

Auditoría de Active Directory

HERRAMIENTAS GRATUITAS

NESSUS + Docker



tenable x
network security



Microsoft
Active Directory

Henrique Alves

Contenido

INTRODUCCION	3
Comprendiendo la Estructura de la Red Antes de la Auditoría	4
Auditoría con Nessus	6
Instalación de Nessus.....	6
Realizar un escaneo del controlador de dominio	8
Hacer un nuevo escaneo del tipo “Advanced Scan”	8

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.

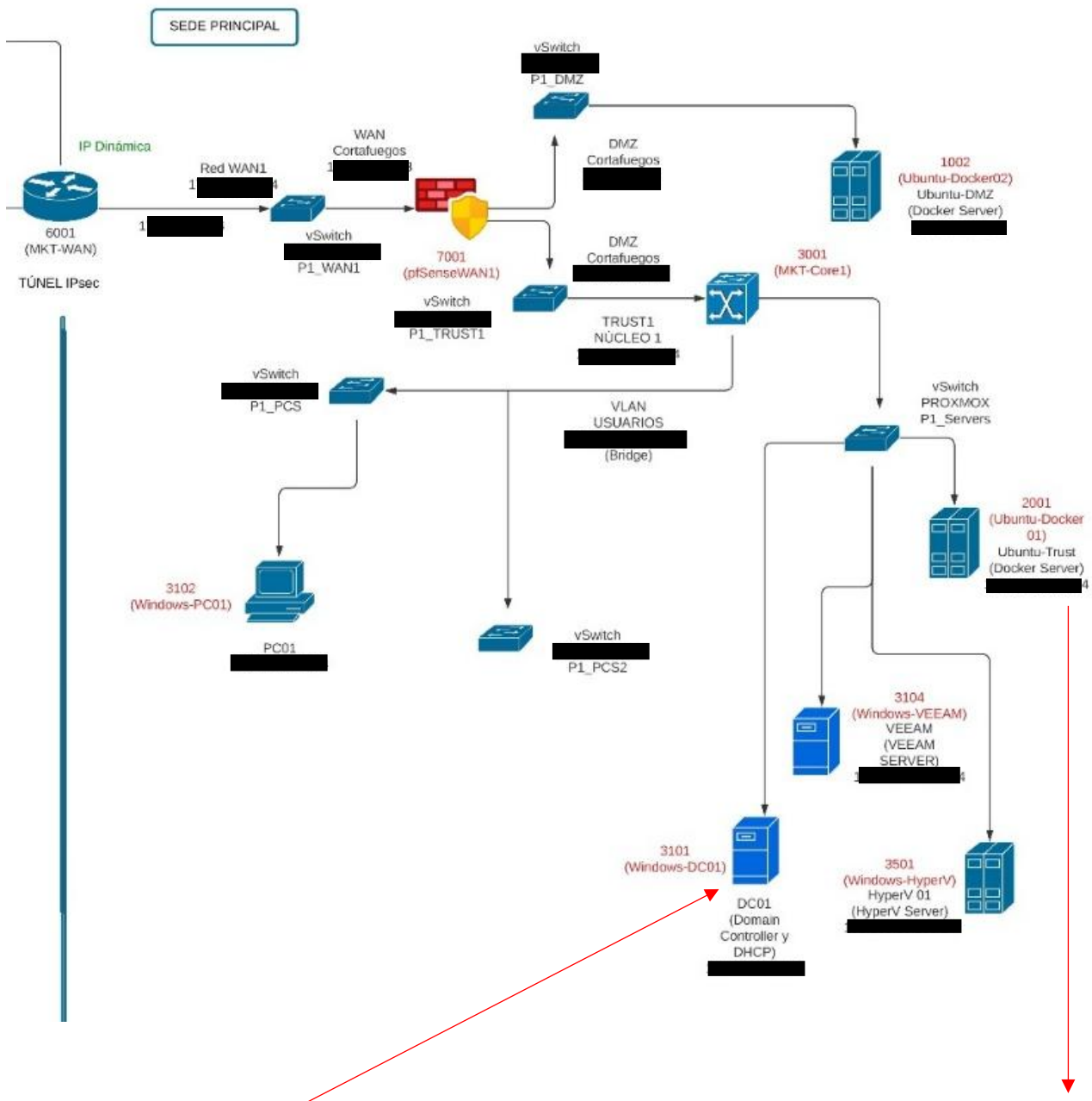
En este caso, se ha utilizado un **servidor Windows con Active Directory** dentro de una **zona de confianza (Trust Zone)**. Active Directory es un componente crítico en la gestión de identidades y accesos dentro de una organización, y su correcta configuración es esencial para evitar ataques como la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

