

# ULTIMATE PREPARATION GUIDE TO OSCP 2021

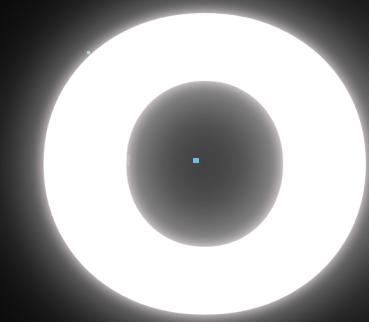
[adithyanak.com](http://adithyanak.com)

# WHOAMI



Adithyan Arun Kumar

- Offensive Security Certified Professional (OSCP)
- Certified Ethical Hacker (Master)
- Head of OWASP Coimbatore
- 7+ Years in Information Security
- Expertise in Application Security (Web and Network) and Open Source Intelligence
- Speaker at various conferences and educational institutions (IITM Research Park, NIT, Defcon, OWASP meetup)
- Acknowledged by Microsoft, Apple, Intel, Avira, Oppo, etc



E X A M   S T R A T E G Y

W H A T

O S C P



## **PEN-200 PWK**

Penetration Testing with Kali Linux

## **24 HOURS**

Rigorous 23 hours 45 minutes practical exam

## **5 HOSTS**

1 Buffer Overflow + 4 Hosts

## **100 POINTS**

70 to pass

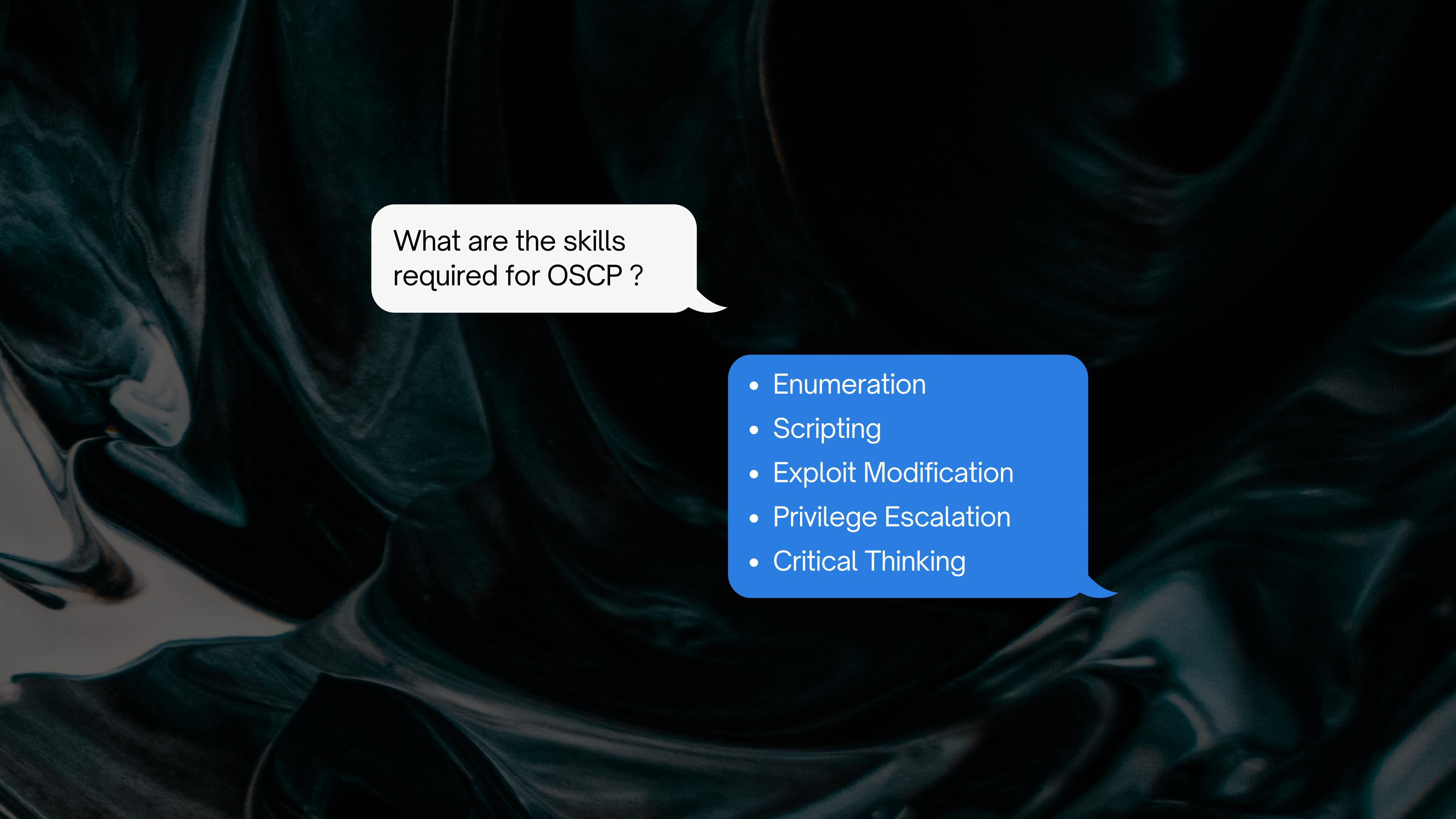


## **OSCP**

**WHAT IS IT ?**

# PWK Syllabus

- Bash Scripting
- Information Gathering
- Vulnerability Scanning
- Web Application Attacks (SQL, XSS, File inclusion)
- Windows Buffer Overflows
- File transfers
- Password Attacks
- AV Evasion
- Privilege Escalation
- Port Redirection and Tunneling
- Active Directory Attacks
- The Metasploit Framework
- PowerShell Empire



