

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?

Retiring
30 Nov 2016



own a Harley



in a band

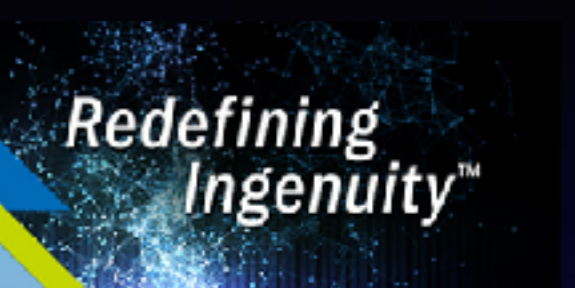
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -nlvp 443  
listening on [any] 443 ...  
connect to [192.168.12.84] from [UNKNOWN] [192.168.13.82]  
] 49157  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights re  
served.  
C:\Program Files\SLmail\System>whoami  
whoami  
nt authority\system  
C:\Program Files\SLmail\System>
```

An OSCP shell

OSCP Basics



Security Certifications – Offensive Security



Certified Professional



Wireless Professional



Certified Expert



Exploitation Expert



Web Expert

OSCP Basics

What is an Offensive Security Certified Professional?

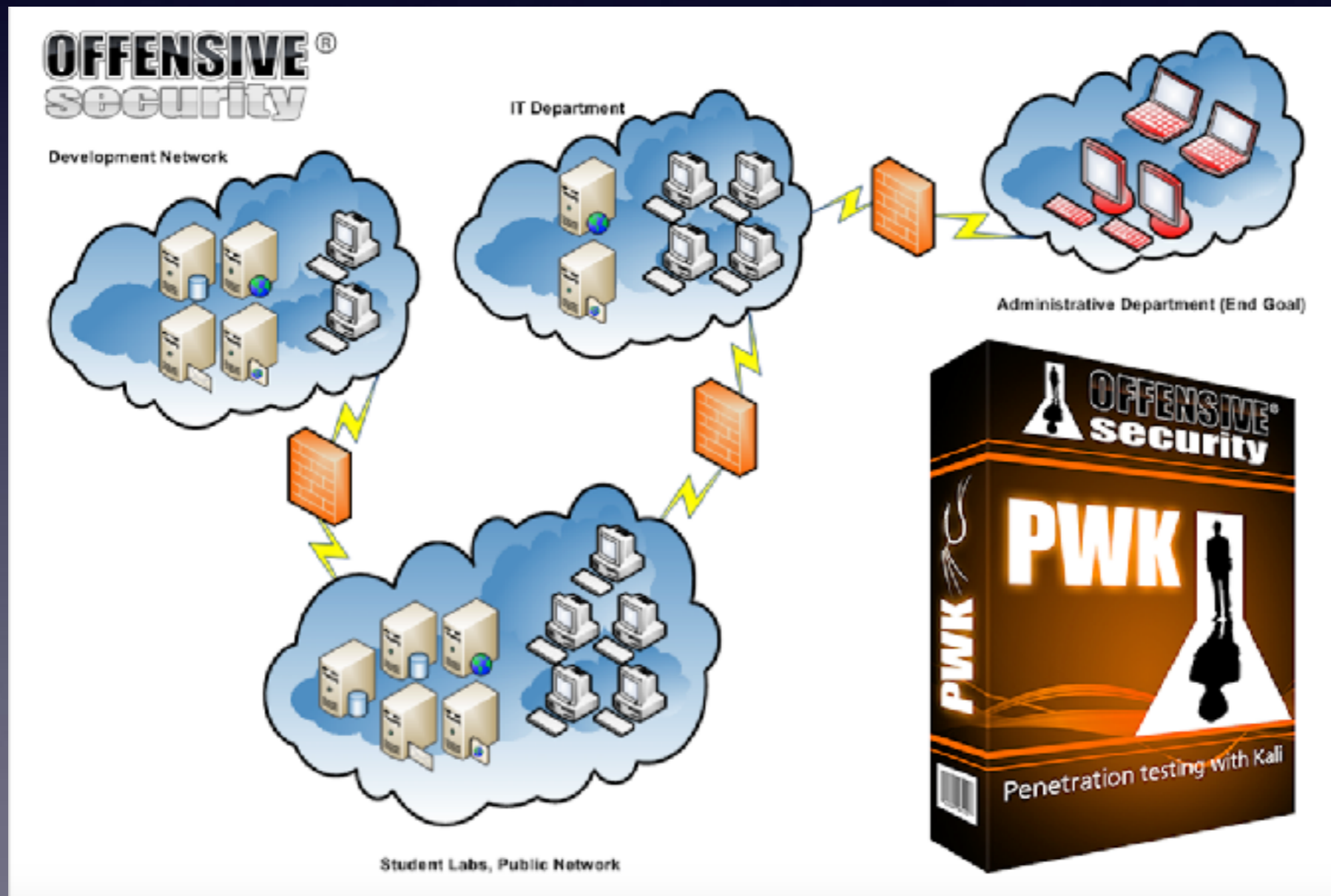
The **Offensive Security Certified Professional (OSCP)** is the companion certification for our **Penetration Testing with Kali Linux training course** and is the world's first completely hands-on offensive information security certification. The OSCP challenges the students to prove they have a clear 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-certified-professional/>

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)



The screenshot shows the Offensive Security website with a navigation menu (Blog, Courses, Certification) and a table listing various services and their prices in USD.

Item	Price in USD
Penetration Testing with Kali + 30 days Lab access + Certification	USD 800.00
Penetration Testing with Kali + 60 days Lab access + Certification	USD 1000.00
