasploit-console-my-own-cheatsheet/)

[REPTILEHAUS/Eternal-Blue: REPTILEHAUS' simplified build process of Worawit Wang' (@sleepya\_) version of EternalBlue.. The NSA exploit brought to you by the ShadowBrokers for exploiting MS17-010](https://github.com/REPTILEHAUS/Eternal-Blue)

[sailay1996/eternal-pulsar: Eternalblue-Doublepulsar without Metasploit or python](https://github.com/sailay1996/eternal-pulsar)

[AusJock/Privilege-Escalation: This contains common local exploits and enumeration scripts](https://github.com/AusJock/Privilege-Escalation)

[SecWiki](https://github.com/SecWiki)

[Best JSBeautifier tool work as JavScript Beautifier and JavScript Viewer](https://codebeautify.org/jsviewer)

[sheets/command\_line.md · master · dud1337 / hackfort · GitLab](https://git.138.io/dud1337/hackfort/blob/master/sheets/command_line.md)

[DDecode - Hex,Octal,HTML Decoder](http://ddecode.com/hexdecoder/?results=500515a282250e28bf5a487caee79a7b)

[OS and Application Fingerprinting Techniques](https://www.sans.org/reading-room/whitepapers/tools/os-application-fingerprinting-techniques-1891)

[SecLists/default-passwords.csv at master · danielmiessler/SecLists](https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/default-passwords.csv)

[lucyoa/kernel-exploits](https://github.com/lucyoa/kernel-exploits)

[Reverse Remote Shell – Freecode](http://freshmeat.sourceforge.net/projects/rrs)

[PoCs · dirtycow/dirtycow.github.io Wiki](https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs)

[MarkBuffalo/exploits: Some random exploits that may or may not be useful. Not responsible for misuse.](https://github.com/MarkBuffalo/exploits)

[galkan/crowbar: Crowbar is brute forcing tool that can be used during penetration tests. It is developed to support protocols that are not currently supported by thc-hydra and other popular brute forcing tools.](https://github.com/galkan/crowbar)

[SSH Keys: A Primer – Hacker Noon](https://hackernoon.com/ssh-keys-a-primer-7ac8b790e849)

[Use Public Key Authentication with SSH](https://www.linode.com/docs/security/authentication/use-public-key-authentication-with-ssh/)

[Linux elevation of privileges](https://guif.re/linuxeop)

[g0tmi1k/debian-ssh: Debian OpenSSL Predictable PRNG (CVE-2008-0166)](https://github.com/g0tmi1k/debian-ssh)

[/etc/shadow file format in Linux Explained ~ Your Own Linux..!](http://www.yourownlinux.com/2015/08/etc-shadow-file-format-in-linux-explained.html)

[Project 12: Cracking Linux Password Hashes with Hashcat (15 pts.)](https://samsclass.info/123/proj10/p12-hashcat.htm)

[tommelo/shadowcrack: CLI Tool for cracking Linux /etc/shadow hashed passwords](https://github.com/tommelo/shadowcrack)

[SUID Executables | Penetration Testing Lab](https://pentestlab.blog/2017/09/25/suid-executables/)

[Reverse Shell Cheat Sheet](https://highon.coffee/blog/reverse-shell-cheat-sheet/)

[bhasbor/OSCP-2: This repo consists of important links (or URLs) which were bookmarked during my journey of OSCP Certification.](https://github.com/bhasbor/OSCP-2)

[ManageEngineFileUploadExploit/me.rb at master · Trek333/ManageEngineFileUploadExploit](https://github.com/Trek333/ManageEngineFileUploadExploit/blob/master/me.rb)

[ankh2054/python-exploits: Repository for python exploits](https://github.com/ankh2054/python-exploits)

[Useful commands for Windows administrators](https://www.robvanderwoude.com/ntadmincommands.php)

[wget vbscript](https://gist.github.com/sckalath/ec7af6a1786e3de6c309)

