Hito 2
ASORC

Andrés Carpena Latour
acl73@alu.ua.es

Índice

CentOS

Licencia

La mayoría de los programas en el sistema están bajo la Licencia Pública General de GNU, más comúnmente conocida como la "GPL". La licencia GPL requiere que el código fuente de los programas esté disponible siempre que se distribuya alguna copia de los binarios del programa; esta condición de la licencia, asegura que cualquier usuario pueda modificar el programa. Por esta misma razón, el código fuente de todos los programas está disponible en el sistema CentOS. Además, el sistema operativo tiene un soporte directo desde RedHat.

1. Exigencia de publicación del código fuente.
2. La redistribución libre.
3. El código fuente debe ser incluido y debe poder ser redistribuido.
4. Todo trabajo derivado debe poder ser redistribuido bajo la misma licencia del original.
5. Puede haber restricciones en cuanto a la redistribución del código fuente, si el original fue modificado.
6. La licencia no puede discriminar a ninguna persona o grupo de personas, así como tampoco ninguna forma de utilización del software.
7. Los derechos otorgados no dependen del sitio en el que el software se encuentra.
8. La licencia no puede 'contaminar' a otro software.

SSH con firma digital

Para utilizar la firma digital al conectarnos a un ssh, utilizamos primero los siguientes comandos de configuracion:
setsebool -P allow_ssh_keysign 1

Creamos directorio de claves
mkdir -m 0700 ~/.ssh/
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorithed_keys
chcon -R -t ssh_home_t ~/.ssh/

(En el cliente)
Generamos clave:
ssh-keygen -t dsa
Cambiamos permisos
chmod -R go-rwX ~/.ssh
Copiamos el contenido de la firma digital publica en el servidor remoto
cat ~/.ssh/id_sha.pub | ssh shirkam@192.168.56.102 "cat >> /home /shirkam/.ssh/authorized_keys"

Enjaulado de usuarios sftp

Editamos el archivo */etc/ssh/sshd_config* y cambiamos la linea *Subsystem sftp /usr/libexec/openssh/sftp-server* por:
Subsystem sftp internal-sftp
Match Group sftpusers
ChrootDirectory %h
ForceCommand internal-sftp

AllowTcpForwarding no

Después reiniciamos el servicio de ssh y añadimos el grupo sftpusers. Hecho esto, creamos el usuario sftpuser1 con contraseña "12345", la misma que los usuarios usados de ejemplo en el resto de los servicios, y le ponemos como grupo sftpusers. Ahora, tenemos que cambiar los permisos de la carpeta del usuario a 755y que pertenezca al grupo y usuario root. Para ello ejecutamos "*chown root:root /home/sftpuser1"* y *"chmod 755 /home/sftpuser1".* Generamos una carpeta donde el usuario y su grupo predeterminado tengan permisos de escritura con *"mkdir -m 0755 /home/sftpuser1/public_html"* y *"chown sftpuser1:users /home/sftpuser1/public_html".* Hecho esto, decimos que el usuario no puede iniciar sesión en el sistema con "*usermod -s /sbin/nologin sftpuser1*". Por ultimo, hay que añadir el usuario a la lista de usuarios permitidos en sshd_config, para luego reiniciar el servicio.

VSFTP

Primero añadimos un nuevo disco desde virtualbox llamado CenOS_FTP_disk. Una vez añadido, hemos de iniciar CentOS y crear una particion en el disco. Para ello, primero nos aseguramos que el disco ha sido reconocido por el sistema con *"ls /dev/sd*"* . Una vez encontrado el disco que acabamos de añadir, que si lo hemos añadido en ultimo lugar debería tener la ultima letra, procedemos a crear su particion. Nos elevamos a root y ejecutamos "*fdisk [nombre del disco]*". En nuestro caso, tenemos el disco "/dev/sdb", por lo que debemos ejecutar "*fdisk /dev/sdb*". Una vez abierto el programa, lo primero que hacemos el consultar las particiones existentes en nuestro disco, con la orden *p*. Visto que no existe ninguna, ya que el disco es nuevo, creamos una nueva partición con el comando *n*. Dentro del comando *n* se nos pide que digamos primero si la partición será primaria o extendida, a lo que nosotros decimos que primaria. Después se nos pide el numero de la particion, de 1a 1 a la 4, y dónde empezará y terminará. Ya que va a ocupar todo el disco, le dejamos los valores por defecto. Una vez especificado todo esto, ejecutamos el comando *w* , que escribe el disco, y cierra el programa.

