CREACIÓN Y USO DE DICCIONARIOS

Jordi Masó Pla

INDICE

1. Descarga Diccionario SecLists

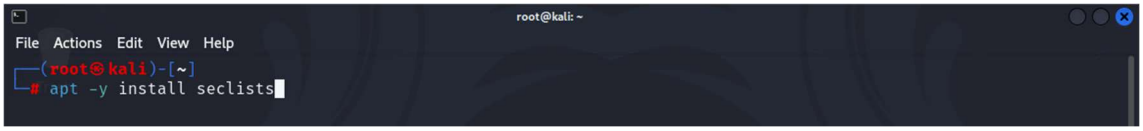
En este ejercicio realizaremos la descargar e instalación de un diccionario llamado SecLists, este mismo diccionario lo utilizaremos para encontrar el acceso a un servicio de nuestro laboratorio con Metasplotable2

1.1. Descarga diccionario

Abrimos el navegador y en la barra de búsqueda ponemos el enlace de Github.com https://github.com/danielmiessler/SecLists, bajamos hasta la parte de la pagina que dice instalación y vemos como podemos instalar este diccionario en Kali Linux.

1.2. Instalación del Diccionario

Desde una CLI dentro de Kali poniendo el siguiente comando: apt -y install seclists.



Al presiona intro se empezará a descargar e instalar automáticamente en la ruta predeterminada en Kali que es /usr/share/wordlists/ en un fichero llamado sectlists.

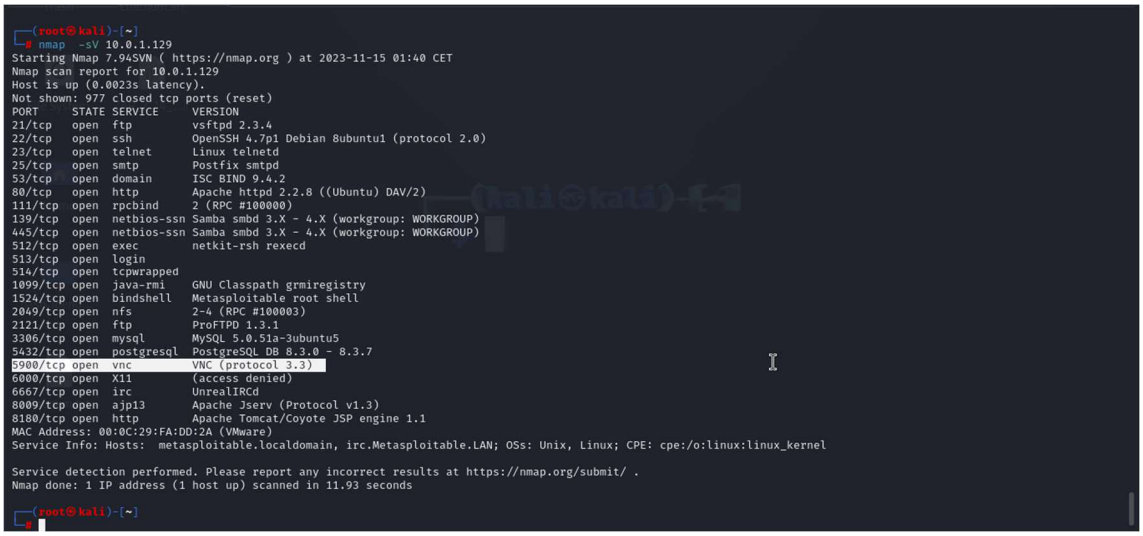
En mi caso, no ha instalado nada, ya que la tenía instalada anteriormente porque la utilice en la página https://tryhackme.com, para hacer retos de CTF. Este diccionario es bastante extenso y tiene listas de usuario, contraseñas y de descubrimiento de ficheros muy extenso y funcional.

2. Uso del Diccionario

Vamos ha utilizar este diccionario el seclists para encontrar la el usuario y la contraseña del servicio VNC de la maquina Metasplotable 2 de nuestro laboratorio.

2.1. Descubrimiento

Con la herramienta nmap hacemos un descubrimiento para saber en que puerto corre el servicio vnc. Con la instrucción en la línea de comando nmap -sV 10.0.1.129, encontramos que el servicio vnc corren en el puerto 5900, con la versión 3.3.



2.2. Ataque con Medusa

En esta ocasión realizaremos un ataque con diccionario al servicio vnc de la maquina Metasplotable 2 con la herramienta Medusa y el diccionario seclists.

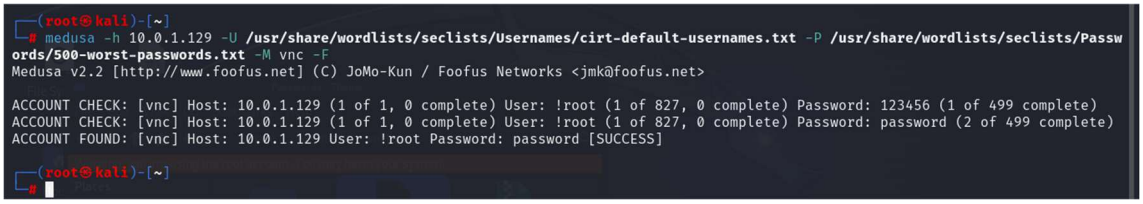
Desde nuestra CLI escribimos medusa --help para que muestre los parámetros que tenemos que utilizar y como lo podemos utilizar.

