risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 03/27/2016
Aceitação/Acceptance: 04/19/2016

Estableciendo controles y perímetro de seguridad para una página web de un CSIRT

Jezreel Mejia Miranda[1], Heltton Ramirez[1]

{jmejia, heltton.ramirez}@cimat.mx

[1] Centro de Investigación en Matemáticas CIMAT A.C. Unidad Zacatecas, Av. Universidad No. 222, Fracc. La Loma, C.P. 98068, Zacatecas, Zacatecas, México

DOI: 10.17013/risti.17.1–15

Resumen: Uno de los principales medios de comunicación de un CSIRT es su sitio web, el cual sirve como principal contacto con el público objetivo y primer frente de vulnerabilidad de la seguridad perimetral de un CSIRT. Es por ello que al crear un sitio web para el CSIRT se debe tomar especial cuidado con las tecnologías a utilizar y aplicar controles de seguridad tanto en el desarrollo de la pagina web, así como, de la seguridad perimetral que permita evitar posibles ataques informáticos los cuales pueden poner en riesgo la reputación de un CSIRT. En este artículo se presenta, la definición del contenido del sitio web del CSIRT, la selección de tecnología para el desarrollo del sitio web, la revisión sistemática para proponer el contenido y controles de seguridad para el sitio web y su seguridad perimetral que debe tenerse en cuenta para un CSIRT.

Palabras-clave: CSIRT, sitio web, controles de seguridad, Wordpress. seguridad perimetral.

Establishing security controls and perimeter for a CSIRT website

Abstract: A website works as the main contact with the CSIRT's target audience, for this reason, when creating a website for the CSIRT, you must be taken special care with technologies when the website is developed and applying security controls, as well as, perimeter security in order to avoid computer attacks that may jeopardize the reputation of the CSIRT. This paper describes a proposal related to content and security controls of the CSIRT website. To achieved this, the systematic review was performed to propose the content and security controls for the website and its perimeter security that must be considered.

Keywords*:* CSIRT, web site, security controls, wordpress, perimeter security.

1. Introducción

Actualmente los equipo de respuesta a incidentes de seguridad informática (CSIRTs por sus siglas en ingles) son fundamentales debido a la creciente operatividad en delincuencia informática. Para el establecimiento de un CSIRT, trabajos como (ENISA, 2006) (Centro Criptológico Nacional, 2013) (Proyecto AMPARO, 2012) (Penedo, 2006)

especifican recursos tecnológicos que son necesarios para su funcionamiento, entre los cuales se encuentra el sitio web. Para muchas personas, el primer contacto que se tiene para un CSIRT se realiza mediante el sitio web (Penedo, 2006). En ella se encuentra información como la misión, visión, servicios, datos de contacto y publicaciones sobre avisos de seguridad así como manuales para la concientización de la seguridad informática (Software Engineering Institute, 2014; Muñoz, et al, 2015).

Sin embargo, hasta el momento no se ha estandarizado el contenido ni los controles de seguridad que debe tenerse en consideración durante el desarrollo del sitio web de un CSIRT. Es por ello que en este artículo se propone el tipo de contenido, la tecnología y los controles de seguridad para el sitio web de un CSIRT (concretamente Wordpress), con la finalidad de establecer un portal web más seguro para evitar posibles ataques informáticos los cuales pueden poner el riesgo la reputación del CSIRT. Para establecer la propuesta, se ha recolectado información a través de una revisión sistemática, una inspección de sitios web oficiales del portal FIRST con un Web Scraping y extrayendo información de sitios web del mismo portal con un web scanner.

Este artículo está estructurado de la siguiente manera: la sección 2 muestra conceptos fundamentales, la sección 3 muestra el contenido de un sitio web de un CSIRT, la sección 4 muestra cómo fue la selección de tecnologías para el sitio web, la sección 5 muestra cómo fue la revisión sistemática para obtener los controles de seguridad del sitio web del CSIRT, la sección 6 muestra la propuesta de contenido y controles de seguridad y la seguridad perimetral que debe establecerse para un sitio web de un CSIRT y al final se presentan las conclusiones.

2. Conceptos básicos

Los conceptos principales que se usan dentro de esta propuesta se describen a continuación.

2.1. CSIRT

Un CSIRT (Computer Security Incident Response Team) es un equipo especialista en seguridad de la información dedicados a responder incidentes de seguridad informática (Centro Criptológico Nacional, 2013). El termino CSIRT es el que se suele usar en lugar del término protegido CERT, registrado en EE.UU, por el CERT Coordination Center(CERT/CC) (ENISA, 2006).

