



ANÁLISIS DE PUERTOS Y VULNERABILIDADES

**Presentado por:
Santiago Peñaranda Mejia**

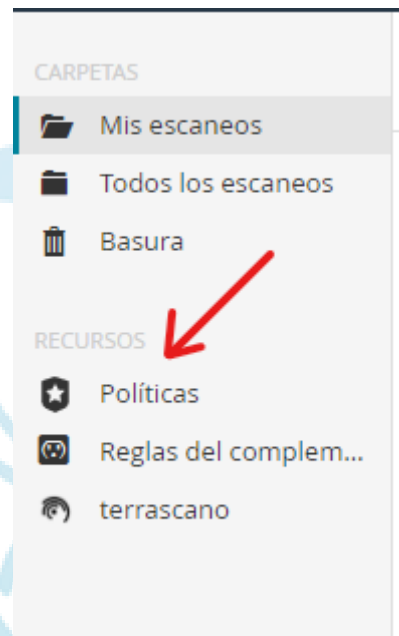
ÍNDICE:

- **Crear una política en Nessus**
- **Ejecutar política en Nessus**
- **Ejecutar Nikto**
- **Ejecutar OWASP-ZAP**
- **Vulnerabilidades encontradas**
- **Explicación del alumno**



Crear una política en Nessus

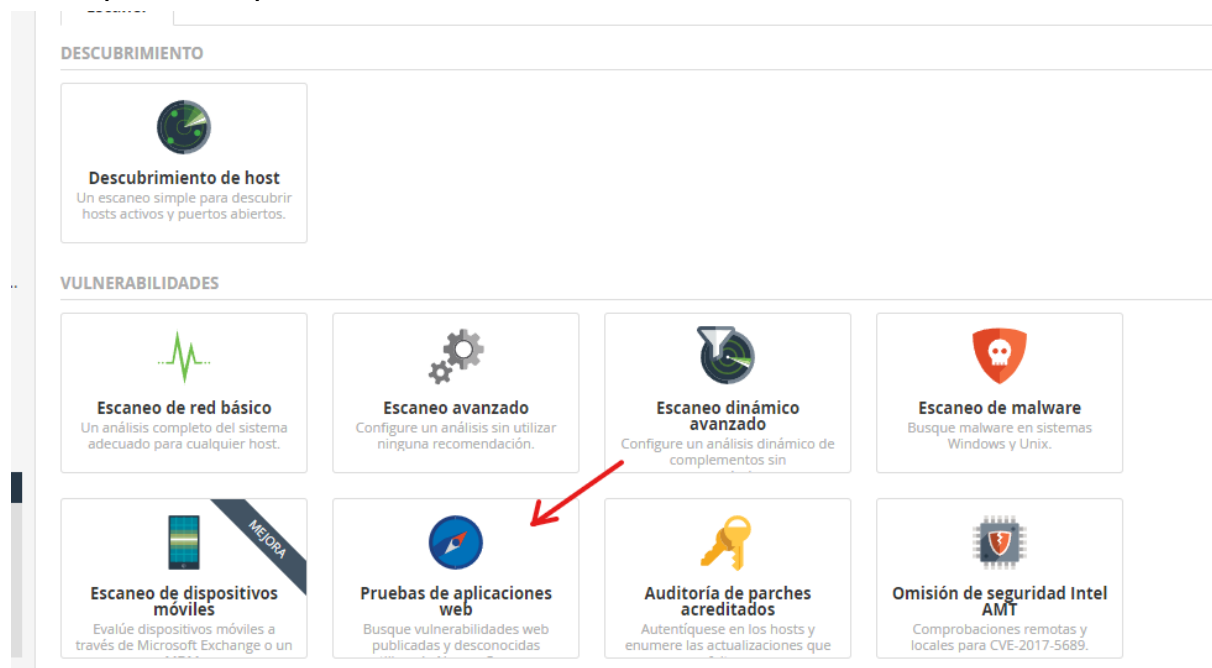
Primero que todo entramos al apartado de Políticas que está ubicado en la parte izquierda de la pantalla.



