UNIVERSIDAD LUTERANA SALVADOREÑA

FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

TECNICO EN DESARROLLO DE APLICACIONES MÓVILES

TEMA:

Seguridad en Redes

ESTUDIANTES:

Ramos Chávez, José Salvador **RC01136962**

Flor Abigail Climaco Rivera **CRR01136922**

Docente:

Eduardo Chachagua Alfaro

FECHA: 04 de junio de 2022

IPS

Definición de IPS:

IPS (Intrusion Prevention System) o sistema de prevención de intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés Unified Threat Management o Gestión Unificada de Amenazas) que controlan el acceso en función de reglas sobre protocolos y sobre el destino u origen del tráfico.

Tipos de IPS:

- Basados en Red Lan (NIPS): monitorizan la red lan en busca de tráfico de red sospechoso al analizar la actividad por protocolo de comunicación lan.
- Basados en Red Wireless (WIPS): monitorean la red inalámbrica en busca de tráfico sospechoso al analizar la actividad por protocolo de comunicación inalámbrica.
- Análisis de comportamiento de red (NBA): Examina el tráfico de red para identificar amenazas que generan tráfico inusual, como ataques de denegación de servicio, ciertas formas de malware y violaciones a políticas de red.
- Basados en Host (HIPS): Se efectúa mediante la instalación de paquetes de software que monitorizan un host único en busca de actividad sospechosa.

Ventajas de un IPS:

- Escalabilidad al gestionar multitud de dispositivos conectados a la misma red;

- Protección preventiva al comprobarse de forma automatizada comportamientos anómalos mediante el uso de reglas prefijadas;
- Fácil instalación, configuración y administración al estar disponibles multitud de configuraciones predefinidas y centralizar en un punto su gestión, aunque puede ser contraproducente para su escalabilidad;
- Defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;
- Aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Desventajas de un IPS:

Destacan los efectos adversos que pueden producirse en el caso de que se detecte un falso positivo, si por ejemplo se ejecuta una política de aislamiento de las máquinas de la red o en el caso de que se reciban ataques de tipo DDoS o DoS que pueden provocar su inutilización.

Proveedores de IPS comerciales:

- Cisco NGIPS
- Corelight y Zeek
- Fidelis Network
- FireEye Intrusion Prevention System
- McAfee Network Security Platform

Cisco NGIPS

El Sistema de Prevención de Intrusiones de Nueva Generación de Cisco (NGIPS) es parte de la oferta de seguridad general del gigante de las redes, que se agrupa bajo la marca Firepower. Cisco promete la visibilidad de los datos de seguridad a través del centro de administración centralizada de Firepower, y el NGIPS también puede integrarse con otras herramientas de seguridad de Cisco.

Corelight y Zeek

Zeek (antes conocido como Bro) es un sistema de detección de intrusos desarrollado por primera vez en el Laboratorio Nacional Lawrence Berkeley en los 90. Zeek ofrece un análisis general en profundidad del tráfico de la red con un enfoque en la seguridad; trabaja para analizar diferentes flujos de actividad y eventos, y los compara con los guiones de políticas escritas en el propio lenguaje de guiones de Zeek.

Fidelis Network

Es el componente IPS de su plataforma Elevate, que también incluye capas de tecnología de respuesta y engaño de punto final. Fidelis Network analiza el tráfico a través de los puertos y utilizando múltiples protocolos para detectar e informar de anomalías, así como para generar metadatos que pueden ser analizados más a fondo por otras herramientas

FireEye Intrusion Prevention System

Puede funcionar como un dispositivo físico o un dispositivo virtual en la nube, incluye un IPS como parte de su funcionalidad de a bordo. Uno de los grandes lanzamientos de seguridad de FireEye es su motor de ejecución virtual multivectorial (MVX, por sus siglas en inglés), que el IPS y otras herramientas utilizan para ejecutar código potencialmente peligroso en un entorno virtual controlado para probarlo.

