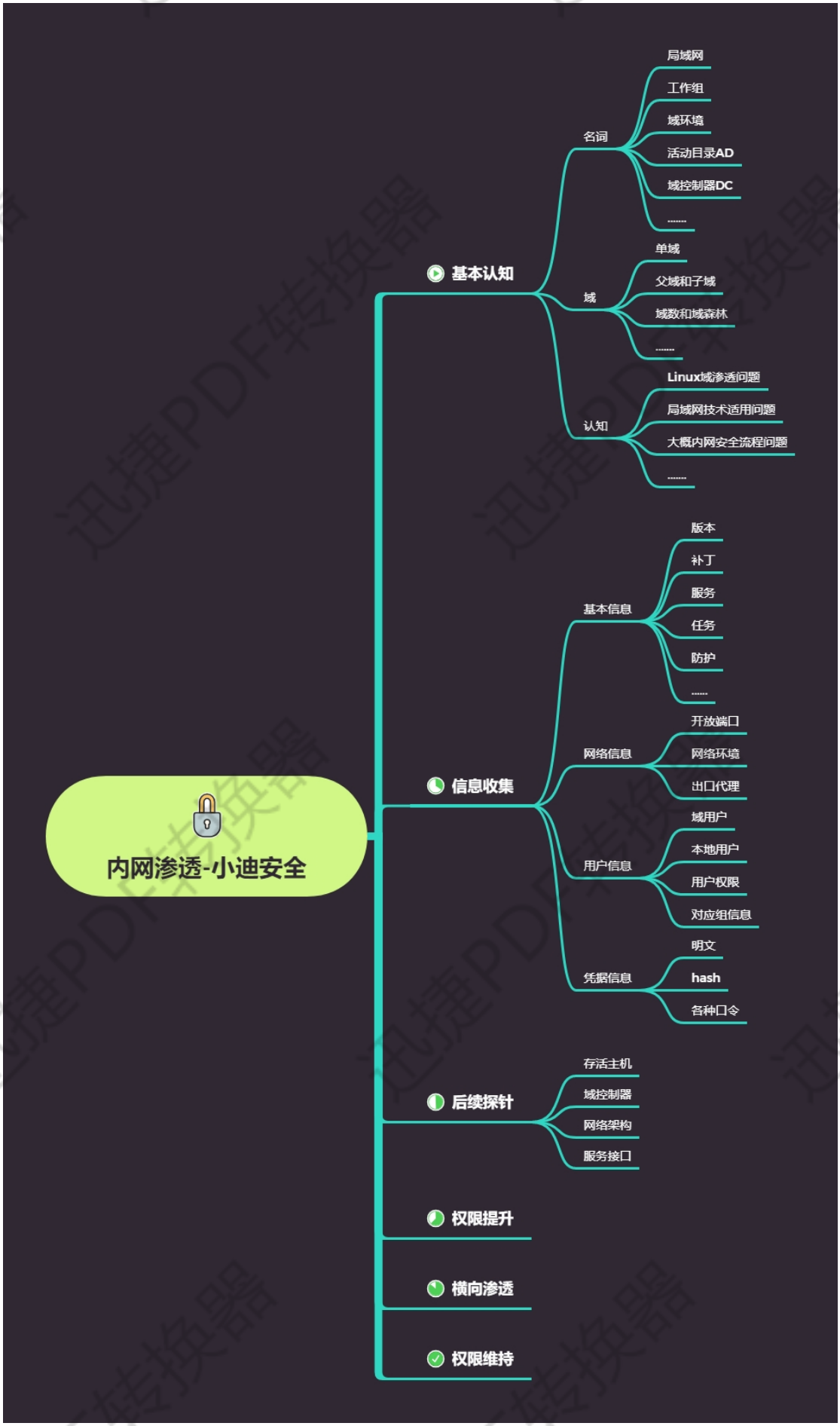
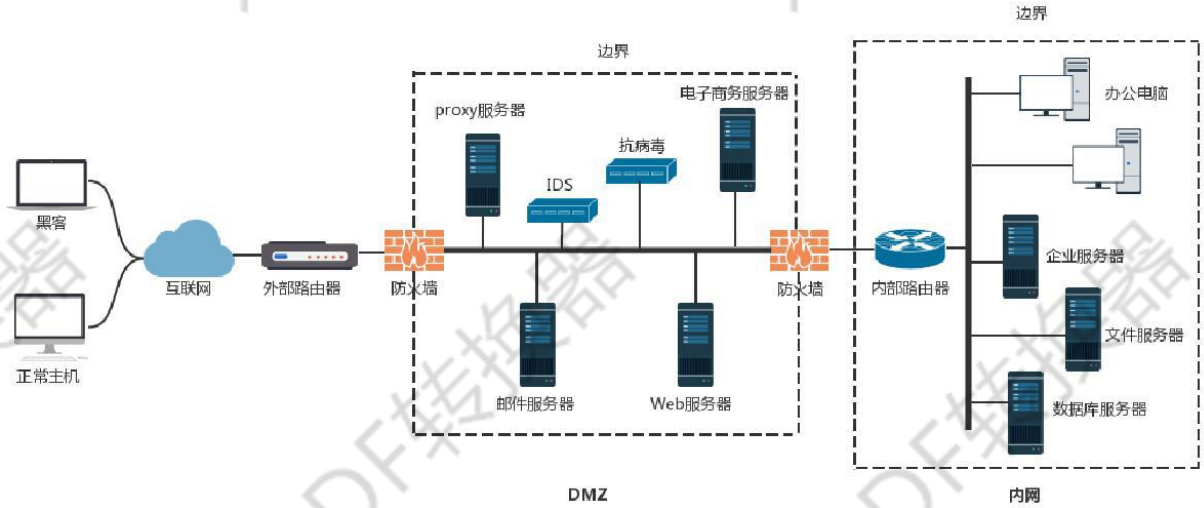
