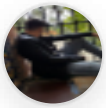


MANSEGROD2
www.wuolah.com/student/MANSEGROD2

Cuestiones TAI.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

Cuestiones TAI

Enero de 2013

Cuestión 1.

- Referente a las VPN

(a) Comente brevemente que aporta una VPN en el ámbito de la seguridad informática.

(Ocultan el contenido del tráfico para evitar que los individuos no autorizados o malintencionados lo descubran)

Una red VPN aporta: Privacidad, ya que sólo los equipos autorizados pueden conectarse a ella; integridad, ya que la información intercambiada no puede alterarse; y disponibilidad, pues la conexión está disponible cuando se necesita.

(b) El término IPSec hace referencia a …

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) Justifique si tiene sentido o no el uso de una VPN en una red local de una pequeña oficina

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.

Cuestión 2.

- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo como sigue:

Describa brevemente cada uno de ellos y ponga un ejemplo de este tipo de ataques:

(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, …

Escribe en la bola de cristal tu nota.
Menciónanos y se cumple.
Somos ...

Wuolah Wuolah Wuolah_apuntes

WUOLAH

(d) Ataques a la integridad. : El **Objetivo** es Modificar o destruir información y/o aplicaciones.Ej: EXPLOITS , Borrado de huellas

Cuestión 3.

- Marque las afirmaciones correctas:

F Un Firewall de filtrado de paquetes trabaja en el nivel de aplicación del modelo OSI.
V Un Firewall de filtrado de paquetes trabaja en el nivel de red del modelo OSI.
V Un Proxy trabaja en el nivel de aplicación del modelo OSI.
F Un Proxy trabaja en el nivel de red del modelo OSI.

Cuestión 4.

- Referente a la las infraestructuras de clave pública PKI responda a las siguientes cuestiones:

(a) ¿Para qué sirven la autoridades de certificación en una infraestructura PKI?

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) ¿Cuál es la diferencia entre una clave pública o privada, y un certificado digital?

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) ¿Qué relación tiene el protocolo SSL con un certificado digital?

(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.

Cuestión 5.

- Enumere y describa brevemente al menos 3 métricas usadas habitualmente en la calidad de servicio para redes IP.

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).

Cuestión 6.

- En el ámbito de QoS tratado en la asignatura, en el jitter influye:

V El tamaño de cola de los enrutadores.
F La velocidad del enlace.
F El retraso de transmisión.

Cuestión 7.

- En el ámbito de QoS tratado en la asignatura, el uso de un buffer mejora la calidad de servicio de los siguientes tipos de aplicaciones IP:

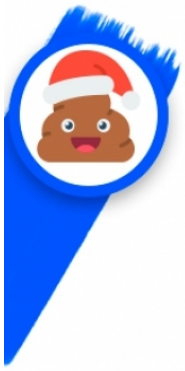
F Aplicaciones dedicadas a VOIP.
V Aplicaciones de vídeo bajo demanda.
F Juegos interactivos.
F Servidores de contenidos Web.

Cuestión 8.

- Indique los principales motivos por los que DIFFSERV ha tenido mayor aceptación que INTERSERV

(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.



Febrero de 2013

Cuestión 1.

- Describa brevemente las similitudes y las diferencias entre un Proxy y un Firewall.

(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.

Cuestión 2.

- En las clases de problemas de la asignatura se realizaron escaneos de puertos utilizando la herramienta NMAP, describa brevemente en qué consiste un escaneo de puertos.

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.

Cuestión 3.

- Señale las afirmaciones correctas:

F Un Firewall protegen de los ataques realizados proveniente de la red interna.
F Un Firewall protege de ataques de ingeniería social.
F Un Firewall protege de virus informáticos.
V Protege de ataques procedentes de la red exterior.

Cuestión 4.

- Describa brevemente la diferencia entre un Proxy HTTP directo y un Proxy HTTP inverso

Proxy HTTP Directo: Gateway genérico del navegador cliente que permite ocultar el direccionamiento de la red interna. Además, actúa en nombre del solicitante (consumidor del servicio), y permite establecer reglas de acceso a la web desde el perímetro de seguridad.

