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

Retiring Who am I? 30 Nov 2016 Dad



in a band





_ 0 ×

root@kali: ~

File Edit View Search Terminal Help

root@kali:~# nc -nlvp 443 listening on [any] 443 ... connect to [192.168.12.84] from (UNKNOWN) [192.168.13.82 | 49157 Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\SLmail\System>whoami whoami An OSCP shell

nt authority\system

C:\Program Files\SLmail\System>

Security Certifications – Offensive Security

Redefining Ingenuity

Redefining ingenuity

Security Certifications Roy Gertig CISSPERCE

event on of duty 2010

Redefining Ingenuity

SAIC



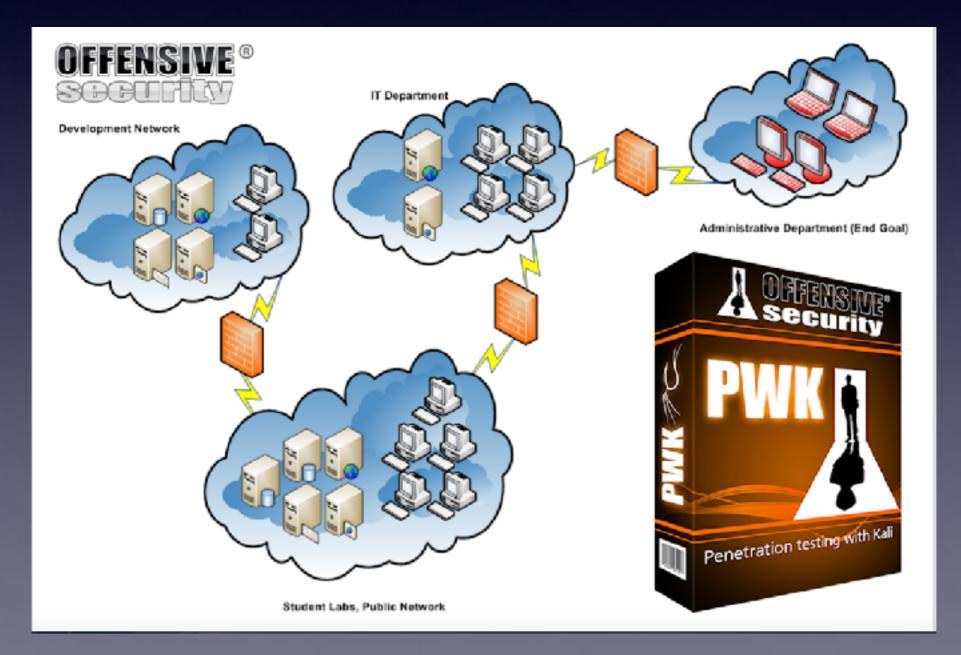
What is an Offensive Security Certified Professional?

The Offensive Security Certified Professional (OSCP) is the companion certification for our Penetration Testing with Kali Linux training course 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.

https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certifiedprofessional/

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



Prerequisites

Required

- Solid understanding of
 - •TCP/IP
 - •Networking

TL:DR

Penetoria in resting with Kali Linux is a foundational security course, but still requires state ets to nove 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 test is and to Try HarderTM.

•Reasonable Linux command line skills

Desired

- Scripting familiarity
 - •Bash
 - •perl
 - •python

Costs

- \$800-1150 (depends on lab time)
- \$150-600 (lab extensions)
- \$60 (exam retake)

| OFFENSIVE® SCCULTUY | Blog | Courses | Certification |
|--|--------------|---------|-----------------|
| Item | | | Price in USD |
| Penetration Testing with Kali + 30 days l Certification | .ab access + | • | USD 800.00 |
| Penetration Testing with Kali + 60 days l Certification | ab access 4 | • | USD 1000.00 |
| Penetration Testing with Kali + 90 days l Certification | ab access + | ł | USD 1,150.00 |
| PWK Lab access - extension of 90 days | | | USD 600.00 |
| PWK Lab access - extension of 60 days | | | USD 450.00 |
| PWK Lab access - extension of 30 days | | | USD 250.00 |
| PWK Lab access - extension of 15 days | | | USD 150.00 |
| Upgrade from PWB v.3.0 to PWK | | | USD 200.00 |
| Upgrade from PWB v.2.0 to PWK | | | USD 300.00 |
| Upgrade from PWB v.1.0 to PWK | | | USD 400.00 |
| OSCP - Certification retake | | | USD 60.00 |

