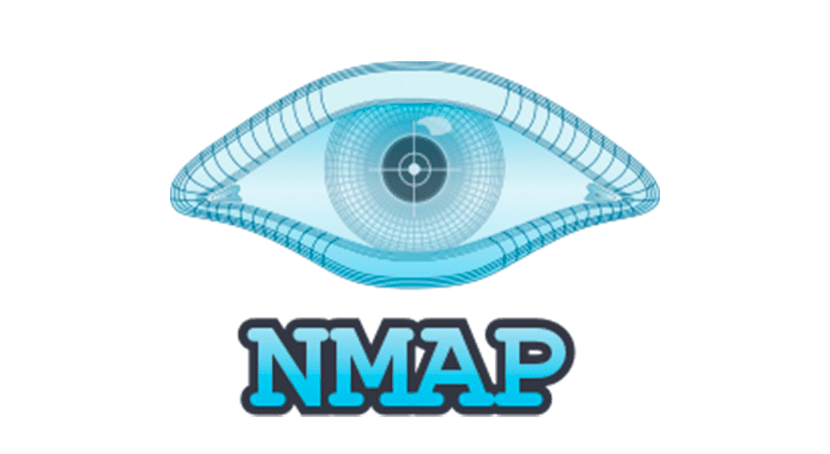
**Análisis y auditoría de redes informáticas para identificar vulnerabilidades y descubrimiento de equipos mediante la herramienta Nmap**



# César de San Pedro Martín

## Índice

1. [**¿ Qué es Nmap?**](#Punto1)**.**
2. [**Preparación del entorno de trabajo**](#Punto2)**.**
3. [**Obtención de Información**](#Punto3)**.**
4. [**Enumeración de activos**](#Punto4)**.**
5. [**Fase de vulnerabilidades**](#Punto5)**.**
6. [**Bibliografía**](#Punto6)**.**

**1.- ¿ Qué es Nmap? .**

Nmap ( network map o “ mapeador de redes “) es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se sugiere para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

Nmap utiliza paquetes IP “crudos” («raw», N. del T.) en formas originales para determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones) ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

Aunque generalmente se utiliza Nmap en auditorías de seguridad, muchos administradores de redes y sistemas lo encuentran útiles para realizar tareas rutinarias, como puede ser el inventariado de la red.

La salida de Nmap es un listado de objetivos analizados, con información adicional para cada uno dependiente de las opciones utilizadas.

La información primordial es la  “tabla de puertos interesantes”. Dicha tabla lista el número de puerto y protocolo, el nombre más común del servicio, y su estado. El estado puede ser open (abierto) ser filtered(filtrado), closed(cerrado), o unfiltered(no filtrado).

Abierto significa que la aplicación en la máquina destino se encuentra esperando conexiones o paquetes en ese puerto. Filtrado indica que un cortafuegos, filtro, u otro obstáculo en la red está bloqueando el acceso a ese puerto, por lo que Nmap no puede saber si se encuentra abierto o cerrado. Los puertos cerrados no tienen ninguna aplicación escuchando en los mismos, aunque podrían abrirse en cualquier momento. Los clasificados como “no filtrados” son aquellos que responden a los sondeos de Nmap, pero para los que Nmap no puede determinar si se encuentran abiertos o cerrados. Nmap informa de las Combinaciones de estado open|filteredy closed|filtered cuando no se puede determinar en cual de los dos estados esta un puerto.

La tabla de puertos también puede incluir detalles de la versión de la aplicación cuando se ha solicitado detección de versiones. Nmap ofrece información de los protocolos IP soportados, en vez de puertos abiertos, cuando se solicita un análisis de protocolo IP con la opción ( -sO).

