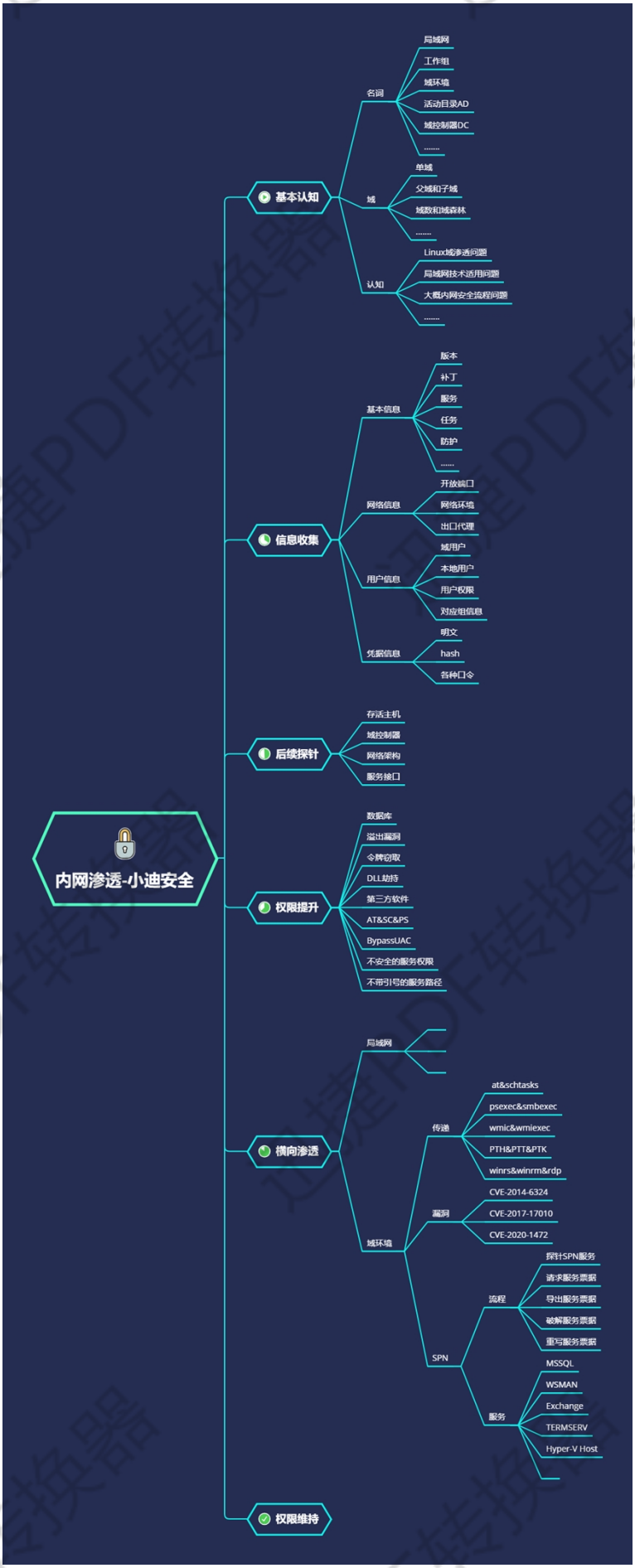
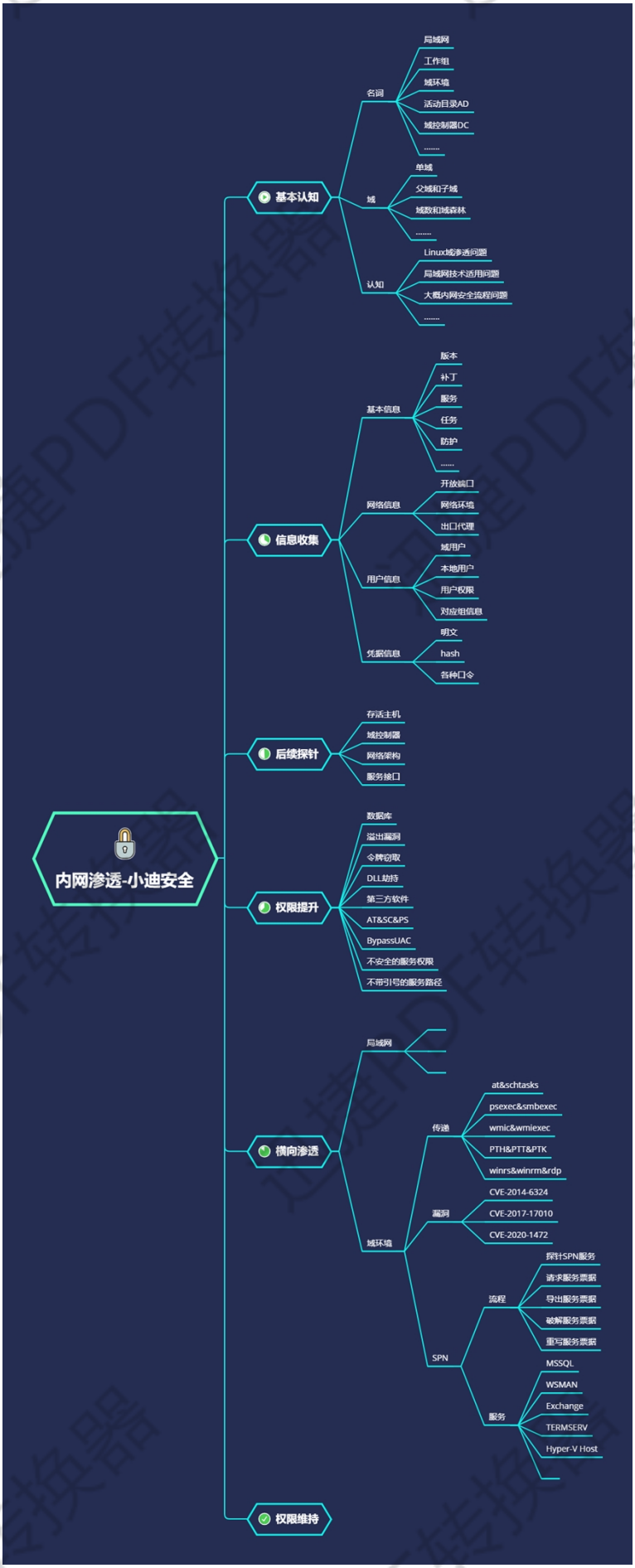
内网安全-域横向 CobaltStrike&SPN&RDP


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
SPN
流程
探针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
权限维持

内网安全-域横向 CobaltStrike&SPN&RDP


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
SPN
流程
探针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
权限维持

SPN扫描

当计算机加入域时,主SPN会自动添加到域的计算机账号的ServicePrincipalName属性中。在安装新的服务后，SPN也会被记录在计算机账号的相应属性中。

SPN扫描也称为”扫描Kerberos服务实例名称”。在活动目录中发现服务的最佳方法就是SPN扫描。SPN扫描通过请求特定SPN类型的服务主体名称来查找服务。与网络端口扫描相比，SPN扫描的主要特点是不需要通过连接网络中的每个IP地址来检查服务端口(不会因为触发内网中的IPS、IDS等设备的规则而产生大量的警告日志)。因为SPN查询是Kerberos票据行为的一部分，所以检测难度很大。

由于SPN扫描是基于LDAP协议向域控制器进行查询的，所以，攻击者只需要获得一个普通的域用户权限，就可以进行SPN扫描。

> 在域环境中，发现服务的最好办法就是通过”SPN扫描”。通过请求特定SPN类型服务主体名称来查找服务。