UNIVERSIDAD NACIONAL DE TUCUMÁN
Facultad de Ciencias Exactas y Tecnología
Depto. de Electricidad, Electrónica y Computación

Protocolos de Comunicación TCP/IP

Trabajo de Laboratorio N° 6

Temas:

- Protocolo de Transporte: TCP

Laboratorio 1: Iniciando una conexión TCP

Configure el equipo para estar en la red 192.168.1.1xx/24 (xx numero de puesto) Ejecute la herramienta "Wireshark" que se encuentra instalada en su equipo.

Verifique con la herramienta netstat con la opción –an los puertos abiertos para recibir conexión (listen).

A través de la herramienta de escritorio remoto (mstsc.exe) trate de ingresar a la IP de su compañero (no debería poder ya que no esta abierto el puerto 3389). Vea en wireshark que sucede con este intento.

Agregue un usuario en la computadora llamado admin con contraseña 12345678 y hágalo pertenecer al grupo administradores

En propiedades de mi computadora habilite la opción de escritorio remoto

Verifique la apertura del puerto 3389 a través de "netstat –an"

Realice nuevamente el intento de conexión a través del cliente de escritorio remoto a su compañero, use el usuario y clave creada para tal fin.

Examine los paquetes generados para establecer la comunicación tcp (filtre los paquetes TCP).

Verifique en los primeros 3 paquetes de conexión los siguientes parámetros:Flags, WindowsSize, Seq number, Ack.

Puede usted identificar el número de secuencia real de la conexión TCP y el número de secuencia relativo?

Vaya al menú statistics del wireshark y elija flow graph, luego seleccione TCP Flow.

Cierre la conexión de terminal server desde el cliente y verifique como exactamente es la secuencia de terminación. Documente en un diagrama o esquema el intercambio de segmentos.

Verifique también como se cierra desde el servidor. Hay diferencia para TCP?

Realice la misma prueba (conexión y desconexión) habilitando el servicio Telnet y conectándose usando el cliente Telnet a la IP de su compañero. ¿Es diferente la desconexión en ambas formas (desde el cliente y desde el servidor)?

Laboratorio 2: Visualizando y modificando parámetros de TCP

LAB#5 : Protocolo de Transporte TCP

Conectese al servidor de Archivos \\192.168.1.4 Usuario: samba y Password: 12345678 y descargue e instale el programa Nettools

Instale el servicio de Internet Information Service (IIS)

Abra el editor del registro del sistema Operativo ejecutando regedit y Expanda la subclave siguiente:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

Verifique que parámetros son configurables

Para cambiar el tamaño de la ventana crear un nuevo registro DWORD denominado TcpWindowSize. Asignele el valor de 50 (Bytes) El intervalo válido para el tamaño de ventana es 0-0x3FFFC000 hexadecimal.

Reinicie la PC para tomar los cambios

Conéctese a una carpeta compartida de su compañero y pruebe enviando y recibiendo un archivo y compare la diferencia de tiempo en ambas direcciones. Verifique con Wireshark el tamaño de la ventana en los paquetes TCP

Abra el programa NetTools y elija http flooder. Elija como ip la dirección de su compañero y pruebe la herramienta.

Verifique con netstat –an el número de conexiones concurrente. Cuál es el puerto origen y destino de las conexiones?

Cuestionario

1. Con redes de gran capacidad y una transferencia de datos grande, es posible agotar los números de secuencia. Si se envían datos en una red de 1 gigabits por segundo (Gbps), enviando paquetes de 1460 bytes en cuanto tiempo agotaría los números de secuencia?
2. Busque por cómo haría para que el tamaño de la ventana **tcpwindowssize** pueda crecer hasta 1gb.
3. Investigue en qué consiste el ataque de RST en TCP.
4. ¿Por qué es necesario que cuando se cierra una conexión TCP el extremo que realizó el "Active Close" permanezca en el estado TIME-WAIT por un tiempo igual a 2*MSL?
5. Explique como funciona el synattackprotect y que otros parámetros se puede configurar y para que sirven?
6. Investigue cual es el rango de puertos efímeros en los siguientes Sistemas Operativos:
    a. Microsoft Windows
    b. Linux Kernel 2.6
    c. FreeBSD
    d. OpenBSD

   ¿Coinciden estos puertos efímeros con los propuestos por IANA? ¿Es importante que los puertos efímeros utilizados en conexiones sucesivas sean aleatorios o pueden ser consecutivos o predecibles? ¿Qué ocurre si se eligen puertos efímeros en uso?
7. ¿Es posible que un error no detectado por IP, haga que el Segmento TCP sea entregado a una aplicación que corre en el mismo puerto destino sobre UDP? Explique.
8. Dibuje y siga el diagrama de estado para el cierre de conexión simultanea (es decir iniciada entre ambas partes). También dibuje un diagrama temporal del intercambio de segmentos entre las partes, con los principales campos o flags usados.