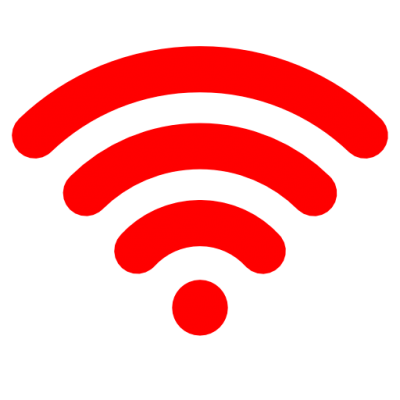
**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

FACULTAD DE CIENCIAS, 2025-1

*Criptografía y Seguridad*



**Práctica 5: Let’s multiSSH our way in**

**Equipo CyberWizards**

**INTEGRANTES:**

Fernández Blancas Melissa Lizbeth (319281778)

López Prado Emiliano (319205806)

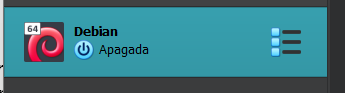
Sánchez Salmerón Ethan Damian (319122323)

**Desarrollo de la práctica**

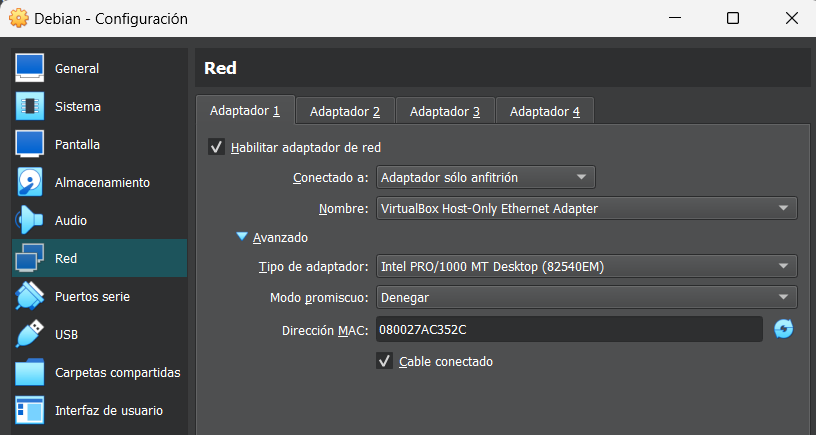
● *Virtualizar la VM adjunta y hacer la configuración de red de tal forma que esa y su*

*máquina atacante estén en el mismo segmento y se puedan comunicar entre ellas.*

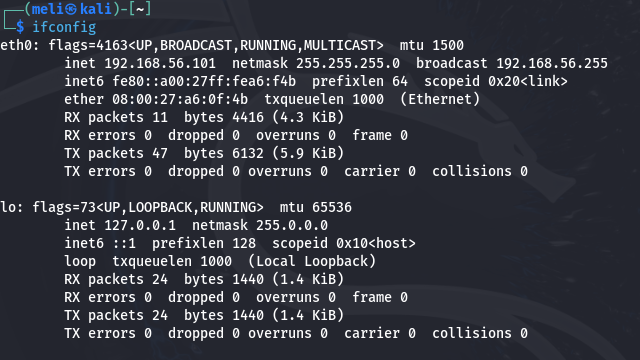
Primero se virtualizó la VM adjunta usando VirtualBox.



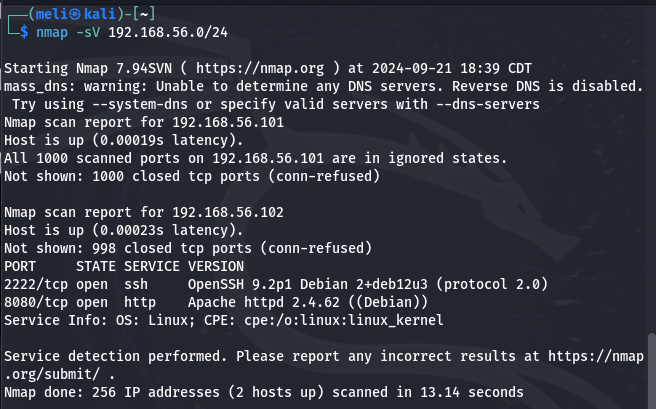
Posteriormente la máquina atacante (Kali) se conectó a una red VirtualBox Host-only que ya está configurada. Lo mismo se hizo con la VM Debian.