McAfee Network Security Platform

Posiciona su Network Security Platform, que puede funcionar en dispositivos físicos o virtuales dentro de su red, como un «sistema de prevención de intrusiones de próxima generación». Combinando motores de detección basados en firmas y sin firmas, Network Security Platform también correlaciona la actividad de las amenazas con el uso de las aplicaciones para controlar el posible mal comportamiento.

Seguridad correo Electrónico

Definición de seguridad correo electrónico

La Confidencialidad es un riesgo asociado al envío de correo electrónico a otra persona a través de Internet. El mensaje de correo electrónico pasa a través de numerosos sistemas antes de llegar al destinatario.

Cómo cuidar la seguridad del correo electrónico.

1. Emplear una contraseña con características robustas de seguridad, modificándola periódicamente. Se sugiere emplear una longitud mínima de 8 caracteres, intercalando letras, números y símbolos especiales, evitando utilizar datos personales como la fecha de nacimiento o el mismo nombre de usuario. Así mismo es importante modificarla con cierta periodicidad con el objetivo de proteger del acceso no autorizado y del robo de identidad a través de nuestro correo electrónico.

2. Cifrar el correo electrónico. En caso de que se requiera preservar la confidencialidad de la información, existen soluciones para cifrar nuestros mensajes. Aplicaciones como Freenigma, GmailEncrypt o FireGPG, trabajan sobre servicios de correo basado en web como Gmail, Hotmail o Yahoo. Asi mismo, los clientes de aplicaciones como Outlook o Thunderbird cuentan con sus opciones de configuración o aplicaciones para hacer posible el cifrado y descifrado de la información.

Marcas comerciales (No gratuitas)

1. Mailjet
2. Email security
3. Gmx mail

Marcas opensource (gratuitas)

1. sothos utn
2. Zextrans
3. Ispy
4. helpsystems

Seguridad web

Consiste en cada acción o herramienta adoptada para evitar que las informaciones sean expuestas o propensas a ataques por parte de cibercriminales. Esas medidas también sirven para proteger a los usuarios, como los clientes de ecommerce y los lectores de blogs, e incluso al host.

Mantén al WordPress actualizado

Asegurarte de que todo el software esté actualizado es crucial para mantener seguro tu sitio web.

Esto se aplica al sistema operativo del servidor y a cualquier software que esté ejecutando en el sitio web, como un CMS. Recuerda que los hackers explotan las brechas de seguridad web en el sitio para realizar ataques.

Sin embargo, si estás utilizando una solución de hospedaje, no tienes que preocuparse por realizar estas actualizaciones de seguridad, ya que es responsabilidad de la empresa contratada.

Crea contraseñas fuertes

Parece obvio ofrecer un consejo como ese, ya que muchas personas saben que deben usar contraseñas complejas, pero eso no significa que esta práctica siempre se adopte.

Es esencial utilizar contraseñas fuertes para los perfiles de administración de servidores y sitios web, pero también es muy importante informar a los usuarios sobre las buenas prácticas que han ayudado a garantizar la seguridad web de la cuenta.

A pesar de que muchas personas lo consideran aburrido, la creación de requisitos de contraseña es una estrategia que ayuda en la protección de las informaciones.

Un ejemplo muy clásico de cómo funcionan esos criterios es la solicitud de contraseña con más de seis caracteres, incluidos un número y una letra mayúscula.

Configura perfiles de usuario

Incluso si las personas mal intencionadas no puedan cambiar el código de tu sitio web, pueden hacerlo con registros de usuarios.

Si tienes las direcciones IP registradas, con los respectivos historiales de actividad, será más fácil hacer un análisis del ataque sufrido.