Se usan diferentes abreviaturas para el mismo tipo de equipos:

- CERT o CERT/CC: (Computer Emergency Response Team / Coordination Center, equipo de respuesta a emergencias informáticas / Centro de coordinación).
- CSIRT: (Computer Security Incident Response Team, equipo de respuesta a incidentes de seguridad informática).
- IRT: (Incident Response Team, equipo de respuesta a incidentes).
- CIRT: (Computer Incident Response Team, equipo de respuesta a incidentes informáticos)
- SERT: (Security Emergency Response Team, equipo de respuesta a emergencias de seguridad).

2.2. Sitio web

Una página web o sitio web se compone de objetos. Un objeto es simplemente un archivo, puede ser HTML, una imagen, un applet de Java o un clip de video. Todo objeto web es alcanzable mediante un único URL (Uniform Resourse Locator, localizador uniforme de recursos), el cual es la forma más común de identificar un recurso Web.

La información que viaja del servidor HTTP hacia el usuario que solicita la información de la pagina lo hace mediante XML, HTML entre otros, y la información es visualizada mediante el navegador del cliente. La seguridad en el sitio web se compone de varios aspectos trabajando en conjunto como lo son el programador, el administrador, la configuración del sitio web y las herramientas utilizadas (Allen, 2001).

2.3. Controles de Seguridad

También llamadas Salvaguardas por la metodología Magerit (Esquema Nacional de Seguridad, 2012) los controles de seguridad son mecanismos de protección frente amenazas, reduciendo la frecuencia de las amenazas y limitan el daño causadas por éstas. Pueden ser buenas prácticas, software o hardware.

2.4. Web Scraping

Web Scraping es el proceso de automatizar la recolección de información útil de portales web (Vargiu & Urru, 2013). Esto se hace mediante programas de software los cuales extraen información simulando la navegación de un ser humano en la World Wide Web ya sea utilizando el protocolo HTTP.

Una vez establecidos los conceptos básicos, en la secciones siguientes se describen cómo se identificó el contenido que se recomienda tener un sitio web de un CSIRT, como se obtuvo las tecnologías a utilizar para el desarrollo del sitio web y los controles de seguridad pertinentes para proteger el sitio web.

3. Contenido de un sitio web para CSIRT

El propósito de esta sección es obtener elementos del contenido de un sitio web para un CSIRT. Es por ello que se realizó un análisis a la propuesta de contenido hecha en (Mejia, et al, 2015) mediante un Web Scraping, la cual contempla elementos que se recomienda tener en la página web de un CSIRT mostrados en la Tabla 1 y un análisis de 10 sitios CSIRT/CERT oficiales mostrados en la Tabla 2.

3.1. Análisis de paginas oficiales de CSIRT con herramienta

Dentro del análisis realizado en (Mejia, et al, 2015) se utilizó una herramienta para la extracción de la información de páginas oficiales de CSIRTs dentro del portal de la organización FIRST del inglés Forum of Incident Response and Security Teams que cuenta con una gran cantidad de CSIRTs registrados. La herramienta es del tipo web scraping la cual funciona recopilando información de portales web. A continuación en la Figura 1 describe gráficamente el funcionamiento de la herramienta.

Figura 1 – Descripción del funcionamiento del robot web.

3.2. Resultados de la revisión de contenido de la pagina web de un CSIRT con herramienta

A continuación se presentan los resultados obtenidos mediante la inspección de páginas web oficial de CSIRTs que se encuentran registrados dentro del portal de FIRST. En la Tabla 1 muestra los resultados encontrados mediante la herramienta dividido entre contenido y funcionalidad que se recomienda debe incluir una página de un CSIRT.

Contenido	Funcionalidad
Información del CERT	Novedades
FAQ	Mapa del sitio
Misión y objetivos	Multilíngüe
Información de contacto	Motor de búsqueda
Eventos	Base de conocimineto de vulnerabilidades
Documentos	Reporte online de incidentes
Herramientas	Zona de accesos restringidos
Avisos / vulnerabilidades	Lista de distribución por correo
Noticias / notas de seguridad	Publicación por RSS
Indicadores / estadísticas	
Enlaces (sitios relacionados)	

Tabla 1 – Elementos propuestos por Uribe (2014) sobre contenido y funcionalidad de un CSIRT.

3.3. Inspección de contenido de sitio web de CSIRT de manera manual

Para reforzar los resultados mostrados en la Tabla 1, también se realizó una inspección de manera manual, revisando contenido de sitios web sobre 10 CSIRTs/CERTs. Los sitios se eligieron al azar tomando en consideración que fueran CSIRTs/CERTs formalmente establecidos. Durante el análisis, se buscaron elementos que se muestran en la Tabla 1 y se añadieron otros que lo complementen. A continuación se enlistan los resultados dentro de la Tabla 2.

