INGENIERÍA TELEMATICA EXAMEN DE ARS- HW
SEGUNDA CONVOCATORIA. JUNIO 2006
Primera Parte. Teoría. Tiempo: 2 horas
Esta parte debe realizarse sin material de consulta. Puede utilizar una calculadora.

1 Pregunta 1 (3 puntos):

Responda en la hoja adjunta. En cada una de las afirmaciones o preguntas marque la respuesta correcta. Solo debe marcar una respuesta en cada caso; si cree que hay varias respuestas correctas debe elegir la que a su juicio mejor se ajuste a la pregunta. Lea los enunciados con atención.

Forma de puntuación:

Respuesta correcta: 1 punto positivo
Respuesta incorrecta: 1/(n-1) puntos negativos (siendo *n* el número de respuestas posibles)
Ausencia de respuesta: 0 puntos

1.-¿Que función de IPSec debería utilizarse para garantizar que un datagrama enviado a través de Internet no se modifica (excepto el checksum y el TTL)?

A) AH
B) DES
C) ESP
D) ISAKMP

2.-La ventana extendida se utiliza en TCP para:

A) Aumentar la seguridad
B) Reducir el número de segmentos ACK en la red
C) Evitar que se queden conexiones medio abiertas
D) Ninguna de las anteriores

3.-¿Cuantos hosts puede haber (en el mejor de los casos) en la subred 170.16.200.128 con máscara 255.255.255.128?

A) 128
B) 64
C) 127
D) 126

4.-Para poder realizar la comunicación full dúplex en una ethernet se necesita:

A) Que solo haya dos estaciones en la red ethernet
B) Que el medio físico soporte la comunicación full dúplex.
C) Deshabilitar el protocolo de colisiones (CSMA/CD).
D) **Todas las anteriores**.

5.-¿En cual de los siguientes mensajes ICMP se basa el funcionamiento del comando ping?

A) Echo
B) Time Exceded
C) Destination Unreachable
D) Source Quench

6.-Diga cual de las siguientes declaraciones es correcta para una interfaz de un router:

A) ip address 166.166.166.191 255.255.255.192
B) ip address 166.166.166.64 255.255.255.192
C) ip address 166.166.166.64 255.255.255.128
D) Ninguna de las anteriores

7.-¿Que protocolo de routing sería el más adecuado para interconectar los routers de dos proveedores de Internet diferentes?

A) OSPF

B) Rutas estáticas
C) BGP-4
D) EIGRP

8.-Al establecer una conexión TCP los dos primeros segmentos que se intercambian llevan el bit SYN puesto; ¿qué ocurre si el número de secuencia en estos dos segmentos es diferente?:
A) Se cierra la conexión y vuelve a establecerse
B) El intercambio de segmentos se realiza normalmente
C) Se establece la conexión, pero los números de ACK no pueden comrpobarse
D) El número de secuencia en esos dos segmentos nunca puede ser diferente

9.- ¿Cual es el mecanismo que indica a TCP que debe enviar ya los datos que tenga en el buffer, sin esperar mas?:
A) Datos 'pushed'
B) Datos urgentes
C) Envío expeditivo
D) Ventana extendida

10.- Diga cual es la información necesaria y suficiente para especificar completamente una conexión TCP:
A) Direcciones IP de origen y destino, protocolo de transporte, puertos de origen y destino
B) Direcciones IP de origen y destino, puertos de origen y destino
C) Direcciones IP de origen y destino, protocolo de transporte y protocolo de aplicación
D) Direcciones IP de origen y destino, puertos de origen y destino y protocolo de aplicación

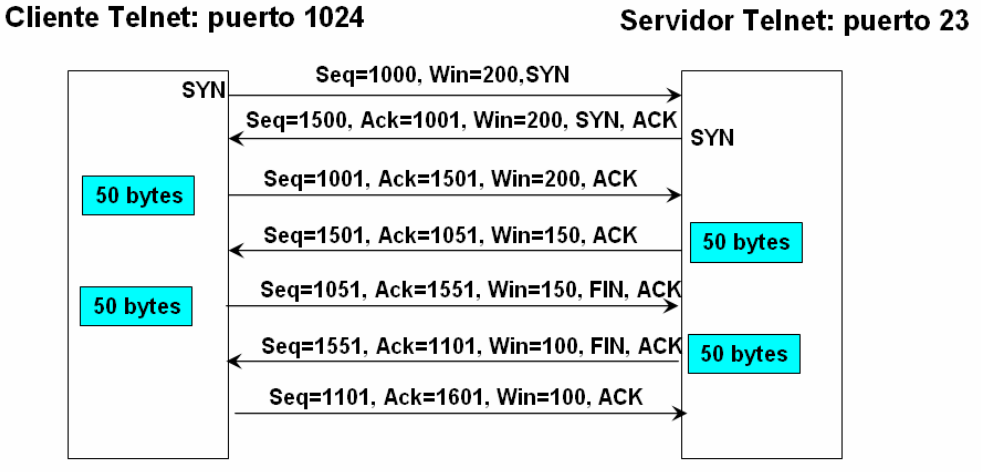
2 Pregunta 1 (3 puntos):

Suponga que tenemos un hub con 3 equipos:

- Equipo Servidor: que actúa como servidor Telnet
- Equipo Cliente: que tiene un cliente Telnet
- Equipo Intruso: un equipo que ha sido comprometido, es decir que alguien ha conseguido introducir aplicaciones que controla remotamente con permisos de administrador.

