内网红队渗透课v1-2

2023 10 12

- 权限提升
  - windows提权之本地提权信息收集
  - windows提权之最优提权方法选择
  - windows提权之exploit集合寻找下载
  - windows提权之本地溢出exploit提权（一）
  - windows提权之本地溢出exploit提权（二）
  - windows提权之端口转发
  - windows提权之本地exploit免杀[非视频]
  - 8.windows提权目录文件理论知识
  - 9.webshell默认权限和IIS提权流程
  - 10.IIS提权流程实操
  - 11.php下的提权及突破限制执行命令
  - 12.可信任服务路径利用
  - 13.服务路径权限配置不当
  - 14.MSSQL提权_xp_cmdshell提权各类问题
  - 15.MSSQL提权_sp_oacreate提权
  - 16.MSSQL提权_利用CLR程序集执行命令
  - 17.MSSQL提权_sp_oacreate中的run方法无回显解决思路
  - 18.MSSQL提权_WarSQLKit
  - 19.MSSQL提权_External Scripting 外部脚本执行命令
  - 20.MSSQL提权_利用Sandbox Mode沙盒模式提权
  - 21.MSSQL提权_利用Agent_jobs提权
  - 22.MSSQL提权_添加注册表启动项提权
  - 23.MSSQL提权_IFEO映像劫持提权【新+久方法】
  - 24.MSSQL提权_文件上传和下载
  - 25.MSSQL提权之SharpSQLTools及其他工具
  - 26.MySQL提权_udf手工和脚本半自动提权
  - 27.MySQL提权_启动项提权+mof提权
  - 28.PostgreSQL提权
- metasploit
  - VPS购买
  - MSF模块及应用
  - MSF两种安装方式
  - MSF4种扫描方式详解
  - MSF扫描模块演示
  - MSF扫描暴破
  - MSF存储结果到PostgreSQL
  - MSF通过账号密码控制目标(smb)
  - MSF通过账号密码控制目标(mssql)
  - MSF通过账号密码控制目标(MySQL)
  - MSF正反向payload详解（1）
  - MSF正反向payload详解（2）
  - MSF上控WEBSHELl目标
  - MSF对Windows的提权
  - MSF对Linux的上控提权
  - MSF上控Liferay的目标
  - MSF内网穿透之路由转发
  - MSF内网穿透之Socks代理
  - Metasploit内网渗透综合篇
- cobaltStrike
  - CobaltStrike简介及通信模型讲解
  - win linux部署CobaltStrike【多版本】
  - CobaltStrike上线初体验
  - CobaltStrike读取密码&HASH
  - CobaltStrike功能之文件管理
  - CobaltStrike功能之Socks4a代理
  - CobaltStrike与MSF联动
  - CobaltStrike功能之键盘记录+屏幕监控+截屏+进程注入
  - CobaltStrike扩展之提权
  - CobaltStrike内网多级上线之rportfwd
  - CobaltStrike内网多级上线之代理上线
  - CobaltStrike两种正向上线
  - CobaltStrike Aggressor Scripts（一）
  - CobaltStrike Aggressor Scripts（二）
  - CobaltStrike Aggressor Scripts（三 实战项目）
  - CobaltStrike反制攻击红队
  - CobaltStrike 上线Linux
  - Cobaltstrike + MSF 实战渗透
- 信息收集
  - 0.信息收集在内网渗透中的意义
  - 1.受害机出网探测
  - 2.受害机各类基础信息收集
  - 3.受害机系统密码&hash收集
  - 4.受害机Google Chrome浏览器信息收集
  - 5.离线获取Google Chrome浏览器保存的密码
  - 6.受害机firefox浏览器信息收集.zip
  - 7.受害机Credentials解密之RDP.zip
  - 8.离线解密目标Credentials【免杀一切】.zip
  - 9.RDP连接记录获取和RDCMan密码获取.zip
- 内网穿透
  - 1.端口转发【单至多层】
  - 2.SHELL反弹【单至多层】
  - 3.Socks代理【单至多层】
  - 3.1.3款代理工具详解
