Tulpa’s Preparation guide for Offensive Security’s ‘Penetration Testing with Kali Linux’ course and the ‘Offensive Security Certified Professional’ exam

Blog: www.tulpa-security.com

Twitter: @tulpa_security

E-mail: tulpa [at] tulpa-security [dot com]

Cybrary: https://www.cybrary.it/members/h4xx0/

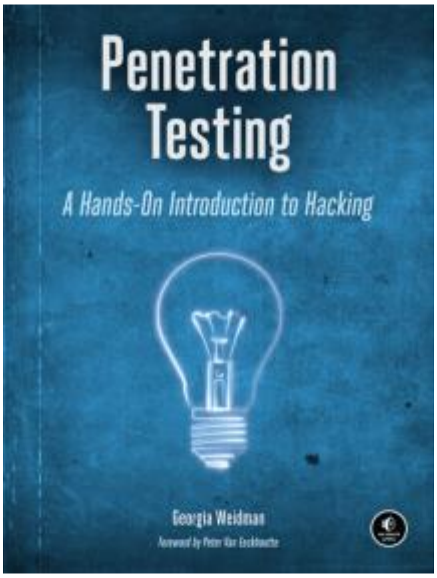
Exploit-db: https://www.exploit-db.com/author/?a=8729

Disclaimer: Take note that the views expressed in this document are my own. I have no affiliation with Offensive Security, Cybrary, No Starch Press or Georgia Weidman. I share my work freely, and in return I ask that you respect the time and effort I have invested for your benefit by refraining from editing or referencing my work in any way without referencing the source. Share freely, but give credit where its due.

Introduction

They say you should write what you want to read. Before starting my 'Penetration Testing with Kali Linux' training course, I wish I could have read a how-to-prep guide. The course does a wonderful job at getting you ready for the exam, but I feel that I could have better utilized my lab time if I had a better foundation of knowledge prior to starting the course. Hence, I have taken the time to design a study plan to achieve just that goal for other aspiring OSCP's.

The goal of this plan is not to teach you what you will learn in the PWK course. What would be the point of that? It's meant to give you a solid base from which you will be able to grasp the lessons in the PWK course faster. You'll find that each module has a minimum time commitment indicator built right in to give you an idea of how deep you should be going. Keep it a mile wide and an inch deep and you'll be well on your way.



Now in order to follow along, you'll have to get your hands of Georgia Weidman's book "A Hands-On Introduction to Hacking" from No Starch Press. You can find more information about the book here: https://www.nostarch.com/pentesting.

Not only is it a phenomenal book, but I would highly recommend any book published by No Starch Press.

You'll notice that I don't follow the order of the book or the videos on Cybrary in the order that the author intended. That's because as far as I am aware the authors did not intend for their material to form part of an OSCP prep guide. I have also excluded some things such as Mobile Hacking, which while interesting, is not going to help you pass your OSCP.

I would love to get your feedback so feel free to hit me up on e-mail. Without further delay, here is the curriculum.

Module	Book Pages	Cybrary Video	Time
Setting up your lab	9-54	None	4 Hours

Details

You're going to have to be creative with getting your hands on a copy of Windows XP. For Windows 7, you can find a VM image from the link under 'Additional Resources'. This isn't the most glamorous of modules, but ensuring that you have a lab environment in good working order will save you time in the long run. Take your time on this one to make sure everything is in place, and remember to take snapshots of your VM's.

Additional Resources

https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/

Module	Book Pages	Cybrary Video	Time
Big Picture	1-6	None	30 mins

Details

Once you got your lab, it's a good idea to get a big picture overview of where everything that you're going to learn comes together. For any penetration test to be successful, you're going to have to follow a structured approach. I would recommend reading the fantastic SANS whitepaper linked below. The six pages from Georgia's book might not look like much, but it's packed with information that you need to know off by heart. This will provide everything else that you're going to do with structure and direction.

Additional Resources

https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67

Module	Book Pages	Cybrary Video	Time
Google-Fu	113-132	Module 4 – Information Gathering	1 Hour

Details

This may sound over the top, but learning how to use google properly for the PWK is critical. You are expected to do an enormous amount of research on your own, so google will be your friend. I would also recommend that you get to know 'searchsploit' which is installed on Kali.

Additional Resources

Google Operators: https://www.cybrary.it/video/information-gathering-part-4/
How Pentesters use Google: https://www.alienvault.com/blogs/security-essentials/how-pen-testers-use-google-hacking
Searchsploit Tutorial: https://www.youtube.com/watch?v=CTYLtgScbuE

Module	Book Pages	Cybrary Video	Time
Linux Basics	55-73	Module 1 Linux	2 Hours

Details

This is really about getting to know Linux, but even more so out of the eyes of a Penetration Tester. Pay special attention to file permissions, netcat, and echo. While netcat and echo might seem basic, their applications can be mind bending to a student so make sure you know them well. Allocate a minimum of two hours to this portion, but take more time if needed because these concepts are critical to your success.