Se pide:

(2 pto) 1.- Describa una conexión TCP entre el Servidor y el Clinte Telnet (en principio obviamos la información de capa de aplicación), a nivel de segmentos intercambiados e información de los flags activados en cada segmento, cuando en la conexión sólo se intercambian en cada sentido 100 bytes. El MSS se fija en 50 bytes y el campo WIN se fija en 200 bytes. La implementación del TCP no intercambia datos en el establecimiento de la sesión.



(1 pto) 2.- Utilizando el escenario anterior y tomándolo como ejemplo, indique qué paquetes enviaría el intruso para "robar la sesión". Indique la cabecera IP que llevarían dichos segmentos. Explique todo el proceso de forma clara y concisa.

En principio para robar la conexión, debería anticiparse a cualquier paquete de datos enviados por el cliente. En este caso, cuando va a mandar los primero 50 bytes por ejemplo, el intruso mandaría un segmento exactamente igual. Es decir con SEQ 1501, Ack 1051, con IP origen la misma que el cliente y como IP destino la misma que el servidor. Es decir, hace suplantación de IP. En ese momento la contestación del servidor, SEQ 1051, con ACK 1551 al cliente suplantado lo deja fuera de juego, porque él no ha enviado nada. Este paquete es interceptado también por el intruso, que puede seguir mandando información de forma normal..

INGENIERÍA TELEMATICA EXAMEN DE ARS- HW
SEGUNCA CONVOCATORIA. JUNIO 2006
Segunda Parte.Tiempo: 1,5 hora
En esta parte se pueden utilizar apuntes.

Problema 1 (4 puntos):

Una empresa dispone de un router con conexión ADSL y con una IP pública en su interfaz WAN asignada por un ISP y sobre la cual se realiza NAT overload (también conocido como NAT extendido o PAT). La empresa tiene una sede central con 35 ordenadores y 2 delegaciones de 4 ordenadores por delegación, que se conectan con puentes inalámbricos 802.11b con la sede central, utilizando antenas parabólicas.

En la sede central se dispone de un servidor, que ofrece correo a los empleados y alberga la web de la empresa.

Se pide:

1.- (1 pto) Diseño gráfico de la red y asignación de IPs a todos los dispositivos que lo necesiten. Indique la puerta por defecto de los ordenadores. Utilice para la asignación, rangos privados y lo más ajustados a las necesidades.

2.- (2 pto) Indique las listas de acceso para permitir sólo tráfico de entrada al servidor en los servicios ofrecidos y para el resto de ordenadores cuando la conexión se inicia desde el interior. Indique en qué interfaz la configuraría y en qué sentido.

Nota: la sintaxis de las listas de acceso es:

```
permit/deny "origen" "puerto-origen" "destino" "puerto-destino" [established]
```

El modo "**established**" es opcional y deja pasar paquetes IP si son de conexión TCP con los flags de SYN y ACK activos.

3.- (1 pto) El gerente le pide que realice un par de comentarios sobre el tráfico broadcast en la empresa en la configuración actual, pues está tratando de realizar un informe interno sobre el funcionamiento de la red. Adjunte aquí dichos comentarios.

Solución
1.-
Las IP necesarios 35+4+4=41, +1 del router dado que todo será el mismo dominio broadcast, dado que los puentes no aislan dicho tráfico.

La máscara será para 64: 255.255.255.192 o /26 para todos los hosts.

Como sólo utilizamos puentes, las IP son comunes y todos forma la misma subred.
Delegación 1----- sede central ----- Delegación 2

Las conexiones ------ son conexiones punto a punto con los puentes inalámbricos, que conmutan tramas.

El rango utilizado es 10.0.0.0/26
La IP del router 10.0.0.1/26 y para el servidor 10.0.0.2/26

Los hosts tienen IP, independientemente de la ubicación 10.0.0.0/26 y puerta de enlace 10.0.0.1

2.- Las listas de acceso son:

permit origen ANY destino IP_PUBLICA puerto SMTP
permit origen ANY destino IP_PUBLICA puerto WEB
permit origen ANY destino IP_PUBLICA puerto any "established", (es decir que sólo permitirá tráfico si se ha inicializado desde el interior)

LA ACL será colocada en la interfaz WAN de entrada.

3.- el tráfico broadcast tanto de MAC como de IP inundará toda la red, básicamente tráfico ARP. El tráfico unicast cruzará por los enlaces via radio cuando las MAC estén en sedes diferentes. Una trama puede cruzar 2 veces los enlaces radio si la MAC origen destino están en las 2 delegaciones respectivamente.