



# Laboratorio: ¿Qué es un Honeypot?

Programa de Fundamentos en Ciberseguridad

Guiado por: Ericka Valdés

**OBJETIVO:** Conocer y probar la tecnología conocida como “Honeypot” en un ambiente controlado.

**MATERIALES:** (2) MVs (Windows 10) + Nmap + KFSensor | **Username:** User-1 **password:** user1



## ¿Qué es un Honeypot?

Una definición de **honeypot** proviene del mundo del espionaje, donde se describe que espías como Mata Hari utilizan una relación romántica para robar secretos, poniendo una *"trampa de miel"* (honeypot en inglés). Muchas veces, un espía enemigo resulta víctima de una trampa de miel y luego se lo chantajea para que revele todo lo que sabe.

En términos de seguridad informática, un honeypot cibernético funciona de manera similar, al tender una trampa para los hackers. Es un sistema informático que se *"sacrifica"* para atraer ciberataques, como un señuelo. Simula ser un objetivo para los hackers y utiliza sus intentos de intrusión para obtener información sobre los cibercriminales y la forma en que operan o para distraerlos de otros objetivos.

Ref. <https://latam.kaspersky.com/resource-center/threats/what-is-a-honeypot>



## Conceptos importantes de un Honeypot

- **El honeypot** se parece a un sistema informático real, con aplicaciones y datos, que hace creer a los ciberdelincuentes que es un objetivo legítimo. Por ejemplo, un honeypot podría imitar el sistema de facturación de clientes de una empresa, un blanco frecuente de los ataques de los delincuentes que quieren encontrar números de tarjetas de crédito. Una vez que los hackers están adentro, se los puede rastrear y evaluar su comportamiento para obtener pistas para mejorar la seguridad de la red.
- **Los honeypots** tienen vulnerabilidades de seguridad intencionales para atraer a los atacantes. Por ejemplo, un honeypot podría tener puertos que respondan a un escaneo de puertos o contraseñas débiles. Los puertos vulnerables podrían dejarse abiertos para atraer a los atacantes al entorno del honeypot, en lugar de la verdadera red en servicio, que sería más segura.
- **Un honeypot** no está configurado para abordar un problema específico, como un firewall o un antivirus. Es una herramienta de información que puede ayudarte a comprender las amenazas actuales para tu empresa y detectar la aparición de nuevas amenazas. Gracias a la información obtenida a través de un honeypot, se pueden priorizar y centrar las iniciativas de seguridad.

En base a la lectura anterior, Conteste las siguientes preguntas:

1. ¿Crees que es importante implementar esta tecnología en una infraestructura tecnológica?

2. ¿Cuáles serían los servicios críticos en la que emplearías una Honeypot?

