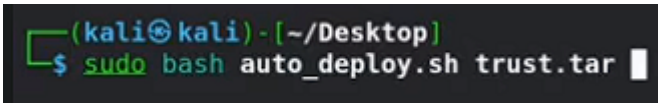
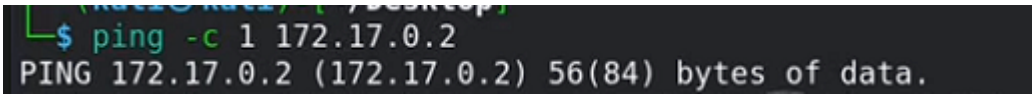
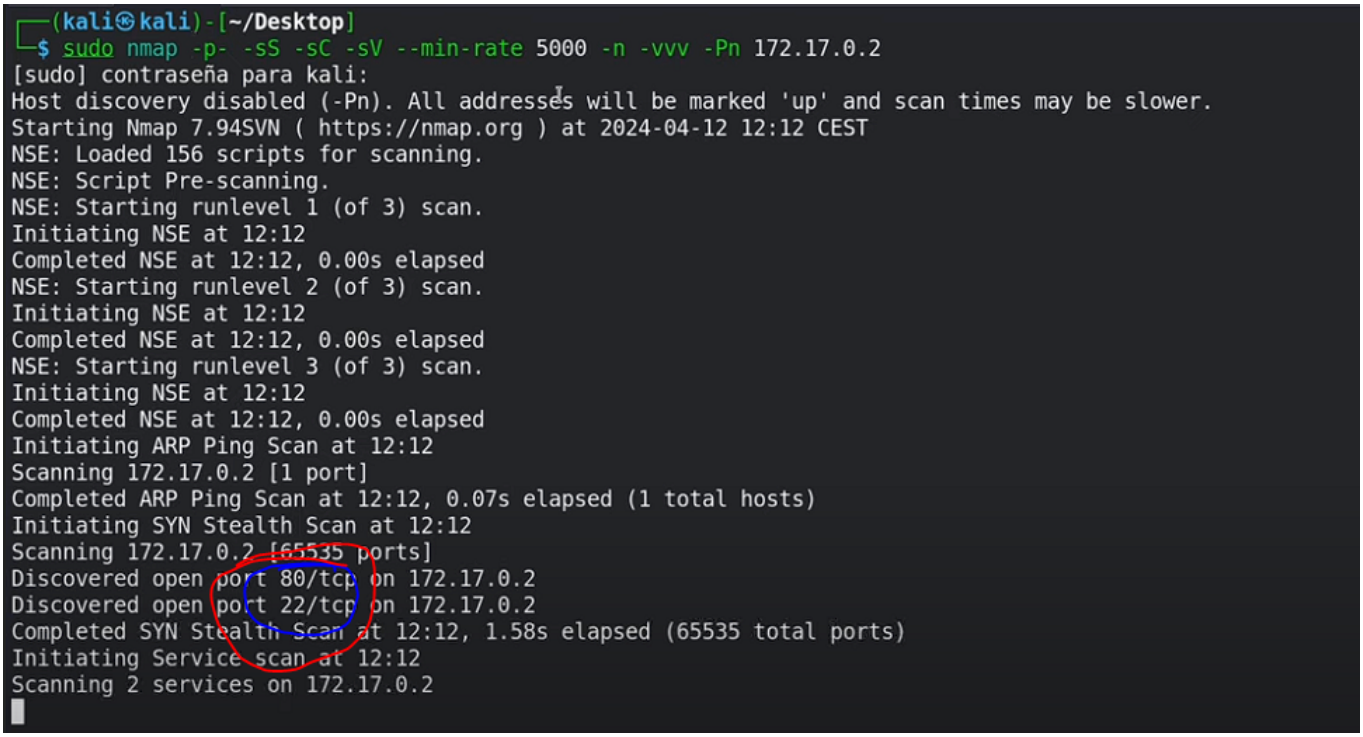
En esta maquina tendremos el puerto 80 de servidor Web i el puerto SSH que es el 22, el ataque en este consiste en averiguar el usuario que encontraremos en el web despues de un dirbuster específico, con hydra y una contraseña descubriremos la shell de root.



