- Schedule the exam halfway through your lab time so you get a feel for the exam and know where your weak points are in time to hone in on them. It's only $60 to do a retake which is significantly cheaper than most.
- Create a plan and stick to it, schedule breaks
- Have your cheat sheets ready and shells for various occasions
- Don't get stuck on any one machine rotate, every 3-4 hours
- Write your report ahead of time so that you only need to add your exam notes in
- Stick to your methodology and enumerate EVERYTHING
- Start off with light port scans and work your way to more advanced ones
- I had better luck with the higher point machines so I always started with those
- Take a break of it all for a day or two before your exam

Resources

Practice

Pushebx: Penetration Testing - Vulnerable - ISO (http://blog.pushebx.com/2011/03/penetration-testing-iso.html)

Practice CTFs (http://captf.com/practice-ctf/)

OverTheWire: Wargames (http://overthewire.org/wargames/)

Penetration Testing Mind Map (http://www.amanhardikar.com/mindmaps/Practice.html)

Vulnerable by Design (https://blog.g0tmi1k.com/2011/03/vulnerable-by-design/)

Exploit Exercises (https://exploit-exercises.com/)

Hack This Site! (https://www.hackthissite.org/pages/programs/programs.php)

Vulnhub OSCP-like machines

SickOs: 1.2 (https://www.vulnhub.com/entry/sickos-12,144/)

Kioptrix: 2014 (https://www.vulnhub.com/entry/kioptrix-2014-5,62/)

SkyTower: 1 (https://www.vulnhub.com/entry/skytower-1,96/)

FristiLeaks: 1.3 (https://www.vulnhub.com/entry/fristileaks-13,133/)

Stapler: 1 (https://www.vulnhub.com/entry/stapler-1,150/)

Mr-Robot: 1 (https://www.vulnhub.com/entry/mr-robot-1,151/)

PwnLab: init (https://www.vulnhub.com/entry/pwnlab-init,158/)

VulnOS: 2 (https://www.vulnhub.com/entry/vulnos-2,147/)

Brainpan: 1 (https://www.vulnhub.com/entry/brainpan-1,51/)

HackLAB: Vulnix (https://www.vulnhub.com/entry/hacklab-vulnix,48/)

pWnOS: 2.0 (https://www.vulnhub.com/entry/pwnos-20-pre-release,34/)

Reporting

Offensive Security - Sample Penetration Test Report (https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf)

What is MagicTree (http://www.gremwell.com/what_is_magictree)

Pivoting

Scenario Based Infrastructure Hacktics (http://www.fuzzysecurity.com/tutorials/13.html)

SSH Tunneling (http://exploit.co.il/networking/ssh-tunneling/)

Pink (http://www.pc-freak.net/blog/creating-ssh-tunnel-windows-plink/)

SSH Tunneling (http://superuser.com/questions/96489/an-ssh-tunnel-via-multiple-hops)

Transparent Multihop (http://sshmenu.sourceforge.net/articles/transparent-mulithop.html)

Tunneling (https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117)

IP tables (http://www.linuxquestions.org/questions/linux-networking-3/iptables-forward-port-to-another-host-844467/)

SSH Meterpreter Pivoting Technqiues (https://highon.coffee/blog/ssh-meterpreter-pivoting-techniques/)

Post Exploitation

Windows Post Exploitation (http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf)

Post Exploitation Using Meterpreter (https://www.exploit-db.com/docs/18229.pdf)

(https://docs.google.com/viewer?url=https%3A%2F%2Fwww.exploit-db.com%2Fdocs%2F18229.pdf&embedded=true&chrome=false&dov=1)