<https://gist.githubusercontent.com/thel3l/993f8ed81a56e10525dd4812ad01ff2a/raw/e97cf87a7bcb310f3272bb0a8427c2aecbea7029/ms17-010_sleepya-fixed.py>

[fuzzdb-project/fuzzdb: Dictionary of attack patterns and primitives for black-box application fault injection and resource discovery.](https://github.com/fuzzdb-project/fuzzdb)

[brutespray/wordlist at master · x90skysn3k/brutespray](https://github.com/x90skysn3k/brutespray/tree/master/wordlist)

[Exploiting Apache Tomcat through port 8009 using the Apache JServ Protocol | Ionize](https://ionize.com.au/exploiting-apache-tomcat-port-8009-using-apache-jserv-protocol/)

[abaykan/CrawlBox: Easy way to brute-force web directory.](https://github.com/abaykan/CrawlBox)

<https://raw.githubusercontent.com/codingo/OSCP-2/master/BASH/PortKnocker.sh>

[Top-Hat-Sec - Index](https://forum.top-hat-sec.com/)

[SecWiki/linux-kernel-exploits: linux-kernel-exploits Linux平台提权漏洞集合](https://github.com/SecWiki/linux-kernel-exploits)

[Privilege escalation - Hackepedia](http://www.hackepedia.org/?title=Privilege_escalation)

[Transferring files - Pentest Notes](https://guide.offsecnewbie.com/transferring-files)

[Infrastructure PenTest Series : Part 1 - Intelligence Gathering — tech.bitvijays.com](https://bitvijays.github.io/LFF-IPS-P1-IntelligenceGathering.html)

[Infrastructure PenTest Series : Part 2 - Vulnerability Analysis — tech.bitvijays.com](https://bitvijays.github.io/LFF-IPS-P2-VulnerabilityAnalysis.html)

[NetBIOS and SMB Penetration Testing on Windows](https://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/)

[PayloadsAllTheThings/Active Directory Attack.md at master · swisskyrepo/PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md)

[AD-Attack-Defense/README.md at master · infosecn1nja/AD-Attack-Defense](https://github.com/infosecn1nja/AD-Attack-Defense/blob/master/README.md)

[DDecode - Hex,Octal,HTML Decoder](http://ddecode.com/hexdecoder/?results=4791fbd22b3c4fc0d1f34a7035d96921)

[WebHacking101/xss-reflected-steal-cookie.md at master · s0wr0b1ndef/WebHacking101](https://github.com/s0wr0b1ndef/WebHacking101/blob/master/xss-reflected-steal-cookie.md)

[ie\_aurora/ie\_aurora.py at master · Muhammd/ie\_aurora](https://github.com/Muhammd/ie_aurora/blob/master/ie_aurora.py)

[渗透测试学习笔记之案例六 - 先知社区](https://xz.aliyun.com/t/7)

[Metasploit Cheatsheet](https://techvomit.net/metasploit-cheatsheet/)

[USEFULL OSCP MATERIAL | Future OSCP](http://futureoscp.blogspot.com/2017/10/usefull-oscp-material.html)

[How to use the "netsh advfirewall firewall" context instead of the "netsh firewall" context to control Windows Firewall behavior in Windows Server 2008 and in Windows Vista](https://support.microsoft.com/en-in/help/947709/how-to-use-the-netsh-advfirewall-firewall-context-instead-of-the-netsh)

[How to edit the Registry using Command Prompt on Windows 10 | Windows Central](https://www.windowscentral.com/how-edit-registry-using-command-prompt-windows-10)

[Pentesting Notes | Walkthrough](https://malikashish8.github.io/Walkthrough/notes/)

[Backdooring EXE Files - Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/)

[MSFvenom - Metasploit Unleashed](https://www.offensive-security.com/metasploit-unleashed/msfvenom/)

[IIS5.1 Directory Authentication Bypass by using “:$I30:$Index\_Allocation” | Soroush Dalili (@irsdl) – سروش دلیلی](https://soroush.secproject.com/blog/2010/07/iis5-1-directory-authentication-bypass-by-using-i30index_allocation/)