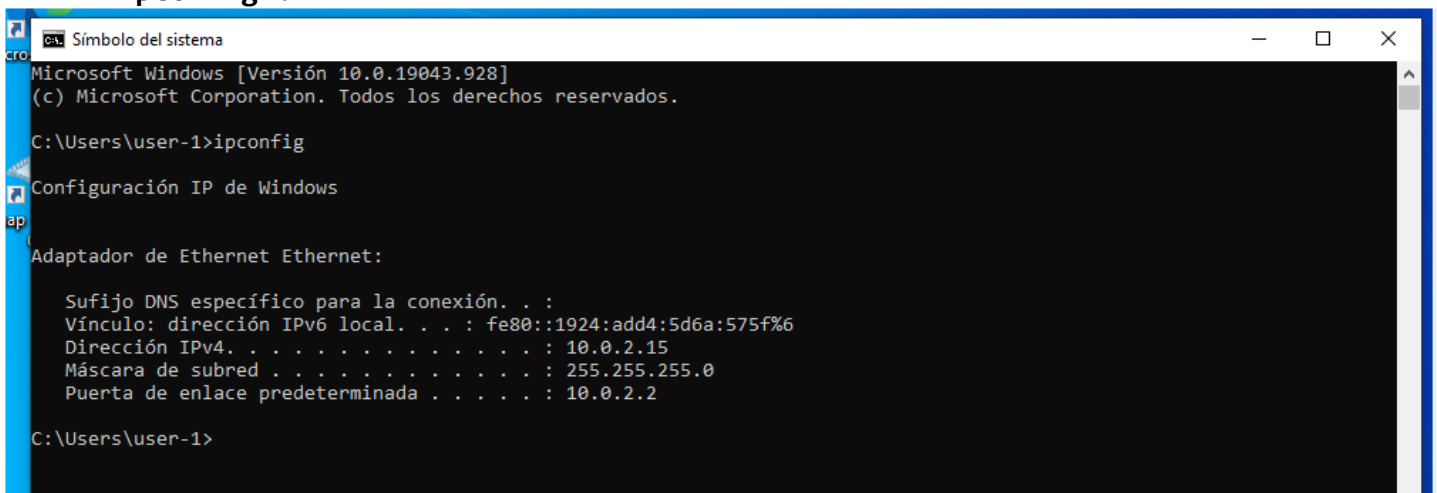
---

## Segunda Parte. KFSensor

**KFSensor** es un honeypot de mediana interacción que se ejecuta bajo Windows y permite simular servicios vulnerables, escuchar el tráfico de red y además interactuar con servicios o aplicaciones instalados en el sistema operativo.

**KFSensor** es un honeypot híbrido, lo que quiere decir que puede implementar tantos servicios simulados (programados por KFSensor) como servicios nativos (instalados y configurados por el usuario), lo que permite dar un ambiente mucho más maduro y real.

1. Encienda las MV “VM with KFsense” y “VM with nmap”
2. Realice un escaneo a la IP de la VM “VM with KFsense” desde la VM “VM with nmap”. Para ver la IP de VM, realice el siguiente comando desde “Símbolo de Sistema”. El comando es: “**ipconfig**”.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.928]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\user-1>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::1924:add4:5d6a:575f%6
    Dirección IPv4. . . . . : 10.0.2.15
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

