UT 1. Prácticas

**P1.1 –Confidencialidad con EFS**

**Objetivo**

Encriptación de archivos y carpetas en Windows mediante EFS (**Encrypting File System**).

**Desarrollo de la Práctica**

**EFS** es un sistema de archivos que trabajando sobre NTFS permite cifrar archivos y carpetas. EFS es incompatible con la compresión de archivos.El usuario que realice la encriptación de archivos será el único que dispondrá de acceso a su contenido, y el único que podrá modificar, copiar o borrar el archivo.

1. **Proceso de encriptación**

Creamos un archivo de texto plano (no cifrado) con una información “confidencial” en su interior. Se indicarán el nombre, apellido y fecha de nacimiento de los alumnos que realicen la práctica

Seleccionamos el archivo y con el botón derecho accederemos a la ventana de Propiedades. En *General*, pulsamos en *Opciones Avanzadas* y en *atributos de compresión y cifrado* marcamos la opción cifrar contenido para proteger datos.

**Nota**: en caso de no tener habilitada dicha opción deberá ejecutarse *gpedit.msc* (editor de directivas de grupo) y habilitar la directiva local: *directiva de equipo local / configuración de Windows / configuración de seguridad / directivas de clave pública / sistema de cifrado de archivos*.

A continuación, comprimimos el archivo.

1. **Proceso de verificación**

Crea un nuevo usuario con permisos de administrador, que pueda acceder a todo el sistema de archivos. Accedemos al archivo con este nuevo usuario. Vemos que el nombre del archivo nos aparece en color verde.

1. ¿Qué ocurre si intentamos acceder a él desde el usuario no propietario?
2. ¿Qué ocurre si intentamos modificar los atributos desde el usuario no propietario
3. ¿Qué ocurre si intentamos enviarlo a una unidad externa desde el usuario no propietario?
4. ¿Qué ocurre si descomprimimos el archivo comprimido desde el usuario no propietario?
5. ¿Qué ocurre si intentamos comprimir el archivo desde el usuario no propietario?
6. ¿Qué ocurre si intentamos borrar el archivo desde el nuevo usuario?
7. ¿Qué relación puedes establecer entre cifrado y compresión para EFS?

<https://www.windowsnoticias.com/cifrar-archivo-windows-10/>

**INVESTIGAR EL FUNCIONAMIENTO DE BitLocker**

**Grupos:**2 alumnos por grupo

**Documentación a Entregar**

Documento PDF con el nombre**UT1\_P11.pdf**. En la portada del documento aparecerá el título de la práctica, junto con los nombres de los componentes del grupo de prácticas:

Deberán aparecer en el documento los resultados de los apartados 1 y 2

**Plazo de entrega:**Por determinar.

**P1.2– Disponibilidad con NMAP**

**Objetivo**

Identificar y analizar la disponibilidad de servicios o servidores, puertos abiertos que supondrá la información base para el estudio de las innumerables vulnerabilidades de los sistemas.

Nmap (“Network Mapper " ) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Cuando ejecutamos comandos se lista una tabla.

Dicha tabla lista **el número de puerto y protocolo**, **nombre del servicio, y el Estado**. El estado puede ser abierto, filtrado, cerrados, o sin filtrar.

* ***Abierto:*** significa que una aplicación en la máquina de destino se encuentra esperando conexiones/paquetes en ese puerto.
* *F****iltrada:*** significa que un cortafuegos, filtro, o obstáculo en la red está bloqueando el puerto para que Nmap no puede saber si está abierto o cerrado.
* ***Cerrado* los puertos** no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento.

Los clasificados como *no filtrados* son aquellos que responden a los sondeos de Nmap, pero que Nmap no puede determinar si están abiertas o cerradas

**Desarrollo de la Práctica**

**Nmap** (mapeador de redes) es una herramienta para exploración de red y auditoría de seguridad. Utiliza paquetes IP para determinar qué equipos se encuentran disponibles en una red, qué servicios ofrecen y qué aplicaciones ejecutan (nombre y versión de la aplicación), qué sistemas operativos ejecutan (y sus versiones), etc.

Una vez finalizado el proceso de mapeo, podremos identificar los puertos o servicios más vulnerables e inseguros, y qué equipos se encuentran con dicho puerto abierto.

1. **Verificación en sistemas Windows**

**Nmap** es puede utilizarse en modo comando o mediante una interfaz gráfica denominada **znmap** o **zenmap**.

Descarga e instala la aplicación desde<https://nmap.org>

Para los escaneos, utiliza la opción –F (quickscan, o escaneo rápido). La opción -A habilita la detección del sistema operativo y la versión.

