# OSCP认证考试指南

更新日期：2018年11月20日

**在开始考试之前，请仔细阅读整篇文档！**

## 介绍

本指南介绍了进攻性安全认证专家（OSCP）认证考试的目标。第1节描述了考试的要求，第2部分提供了重要的信息和建议，第3部分规定了考试完成后的说明。

OSCP认证考试模拟私有VPN中的实时网络，其中包含少量易受攻击的计算机。

你有23小时45分钟完成考试。

这意味着如果您的考试于格林威治标准时间09:00开始，您的考试将于格林尼治标准时间第二天08:45结束。

考试结束后，您还需要24小时将文件发送到进攻性安全挑战部门。下面提供了有关如何提交文件的详细信息。

所有OSCP考试现在都是监考。请务必通过以下网址阅读我们的在线常见问题解答： https：//support.offensive-security.com/proctoring-faq

# 第1节：考试要求

考试由几台必须妥协的目标机器组成。某些机器将需要多个开发步骤，首先是低级本地访问，然后是根或管理权限升级。其他机器将可以远程完全利用。每个目标的具体说明将位于您的考试控制面板中，只有在考试开始后才能使用。

## 文件要求

您需要撰写专业报告，描述每个目标的开发过程。您必须以渗透测试报告的形式记录所有攻击，包括所有步骤，发出的命令和控制台输出。您的文档应该足够彻底，以便技术能力强的读者可以逐步复制您的攻击。

**文件要求非常严格，未能提供足够的文件将导致奖励减少或归零。 请注意，提交考试和实验报告后，您的提交是最终的。 如果缺少任何屏幕截图或其他信息，您将无法发送它们，我们也不会要求它们。**

## 利用代码

如果您尚未对漏洞利用进行任何修改，则应仅提供可在其中找到漏洞的URL。不要包含完整的未修改代码，特别是如果它长了几页。

如果您修改了漏洞，则应包括：

- 修改后的漏洞利用代码
- 原始漏洞利用代码的URL
- 用于生成任何shellcode的命令（如果适用）
- 您所做出的突出改变
- 解释为什么要做出这些改变

## 考试证明

您的目标是利用每台目标计算机并提供利用证据。每台目标机器至少包含一个校样文件，您必须在控制面板中检索该文件，并在文档的屏幕截图中包含该文件。 **未能在给定访问级别的屏幕截图中提供适当的证明文件将导致为目标授予零点。**

您必须使用原始位置的`type`or `cat`命令在目标计算机上的交互式shell中提供证明文件的内容。 **以任何其他方式获取校样文件的内容将导致目标机器的零点; 这包括任何类型的基于Web的shell。**

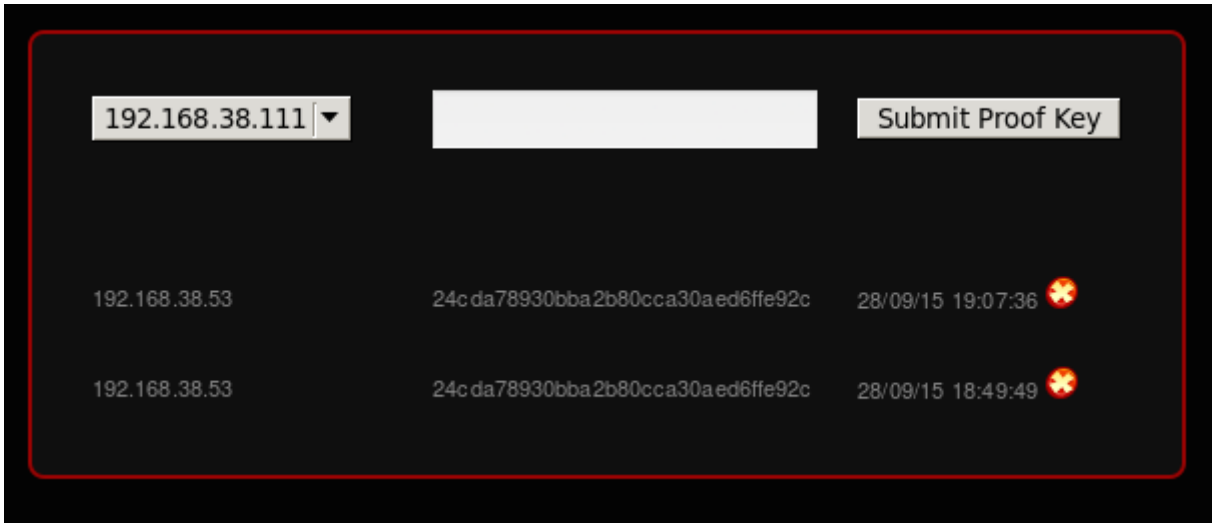
在所有Windows目标上，您必须运行具有以下某个权限的shell才能获得完整点：