Ahora que tenemos una partición en el disco, es necesario crear un sistema de archivos dentro de la misma. Para ello utilizaremos el programa "*/sbin/mkfs.ext4 -L [nombre de la carpeta] [nombre de la particion]*". En nuestro caso, ya que queremos montar un servidor ftp, crearemos la carpeta */data/ftp* así "*/sbin/mkfs.ext4 -L /data/ftp /dev/sdb1*". La crea automaticamente, por lo que no tenemos que realizar más cambios. Una vez hecho esto, vamos a crear un punto de montaje de la partición, así que no dirigimos al directorio raíz y ejecutamos *"mkdir /data"* y *"mkdir /data/ftp"* para que nos cree una carpeta llamada igual que el nombre que le hemos dado a la partición, pese a que no es necesario que se llamen igual. Hecho esto, editamos el fichero */etc/fstab* y añadimos al final la linea *"LABEL=/data/ftp /data/ftp ext4 defaults 1 2".*

Para la instalación de FTP, vamos a ejecutar el comando *"yum install vsftpd".* Una vez instalado, vamos a crear un usuario para ftp llamado *ftpuser* con contraseña *12345* que no podrá loguearse de normal y no tendrá su home en la partición que acabamos de crear, en /data/ftp/ftpuser. Hecho esto, creamos el archivo */etc/vsftp/chroot_list* que nos permite enjaular usuarios, o no, dependiendo de la configuracion. Para crear el archivo, ejecutamos *"touch /etc/vsftp/chroot_list".* Para iniciar el servicio, ejecutamos *"systemctl start vsftpd".* Para ponerlo en el inicio, ejecutamos *"systemctl enable vsftpd"*. Siguiente, debemos de decirle al sistema que FTP debe poder asociarse a cualquier puerto al entrar en modo pasivo con el comando *"setsebool -P ftpd_use_passive_mode 1".* Después ejecutamos *"setsebool -P ftp_home_dir 1".*

Ahora editamos el fichero de configuración de vsftp. Lo primero que hacemos es inhabilidar a los usuarios anonimos con *anonymus_enable=no*. Después habilitamos el enjaulado de usuarios con [imagen].

Hecho esto, vamos a habilitar el soporte SSL/TLS. Navegamos hasta el directorio */etc/pki/tls* y ejecutamos la orden "*openssl req -sha256 -x509 -nodes -days 1825 -newkey rsa:4096 -keyout private/vsftpd.key -out certs/vsftpd.crt*" (hay que tener cuidado porque en *alcancelibre.org* pone las lineas con una '\' al final y eso da error). Una vez la crea, se nos piden datos de la empresa que monta el FTP, como información adicional. Ahora los archivos de certificado y firma digital deben tener permisos de solo lectura para root, para ello utilizamos "*chmod 400 certs/vsftpd.crt private/vsftpd.key*"

Ahora editamos el archivo */etc/vsftpd/vsftpd.conf.* Añadimos el siguiente contenido:

```
# Habilita el soporte de TLS/SSL
ssl_enable=YES
# Deshabilita o habilita utilizar TLS/SSL con usuarios anónimos
allow_anon_ssl=NO
# Obliga a utilizar TLS/SSL para todas las operaciones, es decir,
# transferencia de datos y autenticación de usuarios locales.
# Establecer el valor NO, hace que sea opcional utilizar TLS/SSL.
force_local_data_ssl=YES
force_local_logins_ssl=YES
# Se prefiere TLSv1 sobre SSLv2 y SSLv3
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# Rutas del certificado y firma digital
rsa_cert_file=/etc/pki/tls/certs/vsftpd.crt
rsa_private_key_file=/etc/pki/tls/private/vsftpd.key
# Los desarrolladores de FileZilla decidieron con la versión 3.5.3 que
# eliminarían el soporte para el algoritmo de cifrado 3DES-CBC-SHA,
# con el argumento de que este algoritmo es una de los más lentos.
# Sin embargo con ésto rompieron compatibilidad con miles de
# servidores FTP que utilizan FTPES. La solución temporal, mientras
# los desarrolladores de FileZilla razonan lo absurdo de su
# decisión, es utilizar la siguiente opción:
ssl_ciphers=HIGH
# Filezilla además requiere desactivar la siguiente opción que puede
# romper compatibilidad con otros clientes. Cabe señalar que Filezilla
# se ha convertido en un desarrollo políticamente incorrecto por dejar
# de respetar los estándares.
require_ssl_reuse=NO
```

Para enjaular usuarios, escribimos la linea del usuario del fichero */etc/passwd* y lo copiamos en el archivo */etc/vsftpd/chroot_list.*

Una vez hecho esto, es necesario abrir los puertos tcp 20 y 21, por lo que ejecutamos en CentOS: "*firewall-cmd --permanent –add-port=20/tcp*" y "*firewall-cmd --permanent –add-port=21/tcp*".

