OSCP Preparation

Amien Harisen – Professional Bungkus Tolak Angin Anak. / Kuah Indomie Goreng

What is OSCP

- Offensive Security Certified Professional (OSCP) is a certification program that focuses on hands-on offensive information security skills. It consists of two parts: a nearly 24-hour pen testing exam, and a documentation report due 24 hours after it. OSCP is a very hands-on exam.
- It more about building the mindset of the security professional
- Teach you how to WRITE a professional and standardize report

ATTENTION !

- OSCP is difficult – have no doubts about that! There is no spoon-feeding here. Refer to all the above references and do your own research on topics like service enumeration, penetration testing approaches, post exploitation, privilege escalation, etc. Remember, always take notes as text with a separate note.
- Knowledge and expert skills don't come immediately to anyone. They must be worked upon. But first you need to get started! So, if you are anywhere near the idea of attempting the OSCP, just enroll and get started. Once you are good with all the above pre-enrolling, you are fully ready to enrol for the OSCP.
  - The main thing in OSCP is the lab.
  - **OSCP is not about clearing the exam. It's all about working deeply on labs.**
  - In General,***It's not about the destination. It's all about the journey.***

PRE OSCP Preparation

- Kali Linux Revelaed 1st Edition (PDF Available) - https://www.kali.org/download-kali-linux-revealed-book/
- Tulpa PWK Guide (PDF Available) - https://tulpa-security.com/2016/09/19/prep-guide-for-offsecs-pwk/
- Hacker Playbook 2nd Edition - PDF
- Red Team Field Manual (RTFM) – PDF
- Web Application Hacker Handbook – PDF
- Shellcoders Hacker Handbook - PDF

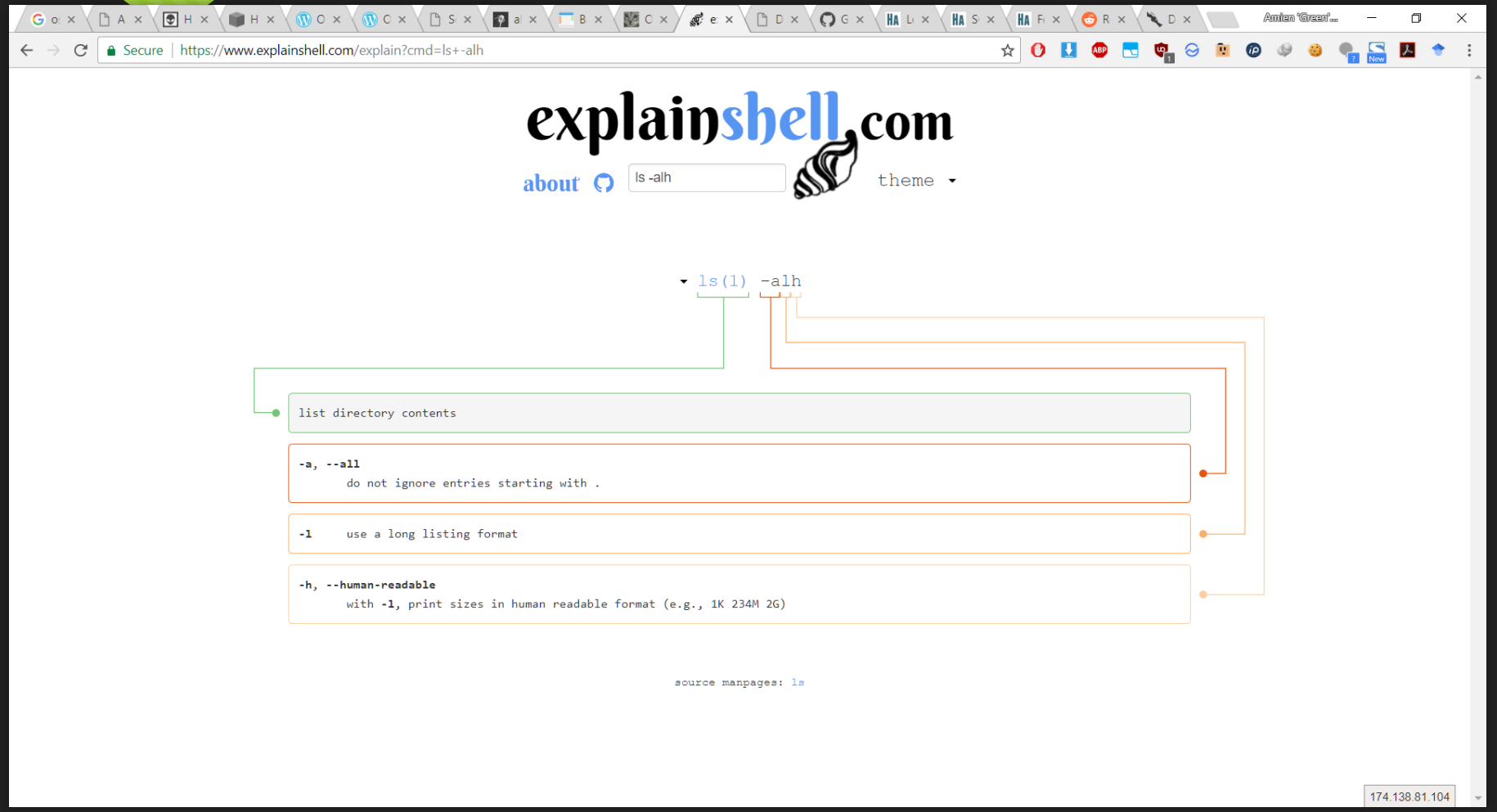
PRE OSCP Preparation

- https://pinboard.in/u:unfo/t:oscp
- http://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob.html
- https://www.youtube.com/playlist?list=PLyPJ3SHNkjIFITR-Lzsc0XSOBS7JUXsOy – VLOG About
- https://www.hacksplaining.com/ - Interactive Hacking and Learning Simulation

Bash Guide

- http://www.tldp.org/LDP/Bash-Beginners-Guide/html/
- http://overthewire.org/wargames/bandit/
- https://www.explainshell.com

Explain Shell



BASIC TOOLS

- Basic tools:
- You will use these tools a lot. Make sure you understand what they do and how you can utilize them.
  - Netcat: Most important tool in the entire course. Understand what it does, what options you have, difference between a reverse shell and a bind shell. Experiment a lot with it. (http://minhhh.github.io/posts/a-netcat-cheatsheet)
  - Ncat: Netcat's mature brother, supports SSL. Part of Nmap.
  - Wireshark: Network analysis tool, play with it while browsing the internet, connecting to FTP, read/write PCAP files.
  - TCPdump: Not all machines have that cute GUI, you could be stuck with a terminal.

INFOGATH & ENUMERATION

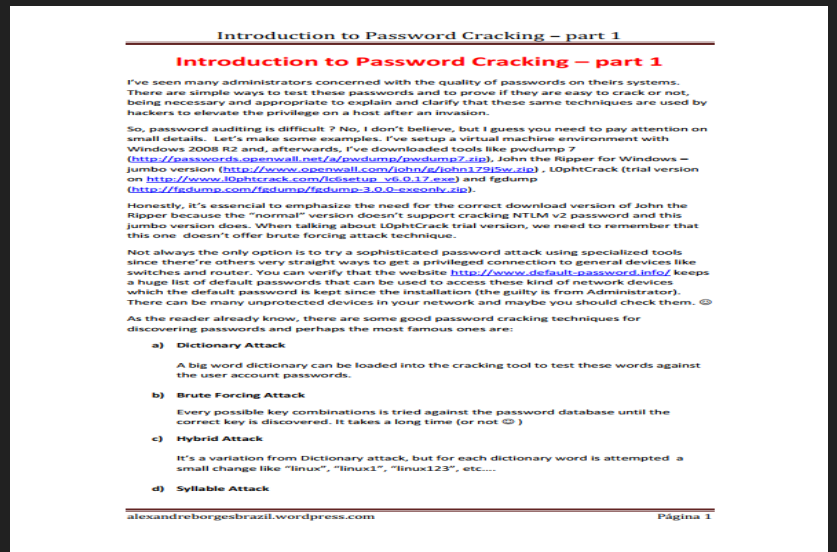
- Read about the following tools/techniques, experiment as much as possible.
  - Google dorks
  - Whois
  - Netcraft
  - Recon-ng: Make sure you check the Usage guide to know how it works.
  - Dmitry
  - theharvester