Marcas comerciales (No gratuitas)

Awesome designs

IBM

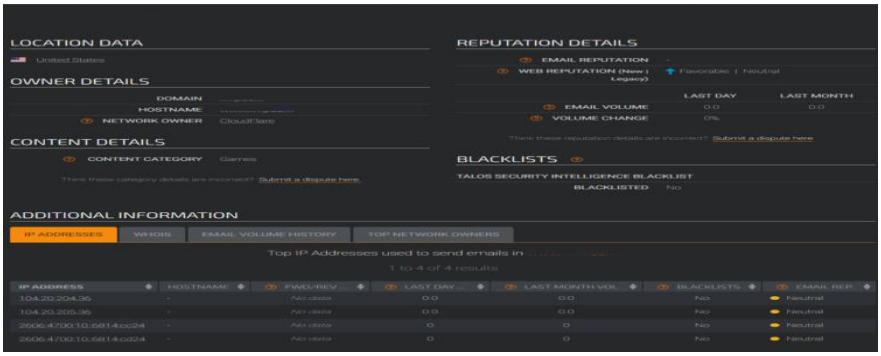
Fortinet

Mandiant

Crowdstrike holdings

Marcas opensource (gratuitas)

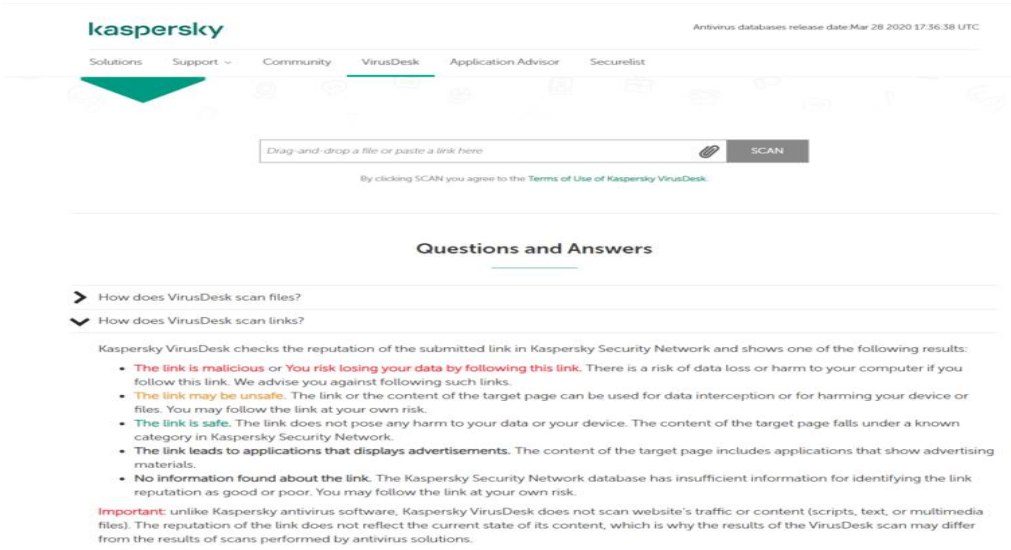
1. TalosInteligencia



TalosInteligencia es una fantástica red de detección de subprocesos y un centro de reputación de dominios.

Esta herramienta analiza los sitios web en busca de diversas amenazas. Proporciona un informe detallado, que contiene información relevante sobre los antecedentes del sitio. TalosIntelligence también muestra la clasificación de reputación, los resultados de la verificación de la lista negra y la información del dominio.

2. Kaspersky VirusDesk



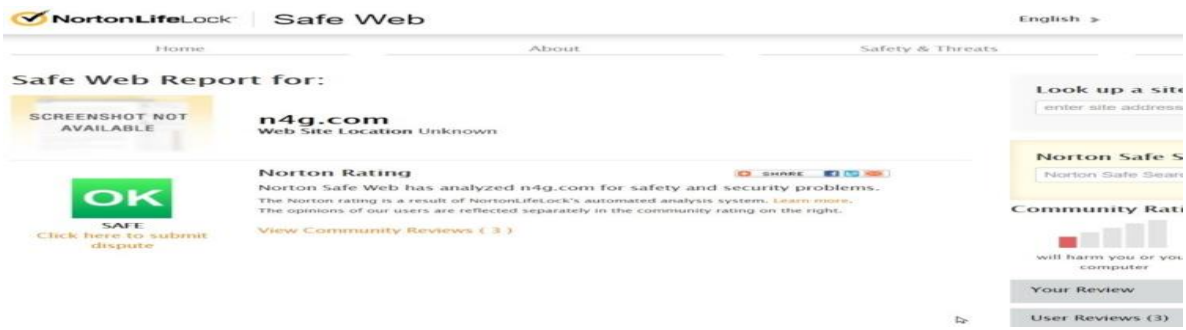
Kaspersky es un proveedor acreditado de soluciones de seguridad con más de 30 años de trayectoria impecable. Y también tiene un comprobador de sitios web falso y un escáner de virus. Simplemente pegue una dirección del dominio en cuestión y obtenga resultados en

unos momentos. Además, puede arrastrar y soltar archivos sospechosos para buscar software dañino.

