Índice:

LILLO ROMERO MIGUEL - 71368153G

Firmado digitalmente por LILLO ROMERO MIGUEL - 71368153G
Fecha: 2023.11.14 23:52:18 +01'00'

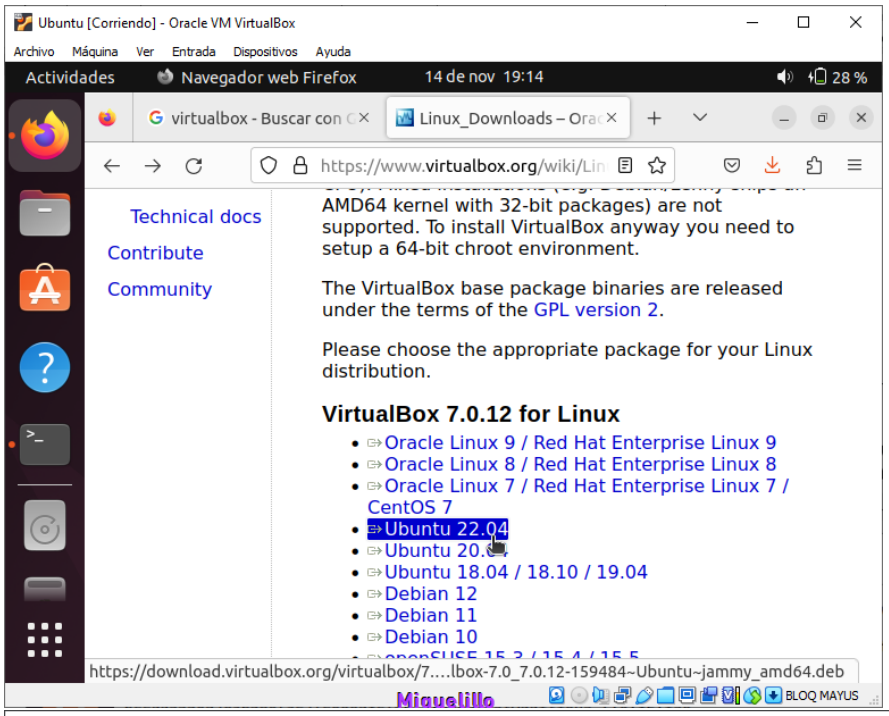
Ejercicio 1

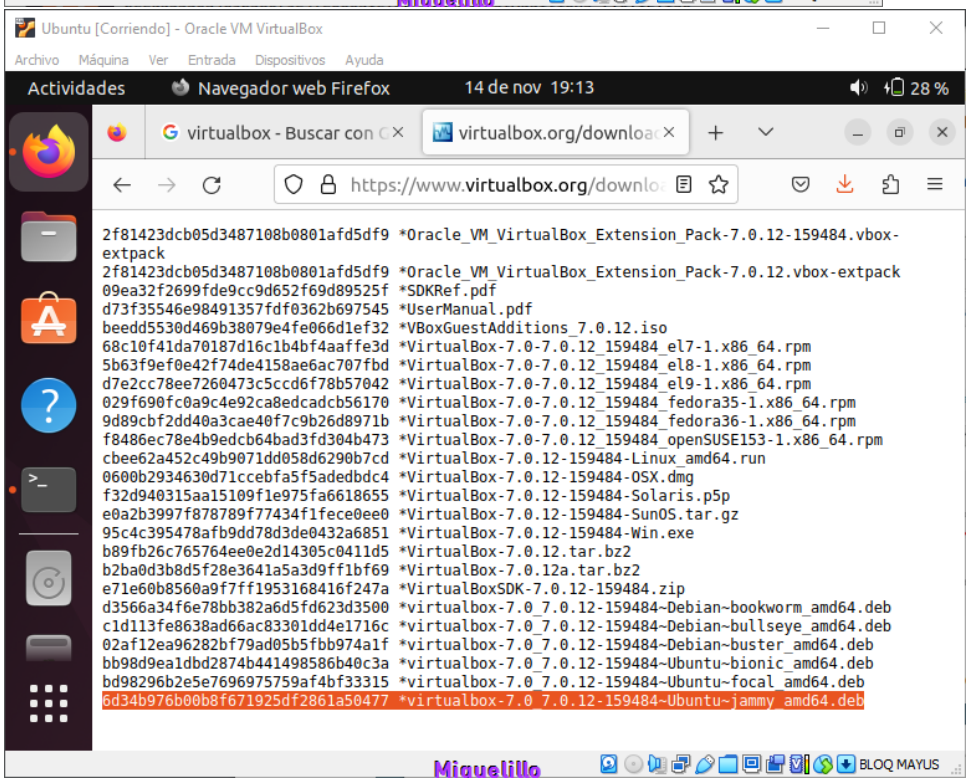
a) SISTEMA DE DETECCIÓN DE INTRUSOS (IDS): HostIDS

Solución:

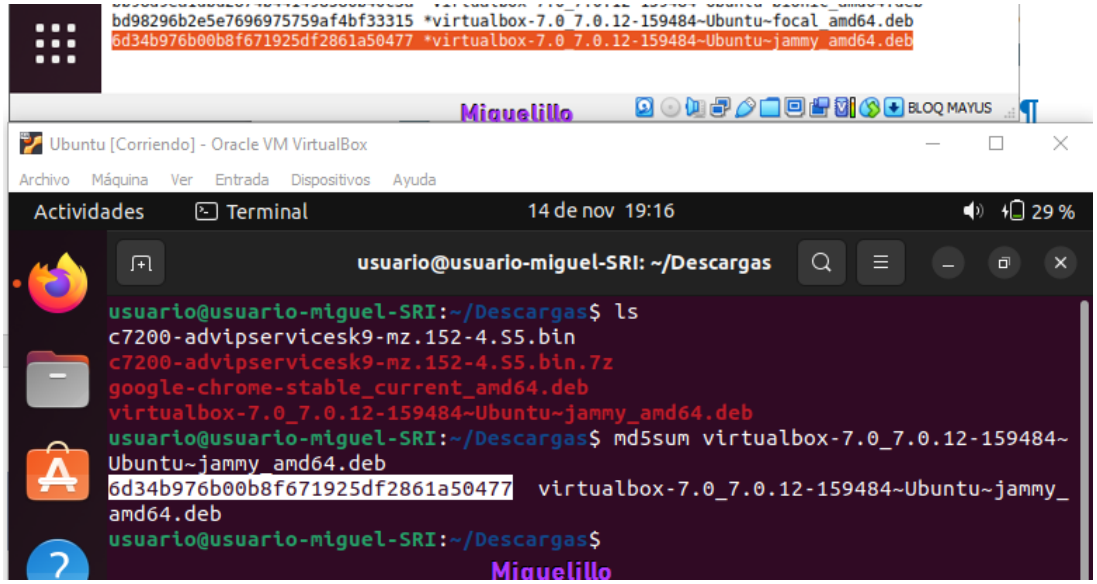
Linux

Descargamos un archivo y comprobamos el código hash que nos dan

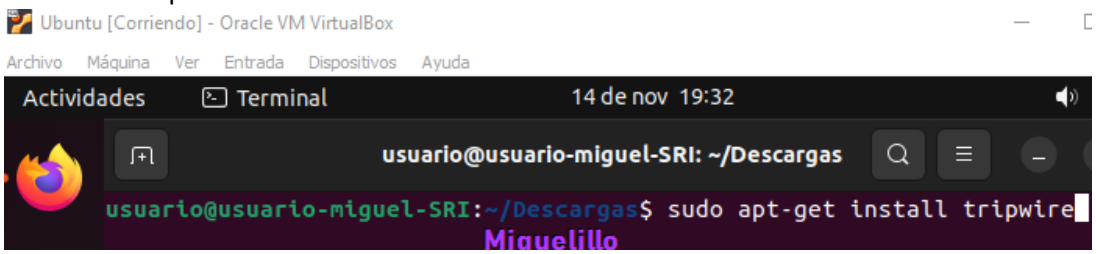




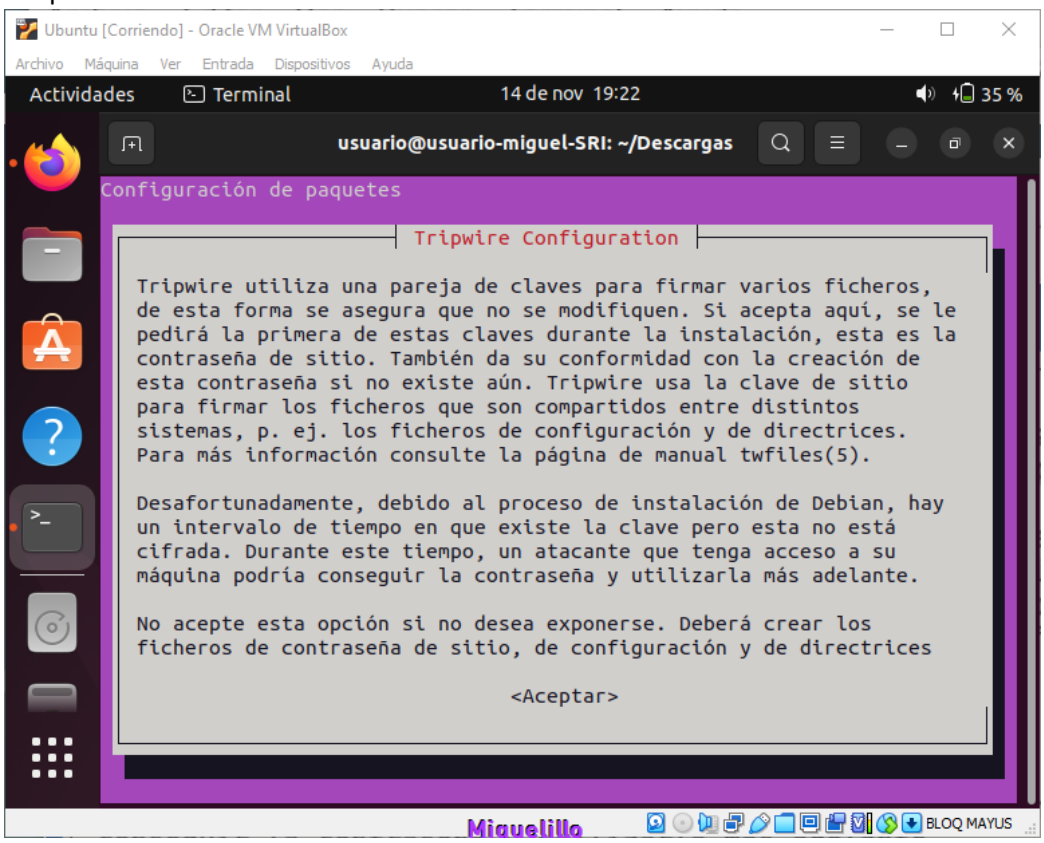
Comprobamos que los números coincidan



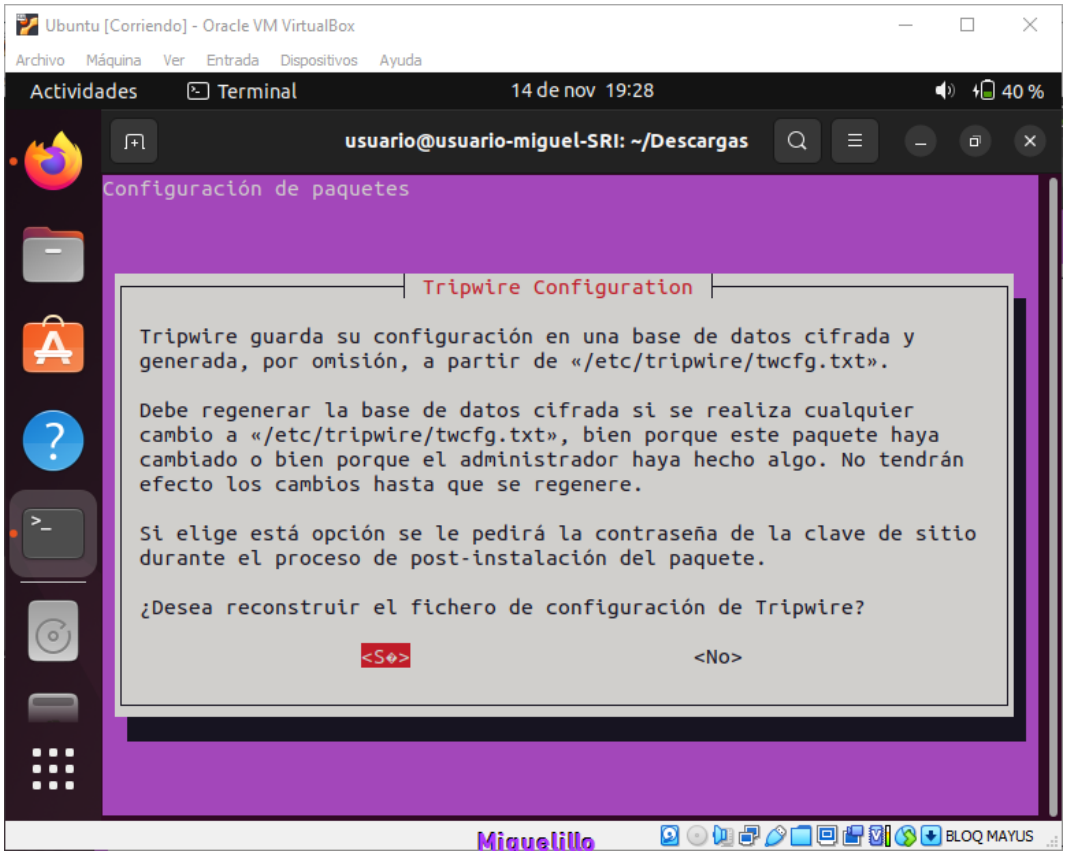
Instalamos tripware



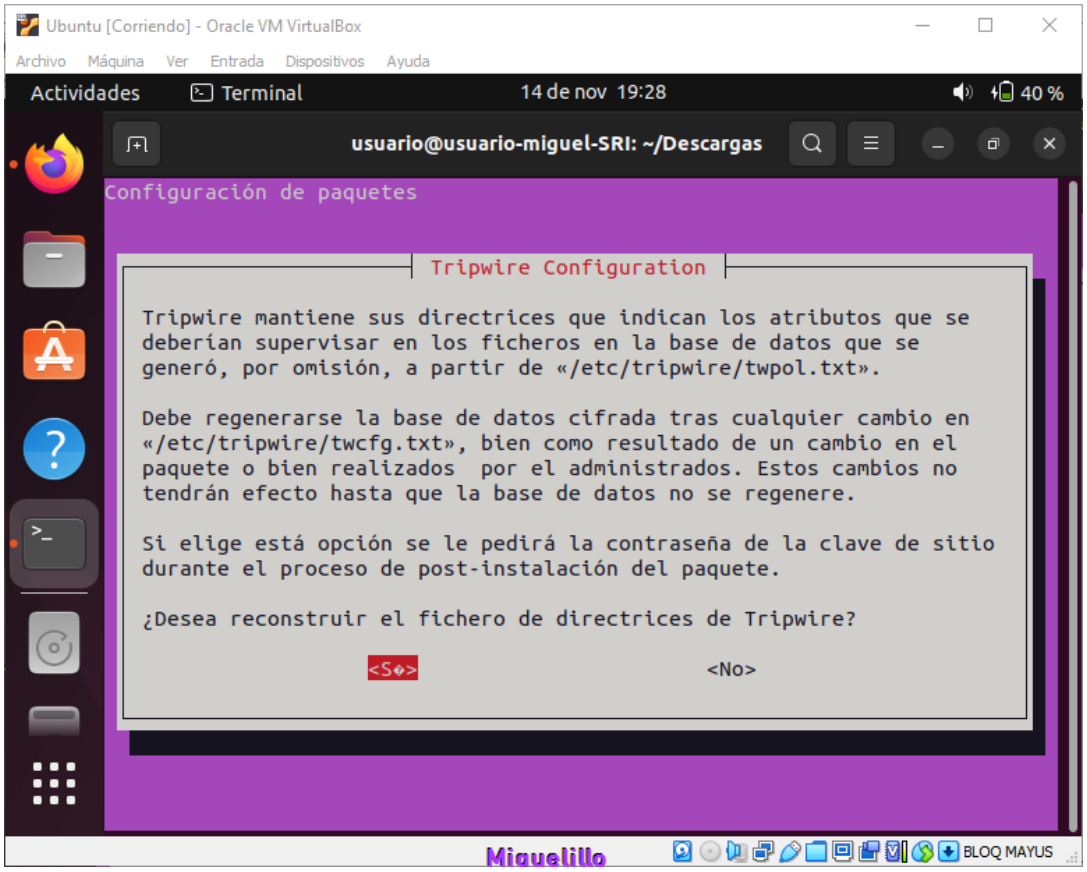
Aceptamos hacer las llaves



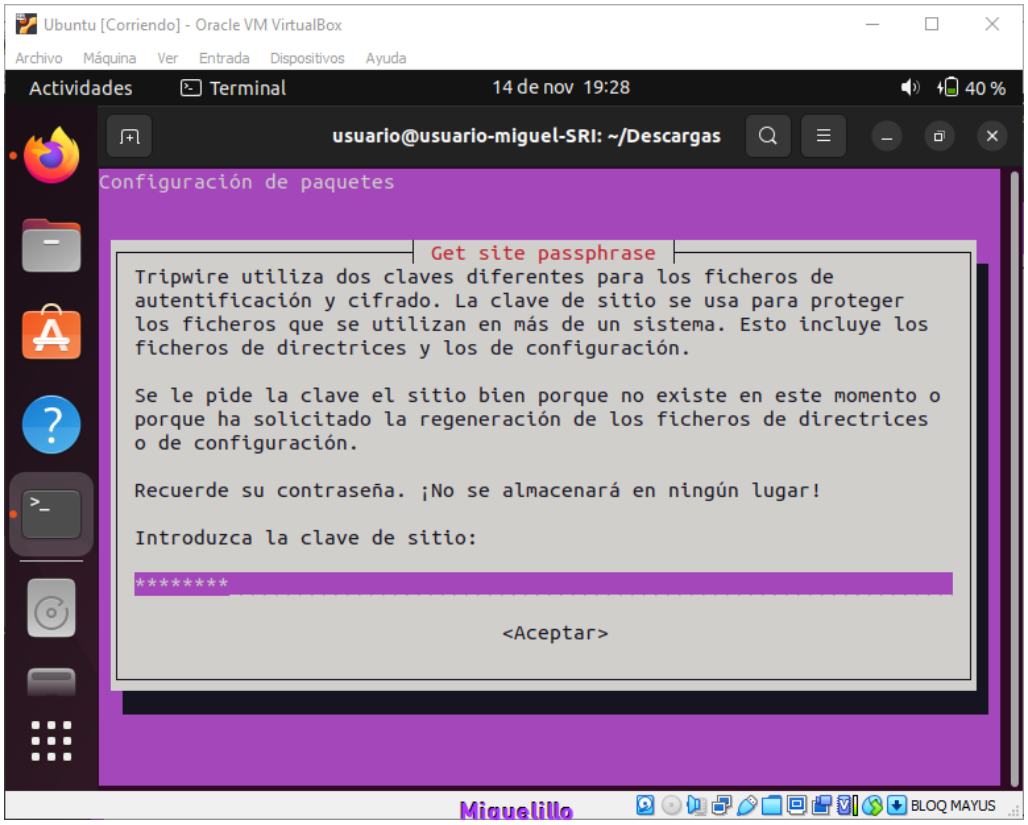
Reconstruimos el fichero de **Tripwire**



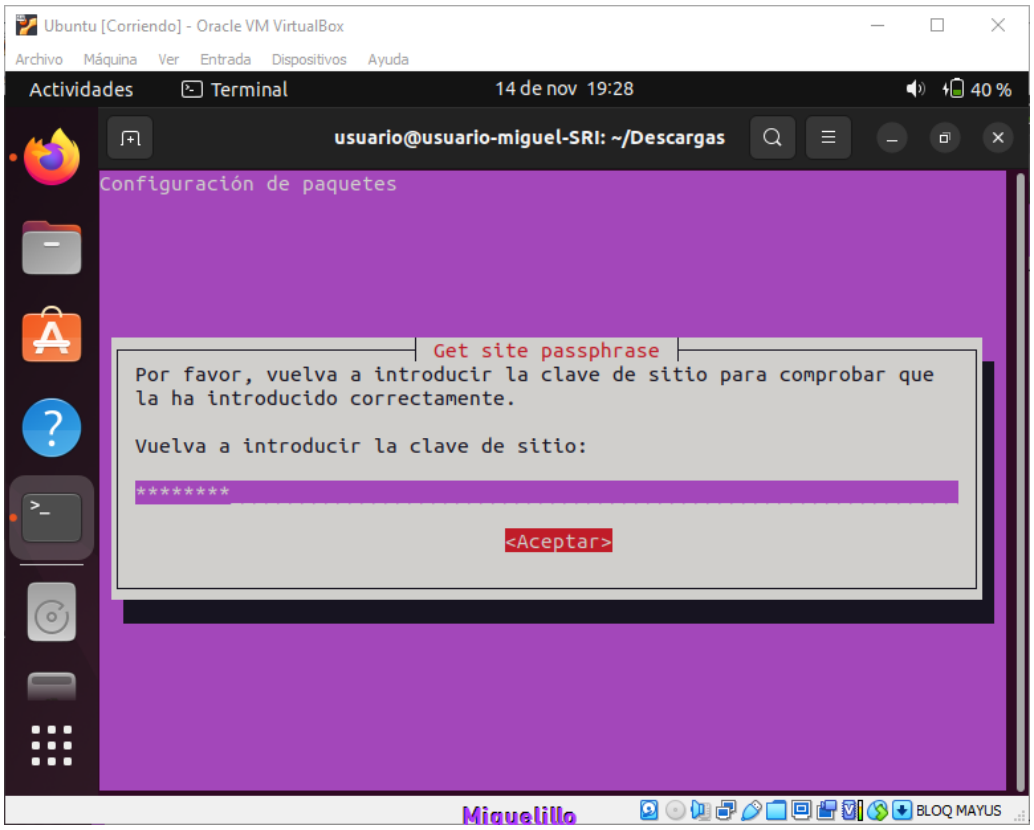
Reconstruimos las directrices de **Tripwire**