C:\Users\user-1>
```

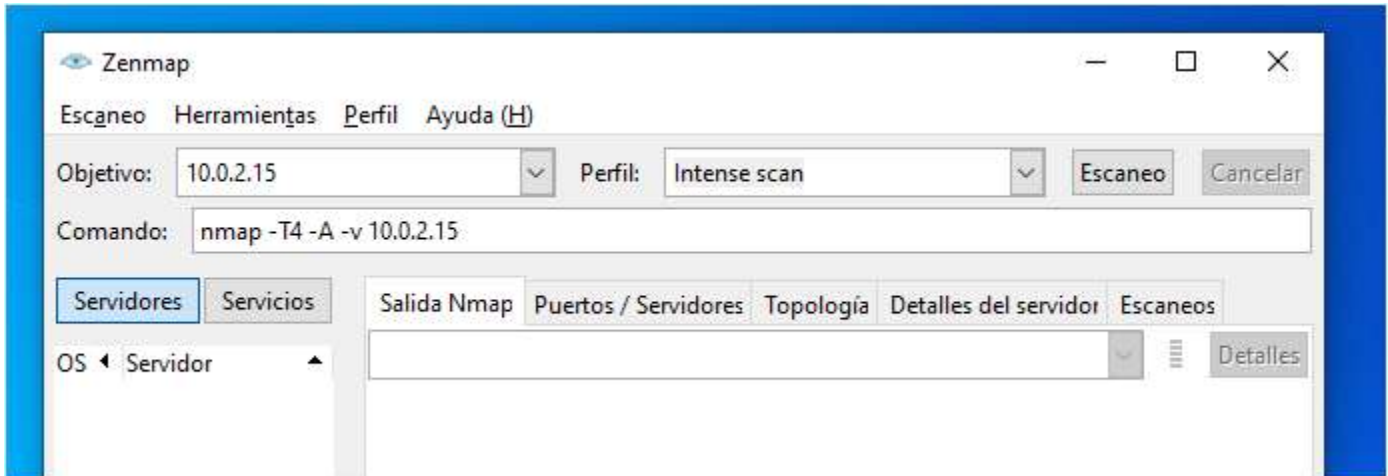
*Hay que recordar que la dirección IP puede variar dependiendo del entorno en la que fue importada la VM.*

**Importante:** la aplicación KFSensor, ya se encuentra configurada para el objetivo del laboratorio. El servicio deberá verse habilitado al iniciar la VM.

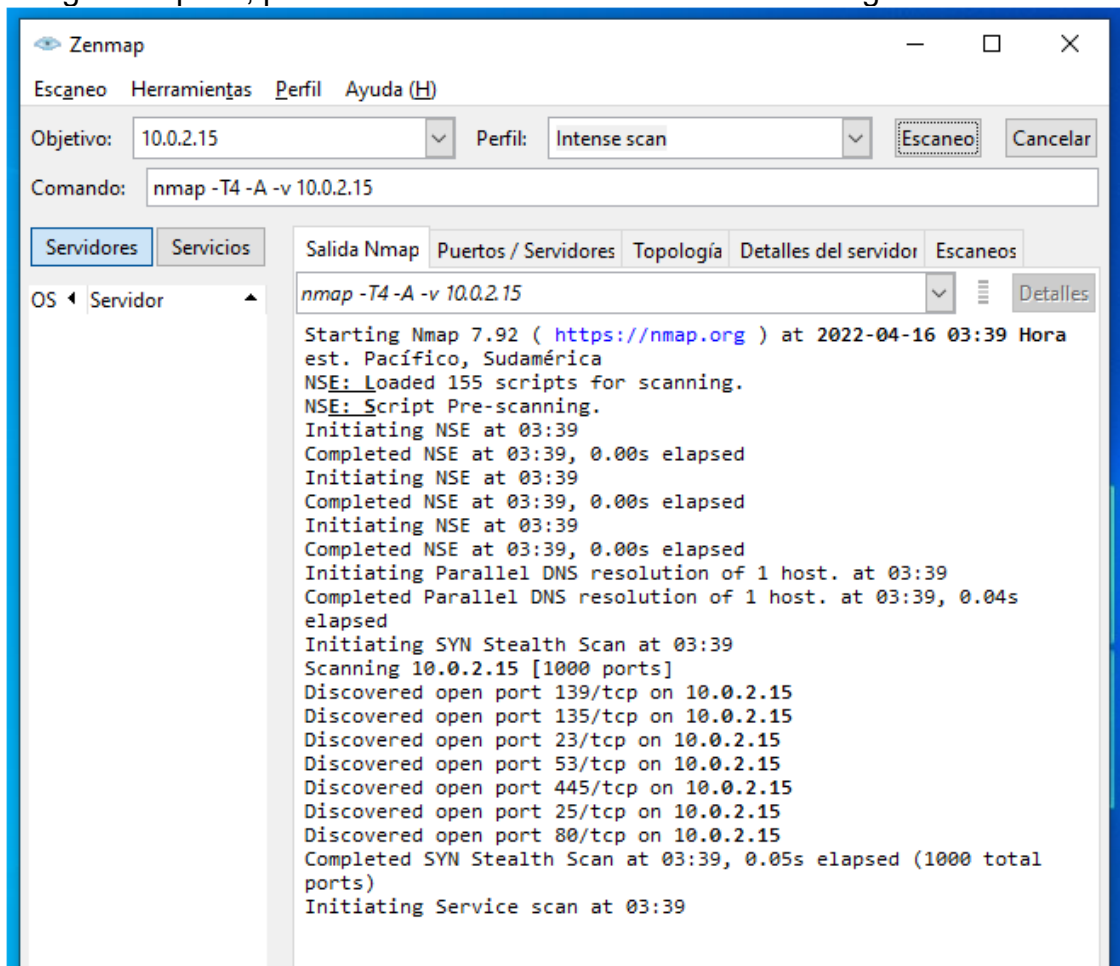
3. A continuación, el comando para escribir en la aplicación de Nmap.

Nmap -T4 -A -v "CoLocar-IP"

Escoge en perfil: "Intense scan"