What are the skills  
required for OSCP ?

- Enumeration
- Scripting
- Exploit Modification
- Privilege Escalation
- Critical Thinking

# Prerequisites for OSCP



- Network Essentials
- Windows & Linux Administration
- Web Application
- Scripting
- Getting comfortable with tools

# Exam Restrictions

SPOOFING

COMMERCIAL TOOLS

AUTO EXPLOITATION TOOLS

MASS VULNERABILITY SCANNERS

YOU'RE RESPONSIBLE



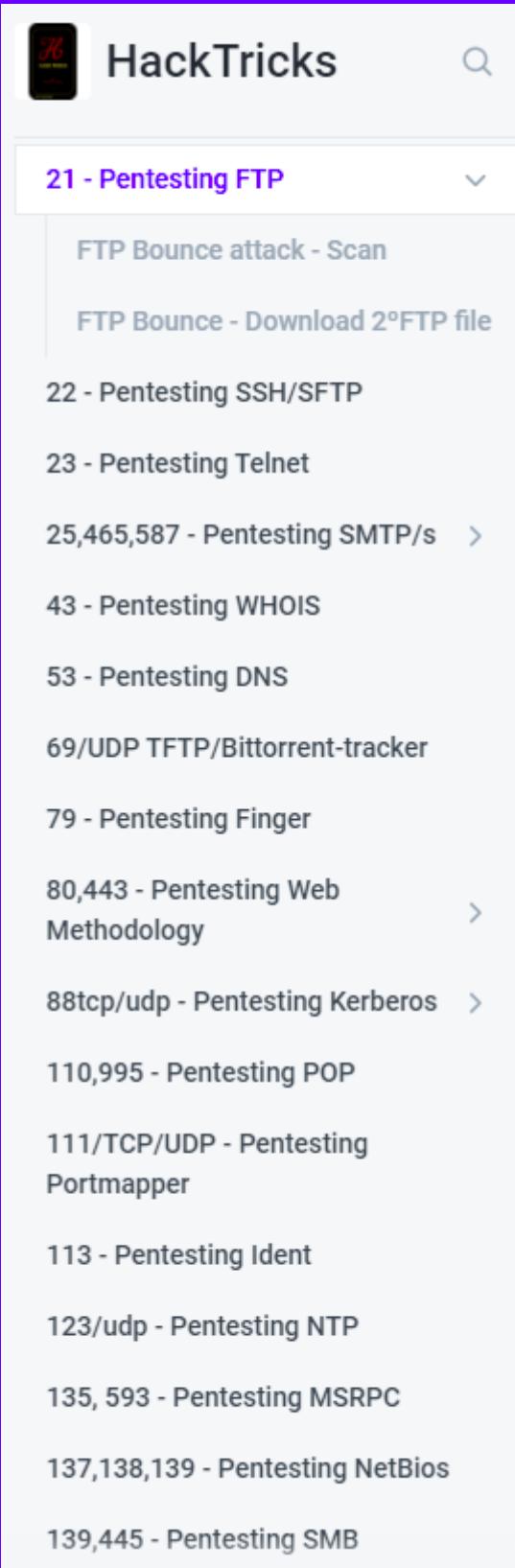
# **PHASE 1**

## **THE PREPARATION**

# Courses

- Beginner
  - [CompTIA's Network+](#)
  - [Practical Ethical Hacking by Heath Adams](#)
- Intermediate
  - [Windows Privilege Escalation for Beginners](#) - TCM
  - [Linux Privilege Escalation for Beginners](#) - TCM
  - [Linux Privilege Escalation for OSCP & Beyond!](#) - Tib3rius
  - [Windows Privilege Escalation for OSCP & Beyond!](#) - Tib3rius
  - [TJnull's OSCP Prep playlist by ipsec](#)

# Blogs



- [Hacktricks.xyz](#)
- [oscpnotes.infosecsanyam.in](#)
- [sushant747.gitbooks.io](#)
- [blog.adithyanak.com](#)
- [github.com/wwong99/pentest-notes](#)
- [scund00r.com](#)

# Youtube Channels

- Ippsec
- Conda
- John Hammond
- JSON Sec
- DC CyberSec
- Elevate Cyber
- Injection
- Michael LaSalvia
- Busra Demir