Además de la tabla de puertos interesantes, Nmap puede dar información adicional sobre los objetivos, incluyendo el nombre de DNS según la resolución inversa de la IP, un listado de sistemas operativos posibles, los tipos de dispositivo, y direcciones MAC**.**

**Opciones de Nmap**

Cuando se ejecuta Nmap sin parámetros se muestra este resumen de opciones

Uso: nmap [Tipo(s) de Análisis] [Opciones] {especificación de objetivos} 

ESPECIFICACIÓN DE OBJETIVO:  
 Se pueden indicar nombres de sistema, direcciones IP, redes, etc.    
   Ej: scanme.nmap.org, microsoft.com/24 , 192.168.0.1; 10.0.0-255.1-254  
   -iL <archivo\_entrada>: Lee una lista de sistemas/redes del archivo.  
   -iR <número de sistemas>: Selecciona objetivos al azar  
   --exclude <sist1[,sist2][,sist3],...>: Excluye ciertos sistemas o redes   
  --excludefile <fichero\_exclusión>: Excluye los sistemas indicados en el fichero

DESCUBRIMIENTO DE HOSTS:   
  -sL: Sondeo de lista - Simplemente lista los objetivos a  
  analizar -sP: Sondeo Ping - Sólo determina si el objetivo está vivo  
 -P0: Asume que todos los objetivos están vivos

-PS/PA/PU [listadepuertos]: Análisis TCP SYN, ACK o UDP de los puertos indicados  
 -PE/PP/PM: Solicita un análisis ICMP del tipo echo, marca de fecha y máscara de red  
 -n/-R: No hacer resolución DNS / Siempre resolver [por omisión: a veces]  
 --dns-servers <serv1[,serv2],...>: Especificar servidores DNS específicos  
 --system-dns: Usando la resolución del sistema operativo

TÉCNICAS DE ANÁLISIS:   
 -sS/sT/sA/sW/sM: Análisis TCP SYN/Connect()/ACK/Window/Maimon

-sN/sF/sX: Análisis TCP Null, FIN, y Xmas   
 - -scanflags <indicador>: Personalizar los indicadores TCP a utilizar  
 -sI <sistema zombi[:puerto\_sonda]>: Análisis pasivo («Idle», N. del T.)  
 -sO: Análisis de protocolo IP   
 -b <servidor ftp rebote>: Análisis por rebote FTP 

ESPECIFICACIÓN DE PUERTOS Y ORDEN DE ANÁLISIS:   
 -p <rango de puertos>: Sólo sondear los puertos indicados   
 Ej: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080   
 -F: Rápido - Analizar sólo los puertos listados en el archivo nmap-services   
 -r: Analizar los puertos secuencialmente, no al azar. 

DETECCIÓN DE SERVICIO/VERSIÓN:

-sV: Sondear puertos abiertos, para obtener información de servicio/versión  
 --version-intensity <nivel>: Fijar de 0 (ligero) a 9 (probar todas las sondas)  
 --version-light: Limitar a las sondas mas probables (intensidad 2)  
 --version-all: Uso de todas las sondas (intensidad 9)  
 --version-trace: Presentar actividad detallada del análisis (para depurar)

DETECCIÓN DE SISTEMA OPERATIVO   
 -O: Activar la detección de sistema operativo (SO)  
 --osscan-limit : Limitar la detección de SO a objetivos prometedores

--osscan-guess: Adivina el SO de la forma más agresiva

TEMPORIZADO Y RENDIMIENTO:  
 -T[0-5]: Seleccionar plantilla de temporizado (los números altos son más rápidos)  
 --min -hostgroup/max-hostgroup <tamaño>: Paralelizar los sondeos  
 --min-parallelism/max-parallelism <numsondas>: Paralelización de sondeos  
 --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <msegs >: Indica el tiempo de ida y vuelta de la sonda  
 --max-retries <reintentos>: Limita el número máximo de retransmisiones de las sondas de análisis de puertos  
 --host-timeout <msegs>: Abandonar un objetivo pasado este tiempo  
 --scan- delay/--max-scan-delay <msegs>: Ajusta el retraso entre sondas

