

Offensive Security OSCP Exam with AD Preparation

Michael Mancao

February 22, 2022



Agenda

- OSCP Exam Changes
- OSCP Exam Preparation
- OSCP Exam Tips
- OSCP Exam Scheduling
- Proctoring Process
- QA

OSCP Exam Changes

OSCP Exam Structure

POINTS	NUMBER OF MACHINES	NOTES
60 points	3 independent targets	<ul style="list-style-type: none">• 2-step targets (low and high privileges)• Buffer Overflow may (or may not) be included as a low-privilege attack vector.• 20 points per machine<ul style="list-style-type: none">◦ 10 points for low-privilege◦ 10 points for privilege escalation
40 points	2 clients 1 domain controller	<ul style="list-style-type: none">• NEW: Active Directory set.• Points are awarded only for the full exploit chain of the domain.• No partial points will be awarded.

10 Bonus Points Requirements

- Complete the lab report AND the course exercises*
- Lab report must contain 10 fully compromised machines in the labs.
- All vulnerabilities exploited in the lab report must be unique.
- After **March 14, 2022**, lab reports must also include the full exploitation of an Active Directory set in the labs.

Approaching the Exam

Attempt Active Directory

- AD gives you 40 points. You can be flexible on how to get the 30 points:
 - AD + 1 stand-alone + lab report
 - AD + 2 stand-alone machines
 - AD + 1 stand-alone machine + partial points
- You must you get all 3 AD machines, no partial points are awarded for this challenge.

Stand-Alone Machines along w/ Lab Report

- Skip AD and focus on the 3 stand-alone machines w/ lab report.
- No room for error, as this gives a maximum of 70 points.

OSCP Exam Preparation

Study Approach



1 Go over course materials for each module

- Read PDF and watch videos
- Practice the course lessons with your client and lab machines
- Take notes!

2

Complete exercises for each module

- Complete [Topic Exercises](#)
- Document your PDF exercises*
- Try the "Extra Mile" exercises

3 Start exploiting labs!

- Learning Path [Blog Post](#) & [Article](#)
- Exploit lab machines
- Create a lab report
- Simulate a practice exam

Course Materials & Exercises

- **The course materials and exercises are not a waste of lab time!**
 - Builds solid understanding of the fundamental concepts and techniques.
- **Your assigned machines are extremely valuable.**
 - Allows you to directly observe attacks on your machine.
 - Gives you a user/admin perspective to better understand the target.
 - The Windows Client and Server are a mini-AD environment.
- **Exercises are great for practicing and for bonus points on the exam.**
 - Complete the Topic Exercises & PDF Exercises.
 - Try the Extra Miles.

Start Exploiting the Labs!

1. To get started, read the [PWK Labs Learning Path](#):

- Walkthroughs for Alpha and Beta lab machines.
- Hints for 9 additional lab machines.

2. Build your methodology using the walkthroughs.

- The write-ups detail the techniques, methodology, and thought process used to exploit Alpha and Beta.
- Refine and practice your methodology on 9 lab machines with hints.
- Continue exploiting the “low-hanging fruit” in the labs.

Find and Exploit AD Lab Machines

- **Post-exploitation is as important as initial enumeration.**
 - Unlike stand-alone machines, AD needs post-exploitation.
 - Practice by finding dependencies between AD lab machines.
- **There are a total of 2 AD sets in the labs. It is up to you to find them.**
 - Enumerate and attack the 2 domains along with the sandbox.local domain from the course materials.
 - Try different tools for AD enumeration and exploitation.

