ATRAK - DOS

# DEFACEMMENT ATTACK

## CREAR PERFIL VOLATILITY

MARCOS | DANIEL | PEDRO

# CONTENIDO

### ANALIZAR LA MEMORIA RAM

Para ello vamos a necesitar la MEMORIA RAM para poder analizarlo y poder crear el perfil necesario para que pueda leer el volatility correctamente y sin fallos.
Vamos a usar el siguiente comando para poder sacar información valiosa para crear nuestro perfil.

**COMANDO**

```
strings RAM.bin | grep -i 'Linux version' | uniq
```

Con lo cual nos proporciona la siguiente salida:

**SALIDA**

```
Jul 20 09:10:35 ip-172-31-47-60 kernel: [    0.000000] Linux version 4.4.0-1061-aws
(buildd@lgw01-amd64-024) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) )
#70-Ubuntu SMP Fri May 25 21:47:34 UTC 2018 (Ubuntu 4.4.0-1061.70-aws 4.4.131)
Linux version 4.4.0-1061-aws (buildd@lgw01-amd64-024) (gcc version 5.4.0 20160609 (Ubuntu
5.4.0-6ubuntu1~16.04.9) ) #70-Ubuntu SMP Fri May 25 21:47:34 UTC 2018 (Ubuntu
4.4.0-1061.70-aws 4.4.131)
Value ranges after VRP/* Bit values & structures for resource limits.  Linux version.
 * may be different for different linux versions..
Value ranges after VRP/* Bit values & structures for resource limits.  Linux version.
MESSAGE=Linux version 4.4.0-1061-aws (buildd@lgw01-amd64-024) (gcc version 5.4.0 20160609
(Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #70-Ubuntu SMP Fri May 25 21:47:34 UTC 2018 (Ubuntu
4.4.0-1061.70-aws 4.4.131)
```

Vemos que existe el Gcc en la versión **[gcc versión 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9)** y el kernel en la version **[Linux version 4.4.0-1061-aws]**, con lo cual en el siguiente punto se va descargar los ficheros.

### ¿QUE SE NECESITA PARA CREAR EL PERFIL?

Para poder crear el perfil vamos a necesitar:

- Ubuntu 16.04.7
- Volatility
- Ubuntu 5.4.0-6ubuntu1~16.04.9
- Linux version 4.4.0-1061-aws

Una vez tengamos todo descargado y instalado en nuestro Sistema Operativo vamos a poner el GCC y el Kernel correspondiente para poder crear el perfil, vamos a usar el siguiente comando:

**COMANDO**

```
sudo dpkg -i gcc-5_5.4.0-6ubuntu1~16.04.9_amd64.deb
```

```
sudo dpkg -i linux-aws-headers-4.4.0-1061_4.4.0-1061.70_all.deb
linux-headers-4.4.0-1061-aws_4.4.0-1061.70_amd64.deb
linux-image-4.4.0-1061-aws-dbgsym_4.4.0-1061.70_amd64.ddeb
linux-image-4.4.0-1061-aws_4.4.0-1061.70_amd64.deb
```

Una vez puesto los comandos nos deberá salir de la siguiente forma si ponemos el GCC [CAPTURA DE GCC] y ponemos el kernel [CAPTURA DE KERNEL] con el comando, una vez instalado debemos hacer reboot para efectuar los cambios.
Ten en cuenta que al hacer este cambio si se está en una máquina virtual no podrá usar ni el ratón ni el teclado, ya que no se detecta.

**CREAMOS EL PERFIL**

Ya tenemos nuestro Ubuntu como la MEMORIA RAM que debemos analizarla, con lo cual vamos a crear el perfil, con lo cual vamos a necesitar los siguiente comando:

| COMANDO | cd volatility/tools/linux |
|---|---|
| | make |

Ahora vemos que se ha creado el make con lo cual se nos muestra su salida [CAPTURA MAKE].