[quentinhardy/msdat: MSDAT: Microsoft SQL Database Attacking Tool](https://github.com/quentinhardy/msdat)

[Enabling xp\_cmdshell in SQL Server](https://www.mssqltips.com/sqlservertip/1020/enabling-xpcmdshell-in-sql-server/)

[Full MSSQL Injection PWNage](https://www.exploit-db.com/papers/12975)

[m8r0wn/enumdb: MySQL and MSSQL brute force and post exploitation tool to search through databases and extract sensitive information.](https://github.com/m8r0wn/enumdb)

[pypsexec · PyPI](https://pypi.org/project/pypsexec/)

[swisskyrepo/PayloadsAllTheThings: A list of useful payloads and bypass for Web Application Security and Pentest/CTF](https://github.com/swisskyrepo/PayloadsAllTheThings)

[Windows oneliners to get shell – ironHackers](https://ironhackers.es/en/cheatsheet/comandos-en-windows-para-obtener-shell/)

[xl7dev/WebShell: Webshell && Backdoor Collection](https://github.com/xl7dev/WebShell)

[UB3RSEC - Reverse Shells](https://ub3rsec.github.io/pages/rev-shell-cheatsheet.html)

[Post Exploitation File Transfers on Windows the Manual Way | Michael Thelen](https://isroot.nl/2018/07/09/post-exploitation-file-transfers-on-windows-the-manual-way/)

[windows-kernel-exploits/MS11-046 at master · SecWiki/windows-kernel-exploits](https://github.com/SecWiki/windows-kernel-exploits/tree/master/MS11-046)

[Penetration-Testing-Grimoire/cadaver.md at master · weaknetlabs/Penetration-Testing-Grimoire](https://github.com/weaknetlabs/Penetration-Testing-Grimoire/blob/master/Post%20Exploitation/cadaver.md)

[AresS31/xmlrpc-bruteforcer: Multi-threaded XMLRPC brute forcer using amplification attacks targeting WordPress installations prior to version 4.4.](https://github.com/AresS31/xmlrpc-bruteforcer)

[Offensive-Security-OSCP-Cheatsheets/ssh-tunnelling-port-forwarding.md at master · mantvydasb/Offensive-Security-OSCP-Cheatsheets](https://github.com/mantvydasb/Offensive-Security-OSCP-Cheatsheets/blob/master/offensive-security/ssh-tunnelling-port-forwarding.md)

[Diary of a reverse-engineer](https://doar-e.github.io/index.html)

[CTF-notes/Kali Linux Offensive Security Certified Professional Playbook.html at master · Shiva108/CTF-notes](https://github.com/Shiva108/CTF-notes/blob/master/Kali%20Linux%20Offensive%20Security%20Certified%20Professional%20Playbook.html)

<https://h4ck.co/wp-content/uploads/2018/06/cheatsheet.txt>

[spencerdodd/kernelpop: kernel privilege escalation enumeration and exploitation framework](https://github.com/spencerdodd/kernelpop)

[From MS14-068 to Full Compromise - Step by Step](https://www.trustedsec.com/2014/12/ms14-068-full-compromise-step-step/)

[Enumerating Windows Domains with rpcclient through SocksProxy == Bypassing Command Line Logging - Red Teaming Experiments](https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/enumerating-windows-domains-using-rpcclient-through-socksproxy-bypassing-command-line-logging)

[Infrastructure PenTest Series : Part 3 - Exploitation — tech.bitvijays.com](https://bitvijays.github.io/LFF-IPS-P3-Exploitation.html)

[citronneur/rdpy: Remote Desktop Protocol in Twisted Python](https://github.com/citronneur/rdpy)

[pWnOS 2 (SQL Injection)](https://blog.g0tmi1k.com/2012/09/pwnos-2-sql-injection/)

[Time based Blind Injection](http://www.securityidiots.com/Web-Pentest/SQL-Injection/time-based-blind-injection.html)

[Explore Hidden Networks With Double Pivoting – Pentest Blog](https://pentest.blog/explore-hidden-networks-with-double-pivoting/)

