ANALISIS DE PUERTOS Y VULNERABILIDADES

Jordi Masó Pla

Índice

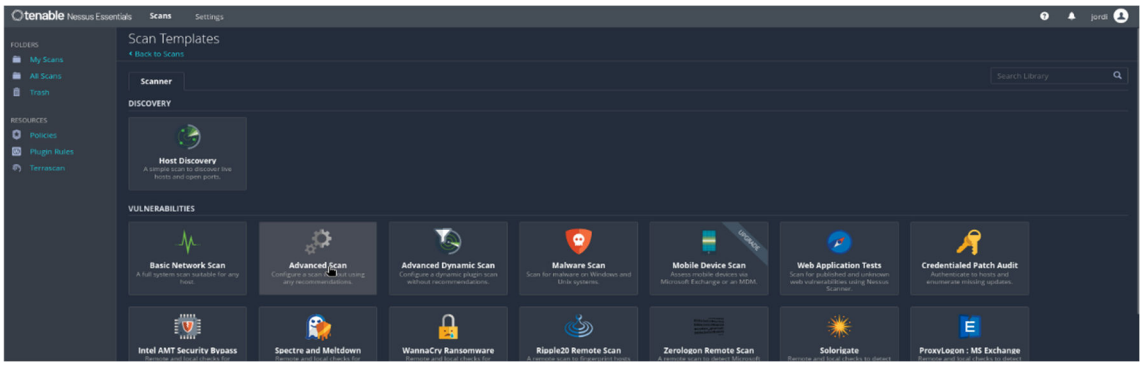
1. Creación de políticas en Nessus

En este ejercicio realizaremos un escaneo a la maquina Metasplotable 2 al puerto 80, el servidor web, las herramientas a utilizar serán las siguiente: Nessus, Nikto y Owasp-ZAP.

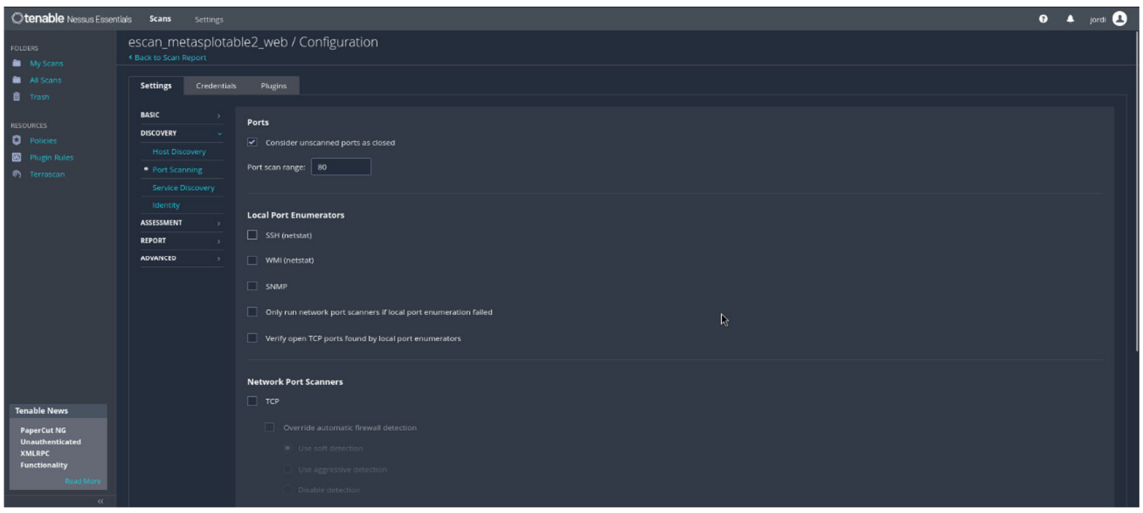
1.2 Crear política en Nessus

En Kali Linux ejecutamos Nessus para iniciar los servicios, acto seguido abrimos el navegador en el localhost con el puerto 8834 y accedemos a la plataforma Nessus.

