

Actividades tema 9

Juan Carlos Navidad García

1.. ¿Cuáles son las principales funciones de la capa de transporte?

- Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino.
- Segmentación de datos y manejo de cada parte.
- Reensamble de segmentos en streams de datos de aplicación.
- Identificación de diferentes aplicaciones.

2.. Explica la diferencia entre aplicación y proceso.

Cada una de las aplicaciones que se encuentran en un dispositivo puede estar ejecutándose o no en un momento dado. Cuando se está ejecutando recibe el nombre de proceso.

3.. En el contexto de la capa de aplicación, ¿qué son los puertos?

Para identificar el proceso de destino se asigna a cada aplicación o proceso un número que le identifica al que llamamos puerto. Los puertos permiten identificar los procesos en cada máquina y, de esta forma, una misma máquina origen podrá establecer enlaces lógicos simultáneos con múltiples procesos de una o más máquinas destino

4.. Haz una tabla comparativa entre UDP y TCP

	UDP	TCP
Características	<p>La PDU del protocolo UDP recibe el nombre de datagrama en lugar de segmento.</p> <p>Multiplexación de envíos entre procesos y/o aplicaciones por encima de un mismo enlace de red.</p> <p>Detección de errores en la transmisión entre extremos para cada datagrama.</p>	<p>Orientado a conexión con conexiones punto a punto.</p> <p>Multiplexación de conexiones entre procesos y/o aplicaciones por encima de un mismo enlace de red.</p> <p>En el host origen, fragmentación de los bloques de datos procedentes de la aplicación.</p> <p>En el host destino, reordenación de los segmentos procedentes de la fragmentación en el origen y reconstrucción de los bloques de datos</p> <p>Detección de errores</p> <p>Entrega fiable</p> <p>Retransmisión automática</p> <p>Eliminación de segmentos que han llegado duplicados</p> <p>Control de flujo y de congestiones</p>
Formato	<p>Puerto origen: número de 16 bits</p> <p>Puerto destino: número de 16 bits</p> <p>Longitud: número de 16 bits</p>	<p>Puertos origen y destino: números de 16 bits</p> <p>Número de secuencia: número de 32 bits</p> <p>Número de reconocimiento: número de 32 bits</p>

	Checksum: número de 16 bits	Longitud de la cabecera: número de 4 bits Campo reservado: 6 bits Indicadores: conjunto de 6 bits
--	-----------------------------	--

7· ¿Cómo podemos averiguar qué puertos están abiertos en nuestro PC? ¿Y en un PC remoto? ¿Existe algún modo de impedir que averigüen qué puertos tenemos abiertos en nuestro PC mediante un escaneo remoto de puertos?

En Windows es tan fácil como en la consola de comandos escribir “netstat -a”

Para saber los puertos abiertos en un pc remoto se utiliza programas como nmap, el cual no tiene interfaz gráfica y zenmap, que este si tiene interfaz gráfica.

Para evitar que se detecten los puertos abiertos en un escaneo remoto de puertos, se pueden instalar firewalls que limiten la respuesta a determinadas IP.

8· Investiga y explica brevemente qué son los ordenadores zombie. ¿Cómo podemos saber si existe alguna conexión establecida mediante alguna aplicación no deseada en nuestro PC?

Un ordenador zombi, también llamado ordenador Bot, es aquel que ha sido infectado por un malware especial, un tipo de troyano que permanece latente, dormido, en el PC. Ese virus está controlado por un ciberdelincuente, a través de Internet. A una orden suya, el troyano se despierta, como un zombi, y comienza a hacer lo que su dueño le dice.

Si dejas el ordenador un rato sin hacer nada y notas que la suspensión no se activa a la hora programada, o que los ventiladores suenan mucho, pero tú no estás haciendo tareas exigentes, es hora de empezar a sospechar.

