Auditoria de redes.

La ciberseguridad es la práctica de proteger las redes de comunicaciones así como los sistemas informáticos, de ataques e intrusiones no deseadas. Muchas veces los grandes corporativos tienden a contratar personal especializado para localizar vulnerabilidades en sus sistemas y entornos de trabajo de su empresa ya que un riesgo potencial puede causar pérdidas y grandes afectaciones a una compañía.

Las vulnerabilidades van desde las físicas como no contar con los sistemas adecuados de revisión del personal, hasta las digitales, cómo tener algún programa infectado sin que nadie sospeche.

Entendiendo correctamente que una buena cultura de protección puede prevenir catástrofes informáticas, se puede lograr tener un sistema inmune a ataques informáticos, algunas de estas medidas puede ser el uso de contraseñas largas (más de 10 caracteres), actualización del software utilizado a su versión más reciente, monitoreo y audiciones de las redes para búsqueda y detección de actividad sospechosa.

Una auditoría hace referencia a una reunión documentada donde se busca analizar en profundidad los sistemas para evaluar su nivel de seguridad y protección ante amenazas. Dentro de ellas pueden usarse diferentes medios para encontrar vulnerabilidades, por lo que regularmente se suelen dividir en dos equipos, el equipo rojo quienes simulan ataques a los sistemas de una compañía y el equipo azul quienes intentan bloquear estos ataques y recuperarse de las fallas provocadas.

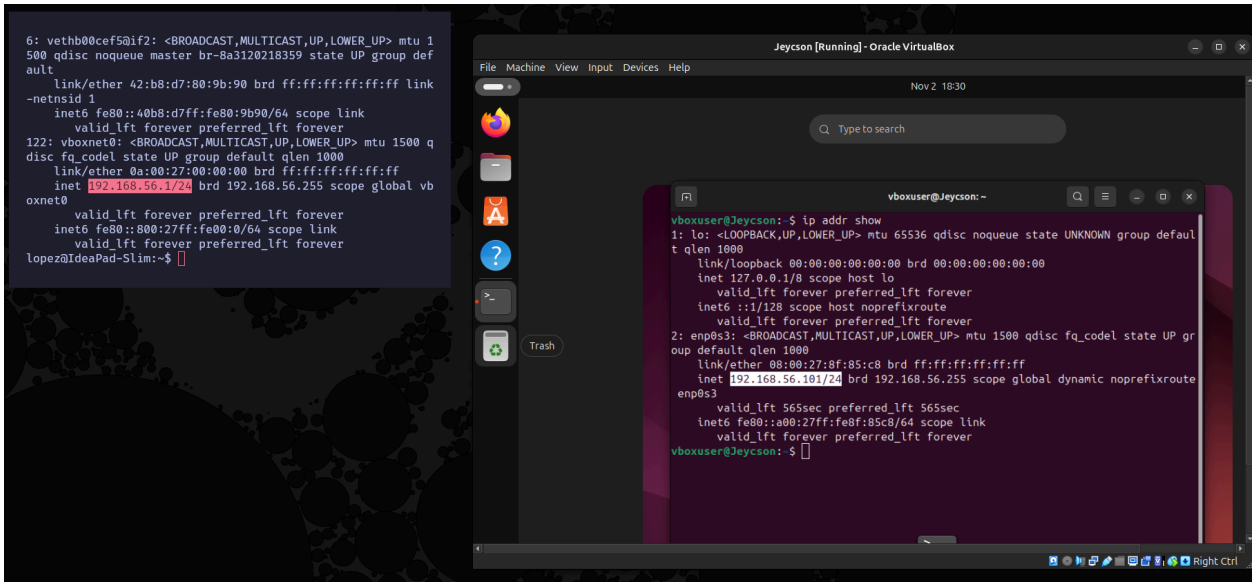
Práctica de análisis de redes.

El objetivo de esta práctica es aprender y comprender como usar NMAP y WireShark para hacer auditoria en redes, en este caso llevándolo a un entorno seguro y limitado entre una máquina virtual y una máquina anfitriona.