- SYSTEM用户
- 管理员用户
- 具有管理员权限的用户

在所有Linux目标上，您必须拥有root shell才能获得满分。

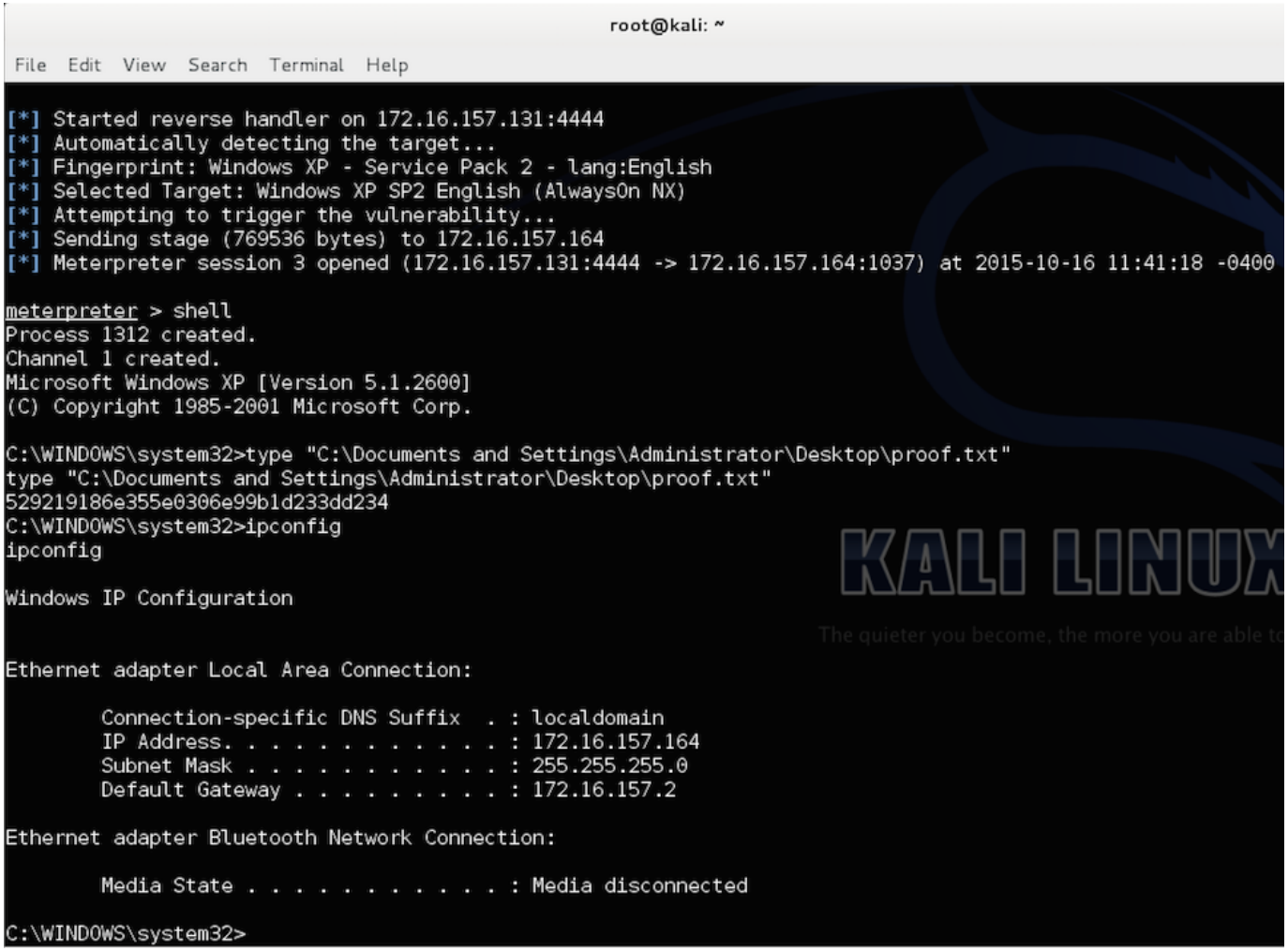
## 控制面板提交

考试控制面板包含可用于提交校样文件的部分。从考试机器获取的local.txt和proof.txt文件的内容*必须在考试结束前在控制面板中提交*。 请注意，控制面板不会指示提交的证明是否正确。下面提供了一个例子：




## 截图要求

找到的每个local.txt和proof.txt都必须显示在屏幕截图中，其中包含文件内容以及使用`ipconfig`或的目标IP地址`ifconfig`。这方面的一个例子如下所示：


root@kali: ~
File Edit View Search Terminal Help
[*] Started reverse handler on 172.16.157.131:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 2 - lang:English
[*] Selected Target: Windows XP SP2 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (769536 bytes) to 172.16.157.164
[*] Meterpreter session 3 opened (172.16.157.131:4444 -> 172.16.157.164:1037) at 2015-10-16 11:41:18 -0400
meterpreter > shell
Process 1312 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
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

## 考试限制

您不能在考试中使用以下任何一项：

- 欺骗（IP，ARP，DNS，NBNS等）
- 商业工具或服务（Metasploit Pro，Burp Pro等）
