Seguridad informática | Tarea 1.1

Fecha de realización: 3 - 10 - 22

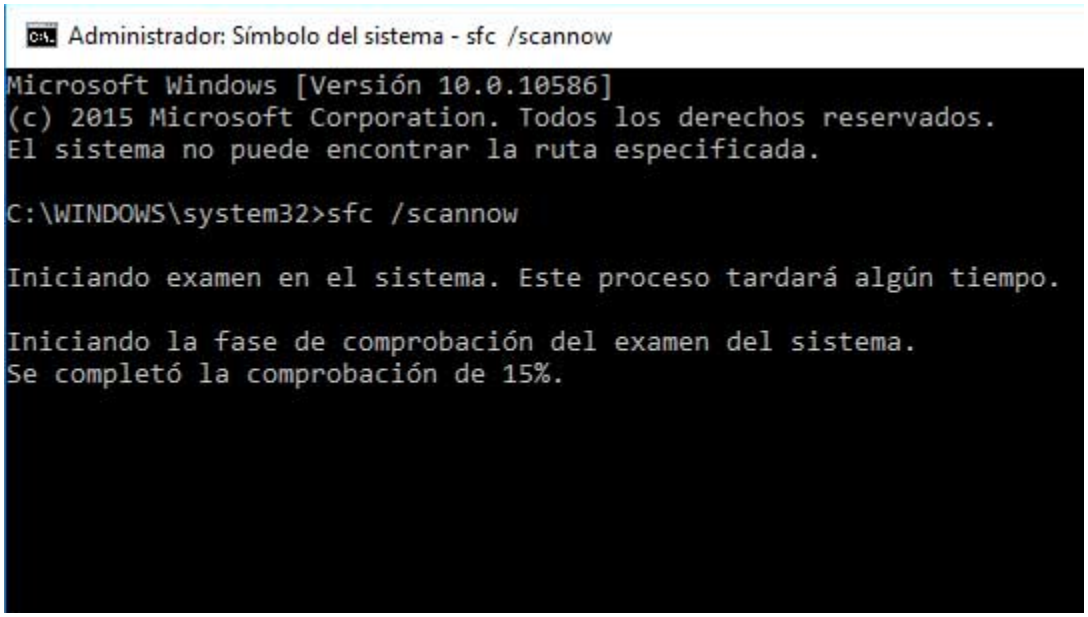
Indice

1. Verificación de la integridad de ficheros:

A) En Windows: ¿Que comandos se usan?, ¿Que hacen? (sfc)

El comando sfc /scannow analiza todos los archivos del sistema protegidos y reemplaza los archivos dañados con las copias en caché ubicadas en la carpeta comprimida %WinDir%\System32\dllcache. El marcador de posición %WinDir% representa el directorio del sistema operativo Windows.

En resumen, este comando se usa para encontrar y reparar archivos corruptos del sistema, como claves de registro y carpetas y archivos que son esenciales para el funcionamiento del sistema, también podemos usar otros comandos como CHKDSK o DISM. Para usar todos estos comandos necesitamos ejecutarlos en CMD.



B) En Linux: Probar el comando "sum" (a un archivo y modificarlo para comprobar)

El comando sum en Linux se usa para mostrar la suma de verificación y el recuento de bloques de cada archivo especificado. Si no se especifica ningún archivo, leerá la entrada estándar. Su sintaxis es la siguiente:

```
sum [OPTION]... [FILE]...
```

Aquí podemos ver un ejemplo básico:

```
ercluster417@ercluster417:~$ nano hola.txt
ercluster417@ercluster417:~$ sum hola
60186     1
ercluster417@ercluster417:~$
```

2. Para cada elemento de la lista asignar si pertenece a seguridad Activa o Pasiva y Física o Lógica.

a) **Detector incendios:** Seguridad física y activa

b) **Ventilador ordenador:** Seguridad física y activa

c) **Veneno Ratas:** Seguridad física y pasiva

d) **SAI:** Seguridad física y depende el modelo SAI (outline o online)

e) **Cámara video vigilancia:** Seguridad física y activa

f) **Cortafuegos:** Seguridad lógica y activa.

g) **Acceso Huella digital:** Seguridad lógica y pasiva

3. Qué objetivos vulneran las siguientes amenazas:

A) **Programa espía:** Confidencialidad.
B) **Ataque DOS:** Disponibilidad.
C) **Incendio:** Integridad, disponibilidad.
D) **Usuario borra accidentalmente el HD:** Integridad, disponibilidad.

