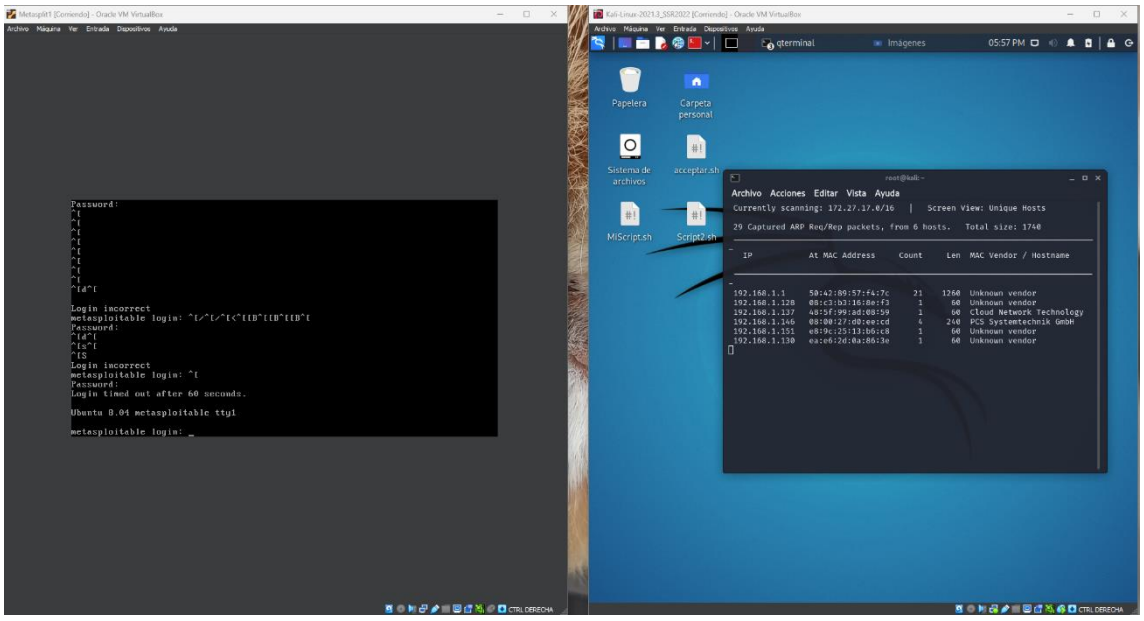
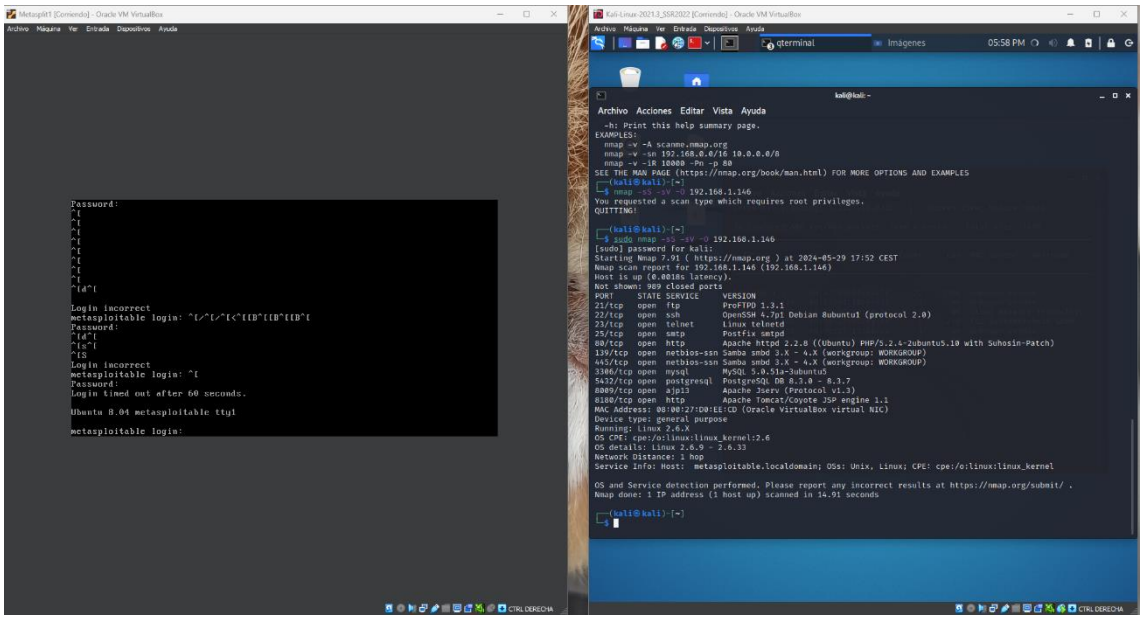
RETO 1 SEGURIDAD EN SISTEMAS Y REDES

