Escanear puertos con nmap

Carlos Vicent Arnau Chuquispuma

Spain-cs-pt-11

Índice

1. Objetivo de la auditoria

Se ha realizado una auditoria sobre la máquina virtual Metasploit con el fin de identificar los puertos que se encuentran abiertos, y los programas que se ejecutan a través de ellos.

2. Alcance de la auditoria

El 22 de enero del 2026 se han realizado acciones de pentesting, de la cual tenemos la siguiente información:

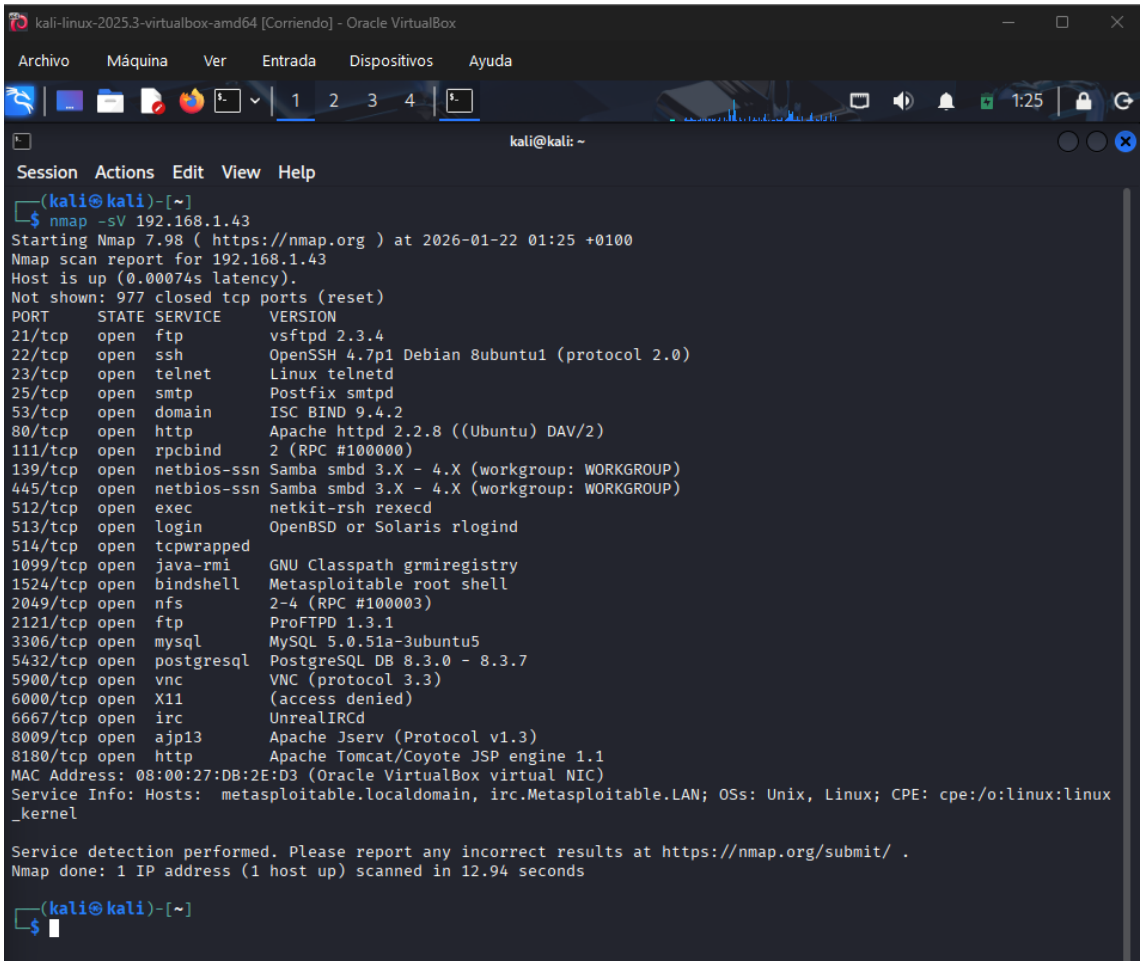
IP	192.168.1.43 (DHCP)
Usuario	msfadmin
Contraseña	Conocida por el equipo auditor

3. Herramientas y técnicas utilizadas

Se han utilizado la herramienta Nmap para realizar el escaneo de puertos.