INFOGATH & ENUMERATION

- Understand what DNS is, how it works, how to perform forward and reverse lookup, what zone transfers are and how to perform them. Great resource here.
  - https://digi.ninja/projects/zonetransferme.php
- Nmap: One of the most used tools during the course (if not the most). I'd recommend to start by reading the man pages, understand different scanning techniques and other capabilities it has (scripts, OS detection, Service detection, …)
  - http://resources.infosecinstitute.com/nmap-cheat-sheet/#article
- Services enumeration: SMTP, SNMP, SMB, and a lot others. Don't just enumerate them, understand what they're used for and how they work.
- http://www.0daysecurity.com/penetration-testing/enumeration.html

PASSWORD ATTACK

- Understand the basics of password attacks, difference between online and offline attacks. How to use Hydra, JTR, Medusa, what rainbow tables are, the list goes on.
- https://alexandreborgesbrazil.files.wordpress.com/2013/08/introduction_to_password_cracking_part_1.pdf



Introduction to Password Cracking – part 1

Introduction to Password Cracking – part 1

I've seen many administrators concerned with the quality of passwords on theirs systems. There are simple ways to test these passwords and to prove if they are easy to crack or not, being necessary and appropriate to explain and clarify that these same techniques are used by hackers to elevate the privilege on a host after an invasion.

So, password auditing is difficult ? No, I don't believe, but I guess you need to pay attention on small details. Let's make some examples. I've setup a virtual machine environment with Windows 2008 R2 and, afterwards, I've downloaded tools like pwdump 7 (http://passwords.openwall.net/a/pwdump/pwdump7.zip), John the Ripper for Windows – jumbo version (http://www.openwall.com/john/g/john179j5w.zip) , L0phtCrack (trial version on http://www.l0phtcrack.com/lc6setup_v6.0.17.exe) and fgdump (http://fgdump.com/fgdump/fgdump-3.0.0-exeonly.zip).

Honestly, it's essencial to emphasize the need for the correct download version of John the Ripper because the "normal" version doesn't support cracking NTLM v2 password and this jumbo version does. When talking about L0phtCrack trial version, we need to remember that this one doesn't offer brute forcing attack technique.

Not always the only option is to try a sophisticated password attack using specialized tools since there're others very straight ways to get a privileged connection to general devices like switches and router. You can verify that the website http://www.default-password.info/ keeps a huge list of default passwords that can be used to access these kind of network devices which the default password is kept since the installation (the guilty is from Administrator). There can be many unprotected devices in your network and maybe you should check them.

As the reader already know, there are some good password cracking techniques for discovering passwords and perhaps the most famous ones are:

a) **Dictionary Attack**

A big word dictionary can be loaded into the cracking tool to test these words against the user account passwords.

b) **Brute Forcing Attack**

Every possible key combinations is tried against the password database until the correct key is discovered. It takes a long time (or not)

c) **Hybrid Attack**

It's a variation from Dictionary attack, but for each dictionary word is attempted a small change like "linux", "linux1", "linux123", etc....

d) **Syllable Attack**

alexandreborgesbrazil.wordpress.com Página 1

Metasploit

- https://www.offensive-security.com/metasploit-unleashed/
- http://www.securitytube.net/groups?operation=view&groupId=10

Public Exploit

- https://www.exploit-db.com/
- https://www.cvedetails.com/
- https://packetstormsecurity.com/files/tags/exploit/
- Pasar Malam
- Pasar Hantu

Privilege Escalation

A never ending topic, there are a lot of techniques, ranging from having an admin password to kernel exploits. Great way to practice this is by using Vulnhub VMs for practice.

- Windows:Elevating privileges by exploiting weak folder permissions
  - http://www.greyhathacker.net/?p=738
- Windows: Privilege Escalation Fundamentals
  - http://www.fuzzysecurity.com/tutorials/16.html
- Windows: Windows-Exploit-Suggester
  - https://github.com/GDSSecurity/Windows-Exploit-Suggester
- Windows: Privilege Escalation Commands
  - http://pwnwiki.io/#!privesc/windows/index.md
- Linux: Basic Linux Privilege Escalation
  - https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- Linux: linuxprivchecker.py
  - http://www.securitysift.com/download/linuxprivchecker.py
- Linux: LinEnum
  - https://github.com/rebootuser/LinEnum
- Practical Windows Privilege Escalation
  - https://www.youtube.com/watch?v=PC_iMqiuIRQ
- MySQL Root to System Root with UDF
  - https://www.adampalmer.me/iodigitalsec/2013/08/13/mysql-root-to-system-root-with-udf-for-windows-and-linux/

Post Exploitation

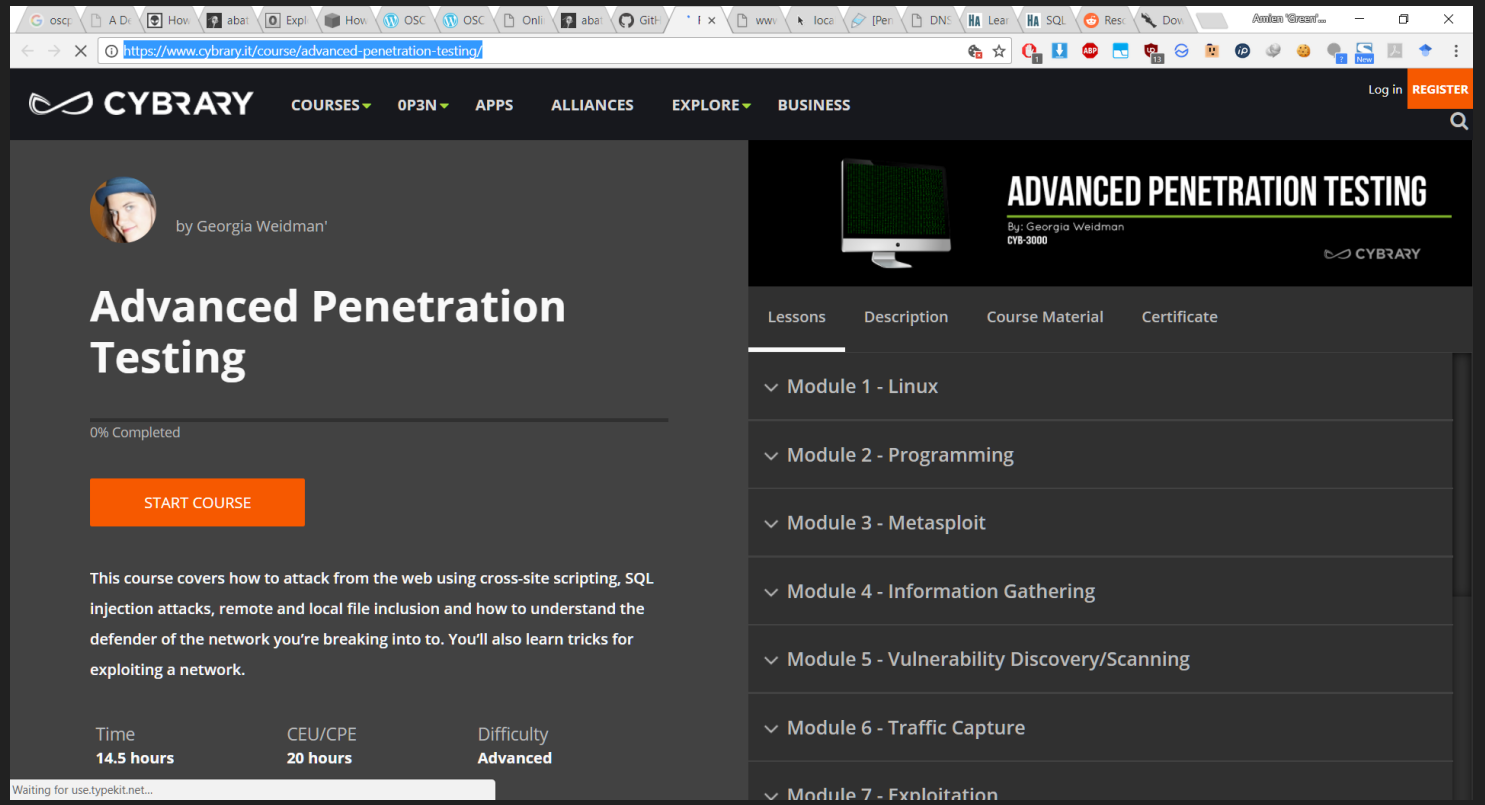
- https://tipstrickshack.blogspot.co.id/2013/08/post-exploitation-using-nishang.html
- Powershell for Penetration Tester (Blackhat PDF Available)
- PowerSploit https://github.com/PowerShellMafia/PowerSploit
- mimikatz - Credentials extraction tool for Windows operating system
- Bloodhound - Graphical Active Directory trust relationship explorer.
- Empire - Pure PowerShell post-exploitation agent.
- DeathStar - Python script that uses Empire's RESTful API to automate gaining Domain Admin rights in Active Directory environments.

