

Uso DE NESSUS PARA EL ANÁLISIS DE VULNERABILIDADES

**Presentado por:
Santiago Peñaranda Mejia**

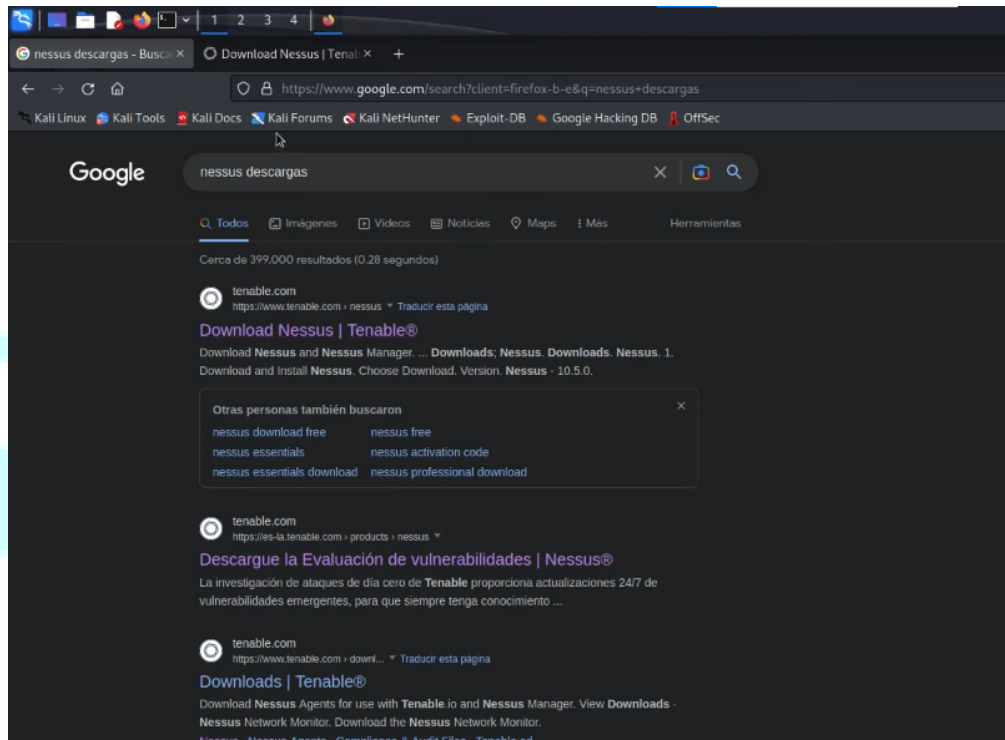
ÍNDICE:

- 1.Instala y configura **Nessus**
- 2.Ejecución de análisis de **Nessus**
- 3.Vulnerabilidades encontradas
- 4.Explicación de las vulnerabilidades

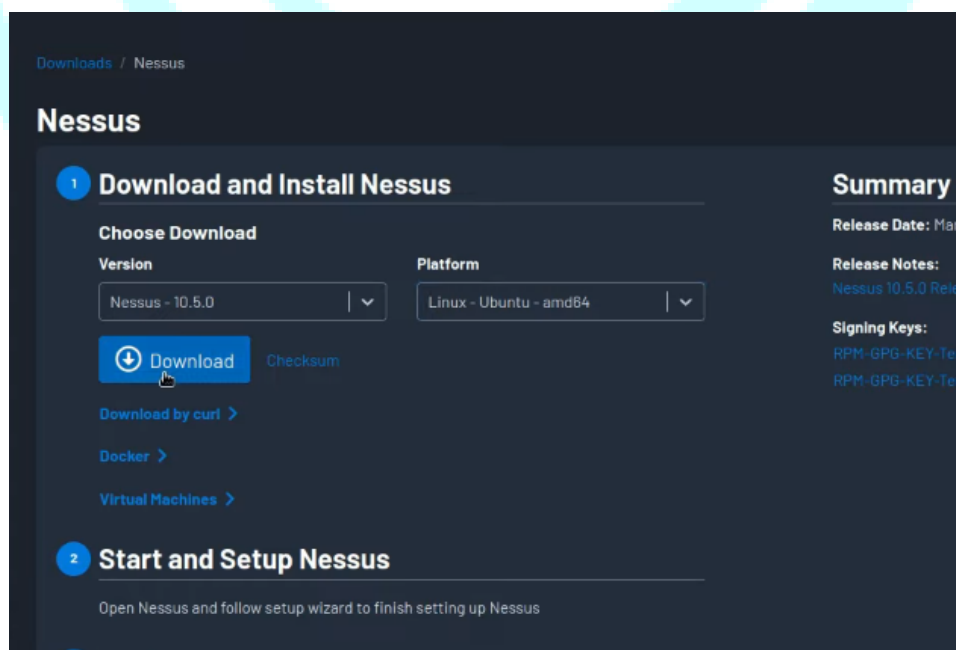


Instala y configura Nessus

Vamos a escribir en el navegador “nessus descargas” tal como aparece en la imagen, y nos dirigiremos al primer link que dice “Download Nessus”.



