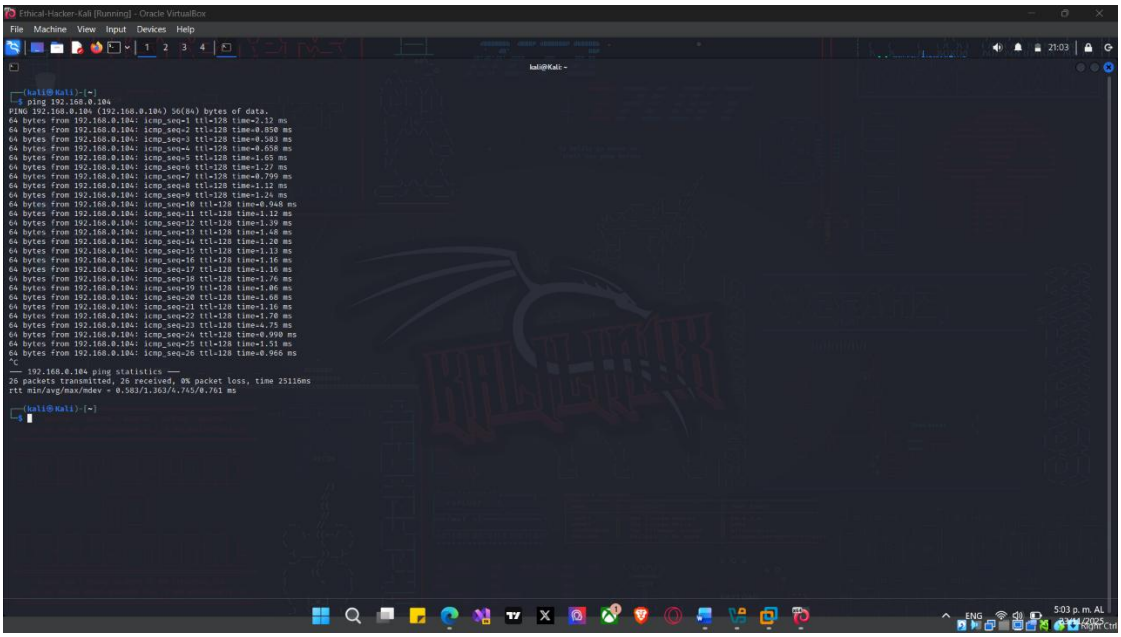
Proyecto Final Hacking Ético

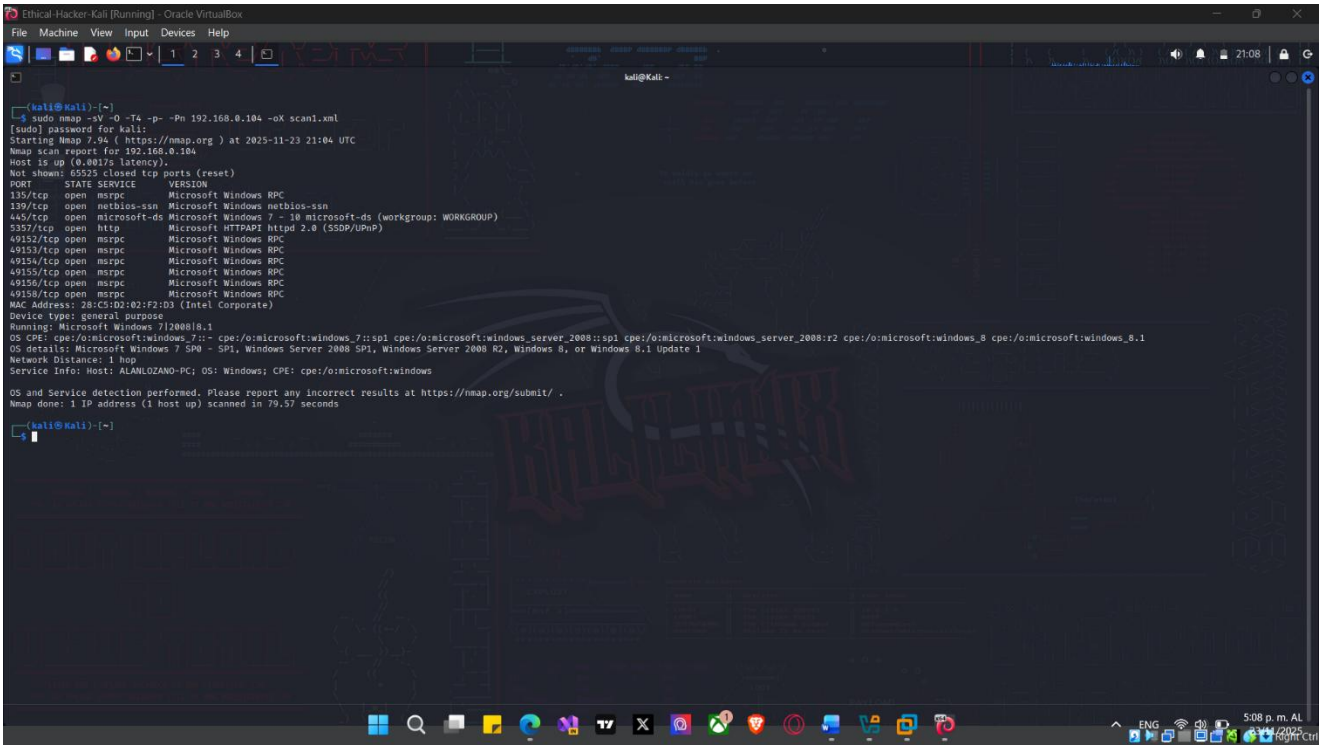
Cada sección vale 10 puntos, para un total de 30 puntos.