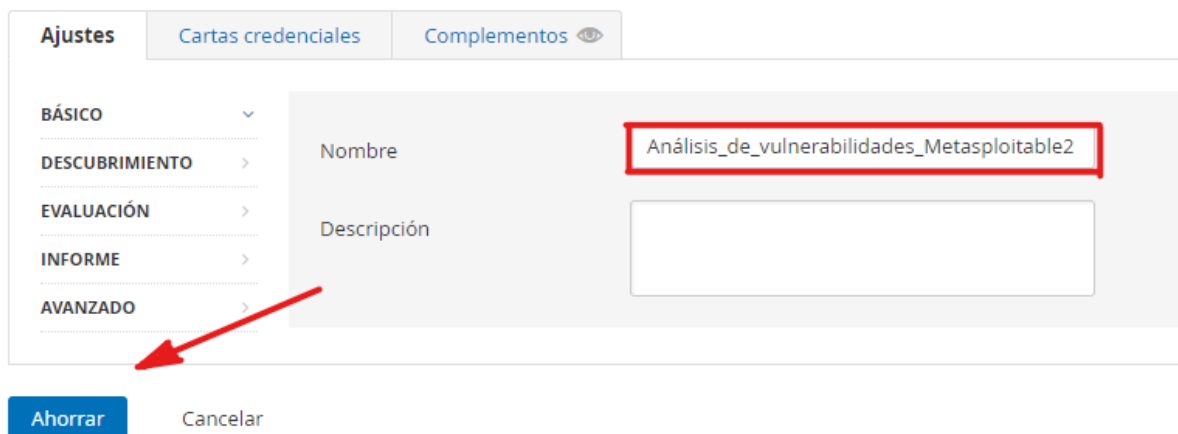
le damos a “nueva política” para iniciar a crear las plantillas personalizadas que definen qué acciones se realizan durante un análisis.



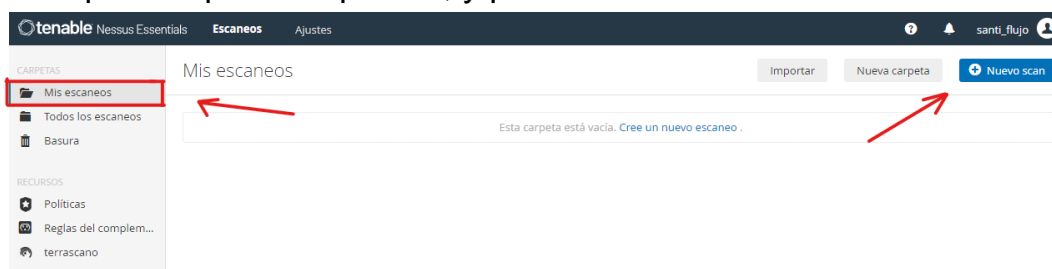
Ahora vamos a escoger nuestra respectiva plantilla que necesitemos, en este caso vamos a utilizar la de “análisis de vulnerabilidades para aplicaciones web” que es la que necesitamos.



Ahora que hemos seleccionado una política de escaneo, da un nombre adecuado y por ahora deja el resto de la configuración como está.