Una vez dentro de la página de descarga seleccionamos la versión correspondiente y le daremos click en Download y ya se nos iniciará a descargar.



Una vez ya descargado el archivo de nessus haremos su ejecución desde la propia terminal de kali.

Después de la pequeña instalación nos aparecerá esto, aquí nos dice el link del servicio y cómo ejecutarlo. Hacemos un start para activar el servicio web de nessus

```
SSKDF : (KAT_KDF) : Pass
K963KDF : (KAT_KDF) : Pass
K942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://kali:8834/ to configure your scanner

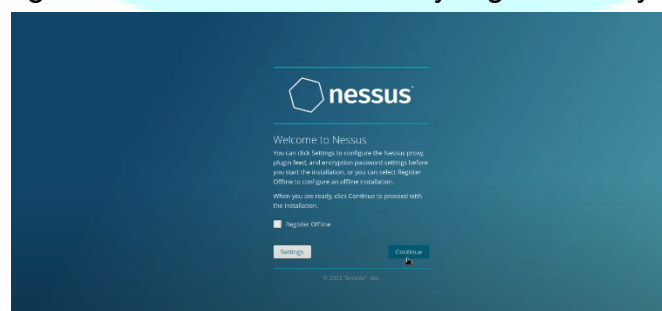
(kali㉿kali)-[~/Downloads]
$ sudo service nessusd start
```

Ahora hacemos un status para ver el estado del servicio y como podemos ver ya está activo.

```
(kali㉿kali)-[~/Downloads]
$ sudo service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Tue 2023-03-14 13:48:02 EDT; 8s ago
     Main PID: 28665 (nessus-service)
        Tasks: 14 (limit: 2275)
       Memory: 127.2M
          CPU: 8.351s
      CGroup: /system.slice/nessusd.service
              └─28665 /opt/nessus/sbin/nessus-service -q
                └─28666 nessusd -q

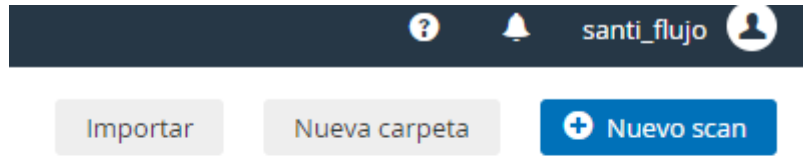
Mar 14 13:48:02 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner
```

Y listo ya tenemos descargado y activado el servicio web de nessus. Ahora solo nos queda entrar a la página web con el link anterior y registrarnos y ya está.

