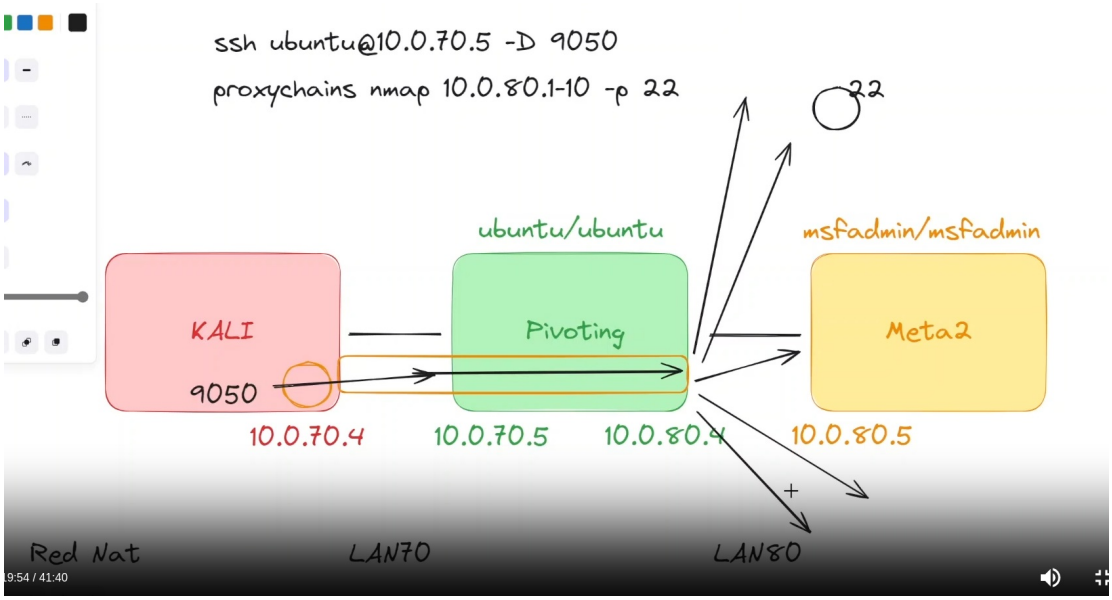
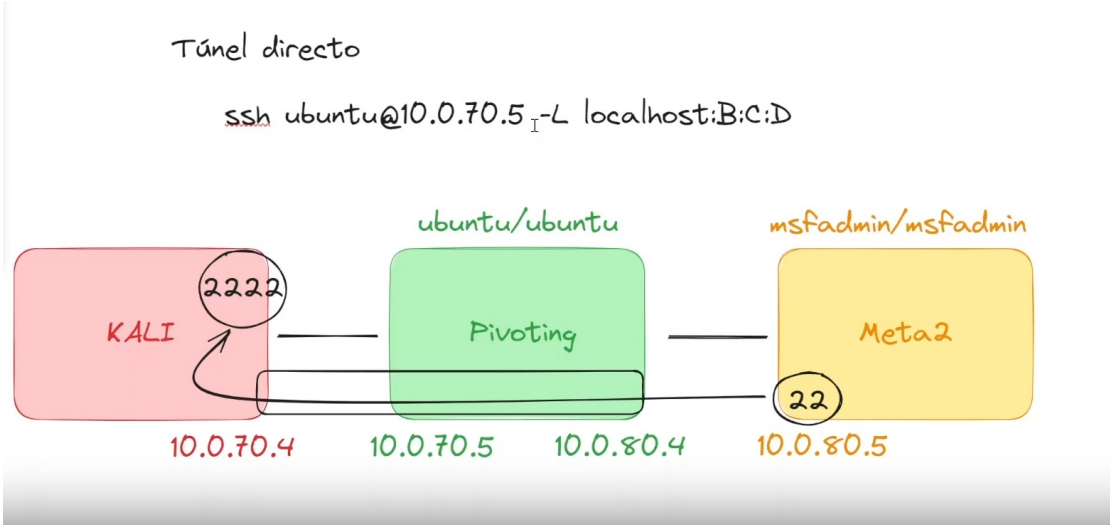
TUNELING A TRAVES DE SSH

1. ***Tunel dinámico.-*** Para descubrir host desconocidos a partir del otro lado de *pivoting:*



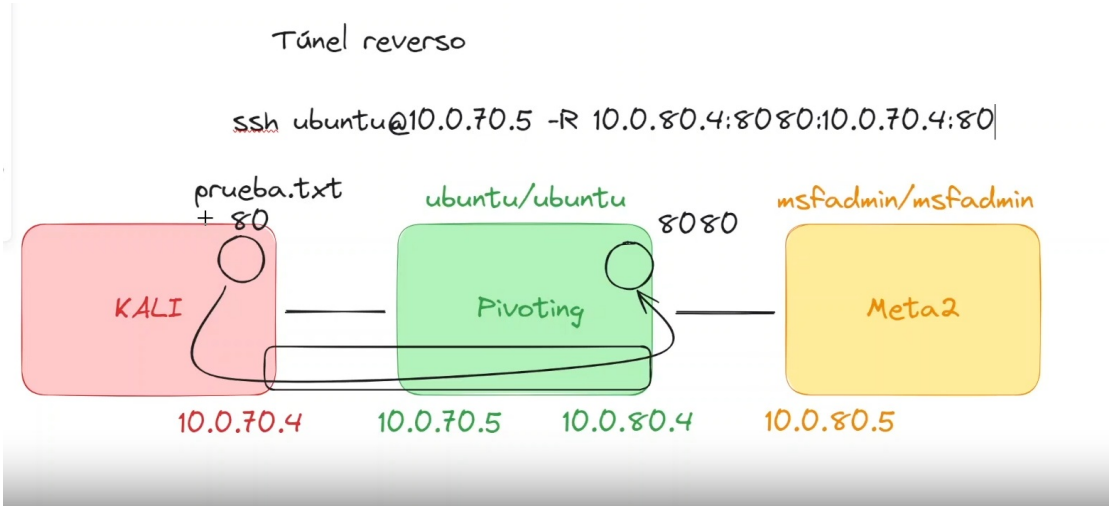
2. ***Tunel directo o local.-*** Para conseguir un *movimiento lateral* y poder conectarnos desde nuestra kali al nuevo host descubieerto (meta 2)



Localhost no es necesario ponerlo, se omite en caso de tuneles locales

A:B: Localhost:Port new1 C:D: IPdesde donde enrutamos el trafico:Port new2
Finalmente nos conectamos mediante SSH a traves de este tunel a la IP de meta2.

3. ***Tunel reverso o remoto.-*** Aqui conseguimos lo contrario que hemos visto hasta ahora, ya que a través de este tunel podremos alcanzar un servicio o un archivo que este en la kali y llevarlo a la maquina meta 2, usando el metodo servidor python: wget.



- Aqui no se establece localhost sino la IP real de KAli, pq la conexion no se produciria ya que localhost no tendría el puerto abierto.

A.B.C.D.- se empieza desde atras, desde la primera IP que ve meta2 hasta llegar a la mauqina donde esta el recurso (Kali).

TUNELING AVANZADO