- 自动开发工具（例如db_autopwn，browser_autopwn，SQLmap，SQLninja等）
- 大规模漏洞扫描程序（例如Nessus，NeXpose，OpenVAS，Canvas，Core Impact，SAINT等）
- 其他工具中的功能可以使用禁止或限制的考试限制

任何执行上述功能的工具也是禁止的。您最终负责了解所选工具使用的功能或外部实用程序。OSCP考试的主要目标是评估您识别和利用漏洞的技能，而不是自动化流程。

但是，您可以对任何目标系统使用Nmap（及其脚本引擎），Nikto，Burp Free，DirBuster等工具。

请注意，除了本考试指南中包含的内容之外，我们不会对允许或限制的工具发表评论。

## Metasploit限制

在考试期间，Metasploit和Meterpreter有效载荷的使用受到限制。您只能使用Metasploit的模块（**辅助，合理开发和邮政**）或反对Meterpreter就会有效载荷**一个**你所选择的单一目标机器。选择一台目标计算机后，不能对任何其他计算机使用Metasploit模块（Auxiliary，Exploit或Post）或Meterpreter有效负载。

在选择一台目标机器之前，**不应**使用Metasploit / Meterpreter 测试多台机器上的漏洞（包括使用**支票**）。您可以使用Metasploit / Meterpreter，因为您可以根据需要多次使用Metasploit / Meterpreter。

如果您决定在特定目标上使用Metasploit或Meterpreter并且攻击失败，那么您**可能不会**尝试在第二个目标上使用它。换句话说，一旦您决定使用其中任何一个，Metasploit和Meterpreter的使用就会被锁定。

您可以对所有目标计算机使用以下内容：

- 多处理程序（又名exploit / multi / handler）
- msfvenom
- pattern_create.rb
- pattern_offset.rb

所有上述限制也适用于使用Metasploit的不同界面（例如Armitage，Cobalt Strike，Metasploit Community Edition等）。