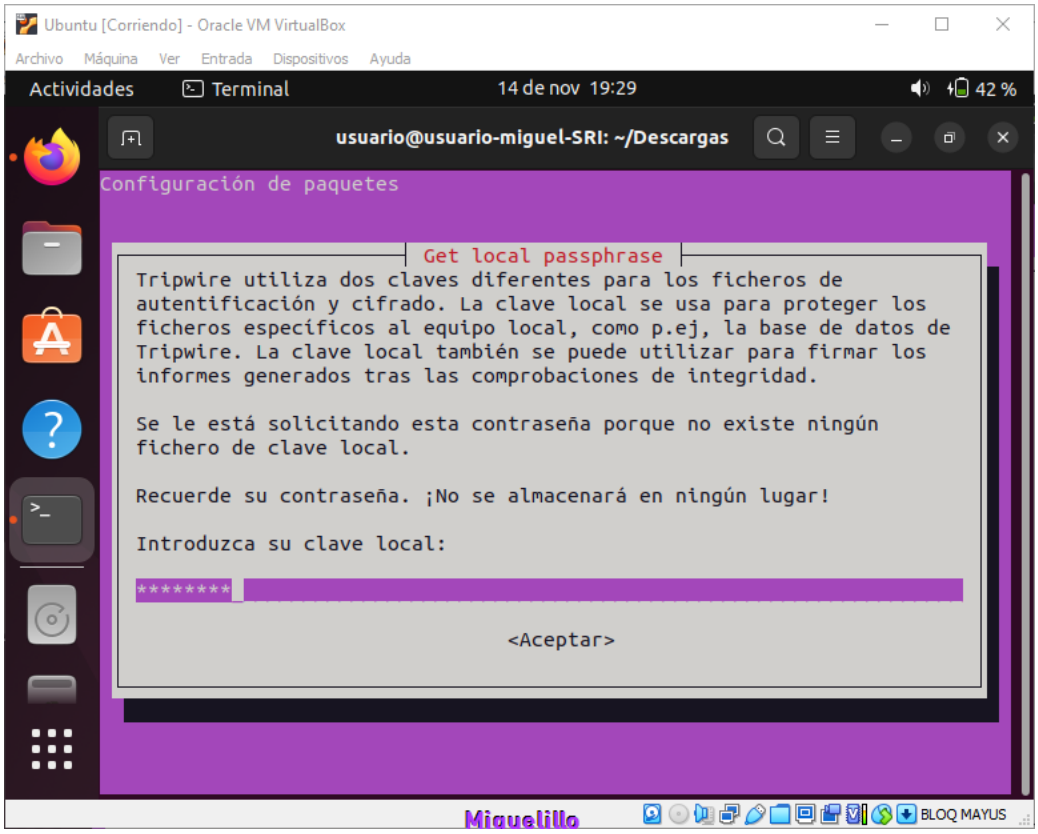
Introducimos la clave



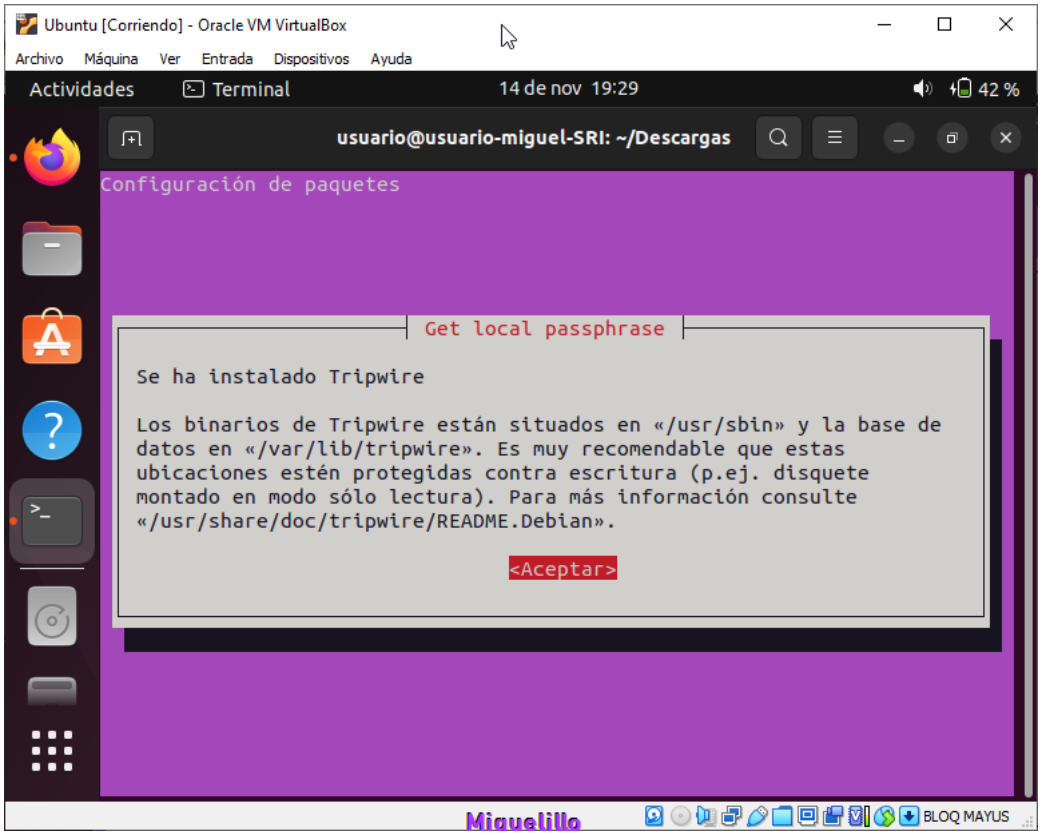
Confirmamos la clave



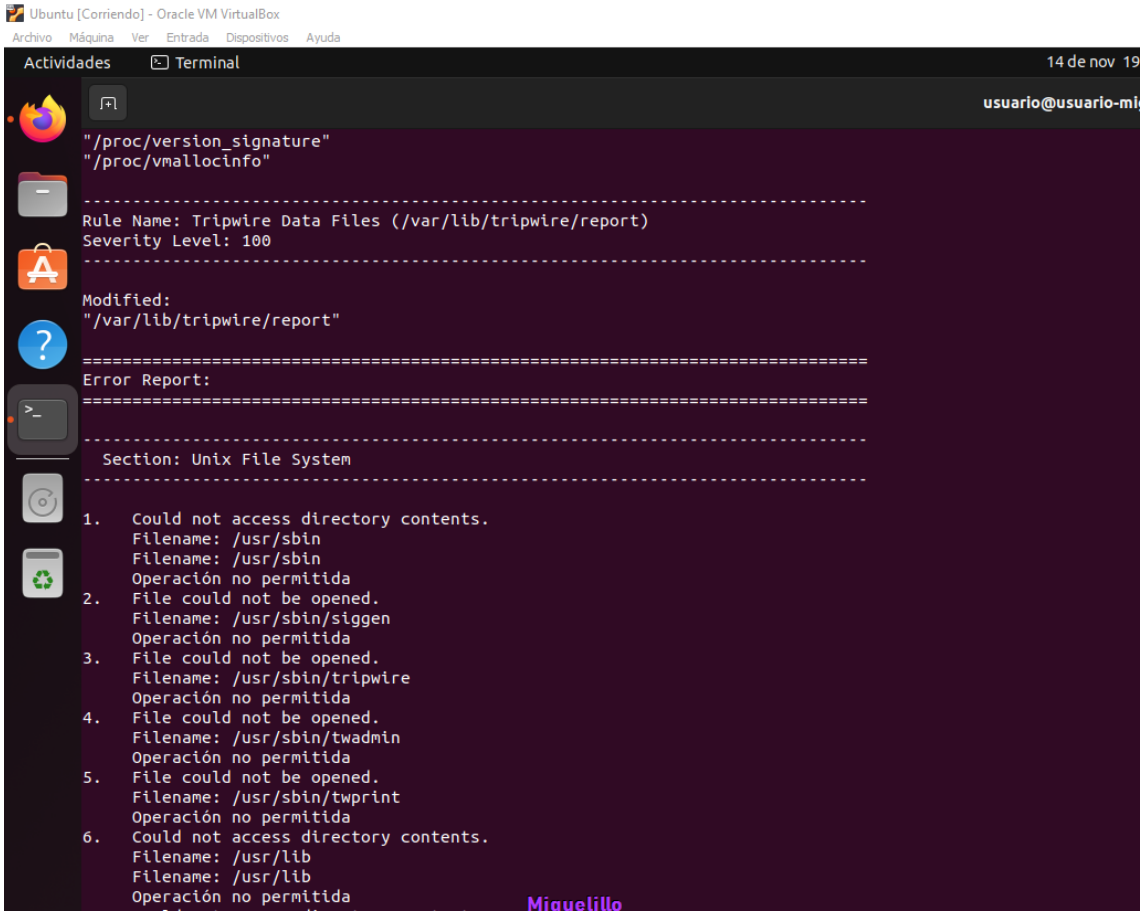
Introducimos su clave



Una vez instalado clicamos en Aceptar

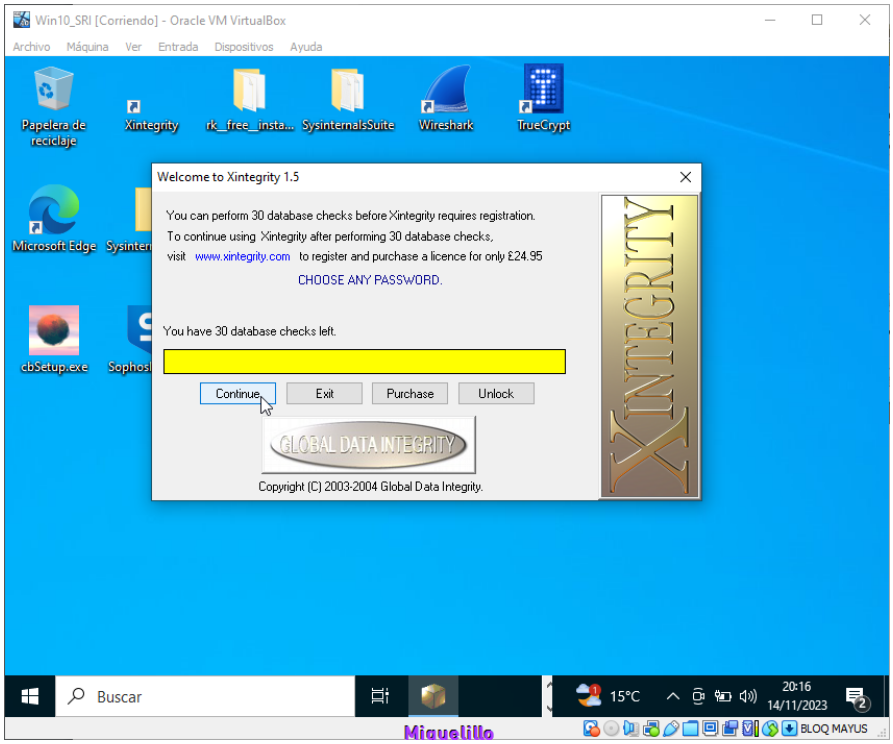


Con el comando `sudo tripwire –init` podemos ver los registros

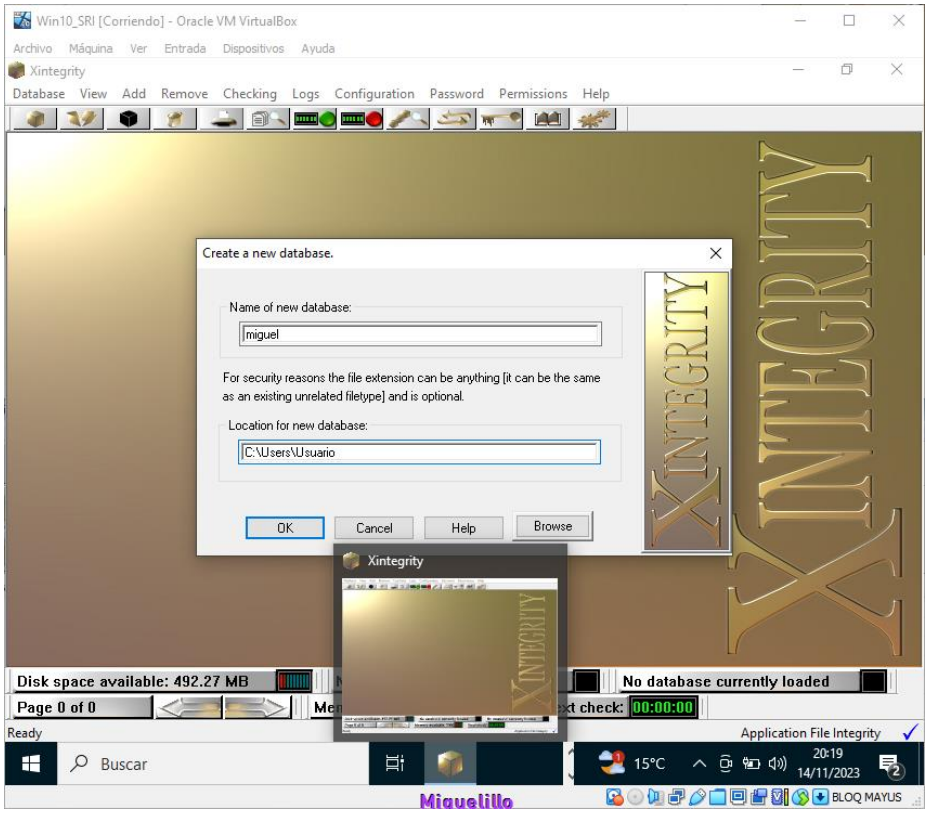


Windows

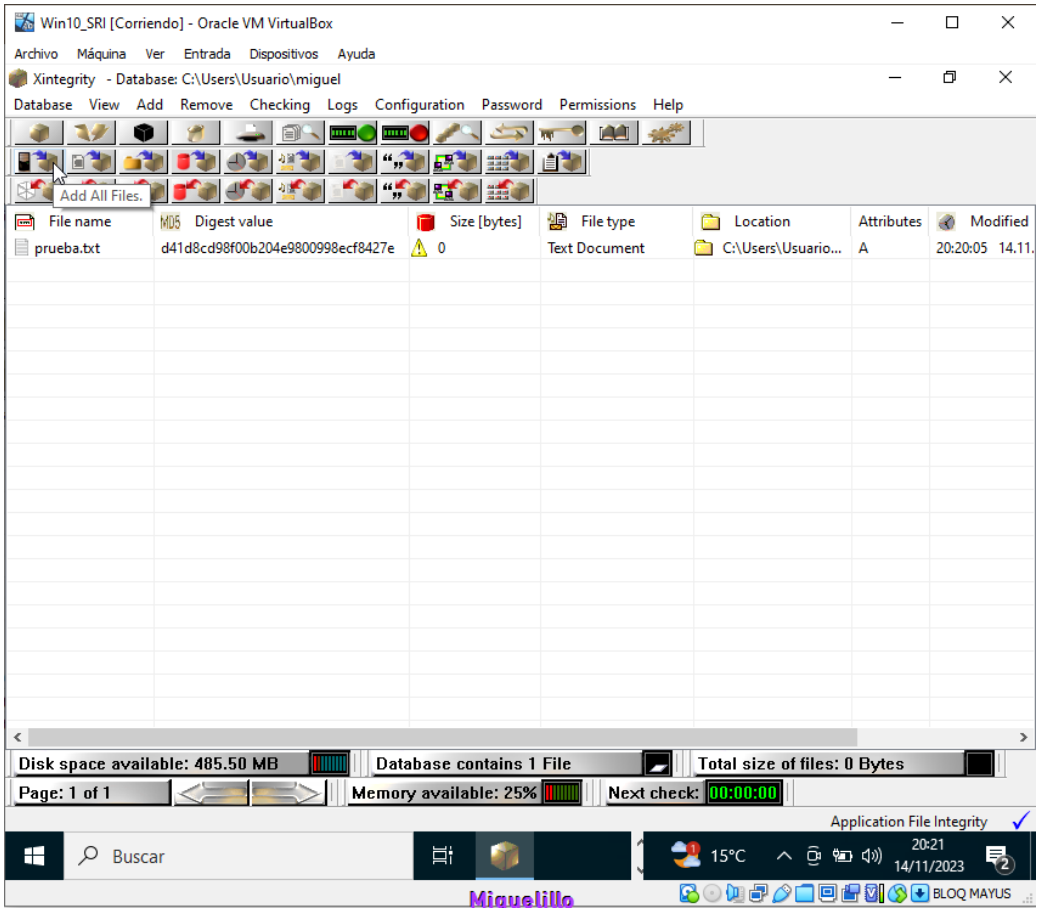
Instalamos Xintengrity le damos a → Continue