# Why Notes

- Not everyone has great memory
- Reinforcing the learning
- known vs unknown
- Develop your own Offensive Security approach
- note taking choices
  - gitbook
  - cherrytree
  - obsidian



# **PHASE 2**

## **THE PRACTICE**

# Practice



## VULNHUB

Free, 500+ machines and exercises, great resource  
<https://www.vulnhub.com/>



## OFFSEC PROVING GROUNDS

Play & Practice, 19\$/Month  
<https://www.offensive-security.com/labs/>



## TRYHACKME

freemium - Linux & Windows  
Privesc + Bufferoverflow  
<https://tryhackme.com/>



## HACKTHEBOX

freemium, 14\$/Month VIP pass  
retired machines  
<https://www.hackthebox.eu>



## VIRTUAL HACKING LABS

45+ hosts + course, 99\$/Month,  
Certificate of Completion  
<https://www.virtualhackinglabs.com>



## PENTESTERLAB PRO

300+ exercises, videos + certificate -  
35\$/3 Months - Student | 20\$/Month  
<https://pentesterlab.com/>

## NetSec OSCP

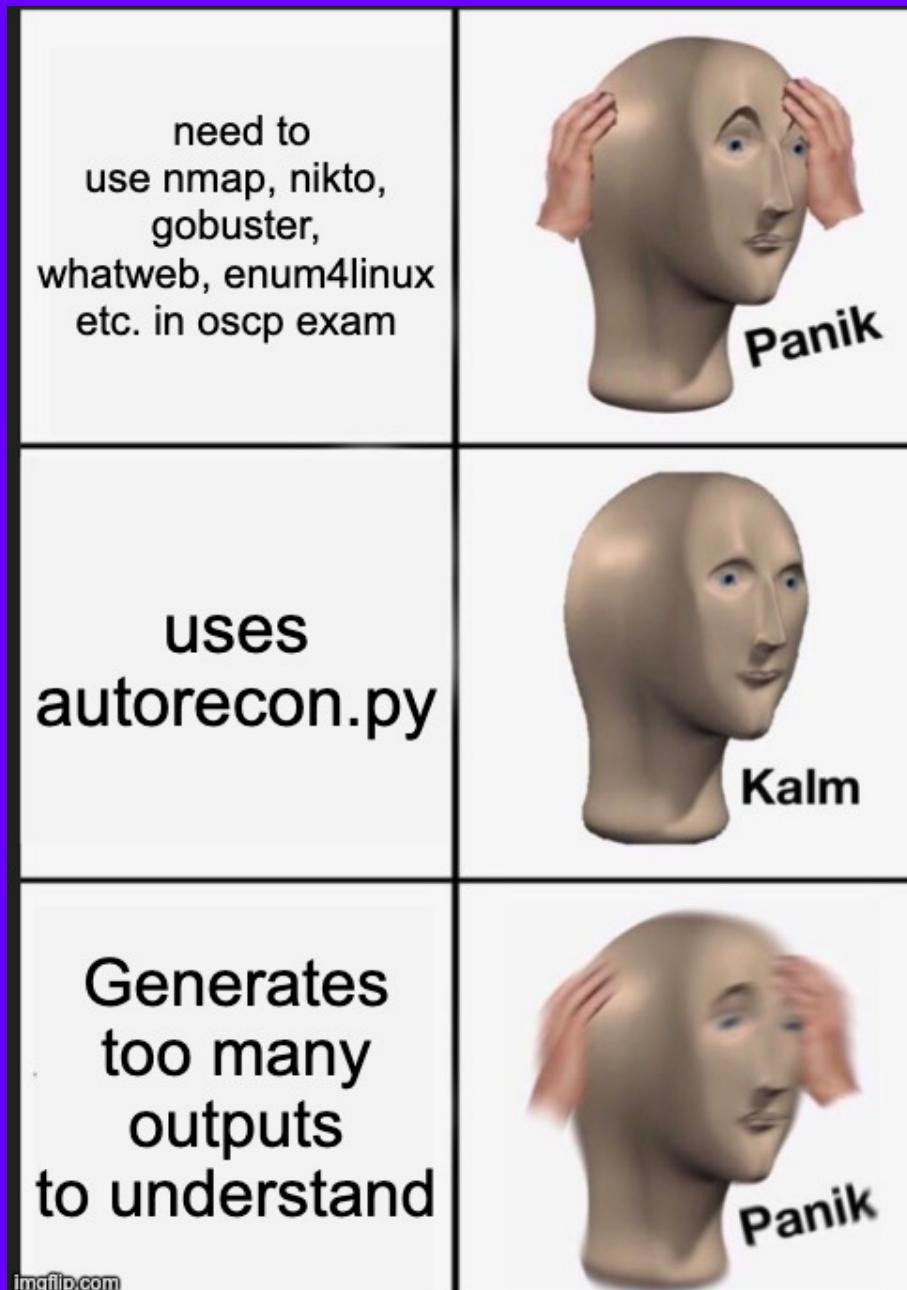
- Frequently updated
- By TJ Null (Community Manager)
- supports range of platforms
  - Vulnhub
  - Offsec proving grounds
  - HackTheBox

