Auditoría de Active Directory

HERRAMIENTAS GRATUITAS

NESSUS + Docker

Henrique Alves

Contenido

INTRODUCCION

En el mundo actual, la seguridad informática es un pilar fundamental para garantizar la integridad, confidencialidad y disponibilidad de los sistemas de información. Active Directory (AD) es una pieza clave en la infraestructura de muchas organizaciones, y su correcta configuración y auditoría son esenciales para prevenir vulnerabilidades y posibles ataques.

Este informe presenta una práctica diseñada con fines de aprendizaje y mejora en la verificación de la seguridad en un entorno de red. A través del uso de NESSUS, una potente herramienta de análisis de vulnerabilidades, y su implementación dentro de un contenedor Docker, se facilita un enfoque flexible y escalable para auditar y evaluar la seguridad de Active Directory.

El propósito de esta práctica es fomentar una estructura ética en la seguridad informática, proporcionando conocimientos y herramientas para fortalecer la protección de los sistemas. Con este enfoque, buscamos capacitar a profesionales y entusiastas en la identificación de riesgos y en la aplicación de buenas prácticas de ciberseguridad.

Comprendiendo la Estructura de la Red Antes de la Auditoría

Antes de realizar esta práctica de auditoría, es fundamental comprender la arquitectura de la red en la que se llevará a cabo el análisis. Tener un conocimiento claro de la infraestructura permitirá identificar posibles vulnerabilidades y aplicar las mejores estrategias para evaluar la seguridad del entorno.

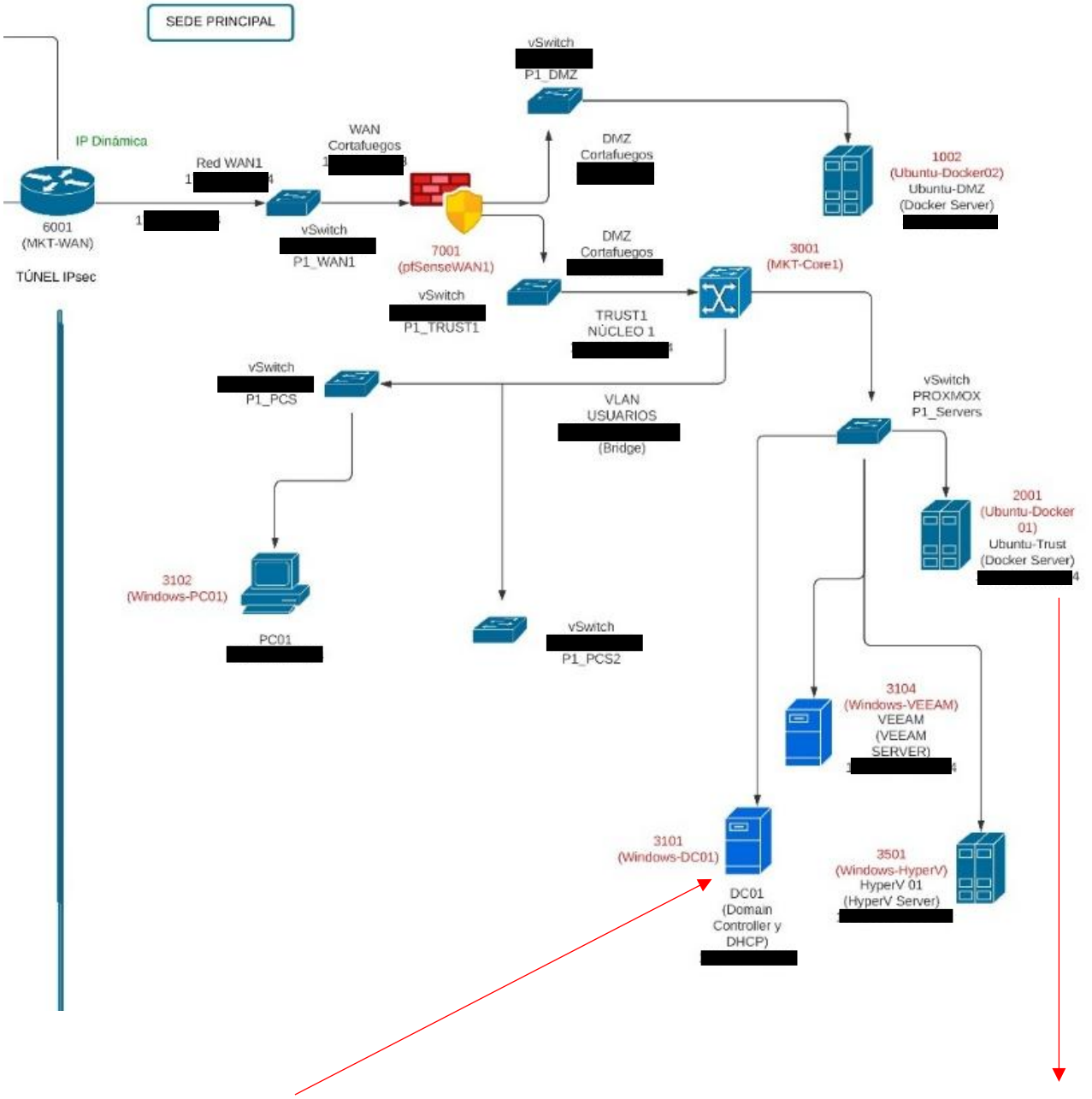
En este caso, se ha utilizado un **servidor Windows con Active Directory** dentro de una **zona de confianza (Trust Zone)**. Active Directory es un componente crítico en la gestión de identidades y accesos dentro de una organización, y su correcta configuración es esencial para evitar ataques como la escalación de privilegios o el movimiento lateral dentro de la red.

