XCTF

第8章 客户端渗透攻击

《Metasploit渗透测试指南》

目录 content

目录 content

0x01 基于浏览器的渗透攻击

基于浏览器的渗透攻击

- 基于浏览器的渗透攻击原理
  - Heap Spraying（堆喷/堆喷射）
- 关于空指令
  - X86：\x90
  - 空指令滑行区+Payload
- 内存保护机制日益完善，单一技术手段已经不足以完成漏洞利用，但是仍可以作为漏洞利用的组成部分，其思路也值得借鉴。

目录 content

0x02 使用ollydbg调试器来揭秘空指令机器码

使用调试器揭秘空指令

- 目的：搞清楚空指令和汇编指令是如何执行的
- OllyDbg动态调试
- 在Shellcode尾部设置断点
- 在攻击机开启监听

目录 content

0x03 对IE浏览器的极光漏洞进行渗透利用

IE浏览器极光漏洞的利用

- msf > use windows/browser/ms10_002_aurora
- 载荷执行过程中，目标用户机器会变迟钝，为了防止用户关闭浏览器，导致渗透攻击中断，Meterpreter提供了一些指令
- 手动迁移进程：meterpreter > run migrate –f
- 模块高级选项：msf exploit(ms10_002_aurora) > show advanced

目录 content

0x04 文件格式漏洞渗透攻击

文件格式漏洞渗透攻击

- MS11-006，在微软Windows系统函数CreateSizedDIBSECTION中存在的一个栈溢出漏洞
- msf > use windows/fileformat/ms11_006_createsizeddibsection
- 确认攻击模块的目标系统版本：
  - msf exploit(ms11_006_createsizeddibsection) > show targets
- 此类攻击方式载荷是文档，往往需要与钓鱼攻击结合起来

目录 content

0x05 发送攻击负载

发送攻击负载

- 邮件，下载链接
- 开启多线程监听
- 如果用户在文件夹中设置了使用缩略图（thumbnails）方式查看文件，当用户打开payload文件所在的文件夹，即可触发攻击

XCTF

Thanks for watching 谢谢