# Seguridad de Sistemas Informáticos.

# 

Omar Teixeira González, UO281847

# Examen Práctico

## Tabla de contenidos

[Seguridad de Sistemas Informáticos. 1](#_Toc136596770)

[Examen Práctico 2](#_Toc136596772)

[Tabla de contenidos 2](#_Toc136596773)

[Ejercicio 1. 3](#_Toc136596774)

[Ejercicio 2. 5](#_Toc136596775)

[Ejercicio 3. 6](#_Toc136596776)

[Ejercicio 4. 7](#_Toc136596777)

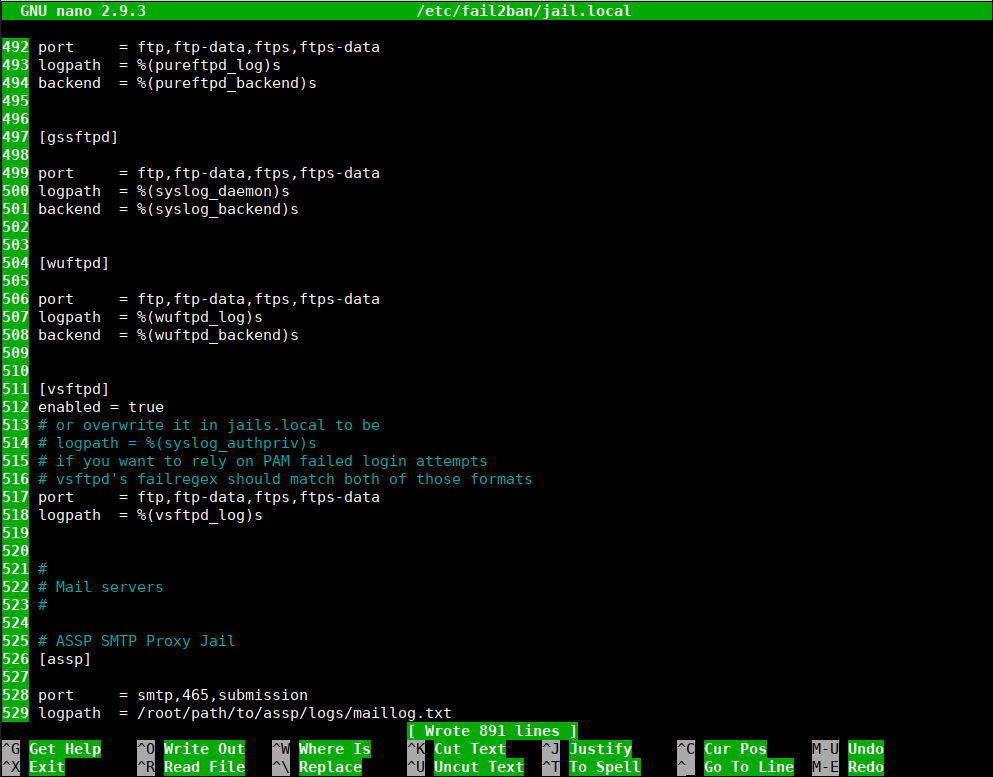
[Ejercicio 5. 9](#_Toc136596778)

