Offensive Security Certified Expert (OSCE)

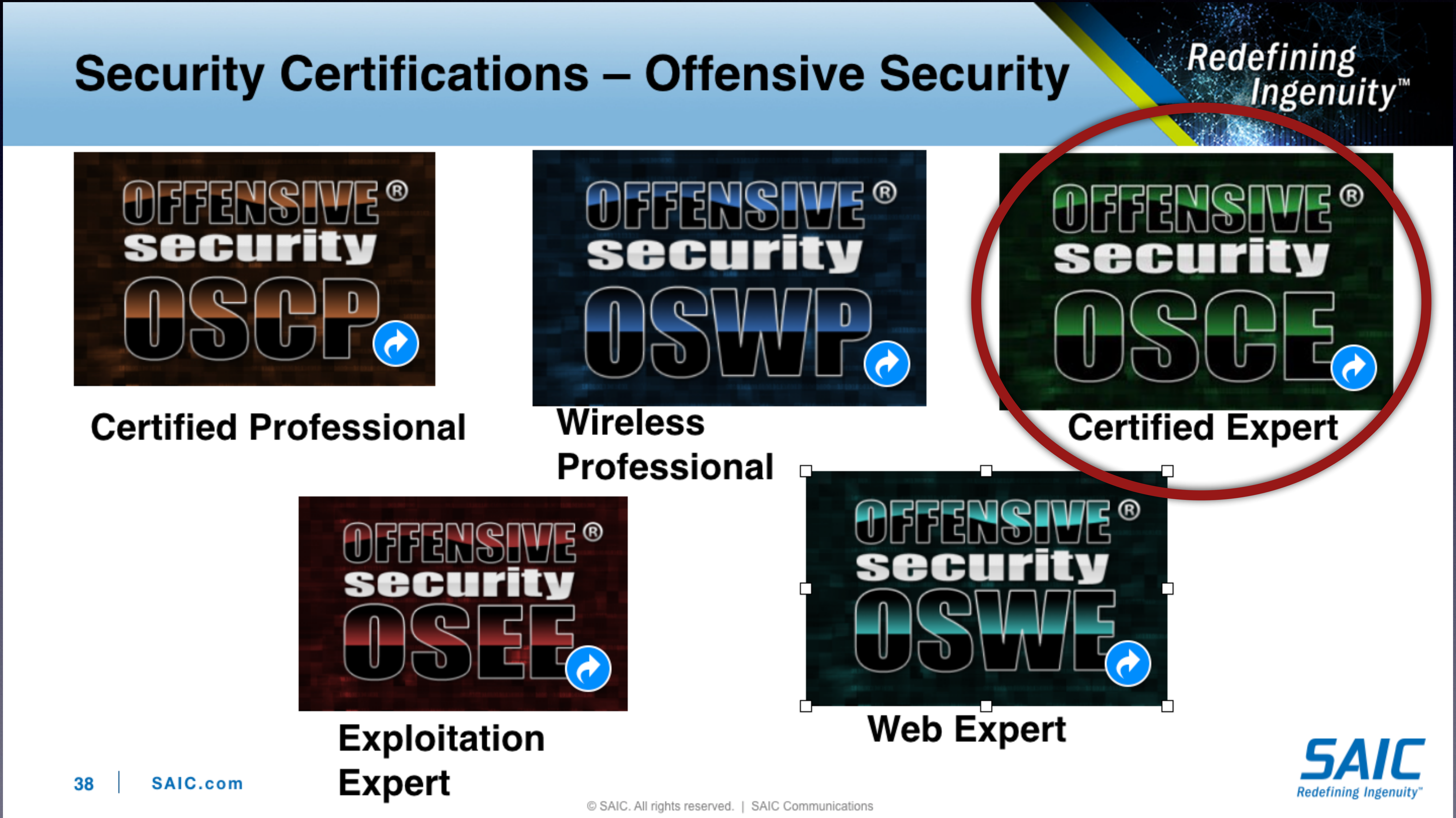
August 22, 2018

John Kennedy
Sr Cybersecurity Analyst, First National Bank
CISSP, OSCE, OSCP, GWAPT, GPEN
Twitter: @clubjk
Blog: jkcybersecurity.org
Email: jk@jkcybersecurity.com