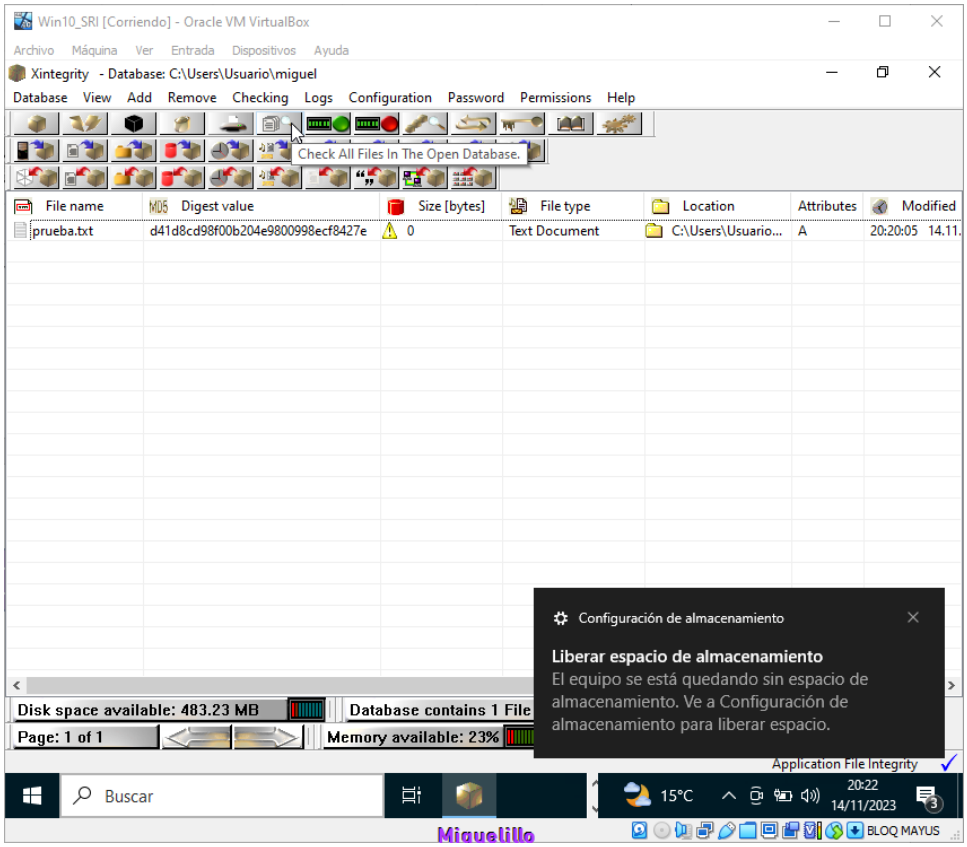
Clico en New database



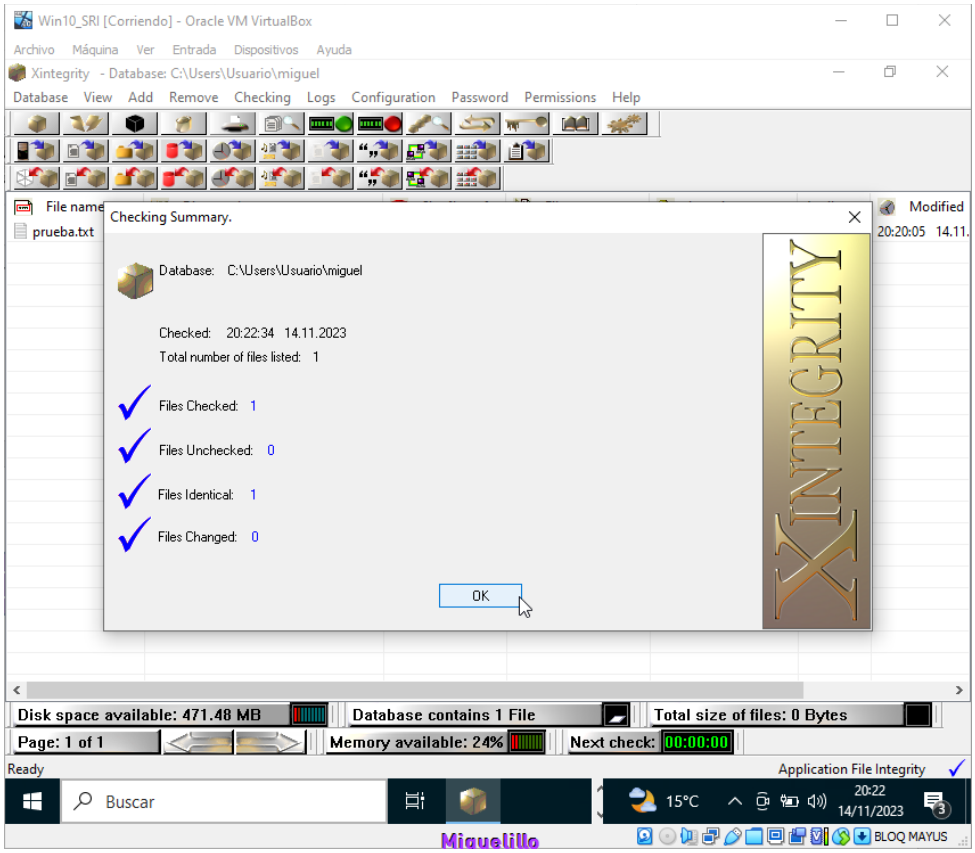
Clicamos para añadir un nuevo archivo



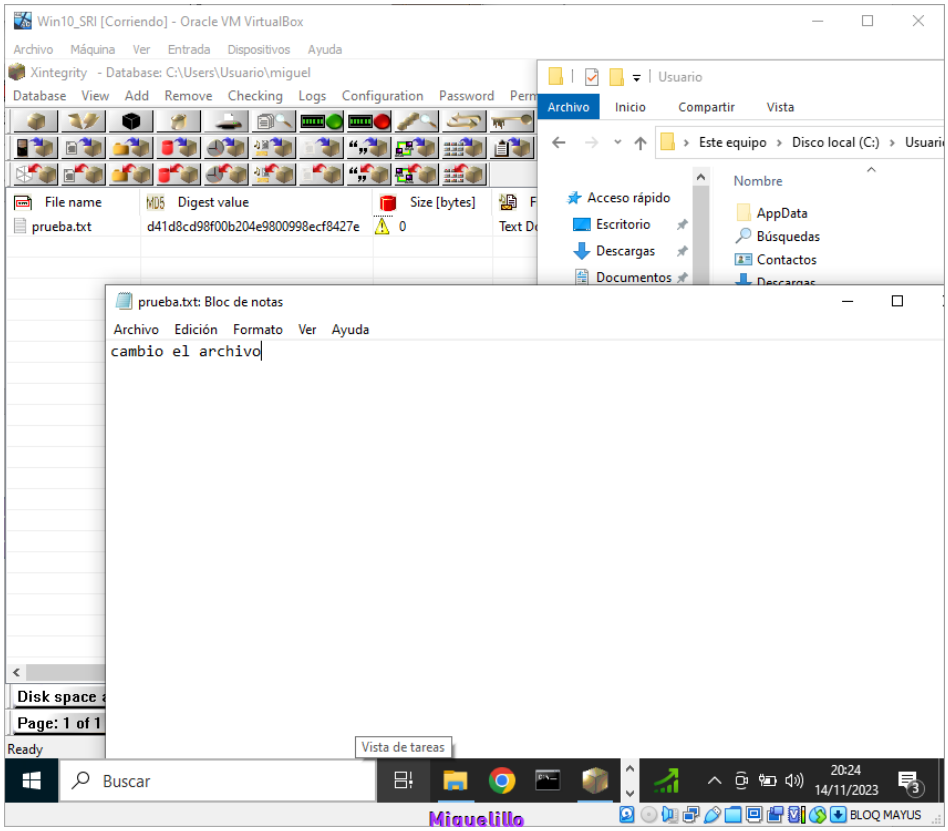
Podemos clicar en chequear para comprobar que no ha sido modificado



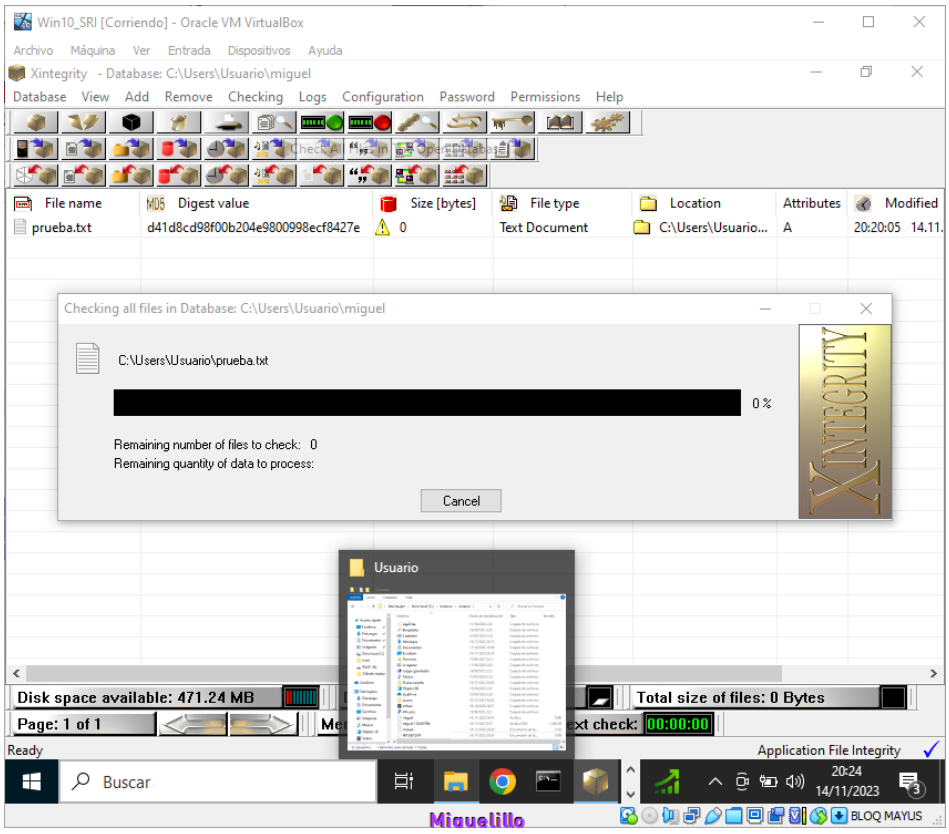
Nos muestra el resultado que no ha sido modificado



