Pwn2Own黑客大赛:全补丁64位Windows7被攻破Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022_Pwn2Own_E9_BB_91_c100_644515.htm 在温哥华举行的Pwn2own黑客大赛上，荷兰黑客Peter Vreugdenhil取得了一个重大胜利，他利用了一个IE8的漏洞成功入侵了一台安装了完整补丁的Windows 7 64Bit系统。 Vreugdenhil是一名自由职业者，他的工作是为他的客户寻找并且解决安全漏洞。在大赛中的攻击演示上，他利用多种手段成功绕过了Windows 7的ASLR DEP(随机化地址空间布局和数据执行保护，是Vista和Win7中引入的防止缓存溢出攻击机制)。 谈到攻击原理时，Vreugdenhil表示，“ 我在IE的一个模块中加载了一些数据，这样来绕过Win7的ASLR。绕过DEP的原理也是一样的。 ”由于这次入侵的成功，Vreugdenhil将得到1万美元的现金和一台崭新的PC机，在谈到他通过何种技术查找软件漏洞时，他表示，“ 我喜欢仔细分析我的攻击失败日志，从里面，我可以发现绕过ASLR的方法。 ”在成功攻破IE8之后，Vreugdenhil表示，他要花两周时间，写一篇文章，详细的讲解如何绕过Windows 7的ASLR与DEP缓存溢出保护机制。 微软的IE研发团队成员在现场集体观摩了Vreugdenhil的入侵过程。微软的发言人表示，他们现在还不太清楚这个安全漏洞的一些细节，但是，安全应急响应流程已经开始启动了，微软会从大赛上尽量搜集信息。由于TippingPoint Zero Day Initiative (ZDI)是比赛的赞助商，拥有漏洞的专有权，因此，他们不会在现在公开漏洞信息，预计3月26日大赛全部结束之后，ZDI会向漏洞所在软件的供应商发送详细资料。 100Test 下载频道开通，各类考试题目直接