## JSONSec OSCP

- Created by JSON Sec
- contains boxes from
  - HackTheBox
  - TryHackMe
  - Offsec Proving Grounds
- also has Buffer Overflow exe

# Unofficial OSCP Approved Tools

- Note Taking
  - One Note
  - Obsidian
- Enumeration
  - AutoRecon
  - NmapAutomator
- Web
  - Gobuster
  - Feroxbuster
  - Wfuzz
  - Nikto



- Network
  - Impacket (SMB, psexec...)
- File transfer
  - Python (SimpleHTTPserver, updog)
  - Impacket (smbserver)
- Wordlists
  - Seclists
  - Rockyou.txt
- Reverse shell
  - Pentest Monkey
- Bruteforce
  - Hydra, ncrack, john

# Privilege Escalation



## Linux Privesc

- [Linux Exploit Suggester](#)
- [SUIDENUM](#)
- [LinEnum.sh](#)
- [linpeas.sh \(v3.1.3 or above\)](#)
- [Linprivchecker](#)
- [pSPY](#)

## Windows Privesc

- [WinPeas](#)
- [PowerUp](#)
- [Seatbelt](#)
- [Windows-Exploit-Suggester](#)
- [Sherlock](#)
- [Accesschk.exe](#)

# Buffer Overflows for OSCP

## TCM BUFFEROVERLOW

- comprehensive guide
- Compromise in 6 steps!
- Buffer Overflows - Adithyan's Blog

## TRYHACKME BOF PREP

- Created by Tib3rius
- the room uses a 32-bit Windows 7 VM
- 10+ OSCP like executables
- walkthrough

## MISC

- Exploit writing tutorial - Corelan
- SLmail
- FreeFloatFTP Server 1.0
- Minishare 1.4.1
- Savant 3.1

# PEN-200 PWK packages

PACKAGES 999\$ - 1350\$

- 30/60/90 days of lab access
- One exam attempt
- Self-guided

PWK 365 - 2148\$

- 365 days of lab access
- Two exam attempts
- Self-guided

OFFSEC ACADEMY

- 90 days of lab access
- One exam attempt
- 1:1 mentoring
- Small group instruction

