07 de mayo de 2021
Ficha N° 2 WHATWEB
CSIRT DE GOBIERNO

Comando de la semana “WHATWEB”

I. Contexto

Este documento, denominado “comando de la semana", tiene como objetivo ilustrar sobre herramientas que pueden ser de utilidad para el lector, a objeto de ir potenciando las capacidades locales de autochequeo, detección simple de vulnerabilidades que están expuestas a internet en sus activos de información y, a su vez, la obtención de una verificación de la subsanación de aquellas que se les han sido reportadas, facilitando la interacción con el CSIRT de Gobierno. El objetivo no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos.

II. Introducción

¿Qué hacer si desde el CSIRT nos llega un ticket señalando que hay problemas con la versión del web Server o de las tecnologías de apoyo como CMS, plugins, JavaScript, PHP u otras? ¿Cómo verificamos, una vez que hemos aplicado alguna mitigación y queremos probar si ha tenido efecto, antes de reportarla como problema solucionado al CSIRT o a nuestros auditores internos?

Para este caso existe un comando Linux que nos ayuda a detectar información relevante sobre nuestra plataforma y tomar decisiones de actualización o estrategias de mitigación: WhatWeb.

WhatWeb identifica sitios web. Su objetivo es responder a la pregunta, "¿Qué es ese sitio web?". WhatWeb reconoce tecnologías web que incluyen sistemas de gestión de contenido (CMS), plataformas de blogs, paquetes de estadísticas / análisis, bibliotecas JavaScript, servidores web y dispositivos integrados. WhatWeb tiene más de 1700 complementos, cada uno para reconocer algo diferente. WhatWeb también identifica números de versión, direcciones de correo electrónico, ID de cuenta, módulos de marco web, errores de SQL y más.

HTTP significa Hypertext Transfer Protocol. Toda la World Wide Web (Internet) utiliza este protocolo, establecido a principios de los 90. Casi todo lo que aparece en un navegador ha sido transmitido a través de HTTP mediante requests y responses entre navegador y servidor.

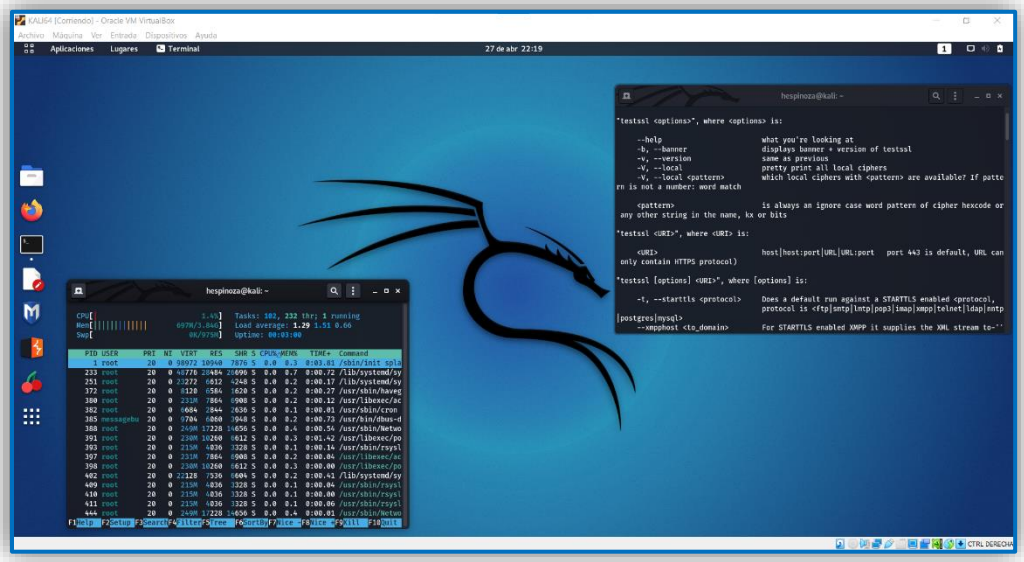
Los HTTP headers son la parte central de los HTTP requests y responses, y transmiten información acerca del navegador del cliente, de la página solicitada, del servidor, etc.

