GUÍA TÉCNICA PRÁCTICAS INSTRUCTOR

MÓDULO 8. TALLER 4

1. TALLER 4: ATAQUE CON HYDRA DICCIONARIO Y MEDUSA

Mediante las herramientas de ataques de fuerza bruta HYDRA y MEDUSA y documentar proceso.

Proceso para atacar la máquina Metasploitable 3.

Para este ejercicio utilizaremos dos máquinas una para atacar y otra la víctima. En este caso, la Metasploitable 3.

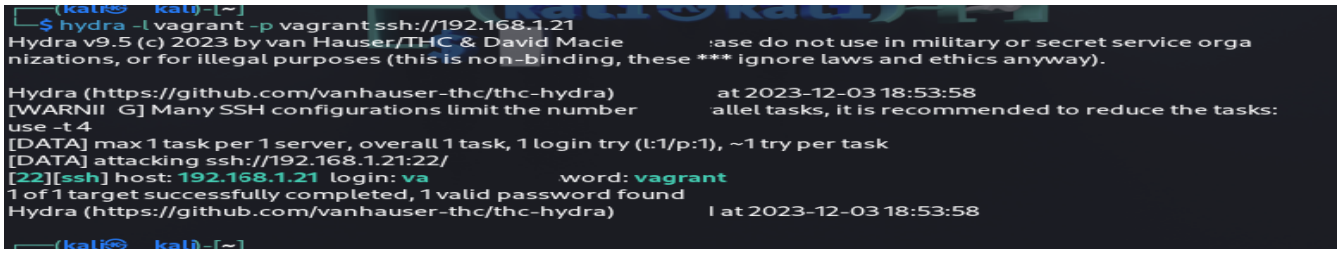
Mediante el uso de HYDRA y MEDUSA intentaremos recolectar las credenciales del usuario a través de distintos ataques.

En primer lugar, averiguamos la IP de la máquina METASPLOITABLE 3 con el comando **ifconfig**

1. PRIMERA PRUEBA.

- Utilizamos HYDRA para saber como funciona la herramienta si le damos las credenciales correctas (usuario: vagrant, Password: vagrant) y atacamos por SSH con el comando

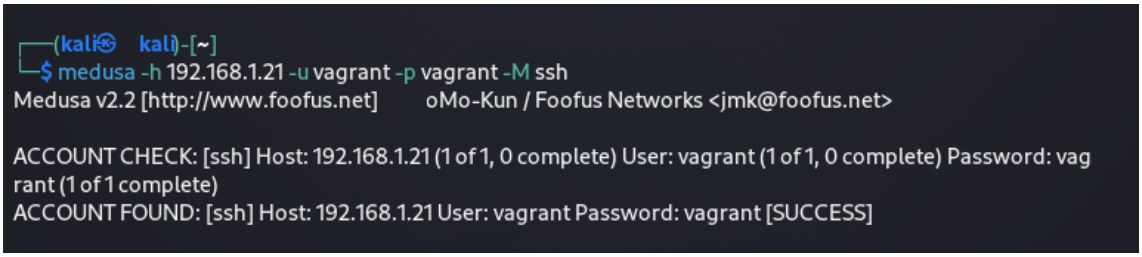
  hydra -l vagrant -p vagrant ssh://192.168.1.21



Vemos que el ataque por SSH ha sido un éxito.

- Ahora usamos MEDUSA para hacer la misma comprobación. En esta ocasión usamos el comando

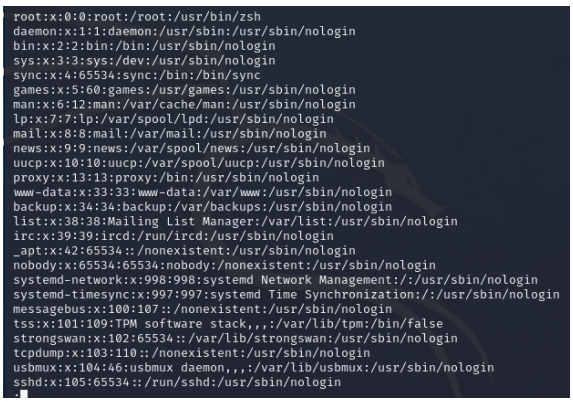
  medusa -h 192.168.1.21 -u vagrant -p vagrant -M ssh



Notamos que el ataque nos da la respuesta de SUCCESS cuando la contraseña y el usuario son los correctos. Si usáramos una lista de usuarios o contraseñas, la herramienta iría probando una a una las credenciales hasta tener la correcta.