[The Journey to Try Harder: TJnull’s Preparation Guide for PWK/OSCP | NetSec Focus](https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html)

[Port Forwarding in Windows | Windows OS Hub](http://woshub.com/port-forwarding-in-windows/)

[How to Pivot the Network (Port-Forwarding/Redirection) - A Hands-On Look - Cybrary](https://www.cybrary.it/0p3n/pivot-network-port-forwardingredirection-hands-look/)

[OSCP Goldmine (not clickbait) | 0xc0ffee☕](http://0xc0ffee.io/blog/OSCP-Goldmine)

[Oscp exam guide - Offensive Security](https://support.offensive-security.com/oscp-exam-guide/)

[Offensive Security Support - Live Chat](https://support.offensive-security.com/chat.php)

[doffensive/wired-courtyard: Handbook and survival guide for hacking over the wire, OSCP-style](https://github.com/doffensive/wired-courtyard)

[doffensive/wired-courtyard: Handbook and survival guide for hacking over the wire, OSCP-style](https://github.com/doffensive/wired-courtyard#information-gathering--vulnerability-scanning)

[Setting up an SSH tunnel to access Remote Desktop using Putty and SSHD on Linux | Johan Driessen](https://johan.driessen.se/posts/Setting-up-an-SSH-tunnel-to-access-Remote-Desktop-using-Putty-and-SSHD-on-Linux/)

[A Red Teamer's guide to pivoting](https://artkond.com/2017/03/23/pivoting-guide/)

[PayloadsAllTheThings/Network Pivoting Techniques.md at master · swisskyrepo/PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Network%20Pivoting%20Techniques.md)

[Dynamic Port Forwarding (SSH)](https://netsec.ws/?p=278)

[Whitelist: SSH Tunneling (III): DYNAMIC port forwarding with PROXYCHAINS](https://www.whitelist1.com/2017/10/ssh-tunneling-iii-dynamic-port.html)

[Pivoting - Hacking](https://www.jdksec.com/methodologies/pivoting)

[Internal Network - Hacking](https://www.jdksec.com/methodologies/internal-network)

<https://raw.githubusercontent.com/eset/malware-research/master/moose/targeted-vendors/default-credentials-list.txt>

[SSH Tunneling - Local, Remote & Dynamic](https://namc.in/2018-06-26-ssh-port-forwarding)

[A Guide to SSH Port Forwarding/Tunnelling - Boolean World](https://www.booleanworld.com/guide-ssh-port-forwarding-tunnelling/)

[WTF? Reverse SSH tunnel and Dynamic proxy via Plink : oscp](https://www.reddit.com/r/oscp/comments/b10ok6/wtf_reverse_ssh_tunnel_and_dynamic_proxy_via_plink/)

[rpivot: socks4 reverse proxy for penetration testing • Penetration Testing](https://securityonline.info/rpivot-socks4-reverse-proxy/)

[klsecservices/rpivot: socks4 reverse proxy for penetration testing](https://github.com/klsecservices/rpivot)

[Exploit Development – Infosec Notes to Myself](https://traviswhitney.com/category/exploit-development/)

[Buffer Overflows – An introduction with SLMail – A site about computers, security, communication and life.](https://www.hugohirsh.com/?p=509)

[Basic Buffer Overflows - Thor-Sec](https://thor-sec.com/tutorial/oscp/basic_bufferoverflows/)

[Handy Commands for Exploit Development · Greycel](http://www.greycel.com/2017/04/15/Handy-Commands-ExpDev/)

[Immunity Debugger basics, part 1 | Blog for and by my students, current and future...](https://sgros-students.blogspot.com/2014/05/immunity-debugger-basics-part-1.html)

[Exploiting "Vulnerable Server" for Windows 7](https://samsclass.info/127/proj/vuln-server.htm)

[whoami | Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/whoami)

[How to Find the Security Identifier of Any User Account in Windows - Make Tech Easier](https://www.maketecheasier.com/find-user-security-identifier-windows/)

