Firewall Personales

son aplicacion basadas en software que protegen un ordenador o servidor del trafico no deseado del internet

Firewall basados en host

funcionan aplicando un conjunto de reglas y politicas contra el trafico que entra y sale de nuestro ordenador

Windows

tiene su propio firewall basado en software ya integrado

se puede acceder en cmd = wf. msc

Linux

tiene iptables

IDS = sistema de deteccion de intrusos

HIDS sistema de deteccion de intrusos basados en host

se basan en firmas, politicas o anomalias

verdadero positico = ha ocurrido algo malo

verdadero negativo = ha ocurrido algo bueno o normal

falsos positivos = actividad legitima esta siendo identificado como un ataque

falso negativo = ocurre algo malo pero se identifica como legitimo

Prevencion de perdida de datos

supervisan los datos de un sistema mientras estan en uso , transito o reposo

DLP de punto final = es un software que se instala en una estacion de trabajo

supervisa los datos que se utilizan en ese ordenador

si se intenta tranferir un archo este lo impedira

o alerta al administrador

DLP de red = solucion colocada en el perimetro de tu red

para analizar los datos que salen de tu red y los que no

deberian salir de tu red

DLP de almacenamiento = software que se instala en un servidor

Asegurar la BIOS

ES un tipo de firmware que es un software en un chip

siglas de sistema basico de entrada salida

actualmente se utiliza la UEFI (unified firmware interface )

flasher la BIOS es asegurarse de que tiene el software

mas actualizado en ese chip

Debemos establecer una contraseña para la bios

Debemos configurar el orden de arranque de tu bios

Debemos desactivar todos los puertos y dispositivos externos

Debemos activar el arranque seguro asi tu pc pasa por

procesos adicionales mientras arranca

Cifrado de discos extraibles como usb o discos duros

Windows lo hace con Bitlocker

AES = cifrado de clave simetrica que admite claves de 128 y 256 bits