CIM31-G11

Descripción del Proceso

Para la realización de la búsqueda de vulnerabilidades y su explotación en primer lugar se procede a la búsqueda de la máquina disponible en la red. Una vez encontrada la máquina con la que se va a desarrollar todo, se procede a buscar los puertos abiertos en esta.



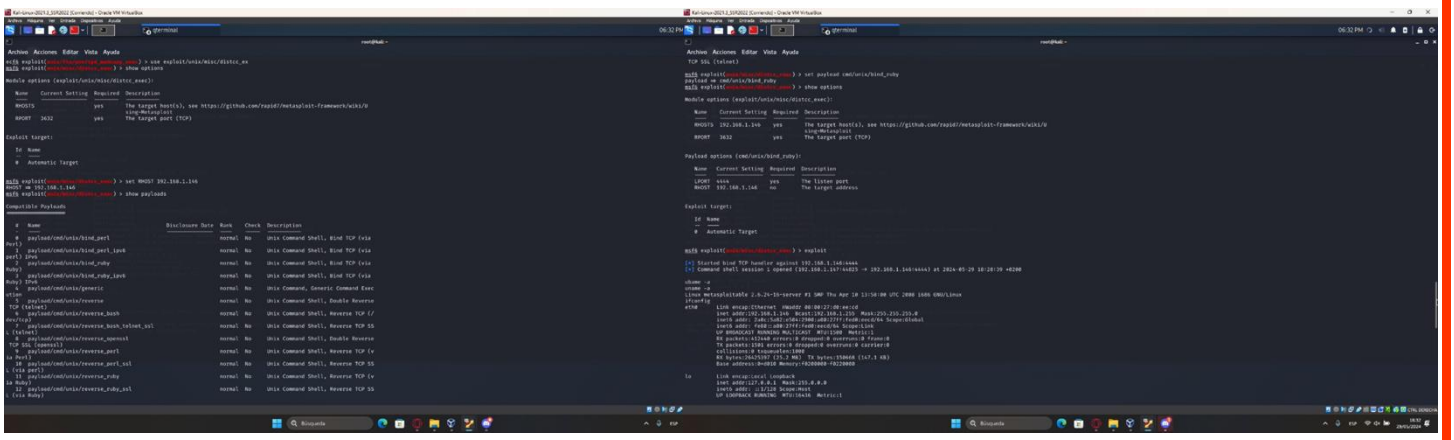


En este caso, Metasploitable tiene varios servicios vulnerables a los cuales se les puede buscar su explotación. Se pone de ejemplo los puertos siguientes:

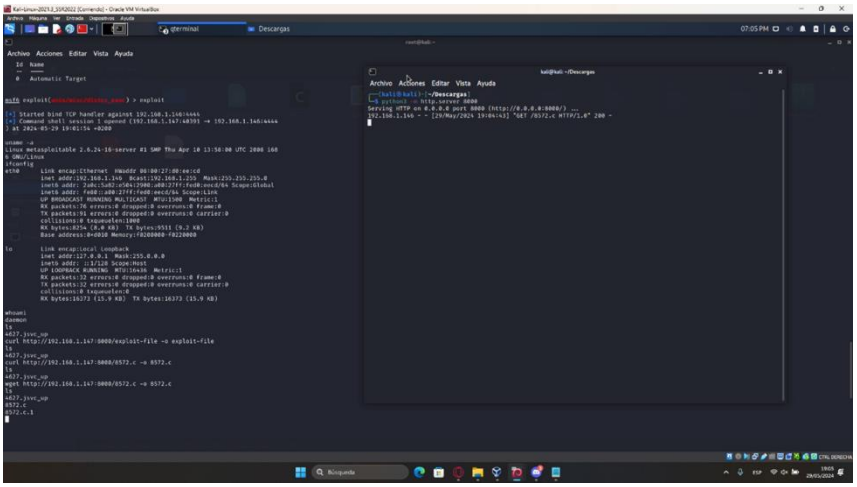
- Puerto 21 (FTP).- Permite acceso anónimo con el usuario anonymous.
- Puerto 23 (Telnet).- Permite el acceso con las credenciales msfadmin (usuario y contraseña).
- Puerto 80 (servicios web).- Navega hacia http://192.168.1.146/, explorando las aplicaciones disponibles.

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez

Una vez vistos los puertos, se selecciona el exploit que se va a utilizar para generar el ataque correspondiente a la máquina. Cuando este haya sido seleccionado, se puede ver cómo se ejecute y que el exploit da acceso a la máquina que está siendo atacada en ese momento.

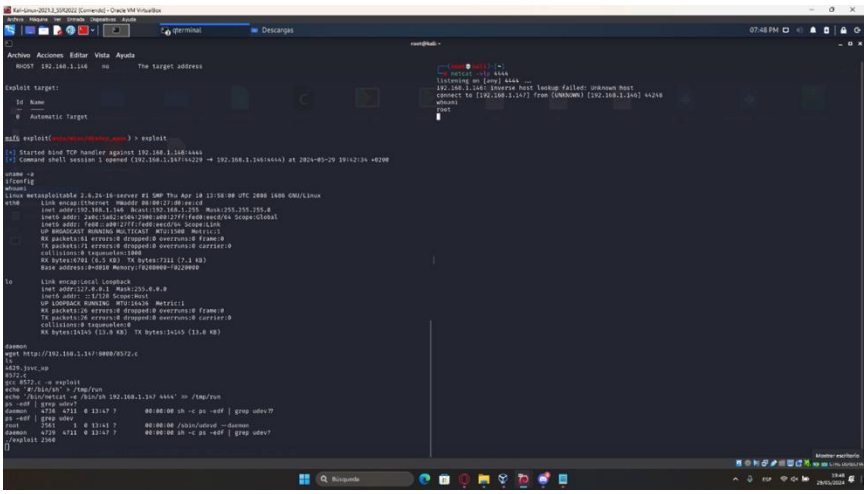


Sin embargo, hubo un inconveniente: no dejaba usar el comando wget. A continuación, se abrió un puerto de la máquina Kali para poder descargarlo desde la otra máquina usando el exploit, tal y como se ve en la próxima captura.