- Cabecera de consulta: Cabeceras que contienen más información sobre el contenido que va a obtenerse o sobre el cliente.
- Cabecera de respuesta: Cabeceras que contienen más información sobre el contenido, como su origen o el servidor (nombre, versión, etc.).

III. Paso a Paso

PASO 1: Un entorno adecuado para trabajar.

Primero debe contar con una distribución de Kali[1] Linux funcionando ya sea en una máquina física o en una máquina virtual[2][3].



[1] https://www.kali.org/downloads/

[2] https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/16_0

[3] https://www.virtualbox.org/wiki/Downloads

PASO 2: Instalar el comando.

Una vez que se cuenta con este sistema operativo de manera funcional podemos instalar el comando WhatWeb; en general este ya viene preinstalado en la distribución KALI, pero si no fuere así puede instalarlo con el siguiente comando:

```
sudo apt-get install whatweb
```

PASO3: Verificar su instalación.

Una vez que se instalado podemos explorar las múltiples opciones que ofrece para su ejecución:

```
root @ kali: ~ # whatweb -h
WhatWeb - Escáner web de próxima generación versión 0.4.9.
Desarrollado por Andrew Horton alias urbanadventurer y Brendan Coles.
Página de inicio: http://www.morningstarsecurity.com/research/whatweb

Uso: whatweb [opciones] <URLs>

SELECCIÓN DE OBJETIVO:
  <TARGETs> Ingrese URL, nombres de host, direcciones IP,
        nombres de archivo o rangos de direcciones IP en formato nmap.
  --input-file = FILE, -i Leer destinos de un archivo. Puede canalizar
      nombres de host o URL directamente con -i / dev / stdin.

MODIFICACIÓN DE OBJETIVO:
  --url-prefix Agrega un prefijo a las URL de destino.
  --url-suffix Agrega un sufijo a las URL de destino.
  --url-pattern Inserta los destinos en una URL.
      por ejemplo, example.com/%insert%/robots.txt

AGGRESSION:
El nivel de agresión controla el equilibrio entre velocidad / sigilo y
confiabilidad.
  --aggression, -a = LEVEL Establece el nivel de agresión. Predeterminado: 1.
  1. Stealthy Realiza una solicitud HTTP por destino y también
        sigue las redirecciones.
  3. Agresivo Si un complemento de nivel 1 coincide,
        se realizarán solicitudes adicionales.
  4. Pesado Realiza muchas solicitudes HTTP por destino.
        Se intentan las URL de todos los complementos.
```

WhatWeb admite un parámetro de nivel de profundidad para controlar el equilibrio entre velocidad y confiabilidad. Cuando visita un sitio web en su navegador, la transacción incluye muchos indicios de qué tecnologías web están impulsando ese sitio web. A veces, una sola visita a una página web contiene suficiente información para identificar un sitio web, pero cuando no es así, WhatWeb puede interrogar más veces al sitio web. El nivel de profundidad predeterminado, llamado 'sigiloso', es el más rápido y requiere solo una solicitud HTTP de un sitio web. Esto es adecuado para escanear sitios web públicos. Se desarrollaron modos más agresivos para su uso en pruebas de penetración.

La mayoría de los complementos de WhatWeb son exhaustivos y reconocen una variedad de pistas, desde sutiles hasta obvias. Por ejemplo, la mayoría de los sitios web de WordPress pueden identificarse, por ejemplo, mediante la meta etiqueta HTML {name=”generator” content=”WordPress”}, pero una minoría de los sitios web de WordPress eliminan esta etiqueta de identificación, lo que no es un obstáculo para WhatWeb. El complemento WordPress WhatWeb tiene más de 15 pruebas, que incluyen la verificación del favicon, los archivos de instalación predeterminados, las páginas de inicio de sesión y la verificación de "/ wp-content /" dentro de los enlaces relativos.