Requisito: para los siguientes puntos debe crear una máquina virtual de windows 7 o windows server 2008 la cual llamaremos víctima.

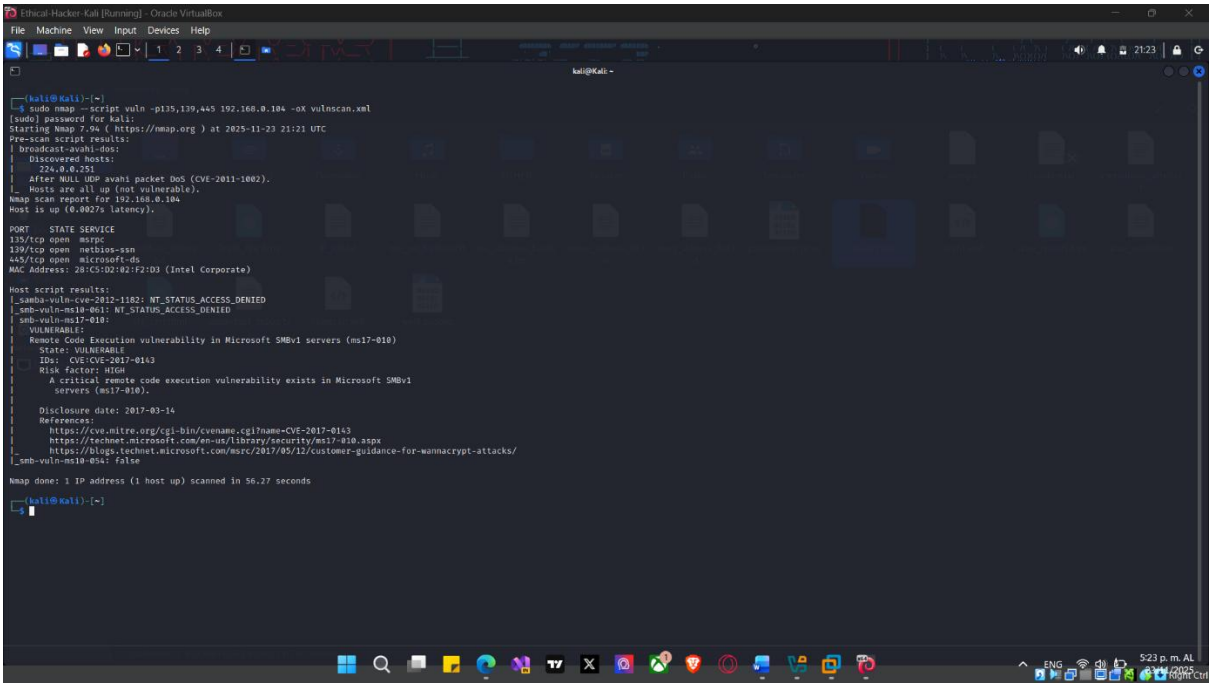
1. **Ataque de reconocimiento a la víctima.**



1.a Utilice nmap y haga un escaneo de puertos y de servicio solo a la ip de la víctima. Identifique cuáles puertos tiene abierto, el sistema sistema operativo, si no le muestra estas informaciones ajuste las opciones de nmap para que le muestre la información solicitada. Exporte el resultado a html y súbalo junto con este documento.

