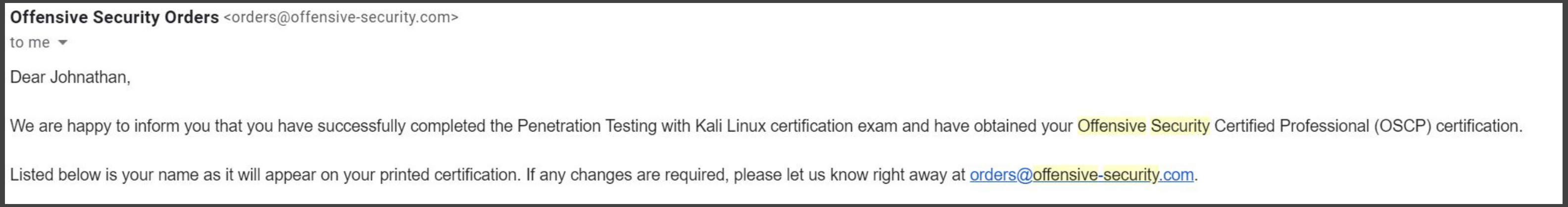
Try Harder? Keep Trying!
Demystifing OSCP/OSCE

Johnathan Miranda

@niden

$ whoami

- Active Duty Air Force - Cyber Warfare Operator
- Part Time Bug Hunter
- Avid CTFer
- Chicken Wrangler
- Fan of Offensive Security Certs
  - OSCP & OSCE
  - AWE/OSEE Virtual?!!?! Maybe!?!

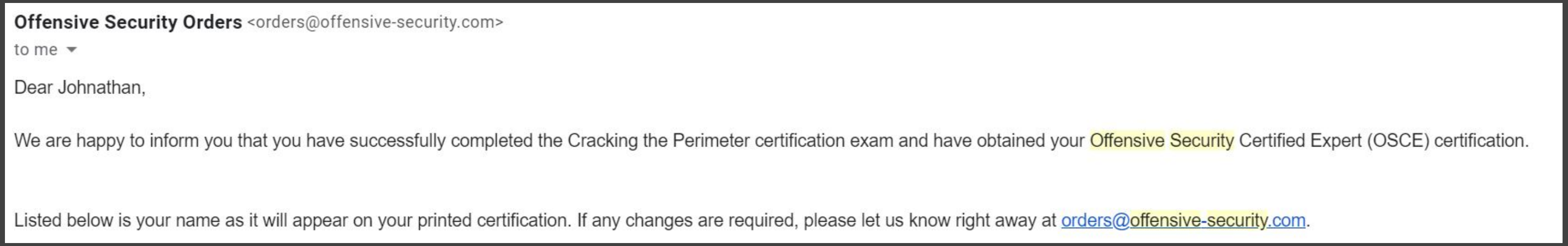


Offensive Security Orders <orders@offensive-security.com>
to me

Dear Johnathan,

We are happy to inform you that you have successfully completed the Penetration Testing with Kali Linux certification exam and have obtained your Offensive Security Certified Professional (OSCP) certification.

Listed below is your name as it will appear on your printed certification. If any changes are required, please let us know right away at orders@offensive-security.com.



Offensive Security Orders <orders@offensive-security.com>
to me

Dear Johnathan,

We are happy to inform you that you have successfully completed the Cracking the Perimeter certification exam and have obtained your Offensive Security Certified Expert (OSCE) certification.

Listed below is your name as it will appear on your printed certification. If any changes are required, please let us know right away at orders@offensive-security.com.

OUTLINE

- Quick Overview on OffSec Certifications
- Try Harder?
- OSCP Preparations
- OSCP Resources
- Testing Strategies
- OSCE Preparations
- OSCE Resources
- Testing Strategies
- Issues with CTP/OSCE (opinion)
- Closing

Quick Overview

- Offensive Security is the “Industry-Leading Online Penetration Testing Training and Certification for Information Security Professionals”

- Offensive Security currently offers six certifications
  - KLCP - Kali Linux Certified Professional
  - OSCP - Offensive Security Certified Professional
  - OSWP - Offensive Security Wireless Professional
  - OSCE - Offensive Security Certified Expert
  - OSWE - Offensive Security Web Expert
  - OSEE - Offensive Security Exploitation Expert

- We’re going to focus on <u>OSCP & OSCE</u> today

Try Harder?

- Anybody has has heard of an Offensive Security has probably heard about their “Try Harder” philosophy.
- Harsh? Maybe? Perseverance is going to carry you a long way with these types of practical certifications.