VPN - uses tap0 interface

root@kali:~# ls access log.txt.gz Downloads lab-connection.tar.bz2 lab-connection password cracking filtered.pcap Desktop root@kali:~# cd lab-connections bash: cd: lab-connections: No such file or directory root@kali:~# cd lab-connections bash: cd: lab-connections: No such file or directory root@kali:~# cd lab-connection root@kali:~/lab-connection# openvpn lab-connection.conf Mon Apr 6 20:06:03 2015 OpenVPN 2.2.1 i486-l_nux-gnu [SSL] [LZ02] [EPCLL] [PKCS11] [eurephia] [MH] [PF INET5] [IPv6 payload 20110424-2 (2.2RC2)] built on Jun 19 2013 Enter Auth Username:OS-15830 Enter Auth Password: Mon Apr 6 20:07:00 2015 WARNING: No server certificate verification method has been enablec. See http://openvon.net/howto.html#mitm for more info. Mon Apr 6 20:07:00 2015 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher t c call user-defined scripts or executables. Mon Apr 6 20:07:00 2015 LZO compression initialized Mon Apr 6 20:07:00 2015 UDPv4 link local: [undef] Mon Apr 6 20:07:00 2015 UDPv4 link remote: [AF INE]67.23.72.124:1194 Mon Apr 6 20:07:00 2015 WARNING: this configuration may cache passwordsmin memory the use the auth-nocache option to prevent this Mon Apr 6 20:07:02 2015 [127.0.3.1] Peer Connection Initiated with [AF INET]67.23.72 .124:1194 Mon Apr 6 20:07:04 2015 TJN/TAP device tap0 opened Mon Apr 6 20:07:0/ 2015 do ifconfig, tt->ipv6—0, tt->did ifconfig ipv6 sctup—0 Mon Apr 6 20:07:04 2015 /sbin/ifconfig tap0 192.168.12.84 netmask 255.255.254.0 mtu 1500 broaccast 192.168.13.255 Mon Apr 6 20:07:04 2015 Initialization Sequence Completed

Student Control Panel - for reverts

Professional Training and Tools for Security Specialists.



Training courses designed to EMPOWER you to step into the World of OFFENSIVE SECURITY

Offensive Security - Lab Control Panel Page: My clients

Personal Submit submet keys My Clients Public servers

Logged in as: OS-15830 (John).

You have 88 days of lab access, until Fri, 03 Jul 2015, 19:00 (America/Chicago)

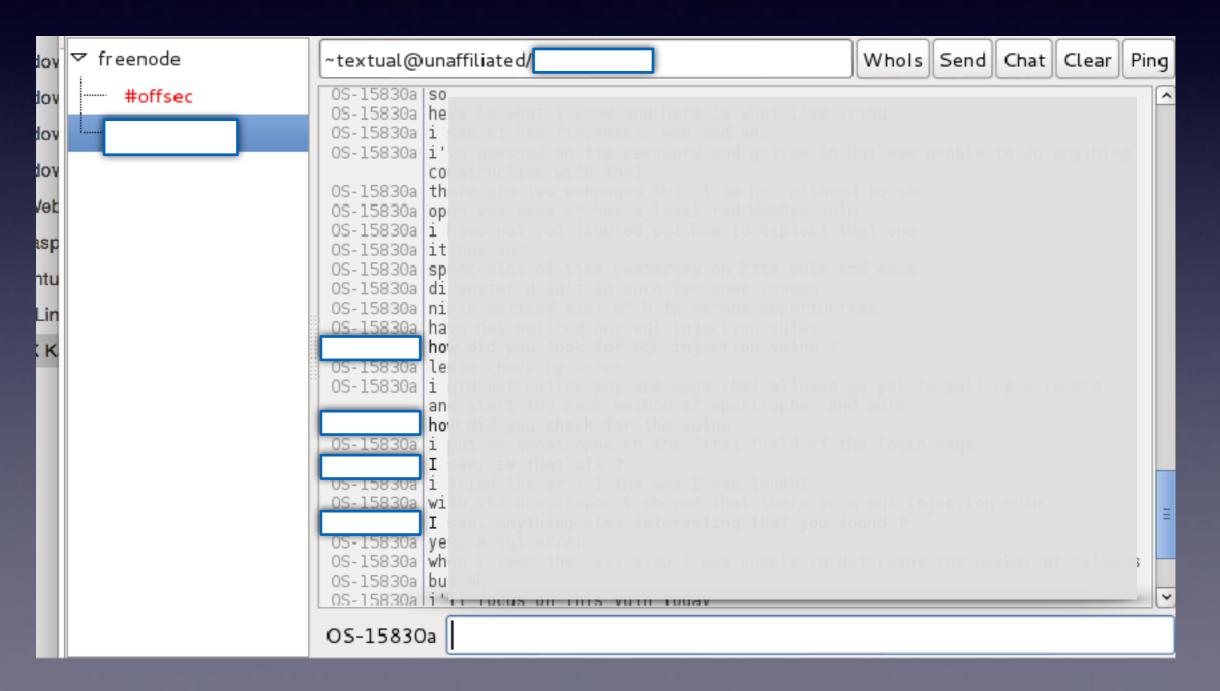
Your last exam date: Thu. 01 Oct 2015, 19:00 (America/Chicago). To book/change your exam, please use <u>this link</u>.

