XCTF

第7章 免杀技术

《Metasploit渗透测试指南》

目录 content

目录 content

0x01 使用MSF攻击载荷生成器创建可独立运行的二进制文件

- msfvenom：载荷生成，载荷编码
- msfvenom --help
- 常用参数：
  - msfvenom -p PAYLOADNAME --payload-options，查看载荷参数
  - msfvenom –f，指定载荷输出格式
  - msfvenom –e，指定载荷编码方式
  - msfvenom –l MODULENAME，列出指定类型的模块清单

目录 content

0x02 躲避杀毒软件的检测

躲避杀毒软件的检测

- 使用MSF编码器
- 多重编码
- 使用MSF默认内置编码器，现在很难成功躲避杀毒软件的检测

目录 content

0x03 自定义可执行文件模板

自定义可执行文件模板

- 使用常见软件作为自定义模版，将载荷嵌入模版中
- msfvenom –x TEMPLATENAME

目录 content

0x04 隐秘地启动一个攻击载荷

隐秘地启动一个攻击载荷

- msfvenom –k，配置攻击载荷在一个独立的线程中启动
- 这种模式下，当包含载荷的程序被启动，宿主程序也会正常运行，避免被用户察觉
- **-k**选项不一定能用在所有的可执行程序上，在实际攻击前请确保你已经在实验环境中进行了测试

目录 content

0x05 加壳软件

加壳软件

- UPX加壳
- 加密，压缩
- 与MSF编码器的情况类似，目前，仅使用加壳，免杀效果不明显

目录 content

0x06 使用Metasploit Pro的动态载荷实现免杀

Metasploit Pro动态载荷

- 商业版本功能
- 与开源版本相比，可能会多一些编码方式
- 实质上也是MSF载荷生成器各模块的随机、多次组合，不保证生成的每个载荷都能免杀，但是由于自动化程度高、效率高，具有实用性

XCTF

Thanks for watching 谢谢