Además, la red cuenta con una **zona desmilitarizada (DMZ)**, una segmentación de seguridad diseñada para alojar servicios accesibles desde el exterior, como servidores web o de correo. La presencia de una DMZ permite simular escenarios en los que un atacante podría intentar explotar vulnerabilidades en los servidores expuestos y moverse lateralmente hacia la red interna protegida.

Con esta infraestructura en mente, la auditoría se llevará a cabo utilizando **NESSUS en un contenedor Docker**, lo que permitirá evaluar la seguridad tanto del Active Directory como de otros activos dentro de la red. A través de esta práctica, se analizarán configuraciones inseguras, accesos no autorizados y posibles brechas de seguridad, contribuyendo a fortalecer la protección del entorno. Así mismo, algunos equipos/servidores tendrán versiones con vulnerabilidades.

A seguir, les adjunto mi ejemplo práctico para esta auditoria:

Aunque en mi caso este utilizando esta red, puedes usar una más pequeña que puedes montar en VirtualBox/VMware.



SERVIDOR QUE ACTUA COMO CONTROLADOR DE DOMINIO QUE UTILIZAREMOS

SERVIDOR QUE INSTALAREMOS NESSUS

Auditoría con NESSUS

Instalación de NESSUS

Consultar la información de los pasos para realizar la instalación de NESSUS en los siguientes enlaces:

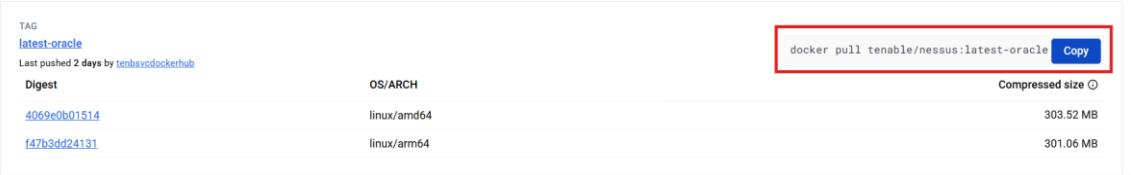
https://medium.com/@deefernando/how-to-deploy-nessus-scanner-as-adocker-container-4a1689615917 (Pasos para instalar Nessus)

https://hub.docker.com/r/tenable/nessus/tags (Las versiones de Nessus)

