4Geeks Academy

Reconocimiento de Pentesting en máquina vulnerable

Por: Juan Cervantes Simón

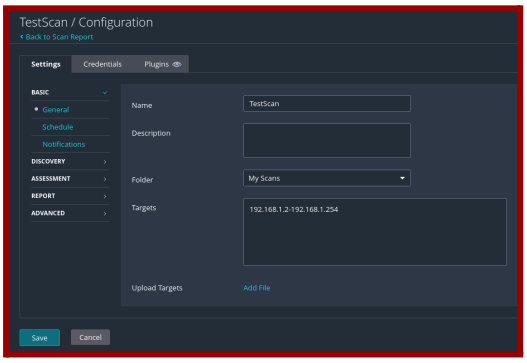
Índice

Resumen del Entorno

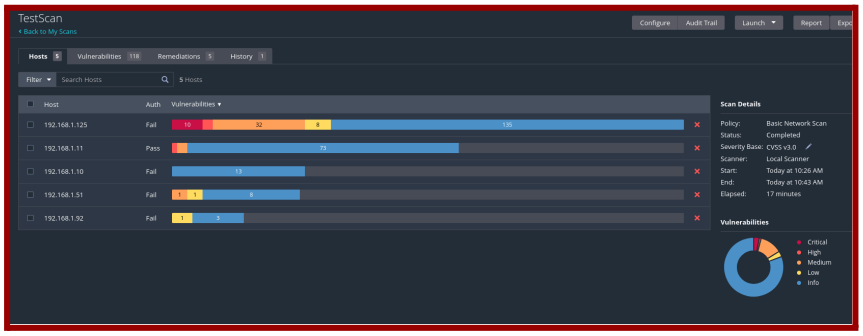
Para este caso se ha dispuesto a analizar la máquina ***Metasploitable2*** alojada en la red local, con objetivo de listar y analizar las vulnerabilidades que pueda tener, a raíz de los servicios expuestos en esta, así como la integridad general del entorno, cuentas, bases de datos y conexiones remotas entre otras, para cubrir todo ello en lo sucesivo, se va a hacer uso de la herramienta ***Tenable Nessus***, para lanzar escaneos básicos y avanzados para recabar información inicial.

Escaneo de Servicios

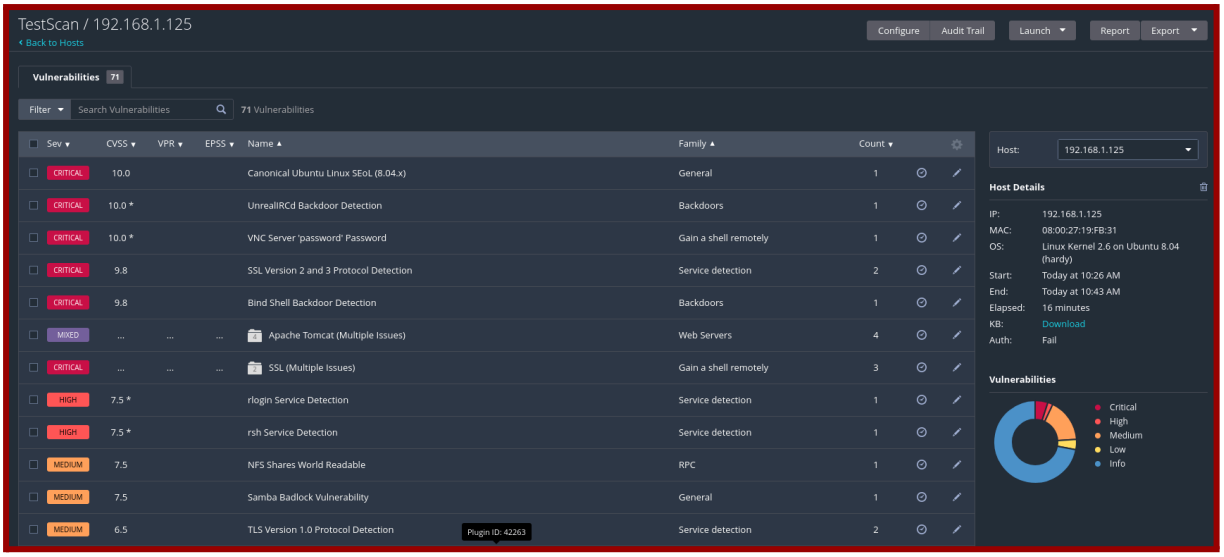
Primeramente, se va a lanzar un escaneo general a la red local, para identificar la máquina objetivo, para ello se va a configurar el scan de Nessus con todo el bloque de direcciones como objetivo:



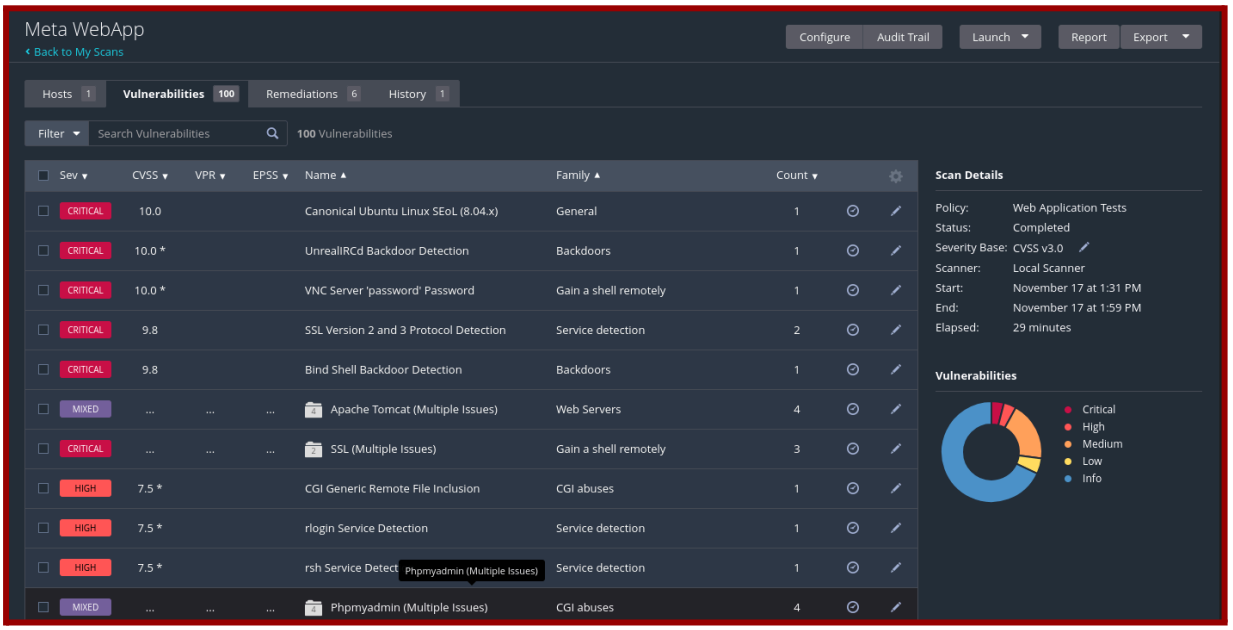
Habiendo hecho esto y pasados unos minutos, la herramienta habrá listado los host que ha encontrado en la red, así como las vulnerabilidades encontradas y su nivel de gravedad, se puede observar tanto en la pestaña de *hosts*, como en la gráfica que Nessus elabora, presente en la esquina inferior derecha de la ventana:



En este caso se sabe que la IP objetivo es la ***192.168.1.125***, puesto que las anteriores direcciones ya fueron identificadas con anterioridad en la red local, entrando a la entrada del host en concreto:



Se han podido identificar un número significativo de vulnerabilidades críticas en los servicios expuestos en la aplicación, para complementar el análisis también se va a realizar el escaneo de las aplicaciones web hosteadas en la IP objetivo, para ello se usará el ***web application scan***, de Nessus, apuntando a la máquina metasploitable:



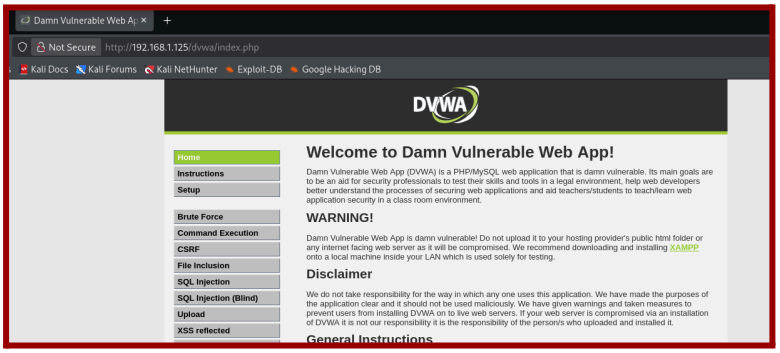
Gracias a estos dos análisis se han podido definir con precisión los servicios que la máquina objetivo.

Enumeración de servicios

Fruto de los scans se han encontrado servicios tales como **SSLv2** y **v3**, así como el servicio de conexión remota **VNC** y **SSH**, adicionalmente se ha observado que cuenta con la herramienta de archivos compartidos **Samba** y **FTP**.
Asimismo cuenta con **PHPMyAdmin**, **postgreSQL** y **MySQL** en el apartado de bases de datos, finalmente también cuenta con **Apache2** como manejador de aplicaciones web.

Vulnerabilidades detectadas y explotación

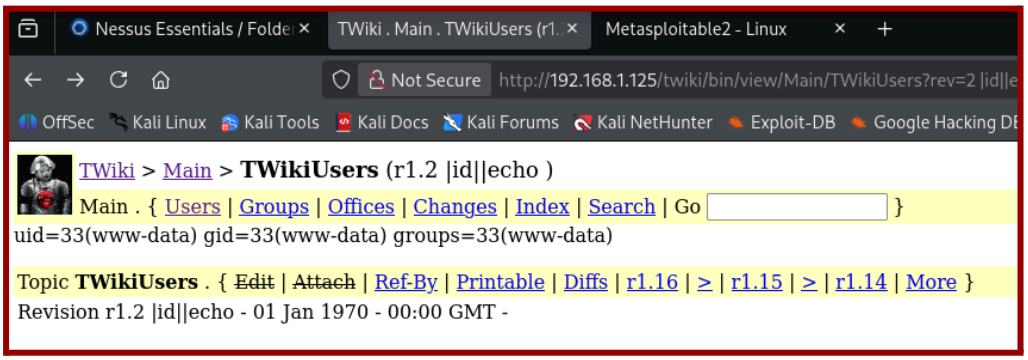
De cara a la explotación de vulnerabilidades se encuentra el uso de la contraseña ***password***, para el acceso a múltiples servicios web, entre ellos el acceso a DVWA, en el cual se entra con la combinación de ***admin/password***, lo cual permite acceder directamente al servicio como administrador:



Siguiendo con esta línea de acción, también se encuentra presente una vulnerabilidad que permite hacer el uso de la disponibilidad de los endpoints para poder obtener un id de usuario, en este caso, haciendo uso de la petición:

http://192.168.1.125/twiki/bin/view/Main/TWikiUsers?rev=2|id||echo|%20

Se ha podido obtener el usuario gestor de apache, ***www-data***, editando la entrada web, un usuario sin autenticar podría obtener la lista completa de usuarios, junto con toda la información referente subida por él, como por ejemplo los correos electrónicos personales.



Estrategias de Mitigación

Para la resolución de las vulnerabilidades descritas se opta, principalmente, por el uso de contraseñas más seguras, así como una actualización de los servicios expuestos.

Adicionalmente, es necesario controlar el nivel de acceso por web que tienen los usuarios externos, de esa forma se podrían evitar las ejecuciones de comandos de forma arbitraria como ha pasado con la segunda vulnerabilidad mencionada, de la misma forma se puede evitar la aparición de futuras vulnerabilidades que puedan resultar en un remote shell o en un XSS, que pueda filtrar muchos más datos y, en definitiva, ser mucho más dañino para el usuario.

Conclusión

Las vulnerabilidades encontradas en la máquina objetivo representan un riesgo serio para la integridad de los datos almacenados en ella, por lo que se sugiere emprender medidas de securización y monitorización tan pronto como sea posible, con objetivo de proteger los datos que se almacenan en ella y, por consiguiente, a los usuarios que la usan.