Proxy HTTP Inverso: Permite al usuario de Internet acceder indirectamente a determinados servidores internos. Actúa en el back-end de los servidores cliente centralizando los servicios ofrecidos en un único punto. Además, puede redireccionar http y https para que se pueda acceder a las páginas en formato URL.

Cuestión 5.

- Describa brevemente en qué consiste un túnel de red en el ámbito de la asignatura y para qué ha sido utilizado.

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.

Cuestión 6.

- Indique las principales diferencias entre el cifrado simétrico y el asimétrico

>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.

Cuestión 7.

- ¿En qué consiste el Jitter? Proponga y defina alguna forma de medirlo.

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.

Cuestión 8.

- Para cada tipo de aplicación, indique cual es la métrica, de las estudiadas en la asignatura, que más afecta a la calidad de dicho servicio:

(a) VOIP: Retraso (menos de 400 ms no afecta) y las fluctuaciones.
(b) Vídeo bajo demanda: Velocidad (Caudal de datos)
(c) IPTV: Retraso y la velocidad (Caudal de datos)
(d) Aplicaciones interactivas: Retraso (menos de 150 ms no afecta) fluctuaciones (afecta medio), Velocidad de datos, pérdida de paquetes,

Septiembre de 2013

Cuestión 1.

- Describa brevemente las similitudes y las diferencias entre un Proxy y un Firewall.

(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 de 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.

Cuestión 4.

- En la asignatura se ha dedicado un tema al estudio de las VPNs. En él se mostraban diferentes tecnologías usadas. Describa brevemente en qué consiste cada una de las siguientes e indique qué relación tiene con una VPN:

(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.

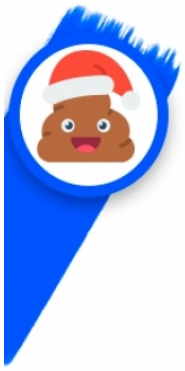
(d) IPSec→Es un conjunto de protocolos para asegurar las comunicaciones sobre IP autentificando y/o cifrando los paquetes IP en un flujo de datos para proteger la capa 4 del modelo OSI.

Enero de 2018

Cuestión 1.

- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo. Para cada ejemplo mostrado a continuación, indique en qué categoría se puede considerar:

(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**



Cuestión 2.

- Referente a los ataques informáticos:

(a) Indique en qué consiste el Spoofing.

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) Describa cada uno de estos ataques: IP Spoofing, DNS spoofing, Web Spoofing, ARP Spoofing.

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) Indique cuáles de los ataques del apartado sólo se pueden realizar en una red local.

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.

Cuestión 3.

- En las prácticas de laboratorio se ha creado una red de 3 equipos, uno de ellos con un firewall, indique a qué tipo de configuración de las estudiadas corresponde:

□ Dual-Homed gateway. X
□ Screened host.
□ DMZ Screened Subnet.

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.

¿Cuál es el cometido de las autoridades de certificación en la infraestructura PKI?
Son sistemas de criptografía basados en el intercambio de claves públicas y privadas.

Cuestión 5.

- En el ámbito de la seguridad informática las funciones HASH se utilizan:

V□ En los procesos de autenticación con contraseña.
□ Para cifrar datos en una comunicación de red.
V□ En el proceso de firma electrónica.
V□ En los certificados digitales usados con el protocolo SSL.

Cuestión 6.

- Las infraestructuras PKI estudiadas durante el curso usan autoridades de certificación para firmar las claves públicas de terceros: (1.5 puntos)

(a) ¿Cuál es el objetivo de firmar las claves públicas de terceros?
Para garantizar y demostrar seguridad y que uno es quien dice ser.

(b) ¿Para qué sirven los listados de revocación de certificados (CRLs) en una infraestructura PKI?
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) ¿Cuál es el eslabón más débil de dicha infraestructura y que medidas adicionales se suelen tomar para aumentar la seguridad de dicho eslabón?
La clave privada de la autoridad.
Medidas→ desconectar la red y habitaciones cerradas.

Cuestión 7.