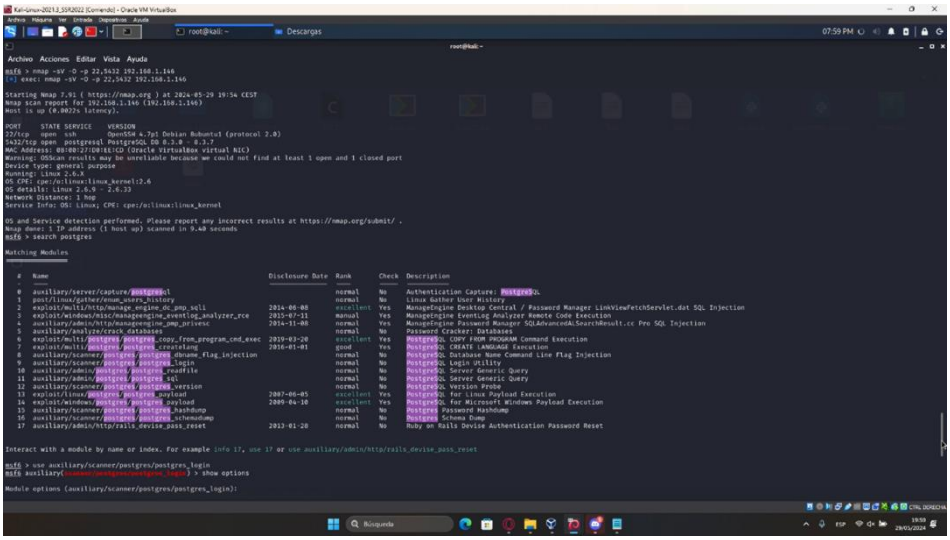


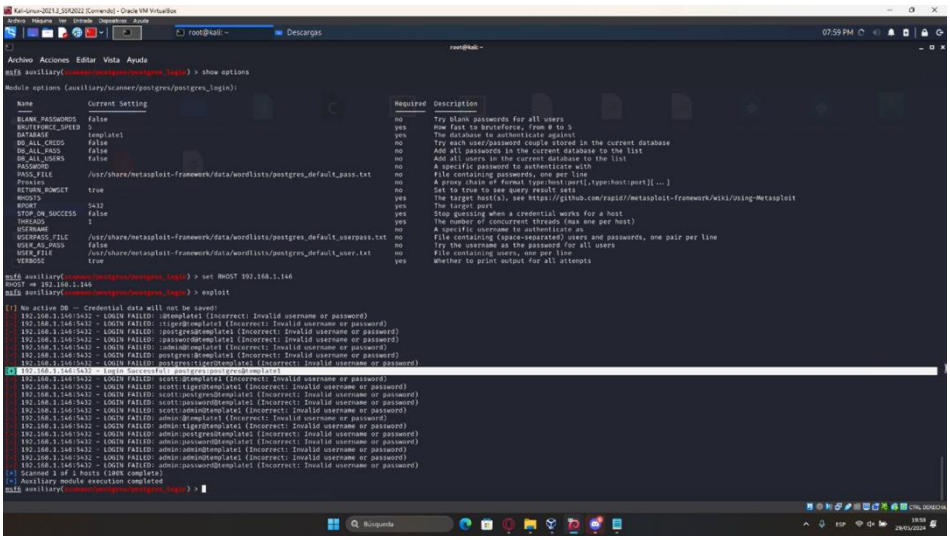
Por otro lado surgió otro inconveniente, ya que a la máquina Kali no se le podían dar permisos. Tras varios intentos sin éxito y gracias a los bajado anteriormente en la web con el exploit, el comando wget logró funcionar tal y como se puede apreciar a continuación:

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez



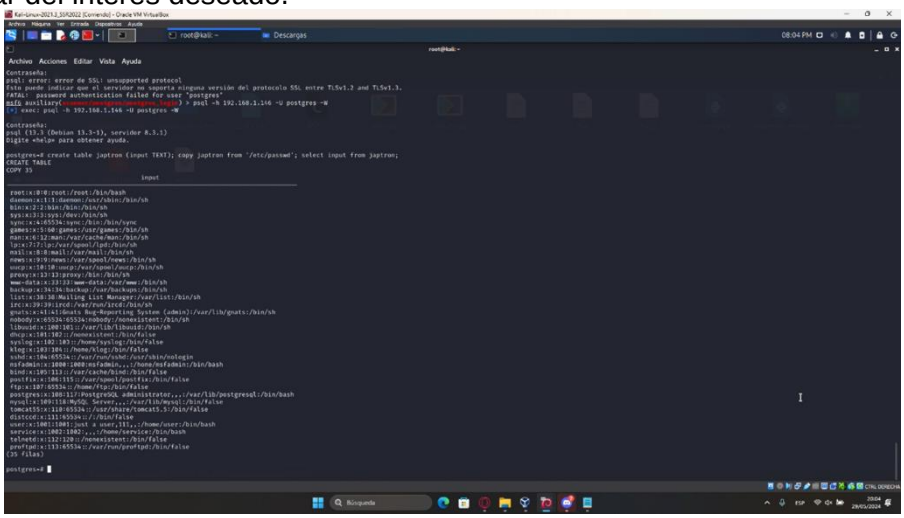
Después con el uso del exploit este se selecciona y posteriormente se consigue ejecutar con éxito, dando como resultado el nombre de usuario y la contraseña de la máquina que ha sido atacada.