TAG		
latest-oracle		
Last pushed 2 days by tenable/dockerhub		
Digest	OS/ARCH	Compressed size
4069e0b01514	linux/amd64	303.52 MB
f47b3dd24131	linux/arm64	301.06 MB

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

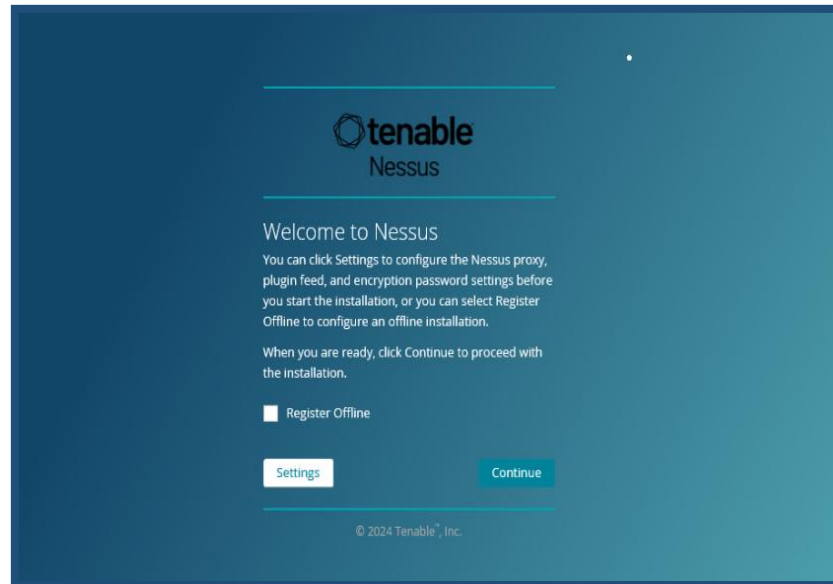
```

root@ub:~# docker pull tenable/nessus:latest-oracle
latest-oracle: Pulling from tenable/nessus
c58430a52ff1: Pull complete
Digest: sha256:923258fefe56e82894d57ad1adc1008e255d5cf4b04fdf5679d253e81a6e6750
Status: Downloaded newer image for tenable/nessus:latest-oracle
docker.io/tenable/nessus:latest-oracle
root@ub:~# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
tenable/nessus      latest-oracle       c58430a52ff1       46 hours ago       999MB
tenable/nessus      <none>              <none>              3 months ago       999MB
tenable/nessus      latest-ubuntu       3 months ago       897MB
mcr.microsoft.com/mssql/server 17 months ago     1.58GB
root@ub:~# docker run --name ub -p 8834:8834 -d 6
90d21295cf58d4860c39ae3db20583f57c10bdc6561dc9d516f0337a25c895aa
root@ub:~# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED             STATUS             PORTS              NAMES
90d21295cf58d4860c39ae3db20583f57c10bdc6561dc9d516f0337a25c895aa 6 "/bin/bash -c 'cat /..." 10 seconds ago     Up 9 seconds       0.0.0.0:8834->8834/tcp, :::8834->8834/tcp  ub

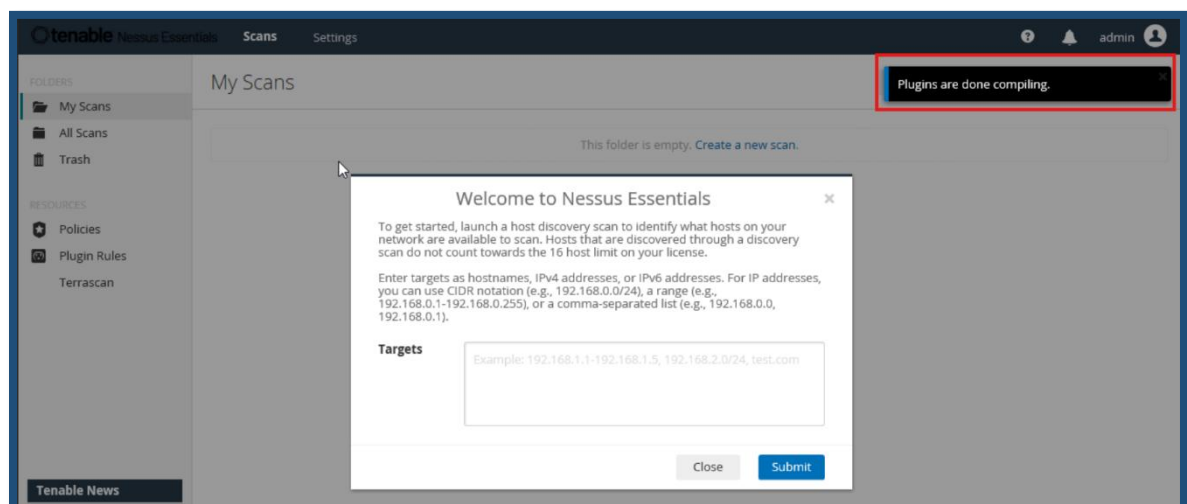
```