Agenda

- OSCE Basics
- What it looks like
- JK’s OSCE Experience

OSCE Basics



Security Certifications – Offensive Security

Certified Professional

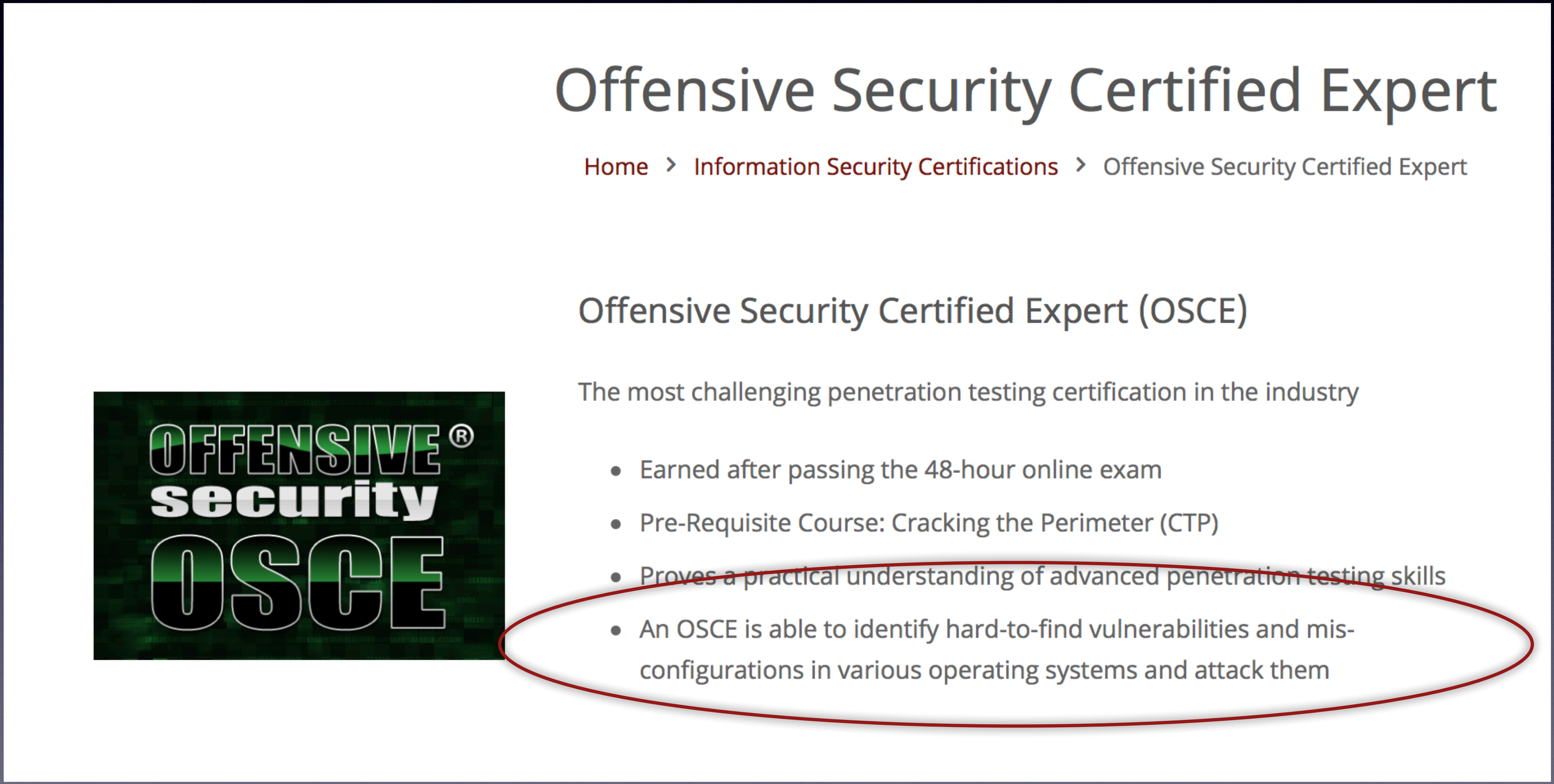
Wireless Professional

Certified Expert

Exploitation Expert

Web Expert

OSCE Basics



Offensive Security Certified Expert

Home › Information Security Certifications › Offensive Security Certified Expert

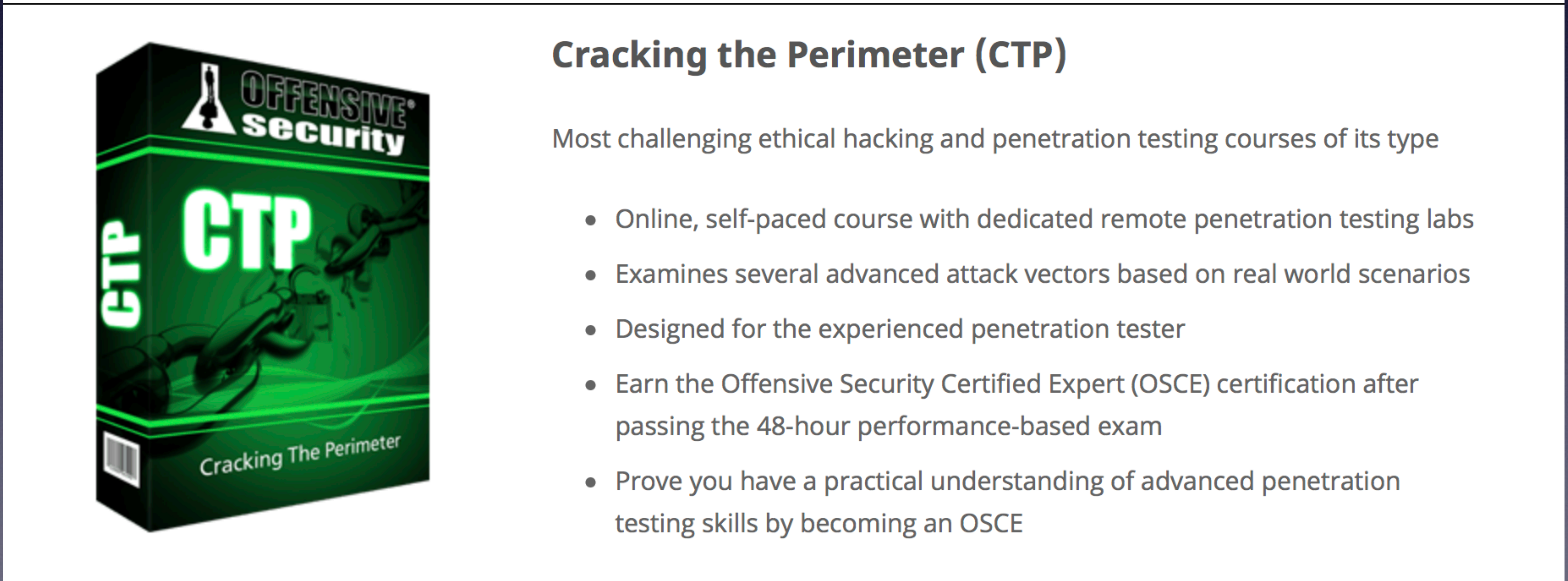
Offensive Security Certified Expert (OSCE)