4. Relaciona los conceptos de las dos columnas:

Integridad	Autenticar
No repudio	Firmar
Confidencialidad	Antivirus
Disponibilidad	Copia de seguridad

- Integridad = Antivirus
- No repudio = firmar
- Confidencialidad = Autenticar
- Disponibilidad = Copia de seguridad

5. ¿Se puede modificar la temperatura de apagado del equipo en la BIOS? ¿Como?

Sí se puede, pero depende mucho de la placa base. En mi caso, explicaré el proceso para la placa base ASUS M4A78T-E. Esta placa base Asus incluye protección térmica.

Para modificar estos parámetros, tendrás que usar las teclas de flecha del teclado para seleccionar la opción Monitor de hardware y presionar "Entrar". Seleccione "Protección contra sobrecalentamiento" y presionar "Enter". Selecciona el valor de temperatura deseado de la lista y presiona "Enter". El rango de temperatura utilizable es de 50 a 90 grados centígrados. Presiona la tecla "F10" en el teclado para guardar los cambios en la BIOS. Y así de fácil y rápida sería la modificación de temperatura de apagado del equipo usando la BIOS.

6. Analiza los perjuicios que puede ocasionar la conexión a una red Wi-Fi que no pide ningún tipo de contraseña.

La primera vulnerabilidad importante es que en una red wifi abierta, tus datos se envían a un punto de acceso abierto, lo cuál está haciéndote vulnerable.
Por ejemplo, a diario podemos ver que en muchas tiendas y espacios públicos, se ofrece WIFI gratuito. Estas redes a las que nos podemos conectar, sin tener que introducir contraseña alguna, significa que no están encriptadas (encriptar es transformar información, utilizando un hash con el fin de protegerla de personas ajenas), por lo que usar esta red puede suponer un riesgo para la seguridad de nuestros datos ya que alguien podría estar en mitad en la red (Man-in-the-middle attack)

7. Analiza los perjuicios que puede ocasionar que tu conexión Wi-Fi no tenga contraseña.

El principal inconveniente sería que cualquiera podría acceder a mi red con gran facilidad. Esto significa que usando programas como Wireshark podría interceptar información sobre lo que hago con mis dispositivos. Además este extraño que se conectara podría quitarme el acceso a mi propio router, añadiendo una simple contraseña. También podría cometer algún delito cibernético y en los logs que verían los investigadores del delito podrían ver la ip de mi router.

8. Busca el algoritmo que proporciona la letra del DNI y realízalo en una hoja de cálculo.

Las letras del DNI se pueden calcular fácilmente a partir de los números. Esto se debe a que las letras del DNI las calcula el Algoritmo 23. Las letras del DNI se obtienen fácilmente con un simple cálculo, a continuación voy a calcularla en una hoja de cálculo.