Características generales de WhatWeb:

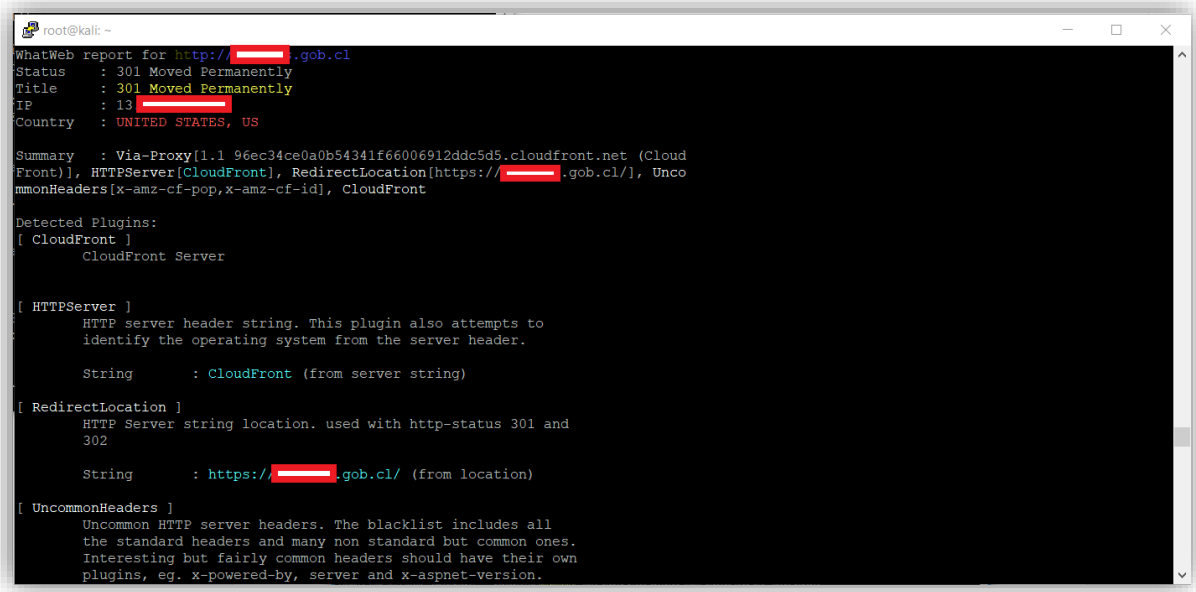
- Más de 1700 complementos
- Control del equilibrio entre velocidad / sigilo y confiabilidad
- Los complementos incluyen URL de ejemplo
- La optimización del rendimiento. Controle cuántos sitios web escanear al mismo tiempo.
- Múltiples formatos de registro: Breve (greppable), Verbose (legible por humanos), XML, JSON, MagicTree, RubyObject, MongoDB, SQL y ElasticSearch.
- Soporte de proxy que incluye TOR
- Encabezados HTTP personalizados
- Autenticación HTTP básica
- Control sobre la redirección de páginas web
- Rangos de IP estilo Nmap
- Coincidencia difusa
- Conciencia de certeza de resultado
- Complementos personalizados definidos en la línea de comando

Paso 4: Ponerlo en marcha para verificar nuestra infraestructura.

Como se ve un fragmento de reporte en una consola KALI después de la ejecución más simple:

```
whatweb -v -a 3 www.interior.gob.cl
```

Vista Parcial:



El resultado de este comando puede ser usado como evidencia de verificación para indicar que se han subsanado los problemas reportados por CSIRT.

Estudie las múltiples opciones que tiene el comando para obtener resultados específicos o redirigir la salida de este hacia otros formatos de archivo, para su inclusión en informes posteriores.

Algunos ejemplos de uso complementarios [reemplace los sitios de ejemplo por el suyo] son:

- Escanee example.com.
  whatweb example.com
- Escanee reddit.com slashdot.org con descripciones detalladas de los complementos.
  whatweb -v reddit.com slashdot.org
- Un escaneo agresivo de wired.com detecta la versión exacta de WordPress.
  whatweb -a 3 www.wired.com
- Escanee la red local rápidamente y elimine errores.
  whatweb --no-errors 192.168.0.0/24
- Escanee la red local en busca de sitios web https.
  whatweb --no-errors --url-prefix https: // 192.168.0.0/24
- Busque políticas de dominio cruzado en Alexa Top 1000.
  ./whatweb -i plugin-development / alexa-top-100.txt \
- --url-suffix /crossdomain.xml -p crossdomain_xml

En caso de cualquier inquietud no dudes en consultarnos a soc-csirt@interior.gob.cl.