The most challenging penetration testing certification in the industry

- Earned after passing the 48-hour online exam
- Pre-Requisite Course: Cracking the Perimeter (CTP)
- Proves a practical understanding of advanced penetration testing skills
- An OSCE is able to identify hard-to-find vulnerabilities and misconfigurations in various operating systems and attack them

OSCE Basics

- The OSCE syllabus uses the Cracking the Perimeter (CTP) online course



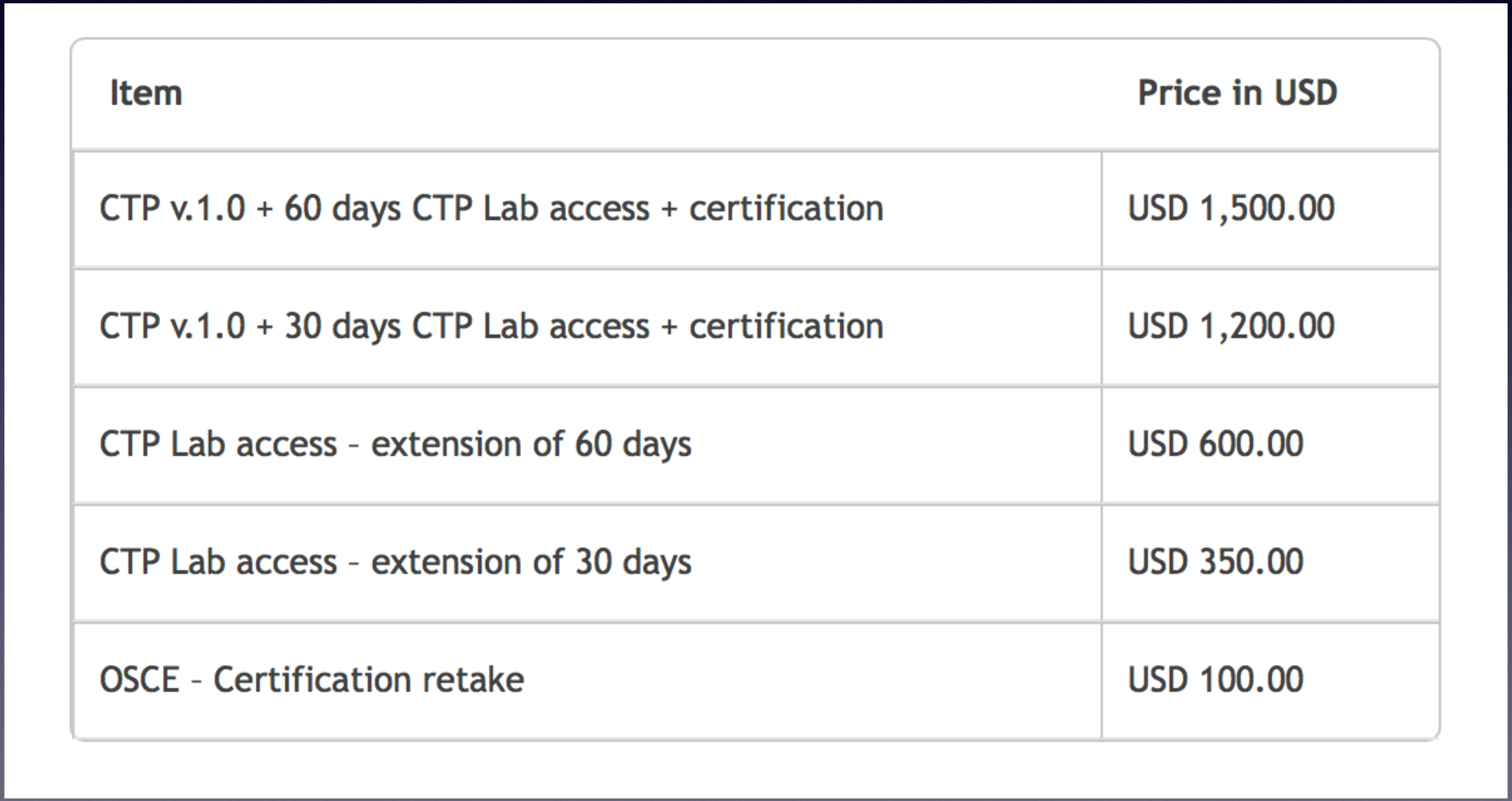
Cracking the Perimeter (CTP)