Got Shell? PIVOT !

- This tutorial is about “moving” through a network (from machine to machine). We use a compromised host as our pivot to move through the network.
- https://www.cybrary.it/0p3n/pivot-network-port-forwardingredirection-hands-look/
- https://artkond.com/2017/03/23/pivoting-guide/
- https://pen-testing.sans.org/blog/2012/04/26/got-meterpreter-pivot
- https://highon.coffee/blog/ssh-meterpreter-pivoting-techniques/

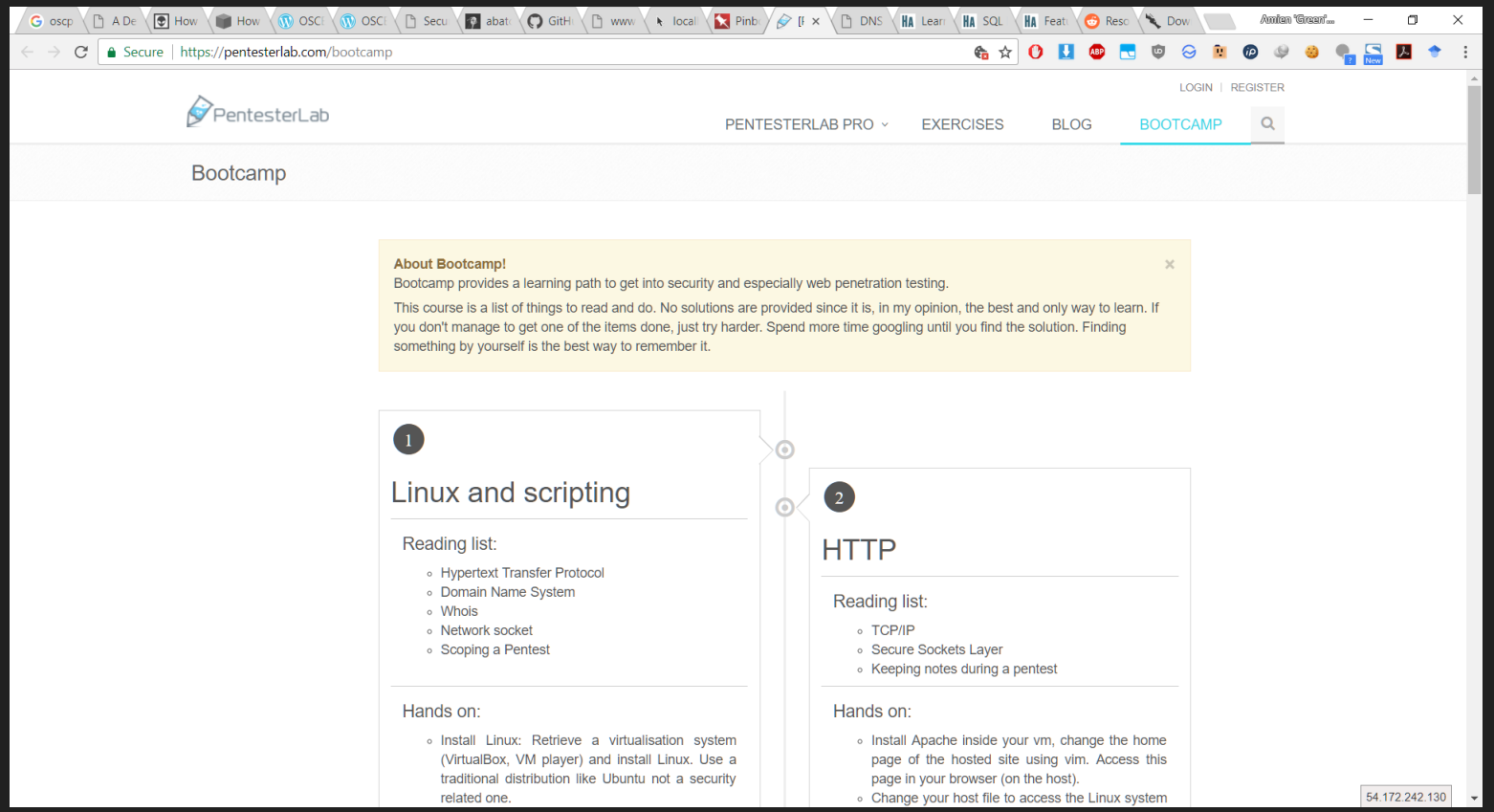
Start Small

- https://www.cybrary.it/course/advanced-penetration-testing/



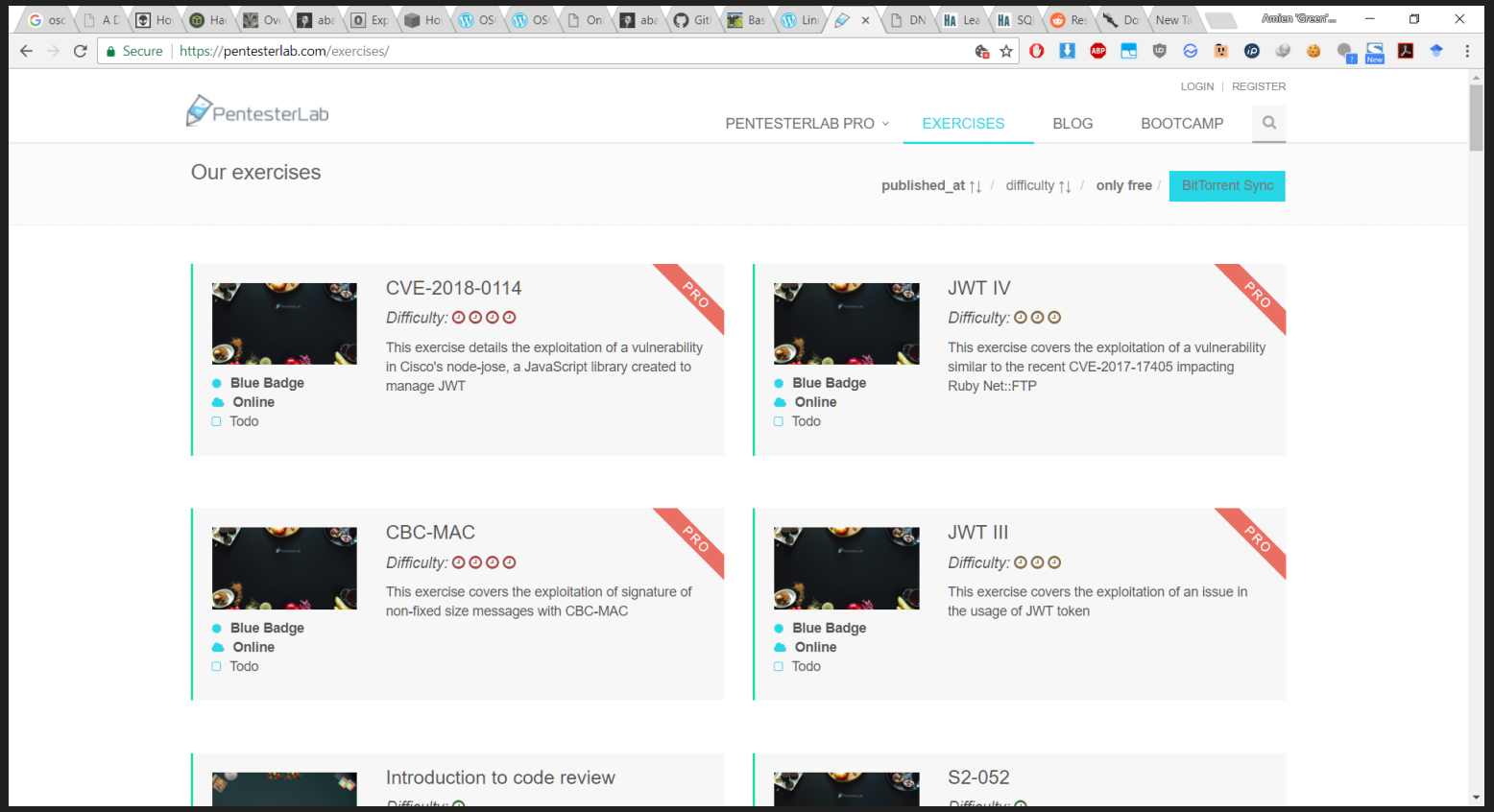
Start Small

- https://pentesterlab.com/bootcamp



Start Small

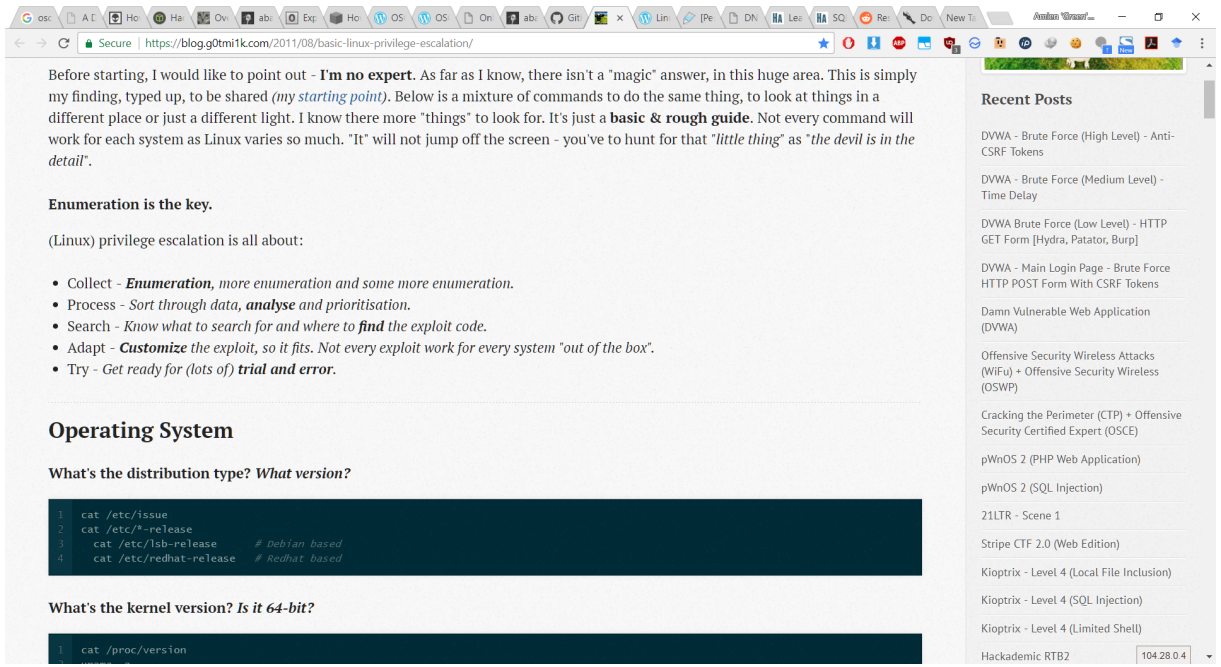
- https://pentesterlab.com/exercises/



Basic Exploitation

Basic Exploitation

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/



Before starting, I would like to point out - **I'm no expert**. As far as I know, there isn't a "magic" answer, in this huge area. This is simply my finding, typed up, to be shared *(my starting point)*. Below is a mixture of commands to do the same thing, to look at things in a different place or just a different light. I know there more "things" to look for. It's just a **basic & rough guide**. Not every command will work for each system as Linux varies so much. "It" will not jump off the screen - you've to hunt for that "*little thing*" as "*the devil is in the detail*".

Enumeration is the key.

(Linux) privilege escalation is all about:

- Collect - ***Enumeration***, *more enumeration and some more enumeration.*
- Process - *Sort through data,* ***analyse*** *and prioritisation.*
- Search - *Know what to search for and where to* ***find*** *the exploit code.*
- Adapt - ***Customize*** *the exploit, so it fits. Not every exploit work for every system "out of the box".*
- Try - *Get ready for (lots of)* ***trial and error****.*

Operating System

What's the distribution type? ***What version?***

```
cat /etc/issue
cat /etc/*-release
  cat /etc/lsb-release      # Debian based
  cat /etc/redhat-release   # Redhat based
```

What's the kernel version? ***Is it 64-bit?***

```
cat /proc/version
```

Recent Posts

DVWA - Brute Force (High Level) - Anti-CSRF Tokens

DVWA - Brute Force (Medium Level) - Time Delay

DVWA Brute Force (Low Level) - HTTP GET Form [Hydra, Patator, Burp]

DVWA - Main Login Page - Brute Force HTTP POST Form With CSRF Tokens

Damn Vulnerable Web Application (DVWA)

Offensive Security Wireless Attacks (WiFu) + Offensive Security Wireless (OSWP)

Cracking the Perimeter (CTP) + Offensive Security Certified Expert (OSCE)

pWnOS 2 (PHP Web Application)

pWnOS 2 (SQL Injection)

21LTR - Scene 1

Stripe CTF 2.0 (Web Edition)

Kioptrix - Level 4 (Local File Inclusion)