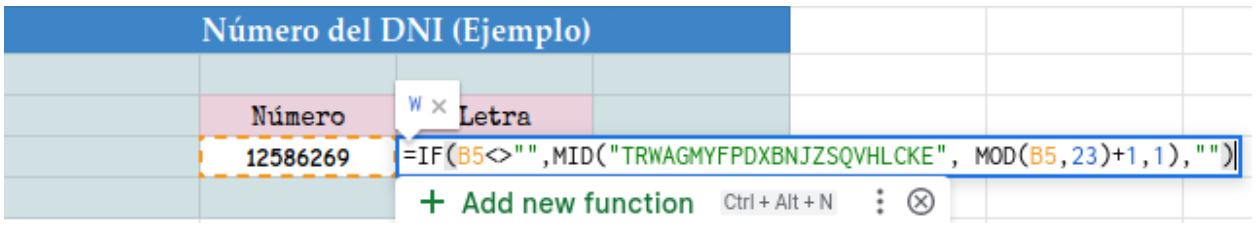
Para calcular las letras del DNI necesitamos aplicar la siguiente fórmula, primero dividir los números del DNI por 23 y luego usar la división que nos sobra para calcular las letras. El resto estará entre 0 y 23, en función del valor resultante, se convierte en una letra, para saber qué letra coincide, utilice el código TRWAGMYFPDXBNJZSQVHLLCE.

Resto	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Letra	T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

Número del DNI (Ejemplo)	
Número	Letra
12586269	W

La fórmula con la que vamos a calcular el número en nuestra hoja de calculo sería:

```
=IF(B5<>"",MID("TRWAGMYFPDXBNJZSQVHLCKE",
MOD(B5,23)+1,1),"")
```



La letra sería en este caso la W

9. Imagina que la empresa en la que eres responsable de seguridad sufre un ataque a través del servidor Web utilizando una vulnerabilidad conocida. ¿Qué medidas tomarías?

Primero analizaría cuál ha sido la vulnerabilidad, mientras hago una copia de seguridad de los datos más importantes de nuestro servidor. Más tarde, cerraría los puertos del servidor, añadiría actualizaciones para esas vulnerabilidades y una vez hecho todo, reiniciaría el servidor..

10. ¿Que son la cookies?

Las cookies son pequeños fragmentos de texto que los sitios web que visitas envían al navegador y se almacenan en nuestro navegador web. Gracias a estos fragmentos, hacen que los sitios web recuerden información sobre tu visita y las cosas que te ha interesado, por ejemplo si fuera una web de una tienda de ropa, este guarda si te han interesado chaquetas o sudaderas, y lo almacena en el navegador. Las cookies, al guardar el historial de los usuarios y otra información extra, ayudan a los sitios web a mejorar sus productos y servicios. Las personas que cometen delitos cibernéticos, gracias a la información extra que se almacena en una cookie como el de inicio de sesión de cuentas y más, pueden sacar beneficios y ventajas. Por esta razón, el robo de cookies es muy valioso e importante para los ciberdelincuentes.

11. Diferencia entre proxy y cortafuegos

Firewall es un software que anula el acceso que no tiene autorización desde una red privada. Todo el tráfico de la red pasa a través del firewall y solo debe pasar el tráfico de red que tiene autorización. El firewall es un sistema ubicado entre dos redes donde ejecuta una política de control de acceso entre esas redes. Funciona en la capa de red del modelo OSI y utiliza un cifrado (hashes) para cifrar los datos antes de la transmisión mientras que el proxy, o también llamado Proxy Server, es un servidor que actúa como intermediario entre cualquier dispositivo y el resto de Internet. Un proxy acepta y reenvía peticiones para conectarse, para luego devolver datos para esas peticiones. Utiliza la identificación de red anónima en lugar de la dirección IP real del usuario (esto quiere decir que oculta la dirección IP del usuario), por lo que no se podría ver la dirección IP real del usuario.

12. Ventajas e inconvenientes de desactivar el uso del puerto USB en una empresa.

Una empresa desactiva el puerto USB porque este puerto es fácilmente vulnerable porque puede propagar rápidamente un virus. Por ejemplo, si despedimos a un empleado, estos en un ataque de ira pueden robar datos fácilmente usando unidades USB o introducir un malware. La principal desventaja sería que estos puertos tan importantes, no podríamos darle ningún tipo de uso.

13. ¿Es totalmente fiable usar las aplicaciones bajadas de Google Play?

