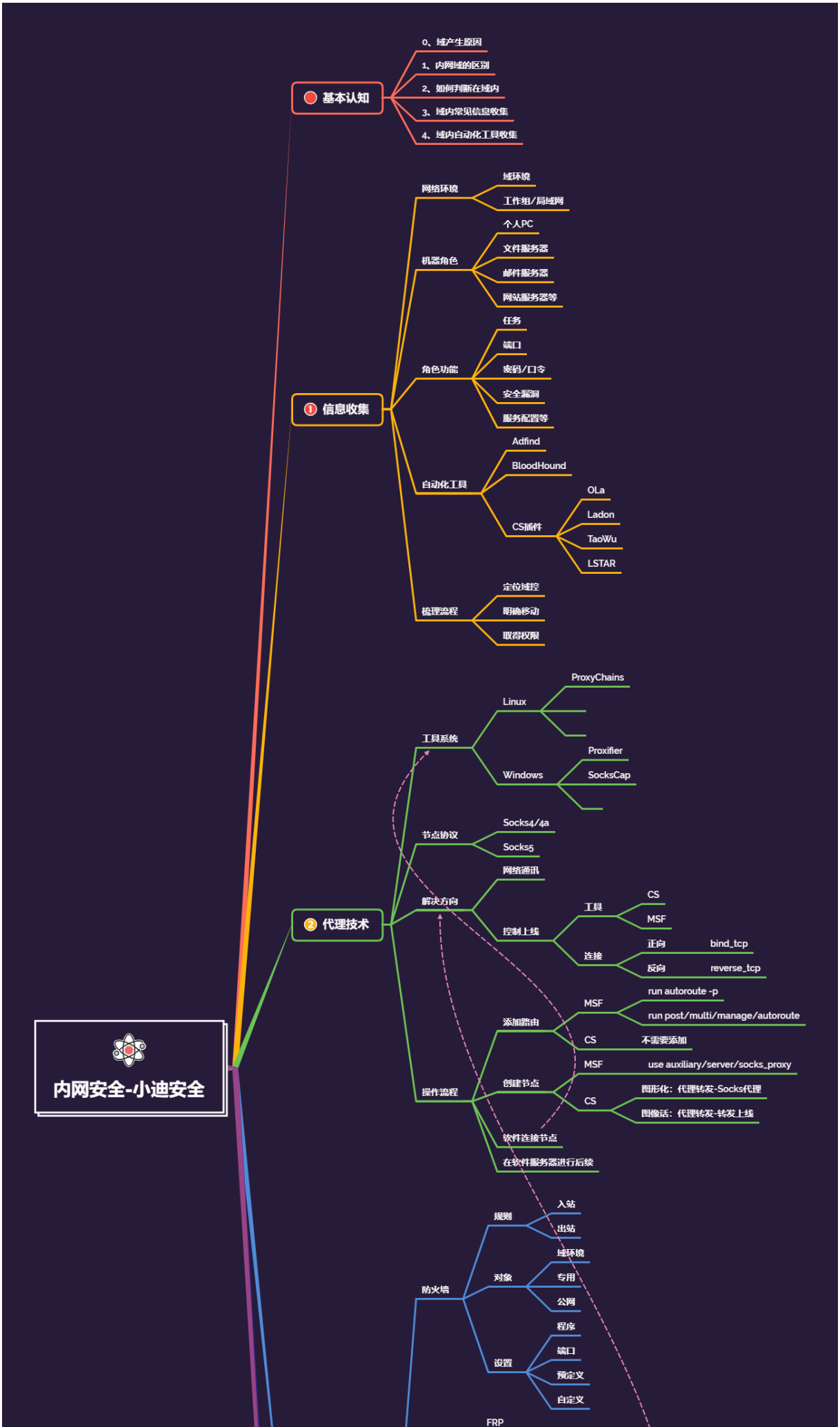
内网安全-横向移动&非约束委派&约束委派&资源约束委派&数据库攻防


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、横向移动-委派-约束委派

2、横向移动-委派-非约束委派

3、横向移动-委派-资源约束委派

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

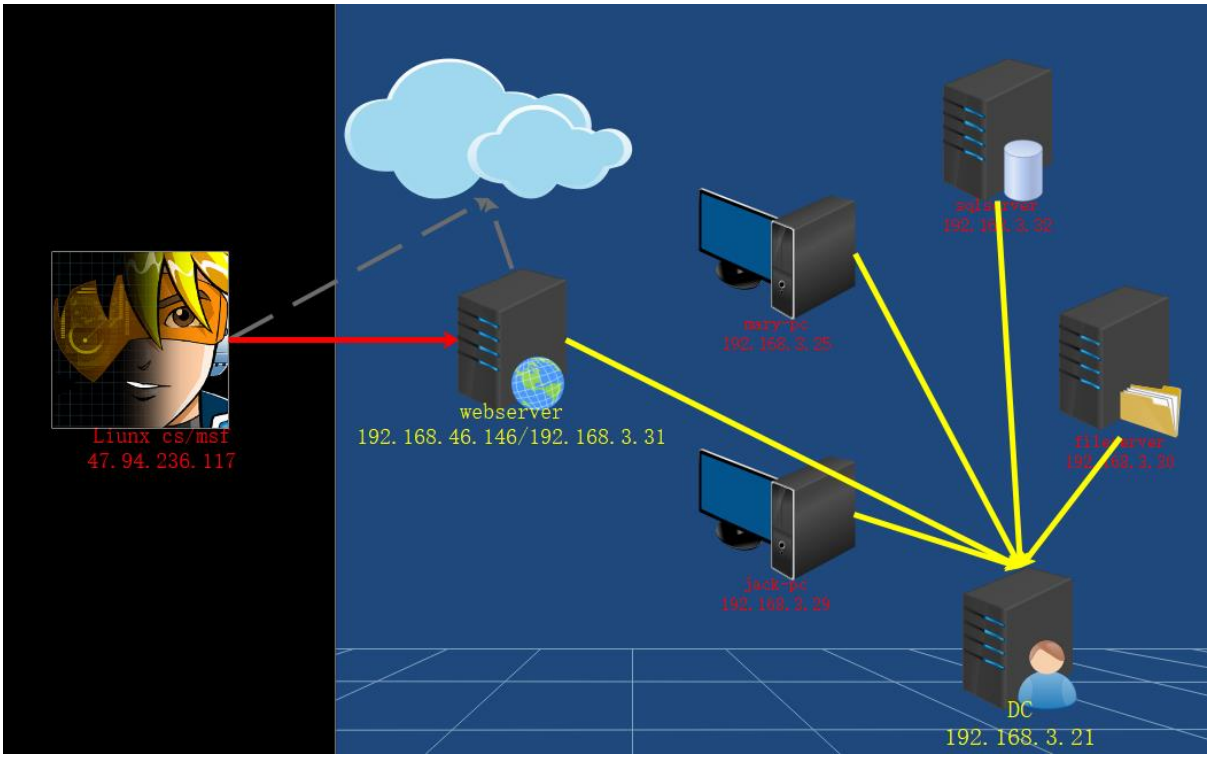
linux->linux

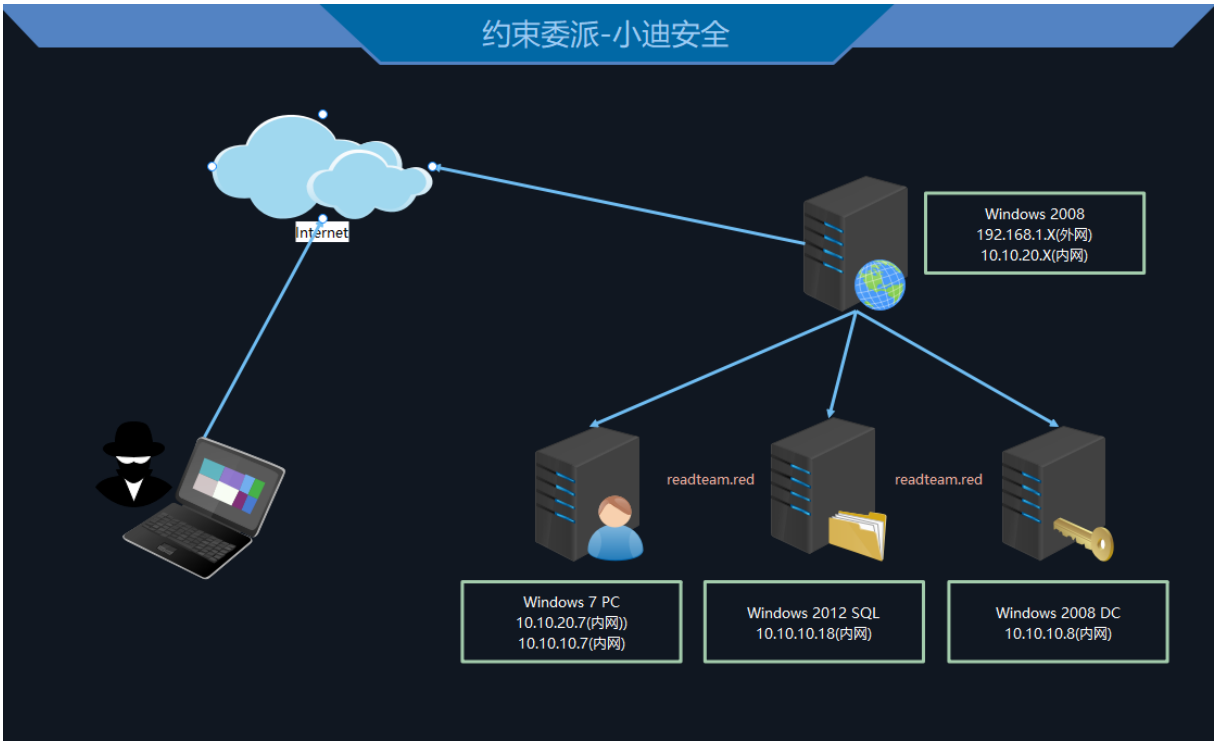
详细点：

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：

- 横向移动-原理利用-约束委派&非约束委派
