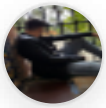


MANSEGROD2
www.wuolah.com/student/MANSEGROD2

Cuestiones TAI resueltas (algunas).pdf

Cuestiones de examenes resueltas

3° Tecnologías Avanzadas de la Información

Grado en Ingeniería Informática - Tecnologías Informáticas

Escuela Técnica Superior de Ingeniería Informática
Universidad de Sevilla

Examen ENERO 2013:

Cuestion 1:
a) Aporta Privacidad mediante técnicas criptográficas ampliamente utilizadas y estudiadas como la clave simétrica y la clave asimetrica. Tambien aporta Integridad, ya que la información intercambiada no puede alterarse. Y por último, Disponibilidad, pues la conexión está disponible cuando se necesita.
b) Hace referencia a VPN en el nivel de red. Es un conjunto de protocolos para asegurar las comunicaciones sobre IP autenticando y/o cifrando los paquetes IP en un flujo de datos para proteger la capa 4 del modelo OSI.
c) Sí quedaría justificada para evitar ataques NAT, y cuando los datos intercambiados son muy valiosos y se precise de mecanismos de autentificación y cifrado de los mismos.

Cuestion 2:
a) Ataques a la confidencialidad: El Objetivo es Obtener información privilegiada.
Ej: Escaneo de puertos o SNIFFING.
b) Ataques a la autenticidad: El Objetivo es Engañar a un sistema víctima haciéndose pasar por alguien de confianza o legítimo.
Ej: SPOOFING , HIJACKING, BACKDOORS, FUERZA BRUTA
c) Ataques a la disponibilidad. : El Objetivo es Inhabilitar el acceso al sistema víctima o a los servicios ofrecidos por éste.
Ej: Denegación de servicio de aplicación: Spam, Bombmail, DDOS . Denegación de servicio de red : Flooding, Smurfing, ...
d Ataques a la integridad: El Objetivo es Modificar o destruir información y/o aplicaciones.
Ej: EXPLOITS , Borrado de huellas

Cuestion 3:
- Un firewall de filtrado de paquetes trabaja en el nivel de red del modelo OSI
- Un Proxy trabaja en el nivel de aplicación del modelo OSI

Cuestion 4:
a) Las Autoridades de Certificación evitan la suplantación. Con su firma certifica que alguien es quien dice ser. Por tanto son una entidad de confianza responsable de emitir y revocar los certificados digitales mediante firmas de clave pública.
b) Una clave (pública o privada) es una firma electrónica aplicada a un contenido, mientras que un certificado digital es un archivo firmado electrónicamente por una
Autoridad de Certificación que vincula la firma del firmante y su identidad.
c) *HTTPS es un protocolo que se encarga de transferir información entre el cliente y el servidor de forma cifrada, Los datos que se transmiten desde el cliente al servidor están a su vez cifrados con su propio protocolo, el primer protocolo creado con este propósito fue SSL. Para cifrar los datos, los sitios requieren un certificado, también llamado firma digital, que confirma que el mecanismo de cifrado es de confianza y cumple con el protocolo)
*SSL (Secure Sockets Layer) es un protocolo que proporciona seguridad en la transferencia de contenido cifrado como el del certificado digital, así como el intercambio de claves.

Cuestion 5:
1. Retraso. Los paquetes pueden llevarse mucho tiempo en colas saturadas de routers o bien tomar rutas menos directas. Componentes: Propagación, Conmutación, Procesado y Transmisión.
2. Jitter. Fluctuación o variación en el tiempo de entrega de dos paquetes consecutivos. Caracteriza la variación del retraso de la red.
3. Velocidad. Capacidad del ancho de banda (velocidad o caudal de datos) que refleja la capa 2 (nivel de enlace del modelo OSI).

Cuestion 6:
- El tamaño de cola de los enrutadores

Cuestion 7:
- Aplicaciones de video bajo demanda

Cuestion 8:
(El notable crecimiento de Internet ha originado un importante crecimiento del tráfico. Este hecho ha

incitado a los expertos a buscar soluciones para controlar y gestionar este tráfico. Una de las soluciones adoptadas serían los servicios integrados (INTERSERV), que de todas las soluciones propuestas para resolver esta problemática, podría considerarse como la más drástica debido a que sugiere modificaciones en todos los equipos que conforman la red de redes y reserva los recursos para una garantía estricta, en cambio los servicios Diferenciados (DIFFSERV) ,Las aplicaciones que lo solicitan reciben una QoS garantizada con alta probabilidad, dotando a internet de la posibilidad de manejar diferentes tipos de tráfico, esto requiere menos complejidad.)

