**CLASSWORK #3**

**REDES 2**

**S2-2022**

Daniel Felipe Martínez Alzate

[dmartin40973@universidadean.edu.co](mailto:dmartin40973@universidadean.edu.co)

**Universidad EAN, Facultad de Ingeniería, Pregrado en Ingeniería de Sistemas**

**CLASSWORK 3  
Activity: Individual**  
**Subject: Network Security**  
**Deliverable:** **Word-File**(LastnameName\_Classwork3.doc)**+** **Other-Files** (LastnameName\_Classwork3.zip)  
**Deadline:** **Sun-23-Oct** (11:59pm)

According to the Labs, make a detailed documentation for all practices done in Matlab and Packet Tracer in class, including all graphical user interface (matlab) and all connectivity testing (packet tracer):

**[40/100]** (Matlab) AppDesigner: Encryption  
**[30/100]** (PKT) Virtual Private Network (VPN): [Classwork3 - Configuring VPNs.pdf](https://virtual.universidadean.edu.co/courses/13631/files/7575957?wrap=1)   
**[30/100]** (PKT) Demilitarized Zone (DMZ)

(Matlab) AppDesigner: Encryption

En primer lugar, tenemos que abrir app designer en Matlab, ejecutando el comando “appdesigner” en el comman window de Matlab

Text

Description automatically generated

Creamos una interfaz nueva

Graphical user interface, text, application

Description automatically generated

Diseñamos nuestra interfaz a gusto: agregando un Dropbox para seleccionar el método de encriptado, tres edid field(text), para el texto original, la clave, binario encriptado, y texto encriptado respectivamente, además, agregaremos un botón para poder realizar el encriptado

Chart, bar chart

Description automatically generated

Asignamos callbacks a el dropbox

% Value changed function: metodoenc

function metodoencValueChanged(app, event)

%ACTIVAR CASILLA CLAVE

%TRAEMOS EL VALOR ACTUAL DEL DROPBOX

value = app.metodoenc.Value;

%SI EL VALOR DEL DROPBOX ES IGUAL A VERNAM, ENTONCES SE

%ACTIVARÁ EL EDIT FIELD DE CLAVE

if value == "VERNAM"

app.CLAVETextArea.Enable = "on";

else

%SI NO SE CUMPLE LA CONDICION ESTARÁ DESACTIVADO

app.CLAVETextArea.Enable = "off";

end

end

Ahora asignamos todo el código al callback del botón

% Button pushed function: ENCRIPTAR

function ENCRIPTARButtonPushed(app, event)

clc

%GUARDAMOS EL TEXTO INGRESADO EN UNA VARIABLE

textoOri = app.TEXTO\_ORIGINAL.Value;

%PASAMOS ESE TEXTO A CODIGO ASCII CON LA FUNCION DOUBLE

ascii = double(textoOri);

% CREAMOS CONDICIÓN PARA CAMBIAR DE CIFRADO DEPENDIENDO DEL

% VALOR DEL DROPBOX

if app.metodoenc.Value == "CESAR INGLES"

% CESAR EN INGLES

for n=1: length(ascii)

%CONDICIONALES PARA QUE LAS ULTIMAS LETRAS EQUIVALGAN A

%LAS PRIMERAS

if (ascii(n)==32)

ascii(n) = 29;

elseif (ascii(n)==120)

ascii(n)=double('a')-3;

elseif (ascii(n)==121)

ascii(n)=double('b')-3;

elseif (ascii(n)==122)

ascii(n)=double('c')-3;

elseif (ascii(n)==88)

ascii(n)=double('A')-3;

elseif (ascii(n)==89)

ascii(n)=double('B')-3;

elseif (ascii(n)==90)

ascii(n)=double('C')-3;

end

end

% A CADA NUMERO SE LE SUMAN 3 POSICIONES

cesar = ascii + 3;

% PASAMOS ASCII A TEXTO

criptograma = char(cesar);

%LO PASAMOS A CODIGO BINARIO

bits = dec2bin(ascii + 3)

% ORDENAMOS LA MATRIZ EN UNA SOLA

bitstream= reshape(bits',1,[])

%ASIGNAMOS LOS VAMORES OBTENID0S A SUS RESPECTIVOS CAMPOS

%DE LA INTERFAZ

app.TEXTO\_ENCRIPTADO.Value = criptograma;

app.BIN\_ENCRIPTADO.Value = bitstream

elseif (app.metodoenc.Value == "CESAR ESPAÑOL")

%CESAR EN ESPAÑOL

for n=1: length(ascii)

if (ascii(n)==32)

ascii(n) = 32-3;

elseif (ascii(n)==120)

ascii(n)=double('a')-3;

elseif (ascii(n)==121)

ascii(n)=double('b')-3;

elseif (ascii(n)==122)

ascii(n)=double('c')-3;

elseif (ascii(n)==88)

ascii(n)=double('A')-3;

elseif (ascii(n)==89)

ascii(n)=double('B')-3;

elseif (ascii(n)==90)

ascii(n)=double('C')-3;