Como no teníamos acceso a la terminal de Debian, lo que se hizo fue obtener la ip de la máquina atacante (Kali) con ifConfig:



Una vez sabiendo esto, usamos el comando nmap -sV con el rango de subred usado para escanear el rango de direcciones IP en la subred y detectar dispositivos activos y servicios que están escuchando.



Con esto pudimos ver que hay dos hosts activos: la máquina atacante Kali y la MV Debian, lo cual nos permitió encontrar la IP de la MV Debian (En este caso 192.168.56.102).

● *Escanear el objetivo:*

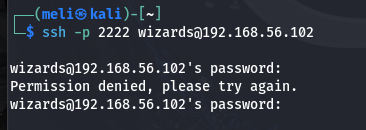
*Recopilar información de puertos, servicios y versiones (utilizando Nmap por ejemplo). Si bien en el laboratorio se vio un ejemplo muy sencillo, pueden consultar la documentación para obtener más información de la herramienta y personalizar sus escaneos.*

A través del nmap realizado anteriormente podemos ver que los puertos activos de Debian son el puerto 2222 con SSH (OpenSSH 9.2p1) y HTTP (Apache HTTPD 2.4.62) en el puerto 8080.

● *Atacar el objetivo y obtener la contraseña de su equipo:*

*Obtener mediante un ataque de diccionario la contraseña correspondiente a su equipo (utilizando Hydra por ejemplo).*

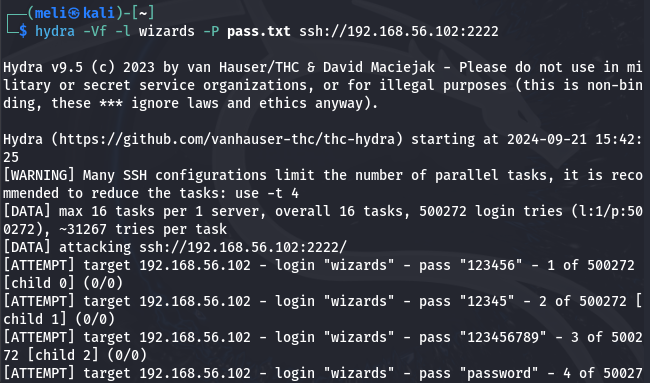
Utilizando la dirección IP y el puerto por donde corre SSH, pudimos tratar de hacer un login:

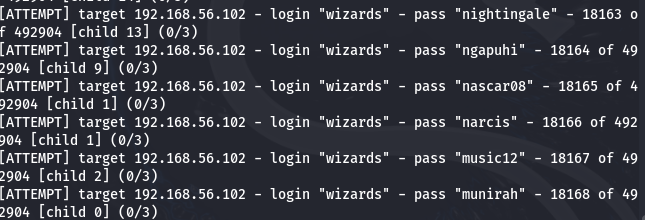


Posteriormente obtuvimos un archivo de las primeras 3 millones de palabras de Rockyou para comenzar el ataque usando Hydra.

Hydra -Vf -l wizards -P rutaAlArchivo ssh://ip/puerto : Es un comando para un ataque de fuerza bruta a SSH. -vF es para el modo verboso, es decir, que muestre todos los intentos y se detenga cuando encuentre la contraseña correcta. -l especifica el nombre de usuario, -P la ruta del archivo de palabras y ssh://ip/puerto es el protocolo y la dirección IP objetivo con el puerto SSH.

La idea inicial era repartir un millón de palabras por cada integrante del equipo. Eso fue lo que hicimos inicialmente





Sin embargo, de acuerdo al estatus mostrado por Hydra, hacer un millón de intentos tardaría aproximadamente 8 días y medio en una máquina.



Además, aunque la máquina de uno de los integrantes del equipo fuera relativamente rápido, al dejar la computadora encendida toda la noche, más 5 horas corriendo el proceso con hydra, éste apenas había tratado con 150 mil contraseñas, de 1 millón.