Priv Esc - Win

Elevating Privileges (https://hackmag.com/security/elevating-privileges-to-administrative-and-further/)
Privilege escalation via weak services (http://travisaltman.com/windows-privilege-escalation-via-weak-service-permissions/)
MS Priv Esc (http://toshellandback.com/2015/11/24/ms-priv-esc/)
Windows Privilege Escalation Fundamentals (http://www.fuzzysecurity.com/tutorials/16.html)
Windows Privesc Check (https://github.com/pentestmonkey/windows-privesc-check)
Post Exploitation without a tty (http://pentestmonkey.net/blog/post-exploitation-without-a-tty)
WinEXE (http://www.desmoulins.fr/index_us.php?pg=informatique!linux!console!winexe)
DLL Hijacking (https://www.exploit-db.com/dll-hijacking-vulnerable-applications/)
Metasploit Unleashed (https://www.offensive-security.com/metasploit-unleashed/portfwd/)
Udev Exploit Allows Local Privilege Escalation (http://www.madirish.net/370)
Create Admin user from command line (http://superuser.com/questions/515175/create-admin-user-from-command-line)
Windows Exploit Suggester (https://github.com/GDSSecurity/Windows-Exploit-Suggester/blob/master/windows-exploit-suggester.py)

UAC - What Pen Testers should know (http://blog.cobaltstrike.com/2014/03/20/user-account-control-what-penetration-testers-should-know/)

Bypassing UAC with Powershell (http://www.labofapenetrationtester.com/2015/09/bypassing-uac-with-powershell.html)

Win Exploit Suggester Intro (https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit-suggester.html)

Infosec Reference (https://github.com/rmusser01/Infosec_Reference/)

Priv Esc - Nix

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

Udev (http://seclists.org/fulldisclosure/2009/Apr/att-198/udev.txt)

Enumeration & Privilege Escalation Cheat Sheet (http://www.rebootuser.com/?p=1623)

Linux Networking How To (http://oss.sgi.com/LDP/HOWTO/Net-HOWTO/x635.html)

AutoLocalPrivilegeEscalation (https://github.com/ngalongc/AutoLocalPrivilegeEscalation)

Escaping Restricted Shells (http://securebean.blogspot.com/2014/05/escaping-restricted-shell_3.html)

Fundamentals of Linux Privilege Escalation (http://www.slideshare.net/nullthreat/fund-linux-priv-esc-wprotections)

LinEnum (https://github.com/rebootuser/LinEnum)

LineEnum Enumeration Privilege Escalation Tool (http://www.darknet.org.uk/2014/11/linenum-linuxenumeration-privilege-escalation-tool/)

Inetd (https://debian-handbook.info/browse/stable/sect.inetd.html)

Introducing LinEnum (https://www.rebootuser.com/?p=1758)

Password Cracking

John the Ripper Cheat Sheet (https://countuponsecurity.files.wordpress.com/2016/09/jtr-cheat-sheet.pdf)

(https://docs.google.com/viewer?url=https%3A%2F%2Fcountuponsecurity.files.wordpress.com%2F2016%2F09%2Fjtr-cheat-sheet.pdf&embedded=true&chrome=false&dov=1)

Hashcat FAQ (https://hashcat.net/wiki/doku.php?id=frequently_asked_questions)

Password Crackers Cheat Sheet (https://www.unix-ninja.com/p/A_cheat-sheet_for_password_crackers)

Generating Wordlists (http://netsec.ws/?p=457)

SQL

Accessing and Hacking MSSQL from Backtrack (http://www.iodigitalsec.com/accessing-and-hacking-mssql-from-backtrack-linux/)

Anatomy of an attack (http://resources.infosecinstitute.com/anatomy-of-an-attack-gaining-reverse-shell-from-sql-injection/)

Blind SQL Injection (https://www.exploit-db.com/docs/12622.pdf)

(https://docs.google.com/viewer?url=https%3A%2F%2Fwww.exploit-db.com%2Fdocs%2F12622.pdf&embedded=true&chrome=false&dov=1)

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

SQL Map (http://carnal0wnage.attackresearch.com/2011/03/sqlmap-with-post-requests.html)

Payloads

Hex Values (http://stackoverflow.com/questions/1996184/all-possible-combination-for-an-hex-value-from-a-given-set-of-chars)

Generating Payloads (https://www.offensive-security.com/metasploit-unleashed/generating-payloads/)

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

Reverse shell with bash (http://www.gnucitizen.org/blog/reverse-shell-with-bash/)

Veil (https://www.youtube.com/watch?v=v1OXNP_bl8U)

AutoMigrate (https://community.rapid7.com/thread/2082)

Reverse Shell Cheat Sheet (https://www.phillips321.co.uk/2012/02/05/reverse-shell-cheat-sheet/)