Características/Sitios	INCIBE	UNAM-CERT	INFOTEC	CERT	US-CERT	CERT-EU	NCI	ENISA	TERENA	TF-CSIRT
Acerca de	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
FAQ	Si	No	Si	Si	Si	No	No	No	No	No
Misión y objetivos	Si	Si	Si	Si	Si	No	Si	Si	No	No
Contacto	No	SI	SI	SI	SI	SI	SI	SI	SI	SI
Eventos	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Documentos	Si	Si	Si	Si	Si	Si	No	Si	Si	No
Herramientas	Si	Si	Si	No	No	Si	No	Si	No	No
Vulnerabilidades	Si	Si	No	Si	Si	Si	No	No	No	No
Noticias	SI	SI	SI	SI	SI	SI	SI	SI	SI	SI
Indicadores/estadísticas	No	SI	No	No	No	SI	No	No	No	No
Enlaces (sitios relacionados)	Si	Si	Si	Si	Si	Si	Si	Si	Si	Si
Seguridad en tu idioma/Tips	No	Si	No	No	Si	No	No	No	No	No
Blogs	Si	No	No	Si	No	No	No	No	No	No
Cursos	No	No	No	SI	No	No	No	SI	No	SI
Reporte de incidencias	SI	SI	No	SI*	SI*	No	No	No	No	No
Suscripción a alertas	Si	Si	No	Si	Si	Si	Si	Si	Si	No
Redes Sociales	Si	Si	Si	Si	Si	No	No	Si	Si	No

Tabla 2 – Cuadro de análisis comparativo entre 10 sitios CSIRT/CERT

Como se puede observar en la Tabla 2, los elementos que complementan a la Tabla 1 son: seguridad en tu idioma/tips, blogs, cursos, suscripción a alertas y redes sociales.

4. Selección de tecnologías.

Para la definición de tecnologías, lenguajes y herramientas a utilizar para la creación del sitio web de un CSIRT, se realizó un censo de las tecnologías utilizadas en sitios oficiales de CSIRT, obtenidas directamente de la página del foro de equipos de seguridad y respuesta a incidentes (FIRST, del inglés Forum of Incident Response and Security Teams) (FIRST.org, Inc., 1995).

Se obtuvo una muestra de 40 sitios web oficiales de CSIRT para conocer qué tecnologías empleaban mediante la herramienta WhatWeb en su versión 0.4.8 (Horton & Coles, 2015). El objetivo de la herramienta WathWeb es responder a la pregunta "¿Qué es este sitio web?", el cual identifica tecnologías incluyendo CMS (Content Management System), plataformas de blog, analiza paquetes, librerías javascripts, servidores web y dispositivos embebidos. Mediante sus 900 plugins, es posible también identificar versiones especificas de tecnologías, direcciones de correo electrónico, errores SQL y más (Morningstar Security, 2011). En la Figura 2 muestra un ejemplo de la información que muestra la herramienta al inspeccionar un sitio web.

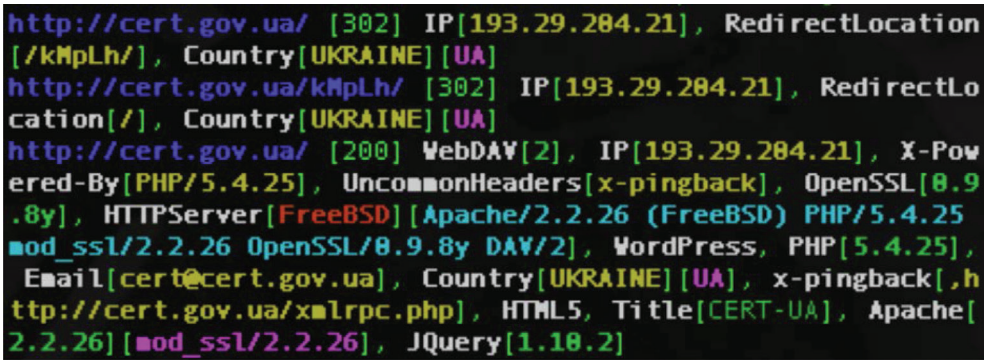

Figura 2 – Información extraída del sitio web cert.gov.ua con la herramienta WhatWeb.

Las tecnologías base más sobresalientes fueron 18 sitios que utilizan Apache como plataforma web, 8 de ellos utilizan ASP.NET, 25 de ellos están desarrollados en Wordpress y sólo 6 en Drupal, entre otras tecnologías. Por lo tanto, se decidió que la plataforma a utilizar sea Wordpress, la cual es más usada en el mundo (Onishi, 2013) y Apache para la creación del sitio web del CSIRT, y así dotarlas de seguridad de forma más especifica.

