2ª Sesión práctica ASRC - 2017/18. Guión de trabajo:

PRIMERA PARTE: ADMINISTRACIÓN DEL SERVIDOR A TRAVÉS DE LA RED.

* WinScp:

Herramienta de software libre, para plataformas windows, utilizada en conexiones a equipos remotos con el servicio SSH, mediante protocolo SFTP, permitiendo, tanto la administración mediante **ssh** como la subida de ficheros desde un equipo cliente hacia el servidor.

Si no estuviera habilitado el servicio ssh, lo instalamos, en caso necesario:

sudo apt-get install openssh-server

Configuración:

sudo gedit /etc/ssh/sshd_config

Alternativas de este cliente para Linux:
Filezilla
Nautilus
Plugin Mozilla Firefox: FireFTP

Ejercicio 1: Las conexiones son creadas, por defecto, por el puerto 22 (SSH, Sftp, scp). En algunas ocasiones, por motivos de seguridad, se recomienda crear estas conexiones por otro puerto diferente al predeterminado. Realizar una conexión mediante Winscp, por SSH, a través de un puerto diferente. Indica lo que has tenido que modificar en el servidor y la configuración en el cliente (puedes adjuntar captura de pantalla) para efectuar la conexión.

A continuación abre una consola (Putty) para lanzar algún comando en el servidor remoto. Prueba, también, a subir algún fichero al servidor.

Para ahondar un poco más en el uso de SSH, investiga cómo podría "enjaular" a un usuario concreto del sistema, para que, cuando se conecte al servidor, no salga de un directorio concreto (el suyo de casa, por ej.). Indica los pasos necesarios y razona qué utilidad puede tener el hacer esto.

* Webmin:

Herramienta web que permite administrar de forma completa toda funcionalidad de un servidor con un sistema Unix/Linux.

Algunos aspectos que se pueden administrar desde esta aplicación, son aquellos relacionados con la configuración de red, seguridad (firewall, proxy ...), actualizaciones, usuarios, etc.

Tiene especial utilidad sobre servidores que no está dotados de capacidades gráficas ya que agrupa de forma visual, toda posibilidad de configuración que posea.

En caso de no tenerla instalada en la máquina virtual que use, puede instalarla, en distribuciones debian, mediante apt-get install webmin.

Una vez instalado, accedemos mediante navegador, desde cualquier máquina de la misma red, a la url: https://ip_servidor:10000

El acceso se puede hacer con el usuario del S.O, habitualmente *root*.

Una vez accedido, analice los datos de la página inicial que aparece.

Vamos descubriendo algunas funcionalidades de la herramienta, mediante sus principales apartados:

PÁGINA PRINCIPAL:

1. Compruebe los paquetes disponibles y pruebe a instalar alguno, si le es posible.
2. Observe qué procesos se encuentran corriendo

CONFIGURACIÓN WEBMIN:

3. Denegar el acceso desde la ip de un compañero y probar a conectar al webmin desde aquél que hayas denegado.
4. Averigue si es posible cambiar el puerto de escucha por el cual conectar con Webmin.
5. Incluya los "logins" y "logouts" en el log de acciones. A continuación, salga y acceda nuevamente a Webmin para comprobar que se graban dichos eventos en el log. Luego, observe los distintos formatos de dichos logs tanto desde el mismo webmin (opción del panel izquierdo, en la zona inferior, 'View logs modules') como desde los 2 ficheros de logs del sistema (los indicados en la pantalla de configuración de los logs). Posiblemente, deba ejecutar antes 'sudo su' o 'sudo' para poder visualizar los ficheros.
6. ¿Cómo posibilitaría que el servidor pueda descargar paquetes desde internet si la salida se hace mediante un proxy?

SISTEMA

7. Configure la copia de seguridad de archivos para que se respalde el contenido de /home/adminuser en /var/backups/copia.tar, comprimido con gzip, de forma planificada a las 4 de la mañana cada viernes. Establezca un email donde enviar la salida programada cuyo asunto sea "Salida de backup". Ejecute el comando y compruebe el resultado.
8. Observe dónde se encuentran los archivos de logs e indique cuáles están activos y cuáles no.
9. Establezca la rotación de los log's de Apache para que sea de forma diaria.
10. Entre en la administración de usuarios, y busque la línea (con todos sus campos) que corresponde al usuario con el que estamos trabajando. ¿A qué grupos pertenece dicho usuario? Indique también cuál es el directorio de casa del usuario de Apache.

SERVIDORES

11. Obtenga el puerto de escucha de alguno de los servidores levantados (MySQL, ssh, Apache, ...)
12. Haz una prueba de restricción de control de acceso por SSH, para que sólo puede hacerlo a través de un usuario concreto del sistema. Prueba, luego, a conectarte mediante ese usuario y

mediante otro nuevo que cree previamente.) al servidor de la máquina virtual usando el usuario creado. Compruebe qué sucede. Pruebe también con el usuario administrador (adminuser en caso de alguna máquina virtual)

RED

13. Observe las diferencias entre las interfaces activadas ahora y las activadas durante el arranque. Compruebe cómo se podría modificar la ip de cualquiera de ellas.
14. Indique cuál es el orden de búsqueda al realizar una resolución de nombres.
15. ¿Cuál es el cortafuegos que hay instalado?

Ejercicio 2: Entrega un punto por cada apartado que has ido probando.

SEGUNDA PARTE: INDAGANDO EN NUESTRA RED.

*** Nmap**: herramienta de código abierto usada con fines de sondeo y exploración de redes, así como para auditorías de seguridad. Empleada tanto para analizar grandes redes como puestos individuales. Obtiene información sobre los equipos que están operativos y servicios que están ejecutando, así como el sistema operativo que tienen.

Es de gran aceptación y uso tanto para administradores de redes y sistemas, como para auditores de seguridad.

Obtenga más información en la web oficial: https://nmap.org/
Guía de referencia: https://nmap.org/man/es/

Instalación desde distribuciones debian:
Apt-get install nmap

O bien descarga del paquete desde la web y posterior instalación.

Ejemplo de ejecución desde la línea de comandos:

```
nmap -sP 192.168.1.0/24
```

Ejercicio 3: indica, al menos, 3 ejemplos que contemple la ejecución de esta herramienta sobre un equipo,varios y la red entera del aula. Especifica las opciones usadas que consideres de interés.

Opcional: Prueba a instalar el front-end llamado Zenmap, y haz las mismas pruebas del ejercicio pero a través de esta interfaz