Apuntes de Seguridad

**OPEN SSL**

Desarrolla y mantiene un conjunto solido de herramientas de grado comercial y con todas las funciones para el uso de criptografía de propósito general y comunicación segura.

Dentro de este proyecto la toma de decisiones es llevada a cabo por OTC (Comité técnico de Openssl) y la OMC (Comité de Gestion Openssl)

Este mismo se encuentra asociado con Hash o Digest.

OpenSsl genera el valor de Hash en un formato hexadecimal utilizando un algoritmo especifico en base a la información contenida en un archivo

Diagrama

Descripción generada automáticamente

**HashDeep/md5deep**

Hashdeep, es un programa de Open Source que se encarga de calcular, verificar y autoditar hashsets. Es decir, se encarga de verificar e informar si un archivo de entrada coincide con un previamente registrado o no. Además, puede informar si los los archivos se encuentran emparejados, si faltan, si se han movido en el conjunto, entre otras cosas.

Este mismo cuenta con una lista de parámetros con las cuales invocando hashdeep -h podemos visualizarlas, pero sin embargo estas son las principales:

* **-a:** Modo de auditoría. Valida Archivos contra una lista de hashes y requiere **-k.**
* **-m:** Modo de coincidencia. Requiere **-k.**
* **-x:** Modo de coincidencia negativa. Requiere **-k.**
* **-w:** En modo **-m**, muestra que archivos conocidos coincidieron
* **-k:** Agrega un archivo de hashes conocidos
* **-r:** Modo recursivo. Incluye subdirectorios
* **-e:** Calcula el tiempo estimado para completar cada archivo
* **-v:** Modo “verborragico”. Provee más detalles en la salida

Otros parámetros opcionales de interés:

* **-c:** alg1, alg2, Selecciona los algoritmos a utilizar, las opciones validas son **md5, sha1,sha256,tiger,whirlpool**
* **-l**: Utiliza valores relativos para la ubicación de archivos
* **-p**: Fracciona los archivos para el proceso de hashing
* **-i:** Procesa solo archivos menores que un límite definido
* **-o:** Procesa solo archivos de un tipo especifico

Al crear la lista de hashes para el directorio “./target” podemos observar la siguiente información:

Diagrama

Descripción generada automáticamente

Para comprobar la integridad de los archivos del directorio “./target” se puede utilizar la lista de hashes del archivo “hashes.text”:

Diagrama

Descripción generada automáticamente

De esta forma podemos listar los archivos de “./target” que coinciden o no con las listas de “hashes.text” :

Diagrama

Descripción generada automáticamente con confianza media

**Tripwire**

Tripwire es un programa de seguridad de código abierto que garantiza la integridad de los datos al monitorear y alertar sobre cambios en los archivos del sistema. Utiliza firmas o hash de archivos para compararlos con una base de datos previa, generada al momento de la instalación y protegida con contraseña cifrada. Se recomienda instalar y configurar Tripwire antes de conectar el sistema a internet, ya que su eficacia puede verse comprometida en sistemas posiblemente infectados. Este software es compatible con sistemas operativos GNU/Linux.

Su política define que archivos se están controlando y que criterio a utilizar en los mismos, con tal fin, debemos editar un archivo de texto con la información correcta.

Durante una verificación, Tripwire genera un informe que se muestra en pantalla y se guarda en el directorio "/var/lib/tripwire/report/" del sistema de archivos. El nombre del informe sigue el formato [Host]-[Año][Mes][Día]-[Hora][Minuto][Segundo].twr y su contenido es binario. Se necesita la herramienta twprint para visualizarlo.

**Unidad Nº 0: Anexo Seguridad**

Los sistemas que manejan información deben cumplir requisitos clave:

1. Preservar la integridad de la información contra alteraciones accidentales o deliberadas debido a fallos en el software o hardware, agentes externos o usuarios.
2. Evitar accesos no autorizados al sistema y a su contenido, garantizando la confidencialidad.
3. Hay que asegurar que la información esté disponible cuando se necesite, asegurando su disponibilidad.