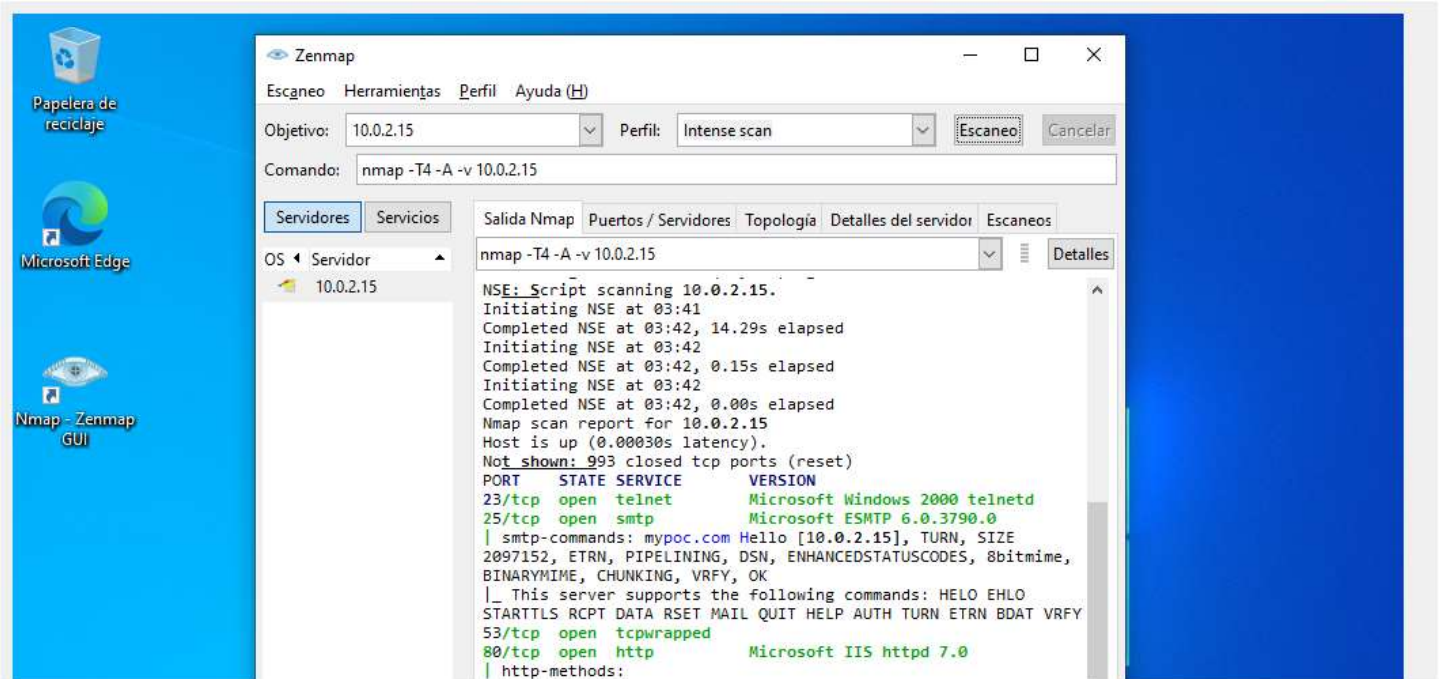


4. Como siguiente paso, presionar "Escaneo". Deberá observa lo siguiente:



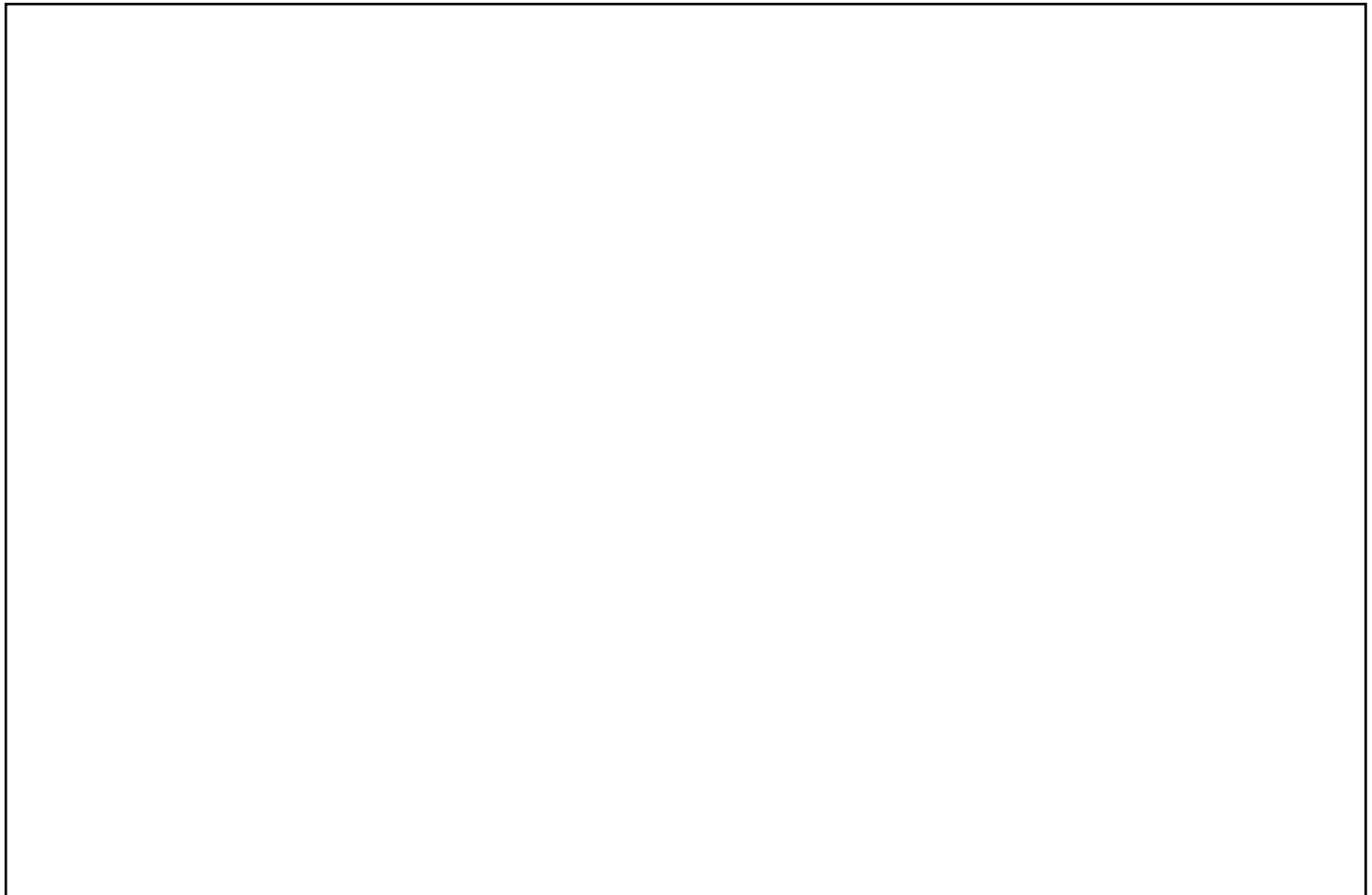
El proceso continuará por un par de minutos. No cierre la aplicación, ni detenga el proceso.

5. Cuando termine el proceso deberá observar algo similar a la siguiente imagen:



En base al resultado, hágase las siguientes preguntas:

- ¿Qué servicios logra detectar?
- ¿Reconoce la versión de los servicios?