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](https://\)

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



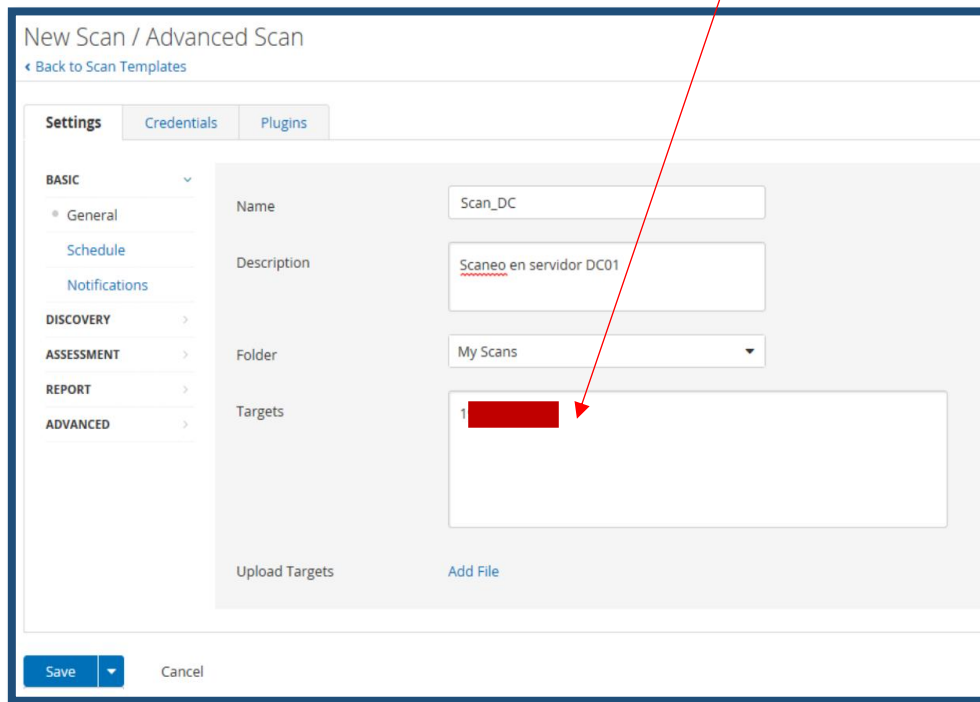
Posteriormente de seguir los pasos que nos indica nos saldrá una ventana similar:



Realizar un escaneo 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.



