XCTF

第13章 编写你自己的模块

《Metasploit渗透测试指南》

目录 content

目录 content

0x01 在MS SQL上进行命令执行

在MS SQL上进行命令执行

- 突破口：MS SQL弱口令
- 调用系统管理员权限的扩展存储过程xp_cmdshell，这个存储过程使得你可以在MS SQL服务的运行账户环境（通常是Local System）下执行底层操作系统命令
- xp_cmdshell的激活
- msf > use auxiliary/admin/mssql/mssql_exec

目录 content

0x02 探索一个已存在的Metasploit模块

XCTF

分析*mssql_exec*模块

- 调用Metasploit核心库的MS_SQL协议模块：
  include Msf::Exploit::Remote::MSSQL
- 激活xp_cmdshell存储过程：
  mssql_xpcmdshell_enable
- 调用mssql_xpcmdshell执行操作系统命令

目录 content

0x03 编写一个新的模块

编写一个新的模块

- PowerShell
- 运行Shell渗透攻击
- 编写Powershell_upload_exec函数
- 从十六进制转换回二进制程序
- 计数器
- 运行渗透攻击模块

XCTF

Thanks for watching 谢谢