Additional Resources

Linux Part 1-https://www.cybrary.it/video/linux-part-1/
Linux Part 2 – https://www.cybrary.it/video/linux-part-2/
Linux Part 3 – https://www.cybrary.it/video/linux-part-3/
Linux Part 4 – https://www.cybrary.it/video/linux-part-4/
Linux Part 5 – https://www.cybrary.it/video/linux-part-5/
Linux Part 6 – https://www.cybrary.it/video/linux-part-6/
A great Netcat cheatsheet - https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
Primer on Linux file permissions - https://www.youtube.com/watch?v=vKTg1ATHl4E

Module	Book Pages	Cybrary Videos	Time
Scripting	75-85	Module 2 Programming Introduction to Python	90 Minutes

Details

I'm not sure why, but Cybrary and Georgia's book both refer to this section as 'programming'. If you don't have a development background, then breathe easy knowing that it's really more scripting. I also only allocate one and a half hour to this module because if you mastered the previous section then you should be well on your way to writing bash scripts and being able to edit python scripts. Again, the time I allocate is the minimum so take more time if you feel you need to.

Additional Resources

Fundamentals for Pen Testers - https://www.cybrary.it/video/programming-part-1/
Bash Scripting - https://www.cybrary.it/video/programming-part-2/
Networking Pings - https://www.cybrary.it/video/programming-part-3/
Introduction to Python - https://www.cybrary.it/video/introductory-python/
Python for Port Scanning - https://www.cybrary.it/video/programming-part-4/
Python Import Command - https://www.cybrary.it/video/programming-part-5/

Module	Book Pages	Cybrary Video	Time
Metasploit	87-109	Module 3 - Metasploit	4 Hours

Details

You might have heard that your use of metasploit in the OSCP exam is limited. That is true, however you will be using parts of it extensively both in the lab and the exam (Meterpreter, Generating Payloads etc). There is A LOT of information in this module, so you might need to come back to it at a later stage for revision towards the end of the course (I'll let you know when).

Additional Resources

Read these sections from the official Offensive Security Metasploit Guide:
https://www.offensive-security.com/metasploit-unleashed/metasploit-fundamentals/
https://www.offensive-security.com/metasploit-unleashed/msfcli/
https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/
https://www.offensive-security.com/metasploit-unleashed/using-exploits/
https://www.offensive-security.com/metasploit-unleashed/payload-types/
https://www.offensive-security.com/metasploit-unleashed/generating-payloads/
https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/
Introduction: https://www.cybrary.it/video/metasploit-part-1/
Fundamentals: https://www.cybrary.it/video/metasploit-part-2/
Operation: https://www.cybrary.it/video/metasploit-part-3/
Auxiliary Module: https://www.cybrary.it/video/metasploit-part-4/
MSFCLI: https://www.cybrary.it/video/metasploit-part-5/
MSFVENOM: https://www.cybrary.it/video/metasploit-part-6/

Module	Book Pages	Cybrary Video	Time
Enumeration 1	113-132	Module 4 – Information Gathering	3 Hours

Details

Enumeration is the number one phase of a pen test that students fail at. Everything else you are learning doesn't mean anything if you're not able to find an attack vector. None of these concepts are difficult as such, but it's very often skipped or overlooked. You don't have to spend much time on Maltego as it's not a component of the PWK labs. Also note that I excluded the Google module because that's already in another module.

Additional Resources

Introduction: https://www.cybrary.it/video/information-gathering-intro-part-1/
Domain Name Services: https://www.cybrary.it/video/information-gathering-part-2/
Maltego (Optional): https://www.cybrary.it/video/information-gathering-part-3/
NMAP and PortScanning: https://www.cybrary.it/video/information-gathering-part-5/
NMAP cheatsheet: http://cs.lewisu.edu/~klumpra/camssem2015/nmapcheatsheet1.pdf
OneTwoPunch (Optional): https://github.com/superkojiman/onetwopunch

Module	Book Pages	Cybrary Video	Time
Enumeration 2	142-153	Module 5 – Vulnerability Scanning	5 Hours

Details

These tools are indispensable for vulnerability scanning. The Nmap scripting engine is incredible powerful so don't overlook it. The Nessus videos are optional because it's not allowed in the OSCP course. The emphasis is on manual enumeration. Some of the tools that I would recommend you get to know at this stage are Nikto, Dirbuster, Enum4linux, and Sparta. This is by no means the only tools that you will encounter, but at this stage of your learning it will provide a solid foundation.

Additional Resources

Introduction: https://www.cybrary.it/video/vulnerability-scanning-intro-part-1/
Nmap Scripting Engine: https://www.cybrary.it/video/vulnerability-scanning-part-3/
Metaploit: https://www.cybrary.it/video/vulnerability-scanning-part-4/
Web Enumeration: https://www.cybrary.it/video/vulnerability-scanning-part-5/
Directory Transversals: https://www.cybrary.it/video/vulnerability-scanning-part-6/
Nikto Tutorial: http://www.hackingtutorials.org/web-application-hacking/scanning-webservers-vulnerabilities-with-nikto
Enum4linux Tutorial: https://labs.portcullis.co.uk/tools/enum4linux/
Sparta Official Website: http://sparta.secforce.com/

Module	Book Pages	Cybrary Video	Time
Traffic Capture	155-160	Module 6 – Traffic Capture	2 Hours

Details

I only included a tiny portion of Georgia's videos and book to keep it applicable to the OSCP specifically. There are really two ways that you can use packet captures to your advantage. Firstly, you can attack by sniffing for passwords as an example. Secondly, it can be used to troubleshoot your attacks. The latter is very important, and if you can't use Wireshark and TCPDump, then you're going to be met with "Try Harder". Note: ARP poisoning is not part of the PWK course.