Most challenging ethical hacking and penetration testing courses of its type

- Online, self-paced course with dedicated remote penetration testing labs
- Examines several advanced attack vectors based on real world scenarios
- Designed for the experienced penetration tester
- Earn the Offensive Security Certified Expert (OSCE) certification after passing the 48-hour performance-based exam
- Prove you have a practical understanding of advanced penetration testing skills by becoming an OSCE

OSCE Basics

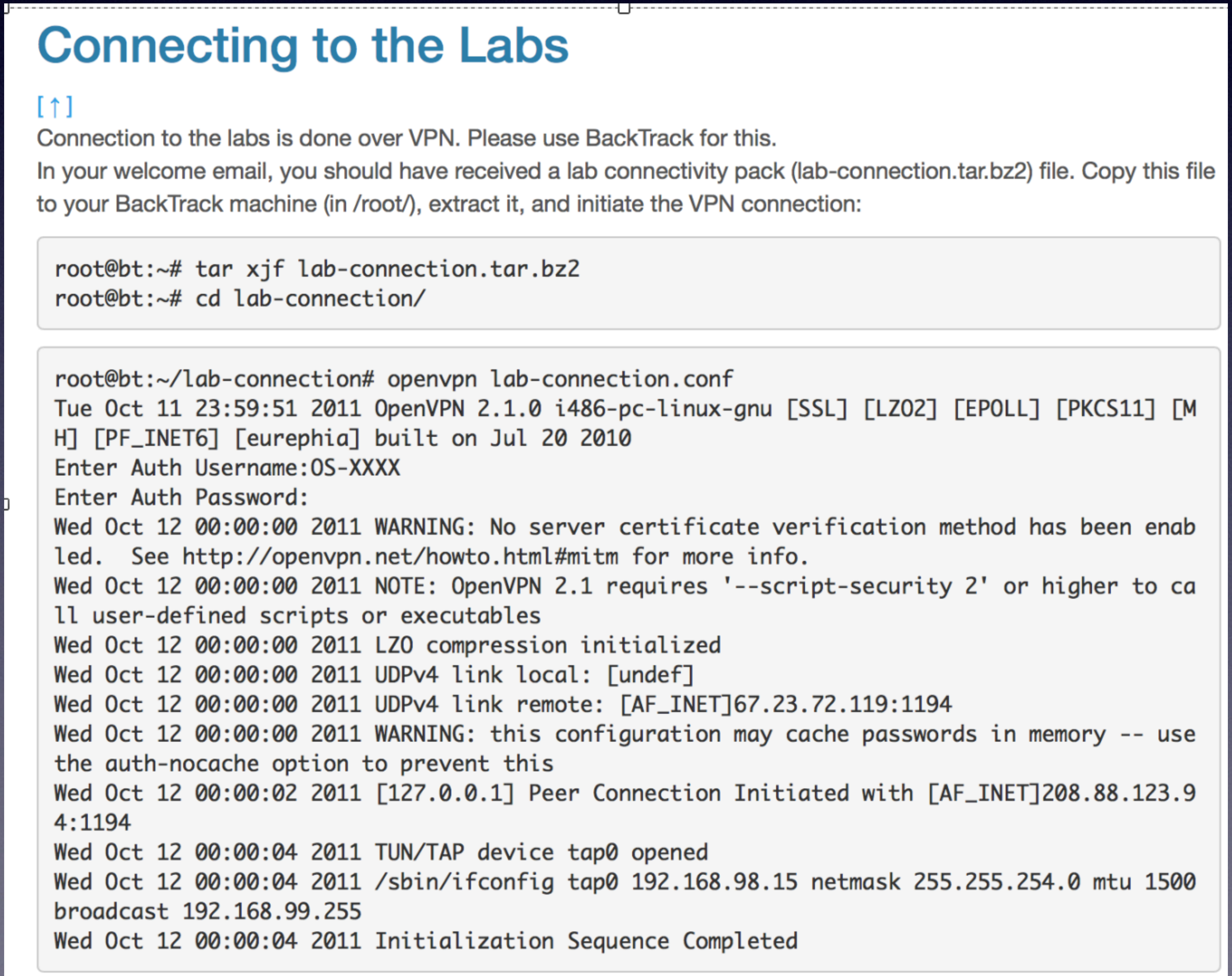
Cost:



Item	Price in USD
CTP v.1.0 + 60 days CTP Lab access + certification	USD 1,500.00
CTP v.1.0 + 30 days CTP Lab access + certification	USD 1,200.00
CTP Lab access – extension of 60 days	USD 600.00
CTP Lab access – extension of 30 days	USD 350.00
OSCE – Certification retake	USD 100.00

What it looks like

- VPN - uses tap0 interface



Connecting to the Labs

[↑]

Connection to the labs is done over VPN. Please use BackTrack for this.

