

Actividad | #1 | Configuración de un Servidor

Sistemas Operativos II

Ingeniería en Desarrollo de Software

TUTOR: Marco Alonso Rodríguez Tapia

ALUMNO: Alejandra Ibarra Carmona

FECHA: 26/06/2025

Indicé

Introducción…………………………………3

Descripción…………………………………3

Justificación………………………………..3

Desarrollo………………………………….4

Conclusión………………………………..8

Referencias………………………………8

Introducción

Las amenazas de programas suelen utilizar fallas de unos de los mecanismos de protección de un sistema para atacar programas, por el contrario, las amenazas del sistema y de la red, con esto se implican los abusos de servicios y conexiones además estas amenazas crean una situación en la que se utilizan indebidamente los recursos del sistema. Algunos ejemplos de amenazas de la red y del sistema se tienen que tomar en cuenta que estos ataques de enmascaramiento y reproducción también se lanzan comúnmente a través de redes entre los sistemas, de echo estos ataques son más efectivos y difíciles de contrarrestar cuando se involucran varios sistemas.

* Gusanos: es un proceso que usa el mecanismo de generación para duplicarse, así que un gusano genera copias de sí mismo.
* Escaneo de puertos: Este no es considerado un ataque si no es un medio para que un craker detecte las vulnerabilidades de un sistema, es decir explorando los puertos automatizados que esta involucra.

Descripción

Con frecuencia los errores de desbordamientos de búfer, nos permiten la creación de un Shell de comandos privilegiados en el sistema y a partir de ahí por supuesto, el craker podría instalar caballos de troya o virus troyanos, programados de puerta traseras etc. La denegación de servicios no tiene como objetivo obtener información o robar recursos, si no interrumpir el uso legítimo del sistema o la instalación, la mayoría de estos ataques involucran sistemas que el atacante no a penetrado, lanzar un ataque que impida el uso legítimo suele ser más fácil que irrumpir en una maquina o instalación.

Los ataques de denegación de servicio resultan un abuso de algunas de las funciones fundamentales de TCP, la conexión ahora está completa y el resultado se puede variar en varias sesiones TCP parcialmente iniciadas.