5. Controles de seguridad y seguridad perimetral

Definidas las tecnologías a utilizar para el sitio web del CSIRT, como resultado de la inspección de sitios web mostrados en la sección anterior, se proponen los controles de seguridad en especifico al CMS Wordpress debido al resultado obtenido en la sección anterior, asi como, la seguridad perimetral necesaria que debe acompañar la pagina web de un CSIRT, ya que la pagina web atrae a una gran cantidad de atacantes el cual su objetivo es penetrar la seguridad del sistema (Onishi, 2013).

Para llevar a cabo esta labor, se realizó una revisión sistemática, la cual es un método de investigación desarrollado para obtener, analizar, y evaluar toda la investigación relevante para una pregunta de investigación o un área de interés particular. Este método cuenta con 3 pasos los cuales son planificación, revisión y publicación los cuales se describen a continuación:

Planificación: la primer fase, en esta etapa se identifica la investigación, se establecen los objetivos y se realizan las siguientes actividades:

- Elección de nombre de la investigación.
- Formulación de las cadenas de búsqueda.
- Selección de fuentes de búsqueda de estudios y establecer los criterios de selección de estudios primarios y secundarios.

Revisión: en esta segunda fase se ejecutan las siguientes actividades:

- Ejecución de la búsqueda.
- Evaluación de la calidad de los estudios.

- Revisión de los estudios seleccionados.
- Extracción de la información.
- Documentos de extracción de datos.
- Ejecución de la extracción.

Publicación: tercera y última fase en la que se resume y analizan los resultados utilizando métodos estadísticos, las actividades que se contemplan son:

- Cálculo estadístico.
- Presentación de resultados.

A continuación se describen elementos principales de la revisión sistemática como lo es la pregunta de investigación, cadena de búsqueda y número de resultados obtenidos.

Preguntas de investigación: ¿Cuáles son las mejores prácticas y tecnologías de seguridad existentes orientados a proteger un sitio web hecho con Wordpress?

¿Cuáles son los activos esenciales para la conformación de una seguridad perimetral de un CSIRT?

Cadena de búsqueda: (Security && Wordpress), ("Infrastructure" AND ("CSIRT" OR "CERT")

Resultados de la consulta: La cadena de búsqueda fue introducida en 4 fuentes formales para su búsqueda, las cuales fueron IEEE, Springer Link, ACM y Google Scholar. En la Tabla 3 se muestra la cantidad de resultados por fuente.

Cadena de búsqueda	IEEE	Springer Link	ACM
(Security && Wordpress)	9	66	410
"Infrastructure" AND ("CSIRT" OR "CERT")	5	44	4,776

Tabla 3 – Resultados de la búsqueda de seguridad en Wordpress.

6. Propuesta

A continuación se muestra la propuesta obtenida mediante herramientas y una revisión sistemática sobre contenido de un sitio web y controles de seguridad para el mismo sitio bajo la plataforma Wordpress. Además, se presentan los dispositivos identificados para establecer la seguridad perimetral necesaria.

6.1. Contenido de un sitio web de un CSIRT

Como se menciona en la sección 3, se realizó un análisis de páginas oficiales de CSIRT mediante una herramienta e inspección de 10 sitios web. Este análisis permite proponer el siguiente contenido recomendado para un sitio web de un CSIRT. El criterio de selección de contenido consiste en que al menos 8 o más sitios de CSIRT dentro de la Tabla 2 hagan uso de la sección, incluyendo también Tips de seguridad el cuál es recompensable para dirigirse al publico sin tanta experiencia en los temas de seguridad.

- **Inicio:** La página principal del sitio CIMAT CERT. En esta página se pretende mostrar primeramente una imagen que sea llamativa con el enlace a las secciones de los reportes de incidentes y a los tips de seguridad.
- **Incidentes (reportes):** En esta página se muestra el formulario correspondiente al reporte de incidencias de seguridad por parte de los usuarios.
- **Tips de seguridad:** En esta página se mostrarán los tips y alertas de seguridad que le permitirán a los usuarios mejorar sus prácticas de seguridad.
- **Publicaciones (documentos):** En este apartado será posible leer y descargar una serie de documentos referentes a investigaciones y actividades de seguridad que el CERT del CIMAT ha llevado a cabo.
- **Contacto:** Se mostrará información de contacto y ubicación del CIMAT CERT.
- **Acerca de (misión, visión y objetivo):** En esta página se pretende mostrar información acerca de las actividades que el CIMAT CERT lleva a bajo.
- **Noticias:** En esta página se presentarán las noticias y notas de seguridad más recientes.
- **Vulnerabilidades:** En esta sección del sitio se mostrarán las vulnerabilidades e incidentes más recientes.
- **Eventos:** En esta página se mostrarán los eventos programados junto con información de contacto relacionados con seguridad informática y de cómputo.
- **Entradas (publicación, vulnerabilidad, noticia, incidente, evento, tip):** Esta página en realidad es una generalización de los diferentes tipos de publicaciones que se realizarán en el sitio, como pueden ser tips de seguridad, noticias, incidentes, eventos, publicaciones y vulnerabilidades.