Para probar el servidor VSFTPD vamos a utilizar el cliente LFTP, por consola de ubuntu.

Para ejecutarlo hacemos "*lftp -e 'set ftp:ssl-force true' -e 'set ssl:verify-certificate no' [IP_server]".* Después ejecutas "*user [nombre_usr]"*. Ya estás en el sistema. Para salir ejecutas "*bye*".

DHCP

Para intalar el servicio de DHCP, el primer paso es ejecutar "*yum install dhcp*". Si se ha configurado DNS antes, es recomendable volver a poner el fichero */etc/resolv.conf* como estaba antes, para que yum encuentre bien nuestros espejos de descarga. Una vez hecho esto, hacemos una copia de seguridad del archivo *dhcpd.conf* con el comando *"cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.original"*. Ahora ya podemos configurar dhcp sin ningún problema. Lo primero que establecemos son las opciones del servidor:

server-identifier 192.168.100.1:

ddns-updddate-style interim;

ignore client-updates;

authoritative;

default-lease-time 900;

max-lease-time 7200;

option ip-forwarding off;

option domain-name "dhcp.centos.asorc.com";

option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org;

Hecho esto, podemos ya establecer las subredes del dhcp. En nuestro caso, se crea una subred por interfaz, a esto hay que añadir que se ha creado una nueva interfaz de conexión host-only sin servidor DHCP para poder probar este servicio. Las subredes quedarían así:

```
subnet 192.168.100.0 netmask 255.255.255.0 {
        interface enp0s9;

        option routers 192.168.100.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.100.255;
        range 192.168.100.3 192.168.100.254;
}
```

DNS

Para instalar el servidor de DNS, basta con escribir *yum install named.* Una vez instalado el servicio, hemos de darlo de alta en el sistema con *systemctl enable named* y añadir el servicio al firewall con *firewall-cmd –permanent –add-service named.* Hecho esto, ya podemos configurar el servidor a nuestro gusto. Lo primero que hacemos es editar *named.conf*, donde establecemos las opciones y zonas del servidor:

```
 options {
        directory "/var/named";
        forwarders {
                193.145.233.5;
                172.25.40.52;
                172.25.40.81;
                8.8.8.8;
                8.8.4.4;
        };
          forward first;
};
zone "centos.asorc.com" IN {
        type master;
        file "db.centos.asorc.com";
        allow-update { none; };
};


zone "embutidosgutierrez.com" IN {
        type master;
        file "db.embutidosgutierrez.com";
        allow-update { none; };
};
zone "56.168.192.in-addr.arpa" IN {
        type master;
        file "db.192.168.56";
        allow-update { none; };
};
```

Una vez hemos declarado los nombres de las zonas, tenemos que crear sus archivos de direcciones. Empezamos por el archivo de *centos.asorc.com:*

```
$TTL 86400
@       IN      SOA     centos.asorc.com.       shirkam.centos.asorc.com 2 3H 15H 1W 3H
```

; serial refresh retry expire miminum

IN NS centos.asorc.com.

IN A 192.168.56.3

mail IN MX 10 centos.asorc.com.

mail IN A 192.168.56.3

www IN CNAME centos.asorc.com.

ftp IN CNAME centos.asorc.com.

Y el dns inverso 192.168.56:

$TTL 86400

@ IN SOA centos.asorc.com. shirkam.centos.asorc.com. 2 3H 15H 1W 3H

; serie refresh retry expire minimum

IN NS centos.asorc.com.

3 IN PTR centos.asorc.com.

VNC

Instalamos x11vnc con la orden *yum install x11vnc.* Una vez instalado,debemos crear una contraseña de acceso con la orden *x11vnc-storepasswd* la que creara una contraseña de acceso en el archivo */home/<user>/.vnc/passwd.* Ahora simplemente debemos iniciar el servidor con la orden *x11vnc -bg -usepw -forever -rfbport [puerto]*. Por último, nos aseguramos que el puerto elegido esté abierto en el firewall en modo TCP.