[List members of a Windows group using command line - Super User](https://superuser.com/questions/344728/list-members-of-a-windows-group-using-command-line)

[Command Line User Administration Tutorial for Windows User](https://www.slashroot.in/command-line-user-administration-tutorial-windows-user)

[Privilege Escalation | Penetration Testing Lab](https://pentestlab.blog/category/privilege-escalation/)

[MyExperiments - Local Linux privilege escalation overview](https://myexperiments.io/linux-privilege-escalation.html)

[iKuppu: Windows Post Exploitation](http://www.ikuppu.com/2011/09/windows-post-exploitation.html)

[OSCP Exam Attempt #2 – FalconSpy – Medium](https://medium.com/@falconspy/oscp-exam-attempt-2-c9e4d5b8f858)

[Tib3rius/AutoRecon: AutoRecon is a multi-threaded network reconnaissance tool which performs automated enumeration of services.](https://github.com/Tib3rius/AutoRecon)

[dzonerzy/goWAPT: Go Web Application Penetration Test](https://github.com/dzonerzy/goWAPT)

[OSCP Course & Exam Preparation - Ellingson Mineral](https://411hall.github.io/OSCP-Preparation/)

[51x/WHP: Micro$oft Windows Hacking Pack](https://github.com/51x/WHP)

[Infosec\_Reference/privesc.md at master · rmusser01/Infosec\_Reference](https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/privesc.md)

[Windows Privilege Escalation Methods for Pentesters – Pentest Blog](https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/)

[Privilege escalation: Windows - Hacker's Grimoire](https://vulp3cula.gitbook.io/hackers-grimoire/post-exploitation/privesc-windows)

[Windows Privilege Escalation Guide](https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/)

[Exploiting Wildcard for Privilege Escalation](https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/)

[Hack the Box Challenge: Europa Walkthrough](https://www.hackingarticles.in/hack-the-box-challenge-europa-walkthrough/)

[Hack the Milnet VM (CTF Challenge)](https://www.hackingarticles.in/hack-milnet-vm-ctf-challenge/)

[Linux Privilege Escalation by Exploiting Cronjobs](https://www.hackingarticles.in/linux-privilege-escalation-by-exploiting-cron-jobs/)

[Privilege Escalation on Windows 7,8,10, Server 2008, Server 2012 using Potato](https://www.hackingarticles.in/privilege-escalation-on-windows-7810-server-2008-server-2012-using-potato/)

[sagishahar/lpeworkshop: Windows / Linux Local Privilege Escalation Workshop](https://github.com/sagishahar/lpeworkshop/blob/master/Lab%20Exercises%20Walkthrough%20-%20Linux.pdf)

[Linux Privilege Escalation using Misconfigured NSF](http://hackersgeeks.blogspot.com/2018/05/linux-privilege-escalation-using_26.html)

[Privilege escalation: Linux - Hacker's Grimoire](https://vulp3cula.gitbook.io/hackers-grimoire/post-exploitation/privesc-linux)

[Day 44: Linux Capabilities Privilege Escalation via OpenSSL with SELinux Enabled and Enforced.](https://medium.com/@int0x33/day-44-linux-capabilities-privilege-escalation-via-openssl-with-selinux-enabled-and-enforced-74d2bec02099)

[abatchy17/WindowsExploits: Windows exploits, mostly precompiled. Not being updated. Check https://github.com/SecWiki/windows-kernel-exploits instead.](https://github.com/abatchy17/WindowsExploits)

[OSCP Review - AwanSec](https://awansec.com/oscp-review.html)

[Beginner’s Guide to Impacket Tool kit (Part 1)](https://www.hackingarticles.in/beginners-guide-to-impacket-tool-kit-part-1/)

[Dumping Domain Password Hashes | Penetration Testing Lab](https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/)

<https://raw.githubusercontent.com/M4ximuss/Powerless/master/Powerless.bat>

[sectalks/ctf-solutions/SYD0x0b/z00nx at master · sectalks/sectalks](https://github.com/sectalks/sectalks/tree/master/ctf-solutions/SYD0x0b/z00nx)