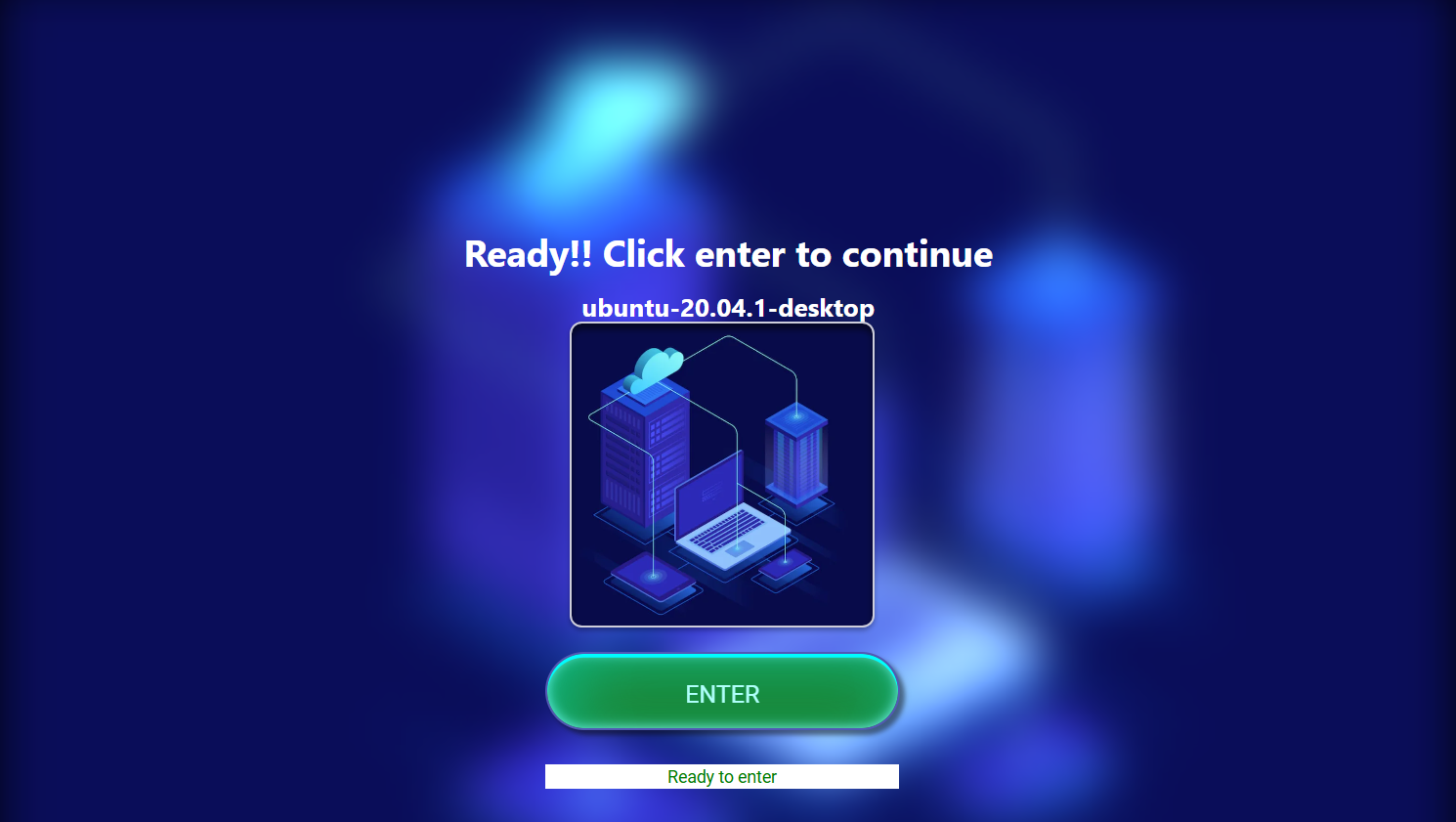
Justificación

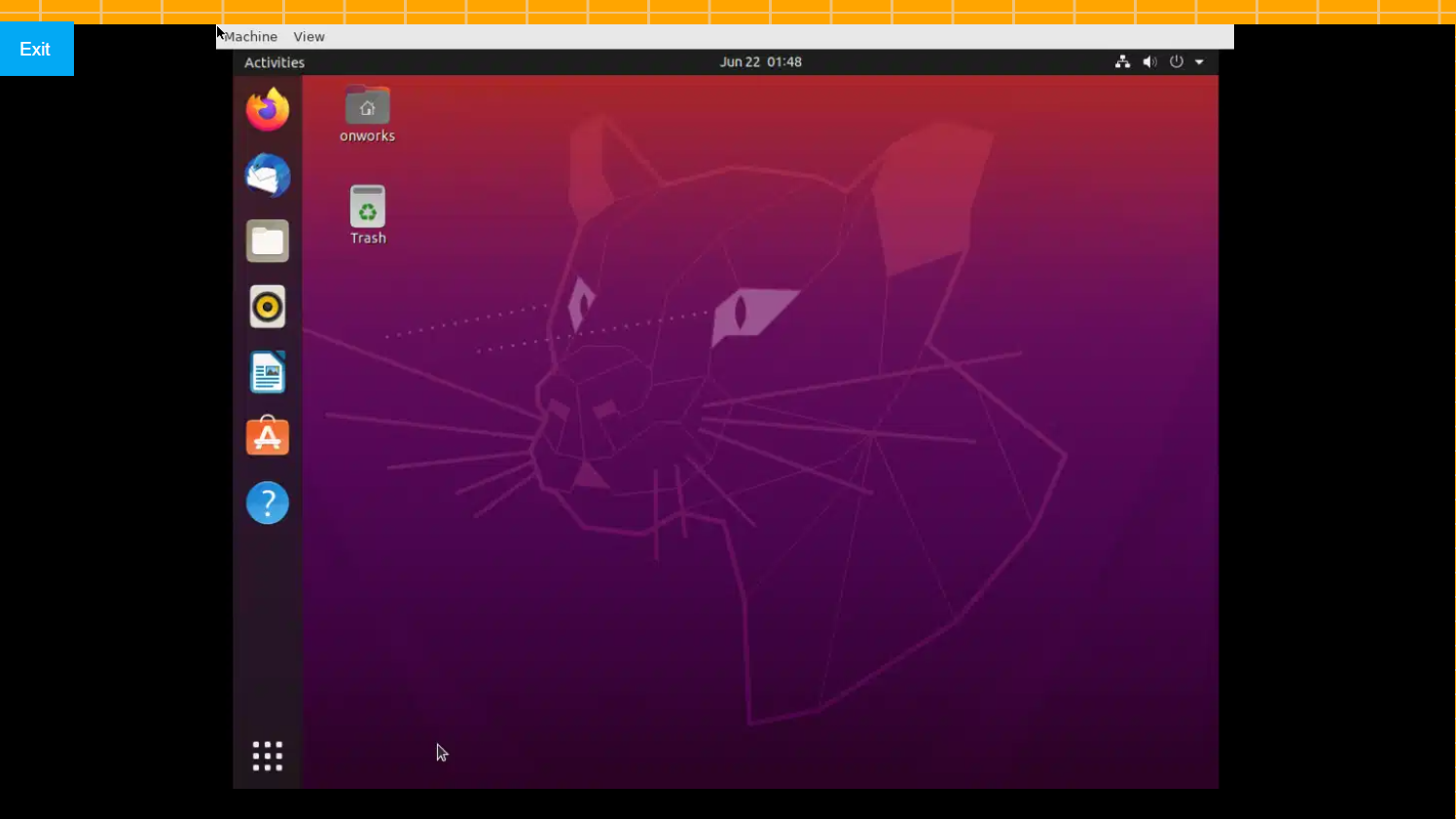
Generalmente es imposible prevenir ataques de denegación de servicio dado que utilizan los mismos mecanismos que el funcionamiento normal, y aun así es mas difícil de prevenir y resolver son los ataques de denegación de servicio distribuido ya que estos se lanzan desde múltiples sitios, estos ataques se han vuelto mas comunes y a veces se asocian con intentos de chantaje y en este sentido es un sitio atacado y los atacantes ofrecen dinero a cambio de detener el ataque.

