Uso de Nessus para el análisis de vulnerabilidades

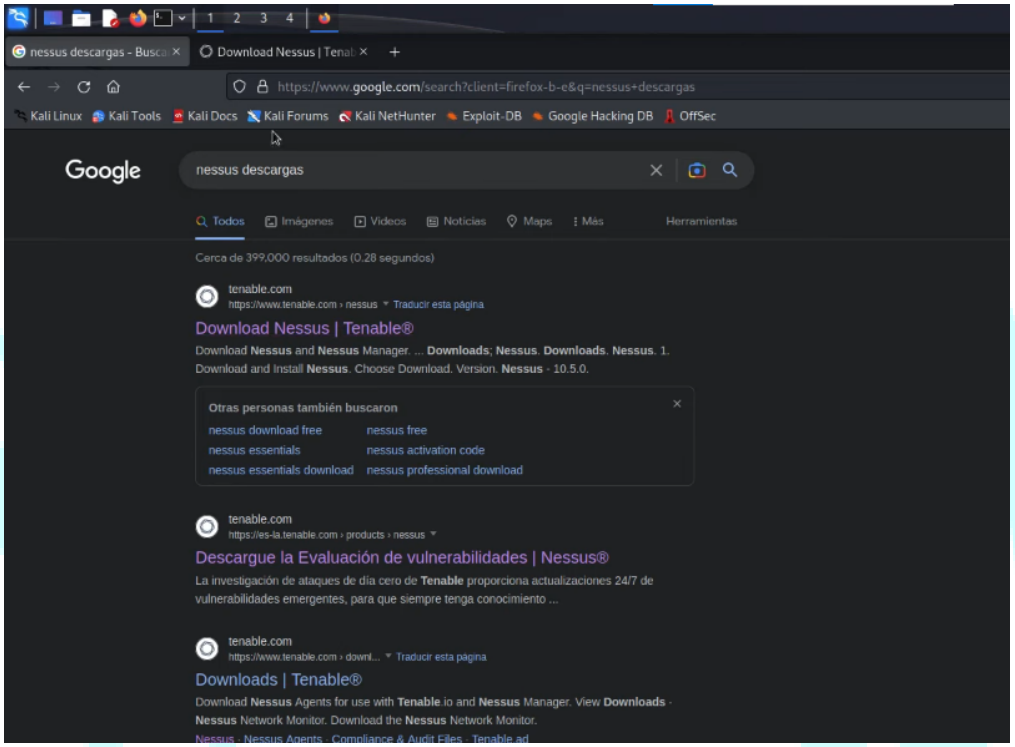
Presentado por:

Santiago Peñaranda Mejia

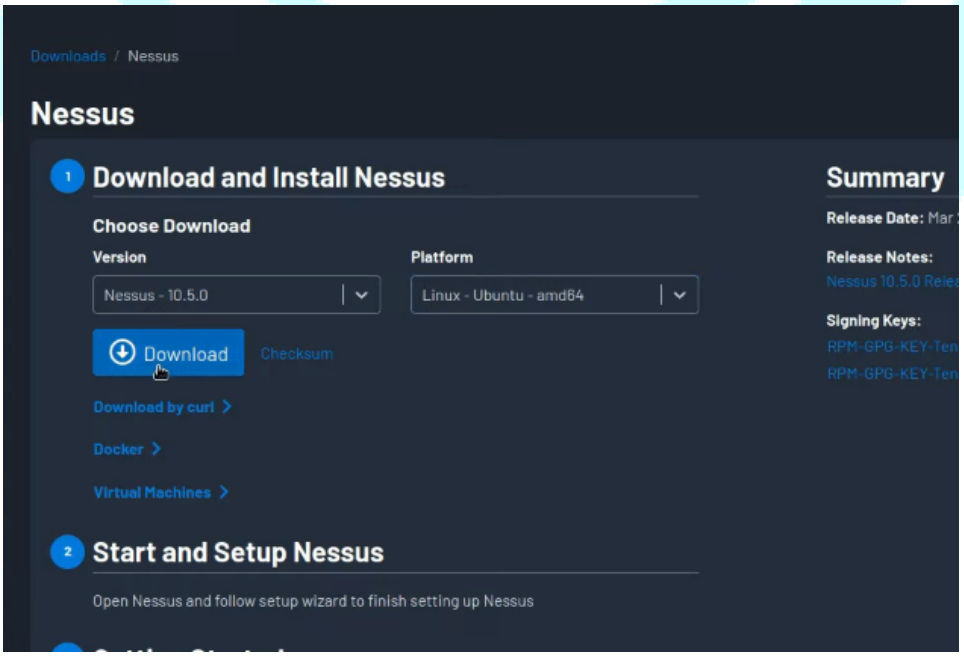
ÍNDICE:

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
X963KDF : (KAT_KDF) : Pass
X942KDF : (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.