WINE

Para instalar wine, solo tenemos que escribir *yum install wine.* Una vez hecho esto, la primera vez que se ejecute descargará un par de librerias necesarias, según la aplicación. Wine viene con una aplicación de ejemplo, el bloc de notas de windows.

FreeBSD

Licencia

La redistribución y el uso en las formas de código fuente y binario, con o sin modificaciones, están permitidos siempre que se cumplan las siguientes condiciones:

1. Las redistribuciones del código fuente deben conservar el aviso de copyright anterior, esta lista de condiciones y el siguiente descargo de responsabilidad.

2. Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente renuncia en la documentación y/u otros materiales suministrados con la distribución.

ESTE SOFTWARE SE SUMINISTRA POR <TITULAR DEL COPYRIGHT> "COMO ESTÁ" Y CUALQUIER GARANTÍA EXPRESA O IMPLÍCITAS, INCLUYENDO, PERO NO LIMITADO A, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN Y APTITUD PARA UN PROPÓSITO DETERMINADO SON RECHAZADAS. EN NINGÚN CASO <TITULAR DEL COPYRIGHT> SERÁ RESPONSABLE POR NINGÚN DAÑO DIRECTO, INDIRECTO, INCIDENTAL, ESPECIAL, EJEMPLAR O CONSECUENTE (INCLUYENDO, PERO NO LIMITADO A, LA ADQUISICIÓN DE BIENES O SERVICIOS; LA PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS; O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) O POR CUALQUIER TEORÍA DE RESPONSABILIDAD, YA SEA POR CONTRATO, RESPONSABILIDAD ESTRICTA O AGRAVIO (INCLUYENDO NEGLIGENCIA O CUALQUIER OTRA CAUSA) QUE SURJA DE CUALQUIER MANERA DEL USO DE ESTE SOFTWARE, INCLUSO SI SE HA ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS.

Las opiniones y conclusiones contenidas en el software y la documentación son las de los autores y no deben interpretarse como la representación de las políticas oficiales, ya sea expresa o implícita, de <titular del copyright>.

SSH clave publica

Para utilizar la firma digital al conectarnos a un ssh, utilizamos primero los siguientes comandos de configuracion:
Creamos directorio de claves

mkdir -m 0700 ~/.ssh/
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorithed_keys

(En el cliente)
Generamos clave:
ssh-keygen -t dsa
Cambiamos permisos
chmod -R go-rwX ~/.ssh

Copiamos el contenido de la firma digital publica en el servidor remoto
cat ~/.ssh/id_sha.pub | ssh shirkam@192.168.56.102 "cat >>/usr/home

/shirkam/.ssh/authorized_keys"

proftpd

Navegamos hasta /usr/ports/ftp/proftpd y hacemos *make install clean.* Una vez hecho, editamos el fichero */usr/local/etc/proftpd.conf* y borramos la parte de acceso anónimo al servicio. Después, tenemos que escribir en el fichero */etc/hosts* nuestra ip de host-only junto con nuestro nombre en la red para que lo reconozca el servicio y pueda iniciarse.

DNS

Vamos a */usr/ports/dns/bind99* y ejecutamos *make install clean.* Hecho esto, vamos a añadir las zonas directas e inversas en */usr/local/etc/namedb/named.conf*

```
zone "freebsd.asorc.com" {
        type master;
        allow-update { none; };
        file "/usr/local/etc/namedb/bd.freebsd.asorc.com";
};

zone "56.168.192.in-addr.arpa" {
        type master;
        allow-update { none; };
        file "/usr/local/etc/namedb/bd.56.168.192";
};
```

Hecho esto, vamos a escribir las zonas para que el servidor funcione. Primero, la zona "freebsd.asorc.com":

```
TTL 86400
@       IN      SOA     freebsd.asorc.com       shirkam.freebsd.asorc.com 2 2H  15H 1W 3H

        IN NS           freebsd.asorc.com.
        IN A            192.168.56.102
www     IN CNAME        freebsd.asorc.com.
mail    IN MX 10        freebsd.asorc.com.
mail    IN A            192.168.56.102
ftp     IN CNAME        freebsd.asorc.com.
```

Y ahora la inversa:

```
TTL 86400
@       IN      SOA     freebsd.asorc.com       shirkam.freebsd.asorc.com 2 2H 15H 1W 3H
```

IN NS freebsd.asorc.com.

IN A 192.168.56.102

www IN CNAME freebsd.asorc.com.

mail IN MX 10 freebsd.asorc.com.

mail IN A 192.168.56.102

ftp IN CNAME freebsd.asorc.com.

