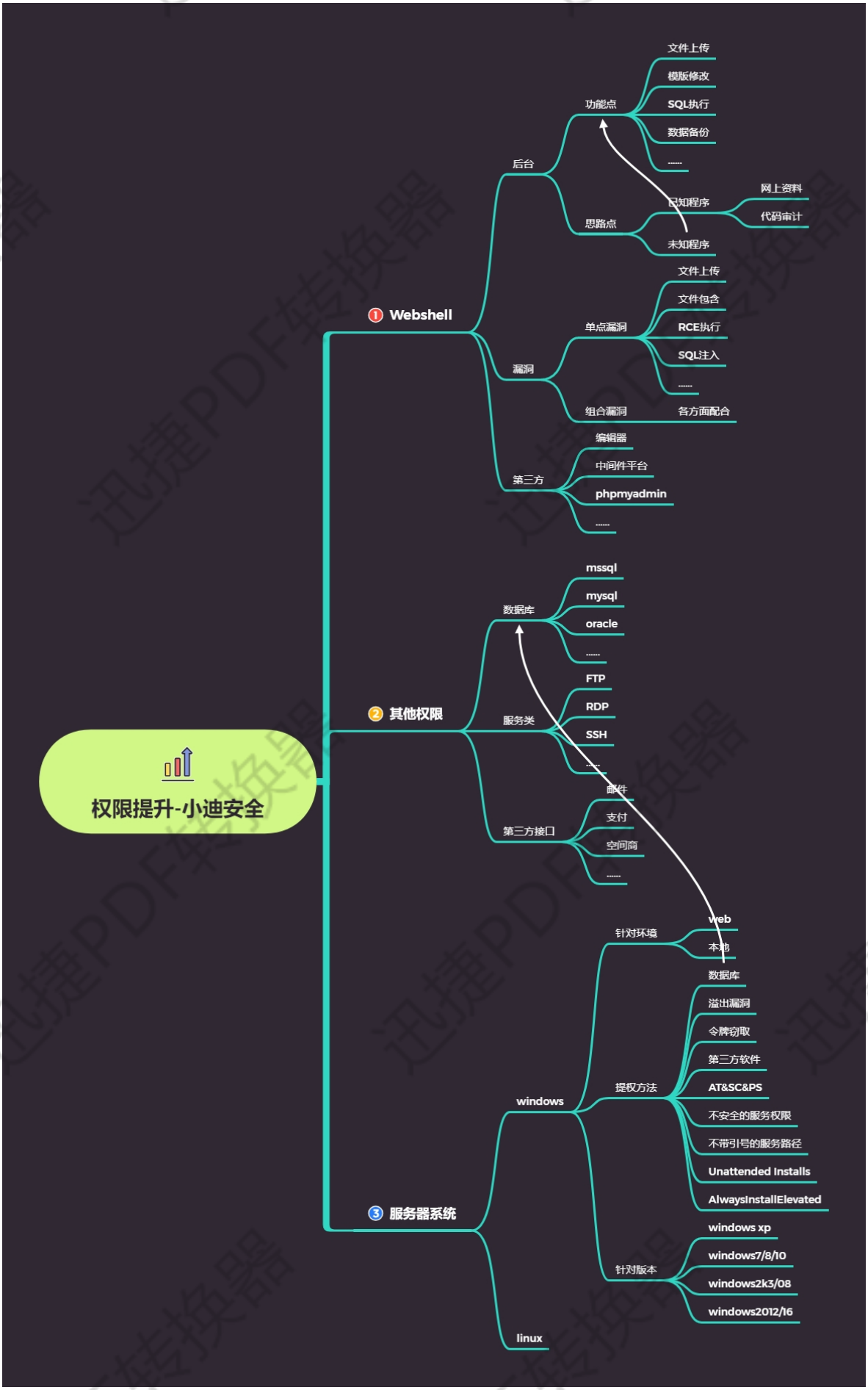
