OSCP Certification Exam Guide

Updated: 20 November 2018

Please read this entire document carefully before beginning your exam!

Introduction

This guide explains the objectives of the Offensive Security Certified Professional (OSCP) certification exam. Section 1 describes the requirements for the exam, Section 2 provides important information and suggestions, and Section 3 specifies instructions for after the exam is complete.

The OSCP certification exam simulates a live network in a private VPN, which contains a small number of vulnerable machines.

You have 23 hours and 45 minutes to complete the exam.

This means that if your exam begins at 09:00 GMT, your exam will end at 08:45 GMT the next day.

Once the exam is finished, you will have another 24 hours to send your documentation to the Offensive Security Challenges Department. Details on how to submit your files are provided below.

All OSCP exams are now proctored. Please make sure to read our online FAQ at the following URL: https://support.offensive-security.com/proctoring-faq

Section 1: Exam Requirements

The exam consists of several target machines that must be compromised. Some of the machines will require multiple exploitation steps, resulting first in low-level local access, and then in root or administrative privilege escalation. Other machines will be fully exploitable remotely. Specific instructions for each target will be located in your Exam Control Panel, which will only become available to you once your exam begins.

Documentation Requirements

You are required to write a professional report describing your exploitation process for each target. You must document all of your attacks including all steps, commands issued, and console output in the form of a penetration test report. Your documentation

should be thorough enough that your attacks can be replicated step-by-step by a technically competent reader.

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.

Exploit Code

If you have not made any modifications to an exploit, you should only provide the URL where the exploit can be found. Do not include the full unmodified code, especially if it is several pages long.

If you have modified an exploit, you should include:

- 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

Exam Proofs

Your objective is to exploit each of the target machines and provide proof of exploitation. Each target machine contains at least one proof file, which you must retrieve, submit in your control panel, and include in a screenshot with your documentation. **Failure to provide the appropriate proof files in a screenshot for a given level of access will result in zero points being awarded for the target.**

You must provide the contents of the proof files in an interactive shell on the target machine with the `type` or `cat` command from their original location. **Obtaining the contents of the proof files in any other way will result in zero points for the target machine; this includes any type of web-based shell.**

On all Windows targets, you must have a shell running with the permissions of one of the following to receive full points:

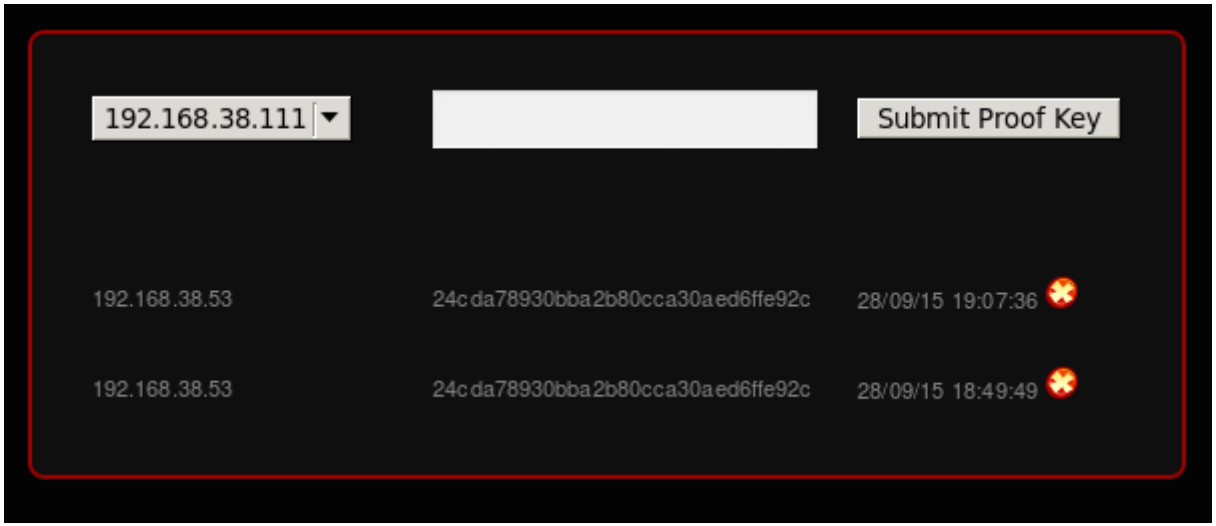
- SYSTEM user
- Administrator user
- User with Administrator privileges

On all Linux targets, you must have a root shell in order to receive full points.