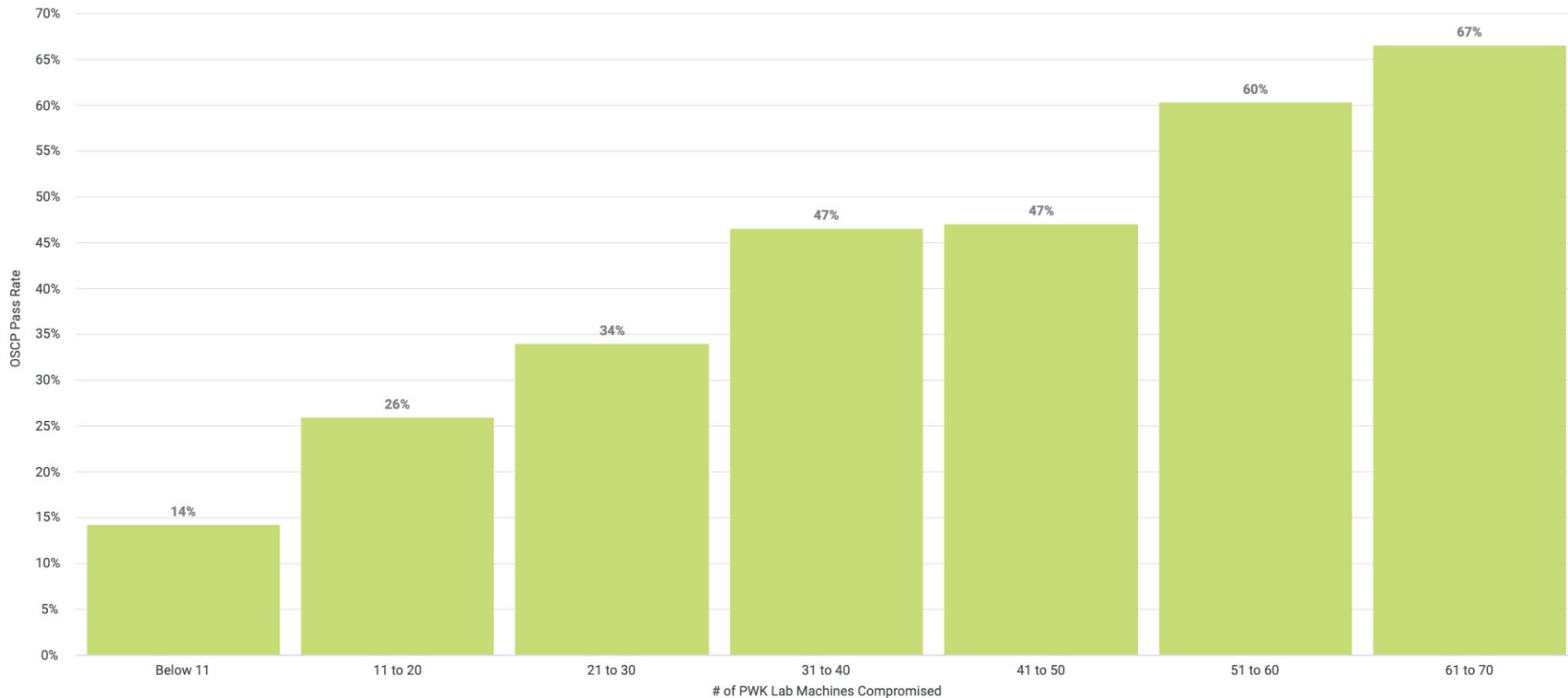
Practice, Practice, Practice!

Practice as many machines as you can on all 3 lab networks.

- Exploit all machines in the public network.
- Pivot and exploit machines in IT, Dev, and Admin networks.
 - *Pivoting is now important with the addition of the AD set.*
- Try to exploit a machine using multiple approaches and/or techniques.
- Re-do exercises and lab machines that presented challenges.
- Avoid relying on hints and walkthroughs.

Lab Machines Key to Success

Higher exam pass rate with >50 lab machines completed



Simulate a Practice Exam Environment

- **Prepare 3 machines and an AD set from the PWK labs.**
 - Try to select stand-alone machines you have not worked on yet.
 - Prepare a script to directly reach IT/Dev/Admin machines you selected.
 - If you have already finished all AD sets, redo it without looking at notes.
 - Practice your report writing skills after exploiting machines
- **Repeat the exam environment to build confidence.**
 - Familiarity with time constraints will help you stay calm and centered.
 - Remember, the exam is just another day in the labs.

Time Management

Avoid rabbit holes

- Set a timer per machine:
 - I.e. 2-3 hours per stand-alone machine and 4 hours for the AD set.
 - The 4 hours can be broken down for each AD machine.
- After getting a shell, allot another two hours for privilege escalation.
- If time runs out, move on. It's easy to get lost in troubleshooting.
- Working on a different machine or taking a break lets you to come back with a fresh perspective.

Time Management

Schedule your breaks

- The 24 hours is not just for hacking machines.
 - Schedule time for breaks, eating, and sleeping.
 - Stick to your schedule. Fatigue and hunger will slow you down.
- Take a step back or a short break after your 2-3 hour allotted machine time.

Don't Panic

- There is more than enough time to finish the exam.
- If you need to work for 24 hours, you need more preparation.

Reporting

- Document your exercises and lab report with the [exam report requirements](#).
 - This will be good practice for writing your exam report.
 - This will also help give you bonus points during the exam.
- **Prepare a report template prior to your exam.**
 - Updated lab & exam report template: [Pen-200 Reporting Requirements](#).
 - The template gives you a direction on what to document.