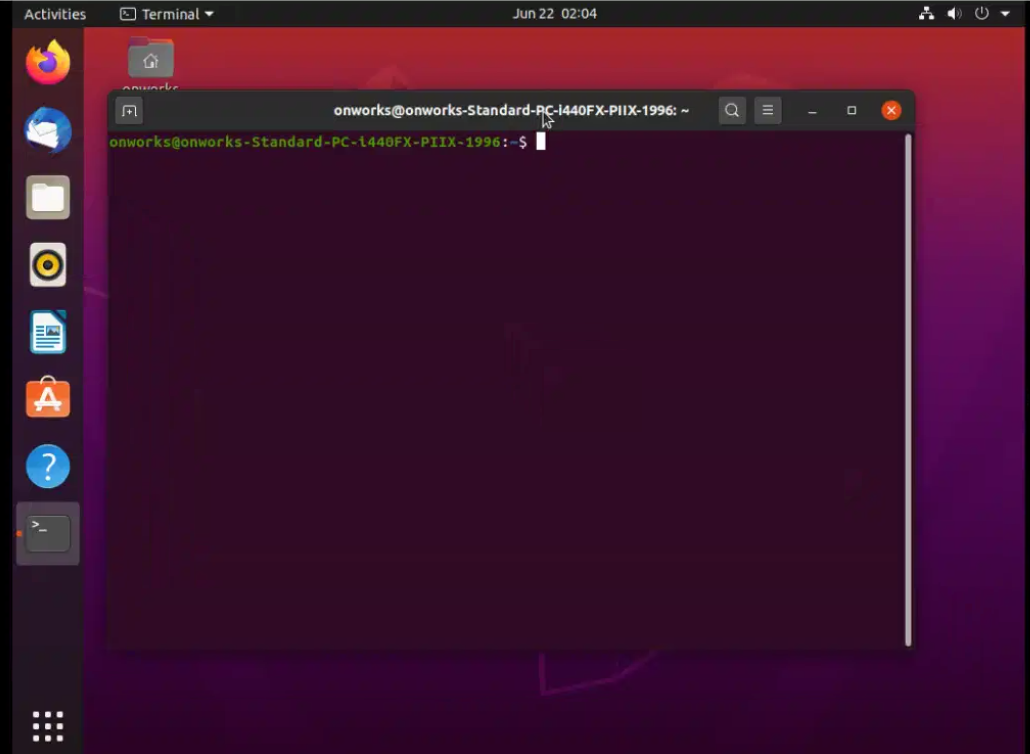
Y para esto también tenemos defensas en realidad se ven algunas formas posibles y veremos que las formas en las que se pueden diseñar e implementar nos ayudan para aumentar la seguridad, su concepto mas importante es la defensa en profundidad y a esto básicamente nos habla de tener varias capas de seguridad para que si se viola una de ellas haya otras que superar.