Kaspersky VirusDesk comprueba la reputación del sitio web y le muestra si el enlace es inseguro o malicioso. Pero eso no es todo. La herramienta de Kaspersky comprende que los anuncios pueden bombardearlo contra su voluntad. Es por eso que muestra URL que tienen muchas ventanas emergentes y spam.

Además, este verificador de sitios web le notifica si no hay datos disponibles sobre el portal. Depende de usted elegir si vale la pena arriesgar la visita.

3.Norton Safe Web

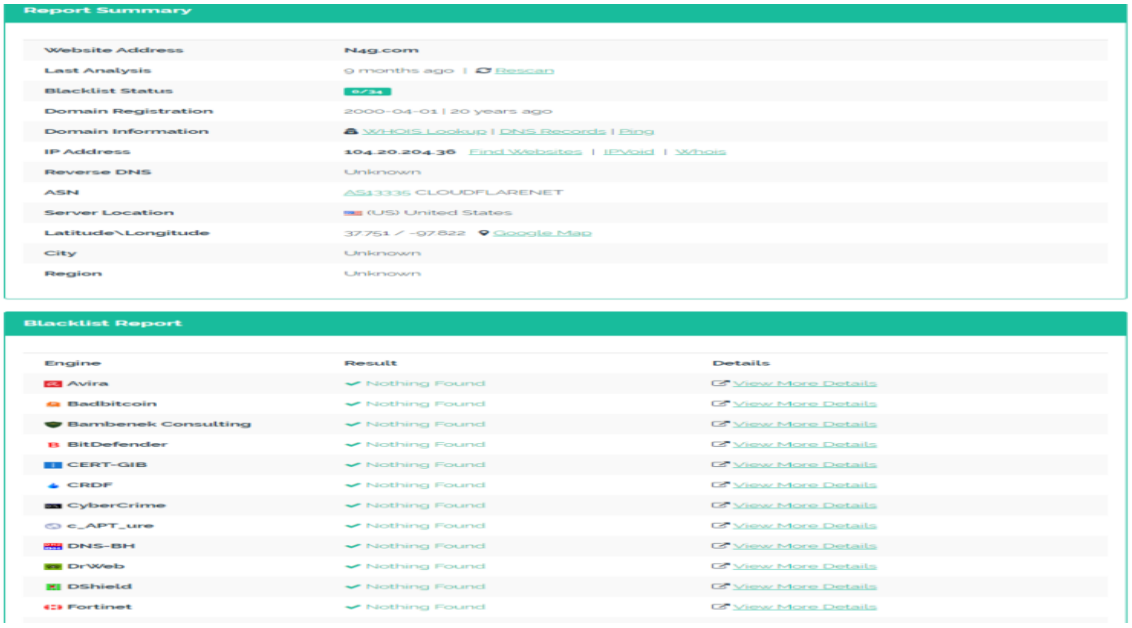


Otra falsificación comprobador de sitios web para un respetado antivirus empresa. Norton SafeWeb es un verificador de enlaces bastante sencillo si ha estado prestando atención hasta este momento. Ingrese una URL, haga clic en "Ingresar" y obtendrá información sobre la seguridad del sitio web. Esto también viene de serie como parte de Norton 360.

El sistema NortonLifeLock compila un informe basado en la reputación, la seguridad y los posibles problemas de seguridad del portal. Aparte de eso, esta herramienta tiene una sección de revisión de la comunidad. Puede leer lo que otros dicen sobre un sitio web. Es útil si desea evitar plataformas con muchos anuncios.