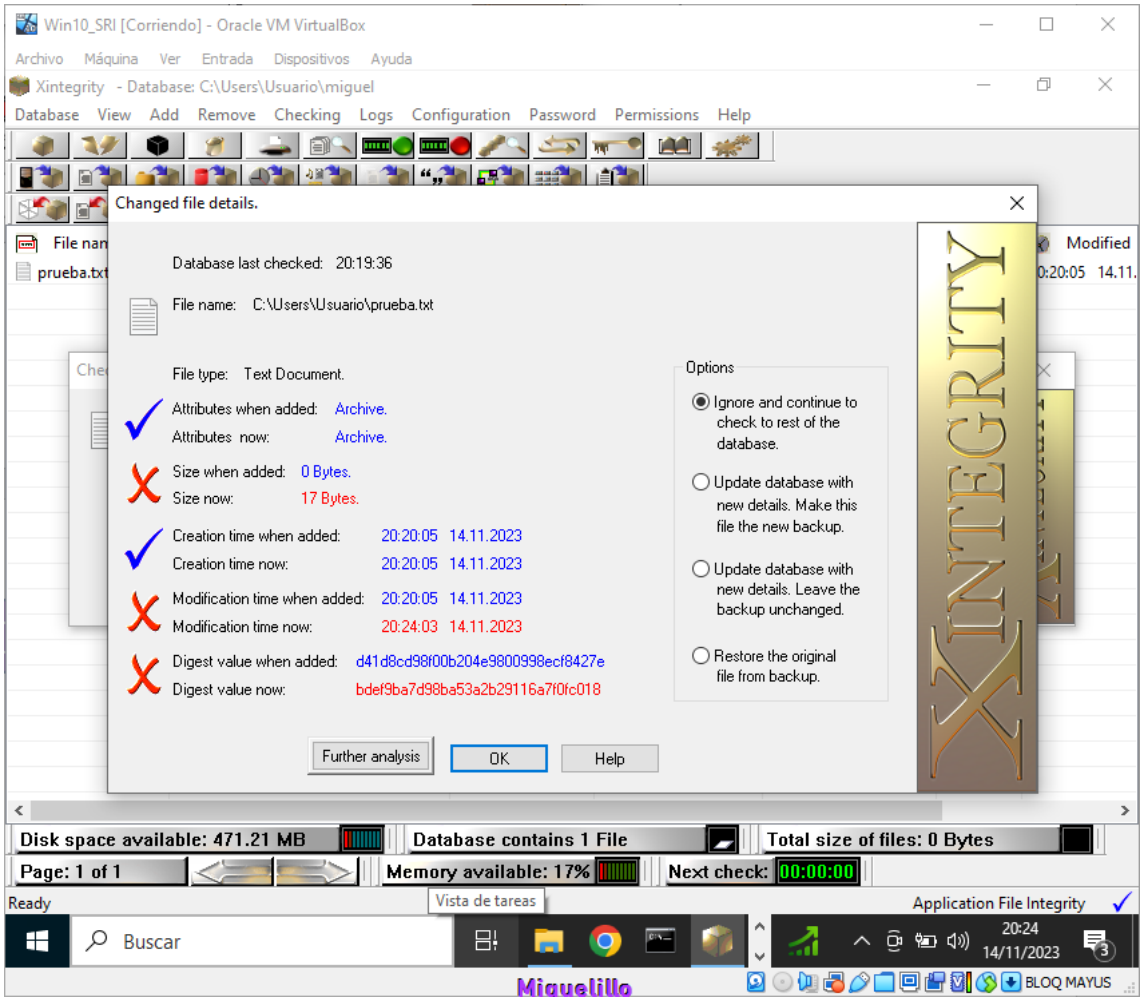
Lo cambiamos y volvemos a analizar



Volvemos a analizar



Vemos que ha sido modificado



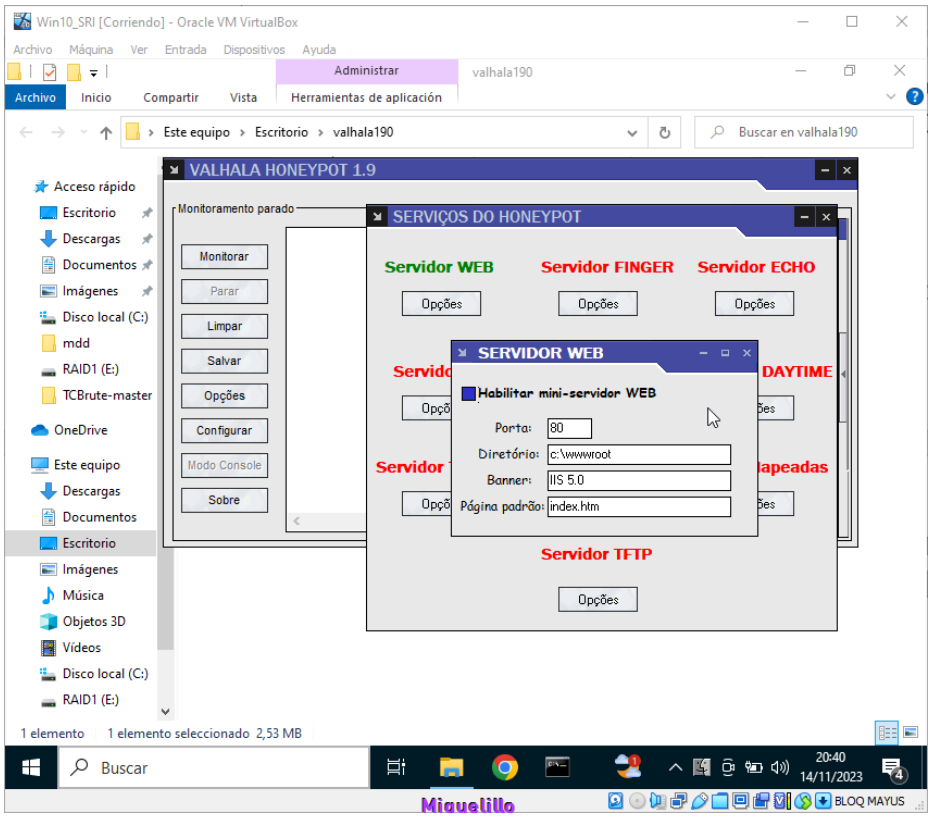
Honey pot

Un honeypot es una trampa de seguridad informática diseñada para atraer y detectar posibles ataques cibernéticos. Se utiliza para estudiar las tácticas, técnicas y procedimientos de los atacantes, así como para recopilar información sobre posibles amenazas y vulnerabilidades.

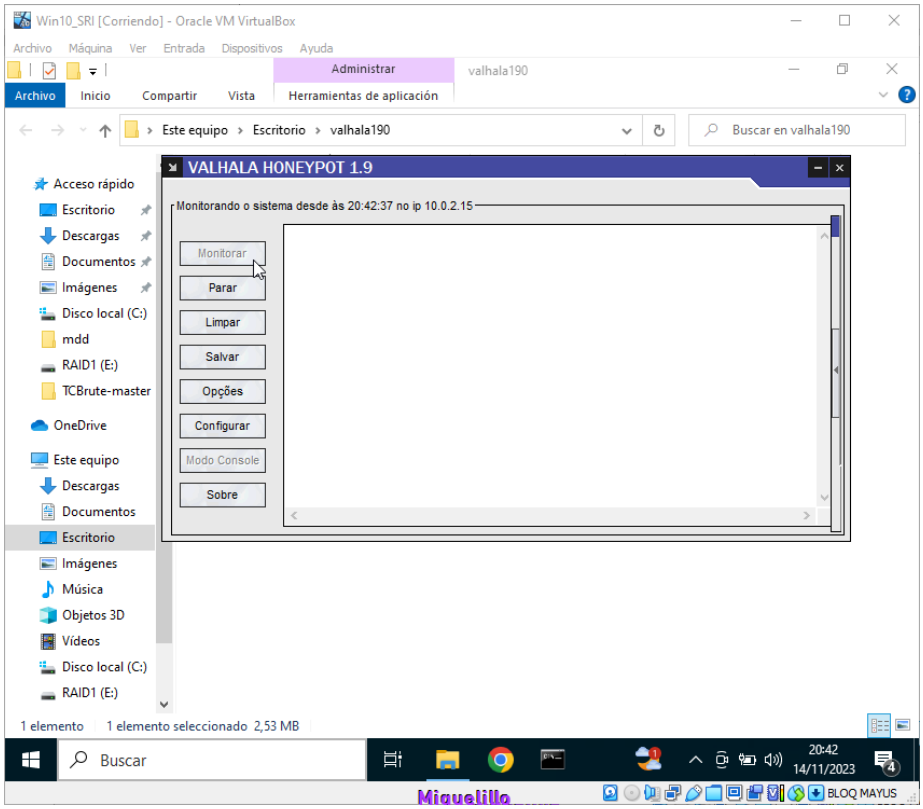
Listado de Software Honeypot:

- Honeyd: Simula múltiples servicios y sistemas operativos.
- Snort: Combina funciones de detección de intrusiones y honeypot.
- Cowrie: Emula un servidor SSH para atraer a atacantes.
- Dionaea: Honeypot de bajo-interacción que emula servicios de red.
- Glastopf: Emula vulnerabilidades web para atraer ataques web.
- Valhala Honeypot es un honeypot fácil de usar para el sistema Windows. El software cuenta con los siguientes servicios: http (web), ftp, tftp, finger, pop3, smtp, echo, daytime, telnet y redireccionamiento de puertos. Algunos servicios son reales, otros son una simulación.

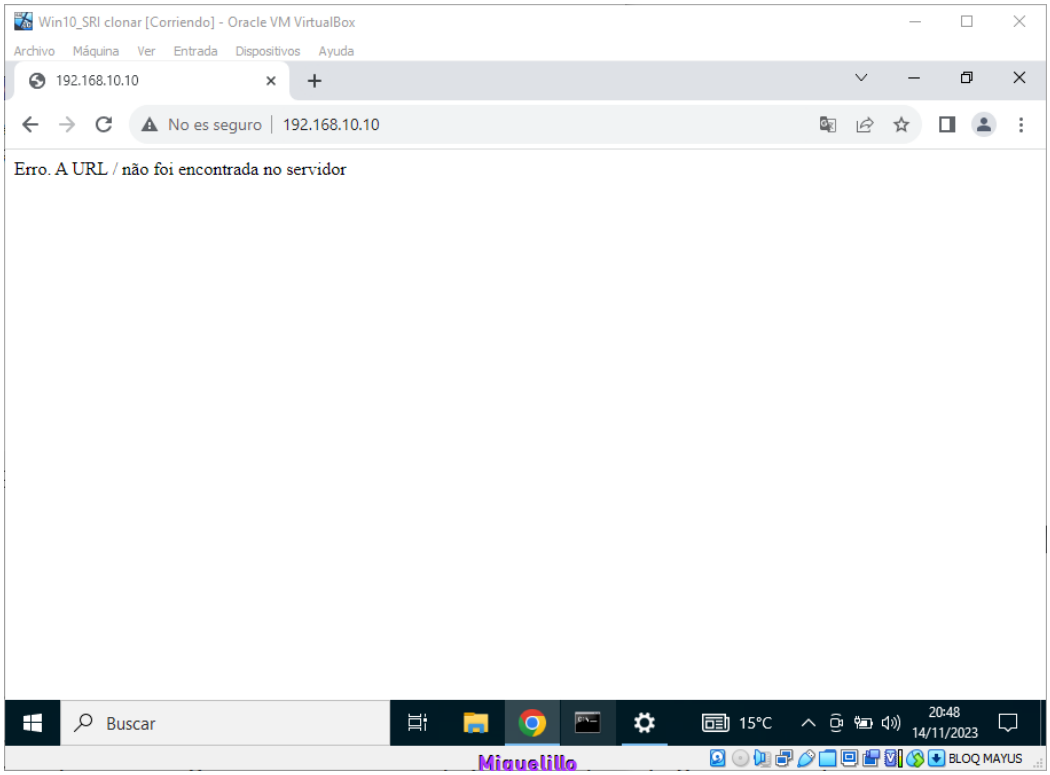
Voy a usar Valhala que es una aplicación portable para activar los servicios del honeypot vamos a **Opçones→Servidor WEB→ Opçones** y marcamos **Habilitar mini-servidor WEB**