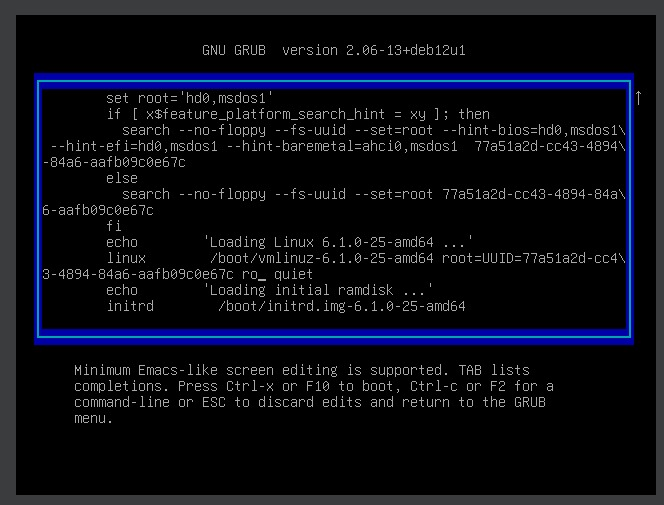
**Perdonen la calidad, me acababa de despertar cuando tomé la foto jajaj**

Por lo cual decidimos intentar con la técnica del /etc/shadow.

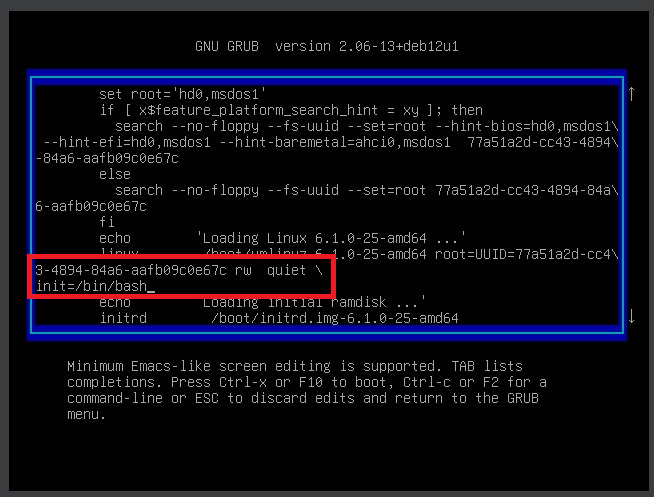
● *Investigar sobre el /etc/shadow , documentar su estructura y proponer una forma de obtener la contraseña de los demás equipos*

**Procedimiento para conseguir /etc/shadow**

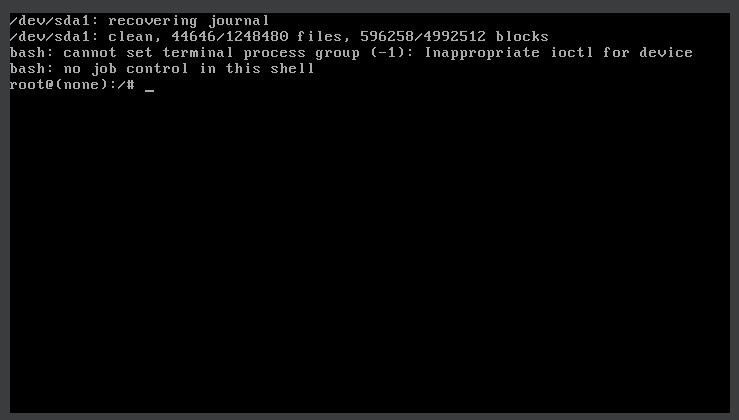
Para conseguir el archivo donde se almacenan todos los hashes de contraseñas, pudimos seguir la ruta “tradicional” que sería esperar a que alguien de los equipos lograra entrar al servicio de la forma que estaba planeada y que escalara privilegios con cualquier método. Sin embargo, tenemos la máquina virtual, y tiene la grandísima desventaja de que al arrancar, te muestra el Grub boot loader, esto ya es una increíble vulnerabilidad, pues podemos modificar los comandos de arranque antes de que bootee el sistema, esto nos permite saltarnos absolutamente toda la seguridad del sistema e iniciar sesión como root:

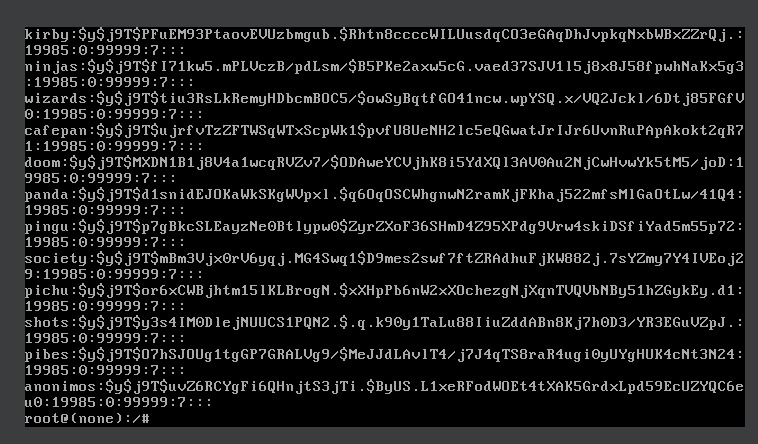


aquí podemos editar los permisos para que sean de escritura y que antes que cualquier cosa, arranque una terminal, y como el que ejecuta este comando es el usuario root, entonces tendríamos una sesión ROOT:

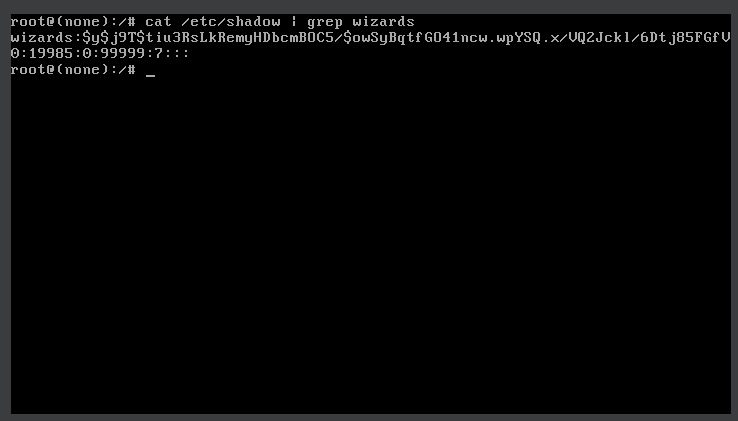


Finalmente, guardamos el archivo con Ctrl + X y el sistema comenzará a bootear, dando el siguiente resultado:



Ya dentro podemos simplemente imprimir en pantalla el archivo /etc/shadow  


O en nuestro caso más particular, imprimimos solo nuestro hash

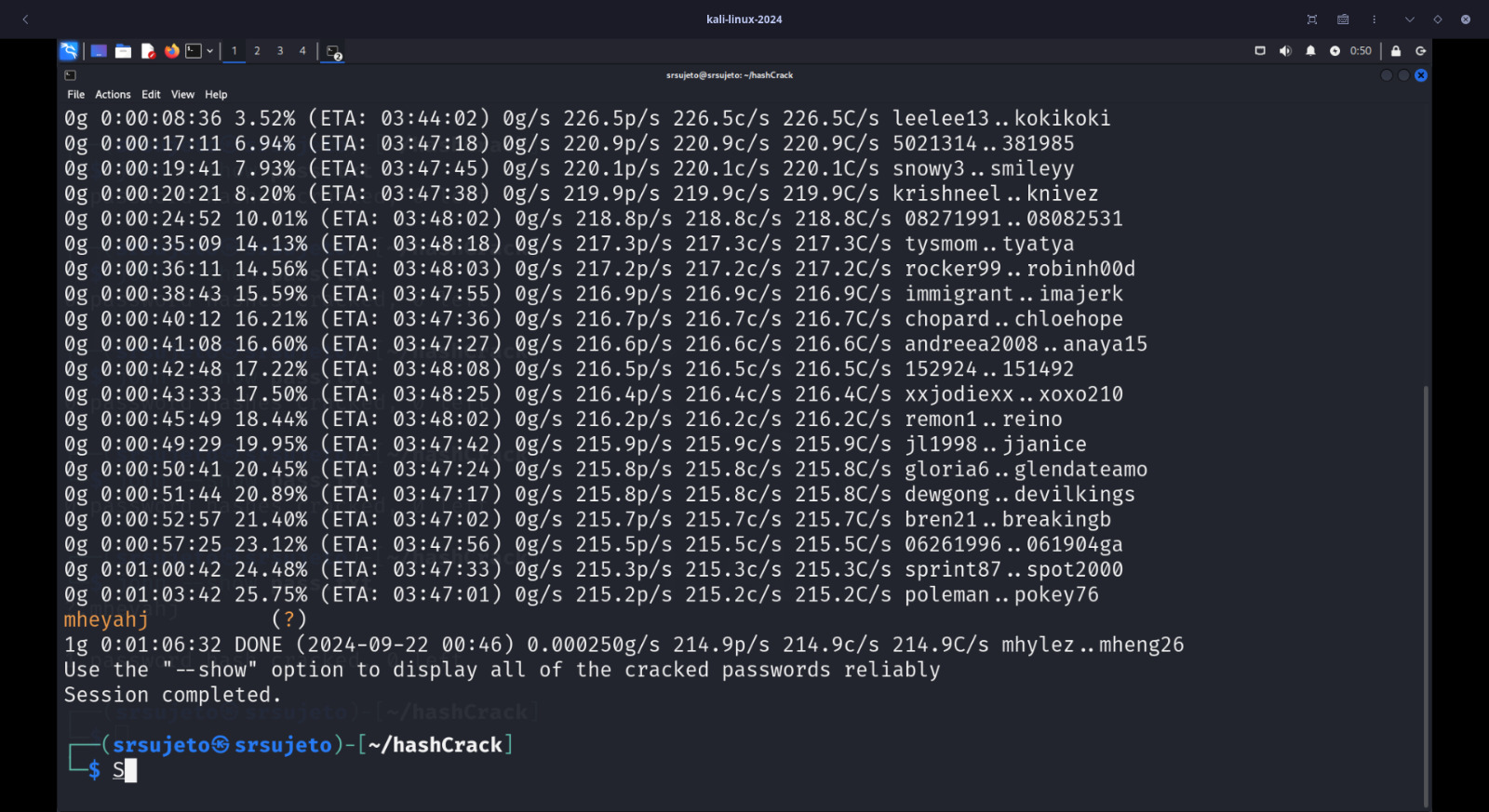


Ya después de copiar este valor con GoogleLens, me di cuenta de que lo copiamos mal xD y que pusimos algunos ceros en vez de “o” mayúscula, por lo que no sirvieron de nada al rededor de 6 millones de comprobaciones usando John the ripper.

Sobre John the ripper, utilizamos esta herramienta ya que en hashcat no se tenía soporte para el tipo de algoritmo de encriptado usado sobre nuestra contraseña, pues después de analizarla con la herramienta de [hash Identifier](https://hashes.com/en/tools/hash_identifier) descubrimos que se trataba de un Yescript , este algoritmo es mucho más robusto contra ataques de fuerza bruta y de diccionario, pues resulta que estos programas de ataque de diccionario no pueden atacar contra Yescript de forma nativa. Nuestra única alternativa es correr estos programas (John the riper) sobre un sistema operativo que nativamente aplique el algoritmo de encriptado Yescript (como Kali), por eso mismo 3 millones de intentos fueron en vano al correrlo sobre Fedora y 3 millones perdidos en Kali por culpa de usar el hash incorrecto. Un total de 8 horas inútiles.

La última tanda (con el hash correcto **wizards**: **$y$j9T$tiu3RsLkRemyHDbcmBOC5/$owSyBqtfGO41ncw.wpYSQ.x/VQ2Jckl/6Dtj85FGfV0:19985:0:99999:7:::**)

Finalizó con éxito después de alrededor de 1 hora, lo cual es INFINITAMENTE más rápido que el método tradicional con el que estaba pensada la práctica.



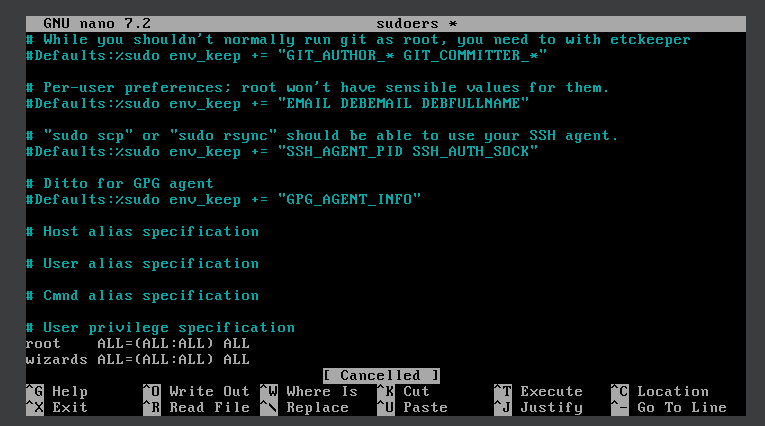
Así, pudimos obtener las credenciales para entrar a la máquina con Debian.