EVASIÓN Y FALSIFICACIÓN PARA CORTAFUEGOS/IDS:  
 -f; --mtu <valor>: fragmentar paquetes (opc. con el MTU indicado)   
 -D <señuelo1,señuelo2[,ME],...>: Disimular el análisis con señuelos N. del T.: «ME» es «YO » mismo.  
 -S <Dirección\_IP>: Falsificar la dirección IP origen   
 -e <interfaz>: Usar la interfaz indicada   
 -g/--source-port <numpuerto>:   
 --data-length <num>: Agregar datos al azar a los paquetes enviados   
 --ttl <val>: Fijar el valor del campo time-to-live (TTL) de IP  
 --spoof-mac <dirección mac/prefijo/ nombre de fabricante>: Falsificar la dirección MAC  
 --badsum: Enviar paquetes con una suma de comprobación TCP/UDP falsa

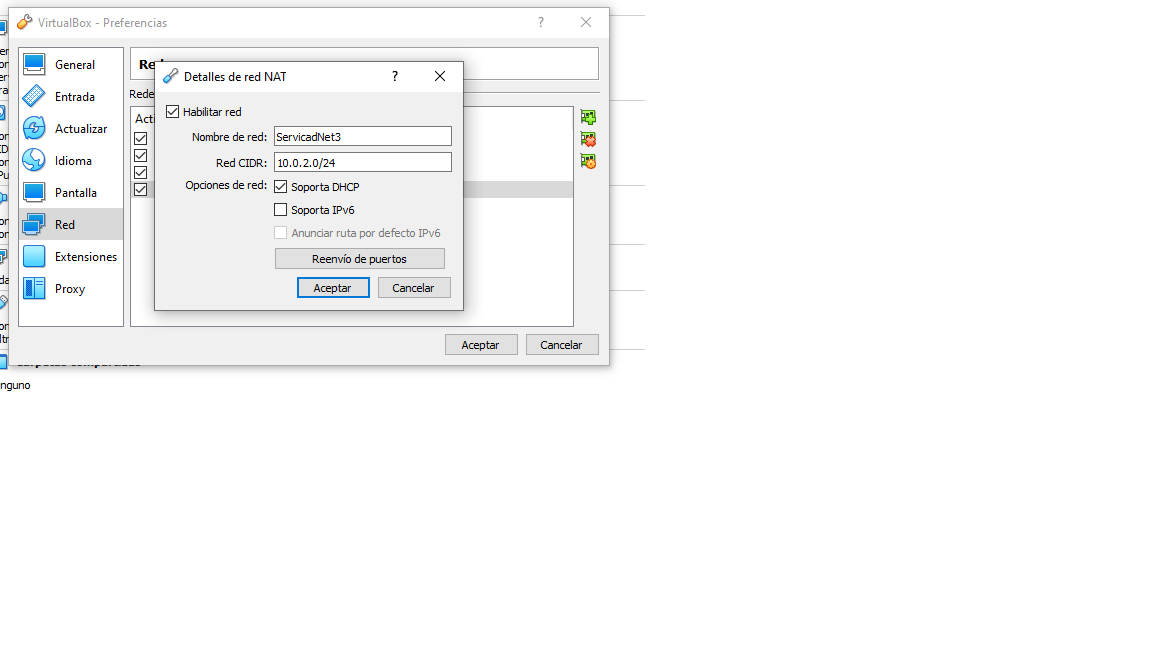
SALIDA:   
 -oN/-oX/-oS/-oG <file>: Guardar el sondeo en formato normal, XML, s|<rIpt kIddi3 (n3n3b4n4n4), y Grepeable (para usar con grep(1), N. del T.),respectivamente, al archivo indicado.   
 -oA <nombre\_base>: Guardar en los tres formatos principales al mismo tiempo  
 -v: Aumentar el nivel de mensajes detallados (-vv para aumentar el efecto)  
 -d[nivel]: Fijar o incrementar el nivel de depuración (Tiene sentido hasta 9)  
 --packet-trace: Mostrar todos los paquetes enviados y recibidos   
 --iflist: Mostrar interfaces y rutas (para depurar)   
 --append-output: Agregar, en vez de sobreescribir, a los archivos indicados con -o.   
 --resume <archivo>: Retomar un análisis abortado / detenido.   
 --stylesheet <ruta/URL>: Convertir la salida XML a HTML según la hoja de estilo XSL indicada  
 --webxml: Referenciar a la hoja de estilo de Insecure.Org para tener un XML más portable  
 --no-stylesheet: No asociar la salida XML con ninguna hoja de estilos XSL