New Scan / Advanced Scan

[Back to Scan Templates](#)

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Scan_DC

Description: Escaneo en servidor DC01

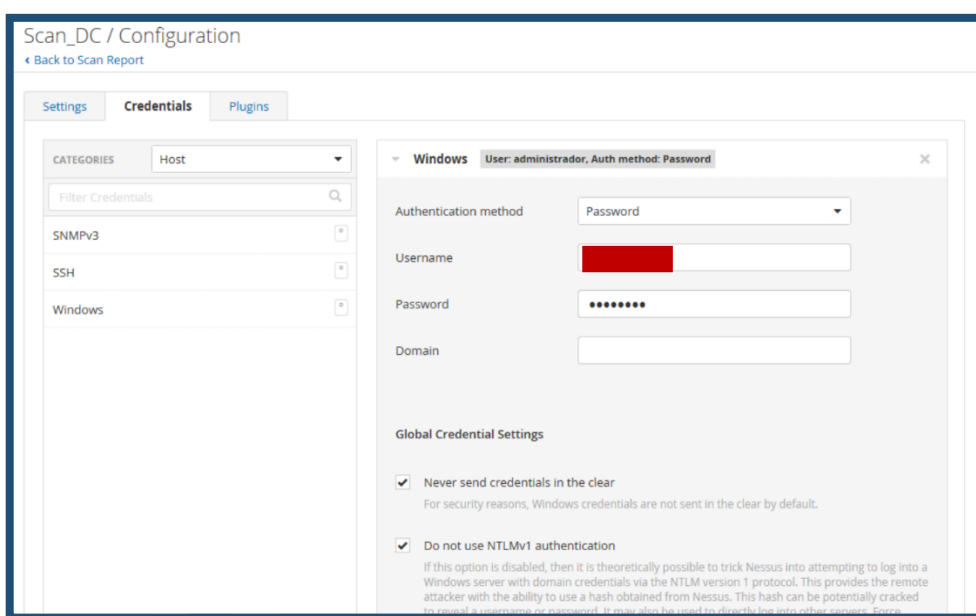
Folder: My Scans

Targets: 1 [Redacted IP]

Upload Targets Add File

Save Cancel

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



Scan_DC / Configuration

[Back to Scan Report](#)

Settings Credentials Plugins

CATEGORIES: Host

Filter Credentials

SNMPv3

SSH

Windows

Windows User: administrador, Auth method: Password

Authentication method: Password

Username: [Redacted]

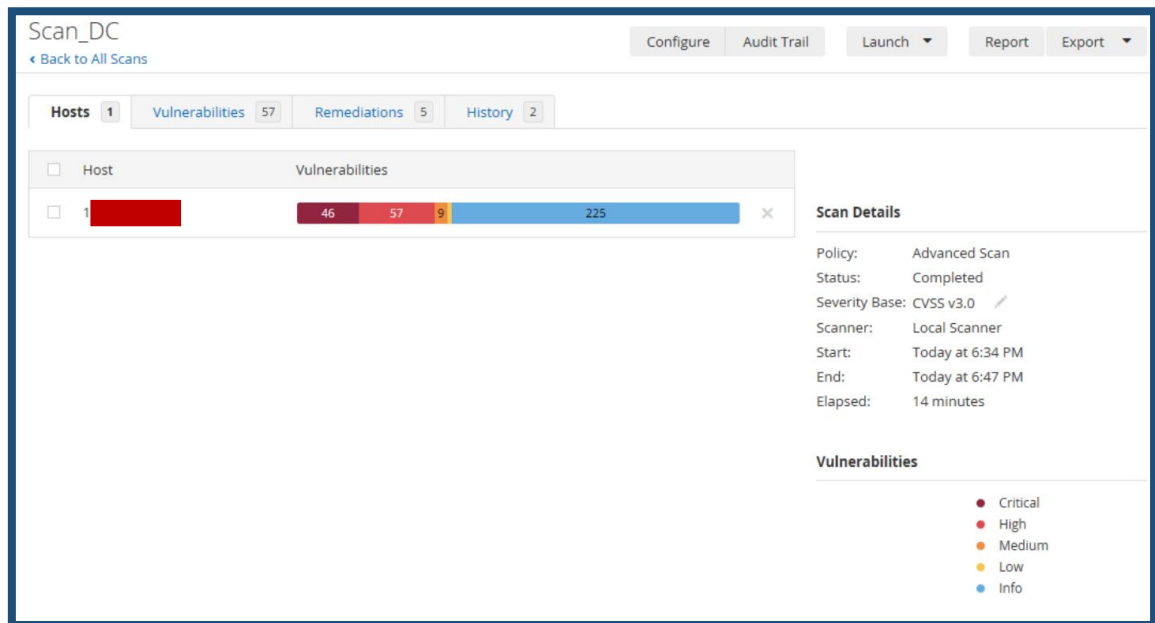
Password: [Redacted]

