UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

Seguridad y Calidad en Aplicaciones Web

Unidad N° 1: Introducción a la Seguridad

Referente de Cátedra: Walter R. Ureta
Plantel Docente: Pablo Pomar, Walter R. Ureta

OpenSSL

El Proyecto OpenSSL desarrolla y mantiene el software OpenSSL, un conjunto sólido de herramientas de grado comercial y con todas las funciones para el uso de criptografía de propósito general y comunicación segura. La toma de decisiones técnicas del proyecto está a cargo del Comité Técnico de OpenSSL (OTC) y la gobernanza del proyecto está a cargo del Comité de Gestión de OpenSSL (OMC). El proyecto opera bajo estatutos formales.

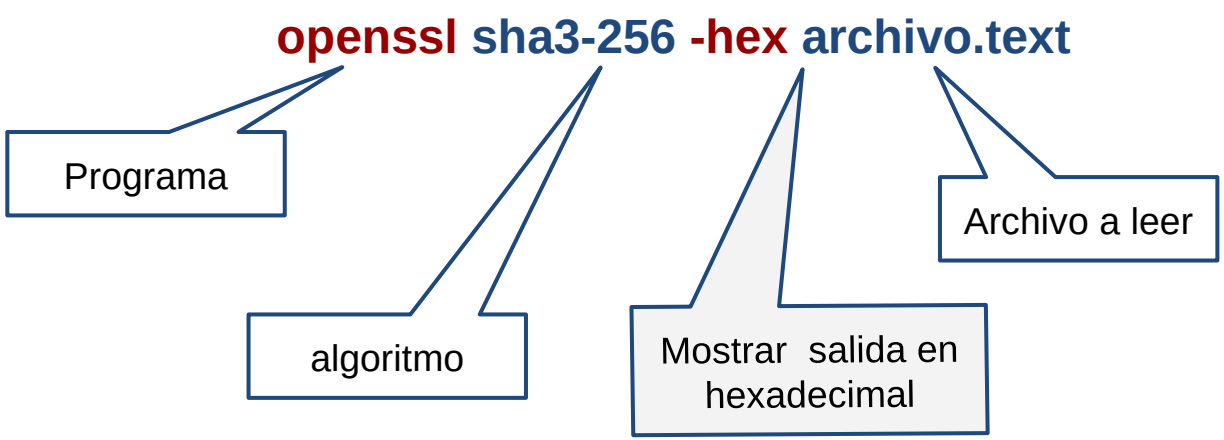
OpenSSL

Opciones asociadas a funciones de Hash o Digest

`blake2b512`	`blake2s256`	`gost`	`md4`
`md5`	`rmd160`	`sha1`	`sha224`
`sha256`	`sha3-224`	`sha3-256`	`sha3-384`
`sha3-512`	`sha384`	`sha512`	`sha512-224`
`sha512-256`	`shake128`	`shake256`	`sm3`

OpenSSL

Generar el valor de hash en formato hexadecimal utilizando un algoritmo determinado en base a la información contenida en un archivo:



HashDeep / md5deep

Hashdeep es un programa **Open Source** para calcular, verificar, y auditar hashsets. Con la comprobación tradicional, los programas informan si un archivo de entrada coincide con uno previamente registrado o no. Es difícil tener una idea completa de la situación de los archivos de entrada en comparación con el conjunto de datos conocidos. En este contexto es posible tener archivos emparejados, archivos que faltan, archivos que se han movido en el conjunto, y encontrar nuevos archivos en el conjunto. Hashdeep puede informar de todas estas condiciones.

HashDeep / md5deep - Instalación

Codigo Fuente

1. Descargar los fuentes de la página oficial
2. Descomprimir los fuentes: **tar zxvf md5deep-4.1.tar.gz**
3. Ingresar a la carpeta: **cd md5deep-4.1**
4. Configurar: **./configure** (usar el parámetro **"--prefix=/tmp/md5deep"** para indicar un directorio de instalación diferente)
5. Construir: **make**
6. Instalar: **make install**

Linux (Ubuntu-Debian)

7. Instalar con el comando: **sudo apt-get install md5deep**

Windows

8. Descargar binarios precompilados de la página oficial
9. Descomprimir la carpeta con los ejecutables.

HashDeep / md5deep - Opciones

Podemos obtener la lista de parámetros del programa invocando **hashdeep -h** ; sin embargo estos son los principales:

- **-a** - Modo de auditoría. Valida archivos contra una lista de hashes. Requiere **-k**
- **-m** - Modo de coincidencia. Requiere **-k**
- **-x** - Modo de coincidencia negativa. Requiere **-k**
- **-w** - en modo **-m**, muestra que archivos conocidos coincidieron.
- **-k** - Agrega un archivo de hashes conocidos
- **-r** - Modo recursivo. Incluye los subdirectorios
- **-e** - Calcula el tiempo estimado para completar cada archivo
- **-v** - Modo "verborrágico". Provee más detalles en la salida

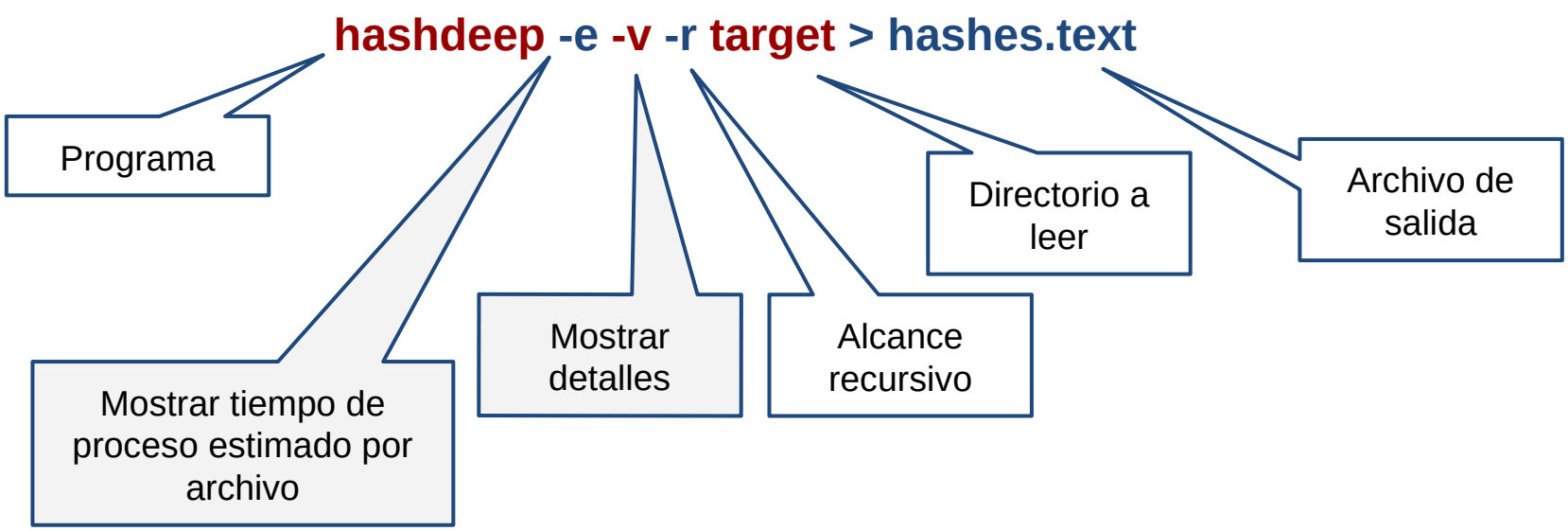
HashDeep / md5deep - Opciones

Otros parámetros opcionales de interés:

- **-c** alg1,alg2 Selecciona los algoritmos a utilizar, las opciones validas son **md5,sha1,sha256,tiger,whirlpool**
- **-l** Utiliza valores relativos para la ubicación de archivos
- **-p** Fracciona los archivos para el proceso de hashing
- **-i** Procesa solo archivo menores que un limite definido
- **-o** Procesa solo archivos de un tipo especifico

