

# Gestión de Vulnerabilidades con Nessus

## Ejercicio 3

Nombre: **Unix Operating System Unsupported Version Detection**

Nivel: Critico

Descripción:

La versión que Nessus ha detectado del sistema operativo Unix que se ejecuta en el host remoto ya no tiene soporte.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Si buscamos la versión del sistema operativo en Google para ver si existe alguna vulnerabilidad encontramos el siguiente exploit:

<https://www.exploit-db.com/exploits/9083>

El cual se puede utilizar para escalar privilegios en la maquina objetivo.

Pero en este caso no vamos a poder ejecutarlo ya que el exploit esta diseñado para sistemas de 64 bits y no de 32 bits, pero si se hubiera dado el caso podrías escalar privilegios compilando y ejecutando el exploit.

Tener un sistema sin actualizar es peligroso y mas si ya no tiene soporte ya que vulnerabilidades que han sido detectadas para este sistema ya no están parcheadas.

Por lo que se recomienda actualizar a una versión actual