Offensive Security Certified Professional (OSCP)

October 19, 2016

John Kennedy
USSTRATCOM PMO Info Assurance Mgr
CISSP, OSCP, GCIH, MBA
Twitter: @clubjk
Blog: jkcybersecurity.org
Email: jk@jkcybersecurity.com
Agenda

• OSCP Basics
• What it looks like
• JK’s OSCP Experience
• The Gouge
Dad

Who am I?

in a band

An OSCP shell

own a Harley

Retiring
30 Nov 2016
OSCP Basics

Security Certifications – Offensive Security

Certified Professional

Certified Expert

Exploitation Expert

Web Expert
OSCP Basics

What is an Offensive Security Certified Professional?

The **Offensive Security Certified Professional (OSCP)** is the companion certification for our [Penetration Testing with Kali Linux training course](https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/) and is the world's first completely hands-on offensive information security certification. The OSCP challenges the students to prove they have a clear and practical understanding of the penetration testing process and life-cycle through an arduous twenty-four (24) hour certification exam.

An OSCP has demonstrated their ability to be presented with an unknown network, enumerate the targets within their scope, exploit them, and clearly document their results in a penetration test report.
OSCP Basics

• The OSCP syllabus uses the Penetration Testing with Kali Linux (PWK) online course
OSCP Basics

• Prerequisites
  Required
  • Solid understanding of TCP/IP
  • Networking
  • Reasonable Linux command line skills
  Desired
  • Scripting familiarity
    • Bash
    • perl
    • python

TL:DR
Penetration Testing with Kali Linux is a foundational security course, but still requires students to have certain knowledge prior to attending the online training class. A solid understanding of TCP/IP, networking, and reasonable Linux skills are required. Familiarity with Bash scripting along with basic Perl or Python is considered a plus. This advanced penetration testing course is not for the faint of heart; it requires practice, testing, and the ability to want to learn in a manner that will grow your career in the information security field and overcome any learning plateau. Offensive Security challenges you to rise above the rest, dive into the fine arts of advanced penetration testing, and to Try Harder™.
OSCP Basics

Costs

• $800-1150 (depends on lab time)

• $150-600 (lab extensions)

• $60 (exam retake)
What it looks like

- VPN - uses tap0 interface
What it looks like

- Student Control Panel - for reverts
What it looks like

• IRC - for Admin help (Freenode:#offsec)
What it looks like

- Forum
What it looks like

- **Twitter**

  - *Michael Cooter liked*

    **PentestingSkills** @Pentest5 · 8h
    Finally Passed and got **#OSCP**, Thanks @offsectraining for the great Experiment

    Dear BourneDiene,
    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.

    ![Twitter screenshot](image)

  - *Hacking tutorials liked*

    **101010101001** @ssdroot7 · Sep 9
    Signed up for 30 days of lab time. Starts in half an hour. The axe has been sharpened during the last few months.

    **#OSCP** **#OffensiveSecurity**

    ![Twitter screenshot](image)

  - *sam taylor @samtaylor1988 · Sep 6*

    First few days into **#oscp** and loving it!!

    ![Twitter screenshot](image)

  - *Twitter students are your friends*
What it looks like
Microsoft OneNote (for note keeping)
My OSCP Experience

09 April - 14 October 2015

My prior experience

IT Manager (no hands on)
MS DOS (1988-1995)
CISSP; CEH; GSEC
My OSCP Experience

• 7 Mar 2015 – Bought ($1150)
  Course - Penetration Testing with Kali (PWK)
    (videos, pdf’s)
  Labs - 90 days Lab access +
  Exam attempt

• 28 Mar 2015 - Lab connectivity check
My OSCP Experience

09 Apr - Began Exercises

20 May - Began Labs
My OSCP Experience

2 Jul 2015– Bought 3 additional months of labs ($600)
My OSCP Experience

30 Sep – Finished lab machines (52 total)
My OSCP Experience

11 Oct – 24-hour exam
5:00AM begin

Hour 17 - crossed 70 pt threshold
(Submitted report the next day)
My OSCP Experience

Host info:

MacBook Pro (2014)

VMWare Fusion ($75)

Kali Linux VM (OffSec’s Penetration Testing w Kali Linux (PWK) version)

Notes – Microsoft OneNote
My OSCP Experience

Study/Lab Routine:

Weekdays
4:00-630AM
11:00AM-1:00PM;
5:00-10:00PM

Weekends (pretty much devoted)
The Gouge

OffSec understates prerequisites, overstates online assist

Hour/Days/(perhaps weeks) of frustrating failure (OffSec Motto: Try Harder)

Punishing for noobs

Key enabler: Twitter contacts also taking the course

Admin assist best at beginning of the box, gets less the closer you get to owning the box.

Nail your information management (notes, screenprints)
The Gouge

Exam Pass Insurance:

If you are close to passing the exam, Offsec will review your optional Lab test report and your Exercise documentation. I had Lab portion of the report complete prior to the exam attempt. Also, my exercise notes and answers.

Exam and Metasploit:

Offsec restricts the use of Metasploit on the exam. Don’t let this stop you from using Metasploit in the labs. By the time you finish the course, it won’t be much of a factor.

Vulnerability analysis:

nmap best option; OpenVAS or Nessus have too many false positives and this will cost you time.
Forward!

vulnhub.com

(hackerone.com)

(great for learning)
OSCP Summary

- Hard (have to really want it)
- Fun (root root root!)
- Glad it’s over, but miss it (kind of)
Questions?