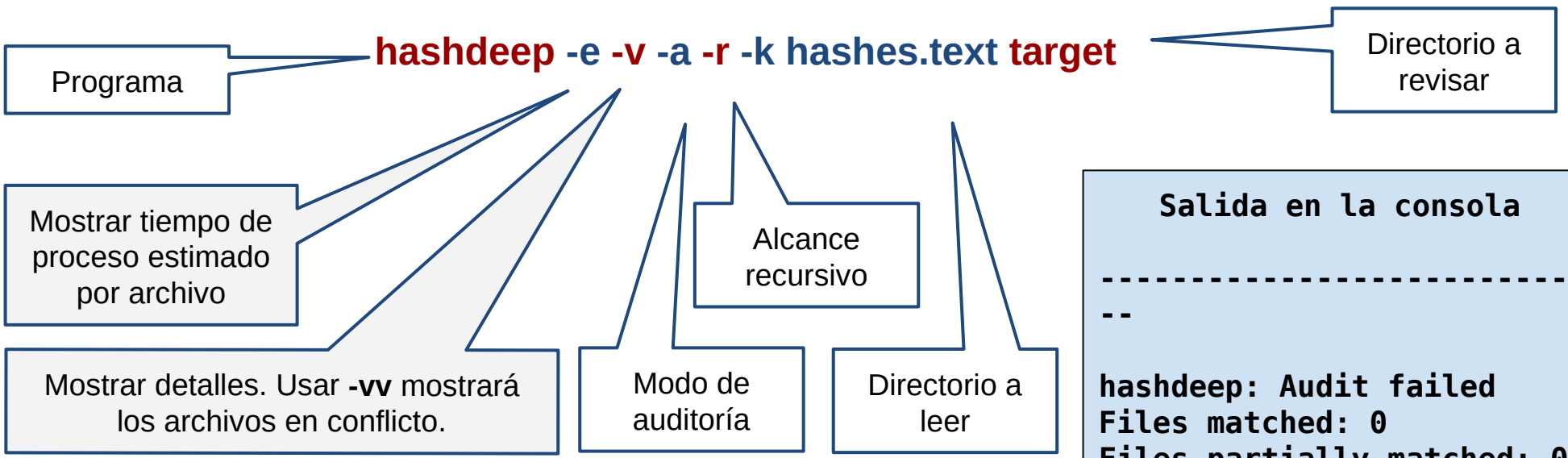
HashDeep / md5deep

Crear la lista de hashes para el directorio **"./target"** con alcance recursivo, almacenando esta información en el archivo **"hashes.text"**. *(-e y -v son opcionales en este caso)*



HashDeep / md5deep

Comprobar recursivamente la integridad de los archivos del directorio **"./target"** utilizando la lista de hashes del archivo **"hashes.text"**.



Salida en la consola

```
--------------------------
--

hashdeep: Audit failed
Files matched: 0
Files partially matched: 0
Files moved: 0
New files found: 2
Known files not found: 2
```

HashDeep / md5deep

Listar los archivos del directorio **"./target"** que **coinciden** o **no** con la lista de hashes **"hashes.text".**

Listar los archivos que **coinciden** con la información de la lista

hashdeep -e -v -m -r -k hashes.text target

hashdeep -e -v -x -r -k hashes.text target

Listar los archivos que **NO coinciden** con la información de la lista

Tripwire

Tripwire es un programa **Open Source** con la finalidad de proveer un control de seguridad sobre la integridad de datos. Es útil para monitorear y alertar de cambios en los archivos del sistema. Opera comparando la firma/hash de archivos y directorios contra una base de datos de los mismos en un instante previo. Esta base de datos se genera tomando una instantánea en el momento de su instalación y se accede a ella mediante contraseña cifrada, por lo que su instalación en un sistema posiblemente infectado, carece de efectividad y se recomienda que su instalación y configuración sea hecha antes de haber conectado el computador por primera vez a internet. Funciona en sistemas operativos GNU/Linux.

Tripwire - Instalación

Ubuntu

1. Ejecutar: **sudo apt-get install tripwire**

Red-Hat (root)

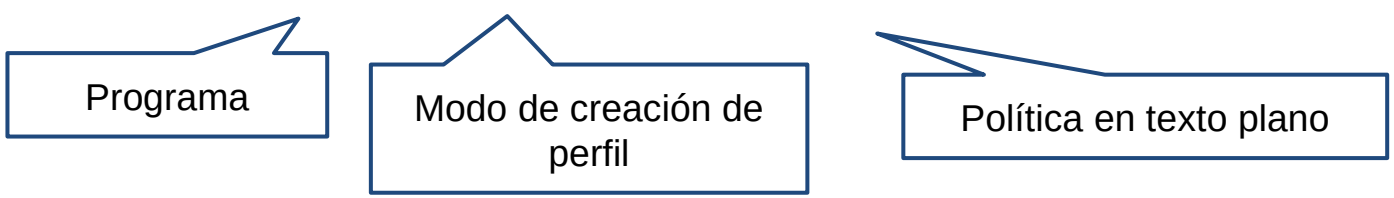
2. Descargar el archivo del sitio oficial
3. Descomprimirlo con el comando: **tar xvzf tripwire.tar.gz**
4. Instalar con: **rpm -ivh tripwire-2.3-47.i386.rpm**
5. Crear las claves del sitio y local: **/etc/tripwire/twinstall.sh**

Tripwire - Política

La política de Tripwire define qué archivos se están controlando y el criterio a utilizar en los mismos. Con tal fin debemos editar un archivo de texto con la información de configuración de dicha política y luego actualizar la instalación.