OSCP Exam Tips

Read the Exam Control Panel

1. Read the instructions for each machine before you start.

- It will give you an idea on the structure of the AD set.
- It will be evident if there is a buffer overflow machine assigned to you.

2. Plan based on the objectives outlined in your Control Panel.

- Identify whether you will start with AD set or stand-alone machines.
- Format your report template in line with the requirements of each machine.

Enumeration Tips

Initial Enumeration

- Perform light scans on your targets .
 - E.g. scan for 10 common ports on your exam machines.
 - Manually interact with services found while waiting for thorough and longer scans.

Enumerate carefully

- Avoid heavy scans on multiple targets.
- Revert machines after running unsafe scans.
- Re-run scans to ensure all information are correct. *Scans can be inaccurate.*
 - Use various tools to verify scan outputs.

Enumeration Tips

Enumeration is a cyclical approach

- After gaining new access, enumerate again in the context of your new privileges.
 - If you gain login access to a webpage, enumerate the webapp as that user
 - If you gain domain user access to a machine, enumerate the domain as that user.
- This concept often overlooked.
 - Students tend to stop enumerating after getting a shell/root access.

Exploitation Tips

Make sure to read exploits prior to using them.

- Do you need to set up files or permissions prior to running the exploit?
- Do you need to modify the exploit to match your target?

Check multiple exploits for the same vulnerability.

- Exploits may use different methods to exploit vulnerabilities.
- Some exploits might be compatible/incompatible with your target.

Active Directory Tips

AD Enumeration

- AD initial enumeration and exploitation is similar to stand-alone machines.
- Identify machine's role (DC/client) and the services present.
- Identify the initial target into the domain (the low-hanging fruit).

AD Exploitation

- Have a [cheatsheet](#) of AD commands.
 - Be thorough for enumeration, exploitation, and post exploitation.
- Do not ignore standard enumeration, check applications and non-AD related services.
- Try using information you obtained on multiple domain machines

Document & Backup!


- Document all commands, outputs, scripts, and code you use.
 - Use terminal loggers to automatically log all commands and outputs in your shell.
- Take snapshots and backups of your work.
- Ongoing documentation saves time from rerunning any commands if you need the outputs again.

Exam Scheduling

Schedule your Exam

- Schedule your exam several weeks prior.
 - We recommend at least 3 weeks before the desired date.
 - You can reschedule your exam up to 3 times.
 - You can reschedule your exam up to 48 hours prior to exam start time.
- Be mindful of the time and timezone (e.g., GMT).
 - If you do not arrive within 1 hour of your exam start time, your exam will be cancelled.

Exam Scheduling

**OFFENSIVE**
security

COURSES

PROVING GROUNDS

Connect to Discord | Help

D Demo_user

PROVING GROUNDS

PLAY PRACTICE

Search by name

Start Kali

Connect to VPN

3:00 h left for today. Need more? Subscribe.

ACTIVITY MY LOGS

ALL WARM UP GET TO WORK TRY HARDER

NAME	POINTS	DIFFICULTY	LAST ACTION	PROGRESS
BrokenGallery	8	Intermediate	Never	
Funbox	8	Intermediate	Never	
SunsetMidnight	8	Intermediate	Never	
SunsetDecoy	5	Easy	Never	
HAWordy	8	Intermediate	Never	
Sar	5	Easy	Never	
Dawn2	8	Intermediate	Never	
InsanityHosting	10	Hard	Never	
BBSCute	5	Easy	Never	
Fowsniff	5	Easy	Never	
PyExp	5	Easy	Never	
FunboxEasyEnum	5	Easy	Never	
InfosecPrep	5	Easy	Never	
Vegeta1	5	Easy	Never	

⊕ Gaara was stopped

OrianeUAT 15 hours ago

⊕ Gaara was started

OrianeUAT 15 hours ago

⊕ Geisha was stopped

n.ayyachamy 15 hours ago

⊕ Geisha was started

n.ayyachamy 15 hours ago

⊕ InsanityHosting was stopped

n.ayyachamy+1 16 hours ago

⊕ Funbox was stopped

n.ayyachamy+1 16 hours ago

⊕ Funbox was started

n.ayyachamy+1 16 hours ago

⊕ Funbox was stopped

n.ayyachamy+1 16 hours ago

⊕ Funbox was started

n.ayyachamy+1 16 hours ago

⊕ InfosecPrep was stopped

octavia311PG 21 hours ago

Exam Confirmation Email

“Penetration Testing with Kali Linux - Proctored Certification Exam Confirmation - OS-XXXX” email contains:

- How to start the exam and login to the proctoring tool.
- Technical requirements to take the proctored exam.
- Exam proctoring rules.
- Instructions on how to submit your exam report.