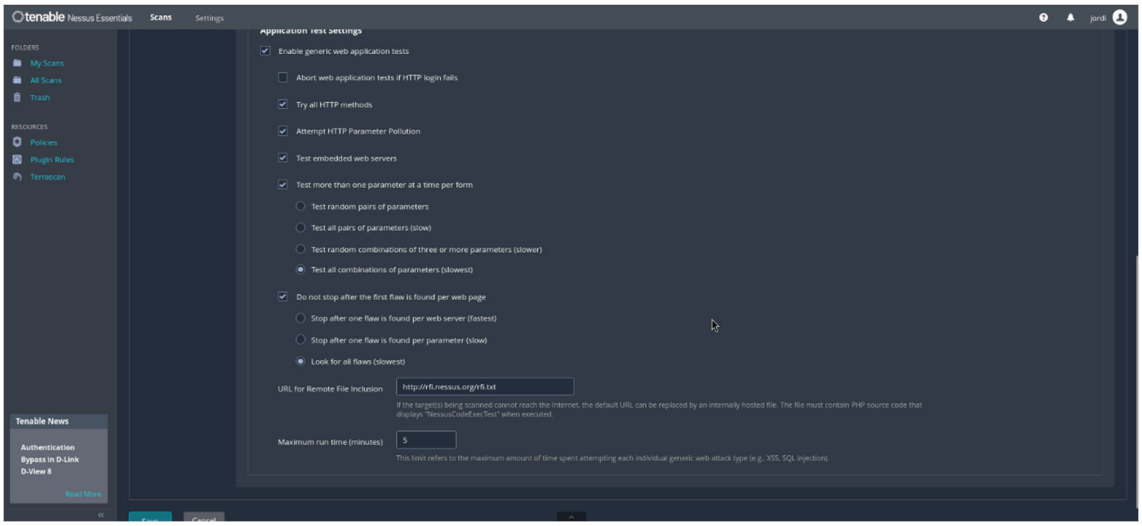
Vamos a crear un nuevo escaneo, clicamos en “Advanced Scan”, ahora podemos crear un nuevo escaneo con las preferencias a nuestro gusto.



Se abre una nueva ventana donde le ponemos un nombre, una pequeña descripción y la ip o rango de ips a escanear. En la siguiente ventana que es descubrimiento lo desmarcamos ya que solo queremos hace un escaneo en el puerto 80 y no hace falta buscar en toda la máquina.



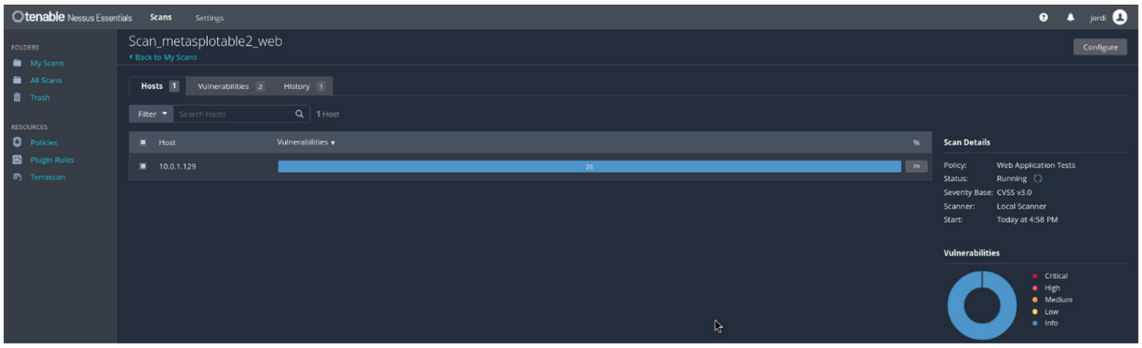
En la siguiente pestaña de evaluación, el apartado general seleccionamos que nos muestre los potenciales falsos positivos, en la siguientes definimos el ataque a fuerza bruta si queremos realizar o no, con un diccionario especifico. En la pestaña de aplicación web se selecciona el tipo de escaneo de las aplicaciones web que necesitamos, seleccionamos todos los escáneres de http, que combine todos los parámetros y que no se para al encontrar una coincidencia.



En las pestañan de Windows, Malware y Database no tocamos nada ya que el escáner solo es de la página web. En la pestaña informe seleccionamos la máxima información posible, que nos muestra y que tipo de depuración de información queremos que nos muestres. Terminada la configuración del escáner lo guardamos y podemos proceder a poner en marcha nuestro escáner.