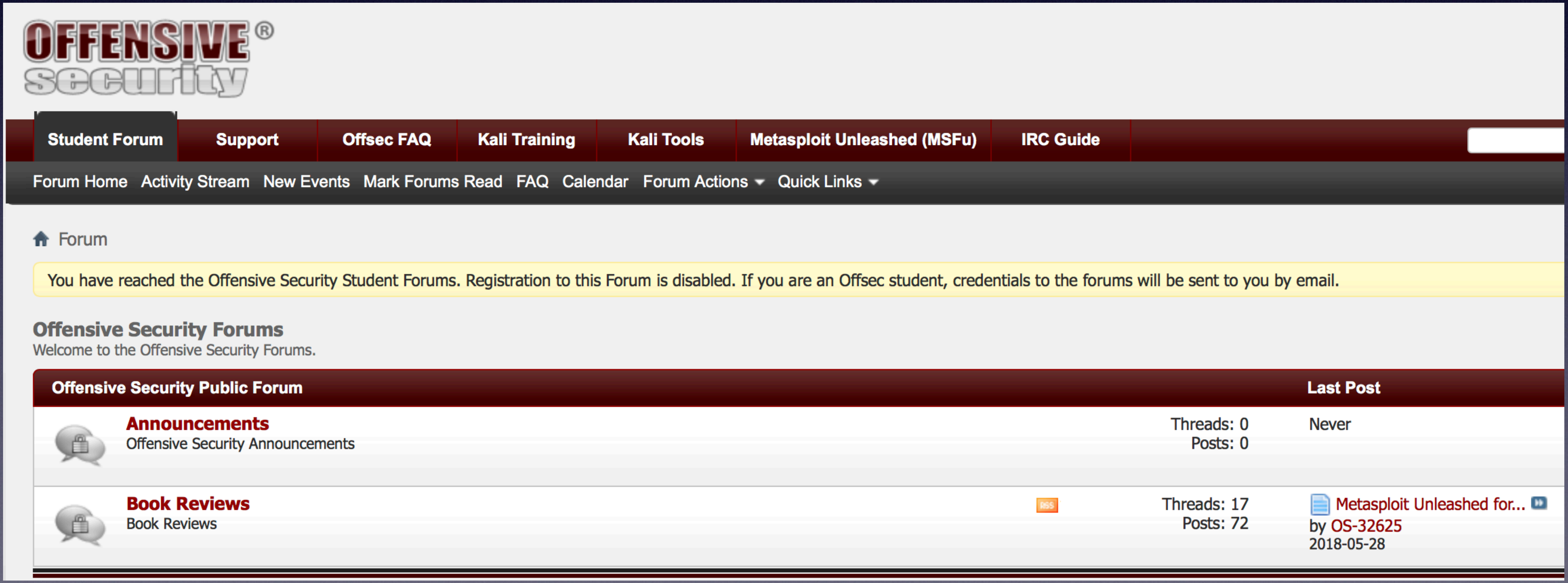
In your welcome email, you should have received a lab connectivity pack (lab-connection.tar.bz2) file. Copy this file to your BackTrack machine (in /root/), extract it, and initiate the VPN connection:

```
root@bt:~# tar xjf lab-connection.tar.bz2
root@bt:~# cd lab-connection/
```

```
root@bt:~/lab-connection# openvpn lab-connection.conf
Tue Oct 11 23:59:51 2011 OpenVPN 2.1.0 i486-pc-linux-gnu [SSL] [LZO2] [EPOLL] [PKCS11] [M
H] [PF_INET6] [eurephia] built on Jul 20 2010
Enter Auth Username:OS-XXXX
Enter Auth Password:
Wed Oct 12 00:00:00 2011 WARNING: No server certificate verification method has been enab
led.  See http://openvpn.net/howto.html#mitm for more info.
Wed Oct 12 00:00:00 2011 NOTE: OpenVPN 2.1 requires '--script-security 2' or higher to ca
ll user-defined scripts or executables
Wed Oct 12 00:00:00 2011 LZO compression initialized
Wed Oct 12 00:00:00 2011 UDPv4 link local: [undef]
Wed Oct 12 00:00:00 2011 UDPv4 link remote: [AF_INET]67.23.72.119:1194
Wed Oct 12 00:00:00 2011 WARNING: this configuration may cache passwords in memory -- use
the auth-nocache option to prevent this
Wed Oct 12 00:00:02 2011 [127.0.0.1] Peer Connection Initiated with [AF_INET]208.88.123.9
4:1194
Wed Oct 12 00:00:04 2011 TUN/TAP device tap0 opened
Wed Oct 12 00:00:04 2011 /sbin/ifconfig tap0 192.168.98.15 netmask 255.255.254.0 mtu 1500
broadcast 192.168.99.255
Wed Oct 12 00:00:04 2011 Initialization Sequence Completed
```

