Protocolos de Comunicación TCP/IP

Trabajo de Laboratorio N° 8

Temas:

- Certificados Digitales
- Protocolo SSL y HHTPS
- IPSEC

Laboratorio 1: Instalación de certificados de clave pública y su uso en protocolo SSL

a) Uniendo un equipo al Dominio

1. Configure en la configuración de TCP/IP, en configuración de DNS tanto del servidor y del cliente ingrese la IP del servidor de dominio LABLAN (192.168.0.100)
2. Vaya al Panel de control y abra Sistema
3. En Nombre de equipo, haga clic en **cambia**r.
4. Cambie a Miembro de Dominio y ponga el dominio LABLAN
5. En nombre de usuario coloque AdminXX (donde XX es el número de puesto) y contraseña 1234
6. Luego Acepte y reinicie el computador.
7. Presione Ctrl derecho+Supr.
8. En el cuadro de diálogo Iniciar sesión en Windows, en el cuadro Nombre de usuario, escriba AdminXX y contraseña 1234
9. En el cuadro "Conectarse a", elija en el nombre del dominio **LABLAN** y acepte.

b) Instalando el servicio de Web Server

1. Haga clic en **Inicio**, haga clic en **Panel de control** y, a continuación, haga clic en **Agregar o quitar programas**.
2. En **Agregar o quitar programas**, haga clic en **Agregar o quitar componentes de Windows**.
3. En el Asistente para componentes de Windows, en la lista **Componentes**, seleccione **Servidor de aplicaciones**.
4. Haga clic en **Siguiente**.

5. Cuando el asistente complete la instalación, haga clic en **Finalizar**.

c) Creando un certificado de clave publica de equipo

1. Inicie Internet Explorer en el servidor e ingrese a http://srvlab/certsrv.
2. Haga clic en **Solicitar un certificado**, y a continuación, haga clic en **Siguiente**.
3. Haga clic en **Solicitud avanzada**, y a continuación, haga clic en **Siguiente**.
4. Haga clic en **Crear y enviar una solicitud a esta CA**, y a continuación, haga clic en **Siguiente** para que se muestre el formulario de solicitud del certificado.
5. Elija la plantilla de **Servidor Web**
6. Especifique en el nombre, el nombre FQDN completo del equipo del servidor, por ejemplo, servidorxx.lablan.com (donde servidorxx es el nombre de su equipo), el resto de los campos ingrese datos genéricos.
7. Para el proveedor de servicios criptográficos (CSP), seleccione **Microsoft RSA**.
8. Active la casilla **Almacenar el certificado en el almacén de certificados del equipo local**.
9. Haga clic en **Enviar** para enviar la solicitud.
10. Descargue e instale el certificado emitido de la entidad emisora de certificados.

d) Verificando la instalación del certificado

1. Escriba **mmc** y haga clic en **Aceptar**.
2. En el menú **Consola** menú, haga clic en **Agregar o quitar complemento**.
3. Haga clic en **Agregar**.
4. Haga clic en **Certificados** y, a continuación, en **Agregar**.
5. Seleccione **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**.
6. Asegúrese de que el equipo local (el equipo servidor) está seleccionado y haga clic en **Finalizar**.
7. Haga clic en **Cerrar**.
8. En la vista de árbol del panel izquierdo, expanda **Certificados (equipo local)**, expanda **Personal** y, a continuación, seleccione **Certificados**.
9. Verifique las propiedades del certificado

e) Asignar un certificado de servidor SSL a un sitio Web

1. Abra el Administrador IIS, expanda el equipo local y, a continuación expanda la carpeta de sitios Web.
2. Haga clic con el botón secundario del mouse en el **Sitio Web predeterminado** y haga clic en **Propiedades**.
3. Seleccione la ficha **Seguridad de directorios** y en **Comunicaciones seguras**, haga clic en **Certificado de servidor**.
4. En **Asistente para certificados de servidor Web**, haga clic en **Asignar un certificado ya existente**.
5. Siga los pasos del **Asistente para certificados de servidor Web** eligiendo el certificado instalado emitido por servidorca. Dejar seleccionado el puerto 443
6. Una vez que haya terminado el asistente, vea la información sobre el certificado haciendo clic en el botón **Ver certificado** de la ficha **Seguridad de directorios** de la página **Propiedades** de los sitios Web.

f) Verificando acceso desde el cliente al servidor Web.

