Evaluación continua 1.1 Sistemas y Redes – Pablo Gagliardi

1. Dibuja los modelos OSI y TCP/IP e indica mediante colores la equivalencia de los niveles de ambos modelos.

Aplicación
Presentación
Sesión
Transporte
Red
Enlace
Física

Aplicación
Transporte
Internet
Acceso a Red

2. Indica los puertos y protocolos de capa de transporte que usan los siguientes protocolos:

Protocolo	Puerto	Protocolo capa Transporte
HTTP	80	TCP
HTTPS	443	TCP
DNS	53	UDP/TCP
SSH	22	TCP

3. Explica y razona cómo realiza la retransmisión de los paquetes el protocolo UDP, cuando no se ha recibido un ACK pasados “5 tics”

UDP a diferencia de TCP no acusa recibido(ACK) ya que no implementa el 3 way handshake.

4. ¿Qué máscara de red (la más ajustada) debería usar si quiero disponer de, al menos, 63 máquinas conectadas a la red?

255.255.255.128/25 permite 126 hosts.

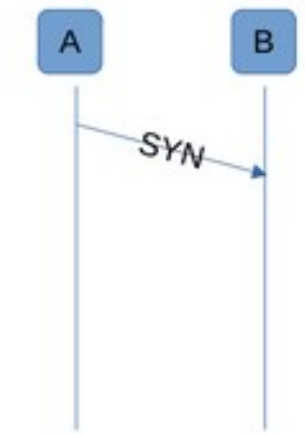
Es la más ajustada al 63 requerido, ya que el máximo inmediato inferior (255.255.255.192/26) admite 64 (se tiene que descontar siempre las direcciones reservadas a broadcast y a la misma red o sub red propiamente dicha y serían 62 maquinas a las que se pueden conectar) .

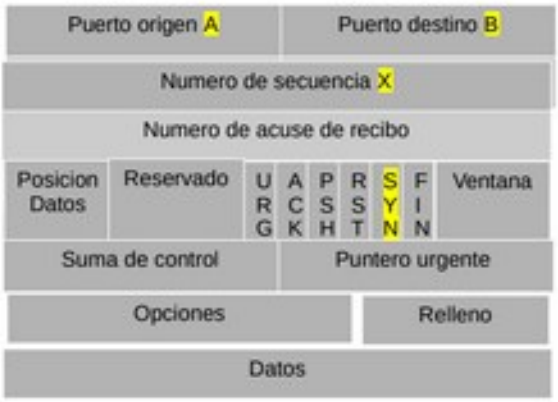
5. Explica detalladamente (y dibuja) como se establece una conexión TCP.
Una conexión TCP se establece en tres pasos:

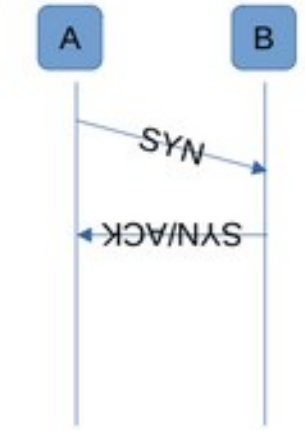
Paso 1: el cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.

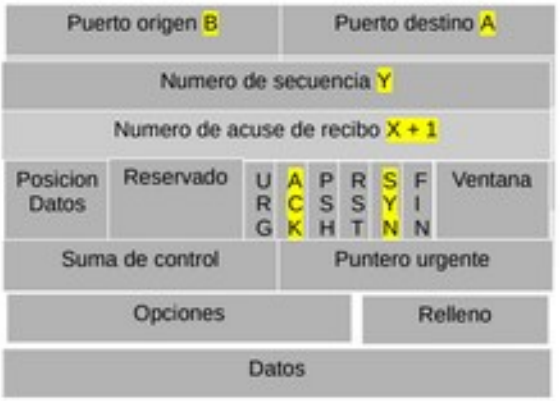
Paso 2: el servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.

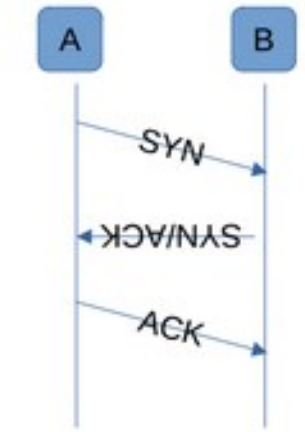
Paso 3: el cliente de origen reconoce la sesión de comunicación de servidor a cliente.