**SALIDA**

```
make -C //lib/modules/4.4.0-1061-aws/build CONFIG_DEBUG_INFO=y
M="/opt/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-4.4.0-1061-aws'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: se sale del directorio '/usr/src/linux-headers-4.4.0-1061-aws'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.4.0-1061-aws/build M="/opt/volatility/tools/linux" clean
make[1]: se entra en el directorio '/usr/src/linux-headers-4.4.0-1061-aws'
  CLEAN   /opt/volatility/tools/linux/.tmp_versions
  CLEAN   /opt/volatility/tools/linux/Module.symvers
make[1]: se sale del directorio '/usr/src/linux-headers-4.4.0-1061-aws'
```

Vamos a crear el Zip para podemos en el perfil y con lo cual se tiene que hacer con el siguiente comando.

| COMANDO | zip $(lsb_release -i -s)_$(uname -r)_profile.zip /opt/volatility/tools/linux/module.dwarf /boot/System.map-$(uname -r) |
|---|---|

Vemos la salida de que se ha creado correctamente el [PERFIL RAM]

**SALIDA**

```
  adding: opt/volatility/tools/linux/module.dwarf (deflated 89%)
  adding: boot/System.map-4.4.0-1061-aws (deflated 79%)
```

Ahora se ve que se ha creado correctamente el Zip [CAPTURA ZIP]

## COMPROBAMOS QUE FUNCIONES CORRECTAMENTE

Ahora vamos comprobar que el perfil se ha creado correctamente y no nos de fallo al realizar el análisis de la memoria ram, con lo cual primero tenemos mover el perfil creado a la carpeta correspondiente con el siguiente comando:

**COMANDO**

```
cp Ubuntu_4.4.0-1061-aws_profile.zip
/opt/volatility/volatility/plugins/overlays/linux/
```

Vemos que se ha copiado correctamente el [PERFIL RAM] vamos ejecutar el Volatility para ver que se ejecuta correctamente para leer la MEMORIA RAM.
Para ello vamos a poner el siguiente comando para ver que el perfil está correctamente en la carpeta.

**CAPTURA**

```
root@usuario-VirtualBox:/opt/volatility/volatility/plugins/overlays/linux# vol.py --info
Volatility Foundation Volatility Framework 2.6.1


Profiles
--------
LinuxUbuntu_4_4_0-1061-aws_profilex64 - A Profile for Linux Ubuntu_4.4.0-1061-aws_profile x64
VistaSP0x64                           - A Profile for Windows Vista SP0 x64
VistaSP0x86                           - A Profile for Windows Vista SP0 x86
VistaSP1x64                           - A Profile for Windows Vista SP1 x64
VistaSP1x86                           - A Profile for Windows Vista SP1 x86
VistaSP2x64                           - A Profile for Windows Vista SP2 x64
VistaSP2x86                           - A Profile for Windows Vista SP2 x86
Win10x64                              - A Profile for Windows 10 x64
```

Ahora vamos a poner el siguiente comando para asegurar que funcione correctamente el perfil y no tenga fallos.

**COMANDO**

```
vol.py -f /home/usuario/Escritorio/RAM.bin
--profile=LinuxUbuntu_4_4_0-1061-aws_profilex64 linux_pslist
```

Vemos que no da ningún fallo en la salida del comando.

**SALIDA**

```
Volatility Foundation Volatility Framework 2.6.1
Offset             Name                 Pid             PPid            Uid             Gid    DTB                Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------------------ ----------
0xffff88003d458000 systemd              1               0               0               0      0x000000003cd48000 2018-07-20 09:10:30 UTC+0000
0xffff88003d458dc0 kthreadd             2               0               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d459b80 ksoftirqd/0          3               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45b700 kworker/0:0H         5               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45d280 rcu_sched            7               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45e040 rcu_bh               8               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45ee00 migration/0          9               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d4c8000 watchdog/0           10              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
```

## LISTO PARA ANALIZAR LA MEMORIA

Ahora solo falta analizar la memoria, pero ya con el perfil creado para que no tenga ningún fallo a la hora de analizarlo y buscar evidencia en él.