1.3 Ejecutar la política en Nessus

En la parte izquierda de la pantalla tenemos una carpeta llamada “My Scans” en esa carpeta están todas las políticas creadas hasta el momento, escogemos la que terminamos de crear y la lanzamos.



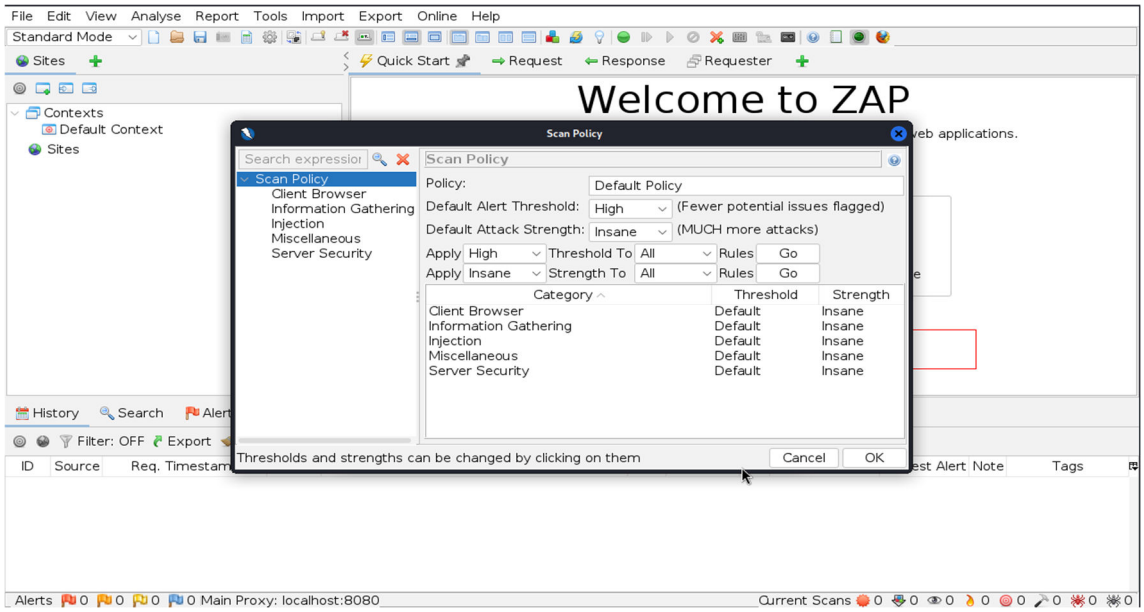
Este escáner de vulnerabilidades es más rápido ya que solo analiza las posibles fallas de la web de Metasplotable 2. El resultado que nos muestra en primera instancia sin entrar en detalle es de 15 posibles vulnerabilidades críticas, 25 de altas, 48 de medias, 2 de baja y 39 posibles recomendaciones a mejorar.

2 Ejecución de Nikto

Nikto es un escáner de vulnerabilidades de línea de comandos de software gratuito que escanea servidores web en busca de archivos/CGI peligrosos, software de servidor obsoleto y otros problemas.
Abrimos una CLI escribimos nikto -help nos aparece todas las opciones de parámetros y configuraciones posibles que podemos realizar con nikto. En este caso escribimos nikto con el parámetro -h y el host a escanear, en este momento nikto empieza a escaneara el objetivo y a reportar información.

3 Ejecutar OWASP-ZAP

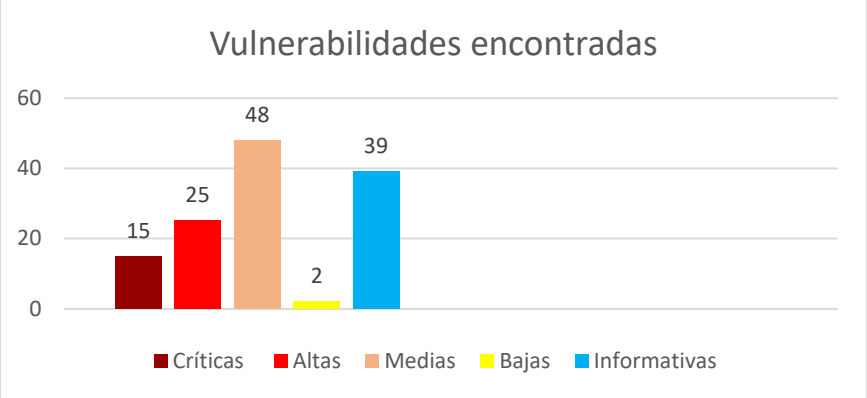
OWASP ZAP es un escáner de seguridad web de código abierto. Pretende ser utilizado como una aplicación de seguridad y como una herramienta profesional para pruebas de penetración.
Para realizar un escaneo nos dirigimos a la pestaña análisis dentro en política de escáner, se nos abrirá una ventana donde podemos modificar toda la política del escaneo que realizamos, en algunas políticas se puede seleccionar el nivel de fuerza a realizar contra el objetivo. Una vez configurado la política ponemos la dirección del objetivo y lanzamos el ataque. Esta herramienta se puede demorar mucho tiempo depende de la configuración de las políticas configuradas.