Estos son los pasos a utilizar

1. Acceder al directorio de configuración: **cd /etc/tripwire**
2. Editar el archivo de texto con la política: **vi twpol.txt**
3. Importar la nueva política a la configuración:
   - **twadmin --create-polfile --cfgfile ./tw.cfg --site-keyfile ./site.key ./twpol.txt**
   - **twadmin -m P /etc/tripwire/twpol.txt**



Tripwire - Envío de mails

La política puede definir el envio de e-mails utilizando la siguiente anotación en la cabecera de cada regla que requiera esta notificación:

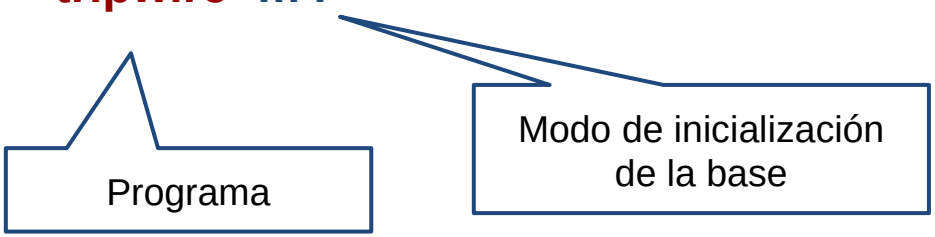
```
...
#      Kernel      Administration      Programs      #      #
(
      rulename   =   "Kernel   Administration   Programs",
     severity   =   $(SIG_HI),   emailto   =   root@localhost
)
{
   /sbin/depmod                                  -> $(SEC_CRIT) ;
   /sbin/adjtimex                                -> $(SEC_CRIT) ;
   /sbin/ctrlaltdel                              -> $(SEC_CRIT) ;
   /sbin/insmod                                  -> $(SEC_CRIT) ;
...
```

Nota: root@localhost debe ser reemplazado por la dirección del destinatario.

Tripwire - Inicializar la Base

Una vez instalada la nueva política debemos relevar la información actual del sistema y volcarla en la base de tripwire para los controles futuros, esta tarea la realizaremos con los siguientes comandos:

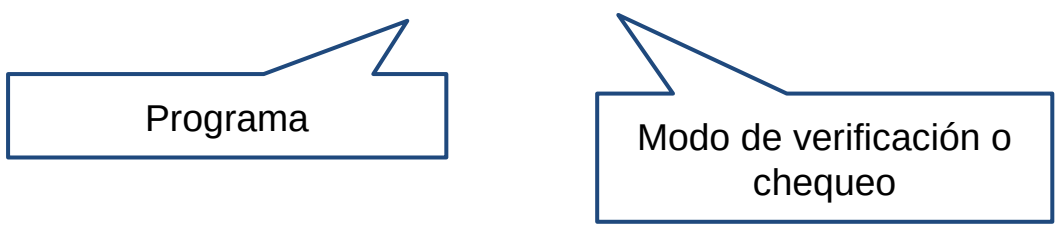
- **tripwire --init --cfgfile /etc/tripwire/tw.cfg --polfile /etc/tripwire/tw.pol --site-keyfile /etc/tripwire/site.key --local-keyfile /etc/tripwire/HOSTNAME-local.key**
- **tripwire -m i**



Tripwire - Verificación del FS

Con la información de los archivos confiables en la base podemos proceder a verificar o chequear su integridad en cualquier momento utilizando los siguientes comandos:

- **tripwire --check**
- **tripwire -m c**



Tripwire - Reportes

El reporte generado durante una verificación o chequeo se muestra por pantalla y se almacena en el directorio **"/var/lib/tripwire/report/"** del sistema de archivos. Su nombre esta sujeto a la siguiente convención **[Host]-[Año][Mes][Día]-[Hora][Minuto][Segundo].twr** y el contenido es binario, por esta razón se requiere de la herramienta **twprint** para poder visualizarlo.