Estos principios se conocen como integridad, confidencialidad y disponibilidad, y son fundamentales para considerar un sistema seguro.

La seguridad de un sistema informático va más allá de proteger los datos con técnicas criptográficas. Se deben considerar múltiples factores internos y externos para garantizarla. Un factor clave es determinar si el sistema está conectado externamente. Esto puede subdividirse en:

* **Aislados:** No tienen acceso a redes y se aseguran mediante controles físicos y protocolos de gestión de usuarios.
* **Interconectados:** Conectados a redes, incluyendo Internet, lo que los hace más comunes, pero también más complejos de gestionar.

Aquí están algunas de las cuestiones clave en seguridad:

1. **Seguridad física:** Incluye medidas para proteger los soportes físicos de la información y restringir el acceso físico a las computadoras.
2. **Seguridad de los canales de comunicación:** Dado que los canales de comunicación son generalmente inseguros, se requieren mecanismos para proteger la información incluso en canales manipulados o hostiles.
3. **Control de acceso a los datos:** Es fundamental permitir el acceso solo a usuarios autorizados, estableciendo privilegios individualizados y utilizando mecanismos como el cifrado para preservar la confidencialidad.
4. **Autenticación:** Se necesita verificar la autenticidad de elementos como la información, los usuarios y los dispositivos para prevenir problemas de suplantación de identidad.
5. **No repudio:** Es crucial que los remitentes asuman responsabilidad sobre la información que envían, evitando que puedan negar su autoría sobre un mensaje.
6. **Anonimato:** Importante para preservar la intimidad y libertad en ciertas aplicaciones, pero también puede ser utilizado para actividades delictivas. Lograr el anonimato es difícil y controvertido, especialmente en entornos donde la seguridad nacional es prioritaria sobre la privacidad de los ciudadanos.

**Unidad Nº 1: Introducción a la Seguridad**

**Información:** Es un grupo de datos procesados y ordenados, que sirven para construir un mensaje que cambia el estado de conocimiento del sujeto o sistema que lo recibe. Esta misma se deriva del latín informatio, la cual significa “dar forma a la mente”

Este presenta las siguientes caractetisticas:

* + **Critica:** Es indispensable para la operación de la organización
  + **Valiosa:** Es un activo apreciado por la organización y sus operaciones
  + **Sensitiva:** Debe ser conocida por las personas autorizadas

Imagen que contiene tarjeta de presentación

Descripción generada automáticamente**Seguridad:** Proviene del latín securitas que significa libre de cualquier daño, el cual desde un punto de vista psicosocial se considera como un estado mental que se produce en los individuos un particular sentimiento de estar libre de peligro ante cualquier situación.

**Seguridad de la Información:** Es la disciplina que habla de los riesgos, amenazas, análisis de escenarios, buenas practicas y esquemas normativos, que exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.

**Seguridad Informática:** Se trata de implementar medidas técnicas para proteger la información, como antivirus, firewalls, sistemas de detección de intrusos y anomalías, y correlación de eventos. Estas acciones, combinadas con prácticas de gobierno de tecnología de información, definen cómo responder a fallos parciales o totales cuando la información está en riesgo.

Diagrama

Descripción generada automáticamenteLa seguridad de la información se fundamenta en tres aspectos clave:

1. **Política de seguridad:** Decisiones y medidas tomadas por una empresa para proteger sus sistemas de información, basadas en la evaluación de los activos y riesgos. También se refiere al documento ejecutivo que establece las directrices de seguridad.
2. **Plan director de seguridad:** Proyecto que define y prioriza medidas de seguridad para reducir los riesgos a niveles aceptables. Debe alinearse con los objetivos estratégicos de la empresa e incluir obligaciones y buenas prácticas de seguridad para los trabajadores y terceros.
3. **Análisis de riesgos:** Proceso para identificar activos de información, vulnerabilidades, amenazas, probabilidad de ocurrencia e impacto, con el fin de determinar controles adecuados para mitigar el riesgo.