MISCELÁNEO:  
 -6: Habilitar análisis IPv6   
 -A: Habilita la detección de SO y de versión  
 --datadir <nombreDir>: Indicar la ubicación de los archivos de datos Nmap personalizados.  
 --send-eth/--send-ip: Enviar paquetes utilizando tramas Ethernet o paquetes IP “crudos”  
 --privileged: Asumir que el usuario tiene todos los privilegios   
 -V: Muestra el número de versión   
 -h: Muestra esta página resumen de la ayuda. 

EJEMPLOS:   
 nmap -v -A scanme.nmap.org   
 nmap -v -sP 192.168.0.0/16 10.0.0.0/8   
 nmap -v -iR 10000 -P0 -p 80

**2.- Preparación del entorno de trabajo.**

* 1. Preparar una maquina Kali Linux(kali-linux-2022.1-virtualbox-amd64) para realizar el análisis de vulnerabilidades Las máquinas ova doble clic sobre la misma para instalarla o en VirtualBox, Archivo 🡪 Importar servicio virtualizado y localizar en nuestro disco duro la carpeta que tiene la ova que queremos instalar. Si en el proceso de instalación nos indica que la máquina ya existe le cambiamos el nombre en la configuración de instalación automática.
     1. Configurar la maquina en modo Red Nat. Hay que crear la Red NAT en VirtualBox a través de Archivo-> Preferencias->Red (ver pantallazo de la configuración de Red NAT). Ambas máquinas deben tener la misma Red NAT
     2. SOLO DEBEMOS TENER HABILITADO UN ADAPTADOR DE RED EN LAS DOS MÁQUINAS. (comprobar las dirección ip (ifconfig) y la conectividad entre ambas máquinas, así como la salida a internet (ping [www.google.es](http://www.google.es)). En modo NAT la ip es similar a 10.0.2.x, tiene salida a internet, sin visibilidad con la máquina anfitriona (cmd-ipconfig adaptador conectado a puerta de enlace 192.168.10.26). Para comprobar las máquinas que haya en la red se hace con nmap
     3. Arrancar la maquina
  2. Preparar la maquina a auditar (Metasploitable.vmdk) Las máquinas que no son owa, hay que instalarlas desde VirtualBox con el icono de nueva -> Nombre de la máquina, seleccionar ubicación de la máquina en nuestro disco duro, Tipo: Linux, Versión: Other Linux 64-bits, memoria siempre en la parte verde de la franja, Disco duro Usar un archivo de disco virtual existente, seleccionamos añadir y buscamos la ubicación del archivo a instalar en nuestro disco duro. Comprobar la configuración de red y verificar que SOLO TIENE ACTIVADO UN SOLO ADAPTADOR DE RED.
     1. Configurar la máquina en modo Red Nat Hay que crear la Red NAT en VirtualBox a través de Archivo-> Preferencias->Red (ver pantallazo de la configuración de Red NAT) Ambas máquinas deben tener la misma Red NAT