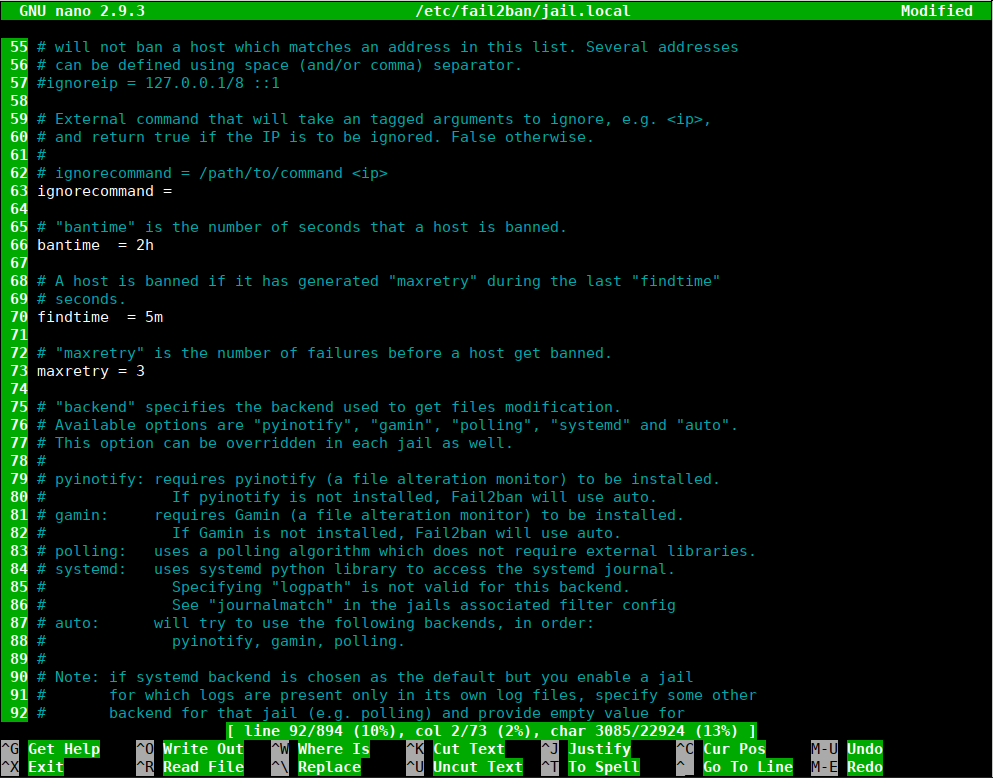
[Ejercicio 6. 10](#_Toc136596779)

## Ejercicio 1.

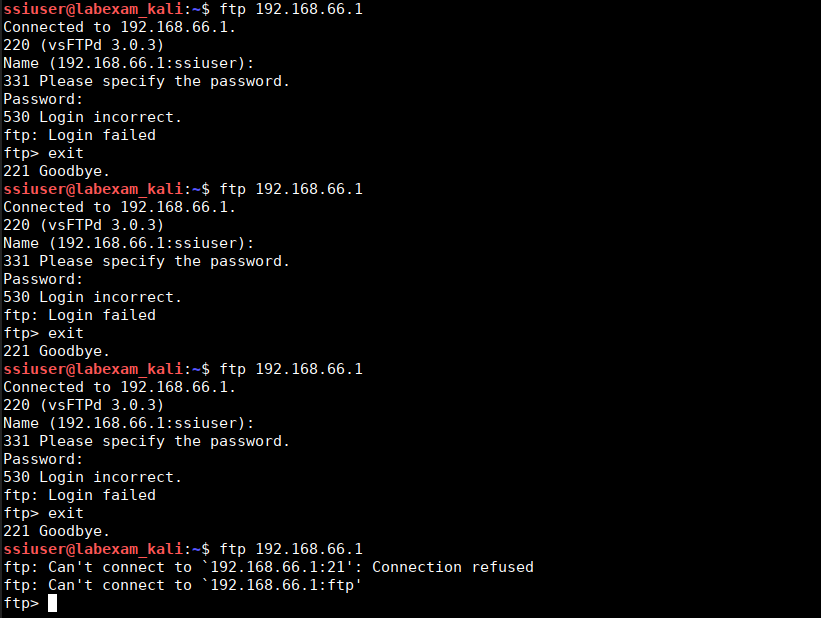
Para realizar este ejercicio se utiliza fail2ban, para ello (como el fichero jail.local no existe, se copia el jail.conf previamente), mediante *cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local* y se accede a este fichero para configurar las opciones.

1. Modificaciones al fichero jail.local:

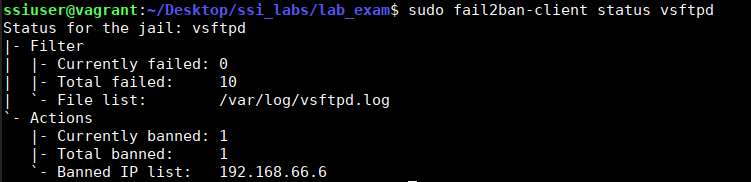




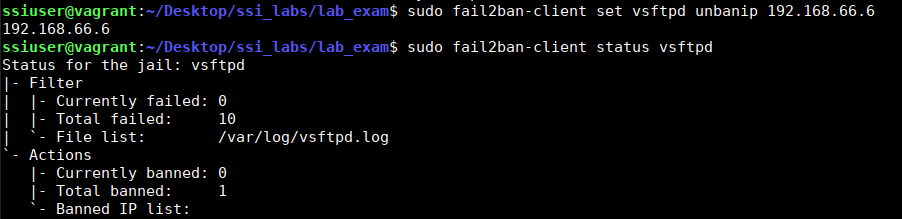
1. Tras intentar acceder 3 veces, se ha bloqueado:



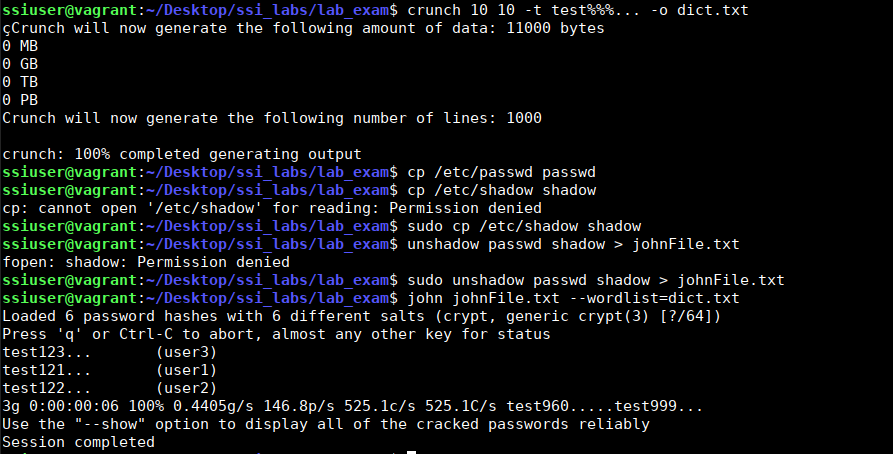
1. Usando el comando *fail2ban-client status vsftpd*, se comprueba que la ip se ha bloqueado:



1. Se desbloquea la ip con *fail2ban-client set vsftpd unbanip 192.168.66.6*, y se comprueba el estado de bloqueo:



## Ejercicio 2.

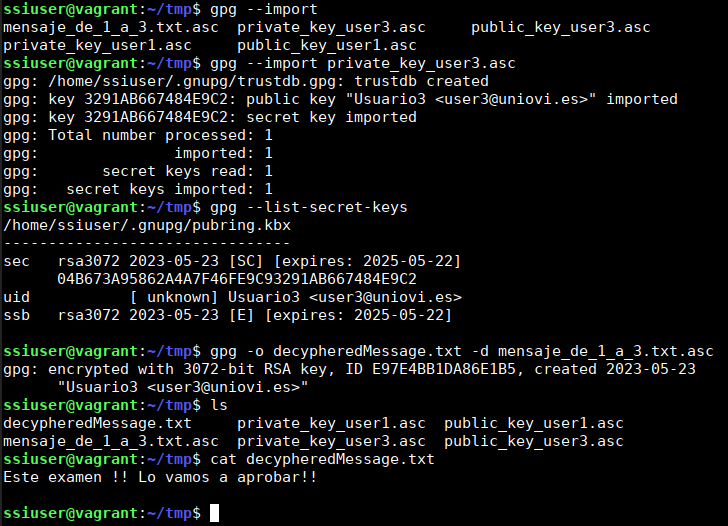


## Ejercicio 3.

Primero se debe importar la clave privada del usuario 3, ya que, al ser el receptor del mensaje, el usuario 1 (emisor) ha cifrado dicho mensaje con nuestra clave pública, por lo que, el descifrado debe ser con la clave privada, por lo que, se importa con *gpg –import private\_key\_user3.asc*.