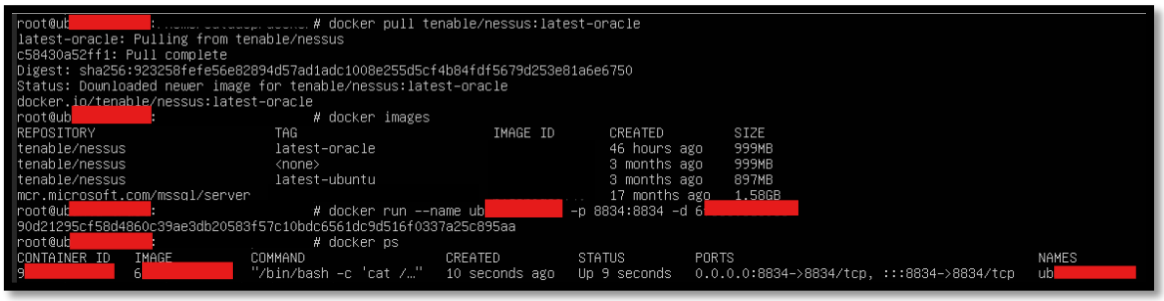
Por si queréis seguir mis pasos para instalarlo los dejo a seguir:

Para realizar el despliegue del contenedor con Nessus. Deberéis tener presente que estamos trabajando en una máquina Ubuntu y que queremos desplegar la última versión de Nessus disponible ("latest").

Usa este comando en la terminal para instalarlo:

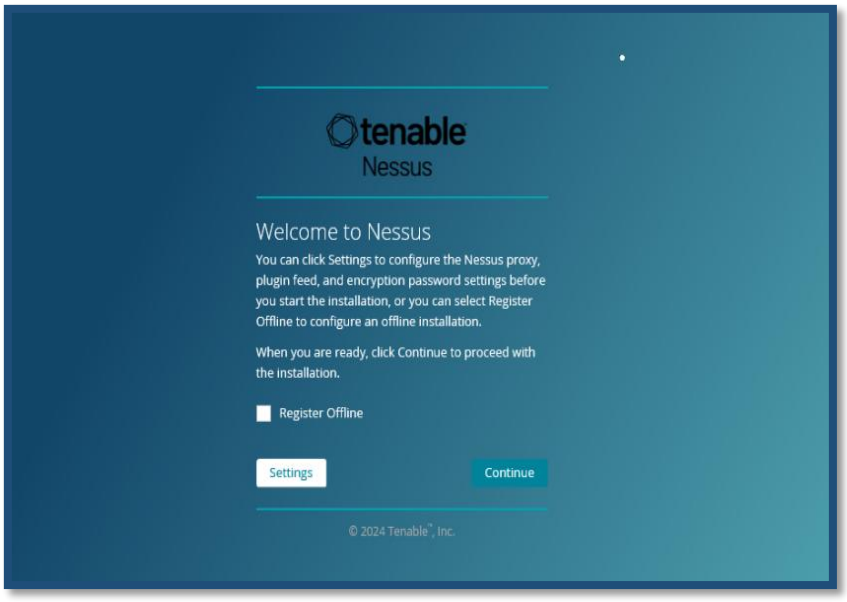


En la siguiente captura están los comandos utilizados para la instalación de NESSUS en el contenedor Docker:

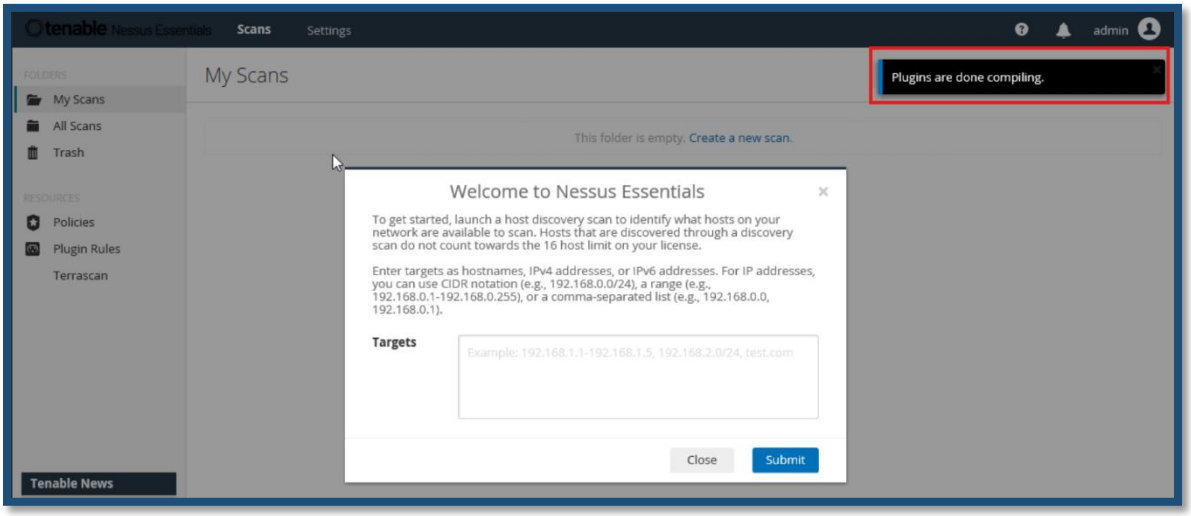


En un equipo que tiene acceso a la misma red del equipo que habéis instalado NESSUS, entrad a la URL https://"LA IP DEL EQUIPO QUE TIENE INSTALADO NESSUS":8834

Os saldrá una alerta de que no es seguro, pero le daréis para entrar en la página, y veréis lo siguiente:



Posteriormente de seguir los pasos que nos indica nos saldrá una ventana similar:

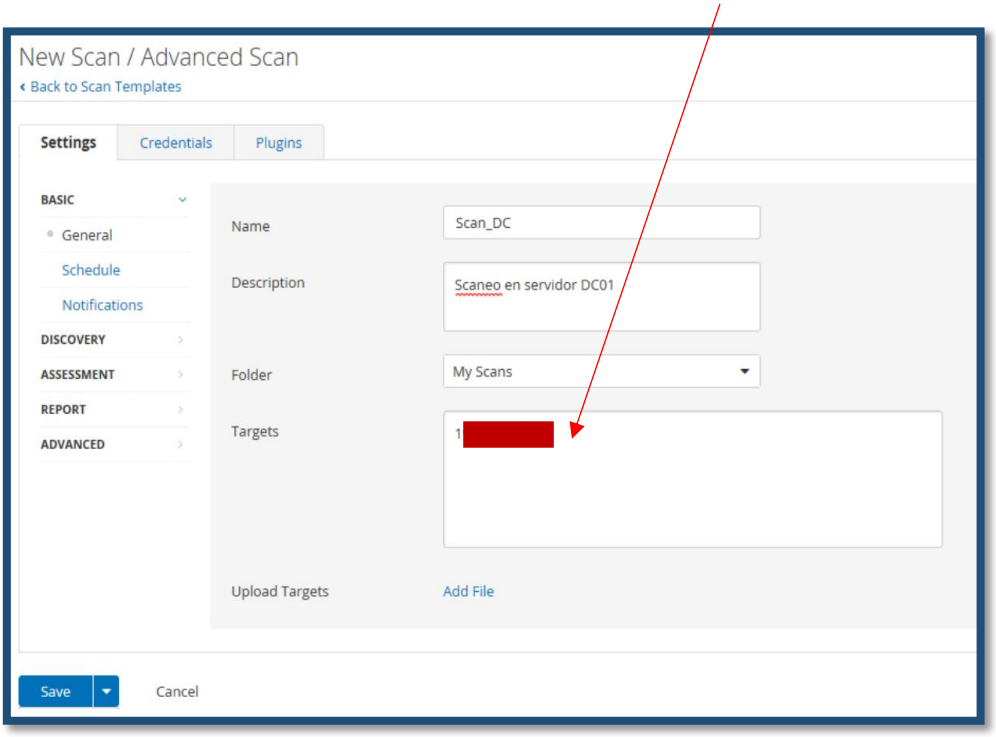


Realizar un escaneado del controlador de dominio

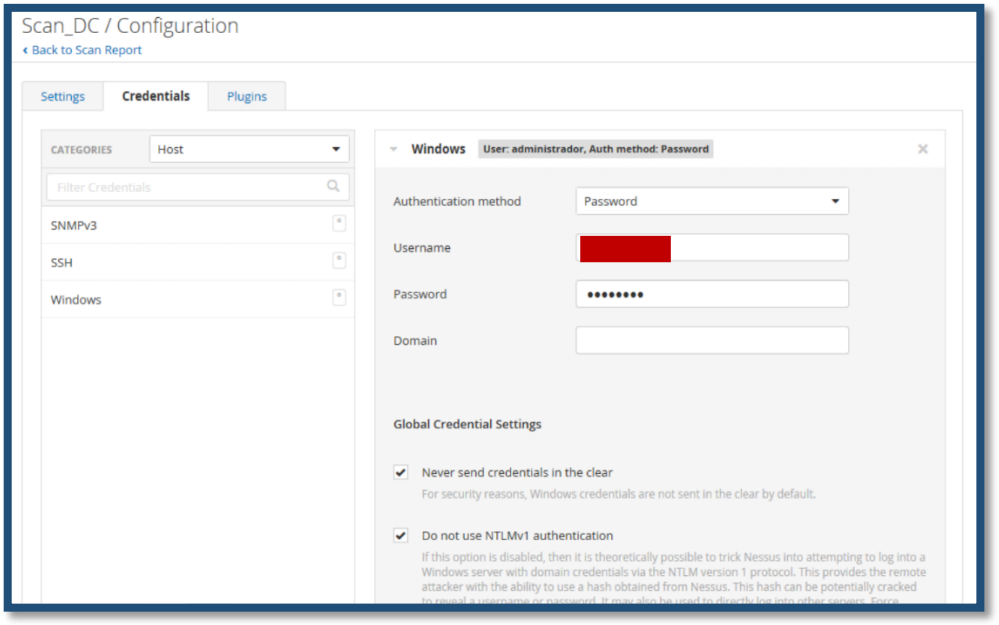
Hacer un nuevo escaneo del tipo “Advanced Scan”

Para ello, iremos en la opción “***Create a new scan***”.