* + 1. Arrancar la maquina

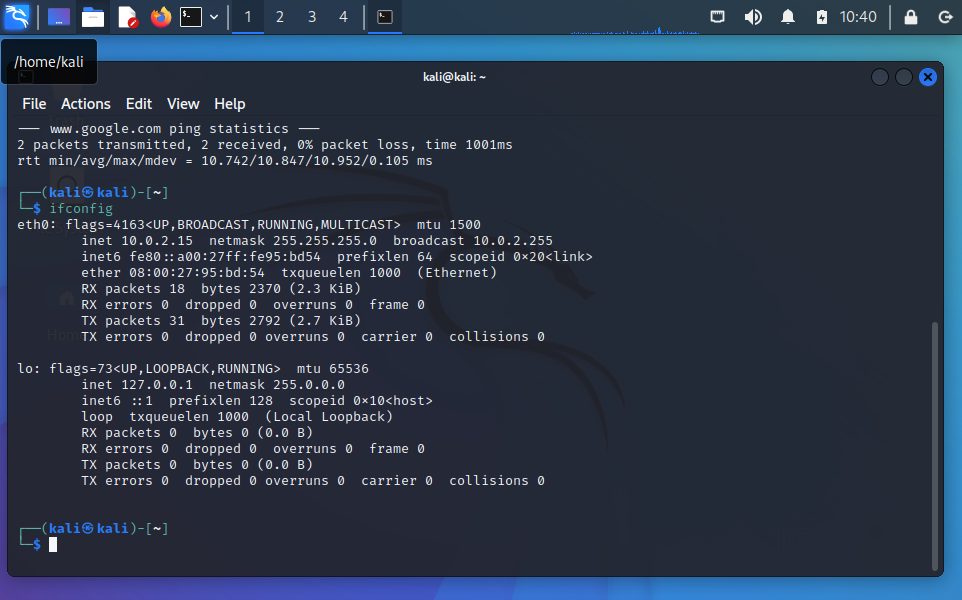
**3.-Obtención de información.**

* 1. Desde la maquina Kali Linux
     1. Comprobar que tienes acceso a internet.

ping [www.google.es](http://www.google.es) -c3 para que nos lance solo 3 paquetes en el ping

* + 1. Ver en qué dirección está la máquina Kali y en que mascara de red tiene.

Ifconfig nos da la 10.0.2.15 netmask 255.255.255.0 (ver pantallazo)

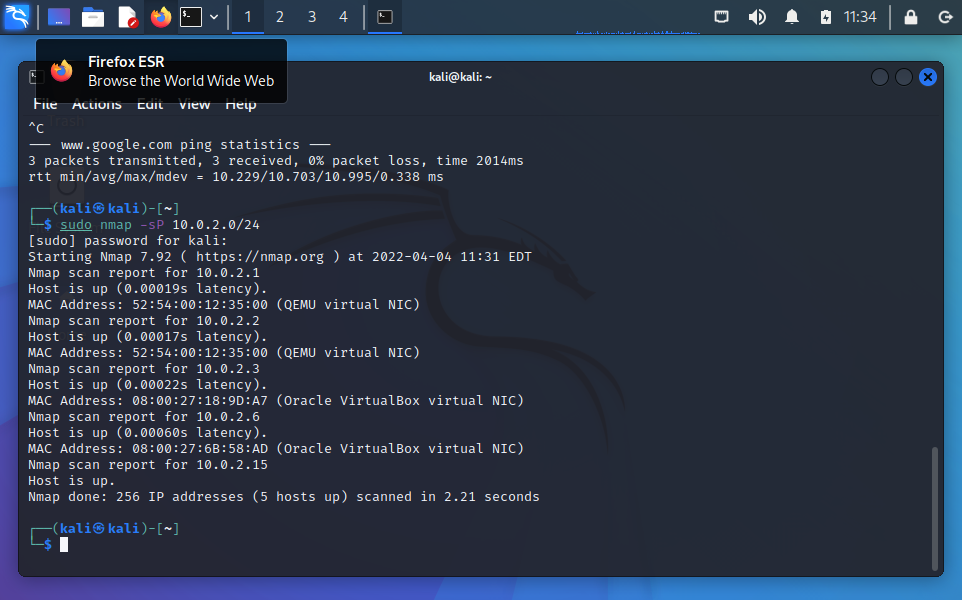


* + 1. Realizar un escaneo para detectar todos los equipos que están en la misma red.