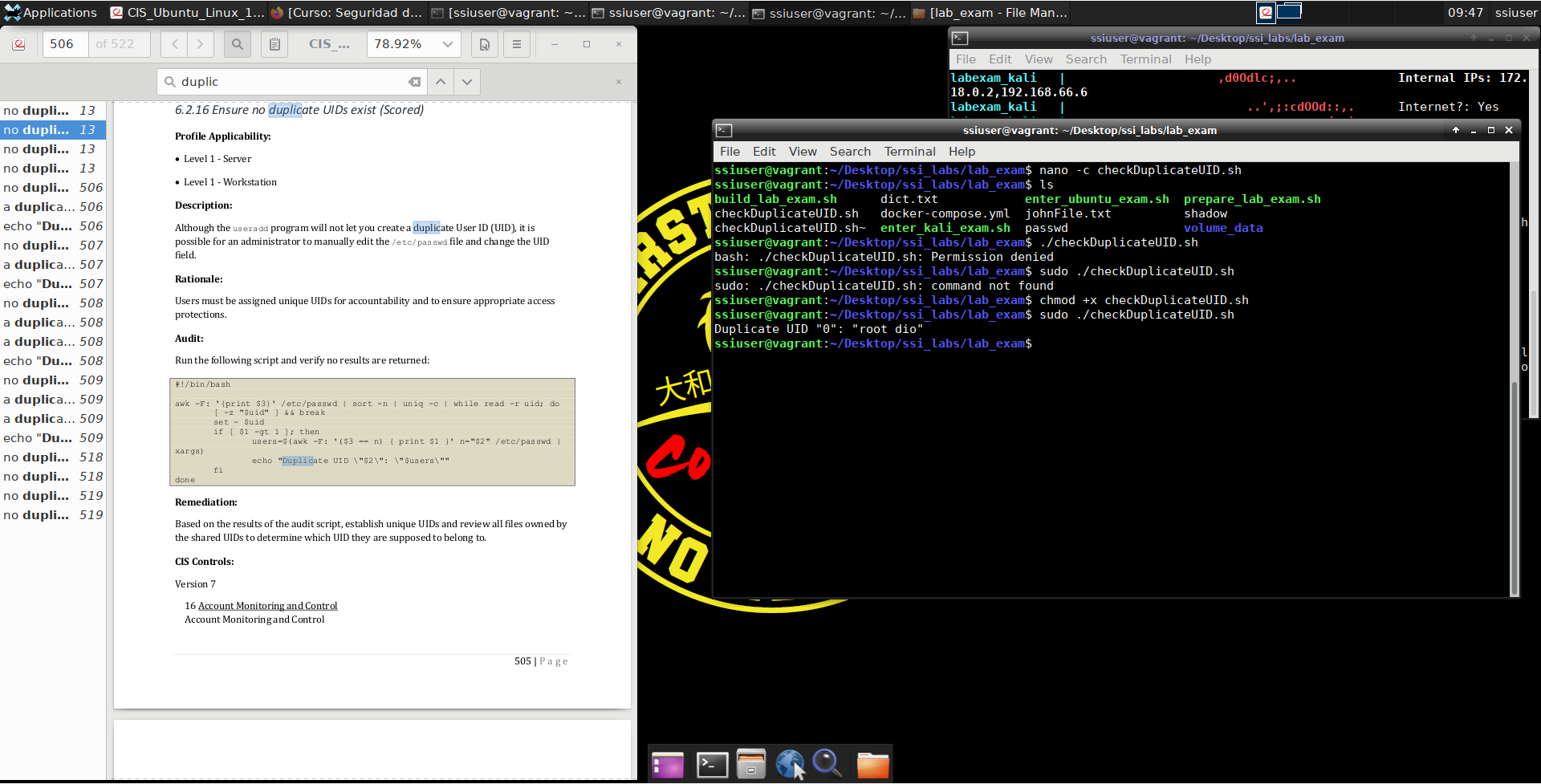
Se podría hacer directamente el descifrado, no obstante, es recomendable comprobar que la clave se ha importado correctamente con *gpg –list-secret-keys*. Una vez hecho esto, se descifra el mensaje con el comando *gpg –o decypheredMessage.txt –d mensaje\_de\_1\_a\_3.txt.asc*, y automáticamente se podrá leer el contenido del mensaje previamente cifrado.