4 Vulnerabilidades encontradas

4.1 Vulnerabilidades encontradas con Nessus

Las vulnerabilidades encontradas con la herramienta Nessus son las siguientes: 15 vulnerabilidades posibles críticas, 25 consideradas altas, 48 medias, 2 de bajas y 39 recomendaciones posibles.



4.1.1 Vulnerabilidades Criticas

Enumeramos las principales vulnerabilidades mas graves que son las críticas, las cuales son lasque podemos llegar a tener acceso al sistema a través de la página web.

- Servicio Apache 2.2.x El servidor web remoto se ve afectado por una vulnerabilidad de desbordamiento de buffer.
- El servicio Apache 2.2.x tiene múltiples vulnerabilidades ataque de inyección, módulo “mod-proxy-ajp” devuelve el código de estado incorrecto, el “mod-isapi” intenta descargar el 'ISAPI.dll' cuando se encuentra con varios estados de error, existe una vulnerabilidad de bypass de autenticación, existe un defecto de referencia del puntero

NULL, Log4j incluye un SocketServer que acepta eventos de registro serializados y los de serializa sin verificar si los objetos están permitidos o no.
- La instalación PHP en el servidor web remoto contiene un fallo que podría permitir a un atacante remoto pasar argumentos de línea de comando.
- Apache Log4j obsoleto sin soporte
- El servidor web remoto alberga una aplicación PHP que se ve afectada por la vulnerabilidad de SQLi
- Apache httpd se encuentra entre 2.2.x. Por lo tanto, ya no es mantenido por su proveedor
- El host remoto contiene una versión no soportada de un lenguaje de scripting de aplicaciones web.
- Según su número de versión del sistema operativo Unix que se ejecuta en el host ya no es compatible

4.1.2 Vulnerabilidades Altas

Las vulnerabilidades altas son casi igual de peligrosos que las críticas, se pueden explotar causando graves problemas al host y comprometer la información que hay en él. Aquí enumeramos las principales en contradas por Nessus.

- La versión de TWiki que se ejecuta en el host remoto permite a un atacante manipular la entrada al parámetro 'rev' con el fin de ejecutar comandos de shell arbitrarios en el host
- Una inyección CRLF que permite ataques de división de la respuesta HTTP para los sitios que utilizan mod-userdir
- El servidor HTTP Apache se ve afectado por una vulnerabilidad de hombre en medio conocida como “httpoxy”
- La versión de Apache HTTP Server que se ejecuta en el host remoto se ve afectada por una vulnerabilidad de denegación de servicio
- La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por múltiples vulnerabilidades por ser una versión obsoleta
- El manejo fallido de error en el soporte de poliset Solaris podría llevar a una denegación de servicio
- Existe un defecto dentro del módulo de los "mod-headers" que permite a un atacante remoto inyectar encabezados arbitrarios
- La utilidad “apachectl” puede recibir un nombre de directorio de longitud cero
- El servidor web remoto alberga scripts CGI que no logran desinfectar adecuadamente
- El servidor web utiliza una versión de PHP que se ve afectada por múltiples vulnerabilidades
- Un error en el archivo “sapi/cgi/cgi-main.c” puede permitir a un atacante remoto obtener código fuente PHP del servidor web
- La versión de PHP que permite la ejecución de código
- El servidor web alberga una aplicación CGI que se ve afectada por múltiples vulnerabilidades
- Sistema operativo obsoleto sin soporte técnico

