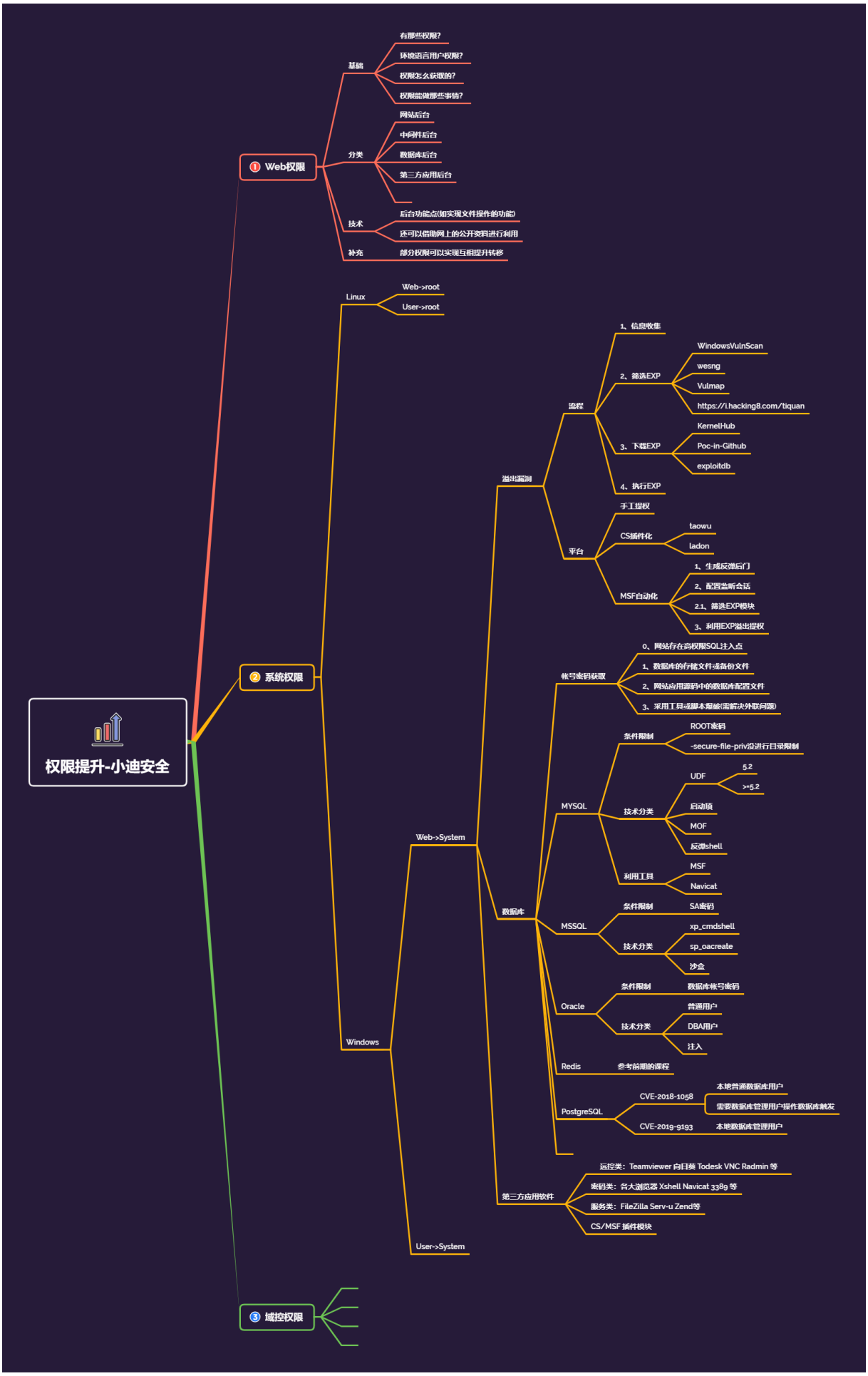
权限提升-Win 本地用户&进程注入&令牌窃取&AT&SC&PS 服务命令


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
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
第三方应用软件
远控类：Teamviewer 向日葵 Todesk VNC Radmin 等
密码类：各大浏览器 Xshell Navicat 3389 等
服务类：FileZilla Serv-u Zend等
CS/MSF 插件模块
User->System
③ 域控权限

#知识点：

1、服务配置-AT&SC&PS 命令

2、权限迁移-令牌窃取&进程注入

#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？

#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

演示案例：

- WIN-本地用户-AT&SC&PS 命令
- WIN-本地用户-进程迁移注入获取
- WIN-本地&Web-令牌窃取&土豆溢出

#WIN-本地用户-AT&SC&PS 命令

1、at 命令提权的原理

at 命令是一个计划命令，可以在规定时间完成一些操作，这个命令调用 system 权限。

适用版本：Win2000 & Win2003 & XP 中还是存在的，在 Win7 以后被剔除.

当我们拿到低权限的用户，通过连接上服务器后，可以通过 at 命令来进行本地提权。

提权命令：Test in Win2k3

at 21:00 /interactive cmd (在 20:33 分生成一个交互式的 System 权限的 cmd)

2、sc 是用于与服务控制管理器和服务进行通信的命令行程序。提供的功能类似于控制面板中管理工具项中的服务。适用版本：windows 7、8、03、08、12、16（win2k3 ok 其他未测基本失败）

提权命令：Test in Win2k3

#创建一个名叫 syscmd 的新的交互式的 cmd 执行服务

sc Create syscmd binPath= "cmd /K start" type= own type= interact

#运行服务

sc start syscmd

3、适用版本：Test in Win2012 and Win2008 & Win2016 其他未测 基本可以

https://docs.microsoft.com/zh-cn/sysinternals/downloads/pstools

psexec.exe -accepteula -s -i -d cmd #调用运行 cmd

#WIN-本地用户-进程迁移注入获取

相当于开了一个后门，注入到其他用户进程下！

1、Win2008 以前版本 -Test in Win2k3-本地权限-本地虚拟机

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址