UNIVERSIDAD POLITÉCNICA DE VICTORIA
UNIDAD IV

ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

August 8, 2018

Dra. Karla E. Vázquez Ortiz
Alumna: Claudia Lizbeth Carrizales Piña
Matrícula: 1730048

INTRODUCCIÓN

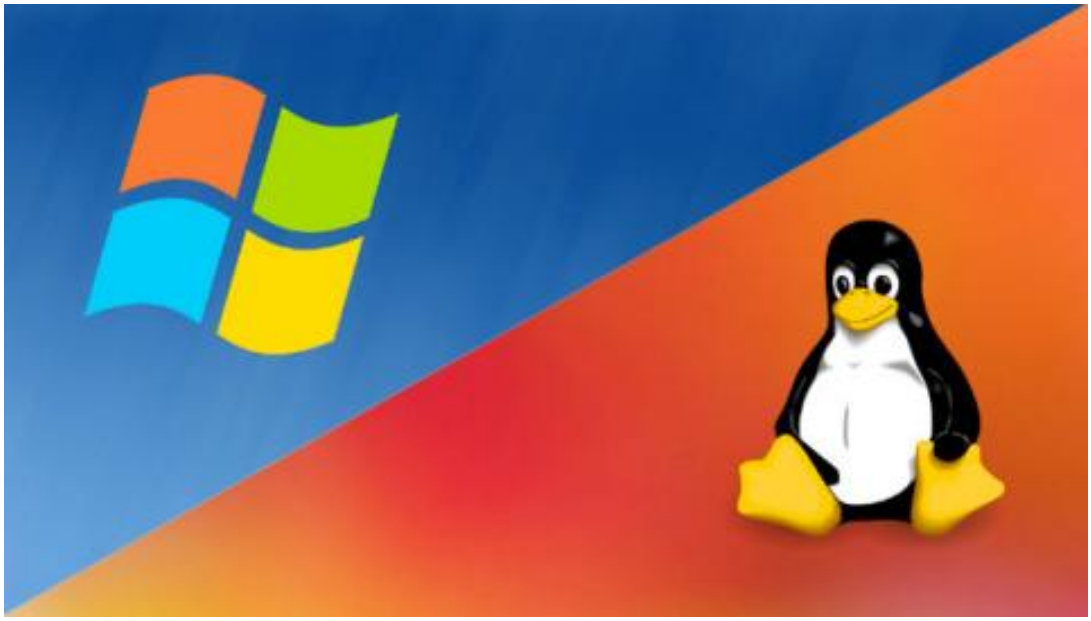
En esta documentación hablaremos y detallaremos algunos de los puntos sobre la seguridad de windows server y linux; hablaremos de la fragmentació y defragmentación de un disco duro y explicaremos el como se lleva acabo esto, algunas de las medidas para proteger un núcleo de windows,la funcionalidad del comando chkconfig y algunas de las evoluciones de las técnicas de protección de datos.

Todo esto para conocer más acerca de la seguridad y como podemos enfrentarla en algunos casos como amenaza de intrusos u otras formas y conocer más acerca del tema.

COMANDO CHKCONFIG

* El comando chkconfig puede ser usado para activar y desactivar servicios en cada nivel de ejecución. Chkconfig no inicia ni detiene servicios al momento, tan solo crea o elimina precisamente los enlaces de una manera mas amigable.
Con este comando seguido de –list nos da una lista completa de todos los servicios instalados y para cada nivel si arrancarÃą (on) al entrar a ese nivel o se detendrá (off) o simplemente no se iniciara.

*El equivalente de este comando en Ubuntu es el comando service nos sirve para iniciar o detener el servicio en tiempo real o manualmente, funciona exactamente igual a como si escribieramos la ruta completa hacía el directorio.



FRAGMENTACIÓN Y DEFRAGMENTACIÓN DE UN DISCO DURO Y LA REALIZACIÓN EN LINUX Y WINDOWS

*La fragmentación es cuando divides al disco en unidades de almacenamiento lógicas individuales. Es la memoria que queda desperdiciada al usar los métodos de gestión de memoria, existen dos tipos de fragmentaciÃşn: interna y externa.
La defragmentación es cuando se vuelven a unir estas unidades logicas, en otras palabras es el proceso conveniente mediante el cual se acomodan los archivos en un disco para que no se aprecien fragmentos de cada uno de ellos, de tal manera que quede contiguo el archivo y sin espacios dentro del mismo.

****UBUNTU****

Haciendo uso de la utilidad e2fsprogs para la desfragmentaciÓN:

-Es necesario instalar la herramienta e2fsprogs: sudo apt install e2fsprogs.

