Universidad de Chile.
Facultad de Cs. Físicas y Matemáticas.
Departamento de Ingeniería Industrial

Curso: IN3501 - Tecnologías de Información y Comunicaciones para la Gestión.
Profesores: Juan D. Velasquez, Gastón L'Huillier, Víctor Rebolledo
Profesores Auxiliar: Evelyn Andaur, Claudio Millán, Iván Videla
Semestre: Primavera 2009

CONTROL 1

Pauta

1. Pregunta 1

Parte 1. Los servidores DNS se encargan de traducir los nombres de dominio en direcciones IP. Al realizar una petición, ésta se envía al servidor DNS local del sistema operativo. El sistema operativo, antes de establecer comunicación, comprueba si la respuesta se encuentra en la memoria caché. En el caso de que no se encuentre, la petición se enviará a uno o más servidores DNS. Por lo tanto, si se produjera un ataque a los mayores DNS, la petición solicitada por parte del usuario no tendrá respuesta, a menos que la información solicitada se encuentre en el caché[1]. Un caso dramático sería que los servidores DNS no recuperaran la información hackeada, esto traería como consecuencia la utilización de direcciones IP directamente. En todos los casos mencionados, el cliente perderá la confianza en el sitio web y la comunicación se hará cada vez más difícil.

Sin embargo, hay que tener presente que si bien algunos servidores DNS pueden estar caídos, existen segmentos en la Internet que estarán funcionando, pues la información está replicada en un árbol n-ario y muchas veces existe más de una rama para llegar al mismo objetivo.

Parte 2. El paradigma End to End: "La inteligencia está en las puntas" hace referencia a que los datagramas durante el proceso de transporte no sufren ninguna modificación, pues son los nodos (receptores) quienes toman la decisión de qué hacer con éstos. La información enviada desde un emisor debe ser reestructurada sólo en el punto de destino (las decisiones se toman

[1]Si es que éste aún no es actualizado y tiene almacenadas las IPs correspondientes

al final del trayecto). La razón de esto fue liberar los contenidos a través de la red, que en ese entonces gozaba de un ancho de banda limitada.

Actualmente la gran mayoría de los protocolos de transferencia de datos funcionan bajo este principio, sin embargo dado que las IPs son limitadas, se utiliza un mecanismo utilizado por routers llamado NAT, que se encarga de tomar los datagramas que llegan, cambiarles el destinatario y dirigirlos donde corresponda, de esta forma el router quiebra el paradigma end to end.

Otras prácticas que violan el principio son: tecnología de redes VPN (enmascaramiento de IP interviene sobre el datagrama mismo) y las técnicas para combatir el SPAM (el datagrama es abierto para identificar el emisor antes de llegar al receptor). Las razones de su no cumplimiento actual son las necesidades de direcciones IP v4 (son escasas para la cantidad de dominios existentes) y la seguridad en el envío de información.

Parte 3. Algunas razones: · No se modificó su servidor DNS, por lo que NIC no logra encontrar la dirección.
· El Firewall del computador del usuario está bloqueando el servidor del web hosting.
· Al interior de la red del usuario existe algún proxy que este filtrando la página a la que trata de acceder.
· Mala digitación de parámetros en el registro de NIC.
· Corrupción en los archivos de la página web enviados mediante SFTP al servidor de Hosting.

Asignación de puntajes

Parte 1: · Tener conocimiento de lo que son los servidores DNS (1 pto.)
· Efecto del ataque a estos servidores (1 pto.)

Parte 2: · Explicar el paradigma end to end (1 pto.)
· Validez del paradigma actualmente (1 pto.)

Parte 3: · Al menos 2 razones (1 pto. cada una)

2. Pregunta 2

1. Si existe el protocolo HTTP para la transmisión de documentos de hipertexto escritos en HTML ¿Por qué se dice que los protocolos TCP e IP aseguran el funcionamiento de

Internet?

- Distinguir que http y TCP/IP son distintos, saber que es cada uno.

(0,4) Puntos

- Distinguir que Internet es una red que puede transferir mucho mas que solo hipertexto, ejemplo: FTP, NTP, HTTPS, FTPS, entre otros.

(0,3) Puntos

- Explicar como TCP/IP asegura el funcionamiento de INTERNET.

(0,3) Puntos

2. Dentro del encabezado de cualquier datagrama IP hay un campo llamado "Time to Live" ¿A qué se refiere dicho campo y para qué sirve?

- Saber de qué se trata del tiempo de vida del paquete

(0,5) Puntos

- Saber que va a ayudar identificar cuando un paquete se ha perdido y en ese sentido el protocolo TCP-IP mandará un nuevo paquete

(0,3) Puntos

- Su principal función es evitar la saturación de la red con paquetes inservibles, que de otro modo estarían caducados y solo reducen el ancho de banda efectivo de la red.

(0,2) Puntos

3. Explique por qué el protocolo IP no es confiable en el envío de paquetes a través de Internet

- Dar razones porque IP no es confiable en el envió de paquetes a través de internet.

(0,5) Puntos

- Explicar detalladamente porque se produce esto, y de modo mejor, sugerir que de esto surge TCP.

(0,5) Puntos

4. Describa los 3 pasos que son necesarios para establecer una conexión TCP entre dos hosts que desean intercambiar información.