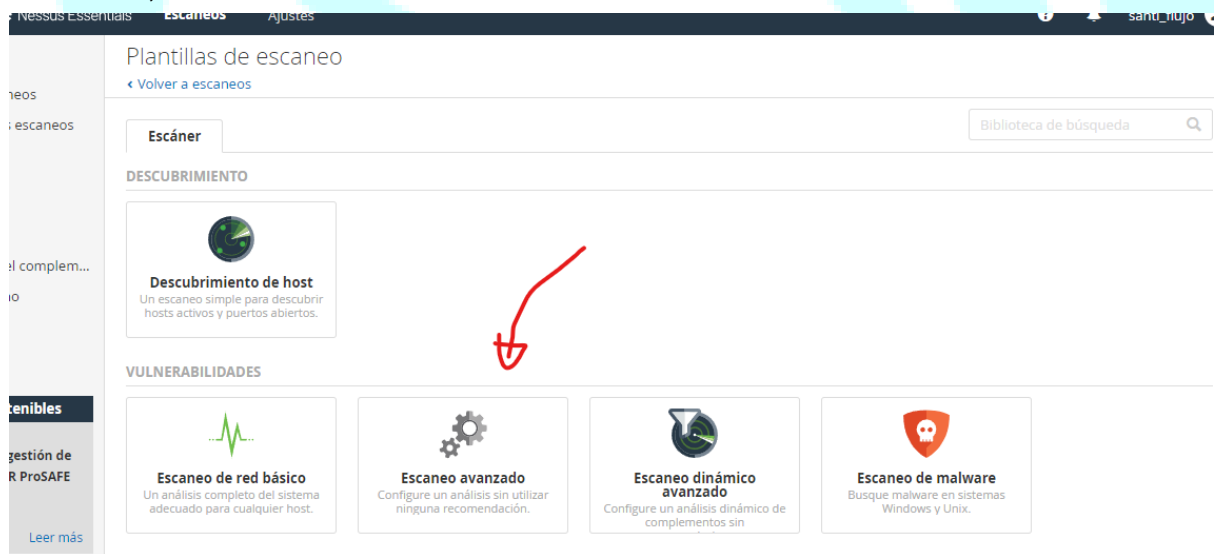


Ejecución de análisis de Nessus

Lo primero que vamos a hacer para hacer un análisis en Nessus es que nos vamos a dirigir a la parte superior derecha de la pantalla y le damos a “Nuevo scan”



Ahora vamos a escoger el tipo de escaneo que vamos a hacer, siempre se recomienda el escaneo avanzado porque es un escaneo más completo que los anteriores, en este caso vamos a utilizar ese.



Una vez ya dentro de “Escaneo Avanzado” vamos a configurar nuestro escaneo, le ponemos el nombre de como queremos que se llame nuestro escaneo, una descripción, donde queremos que se guarde y lo más importante el target o sea nuestro objetivo, aquí ponemos la dirección IP de nuestro objetivo y ya está.

Nombre

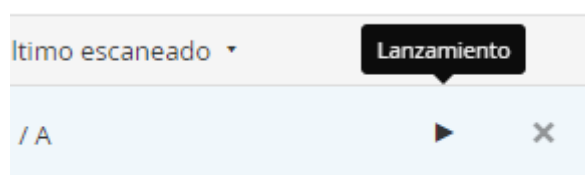
Descripción

Carpeta

Objetivos

[Cargar objetivos](#) [Agregar archivo](#)

Después de haberlo guardado vamos a darle a play para que inicie el escaneo de vulnerabilidades.



Vulnerabilidades encontradas

Después de un buen rato de escaneo esta super herramienta nos a encontrado 21 vulnerabilidades de todo tipo como críticas, de alto riesgo, de medio riesgo y de bajo riesgo.

Escaneo_Vulnerabilidades [Configurar](#) [Pista de auditoria](#)

[Volver a Mis escaneos](#)

Hospedadores 1 Vulnerabilidades 21 Remediaciones 2 Historia 2

Filtrar Buscar anfitriones 1 anfitrión

Anfitrión	Vulnerabilidades
192.168.1.83	<div> <div>Critico: 2 (4,55%)</div> <div> <div>2</div> <div>3</div> <div>4</div> </div> <div>35</div> </div>

Ahora vamos a la sección de vulnerabilidades y ahí nos aparecerán todas las vulnerabilidades encontradas enumeradas de las más críticas a las menos críticas

Escaneo_Vulnerabilidades									
Volver a Mis escaneos									
<div> <div>Hospedadores 1</div> <div>Vulnerabilidades 21</div> <div>Remediaciones 2</div> <div>Historia 2</div> </div>									
<div> <div>Filtrar</div> <div> <div>Buscar vulnerabilidades</div> <div></div> </div> <div>21 vulnerabilidades</div> </div>									
<input type="checkbox"/>	sev	cvss	VPR	N...	Familia	Contar			
<input type="checkbox"/>	CRÍTICO	10.0 *	5.9	D...	RPC	1			
<input type="checkbox"/>	MEZCLADO	4	DNS	4			
<input type="checkbox"/>	ALTO	7.5	6.7	V...	General	1			
<input type="checkbox"/>	ALTO	7.5		N...	RPC	1			
<input type="checkbox"/>	MEZCLADO	5	DNS	5			
<input type="checkbox"/>	MEZCLADO	2	Varios.	2			
<input type="checkbox"/>	INFORMACIÓN	6	ventanas	7			

Ahora vamos a explicar las vulnerabilidades críticas y altas en el siguiente apartado

<div> <div>Hospedadores 1</div> <div>Vulnerabilidades 21</div> <div>Remediaciones 2</div> <div>Historia 2</div> </div>									
<div> <div>Filtrar</div> <div> <div>Buscar vulnerabilidades</div> <div></div> </div> <div>21 vulnerabilidades</div> </div>									
<input type="checkbox"/>	sev	cvss	VPR	N...	Familia	Contar			
<input type="checkbox"/>	CRÍTICO	10.0 *	5.9	D...	RPC	1			
<input type="checkbox"/>	ALTO	7.5	6.7	V...	General	1			
<input type="checkbox"/>	ALTO	7.5		N...	RPC	1			

Explicación de las vulnerabilidades

VULNERABILIDAD CRÍTICA

Esta vulnerabilidad crítica llamada Divulgación de información sobre acciones exportadas de NFS conocida en inglés como “NFS Exported Share Information Disclosure” se refiere a situaciones en las que la información sensible o confidencial almacenada en un recurso compartido NFS es expuesta de manera no autorizada.

Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en un host remoto.

CRÍTICO

Divulgación de información sobre acciones exportadas de NFS

>

Detalles del complemento

Descripción

El host de escaneo podría montar al menos uno de los recursos compartidos NFS exportados por el servidor remoto. Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en un host remoto.

Solución

Configure NFS en el host remoto para que solo los hosts autorizados puedan montar sus recursos compartidos remotos.

Gravedad:

Crítico

IDENTIFICACIÓN:

11356

Versión:

1.21

Tipo:

remoto

Familia:

RPC

Publicado:

12 de marzo de 2003

Modificado:

30 de agosto de 2023

Port	Hosts
2049 / udp / rpc-nfs	192.168.1.83

VULNERABILIDAD ALTA

Esta vulnerabilidad alta llamada **Vulnerabilidad de Samba Badlock** conocida en inglés como **Samba Badlock Vulnerability** esta vulnerabilidad Badlock se refiere a una serie de vulnerabilidades de seguridad en el protocolo SMB que afectan a sistemas que utilizan la implementación Samba. Esta vulnerabilidad fue anunciada en abril de 2016, al principio se anunció con gran publicidad y se consideró crítica en ese momento, también recibió críticas por la forma en que se presentó, ya que algunos argumentaron que la publicidad exagerada podría haber llevado a expectativas poco realistas.

La vulnerabilidad Badlock permitía a un atacante realizar ataques de hombre en el medio (MITM) y descifrar contraseñas y otros datos sensibles transmitidos a través del protocolo SMB.

Hospedadores 1

Vulnerabilidades 21

Remediasiones 2

Historia 2

Configurar

Pista de audit

ALTO

Vulnerabilidad de Samba Badlock

< >

Detalles del complemento

Descripción

La versión de Samba, un servidor CIFS/SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock, que existe en el Administrador de Cuentas de Seguridad (SAM) y la Autoridad de Seguridad Local (Política de Dominio) (LSAD).) protocolos debido a una negociación inadecuada del nivel de autenticación en los canales de llamada a procedimiento remoto (RPC). Un atacante intermediario que pueda interceptar el tráfico entre un cliente y un servidor que aloja una base de datos SAM puede explotar esta falla para forzar una degradación del nivel de autenticación, lo que permite la ejecución de llamadas arbitrarias a la red Samba. en el contexto del usuario interceptado, como ver o modificar datos de seguridad confidenciales en la base de datos de Active Directory (AD) o deshabilitar servicios críticos.

Solución

Actualice a la versión Samba 4.2.11 / 4.3.8 / 4.4.2 o posterior.

Gravedad:

Alto

IDENTIFICACIÓN:

90509

Versión:

1.8

Tipo:

remoto

Familia:

General

Publicado:

13 de abril de 2016

Modificado:

20 de noviembre de 2019

Controladores clave VPR

Amenaza reciente:

no hay eventos registrad

Intensidad de amenaza:

muy baja

Madurez del código de explotación:

no prob

Para ver los registros de depuración, visite el host individual

Puerto ▾	Hospedadores
445/tcp/cif	192.168.1.83

VULNERABILIDAD ALTA

Esta vulnerabilidad de alto riesgo llamada **NFS comparte legibilidad mundial** conocida en inglés como **NFS Shares World Readable** esta vulnerabilidad se trata que los recursos compartidos a través de NFS sean legibles por cualquier usuario en el mundo, es decir, por cualquier usuario que tenga acceso al sistema a través de NFS. Osea el servidor NFS remoto está exportando recursos compartidos sin restringir el acceso.

Hospedadores 1

Vulnerabilidades 21

Remediaciones 2

Historia 2

Configurar

Pista de auditor

ALTO

NFS comparte legibilidad mundial

< >

Detalles del complemento

Descripción
El servidor NFS remoto está exportando uno o más recursos compartidos sin restringir el acceso (según el nombre de host, la IP o el rango de IP).

Solución
Coloque las restricciones apropiadas en todos los recursos compartidos de NFS.

Gravedad: Alto

IDENTIFICACIÓN: 42256

Versión: 1.11

Tipo: remoto

Familia: RPC

Publicado: 26 de octubre de 2009

Modificado: 5 de mayo de 2020

Para ver los registros de depuración, visite el host individual

Puerto ▾	Hospedadores
2049/tcp/rpc-nfs	192.168.1.83