No, no todas son fiables. De hecho todos los meses en google play, se reportan muchas aplicaciones con malware oculto. Por ejemplo, hace dos meses se detectó una aplicación que te escaneaba folios y los pasaba a pdf, pero en esta App, había oculto un troyano que registraba las tarjetas de créditos que introdujeras para pagar en cualquier tienda y a la semana, la quitaron de la google play.

14. ¿Qué es un TIGER TEAM?

Basándonos en un artículo de 1964, Tiger Team es un grupo de expertos asignados para investigar y resolver problemas técnicos o sistémicos. Este artículo publicado en 1964 definió el término como "un equipo de especialistas técnicos no domesticados y desinhibidos, seleccionados por su experiencia, energía e imaginación, y asignados para rastrear sin descanso todas las posibles fuentes de fallas en un subsistema de naves espaciales", en otras palabras, conjunto de personas que trabajan por su propia cuenta que los contratan para ejecutar o llevar a cabo una tarea difícil e importante.

15. Un usuario aunque tenga privilegios limitados ¿es peligroso todavía?

Si, puede llegar a ser peligroso ya que siempre habrá alguna vulnerabilidad presente. Por eso nuestro trabajo sería reducir las posibilidades de que exista alguna vulnerabilidad para que ningún programa o persona pueda acceder a nuestro sistema. Por ejemplo, hay un famoso sistema que se llama escalar privilegios, convertirnos de un usuario no privilegiado dentro de un equipo a un usuario con los suficientes permisos para ejecutar más acciones en el sistema y ser el Root.

Por ejemplo pongámonos en la situación que estamos en un equipo que como sistema operativo usa Linux Mint y somos el usuario Antonio, pero Antonio no tiene control de todo el ordenador y sus funciones, para ello tendremos que convertirnos en un usuario con más privilegios como lo es Root o como lo sería Administrator en Windows, a esto se le conoce como escalar privilegios.

16. ¿Cómo detectarías un ataque DOS y qué harías para defenderte?

Para empezar, un ataque DOS (Denegación de Servicios, Denial of Service) es un tipo de ciberataque en el que un usuario maligno tiene como objetivo generar una cantidad masiva de peticiones al servicio elegido para atacar. Estas peticiones se generan desde un mismo ordenador o dirección IP, reduciendo así los recursos que tiene el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar todas las peticiones, esto es cuando se hace realidad la denegación del servicio.

Un ataque DoS se caracteriza por utilizar un único ordenador para lanzar el ataque. Ahora vamos a ver que tendríamos que hacer si queremos analizar si estamos sufriendo un ataque DoS, lo podremos saber siguiendo las siguientes características:

- Rendimiento por debajo de lo normal de la red, como tiempos de carga de archivos o sitios web demasiado extensos.
- No poder cargar un sitio web concreto, como tu servidor web
- Pérdida de conectividad en los dispositivos de la misma red

Si queremos protegernos de un ataque como este tendremos que tomar en cuenta la siguiente información

- Como usuarios tendríamos que revisar la configuración de nuestros routers y firewalls para detectar IP's falsas o extrañas que provengan de posibles atacantes. Normalmente, nuestro Proveedor de Servicios de Internet (ISP) se encarga de que nuestro router esté al día con esta configuración.
- Por otro lado, las empresas que ofrecen estos servicios, tienen que proteger tanto su red, como toda su infraestructura para poder repeler estos ataques y que puedan afectar al funcionamiento de su trabajo y como consecuencia relacionada de ello, a sus clientes. Si una empresa es atacada por un ataque de denegación de servicio (DoS), los clientes dejarán de confiar en este servicio y la gente dejará de pensar en la contratación de esa empresa

17. Qué objetivos se están violando en estas situaciones:

A) **Destrucción de un elemento del hardware:** Disponibilidad

B) **Robo de un portátil con información de interés de la empresa:** Confidencialidad e integridad

C) **Escuchas electrónicas:** Confidencialidad

D) **Modificación de los mensajes entre programas para variar su comportamiento:** integridad

E) **Deshabilitar los sistemas de administración de archivos:** Integridad

F) **Robo de sesiones:** Confidencialidad