6.2. Seguridad para el sitio web del CSIRT

Como resultado de la revisión sistemática nombrada en la sección 5, a continuación se presentan los controles de seguridad que se recomiendan implementar en un sitio web creado con Wordpress. Los controles de seguridad se seleccionaron para proteger los tipos de ataques en sitios web mostrados en el trabajo (Patel, Rathod, & Prajapati, 2013) enfocados a Wordpress los cuales son memoria Cache, acceso seguro, seguridad en archivos.httpaccess/wp-config.php, directorios transversales, bases de datos y copias de seguridad.

6.2.1. Seguridad en plataformas web apache

Antes de describir los controles de seguridad a tener en cuenta en la pagina web de un CSIRT desarrollada bajo el CMS wordpress, se describe la seguridad que se debe considerar en un servidor apache.

El servidor HTTP Apache es un servidor web HTTP de código abierto y se caracteriza por ser estable, multiplataforma, modular y altamente configurable, además, dispone de componentes de seguridad, los cuales configurados de forma correcta, son aprovechados para fortalecer las condiciones de acceso a los recursos web disponibles para ser recuperados a través de solicitudes http realizadas por un navegador, además Apache es de código abierto (Open Source) y gratuito (Gomez, et al, 013). Además, de ser el servidor http mas común para ejecutar paginas web creadas en wordpress.

Una configuración adecuada de Apache permite evitar que se entregue información en líneas de encabezado de los mensajes de respuesta http. También se puede configurar Apache para recibir conexiones seguras mediante el protocolo HTTPS, el cual es http sobre SSL (Secure Socket Layer) (Geeknet, 2012). Inclusive, es conveniente la instalación y configuración del Firewall de aplicación ModSecurity (Modsecurity, 2015), la cual funciona como una herramienta de registro, detección y mitigación contra ataques al servidor web apache (Geeknet, 2012).

Otras recomendaciones o buenas prácticas relevantes se encuentran el tener un conocimiento completo de todos y cada uno de los elementos del archivo de configuración de Apache (estructura, parámetros y valores), ya que incluir elementos desconocidos o cargar módulos innecesarios puede comprometer la seguridad del sitio. Realizar una gestión de usuarios para administrar el monitoreo constante del ciclo de vida de los usuarios del sistema, entre los cuales se incluye la eliminación de cuentas de usuario innecesarias para la prestación del servicio y analizar el alcance de permisos y privilegios de cada usuario del sistema. Verificar la existencia de archivos en el sistema con permisos de ejecución y monitorear el listado de tareas programadas para prevenir la ejecución de acciones no previstas por el administrador del sistema. Proveer lo mínimo de información sobre la huella identificativa del servidor Web, y si es necesario, cambiar la información para que funcione como distractor para el atacante. Como ultima recomendación, aislar el servidor web Apache del sistema operativo con el objetivo de mitigar el impacto que podría sufrir una organización si el servidor web se ve comprometido por un atacante. Este procedimiento se conoce como Jail (Jaula).

6.2.2. Memoria cache

La memoria caché es una forma de optimización muy utilizada para ahorrar memoria, procesamiento y poder acelerar el tiempo de carga de una página web de forma considerable. La memoria caché es una forma de optimización muy utilizada para ahorrar memoria, procesamiento y poder acelerar el tiempo de carga de una página web de forma considerable. Wordpress por naturaleza es lento, conforme se van añadiendo más utilidades, temas o complejidad al sitio la página web crece y las velocidades de carga se van reduciendo, además el lenguaje de programación con el que funciona Wordpress (PHP) es poco eficiente. Cualquier página web puede sufrir de tráfico masivo (slashdotted) por lo que causa que deje de responder el sitio, esto es consecuencia de almacenamiento de caché insuficiente. La solución es almacenar en caché las páginas, esto es guardar copias estáticas de archivos en directorios ocultos y re direccionar las visitas entrantes a estas páginas, además de acelerar las cosas para los visitantes, también reduce considerablemente el uso CPU (Leary, 2013).

Lamentablemente Wordpress no cuenta con caché integrada, pero cuenta con diferentes opciones de caché. El que se implementó en la página web fue WP Super Cache, éste trabaja reescribiendo en el archivo.htaccess para re direccionar las peticiones de las páginas dinámicas de wordpress a los archivos estáticos guardados en un directorio oculto en su instalación.