OSCP Preparation

- This is a really important part and often overlooked.
- If you are not familiar with a linux command line, start there.
- Even the most basic familiarization of common pentesting tools will be helpful here.
- Not a requirement, but it can never hurt to begin getting yourself comfortable with any scripting language that interests you.
- Read Reviews!
- Once you get and have reviewed the course material, make sure you spend the majority of your time in the lab enviornment!

OSCP Resources

- There is a HUGE amount of content out there in regards to OSCP. Here is a list I personally used and found helpful.

- JohnHammond's YouTube Videos. General CTF + Recent OSCP videos
- 31 Days of OSCP Experience - https://scriptdotsh.com/index.php/2018/04/17/31-days-of-oscp-experience/
- Obviously ippsec's videos - https://www.youtube.com/playlist?list=PLidcsTyj9JXK-fnabFLVEvHinQ14Jy5tf
- 0xdf hacks stuff - https://0xdf.gitlab.io/
- Hakluke's Ultimate OSCP Guide - https://medium.com/@hakluke/haklukes-ultimate-oscp-guide-part-1-is-oscp-for-you-b57cbcce7440
- TryHackMe - https://tryhackme.com/
- **TJ's Massive OSCP Guide** - https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html
  - His OSCP-Like VM Spreadsheet - https://t.co/sBy0l6uitf?amp=1
- Buffer Overflow Practice - https://github.com/justinsteven/dostackbufferoverflowgood

PWKv2 Resources!

- There have been some AMAZING improvements to PWK with their 2020 update. Here are some updated resources that have been released for it. **(Disclaimer, I have not taken the exam for PWKv2)**

  - TheCyberMentor's OSCP Review 2020 - https://youtu.be/T1AUCXXKzL8

  - thomfre.dev OSCP Experience - https://thomfre.dev/my-oscp-experience

  - LPEWorkshop - https://github.com/sagishahar/lpeworkshop

  - PSEmpire3.0 - https://www.bc-security.org/post/the-empire-3-0-strikes-back

  - JohnHammond's OSCP Review 2020 - https://youtu.be/wjTt-5mfyhY

Testing Strats

- You’re probably never going to feel ready
- Create a REPEATABLE enumeration process that you use for everything
    - Basically, the exam is not time to start something new.
- If you get stuck on the Buffer Overflow REWATCH THE VIDEOS!
- The above goes for any concepts that might have escaped you
- Relax and take a break or two!
- Good Documentation is key.
    - My personal choice is OneNote 2016. OCR’d screenshots ftw!

OSCE Preparations

- You **don’t** need to complete OSCP to do OSCE. Much more targeted for 32bit exploitation
- If you’re used to doing VR/RE on modern systems with modern workflows it might be a difficult transition for OSCE.
    - OSCE uses perl, ollydbg, course ships with BackTrack 5 -.-
- Basic familiarity with x86 Intel ASM is helpful. (Not Required)
- Being able to work a debugger (setting breakpoints, step over functions)
- Vulnserver for Windows..
- Seriously Vulnserver for Windows

OSCE Resources

- NetSec Focus’s OSCE channel
- h0mbre’s blog - https://h0mbre.github.io/
- AnubisSec blog - https://anubissec.github.io/
- ASCII/OPCODE Table - http://www.bluesock.org/~willg/dev/ascii.html
- Binaries to practice on - https://github.com/73696e65/windows-exploits
- Tulpa Security’s OSCE Guide - https://tulpa-security.com/2017/07/18/288/
- PayloadAllTheThings LFI - https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/File%20Inclusion

Testing Strategies

- Like OSCP, you’re probably not going to feel “ready”
- You have 48 hours, take your time and try to avoid tunnel vision
- Start with what you feel most comfortable with.
- You may need to hit google up quite a bit, you have PLENTY of time.
- Unlike OSCP, I suggest reading some of the above resources during the exam and NOT the videos
- You have time to catch some sleep for this exam. Do that!
- Knowing Vulnserver attack vectors is going to help immensely!

Issues with CTP/OSCE

- Teaches very important concepts, course is has outdated material but still very valuable.
- CTP/OSCE shipped with BackTrack5, I used the OSCP Kali 32bit VM for the exam.
- If you run out of lab time, look to replicate the lab and integrate vulnserver
- This feels like OffSec's forgotten course, just need a refresh imo
- If you do VR/RE as your day job, your workflow will be disrupted quite a bit, be ready for that.
- Sometimes the videos and slides do not match up well.

Conclusion

- Don’t believe the hype, OSCP and OSCE are very achievable.
- If you happen to fail, don’t stop, retakes are relatively inexpensive.
- Try to take the course with a co-worker so you can kick ideas back and forth while working with the course material.
- Check out Netsec Focus, they have a very active OSCP & OSCE channels
-

THANKS FOR WATCHING MY TALK!

Additional questions after VirSecCon?

@niden