8 reverts left ioday. Counter resets at 0h00 CMT If you require more reverts, please email help@ottensive-security.com



🧔 Problem loading page ... 🛛 🦉 Offensive Security | L. .

• IRC - for Admin help (Freenode:#offsec)





OFFENSIVE SCOUFILY

What's New? Forum

New Posts Private Messages FAQ Calendar Community - Forum Actions - Quick Links -

♣ Forum
♦ Pentesting With Kali
♦ Lab Machines
♦ Public Network
♦ 10.11.1.5

Post New Thread

Forum: 10.11.1.5

Threads 1 to

Forum Tools - Search F

| Title / | Thread Starter | Replies / Views | Last Post By |
|---------|---|-----------------------------|------------------------------------|
| | ALICE 10.11.1.5 , makes me mad Started by OS-22371, 06-26-2016 07:12 PM 1 2 3 | Replies: 21 Views: 1,633 | OS-23640 09-08-2016, D2:26 PM 🔛 |
| | Started by OS-21052, 06-21-2016 12:04 AM 12 | Replies: 14 Views: 723 | OS-22156 09-08-2016, 03:28 AM 💷 |
| | Started by OS-22024, 07-19-2016 10:09 AM 12 | Replies: 11 Views: 406 | OS-21370 09-05-2016, 04:08 PM 📼 |
| | Where is the proof.txt Started by OS-23628, 09-04-2016 01:47 PM | Replies: 3 Views: 103 | OS-21705 09-05-2016, 03:11 PM 📟 |
| | Cracking 10.11.1.5's password hashes Started by OS-18899, 05-23-2016 11:22 PM 1 2 | Replies: 18 Views: 1,507 | OS-21675 08-30-2016, 08:48 AM 🚥 |
| | manual exploit rather than metasploit exploit Started by OS-20732, 05-23-2016 02:36 PM | Replies: 6 Views: 1,212 | OS-16023 08-23-2016, 03:19 PM 📼 |
| | Alice - what should we find Started by OS-23268, 08-23-2016 03:40 AM | Replies: 1 Views: 155 | Link 08-23-2016, 06:30 AM 💷 |
| | Has ALICE changed? Started by OS-17100, 08-03-2016 07:48 PM | Replies: 4 Views: 263 | OS-21477 08-11-2016, D5:46 PM 🚥 |

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.

.....

43 1

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.

.....

....

95

5

-5

#OSCP #OffensiveSecurity

47



47



sam taylor @samtaylor1988 · Sep 6 First few days into **#oscp** and loving it!!



Twitter students are your friends

What it looks like Microsoft OneNote (for note keeping)