Esta explicación puede verse en la siguiente captura:



## Ejercicio 4.

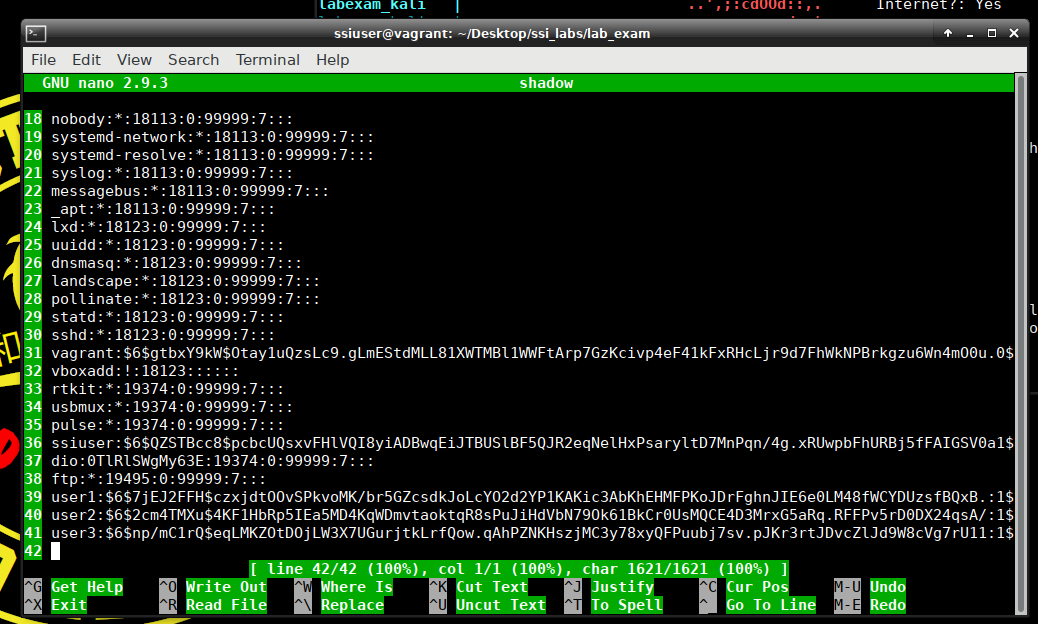
1. Se ha seguido el control *6.2.16 Ensure no duplicate UIDs exist (Scored)* en el CIS, y el resultado de ejecutar el script ha sido:

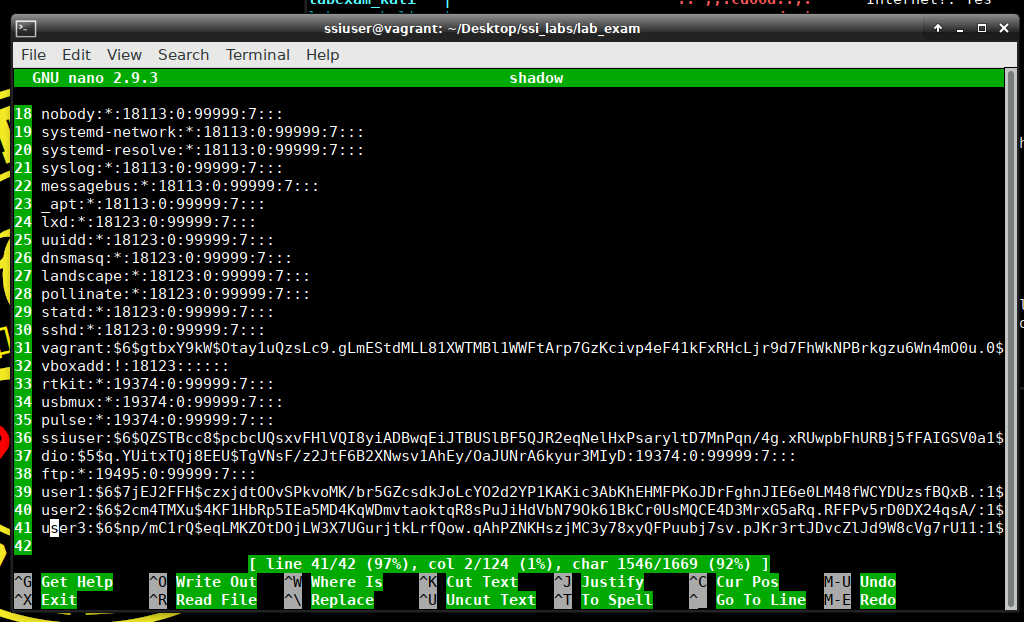


1. Para ello, primero generamos la contraseña con la encriptación correcta, es decir, sha256, utilizamos el comando mkpasswd –m sha-256 aversiapruebo.