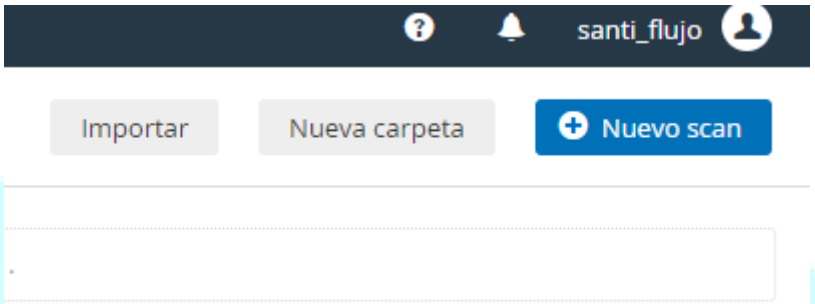
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Tue 2023-03-14 13:48:02 EDT; 8s ago
   Main PID: 28665 (nessus-service)
      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
```

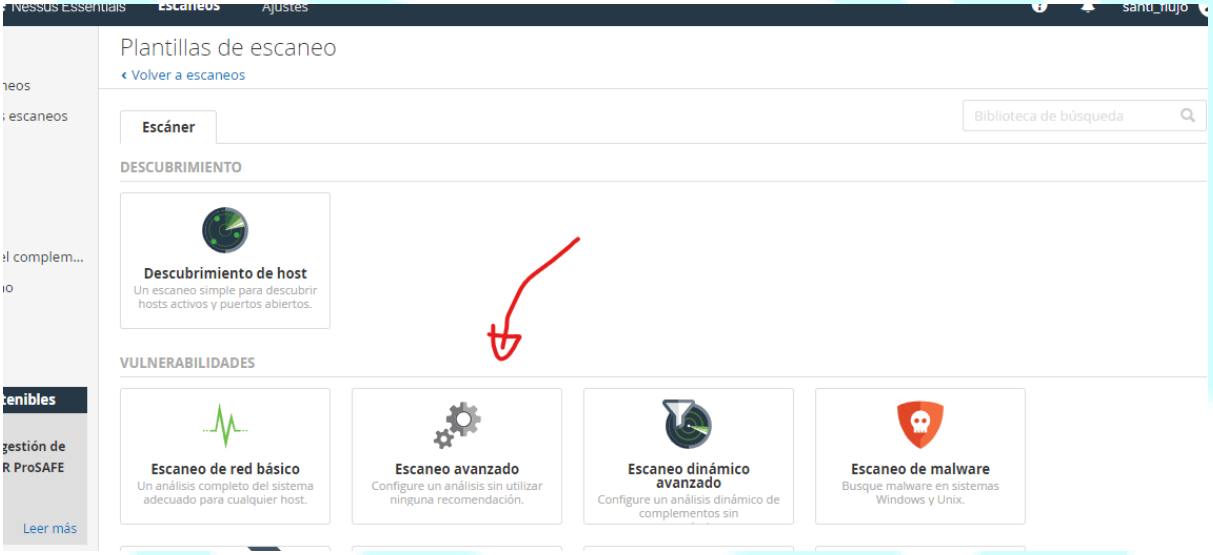
Y listo ya tenemos descargado y activado el servicio web de nessus. Ahora solo nos queda entrar a la página web con el link anterior y registrarnos y ya está.

Ejecución de análisis de Nessus

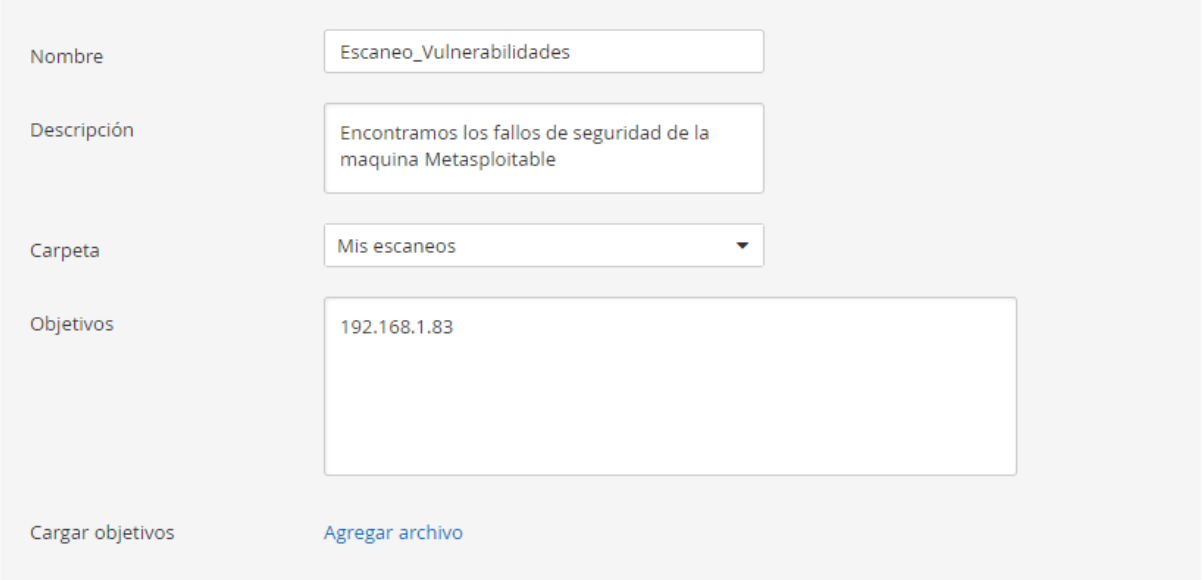
Lo primero que vamos hacer para hacer un análisis en nessus es que nos vamos a dirigir a la parte superior derecha de la pantalla y le damos a “Nuevo scan”



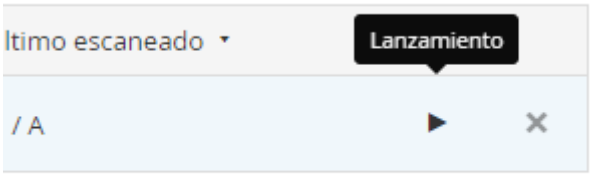
Ahora vamos a escoger el tipo de escaneo que vamos hacer, siempre se recomienda el escaneo avanzado porque es un escaneo más completo que los anteriores, en este caso vamos a utilizar ese.



