

## 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](mailto: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

```
root@metasploitable:/home/msfadmin# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:78:82:8e
          inet addr:172.25.11.7  Bcast:172.25.31.255  Mask:255.255.224
          inet6 addr: fe80::a00:27ff:fe78:828e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23660 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7075 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4022546 (3.8 MB)  TX bytes:767685 (749.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:7034 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7034 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:329905 (322.1 KB)  TX bytes:329905 (322.1 KB)

root@metasploitable:/home/msfadmin#
```

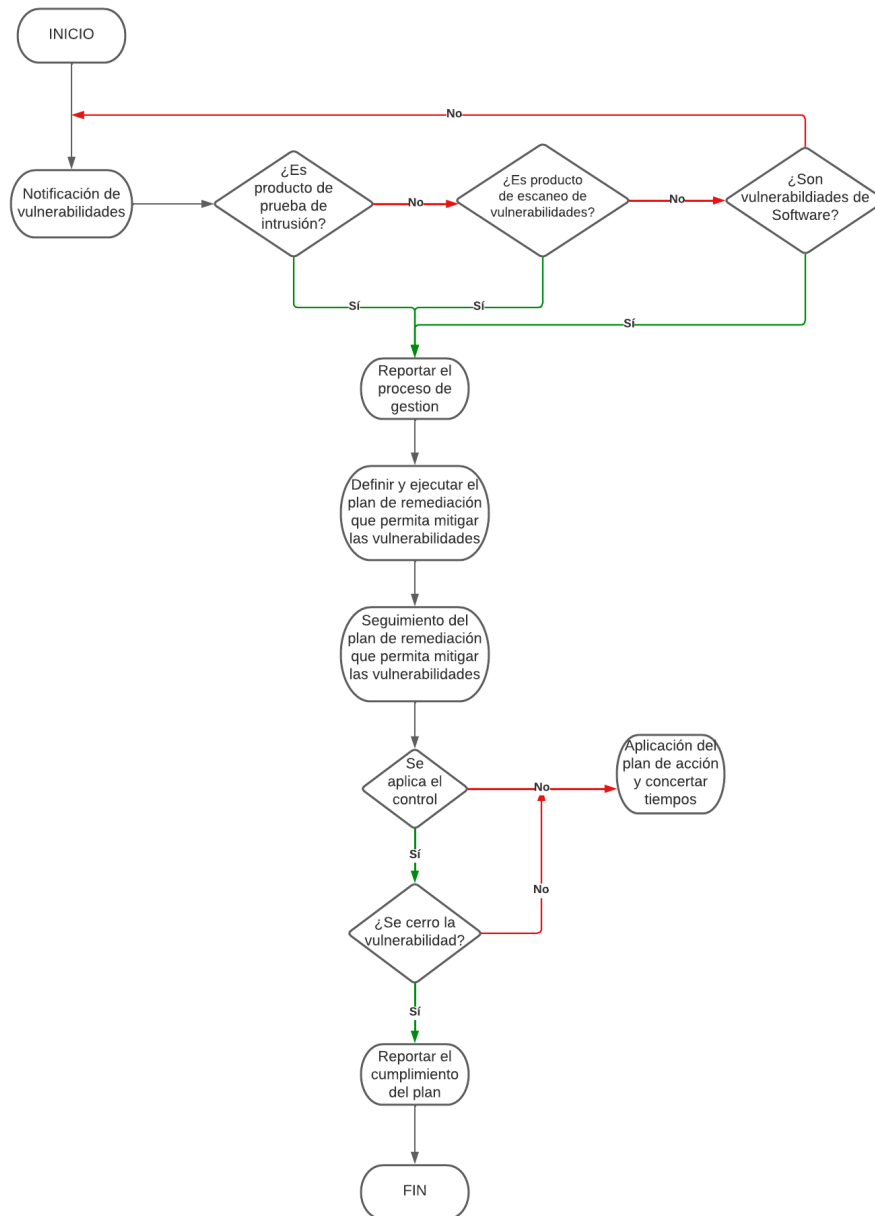
```
inet addr:172.25.11.7
```

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

```
nmap 172.25.11.7
```

```
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgres
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
```

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.