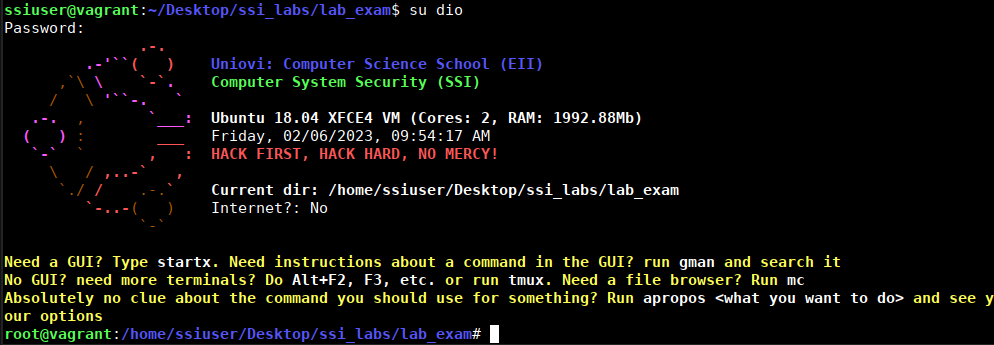


Se edita el fichero shadow con la nueva contraseña.

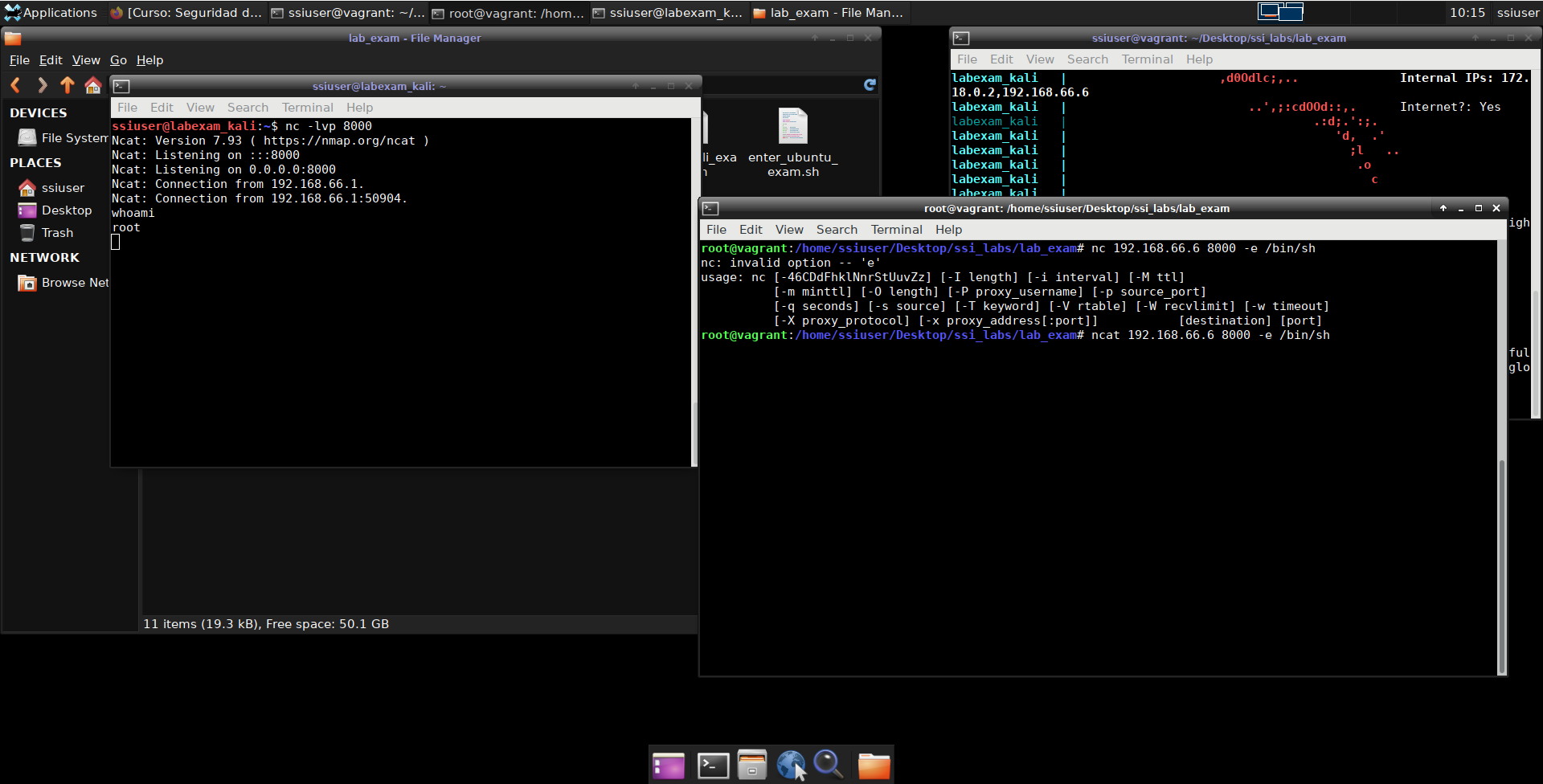




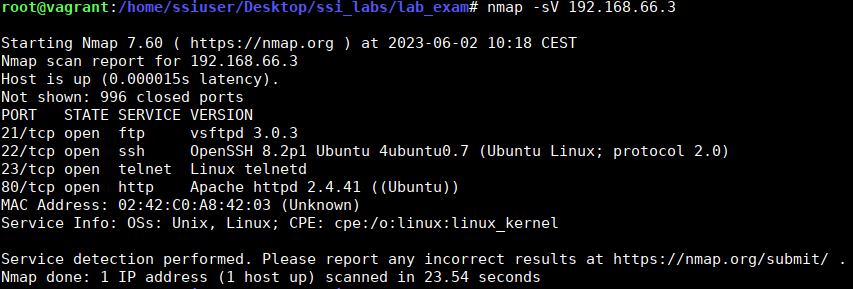
1. Entramos en sesión como el usuario dio, con la