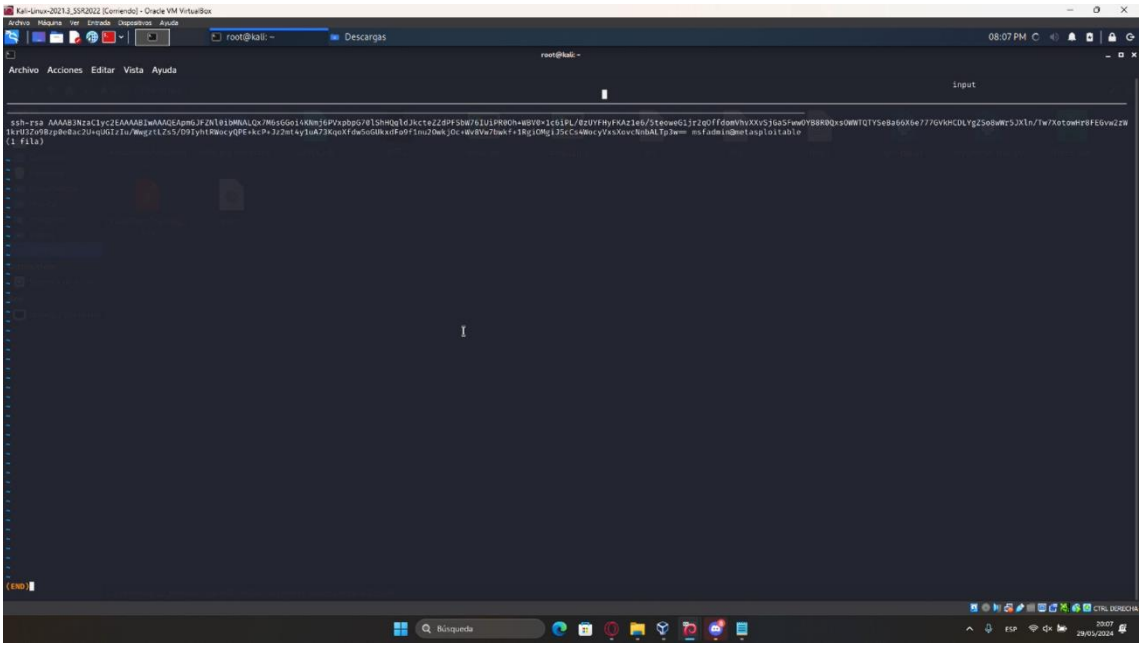


Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez

Posteriormente, se crea una tabla, la cual almacena datos del archivo /etc/passwd. De forma rápida explicada, se crea la tabla con una columna de tipo TEXT, copia los datos del archivo anterior a la nueva tabla y muestra todos esos datos. El archivo etc/passwd contiene información sobre los usuarios de todo el sistema, migrando todos esos datos a un lugar del interés deseado.