Control Panel Submission

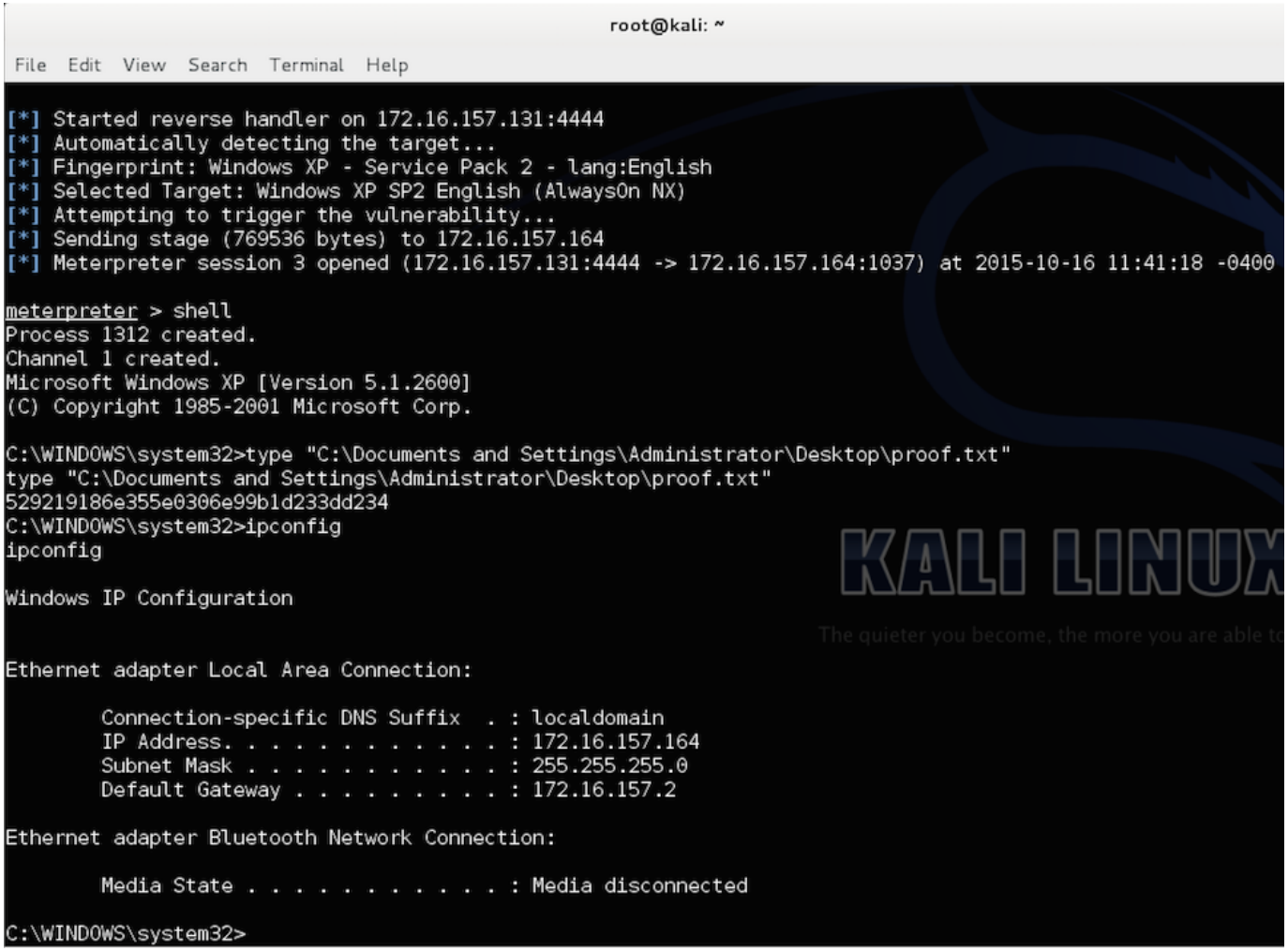
The exam control panel contains a section available to submit your proof files. The contents of the local.txt and proof.txt files obtained from your exam machines *must be submitted in the control panel before your exam has ended.* Note that the control panel will

not indicate whether the submitted proof is correct or not. An example of this is provided below:



Screenshot Requirements

Each local.txt and proof.txt found must be shown in a screenshot that includes the contents of the file, as well as the IP address of the target by using `ipconfig` or `ifconfig`. An example of this is shown below:



Exam Restrictions

You cannot use any of the following on the exam:

- Spoofing (IP, ARP, DNS, NBNS, etc)
- Commercial tools or services (Metasploit Pro, Burp Pro, etc.)
- Automatic exploitation tools (e.g. db_autopwn, browser_autopwn, SQLmap, SQLninja etc.)
- Mass vulnerability scanners (e.g. Nessus, NeXpose, OpenVAS, Canvas, Core Impact, SAINT, etc.)
- Features in other tools that utilize either forbidden or restricted exam limitations

Any tools that perform similar functions as those above are also prohibited. You are ultimately responsible for knowing what features or external utilities any chosen tool is using. The primary objective of the OSCP exam is to evaluate your skills in identifying and exploiting vulnerabilities, not in automating the process.

You may however, use tools such as Nmap (and its scripting engine), Nikto, Burp Free, DirBuster etc. against any of your target systems.

Please note that we will not comment on allowed or restricted tools, other than what is included inside this exam guide.

Metasploit Restrictions

The usage of Metasploit and the Meterpreter payload are restricted during the exam. You may only use Metasploit modules (**Auxiliary, Exploit, and Post**) or the Meterpreter payload against **one** single target machine of your choice. Once you have

selected your one target machine, you cannot use Metasploit modules (Auxiliary, Exploit, or Post) or the Meterpreter payload against any other machines.

Metasploit/Meterpreter **should not** be used to test vulnerabilities on multiple machines before selecting your one target machine (this includes the use of **check**) . You may use Metasploit/Meterpreter as many times as you would like against your one target machine.

If you decide to use Metasploit or Meterpreter on a specific target and the attack fails, then you **may not** attempt to use it on a second target. In other words, the use of Metasploit and Meterpreter becomes locked in as soon as you decide to use either one of them.

You may use the following against all of the target machines:

- multi handler (aka exploit/multi/handler)
- msfvenom
- pattern_create.rb
- pattern_offset.rb

All the above limitations also apply to different interfaces that make use of Metasploit (such as Armitage, Cobalt Strike, Metasploit Community Edition, etc).

Section 2: Exam Information

Exam Connection

Your connection to the exam is to be done with Kali Linux using OpenVPN. Your exam connection pack and details will be sent by email at the exact start time of your exam and not in advance.

1) Download the exam-connection.tar.bz2 file from the link provided in the exam email to your Kali machine.

2) Extract the file:

```
root@kali:~# tar xvfj exam-connection.tar.bz2
OS-XXXXX-OSCP.ovpn
```

3) Initiate a connection to the exam lab with OpenVPN:

```
root@kali:~# openvpn OS-XXXXX-OSCP.ovpn
```

4) Enter the username and password provided in the exam email to authenticate to the VPN:

```
root@kali:~# openvpn OS-XXXXX-OSCP.ovpn
OpenVPN 2.3.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH] [IPv6] built o
Enter Auth Username: OS-XXXXX
Enter Auth Password: XXXXXXXXXX
Thu Mar 18 21:22:06 2016 WARNING: No server certificate verification method has been enabled
Thu Mar 18 21:22:06 2016 LZO compression initialized
Thu Mar 18 21:22:06 2016 UDPv4 link local: [undef]
Thu Mar 18 21:22:06 2016 UDPv4 link remote: x.x.x.x:1194
Thu Mar 18 WARNING: this configuration may cache passwords in memory
Thu Mar 18 [127.0.0.1] Peer Connection Initiated with x.x.x.x:1194
Thu Mar 18 21:22:07 2016 TUN/TAP device tap0 opened
Thu Mar 18 /sbin/ifconfig tap0 192.168.xx.xx netmask 255.255.254.0 mtu 1500
Thu Mar 18 21:22:07 2016 Initialization Sequence Completed
```