4.1.3 Vulnerabilidades Medias

Las vulnerabilidades medias son importantes, pero hay algunas que vienen dadas por las críticas y las altas, al solucionar algunas vulnerabilidades críticas y altas se soluciona también las medias

- Una aplicación PHP tiene vulnerabilidad de solicitud de demanda (XSRF) que existe en la página de configuración

- Una aplicación PHP que se ve afectada por una vulnerabilidad de Scripting cross-site
- Sistema operativo obsoleto sin soporte
- El servidor web aloja lo que puede ser un archivo de .bash-history de acceso público
- Una vulnerabilidad de denegación de servicio en mod.cache y mod.dav
- Apache 2.2.x se ve afectado por una vulnerabilidad de denegación de servicio
- El servidor web remoto se ve afectado por múltiples vulnerabilidades de cross-site scripting
- El servidor web revela información a través de encabezados HTTP
- Algunos directorios en el servidor web remoto son navegables
- El servidor web soporta los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidores web
- La versión de PHP que se ejecuta se ve afectada por una vulnerabilidad de inyección de encabezado de correo electrónico
- La aplicación web alberga archivos estáticos que pueden ser de naturaleza sensible
- La página de error por defecto enviada por el servidor web revela información que puede ayudar a un atacante
- Muchos tutoriales de instalación PHP instruyen al usuario a crear un archivo PHP que llame a la función PHP “phpinfo()” para propósitos de depuración
- La versión de PHP es potencialmente afectada por una vulnerabilidad de bypass de seguridad
- La configuración de PHP en el host remoto permite la divulgación de información sensible
- La versión instalada de TWiki permite a un atacante manipular la entrada al parámetro

4.1.4 Vulnerabilidades Bajas

Las vulnerabilidades bajas pueden ser por mala configuración o por falta de actualización de los servicios, estas vulnerabilidades no suelen llevar consecuencias tan graves como las demás escritas anteriormente, alguna de estas se describe a continuación.

- El atributo 'autocompleto' no está deshabilitado en los campos de contraseña
- El servidor web remoto podría transmitir credenciales en texto claro

4.1.5 Vulnerabilidades Informativas

Las vulnerabilidades informativas son aquellas que de mala configuración o de dejar los parámetros por defecto, como usuarios y contraseñas por defecto, habilitar más permisos de los necesarios a un servicio o usuario. En esta máquina se han encontrado una gran cantidad de estos defectos, que no son explotables directamente, pero mediante otros fallos si se pueden llegar a explotar.

4.2 Vulnerabilidades de Nikto

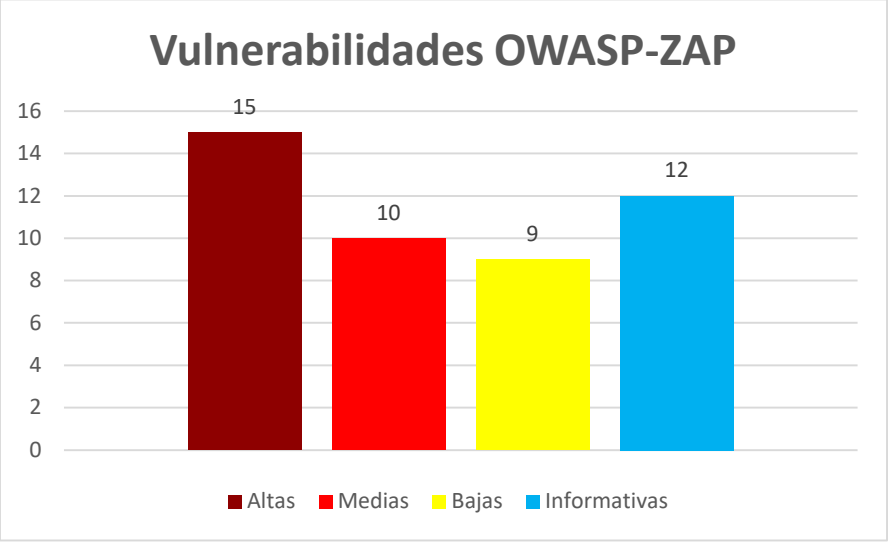
Descripción de las principales vulnerabilidades encontradas con Nikto, esta herramienta no cataloga las vulnerabilidades es su gravedad sino solo las enumera.