Este es un ejemplo de la visualización de un reporte previo

```
twprint -m r -r /var/lib/tripwire/report/HOST-20130101-123456.twr
```

Programa

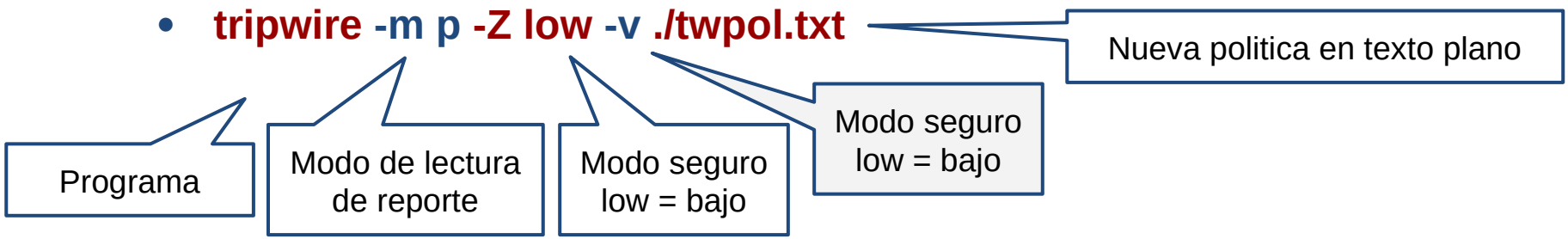
Modo de lectura de reporte

Reporte a leer

Tripwire - Actualización de Política

La política de control puede actualizarse regularmente utilizando los siguientes comandos:

- **tripwire --update-policy -v -Z low --cfgfile ./tw.cfg --polfile ./tw.pol --site-keyfile ./site.key --local-keyfile ./HOSTNAME-local.key ./twpol.txt**
- **tripwire -m p -Z low -v ./twpol.txt**

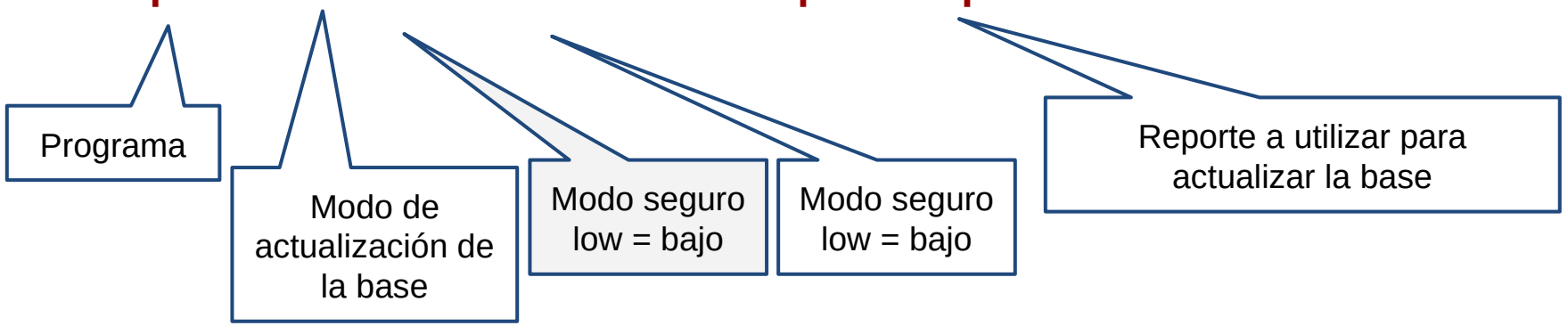


Nota: Los archivos de configuración y política permanecen encriptados en el sistema pero para ser ingresados se utilizan archivos en texto plano que pueden exponer información crítica ante un ataque. Por esta razón se recomienda que sean eliminados luego de su uso con **rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt**

Tripwire - Actualización de la Base

La base con información de los archivos confiables puede ser actualizada para incluir cambios controlados en el sistema. Esta tarea puede realizarse con los siguientes comandos:

- **tripwire --update -v -Z low -r /var/lib/tripwire/report/HOST-20130101-221053.twr**
- **tripwire -m u -v -Z low -r /var/lib/tripwire/report/HOST-20130101-221053.twr**



Nota: Es recomendable realizar un check inmediatamente ante de la actualización de la base. En caso contrario pueden aparecer errores en referencia a un archivo de reporte perdido.

Referencias

Lista de Software

OpenSSL: https://www.openssl.org/
Hashdeep/Md5deep: http://md5deep.sourceforge.net/
TripWire: http://www.tripwire.org/
Tripwire O.S.: http://sourceforge.net/projects/tripwire/