Penetration Testing with Kali + 90 days Lab access + Certification	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

What it looks like

- VPN - uses tap0 interface

```
root@kali:~# ls
access_log.txt.gz  Downloads          lab-connection.tar.bz2
Desktop            lab-connection    password_cracking_filtered.pcap
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-linux-gnu [SSL] [LZO2] [EPCLL] [PKCS11] [
eurephia] [MH] [PF_INET6] [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
enabled. See http://openvpn.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
o call user-defined scripts or executables
Mon Apr  6 20:07:00 2015 LZ0 compression initialized
Mon Apr  6 20:07:00 2015 UDPv4 link local: [unde-]
Mon Apr  6 20:07:00 2015 UDPv4 link remote: [AF_INET]67.23.72.124:1194
Mon Apr  6 20:07:00 2015 WARNING: this configuration may cache passwords in memory th-
use the auth-nocache option to prevent this
Mon Apr  6 20:07:02 2015 [127.0.0.1] Peer Connection Initiated with [AF_INET]67.23.72
.124:1194
Mon Apr  6 20:07:04 2015 TUN/TAP device tap0 opened
Mon Apr  6 20:07:04 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Mon Apr  6 20:07:04 2015 /sbin/ifconfig tap0 192.168.12.84 netmask 255.255.254.0 mtu
1500 broadcast 192.168.13.255
Mon Apr  6 20:07:04 2015 Initialization Sequence Completed
```

What it looks like

- Student Control Panel - for reverts

Professional Training and Tools for Security Specialists.

OFFENSIVE security

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

Offensive Security - Lab Control Panel Page: My clients

Personal Submit subnet 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 [this link](#).