Exam Control Panel

The exam control panel is available via a link provided in your exam email. Through the exam control panel you will be able to:

- Submit proof files
- Revert target machines
- View specific target objectives and point values

Machine Reverts

You have a limit of 24 reverts. This limit can be reset once during the exam. All of the machines have been freshly reverted at the start of your exam so you will not be required to revert the machines when you begin. Please wait patiently for the machine

to revert and only click the button once per attempt. Note that reverting a target machine will cause it to return to its original state and any changes you have made to the machine will be lost.

Exam Proof Filenames

- proof.txt - This file is only accessible to the root or Administrator user and can be found under the **/root/** directory or the **Administrator Desktop.** This file is available on every target machine.
- local.txt - This file is accessible to an un-privileged user account and can only be found on certain machines. The targets containing these files are detailed in your control panel.

Point Allocation

- The order in which the exam machines are documented inside your exam report is the same order in which the exam machines will be graded and valued
- Points will be awarded for partial and complete administrative control of each target machine
- Each machine has a specific set of objectives that must be met in order to receive full points
- You must achieve a minimum score of 70 points to pass the exam
- It is possible to achieve a maximum of 100 points on the exam
- Specific objectives and point values for each machine are located in your exam control panel

Point Disqualification

You will receive no points for a specific target for the following:

- Using a restricted tool

- Using Metasploit Auxiliary, Exploit, or Post modules on multiple machines
- Using the Meterpreter payload on multiple machines
- Failure to provide the local.txt and proof.txt file contents in both the control panel and in a screenshot

Suggested Documentation Templates

Ideally, one of the following templates should be used for the penetration test report:

- https://www.offensive-security.com/pwk-online/PWKv1-REPORT.doc (Microsoft Word)
- https://www.offensive-security.com/pwk-online/PWKv1-REPORT.odt (OpenOffice/LibreOffice)

You may use your own template as long as the information is presented in a structured, professional manner and follows all other requirements outlined above.

Bonus Points

Five bonus points may be earned by submitting your lab report and course exercises.

- In order to receive five bonus points, you must complete the lab report AND the course exercises
- The lab report must be submitted in a separate PDF file, archived with your exam report. Failure to submit the file in the correct format will result in 0 bonus points being awarded. See below for additional details
- The lab report must contain a description of your attack steps for no less than 10 fully compromised unique machines

- All Information provided regarding the machines' configurations or exploits used must be correct
- Each machine's proof.txt must be shown in a screenshot that includes the contents of the file, as well as the IP address of the target by using `ipconfig` or `ifconfig`
- Machines which are clones may only be used once
- `Offensive Security Complete Guide` machines may not be included in your report: Alpha (https://forums.offensive-security.com/showthread.php?t=4689)
- All vulnerabilities exploited within the lab report must be unique. You may not use the same exploit against multiple machines
- You must successfully attack ten different targets. Documenting multiple attack vectors for the same machine will not grant additional points.
- The course exercises must be appended to the end of your lab report
- The course exercises must ALL be complete and correct, with the exception of those which explicitly state otherwise

For more information about PWK reporting requirements, please refer to the PWK Reporting page (https://support.offensive-security.com/pwk-reporting).

Internet Connection Issues

This subsection of the exam guide documents what you should do in case you are unable to complete your exam due to severe external factors. Please make sure to read and understand it carefully.

The exam lab is a dedicated environment with no students connected other than yourself. The total allotted time of 23:45 hours *does* take life and its situations into consideration:

- You are expected to take rest breaks, eat, drink and sleep
- You are also expected to have a contingency plan in the event that there is an issue outside your control. (e.g. make sure you have access to a backup Internet connection)

If you have a legitimate issue, please send an email with your OSID to “challenges AT offensive-security DOT com” immediately. Make sure to include all the necessary details and supporting information such as a letter from your power company, ISP or any other relevant documentation.