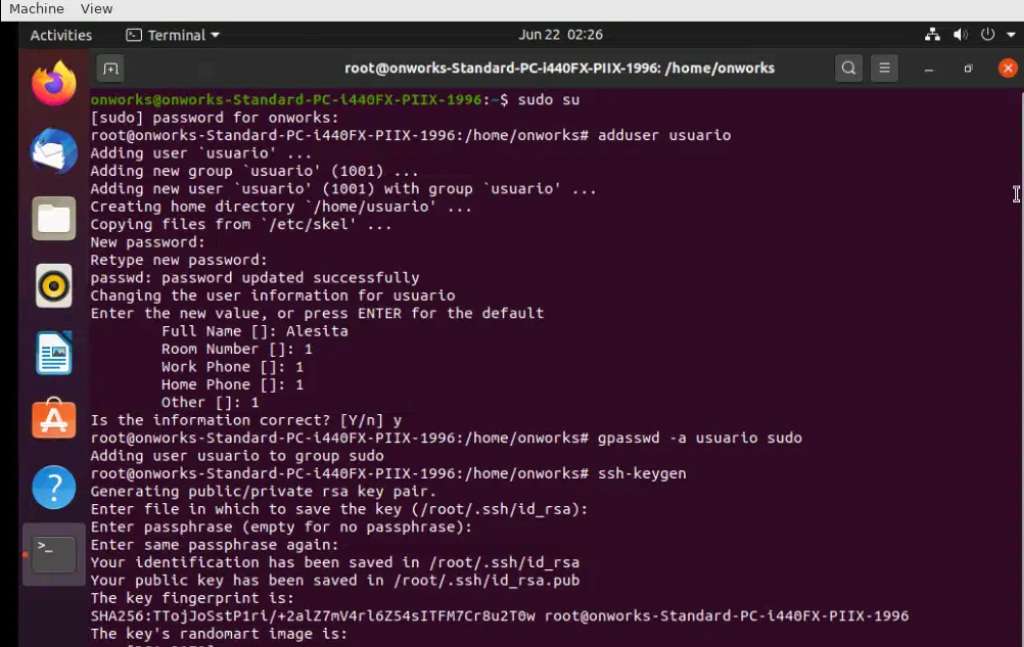
Desarrollo

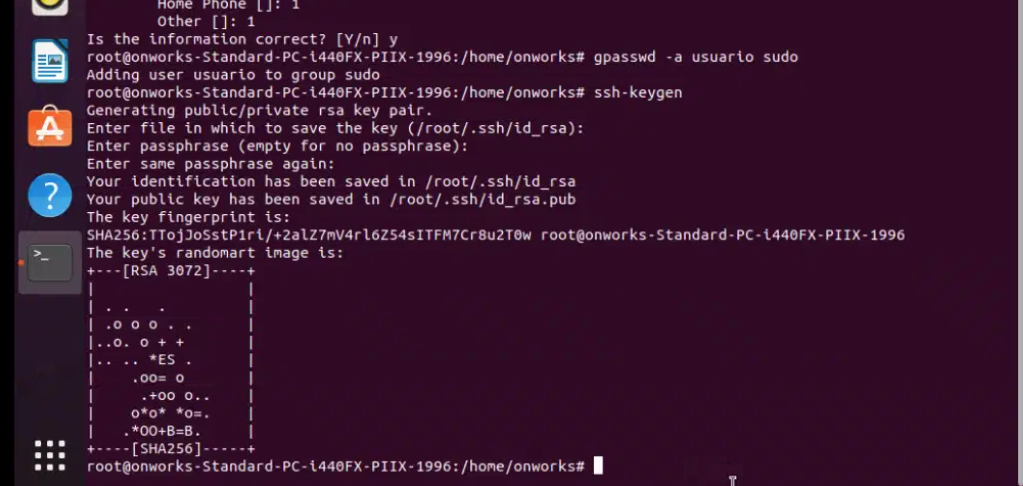


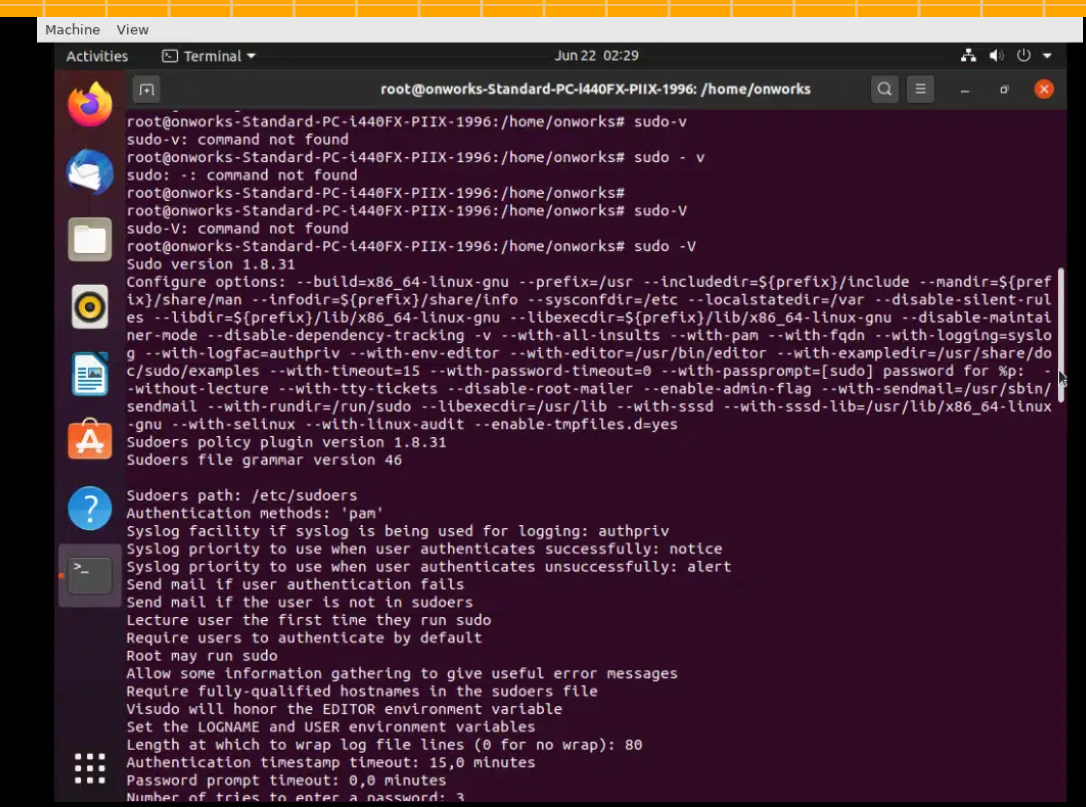


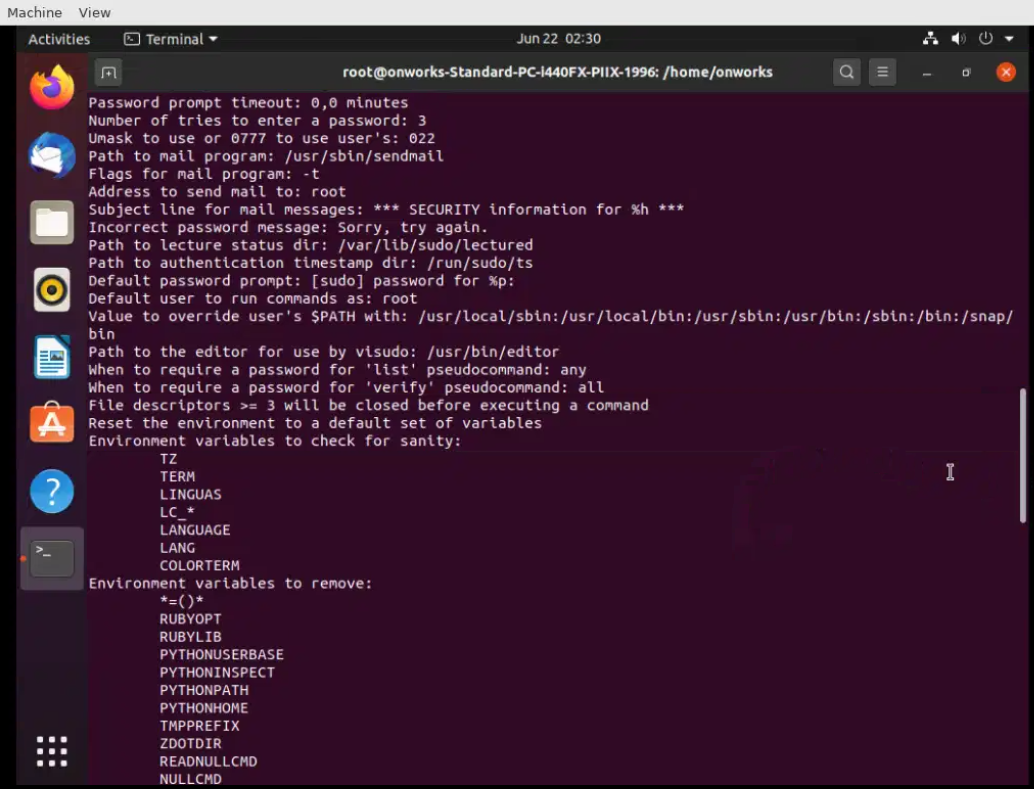


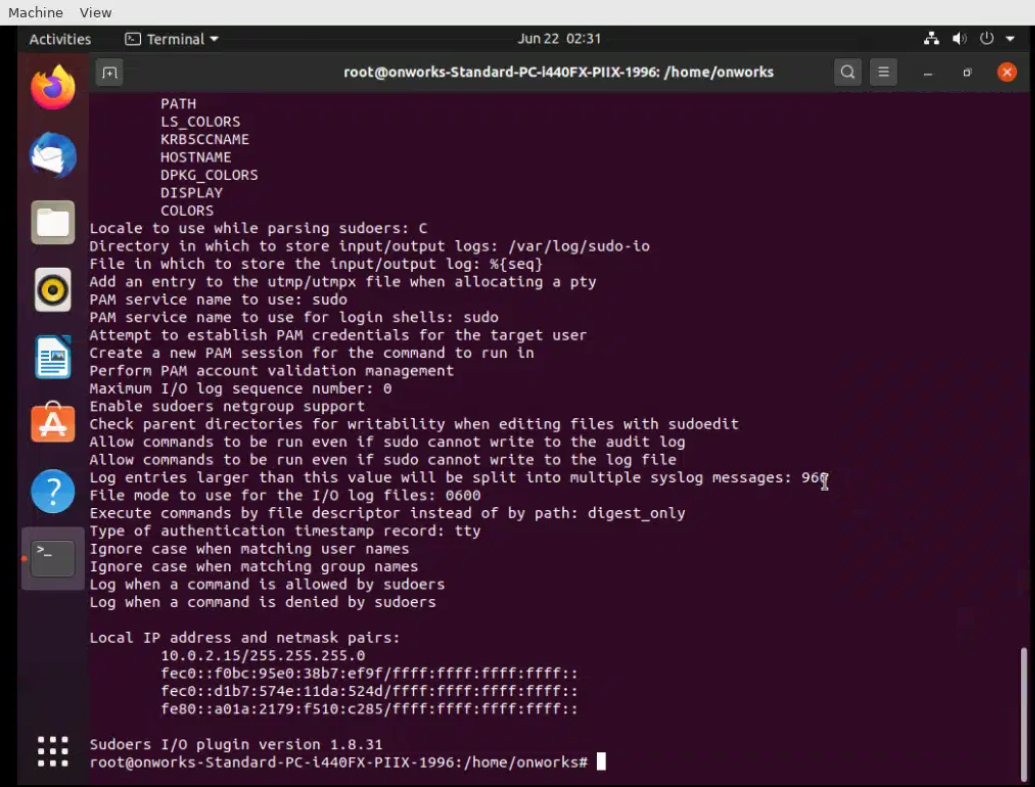












Conclusión

Los antivirus también combaten gusanos y spyware, estos virus intentan esconderse y los usuarios intentan encontrarlos lo que llevan a un juego como el del gato y el ratón, bajo las perspectivas el administrador del sistema es la persona responsable de la seguridad de Linux y de su caja. El cifrado de comunicación de datos para el servidor y todos estos datos son trasmitidos a través de una red abierta a monitoreos, por lo anterior para cifrar los datos que son transmitidos continuamente son viables y es necesario contar con una contraseña. Linux ofrece cada una de las herramientas importantes para que el sistema se conserve actualizado y así poder facilitar las actualizaciones sencillas y variantes por ello cada una de las actualizaciones de seguridad debe revisarse y aplicarse lo antes posible y utilizar un paquete de RMP como yum y/o apt-get para que cada una de las actualizaciones tenga estabilidad.

Referencias