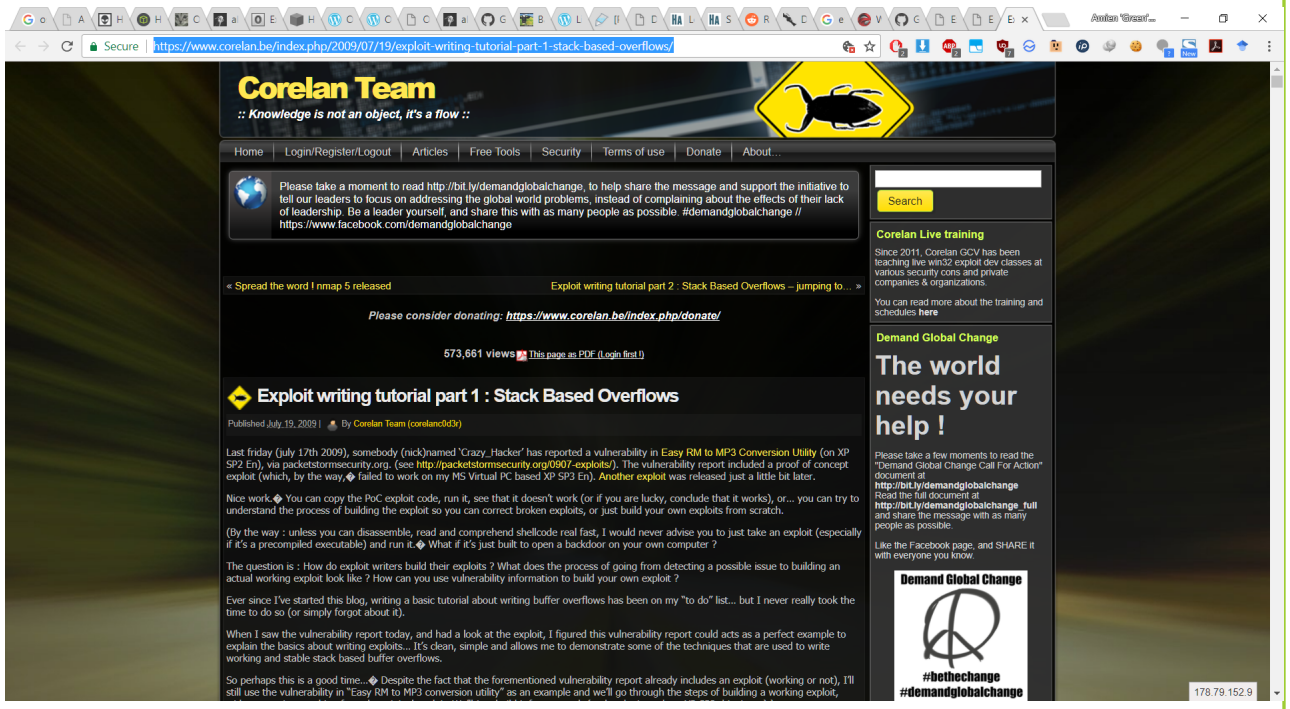
Kioptrix - Level 4 (SQL Injection)

Kioptrix - Level 4 (Limited Shell)