What it looks like

- Forum



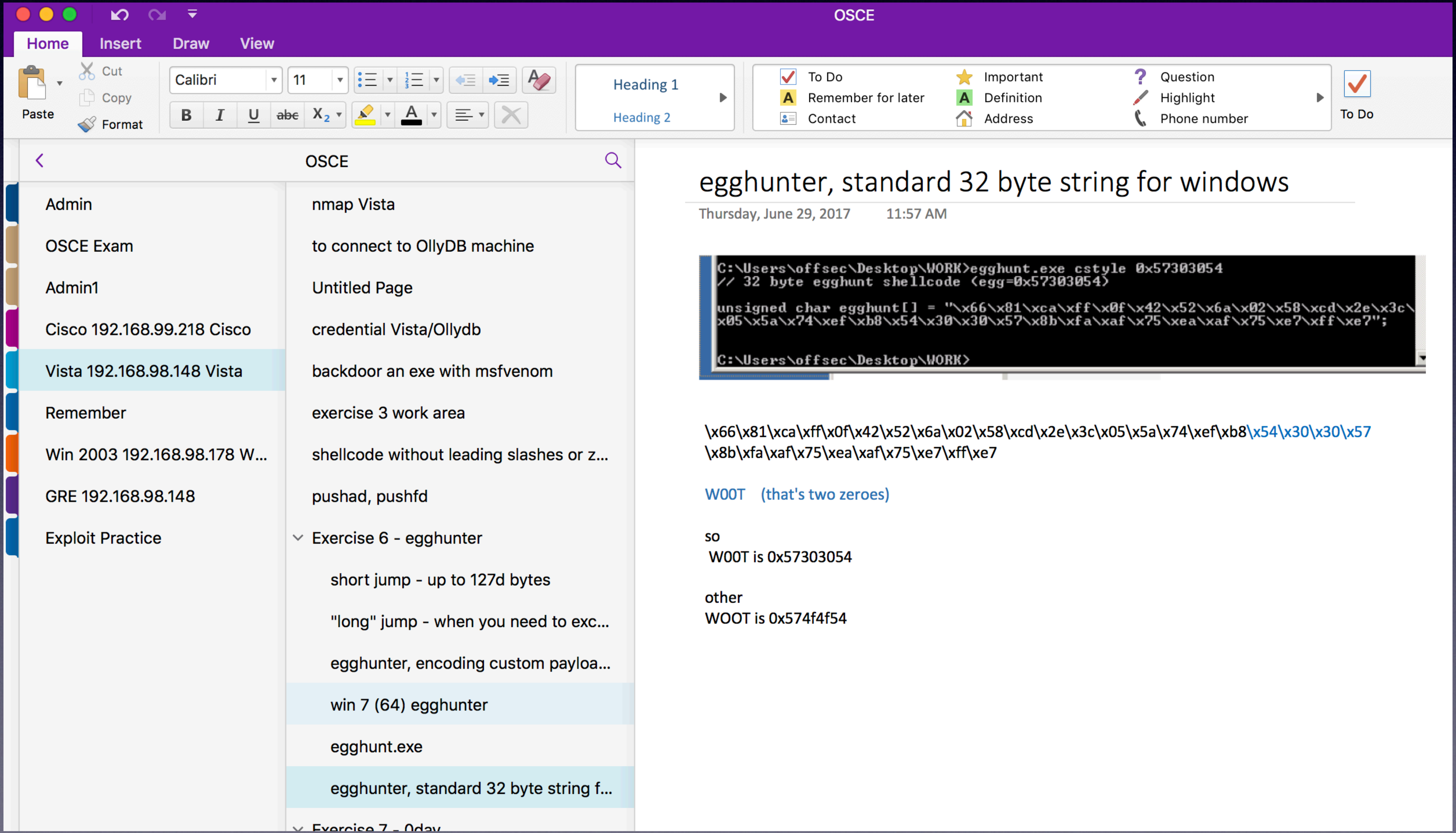
You have reached the Offensive Security Student Forums. Registration to this Forum is disabled. If you are an Offsec student, credentials to the forums will be sent to you by email.

Offensive Security Forums
Welcome to the Offensive Security Forums.