setxkbmap es para establecer teclado en castellano

sudo nmap -sP 10.0.2.0/24 o bien lanzar

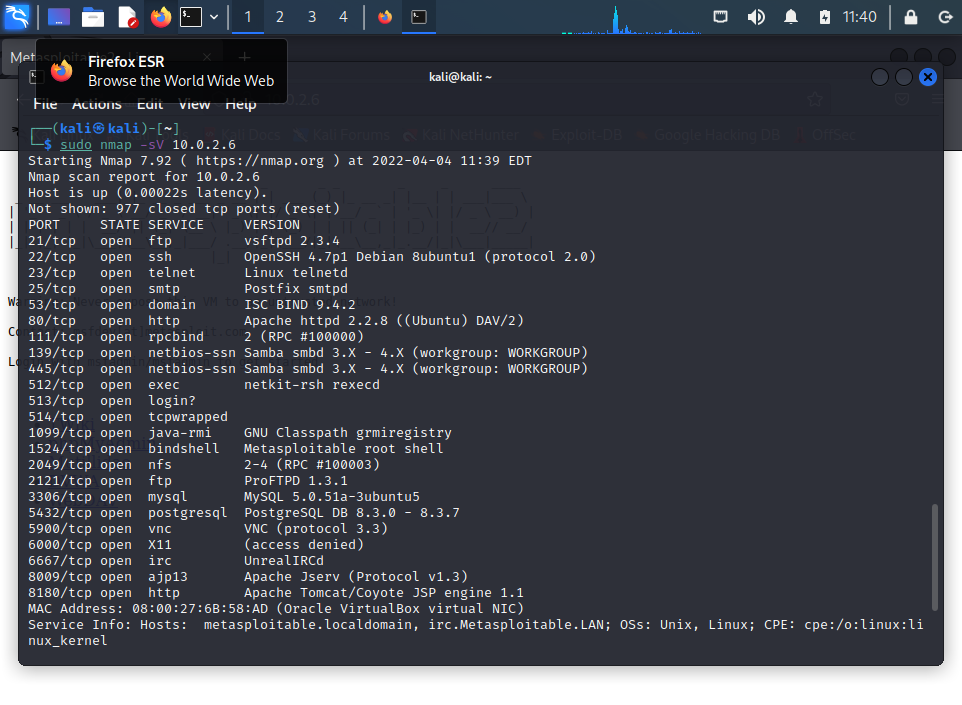
sudo nmap -P 10.0.2.0/24 la máquina que tenga los puertos abiertos será el servidor metasploit



* + 1. Indicar la IP del equipo mestasploitable 2

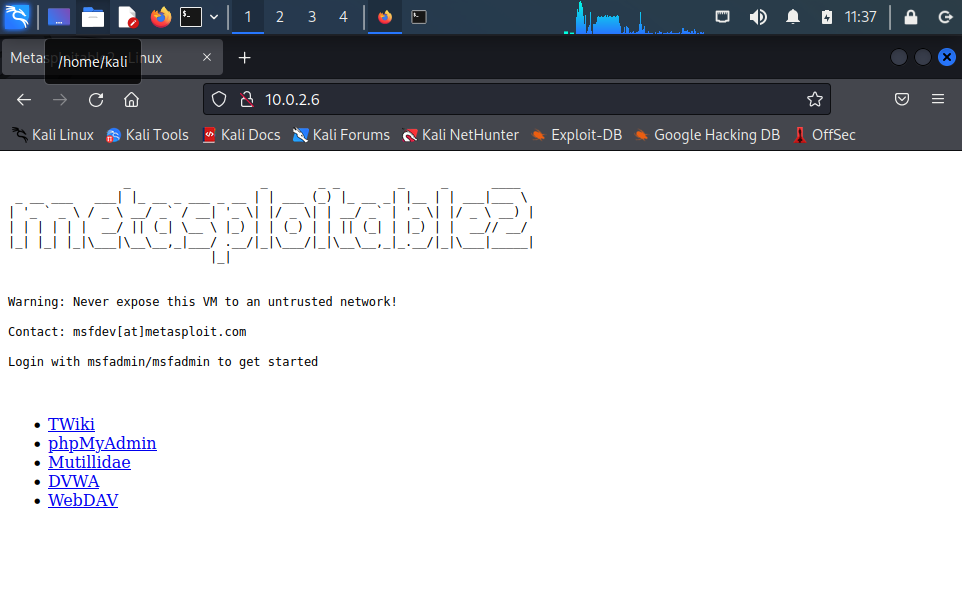
Lanzar nmap -sV 10.0.2.0/24 ó nmap -sV 10.0.2.6 (que es la máquina de metasploit)