contraseña definida anteriormente



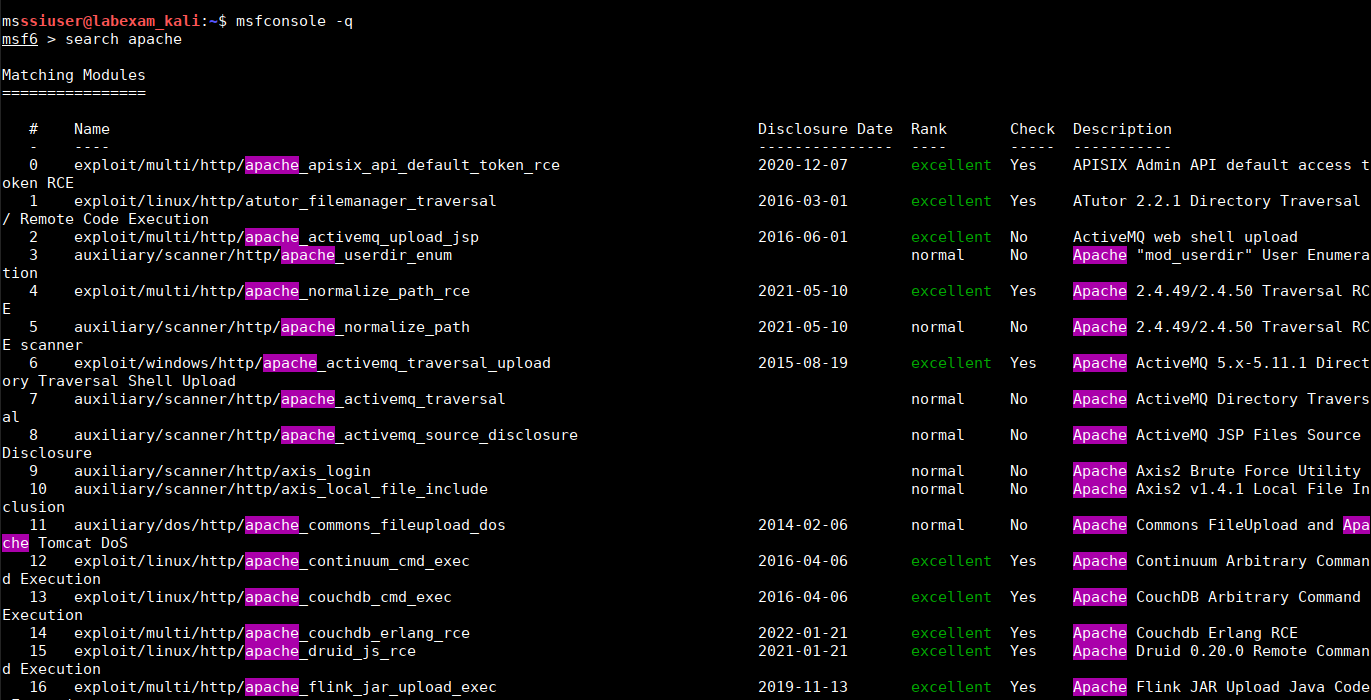
Posteriormente, se hace un reverse shell, escuchando en la máquina atacante, y se ve que, al ejecutar whoami, somos el usuario al que hemos accedido antes.