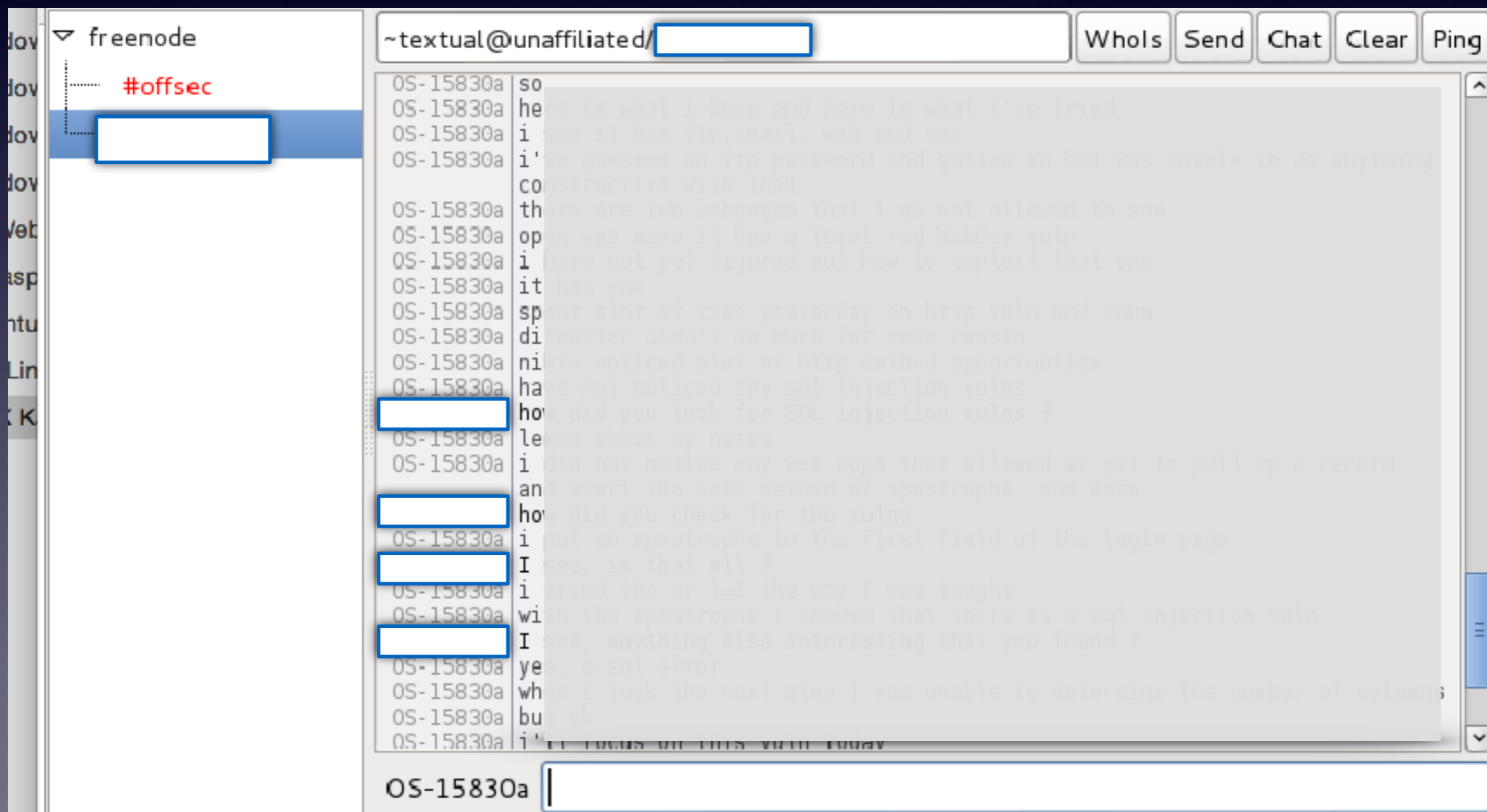
8 reverts left today. Counter resets at 0h00 CMT
If you require more reverts, please email help@offensive-security.com

Select IP  Revert

OSCP Labs: My Wi... root@kali: ~ Problem loading page ... Offensive Security | L...