1. Realiza un escaneo en la máquina virtual de Windows 7 poniendo tu IP en la casilla target. Guarda el escaneo como **WindowsXX.nmap**, donde xx es el último dígito de tu IP.
2. Realiza un escaneo de toda la red (poniendo la IP de la red con la máscara en la casilla target). Guárdalo como **WindowsXXred.nmap**, donde xx es el último dígito de tu IP.
3. Repite el escaneo de tu equipo en consola (fíjate en la casilla command del primer escaneo). Haz una captura de pantalla, y guárdala como **WindowsXXconsola**

**EJEMPLO:**

* Una vez instalado el programa lo ejecutamos y procedemos por ejemplo a realizar un escáner de los puertos de www.google.es





* También podemos realizar el escáner en modo consola. Nos muestra los puertos abiertos y cerrados.

1. **Verificación en sistemas Linux**

instala la aplicación desde la consola de Linux con el comando:

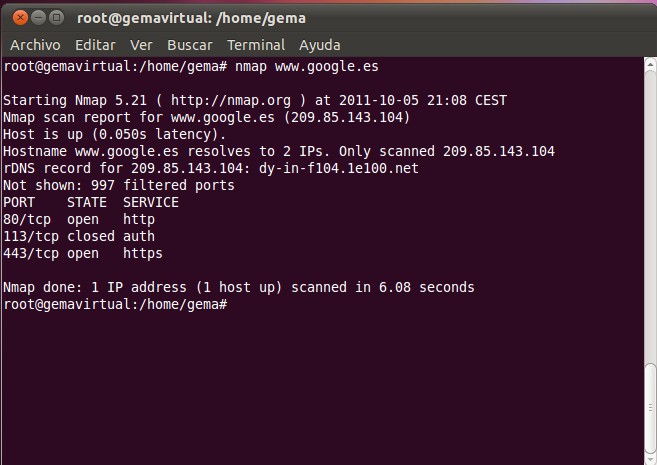
sudo apt-get install zenmap

1. Realiza un escaneo en la máquina virtual de poniendo tu IP en la casilla target. Guarda el escaneo como **LinuxXX.nmap**, donde xx es el último dígito de tu IP.
2. Realiza un escaneo de toda la red (poniendo la IP de la red con la máscara en la casilla target. Guárdalo como **LinuxXXred.nmap**, donde xx es el último dígito de tu IP.

**AYUDA A TENER EN CUENTA**

 Una vez instalada la aplicación con el comando >apt-get install nmap procedemos a realizar el primer escáner.

 Hacemos un nmap a [www.google.es y](http://www.google.es/) nos muestra los puertos abiertos y cerrados.



Cabe resaltar que existen varios tipos de modificadores de scan lo más importante es lograr identificar la combinación más apropiada, los modificadores que se pueden utilizar para realizar el scan son los siguientes:

- **sT** se intenta hacer un barrido de puertos por TCP.

- **sU** se intenta hacer un barrido de puertos por UDP, es útil cuando se intentan descubrir puertos de nivel superior que pueden estar detrás de un firewall.

- **sA** se usan mensajes de ACK para lograr que sistema responda y así determinar si el puerto

está abierto.

- **sX** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red

- **sN** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose

dentro de la red

- **sF** puede pasar algunos Firewall con malas configuraciones y detectar servicios prestándose dentro de la red

- **sP** similar a Ping.

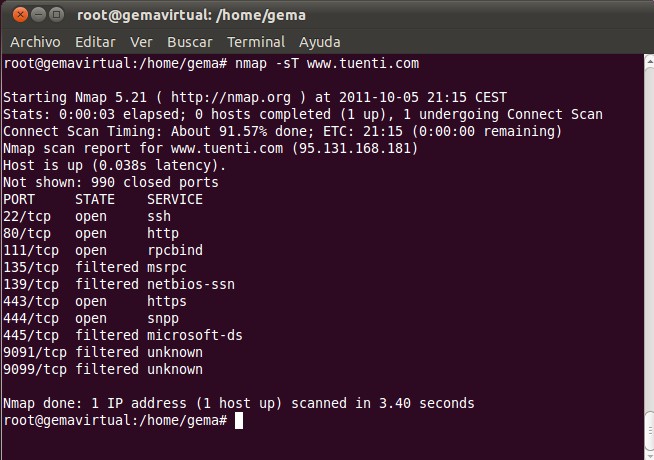
- **sV** intenta identificar los servicios por los puertos abiertos en el sistema esto permite evaluar cada servicio de forma individual para intentar ubicar vulnerabilidades en los mismos.

- **sO** con esta opción se identifica que protocolos de nivel superior a capa tres (Red o Network) responden en el sistema, de esta manera es más fácil saber las características de la red o el sistema que se intenta evaluar.

