SWRhapsody

Linux Privilege Escalation Cheat Sheet

于3月 9, 2018由**SWRhapsody**发布

从各个网站收集的Cheet sheet

各种脚本:

LinEnum : github

LinuxPrivChecker: download url

Blog:

g0tmi1k's Blog: blog url

Kernel, Operating System & Device Information:

```shell
uname -a    #Print all available system information
uname -r    #Kernel release
uname -n    #System hostname
hostname    #As above
uname -m    #Linux kernel architecture (32 or 64 bit)
cat /proc/version   #Kernel information
cat /etc/*-release  #Distribution information
cat /etc/issue          #As above
cat /proc/cpuinfo   #CPU information
df -a                   #File system information
```

Users & Groups:

```shell
cat /etc/passwd     #List all users on the system
cat /etc/group          #List all groups on the system

for i in $(cat /etc/passwd 2>/dev/null| cut -d":" -f1 2>/dev/null);do id $i;done 2>/dev/null
#List all uid's and respective group memberships

cat /etc/shadow     #Show user hashes – Privileged command

grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}'
#List all super user accounts

```

SWRhapsody

```
17 last                    #Listing of last logged on users
18 lastlog              #Information on when all users last logged in
19 lastlog -u %username%   #Information on when the specified user last logged in
20 lastlog |grep -v "Never"    #Entire list of previously logged on users
```

User & Privilege Information:

```shell
1  whoami      #Current username
2  id          #Current user information
3  cat /etc/sudoers    #Who's allowed to do what as root - Privileged command
4  sudo -l             #Can the current user perform anything as root
5
6  sudo -l 2>/dev/null | grep -w 'nmap|perl|'awk'|'find'|'bash'|'sh'
7  |'man'|'more'|'less'|'vi'|'vim'|'nc'|'netcat'|python
8  |ruby|lua|irb' | xargs -r ls -la 2>/dev/null
9  #Can the current user run any 'interesting' binaries as root
10 #and if so also display the binary permissions etc
```

Environmental Information:

Interesting Files:

```shell
1  find / -perm -4000 -type f 2>/dev/null  #Find SUID files
2  find / -uid 0 -perm -4000 -type f 2>/dev/null   #Find SUID files owned by root
3  find / -perm -2000 -type f 2>/dev/null  #Find GUID files
4  find / -perm -2 -type f 2>/dev/null     #Find world-writeable files
5
6  find / ! -path "*/proc/*" -perm -2 -type f -print 2>/dev/null
7  #Find world-writeable files excluding those in /proc
8
9  find / -perm -2 -type d 2>/dev/null     #Find word-writeable directories
10 find /home -name *.rhosts -print 2>/dev/null    #Find rhost config files
11
12 find /home -iname *.plan -exec ls -la {} ; -exec cat {} 2>/dev/null ;
13 #Find *.plan files, list permissions and cat the file contents
14
15 find /etc -iname hosts.equiv -exec ls -la {} 2>/dev/null ; -exec cat {} 2>/dev/null ;
16 #Find hosts.equiv, list permissions and cat the file contents
17
18 ls -ahlR /root/
19 #See if you can access other user directories to find interesting files
20
21 cat ~/.bash_history     #Show the current users' command history
22 ls -la ~/.*_history     #Show the current users' various history files
23 ls -la /root/.*_history     #Can we read root's history files
24 ls -la ~/.ssh/          #Check for interesting ssh files in the current users' directory
25
26 find / -name "id_dsa*" -o -name "id_rsa*" -o -name "known_hosts" -o -name "authorized_hosts" -
27 #Find SSH keys/host information
28
29 ls -la /usr/sbin/in.*      #Check Configuration of inetd services
30 grep -l -i pass /var/log/*.log 2>/dev/null
31 #Check log files for keywords ('pass' in this example) and show positive matches
```

SWRhapsody

```
#List .log files in specified directory (/var/log)

find /etc/ -maxdepth 1 -name *.conf -type f -exec ls -la {} ; 2>/dev/null
#List .conf files in /etc (recursive 1 level)

ls -la /etc/*.conf  #As above
find / -maxdepth 4 -name *.conf -type f -exec grep -Hn password {} ; 2>/dev/null
#Find .conf files (recursive 4 levels) and output line number where the word 'password' is loc
lsof -i -n          #List open files (output will depend on account privileges)
head /var/mail/root     #Can we read roots mail
```

Service Information:

Jobs/Tasks:

Networking, Routing & Communications:

Programs Installed:

Common Shell Escape Sequences:

Escape pseudo TTY

```shell
python -c "import pty; pty.spawn('/bin/bash');"
```

参考:

[1] https://www.rebootuser.com/?p=1623

分类: CHEAT SHEET PENETRATION TEST

0 条评论

SWRhapsody

名称 *

电子邮件 *

网站

在想些什么?

发表评论

近期文章

携程Apollo YAML 反序列化

CVE-2020-5410

CodeQL部分源码简读

服务器与网关的不一致

CodeQL 部分使用记录

近期评论

文章归档

2020年8月

SWRhapsody

2020年3月

2020年1月

2019年12月

2019年11月

2019年8月

2019年7月

2019年5月

2019年4月

2019年1月

2018年11月

2018年10月

2018年9月

2018年4月

2018年3月

2018年2月

2018年1月

分类目录

Article Collection

Cheat Sheet

cryptography

Exercise

Exploit

SWRhapsody

Uncategorized

相关文章

PENETRATION TEST

服务器与网关的不一致

前言 一次渗透测试时遇到的，官方认为不是漏洞。 Code 遇到了大约这 阅读更多…

CHEAT SHEET

CodeQL 部分使用记录

前言 CodeQL 是一个代码分析引擎，主要原理是通过对代码进行构建并 阅读更多…

CHEAT SHEET

Wpscan

记录些收集的wpscan的cheat sheet 和一些对wordpr 阅读更多…

SWRhapsody

Hestia | 由 Themeisle 开发