- Descripción del proceso de conexión TCP

(0,4) Puntos

- Diagrama con todos los elementos relevantes (de no haber diagrama, corroborar completitud y entendimiento de cada elemento)(SYN, ACK, Sec X, Sec Y)

(0,6) Puntos

5. ¿Cuál es la utilidad del modelo OSI en el desarrollo de las tecnologías de conexión entre sistemas abiertos?

   - Saber que su principal utilidad es la estandarización en el desarrollo de tecnologías de conexión.

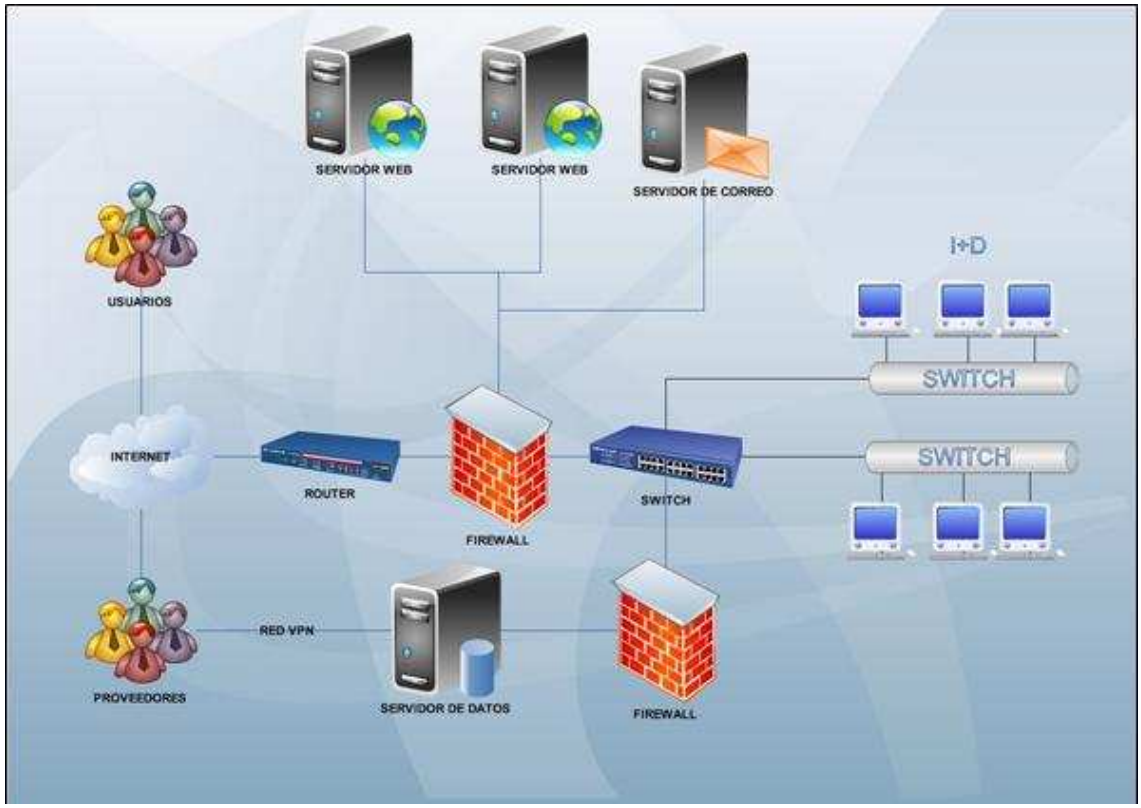
   (0,5) Puntos

   - Ejemplificar dicha estandarización mediante el uso de ciertas tecnologías protocolos en las capas de Enlace, Red y Transporte.

   (0,5) Puntos

3. Pregunta 3

Parte 1:



Consideraciones:

- Cada parte vale 0,3 lo cual tiene un ticket (las áreas y los switch que conectan los pcs son un todo).
- La red VPN tiene 0,1.
- Las áreas tenían que estar aparte, al igual que la base de datos con el servidor web, y en este último era necesario considerar más de uno por la alta cantidad de usuarios (usando DMZ o Balanceador de carga).

Parte 2:

Utilice switch cuando pueda, pero sólo utilice routers cuando deba

Los Switchs permiten conectar múltiples computadores en una red cerrada, son más baratos y tienen una mayor performance que el router. En cambio, el router permite conectar la red a otras redes como internet, actuando como Gateway, tiene mayor "inteligencia" y una mayor capacidad de procesamiento. Entre sus diferencias fundamentales esta que uno opera en la capa 2 del modelo OSI(nivel de MAC) y el otro en la 3(nivel de IP). En conclusión, dependiendo de la función a realizar es la elección a realizar, considerando los costos y el desempeño, aconsejando usar router cuando sea necesario, sino es preferible utilizar switch.

Definiciones según Cisco:

- Los Switches se utilizan para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, un switch puede conectar sus computadoras, impresoras y servidores, creando una red de recursos compartidos. El switch actuaría de controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, los switches permiten ahorrar dinero y aumentar la productividad.
- Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. El router actuará como distribuidor, seleccionado la mejor ruta de desplazamiento de la información para que la reciba rápidamente. www.cisco.com