2. SEGUNDA PRUEBA.

- Para la segunda prueba que realizo será necesario crear una lista de usuarios. Creamos la lista usando el comando less /etc/passwd para ver la lista de posibles usuarios del sistema.

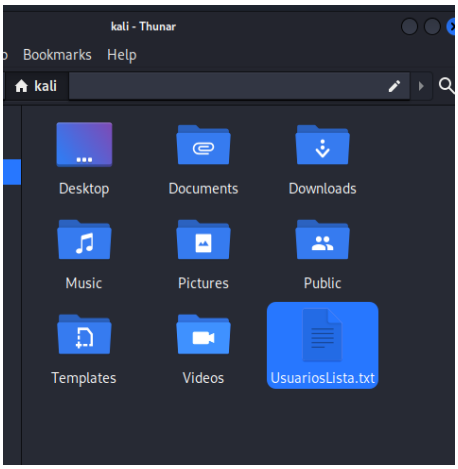


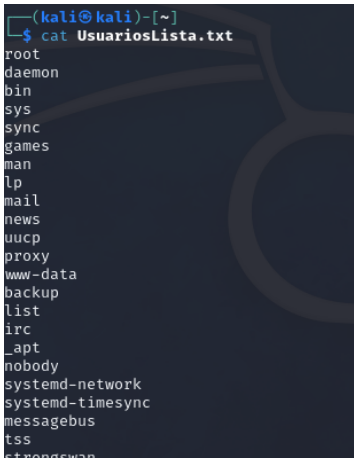
Para hacer la lista de usuarios que queremos tenemos que borrar todo lo que viene después de los primeros dos puntos. Lo haremos de la siguiente manera con el comando

cut -d: -f1 /etc/passwd

Observamos que nos queda un fichero solamente con los nombres que queremos para hacer la lista de usuarios. Para rematar haremos un .txt con el siguiente comando:

cut -d: -f1 /etc/passwd > UsuariosLista.txt



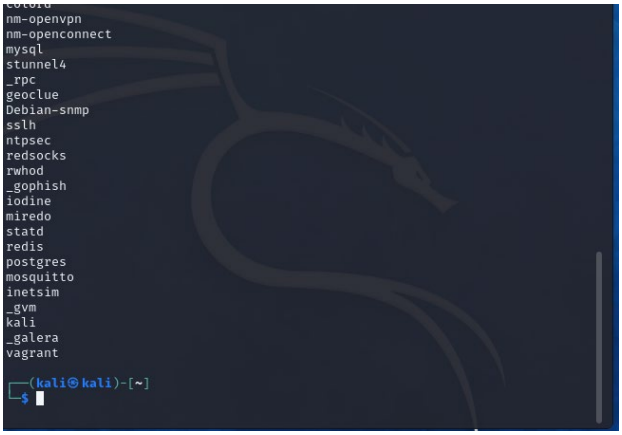


Con el comando **cat UsuariosLista.txt** vemos el contenido del fichero.txt.

Pero en este fichero no tenemos a nuestro usuario de la máquina Metasploitable. Para ello tenemos que añadirlo manualmente con el comando:

echo 'vagrant' >> UsuariosLista.txt

Volvemos a ejecutar el comando **cat UsuariosLista.txt** para verificar que tenemos el usuario registrado en la lista. Aparecerá al final.



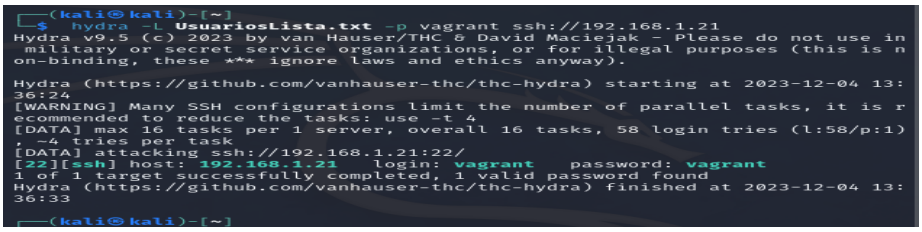
Después de crear la lista con el comando **cut -d: -f1 /etc/passwd > UsuariosLista.txt** y de agregar "vagrant" con **echo 'vagrant' >> UsuariosLista.txt**

Procedemos a realizar nuestra segunda prueba con las herramientas HYDRA y MEDUSA.

- HYDRA.