6.2.3. Seguimiento de problemas de rendimiento

Si el sitio Wordpress sufre de problemas de rendimiento y no está siendo atacado, es muy probable que cuente con alguna mala configuración con respecto a red, plugins, temas Wordpress o base de datos.

Si el problema persiste, mediante herramientas propias de Firefox como YSlow (Yslow, 2015) junto con Firebug pueden ser de utiliza para verificar que existen muchas imágenes o elementos en el sitio al arrancar. Si no es el caso, puedes probar con un plugin llamado WP Tunner y visitar la página principal, debajo de ella se verán todas las consultas a la base de datos y así darse cuenta si se trata de problemas con el motor de la base de datos. Si los problemas persisten, prueba desactivando plugins o cambiar el tema por el de default para verificar si cuenta con mejor rendimiento (Onishi, 2013).

6.2.4. Acceso seguro

En las versiones más antiguas de Wordpress, la cuenta del primer usuario siempre era Admin. Esto era relativamente fácil para los piratas informáticos crackear el acceso al sitio. Desde la versión 3.0, el usuario puede elegir el nombre de usuario durante la instalación, esto acorta el problema en escala, pero no mitiga por completo el riesgo. Un Método para proteger Wordpress ante ataques de fuerza bruta es bloquear la pantalla de login. Para mayor seguridad usar siempre SSL en el proceso de login para que las credenciales viajen de manera encriptada, inclusive, es posible que se considere usar SSL en todas las tareas administrativas.

Para el bloqueo del login de Wordpress existe un plugin llamado Login Lockdown, el cual funciona bloqueando un rango de IP después de haber fallado muchos intentos de acceder en un periodo de tiempo corto.

6.2.5. Remover la etiqueta cabecera generada

Una de las cosas que wp_head() agrega al tema de Wordpress es una etiqueta la cual muestra la versión exacta de Wordpress que se está usando, esto ayuda a los desarrolladores a ver cuántas versiones de wordpress hay en el mundo, sin embargo, esto también puede advertir a un pirata informático de qué versión de Wordpress se está usando en el sitio y así buscar vulnerabilidades de Wordpress en caso que no se esté al día. Para remover la etiqueta es con la siguiente línea de código. *Remove_action('wp_head', 'wp_generator')*

6.2.6. Seguridad en el archivo.htaccess y wp-config.php

Existen muchas maneras en las cuales piratas informáticos pueden usar el archivo. htaccess de manera maliciosa. Podrían reescribir reglas para re direccionar a los visitantes a otras páginas que no sea la genuina. Otra manera de hacer mal uso del archivo es escribir un archivo dentro de un subdirectorio de Wordpress lleno de enlaces SPAM y usar los directorios de PHP como auto_prepend_file o auto_append_file para incluir el archivo al archivo index.php del tema en funcionamiento.

Para proteger en ese sentido, es recomendable colocar permisos para que sólo el administrador pueda modificar el archivo.htaccess. También es posible modificar el

archivo.htaccess para asegurar que sólo tu puedas ver y modificar el archivo wp-config.php. Para realizar esta protección, es posible hacerlo mediante el siguiente código.

<Files wp-config.php>
order allow, deny
deny from all
</Files>
<Files.htaccess>
order allow, deny
deny from all
</Files>

6.2.7. Cambiar de localización archivos

Es posible mover el archivo wp-config.php y la carpeta wp-content a un lugar diferente del index.php. Todo esto ayuda a minimizar el ataque mediante un exploit de directorios con permisos de escritura en lugares predecibles. Un archivo importante de mover es el wp-config.php debido a que ahí se almacenan contraseñas de la base de datos al igual que otros datos importantes. Es posible mover el archivo a una localización externa a la carpeta publica del servidor web y Wordpress detectará automáticamente el nuevo archivo. Para mover el contenido de Wordpress, se debe definir constantes de todo dentro del archivo de configuración para que plugins que requieran de una ruta especifica no dejen de funcionar.

6.2.8. Seguridad en Base de Datos

Es necesario elegir unas buenas credenciales (elegir una buena contraseña) para la base de datos al igual que cambiar el prefijo de las tablas y respaldar la base de datos con regularidad. Para cambiar el prefijo que cuenta por default Wordpress es sencillo mediante el proceso de instalación, a la hora de configurar la base de datos de Wordpress, se muestra la opción de cambiar el prefijo. Esto funciona como medida de protección ante ataques básicos de SQLInjection, pero no los detiene del todo. Esto es útil cuando un atacantes hace usos de herramientas de hackeo automatizadas para sitios Wordpress.