Merece la pena utilizar el Servicio AntiBotnet que ofrece la Oficina de Seguridad del Internauta (OSI), desarrollado por el Instituto Nacional de Ciberseguridad. Existen bases de datos que almacenan las direcciones IP de ordenadores zombis que han participado en ataques, o forman parte de redes Botnet. El Servicio AntiBotnet chequea si tu dirección IP aparece en una de estas bases de datos, y si es así, es que tu PC es un Bot, o lo ha sido en el pasado.

Otra forma de comprobarlo es con ayuda del Administrador de Tareas de Windows. Reinicia el ordenador para liberar memoria y pulsa las teclas CTRL + ALT + DEL. En el menú que aparece elige Administrador de Tareas. Selecciona la solapa Rendimiento, y pulsa en CPU para que se vea su gráfica de uso. Deja el ordenador sin utilizar un tiempo. Si notas que la gráfica tiene picos grandes sin que tu hagas nada, es que algo está funcionando en segundo plano

10· Investiga y resume en un párrafo qué son los sistemas de detección de intrusos y cómo actúan.

Un sistema de detección de intrusiones (IDS) es un programa de detección de accesos no autorizados a un computador o a una red. El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no solo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento. Normalmente esta herramienta se integra con un firewall. (Wikipedia)

12· Detectamos que una máquina tiene abiertos los puertos TCP 80, 443 y 3306. Investiga a qué aplicaciones se corresponden estos puertos. ¿De qué tipo de servidor crees que se trata?

- El puerto 80 sirve para publicar cualquier servicio web estándar que no sea por protocolo seguro HTTPS.
- El puerto 443 es el predeterminado que utiliza el HTTPS.
- El puerto 3306 es el puerto por defecto usado para el protocolo MySQL. Lo usarás para conectar con clientes de MySQL y utilidades como mysqldump.

15· Hemos instalado un servidor de correo electrónico en nuestra red local y queremos acceder a él desde Internet. ¿Qué deberemos hacer?

Deberíamos de abrir los puertos correspondientes y necesarios para poder usar el cliente-servidor de correo electrónico. Estos puertos son:

- Puerto 25 SMTP
- Puerto 110 NTP
- 143 TCP

16. Indica 3 ejemplos de aplicaciones que usen TCP y otros 3 de UDP.

TCP: Google Chrome, Mozilla Firefox y Edge.

UDP: Cualquier VPN, Facetime y Skype.

2· Lee la ayuda de netstat y averigua la forma de analizar qué puertos se están utilizando en tu PC, tanto para TCP como para UDP, y qué aplicaciones los están utilizando. Una vez hecho esto, investiga si se trata de aplicaciones lícitas o no

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/powershell

PS C:\Users\jcnav> netstat -help

Muestra estadísticas de protocolo y las conexiones de red TCP/IP actuales.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a      Muestra todas las conexiones y los puertos de escucha.
-b      Muestra el archivo ejecutable implicado en la creación de cada conexión o
        puerto de escucha. En algunos casos los archivos ejecutables conocidos hospedan
        varios componentes independientes y, en esos casos, se muestra la
        secuencia de componentes implicados en la creación de la conexión
        o el puerto de escucha. En este caso, el nombre del archivo ejecutable
        está entre corchetes ([]) en la parte inferior; en la parte superior se encuentra el componente al que se llamó,
        y así hasta que se llega al valor de TCP/IP. Ten en cuenta que esta opción
        puede llevar bastante tiempo; además, es posible que se produzca un error si no tienes suficientes
        permisos.
-e      Muestra las estadísticas de Ethernet. Este valor se puede combinar con la
        opción -s.
-f      Muestra los nombres de dominio completos (FQDN) de las direcciones
        externas.
-n      Muestra las direcciones y los números de puerto de forma numérica.
-o      Muestra el id. de cada proceso de propiedad asociado a la conexión.
-p proto Muestra las conexiones del protocolo que especificó el valor proto; este valor proto
        puede ser: TCP, UDP, TCPv6 o UDPv6. Si se usa con la opción -s
        para mostrar las estadísticas de cada protocolo, el valor proto será cualquiera de estos:
        IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
-q      Muestra todas las conexiones, puertos de escucha y puertos
        TCP enlazados que no sean para la escucha. Estos últimos pueden (o no) asociarse
        a una conexión activa.
-r      Muestra la tabla de enrutamiento.
-s      Muestra las estadísticas por protocolo. De forma predeterminada, las estadísticas se muestran
        en función de los valores de IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP y UDPv6;
        la opción -p se puede usar para especificar un subconjunto del valor predeterminado.
-t      Muestra el estado de descarga de la conexión actual.
-x      Muestra conexiones, agentes de escucha y puntos de conexión compartidos de
        Netsh\QoS\direct.
-y      Muestra la plantilla de conexión TCP para todas las conexiones.
        No se puede combinar con otras opciones.
interval Vuelve a mostrar las estadísticas seleccionadas y realiza pausas en intervalos de varios segundos
        entre cada visualización. Presiona CTRL+C para que dejen de mostrarse las
        estadísticas. Si omites esta opción, netstat imprimirá una sola vez
        la información de configuración.