*DiffServ es una arquitectura alternativa a la reserva de recursos (ancho de banda) de InterServ, que posibilita manejar diferentes clases de tráfico sin cambiar la configuración actual de las capas de red y de transporte.

*DiffServ Simplifica la complejidad de InterServ.

*DiffServ no requiere del protocolo RSVP como sí lo requiere InterServ.

*DiffServ utiliza el campo TOS.

Cuestion 9:

a) CFQ = 1
WFQ = x

quatums A = 3mbps |
quatums B = 1mbps |--- ()- 10mbps (3/(3+1+1)) * 10mbps = 6mbps
quatums C = 1mbps |

NBytes / 6mbps < 50ms --> (N * 8) bits / (6 * 10e6) bits < (50 * 10e-3) s

b) Tiempo que tarda en vaciarse la cola. Las otras colas no tienen el tamaño definido, ni se preguntaba por ellas.

Cuestion 10:

Cubetas = Algoritmo diferente. Permite acumular datos a los quatums hasta 3 ciclos maximo.

Problemas: el router debe dar servicio a todas las rafagas al mismo tiempo, es decir, si la suma de todas ellas son 30KiB, la qsize del router debe ser 30KiB y no menos como en se aprecia en la imagen

Examen FEBRERO 2013:

Cuestion 1:

(Ambos elementos están encargados de proteger una red, como diferencias cabe destacar que el Firewall es a nivel de red y el proxy a nivel de aplicación)

Similitudes :

1.Protegen de las intrusiones, ya que sólo los elementos autorizados entran en la red.

2.Protegen la información privada.

3.Optimizan los recursos, ya que identifican los elementos de la red interna y permite que la comunicación sea más directa.

Diferencias :

1.El firewall no puede proteger la red interna de un ataque procedente de dicha red, mientras que el proxy sí puede.

2.El firewall trabaja a nivel de red, mientras que el proxy trabaja a nivel de aplicación.

Cuestion 2:

Escanear un puerto consiste en analizar por medio de un programa el estado de un puerto de una máquina conectada a una red, detectando si está abierto, cerrado o protegido por un firewall. Si una máquina tiene un puerto abierto entonces se puede establecer una comunicación con ella a través de dicho puerto.

Cuestion 3:

- Protege de ataques procedentes de la red exterior

Cuestion 4:

(NO SE VA A PREGUNTAR PORQUE NO LO HEMOS DADO)

Cuestion 5:
Un túnel de red es un canal de comunicación para encapsular un protocolo dentro de otro.Ha sido utilizado para cifrar el contenido del paquete original y encapsularlo en un nuevo paquete que sólo tiene "visible" el destino y origen del mismo. Por lo que este nuevo paquete se podrá capturar pero no descifrar.

Cuestion 6:
En el cifrado simétrico, tanto emisor como receptor, utiliza la misma clave tanto para cifrar como para descifrar, mientras que en el cifrado asimétrico, cada parte tiene dos claves, una privada para descifrar y otra pública, que es la que comparte, para cifrar.
El cifrado simétrico tiene una gran velocidad de ejecución, mientras que el cifrado asimétrico es lento y muy costoso.
Si se obtiene la clave utilizada en un tráfico VPN utilizando cifrado simétrico se podrán cifrar y descifrar toda la información, mientras que con el cifrado asimétrico, se requiere obtener la clave privada, que no se entrega, para poder descifrar la información, por lo que garantiza la seguridad y confidencialidad de la información circulante.

Cuestion 7:
Jitter es la fluctuación o variación en el tiempo de entrega de dos paquetes consecutivos. Caracteriza la variación del retraso de la red. Se puede establecer dos tipos de medidas: Variación en el tiempo de propagación terminal-terminal y Variación respecto al mínimo retraso.

Cuestion 8:
VOIP -> Retraso (menos de 400 ms no afecta) y las fluctuaciones.
Video bajo demanda -> Velocidad (Caudal de datos)
IPTV -> Retraso y la velocidad (Caudal de datos)
Aplicaciones interactivas -> Retraso (menos de 150 ms no afecta), fluctuaciones (afecta medio), Velocidad de datos, pérdida de paquetes.