# Comprehensive OSCP Journey (5 Months)

## Vulnhub

- 30 DAYS
- FREE

## HackTheBox / OSPG

- 30 DAYS
- 20 + 35\$

## OSCP Labs

- 90 DAYS
- 1350\$

Total : 1405\$

# Modest OSCP Journey (3 Months)

## Vulnhub

- 30 DAYS
- 500+ HOSTS
- FREE

## HackTheBox / OSPG

- 30 DAYS
- 150+ HOSTS
- 20 + 35\$

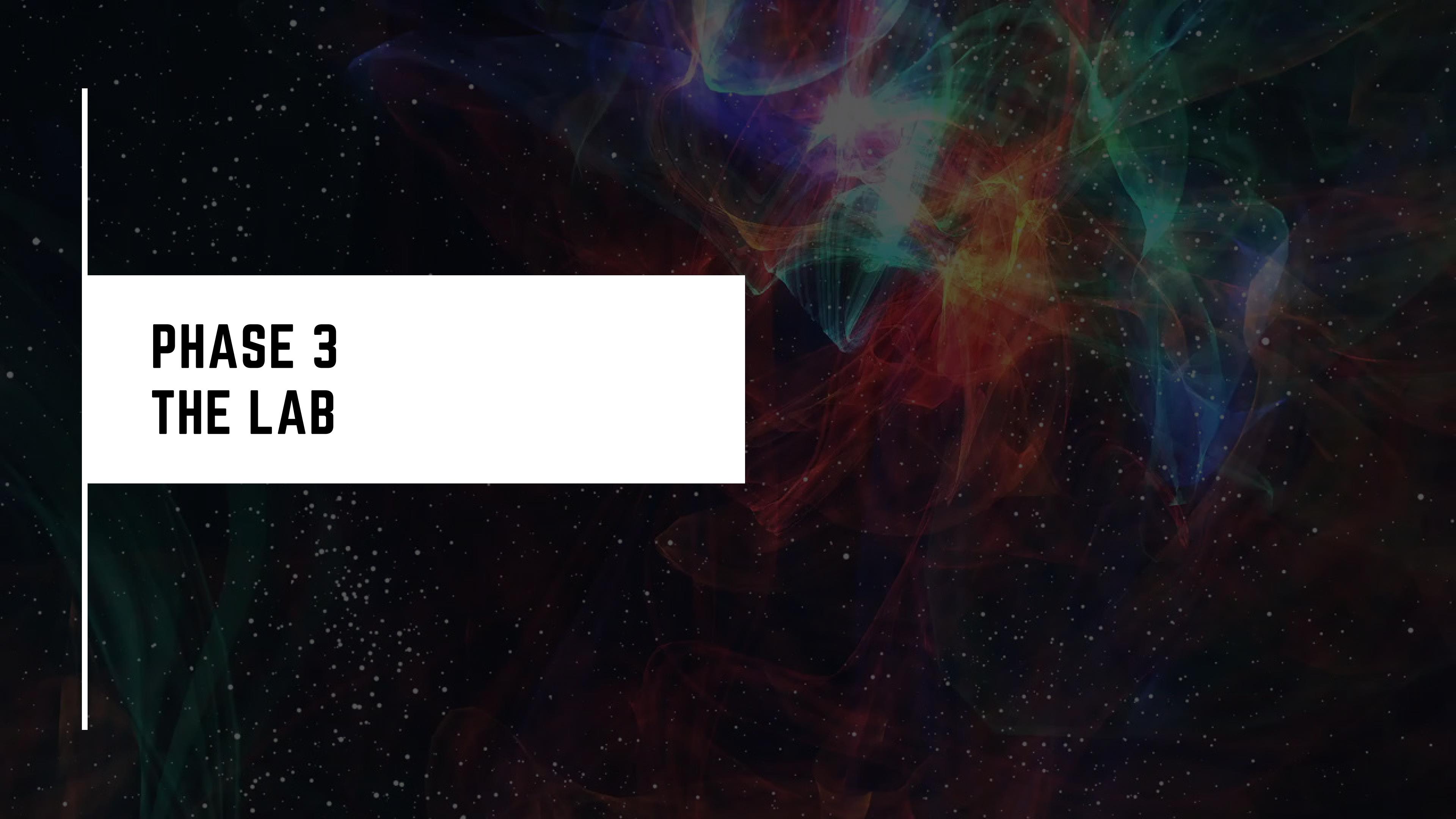
## OSCP Lab + Exam attempt

- 30 DAYS
- 70+ HOSTS
- 1000\$

Total : 1055\$

+ 2 attempt = 300\$

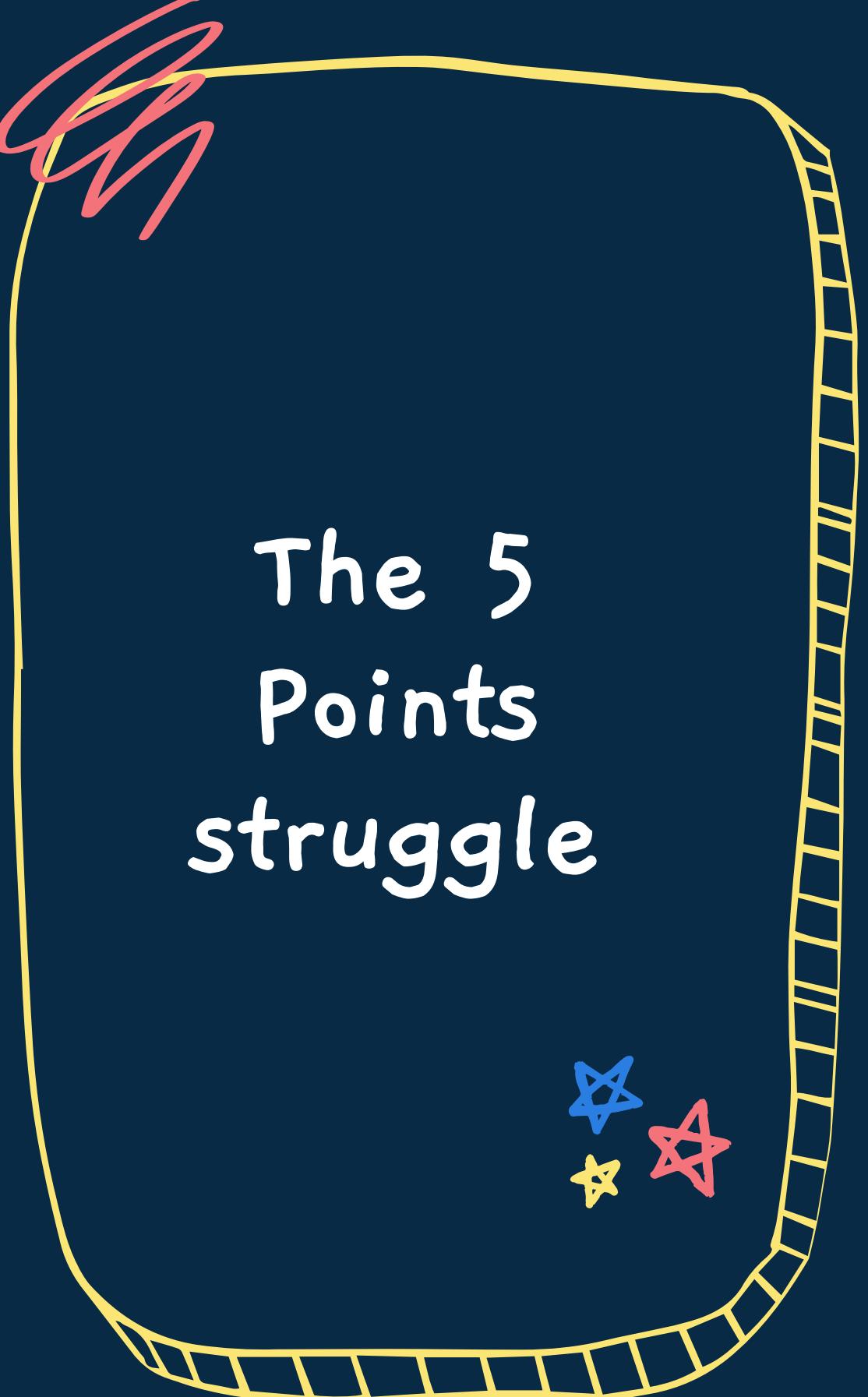