PS C:\Users\jcnav>
```

```
PS C:\Users\jcnay> netstat -b

Conexiones activas

Proto Dirección local Dirección remota Estado
TCP 127.0.0.1:14622 Juanca-PC:49081 ESTABLISHED
[VoiceControlEngine.exe]
TCP 127.0.0.1:49742 Juanca-PC:65001 ESTABLISHED
[nvcontainer.exe]
TCP 127.0.0.1:49744 Juanca-PC:49762 ESTABLISHED
[NVIDIA Web Helper.exe]
TCP 127.0.0.1:49744 Juanca-PC:52478 TIME_WAIT
TCP 127.0.0.1:49744 Juanca-PC:52484 TIME_WAIT
TCP 127.0.0.1:49744 Juanca-PC:52526 TIME_WAIT
TCP 127.0.0.1:49744 Juanca-PC:52531 FIN_WAIT_2
[NVIDIA Web Helper.exe]
TCP 127.0.0.1:49744 Juanca-PC:52532 ESTABLISHED
[NVIDIA Web Helper.exe]
TCP 127.0.0.1:49744 Juanca-PC:52533 ESTABLISHED
[NVIDIA Web Helper.exe]
TCP 127.0.0.1:49762 Juanca-PC:49744 ESTABLISHED
[NVIDIA Share.exe]
TCP 127.0.0.1:49801 Juanca-PC:14622 ESTABLISHED
[LEDKeeper2.exe]
TCP 127.0.0.1:52479 Juanca-PC:49744 TIME_WAIT
TCP 127.0.0.1:52485 Juanca-PC:49744 TIME_WAIT
TCP 127.0.0.1:52527 Juanca-PC:49744 TIME_WAIT
TCP 127.0.0.1:52531 Juanca-PC:49744 CLOSE_WAIT
[NVIDIA Share.exe]
TCP 127.0.0.1:52532 Juanca-PC:49744 ESTABLISHED
[NVIDIA Share.exe]
TCP 127.0.0.1:52533 Juanca-PC:49744 ESTABLISHED
[NVIDIA Share.exe]
TCP 127.0.0.1:55001 Juanca-PC:49742 ESTABLISHED
[nvcontainer.exe]
TCP 192.168.1.95:40675 48.67.251.132:https ESTABLISHED
WpnService
[svchost.exe]
TCP 192.168.1.95:50629 a23-40-114-33:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50630 a23-40-114-33:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50631 a23-40-114-33:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50632 a23-40-114-33:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50634 a2-22-62-91:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50656 a23-210-36-105:https CLOSE_WAIT
[WinStore.App.exe]
TCP 192.168.1.95:50728 48.101.92.2:https ESTABLISHED
```

Todas las aplicaciones que me han salido se podían identificar fácilmente por su nombre, ha habido otras que las he tenido que buscar, pero nada extraño.