- ¿Qué servicios pueden ser vulnerables?
- Investigue un poco acerca de las vulnerabilidades presente sobre el servicio o los servicios detectados.

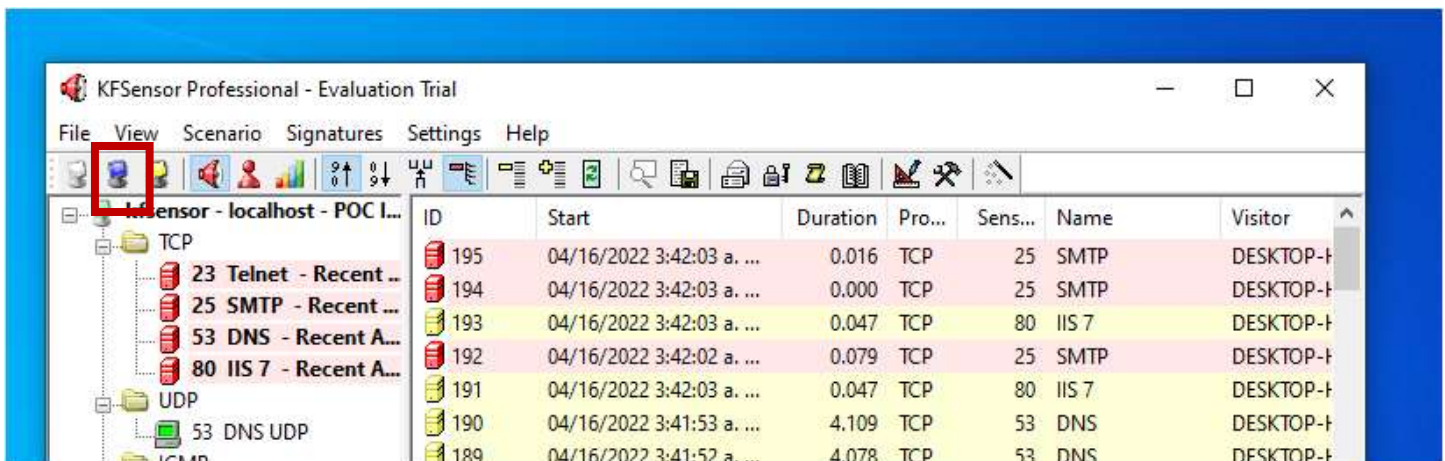


### Tercera Parte. Validar Servicios

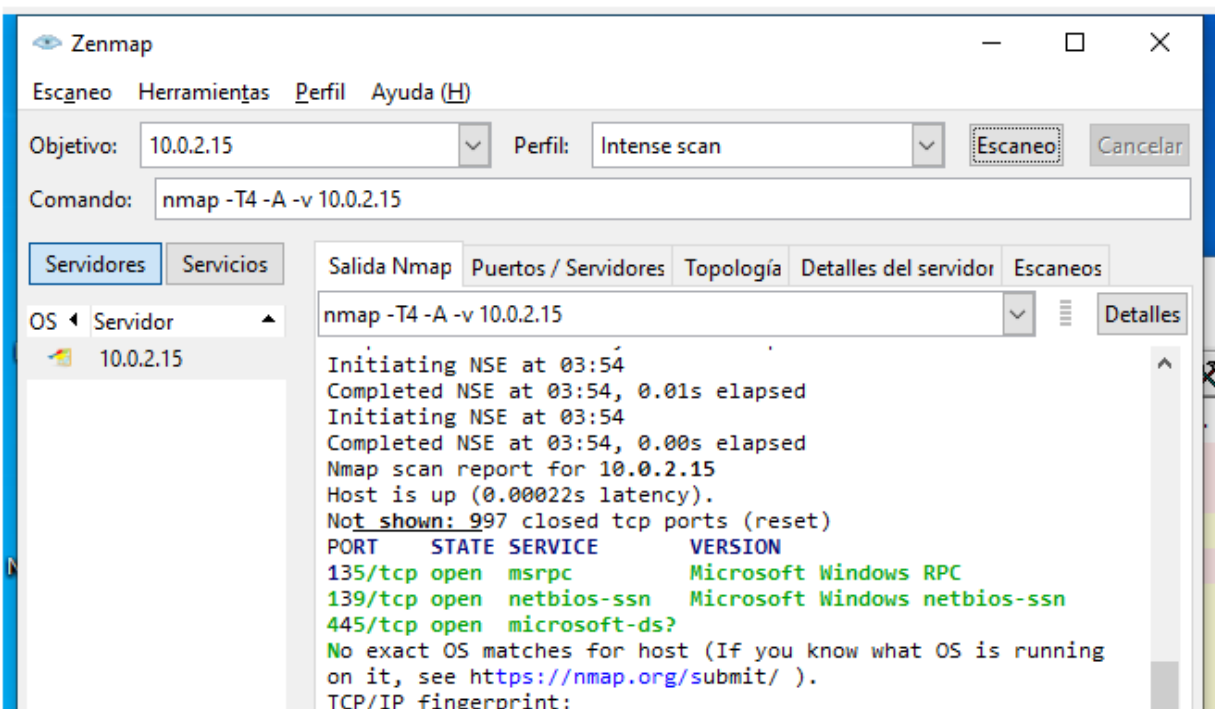
- En la VM “VM with KFSense”, diríjase al siguiente icono ubicado en la barra de tarea de la VM. Dar click sobre el icono.



- A continuación, detendremos el servicio de KFSensor. Presione en el siguiente icono.