Additional Resources

Wireshark: https://www.cybrary.it/video/traffic-capture-part-2/
Great Tutorial: https://www.youtube.com/watch?v=r0l_54thSYU
TCPDump: https://www.giac.org/paper/gsec/3489/beginners-guide-tcpdump/105700

Module	Book Pages	Cybrary Video	Time
Passwords	197-214	Module 8 – Passwords	2 Hours

Details

Georgia does a good job of explaining the concepts and tools at a high level. I would recommend that you become familiar with where Windows and Linux stores its user passwords. You can go much deeper into this field, but I urge you to keep it basic at this stage. Remember that this is a prep course, not the actual course itself.

Additional Resources

Password attacks: https://www.cybrary.it/video/passwords-part-1/
Online password cracking: https://www.cybrary.it/video/passwords-part-2/
Offline password cracking: https://www.cybrary.it/video/passwords-part-3/
CeWL: https://www.youtube.com/watch?v=7cz9OyhFFps
SAM Database:
http://www.computersecuritystudent.com/SECURITY_TOOLS/PASSWORD_CRACKING/lesson2/
Passwd and Shadow file: http://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/

Module	Book Pages	Cybrary Video	Time
Exploitation 1	179-196	Module 7 - Exploitation	4 Hours

Details

So this module is really what you have been waiting for. Everything that you see in the videos and the book you should be doing in your labs. Make sure you got snapshots of your VM's in case the exploits break them. I would also recommend that you spend a bit of time on exploit-db. When going through the material, instead of just focusing on the step by step methods, consider the type of thinking that goes into each process. A huge part of successfully passing the OSCP exam relies on your ability to think "How does this work and how can I use it in ways that it was not intended for"

Additional Resources

Direct Exploitation: https://www.cybrary.it/video/exploitation-part-1/
Directory Traversal: https://www.cybrary.it/video/exploitation-part-3/
Open Source Vulnerability: https://www.cybrary.it/video/exploitation-part-4/
Backdoor FTP: https://www.cybrary.it/video/exploitation-part-5/
Attaching to an IP: https://www.cybrary.it/video/exploitation-part-6/

Module	Book Pages	Cybrary Video	Time
Exploitation 2	277-287 309-311	Module 10 – Post Exploitation	4 Hours

Details

Exploit Development was one of the PWK modules that was the most challenging for me initially (because I don't work with debuggers on a day to day basis), but it has turned into something which I deeply enjoy. It can be quite overwhelming at first, but the good news is that Georgia's book does a great job of explaining the concepts that you need to know. Her Cybrary videos on the subject are good, but I did not include it here because the PWK course itself are phenomenal.

Additional Resources

File Transfer without Interactive Shell: https://www.cybrary.it/video/post-exploitation-part-1/
Exploit Development: https://www.cybrary.it/video/post-exploitation-part-2/
Basic Exploit Development: http://www.securitysift.com/windows-exploit-development-part-1-basics/

Before continuing, go back to the Metasploit module at the beginning of the course for a review.

Module	Book Pages	Cybrary Video	Time
Client Side Attacks	215-240 257-274	Module 9 – Advanced Exploitation	3 Hours

Details

You will be surprised to learn that client side attacks are very relevant to the PWK labs. You can go ahead and skip the social engineering chapter and videos for obvious reasons. Also make sure you get to know the sections on how to deal with Antivirus Software.

Additional Resources

Introduction: https://www.cybrary.it/video/advanced-exploitation-part-1/
Client Side Attacks: https://www.cybrary.it/video/advanced-exploitation-part-2/
Exploiting Java: https://www.cybrary.it/video/advanced-exploitation-part-3/
Bypassing Antivirus Software: https://www.cybrary.it/video/advanced-exploitation-part-5/

Module	Book Pages	Cybrary Video	Time
Web Applications	215-240	Module 11 – WebApps	4 Hours

Details

After this module, I would recommend going back to the enumeration phase and looking closer at the output of Nikto and making sure that you understand the information that it’s providing you. It’s a huge field, so remember that this is merely to prep you for the PWK.

Additional Resources

Vulnerable Web Applications: https://www.cybrary.it/video/webapp-part-2/
SQL Commands: https://www.cybrary.it/video/exploitation-part-2/
SQL Injection: https://www.cybrary.it/video/webapp-part-3/
RFI/LFI: https://www.cybrary.it/video/webapp-part-4/
XSS: https://www.cybrary.it/video/webapp-part-5/
HTTP Methods: https://www.sans.org/reading-room/whitepapers/testing/penetration-testing-web-application-dangerous-http-methods-33945