-Ya hecha la instalación podemos utilizar la herramienta para utilizarla es importante señalar que es aconsejable desmontar los dispositivos o unidades de su sistema en el que utilizará esta utilidad o algo similar para evitar la corrupción de datos.

Para utilizar la herramienta, debemos de abrir una terminal y ejecutar el siguiente comando: sudo e4defrag -c.

-Como resultado, obtendremos una imágen que nos va indica un valor de fragmentación de nuestra unidad.

-Para desfragmentar una unidad, ejecute la aplicación con el siguiente comando sustituya /ruta/de/partición por el nombre de la partición: sudo e4defrag /ruta/de/partición.

-Solo tendremos que esperar a que nuestra partición o unidad sea desfragmentada con éxito.

WINDOWS*

-Selecciona la barra de búsqueda de la barra de tareas y escribe desfragmentar.

-Selecciona Desfragmentar y optimizar las unidades.

-Selecciona la unidad de disco que quieres optimizar.

-Selecciona el botón Optimizar .

-Sólo es cuestión de esperar y listo.

MEDIDA PARA PROTEGER EL NÚCLEO DE WINDOWS

-Resistencia a malware incluye cambios en la arquitectura que pueden aislar de las amenazas a los componentes críticos del sistema y de seguridad.
-Identidad y control de acceso se han ampliado las caracterÃŋsticas en gran medida para simplificar y mejorar la seguridad de autenticación de usuario.
-ProtecciÓn de la información que protege la información en reposo, en uso y en tránsito.

Hay que tener en cuenta que estos ataques están relacionados pero no tienen el mismo alcance ni las mismas repercusiones. Ambos se aprovechan de un error de diseÃśo en la ejecuciÃşn especulativa del procesador para acceder a la memoria del kernel, donde se almacenan nuestras contraseÃśas, pero Meltdown se puede arreglar (a cambio de capar el rendimiento del procesador) y Spectre solo se puede mitigar. Aunque un ataque sea muy complicado, no hay una soluciÃşn de software definitiva.

****Windows****
Microsoft publicó una actualización de emergencia para Windows que se instalará automáticamente si usas Windows 10 y que puedes descargar de forma manual.

****LINUX****
La comunidad de desarrolladores de Linux ha estado rápida en actualizar el kernel del sistema operativo para enmendar la vulnerabilidad que afecta a los procesadores.

EVOLUCIÓN DE LAS TÉCNICAS DE PROTECCIÓN DE DATOS

****WINDOWS 10****

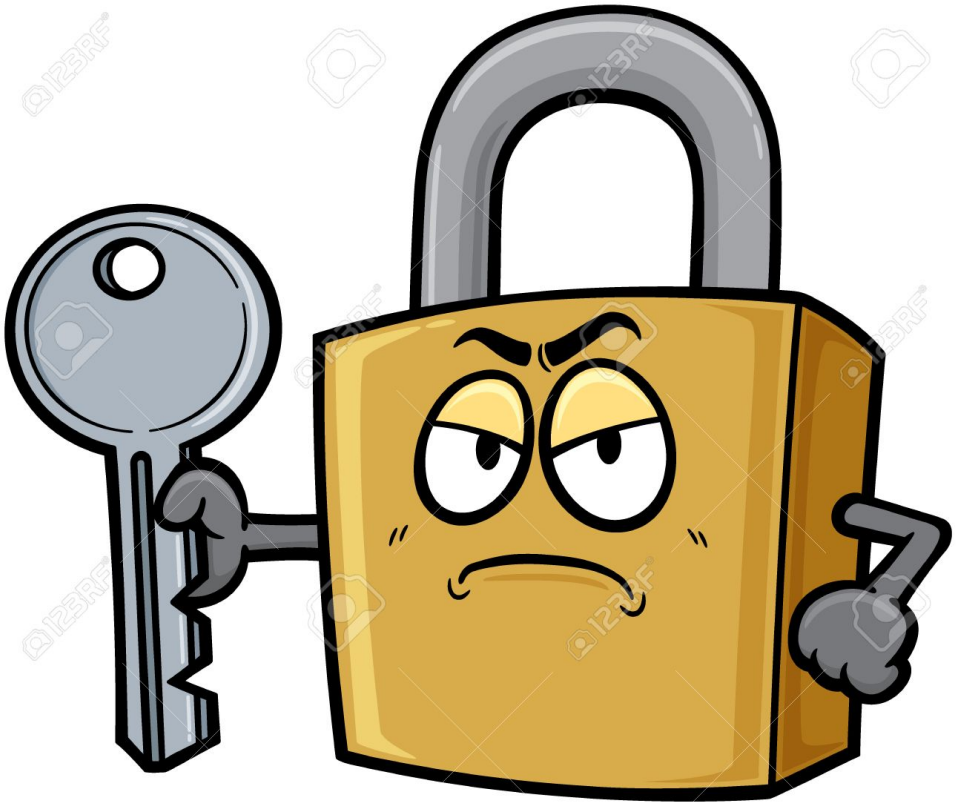
Estas mejoras se centran en tres áreas clave: resistencia a las amenazas, protección de la información y protección de la identidad y control de acceso. Windows 10 incluye varias mejoras en la protección de la información integrada, como un nuevo componente de prevención de pérdidas de datos (DLP). A diferencia de otras soluciones DLP, Microsoft integró esta funcionalidad en profundidad en la plataforma de Windows, ofreciendo el mismo tipo de funcionalidades de seguridad que las soluciones basadas en contenedor pero sin alterar dichas experiencias de usuario, como la necesidad de cambiar el modo o alternar entre aplicaciones.