| 🔴 🕘 🗁 🔚 🕘 🖉 | CII Exploit development 207 | | | Q- milton | 0 | |
|---|---|--|--|--|---|-------------|
| Home Insert Draw View | | | | | | ©- |
| Copy | | Heading 1 Heading 2 | To Do Remember for later Contact | ★ Important ▲ Definition ☆ Address | Question Highlight Ehone number | To Do |
| CCSP Notes * BAPP Info | PWK Exam Prep V Exam 11 Oct15 | PWK Course | PWK Exercise Admin | Public 2 | blic IT Dept Dev Dep | t Admin Dep |
| Exploit development 207 | 7 | | | 🕀 Add Page | • | 1 |
| Saturday, August 8, 2015 10:31 AM | | | Px 204 limi | ted privs | | |
| | | | 204 Priv Es | 204 Priv Escalation | | |
| 45 Annow Prompt 45 His Proof & Windows (Version 5.2.3796) C2 Copyright 1985-2083 Microsoft Carp. | | PX 204 Bol | System Privs | | | |
| | | 205 Pwn 192. | 168.13.205 IS Oracle - Oracle (P | ublic webserver) | | |
| CINDecuments and SettingenetlohjkAmetetat - av Retive Connections | 67 | | | Rdp 205 | | |
| Pesto Local Address Persign Address State ICP 8.4.8.0.25 8.8.8.8.8.8 LISTENDING ICP 8.4.8.0.25 8.8.8.8 LISTENDING ICP 8.4.0.0280 8.8.8.8 LISTENDING ICP 8.4.0.0280 8.8.8.8 LISTENDING ICP 8.4.0.0280 8.8.8 LISTENDING ICP 8.4.0.0138 6.8.828 LISTENDING ICP 8.8.0.0133 6.8.828 LISTENDING ICP 8.8.0.0143 6.8.828 LISTENDING ICP 8.8.0.0143 6.8.828 LISTENDING ICP 8.8.0.0143 8.8.8288 LISTENDING ICP 8.8.0.014389 8.8.8288 LISTENDING ICP 8.8.0.013899 8.8.8288 LISTENDING ICP 8.8.0.01389 8.8.8288 LISTENDING ICP 127.0.0.11142424 8.8.8288 LISTENDING ICP 192.168.13.227110 192.168.13.20752379 LISTENDING ICP 192.168.13.227110 <td>G1333890 MG</td> <td rowspan="4">LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING JIGTENDING JIGTENDING JIGTENDING JIGTENDING</td> <td>All Port TC</td> <td>Scan</td> <td></td> | G1333890 MG | LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING LIGTENDING JIGTENDING JIGTENDING JIGTENDING JIGTENDING | All Port TC | Scan | | |
| | LISTEND MG LISTEND MG | | | 206 PWN 192 | .168.13.206 IS Oracle2 - | |
| | LISTENONG LISTENING LISTENING | | RDP sessio | RDP session 206 | | |
| | LISTENDING 207:2379 TIME_MODI | | | All Port TC | 2 Scan | |
| TOP 192.164.101.2279105 192.164.10 TOP 192.164.101.2279107 H.M.M.MM TOP 192.164.10.2279107 H.M.M.MM | L 239 2105 4 ISTROLISHID LASTROLISHID L 218 05 1990 ESTROLISHED | | | 192.168.13.20 | 7 - Pedro | |
| This is from admin level access on 229 thing mail server. Shows that 229 has a time wait relationship with the target Pedro 207 Try generate traffic from 229 to Pedro and watch 207 on Wireshark or <u>TCPdump</u> See below sending an email with Kali's sendEmail command | | | rdp passwo | rd guessing 207 | | |
| | | | topdump 2 | 07 | | |
| | | | Exploit dev | alopmant 207 | | |
| | | | Passwords | 207 | | |
| | | enum scan | 207 | | | |
| MaiServer Administrator - (localhest) Els Help | | | | All Port TCI | Scan | |
| Welcone | Accounts | - | | All Port UD | P Scan | |
| E Domaine | None Enabled | | | Somp cour | 1 | |
| in the cos | bob§4/mc.local Yes breh§4/mc.local Yes carb§2/mc.local Yes | | | SMTP Enur | | |
| 💭 🚽 Distribution liste | carie@@inc.local Yes con@@inc.local Yes | | | | s12-020.nse | |
| F 🕼 Secingo | janes@hinc.local Yes ief@hinc.local Yes | | | rop-vuin-m | 512-020.030 | |