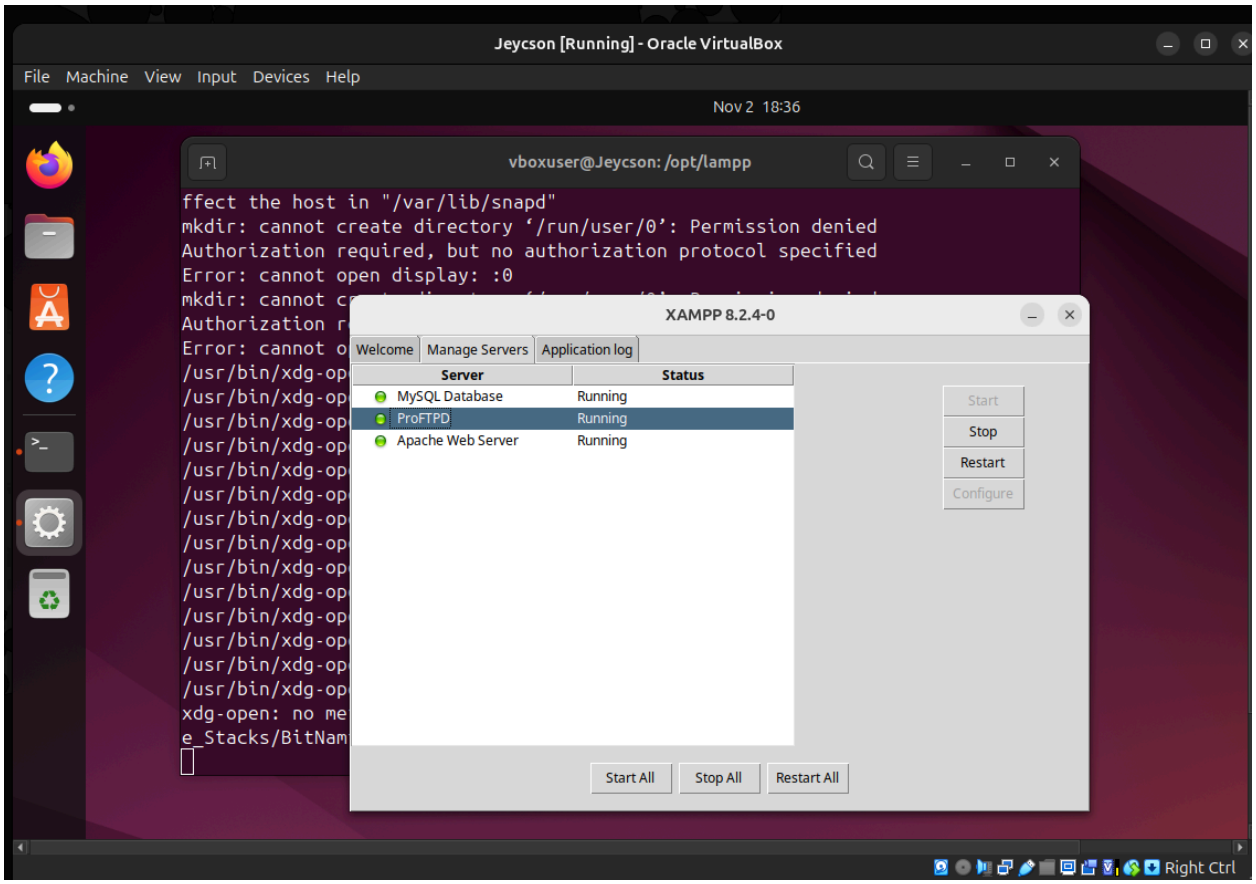
En el caso de la práctica realizada, ambas máquinas sirven el sistema operativo Ubuntu, aunque en WireShark y el NMAP están instalados en la máquina anfitriona, mientras que en la máquina virtual tenemos instalada la aplicación de XAMPP, para servir diferentes aplicaciones.

Como primer paso después de instalar las herramientas necesarias, es configurar nuestra máquina virtual para crear una red privada entre las dos máquinas simulando un entorno real donde la empresa tiene una red para cierto departamento.

