2DA PARTE PARCIAL

Seguridad de la Información

Bryan Ferney Hernández Pineda

Daniel Alejandro Olarte Ávila

Michael Steven Pinzón Villanueva

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: daniel.olarte01@correo.usa.edu.co

Escuela de Ciencias Exactas e Ingeniería

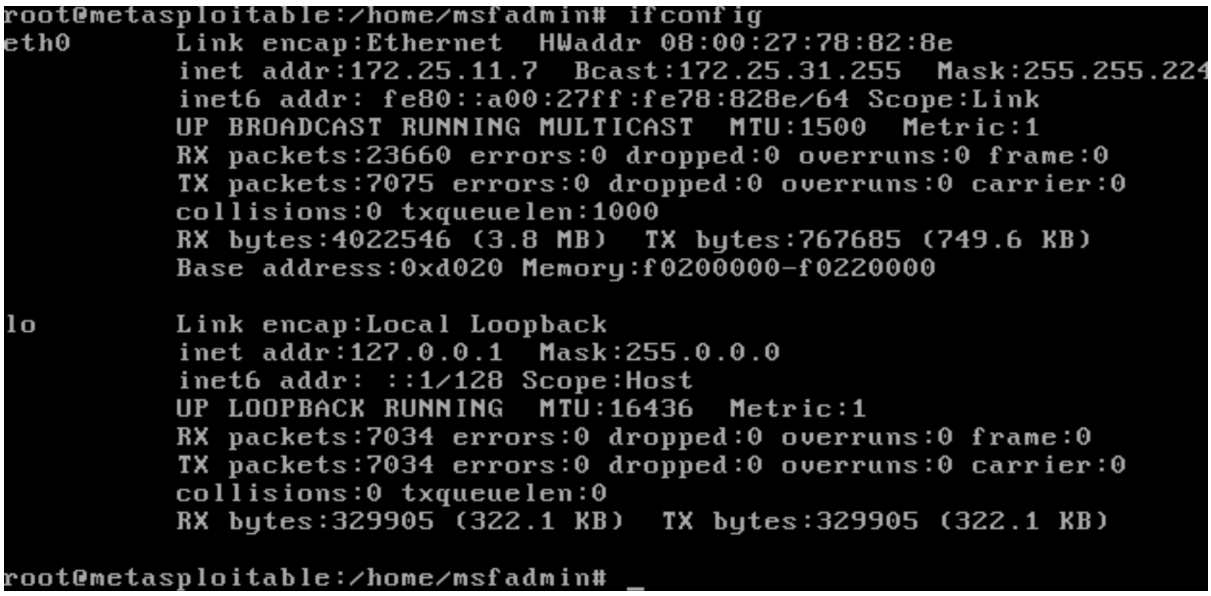
Profesor: Gustavo Higuera

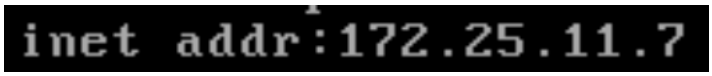
28/04/2023

Con base a los puertos abiertos encontrados en metasploitable, plantear un procedimiento y/o política que ayude a mitigar el riesgo

Desarrollo:

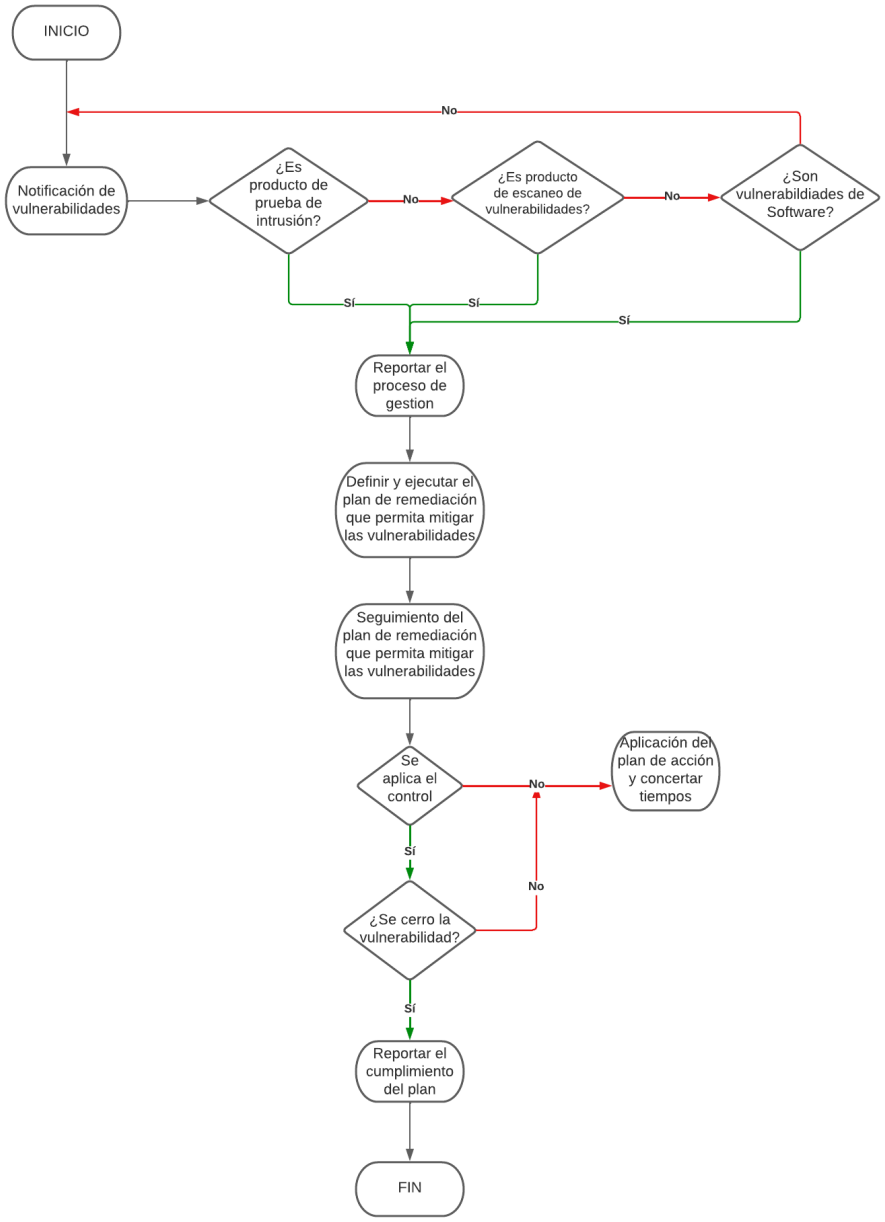
Se revisa la ip de la maquina con el comando ifconfig





Se revisan los puertos abiertos con nmap para la ip de metasploitable

Procedimiento para la gestión de vulnerabilidades



Política para la gestión de vulnerabilidades

1. DEFINICIÓN

   Esta política define los lineamientos para llevar a cabo el proceso de gestión de vulnerabilidades de la máquina virtual metasploitable, permitiéndonos analizar y pensar el proceso para evitar dichas vulnerabilidades

2. OBJETIVO

Obtener información de forma oportuna de las vulnerabilidades de la máquina virtual metasploitable que permita evaluar las medidas necesarias y mitigar riesgos detectados a través del procedimiento planteado.

3. ALCANCE

Este documento describe la manera como se debe mitigar las vulnerabilidades asociadas a metasploitable

4. ROL Y RESPONSABILIDAD

ROL	RESPONSABILIDAD
Encargado de la seguridad de la información	Controlar la aplicación de la política

5. POLÍTICA

Se deben definir roles y responsabilidades en la gestión de vulnerabilidades para el monitoreo periódico de las vulnerabilidades y la mitigación de las vulnerabilidades detectada

Se debe implementar firewall

Se debe implementar autenticación de usuarios y contraseñas seguras.