Hackademic RTB2

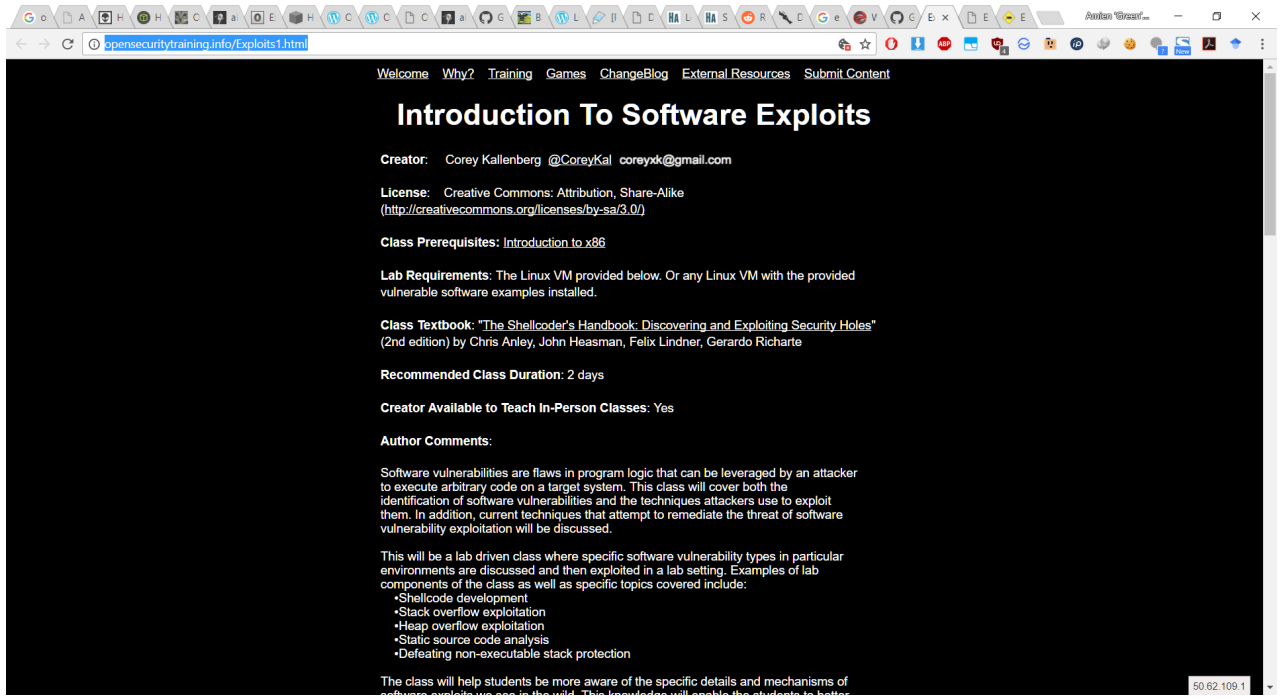
Basic Exploitation

https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/



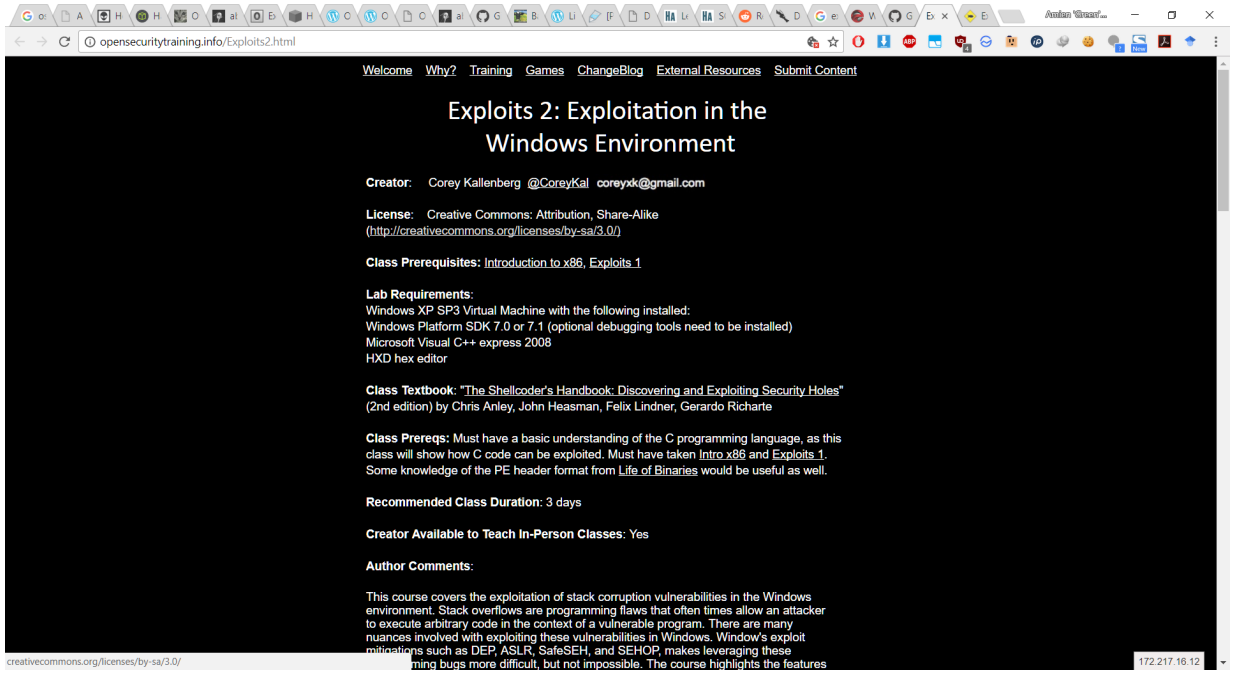
Basic Exploitation

http://opensecuritytraining.info/Exploits1.html



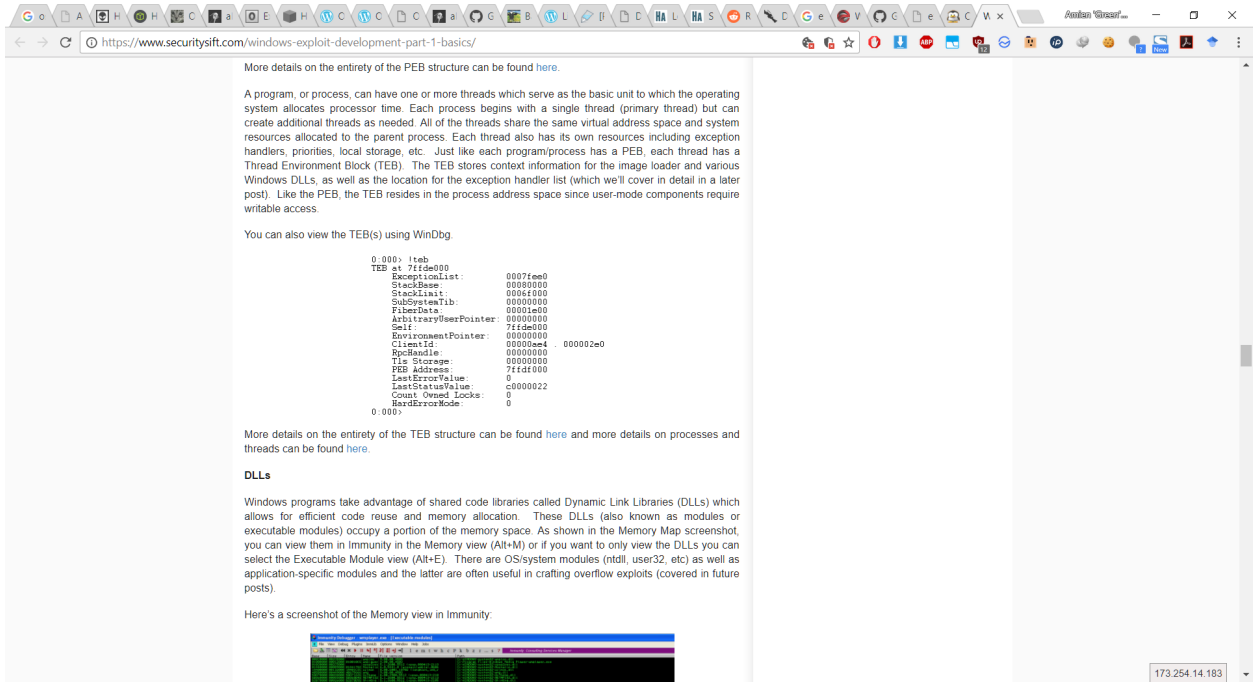
Basic Exploitation

http://opensecuritytraining.info/Exploits2.html



Basic Exploitation

https://www.securitysift.com/windows-exploit-development-part-1-basics/



https://www.securitysift.com/windows-exploit-development-part-1-basics/

More details on the entirety of the PEB structure can be found here.

A program, or process, can have one or more threads which serve as the basic unit to which the operating system allocates processor time. Each process begins with a single thread (primary thread) but can create additional threads as needed. All of the threads share the same virtual address space and system resources allocated to the parent process. Each thread also has its own resources including exception handlers, priorities, local storage, etc. Just like each program/process has a PEB, each thread has a Thread Environment Block (TEB). The TEB stores context information for the image loader and various Windows DLLs, as well as the location for the exception handler list (which we'll cover in detail in a later post). Like the PEB, the TEB resides in the process address space since user-mode components require writable access.

