Examen Semana 1

Instrucción

El propósito del Examen 01 es el de aplicar los conocimientos de certificados digitales, dentro de la configuración de servicios/servidores en Linux.

En este sentido se debe prepara una maquina virtual con sistema operativo ***Ubuntu Server*** 20.04 LTS https://ubuntu.com/download/server con las siguientes características:

- Memoria RAM 2G
- 2 CPU
- Almacenamiento 16 G
- Una Tarjeta de Red
- Acceso a Internet

En este servidor luego de actualizarlo (update) se deben instalar un servidor ***DNS*** (***Bind***) y un servidor ***Web*** (***Nginx***).

En ambos casos se procederá a, la configuración de los mismos incluyendo las capas de seguridad criptográfica. (***DNSSEC*** y ***SSL***)

En el caso de la configuración ***SSL*** se utilizara un certificado ***auto firmado***, por lo que se debe implementar un CA (***myCA***) con ***openssl***

Detalle de la configuración

El servidor Ubuntu/Linux sera configurado de la siguiente forma:

En el archivo de dominios ***Dominios.md*** (***Dominios.pdf***); cada alumno deberá buscar su nombre y tomar el nombre de Host y el nombre de Domino que le corresponde para este documento tomaremos el nombre ejemplo de ***Jhon Doe*** al que le corresponde el dominio ***jhondoe.com*** y el nombre de host ***server01.jhondoe.com***.

En este sentido esta seria la configuración de los distintos servicios :

DNS

1. Se debe configurar el nombre del servidor de acuerdo a la asignación antes defendida; en este caso el nombre del servidor debe ser ***sever01.jhondoe.com***, la configuracoin debe ser FQND (fully qualified domain name), y debe ser reflejada en el archivo de /etc/host con el ***ip*** del servidor
2. Luego se configura el servido DNS (bind) como ***master primario*** del domino ***jhondoe.com***, NO se configurara un servidor secundario. El servidor DNS debe tener un acl de tal modo que solo sea recursivo para si mismo.

3. Debe existir un registro **A** de ***server01.jhondoe.com*** apuntando al **ip** del servidor
4. Debe existir un registro **MX** de prioridad 10 apuntando a ***server01.jhondoe.com***
5. Debe existir un registro **CNAME** de ***www.jhondoe.com*** apuntando a ***server01.jhondoe.com***
6. Se debe configurar la Zona reversa (PTR) acorde a la red y el ip del servidor.
7. Se debe verificar toda la configuración y reiniciar el servicio, el DNS debe ser funcional
8. Una vez que el dominio este configurado se debe genera dos pares de llaves (ZSK, KSK) para el domino ***jhondoe.com***
9. Se debe configurar los registros DNSKEY del dominio (o en la zona) ***jhondoe.com***
10. Se debe firmar toda la zona/dominio ***jhondoe.com*** generando el archivo de configuración del dominio ***jhondoe.com***
11. Se debe apuntar al nuevo archivo de zona/domino con la extencion ***.signed***
12. Se debe comprobar que la configuración este correcta y reiniciar el servicio,
13. El servidor DNS debe ser funcional al final del ejercicio
14. Por último se debe configurar el servidor ubuntu/linux para que su resolver DNS sea el local que acabamos de configurar

NGINX

1. Se debe crear con ayuda de openssl una Autoridad de Certificación (local), para este efecto, se creara en el **home** del usuario (alumno) el directorio myCA y su correspondiente estructura:
    1. serial
    2. index.txt
    3. private (directorio)
    4. signedcerts (directorio)
2. Se debe crear un archivo de configuración de openssl (caconfig.cnf), con el siguiente detalle
    1. commonName = UAGRM Root Certificate Authority
    2. stateOrProvinceName = Santa Cruz
    3. countryName = BO
    4. emailAddress = postgradocomputacion@uagrm.edu.bo
    5. organizationName = Universidad Autonoma Gabriel Rene Moreno
    6. organizationalUnitName = SCHOOL OF ENGINEERING
3. Se debe generar la llave pública y privada del CA (pasword sesamo) (ojo con el SHA256)

4. Para genera un archivo CSR (Certificate Signing Request) del dominio ***jhondoe.com*** se debe prepara un archivo de configuración : **jhondoe.cnf**, con el sigiente detalle : (ojo , aquí deben usar su propio dominio y remplazar su información que corresponda)
    1. commonName = www.jhondoe.com < – el dominio asignado a cada alumno mas www>
    2. stateOrProvinceName = Santa Cruz
    3. countryName = BO
    4. emailAddress = jhon123@jhondoe.com < – el correo real de cada alumno >
    5. organizationName = Jhon Doe < – Nombre completo de cada alumno >
    6. organizationalUnitName = Diplomado infraestructura TI
5. Con la configuración de **jhondoe.cnf**, generar un CSR por 1 año (pasword sesamo)
6. Luego con la configuración de CA (caconfig.cnf) firmar y genera el certificado SSL
7. En el paso 6 ya se crearon la llave privada y el certificado del servidor ***www.jhondoe.com*** estos deben ser adecuados para que el NGINX los utilice :
    1. Quitar el password a la llave privada
    2. Crear un archivo crt a partir de el archivo pem
    3. Y crear el archivo **jhondoe.crt** (boundle), con la unión del crt de mi dominio y el crt del CA
8. Configurar los snippets (pedazos) de configuración ssl (ssl-params.conf) y path de los certificados (jhondoe.conf)
9. Configurar el virtual host de nginx para el nombre de servidor ***www.jhondoe.com***, con ayuda de los snippets
10. Crear una página html de bienvenida (hola mundo) que responda a la petición ***https://www.jhondoe.com***
11. Verificar todo con el comando ***nginx -t***
12. Por último reiniciar el servidor Nginx y verificar que todo funciona
    1. Si se navega por IP debe responder la pagina por defecto
    2. Si se navega ***https://www.jhondoe.com***, debe mostrarse la página que se creó en el paso 10 (el navegador no podrá verificar la autenticidad del certificado auto firmado por lo que se debe incluir como excepción en el navegador)

3. Si se navega ***http://www.jhondoe.com***, debe mostrarse la página que se creó en el paso 10

Referencias

Se pueden usar las referencia de configuración siguientes:

https://www.digitalocean.com/community/tutorials/how-to-setup-dnssec-on-an-authoritative-bind-dns-server-2

https://www.ibm.com/docs/es/oala/1.3.5?topic=SSPFMY_1.3.5/com.ibm.scala.doc/config/iwa_cnf_lgsth_lfa_t.html

https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-nginx-in-ubuntu-20-04-1

NOTA

> No olvide que el Dominio –> jhondoe.com es un ejemplo se debe usar el que, a cada alumno le corresponde, este es una combinación de su nombre y segundo apellido, y esta definido en el archivo adjunto Dominios.pdf (Dominios.md)