Guía experimental - Taller Nº4 Explotación

*Taller de Hacking Ético – II Semestre – 2024*

*Prof. Marco Aravena, Ayudante Juan Larenas*

**Objetivo**: Utilizar Metasploit para la fase de explotación.

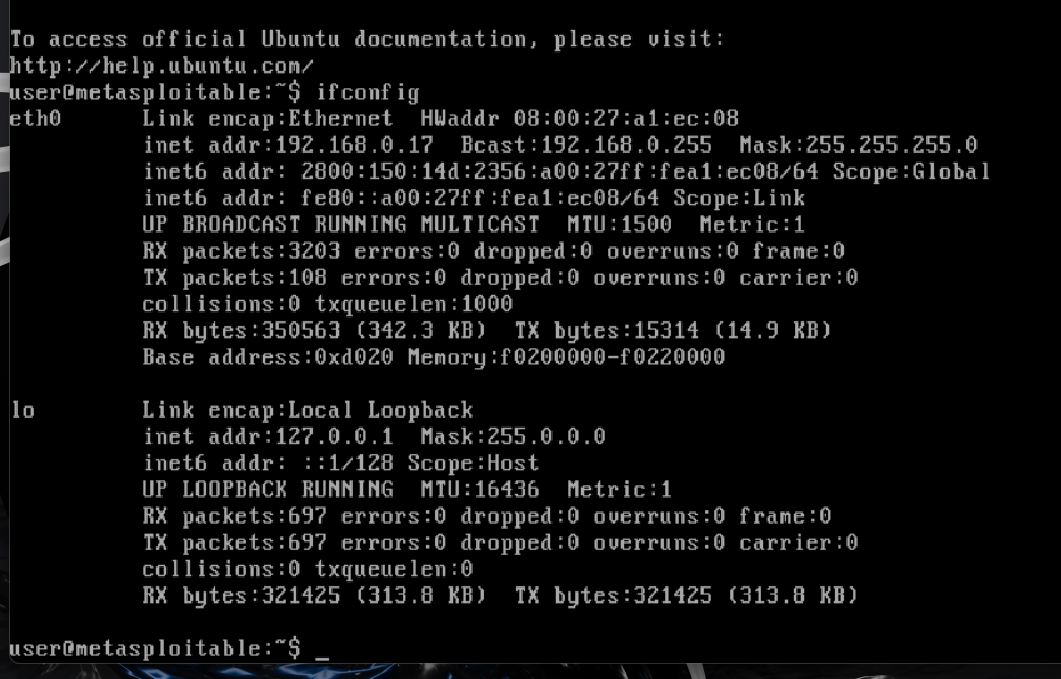
**Entregable**: Documento con captura de pantalla ilustrando lo solicitado en la sección actividades.

**Herramienta**: Máquina virtual KALI y servidor virtual Metasplotaible.

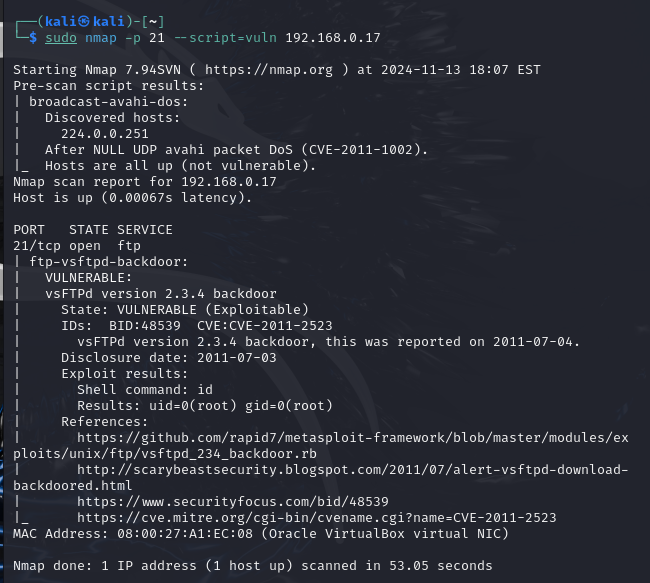
**Actividades**:

**1.- Explotación Servicio FTP en Metasplotaible**

1. Determine la IP de la máquina objetivo utilizando los comandos practicados en el taller anterior. Adjunte captura.



1. Ejecute un nmap con script para ver las vulnerabilidades del puerto 21. “nmap -p 21 –script=vuln IP\_objetivo”. Adjunte captura. (Se espera ver el nombre de la vulnerabilidad y su código cve en algunos casos)



1. Busque información sobre la vulnerabilidad en internet. Explique e indique que se puede llegar a hacer una vez explotada la vulnerabilidad respecto de las dimensiones de Confidencialidad, Integridad y Disponibilidad. Para ello revise en Internet en análisis del CVSS.
2. Ingrese a metasploit, para esto es necesario colocar en una consola nueva de KALI el comando “msfconsole”.
3. Ingrese en consola “help” para visualizar todas las opciones del software. Ejecute el comando “search” para buscar posibles exploit para la vulnerabilidad encontrada, para ello ejecute “search nombre\_servicio” en metasploit, para este caso el servicio es vsftpd. Aparecerá un listado con los exploit presentes en la base de datos de metasploit
4. Inicie la captura de paquetes con Wireshark.
5. En la consola ejecute “use nombre\_completo\_exploit” o “use numero\_en\_el\_listado”
6. Ingrese en consola “show options”. ¿Qué significa este comando? (Se espera que se muestre una tabla con las opciones del exploit).
7. Ingrese en consola “set RHOST IP\_objetivo” y luego otra vez “show options” para confirmar que se cambió.
8. Comience la captura de paquetes con Wireshark.
9. Ejecute “run” en la consola de metasploit
10. Una vez que el exploit tenga éxito ingrese el comando “ls”. Adjunte captura. ¿Qué es lo que se muestra? ¿Qué es lo que ocurrió?
11. ¿Qué es lo que se muestra en Wireshark? ¿Se verifica lo indicado sobre el puerto 6200 en la documentación del exploit?