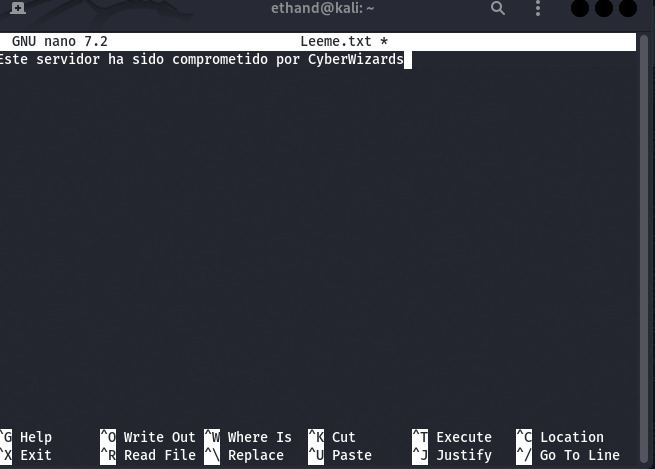
**Usuario : wizards**

**Contraseña : mheyahj**

**Extra**

Como algo que se puede realizar también, es aprovechar la vulnerabilidad de poder entrar al root de la máquina con Debian, y así poner al usuario wizards en el archivo de sudoers para que tenga permisos de administrador:



Por lo que ya teniendo acceso al usuario wizards desde Kali, podemos realizar acciones como administrador, con sudo.   
  


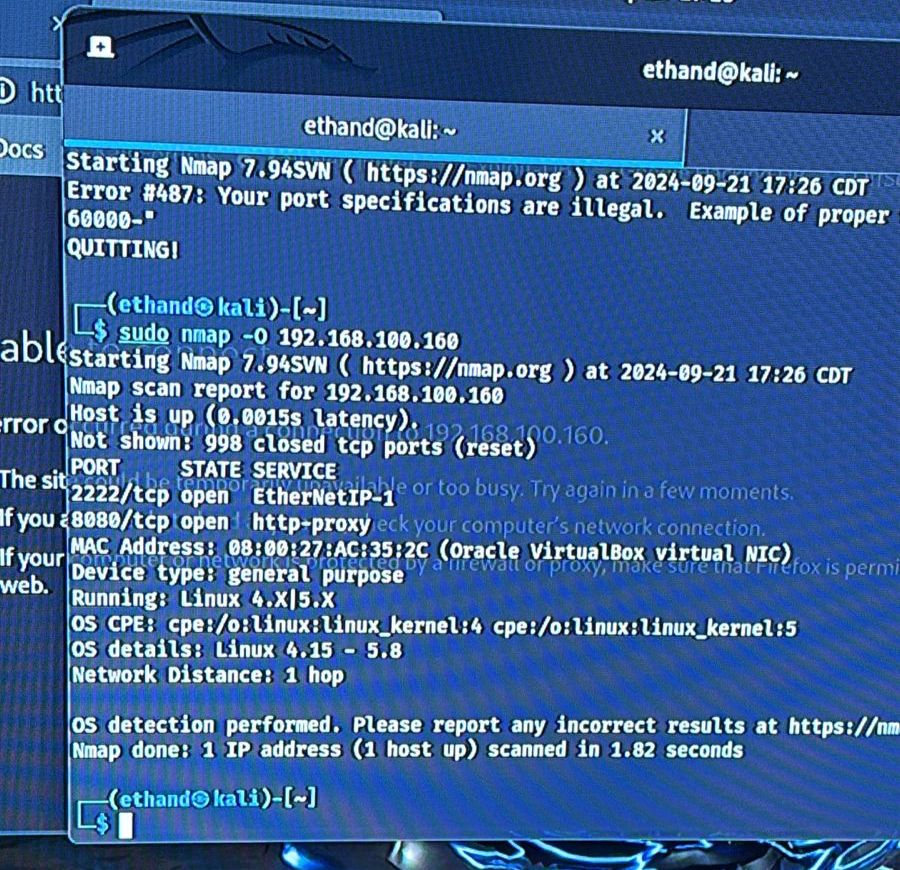


Que en este caso solo fue escribir en un .txt, que se puede ver desde la máquina con Debian.