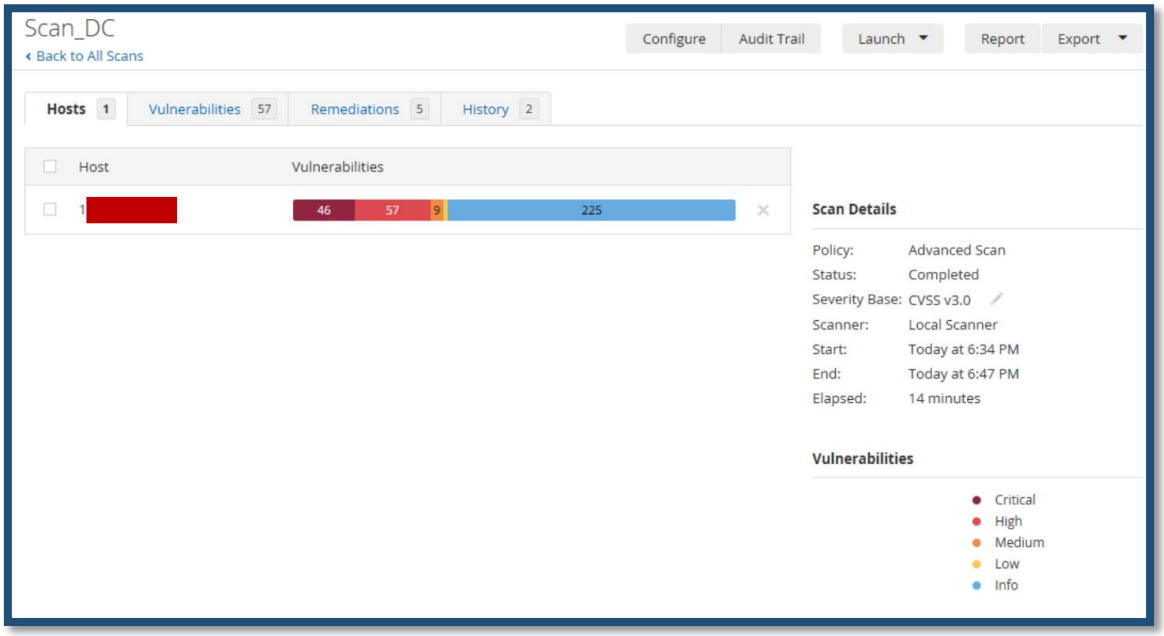
Realizaremos un escaneo en el equipo que instalamos NESSUS, que en mi caso es un servidor de controlador de dominio en el cual introduciremos su dirección IP.



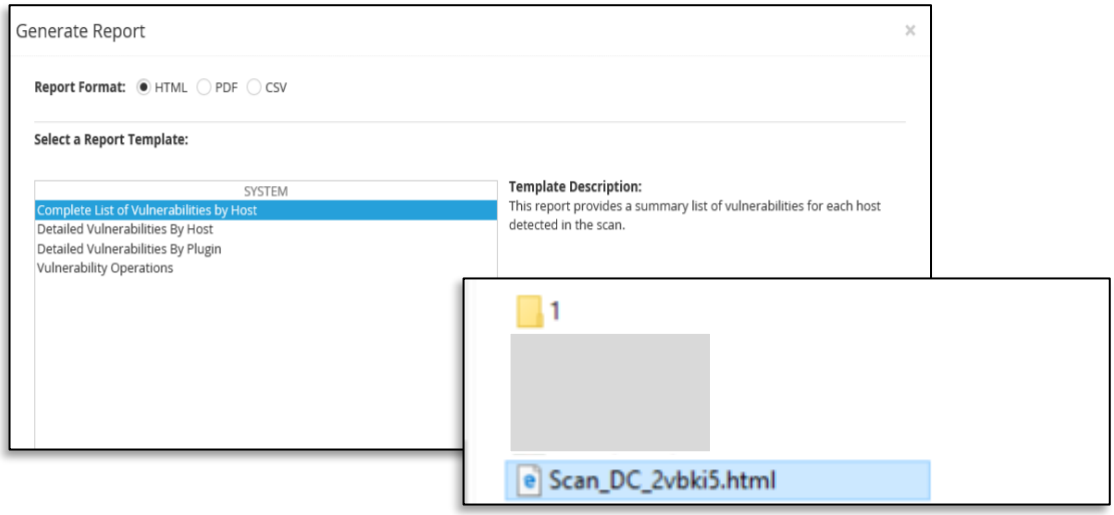
Y procedemos a introducir las credenciales de nuestro usuario “administrador” del equipo que se instaló NESSUS y confirmamos.