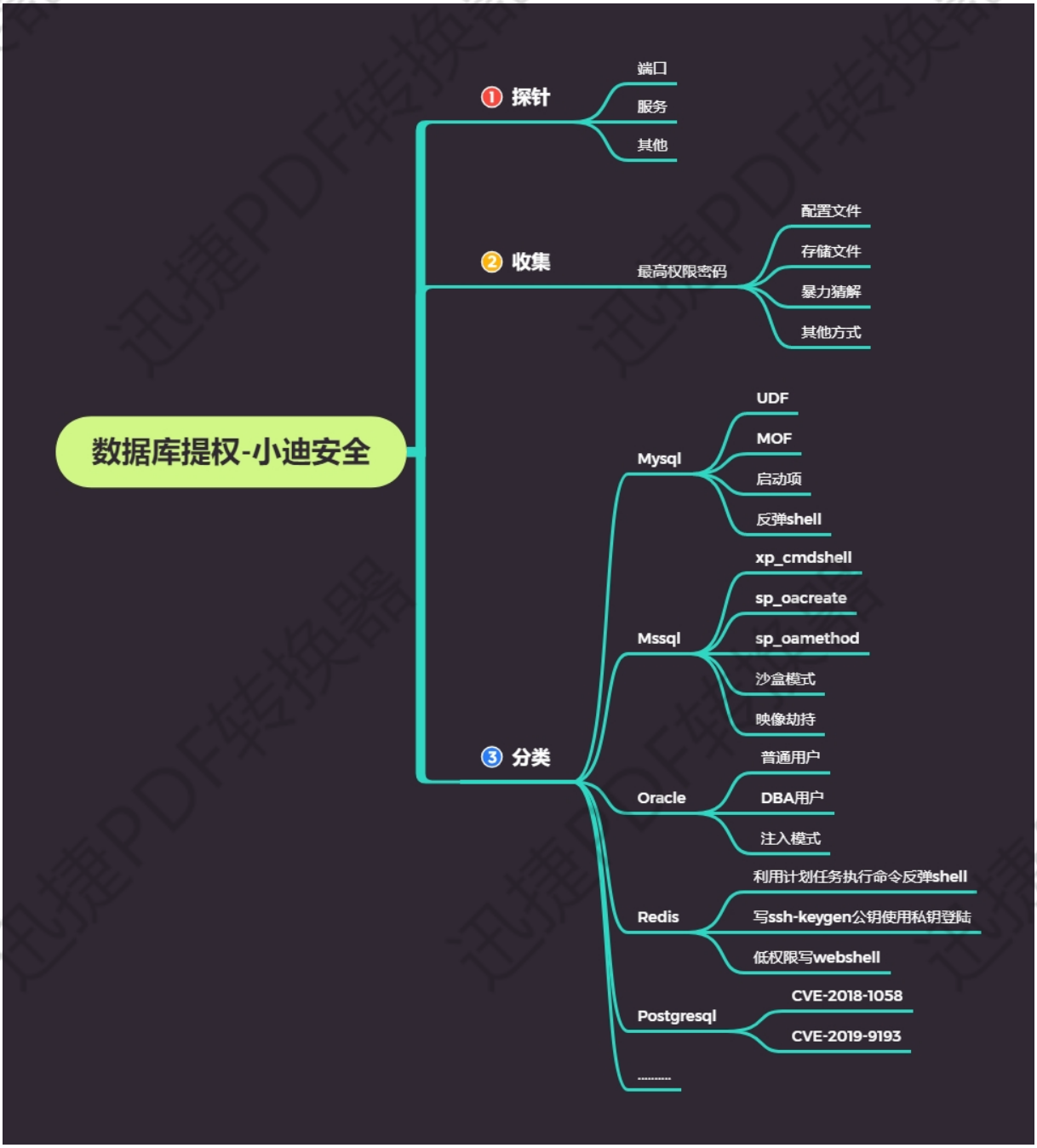
权限提升-Redis&Postgre&令牌窃取&进程注入