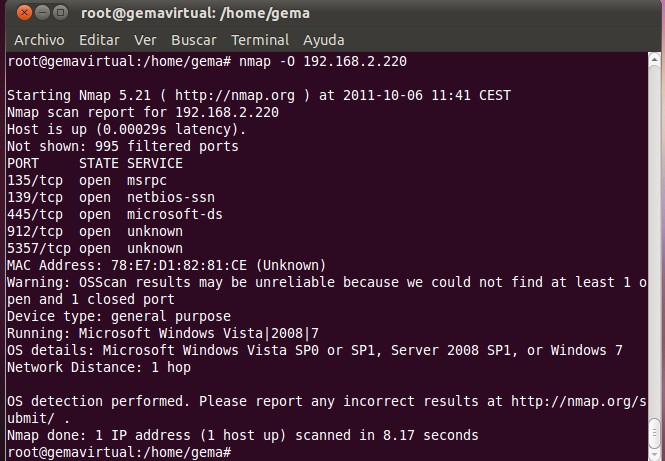
**EJEMPLO:**

**Como sabemos esta dirección ha desaparecido. Utilizar otra**

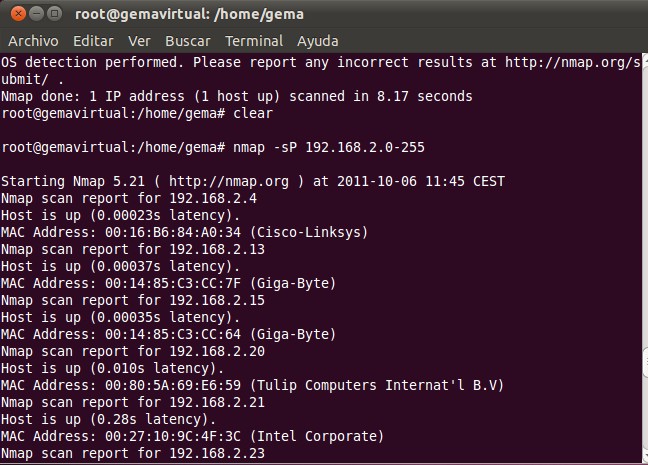
 Hacemos un nmap a [www.tuenti.com y](http://www.tuenti.com/) nos muestra un barrido de puertos por tcp.



 Con el comando del siguiente ejemplo podemos ver los puertos abiertos y el sistema operativo del host al que le corresponda la ip que le indiquemos.



 Con el comando del siguiente ejemplo podemos ver los host que están disponibles dentro de la red que le indiquemos.



**Grupos:**2 alumnos por grupo

**Documentación a Entregar**

Documento PDF con el nombre **UT1\_P12.pdf**. En la portada del documento aparecerá el título de la práctica, junto con los nombres de los componentes del grupo de prácticas:

Deberán aparecer en el documento los resultados de los apartados a, b, c, d y e.

**Plazo de entrega:** Por determinar.

**P1.3– Integridad Sistemas**

**Objetivo**

Utilizar herramientas/comandos que nos permitan verificar la integridad de los sistemas de archivos tanto en sistemas Windows como Linux.

**Desarrollo de la Práctica**

1. **Integridad en Sistemas Windows**

**SFC (System File Checker)** es una utilidad de los sistemas Windows que comprueba la integridad de los archivos de sistema.

* La opción **/*scannow*** reemplaza los que están corruptos o dañados por versiones correctas (siempre que sea posible). Si el sistema detecta que tiene algún problema y necesita reparar algún fichero dañado, lo copia del fichero de instalación, que solicita al inicio de la ejecución.
* La opción **/*verifyonly*** no realiza reparaciones.

Al ejecutar **SFC**, se crea un archivo de registro que podemos consultar en **C:\Windows\Logs\CBS\CBS.log**

1. En tu máquina virtual ejecuta sfc /scannow, en una consola con permisos de administrador. Guarda el archivo log.
2. Ejecuta ahorasfc/verifyonly. Guarda el archivo log.

**Comando chkdsk (check disk)** comprueba la integridad de las unidades de disco duro o unidades de almacenamiento y repara errores lógicos en el sistema de archivos.

1. Ejecutar*chkdsk c: /F*, la opción /*F* es para corregir los errores del disco. La comprobación se realizará la próxima vez que se inicie el sistema. Captura la pantalla durante la ejecución.
2. **Integridad en Sistemas Linux**

**Comando *sum*** permite obtener un número a partir de un fichero, equivalente al dígito de control de una cuenta bancaria. Si se modifica el contenido de un fichero, el valor de suma cambia, por muy pequeña que sea la modificación.