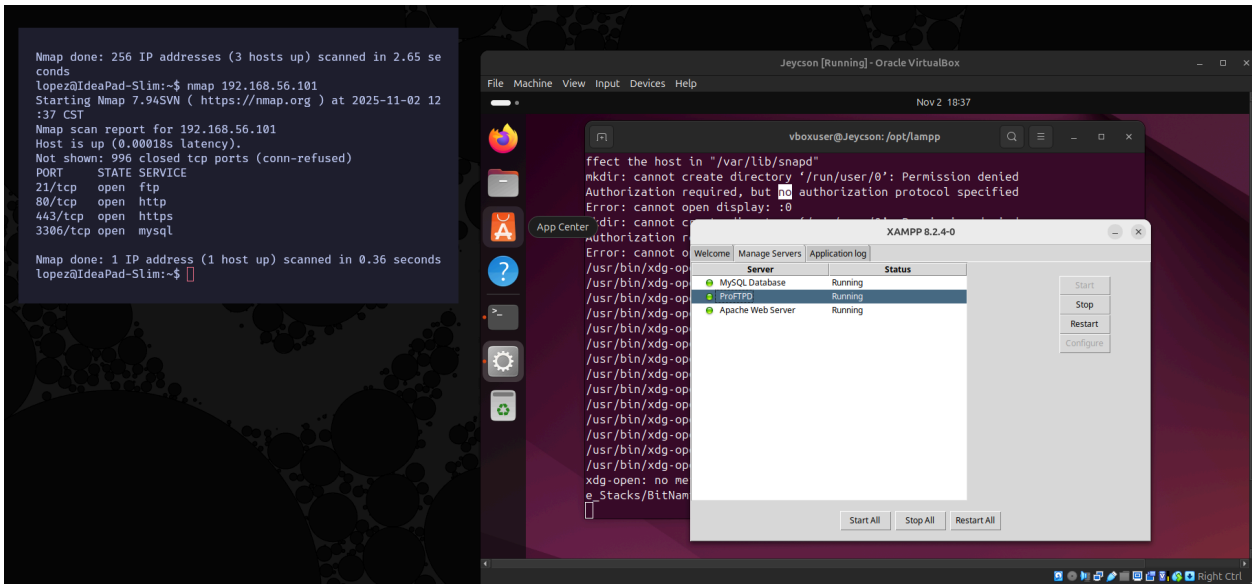
La siguiente imagen muestra las dos IP´s de nuestras máquinas, a la izquierda la IP de la máquina anfitriona y a la derecha la IP de la máquina virtual.



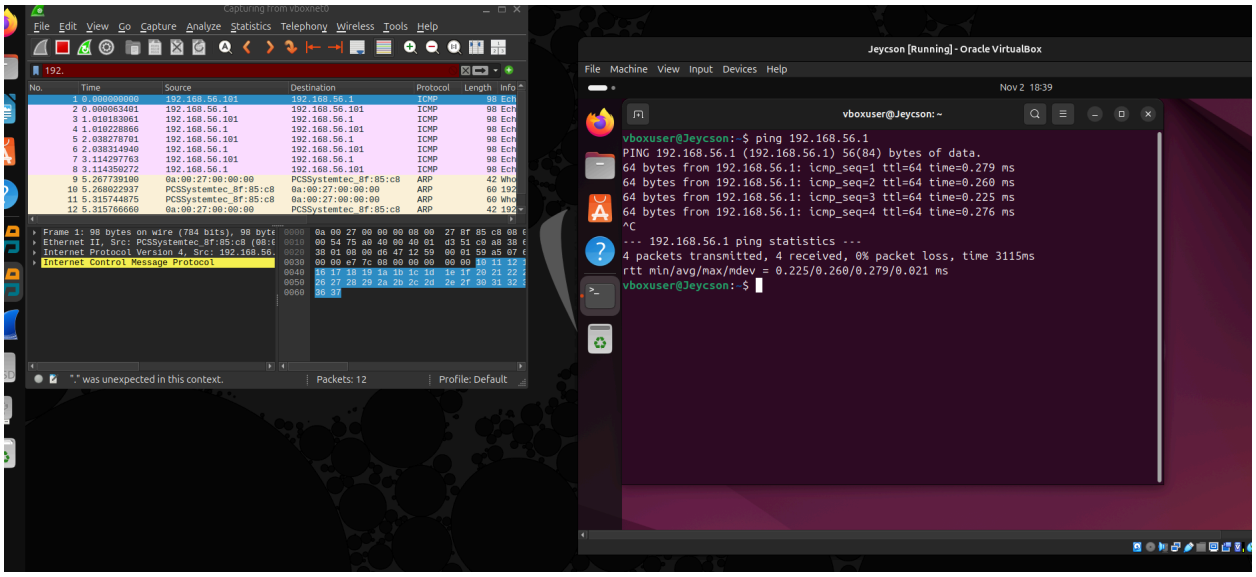
El siguiente paso es encender en nuestra máquina virtual los servicios de apache como son MySQL, ProFTPD y Apache Web Server.



Con ayuda de NMAP vamos a analizar que puertos estan abiertos en la maquina victima en este caso, nos muestra los servicios que nosotros hemos activado con XAMPP.



WireShark es una herramienta más completa que captura y analiza el tráfico de red, para esta práctica, la máquina virtual lanza un ping a la máquina anfitriona enviando 4 paquetes, y en nuestra máquina anfitriona vemos reflejado precisamente ese flujo de datos en la aplicación del WireShark. Dentro de cada solicitud podemos ver el contenido de los paquetes y cómo están organizados.



Finalmente se adjunta la evidencia de la conectividad entre ambas máquinas enviando un mensaje a través de nuestra red privada.