6.2.9. Copias de seguridad de base de datos y archivos

Realizar copias de seguridad de tu base de datos con frecuencia es esencial si pretendes restablecer tu sitio cuando un desastre ocurra. Esto puede ser provisto por tu compañía de hosting aunque siempre es recomendable tener respaldos propios. Existen muchos plugins que ayudan a hacer respaldos, uno de ellos es el WP-DB-Backup, una vez instalado es posible realizar un respaldo con su menú de herramientas. Para realizar respaldos de archivos es mucho más sencillos, sólo es necesario copiarlos. Es posible automatizar el proceso mediante herramientas como rsync o usar clientes FTP para sincronizar, descargar y actualizar copias cada vez que sea necesario.

6.2.10. Monitorizar problemas de seguridad

Existen muchos plugins que permiten mantener una segura instalación de Wordpress. Enseguida se muestra una lista de ellos.

- WP Security Scan verifica los permisos de los archivos, contraseñas, seguridad en base de datos y más. Provee de herramientas para arreglar muchos de los problemas identificados.
- Wordpress Firewall monitoriza las peticiones HTTP con una lista negra de firmas conocidas como maliciosas y puede mandar un email cuando algo sospechoso aparezca.
- Exploit Scanner busca en los archivos y base de datos cualquier entrada maliciosa, como archivos llenos de links SPAM.
- Audit Trail es útil para hacerle saber cuando alguien ha intentado acceder.

6.3. Seguridad perimetral

La seguridad perimetral es una parte fundamental en el funcionamiento de un CSIRT debido al uso de la pagina web como principal medio de contacto con el publico objetivo. Este medio hace énfasis en el tráfico de información a través de la red, y en el uso de puertos de conexión, los cuales están asociados con los servicios que se presentan. Aquí es donde entran dispositivos a tenerse en cuenta para establecer una seguridad perimetral adecuada como los cortafuegos (Firewalls), sistemas de detección de intrusos (IDS), criptografía asimétrica, SSL (Secure Socket Layer), Proxies, entre otros. A continuación se presenta una breve descripción de estos principales mecanismos de seguridad.

6.3.1. Cortafuegos

Es una tecnología que busca desarrollar un control de acceso en el tráfico de la red, identificando qué paquetes pueden o no ingresar o salir del perímetro de la red de la organización. Este equipo funciona como control de acceso del tráfico para evitar que personas no autorizadas traten de invadir desde el exterior la red interna. El uso de un Firewall o cortafuego es importante ya que protege de ataques del exterior a organizaciones que se encuentran conectadas a internet. Sin un Firewall, la organización está expuesta a un gran número de riesgos, incluyendo los siguientes (Picouto, et al, 2008).

- Pérdida de información sensible de la organización como registros financieros, estrategias de negocios, modelos arquitectónicos y prototipos, planteamientos, registros médicos.
- Exposición de datos críticos con respecto a la infraestructura tecnológica que un atacante puede aprovechar para planear sus ataques.
- Consecuencias legales cuando un adversario hace uso de las computadoras de la organización para afectar sus ataques.
- Vandalismo en servicios públicos (como lo es el sitio web).

6.3.2. Cortafuego de tipo filtrado de paquetes

Los cortafuegos del tipo filtrado de paquetes verifican las cabeceras de los paquetes que contienen las direcciones IP origen y destino, protocolo, puerto, permitiendo o denegando el acceso a la red que protege. De aquí se desprenden algunas tecnologías utilizadas para los filtrados, los cuales son filtrado estático, filtrado dinámico o inspección de estado.

De este dispositivo se desprenden algunas tecnologías utilizadas para los filtrados, los cuales son filtrado estático, filtrado dinámico o inspección de estado. En el trabajo (Allen, 2001), se recomienda utilizar inspección de estado, este genera una tabla donde se mantienen los estados de las conexiones de todas las sesiones para que los paquetes pasen secuencialmente y sean filtrados por las reglas configuradas.

6.3.3. Cortafuego de tipo proxy de aplicación

Un cortafuegos del tipo proxy de aplicación es un programa que corre en un sistema cortafuegos entre dos redes. Cuando un programa cliente establece conexión atreves de un proxy hacia su servicio de destino, éste primero establece conexión con el programa proxy. El cliente negocia con el proxy para que el establezca una conexión con el servicio de destino, si la negociación es exitosa, entonces se establecen 2 conexiones, una desde el cliente hacia el proxy, y otra del proxy hacia el servicio solicitado.

Como en el caso de filtrado de paquetes, aquí también se desprenden tecnologías, una de ella son los Proxies transparentes. Esta tecnología combina filtrado de paquetes, reescritura de paquetes y una aplicación de proxy.