# 第2节：考试信息

### 考试连接

您使用OpenVPN与Kali Linux完成考试的连接。您的考试连接包和详细信息将在考试的确切开始时间通过电子邮件发送，而不是提前发送。

1）将exam-connection.tar.bz2文件从考试邮件中提供的链接下载到您的Kali机器。

2）提取文件：

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

3）使用OpenVPN启动与考试实验室的连接：

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

4）输入考试电子邮件中提供的用户名和密码以对VPN进行身份验证：

```
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
```

## 考试控制面板

考试控制面板可通过考试电子邮件中提供的链接获得。通过考试控制面板，您将能够：

- 提交证明文件
- 还原目标计算机
- 查看特定目标目标和点值

## 机器还原

您有24个恢复的限制。在考试期间可以重置此限制一次。所有机器在考试开始时都已经恢复原状，因此您不需要在开始时还原机器。请耐心等待机器恢复，并且每次尝试只需单击一次按钮。请注意，还原目标计算机将使其返回其原始状态，并且您对计算机所做的任何更改都将丢失。

## 考试证明文件名

- proof.txt - 此文件只能由root用户或管理员用户访问，可以在**/ root /**目录或**Administrator桌面下找到。**此文件在每台目标计算机上都可用。
- local.txt - 此文件可供非特权用户帐户访问，并且只能在某些计算机上找到。包含这些文件的目标在控制面板中详细说明。

## 点分配

- 在考试报告中记录考试机器的顺序与考试机器的评分和评估顺序相同
- 对每台目标机器的部分和完整管理控制将获得积分
- 每台机器都有一组特定的目标，必须满足这些目标才能获得满分

- 你必须达到70分的最低分才能通过考试
- 考试中最多可以达到100分
- 每台机器的具体目标和点值都位于您的考试控制面板中

## 点取消资格

您将不会收到以下特定目标的积分：

- 使用受限制的工具
- 在多台计算机上使用Metasploit Auxiliary，Exploit或Post模块
- 在多台计算机上使用Meterpreter有效负载
- 无法在控制面板和屏幕截图中提供local.txt和proof.txt文件内容

## 建议的文档模板

理想情况下，渗透测试报告应使用以下模板之一：

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

只要信息以结构化，专业的方式呈现并遵循上述所有其他要求，您就可以使用自己的模板。

## 奖励积分

通过提交实验报告和课程练习可以获得五个奖励积分。

- 要获得五个奖励积分，您必须完成实验报告和课程练习
- 实验报告必须以单独的PDF文件提交，并与您的考试报告一起存档。如果未能以正确的格式提交文件，将获得0奖励积分。请参阅下面的其他详细信息
- 实验报告必须包含对不少于10个完全受损的独特计算机的攻击步骤的描述
- 提供的有关机器配置或使用的所有信息必须正确无误
- 必须在屏幕截图中显示每台计算机的proof.txt，其中包含文件内容以及目标的IP地址，方法是使用 `ipconfig` 或 `ifconfig`
- 克隆的机器只能使用一次
- `Offensive Security Complete Guide` 机器可能未包含在您的报告中：Alpha (https://forums.offensive-security.com/showthread.php?t=4689)
- 实验室报告中利用的所有漏洞必须是唯一的。您可能不会对多台计算机使用相同的漏洞
- 你必须成功攻击十个不同的目标。记录同一台机器的多个攻击向量不会授予额外的点数。
- 课程练习必须附加到实验报告的末尾
- 课程练习必须完整且正确，但明确说明的除外

有关PWK报告要求的更多信息，请参阅PWK报告页面 (https://support.offensive-security.com/pwk-reporting)。

## 互联网连接问题

考试指南的这一小节记录了如果由于严重的外部因素导致您无法完成考试时应该采取的措施。请务必仔细阅读并理解。

考试实验室是一个专门的环境，除了你自己以外没有其他学生。23:45小时的总分配时间*确实*考虑了生命及其情况：

- 您需要休息，吃喝玩乐
- 如果您无法控制问题，您还应该制定应急计划。（例如，确保您可以访问备份Internet连接）

如果您有合法的问题，请立即发送一封包含您的OSID的电子邮件，以“挑战攻击性安全DOT com”。确保包括所有必要的详细信息和支持信息，例如您的电力公司，ISP或任何其他相关文档的信函。

