XCTF

第16章 Meterpreter脚本编程

www.cyberpeace.cn

《Metasploit渗透测试指南》

目录 content

www.cyberpeace.cn

XCTF

目录 content

www.cyberpeace.cn

0x01 Meterpreter脚本编程基础

分析multi_meter_inject脚本

- 查看命令行选项和配置语法格式
- 变量和函数定义，命令行选项
- host_process.memory.allocate调用
- 隐藏启动远程进程

www.cyberpeace.cn

目录 content

www.cyberpeace.cn

0x02 Meterpreter API

Meterpreter API

- 打印输出
- 基本API调用
- Meterpreter Mixins

www.cyberpeace.cn

目录 content

www.cyberpeace.cn

0x03 编写Meterpreter脚本的规则

www.cyberpeace.cn

- 只使用临时、本地和常数变量，永远不要使用全局或者类变量，因为他们可能与框架内的变量相互冲突。
- 使用tab键进行缩进，不要使用空格键。
- 对程序块来说，不要使用大括号{}，使用do和end语法模式。
- 当声明函数时，养成在声明前进行注释，提供函数用途简要介绍的习惯。
- 不要使用sleep函数，使用"select(nil, nil, nil, <time>)"。
- 不要使用puts等其他标准的输出函数，使用print,print_line、print_status、print_error、和print_good函数。
- 总是包含-h选项，该选项将对脚本进行简要的功能说明，并列出所有的命令行选项。
- 如果你的脚本需要在特定操作系统或者Meterpreter平台运行，确保他们只能在所支持的平台上运行，并在不支持的操作系统和平台运行时报错。

目录 content

www.cyberpeace.cn

0x04 创建自己的Meterpreter脚本

XCTF

- 自定义Meterpreter脚本：execute_upload
- 绕过Windows用户账户控制（UAC）防护功能
  - msf > use exploit/windows/local/bypassuac
  - 对已经建立的、受UAC限制的Meterpreter会话使用，建立绕过UAC限制的会话，达到提权的目的

www.cyberpeace.cn

XCTF

www.cyberpeace.cn

Thanks for watching 谢谢

版权所有：XCTF