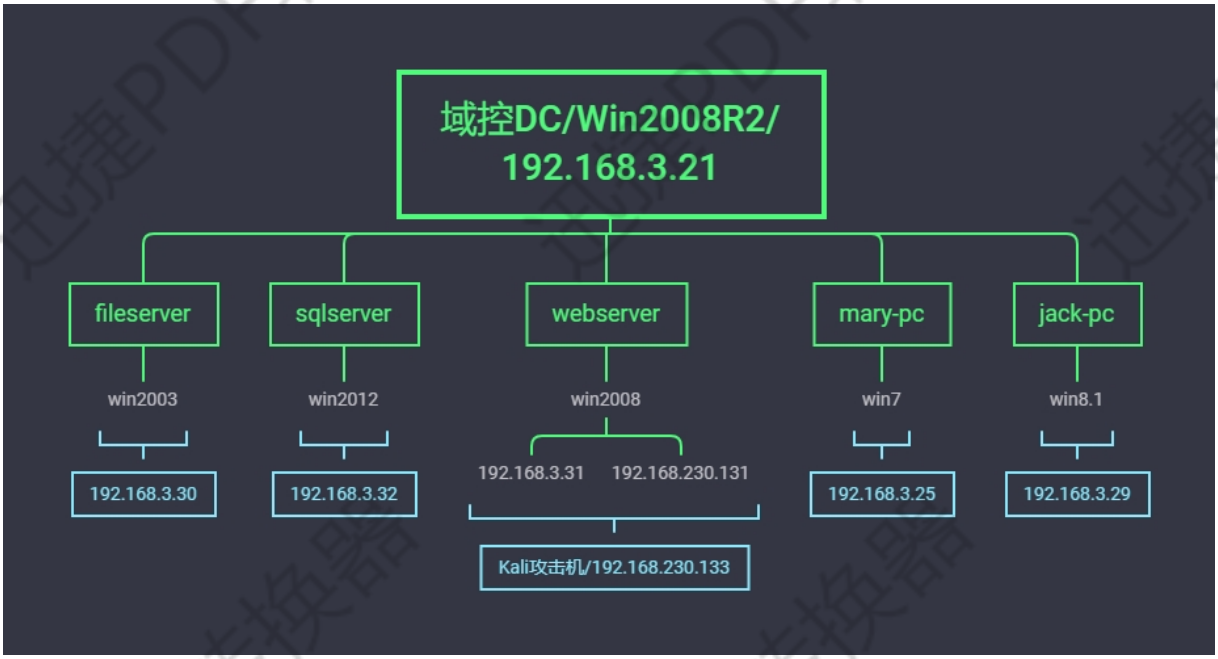
内网安全-域环境&工作组&局域网探针方案