[CTF Series : Vulnerable Machines — tech.bitvijays.com](https://bitvijays.github.io/LFC-VulnerableMachines.html)

[Hack the Box: Solid State Walkthrough – Deceptive Security](https://deceiveyour.team/2018/01/27/hack-the-box-solid-state-walkthrough/)

[Optimum write-up - The Portal of Knowledge](https://alamot.github.io/optimum_writeup/)

[yanncam/exe2powershell: exe2powershell - exe2bat reborn for modern Windows](https://github.com/yanncam/exe2powershell)

[Windows Privilege Escalation – daya's blog](https://daya.blog/2018/01/06/windows-privilege-escalation/)

[Always Install Elevated | Penetration Testing Lab](https://pentestlab.blog/2017/02/28/always-install-elevated/)

[Windows Privilege Escalation (AlwaysInstallElevated)](https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/)

[PayloadsAllTheThings/Linux - Privilege Escalation.md at master · swisskyrepo/PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md)

[MySQL Root to System Root with lib\_mysqludf\_sys for Windows and Linux](https://www.adampalmer.me/iodigitalsec/2013/08/13/mysql-root-to-system-root-with-udf-for-windows-and-linux/)

[juliocesarfort/public-pentesting-reports: Curated list of public penetration test reports released by several consulting firms and academic security groups](https://github.com/juliocesarfort/public-pentesting-reports)

[ohpe/juicy-potato: A sugared version of RottenPotatoNG, with a bit of juice, i.e. another Local Privilege Escalation tool, from a Windows Service Accounts to NT AUTHORITY\SYSTEM.](https://github.com/ohpe/juicy-potato)

[Privilege Escalation | Penetration Testing Lab | Page 2](https://pentestlab.blog/category/privilege-escalation/page/2/)

[MSIEXEC | Penetration Testing Lab](https://pentestlab.blog/tag/msiexec/)

[Nishang | Penetration Testing Lab](https://pentestlab.blog/tag/nishang/)

[Offensive Security FAQ](https://www.offensive-security.com/faq/#exam-proc)

[Identifying and Cracking Hashes](https://infosecadventures.com/2019/01/21/Identifying-and-Cracking-Hashes/)

[Hack the Box Challenge Lazy Walkthrough](https://www.hackingarticles.in/hack-the-box-challenge-lazy-walkthrough/)

[https://raw.githubusercontent.com/Dhayalanb/windows-php-reverse-shell/master/Reverse Shell.php](https://raw.githubusercontent.com/Dhayalanb/windows-php-reverse-shell/master/Reverse%20Shell.php)

[Apache CouchDB < 2.1.0 - Remote Code Execution](https://www.exploit-db.com/exploits/44913)

[PayloadsAllTheThings/Reverse Shell Cheatsheet.md at master · swisskyrepo/PayloadsAllTheThings](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#nodejs)

[Apache CouchDB 1.7.0 / 2.x < 2.1.1 - Remote Privilege Escalation](https://www.exploit-db.com/exploits/44498)

[oscommerce exploit - Google Search](https://www.google.com/search?ei=_cbzXJnBO82f9QO7ta-YDg&q=oscommerce+exploit&oq=oscommerce+exploit&gs_l=psy-ab.3..0i7i30l6j0i8i7i10i30j0i13i30.2249524.2251755..2251870...0.0..0.185.1357.0j9......0....1..gws-wiz.......0i71.LFTz4j6rRoA)

[osCommerce 2.3.4.1 - Remote Code Execution](https://www.exploit-db.com/exploits/44374)

[September | 2016 |](https://www.mrb3n.com/?m=201609)

[ProFTPd 1.3.5 Remote File Copy - CXSecurity.com](https://cxsecurity.com/issue/WLB-2015040075)

[windows-php-reverse-shell/Reverse Shell.php at master · Dhayalanb/windows-php-reverse-shell](https://github.com/Dhayalanb/windows-php-reverse-shell/blob/master/Reverse%20Shell.php)