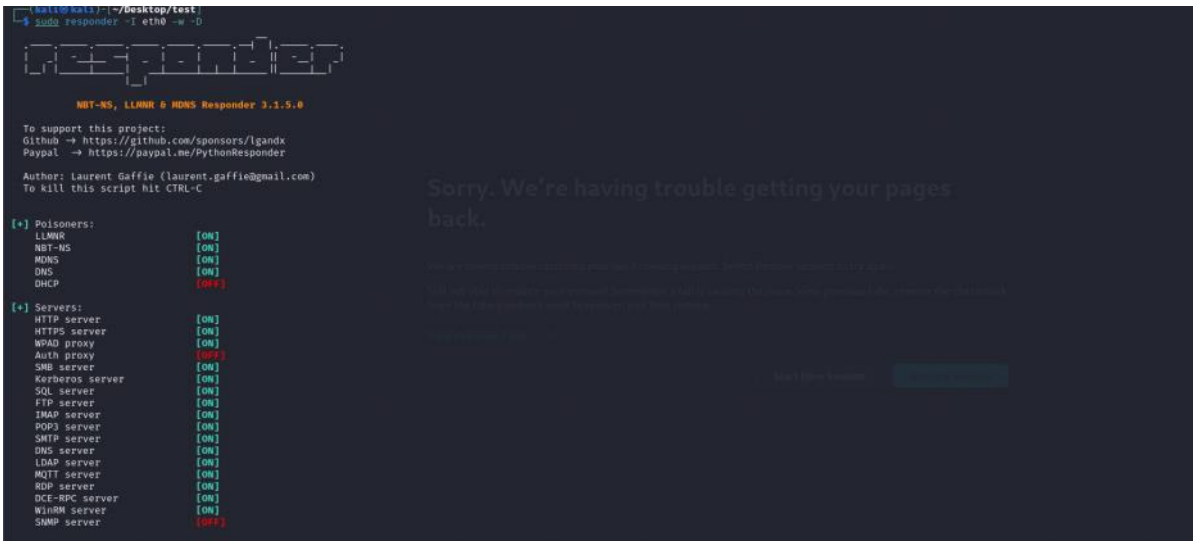
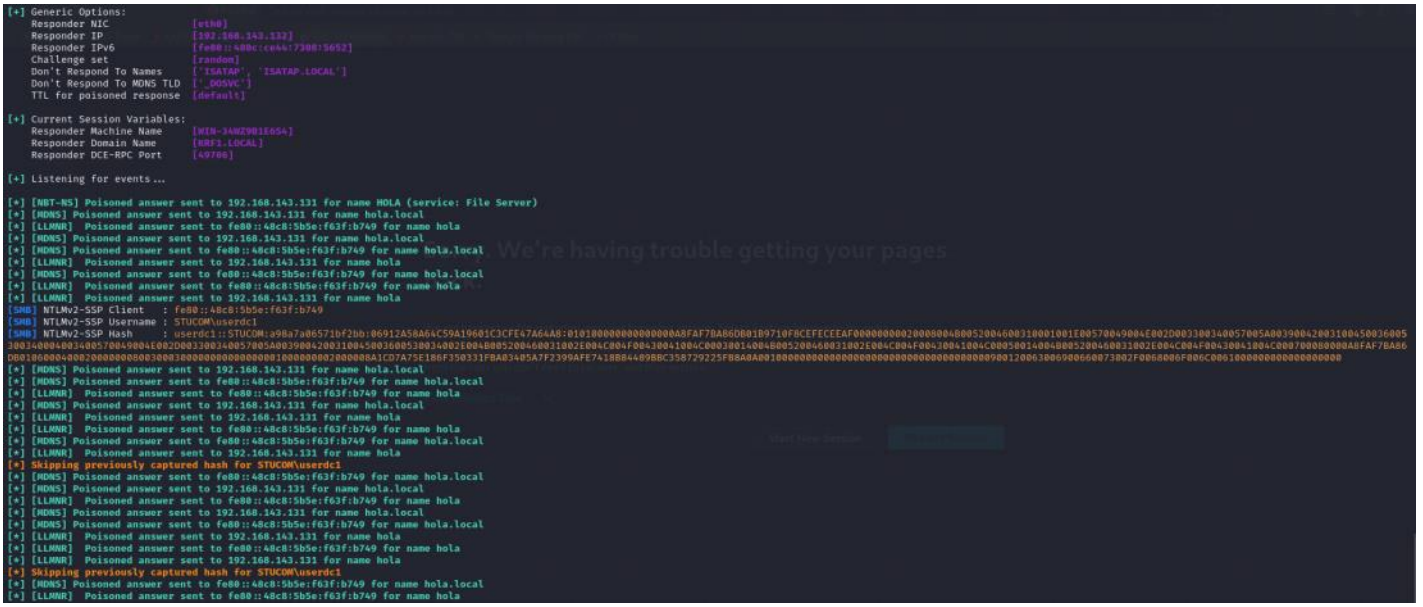
Responder

