**Herramientas utilizadas**

**Maquina virtual:**

Una maquina virtual es un entorno que funciona como un sistema informatico virtual con su propia CPU, Memoria, interfaces de red y almacenamiento, pero se crean en el sistema de hardware físico, ya sea localmente o no. El sistema de software se denomina hipervisor, que se encarga de separar los recursos de la máquina del sistema de hardware e implementarlos correctamente para que la VM pueda utilizarlos. Estos se denominan hosts, computadoras host, sistemas operativos host o simplemente hosts. Las diversas máquinas virtuales que utilizan sus recursos son equipos invitados, equipos invitados, sistemas operativos invitados o simplemente invitados. La máquina virtual está aislada del resto del sistema, pero puede haber varias máquinas virtuales en una sola pieza de hardware (como un servidor). Además, se pueden mover entre servidores host según sea necesario o utilizar los recursos de manera más eficiente. La VM permite que varios sistemas operativos diferentes se ejecuten simultáneamente en la misma computadora, como la distribución de Linux en una computadora portátil MacOS.

El software en especifico es Oracle VM VirtualBox es el software de virtualización multiplataforma de código abierto más popular del mundo, que permite a los desarrolladores entregar código antes mediante la ejecución de múltiples sistemas operativos en un solo dispositivo. Los equipos de TI y los proveedores de soluciones usan VirtualBox para reducir los costos operativos y reducir el tiempo requerido para implementar aplicaciones de manera segura localmente y en la nube. El software de virtualización de escritorio multiplataforma, de código abierto y de bajo costo reduce los costos operativos del equipo al reducir la cantidad de configuraciones de escritorio y servidor requeridas. Con una interfaz gráfica de usuario (GUI) fácil de usar y una potente interfaz de línea de comandos, los desarrolladores pueden utilizar varios sistemas operativos en el mismo sistema



**Cliente SSH:**

OSSH, o Secure Shell, es un protocolo de administración remota que permite a los usuarios controlar y modificar su servidor remoto a través de Internet a través de un mecanismo de autenticación. Proporciona un mecanismo para autenticar a los usuarios remotos, transferir la entrada del cliente al host y retransmitir la salida al cliente. El servicio se creó como una alternativa segura a Telnet sin cifrar y utiliza tecnología de cifrado para garantizar que todas las comunicaciones hacia y desde servidores remotos estén cifradas. La ventaja significativa que proporciona el protocolo SSH sobre su predecesor es el uso de cifrado para garantizar la transmisión segura de información entre el host y el cliente. El host se refiere al servidor remoto al que está intentando acceder y el cliente es la computadora que utiliza para acceder al host. SSH utiliza tres tecnologías de cifrado diferentes:

1.Cifrado simétrico:

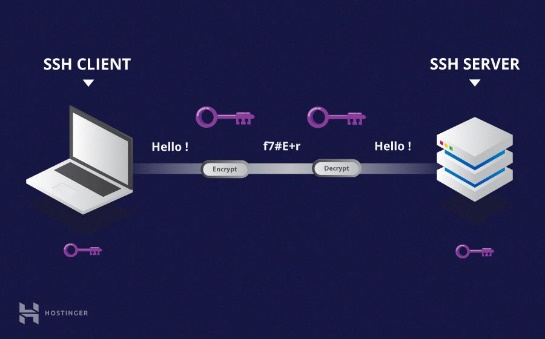
El cifrado simétrico es una forma de cifrado en la que tanto el cliente como el host utilizan una clave para cifrar y descifrar mensajes. De hecho, cualquiera que tenga la clave puede descifrar el mensaje que se transmite. El cifrado simétrico suele denominarse cifrado de clave compartida o cifrado secreto compartido. Por lo general, solo se usa una clave o, a veces, se usa un par de claves donde una clave se puede calcular fácilmente con otra clave. La clave simétrica se utiliza para cifrar todas las comunicaciones durante la sesión SSH. Tanto el cliente como el servidor utilizan el método acordado para derivar la clave, y la clave generada nunca será revelada a un tercero. El proceso de creación de una clave simétrica se realiza mediante un algoritmo de intercambio de claves.

2.Cifrado asimétrico:

El cifrado asimétrico utiliza dos claves independientes para el cifrado y el descifrado. Estas dos claves se denominan clave pública y clave privada. Juntas, estas claves forman un par de claves pública-privada. La clave pública, como su nombre indica, se distribuye públicamente y se comparte con todas las partes. Aunque está estrechamente relacionada con la clave privada en términos de función, la clave privada no se puede calcular matemáticamente a partir de la clave pública. La relación entre estas dos claves es muy complicada: los mensajes cifrados con la clave pública de la máquina solo se pueden descifrar con la misma clave privada de la máquina. Esta relación unidireccional significa que la clave pública no puede descifrar sus propios mensajes ni descifrar ningún contenido cifrado por la clave privada.

3.Hashing:

es otra forma de criptografía utilizada en Secure Shell Connections. Las funciones de hash unidireccionales difieren de las dos formas anteriores de encriptación en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir. Para generar un hash criptográfico de una entrada dada, pero imposible de generar la entrada del hash. Esto significa que si un cliente tiene la entrada correcta, pueden generar el hash criptográfico y comparar su valor para verificar si poseen la entrada correcta.



**Apache:**

El servidor HTTP Apache es un servidor web HTTP de código abierto, adecuado para Linux, Microsoft u otras plataformas, e implementa el protocolo HTTP / 1.1. Su nombre se debe a que algunas personas esperan que tenga una connotación firme y enérgica pero no agresiva. La tribu Apache Es el último que se rindió al hombre que estaba a punto de convertirse en el gobierno de Estados Unidos, cuando su equipo temía que la empresa llegara y "civilizara" el panorama creado por el primer grupo de ingenieros de Internet. Además, Apache solo incluye un conjunto de parches para el servidor NCSA. El servidor Apache es desarrollado y mantenido por la comunidad de usuarios bajo la supervisión de Apache Software Fundación dentro del proyecto HTTP Server (httpd). Otras características altamente configurables, bases de datos de autenticación y negociación de contenido han sido criticadas por la falta de una interfaz gráfica para ayudar con su configuración.

Apache se utiliza principalmente para enviar páginas web estáticas y dinámicas en la World Wide Web. Muchas aplicaciones web están diseñadas para asumir Apache como el entorno de implementación, o utilizarán las funciones del servidor web. Apache es el componente de servidor web de la popular plataforma de aplicaciones LAMP, que sigue el ritmo de los lenguajes de programación MySQL y PHP / Perl / Python (y ahora Ruby). El servidor web se redistribuyó como parte de varios paquetes de software patentados, incluidos Oracle Database e IBM WebSphere Application Server. MacOS integra apache como parte de su propio servidor web y como soporte para su servidor de aplicaciones WebObjects. Borland de alguna manera lo admite en las herramientas de desarrollo de Kylix y Delphi. Apache se incluye en Novell NetWare 6.5, es el servidor web predeterminado y se incluye en muchas distribuciones de Linux.

Apache se utiliza para muchas otras tareas que requieren que el contenido se proporcione de manera segura y confiable. Por ejemplo, al compartir archivos desde una computadora personal a Internet. Los usuarios que han instalado Apache en su escritorio pueden colocar archivos arbitrariamente en el directorio raíz de documentos de Apache y compartirlos desde allí. Los desarrolladores de aplicaciones web a veces usan la versión local de Apache para obtener una vista previa y probar el código desarrollado.

