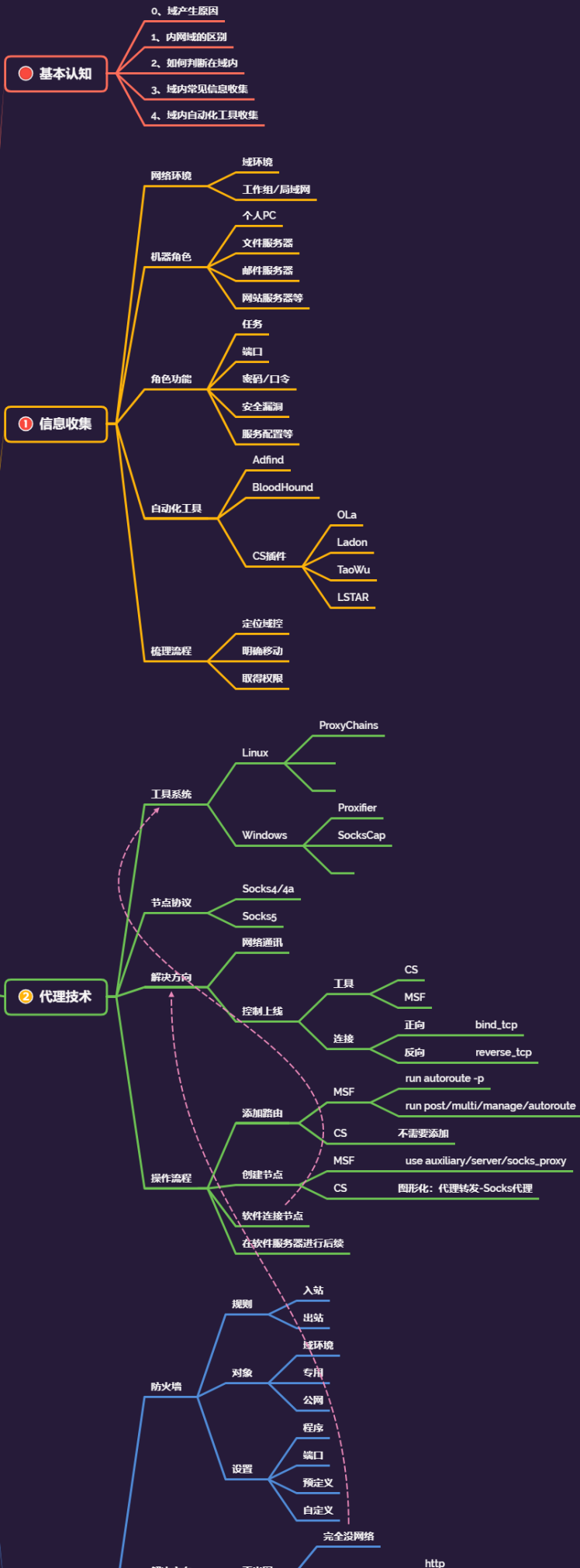


内网安全-隧道技术&SMB&ICMP&正反向连接&防火墙出入规则上 线

内网安全-小迪安全



#知识点:

- 1、进站规则不出网上线方案
- 2、出站规则不出网上线方案
- 3、规则-隧道技术-SMB&ICMP

-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)

