XCTF

第15章 将渗透代码移植到Metapsloit框架

《Metasploit渗透测试指南》

目录 content

目录 content

0x01 汇编语言基础

汇编语言基础

- EIP和ESP寄存器
- JMP指令集
- 空指令和空指令滑行区

目录 content

0x02 移植一个缓冲区溢出攻击代码

移植一个缓冲区溢出攻击代码

- 裁剪一个已有的渗透攻击代码
- 构造渗透攻击过程
- 测试我们的基础渗透代码
- 实现框架中的特性
- 增加随机化
- 消除空指令滑行区
- 去除伪造的Shellcode
- 我们完整的模块代码

目录 content

0x03 SEH覆盖渗透代码

SEH覆盖渗透代码

- POP-POP-RETN技术
  - POP：从栈中弹出一个内存地址，通常清除掉一个内存地址指令
  - POP： 从栈中弹出一个内存地址
  - RETN：返回到一块用户控制的代码空间，在那里执行构造好的内存指令
- 更多关于SHE覆盖的技术
  http://bbs.pediy.com/thread-102040.htm

XCTF

Thanks for watching 谢谢