

Practica 03

Uso de Windows SFC

Uso de GNU/LINUX Rootkit Hunter

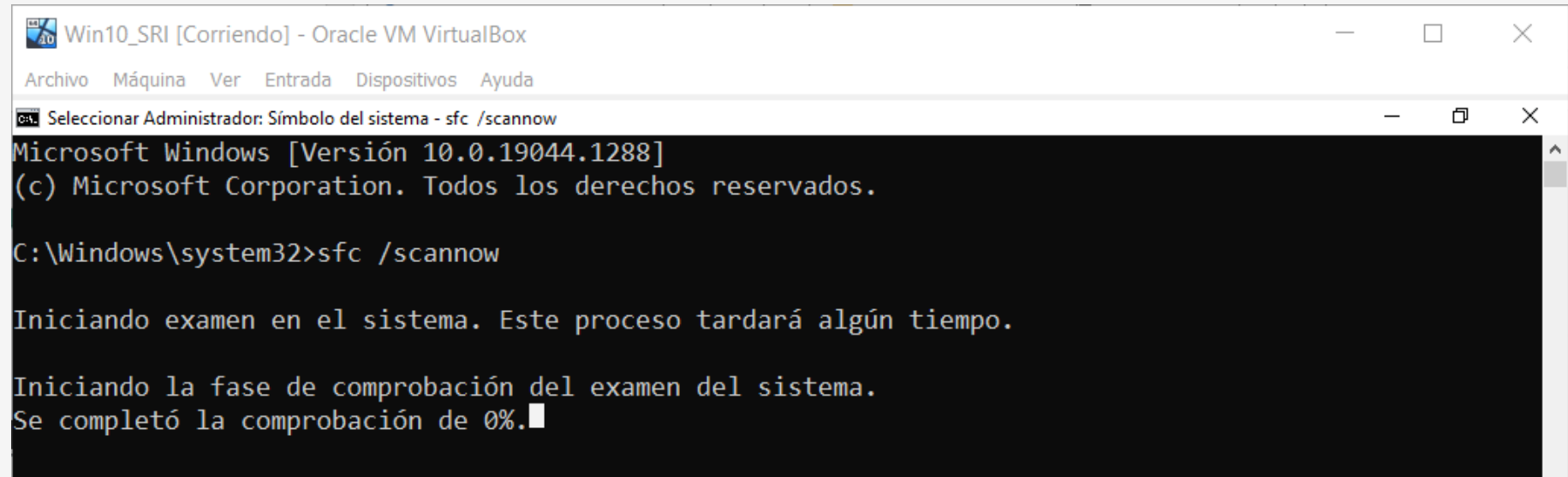
Windows SFC

¿Qué es SFC?

SFC o (System File Checker) es una utilidad de Windows que verifica y repara archivos de sistema dañados o faltantes en el sistema operativo para mantener la estabilidad y el rendimiento del sistema.

Windows SFC

Ejecutamos el CMD como administrador
Introducimos el comando *sfc /scannow*



The screenshot shows a Windows 10 command prompt window titled "Win10_SRI [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The command prompt shows the following text:

```
Seleccionar Administrador: Símbolo del sistema - sfc /scannow
Microsoft Windows [Versión 10.0.19044.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32>sfc /scannow

Iniciando examen en el sistema. Este proceso tardará algún tiempo.

Iniciando la fase de comprobación del examen del sistema.
Se completó la comprobación de 0%.
```