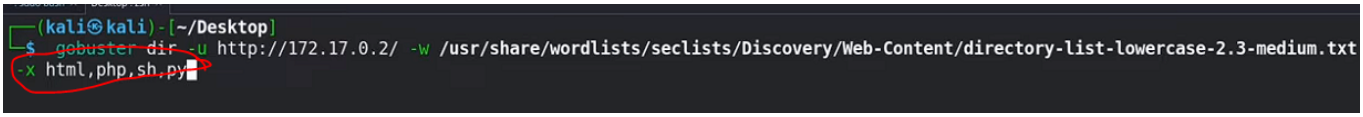
Primero de todo abrimos la maquina

Pingueamos conectividad i seguidamente realizamos el NMAP con los parámetros habituales



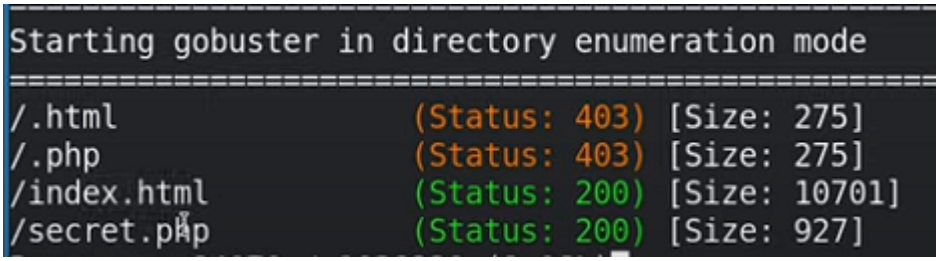


H

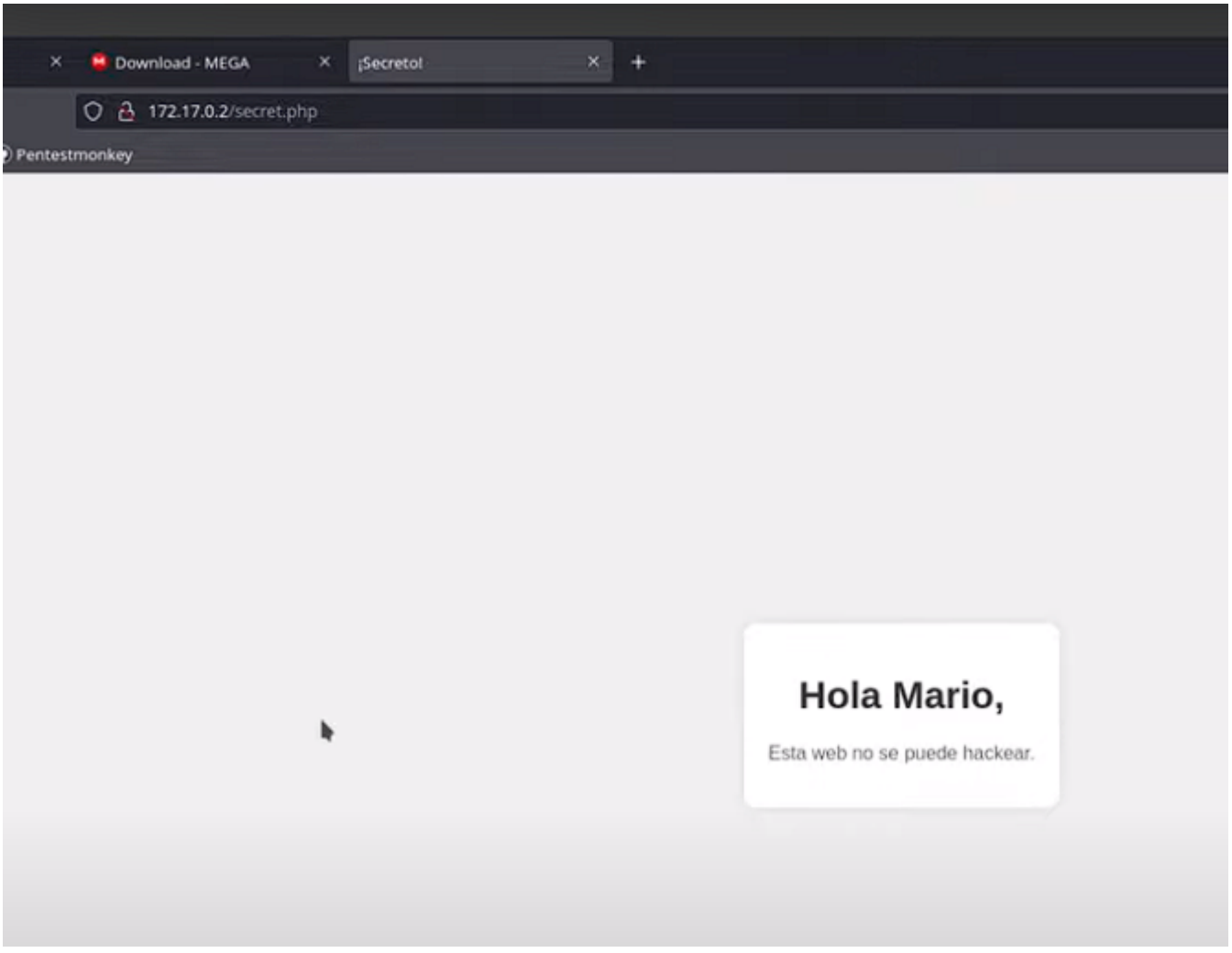


A continuación haremos un gobuster, es importante el -x y buscar

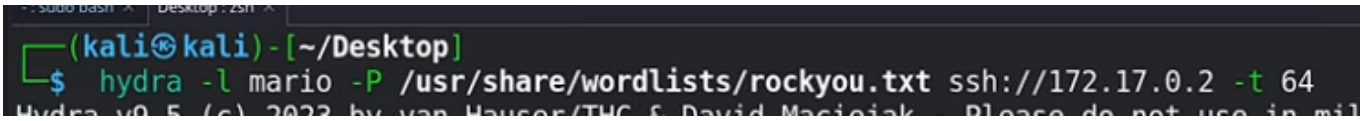
también extensiones porque en este caso en particular tal y como muestra la siguiente captura la hemos encontrado gracias a eso. Omito la parte de acceder por ip a la pagina web ya que en ella no había nada



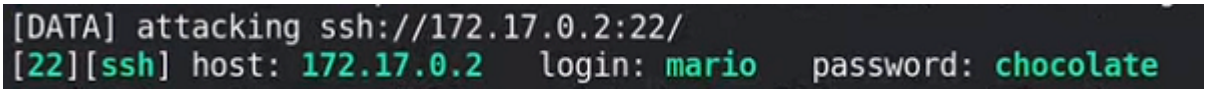
accedemos a secret.php



Gracias a esta web podemos ver que un posible nombre de usuario para acceder por ssh es "Mario" por parte de la pagina web del puerto 80 ya no se puede realizar nada nuevo, pero con el usuario podemos realizar un HYDRA, ataque de fuerza bruta

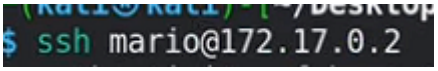