* **Incidentes de Seguridad:** Son violaciones de la seguridad que ocasionan la destrucción, acceso no autorizado, perdida o alteración(accidental o deliberada) de datos personales cuando están siendo transmitiros, están almacenados o son objetos de otros tratamientos. Los orígenes de los incidentes pueden ser **Accidente, Interno**(miembros de la organización), **Ciberataque.**
* **Ciberataque:** es un intento deliberado de acceder a un sistema informático sin autorización, utilizando diversas técnicas y vulnerabilidades con fines maliciosos como robo de información, extorsión o daños al sistema
* **Intrusión:**  es la acción de un atacante que aprovecha una vulnerabilidad en el sistema para acceder sin autorización y llevar a cabo actividades ilegítimas.

Términos relevantes

Aquí tienes un resumen de los términos relevantes en seguridad:

1. **Riesgos**: Son posibles eventos que pueden causar pérdidas o daños a los activos de información de una organización. Por ejemplo, el riesgo de una brecha de seguridad debido a una vulnerabilidad en el software.
2. **Amenazas:** Son eventos o acciones que pueden explotar las vulnerabilidades de un sistema y causar daño. Por ejemplo, un virus informático que infecta un sistema y roba información confidencial.
3. **No repudio:** Es la capacidad de asegurar que el emisor de un mensaje no pueda negar haber enviado ese mensaje. Por ejemplo, cuando una firma electrónica garantiza que un usuario no pueda negar haber firmado un documento.
4. **Vulnerabilidades:** Son debilidades en un sistema que pueden ser explotadas por amenazas para comprometer la seguridad. Por ejemplo, una vulnerabilidad en un software que permite a un atacante ejecutar código malicioso en un sistema.
5. **Anonimato:** Es la capacidad de mantener la identidad de un usuario oculta mientras realiza actividades en línea. Por ejemplo, el uso de redes privadas virtuales (VPN) para ocultar la dirección IP de un usuario y proteger su privacidad.

**Contendores de Información:**

Los contenedores de información se pueden clasificar en dos categorías principales: sistemas aislados y sistemas interconectados. La diferencia clave entre ellos radica en su nivel de conexión externa:

* **Sistemas Aislados:** Estos sistemas no tienen acceso a ninguna red externa. Operan de manera independiente y no están conectados a Internet ni a ninguna otra red. Su seguridad se basa principalmente en controles físicos y protocolos de gestión de usuarios. Por ejemplo, una computadora de una red de aire cerrado en una instalación militar.
* **Sistemas Interconectados:** Estos sistemas están conectados a una red externa, como Internet o una red corporativa. Pueden enviar y recibir información constantemente y son vulnerables a una amplia gama de amenazas cibernéticas. La seguridad de estos sistemas requiere medidas adicionales, como firewalls, sistemas de detección de intrusiones y cifrado de datos. Por ejemplo, una computadora de escritorio conectada a Internet en una oficina corporativa.

**Causas de Inseguridad :**

El **estado de inseguridad** activa se refiere a la falta de conocimiento del usuario sobre funciones del sistema que pueden ser dañinas. Esto está relacionado con acciones humanas que pueden ser aprovechadas por atacantes para causar daño al sistema, como activar servicios de red innecesarios, abrir archivos adjuntos maliciosos o proporcionar información confidencial a fuentes no confiables.

La **inseguridad pasiva** es la falta de conocimiento sobre medidas de seguridad disponibles. No está relacionada con la actividad humana, sino con condiciones preexistentes que pueden ser aprovechadas por un atacante para causar daño. Ejemplos incluyen falta de conocimiento sobre dispositivos de seguridad, errores en código de programas, permisos incorrectos o configuraciones desactualizadas, y defectos de hardware.

**Requisitos funcionales para la seguridad:**

* **Auditoría de Seguridad**, registro de actividades.
* **Soporte de cifrado**, uso de criptografía para la protección de datos.
* **Gestión de seguridad**, gestión de perfiles de usuario y niveles de acceso vinculados a los mismos.
* **Privacidad**, soporte del anonimato de los usuarios.
* **Autodefensa,** controles para fallar de manera contenida o prevista.
* **Control de acceso**, manejo de la cantidad y tiempo de las sesiones, concurrencia e información sobre sesiones previas.
* **Rutas o canales fiables**, mecanismos que permitan confiar en los recursos accedidos, como los certificados.