* En algún fichero pequeño el comando sum puede fallar y generar el mismo par de números, aunque se hayan producido algunos cambios. En estos casos es más fiable el comando cksum

**Comando *md5sum***, obtienen una resultado parecido, aunque es algo más complejo. Utiliza una función *hash*, que veremos en un tema posterior. Para utilizarlo, debes instalar el paquete coreutils:

sudo apt-get install coreutils

1. Crea un pequeño archivo de texto con los nombres y apellidos de los integrantes del grupo. Ejecuta en consola el comando ***sum****archivoTexto.* Añade ahora la fecha de nacimiento al final del fichero (puedes hacerlo desde la consola, sin abrir el archivo utilizando las redirecciones >>). Vuelve a ejecutar el comando *sum*, y comprueba cómo cambia el resultado. Haz una captura de pantalla donde se vean los dos resultados.
2. Repite el mismo proceso, ahora con *md5sum*. Haz una captura de pantalla donde se vean los dos resultados.

**Grupos:** 2 alumnos por grupo

**Documentación a Entregar**

Documento PDF con el nombre **UT1\_P13.pdf**. En la portada del documento aparecerá el título de la práctica, junto con los nombres de los componentes del grupo de prácticas:

Deberán aparecer en el documento los resultados de los apartados a, b, c, d y e.

**Plazo de entrega:** Por determinar.

**AMPLIACIÓN**

***1.2 INTEGRIDAD EN LINUX( en el sistema).***

***Busca información acerca de rookit.***

• En caso de que algún tipo de malware reemplace o falsifique archivos del SO, los administradores de sistemas no dudarán de la veracidad de dichos archivos y procesos.

• A este tipo de malware se le denomina rootkit, programa que sustituye los ejecutables binarios del sistema para ocultarse mejor, pudiendo servir de puertas traseras o backdoor para la ejecución malware remota.

 Vamos a chequear que el sistema operativo de Linux no está corrupto, para ello utilizaremos la herramienta “hunter”.

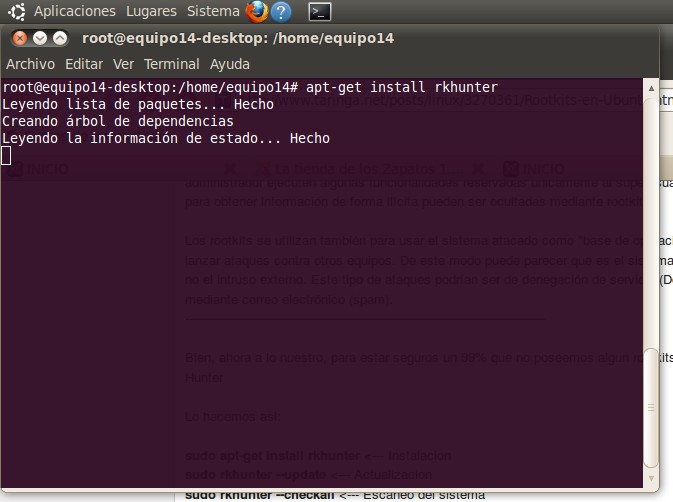
 Lo primero que debemos hacer es ejecutar una consola e instalar la herramienta

Rootkit hunter con el commando= >apt-get install **rkhunter.**

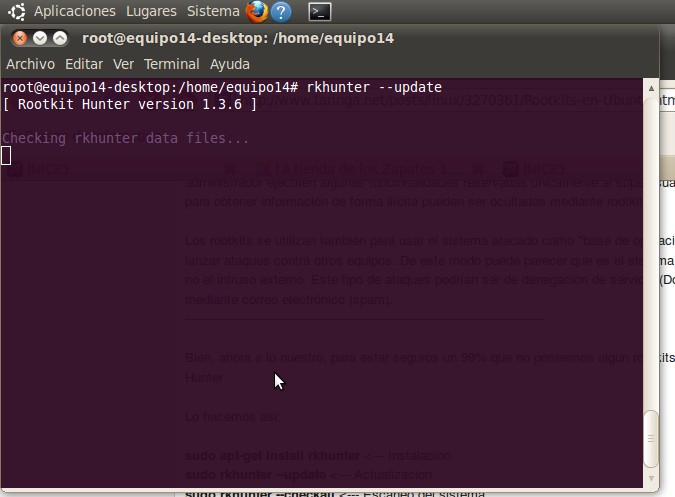
o

sudo aptitude install rkhunter

O bien desde Sistema/Administración/gestor de paquete Synapstic



 Seguidamente actualizamos la aplicación con el comando =>rkhunter –update.



* Una vez actualizada la aplicación comenzamos el chequeo con el comando >rkhunter --checkall.

Se ejecuta verificando todas sus opciones=> sudo rkhunter --checkall

