

ANEXO-Comprobadores-de-integridad_1

Unidad N° 1: Introducción a la Seguridad

OpenSSL

¿Qué es OpenSSL?

OpenSSL es un conjunto de herramientas que se usa para:

- Cifrar y descifrar datos (criptografía).
- Hacer comunicaciones seguras (como HTTPS en los navegadores).
- Generar y verificar firmas digitales, certificados SSL, y más.

¿Para qué se usa en general?

- Crear conexiones seguras (HTTPS).
- Generar certificados digitales.
- Calcular valores de hash o digest (que sirven para verificar la integridad de datos).
- Probar o usar distintos algoritmos de cifrado y firma.

¿Qué es un Hash?

Un hash es como una "huella digital" de un archivo o texto. Si el contenido cambia, el hash también cambia.

Sirve para:

- Verificar si un archivo fue modificado.
- Comparar contraseñas sin guardarlas directamente.
- Validar integridad de archivos descargados.

¿Qué son los algoritmos de hash?

Son los métodos para crear esos valores de hash. Algunos ejemplos son:

- `md5`, `sha256`, `sha3-512`, etc. Cada uno tiene diferentes niveles de seguridad y longitud del resultado.

¿Cómo se usa OpenSSL para calcular un hash?

Desde la consola o terminal, podés escribir algo como:

bash

`openssl sha3-256 -hex archivo.txt`

Eso te va a dar el valor de hash del archivo `archivo.txt` usando el algoritmo `sha3-256`, en formato hexadecimal.


[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.

¿Qué es HashDeep / md5deep?

HashDeep (y su versión más conocida md5deep) es una herramienta de código abierto que sirve para:

- Calcular hashes de archivos.
- Verificar si los archivos fueron modificados o si coinciden con un conjunto conocido.
- Auditar archivos comparándolos con una lista previa de hashes.
- Detectar archivos nuevos, faltantes o movidos.

 *Es como un detector de cambios o manipulaciones en archivos. Muy útil en seguridad informática y análisis forense.*

¿Para qué se usa?

- Crear un registro (lista) de archivos y sus hashes.
- Verificar después si esos archivos siguen iguales o fueron modificados.
- Detectar archivos nuevos, faltantes, o movidos.

Por ejemplo:

- Te bajás una carpeta de archivos de una página y luego querés saber si alguien los cambió.
- O tenés un backup y querés validar si sigue siendo idéntico al original.

✓ ¿Qué diferencia hay entre HashDeep y md5deep?

- `md5deep` fue el nombre original del proyecto.
- `hashdeep` es una versión más moderna que soporta **más algoritmos de hash**, no solo MD5.

✓ Algoritmos que soporta:

Podés usar varios algoritmos, por ejemplo:

- `md5`, `sha1`, `sha256`, `tiger`, `whirlpool`

Instalación

Desde código fuente:

1. Descargar: desde la página oficial.
2. Descomprimir:tar zxvf md5deep-4.1.tar.gz
3. Entrar a la carpeta:cd md5deep-4.1
4. configurar:./configure --prefix=/tmp/md5deep
5. Compilar e instalar:make install

En Linux:

(Ubuntu/Debian):bash `sudo apt-get install md5deep`

En Windows:

- Descargar los binarios precompilados desde la página oficial.

- Descomprimir la carpeta con los ejecutables.

[Opciones principales](#)

Opción	Función
<code>-a</code>	Modo auditoría: compara con lista de hashes (requiere <code>-k</code>).
<code>-m</code>	Modo coincidencia: busca archivos que coinciden con la lista (requiere <code>-k</code>).
<code>-x</code>	Coincidencia negativa: muestra los que no coinciden (requiere <code>-k</code>).
<code>-w</code>	En <code>-m</code> , muestra qué archivos conocidos coinciden.
<code>-k archivo</code>	Usa una lista de hashes conocida.
<code>-r</code>	Recursivo: analiza subdirectorios.
<code>-e</code>	Estima tiempo de proceso.
<code>-v</code>	Verborrágico: muestra más información.


[Opciones adicionales](#)

Opción	Función
<code>-c alg1,alg2</code>	Elegir algoritmos: <code>md5</code> , <code>sha1</code> , <code>sha256</code> , <code>tiger</code> , <code>whirlpool</code> .
<code>-l</code>	Usa rutas relativas.
<code>-p</code>	Fracciona archivos para hashing.
<code>-i</code>	Procesa solo archivos menores a un límite.
<code>-o</code>	Procesa solo archivos de un tipo específico .

Tripwire


¿Qué es Tripwire?

Tripwire es una herramienta open source que sirve para controlar la integridad de los archivos del sistema.

 ¿Qué significa esto? Que detecta si algún archivo fue cambiado, eliminado o agregado sin autorización.

¿Cómo lo hace?

- Guarda una base de datos con "firmas" (hashes) de todos los archivos importantes.
- Luego, compara periódicamente el estado actual del sistema con esa base de datos para detectar cambios.

 *Solo funciona bien si se instala en un sistema limpio (sin malware), antes de conectarlo a internet.*

Instalación


En Ubuntu / Debian:

```
sudo apt-get install tripwire
```

En Red Hat (Fedora, CentOS):

1. Descargar desde la web oficial.
2. Descomprimir: `tar xvzf tripwire.tar.gz`
3. Instalar: `rpm -ivh tripwire-2.3-47.i386.rpm`
4. Crear claves: `/etc/tripwire/twinstall.sh`

Política de Tripwire

 ¿Qué es la política? Es un archivo que define qué archivos se van a controlar, y cómo.

Pasos para configurar una política:

1. Ir al directorio de configuración: `cd /etc/tripwire`
2. Editar el archivo de política: `vi twpol.txt`
3. Compilar la política para que se aplique: `twadmin --create-polfile --cfgfile ./tw.cfg --site-keyfile ./site.key ./twpol.txt`

Tripwire - Envío de mails

Envío de correos (Opcional)

Podés configurar la política para que envíe mails cuando detecta cambios, agregando una línea especial en la cabecera de las reglas del archivo de política.

Inicialización de la base:

Una vez definida la política, hay que generar la "foto inicial" del sistema para comparar en el futuro:

```
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
```

Verificación del sistema (chequeo de integridad)

Se puede ejecutar Tripwire para verificar si hubo cambios no autorizados en los archivos:

```
tripwire --check
```

El reporte se guarda en:

```
/var/lib/tripwire/report/
```

Ejemplo de cómo ver un reporte:

```
twprint -m r -r  
/var/lib/tripwire/report/HOST-20250421-123456.twr
```

Actualizar la política

Si necesitás cambiar la política (por ejemplo, agregar nuevas carpetas a monitorear), usás estos comandos:

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

```
o tripwire -m p -Z low -v ./twpol.txt
```

¡IMPORTANTE!: Después de aplicar la política, eliminá los archivos `twcfg.txt` y `twpol.txt` porque contienen info sensible en texto plano: `rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt`

Actualizar la base de datos de hashes

Cuando hacés cambios legítimos en el sistema (como actualizar programas), podés actualizar la base de datos con este comando:

```
tripwire --update -v -Z low -r  
/var/lib/tripwire/report/HOST-20250421-221053.twr
```

```
tripwire --update -v -Z low -r  
/var/lib/tripwire/report/HOST-20250421-221053.twr
```

```
o tripwire -m u -v -Z low -r  
/var/lib/tripwire/report/HOST-20250421-221053.twr
```

Consejo: hacé una verificación (`--check`) antes de actualizar, para evitar errores si falta un reporte.