Como en este caso sabemos el usuario pero NO la contraseña, ponemos -P mayuscula para decir que es eso lo que no sabemos. Seguidamente del ssh i la ip de la maquina que estamos atacando

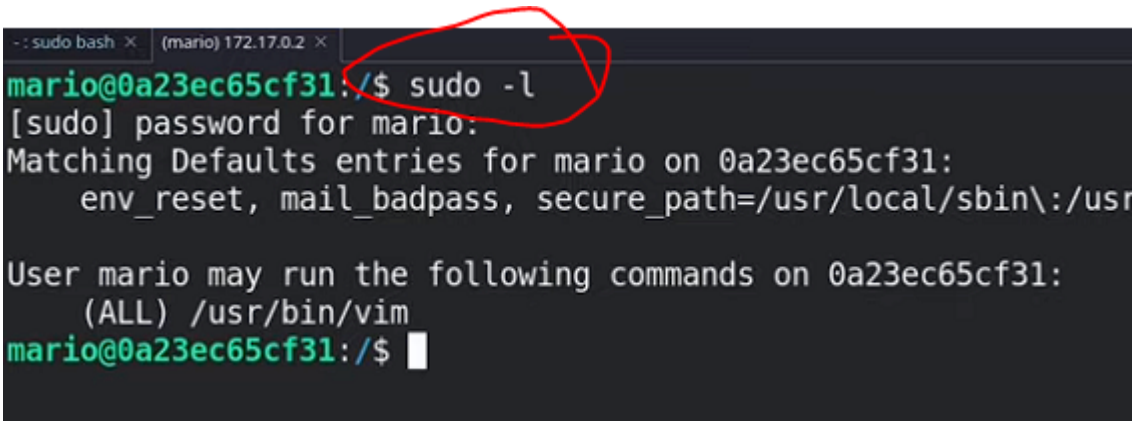


Si da problemas de hosts hay que eliminar el siguiente directorio

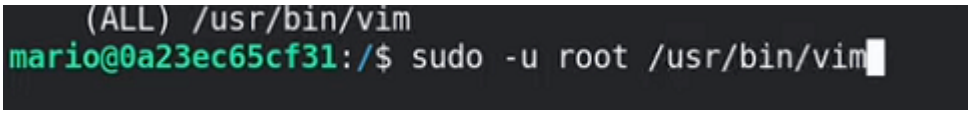
Accedemos por ssh a la maquina poniendo de passwd "chocolate"

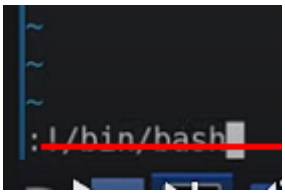


Buscando por los directorios no parece haber nada interesante para vulnerar que nos de una pista, así que hay que buscar directamente sin ayuda una manera de escalar privilegios en esta maquina. Con la comanda ENV, puedes ver las variables establecidas del sistema



Podemos hacer servir vim como root, eso vamos a usar para escalar privilegios esta vez. Realizamos la siguiente comanda y al final de esta ponemos:





Y así ya escalaríamos privilegios y seriamos ROOT por otra parte hay una alternativa final2 que seria acceder a la pagina de gtfobins para ver de forma manual como exploitear ese sudo -l