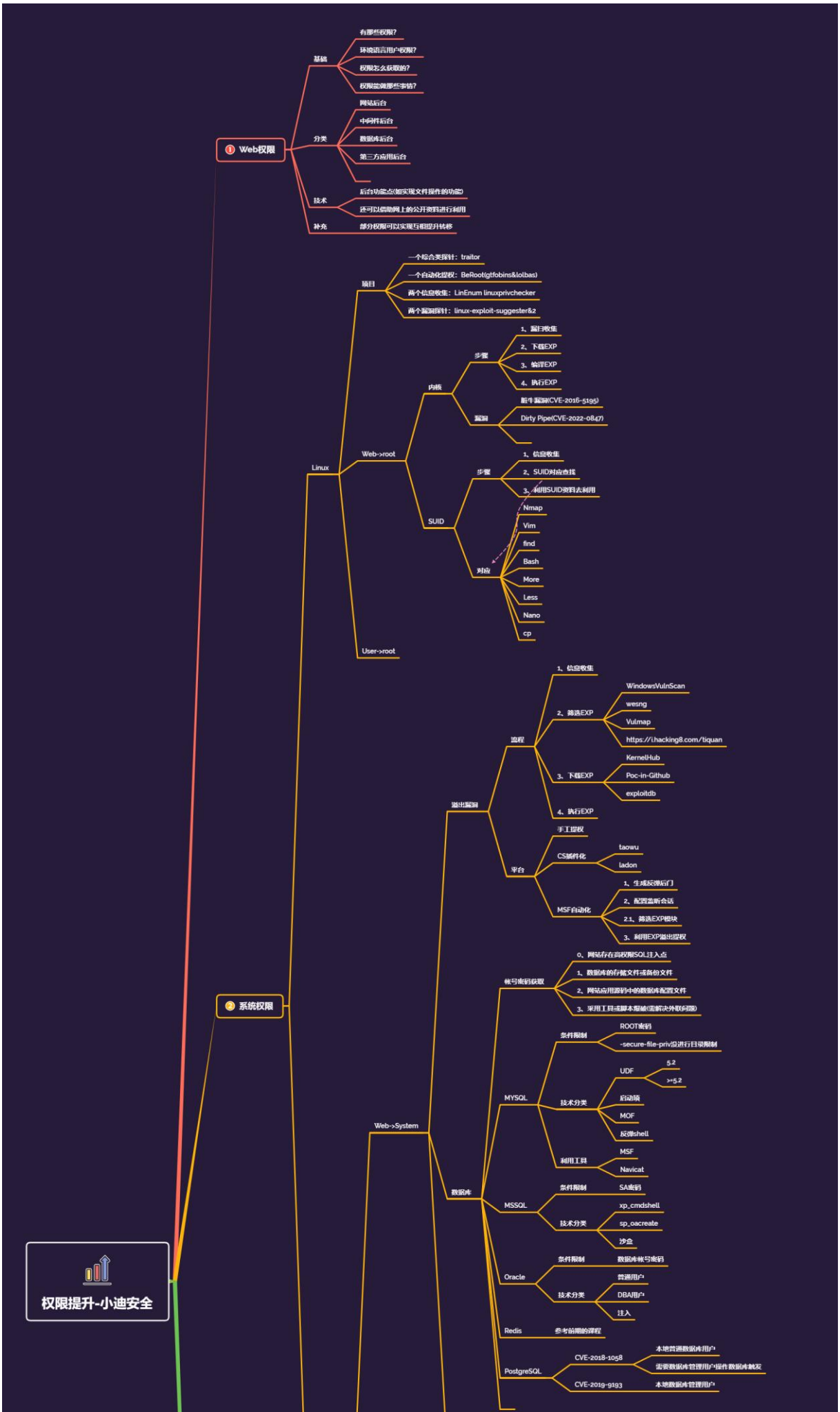
权限提升-Linux 系统&辅助项目&脏牛&Dirty&内核漏洞&SUID&GUID


