Explotación del Servicio samba del puerto 445.

Escaneo de la ip víctima.

Escaneo del puerto 445. Y vemos el servicio y versión. (samba netbios-ssn Samba smbd 3.X - 4.X)

Desde msf ejecutar el: auxiliary/scanner/smb/smb_version

Ingresamos la ip victima.

Búsqueda de vulnerabilidades en Google, foros, blogs, etc.

Cve encontrado 2007-2447

Ingresamos la búsqueda del cve por msf.

Consigimos el exploit, seteo la IP y el puerto destino.

Buscamos el payload desde msf.

Lo sesteamos y ya podemos correr el comando exploit

Inicia sesión desde nuestro servidor a metasploitable.