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 importarte el target osea nuestro objetivo, aquí ponemos la dirección IP de nuestro objetivo y ya está.



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.

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

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

Explicación de las vulnerabilidades

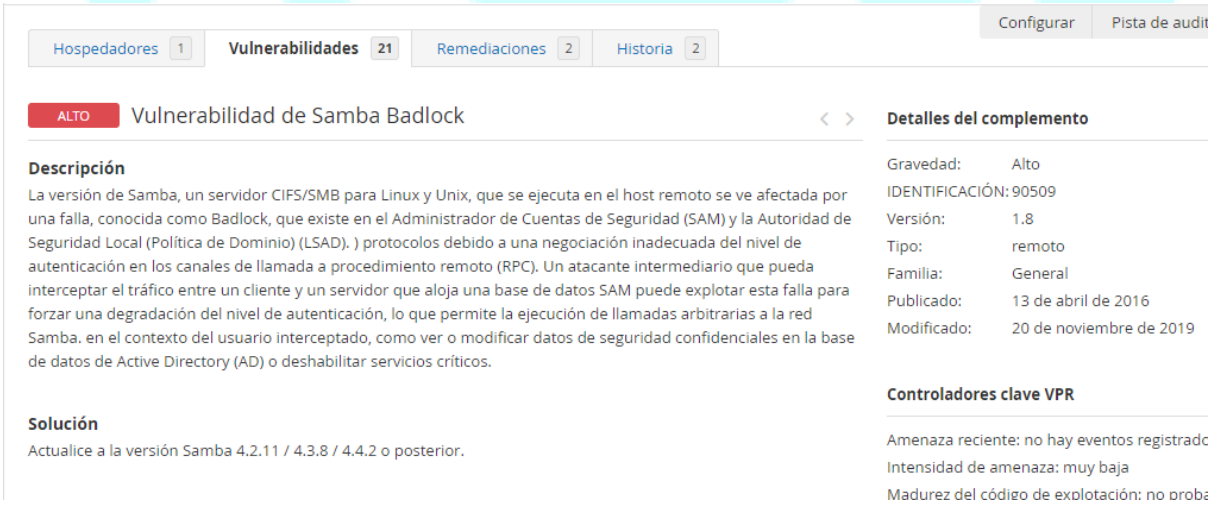
VULNERABILIDAD CRÍTICA

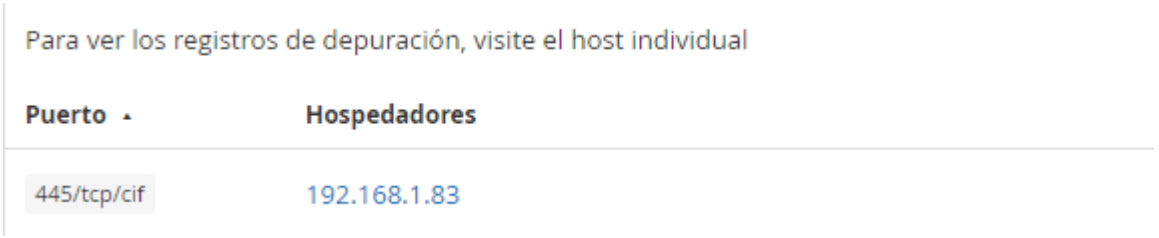
Esta vulnerabilidad crítica llamada Divulgación de información sobre acciones exportadas de NFS conocida en inglés como “NFS Exported Share Information Disclosure” se refiere a situaciones en las que la información sensible o confidencial almacenada en un recurso compartido NFS es expuesta de manera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

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

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.





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.