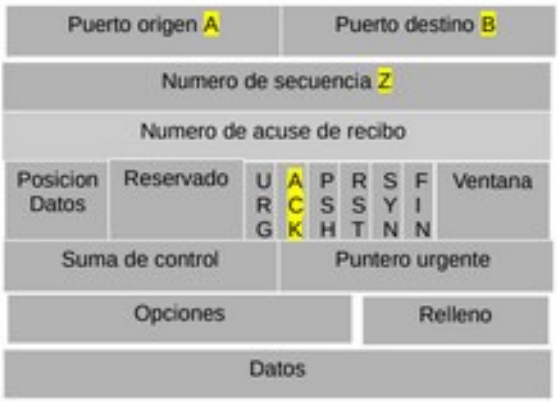












6. Representa la IP 192.168.1.23 con máscara 255.255.192.0 en notación CIDR

192.168.1.23 /18

7. Define, con tus propias palabras, los siguientes conceptos:
a. **SWITCH: Dispositivo encargado de** Acumular los paquetes entrantes en buffers, reenviándolos por los puertos adecuados, gestionando el ancho de banda entre los puertos por los que quiere enviar. Trabaja en el nivel 2.

Los switches tienen la capacidad de aprender y guardar las direcciones de red MAC de las máquinas conectadas directamente a ellos a través de sus puertos.

b.**ROUTER:** Interconectan diferentes subredes trabajando en el nivel de red o capa 3. Los routers son conscientes de su existencia en la red. importante es enviar y encaminar por la ruta más adecuada en el momento datos de una red a otra (pudiendo ser también subredes).

Almacena los paquetes que recibe y procesar los datos de origen y destinatario con los que cuenta. En relación a estos datos envía los paquetes al siguiente router en su camino o al router final, mediante lo que se denomina “encaminamiento”. Cada router en el camino del paquete decide el siguiente salto consultando
su tabla de encaminamiento, generada por protocolos que le permiten decidir cuál es la ruta más corta en ese momento.

c. **Firewall** (Cortafuegos)
Firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red, tanto entrante como saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

d. **NAT** (Network Address Translation)
NAT ofrece una solución al límite ya alcanzado de direcciones IPV4 y consiste en dar sólo una IP pública a cada router NAT responsable de la conexión de una sub-red con Internet. Dicho router es responsable de asignar las direcciones IP privadas a cada dispositivo que se conecte a él. Debiendo ser diferentes dentro de esa sub-red pero siendo indiferente si es igual a una IP perteneciente a otra red diferente. De este modo puede suceder que dos dispositivos, en dos redes diferentes, en distintos puntos del planeta, tengan la misma ip privada. Lo que no puede suceder es que dos routers NAT tengan la misma IP pùblica.

8. Dado el siguiente paquete IP (paquete teórico), indica que direcciones IP y puertos se están comunicando, así como el protocolo de capa 7 que se seguramente se esté empleando. Además, indica cuantos “saltos” dará el paquete antes de descartarse.

IP Origen : 192.168.8.59
IP Destino 2.212.13.165
Puerto origen: 273
Puerto destino: 7
Protocolo de capa 7 : 6 (TCP)
“Saltos” dará el paquete antes de descartarse (TTL): 2

9. Dada la red 192.160.0.0/11, indica y razona:
a. La máscara de red
255.224.0.0 = 11 11111111.111 00000.00000000.00000000

b. El número de host disponibles
2097150
c. La dirección de broadcast
192.191.255.255

d. Calcula si 192.191.13.80 y 192.168.90.45 están en la misma red
Es necesario tener una máscara de red para saber de que clase de red se trata, conocer el tamaño de los segmentos de red y de host, y determinar si pueden verse entre si.

10. Enumera y explica detalladamente (con tus propias palabras) todos los ataques de red que conoces, tanto para IPv4 como para Ipv6

IPV4

Vlan Hopping

VLAN Hopping aprovecha la vulnerabilidad que se da en entornos VLAN, en los que hay una conexión por puertos troncales en los Switch. Realizando este ataque podremos mandar y recibir paquetes desde una VLAN a la que el sistema final no debería poder acceder.El modo de operación consiste en el doble etiquetado, en que la máquina atacante aspira a conseguir acceso a una VLAN en la que no es autorizado mediante el anexo de dos etiquetas en los paquetes que salen del cliente.
Dichas etiquetas se añaden a los paquetes que establecen a qué VLAN corresponden (VLAN ID).

El ataque comienza cuando el atacante envía un paquete conectado a un switch añadiendo dos etiquetas VLAN en la cabecera del paquete. Si el primer atacante está conectado al switch, la primera etiqueta coincide. Si el atacante está conectado a un 802.1Q Trunk, la primera etiqueta coincide con la VLAN nativa (generalmente 1). La segunda etiqueta identifica la VLAN a la que el atacante le gustaría reenviar el paquete.

Cuando el switch recibe el paquete del atacante, elimina la primera etiqueta. A continuación, reenvía el paquete a todos los switches vecinos (ya que también utilizan la misma VLAN nativa). Debido a que la segunda etiqueta nunca se eliminó después de entrar en el primer switch, los siguientes switches que reciben el paquete ven la etiqueta restante como el destino de la VLAN y reenvían el paquete al puerto de destino en esa VLAN.

Man in the Middle

Man in the Middle (MITM) es un conocido sistema de ataque en el que se vulnera un canal entre dos máquinas, y sin que ninguno de los dos extremos sea consciente, la información que se envía entre las dos máquinas puede ser leída o modificada.