  Para hacer esta prueba iniciamos hydra y ejecutamos el comando

  hydra -L UsuariosLista.txt -p vagrant ssh://192.168.1.21



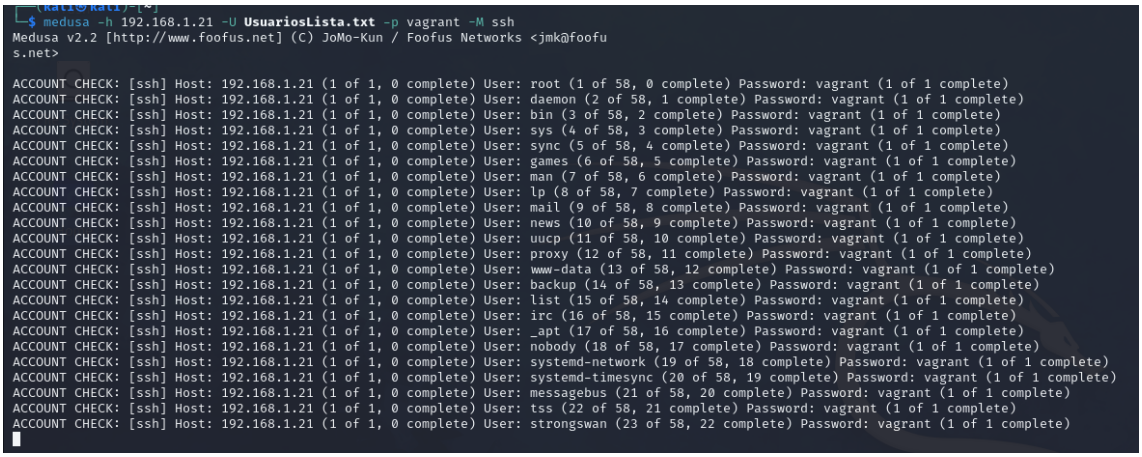
  Como podemos observar, HYDRA nos consigue las credenciales usando

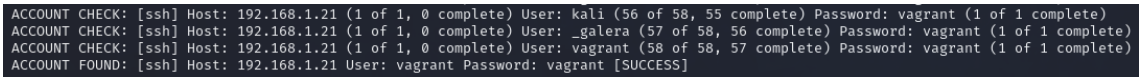
  -L UsuariosLista.txt

  Usamos -L mayúscula porque estamos usando un fichero en lugar de una palabra.

- MEDUSA.

Usamos el comando **medusa -h 192.168.1.21 -U UsuariosLista.txt -p vagrant -M ssh** y observamos quela herramienta va verificando una a una las líneas del fichero hasta dar con el usuario y contraseña "vagrant".





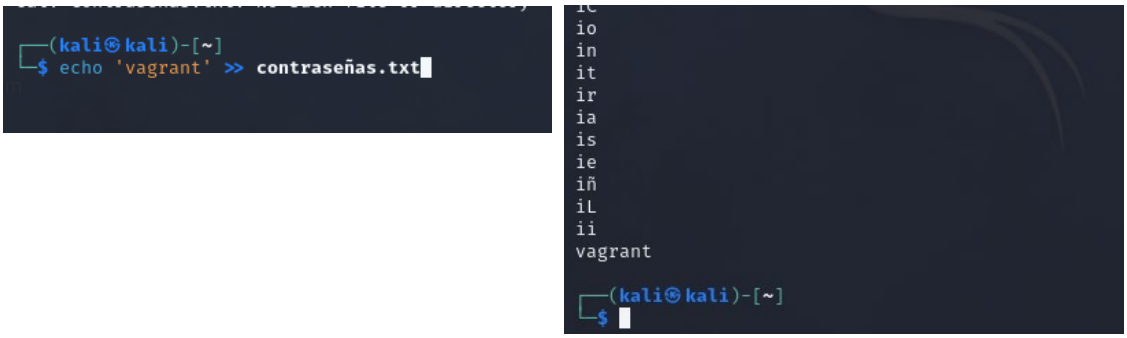
Al finalizar nos muestra el resultado : **ACCOUNT FOUND: User: vagrant Password: vagrant SUCCESS.**

3. TERCERA PRUEBA.

Ahora haremos la inversa. En lugar de una lista de usuarios crearemos una lista de contraseñas.

Para ello buscamos cualquier diccionario o creamos uno propio. En mi caso, haré mi propio diccionario.

Con el comando crunch le asignamos el mínimo de caracteres "1" y el máximo "2" y le ponemos un nombre cualquiera después le ponemos ">" para crear un fichero.