Pero espera. ¡Eso no es todo lo que Norton tiene para ofrecer para garantizar la seguridad de su navegación web! Es posible que desee prestar atención a las siguientes dos utilidades si es fanático de Google Chrome.

4. URLVid



Report Summary

Website Address	N4g.com
Last Analysis	9 months ago | Rescan
Blacklist Status	6/34
Domain Registration	2000-04-01 | 20 years ago
Domain Information	WHOIS Lookup | DNS Records | Ping
IP Address	104.20.204.36 Find Websites | IPVoid | Whois
Reverse DNS	Unknown
ASN	AS13335 CLOUDFLARENET
Server Location	(US) United States
Latitude\Longitude	37.751 / -97.822 Google Map
City	Unknown
Region	Unknown

BlackList Report

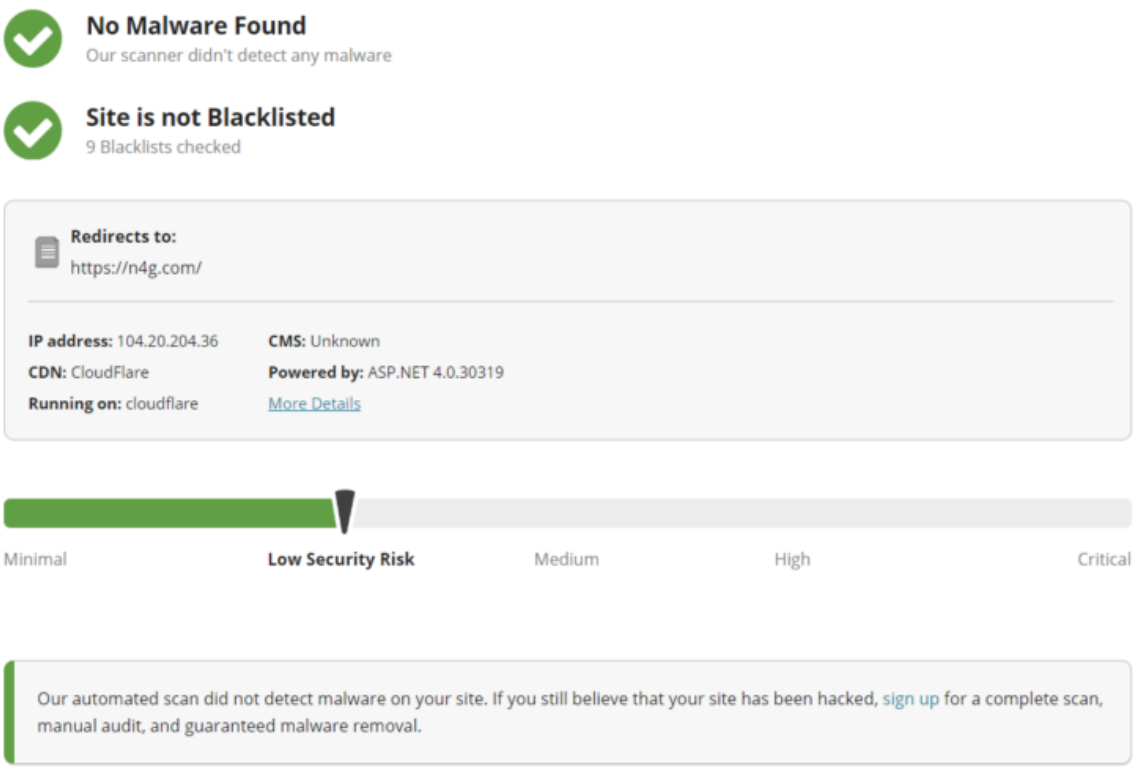
Engine	Result	Details
Avira	Nothing Found	View More Details
Badbitcoin	Nothing Found	View More Details
Bambenek Consulting	Nothing Found	View More Details
BitDefender	Nothing Found	View More Details
CERT-GIB	Nothing Found	View More Details
CRDF	Nothing Found	View More Details
CyberCrime	Nothing Found	View More Details
c_APT_ure	Nothing Found	View More Details
DNS-BH	Nothing Found	View More Details
DrWeb	Nothing Found	View More Details
DShield	Nothing Found	View More Details
Fortinet	Nothing Found	View More Details

URLVoid es una herramienta de verificación de sitios web falsos increíblemente popular de APIVoid. Puede escanear cualquier portal en busca de malware y amenazas de phishing utilizando software avanzado (incluidos más de 30 motores de listas negras).