Domain: [Redacted]

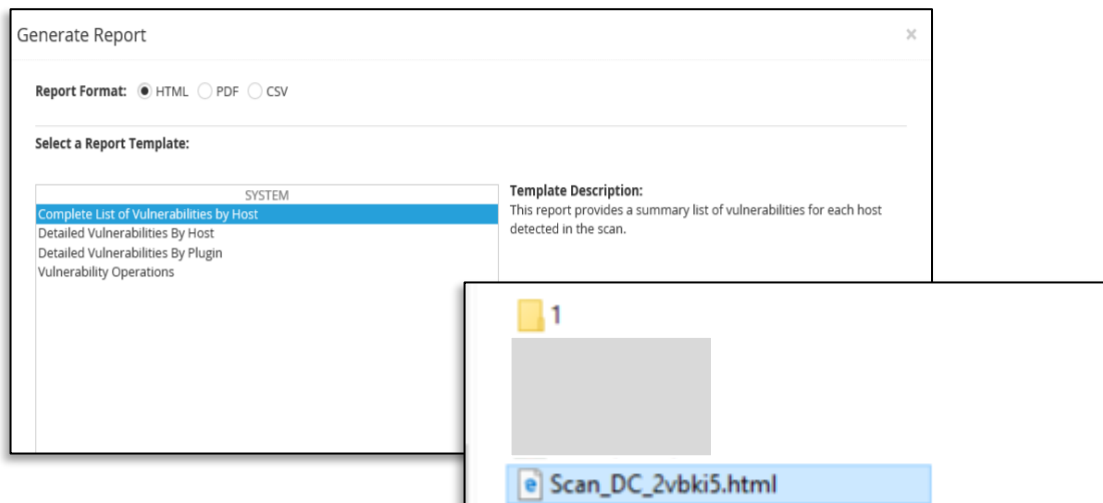
Global Credential Settings

- ☒ Never send credentials in the clear
For security reasons, Windows credentials are not sent in the clear by default.
- ☒ Do not use NTLMv1 authentication
If this option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Nessus. This hash can be potentially cracked to reveal a username or password. It never should be used to directly log into other services. Source

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)”.

Severity	CVSS v3.0 Base Score	CVSS v3.0 Temporal Score	CVSS v3.0 Environmental Score	CVE ID	Description
CRITICAL	9.8	6.7	0.0313	119612	Security Updates for Microsoft .NET Framework (December 2018)
CRITICAL	9.8	7.4	0.9742	132999	Security Updates for Microsoft .NET Framework (January 2020)
CRITICAL	9.8	6.7	0.2112	117431	Security Updates for Microsoft .NET Framework (September 2018)
CRITICAL	9.4	9.8	0.9664	150367	KB5003638: Windows 10 version 1607 / Windows Server 2016 Security Update (June 2021)
CRITICAL	9.0	9.2	0.0106	208298	KB5044293: Windows 10 Version 1607 / Windows Server 2016 Security Update (October 2024)
CRITICAL	10.0	9.0	0.4463	139488	KB4571694: Windows 10 Version 1607 and Windows Server 2016 August 2020 Security Update
HIGH	8.8	8.9	0.9509	108967	KB4093119: Windows 10 Version 1607 and Windows Server 2016 April 2018 Security Update
HIGH	8.8	9.7	0.9737	109606	KB4103723: Windows 10 Version 1607 and Windows Server 2016 May 2018 Security Update
HIGH	8.8	6.7	0.9439	110491	KB4284880: Windows 10 Version 1607 and Windows Server 2016 June 2018 Security Update
HIGH	8.8	8.9	0.9437	110980	KB4338814: Windows 10 Version 1607 and Windows Server 2016 July 2018 Security Update
HIGH	8.8	9.4	0.9529	111685	KB4343887: Windows 10 Version 1607 and Windows Server 2016 August 2018 Security Update (Foreshadow)

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.