权限提升-小迪安全
1 Web权限
基础
有哪些权限?
环境语言用户权限?
权限怎么获取的?
权限能做那些事情?
分类
网站后台
中间件后台
数据库后台
第三方应用后台
技术
后台功能点(如实现文件操作的功能)
还可以借助网上的公开资料进行利用
补充
部分权限可以实现互相提升转移
2 系统权限
Linux
项目
一个综合类探针：traitor
一个自动化提权：BeRoot(gtfobins&lolbas)
两个信息收集：LinEnum linuxprivchecker
两个漏洞探针：linux-exploit-suggester&2
Web->root
内核
步骤
1、漏扫收集
2、下载EXP
3、编译EXP
4、执行EXP
漏洞
脏牛漏洞(CVE-2016-5195)
Dirty Pipe(CVE-2022-0847)
SUID
步骤
1、信息收集
2、SUID对应查找
3、利用SUID资料去利用
对应
Nmap
Vim
find
Bash
More
Less
Nano
cp
User->root
Web->System
溢出漏洞
流程
1、信息收集
2、筛选EXP
WindowsVulnScan
wesng
Vulmap
https://i.hacking8.com/tiquan
3、下载EXP
KernelHub
Poc-in-Github
exploitdb
4、执行EXP
平台
手工提权
CS插件化
taowu
ladon
MSF自动化
1、生成反弹后门
2、配置监听会话
2.1、筛选EXP模块
3、利用EXP溢出提权
数据库
帐号密码获取
0、网站存在高权限SQL注入点
1、数据库的存储文件或备份文件
2、网站应用源码中的数据库配置文件
3、采用工具或脚本爆破(需解决外联问题)
MYSQL
条件限制
ROOT密码
-secure-file-priv没进行目录限制
技术分类
UDF
5.2
>=5.2
启动项
MOF
反弹shell
利用工具
MSF
Navicat
MSSQL
条件限制
SA密码
技术分类
xp_cmdshell
sp_oacreate
沙盒
Oracle
条件限制
数据库帐号密码
技术分类
普通用户
DBA用户
注入
Redis
参考前期的课程
PostgreSQL
CVE-2018-1058
本地普通数据库用户
需要数据库管理用户操作数据库触发
CVE-2019-9193
本地数据库管理用户

#知识点：

1、Linux 提权辅助项目-探针&漏扫

2、Linux 提权-配置 SUID&内核 CVE

#系列内容：

内核，数据库，第三方服务，SUID&GUID，定时任务，环境变量，SUDO，权限不当等

脏牛漏洞(CVE-2016-5195)

Dirty Pipe(CVE-2022-0847)

SUDO(CVE-2021-3156）

Polkit(CVE-2021-4034)

#截至目前思路点总结如下：

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

#截至目前思路点总结如下：

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

#思考点：

1、如何判断采用什么数据库提权？

2、数据库提权首要条件密码获取？

3、有那些数据库类型可以进行提权？

4、操作系统在数据库提权中有那些疑问？

演示案例：

- Linux-辅助项目配置安全&内核漏洞-探针漏扫
- Linux-配置安全 SUID 提权探针&利用-云服务器
- Linux-内核漏洞本地用户提权-探针&利用-墨者
- Linux-内核漏洞 Web 用户提权-探针&利用-脏牛
- Linux-内核漏洞本地用户提权-探针&利用-DirtyPipe

#Linux-辅助项目配置安全&内核漏洞-探针&漏扫

https://github.com/liamg/traitor

https://github.com/AlessandroZ/BeRoot

https://github.com/rebootuser/LinEnum

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

https://github.com/sleventyeleven/linuxprivchecker

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

一个综合类探针：traitor

一个自动化提权：BeRoot(gtfobins&lolbas)

两个信息收集：LinEnum linuxprivchecker

两个漏洞探针：linux-exploit-suggester&2

二进制文件提权查询：

Linux：https://gtfobins.github.io/

Windows：https://lolbas-project.github.io/

#Linux-配置安全 SUID 提权-探针&利用-云服务器

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

手工命令探针安全：

```
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 {} \;
```

脚本项目探针安全

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址