Offensive Security Public Forum		Last Post
Announcements Offensive Security Announcements	Threads: 0 Posts: 0	Never
Book Reviews Book Reviews	Threads: 17 Posts: 72	Metasploit Unleashed for... by OS-32625 2018-05-28

What it looks like

Microsoft OneNote (for note keeping)



Admin
OSCE Exam
Admin1
Cisco 192.168.99.218 Cisco
Vista 192.168.98.148 Vista
Remember
Win 2003 192.168.98.178 W...
GRE 192.168.98.148
Exploit Practice

nmap Vista
to connect to OllyDB machine
Untitled Page
credential Vista/Ollydb
backdoor an exe with msfvenom
exercise 3 work area
shellcode without leading slashes or z...
pushad, pushfd
Exercise 6 - egghunter
short jump - up to 127d bytes
"long" jump - when you need to exc...
egghunter, encoding custom payloa...
win 7 (64) egghunter
egghunt.exe
egghunter, standard 32 byte string f...
Exercise 7 - 0day

egghunter, standard 32 byte string for windows

Thursday, June 29, 2017 11:57 AM

```
C:\Users\offsec\Desktop\WORK>egghunt.exe cstyle 0x57303054
// 32 byte egghunt shellcode (egg=0x57303054)

unsigned char egghunt[] = "\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\
x05\x5a\x74\xef\xb8\x54\x30\x30\x57\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7";


C:\Users\offsec\Desktop\WORK>
```

\x66\x81\xca\xff\x0f\x42\x52\x6a\x02\x58\xcd\x2e\x3c\x05\x5a\x74\xef\xb8\x54\x30\x30\x57
\x8b\xfa\xaf\x75\xea\xaf\x75\xe7\xff\xe7

W00T (that's two zeroes)

so
W00T is 0x57303054

other
WOOT is 0x574f4f54

My OSCE Experience

06 April - 22 August 2017

My prior experience

OSCP

SLAE-32, SLAE-64

GWAPT

My OSCE Experience

- 5 Apr 2017 - Registration Challenge
- 6 Apr 2017 – Bought ($1500)

  Course - Cracking the Perimeter

  (videos, pdf's)

  Labs - 60 days Lab access +

  Exam attempt

My OSCE Experience

12 Apr - Began Lab Exercises

Exercises:

Web App XSS
Web App LFI
Backdoor an EXE
ASLR Bypass
Egghunter BOF
0-day TFTP BOF
0-day Alphanumeric Shellcode
Router exploit

(Muts' Greatest Hits of 2008)

My OSCE Experience

8 July – Finished lab exercises

My OSCE Experience

The exam has four challenges:

Machine 1 (30 points)

Machine 2 (30 points)

Machine 3 (15 points)

Machine 4 (15 points)

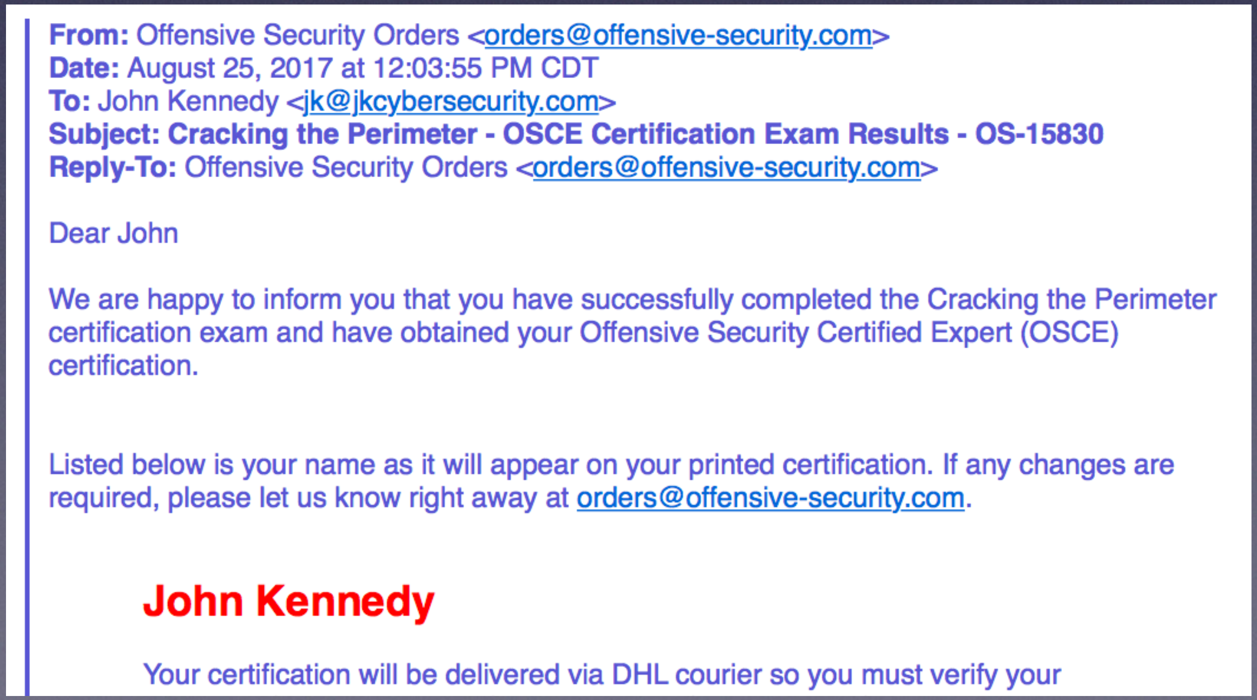
For a total of 90 points; Passing is 75 points

My OSCE Experience

19 Aug: Passed exam

20 Aug: Sent report

25 Aug: Good news



From: Offensive Security Orders <orders@offensive-security.com>
Date: August 25, 2017 at 12:03:55 PM CDT
To: John Kennedy <jk@jkcybersecurity.com>
Subject: Cracking the Perimeter - OSCE Certification Exam Results - OS-15830
Reply-To: Offensive Security Orders <orders@offensive-security.com>

Dear John

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.