Rootkit Hunter

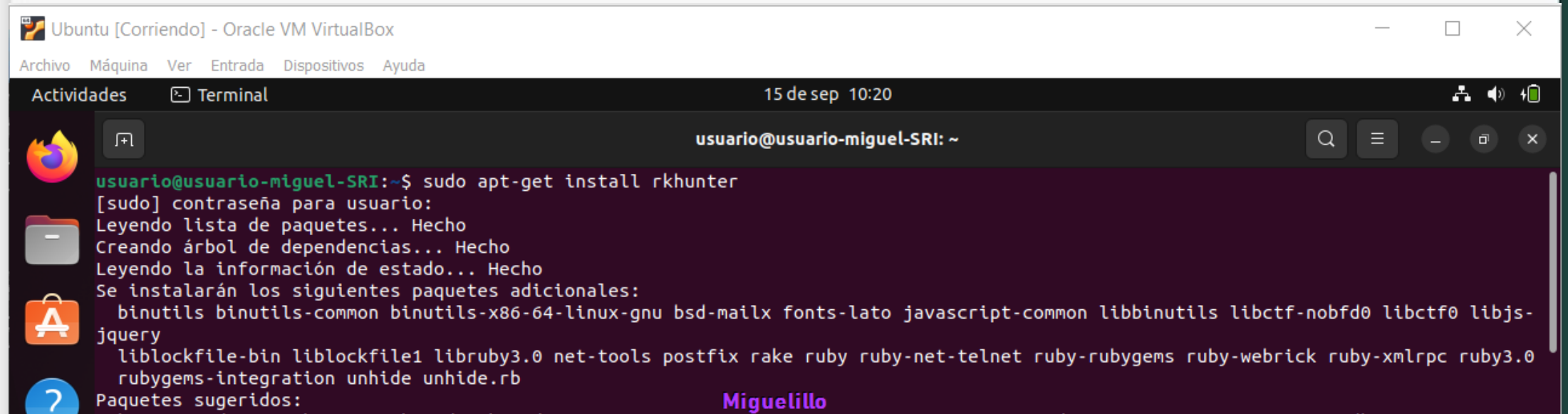


¿Qué es Rootkit Hunter?

Rootkit Hunter, también conocido como rkhunter, es una herramienta de seguridad utilizada en sistemas basados en GNU/Linux. Su función principal es detectar y ayudar a eliminar rootkits, que son programas maliciosos diseñados para ocultar actividades no autorizadas en un sistema.

Rootkit Hunter

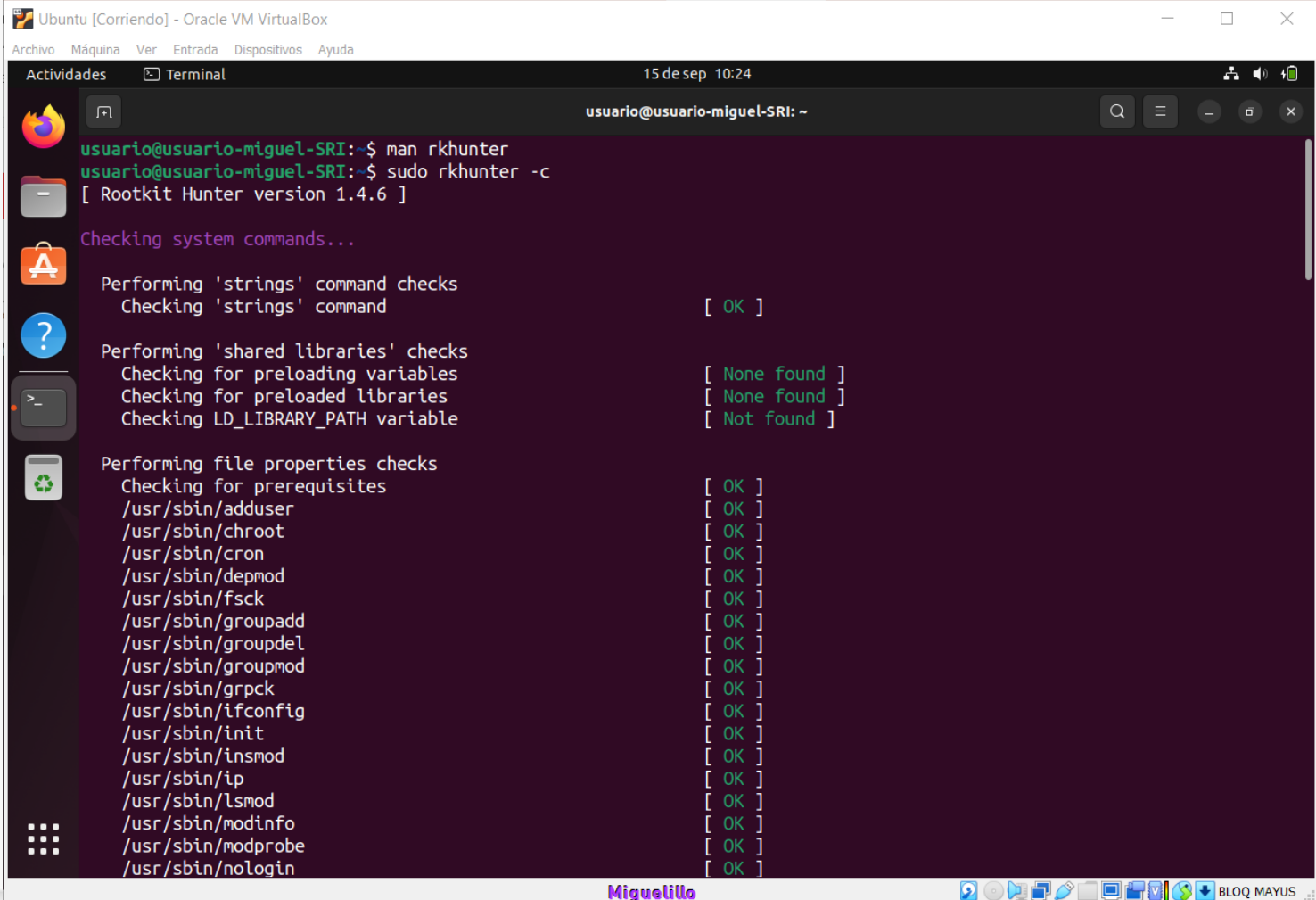
Primero instalaremos Rootkit Hunter



```
Ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
15 de sep 10:20
usuario@usuario-miguel-SRI: ~
usuario@usuario-miguel-SRI:~$ sudo apt-get install rkhunter
[sudo] contraseña para usuario:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
 binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato javascript-common libbinutils libctf-nobfd0 libctf0 libjs-
jquery
 liblockfile-bin liblockfile1 libruby3.0 net-tools postfix rake ruby ruby-net-telnet ruby-rubygems ruby-webrick ruby-xmlrpc ruby3.0
rubygems-integration unhide unhide.rb
Paquetes sugeridos:
```

