INSTALAR ZENMAP en Kali Linux

Para instalar Zenmap en Kali Linux 2020.1 en adelante debes seguir estos pasos:

1. Abre una Terminal y verifica la última versión del paquete RPM de Zenmap desde el sitio oficial de Nmap (https://nmap.org/download.html). Asegúrate de descargar la versión adecuada para tu sistema. (zenmap-7.94-1.noarch.rpm por ejemplo)

2. Actualizar el sistema:

Antes de instalar cualquier software nuevo, es una buena práctica actualizar tu sistema Kali Linux. Abre una terminal y ejecuta los siguientes comandos:

```
sudo apt update
```

```
sudo apt upgrade
```

3. Descarga la última versión del paquete RPM de Zenmap desde el sitio oficial de Nmap:

```
sudo wget https://nmap.org/dist/zenmap-7.94-1.noarch.rpm
```

4. Instala la herramienta `alien`, que te permitirá convertir el paquete RPM en un paquete DEB, si aún no está instalada:

```
sudo apt install alien
```

5. Luego, utiliza `alien` para convertir el paquete RPM descargado en un paquete DEB. Reemplaza `"nombre_del_paquete.rpm"` con el nombre del archivo RPM que descargaste:

```
sudo alien zenmap-7.94-1.noarch.rpm
```

6. Una vez que la conversión haya finalizado, obtendrás un archivo DEB. Instálalo con `dpkg`:

```
sudo dpkg -r zenmap-7.94-1.noarch.deb
```

7. A continuación, es posible que encuentres problemas de dependencias al tratar de instalar Zenmap. Para resolverlos, ejecuta el siguiente comando para instalar las dependencias faltantes:

```
sudo apt install –f
```

INSTALAR OpenVAS en Kali Linux

Para instalar OpenVAS en Kali Linux la forma más común es a través del paquete llamado "gvm" (Greenbone Vulnerability Management) ; para lo cual debes seguir estos pasos:

1. Abre una Terminal y actualiza el sistema:

Antes de instalar cualquier software nuevo, es una buena práctica actualizar tu sistema Kali Linux. Abre una terminal y ejecuta los siguientes comandos:

```
sudo apt update
```

```
sudo apt upgrade
```

2. Asegurarse los paquetes requeridos:

```
sudo apt install wget bzip2 build-essential cmake pkg-config
```

3. Instalar el paquete "gvm":

```
sudo apt install gvm
```

4. Inicializar la base de datos de OpenVAS:

```
sudo gvm-setup
```

Este comando configurará la base de datos y generará las claves necesarias. Los errores más comunes en esta etapa es olvidar las claves o conflicto de puertos/cluster por más de una versión de PostgreSQL instalada; si se presentan investigar las soluciones!

5. Iniciar los servicios de OpenVAS:

```
sudo systemctl start openvas-scanner
```

```
sudo systemctl start openvas-manager
```

```
sudo systemctl start gsad
```

Opcionalmente se pueden habilitar los servicios para que se inicien automáticamente al arrancar cambiando el comando por `systemctl enable`

7. Acceder a la interfaz web de OpenVAS:

Una vez que los servicios se hayan iniciado, puedes acceder a la interfaz web de OpenVAS utilizando un navegador web. Abre tu navegador y ve a la siguiente dirección:

```
https://localhost:9392
```

Deberás aceptar el certificado de seguridad (puede que muestre una advertencia, ya que usa un certificado autofirmado por defecto) y luego podrás iniciar sesión en OpenVAS utilizando las credenciales que configuraste durante el proceso de instalación.

INSTALAR Nikto en Kali Linux

Nikto es una herramienta de escaneo de vulnerabilidades web ampliamente utilizada para identificar problemas de seguridad en servidores web y aplicaciones. Los pasos básicos para instalar Nikto en Kali Linux son estos:

1. Abre una Terminal y actualiza el sistema:

Antes de instalar cualquier software nuevo, es una buena práctica actualizar tu sistema Kali Linux. Abre una terminal y ejecuta los siguientes comandos:

```
sudo apt update
```

```
sudo apt upgrade
```

2. Instala Nikto**

Puedes instalar Nikto directamente desde los repositorios de Kali Linux con el siguiente comando:

```
sudo apt install nikto
```

Confirma la instalación escribiendo 'Y' cuando se te solicite.

3. Ejecuta Nikto

Una vez que Nikto esté instalado, puedes ejecutarlo en una terminal. El comando básico para escanear un sitio web es el siguiente:

```
sudo nikto -h URL_del_objetivo
```

Sustituye `URL_del_objetivo` por la dirección web del sitio que deseas escanear. Por ejemplo:

Diferencias en OpenVas y Nikto

OpenVAS y Nikto son dos herramientas diferentes en el campo de la seguridad cibernética y se utilizan para propósitos diferentes, aunque ambos están relacionados con la evaluación de la seguridad en sistemas y aplicaciones web.

OpenVAS: Es una herramienta de escaneo de vulnerabilidades de red. Se utiliza para identificar vulnerabilidades en sistemas operativos, aplicaciones y servicios que se ejecutan en una red.

Nikto: Es una herramienta de escaneo de vulnerabilidades web. Está diseñada específicamente para analizar servidores web y aplicaciones web en busca de problemas de seguridad.