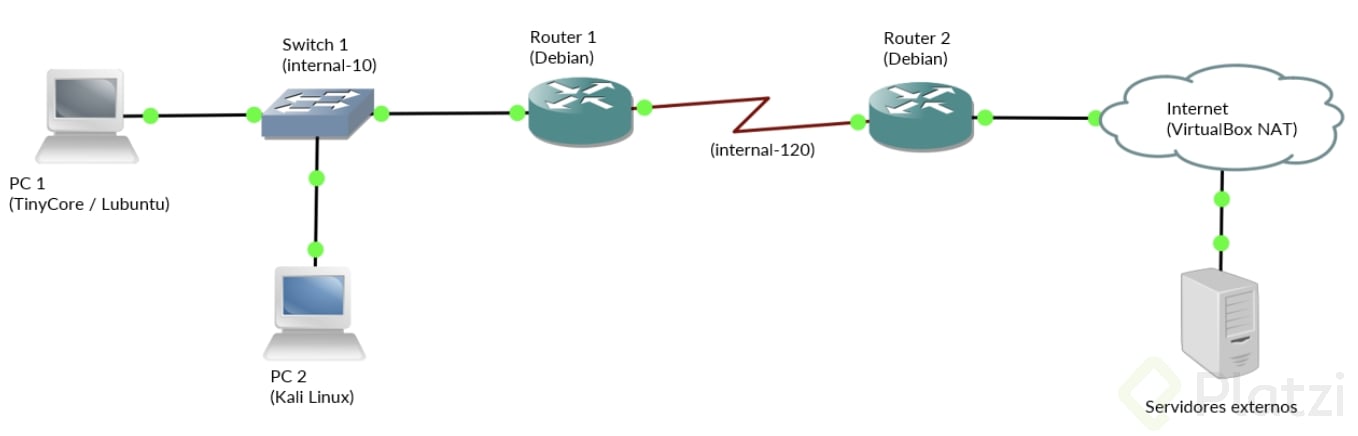
A lo largo de este curso vamos a estar usando una estructura de red definida para muchos de los ejemplos y ataques que vamos a realizar, de manera que es bueno que te vayas familiarizando con el entorno de red que estaremos configurando.

En general, este es el diagrama de red que vamos a usar a lo largo del curso:



Este diagrama tal vez cambie un par de veces en algunas clases, para algún requerimiento específico, pero en la mayoría de casos lo vamos a usar tal cual está en la imagen. Vamos a analizar un poco los elementos que tiene y las configuraciones que vamos a necesitar para cada uno de ellos:

**PC 1**  
Esta es la máquina virtual de nuestra “víctima”. Vamos a estar usando una distribución de Linux ligera (TinyCore o Lubuntu funcionan bastante bien para esto), y la idea es simular a un usuario normal con navegación y demás, por lo que no necesitamos algo demasiado complicado. Lo importante es que sea ligera para no ocupar demasiada memoria.

**PC 2**  
Nuestra máquina virtual de Kali Linux. Si tomaste el curso de Fundamentos de Pentesting, ya la tienes configurada y lista para ser usada.

**Switch 1**  
Este switch está representado por una de las redes internas de VirtualBox. Para los ejemplos que haremos durante el curso, vamos a usar la red internal-10. Es posible que en algunos ejemplos necesitemos conectar más equipos que PC1 y PC2.

**Router 1**  
Este es un enrutador que simularemos usando una distribución de Linux sin interfaz gráfica (En los ejemplos del curso usamos Debian). Para este curso, configuraremos rutas usando protocolos dinámicos en lugar de usar rutas estáticas, y en este enrutador también configuraremos un servidor DHCP para asignar direcciones a los dispositivos que se conecten al Switch 1.

**Router 2**  
Este es un segundo router en Linux que usaremos para salir a Internet. Una de sus interfaces está conectada a una red interna (internal-120 en el caso de los ejemplos del curso), y la otra estará conectada a la red NAT de VirtualBox. Lo que buscamos es configurar los protocolos de enrutamiento y traducción de direcciones de tal manera que todos los dispositivos de internal-10 tengan salida a Internet, de la misma forma en que lo harían en una red local normal, como la de una empresa o la red inalámbrica de un café.

**Internet**  
La salida a Internet será a través de una interfaz NAT de VirtualBox. En nuestra configuración de enrutamiento tendremos esta salida como una ruta por defecto, que es un concepto que veremos al momento de hacer análisis de las tablas de enrutamiento.

**Servidores externos**  
Estos son los servidores en Internet que usaremos para probar que estemos capturando el tráfico de nuestra víctima, o que hayamos hecho efectivamente ataques Main-In-The-Middle. Pueden ser servidores comunes como Facebook, Twitter, Google, y en algunos casos vamos a configurar servidores web propios en otros puntos de la red.

A partir de la próxima clase, y por lo que queda de este módulo, estaremos configurando cada uno de los protocolos que necesitamos para que este entorno de red funcione. Durante el resto del curso, atacaremos y aprovecharemos vulnerabilidades precisamente de los protocolos que hayamos configurado en este entorno de red.

¡Continúa con el curso!, en próximas clases comenzaremos configurando el servidor DHCP que asigna direcciones a las máquinas locales.