## ANEXO

### MEMORIA RAM

| | | |
|---|---|---|
| RAM | https://drive.google.com/file/d/1a32mvxnNhVIJDvtfJxji5mvcgLQMuhDx/view?usp=sharing | |
| HASH | SHA1 | bc2ebb435e75b3406280a2967b1c2696fc3e160a |
| | MD5 | e063c257d2f41ddee65ea1fdabe64e95 |

### PERFIL RAM

| | | |
|---|---|---|
| PERFIL | https://drive.google.com/file/d/1aet1uvfbV9l7TGAwmN6Vny_DuPL-eA9c/view?usp=share_link | |
| HASH | SHA1 | b0a43a53303c887879caad9ef02e24c7822328e5 |
| | MD5 | 2141106bc6a8530493d7756e44274b67 |

### CAPTURA DE GCC

**CAPTURA**

```
usuario@usuario-VirtualBox:~/Escritorio/GCC-KERNEL$ sudo dpkg -i gcc-5_5.4.0-6ubuntu1~16.04.9_amd64.deb
[sudo] password for usuario:
(Leyendo la base de datos ... 208842 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar gcc-5_5.4.0-6ubuntu1~16.04.9_amd64.deb ...
Desempaquetando gcc-5 (5.4.0-6ubuntu1~16.04.9) sobre (5.4.0-6ubuntu1~16.04.9) ...
dpkg: problemas de dependencias impiden la configuración de gcc-5:
 gcc-5 depende de cpp-5 (= 5.4.0-6ubuntu1~16.04.9); sin embargo:
  La versión de `cpp-5' en el sistema es 5.4.0-6ubuntu1~16.04.12.
 gcc-5 depende de gcc-5-base (= 5.4.0-6ubuntu1~16.04.9); sin embargo:
  La versión de `gcc-5-base:amd64' en el sistema es 5.4.0-6ubuntu1~16.04.12.
 gcc-5 depende de libgcc-5-dev (= 5.4.0-6ubuntu1~16.04.9); sin embargo:
  La versión de `libgcc-5-dev:amd64' en el sistema es 5.4.0-6ubuntu1~16.04.12.

dpkg: error al procesar el paquete gcc-5 (--install):
 problemas de dependencias - se deja sin configurar
Procesando disparadores para man-db (2.7.5-1) ...
Se encontraron errores al procesar:
 gcc-5
usuario@usuario-VirtualBox:~/Escritorio/GCC-KERNEL$ gcc --version
gcc (Ubuntu 5.4.0-6ubuntu1~16.04.9) 5.4.0 20160609
Copyright (C) 2015 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

### CAPTURA DE KERNEL

**CAPTURA**

```
usuario@usuario-VirtualBox:~/Escritorio/GCC-KERNEL$ sudo dpkg -i linux-aws-headers-4.4.0-1061_4.4.0-1061.70_all.deb linux-headers-4.4.0-1061-aws_4.4.0-1061.70_amd64.deb linux-image-4.4.0-1061-aws-dbgsym_4.4.0-1061.70_amd64.ddeb linux-image-4.4.0-1061-aws_4.4.0-1061.70_amd64.deb
Seleccionando el paquete linux-aws-headers-4.4.0-1061 previamente no seleccionado.
(Leyendo la base de datos ... 208842 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar linux-aws-headers-4.4.0-1061_4.4.0-1061.70_all.deb ...
Desempaquetando linux-aws-headers-4.4.0-1061 (4.4.0-1061.70) ...
```

CAPTURA

```
usuario@usuario-VirtualBox:~$ uname -a
Linux usuario-VirtualBox 4.4.0-1061-aws #70-Ubuntu SMP Fri May 25 21:47:34 UTC 2
018 x86_64 x86_64 x86_64 GNU/Linux
```

CAPTURA MAKE

CAPTURA