ARP Spoofing

En este tipo de ataque el atacante envenena la tabla ARP de la víctima de forma que envía falsos mensajes ARP a dicha víctima. ARP Spoofing no se realiza en redes con hubs, sino en redes switcheadas.El atacante ha conseguido que todos los envíos de información de la máquina VÍCTIMA 1 hacia cualquier destino pasarán por la máquina del atacante. Del mismo modo, la información que envíe la VÍCTIMA 2 (por ejemplo, el router) a la VÍCTIMA 1 también pasarán por la máquina del atacante.

Network Packet Manipulation

La técnica Network Packet Manipulation permite modificar el contenido de un paquete de red. Un atacante que se encuentre en una situación privilegiada, como puede ser en medio de una comunicación, gracias entre otras posibilidades a un ARP Spoofing en una red de área local, puede observar el tráfico que circula a través de él. Además de observar, imagine que puede modificar algún dato de un paquete que circula por la tarjeta de red. En esto se basa la técnica Network Packet Manipulation, por lo que, a priori se necesita realizar un MiTM y poder colocarse en medio de la comunicación.

Ataques a DHCP

Es una variante del ataque MITM que es bastante utilizada y se basa en la implementación de un servidor DHCP falseado. El ataque simple se basa en implementar un servidor DHCP falso en la red, de forma que cuando el cliente envía una trama tipo DISCOVERY, responden con un OFFER tanto el DHCP real como el falso. El clienta atenderá al que antes envíe la respuesta DHCP OFFER.

DHCP ACK injection:

La ventaja de este ataque es que no necesita conocer el rango de direcciones IP válidas ni qué direcciones están libres y cuáles ocupadas. Se deja en manos del servidor DHCP real el que ofrezca toda esa información y sólo se interviene en la fase final, en el reconocimiento que da el servidor sobre la configuración seleccionada. También es más difícil de detectar. Sólo se envía un paquete y puede es enviado con la IP suplantada del servidor DHCP.

Sin embargo, como en el anterior escenario existe la posibilidad de que la respuesta proceda tanto del atacante como del servidor DHCP real y el cliente sólo hará caso al primero de ellos que responda.

Algunas veces será más rápido el servidor DHCP real, otras el atacante.

El atacante no tendrá que tener conocimiento ni de las IP dadas ni de las que pueden ofrecerse, sólo se facilitarán los parámetros necesarios para interceptar por ejemplo los paquetes dirigidos al router o plantear la base para un ataque de DNS Spoofing.

IP Spoofing

La técnica de IP Spoofing permite falsificar la dirección IP origen de un paquete. Generalmente, está muy ligado al protocolo de transporte UDP, ya que dicho protocolo no está orientado a conexión, por lo que el equipo que recibe un paquete por UDP puede contestar directamente sin más. Cuando se trata del protocolo TCP, es más raro ver este tipo de técnicas, ya que, al estar orientado a conexión, no tendría demasiado sentido que se envíe un SYN con dirección IP falsa

DNS Spoofing

DNS Spoofing es un tipo de ataque con el cual, un atacante puede redirigirnos a un sitio web diferente al que nos queremos conectar. se trata de la manipulación de una relación Dominio-IP, resolviendo un cierto nombre DNS con una dirección IP falsa, o al contrario. El atacante consigue este objetivo falseando dicha relación aprovechando una vulnerabilidad del servidor o su confianza hacia servidores poco fiables. Además, dichas entradas son sensibles de envenenar la caché DNS de otro servidor DNS.

IPV6

Envenenamiento de caché

Los ataques de envenenamiento de caché tienen el objetivo de hacer pensar a la víctima que la dirección MAC de un dispositivo es una diferente a la que verdaderamente tiene.La forma en que se utiliza ICMPV6 para esta función se basa en los mensajes que este protocolo envía preguntando por las direcciones MAC.
Los ataques Man In the Middle en IPv6 tienen como fundamento el envío periódico de mensajes “Neighbor Advertisment” con datos falsos, previamente modificados por el atacante. Así, el objetivo es actualizar las tablas caché de las víctimas con información maliciosa o manipulada para que las máquinas envíen la información hacia el atacante o la MAC que ha sido introducida en la tabla.

Ataques SLAAC (StateLess Address Auto Configuration)

El ataque de SLAAC consiste en introducir en una red un sistema malicioso que permita proporcionar la información que un equipo puede requerir de SLAAC. Este deber realizar el enrutamiento del tráfico IPv6 hacia Internet para todos los clientes engañados.

Para conseguir el ataque es necesario inicialmente montar un sistema que se encargará de los encaminamientos falsos. Dicho sistema contará con dos adaptadores de red, uno interno con direccionamiento IPv6 y otro IPv4 para la conexión externa hacia Internet.

Este ataque es también válido para comunicaciones WiFi, lo que hace que pueda ampliarse el alcance de potenciales víctimas.