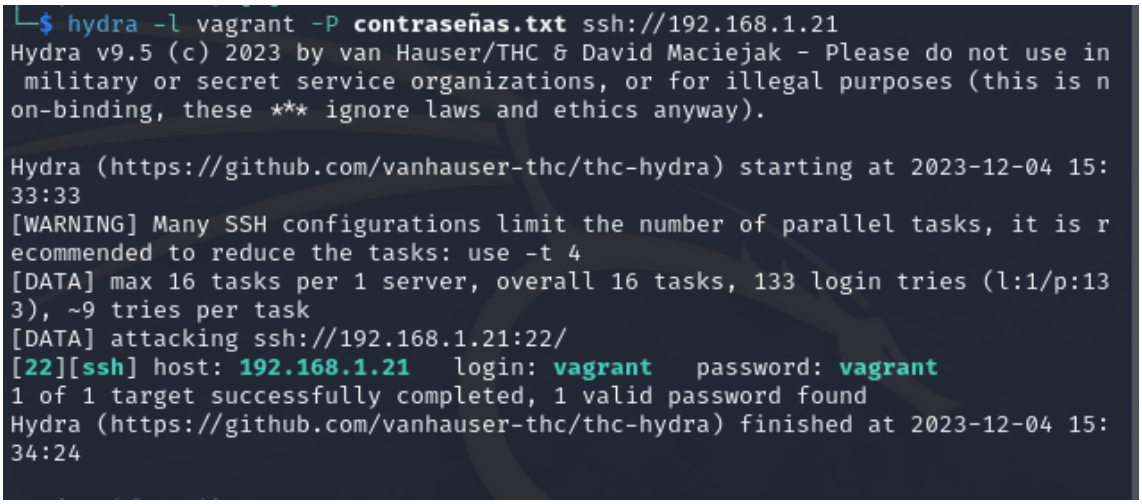
Usamos **echo 'vagrant >> contraseñas.txt** para añadir la contraseña vagrant.

Cuando ya tengamos el fichero de contraseñas hecho procederemos a hacer la prueba en HYDRA y MEDUSA con el fichero.

- HYDRA.

  El comando para ejecutar será similar al anterior, pero cambiando la -p por -P porque se trata de un fichero.

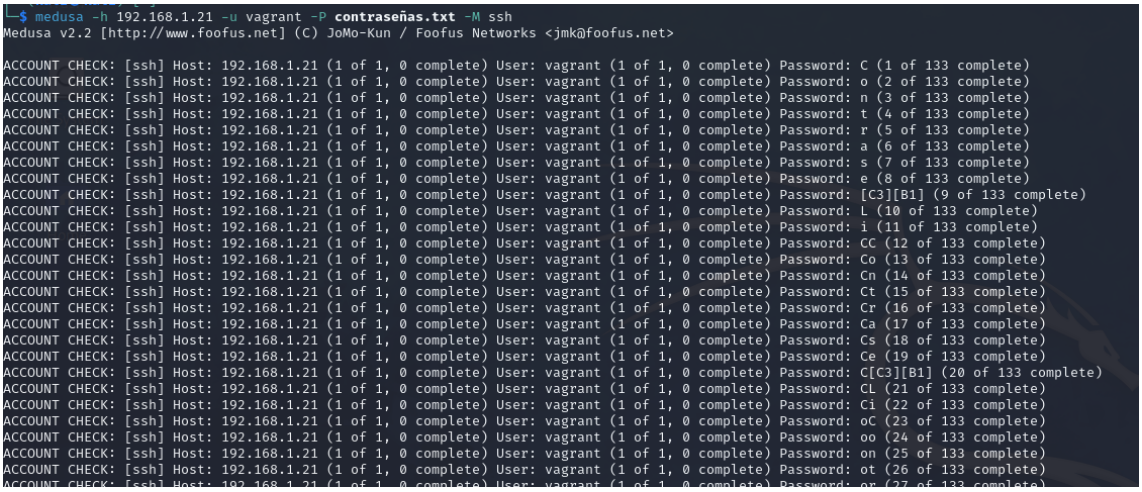
  hydra -l vagrant -P contraseñas.txt ssh://192.168.1.21



- MEDUSA.

  En la herramienta MEDUSA, usamos el comando:

  medusa -h 192.168.1.21 -u vagrant -P contraseñas.txt -M ssh



  Medusa sigue una secuencia por todo el fichero hasta encontrar la contraseña correspondiente al usuario "vagrant" de la máquina víctima, esperamos hasta que termine el proceso...

  Después de un rato, (133 intentos), MEDUSA nos aporta las credenciales de usuario y contraseña de la máquina Metasploitable.