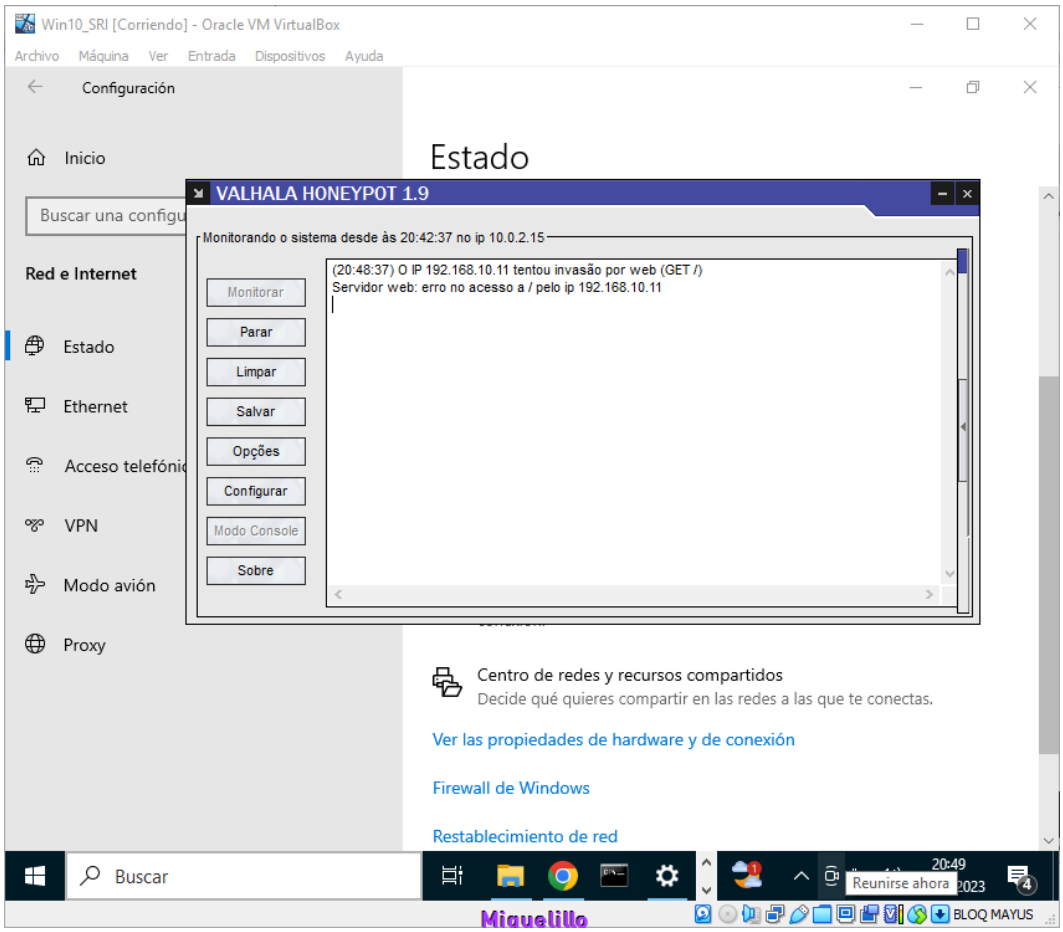
Y clicamos en **Monitorear**



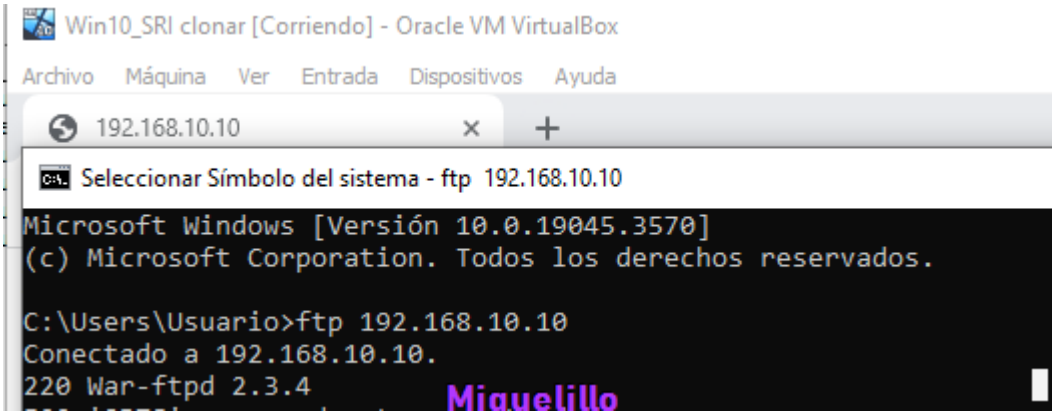
Desde un cliente accedemos al servicio web



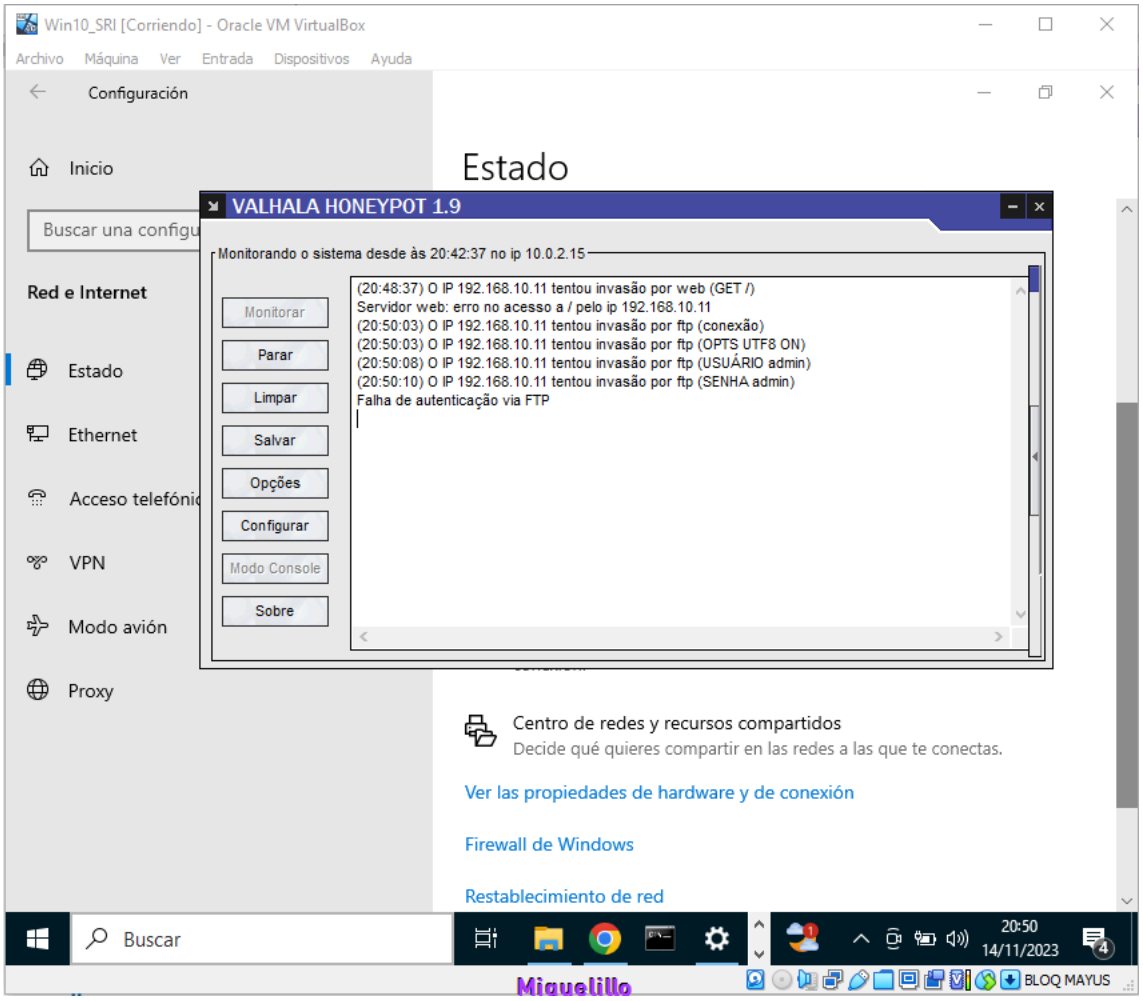
Registra la IP en el honeypot y que han intentado acceder



Probamos a acceder por ftp



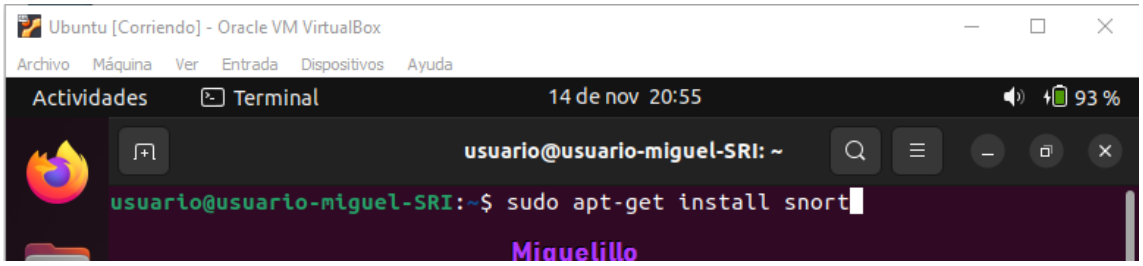
Podemos ver el fallo de autentificación y los registros con la IP



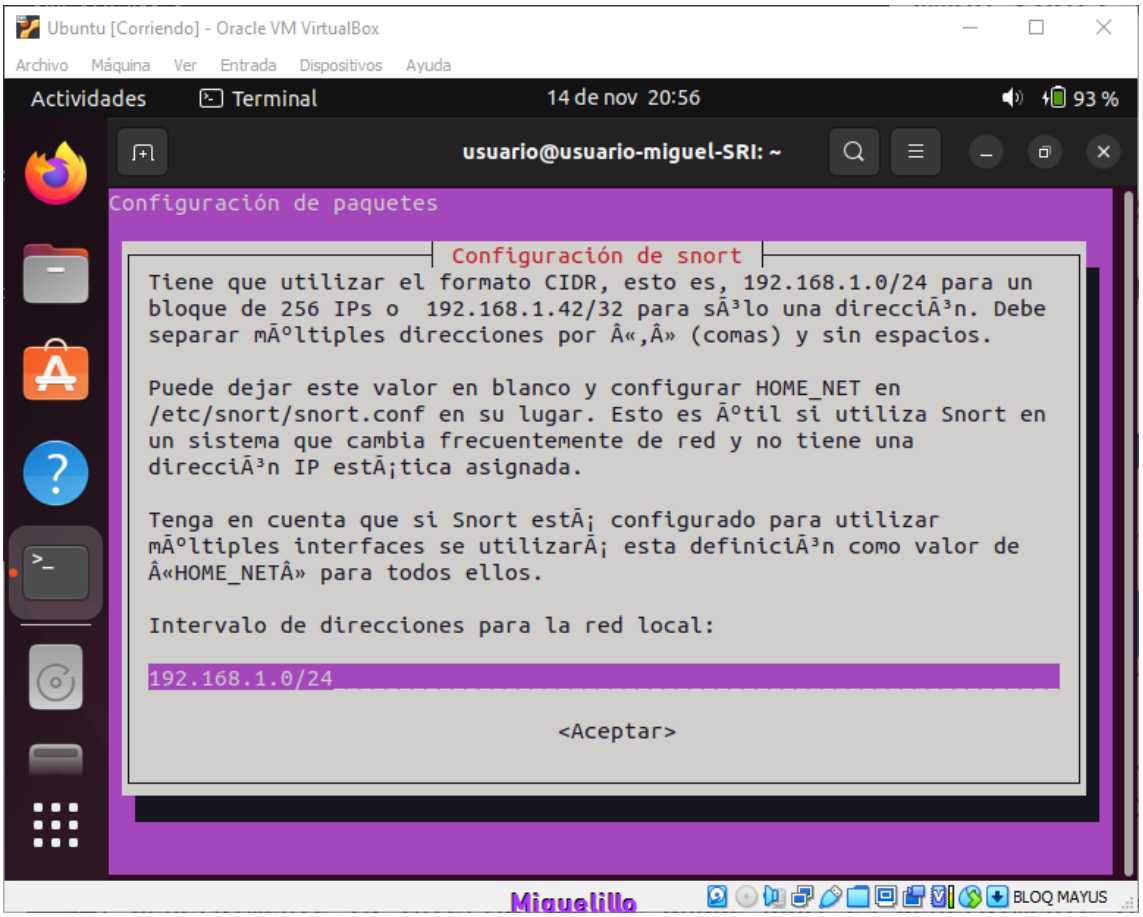
b) SISTEMA DE DETECCIÓN DE INTRUSOS (IDS) : NetIDS

Solución:

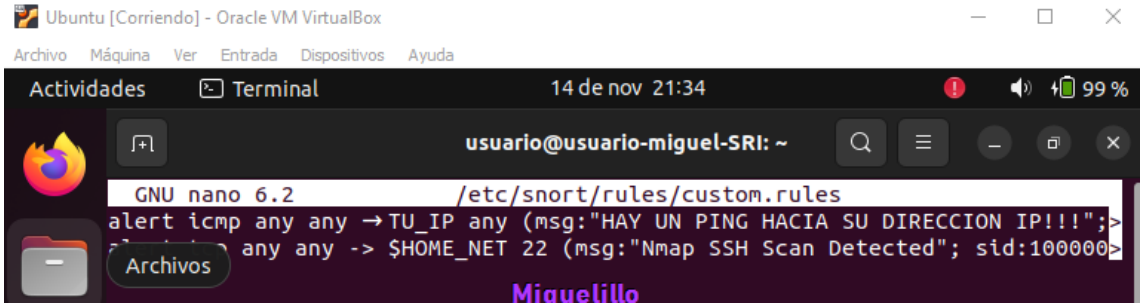
Instalamos Snort



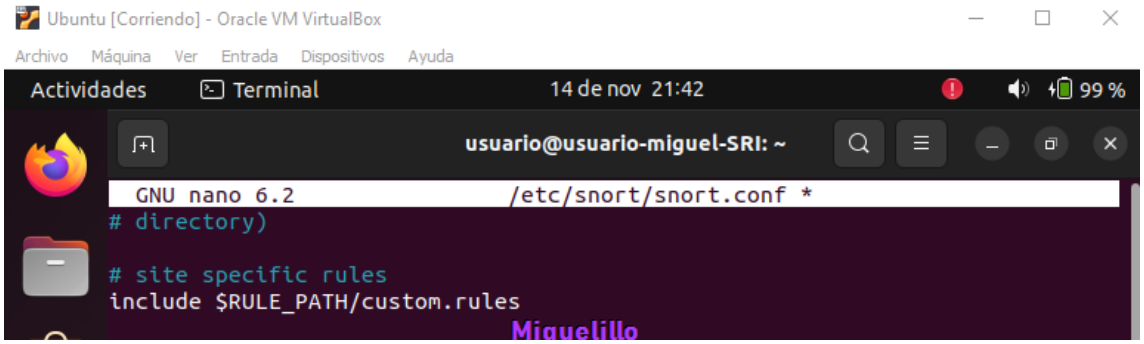
Configuramos la red



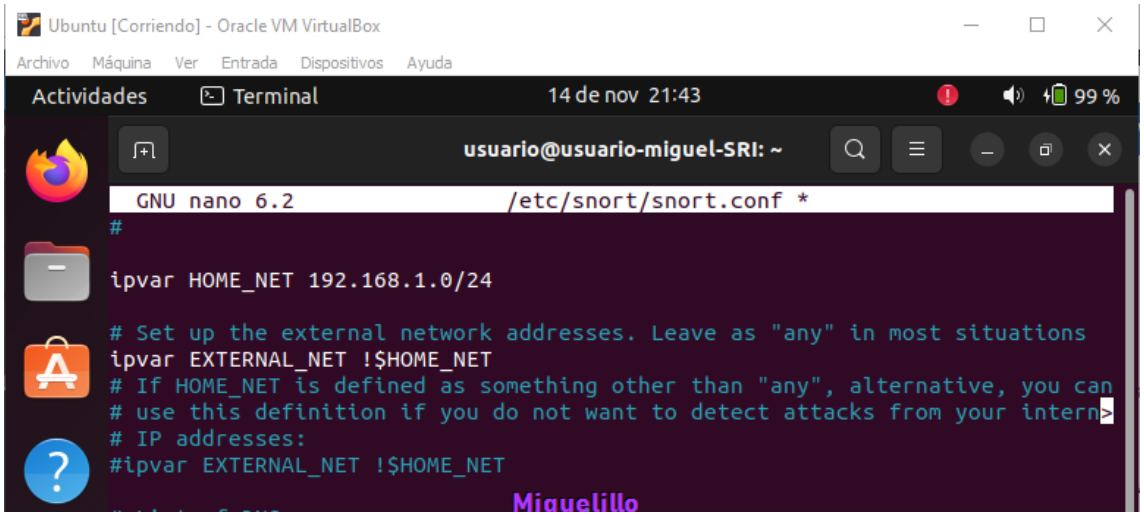
Creamos un archivo con regla para detectar NMAP y pings a el router este archivo estará en **/etc/snort/rules** y se llamará **custom.rules**