Exam Logistics & Proctoring

Exam Logistics

- Identify where you intend to take the exam.
- Check government cybersecurity laws. Some countries have strict firewall restrictions.
- Prepare backup Internet connection in case of emergencies.
- Check for scheduled power outages in your area.
- Prepare food and snacks for the 24 hour exam.
 - *Water is critical, remain hydrated.*
- If other people will be in the room during the exam, inform them regarding the exam protocol.

Proctoring Requirements

Technical Requirements

- Proctoring technical requirements are outlined [here](#).
- Schedule a [test session](#) if you are using a Linux variant.

ID requirements

- Valid government-issued ID in english.
 - Contains your full name, photo, birthdate, country, issue and expiry date.
- Prepare a scanned copy in case your ID is not clear in the camera.

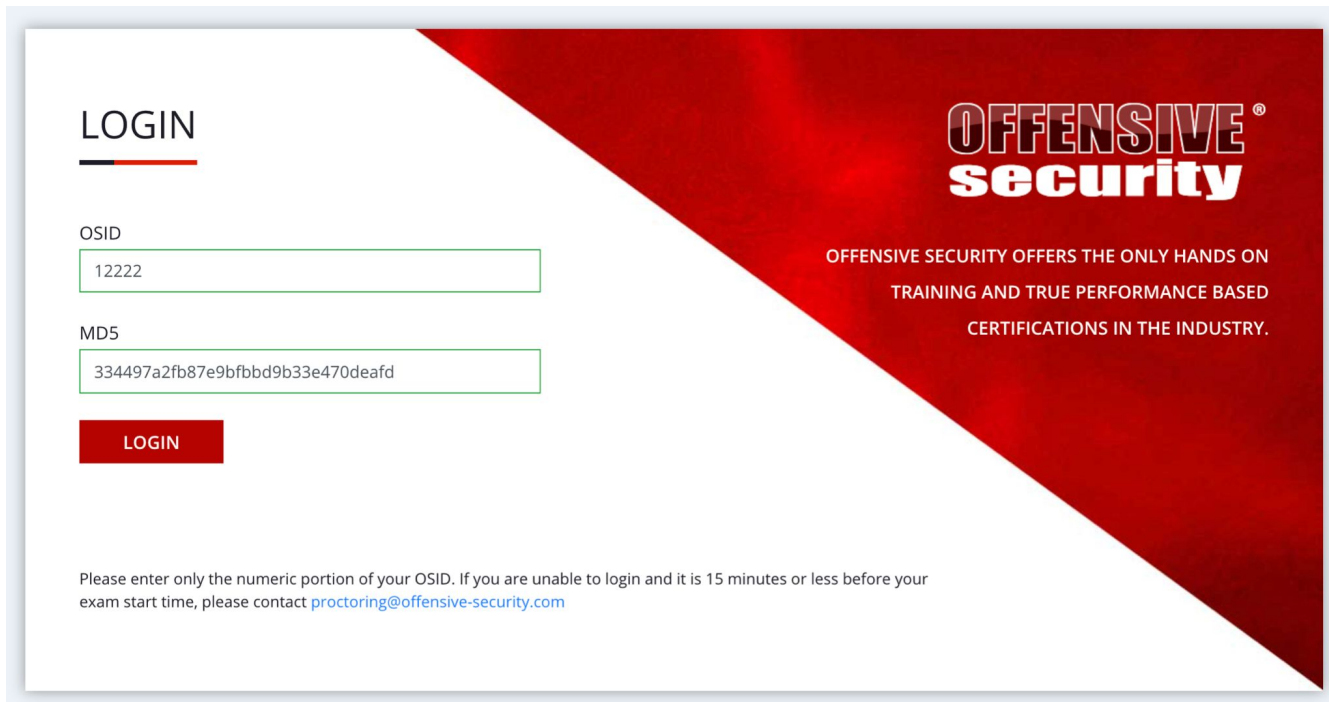
Mentally Prepare Yourself

- **Be confident in the preparation you completed.**
 - Remember, the exam is just another day in the labs.
- **Be calm and avoid worrying about the exam.**
 - Try eating out or going to the gym (activities that relax your mind).
- **Be healthy.**
 - Get plenty of sleep and rest, stay hydrated.