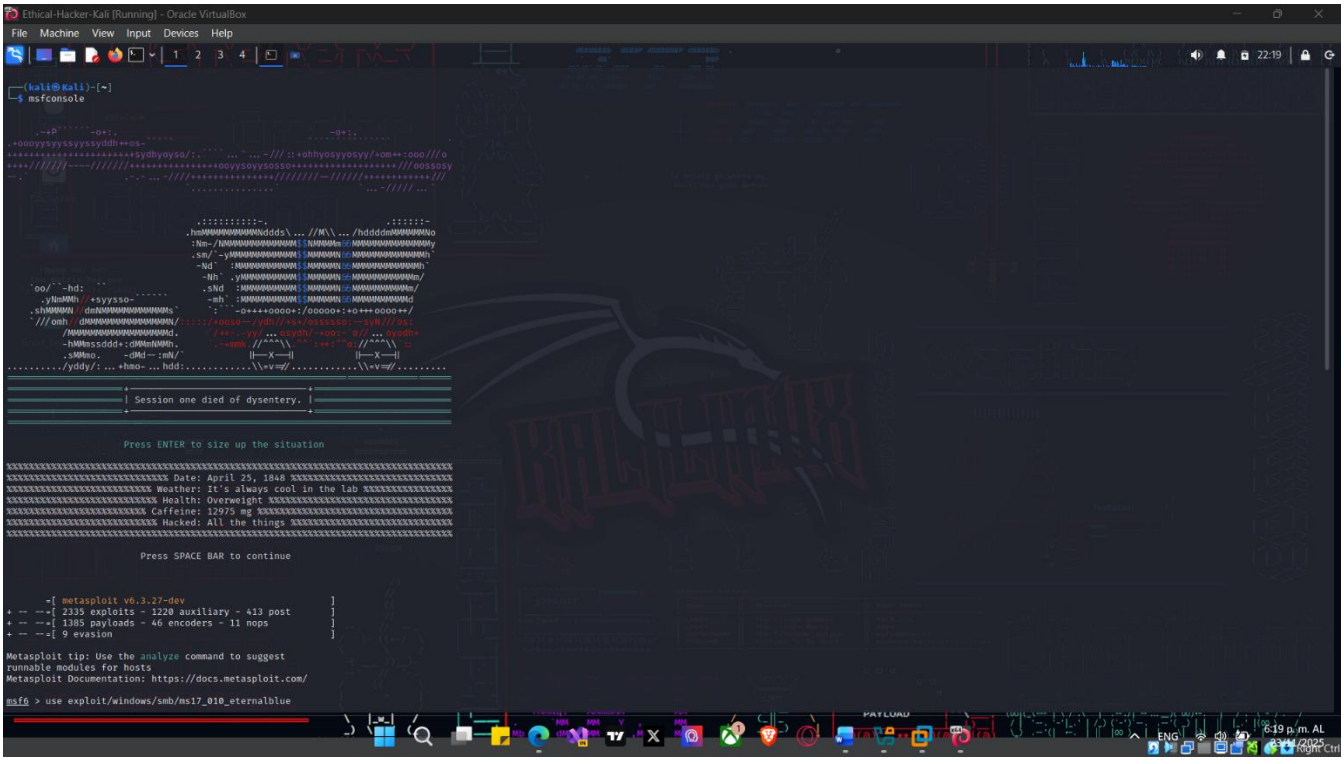


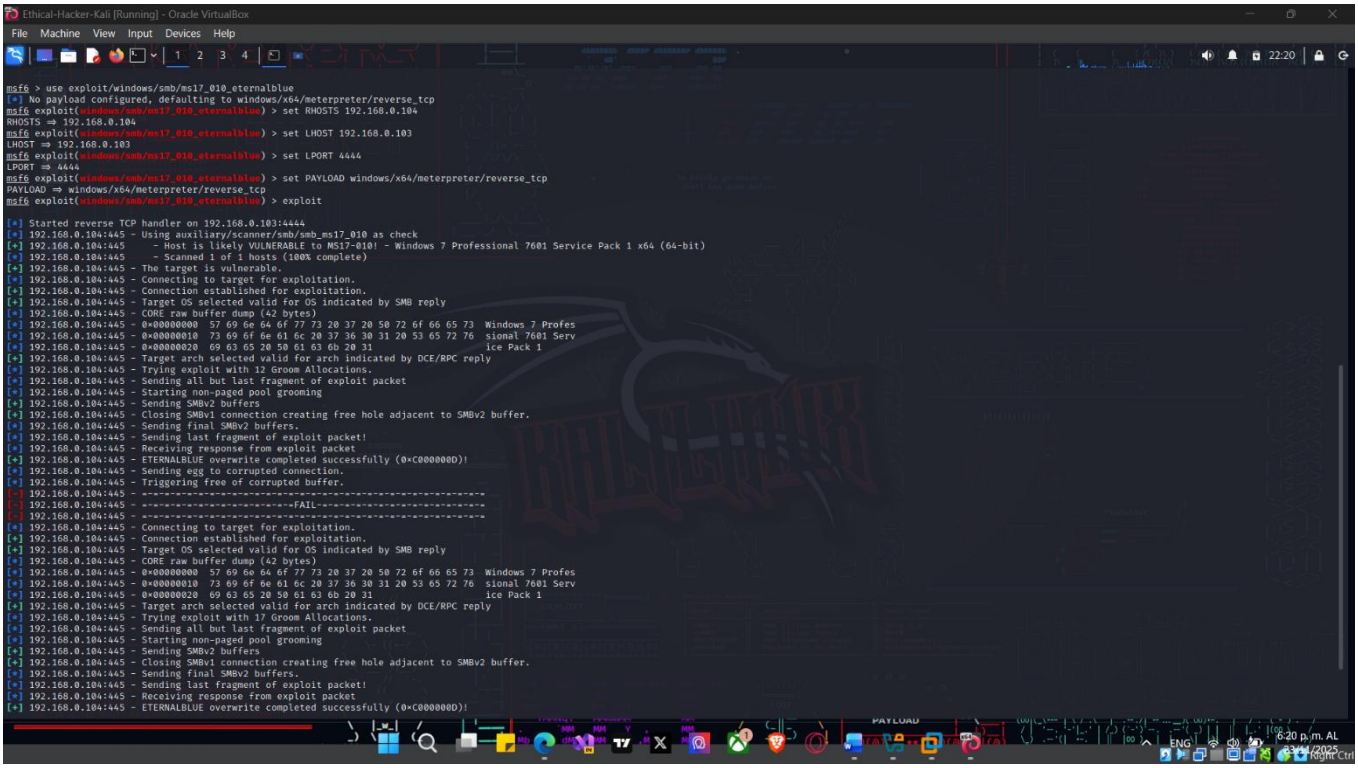
1.b Vuelva a ejecutar nmap utilizando los scripts de vulnerabilidades. Identifique las vulnerabilidades encontradas. Verifique si entre las vulnerabilidades está la de eternalblue (es posible que salga con otro nombre, favor investigar). Exporte el resultado a html y súbalo junto con este documento.