You can also view the TEB(s) using WinDbg.

```
0:000> !teb
TEB at 7ffde000
    ExceptionList:          0007fee0
    StackBase:              00080000
    StackLimit:             0006f000
    SubSystemTib:           00000000
    FiberData:              00001e00
    ArbitraryUserPointer:   00000000
    Self:                   7ffde000
    EnvironmentPointer:     00000000
    ClientId:               00000ae4 . 000002e0
    RpcHandle:              00000000
    Tls Storage:            00000000
    PEB Address:            7ffdf000
    LastErrorValue:         0
    LastStatusValue:        c0000022
    Count Owned Locks:      0
    HardErrorMode:          0
0:000>
```

More details on the entirety of the TEB structure can be found here and more details on processes and threads can be found here.

DLLs

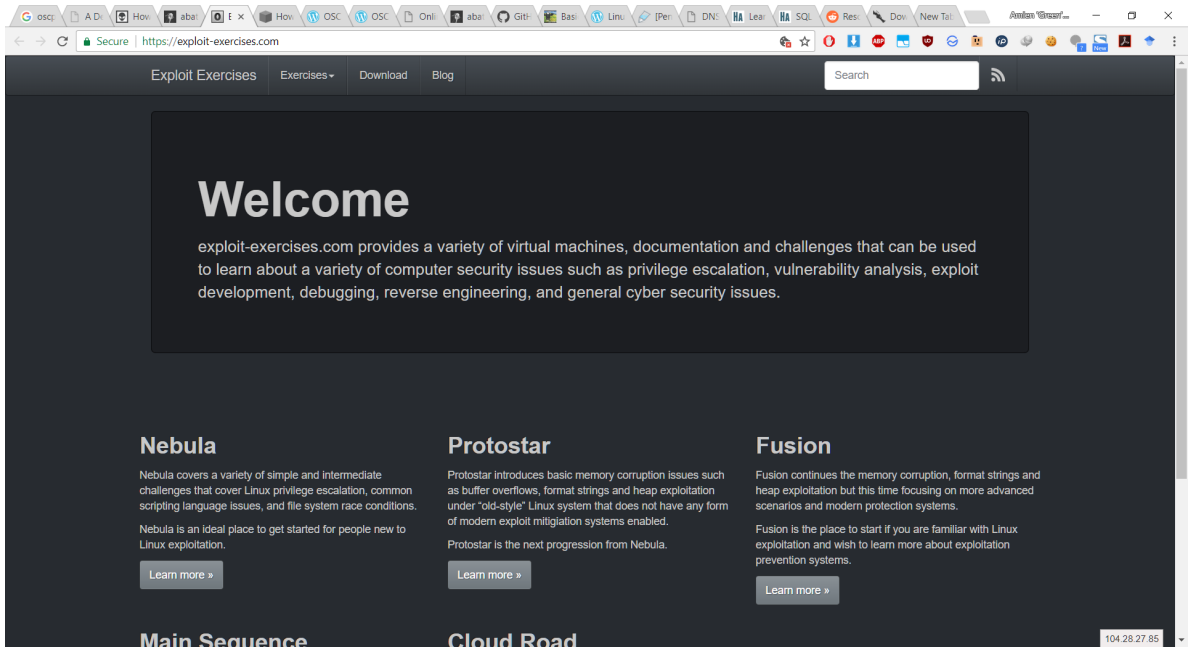
Windows programs take advantage of shared code libraries called Dynamic Link Libraries (DLLs) which allows for efficient code reuse and memory allocation. These DLLs (also known as modules or executable modules) occupy a portion of the memory space. As shown in the Memory Map screenshot, you can view them in Immunity in the Memory view (Alt+M) or if you want to only view the DLLs you can select the Executable Module view (Alt+E). There are OS/system modules (ntdll, user32, etc) as well as application-specific modules and the latter are often useful in crafting overflow exploits (covered in future posts).