En el archivo snort.conf declaramos donde se encuentran las reglas



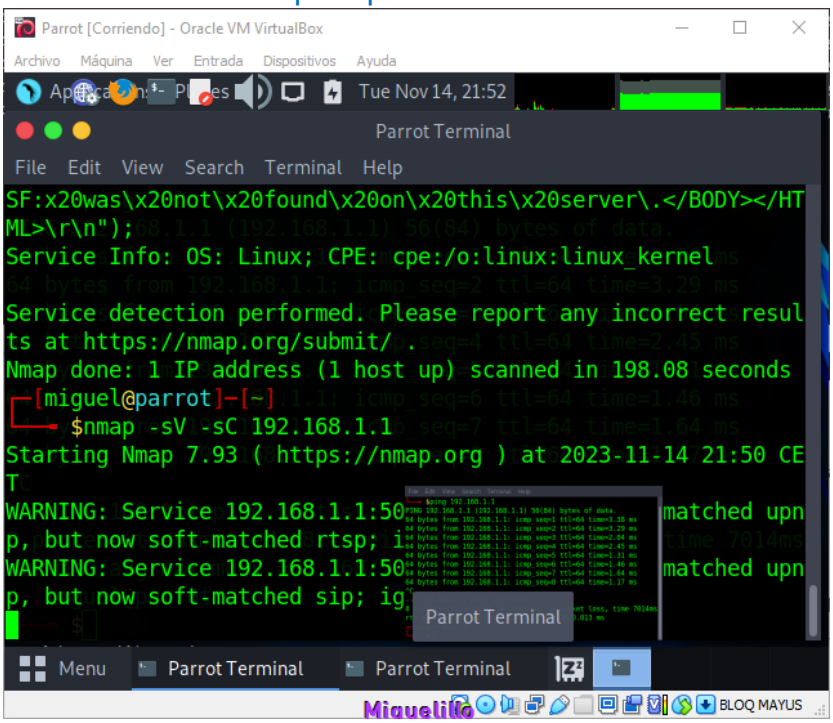
Declaramos la dirección de red y guardamos



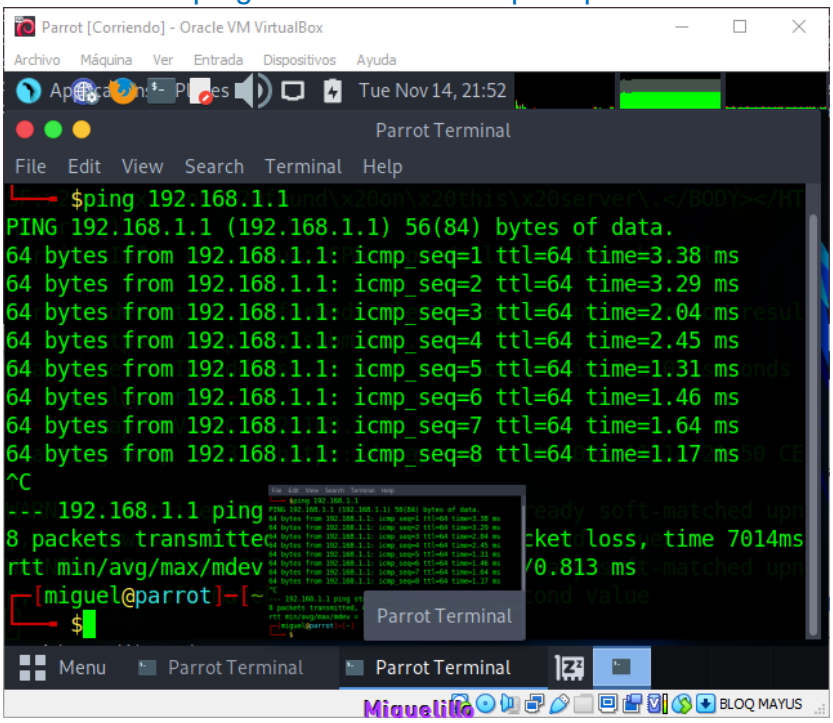
Importante darle permisos al archivo que hemos creado

Ejecutamos el snort con nuestra reglas

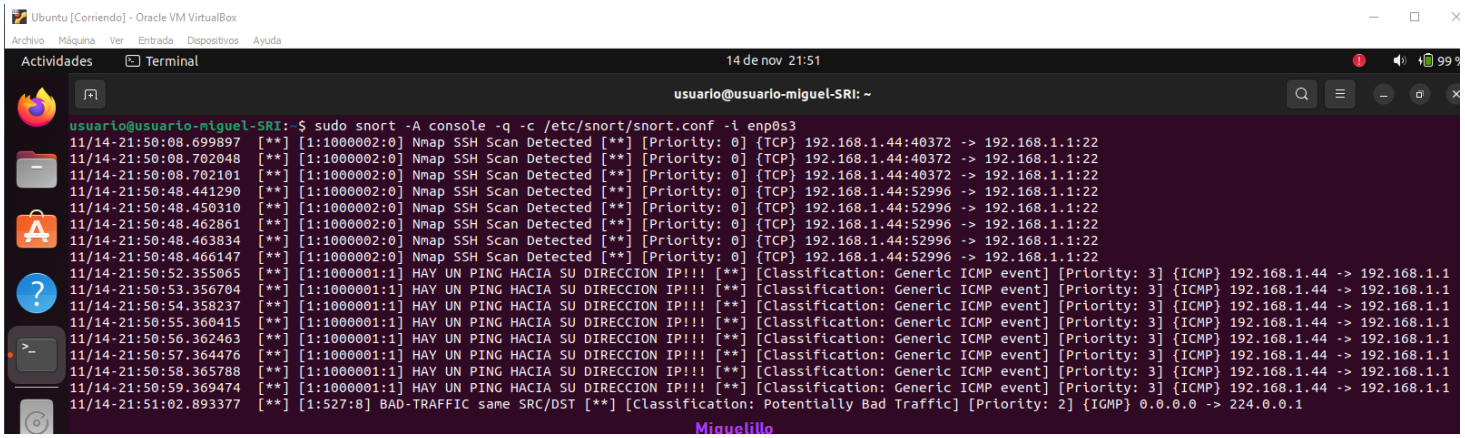
Hacemos un NMAP para probarlo



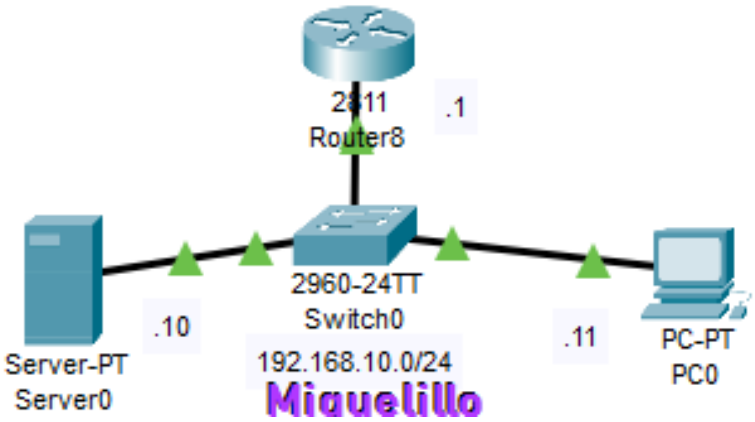
Hacemos un ping al router también para probarlo