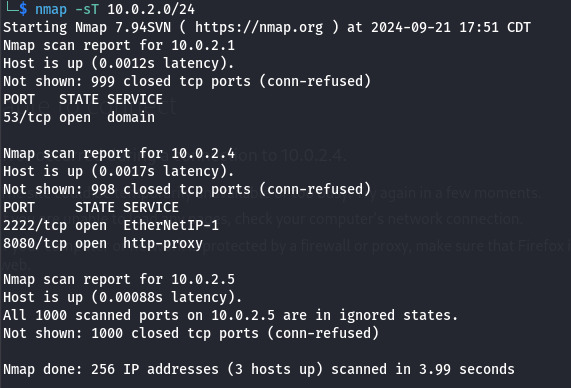
**Complicaciones en la práctica.**

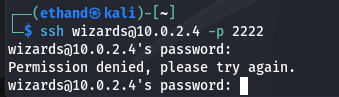
***Ethan Sanchez:***

Tuve problemas para configurar las máquinas virtuales en la misma red, ya que, primero intenté conectarlas a la misma red Host que tenía. Y al hacer escaneo con nmap pude obtener la dirección IP de la máquina virtual con Debian. Usé el comando ***sudo nmap -O 192.168.100.160*** para estar seguro de que esa era la dirección IP de la máquina con Debian, con este comando se puede ver el sistema operativo de la dirección IP, así como un reporte de este.



Y con ese reporte, pude ver que los puertos abiertos de esta dirección IP eran los 2222/tcp y el 8080/tcp. Sin embargo, al intentar iniciar sesión mediante ssh al puerto 2222 con el comando ***ssh wizards@192.168.100.160 -p 2222***, pero me arrojaba un mensaje de error con el mensaje “No route host”.   
Por lo tanto creé una red NAT 10.0.2.0/24 en la aplicación de VirtualBox y configuré las máquinas virtuales para que estuvieran en esa red NAT.   
Y así, haciendo un escaneo con nmap en la nueva red desde la máquina con Kali:



Pude ver que la máquina con Debian se encontraba con la IP 10.0.2.4 y que los puertos 2222 y 8080 eran los puertos abiertos, y tratando de iniciar sesión mediante ssh al puerto 2222

Y ya pude conectarme correctamente a la máquina con Debian.

***Melissa Fernández:***

No hubo complicaciones en particular, solamente al momento de tratar de hacer el ataque de diccionario separé el millón de palabras en dos archivos para que corrieran dos terminales al mismo tiempo (no mejoró nada), por lo que cuando me marcó error de red decidí volver a ponerlo ya solamente con una terminal desde la palabra en que se quedó.

***Emiliano López:***

No hubo complicaciones más allá de lo comentado sobre los hashes.

**Conclusiones**

Con esta práctica pudimos aprender a cómo realizar un ataque a diccionario usando herramientas como nmap, que nos ayuda a realizar un escaneo sobre direcciones IP 's para descubrir vulnerabilidades en esa máquina. A su vez, pudimos ver que usar hydra como herramienta para realizar el ataque a diccionario puede tardar demasiado si lo hacemos con un archivo lo suficientemente grande, con posibles contraseñas, como es el archivo de rockYou.txt Así que otra solución es intentar usar el valor hash de la contraseña para poder intentar obtener información sobre cómo fue cifrada y así usar otra herramienta como jack the reaper que nos permite descifrar contraseñas con algún algoritmo, en este caso fue Yescript, de esta forma, pudimos ingresar al sistema con las credenciales obtenidas.

Nos pareció interesante todo este proceso ya que podemos darnos cuenta de lo que las personas con malas intenciones deben hacer para intentar ingresar a un sistema. Es por eso que debemos tener cuidado en la forma en que ponemos una contraseña para un sistema, estas contraseñas deben de ser difíciles de descifrar y sobre de todo difíciles de adivinar por sistemas que intentan por fuerza bruta, además, otra capa de seguridad como lo es la autenticación de dos pasos puede ayudar a mejorar la seguridad de un sistema.  
  
Esta práctica nos deja un buen aprendizaje sobre la protección de nuestras contraseñas y de nuestros datos, pues en el mundo hay personas que no tienen buenas intenciones y nuestra integridad puede ser afectada.

**Referencias:**

* *Command-line Flags | NMAP Network Scanning*. (s. f.). <https://nmap.org/book/port-scanning-options.html>
* An0n Ali. (2023, 5 julio). *Introduction to NMAP for Beginners!* [Vídeo]. YouTube. <https://www.youtube.com/watch?v=NYgDzO8iQJ0>