Here's a screenshot of the Memory view in Immunity:

173.254.14.183

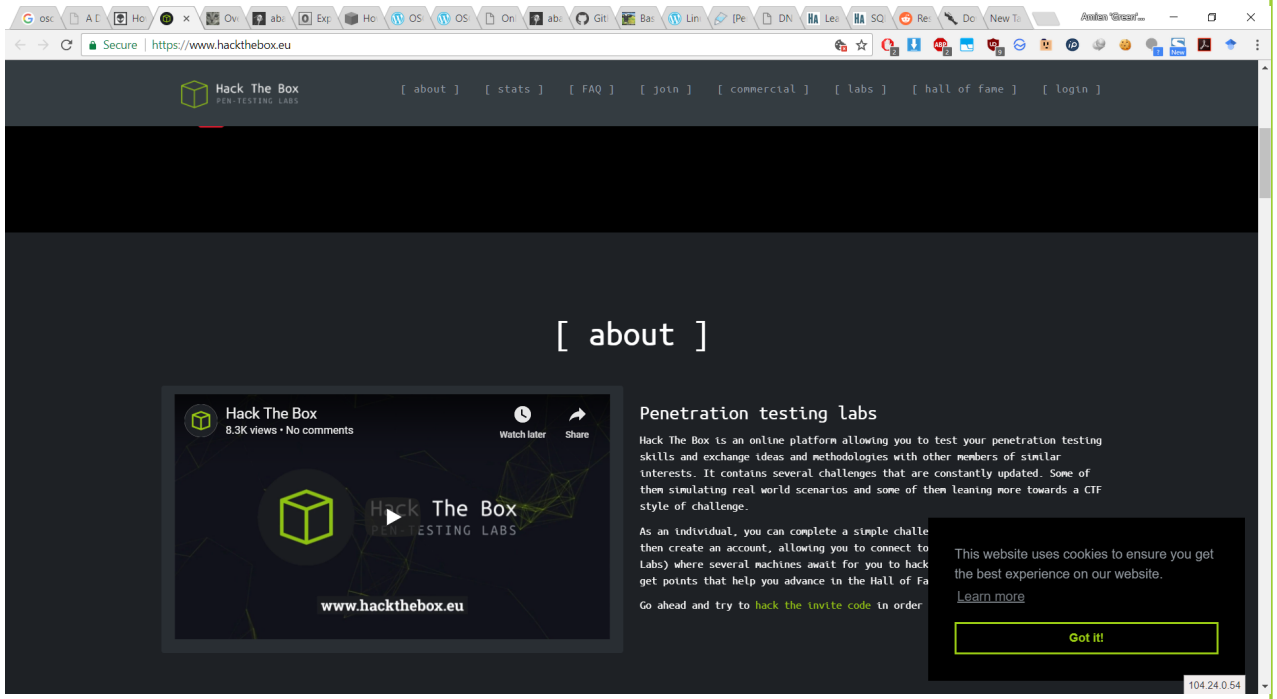
Exploit Exercise

https://exploit-exercises.com/



Exploit Exercise

https://www.hackthebox.eu/



OSCP Like VMS

- Beginner friendly
  - Kioptrix: Level 1 (#1)
  - Kioptrix: Level 1.1 (#2)
  - Kioptrix: Level 1.2 (#3)
  - Kioptrix: Level 1.3 (#4)
  - FristiLeaks: 1.3
  - Stapler: 1
  - PwnLab: init

  http://www.abatchy.com/2017/02/oscp-like-vulnhub-vms

OSCP Like VMS

- Intermediate
  - Kioptrix: 2014
  - Brainpan: 1
  - Mr-Robot: 1
  - HackLAB: Vulnix

  http://www.abatchy.com/2017/02/oscp-like-vulnhub-vms

OSCP Like VMS

- Not so sure
  - VulnOS: 2
  - SickOs: 1.2
  - /dev/random: scream
  - pWnOS: 2.0
  - SkyTower: 1
  - IMF

  http://www.abatchy.com/2017/02/oscp-like-vulnhub-vms

OSCP Like VMS

- Windows
- There aren't many Windows machines around due to licensing. Few options:
  - Hack The Box: Got a nice set of Windows machines from Windows 2000 up to Windows 8.1 I believe.
  - Metasploitable 3, will download a trial version of Windows Server.
  - https://github.com/magnetikonline/linuxmicrosoftievirtualmachines you can download Windows VMs legally then hack your way through them through an unpatched vulnerability or setting up a vulnerable software.
  - Set up your own lab. Default Windows XP SP0 will give you the chance to try out a few remote exploits, or doing some privilege escalation using weak services.
  - /dev/random: Sleepy (Uses VulnInjector, need to provide you own ISO and key.)
  - Bobby: 1 (Uses VulnInjector, need to provide you own ISO and key.)

http://www.abatchy.com/2017/02/oscp-like-vulnhub-vms

Enroling the Class

Welcome to OSCP

- You will get your training materials (in PDF), video materials, and lab connectivity pack via email. The link for the pdf and video will expire in 2 days. You should download and back it up before that. Check your lab connectivity as mentioned in the lab connectivity guide. Don't start diving into labs immediately. Follow the below given steps once you receive the email.
- Go through the video material
- Go through the pdf completely
- Do the exercises in pdf and document it.
- Mostly people only go through the video and then start labs. But that is the biggest mistake. The PDF has a lot more than what is mentioned in the videos. Do not feel bored when going through all the material and doing the exercises.
- The exercises in the PDF help in sharpening one's axe. I found some useful tips and tricks whenever I used to get stuck in the lab exercises.
- What's more, you will get an additional 5 points for submitting exercise documentation.

Hacking Phase

- Now is the main part of OSCP. The labs. The lab environment consists of 55 machines each with a different approach and different difficulty level. The lab infra has 4 networks. Public, IT, Development, and Admin network. You will get direct access only to the public network. You need to unlock other networks by the secret keys obtained by proper post exploitation. You will be connected to other networks by port forwarding and proxy chaining. A lab is the place where you try out all your research ideas and various tools.
- Before starting the lab machines, go through the buffer overflow exploitation in the video material 2-3 times and practice the same on your dedicated Windows 7 machine provided along with the lab machines. Same tools explained in the material will be there on your Windows 7 machine. Practice buffer overflow by following the same steps used by the instructor.

Hacking Phase

- Exploiting a machine is a Systematic Process:
  - Find the open ports and services running on ports
  - Enumerate the services and the machine
  - Exploit the correct vulnerability and gain access
  - Do proper post exploitation enumeration
  - Privilege Escalation
- For some machines, you will get direct admin/root/system access at the initial stage itself. But still, you need to do proper post exploitation enumeration on that machine. This is because in the labs the information gathered on post exploitation on one machine will be used to solve another one.
- There are 4 main difficult machines in the OSCP lab called as pain, sufferance, humble and gh0st. its nature is as per the name. I gained a lot of confidence after solving these machines.

Hacking Phase

- You need to give your maximum dedication in the labs. Do the research, lots and lots of research. Try all kind of possibilities, try stupid things. Google is your friend. Always use Google at any point and at every machine. Google everything that is in front of you. You will experience lots and lots of pain, frustration, etc. Many times you may lose your patience. But **NEVER GIVE UP!**
- Try Harder. If you get stuck and you don't know how to proceed, you can visit offsec student forums
  - https://forums.offensive-security.com/
  - Log into you OS ID and navigate to lab machine discussion. You will find some useful hints.
- Also, you can join a slack team https://netsecfocus.slack.com and request them to add you to the OSCP channel. You can get some useful ideas here.

Hacking Phase

- But nowhere no one will give you a direct solution for any of the lab machines. You will only get a small hint and some suggestions. You must figure out the solution by yourself.
- Remember, the enumeration is the key for OSCP. It took me 2 months to know the exact meaning of enumeration. Never get excited to exploit any machine at first. Do not follow the approach of monkey testing and blindly downloading and running the exploits. Trust me, this approach will make you fall into a rabbit hole. There will be some decoy vulnerabilities to trick you in the wrong direction.