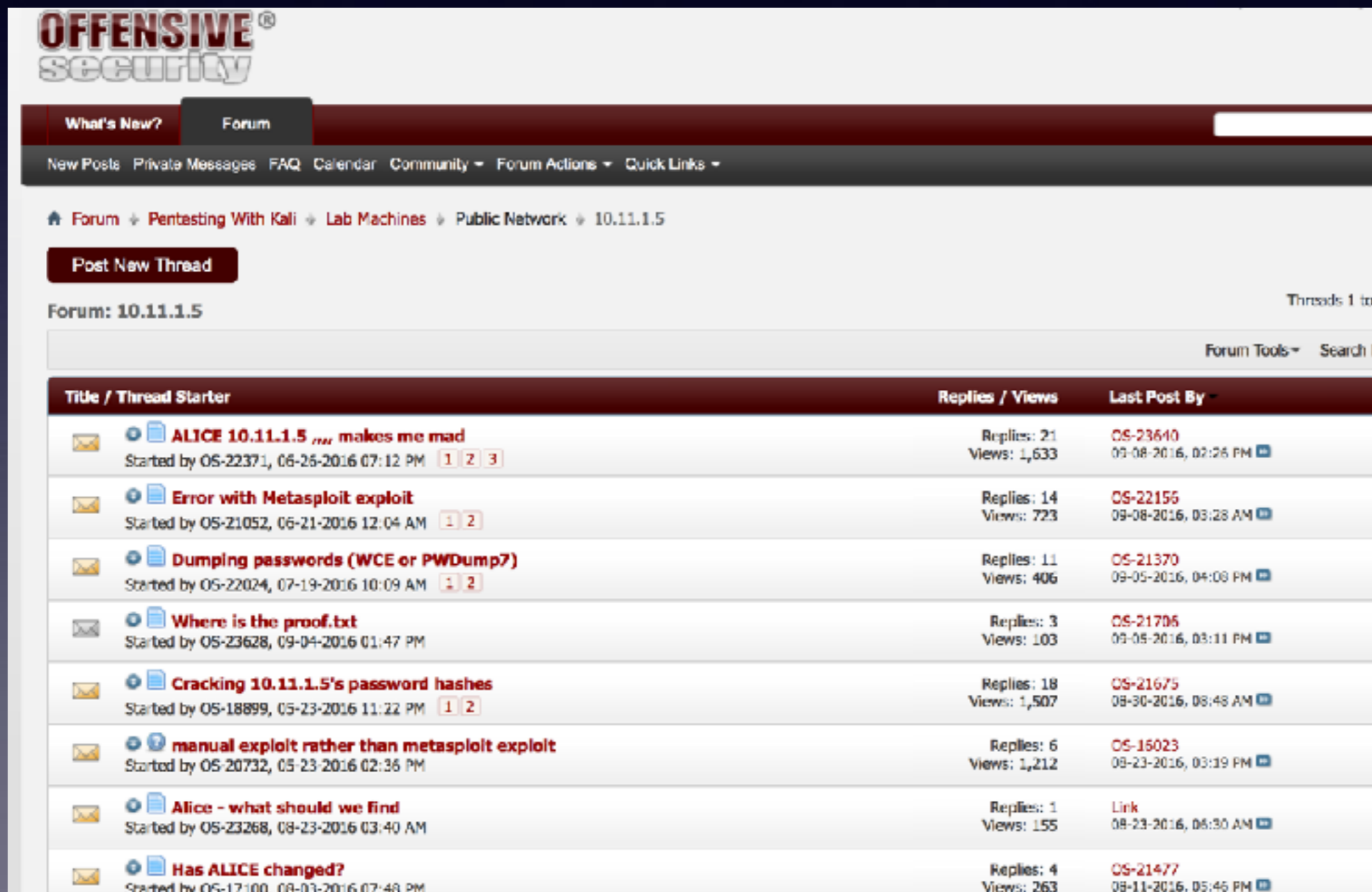
What it looks like

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



























What it looks like

- Forum



The screenshot displays the Offensive Security forum interface. At the top, the logo "OFFENSIVE SECURITY" is visible. Below it, a navigation bar includes "What's New?" and "Forum". A secondary bar contains links for "New Posts", "Private Messages", "FAQ", "Calendar", "Community", "Forum Actions", and "Quick Links". The breadcrumb trail reads: "Forum > Pentesting With Kali > Lab Machines > Public Network > 10.11.1.5". A "Post New Thread" button is located on the left. The forum title "Forum: 10.11.1.5" is shown, along with "Threads 1 to" and "Forum Tools" and "Search" options. The main content is a table of threads with columns for "Title / Thread Starter", "Replies / Views", and "Last Post By".