%Español

%AGREGAMOS LAS CONDICIONES PARA LAS LETRAS EN ESPAÑOL,

%PUES SE AGREGA LA Ñ AL ABECEDARIO

elseif (ascii(n)==108)%l

ascii(n)=double('ñ')-3;

elseif (ascii(n)==109)%m

ascii(n)=double('o')-3;

elseif (ascii(n)==110)%n

ascii(n)=double('p')-3;

elseif (ascii(n)==double('ñ'))%ñ

ascii(n)=double('q')-3;

elseif (ascii(n)==76)%L

ascii(n)=double('Ñ')-3;

elseif (ascii(n)==77)%M

ascii(n)=double('O')-3;

elseif (ascii(n)==78)%N

ascii(n)=double('P')-3;

elseif (ascii(n)==double('Ñ'))%Ñ

ascii(n)=double('Q')-3;

end

end

%MISMO PROCESO QUE CON EL CIFRADO EN INGLES

cesar = ascii + 3;

criptograma = char(cesar);

bits = dec2bin(cesar);

bitstream = reshape(bits',1,[])

app.TEXTO\_ENCRIPTADO.Value = criptograma;

app.BIN\_ENCRIPTADO.Value = bitstream

app.TEXTO\_ENCRIPTADO.Value = criptograma;

else

% CIFRADO VERNAM

% TRAEMOS EL TEXTO, LO PASAMOS A BINARIO Y LO ORDENAMOS EN

% UNA FILA

bits = dec2bin(ascii)

bitstream = reshape(bits',1,[])

%RECORREMOS LA MATRIZ Y LA GUARDAMOS EN UN ARREGLO CON

%VALORES NUMERICOS

arraytexto = [];

longitud = length(bitstream);

for x=1 : longitud

if (bitstream(x)=='0')

arraytexto=[arraytexto 0];

elseif (bitstream(x)=='1')

arraytexto=[arraytexto 1];

end

end

%CREAMOS UNA CLAVE ALEATORIA CON LOS VALORES DE 0 Y 1, CON

%LA MISMA LONGITUD QUE EL BITSTREAM OBTENIDO ANTERIORMENTE

clavem = randi([0 1],1,longitud)

%PASAMOS LA MATRIZ A UN ARREGLO

clave = mat2str(clavem)

%UNA VEZ TENIDO LOS DOS ARREGLOS RESULTANTES, PODREMOS

%HACER LA COMPARACION XOR

result = xor(arraytexto,clavem)

%RECORREMOS EL ARREGLO OBTENIDO PARA PASAR LOS VALORES

%LÓGICOS A TEXTO

cifrado = []

for x=1 : length(result)

if (result(x)== 0)

cifrado=[cifrado '0'];

elseif (result(x)== 1)

cifrado=[cifrado '1'];

end

end

%PASAMOS EL BITSTREAM RESULTANTE A CARÁCTERES, RECORRIENDO

%LA MATRIZ, SEPARANDOLA EN CONJUNTOS DE 7 CARACTERES,

%PASANDOLAS A CODIGO ASCCI Y LUEGO A CADENA DE TEXTO

a = (char(bin2dec(reshape(cifrado,7,[]).')).')

%ASIGNAMOS LOS VALORES EN SU RESPECTIVO CAMPO DE LA

%INTERFAZ

app.CLAVETextArea.Value = clave

app.TEXTO\_ENCRIPTADO.Value = a

app.BIN\_ENCRIPTADO.Value = cifrado

end

end

Pruebas funcionamiento

Graphical user interface, text, application, chat or text message

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

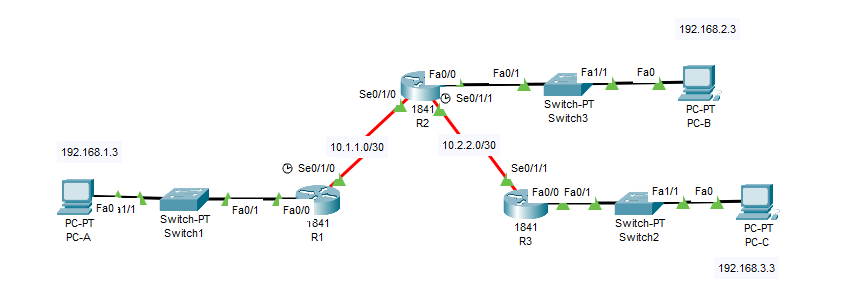
**Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated**

**(PKT) Virtual Private Network (VPN)**

A continuación la configuración de VPN(operativo) para la siguiente red



**Tabla de direccionamiento**

Table

Description automatically generated

Se ultilizará el Router 184, pues este ya viene con el modulo securityk9 activado por defecto.