lunes, 24 de febrero de 2025 18:53

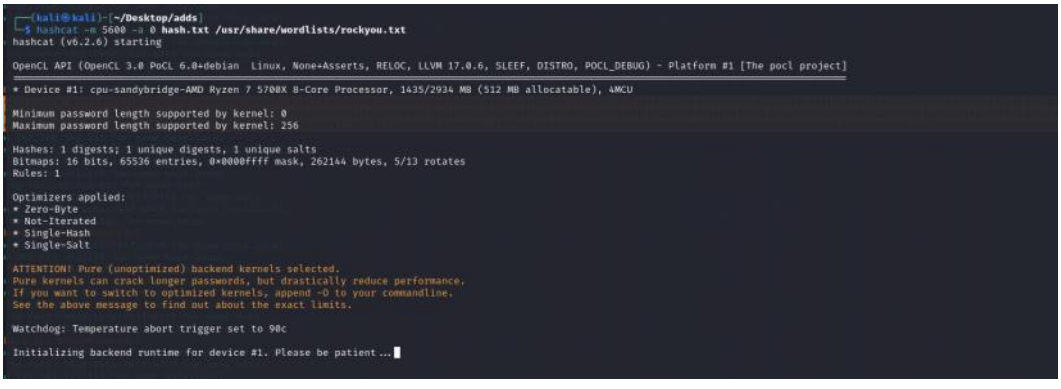
Primero de todo nos pondremos a escuchar con el responder a través de la interfaz eth0 para capturar algún hash ntlm

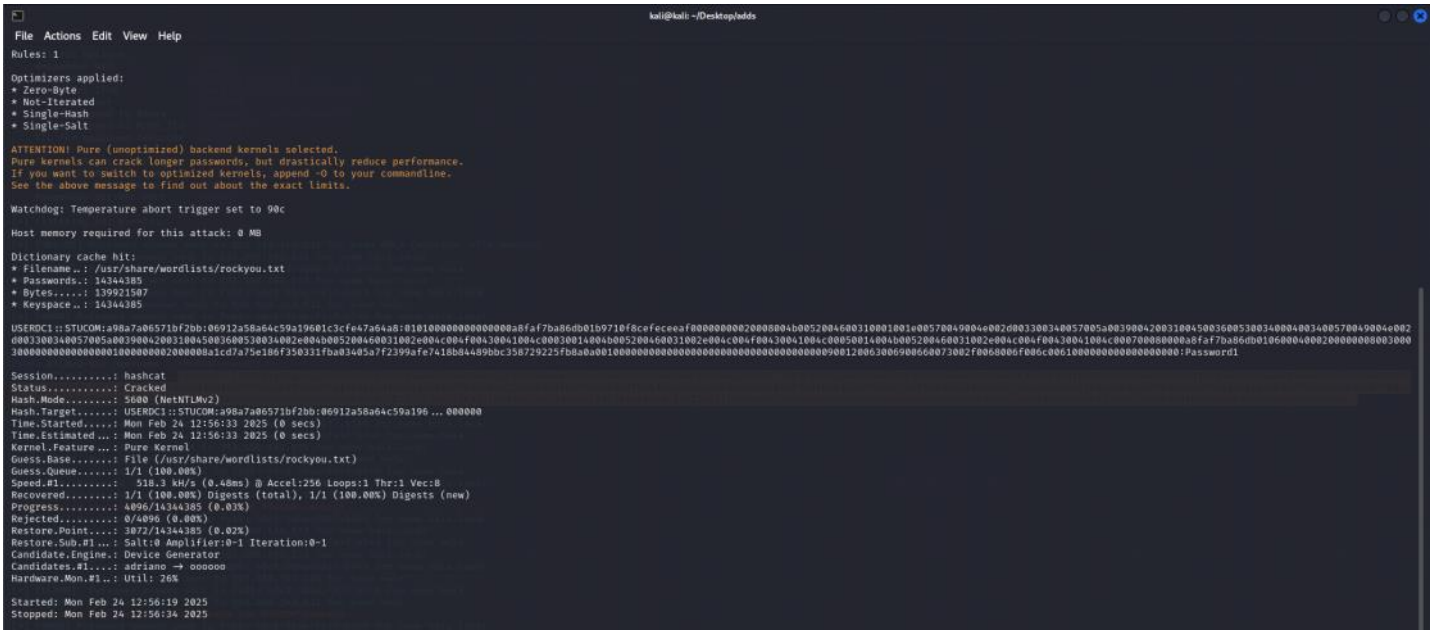


Luego generamos una conexión hacia \\hola desde el cliente windows para simular una conexión por SMB.



Como vemos en la imagen el responder captura el hash ntlmv2, hash que podemos crackear como veremos a continuación usando hashcat:





El password del userdc1 es Password1.