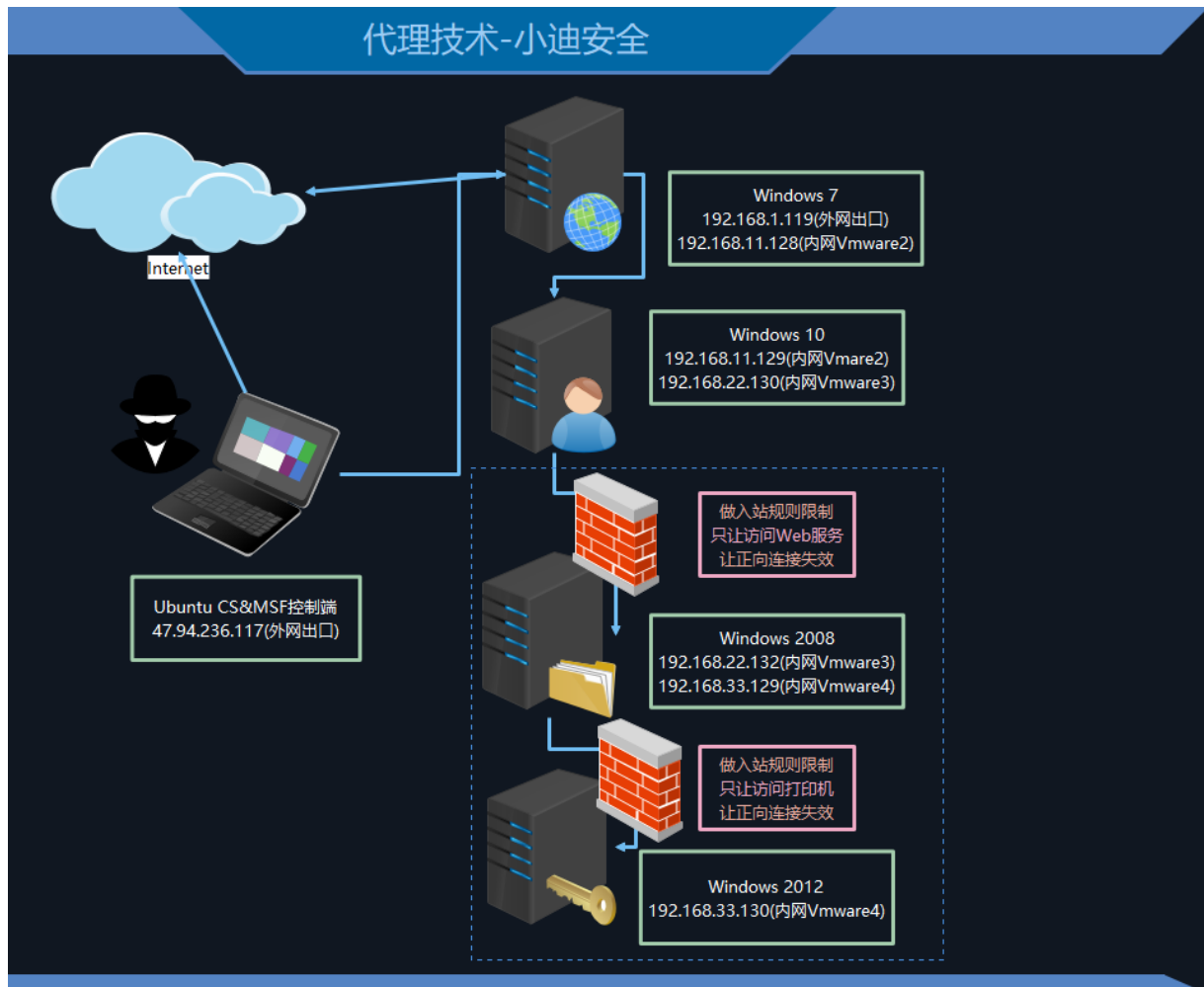
-连接方向: 正向&反向 (基础课程有讲过)

#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



代理技术-小迪安全



演示案例:

- 不出网-控制上线-CS-反向连接
- 不出网-控制上线-CS-SMB 隧道
- 不出网-控制上线-CS-ICMP 隧道
- 不出网-控制上线-CS-关闭防火墙

入站过滤上线：

- 1、隧道技术硬刚
- 2、反向连接跳过
- 3、关闭&删除&替换

适用利用入站通行拿到的高权限

出站过滤上线：

- 1、隧道技术硬刚
- 2、正向连接跳过
- 3、关闭&删除&替换

适用利用入站通行拿到的高权限

隧道技术上线：

HTTP/S & DNS & SSH & ICMP & SMB & 协议穿透等

Windows 防火墙命令：

<https://www.cnblogs.com/tomtellyou/p/16300557.html>

查看当前防火墙状态：`netsh advfirewall show allprofiles`

关闭防火墙：`netsh advfirewall set allprofiles state off`

开启防火墙：`netsh advfirewall set allprofiles state on`

恢复初始防火墙设置：`netsh advfirewall reset`

启用桌面防火墙：`netsh advfirewall set allprofiles state on`

设置默认输入和输出策略：`netsh advfirewall set allprofiles
firewallpolicy allowinbound,allowoutbound`

如果设置为拒绝使用 `blockinbound,blockoutbound`

涉及资源：

[补充：涉及录像课件资源软件包资料等下载地址](#)
