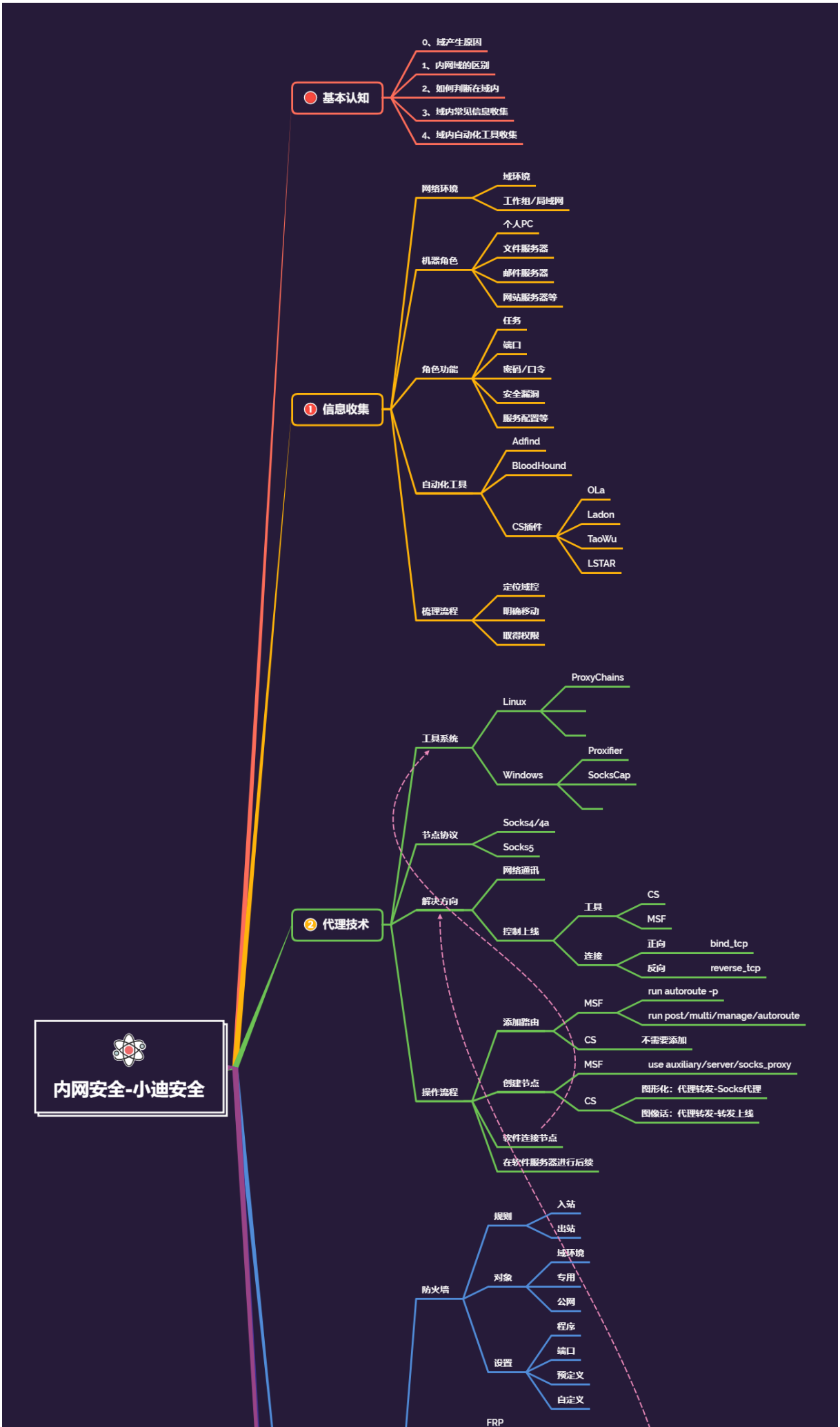
内网安全-Win&Linux&内存离线读取&Hashcat 破解&RDP&SSH 存储提取


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、密码获取-Windows&Linux

2、密码破解-Hash&字典&暴力

3、密码存储-RDP 保存&SSH 密匙

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。

如果禁用了 ntlm 认证，PsExec 无法利用获得的 ntlm hash 进行远程连接，但是使用 mimikatz 还是可以攻击成功。对于 8.1/2012r2，安装补丁 kb2871997 的 Win 7/2008r2/8/2012 等，可以使用 AES keys 代替 NT hash 来实现 ptk 攻击

演示案例：

- 明文获取-Windows&Linux-内存读取&离线读取
- 密文破解-Windows&Linux-Hashcat&字典&暴力
- 密匙存储-Windows&Linux-RDP 保存&SSH 密匙

注意：

1、Windows-Mimikatz 适用环境：

微软为了防止明文密码泄露发布了补丁 KB2871997，关闭了 Wdigest 功能。

当系统为 win10 或 2012R2 以上时，默认在内存缓存中禁止保存明文密码，

此时可以通过修改注册表的方式抓取明文，但需要用户重新登录后才能成功抓取。

2、Linux-mimipenguin 适用环境：

```
Kali 4.3.0 (rolling) x64 (gdm3)
Ubuntu Desktop 12.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
Ubuntu Desktop 16.04 LTS x64 (Gnome Keyring 3.18.3-0ubuntu2)
XUbuntu Desktop 16.04 x64 (Gnome Keyring 3.18.3-0ubuntu2)
VSFTPd 3.0.3-8+b1 (Active FTP client connections)
Apache2 2.4.25-3 (Active/Old HTTP BASIC AUTH Sessions)
openssh-server 1:7.3p1-1 (Active SSH connections - sudo usage)
```

所以出现以下：

0、Windows-强开

1、正面刚密文-Hashcat

2、侧面找思路-RDP 保存&SSH 密匙

#Linux-密码获取-内存读取&密文破解&存储凭证

1、密码读取：

```
https://github.com/huntergregal/mimipenguin
chmod 755 ./mimipenguin.sh
./mimipenguin.sh
```

2、密码破解：

```
cat /etc/shadow
hashcat.exe -a 3 -m 1800 linuxhash.txt pass.txt
```

加密形式：

```
linux sha512crypt $6$, SHA512 (Unix)加密方式：
hashcat -m 1800 sha512linux.txt p.txt
linux sha256crypt $5$, SHA256 (Unix)加密方式：
hashcat -m 7400 sha256linux.txt p.txt
linux 下 md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)加密方式：
hashcat -m 500 linuxmd5.txt p.txt
inux 下 bcrypt $2*$, Blowfish 加密方式：
hashcat -m 3200 linuxmd5.txt p.txt
```

3、密码存储：SSH 密匙-上节课知识点

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址