Please note we are only able to extend the lab time if the issues were present on our side and only when the exam subnet is not immediately in use by another student following your exam. In the event of an issue on our side and the exam subnet is scheduled immediately following your exam we will provide a free exam retake attempt. We work very hard to ensure our environments are highly available and issues are very rare.

Contact Protocol

If you encounter any connectivity problems with the VPN or target machines, inform us immediately. The preferred method of contact is through the live chat available at https://support.offensive-security.com/chat.php or via email to “help AT offensive-

security DOT com”.

Please note that we will not be able to assist with, or give hints on, any exam objectives and will only be available for technical problems during the exam.

All questions related to the exam documentation and submission, or other non-technical exam related issues should be sent to “challenges AT offensive-security DOT com". The live chat administrators will NOT BE ABLE TO HELP you with exam-related queries unless you are having technical issues with the VPN connection or exam environment.

Section 3: Submission Instructions

Submission Checklist:

- ☑ Your exam is in PDF format
- ☑ Your PDF has been archived into a password-protected .7z file
- ☑ You used your OSID as part of the name of your .7z file
- ☑ You have uploaded your .7z file to https://upload.offsec.com
- ☑ You have emailed the link from the upload page to "oscp AT offensive-security DOT com"

The following subsections provide details on each of these requirements.

Submission Format and Name

Your exam report must be submitted in PDF format. No other formats will be accepted. If you submit your report in another format, we will not request or remind you to send a PDF and your exam report will not be scored.

Before submitting your exam report, please review the PDF document to ensure it appears as it did in the previous file type and that there are no formatting errors.

Use the following format for the file name: “OSCP-OS-XXXXX-Exam-Report.pdf”, where "OS-XXXXX" is your OSID.

If you are submitting a lab report as well, you may use the following format for the file name: "OSCP-OS-XXXXX-Lab-Report.pdf".

Archive File

You must submit your documentation in a password-protected .7z file, using your OSID as the password with the format “OS-XXXXX”. This can be accomplished with: 7z a -p

```
root@kali:~# 7z a OSCP-OS-XXXXX-Exam-Report.7z -pOS-XXXXX OSCP-OS-XXXXX-Exam-Report.pdf

7-Zip 9.20  Copyright (c) 1999-2010 Igor Pavlov  2010-11-18 p7zip Version 9.20 (locale=en_US

Scanning

Updating archive OSCP-OS-XXXXX-Exam-Report.7z


Everything is Ok
```

Submission Upload

Please submit your .7z file via https://upload.offsec.com and follow the provided instructions in order to upload your archived exam report. No other download links (including ExpireBox, Dropbox, Google Drive, personal webserver, etc) will be accepted. Please note that only archived files are permitted.

After the file has been submitted, you will be presented with a “File uploaded!” page where a link to your exam report will be displayed.

You must email the displayed URL to "oscp AT offensive-security DOT com" within **24 hours** of completion of the exam.

*If you do not send your uploaded exam-report link to the above address, it will **not** be graded.*

Please note that if you submit your documentation while your exam is still active, upon accepting your documentation your VPN access will be terminated and you will no longer be able to access the exam labs. Once terminated, your VPN access cannot be re-enabled.

Acknowledgement of Receipt

Please wait 12 hours after your report submission before contacting us to verify the receipt. Once we successfully review and accept your documentation, a confirmation email will be sent acknowledging receipt. If you have not received a confirmation email after 12 hours have passed, please send us an email at challenges AT offensive-security DOT com

Additional Required Information

In the unlikely event that we require additional clarification on your exam report, we will get in contact with you via email. You must submit the requested information within **24 hours** from the time we have requested it.

Results

You will receive an email with your certification exam results (pass/fail) within three business days after submitting your documentation. If you have passed the exam, you will receive an exam results email containing a link to update and confirm your certificate delivery address. Please note that we do not provide the exam score, solutions to the exam targets, or digital versions of the certificate.