  - 4.ew和Termite的使用
  - 5.ssocks代理工具使用【正反代理】
  - 6.利用frp进行加密高速稳定的内网穿透
  - 7.利用reGeorg建立http加密代理
  - 8.利用系统自带的netsh进行内网转发
  - 9.利用[abptts]建立https加密转发隧道
  - 10.netsh在渗透中应用【防火墙】
  - 11.frp使用二及改造
  - 12.内网穿透工具dog-tunnel
  - 13.内网穿透工具dog-tunnel 2 udp版本
  - 14.http代理隧道和http端口映射出网之pystinger
  - 15.DNS隧道之dns2tcp
  - 16.SSH隧道
  - 16.SSH隧道之本地转发
  - 17.SSH隧道之远程转发
  - 18.SSH隧道之动态转发
  - 19.免密登录ssh
  - 20.ssh隧道搭建反向代理
  - 21.icmp隧道之pingtunnel
  - 22.利用icmp建立反向代理
  - 23.icmp隧道之icmpsh获得os shell
  - 24.dns隧道之iodine上线、端口映射（稳定）.dns隧道之iodine（稳定）
  - 25.Linux下的穿透神器socat
  - 26. iox流量加密转发代理工具及免杀
  - 27.HTTP协议下的代理工具ecloud【已免杀】
  - 28. 跨平台、稳定、隐秘的多级穿透rakshasa
- 横向移动
  - 0.[445]IPC+计划任务进行手工横向移动
  - 1.[445]IPC+计划任务进行手工横向移动2
  - 2.[445]IPC+sc进行手工横向移动
  - 3.[135]wmic进行手工横向移动
  - 4.[5985]winRM进行手工横向移动
  - 5.横向移动工具合集（一）Psexec
  - 6.横向移动工具合集（二）scshell
  - 7.横向移动工具合集（三）wmiexec
  - 8.横向移动工具合集（四）基于WMI的3款工具
  - 9.横向移动工具合集（五）atexec-smbexec-dcomexec
  - 10.横向移动工具合集（六）其余的横向工具
- AD域渗透初级
  - 1.域基础知识一（杂项）
  - 2.Windows Svr 2016单域环境搭建
  - 3.windows svr 2016 多域（子域）环境搭建
  - 4.windows svr 2016 多域控环境搭建
  - 5.域内信息收集（一）
  - 6.域控制器DC定位
  - 7.利用特定漏洞攻击域控
  - 8.常规横向移动手法进入域控
  - 9.利用SYSVOL保存的密码攻击域控
  - 10.导出域用户的HASH之获取NTDS.DIT
  - 11.远程导出NTDS.DIT
  - 12.导出域用户的HASH之提取NTDS.DIT
  - 13.导出域用户的HASH之解密NTDS.DIT错误解决
  - 14.利用DcSync域内远程获取域用户hash
  - 15.部署密码爆破神器Hashcat
  - 16.利用Hashcat爆破各类密码
  - 17.利用exchange-outlook上控指定目标
  - 18.创建远程匿名文件共享
  - 19.域基础知识二（活动目录）
  - 20.域基础知识三（LDAP）
  - 21.获取域内所有用户和机器
  - 22.用Csharp定制自己的域内信息导出工具
  - 23.用户登录脚本攻击指定用户
  - 24.GPO任务计划批量下发恶意程序
  - 25.GPO任务计划设置安全筛选攻击指定目标
  - 26.GPO策略用户登录（开机）下发恶意程序
  - 27.Kerberos协议初探
  - 28.黄金票据 Golden Ticket
  - 29.白银票据(Silver Ticket)攻击
  - 30.pass the hash[key]
  - 31.AS-REP Roasting
  - 32.SPN扫描信息收集
  - 33.Kerberoasting攻击
  - 34.LDAP用户枚举
  - 35.LDAP密码喷洒
  - 36.目标内网架构分析之dns记录
  - 37.目标用户机器定位之日志
  - 38.MS14-068提权
  - 39.SMB密码喷洒
  - 40.命令行修改GPO策略文件"关闭"防火墙
- 权限维持
  - 1.Sid-history
  - 2.DSRM域后门
  - 3.SSP驻留域控权限
  - 4.Hook PasswordChangeNotify
  - 5.注册表自启动及目录启动项
  - 6.任务计划后门
  - 7.DLL劫持
  - 8.服务自启动
  - 9.Netsh Helper DLL
  - 10.辅助功能镜像劫持