6.3.4. Sistema de detección/prevención de intrusos

Del inglés IDS (Instrusion Detection System), actúan como un monitor del tráfico de red, describiendo y analizando ahora el contenido de los paquetes que ingresan a la organización. Sus principales funcionalidades son las siguientes:

- Detectar ataques y otras violaciones de seguridad.
- Implementar calidad de control para eventos de seguridad y administración.
- Proporciona información acerca de los intrusos que intentan acceder a la red o sistemas.
- Previene problemas de comportamiento de abusos en el sistema o red.

La diferencia con respecto a un Firewall, es que un IDS examina los paquetes a más profundidad sobre su contenido y con ello definir las intenciones del mismo.

7. Conclusiones

Un sitio web de un CSIRT, es un elemento principal de un CSIRT debido a que en ella se da a conocer al CSIRT hacia el público objetivo, publicar alertas, amenazas y concientizar a las personas sobre los peligros del internet, entre otras cosas. Gracias a herramientas como los web scraping fue posible analizar de manera automática todos los sitios web de los CSIRT del portal FIRST y junto con la inspección manual se concluye que no todos los sitios oficiales de CSIRT cuentan con la misma estructura. Además, fue confirmado por la herramienta WhathWeb donde se obtuvo como resultado que no existe el uso de una misma tecnología para la creación de los sitios web. Como resultado de la revisión sistematica se obtuvieron los controles de seguridad base para una de las tecnologías más usadas en la creación de sitios web para CSIRT la cual es Wordpress. Así como, identificar los principales dispositivos necesarios para robustecer la seguridad perimetral que debe acompañar la pagina web de un CSIRT.

Referencias

ENISA.(2006). “Cómo crear un CSIRT paso a paso. [Online] https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport.

Centro Criptológico Nacional. (2013, Junio) www.ccn-cert.cni.es/. [Online]. https://ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/820/820-Proteccion_contra_DoS-jun13.pdf

Proyecto AMPARO. (2012). Manual básico de: Gestión de incidentes de seguridad informática.

Penedo, David. (2006). Technical Infrastructure of a CSIRT. IEEE 0-7695-2649-7/06, 2006.

Software Engineering Institute. (2014). Cert. [Online]. http://www.cert.org/incident-management/services.cfm?

Muñoz, Mirna, & Rivas, Lizbeth. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (spe3), 1–15. https://dx.doi.org/10.17013/risti.e3.1–15

Allen, Julia H. (2001). The CERT Guide to System and Network Security Practices. 480 pages, Addison-Wesley Professional; 1 edition (June 17, 2001), ISBN-10: 020173723X, ISBN-13: 978-0201737233

Esquema Nacional de Seguridad. (2012) MAGERIT - Versión 3.0 Metogolodía de Análisis y Gestión de Riesgos de los Sistemas de Información.

Vargiu, Eloisa and Urru, Mirko. (2013). Exploiting web scraping in a collaborative filtering- based approach to web advertising. Artificial Intelligence Research, vol. 2, no. 1.

Mejia, Jezreel, Muñoz, Mirna and Uribe, Edgar. (2015). Services establishment in the computer security incident response teams: A review of state of art. *CISTI)*, Aveiro, 2015, pp. 1–6. doi: 10.1109/CISTI.2015.7170502

FIRST.org, Inc. (1995). https://www.first.org. [Online]. https://www.first.org/members/teams

Horton, Andrew and Coles, Brendan. (2015). https://github.com/urbanadventurer/whatweb. [Online].

Morningstar Security. (2011) http://www.morningstarsecurity.com/research/whatweb. [Online].

Onishi, Adam. (2013). Security and Performance in Pro WordPress Theme Development. Apress, 2013, pp. pp 297–332.

Patel, Savan K, Rathod, V. R. and Prajapati, Jigna B. (2013). Comparative Analysis Of Web Security In Open Source Content Management System. International Conference on Intelligent Systems and Signal Processing (ISSP).

Gómez Montoya, Carlos E; Candela Uribe, Christian A. and Sepúlveda Rodríguez, Luis E. (2013). Seguridad en la configuración del servidor web Apache. INGE CUC,, vol. 9, no. 2, pp. pp 31–38.

Geeknet. (2012). Securing a Linux/Apache Webserver with comon opensourse tools. [Online]. http://reg.accelacomm.com/servlet/Frs.FrsGetContent?id=40115117

ModSecurity. (2015, Nov.) https://www.modsecurity.org/. [Online]. https://www.modsecurity.org/

Leary, Stephanie. (2013). Performance and Security. in WordPress for Web Developers. Apress, 2013, pp. pp 125–140.

Yslow. (2015) http://yslow.org/. [Online]. http://yslow.org/

Picouto Ramos, Fernando; Lorente Pérez, Iñaki; Garía-Moran, Jean Paul and Ramos Varón, Antonio Ángel. (2008). Firewalls. in Hacking y seguridad en Internet.