Offset-DB (http://offset-db.com/)

Specific Exploits

LARES-ColdFusion (http://www.carnal0wnage.com/papers/LARES-ColdFusion.pdf)

(https://docs.google.com/viewer?url=http%3A%2F%2Fwww.carnal0wnage.com%2Fpapers%2FLARES-ColdFusion.pdf&embedded=true&chrome=false&dov=1)

Hacking a domain controller (http://web.archive.org/web/20141004091538/http:/www.slaughterjames.com/blog/2012/10/23/hacking-a-domain-controller-part-1-enumeration.html)

Mimikatz (https://adsecurity.org/?p=556)

Client Side Exploits (https://www.offensive-security.com/metasploit-unleashed/client-side-exploits/)

C Pointers (https://www.tutorialspoint.com/cprogramming/c_pointers.htm)

Networking

ethereal tcpdump (http://alumni.cs.ucr.edu/~marios/ethereal-tcpdump.pdf)

tcpdump (https://danielmiessler.com/study/tcpdump/)

traffic accounting with ip tables (https://openvz.org/Traffic_accounting_with_iptables)

Netsh Commands for Windows Firewall (https://technet.microsoft.com/en-us/library/cc771920(v=ws.10).aspx)

Misc

Tactical Exploitation (https://www.exploit-db.com/docs/172.pdf)

Help Beacon Peer (http://www.advancedpentest.com/help-beacon-peer)

Stealthy peer to peer (http://blog.cobaltstrike.com/2013/12/06/stealthy-peer-to-peer-cc-over-smb-pipes/)

Nishang (https://github.com/samratashok/nishang/tree/master/Escalation)

Powershell Empire (http://www.powershellempire.com/)

Pentest tips and tricks (https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/)

g0tmi1k github (https://github.com/g0tmi1k/)

Pen Testing Cheat Sheet (https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/)

Metasploit

MPC (https://github.com/g0tmi1k/mpc)

Converting Metasploit Modules (http://netsec.ws/?p=262)

msfconsol commands (https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/)

msfcli (https://www.offensive-security.com/metasploit-unleashed/msfcli/)

misc tools sheet (https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf)

wirting meterpreter scripts (https://www.offensive-security.com/metasploit-unleashed/writing-meterpreter-scripts/)

Recon

Information gathering (http://www.sersc.org/journals/JSE/vol5_no5_2008/6.pdf)

Intelligence gathering (http://www.pentest-standard.org/index.php/Intelligence_Gathering)

Top 10 nmap commands (http://bencane.com/2013/02/25/10-nmap-commands-every-sysadmin-should-know/)

Nmap cheat sheet (http://resources.infosecinstitute.com/nmap-cheat-sheet-discovery-exploits-part-2-advance-port-scanning-nmap-custom-idle-scan/)

DotDotPwn (https://media.blackhat.com/bh-us-11/Arsenal/BH_US_11_Nitrous_DotDotPwn_Slides.pdf)
Generates 8.3 File Names from Long File Names (https://support.microsoft.com/en-us/kb/142982)
Window version from file (http://security.stackexchange.com/questions/110673/how-to-find-windows-version-from-the-file-on-a-remote-system)
Enumerating user accounts (http://carnal0wnage.attackresearch.com/2007/07/enumerating-user-accounts-on-linux-and.html)
Nikto (https://scottlinux.com/2012/07/12/create-html-reports-with-nikto-web-server-scanner/)
httpscripting (https://curl.haxx.se/docs/httpscripting.html)
Netcat (https://www.digitalocean.com/community/tutorials/how-to-use-netcat-to-establish-and-test-tcp-and-udp-connections-on-a-vps)
Offsec PWB OSCP Experience (http://www.securitysift.com/offsec-pwb-oscp/)

Conclusion

I strongly recommend anyone take the OSCP if you have an interest in information security. In comparison to many of the other security certifications, this one gives you hands-on experience and isn’t just memorizing theories and definitions. It will give you a solid foundation in the penetration testing realm that can spring board into even further research and understanding. I’ve found that it gives people increased confidence to go out and participate in those CTF’s, tear apart