- Recuperación de x-impedor por cabecera: PHP/5.2.42.4-2ubuntu5.10
- La cabecera anti-clickjacking X-Frame-Options no está presente
- La cabecera X-Content-Type-Options no está ambientada. Esto podría permitir al agente de usuario renderizar el contenido del sitio de una manera diferente al tipo MIME

- La cabecera X-Content-Type-Options no está ambientada. Esto podría permitir al agente de usuario renderizar el contenido del sitio de una manera diferente al tipo MIME
- índex: Poco frecuentes cabeceras “tcn” encontrado, con contenido: lista
- Apache mod_negotiation está habilitado con MultiViews, lo que permite a los atacantes forzar fácilmente los nombres de los archivos
- Apache 2.2.8 parece estar desactualizado
- El servidor web devuelve una respuesta válida con métodos HTTP basura que pueden provocar falsos positivos
- El método HTTP TRACE está activo, lo que sugiere que el host es vulnerable a XST
- phpinfo.php: Se encontró la salida de la función phpinfo()
- Se encontró indexación de directorios
- El directorio /doc/ es navegable. Este puede ser /usr/doc
- PHP revela información potencialmente sensible a través de ciertas solicitudes HTTP que contienen cadenas QUERY específicas
- phpMyAdmin es para administrar bases de datos MySQL y debe protegerse o limitarse a hosts autorizados
- El servidor puede filtrar inodos a través de ETags
- phpMyAdmin es para administrar bases de datos MySQL y debe protegerse o limitarse a hosts autorizados
- Se encontró indexación de directorios
- Archivo encontrado /.wp-config.php. Este archivo contiene las credenciales

4.3 Vulnerabilidades OWASP-ZAP

La herramienta OWASP-ZAP si que reporta las vulnerabilidades por categoría de riegos. Ha detectado las siguientes vulnerabilidades: 15 vulnerabilidades altas, 10 de medias, 9 de baja y 12 vulnerabilidades informativas.



4.3.1 Vulnerabilidades Altas

- Cross-site Scripting (XSS) es una técnica de ataque que implica hacer eco proporcionada por el atacante código en la instancia del navegador de un usuario
- Los redirectores de URL no representan necesariamente un Vulnerabilidad de seguridad directa, pero los atacantes pueden abusar de ella al intentar manipular a las víctimas

mediante ingeniería social. haciéndoles creer que están navegando a un sitio distinto al verdadero destino
- La técnica de ataque Path Traversal permite a un atacante acceder a archivos, directorios y comandos que potencialmente residen fuera del directorio raíz del documento web. Un atacante puede manipular una URL de tal manera que el sitio web ejecute o revele el contenido de archivos arbitrarios en cualquier parte del servidor web
- Algunas versiones de PHP, cuando se configuran para ejecutarse mediante CGI, no manejan correctamente las cadenas de consulta que carecen de un carácter "=" sin escape, lo que permite la ejecución de código arbitrario
- La inclusión remota de archivos (RFI) es una técnica de ataque utilizada para explotar los mecanismos de "inclusión dinámica de archivos" en aplicaciones web
- Remote OS Command Injection. Técnica de ataque utilizada para la ejecución no autorizada de comandos del sistema operativo
- La inyección SQL puede ser posible
- Cuando la entrada del usuario se inserta en la plantilla en lugar de usarse como argumento en la representación, el motor de plantillas la evalúa. Dependiendo del motor de plantilla, puede conducir a la ejecución remota de código
- Algunas versiones de PHP, cuando se configuran para ejecutarse mediante CGI, no manejan correctamente las cadenas de consulta que carecen de un carácter "=" sin escape, lo que permite la divulgación del código fuente de PHP y la ejecución de código arbitrario

4.3.2 Vulnerabilidades Medias

- Los archivos htaccess se pueden utilizar para modificar la configuración del software del servidor web Apache para habilitar/deshabilitar funciones y características adicionales que el software del servidor web Apache tiene para ofrecer.
- No se encontraron tokens Anti-CSRF en un formulario de envío HTML
- Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial, como la ubicación del archivo que produjo la excepción no controlada. Esta información se puede utilizar para lanzar más ataques contra la aplicación web
- Encabezado de la política de seguridad de contenido (CSP) no está establecido. La política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la destrucción de sitios o la distribución de malware
- Es posible ver una lista del contenido del directorio
- Se identificó un archivo confidencial como accesible o disponible. Esto puede filtrar información administrativa, de configuración o de credenciales que una persona malintencionada puede aprovechar para atacar aún más el sistema
- La respuesta no incluye ni la Política de seguridad de contenido para proteger contra ataques de “ClickJacking”
- La biblioteca identificada jQuery, versión 1.3.2, es vulnerable
- La inyección mediante transformaciones XSL puede ser posible y permitir a un atacante leer información del sistema, leer y escribir archivos o ejecutar código arbitrario.