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
对应组信息
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
横向渗透
权限维持



演示案例：

- 基本信息收集操作演示
- 网络信息收集操作演示
- 用户信息收集操作演示
- 凭据信息收集操作演示
- 探针主机域控架构服务操作演示



#案例 1-基本信息收集操作演示
旨在了解当前服务器的计算机基本信息，为后续判断服务器角色，网络环境等做准备
systeminfo 详细信息
net start 启动服务
tasklist 进程列表
schtasks 计划任务

#案例 2-网络信息收集操作演示
旨在了解当前服务器的网络接口信息，为判断当前角色，功能，网络架构做准备
ipconfig /all 判断存在域-dns
net view /domain 判断存在域
net time /domain 判断主域
netstat -ano 当前网络端口开放
nslookup 域名 追踪来源地址

#案例 3-用户信息收集操作演示
旨在了解当前计算机或域环境下的用户及用户组信息，便于后期利用凭据进行测试
系统默认常见用户身份：
Domain Admins：域管理员（默认对域控制器有完全控制权）
Domain Computers：域内机器
Domain Controllers：域控制器
Domain Guest：域访客，权限低
Domain Users：域用户
Enterprise Admins：企业系统管理员用户（默认对域控制器有完全控制权）
相关用户收集操作命令：
whoami /all 用户权限
net config workstation 登录信息
net user 本地用户
net localgroup 本地用户组
net user /domain 获取域用户信息
net group /domain 获取域用户组信息
wmic useraccount get /all 涉及域用户详细信息
net group "Domain Admins" /domain 查询域管理员账户
net group "Enterprise Admins" /domain 查询管理员用户组
net group "Domain Controllers" /domain 查询域控制器

#案例 4-凭据信息收集操作演示
旨在收集各种密文，明文，口令等，为后续横向渗透做好测试准备
计算机用户 HASH，明文获取-mimikatz(win)，mimipenguin(linux)
计算机各种协议服务口令获取-LaZagne(all)，XenArmor(win)
Netsh WLAN show profiles
Netsh WLAN show profile name="无线名称" key=clear
1.站点源码备份文件、数据库备份文件等
2.各类数据库 Web 管理入口，如 PHPMyAdmin
3.浏览器保存密码、浏览器 Cookies

4.其他用户会话、3389 和 ipc$连接记录、回收站内容
5.Windows 保存的 WIFI 密码
6.网络内部的各种帐号和密码，如：Email、VPN、FTP、OA 等

#案例 5-探针主机域控架构服务操作演示
为后续横向思路做准备，针对应用，协议等各类攻击手法
探针域控制器名及地址信息
net time /domain nslookup ping
探针域内存活主机及地址信息
nbtscan 192.168.3.0/24 第三方工具
for /L %I in (1,1,254) DO @ping -w 1 -n 1 192.168.3.%I | findstr "TTL=" 自带内部命令
nmap masscan 第三方 PowerShell 脚本 nishang empire 等
#导入模块 nishang
Import-Module .\nishang.psm1
#设置执行策略
Set-ExecutionPolicy RemoteSigned
#获取模块 nishang 的命令函数
Get-Command -Module nishang
#获取常规计算机信息
Get-Information
#端口扫描（查看目录对应文件有演示语法，其他同理）
Invoke-PortScan -StartAddress 192.168.3.0 -EndAddress 192.168.3.100 -ResolveHost -ScanPort
#其他功能：删除补丁，反弹 Shell，凭据获取等
探针域内主机角色及服务信息
利用开放端口服务及计算机名判断
核心业务机器:
1.高级管理人员、系统管理员、财务/人事/业务人员的个人计算机
2.产品管理系统服务器
3.办公系统服务器
4.财务应用系统服务器
5.核心产品源码服务器（自建 SVN、GIT）
6.数据库服务器
7.文件或网盘服务器、共享服务器
8.电子邮件服务器
9.网络监控系统服务器
10.其他服务器（内部技术文档服务器、其他监控服务器等）

涉及资源：

http://unixwiz.net/tools/nbtscan.html

https://github.com/samratashok/nishang