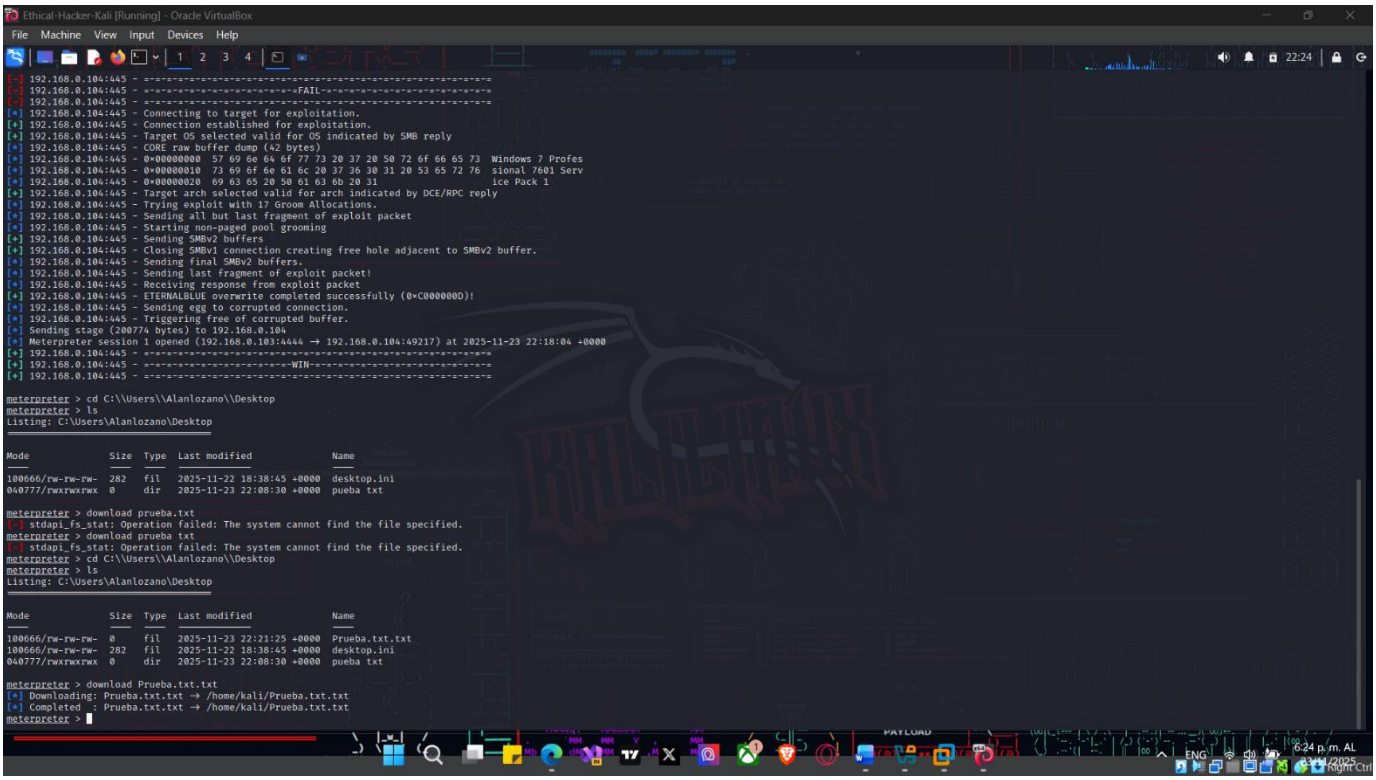
2. Realizar el ataque de penetración con eternalblue a la víctima.

2.a Tener acceso por terminal a la máquina virtual víctima mediante el ataque eternalblue. Debe investigar cómo hacerlo.