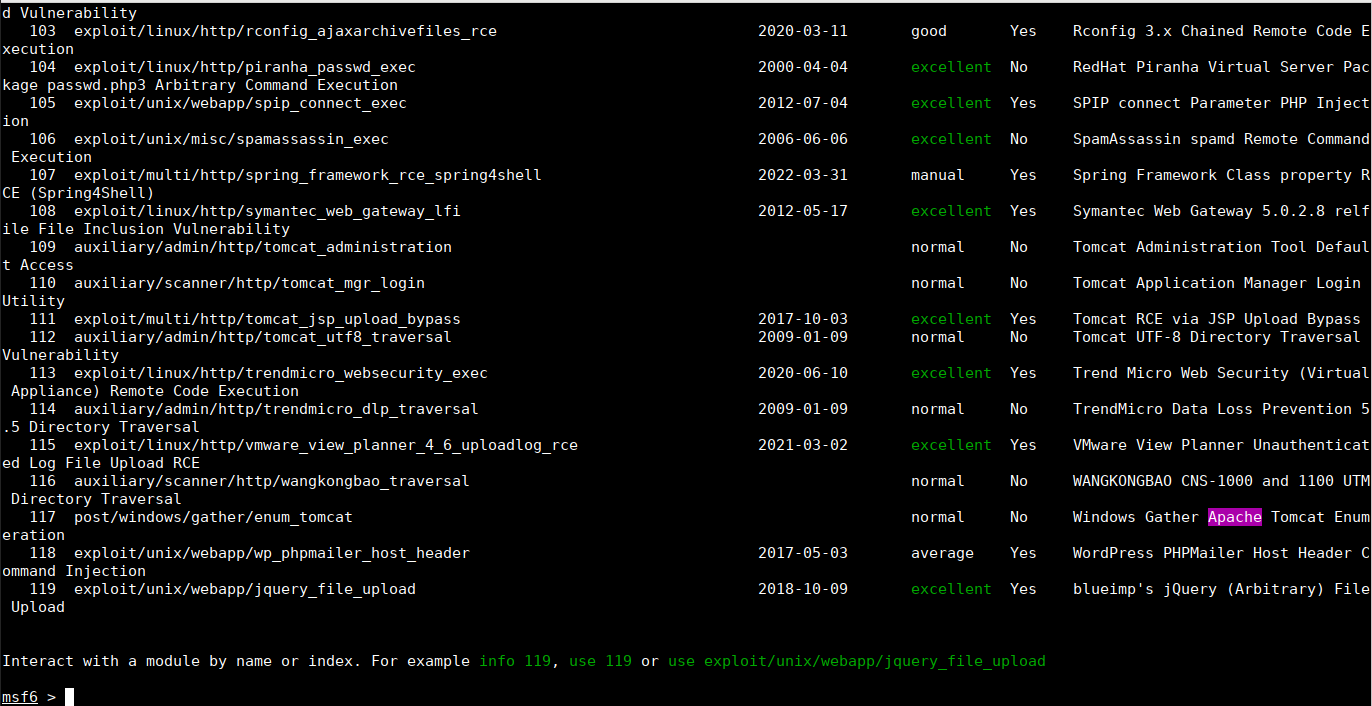


## Ejercicio 5.



* A la lista de vulnerabilidades en el CVE.
* Utilizar una base de datos de exploits en la que buscar dichos servicios y versiones.
* Metasploit.





## Ejercicio 6.