

内网安全-实战项目&VPC3 线上&三层代理路由&免杀对抗&域控提
权

基本认知

- 0、域产生原因
- 1、内网域的区别
- 2、如何判断在域内
- 3、域内常见信息收集
- 4、域内自动化工具收集

① 信息收集

- 网络环境
 - 域环境
 - 工作组/局域网
 - 个人PC
- 机器角色
 - 文件服务器
 - 邮件服务器
 - 网站服务器等
- 角色功能
 - 任务
 - 端口
 - 密码/口令
 - 安全漏洞
 - 服务配置等
- 自动化工具
 - Adfind
 - BloodHound
 - CS插件
 - OLa
 - Ladon
 - TaoWu
 - LSTAR
- 梳理流程
 - 定位域控
 - 明确移动
 - 取得权限

② 代理技术

- 工具系统
 - Linux
 - ProxyChains
 - Windows
 - Proxifier
 - SocksCap
- 节点协议
 - Socks4/4a
 - Socks5
- 解决方向
 - 网络通讯
 - 控制上线
 - 工具
 - CS
 - MSF
 - 连接
 - 正向
 - bind_tcp
 - 反向
 - reverse_tcp
 - 添加路由
 - MSF
 - run autoroute -p
 - run post/multi/manage/autoroute
 - CS
 - 不需要添加
 - MSF
 - use auxiliary/server/socks_proxy
 - 创建节点
 - CS
 - 图形化: 代理转发-Socks代理
 - 图像话: 代理转发-转发上线
 - 软件连接节点
 - 在软件服务器进行后验

防火墙

- 规则
 - 入站
 - 出站
- 对象
 - 域环境
 - 专用
 - 公网
- 设置
 - 程序
 - 端口
 - 预定义
 - 自定义
- FRP

#知识点:

- 1、vpc-1-不涉及杀毒 防火墙
- 2、vpc-2-涉及杀毒 防火墙
- 3、vpc-3-涉及杀毒 防火墙 高级攻防
- 4、vpc-4-涉及杀毒 防火墙 高级攻防 多域森林

权限维持知识点:

系统: Win&Linux

层面: 单机版&域环境&WEB

与 NTLM 认证相关的安全问题主要有 Pass The Hash、利用 NTLM 进行信息收集、Net-NTLM Hash 破解、NTLM Relay 几种。PTH 前期已经了, 运用 mimikatz、impacket 工具包的一些脚本、CS 等等都可以利用, NTLM Relay 又包括 (relay to smb, ldap, ews)

-连接方向: 正向&反向 (基础课程有讲过)

-内网穿透: 解决网络控制上线&网络通讯问题

-隧道技术: 解决不出网协议上线的问题 (利用出网协议进行封装出网)

-代理技术: 解决网络通讯不通的问题 (利用跳板机建立节点后续操作)

#代理隧道系列点:

- 1、判断什么时候用代理
- 2、判断什么时候用隧道
- 3、判断出网和不出网协议
- 4、如何使用代理建立节点并连接
- 5、如何使用隧道技术封装协议上线
- 6、判断哪些代理或隧道情况选择放弃

#横向移动系列点:

系统点:

windows->windows

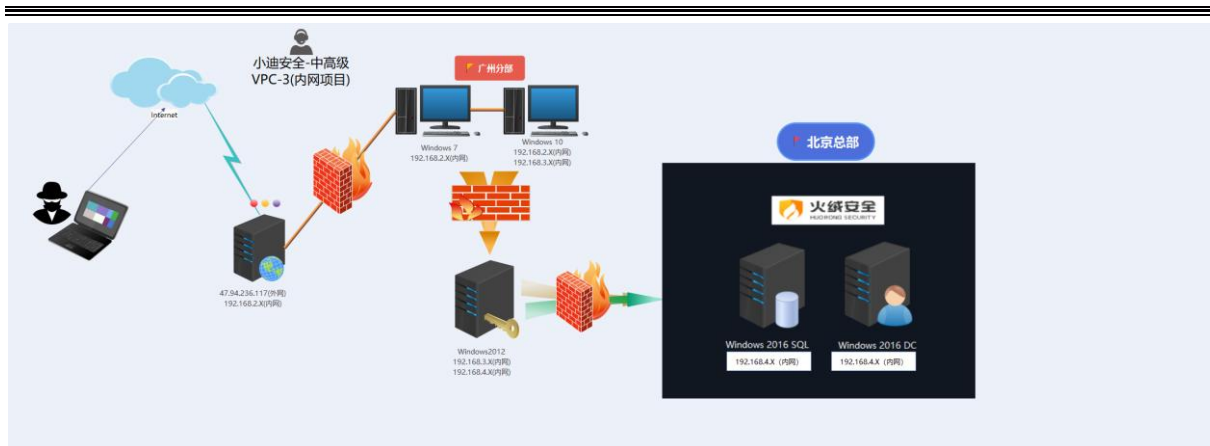
windows->Linux

linux->windows

linux->linux

详细点:

IPC, WMI, SMB, PTH, PTK, PTT, SPN, WinRM, WinRS, RDP, Plink, DCOM, SSH; Exchange, LLMNR 投毒, NTLM-Relay, Kerberos_TGS, GPO&DACL, 域控提权漏洞, 约束委派, 数据库攻防, 系统补丁下发执行, EDR 定向下发执行等。



演示案例：

➤ 线上 VPC3-打靶 WP

难度评分：7

难度等级：中级

考核内容：

从外网打到内网域，成功拿到所有靶场权限。

主要技术：

Web 攻防 (PHP, Java)，内网打点，免杀对抗，域横向移动，域控提权，代理隧道等。

注意事项：

1. 禁止使用扫描器进行批扫。
2. 测试过程中要对进行保密。
3. 禁止攻击靶场以外的主机。
4. 完成后编写文档发给小迪。

入口点：

<http://47.94.236.117:8080/>

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