Total : 1355\$



# **PHASE 3 THE LAB**

Every Battle is won before it's fought

*Sun Tzu*



# The 5 Points struggle



ALL LAB EXERCISE + SCREENSHOTS



REPORT FOR MINIMUM 10 LAB HOSTS



40 (ISC)2 CPE CREDITS

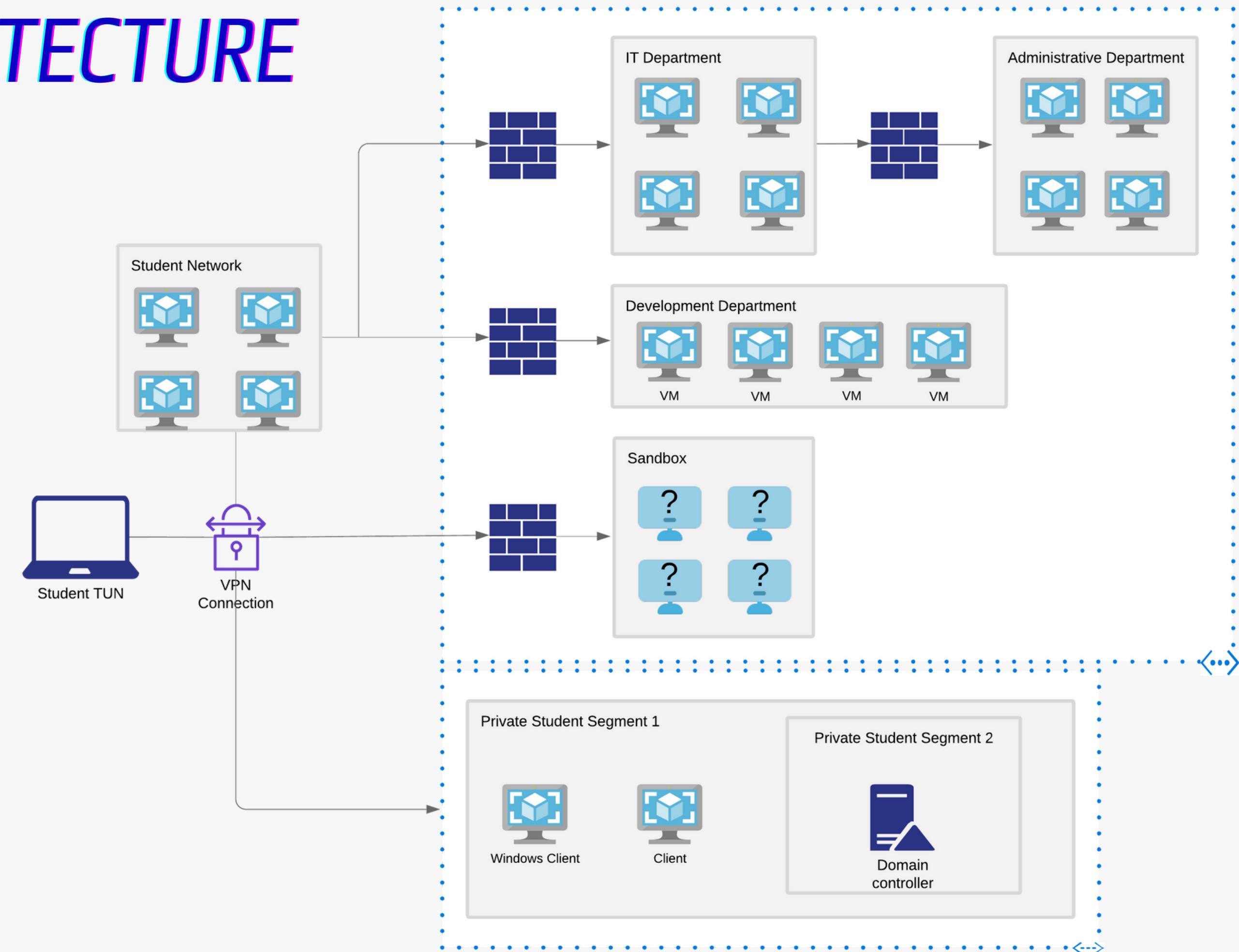


ONLY APPLICABLE IF YOU SCORE 65 POINTS



25 + 20 + 20

# LAB ARCHITECTURE



# OFFENSIVE SECURITY - LAB CONTROL PANEL: PUBLIC SERVERS

MY CLIENTS

PUBLIC SERVERS

SANDBOX

SUBNET KEYS

PROOF KEYS

LOGGED IN AS:

OS-[REDACTED]

EXAM DATE: NOT SCHEDULED

Set or change date

Your last exam date: Tue, 09 Jun 2020,  
04:20

You have 3 days of lab access, until Mon,  
10 Feb 2020, 10:16

Revert Machines

Select IP:

- ✓ 10.11.1.1 (last revert: 2 days)
- 10.11.1.2 (last revert: 8 days)
- 10.11.1.3 (last revert: 8 days)
- 10.11.1.4 (last revert: 8 days)
- 10.11.1.5 (last revert: 2 hours)
- 10.11.1.6 (last revert: 7 days)
- 10.11.1.7 (last revert: 7 days)
- 10.11.1.8 (last revert: 7 days)
- 10.11.1.9 (last revert: 2 hours)
- 10.11.1.10 (last revert: 2 hours)
- 10.11.1.11 (last revert: 2 hours)
- 10.11.1.12 (last revert: 2 hours)
- 10.11.1.13 (last revert: 7 days)

REVERT

Job Status:

READY

8 reverts left today. Counter resets at 0h00 GMT  
If you require more reverts, please email [help@offensive-security.com](mailto:help@offensive-security.com)



## MESSAGES

now



FBI

you've learned so much in the process. It's worth even to retake.

# Google

Am I ready to take OSCP ?



ALL

NEWS

VIDEOS

IMAGES

MAPS

# **PHASE 4 THE EXAM**



**OSCP EXAM DAY**

# PROCTORING



NO SCREEN RECORDING

SCREENSHOTS FTW

JANUS WEBRTC SCREENSHARING

DUAL SCREEN / CONNECTIVITY



OSCP HAS ALWAYS BEEN AN “OPEN BOOK” EXAM.  
WE ENCOURAGE YOU TO USE GOOGLE, YOUR  
NOTES, OR OTHER TOOLS AND THE PROCTOR WILL  
NOT DISQUALIFY YOUR EXAM FOR ANY OF THOSE  
REASONS OR FOR HAVING YOUR PHONE OR  
ANOTHER PERSON ENTER THE ROOM.

- OFFSEC

## LOGIN

---

OSID

MD5

**LOGIN**

**OFFENSIVE®  
security**

OFFENSIVE SECURITY OFFERS THE ONLY HANDS ON  
TRAINING AND TRUE PERFORMANCE BASED  
CERTIFICATIONS IN THE INDUSTRY.

Please enter only the numeric portion of your OSID. If you are unable to login and it is 15 minutes or less before your exam start time, please contact [proctoring@offensive-security.com](mailto:proctoring@offensive-security.com)

# PROOF Screenshot

```
C:\WINDOWS\system32>type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
type "C:\Documents and Settings\Administrator\Desktop\proof.txt"
529219186e355e0306e99b1d233dd234
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix . : localdomain
  IP Address . . . . . : 172.16.157.164
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 172.16.157.2

Ethernet adapter Bluetooth Network Connection:

  Media State . . . . . : Media disconnected

C:\WINDOWS\system32>
```

KALI LINUX

The quieter you become, the more you are able to hear.

Windows : type proof.txt && whoami && hostname && ipconfig  
Linux : cat proof.txt && whoami && hostname && ip addr

# EXAM CONTROL PANEL

192.168.38.111 ▾

Submit Proof Key

192.168.38.53

24cda78930bba2b80cca30aed6ffe92c

28/09/15 19:07:36 

192.168.38.53

24cda78930bba2b80cca30aed6ffe92c

28/09/15 18:49:49 

# Points Distribution



## 25 POINTS BOF

Straight forward, maximum 45 minutes with enough practice



## 25 POINTS HARD

rabbitholes, local.txt and proof.txt  
 $12.5 + 12.5 / 10 + 15$



## 20 POINTS MEDIUM

rabbitholes, local.txt and proof.txt



## 20 POINTS MEDIUM-HARD

rabbitholes, local.txt and proof.txt



## 10 POINT EASY

figure out the rabbit hole and you'll get the shell in minutes.  
No privesc.