- 横向移动-实战靶机-约束委派&数据库攻防

#委派攻击分类：

1、非约束性委派

2、约束性委派

3、基于资源的约束性委派

#横向移动-原理利用-约束委派&非约束委派

-非约束委派

原理：

机器 A（域控）访问具有非约束委派权限的机器 B 的服务，会把当前认证用户（域管用户）的的 TGT 放在 ST 票据中，一起发送给机器 B，机器 B 会把 TGT 存储在 lsass 进程中以备下次重用。从而机器 B 就能使用这个 TGT 模拟认证用户（域管用户）访问服务。

利用场景

攻击者拿到了一台配置非约束委派的机器权限，可以诱导域管来访问该机器，然后得到管理员的 TGT，从而模拟域管用户。

复现配置：

1、信任此计算机来委派任何服务

2、setspn -U -A priv/test webadmin

判断查询：

查询域内设置了非约束委派的服务账户：

```
AdFind -b "DC=god,DC=org" -f
"(&(samAccountType=805306368)(userAccountControl:1.2.840.113556.1
.4.803:=524288))" dn
```

查询域内设置了非约束委派的机器账户：

```
AdFind -b "DC=god,DC=org" -f
"(&(samAccountType=805306369)(userAccountControl:1.2.840.113556.1
.4.803:=524288))" dn
```

利用步骤：

1、域控与委派机器通讯

主动：

```
net use \\webserver
```

钓鱼：

```
http://192.168.3.31/31.html
<!DOCTYPE html>
<html>
<head>
  <title></title>
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址