Tema4.4.3.4.EnriqueGomezTagle

sábado, 17 de febrero de 2024 11:40

Enrique Ulises Báez Gómez Tagle – 0241823 - 0241823@up.edu.mx
UP. 2024. Ene-Jun. Hackeo Ético y Recuperación Ante Desastres – Yoel Ledo Mezquita

<some output omitted>

¿Por qué fue necesario ejecutar **ps** como root (anteponiendo **sudo** al comando)?

Hay procesos que no le pertenecen a un usuario

<some output omitted>

¿Cómo representa **ps** la jerarquía de procesos?

Con sangría

¿Qué significan las opciones **–t**, **-u**, **–n**, **–a** y **–p** en **netstat**? (utilicen **man netstat** para responder)

-t: conexiones TCP -u: conexiones UDP -p: PID del proceso de conexión
-n: salida numérica -a: sockets de escucha y no escucha.

¿El orden de las opciones es importante para **netstat**?

NO, es irrelevante

Si nos basamos en el resultado de **netstat** que se muestra en el punto (d), ¿cuál es el protocolo de Capa 4, el estado de conexión y el PID del proceso que se están ejecutando en el puerto 80?

TCP, escucha y 595

Aunque los números de puerto son solo una convención, ¿pueden intuir qué clase de servicio se está ejecutando en el puerto 80 de TCP?

Servidor web

¿Qué es **nginx**? ¿Cuál es su función? (Busquen nginx en Google)

Servidor web (proxy inverso, load balancer, Proxy) también para encontrar procesos no identificados

En la segunda línea vemos que el proceso 396 es propiedad de un usuario de nombre http y que tiene el número de proceso 395 como proceso matriz. ¿Qué significa? ¿Es común este comportamiento?

NGINX inicia 396 con usuario http. Si es normal

¿Por qué vemos grep 395 en la última línea?

línea de comando NGINX

secuencia de letras aleatorias que se le envió y devuelve un error en formato de página web.

¿Por qué el error se envió como página web?

NGINX es un servidor web, tiene el protocolo HTTP

Utilicen Telnet para conectarse con el puerto 68. ¿Qué ocurre? Explique.

68 es un puerto UDP.
No podemos conectarnos pues telnet está basado en TCP.

Preguntas de reflexión

1. ¿Cuáles son las ventajas de utilizar netstat?

Ver las conexiones presentes en una computadora.
Ver direcciones de origen y destino.
Puertos, IDS de proceso. Datos generales de las conexiones

2. ¿Cuáles son las ventajas de utilizar Telnet? ¿Es seguro?

Sí, si no es un shell remoto.
Sirve para probar o tener información sobre algún servicio de red.