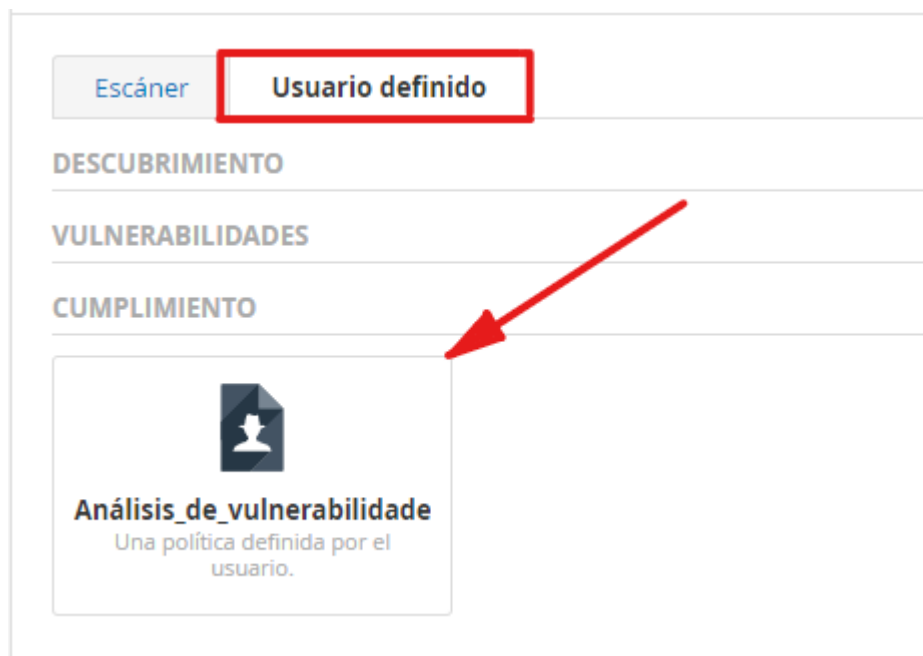


Después de guardar la política, ya estamos preparados para crear un nuevo escaneo bajo esta política. Ahora selecciona la etiqueta «Mis Escaneos» en la esquina superior izquierda, y pulsa el botón «Nuevo Escaneo».



Ejecutar política en Nessus

En la nueva página, ve a la pestaña «Definido por el usuario» y selecciona nuestra política personalizada que hemos creado



El nuevo análisis tiene el mismo nombre que nuestra política personalizada, como se muestra aquí:

A screenshot of the 'Ajustes' (Settings) page in Nessus. On the left, there is a sidebar with 'BÁSICO' expanded, showing 'General', 'Cronograma', and 'Notificaciones'. The main area contains a form with the following fields: 'Nombre' (pre-filled with 'Análisis_de_vulnerabilidades_Metasploitable2'), 'Descripción' (empty text box), 'Carpeta' (dropdown menu showing 'Mis escaneos'), and 'Objetivos' (text area with an example IP range and a 'REQUIRED' label). A large blue arrow points from the policy card in the previous image to this settings page.

Cambiaremos este nombre por «Mi Escaneo 1» para evitar cualquier confusión. También puedes dar una descripción opcional para esta Exploración, nosotros la hemos dejado en blanco. En el campo de texto correspondiente a la etiqueta 'Objetivos', pon los nombres de host o las direcciones IP del sistema objetivo que quieres escanear. Guarda el archivo para continuar.

Ajustes

BÁSICO

General

Cronograma

Notificaciones

Nombre

MI_Escaneo_1

Descripción

Carpeta

Mis escaneos

Objetivos

192.168.1.83

Cargar objetivos

Agregar archivo

Ahorrar

Cancelar

Ahora ha terminado toda la configuración. Ahora sólo nos queda lanzar el Escaneo para ver si funciona correctamente. En la nueva ventana, verás un botón de Play, haz clic en él para iniciar el escaneo

Mis escaneos

Importar

Nueva carpeta

Nuevo scan

Buscar escaneos

1 escaneo

<input type="checkbox"/>	Nombre	Cronograma	Último escaneado	Lanzamiento
<input type="checkbox"/>	MI_Escaneo_1	Bajo demanda	N / A	<div><div></div></div>

Una vez haya terminado el escaneo de vulnerabilidades haz clic en el nombre del escaneo

Mis escaneos

Importar

Nueva carpeta

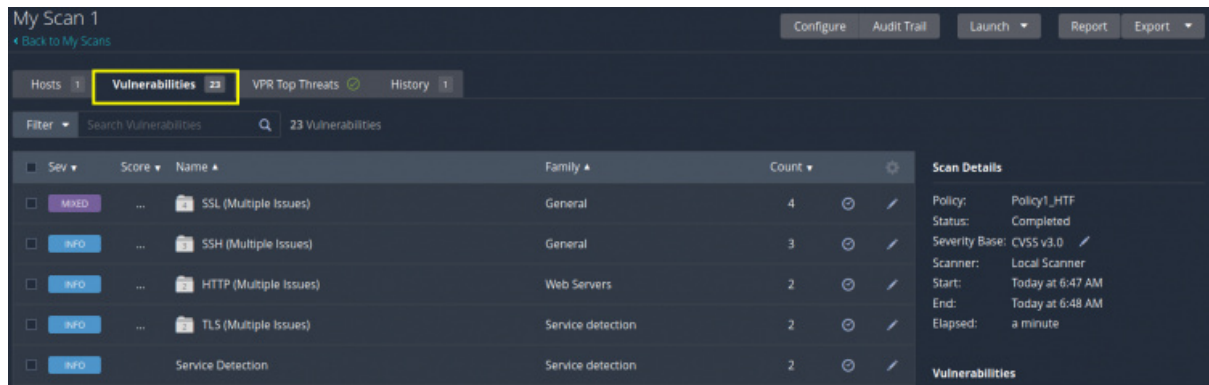
Nuevo scan

Buscar escaneos

1 escaneo

<input type="checkbox"/>	Nombre	Cronograma	Último escaneado	
<input type="checkbox"/>	MI_Escaneo_1	Bajo demanda	<div><div></div></div> Hoy a las 13:04	<div><div></div></div>

En la nueva ventana, haz clic en la pestaña «Vulnerabilidades» para ver el resumen del informe.



y ya está terminado..