John Kennedy

Your certification will be delivered via DHL courier so you must verify your

My OSCP Experience

Host info:

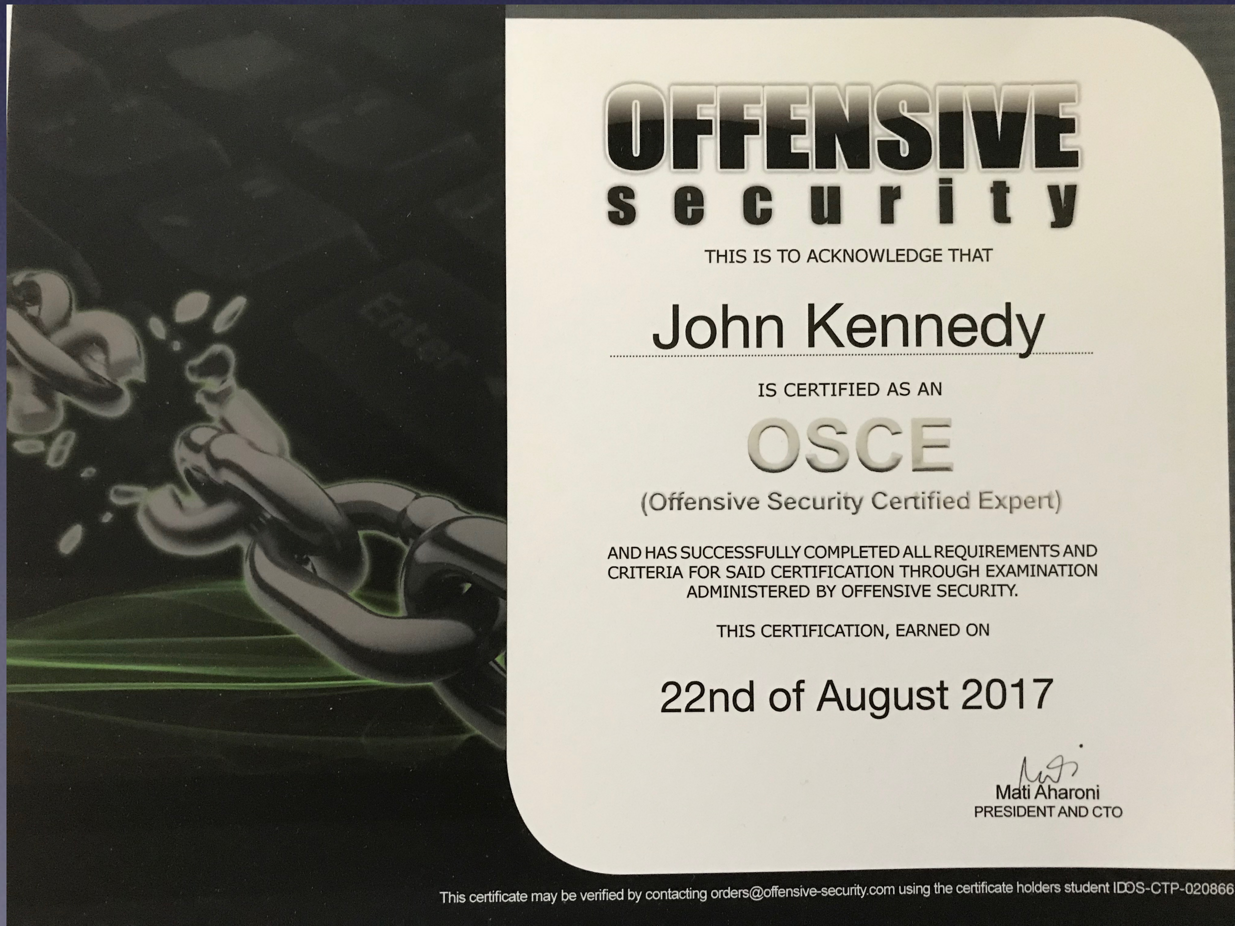
- MacBook Pro (2017)
- VMWare Fusion ($75)

Kali Linux VM

Notes – Microsoft OneNote

OSCE Summary

- Kind of a pain
- One area very useful; three others somewhat
- Glad it’s over



OFFENSIVE
security

THIS IS TO ACKNOWLEDGE THAT

John Kennedy

IS CERTIFIED AS AN

OSCE

(Offensive Security Certified Expert)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

22nd of August 2017

Mati Aharoni
PRESIDENT AND CTO

This certificate may be verified by contacting orders@offensive-security.com using the certificate holders student IDOS-CTP-020866

Questions?