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, 02:26 PM 
  Error with Metasploit exploit Started by OS-21052, 06-21-2016 12:04 AM 1 2	Replies: 14 Views: 723	OS-22156 09-08-2016, 03:28 AM 
  Dumping passwords (WCE or PWDump7) Started by OS-22024, 07-19-2016 10:09 AM 1 2	Replies: 11 Views: 406	OS-21370 09-05-2016, 04:09 PM 
  Where is the proof.txt Started by OS-23628, 09-04-2016 01:47 PM	Replies: 3 Views: 103	OS-21706 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-15023 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 07:46 PM	Replies: 4 Views: 263	OS-21477 08-11-2016, 05:46 PM 

What it looks like

- Twitter



The screenshot shows three tweets from Twitter. The first tweet is from Michael Cooter, who liked a tweet from PentestingSkills (@Pentest5) posted 8 hours ago. The tweet text is "Finally Passed and got #OSCP, Thanks @offsectraining for the great Experiment". Below the text is a screenshot of an email notification: "Dear Boumediene, 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." The tweet has 1 retweet and 5 likes. The second tweet is from Hacking tutorials, who liked a tweet from 101010101001 (@sssdroot7) posted on Sep 9. The tweet text is "Signed up for 30 days of lab time. Starts in half an hour. The axe has been sharpened during the last few months." It includes the hashtags #OSCP and #OffensiveSecurity and has 5 likes. The third tweet is from sam taylor (@samtaylor1988) posted on Sep 6, with the text "First few days into #oscp and loving it!!" and 5 likes.



Twitter students
are your friends

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

4:00-6:30AM

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:

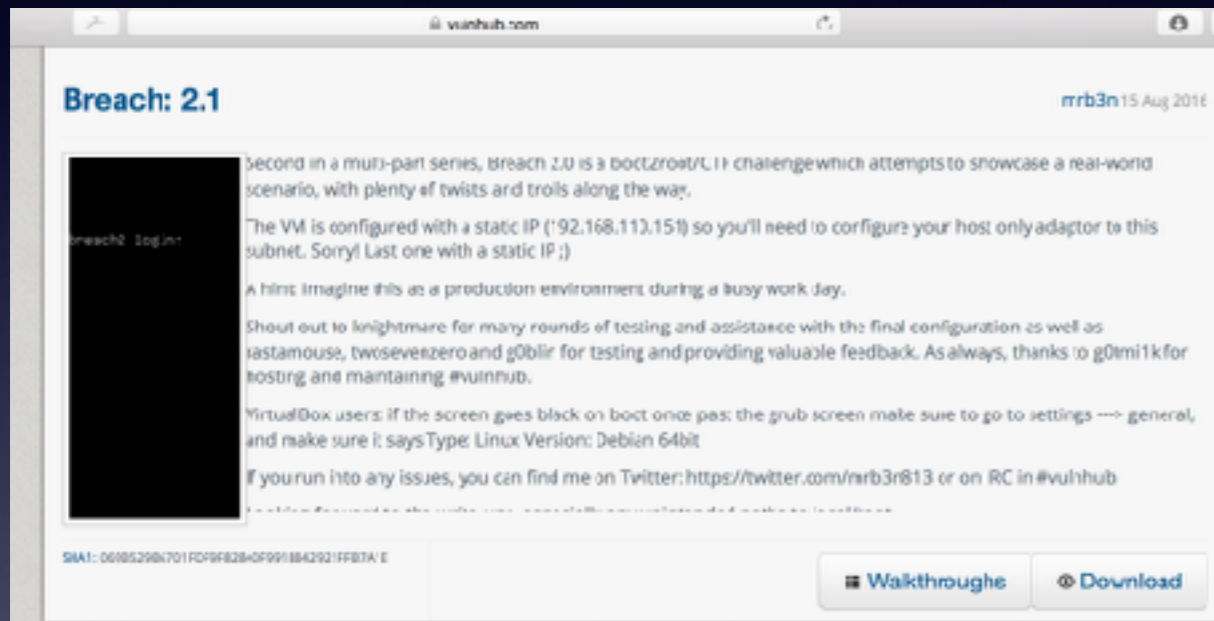
Offsec restricts the use of Metasploit on the exam. Don't let this stop you from using Metasploit in the labs. By the time you finish the course, it won't be much of a factor.