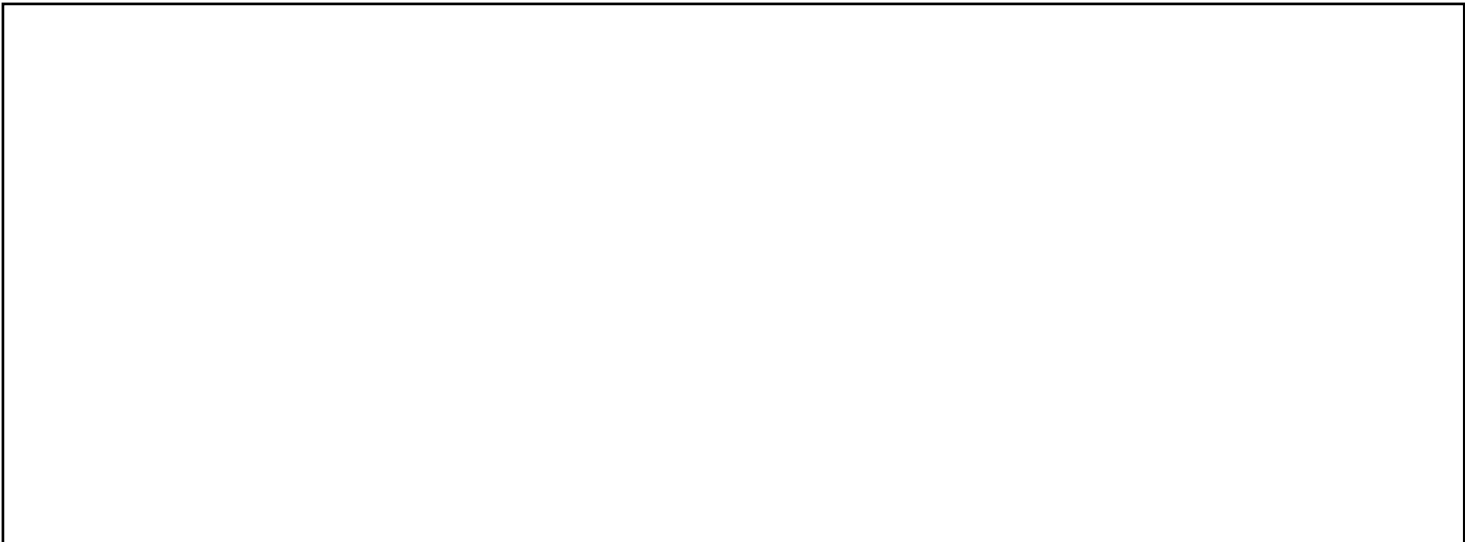


- Una vez detenido el servicio, realicemos otra vez el escaneo realizado en los puntos 3 al 5. Deberá obtener el siguiente resultado.

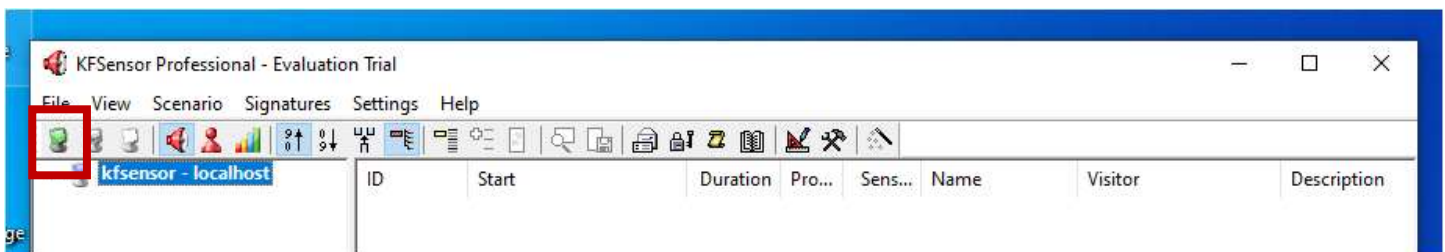




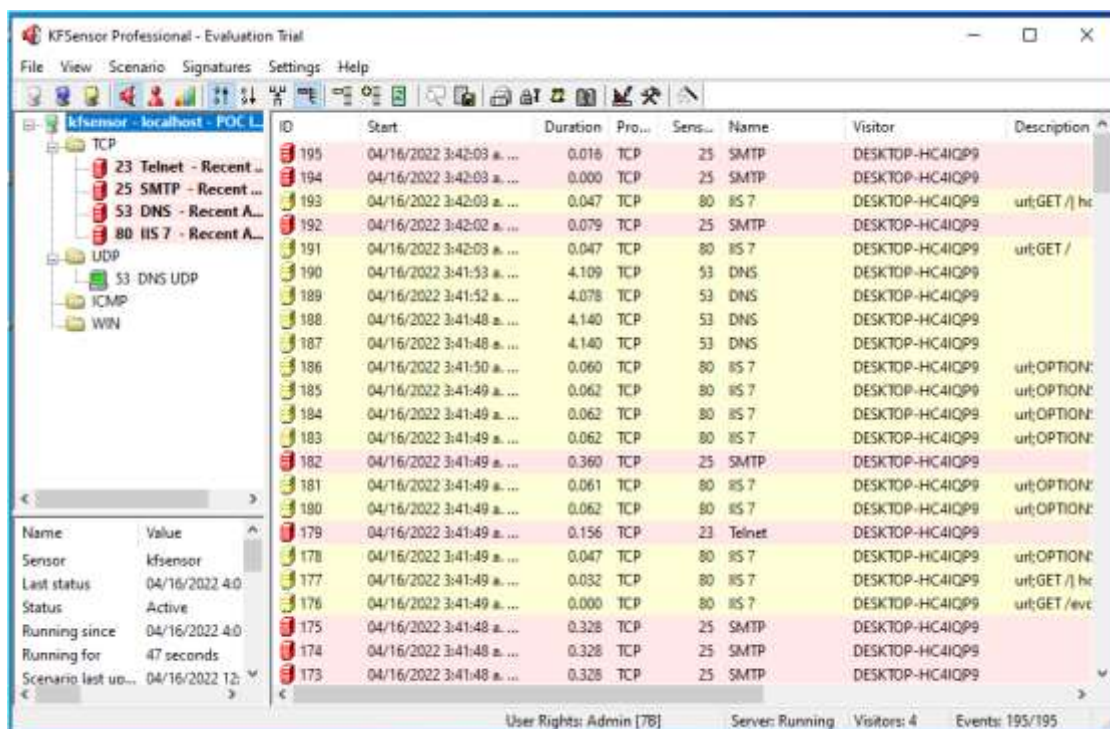
9. Una vez, analizado el resultado, hágase las siguientes preguntas:
  - a. ¿Existe alguna diferencia con el primer escaneo? Si o no y ¿por qué?
  - b. En los servicios detectados, ¿Puede identificar para que funcionan?
  - c. ¿Existe alguna vulnerabilidad en ellos?



10. Por último, encienda nuevamente el servicio de KFSensor.



Ahora analice el resultado del primer escaneo detectado por el servicio de KFSensor.



Como podrá observar KFSensor detecto la actividad generada por el escaneo de puerto nmap. Esta actividad puede ser analizada para reconocer si existe posibles patrones de ataques en un escenario más robusto.

Todos los intentos de conexión quedan perfectamente trazados, y en espera los examinemos para examinar toda esa información.

### Investigue un poco más....

- ¿Cómo el comando telnet nos puede ayudar a verificar si un puerto responde o no? Y ¿Cómo es su sintaxis?
- ¿Qué respuesta recibido si realizo un “**Telnet** *dirección ip 25*” y “**Telnet** *dirección ip 23*”
- ¿Esta última prueba fue detectada por el KFSensor?
- ¿Qué otra información adicional podemos obtener realizando un escaneo?

### Material adicional:

#### Lista de comandos para uso en nmap



Listado de  
comandos Nmap.pdf