What is the Approach

- Only with proper enumeration, you can successfully exploit any target.
- 1. Do a full port scan on the target.
  - Refer fyodor's defcon video on "nmap: scanning the internet" **https://www.youtube.com/watch?v=Hk-21p2m8YY**
- 2. Enumerate every port. Find what service is running. If you are unaware, simply google the port. Also refer to the below article.
  - **http://www.0daysecurity.com/penetration-testing/enumeration.html**
- 3. After understanding the target, now try to find vulnerabilities. Some target might be exploitable with more than 1 way

What is the Approach

- If you find a vulnerability, read about that vulnerability. Many of the exploits will not work without modification. So, learn the vulnerability and read the exploit carefully. Sometimes, there will be another manual way of exploiting the vulnerabilities instead of using public exploits. So, google a lot. Pages not listed under top will also have some useful stuffs. Refer all pages.
- In some cases, the machine might be busy since other students will also be working. So, revert the machine and try again. Look for the attacks on the vulnerability online. There will be many blogs written on how to exploit that vulnerability.

What is the Approach

- Once you gain access to the system, always upgrade your shell. Enumerate well. Search for misconfigurations, credentials, try to use the credentials at whichever place possible.
- It is not required to solve all the machines to take the exam. It's for enhancing your pentest skills. I'd recommend getting at least 25+ targets and 2 of the four difficult ones. If you can't solve these many target machines then you probably need to extend the labs and start working on it.
- Document all your lab works and take notes of everything that you learned. Submitting the lab report will give you an additional 5 points.

THE EXAM

Exam Best Practice

- Once you are confident enough after working in the labs, you can take the exam. Make sure you schedule your exam date at least 1 month in advance.
- In the exam, you will be given 5 machines. You have 23.45 hours to crack all the given machines. Each machine carries marks. You require minimum of 70 marks to pass the exam in the given period. You will be given additional 1 day for preparing the report.
- You need proper sleep, food, and regular breaks during the exam. Because your brain needs to function 2-3 times more creatively and spontaneously than usual.
- Grab all your notes, lab notes and make a revision before starting.

Exam Best Practice

- Metasploit usage is restricted in the exam. You should use it only once. So, use it wisely.
- Start with the exploit writing (Buffer Overflow) machine. It holds one of the maximum marks. If you have proper practice on this before the lab, you can finish this within maximum 2 hours.
- Next, focus on the machine which has minimum marks. You require some proper enumeration here.
- The real exam starts with the remaining 3 machines. Never lose your patience and stay calm. Enumerate, enumerate, and enumerate. Never leave anything. Try all stupid things. Do not panic. Assume like you are working in the lab.

Exam Best Practice

- After completing the exam, you will be given 1 day to prepare the report and send them. There will be a report template in the reporting guide. You can use your own report as well. Read the offsec reporting guide carefully before starting the report and send them in the exact format and the way they are mentioned.

Tips for EXAM

- Be confident
- Be very cool and calm
- Never bother if you didn't get access to one or two machines in short time as mentioned in other blogs
- Enumerate well
- Take regular breaks. Go for a small walk and get some fresh air.
- Take screenshots and POCs immediately after each exploitation steps.
- Submit the flags (local.txt & proof.txt) in the exam panel immediately once you retrieve them
- I have seen many people failing in the exam once they lose their patience. So never get tensed. Always be calm and relaxed. TRY HARDER!

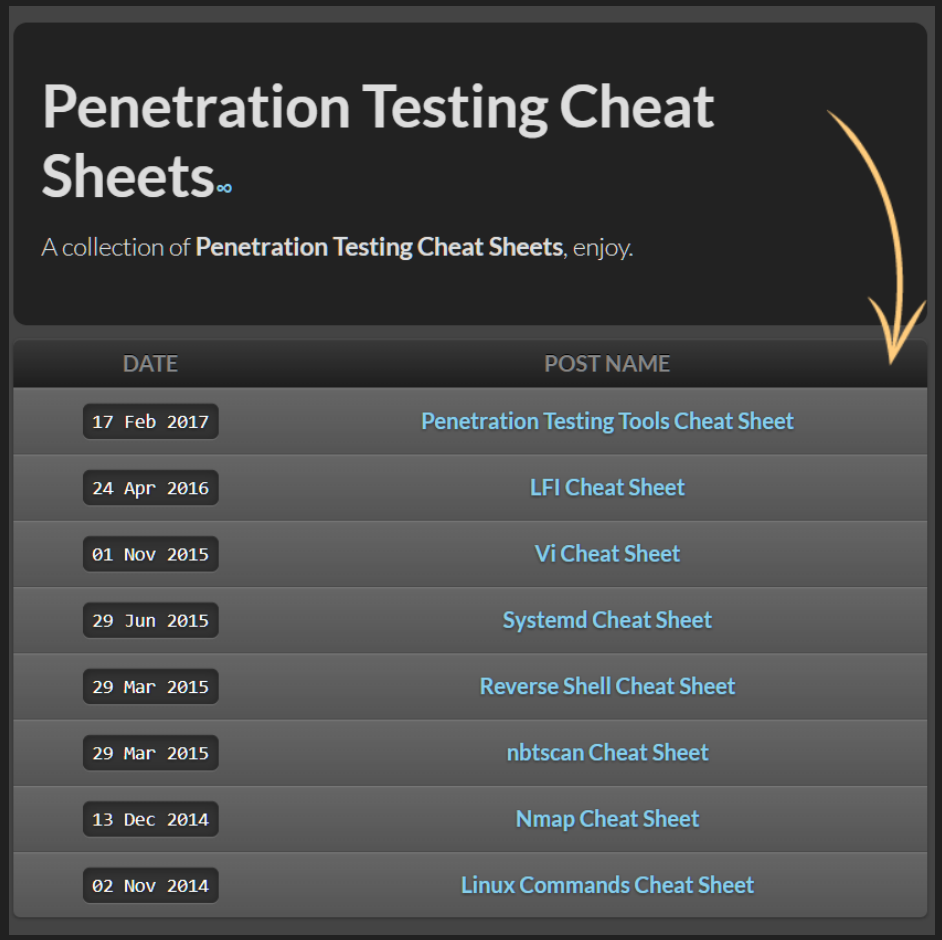
CONCLUSION

- OSCP is not just a certification. It is an awesome journey which teaches you many things apart from technical perspective. It will teach you to think creatively, develop a ton of patience and most of all you will 'NEVER GIVE UP'.
- So never see this as a certification and don't target only on clearing the exam and getting certification. Work on labs. Try to pwn as many machines as you can. Again, TRY HAAAAARDER.
- http://niiconsulting.com/checkmate/2017/06/a-detail-guide-on-oscp-preparation-from-newbie-to-oscp/

WAIT THERE'S MORE !!

LIST OF ALL CHEAT SHEET

- https://highon.coffee/blog/cheat-sheet/



Penetration Testing Cheat Sheets∞

A collection of **Penetration Testing Cheat Sheets**, enjoy.

DATE	POST NAME
17 Feb 2017	Penetration Testing Tools Cheat Sheet
24 Apr 2016	LFI Cheat Sheet
01 Nov 2015	Vi Cheat Sheet
29 Jun 2015	Systemd Cheat Sheet
29 Mar 2015	Reverse Shell Cheat Sheet
29 Mar 2015	nbtscan Cheat Sheet
13 Dec 2014	Nmap Cheat Sheet
02 Nov 2014	Linux Commands Cheat Sheet

LIST OF ALL CHEAT SHEET

- https://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
- https://highon.coffee/blog/nmap-cheat-sheet/
- http://www.cheat-sheets.org/saved-copy/Notepad++_Cheat_Sheet.pdf
- http://www.isical.ac.in/~pdslab/2016/lectures/bash_cheat_sheet.pdf
- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
- https://www.sans.org/security-resources/GoogleCheatSheet.pdf
- https://www.tunnelsup.com/python-cheat-sheet/
- https://www.tunnelsup.com/metasploit-cheat-sheet/

SOURCE

- https://github.com/enaqx/awesome-pentest
- https://github.com/burntmybagel/OSCP-Prep
- https://github.com/FabioBaroni/awesome-exploit-development