Será necesario añadir la placa WIC-2T y la WIC 2AM a los tres routers para poder conectarlos mediante cable serial DCE y para tener los puertos modem

Interfaz de usuario gráfica

Descripción generada automáticamente

Conectamos todos los dispositivos en los puertos correspondientes

Diagrama

Descripción generada automáticamente

Comenzamos a configurar las direcciones ips, basandonos en la tabla de direccionamiento.

PC-A

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

PC-B

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

PC-C

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Creamos las vlans, y añadimos las interfaces a la vlan

SWITCH A

Imagen que contiene Texto

Descripción generada automáticamente

SWITCH B

Texto, Carta

Descripción generada automáticamente con confianza media

SWITCH C

Imagen que contiene Tabla

Descripción generada automáticamente

Ahora se configuran los routers

RIP



CONEXIÓN AL SWITCH FA0/0



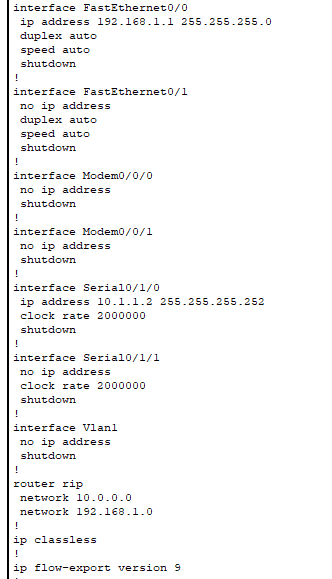
SERIAL



NO OLVIDAR HABILITAR TODOS LOS PUERTOS



ROUTER -A



ROUTER-B

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

ROUTER - C

Texto, Carta

Descripción generada automáticamente

CONFIGURACIÓN VPN

Paso 1: Probar la conectividad.

PING PC -A PC-C

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Paso 2: Identificar el tráfico interesante en el R1.



Paso 3: Configurar las propiedades de la fase 1 de ISAKMP en el R1

Texto, Carta

Descripción generada automáticamente

Paso 4: Configurar las propiedades de la fase 2 de ISAKMP en el R1

Texto, Carta

Descripción generada automáticamente

Paso 5: Configurar la asignación criptográfica en la interfaz de salida.



Parte 3: Configurar los parámetros de IPsec en el R3

Paso 1: Configurar el router R3 para admitir una VPN de sitio a sitio con el R1



Paso 2: Configurar las propiedades de la fase 1 de ISAKMP en el R3.

Texto

Descripción generada automáticamente

Paso 3: Configurar las propiedades de la fase 2 de ISAKMP en el R3

Texto, Carta

Descripción generada automáticamente

Paso 4: Configurar la asignación criptográfica en la interfaz de salida.



Parte 4: Verificar la VPN con IPsec

Texto

Descripción generada automáticamente

Ping a C

Texto

Descripción generada automáticamente con confianza baja

Texto

Descripción generada automáticamente

PING a B

Calendario

Descripción generada automáticamente con confianza media

Verificar que no se cifró el trafico no interesante

Texto

Descripción generada automáticamente

Y si vuelvo a enviar un paquete



Texto

Descripción generada automáticamente

Configuración Finalizada

Diagrama

Descripción generada automáticamente

**(PKT) Demilitarized Zone (DMZ)**

Para configurar una zona desmilitarizada se usa un firewall, en este caso se usará el 5505



Se crean tres zonas, la inside y la outside.

La inside será una zona con un nivel de siguridad del 100%, eso significa que todos los paquetes de revisan por el firewall, asi mismo no podran ingresar paquetes con nivel de seguridad inferior.

La zona Outside no cuenta con seguiridad, por lo que todos los paquetes podran entrar y salir de acá, pero esta no puede enviar paquetes a zonas con un nivel de seguridad mayor.

Por ultimo se crea la zona DMZ, la cual contará con una seguridad del 50%. El objetivo de una zona DMZ es que las conexiones desde la red OUTSIDE a la DMZ estén permitidas, pero las conexiones desde la DMZ hacia la red INSIDE no se permitan. Esto sirve para que los equipos de la DMZ den servicios a la red externa, y protegan la red interna de cualquier amenza.