Windows

Licencia

Estas licencias también se conocen con el nombre de software de código privado o privativo. En ellas los propietarios establecen los derechos de uso, distribución, redistribución, copia, modificación, cesión y en general cualquier otra consideración que se estime necesaria. Este tipo de licencias, por lo general, no permiten que el software sea modificado, desensamblado, copiado o distribuido de formas no especificadas en la propia licencia (piratería de software), regula el número de copias que pueden ser instaladas e incluso los fines concretos para los cuales puede ser utilizado. La mayoría de estas licencias limitan fuertemente la responsabilidad derivada de fallos en el programa. Los fabricantes de programas sometidos a este tipo de licencias por lo general ofrecen servicios de soporte técnico y actualizaciones durante el tiempo de vida del producto. Distinguimos dos tipos de licencias:

1. EULA

   En inglés End User License Agreement, es una licencia por la cual el uso de un producto sólo está permitido para un único usuario (el comprador). La licencia EULA tiene por objetivo limitar al usuario a tomar acciones, elecciones u opciones sobre el software, entre tanto que la GNU GPL se dedica a salvaguardar los derechos de los desarrolladores originales para mantener la continuidad y la accesibilidad del código fuente para el software.
   Esta licencia prohíbe la copia, permite el empleo en un único computador con un máximo de 2 procesadores. Puede ser empleado como Web Server o File Server, exige registro a los 30 días, puede dejar de funcionar si se efectúan cambios en el hardware. Sólo puede ser transferida una vez a otro usuario. Impone limitación sobre la ingeniería inversa. Da a Microsoft derecho para en cualquier momento recoger información del sistema y su uso, y también para entregar dicha información a terceros. La garantía es sólo por los primeros 90 días. Las actualizaciones y los parches no quedan cubiertos por la garantía.
2. CAL

   Si se tienen PCs conectados en red, y se utiliza un servidor en red y los PCs de la red acceden al software del servidor (o servidores) para realizar determinadas funciones como compartir archivos e imprimirlos se necesita este tipo de licencia. Para poder acceder a este software de manera legal, se necesita una Client Access License o CAL. Una CAL es una licencia que le da al usuario el derecho a utilizar los servicios de un servidor.

SSH

Para instalar ssh en windows, vamos a emplear FreeSSH. Primero lo descargamos de la pagina principal.Hecho esto, abrimos el instalador y dejamos todas las opciones que nos de por defecto. Al terminar de instalar, nos preguntará si lo queremos como servicio del sistema. Le decimos que sí y ya tenemos ssh en windows. Una vez instalado, tenemos que cambiar el puerto del servidor, ya que no deja iniciarlo en el puerto por defecto, el 22, ya que dice que el puerto ya está en uso. Además de eso, añadimos dos usuarios, uno que se loguea con una contraseña, y otro que se conecta mediante una clave pública. Para utilizar la clave pública, cogemos la clave generada para los anteriores servidores, y la copiamos en un archivo con el nombre del usuario que va a conectarse de esta manera. Es importante que este archivo no lleve extensión. Hecho esto, ya podemos conectarnos de las dos formas a windows server.

VNC

Para instalar vnc, lo descargamos de realvnc.com. Durante la instalación se nos pide una licencia, y obtenemos una gratuita, para un solo usuario. El programa se instala y detecta automaticamente las redes a las que estás conectado. Hecho esto, ya podemos conectarnos con cualquier cliente al servidor.

DNS

Para DNS, lo instalamos desde el asistente de roles. Una vez termina el instalador, tenemos que entrar en la vista de DNS en el *server manager*,, y un avez ahi, abrir de *tools* el *DNS manager.* En esa ventana, podemos observar todos los servidores que tenemos en la maquina, y crear nuevas zonas dentro de cada uno de ellos, además de editar las antiguas y añadir entradas en las zonas.

CYGWIN

Para CYGWIN, vamos a la página oficial y lo descargamos. Una vez abrimos el instalador, es necesario elegir el mínimo numero de paquetes necesarios, puesto que la instalación del sistema entero ocupa demasiado espacio, y trae demasiados paquetes que no utilizariamos.

Bibliografia

http://www.cyberciti.biz/faq/centos-ssh/
https://ramilcanosys.wordpress.com/2012/06/12/configurar-un-servidor-ssh-windows-con-autenticacion-de-usuario-con-public-keys-para-que-no-pida-contrasena/