

## **Explotación del Servicio ftp del puerto 21.**

Escaneo de la ip víctima.

Escaneo del puerto 21. Vemos el servicio y versión. ( ftp

vsftpd 2.3.4 )

Ejecutamos nmap -p 21 --script vuln y así obtenemos información de las vulnerabilidades del puerto.

Nos da un CVE, lo buscamos en CVE.mitre.org y nos dice que: contiene una puerta trasera que abre

un shell en el puerto 6200/tcp.

Desde msf buscamos la versión (vsftpd) y nos arroja como resultado un exploit

Ingresamos la ip y puerto víctima.

Buscamos el payload con el comando: show payload.

Lo separamos y ya podemos correr el comando exploit.

Conseguimos una sesión abierta a metasploitable.