Una vez ya sabemos el parámetro a utilizar hace falta los módulos para el ataque al servicio vnc. Con el comando medusa -d nos muestra todos los módulos que soporta medusa.

En este punto ya tenemos toda la información necesaria para poder configura nuestro ataque al servicio, el comando será el siguiente: medusa -h 10.0.1.129 -U /usr/share/wordlists /seclists/Username/cirt-default-usernames.txt -P /usr/share/wordlists/seclists/Password/500-worst-password.txt -M vnc -F

Don de **-h** es la ip a atacar. **-U** es la ruta del diccionario de usurarios. **-P** es la ruta del diccionario de contraseñas. **-M** es el modulo que se va atacar. **-F** es que cuando encuentre una coincidencia correcta pare el ataque y no termine el diccionario.

Lanzamos el ataque y observamos que en muy poco tiempo tiene el resultado. Por loque puedo observar no hay usuario solo contraseña que “password”.

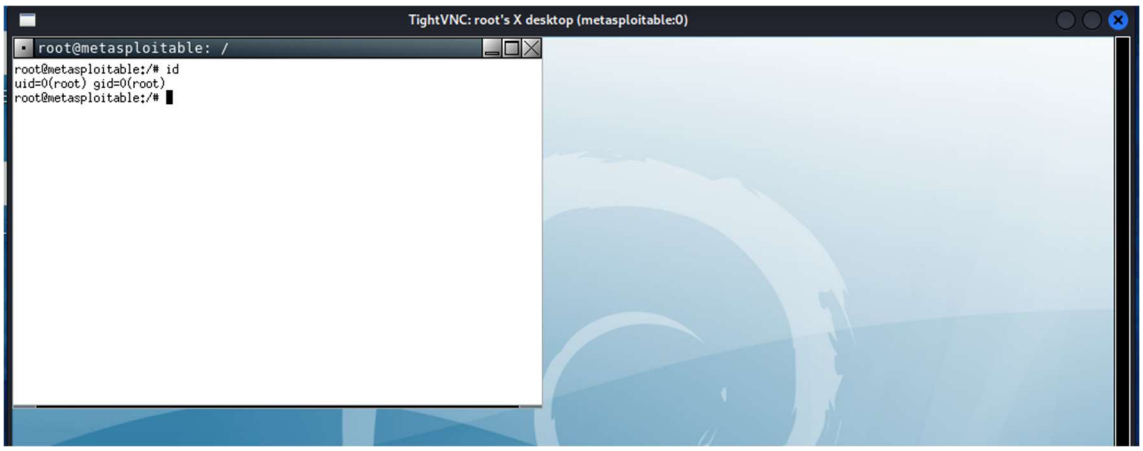


2.2.1. Comprobación

Realizaremos la comprobación de las credencias si son correctas, con el comando **xtightvncviewer** de Kali no podemos conectar al servicio vnc.

Se abrirá una pequeña ventana donde podremos la dirección ip a conectarnos y luego introducimos la contraseña, de esta forma accedemos al servicio de vnc de Metasplotable 2 con credenciales de root.

Una vez introducido la ip y las credenciales se nos abre una ventana con el servicio vnc de la máquina.



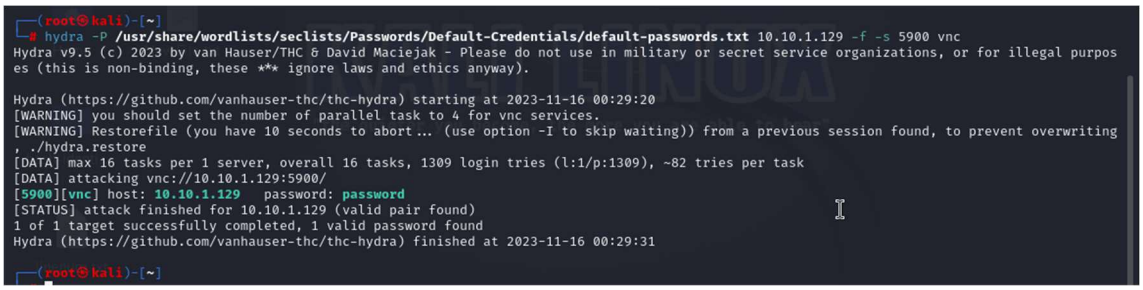
2.3. Ataque con Hydra

Vamos a realizar el mismo ataque con la herramienta Hydra. Desde nuestra terminal con el comando hydra -h se va a mostrar todos los parámetros necesarios para configurar hydra.

Teniendo claro los parámetros a utilizar vamos a configurar nuestro ataque. En este caso hydra nos dice que no hace falta usuario par el servicio vnc. La línea de comando que escribimos es lo siguiente: hydra -P /usr/share/wordlists/seclists/Password/Default-Credentials/default-password.txt 10.0.1.129 -s 5900 vnc -f

Donde **-P** es la ruta del diccionario de contraseñas. **10.0.1.129** es la ip de la víctima. **-s** es el puerto del servicio. **Vnc** es el servicio a atacar. **-f** finalice el ataque cuando tenga una credencial correcta.

Una vez configurado el ataque lo lanzamos y esperamos el resultado, en un espacio de tiempo muy corto nos muestra el resultado.



Las credenciales encontradas con hydra concuerdan con las de medusa y utilizando un diccionario diferente del seclists. En este caso no realizamos la comprobación de las credenciales ya que son las mismas que anteriormente ya comprobadas.