During the Exam

Proctoring Process

Proctoring process can start 15 minutes before your exam time.

The image is a screenshot of the Offensive Security login interface. It features a white background on the left and a red background on the right, separated by a diagonal line. The 'OFFENSIVE security' logo is in the top right. The login form on the left includes fields for OSID (containing '12222') and MD5 (containing a long alphanumeric string), a 'LOGIN' button, and a footer with contact information.

LOGIN

OSID

12222

MD5

334497a2fb87e9bfbdbd9b33e470deafd

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

Overcoming Stress & Anxiety

- If you are panicking, take a moment to stop and collect yourself.
 - Do activities that calm you like meditating or taking a walk.
- Stick to your time schedule.
 - As long as there is time, keep working.
 - Many students finish exams in buzzer beaters.
- It's ok if you don't do well.
 - Many OffSec employees had multiple attempts.
 - You will also learn and gain the exam experience.

Before Ending the Exam

- Double check the exam requirements.
- Review and finalize all of your notes.
- Make sure you have captured all the necessary screenshots and proofs.
- If you have the time, re-exploit machines after a revert.
 - Ensures your steps results are correct.
 - Double check proofs and screenshots are correct.

Contact Protocol

- **For connectivity issues & issues with machines, contact us immediately.**
 - Chat: <https://chat.offensive-security.com>
 - Email: help@offensive-security.com
- **OffSec Student Mentors (SMs) will not assist with exam objectives.**
 - However, reach out if you feel overwhelmed or need a sounding board.

Post Exam

Writing your Report

- **Get sleep & refresh your mind.**
 - You have 24 hours for the report, there is time to rest.
- **Take the time to write a detailed report.**
 - The report is important, it is the product you are delivering to the client.
 - It should be organized, professional and will be clearly understood.
- **Proofread your report.**
 - Double check if the necessary screenshots and proof files are present and correct.
 - We do not accept changes or updates to submitted reports.

Upload Login Page


Upload Exam Report

OS-ID

MD5

☐

I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Continue

Please make sure to use the MD5 hash provided in your exam email to login.

Upload Report Page

Upload Exam Files

The documentation requirements are very strict and failure to provide sufficient documentation will result in reduced or zero points being awarded. Please note that once your exam and lab report is submitted, your submission is final. If any screenshots or other information is missing, you will not be allowed to send them and we will not request them.

We only accept one .7z file with maximum size of 300MB and 400MB for the PDF documents.

For more information regarding submission instructions, please visit the Exam Guide.

- OSCP: <https://help.offensive-security.com/hc/en-us/articles/360040165632-OSCP-Exam-Guide>
- OSCE: <https://help.offensive-security.com/hc/en-us/articles/360046801331-OSCE-Exam-Guide>
- OSWE: <https://help.offensive-security.com/hc/en-us/articles/360046869951-OSWE-Exam-Guide>
- OSWP: <https://help.offensive-security.com/hc/en-us/articles/360046904731-OSWP-Exam-Guide>
- OSEE: <https://help.offensive-security.com/hc/en-us/articles/360046458732-OSEE-Exam-Guide>
- OSEP: <https://help.offensive-security.com/hc/en-us/articles/360050293792-OSEP-Exam-Guide>
- OSed: <https://help.offensive-security.com/hc/en-us/articles/360052977212-OSed-Exam-Guide>

SELECT FILE

Double Check the MD5 Hash

```
root@kali:~# md5sum OSCP-OS-XXXXX-Exam-Report.7z  
f7feecea01ac1eca9ee522906b087d5e OSCP-OS-XXXXX-Exam-Report.7z
```

1. After uploading your report, upload.offsec.com will provide the MD5 hash of your report.
2. Compare MD5 hash of the uploaded file with your local copy.
3. If the values do not match, your file did not upload successfully.

Additional Resources

OSCP Exam Resources

OSCP Exam Resources:

- [What to Expect From the New OSCP Exam](#)
- [OSCP Exam Change](#)
- [PEN-200 Reporting Requirements](#)
- [OSCP Exam Guide](#)
- [Important information about exam scheduling in the Training Library](#)
- [Proctoring Tool Student Manual](#)

Support Channels

What Do You Need?	Students
Exam scheduling	orders@offensive-security.com
Proctoring	proctoring@offensive-security.com
VPN connectivity issues	https://chat.offensive-security.com/ or email help@offensive-security.com
Exam machine testing	
Non-technical exam related inquiry	challenges@offensive-security.com

Q & A

Good Luck!