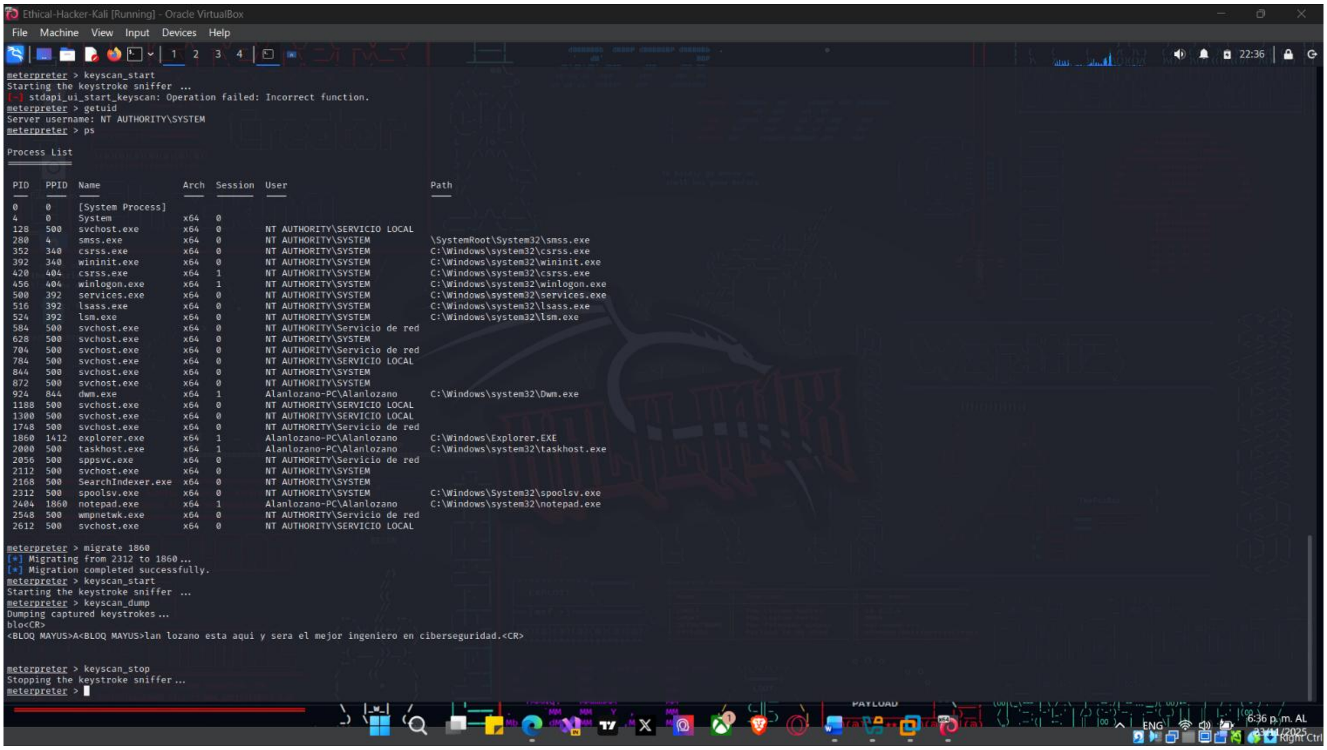




2.b Copiar un archivo de prueba ubicado en el escritorio del usuario de la víctima.



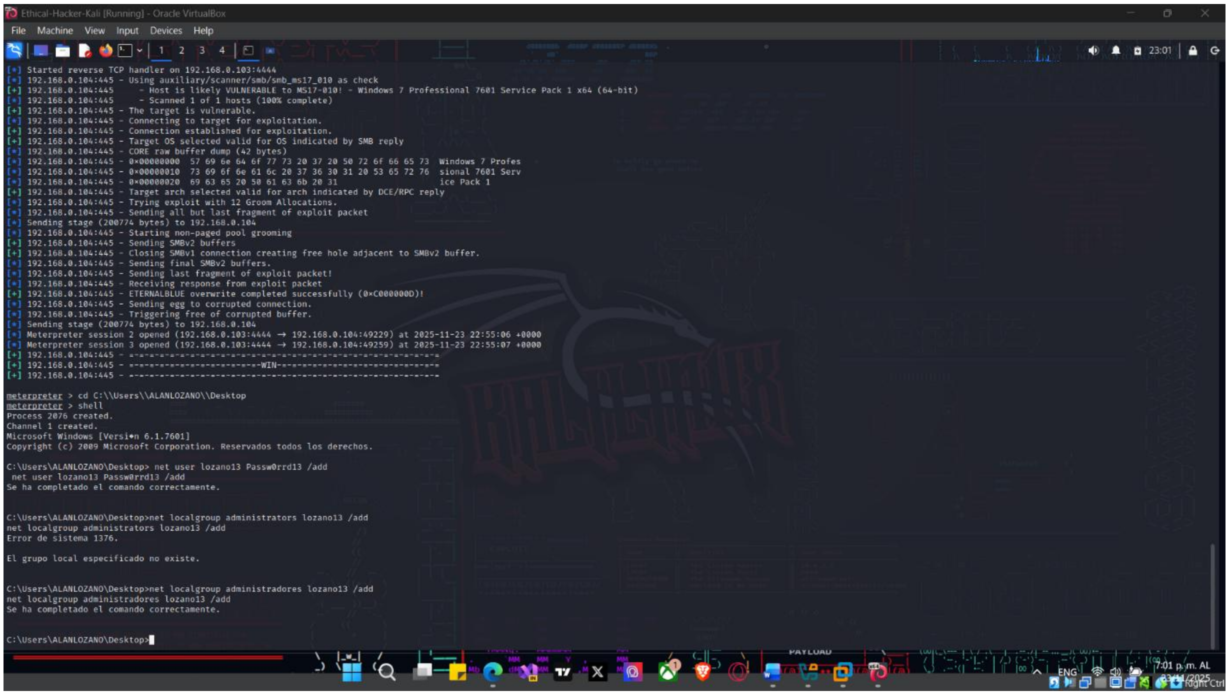
2.c Capturar un texto escrito por la víctima.



3. Mantener el acceso (post-explotación).

Nota: si usted reinicia la víctima se dará cuenta que se pierde la conexión realizada en el ataque del punto dos. Para evitar esto debe crear una puerta trasera (backdoor) persistente.

3.a Investigar e implementar un mecanismo de persistencia. Esto podría ser la creación de un nuevo usuario con privilegios de administrador, o la configuración de un payload de Metasploit (como un meterpreter) que se inicie automáticamente con el sistema.



3.b Entre a la víctima de manera normal, busque evidencias de lo realizado en el punto 3.a, ejemplo: tome capturas de pantalla que demuestren que se creó el usuario nuevo o que hay un puerto abierto y un programa que se ejecuta cada vez que inicia windows.