XCTF

第6章 Meterpreter

《Metasploit渗透测试指南》

目录 content

目录 content

XCTF

0x01 攻陷Windows XP虚拟机

攻陷Windows XP虚拟机

- 攻击路径：
  - 使用nmap扫描端口
  - 攻击MS SQL
  - 暴力破解MS SQL服务
  - xp_cmdshell
  - Meterpreter基本命令
  - 获取键盘记录

目录 content

XCTF

0x02 挖掘用户名和密码

挖掘用户名和密码

- 提取密码哈希值
  - Windows系统存储哈希值的方式一般为LAN Manager（LM）、NT LAN Manager（NTLM），或NT LAN Manager v2（NTLMv2）。
- 使用Meterpreter命令获取密码哈希值
  - meterpreter > use priv
  - meterpreter > run post/windows/gather/hashdump
  - 彩虹表

目录 content

XCTF

0x03 传递哈希值

传递哈希值

- smb/psexec模块
- 使用密码哈希值进行认证，绕过密码破解

目录 content

XCTF

0x04 权限提升

权限提升

- 利用低权限用户建立反向shell连接，获得Meterpreter会话
- 利用Meterpreter的priv扩展
  - meterpreter > use priv
  - meterpreter > getsystem
  - meterpreter > getuid
- 这样的方法是否奏效，取决于低权限用户具有的权限
- MSF会话管理
  - CTRL-Z
  - sessions –l
  - sessions –i SESSION_ID

目录 content

XCTF

0x05 令牌假冒

令牌假冒

- 令牌假冒是Meterpreter最强大的功能之一，对渗透测试非常有帮助。
- 示例场景：你正在对某个组织进行渗透测试，成功地入侵了系统并建立了一个Meterpreter的终端，而域管理员用户在13小时内登录过这台机器。在该用户登入这台机器的时候，一个Kerberos令牌将会发送到服务器上（进行单点登录）并将在随后的一段时间之内有效。你可以使用这个活动令牌来入侵系统，通过Meterpreter你可以假冒成域管理员的角色，而不需要破解他的密码，然后你就可以去攻击域管理员账号，甚至是域控制器。
- 示例体现了令牌假冒的强大，也描述了使用的前置条件，如：建立Meterpreter，启用域，受控机器上有域管理员的有效令牌，等。

目录 content

XCTF

0x06 使用PS

使用PS

- 盗取令牌的两种方式：

1. steal_token PID
   - meterpreter > ps，获取PID
   - steal_token PID，盗取令牌
2. incognito模块
   - 有些情况下ps命令不能列出域管理员账号
   - meterpreter > use incognito
   - meterpreter > list_tokens –u
   - meterpreter > impersonate_token DOMAIN\\USERNAME

目录 content

XCTF

0x07 通过跳板攻击其他机器

通过跳板攻击其他机器

- Meterpreter进行跳板攻击
  - meterpreter > run get_local_subnets
  - msf > route add
  - 通过添加路由实现跳板，依赖于攻击机与跳板机之间的Meterpreter会话，一旦会话断开，跳板将失效
- 使用Metasploit Pro的VPN跳板
  - 商业版本功能
  - 接入目标内网，扩大了攻击面和可选攻击方式

目录 content

0x08 使用Meterpreter脚本

使用Meterpreter脚本

- 迁移进程
- 关闭杀毒软件
- 获取系统密码哈希值
- 查看目标机上的所有流量
- 攫取系统信息
- 控制持久化

目录 content

0x09 向后渗透攻击模块转变

向后渗透攻击模块转变

- 如果想列举所有的后渗透攻击模块，可以这样输入然后在末尾按TAB键：
  - meterpreter > run post/
  - Display all 199 possibilities? (y or n)

目录 content

XCTF

0x10 将命令行shell升级为Meterpreter

XCTF

将命令行shell升级为Meterpreter

- sessions –u
- **setg**命令将LPORT和LHOST参数设置为Metasploit的全局变量，而不是局限在这一个模块之内。在使用**sessions -u**命令升级为Meterpreter的时候是必需的。
- exploit –z, CTRL-Z

目录 content

XCTF

0x11 通过附加的Railgun组件操作Windows API

通过附加的Railgun组件操作Windows API

- meterpreter > irb
- irb shell允许使用Ruby的语法与Meterpreter直接交互
- Railgun能为你提供与Win32本地应用程序一样访问Windows API的能力

XCTF

Thanks for watching 谢谢