Rootkit Hunter

Con el comando *sudo rkhunter -c* podremos chequear



```
Ubuntu [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal
15 de sep 10:24
usuario@usuario-miguel-SRI: ~
usuario@usuario-miguel-SRI:~$ man rkhunter
usuario@usuario-miguel-SRI:~$ sudo rkhunter -c
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

Performing 'strings' command checks
Checking 'strings' command                [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables         [ None found ]
Checking for preloaded libraries          [ None found ]
Checking LD_LIBRARY_PATH variable         [ Not found ]

Performing file properties checks
Checking for prerequisites                [ OK ]
/usr/sbin/adduser                        [ OK ]
/usr/sbin/chroot                         [ OK ]
/usr/sbin/cron                          [ OK ]
/usr/sbin/depmod                         [ OK ]
/usr/sbin/fsck                          [ OK ]
/usr/sbin/groupadd                       [ OK ]
/usr/sbin/groupdel                      [ OK ]
/usr/sbin/groupmod                      [ OK ]
/usr/sbin/grpck                         [ OK ]
/usr/sbin/ifconfig                      [ OK ]
/usr/sbin/init                          [ OK ]
/usr/sbin/inssmod                       [ OK ]
/usr/sbin/ip                            [ OK ]
/usr/sbin/lsmmod                        [ OK ]
/usr/sbin/modinfo                       [ OK ]
/usr/sbin/modprobe                      [ OK ]
/usr/sbin/nologin                       [ OK ]
```

Conclusión

SFC es una utilidad que nos ofrece Windows que nos puede ser de gran ayuda ya que ayuda a garantizar que su sistema esté libre de archivos dañados o faltantes, lo que puede mejorar la estabilidad y el rendimiento.

Rootkit Hunter es una herramienta valiosa para detectar y eliminar rootkits que podrían comprometer la seguridad de su sistema.

Ambas herramientas son importantes para mantener su sistema operativo en un estado óptimo y seguro, asegurándose de que esté protegido contra posibles amenazas y problemas de integridad de archivos.