Cuestion 9:

Cuestion 10:

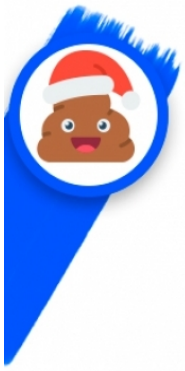
Examen SEPTIEMBRE 2013:

Cuestion 1:
(Igual que la cuestion 1 de FEBRERO 2013)

Cuestion 4:
a) Túnel de red: Canal de comunicación que permite encapsular un protocolo dentro de otro protocolo. Los datos, que se cifran antes de enviarse por el túnel (lo que produce una sobrecarga en el tráfico) sólo tienen "visibles" el origen y destino de los mismos.
b) Cifrado simétrico: Todos los equipos (emisores y receptores) utilizan la misma y única clave que han acordado previamente, tanto para cifrar como para descifrar la información. Es un proceso mucho más ligero que el asimétrico.
c) Cifrado asimétrico: Cada una de las partes en la conexión tiene dos claves relacionadas, una privada que no se comparte, con la que se descifra la información, y otra pública que es la que se comparte, para cifrar la información.
d) IPSec: Es un conjunto de protocolos para asegurar las comunicaciones sobre IP autentificando y/o cifrando los paquetes IP en un flujo de datos para proteger la capa 4 del modelo OSI.

Examen ENERO 2018:

Cuestion 1:
a) Un secuestro de sesión en un navegador Web se considera un ataque: Autenticidad
b) Realizar IP spoofing en una red local se considera un ataque: Autenticidad
c) Realizar DNS spoofing a un equipo informático se considera: Autenticidad
d) Saturar una red local con paquetes UDP se considera un ataque: Disponibilidad



e) Enviar peticiones masivas HTTP desde una botnet contra un servidor WEB se considera un ataque: Disponibilidad
f) Usar un exploit contra un navegador Web vulnerable se considera un ataque: Integridad

Cuestion 2:
a) Puede traducirse como "hacerse pasar por otro". El objetivo de esta técnica es actuar en nombre de otros usuarios para que, una vez conseguido el engaño, realizar otro tipo de acciones maliciosas. Una forma común de spoofing es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, realizar acciones en nombre de él.
b) *IP Spoofing: Se busca usurpar la dirección IP de una máquina que permita al atacante ocultar el origen de su ataque
*DNS Spoofing: Este ataque se consigue mediante la manipulación de paquetes UDP para comprometer el servidor DNS.
*Web Spoofing: el atacante crea un sitio web completo, falso y similar al que la víctima desea entrar.
*ARP Spoofing: redirecciona el tráfico de una, o varias máquinas de la red hacia la del atacante. El atacante falsifica los paquetes ARP proporcionando su MAC en relación a la IP suplantada.
c) IP Spoofing: Usurpación de una dirección IP (debe estar en la misma red local).
ARP Spoofing: El atacante falsifica los paquetes ARP proporcionando su MAC en relación a la IP suplantada.

Cuestion 3:
- Dual-Homed gateway.
Un host dual-homed (o gateway dual-homed) es un sistema equipado con dos interfaces de red (NIC) que se encuentra entre una red no confiable (como Internet) y una red confiable (como una red corporativa) para proporcionar seguridad acceso. Dual-homed es un término general para proxies, gateways, firewalls o cualquier servidor que proporcione aplicaciones o servicios seguros directamente a una red que no sea de confianza.

Cuestion 5:
- En los procesos de autenticación con contraseña.
- En el proceso de firma electrónica.
- En los certificados digitales usados con el protocolo SSL.

Cuestion 6:
a) Para garantizar y demostrar seguridad y que uno es quien dice ser.
b) En la operación de algunos sistemas criptográficos, usualmente los de infraestructura de clave pública (PKI), una CRL es una lista de certificados (más concretamente sus números de serie) que han sido revocados, ya no son válidos y en los que no debe confiar ningún usuario del sistema. El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.
c) La clave privada de la autoridad.
Medidas -> Desconectar la red y habitaciones cerradas.

Cuestion 7:
- Para verificar una firma electrónica es necesaria la clave privada del firmante.
- Los datos cifrados con la clave pública sólo se pueden descifrar con la clave privada.

Cuestion 9:
b) Retraso -> VOIP y IPTV
Jitter -> VoIP y Juegos en red en R.T.
Ancho de banda -> Juegos Online y aplicaciones interactivas

PREGUNTAS SUELTAS:

Indique las métricas QoS estudiadas que más afectan a las siguientes aplicaciones concretas:
a) Skype -> Pérdida de paquete y ancho de banda
b) Mario Karts on line -> Ancho de banda
c) Netflix -> Pérdida de paquete
d) Mensajería con WhatsApp -> Jitter
e) Twitter ->

f) Gmail -> Pérdida de paquete
g) Dropbox -> Ancho de banda
h) SSH ->