09 April - 14 October 2015

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

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

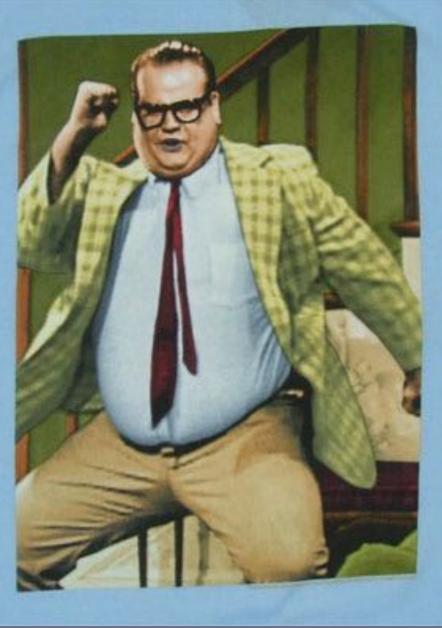
•28 Mar 2015 - Lab connectivity check

09 Apr - Began Exercises

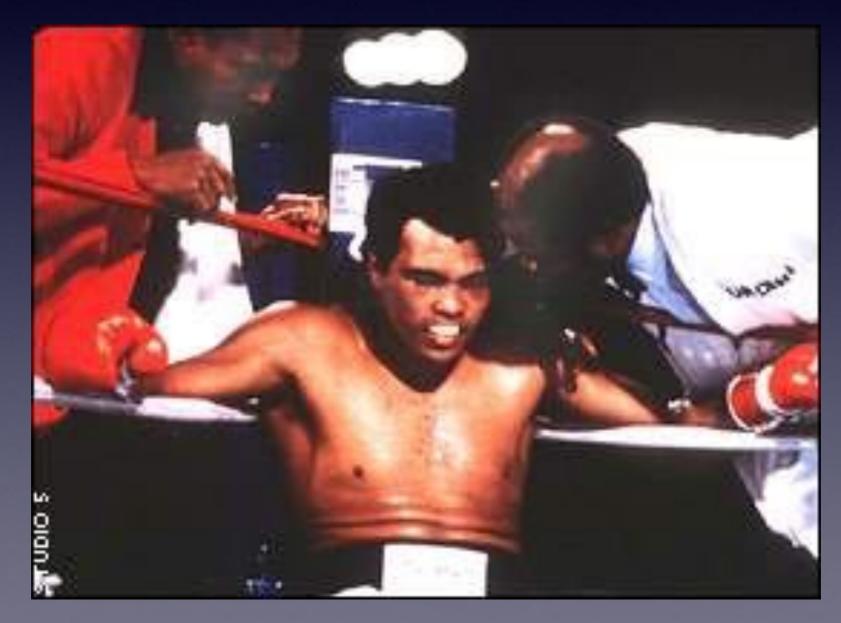
20 May - Began Labs



2 Jul 2015– Bought 3 additional months of labs (\$600)



30 Sep – Finished lab machines (52 total)



11 Oct – 24-hour exam

5:00AM begin



Hour 17 - crossed 70 pt threshold

(Submitted report the next day)



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 your 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

| Breach: 2.1 | | | mrb3n 15 Aug 20 | |
|------------------------|---|----------------------------------|-------------------|--|
| | Second in a multi-part series, Breach 2.0 is a boct2rowt/CTE cha scenario, with plenty of twists and trols along the way. | allenge which attempts to showca | ise a real-world | |
| breach2 login: | The VM is configured with a static IP (192.168.113.151) so you'll need to configure your host only adaptor to this subnet. Sorry! Last one with a static IP () | | | |
| | A hint imagine this as a production environment during a busy | y work day. | | |
| | Shout out to knightmare for many rounds of testing and assist rastamouse, twosevenzero and g0blir for tasting and providing tosting and mantaining #vunnub. | | | |
| | YirtualDox users if the screen gees black on boct once past the and make sure it says Type: Linux Version: Debian 64bit | s grub screen make sure to go to | settings> general | |
| | If you run into any issues, you can find me on Twitter: https://tv | witter.com/mrb3n813 or on RC in | #vulhhub | |
| | Les des des contra de contra com encontrator de la contrator de | ab - a - 1a - 18 a - a | | |
| SIA1: 000052906701FDF9 | F82840F9918642921FF87A1E | | | |

(great for learning)

hackerone.com

| * | A HackerOne, Inc. | 8 |
|----------------|--|---|
| Hacktivity | Directory Reports | |
| | Q, type:hackerone | |
| | | |
| * | Yelp heckerone.com/yelp | |
| | There's no such thing as a perfect technology — not since they put the finishing touches on the wheel — but here at Yelp we are committed to getting as close as we can. It's a big world and we believe that working with skilled security researchers fr | |
| Boszt | Boozt Fashion AB hackerone.com/boort At Boozt we take security seriously, we want our customers not to only have great shopping experience but also feel and know they are safe. But nobody's perfect and top- notch security online is possible only with everyone's help. If you think you fou | |
| LEGAL ROBOT | Legal Robot hackerone.com/legalrobot If you believe you have found a security vulnerability in Legal Robot, we encourage you to let us know right away. We will investigate all legitimate reports and do our best to quickly fix the problem. However, the product is currently in beta, so we | |
| P | Skyliner hadkerone.com/skyliner | |
| | | |



OSCP Summary

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



Questions?