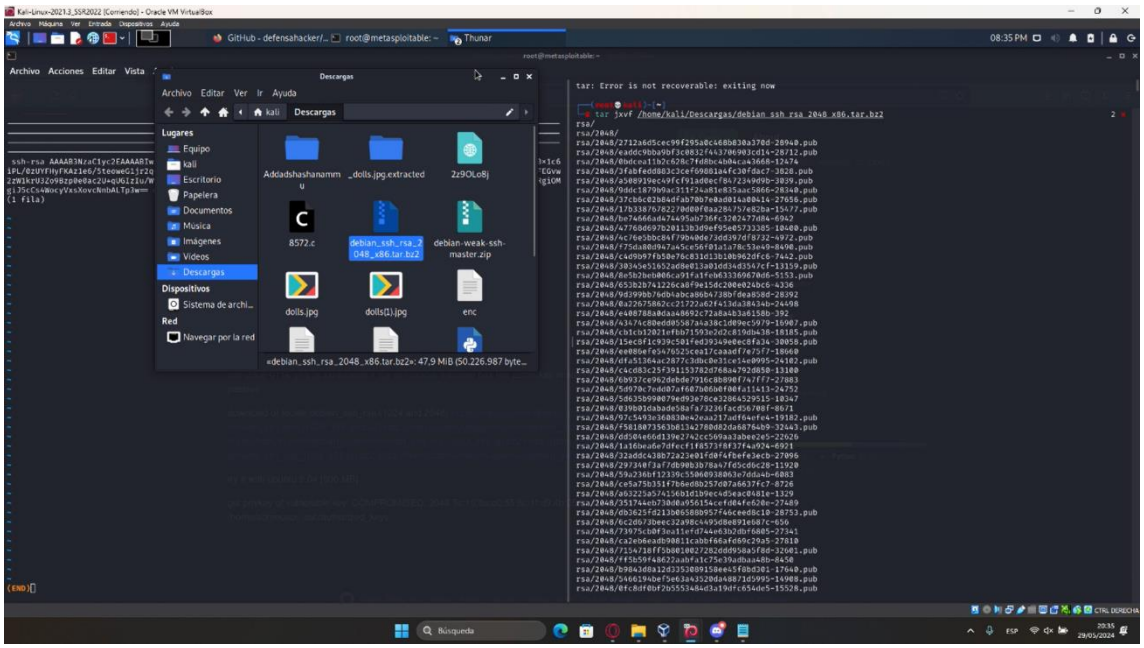


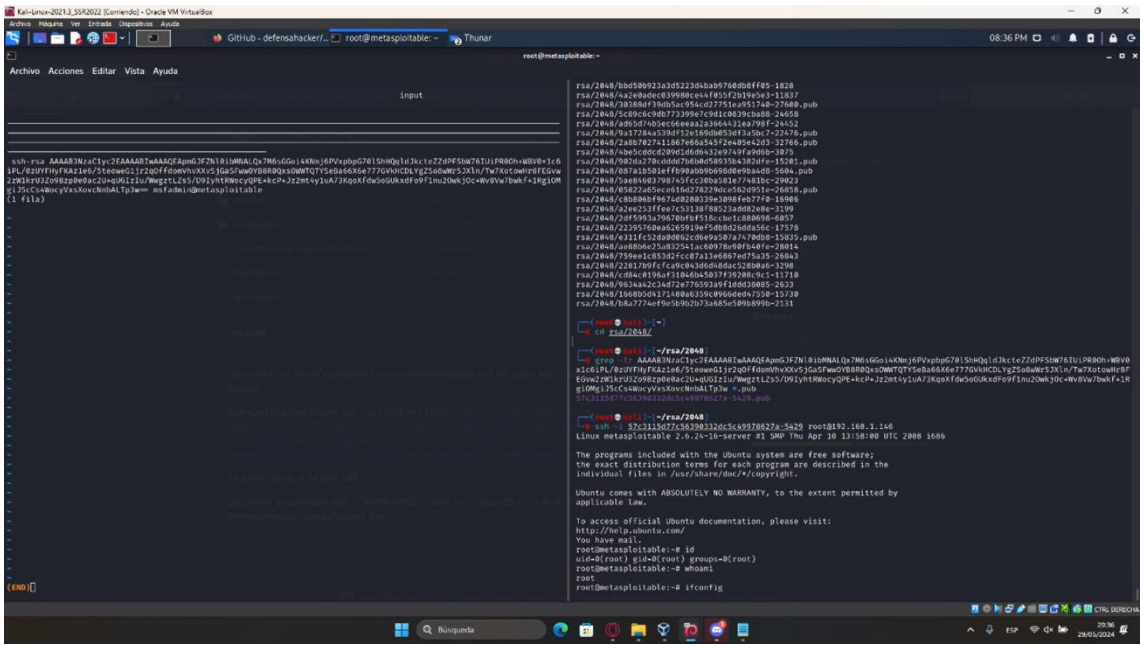
Luego se vuelve a crear una tabla más, en este caso mostrará nítidamente la clave ssh del administrador.