Diagram, box and whisker chart

Description automatically generated

**Una vez diseñada la red se proceden a configurar los equipos**

**En primer lugar, se configura el firewall.**

**Primero se asigna la vlan 2 a la interfaz conectada a la red de OUTSIDE, por defecto todas vienen en la VLAN 1, la cual corresponde a la red INSIDE.**

**Igualmente, se le asignará la vlan 3 para la zona DMZ**

**Text

Description automatically generated**

**Una vez asignadas las vlans, se deben configurar**

**INSIDE:**

**Text, letter

Description automatically generated**

**Lo primero es asignarle el nombre, en este caso es INSIDE, y el nivel de seguridad será 100**

**Text

Description automatically generated**

**Ahora le podemos cambiar el ip address**

**A picture containing text

Description automatically generated**

****

**Por defecto viene así, pero para cambiarla primero toca borrar alguno de los dos códigos, debido a que, si se trata de cambiar entrará en conflicto con el dhcp**

****

**Se niega la instrucción de dchp address**

****

**Una vez negada, ya permitirá realizar el cambio en la dirección de la vlan y en el DHCP**

**Schematic

Description automatically generated with low confidence**

**Ahora la vlan 2**

**Text

Description automatically generated**

**Y la Dmz**

**Text

Description automatically generated**

**Este error ocurre debido a que la licencia de cisco packet tracer no cuenta con todas las funcionalidades del sistema operativo de un firewall, por lo que solo permite 2 vlans, para solucionar este error, tendremos que hacer un no forward a la red inside o Vlan1.**

**Y ya se le pueden configurar el resto de parámetros.**

**Text, letter

Description automatically generated**

**Asignamos a la interfaz ethernet 0/2 la vlan 3 correspondiente al DNZ**

****

****

**Luego se configura la ip del equipo de la red INSIDE para que sea dhcp, luego hacemos un renew y un release, para que tome una dirección ip**

**Graphical user interface, text, application, email

Description automatically generated**

**Luego se configura el equipo de la red OUTSIDE y se le asigna una ip estáticaGraphical user interface, text, application, email

Description automatically generated**

**Finalmente, se le asigna una ip estática al servidor**

**Graphical user interface, application

Description automatically generated**

**Ahora devuelta al firewall y se configura la seguridad**

**Se crea un class map, con el nombre inspection\_default y luego se hace match con el tipo de inspección estándar de paquetes, con el comando “match default-inspection-traffic”**

**Table

Description automatically generated**

**Text

Description automatically generated**

**Ahora se crea un policy map con el nombre de global\_policy, luego se vincula con el mapa de clase creado anteriormente llamado inspection default con el siguiente comando.**

**Text

Description automatically generated**

**Y a continuación se le asignara que inspeccione los paquetes ICMP**

**Text

Description automatically generated**

**Finalmente se agrega la service policy, donde se vincula con el policy map creado anteriormente seguido de global.**

**Text, letter

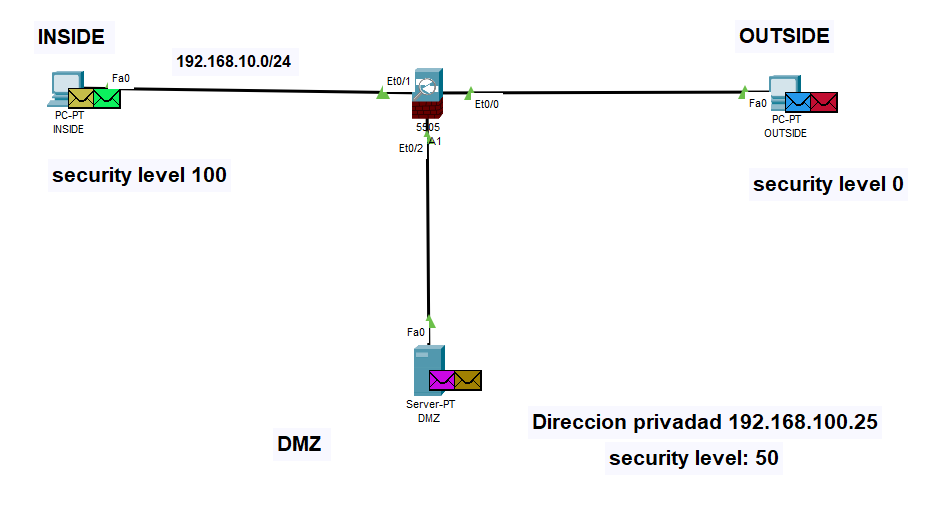
Description automatically generated**

**Se ejecuta el comando show runnig config, para ver la configuración completa del firewall, y queda de la siguiente manera.**

**Graphical user interface

Description automatically generated with low confidence**

**Pruebas**

****

**Si queremos enviar paquetes desde Un nivel de seguridad superior a un nivel inferior, va a ser exitoso**

**Graphical user interface

Description automatically generated with medium confidence**

**A picture containing table

Description automatically generated**

**Pero si queremos enviar paquetes desde un nivel de seguridad inferior a un nivel de seguridad superior, el firewall devolverá el paquete**

**Diagram

Description automatically generated**

**Graphical user interface

Description automatically generated with medium confidence**

****