4.3.3 Vulnerabilidades Bajas

- Esta página contiene un mensaje de error/advertencia que puede revelar información confidencial

- Se ha configurado una cookie sin el indicador HttpOnly, lo que significa que se puede acceder a la cookie mediante JavaScript
- Se ha configurado una cookie sin el atributo SameSite, lo que significa que la cookie se puede enviar como resultado de una solicitud "entre sitios"
- La respuesta parecía contener mensajes de error comunes devueltos por plataformas como ASP.NET y servidores web como IIS y Apache
- El servidor web/de aplicaciones está filtrando información a través de uno o más encabezados de respuesta HTTP "X-Powered-By"
- La aplicación/servidor web reveló una marca de tiempo: Unix
- El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado en “nosniff”. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que potencialmente hace que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado

4.3.4 Vulnerabilidades informativas

- Parece que se han ubicado uno o más archivos que se pueden acceder
- Los archivos htaccess se pueden utilizar para modificar la configuración del software del servidor web Apache
- Una solicitud que originalmente se observó como POST también se aceptó como GET
- La solicitud parecía contener información confidencial filtrada en la URL
- La respuesta parece contener comentarios sospechosos que pueden ayudar a un atacante
- Se ha identificado que la respuesta proporcionada contiene un token de gestión de sesión
- Se encontró que ASP.NET Trace Viewer (trace.axd) estaba disponible. Este componente puede filtrar una cantidad significativa de información valiosa
- Esta verificación analiza la entrada proporcionada por el usuario en los parámetros de la cadena de consulta y los datos POST para identificar dónde las declaraciones de conjunto de caracteres de meta etiquetan o tipo de contenido pueden estar controladas por el usuario
- Esta verificación analiza la entrada proporcionada por el usuario en los parámetros de la cadena de consulta y los datos POST para identificar dónde se pueden controlar ciertos valores de atributos HTML

5 Explicación

En esta prueba emos utilizado tres herramientas para comprobar las vulnerabilidades de la maquina Mestasplotable 2 en el puerto 80 o que es los mismo el servicio web por defecto sin cifrado. Este servicio tiene múltiples vulnerabilidades, las principales son por programas obsoletos, malas configuraciones y el código fuente revela información confidencial.
La herramienta Nessus, es una herramienta muy funcional, con mucho potencial de análisis e interfaz gráfica, siempre y cuando las políticas estén bien diseñadas, sino puede mostrar información que no es relevante con la parte que nos interesa y hay que filtrar toda esa información, que nos das sin que sea interesante en ese momento. La interfaz es muy amigable no es complicado de utilizar. Proporciona unos informes muy completos y con muy buena explicación de cada falla que ha encontrado.

La herramienta Nikto es un programa muy potente con gran variedad de opciones de análisis y comprobación de robustez de la aplicación web que se analiza. La interfaz que utiliza es la CLI o línea de comandos, pero los informes se pueden extraer de múltiples formatos. La información que nos reporta no viene catalogada por su gravedad ni explotabilidad, sino más bien como una lista de posibles fallos encontrados, directos y fiables.
La herramienta OWASP-ZAP es una herramienta con interfaz gráfica, con un gran potencial de análisis y muchas comprobaciones de cada servicio y elemento que está analizando, según la política que se ha seleccionado el análisis puede ser bastante largo. Este programa clasifica las vulnerabilidades encontradas por categoría de gravedad. Los informes que proporciona son muy extensión mostrando cada prueba que ha realizado al host atacado.
Por último, una herramienta que para analizar un servicio web, para tener una pequeña idea de cómo está distribuida los ficheros, y si se pueden acceder mediante una url es Gobuster. Este programa de CLI con un diccionario nos va ha mostrar lo ficheros que hay, y los que se pueden acceder y los que no podemos acceder directamente o los que están ocultos.