La imagen anterior es el resultado de ejecutar el comando create table sshkey (input TEXT); copy sshkey from '/root/.ssh/autorized_keys'; select input from sshkey;

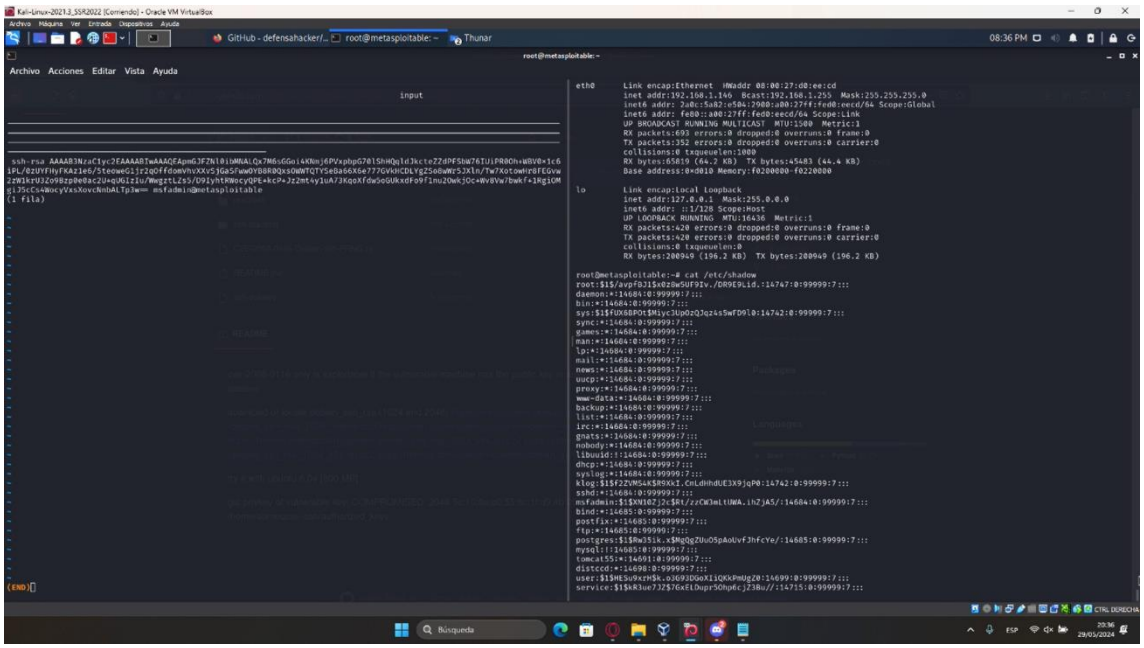
Descargamos un programa para descifrar claves cifradas para así posteriormente descifrar la clave de administrador y tener los accesos de este (esto es acceso a todo lo que puede tener el administrador).





Por último, se accede a las carpetas con todas las contraseñas cifradas a las que solo puede acceder el administrador, pero como se tienen los permisos de este las carpetas son accesibles, demostrando que el ataque se ha ejecutado con éxito y demostrando las debilidades de la máquina.

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez



Conclusiones

Con todo esto se puede apreciar cómo la máquina tiene las vulnerabilidades de dos de los exploits, ya que se ha conseguido finalmente atacar la máquina Kali y que se pueda navegar con los permisos de administrador sin ningún problema.

Diego Espinosa, Manuel Neto, Lucía González y Paul Rodríguez