La función de hash se define como un método no reversible para generar un valor que represente de manera casi univoca un dato

**Seguridad Lógica:** Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo permita acceder a ellos a las personas autorizadas para hacerlo.

Este se define en las siguientes características:

* + Controles de Acceso
  + Identificación y Autentificación
  + Roles
  + Transacciones
  + Limitaciones a los Servicios
  + Modalidad de Acceso
  + Ubicación y Horario
  + Control de Acceso Interno
    - Palabras Claves (Passwords)
    - Cifrado
    - Listas de Control de Accesos
    - Límites sobre la Interfaz de Usuario
    - Etiquetas de Seguridad
  + Control de Acceso Externo
    - Dispositivos de Control de Puertos
    - Firewalls o Puertas de Seguridad
    - Acceso de Personal Contratado o Consultores
    - Accesos Públicos
  + Administración
    - Administración del Personal y Usuarios
    - Organización del Personal

Las prácticas de seguridad lógica en móviles se ejemplifican de la siguiente manera:

* + Usar contraseñas robustas y bloqueo automático
  + Realizar copias de seguridad periódicas
  + Instalar software solo de fuentes oficiales.
  + Utilizar software solo con acceso legal a sus funcionalidades.
  + Considerar el uso de software de seguimiento, borrado de datos y/o bloqueo remoto.
  + Evitar o restringir conexiones a redes públicas o no confiables.
  + Deshabilitar sistemas de Bluetooth, NFC y otras tecnologías inalámbricas cuando no se requiera el uso de estos en dispositivos confiables.
  + En dispositivos con conexión de datos móviles tener el PIN activado y su el PUK e IMEI memorizado.

**BYOD**: es una política empresarial que permite a los empleados utilizar sus propios dispositivos personales (como portátiles, smartphones y tablets) para el trabajo, así como acceder a las redes corporativas desde estos dispositivos. Esta política implica compartir el uso de los dispositivos tanto para tareas profesionales como personales.

**Rastreo y gestión remota de dispositivos:**

Este software de control remoto permite acciones como rastreo, borrado y bloqueo de dispositivos, así como la obtención de información del medio. Es útil en casos de pérdida o robo, pero su funcionalidad puede verse limitada por la conectividad del equipo.

**Copias de Seguridad:**

Una política de copias de seguridad es un documento que establece reglas y procedimientos para crear, almacenar y gestionar copias de seguridad de datos en una organización. Se debe revisar y actualizar regularmente para adaptarse a las necesidades. La política define la frecuencia y los tipos de copias, que pueden ser total, diferencial o incremental.

La definición de la política y su ejecución debe considerar los siguientes puntos:

* + Soporte de la copia (Cintas, Discos, Memorias, Cloud, etc)
  + Pruebas de restauración periódicas
  + Control de acceso a las copias
  + Rotación de medios y periodo de retención
  + Almacenamiento y traslados
  + Eliminación y reutilización de soportes

Estos son otros elementos comunes en el manejo de la seguridad lógica de sistemas:

* Firewalls
* Firewalls personales
* Escaners de vulnerabilidades
* Honeypots, Honeynets, Padded cells
* Verificadores de integridad
* IDS (lntrusion Detection System)
* IPS(lntrusion Protection System)
* Antivirus
* WAF(Web Application Firewall)

**VPN:** Una estructura de red que con soporte lógico que permite el tráfico de información privada sobre una infraestructura de red pública mediante el uso de criptografía.

Protocolos:

* + IPSec
  + SSL/TLS
  + PPTP, L2TP

**Seguridad Física:**

Consiste en mecanismos destinados a proteger físicamente cualquier recurso del sistema de amenazas producidas tanto por el hombre como por la naturaleza; en general serán prevención y detección.