```
root@usuario-VirtualBox:/opt/volatility/tools/linux# make
make -C //lib/modules/4.4.0-1061-aws/build CONFIG_DEBUG_INFO=y M="/opt/volatility/tools/linux" modules
make[1]: se entra en el directorio '/usr/src/linux-headers-4.4.0-1061-aws'
  Building modules, stage 2.
  MODPOST 1 modules
make[1]: se sale del directorio '/usr/src/linux-headers-4.4.0-1061-aws'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/4.4.0-1061-aws/build M="/opt/volatility/tools/linux" clean
make[1]: se entra en el directorio '/usr/src/linux-headers-4.4.0-1061-aws'
  CLEAN   /opt/volatility/tools/linux/.tmp_versions
  CLEAN   /opt/volatility/tools/linux/Module.symvers
make[1]: se sale del directorio '/usr/src/linux-headers-4.4.0-1061-aws'
root@usuario-VirtualBox:/opt/volatility/tools/linux#
```

CAPTURA ZIP

CAPTURA

```
root@usuario-VirtualBox:/opt/volatility/tools/linux# ll
total 2976
drwxr-xr-x 3 root root    4096 mar  5 18:21 ./
drwxr-xr-x 6 root root    4096 mar  5 17:58 ../
drwxr-xr-x 2 root root    4096 mar  5 17:58 kcore/
-rw-r--r-- 1 root root     384 mar  5 17:58 Makefile
-rw-r--r-- 1 root root     314 mar  5 17:58 Makefile.enterprise
-rw-r--r-- 1 root root   17625 mar  5 17:58 module.c
-rw-r--r-- 1 root root 1993458 mar  5 18:14 module.dwarf
-rw-r--r-- 1 root root 1008463 mar  5 18:21 Ubuntu_4.4.0-1061-aws_profile.zip
```

CAPTURA CAMBIO DE CARPETA

CAPTURA

```
root@usuario-VirtualBox:/opt/volatility/volatility/plugins/overlays/linux# ll
total 1228
drwxr-xr-x 2 root root    4096 mar  5 18:31 ./
drwxr-xr-x 5 root root    4096 mar  5 17:59 ../
-rw-r--r-- 1 root root   26000 mar  5 17:58 elf.py
-rw-r--r-- 1 root root   28796 mar  5 17:59 elf.pyc
-rw-r--r-- 1 root root       0 mar  5 17:58 __init__.py
-rw-r--r-- 1 root root     148 mar  5 17:59 __init__.pyc
-rw-r--r-- 1 root root   86987 mar  5 17:58 linux.py
-rw-r--r-- 1 root root   80587 mar  5 17:59 linux.pyc
-rw-r--r-- 1 root root 1008463 mar  5 18:31 Ubuntu_4.4.0-1061-aws_profile.zip
```

## CAPTURA VOLATILITY

### CAPTURA

```
root@usuario-VirtualBox:/opt/volatility/volatility/plugins/overlays/linux# vol.py -f /home/usuario/Escritorio/RAM.bin --profile=LinuxUbuntu_4_4_0-1061-aws_profilex64 linux_pslist
Volatility Foundation Volatility Framework 2.6.1
Offset             Name                 Pid             PPid            Uid             Gid    DTB                Start Time
------------------ -------------------- --------------- --------------- --------------- ------ ------------------ ----------
0xffff88003d458000 systemd              1               0               0               0      0x000000003cd48000 2018-07-20 09:10:30 UTC+0000
0xffff88003d458dc0 kthreadd             2               0               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d459b80 ksoftirqd/0          3               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45b700 kworker/0:0H         5               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45d280 rcu_sched            7               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45e040 rcu_bh               8               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d45ee00 migration/0          9               2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d4c8000 watchdog/0           10              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d4fd280 kdevtmpfs            11              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d4fe040 netns                12              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d4fee00 perf                 13              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5a8000 xenwatch             14              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5a8dc0 xenbus               15              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5aa940 khungtaskd           17              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5ab700 writeback            18              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5ac4c0 ksmd                 19              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5ad280 khugepaged           20              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5ae040 crypto               21              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d5aee00 kintegrityd          22              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d618000 bioset               23              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d618dc0 kblockd              24              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
0xffff88003d619b80 ata_sff              25              2               0               0      ------------------ 2018-07-20 09:10:30 UTC+0000
```