- Respecto al cifrado asimétrico, certificados digitales y PKIs, indique las afirmaciones que son correctas:

V□ Para verificar una firma electrónica es necesaria la clave privada del firmante.
F□ Los datos cifrados con la clave privada sólo se pueden descifrar con la clave pública.
V□ Los datos cifrados con la clave pública sólo se pueden descifrar con la clave privada.
F□ El cifrado simétrico es más lento que el cifrado asimétrico.
F□ El cifrado simétrico es más seguro que el cifrado asimétrico.
F□ En multitud de protocolos, como por ejemplo IPSec, el cifrado asimétrico solo se usa para intercambiar claves simétricas, y después, se cifran los datos sólo con claves simétricas.

Cuestión 8.

- Describa brevemente en qué consiste un túnel de red en el ámbito de la asignatura y para qué ha sido utilizado

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.

Cuestión 9.

- En el ámbito de QoS tratado en la asignatura:

(a) Describa brevemente 3 métricas de las estudiadas en la asignatura.

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)

(b) Para cada métrica del apartado (b) indique 2 aplicaciones cuya calidad de servicio se ve afectada fuertemente por dicha métrica.

Retraso→ VOIP y IPTV
Jitter→ VoIP y Juegos en red en R.T.
Ancho de banda→ Juegos Online y aplicaciones interactivas

Cuestión 7.

- 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 →

Cuestión 1.

- En el ámbito de la asignatura se ha optado por clasificar los ataques en función del objetivo, indique cuál es la clasificación propuesta y ponga un ejemplo de cada tipo de ataque.

(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

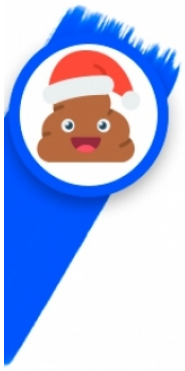
(c) Ataques a la disponibilidad. : El **Objetivo** es Inhabilitar el acceso al sistema víctima o a los servicios ofrecidos por éste. Ej: Denegación de servicio de aplicación: Spam, Bombmail, DDOS .Denegación de servicio de red: Flooding, Smurfing, …

(d) Ataques a la integridad. : El **Objetivo** es Modificar o destruir información y/o aplicaciones.Ej: EXPLOITS , Borrado de huellas

Cuestión 2.

- La ingeniería social es el origen de la mayoría de los ataques informáticos. Describa brevemente en qué consiste e indique cuál es la única contramedida efectiva.

El término ingeniería social es equivalente a engañar o mentir para conseguir que la persona atacada haga cosas que la parte atacante quiere que haga. Es difícil de parar, al menos técnicamente, pues no usa métodos informáticos. Va a uno de los eslabones más débiles de la cadena de la seguridad: el factor humano. La única contramedida efectiva es aplicar el sentido común.



Cuestión 3.

- Señale las afirmaciones correctas:

F□ Un firewall de filtrado de paquetes protege de los ataques provenientes de la red interna.
F□ Un proxy protege de ataques de ingeniería social.
F□ Un firewall de filtrado de paquetes opera con menos recursos que un proxy.
V□ Un proxy se puede utilizar para realizar operaciones de filtrado en el nivel de aplicación.
F□ Un firewall de filtrado de paquetes trabaja a nivel de aplicación.
V□ Un firewall de filtrado de paquetes trabaja a nivel de red.

Cuestión 4.

-En el ámbito de la seguridad informática las funciones HASH se utilizan:

V□ En los procesos de autenticación con contraseña.
F□ Para cifrar datos en una comunicación de red.
V□ En el proceso de firma electrónica.
V□ En los certificados digitales usados con el protocolo SSL

Cuestión 4.

-En los routers actuales existe una opción de configuración llamada DMZ que hace referencia a DeMilitarized Zone. Comente brevemente en qué consiste y cuál es el efecto cuando se activa.

En esta zona suelen situarse los servicios públicos. Su objetivo es separar los servidores que sirven aplicaciones visibles desde redes externas, de aquellos servidores internos.
Sirve sobre todo para evitar problemas existentes para ejecutar programas o acceder a determinados servicios desde el exterior que se encuentran en el dispositivo que se encuentra bajo la regla DMZ. Sin embargo, implica que cualquier persona pueda realizar un rastreo como escanear los puertos abiertos para detectar vulnerabilidades en los servicios que se están utilizando.