## 5 POINT LAB

complete all lab exercises + 10 lab hosts

# EXAM TIMELINE

- 0 HOURS 30 MINUTES  
Buffer Overflow = 25 points
- 04 HOURS 01 MINUTES  
BOF + 25 = 50 points
- 05 HOURS 53 MINUTES  
BOF + 25 + 20 = 70 points
- 07 HOURS 23 MINUTES  
BOF + 25 + 20 + 10 = 80 points
- 12 HOURS 35 MINUTES  
BOF + 25 + 20 + 10 + 20 = 100 points



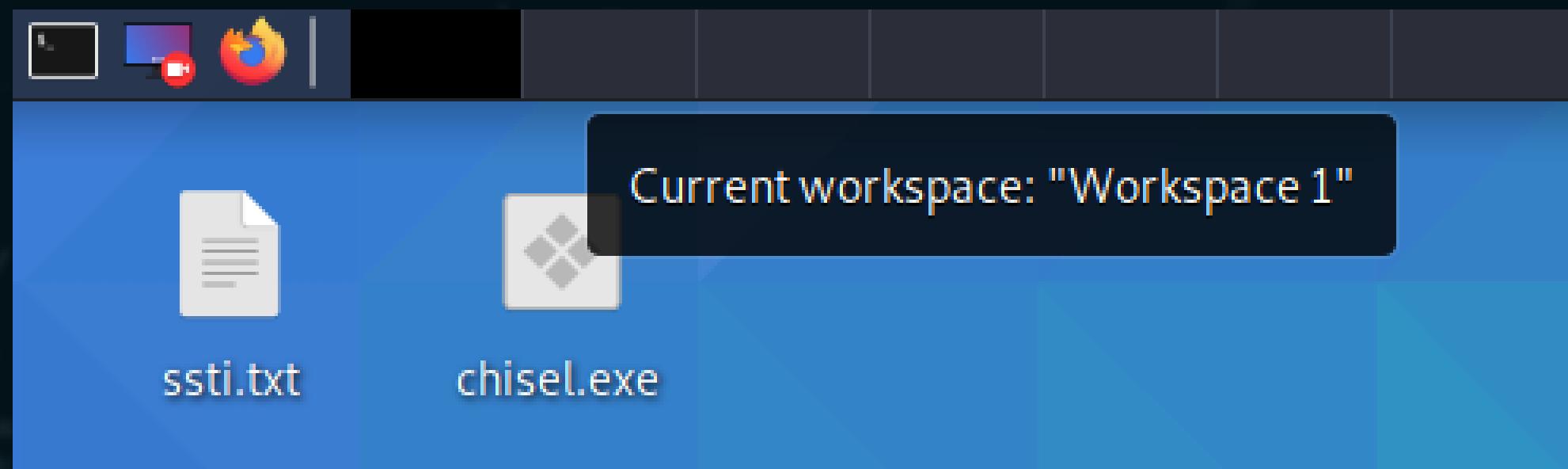
# Exam Setup

Workspace

5 machines + report + vpn

tools and locations

zshrc



# DEMYSTIFYING METASPLOIT RESTRICTIONS

- allowed to use on one target
  - Auxiliary, Exploit, and Post
  - Meterpreter payload
- unlimited to use
  - multi handler (aka exploit/multi/handler)
  - msfvenom
  - pattern\_create and pattern\_offset



# Wholesome Advice



- unlimited breaks
- skip after 2 hours
- 24 reverts
- All are intentionally vulnerable machines
- [ippsec.rocks](http://ippsec.rocks)

# **PHASE 5**

## **THE REPORT**

## 24 HOURS

More than enough to write your report

## SAMPLE REPORT & VIDEOS

- [OSCP Official sample report](#)
- [How to Write OSCP Report - Conda](#)
- [OSCP Report made easy - Michael LaSalvia](#)
- [Writing a Pentest Report - TheCyberMentor](#)

## SCREENSHOTS!

include as much screenshots as possible

## COMPREHENSIVE

include all steps, commands and output

# Reporting

# Exploit Code

- THE MODIFIED EXPLOIT CODE
- THE URL TO THE ORIGINAL EXPLOIT CODE
- THE COMMAND USED TO GENERATE ANY SHELLCODE (IF APPLICABLE)
- HIGHLIGHTED CHANGES YOU HAVE MADE
- AN EXPLANATION OF WHY THOSE CHANGES WERE MADE

# Takeaway

OSCP is not an exam. It's a journey. Cherish your way  
into it.

# FAQ



## IS PROGRAMMING SKILLS MANDATORY?

Recommended, but not mandatory.

## WHAT SCRIPTING KNOWLEDGE IS NEEDED, TO WHAT EXTENT

Python and Bash

## HOW MANY HOURS PER DAY DID YOU SPEND?

4-6 hours/day for 2 months

16 Hours/day for a month

# Shoot your Queries

 [akoffsec](#)

 [root@adithyanak.com](mailto:root@adithyanak.com)

 [akoffsec](#)

 [akoffsec](#)

 [akoffsec](#)

 [Adithyan AK](#)

 [adithyanak.com](http://adithyanak.com)

 [adithyan\\_ak](#)