* + **Tipos de Desastres**
    - Desastres naturales, incendios accidentales tormentas e inundaciones.
    - Disturbios, sabotajes internos y externos deliberados.
    - Amenazas ocasionadas por el hombre.
  + **Acciones Hostiles**
    - Robo
    - Fraude
    - sabotaje
  + **Control de Accesos**
    - Utilización de Guardias
    - Utilización de Detectores de Metales
    - Utilización de Sistemas Biométricos
    - Verificación Automática de Firmas (VAF)
    - Seguridad con Animales
    - Protección Electrónica

**Prácticas de Seguridad Física en móviles:** incluyen evitar manipular el dispositivo en lugares públicos y no transportarlo en contenedores visibles a terceros. Se recomienda utilizar contenedores de transporte que reduzcan el impacto y protejan el dispositivo del contacto con líquidos.

**Impacto en la Organización:**

* + **Pérdida de datos:** Puede afectar la reputación, la productividad y la rentabilidad de la organización.
  + **Robo de identidad:** Puede afectar a los clientes y empleados de la organización.
  + **Interrupción del negocio:** Puede causar daños económicos y afectar la imagen de la organización.
  + **Daño a la reputación**: Puede afectar la confianza de los clientes y socios de la organización.

Al considerar el impacto de la seguridad en una organización, es esencial abordar varios aspectos clave. Esto incluye la evolución de los riesgos de seguridad, las políticas corporativas, la evaluación y gestión del riesgo, el control de acceso, la continuidad del negocio, el cumplimiento de políticas y la gestión de incidentes. También se deben tener en cuenta la gestión de activos, el desarrollo de sistemas seguros, la seguridad física y la organización e integración de la seguridad de la información en toda la empresa. Estos aspectos garantizan una postura sólida en seguridad y protección de los activos de la organización.

**Seguridad Lógica:** La seguridad lógica se centra en la identificación y autenticación de usuarios, utilizando métodos como contraseñas o biométricos. Se deben gestionar las credenciales eficientemente y garantizar acceso solo a lo necesario. Es importante establecer un "single login" para simplificar el acceso a sistemas y aplicaciones. También se requieren procesos para administrar cuentas de usuarios, realizar revisiones periódicas de permisos de acceso y detectar actividades no autorizadas. Para casos de desvinculación de personal, como despidos, es vital contar con procedimientos claros para anular rápidamente los permisos de acceso y evitar posibles riesgos de seguridad.

**Modalidad de Acceso:**

Las modalidades de acceso se refieren al tipo de acciones que un usuario puede realizar sobre los recursos y la información. Estas modalidades incluyen:

* **Lectura:** el usuario puede ver o leer la información, pero no modificarla.
* **Escritura:** permite agregar, modificar o eliminar datos.
* **Ejecución:** el usuario puede ejecutar programas.
* **Borrado:** permite al usuario eliminar recursos del sistema.
* Todas las anteriores.

Además, hay modalidades especiales como:

* **Creación:** permite al usuario crear nuevos archivos, registros o campos.
* **Búsqueda:** permite listar los archivos de un directorio específico.

**Control de Acceso Interno:**

El control de acceso interno se basa en el uso de contraseñas para autenticar a los usuarios y proteger los datos y aplicaciones. Aunque de bajo costo, el uso de contraseñas puede resultar problemático cuando los usuarios deben recordar varias, lo que puede llevar a la elección de contraseñas débiles o a escribirlas, comprometiendo la seguridad. La sincronización de contraseñas permite que un usuario acceda con la misma contraseña a diferentes sistemas interrelacionados, lo que, si bien puede parecer un riesgo, estudios muestran que las personas tienden a usar una sola contraseña para múltiples sitios, aumentando el riesgo si se las obliga a usar diferentes contraseñas. La caducidad y control de contraseñas establece períodos para cambiarlas, asegurando su vigencia y seguridad.