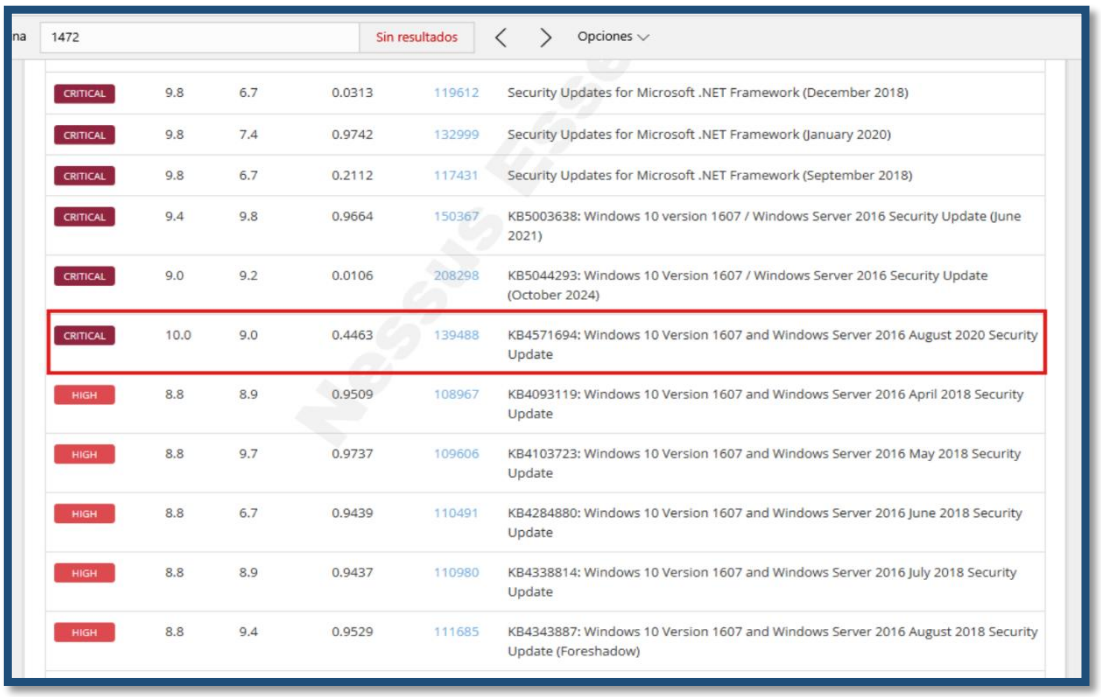
Tras realizar el escaneo procederemos a ver información importante como las siguientes en mi caso:



Desde la pestaña de "Report" en la parte superior derecha descargamos en HTML el resumen del escaneo:



Como podemos ver, con la ayuda de “Nessus”, la gravísima vulnerabilidad conocida como “Zerologon” (CVE-2020-1472) que afectó al Directorio Activo de Microsoft desde Agosto de 2020 hasta prácticamente Marzo de 2021, vulnerabilidad que obtuvo la terrible puntuación de 10 (la máxima) en los índices CVSS v3.0 y que permitía, usando el “Netlogon Remote Protocol (MS-NRPC)”.



A través del siguiente enlace podemos acceder a la vulnerabilidad nombrada anteriormente:

https://www.tenable.com/plugins/nessus/139488

“Zerologon” (CVE-2020-1472): https://www.tenable.com/cve/CVE-2020-1472

La vulnerabilidad CVE-2020-1472, también conocida como Zerologon, es una falla crítica de elevación de privilegios en el protocolo Netlogon de Windows. Permite que un atacante no autenticado se conecte a un controlador de dominio y obtenga acceso de administrador de dominio mediante el uso de un canal seguro Netlogon vulnerable. Al aprovechar esta vulnerabilidad, un atacante podría ejecutar una aplicación especialmente diseñada en un dispositivo de la red para comprometer el sistema.

La vulnerabilidad afecta cómo Netlogon maneja las conexiones de canales seguros y fue abordada por Microsoft a través de una actualización en dos fases, con la implementación final de las medidas de seguridad prevista para 2021. Esta vulnerabilidad ha sido una de las más explotadas por actores de amenazas, debido a su gravedad y facilidad de explotación.