OffSec四大认证对比表

认证	发证机构	级别	内容	Lab环境	要点
 **OSCP**	Offensive Security	PEN-200	OSCP是OffSec中**知名度最高**的认证。 内容包括渗透测试方法和 Kali Linux 中所包含工具的使用方法。这是一项**实践**的渗透测试认证，要求持证者在安全的实验室环境中成功攻击和渗透各种实验机器。	90天Lab	OSCP需要**不断练习打靶和总结，根据细节精准搜寻**漏洞利用点
 **OSEP**	Offensive Security	PEN-300	OSEP**以实战为主**，主要聚焦于**横向移动、域渗透和免杀**，对具有既定安全功能的成熟组织执行高级渗透测试。	90天Lab	OSEP的重点是目标关联信息的**细颗粒度搜集**，结合丰富的专家经验，完成对目标的准确击杀。
 **OSWE**	Offensive Security	WEB-300	OSWE属于**高级Web应用安全**课程，旨在培养学生进行白盒渗透测试所需要的能力	90天Lab	OSWE**注重Web白盒测试**，需**理解业务逻辑、理清路由**是查找漏洞点的关键所在。
 **OSED**	Offensive Security	EXP-301	OSED是专注于**Windows环境下的二进制安全**开发与利用以及基本缓解机制，如SEH、DEP、ASLR的绕过，最后涉及到Win32程序的逆向和漏洞利用	90天Lab	OSED专注在二进制安全，对**前提知识的要求会相对高一些**，例如Win32的汇编、C语言、操作系统原理，Windbg动态调试，IDA free逆向分析等； OSED的重点是Win32 API函数对应汇编代码的快速实现，ROP链的合理构造和实现，逆向分析汇编代码的快速解读和漏洞定位。