Vemos como lo detecta la regla

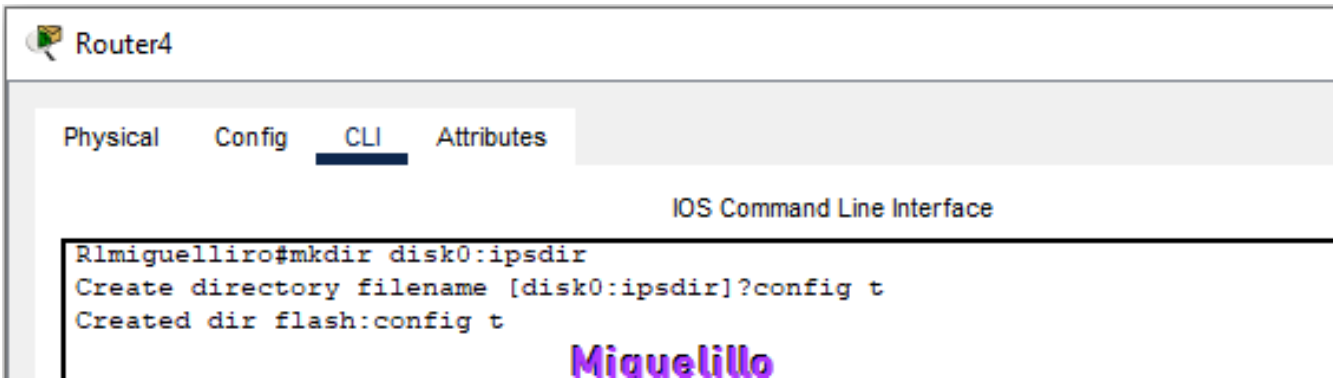


Escenario

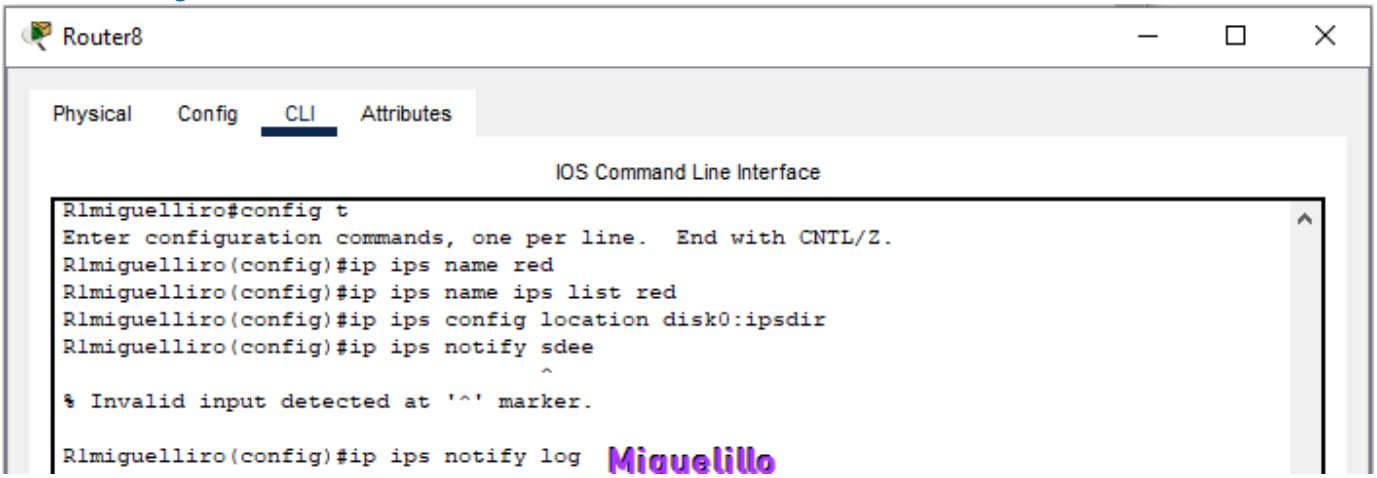


Configuramos los parámetros básicos del router, como la dirección IP

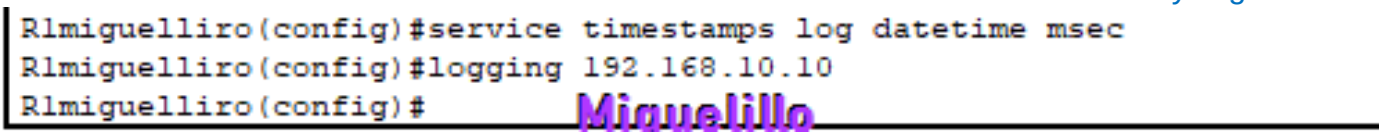
Creo la carpeta ipsdir



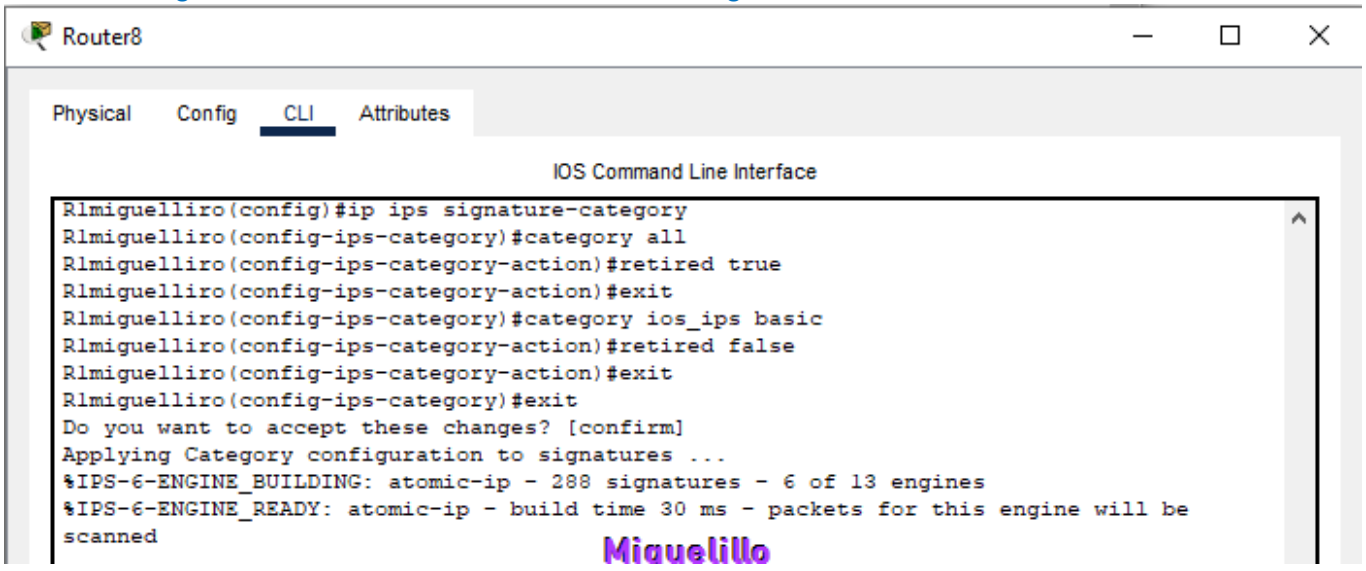
Configuramos el IPS



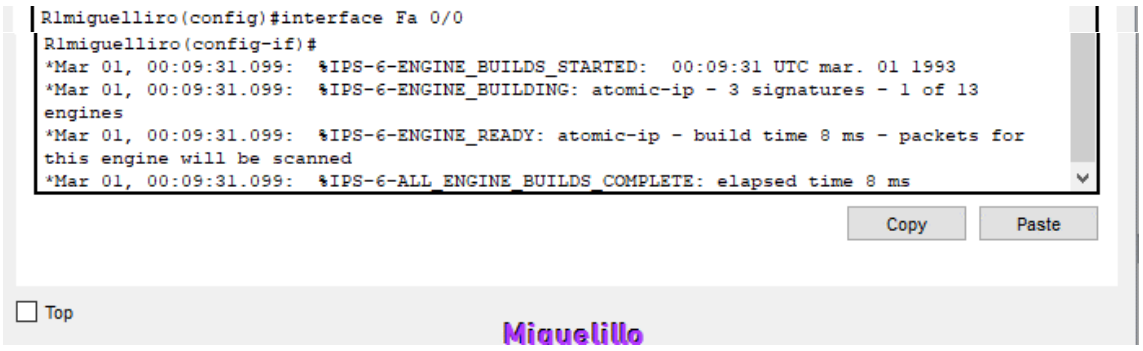
Añadimos el syslog



Configuramos la categoría del IPS



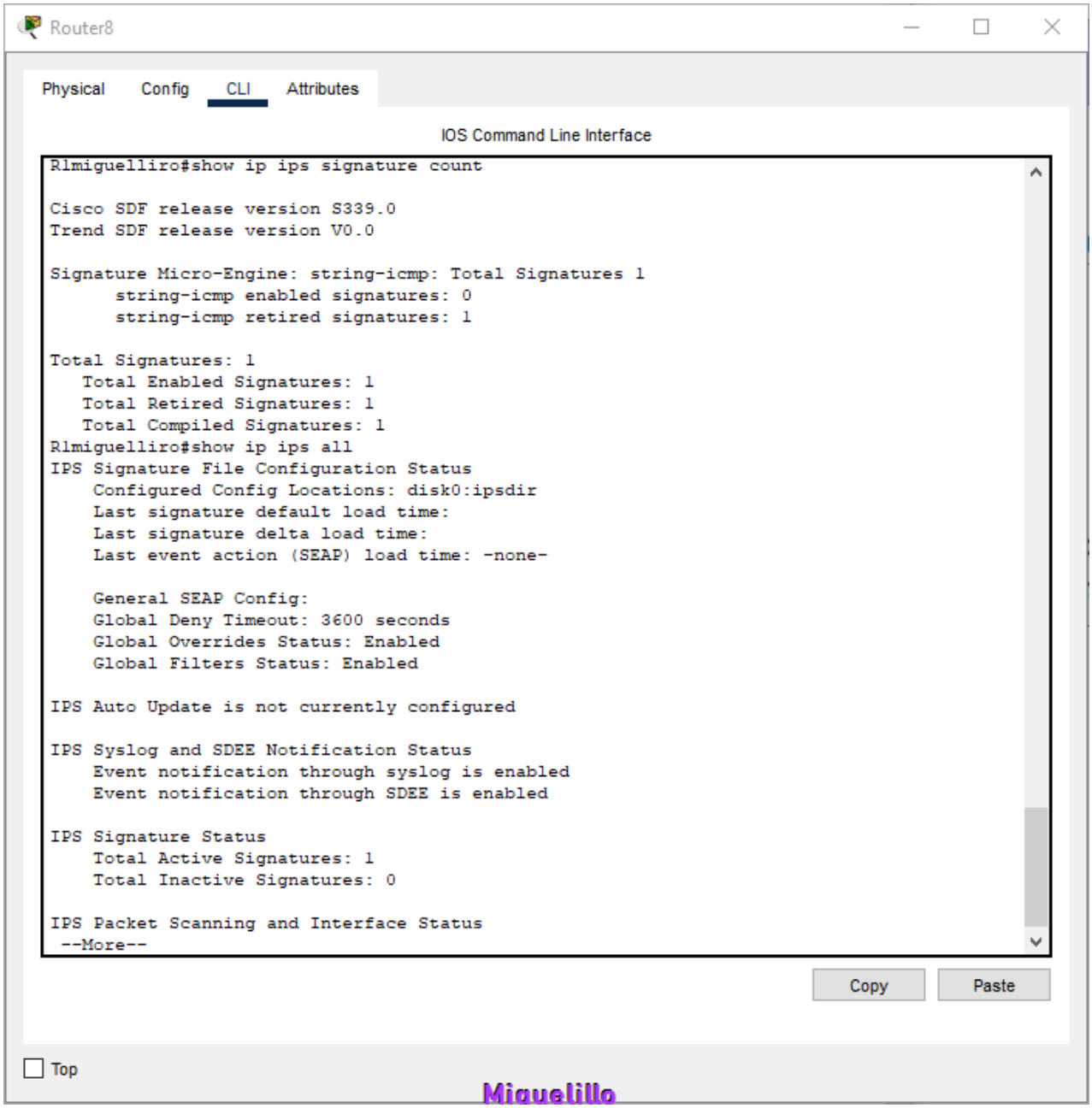
Configuramos la interfaz



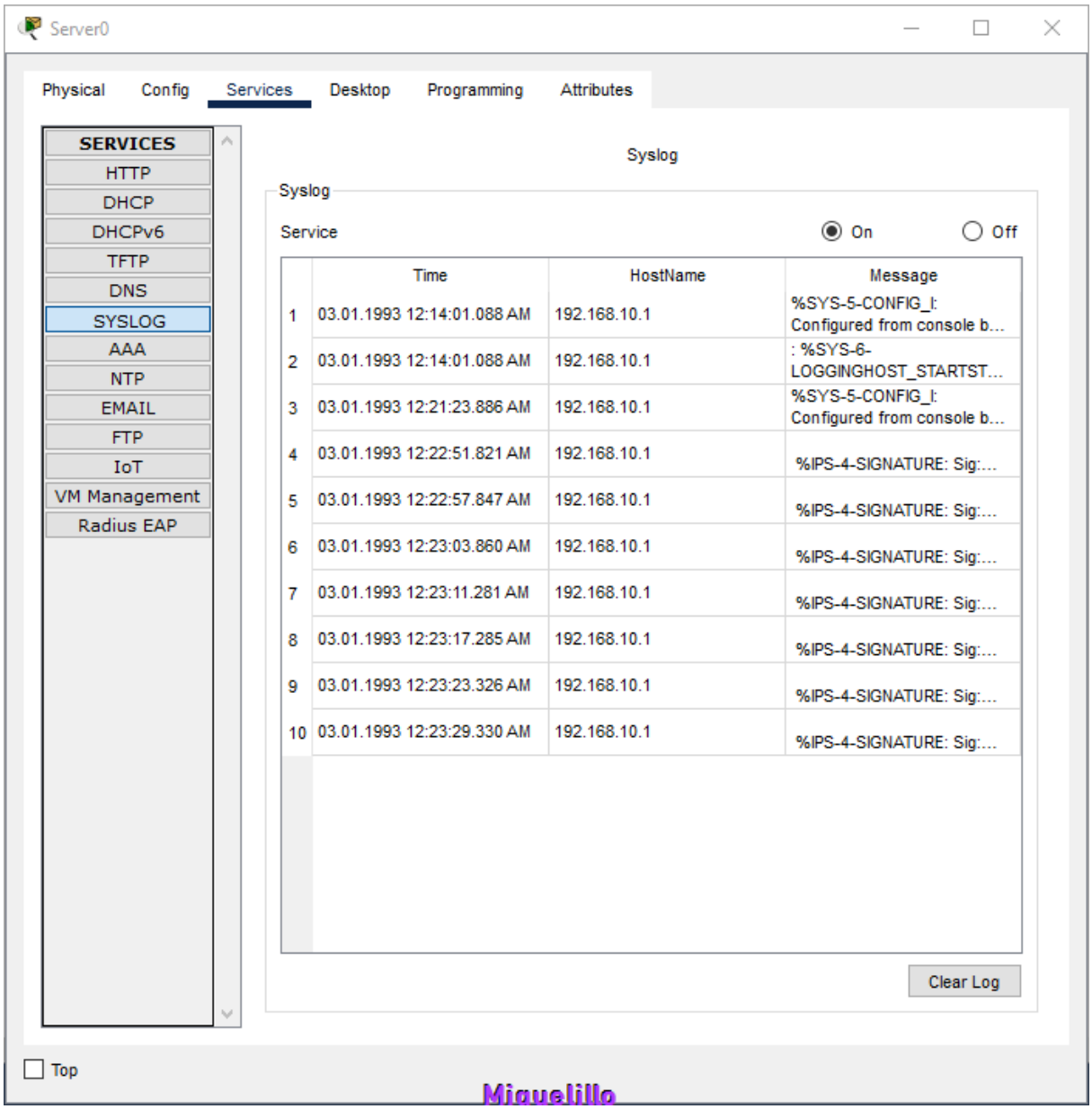
Configuramos los eventos del IPS para que se notifique al Syslog

```
Rlmiguelliro(config)#ip ips signature-definition
Rlmiguelliro(config-sigdef)#signature 2004 0
Rlmiguelliro(config-sigdef-sig)#status
Rlmiguelliro(config-sigdef-sig-status)#retired false
Rlmiguelliro(config-sigdef-sig-status)#enable true
Rlmiguelliro(config-sigdef-sig-status)#engine
Rlmiguelliro(config-sigdef-sig-engine)#event-action produce-alert
Rlmiguelliro(config-sigdef-sig-engine)#event-action deny-paket-inline
```


Podemos ver la configuración del IPS



Mensajes de syslog



Ping desde cliente