* **Cifrado :** El cifrado de datos proporciona una medida robusta de control de acceso al permitir que solo aquellos con la clave correcta puedan descifrar la información.
* **Listas de Control de Accesos :** Las listas de control de accesos son registros que enumeran los usuarios autorizados a acceder a recursos del sistema y sus niveles de acceso, variando en capacidad y flexibilidad.
* **Límites sobre la Interfaz de Usuario :** Los límites sobre la interfaz de usuario restringen las funciones disponibles, como en los cajeros automáticos, donde los usuarios solo pueden ejecutar acciones específicas
* **Etiquetas de Seguridad:** Las etiquetas de seguridad son designaciones asignadas a recursos, como archivos, para controlar el acceso y especificar medidas de protección, siendo inalterables.
* **Dispositivos de control de puertos:** autorizan el acceso a puertos específicos y pueden ser físicamente independientes o integrados en otros dispositivos de comunicación.
* **Firewalls o puertas de seguridad:** separan redes públicas de redes privadas mediante la filtración del tráfico y su clasificación puede ser por software o hardware, con funcionalidades adicionales como VPN, escaneo de virus y filtrado de contenido.
* **Cifrado:** protege la información al permitir que solo aquellos con la clave correcta puedan descifrarla.
* **Listas de control de acceso:** registran usuarios autorizados y sus niveles de acceso.
* **Límites en la interfaz de usuario**: restringen las funciones disponibles para los usuarios.
* **Etiquetas de seguridad:** designaciones asignadas a recursos para controlar el acceso y especificar medidas de protección.
* **Clasificaciones de firewalls:** se dividen en filtros de paquetes, gateways de nivel de circuito, gateways de nivel de aplicación y de inspección multinivel del estado, cada uno con características y consideraciones de uso específicas**.**
* **Firewalls personales:** son software instalados en terminales individuales que filtran la información de red por interfaz o aplicación, complementando los firewalls de red para prevenir ataques internos. Son comunes en la mayoría de los sistemas operativos.
* **IDS (Sistema de Detección de Intrusiones):** detecta, identifica y responde a actividades anormales o no autorizadas.
* **Intrusión:** conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.
* **Modelo de funcionamiento de un IPS:** recolección de datos (registros de auditoría, sistemas, aplicaciones, paquetes de red), análisis de usos indebidos o anomalías, y respuesta activa o pasiva.
* **HIDS (Sistema de Detección de Intrusiones de Máquina):** Utilizan registros de auditoría, sistemas, aplicaciones (Servidor Web, FTP, etc.) y sistema de archivos como fuente de datos. Ejemplos: Tripwire, Prelude, lmsafe, GFI, LANguard, S.E.L.M.
* **NIDS (Sistema de Detección de Intrusiones de Red) y NNIDS (Sistema de Detección de Intrusiones de Nodo de Red):** Utilizan paquetes de red (TCP,UDP,IP) y pueden emplear agentes (IDS Distribuido). Ejemplos: Snort, Bro, Prelude, Suricata.
* **Por detección de uso indebido:** Utilizan datos de auditoría para establecer un perfil del sistema y activar alertas cuando las actividades no se ajustan al perfil. Ejemplos: Snort, Bro.
* **Por detección de anomalías:** Generan un perfil del sistema dinámicamente y declaran un estado de ataque ante una desviación estadística entre la información y el comportamiento actual. Ejemplos: lmsafe, Prelude.
* **Respuesta pasiva:** Generan un registro de evento o envían alertas, como correos electrónicos, ante una situación de ataque.
* **Respuesta activa:** Toman acciones automáticas para detener la continuidad del ataque, como cerrar sesiones de usuario o bloquear conexiones de intrusos.
* **IPS (Sistemas de Prevención de Intrusiones):** Combinan funciones de IDS y Firewall con respuesta activa, identificando y bloqueando ataques antes de que ocurran. Ejemplos incluyen lntruShield, Hogwash, Radware, StormWatch, entre otros como Sophos, Juniper, Tipping Point (3Com), Cisco, y Suricata.
* **Dispositivos UTM (Gestión Unificada de Amenazas):** Son firewalls que integran múltiples servicios en un solo equipo, incluyendo inspección de paquetes, VPN, antispam, antiphishing, antispyware, filtrado de contenidos, antivirus perimetral y detección/preventión de intrusos (IDS/IPS). Son soluciones fáciles de instalar y centralizadas, capaces de examinar paquetes en tiempo real sin impactar el rendimiento de la red.