Ejecutar Nikto

Ahora vamos a ejecutar Nikto, esta es una herramienta para el análisis de vulnerabilidades web. Este escaneo de vulnerabilidades va a intentar recopilar todos los fallos de seguridad que sean visibles e identificables dentro del servidor de aplicaciones web en cuestión.

```
(root@kali)-[/home/kali]
# nikto -host 192.168.1.83
- Nikto v2.5.0

+ Target IP: 192.168.1.83
+ Target Hostname: 192.168.1.83
+ Target Port: 80
+ Start Time: 2024-01-04 05:11:36 (GMT-5)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
```

En este análisis de vulnerabilidades hemos escaneado el host de la aplicación web del Metasploitable2, y encontramos ciertas vulnerabilidades que verás a continuación:

- The anti-clickjacking: Es un tipo de ataque en el que un atacante engaña a un usuario para que haga clic en algo diferente de lo que el usuario percibe, generalmente mediante la superposición de elementos engañosos en una página web.
- X-Content-Type-Options:

Y también nos muestra la versión del servidor y más.

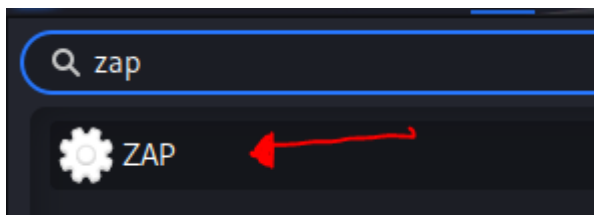
```

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive

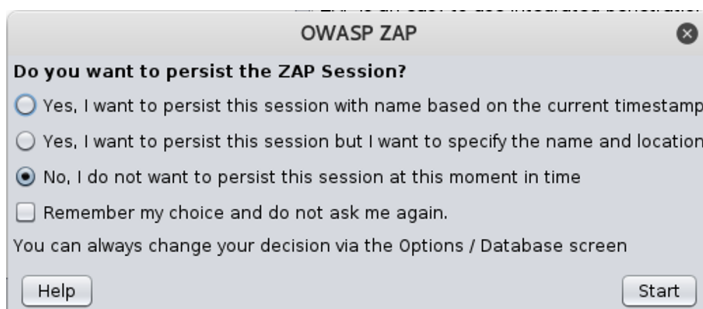
```

Ejecutar OWASP-ZAP

Vamos a buscar en la barra de búsqueda **OWASP-ZAP** o **ZAP** y le damos clic para entrar en la herramienta.



Al iniciar nos preguntará si queremos salvar la sesión, le damos a la que dice NO, cómo lo ves en la imagen.



En el apartado derecho tenemos para escribir la URL de nuestro objetivo. Tras eso, simplemente debemos pulsar el botón “Attack” para que comience el análisis de vulnerabilidades a la aplicación web.

Welcome to the OWASP

ZAP is an easy to use integrated penetration testir

Please be aware that you should only attack applic

To quickly test an application, enter its URL below a

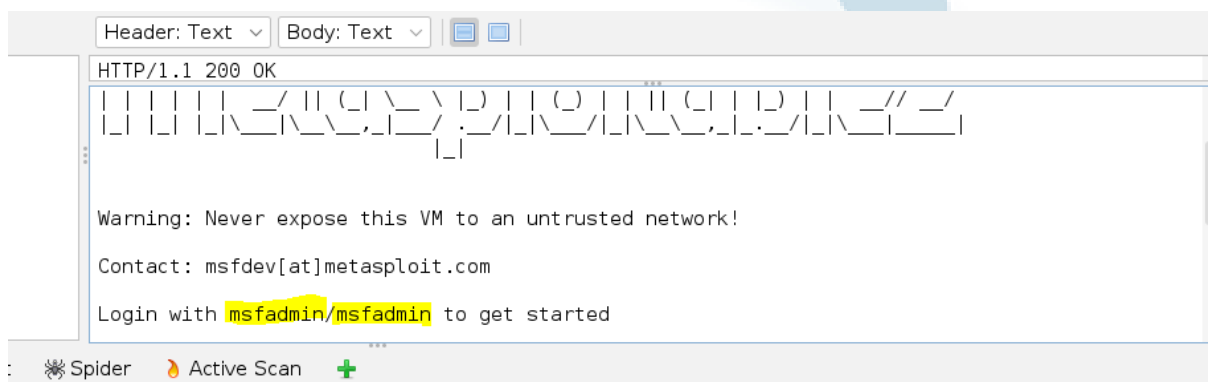
URL to attack:



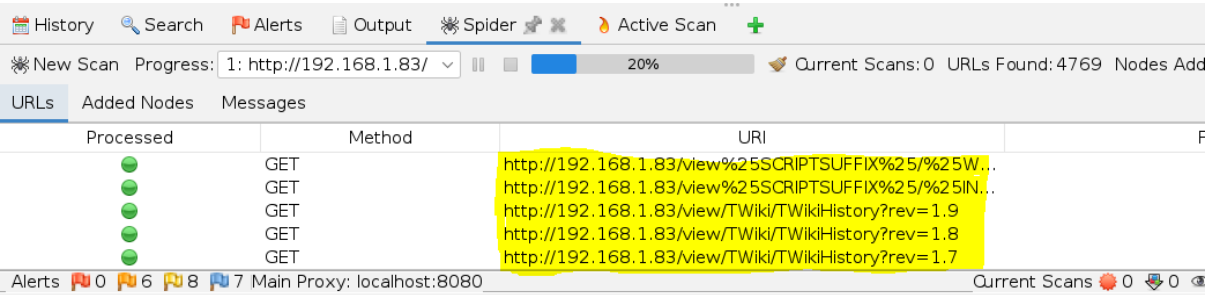
Una vez terminado el análisis, únicamente tenemos que observar con detalle cada una de las incidencias listadas en el apartado inferior. Cada tipo de incidencia va englobada en una categoría, la cual podemos desplegar para observar con detalle qué URL es vulnerable a esta y el detalle de lo que ha recabado OWASP-ZAP.

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
1	Pr...	1/4/24, 9:14:11 AM	GET	http://192.168.1.83/	200	OK	1...	891 bytes	Medium		
2,884	Pr...	1/4/24, 9:17:16 AM	GET	http://192.168.1.83/mutillidae/javascript/dd...	200	OK	1...	57,254 bytes	Medium	Script, Comment	
2,885	Pr...	1/4/24, 9:19:24 AM	GET	http://192.168.1.83/	200	OK	1...	891 bytes	Medium		

Aquí hemos encontrado algo MUY IMPORTANTE como es el usuario del dominio que hicimos el análisis que en este caso es Metasploitable2



Además, OWASP-ZAP cuenta con un motor para poder sacar los subdominios del *hostname* que le hayamos indicado, investigando cada uno de los *websites* que componen el dominio de nuestro objetivo.



The screenshot shows the OWASP ZAP web interface. At the top, there's a navigation bar with tabs: History, Search, Alerts, Output, Spider, and Active Scan. Below this, a progress bar indicates the scan is at 20% completion for the target '1: http://192.168.1.83/'. The 'Current Scans' section shows 0 scans, 4769 URLs found, and some nodes added. The 'URLs' tab is selected, displaying a table of discovered URLs. The table has columns for 'Processed' (green dots), 'Method' (GET), and 'URI'. The URIs listed are: 'http://192.168.1.83/view%25SCRIPTSUFFIX%25/%25W...', 'http://192.168.1.83/view%25SCRIPTSUFFIX%25/%25IN...', 'http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.9', 'http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.8', and 'http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.7'. The bottom status bar shows 0 alerts, 6 warnings, 8 errors, and 7 main proxy messages, with the main proxy set to localhost:8080.

Processed	Method	URI
●	GET	http://192.168.1.83/view%25SCRIPTSUFFIX%25/%25W...
●	GET	http://192.168.1.83/view%25SCRIPTSUFFIX%25/%25IN...
●	GET	http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.9
●	GET	http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.8
●	GET	http://192.168.1.83/view/TWiki/TWikiHistory?rev=1.7

Y pues ya está.