Vulnerability analysis:

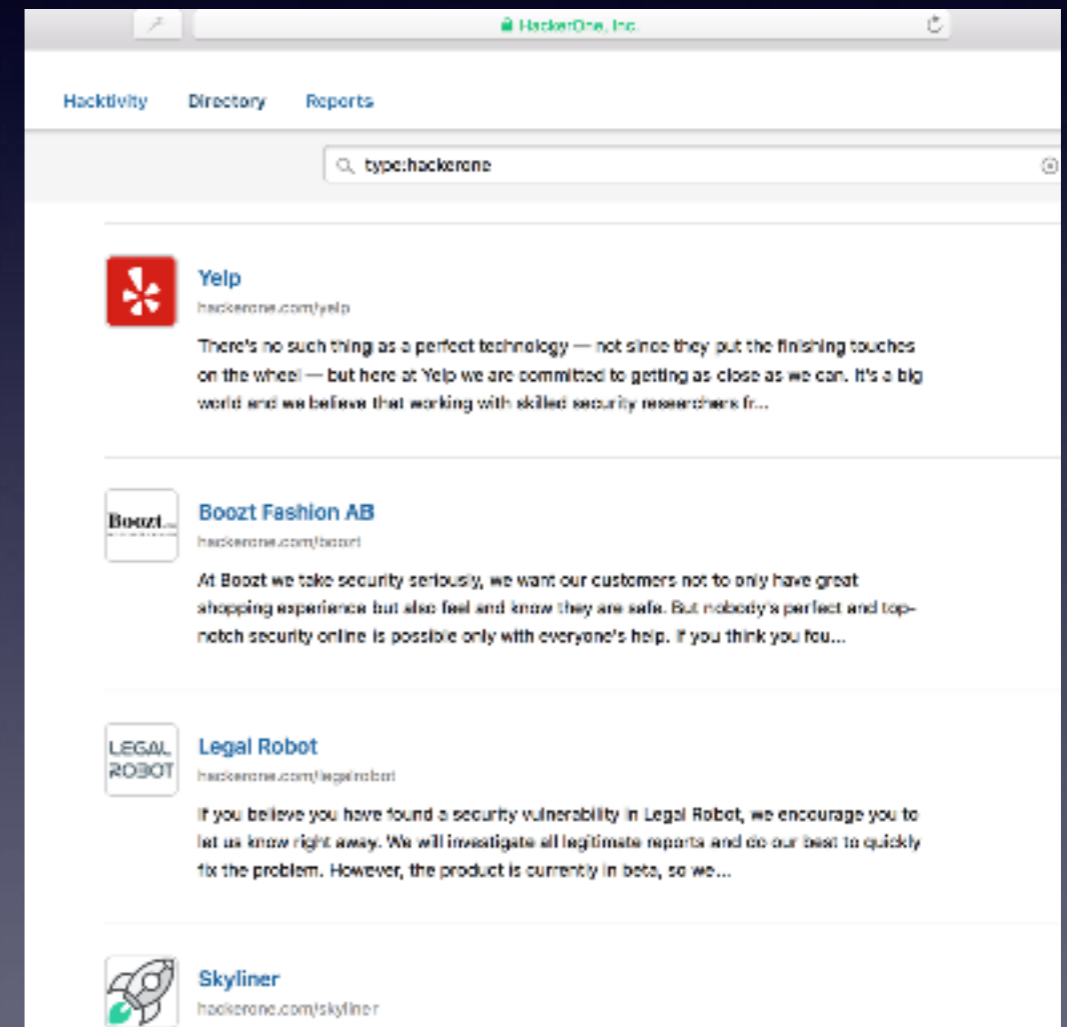
nmap best option; OpenVAS or Nessus have too many false positives and this will cost you time.

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?