**Modos de configuración de UTM:**

* **Modo Proxy:** Utilizan proxies para procesar y redirigir el tráfico interno, actuando como intermediarios entre la red interna y el internet.
* **Modo Transparente:** Procesan paquetes en tiempo real sin redirigirlos, requiriendo altas prestaciones hardware, pero ofreciendo una excelente alternativa de UTM.
* N**GFW (Firewalls de Nueva Generación):** Realizan inspección profunda de paquetes y utilizan tecnologías avanzadas para evitar intrusiones, combinando capacidades de firewall tradicional con características de próxima generación.
* **Desafíos de seguridad empresarial:** Incluyen la gestión de la configuración de red, la falta de aplicación de políticas por parte de ejecutivos senior, la actualización de parches, y el tráfico complejo y elevado en las redes.
* **WAF (Firewall de Aplicaciones Web):** Analiza el tráfico web para proteger contra ataques como SQL Injection, Cross Site Scripting, Buffer Overflows, entre otros, dirigidos al servidor web y que no pueden ser defendidos por IDS/IPS.
* **Modelo de Seguridad Positiva:** Los WAF en este modelo deniegan por defecto todas las transacciones y solo aceptan las consideradas seguras según reglas previamente definidas. Aunque es efectivo, puede volverse difícil de mantener con cambios en el diseño de la aplicación. No depende de actualizaciones, protegiendo contra ataques desconocidos, pero es propenso a falsos positivos y requiere un proceso de aprendizaje.
* **Modelo de Seguridad Negativa:** En este modelo, el WAF acepta todas las transacciones y solo bloquea las detectadas como amenazas. Menos preciso, depende de actualizaciones y bases de firmas de ataques, pero requiere menos ajustes y es fácil de administrar.
* **Ataques Detectados:** Los WAF pueden bloquear ataques comunes como buffer overflow, Cross Site Scripting y SQL Injection, monitoreando variables en peticiones GET y POST y detectando palabras clave en el tráfico web.
* **Proceso de Aprendizaje:** El WAF aprende el comportamiento de la aplicación y puede detectar anomalías, como intentos de inyección de código malicioso.
* **Riesgos:** Configurado incorrectamente, puede causar falsos positivos y retrasos en las transferencias, aunque se pueden mitigar con aceleradores SSL y otras técnicas.
* **Modos de Funcionamiento:** Pueden operar como bridge, router, proxy o plugin, disponibles en hardware y software. ModSecurity es un ejemplo de WAF software. La mayoría ofrece funciones de registro o logs.
* **Acceso de Personal Contratado o Consultores**: Requiere una política y administración de accesos especial para personal temporal.
* **Accesos Públicos:** Los sistemas de información para el público deben tener medidas especiales de seguridad, ya que los ataques pueden afectar negativamente la imagen de la organización.
* **Administración de Seguridad:** Implica implementar, dar seguimiento, probar y modificar los controles de acceso a sistemas y aplicaciones.
* **Política de Seguridad:** Debe guiar las decisiones sobre controles de acceso y perfiles de usuarios, considerando la clasificación de la información y el riesgo de exposición.
* **Implementación Priorizada:** Se inicia definiendo medidas de seguridad para la información más sensible y aplicaciones críticas, avanzando en orden de prioridad descendente.
* **Clasificación de Datos:** Los diferentes niveles de información requieren distintas medidas y niveles de seguridad.
* Conciencia Organizacional sobre Seguridad: Es crucial que todos los empleados estén conscientes de la seguridad, liderados por el ejemplo del personal directivo y estableciendo compromisos firmados que especifiquen responsabilidades.
* **Concientización sobre la Importancia de la Información:** La administración debe destacar la importancia de la información y las posibles consecuencias de su pérdida o apropiación por agentes externos.