Esta herramienta proporciona un resumen del sitio, información de dominio y otros datos disponibles públicamente. URLVoid también ofrece informes detallados de listas negras para cada motor que analizó el sitio web.

¿Le gusta esta herramienta de verificación de sitios web? Entonces siéntase libre de probar otros productos de APIVoid como Reputación de URL inspector y Dirección IP escáner.

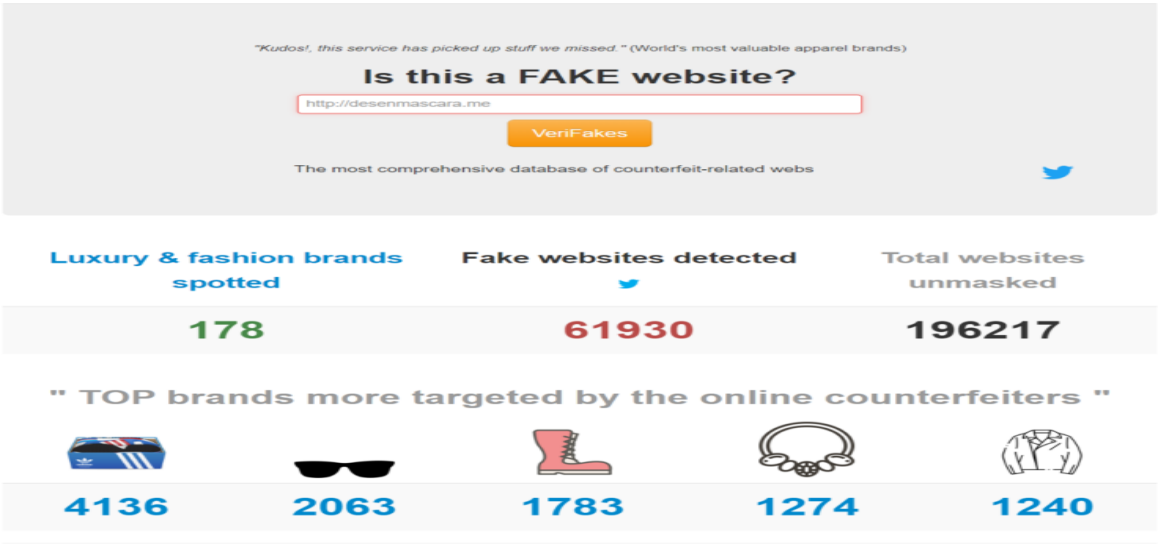
5. Sucuri



¿Encontraste un sitio web potencialmente defectuoso? Compruebe la seguridad del sitio web con Sucuri. Es un escáner de seguridad y malware gratuito y comprensible. También ofrecen servicios premium para que los propietarios de sitios web también aseguren sus propios sitios.

Ingresa la dirección de un sitio web y dale unos segundos. Sucuri analiza los portales en busca de virus, errores, software espía y código sospechoso. Esta herramienta clasifica la seguridad de un sitio web en una escala de "Mínima" a "Crítica".

Para que conste, puedes contactar con el equipo de Sucuri si quieres realizar un análisis exhaustivo.



A los falsificadores online les encanta falsificar productos de las mejores marcas. Y las marcas adoran desenmascara.me por la gran cantidad de estafadores que reveló a lo largo de los años. Este verificador de sitios web falsos ha detectado más de 61000 portales fraudulentos.

Desenmascara.me es una herramienta imprescindible para los amantes de las compras. ¿Quiere evitar comprar productos falsos? Solo necesita unos pocos clics para verificar la autenticidad de un portal y evitar posibles estafas.

Enlace para poder observar el video

https://www.youtube.com/watch?v=E7_FSwzGCWI