XCTF

第14章 创建你自己的渗透攻击模块

《Metasploit渗透测试指南》

目录 content

XCTF

目录 content

0x01 Fuzz测试的艺术

Fuzz测试器模块

- 目标：使服务器端崩溃
- 使用Ollydbg对服务器端进行调试
- 根据调试结果对Fuzz字符串长度进行调整

目录 content

0x02 控制结构化异常处理链

控制结构化异常处理链

- 查看SEH链内容
- 查看导致SEH改写的堆栈内容
- 计算SEH覆盖发生位置：tools/pattern_offset.rb
- 调整Fuzz长度字符串长度

目录 content

0x03 绕过SEH限制

绕过SEH限制

- 一段任意的缓冲区填充
- NOP空指令滑行区
- Shellcode
- 近跳转
- 短跳转
- POP-POP-RETN

目录 content

XCTF

0x04 获取返回地址

获取返回地址

- 定位POP-POP-RETN指令序列
- 使用工具查找：
  msfpescan –p TARGETAPP.exe
- 用于调试攻击载荷（发送中断指令）：
  generic/debug_trap
- 调整初始缓冲区长度

目录 content

0x05 坏字符和远程代码执行

坏字符和远程代码执行

- 坏字符：导致shellcode被截断的字符
- 坏字符取决于攻击目标，最快的方法是从攻击目标相同/相似的渗透代码中找坏字符
- http://en.wikibooks.org/wiki/Metasploit/WritingWindowsExploit#Dealing_with_badchars

XCTF

Thanks for watching 谢谢