1. Arranque el wireshark en el servidor o cliente
2. Desde el cliente acceda a la página por defecto del servidor web de su servidor (http://servidorxx.lablan.com) donde servidorxx es el nombre del servidor.
3. Verifique con wireshark que puede ver el dialogo entre el cliente y el servidor
4. Ahora acceda a la página por defecto a través del protocolo SSL (https://servidorxx.lablan.com)
5. ¿Qué mensaje de advertencia le aparece? ¿Por qué?
6. Acepte la advertencia ingresando al sitio web
7. Haga clic en **error de certificado, ver certificado**
8. Ingrese a **Ruta de certificación** y vea cual es el problema indica sobre el certificado
9. Ingrese desde el cliente al servidor de certificados http://srvlab/certsrv con usuario adminxx y password 1234
10. Acceda a **descargar un certificado de entidad emisora**
11. Elija descargar certificado de entidad emisora en codificación DER
12. Abra el certificado y elija Instalar certificado
13. Coloque el certificado en el almacén de certificados “Entidades de certificación raíz de confianza”, acepte las advertencias leyendo el porqué de la misma.

14. Acceda nuevamente a la pagina del servidor a través del protocolo SSL https://servidorxx.lablan.com
15. Sigue la advertencia del certificado?

Laboratorio 2: Configuración e implementación de IPSec

Observación: Se trabajará de a pares (uno será el servidor y el otro el cliente, ambos virtuales)

a) Verificando y Configurando IPSEC en Servidor

1. En el servidor, En **Herramientas administrativas** acceder a directiva de seguridad local
2. En la consola, haga clic en **directivas de seguridad IP**
3. En el panel de detalles, haga clic derecho en **Servidor seguro** y luego haga clic en **Propiedades**
   ¿Cuál es el método de autenticación predeterminado para todo el tráfico IP y las reglas de seguridad IP <Dinámicas>?
4. Ponga modificar para ver las diferentes configuraciones que se se pueden cambiar.
5. Haga clic en **Aceptar**
6. En el panel de detalles, haga clic derecho en **Servidor seguro** y luego haga clic en **Asignar**
7. Haga clic en **Inicio** y luego **Ejecutar,** ejecute **gpupdate/force**
8. En **Herramientas administrativas** y entre en **Servicios**
9. En la consola de servicios, en el panel de detalles, haga clic derecho en **Servicios IPSec** y luego **Reiniciar**

b) Verificando y Configurando IPSEC en Cliente

1. En el cliente, en **Ejecutar** escriba **\\servidorxx** (donde servidor es el nombre del servidor recién configurado ¿Se estableció una conexión con el servidorxx? **La conexión debe fallar**
2. En **Herramientas administrativas** acceder a directiva de seguridad local
3. En la consola, haga clic en **directivas de seguridad IP**

4. En el panel de detalles, haga clic derecho en **Cliente** y luego haga clic en **Propiedades.** ¿Cuál es el método de autenticación predeterminado las reglas de seguridad IP <Dinámicas>?
5. Haga clic en **Aceptar**
6. En el panel de detalles, haga clic derecho en **cliente** y luego haga clic en **Asignar**
7. Haga clic en **Inicio** y luego **Ejecutar,** ejecute **gpupdate/force**
8. En **Herramientas administrativas** y entre en **Servicios**
9. En la consola de servicios, en el panel de detalles, haga clic derecho en **Servicios IPSec** y luego **Reiniciar**
10. Inicie wireshark y comience a capturar los paquetes
11. En el cliente, en **Ejecutar** escriba **\\servidorxx** (donde servidor es el nombre del servidor recién configurado ¿Se estableció una conexión con el servidorxx?
12. Desde el cliente acceda a la página por defecto del servidor web de su servidor (http://servidorxx.lablan.com) donde servidorxx es el nombre del servidor.
13. ¿Es posible descifrar el contenido en el wireshark como en el ejercicio anterior?