请注意，如果问题出现在我们这边，并且只有在考试后其他学生没有立即使用考试子网时，我们才能延长实验时间。如果我们方面出现问题且考试子网在考试后立即安排，我们将提供免费的考试重考。我们非常努力地确保我们的环境高度可用并且问题非常罕见。

## 联系协议

如果您遇到VPN或目标计算机的任何连接问题，请立即通知我们。首选的联系方式是通过https://support.offensive-security.com/chat.php上的在线聊天或通过电子邮件发送到“帮助AT攻击性安全DOT com”。

请注意，我们无法为任何考试目标提供帮助或提示，并且仅在考试期间出现技术问题。

所有与考试文件和提交相关的问题，或其他非技术考试相关问题都应该发送到“攻击性攻击 - 安全DOT com”。实时聊天管理员无法帮助您解决与考试相关的问题，除非你有VPN连接或考试环境的技术问题。

# 第3节：提交说明

**提交清单：**

- [x] 您的考试是PDF格式
- [x] 您的PDF已存档为受密码保护的.7z文件
- [x] 您使用OSID作为.7z文件名的一部分
- [x] 您已将.7z文件上传到https://upload.offsec.com
- [x] 您已通过电子邮件将上传页面中的链接发送至“oscp AT offensive-security DOT com”

以下小节提供了有关这些要求的详细信息。

## 提交格式和名称

您的考试报告必须以PDF格式提交。不接受其他格式。如果您以其他格式提交报告，我们将不会要求或提醒您发送PDF，也不会对您的考试报告进行评分。

在提交您的考试报告之前，请查看PDF文档以确保它与之前的文件类型一样，并且没有格式错误。

使用以下格式作为文件名：“OSCP-OS-XXXXX-Exam-Report.pdf”，其中“OS-XXXXX”是您的OSID。

如果您也要提交实验室报告，则可以使用以下格式作为文件名：“OSCP-OS-XXXXX-Lab-Report.pdf”。

## 存档文件

您必须使用OSID作为密码并使用格式为“OS-XXXXX”的密码保护的.7z文件提交您的文档。这可以通过以下方式实现：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
```

## 提交上传

请通过https://upload.offsec.com提交.7z文件，并按照提供的说明上传您的存档考试报告。不接受其他下载链接（包括ExpireBox，Dropbox，Google Drive，个人网络服务器等）。请注意，只允许存档文件。

文件提交后，您将看到“文件已上传！”页面，其中将显示指向您的考试报告的链接。

**您必须**在完成考试后的**24小时**内将显示的URL通过**电子邮件发送**到“oscp AT攻击性安全DOT com” 。

*如果您未将上传的考试报告链接发送到上述地址，则**不会**对其进行评分。*

请注意，如果您在考试仍处于活动状态时提交文档，则在接受您的文档后，您的VPN访问将被终止，您将无法再访问考试实验室。终止后，无法重新启用VPN访问。

## 收到确认书

请在提交报告后等待12小时，然后与我们联系核实收据。一旦我们成功审核并接受您的文档，我们将发送确认电子邮件并确认收到。如果您在12小时后仍未收到确认电子邮件，请发送电子邮件至challenge AT offensive-security DOT com

## 其他必要信息

万一我们需要对您的考试报告进行额外说明，我们会通过电子邮件与您联系。您必须在我们提出要求后的**24小时**内提交所要求的信息。

## 结果

您将在提交文档后的三个工作日内收到包含认证考试结果（通过/未通过）的电子邮件。如果您通过了考试，您将收到一份考试结果电子邮件，其中包含更新和确认您的证书交付地址的链接。请注意，我们不提供考试分数，考试目标的解决方案或证书的数字版本。