La protección de la integridad de los datos de la empresa, así como evitar la divulgación inadecuada y el uso compartido de dichos datos son una prioridad para las organizaciones de

TI. Las tendencias como BYOD y la movilidad hacen que la tarea de proteger la información sea más difícil que nunca. Windows 10 incluye varias mejoras para la protección de la información integrada, incluida una nueva característica de Enterprise Data Protection (EDP) que ofrece la funcionalidad DLP. Esta caracteristica permite a los usuarios de las organizaciones clasificar datos por sí mismos y te proporciona la capacidad de clasificar automáticamente los datos a medida que se introducen a partir de los recursos empresariales. TambiÃl'n puede ayudar a impedir que los usuarios copien contenido empresarial en ubicaciones no autorizadas, como documentos personales o sitios web.

****WINDOWS 7****

Windows 7 ofrece la posibilidad de cifrar los datos, pero no tiene DLP (Data Lost Prevention, Prevencion de PÃl'rdida de Datos). Uso de aplicaciones de terceros, con diferentes resultados en equipos informaticos y dispositivos móviles. En Windows 7, una plataforma de seguridad basada Ãžnicamente en software puede permitir que el malware se esconda de las soluciones de seguridad y se incruste en el propio dispositivo.



ESTRATEGIAS DE SEGURIDAD EN LOS SISTEMAS OPERATIOVOS INUX Y WINDOWS SERVER

****LINUX****

- Seguridad física del sistema: Configurar el BIOS para deshabilitar el arranque por CD/DVD, dispositivos externos y diskettes. DespuÃl's, habilitar la contraseÃśa del BIOS y proteger el archivo GRUB con contraseña para restringir el acceso físico al sistema.

-Disco particionado: Es importante contar con diferentes particiones para conseguir mayor seguridad de los datos en caso de que algún desastre ocurra. Al crear diferentes particiones, los datos pueden ser separados o agrupados según su tipo.

- Minimizar paquetes para minimizar vulnerabilidades: se recomienda evitar instalar paquetes que no se utilizan para evitar las vulnerabilidades de esos paquetes. Esto minimiza el riesgo de que comprometan un servidor.

-verifica los puertos de red que escuchan conexiones: Con la ayuda del comando "netstat" es posible listar todos los puertos abiertos y los programas que los utilizan. - Utiliza Secure Shell (SSH): Los protocolos Telnet y rlogin utilizan texto plano para el envio de la informacion, en

cambio, Secure Shell es un protocolo seguro ya que utiliza cifrado en todas las comunicaciones entre equipos.
-Mantener actualizado el sistema: Siempre se debe mantener actualizado el sistema y aplicar los parches, soluciones de seguridad y actualizaciones de kernel mÃąs recientes y tan pronto se encuentre encuentren disponibles.

****WINDOWS SERER****
-Proteger las credenciales de dominio derivadas con Credential Guard: Credential Guard usa la seguridad basada en virtualizaci"on para aislar los secretos, de forma que solo el software de sistema con privilegios pueda acceder a ellos. El acceso no autorizado a estos secretos puede derivar en ataques de robo de credenciales.
-Blog de seguridad de centro de datos y nube privada: Es el contenido técnico del equipo de seguridad del centro de datos y la nube privada de Microsoft.
-Virtualización segura con VM blindadas.
-Privileged Access Management.
-Protección de credenciales.
-Protección del sistema operativo y las aplicaciones.
-Detección y respuestas a las amenazas.
-Seguridad de red.

CONCLUSIÓN

Con base a lo que fuimos investigando nos queda mas en claro el concepto de fragmentación y defragmentación por si aun no sabíamos exactamente lo que esto era, también a tener en cuenta algunas estrategias de medida de seguridad y como podemos aplicarlas.
Así también en saber el uso del comando chkconfig en su dado caso si s llega a usar en windows o ubuntu.