Se puede probar con el navegador de Kali poniendo la dirección que nos da, probar con todas y con la correcta nos aparece la máquina de metasploit



* + 1. Acceder a la ip de metasploitable 2 a través del navegador

Poner en el navegador de Kali en la barra de direcciones la ip correspondiente a la máquina virtual de metasploit y nos aparece metasploit.



**4.- Enumeración de activos.**

* 1. Desde la máquina Kali Linux
     1. Realizar un escaneo para detectar los puertos abiertos, servicios corriendo y versiones de los servicios de la maquina mestasploitable 2

sudo nmap -sV 10.0.2.6 (ip máquina metasploit)

* + 1. Indicar cuantos puertos TCP están abiertos

sudo nmap -sT 10.0.2.6 (ip máquina metasploit)

* + 1. Indicar cuantos puertos UDP están abiertos

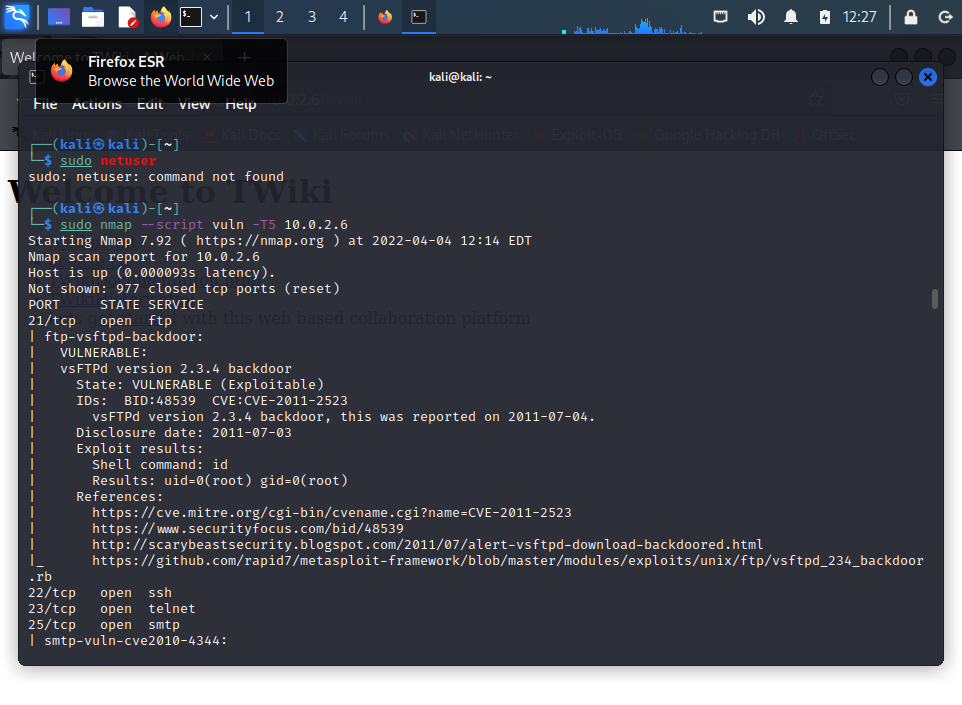
sudo nmap -sU 10.0.2.6 (ip máquina metasploit)

sudo nmap -p- -T5 10.0.2.6 se obtiene un listado de puertos abiertos de forma muy rápida

**5.- Análisis de vulnerabilidades**

* + Desde la máquina Kali Linux
    - Realizar un escaneo de vulnerabilidades con los scripts de nmap

sudo nmap—script vuln -T5 10.0.2.6



* + - Realizar un escaneo de vulnerabiliades con nikto

nikto -h 10.0.2.6

**6.- Bibliografía.**

* <https://nmap.org/man/es/index.html>