4. Enumeración de puertos y servicios

`nmap -sV <IP >`



5. Documentar Vulnerabilidades Asociadas a los Servicios

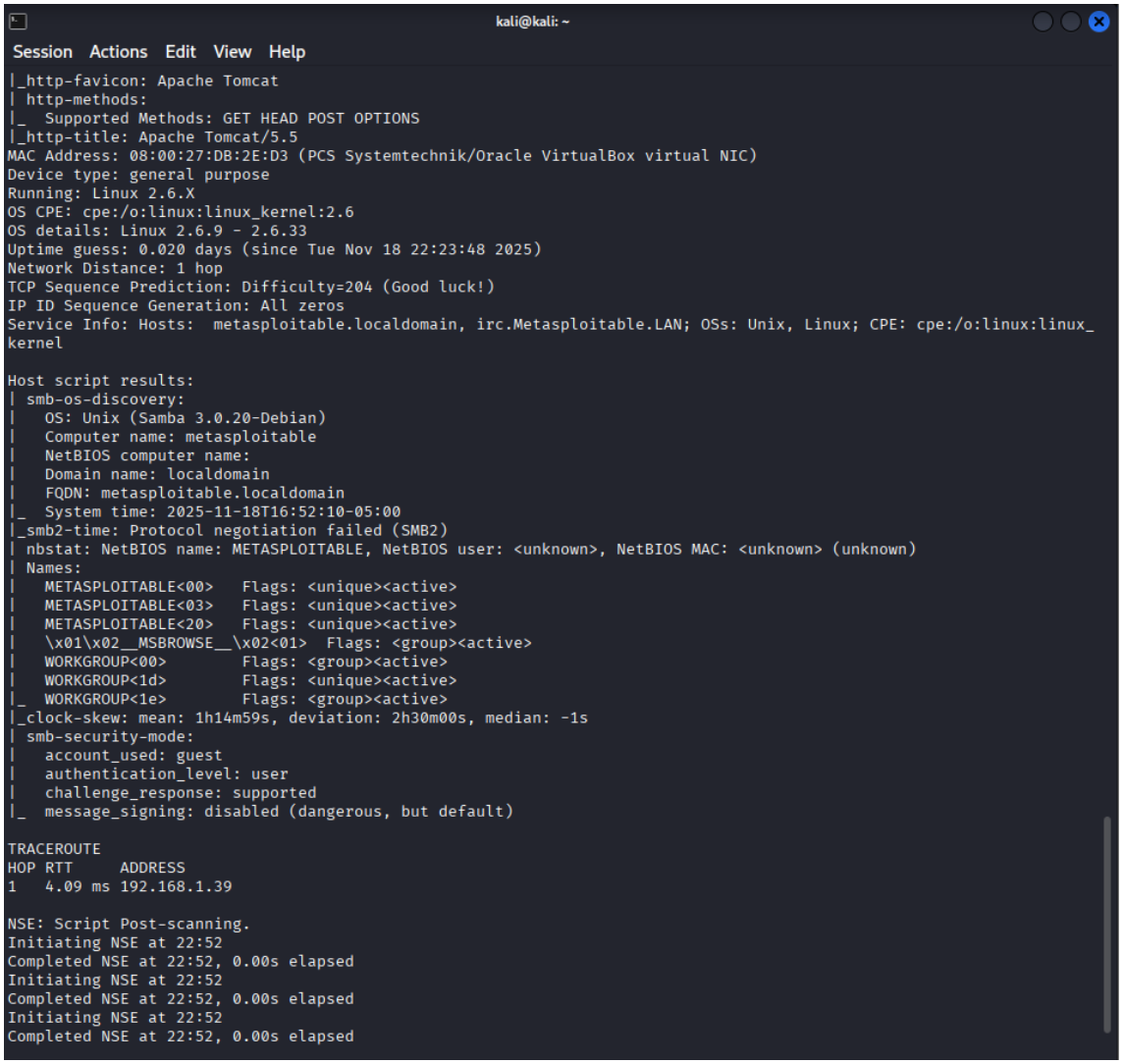
Se han encontrado varias vulnerabilidades. De las cuales se han seleccionado las siguientes:

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
21	FTP	Vsftpd 2.3.4	CVE-2011-2523	La versión instalada de vsftpd contiene una puerta trasera, que permite al atacante abrir una terminal de comandos en el puerto 6200. Lo que permite el acceso remoto sin necesidad de una autentificación adecuada.	Enlace
22	SSH	OpenSSH 4.7	CVE-2023-38408	OpenSSH presenta una vulnerabilidad en la función de reenvío del agente (ssh-agent). Si un usuario se conecta a un servidor malicioso con esta función activada, puede provocar que el atacante cargue módulos inseguros, permitiendo la ejecución de código en el equipo del usuario.	Enlace
80	HTTP	Apache 2.2.8	CVE2017-1001000	Esta versión de Apache contiene una vulnerabilidad en que permite a un atacante provocar un fallo en el servidor al manipular nombres de directorios de usuarios. Esto puede generar una denegación de servicio (DoS), haciendo que el servidor web deje de responder o se bloquee cuando procesa solicitudes especialmente diseñadas.	Enlace
3306	MYSQL	MySQL 5.0.51	CVE-2017-15945	MySQL tiene una vulnerabilidad que permite a un atacante ejecutar consultas especialmente manipuladas que pueden provocar un fallo en el servidor o una condición de denegación de servicio. Versiones antiguas como la 5.0.51 son especialmente sensibles, ya que no incluyen las protecciones actuales frente a consultas malformadas o	Enlace

				comportamiento inesperado en la gestión de datos.	

5.1. Sistema operativo del target

Se ha realizado el comando “nmap -A -v 192.168.1.39” para obtener información del target como el sistema operativo.



5.2. Vulnerabilidades reportadas del target

Se ha realizado el comando “nmap –script vuln 192.168.1.39” para obtener las vulnerabilidades reportadas del sistema.