权限提升-Redis&Postgre&令牌窃取&进程注入


权限提升-小迪安全
1 Webshell
后台
功能点
文件上传
模版修改
SQL执行
数据备份
.....
思路点
已知程序
网上资料
代码审计
未知程序
漏洞
单点漏洞
文件上传
文件包含
RCE执行
SQL注入
.....
组合漏洞
各方面配合
第三方
编辑器
中间件平台
phpmyadmin
.....
2 其他权限
数据库
mssql
mysql
oracle
.....
服务类
FTP
RDP
SSH
.....
第三方接口
邮件
支付
空间商
.....
3 服务器系统
windows
针对环境
web
本地
提权方法
数据库
溢出漏洞
令牌窃取
第三方软件
AT&SC&PS
不安全的服务权限
不带引号的服务路径
Unattended Installs
AlwaysInstallElevated
针对版本
windows xp
windows7/8/10
windows2k3/08
windows2012/16
linux

在利用系统溢出漏洞无果的情况下，可以采用数据库进行提权，但需要知道数据库提权的前提条件：服务器开启数据库服务及获取到最高权限用户密码。除 Access 数据库外，其他数据库基本都存在数据库提权的可能。

#数据库应用提权在权限提升中的意义
#WEB 或本地环境如何探针数据库应用
#数据库提权权限用户密码收集等方法
#目前数据库提权对应的技术及方法等



演示案例：

- Redis 数据库权限提升-计划任务
- PostgreSQL 数据库权限提升-漏洞
- Windows2008&7 令牌窃取提升-本地
- Windows2003&10 进程注入提升-本地

#案例 1：Redis 数据库权限提升
Redis 服务因配置不当，可被攻击者恶意利用。黑客借助 Redis 内置命令，可将现有数据恶意清空；如果 Redis 以 root 身份运行，黑客可往服务器上写入 SSH 公钥文件，直接登录服务器。
连接(未授权或有密码)-利用如下方法提权
参考：https://blog.csdn.net/fly_hps/article/details/80937837
(1).利用计划任务执行命令反弹 shell
(2).写 ssh-keygen 公钥然后使用私钥登陆
(3).权限较低往 web 物理路径写 webshell
修复方案：
注意：以下操作，均需重启 Redis 后才能生效。
绑定需要访问数据库的 IP。 将 127.0.0.1 修改为需要访问此数据库的 IP 地址。
设置访问密码。在 Redis.conf 中 requirepass 字段后，设置添加访问密码。
修改 Redis 服务运行账号。以较低权限账号运行 Redis 服务，禁用账号的登录权限。

#案例 2：PostgreSQL 数据库权限提升
PostgreSQL 是一款关系型数据库。其 9.3 到 11 版本中存在一处“特性”，管理员或具有“COPY TO/FROM PROGRAM”权限的用户，可以使用这个特性执行任意命令。
提权利用的是漏洞：CVE-2019-9193 CVE-2018-1058
连接-利用漏洞-执行-提权
参考：https://vulhub.org/#/environments/postgres/
修复方案：升级版本或打上补丁

#案例 3:Windows2008&7 令牌窃取提升-本地
进行远程过程调用时请求提升权限，然后调用它从而生成特权安全令牌以执行特权操作。当系统允许令牌不仅用于进程本身，还用于原始请求进程时，漏洞就会出现。
本地提权实验：获取会话-利用模块-窃取令牌-提权
Microsoft Windows XP Professional SP3 和之前版本
Windows Server 2003 SP2 和之前的版本
Windows Server 2003 x64 和 x64 SP2
Windows Server 2003（用于基于 Itanium 的系统 SP2 和先前版本）
Windows Server 2008 x32 x64
Windows Server 2008（用于基于 Itanium 的系统）
Windows Vista SP1 和之前的版本
Windows Vista x64 SP1 和之前的版本
use incognito
list_tokens -u

impersonate_token "NT AUTHORITY\SYSTEM"

#案例 4:Windows2003&10 进程注入提升
进程注入提权是本地提权方式的一种较为老的安全技术了，利用的是注入进程的所有者实现权限共享机制，这类技术主要利用在 windows2008 之前操作系统上.所以我们需要学习后续的本地提权更多的手法才能有针对高版本的系统。
pinjector 进程注入工具针对-win2008 以前操作系统
pexec64 32 进程注入工具针对-win2008 及后操作系统-（佛系）

涉及资源:

https://www.blib.cn/soft/pexec.zip

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

https://www.tarasco.org/security/Process_Injector/processinjector.zip

---