Guía de repaso - Segundo Parcial

Estas preguntas son orientadoras en la lectura de los temas trabajados en la materia y deben utilizarse como una ayuda al momento de estudiar, de ninguna manera constituyen una selección estricta de los temas que serán evaluados. Los temas evaluados son los trabajados hasta la clase anterior al parcial junto con la bibliografía recomendada en cada uno de esos temas.

Sobre Spaning Tree Protocol (STP)

1. ¿Cuál es el propósito del Spanning Tree Protocol en redes de área local conmutadas? ¿Qué inconveniente/s resuelve?
2. Describa la operatoria del protocolo mediante una serie de pasos, incluyendo la selección del conmutador raíz, la determinación del costo de los caminos, la determinación de puertos raíz, puertos designados y, finalmente, puertos bloqueados. Mencione, además, cómo se resuelven los casos de equivalencia de costos.
3. Describa el formato de las PDU utilizadas por el protocolo. ¿A qué dirección multicast se remiten las tramas que encapsulan BPDUs?
4. ¿Cómo se determina el costo de cada enlace? ¿Qué valores se han definido en los estándares?
5. Con respecto a STP, ¿en qué estados puede estar cada puerto de un switch?
6. ¿Cuándo se puede afirmar que STP ha convergido en una red conmutada?

Sobre VLAN

7. ¿Qué ventajas presenta utilizar VLAN para separar la interconexión de red entre equipos de la misma organización frente a realizar esta misma separación por ruteo tradicional (separando las redes a nivel de capa 3)?
8. ¿Cuál es la norma que define el protocolo para las redes Ethernet? ¿Qué campos agrega a la trama ethernet el estandar 802.1q ?
9. Respecto a VLAN, ¿cuáles son los distintos modos de operación que pueden configurarse para un puerto de un switch? ¿cuál es la principal diferencia de cada uno?
10. ¿En qué escenario puede resultar útil que un host genere y reciba tramas etiquetadas?
11. ¿Es posible apilar etiquetas de vlan?

Sobre VOIP

11. ¿Cuáles son los dos principales tipos de protocolos que intervienen en el contexto de una comunicación VoIP? ¿Cuántos protocolos de VoIP intervienen en un escenario de SIP y RTP?
12. ¿Cuáles protocolos no relacionados a VoIP intervienen en una comunicación VoIP?
13. ¿Qué otros protocolos de señalización existen además de SIP?
14. ¿Cuál es el intercambio típico de mensajes SIP y RTP que se produce en a tríada UAC-UAS-UAC?
15. ¿Cuál es el escenario típico y qué intercambios de mensaje se producen al encender un teléfono IP conectado una red?
16. ¿Qué características de red son las que más perjudican una comunicación VoIP?
17. ¿Qué es un CODEC? ¿Cuáles son los más habituales en una comunicación VoIP?
18. ¿Qué es un PBX? ¿Existe solamente en el contexto de la comunicación VoIP o existía ya en el contexto de las comunicaciones telefónicas tradicionales?

Sobre Seguridad en Redes de Datos

20. ¿Cuáles son los servicios de seguridad definidos por la recomendación ITU-T X.800?
21. Según el modelo OSI ¿Cuáles son los tres elementos de la arquitectura de la seguridad?
22. ¿Qué mecanismos de seguridad se encuentran definidos en la recomendación X.800 y en que consisten?
23. A grandes rasgos, ¿cuáles son las principales políticas de seguridad (de filtrado de tráfico) que pueden adoptarse?
24. ¿Cuáles son los dispositivos o roles que se pueden definir para proveer mecanismos de seguridad de red y cuáles son sus funciones?
25. ¿Cuáles son los principales tipos de firewall y qué diferencias caracteriza a cada uno de ellos?
26. ¿En qué consiste el concepto de “Seguridad como un Servicio” (Security as a Service)?
27. Los algoritmos de cifrado pueden diferenciarse según tres características, donde cada clasificación los separa a su vez en dos tipos diferentes ¿cuáles son esas características? ¿cómo se clasifican según cada una de ellas?
28. ¿Cuáles son los elementos de la arquitectura de un sistema de cifrado simétrico?
29. ¿Qué ventajas y desventajas tienen los algoritmos de cifrado simétricos vs los algoritmos asimétricos?
30. ¿Por qué no se recomienda la seguridad por oscuridad?
31. ¿Cuáles son los dos tipos de ataques se pueden pueden realizar a un algoritmo de cifrado?
32. ¿Qué mecanismos existen para asegurar la integridad de los datos?
33. ¿Qué define la RFC 4880?
34. Si decimos que un usuario ha firmado electrónica o digitalmente un mensaje de correo electrónico, ¿qué procedimientos y qué algoritmos se han aplicado sobre el mensaje? ¿cuál es el resultado final? ¿qué servicios de seguridad se proveen?
35. ¿Qué procedimiento o procedimientos aplica el destinatario del mensaje para determinar si el mensaje sufrió alteraciones luego de su envío?

Sobre VPN

1. ¿En qué niveles de la capa OSI es posible aplicar servicios de seguridad? ¿qué tecnologías o protocolos permiten hacerlo?
2. ¿Qué es una VPN? ¿Qué problema soluciona?
3. ¿Cuales son los escenarios más usuales de utilización de una VPN?
4. ¿Qué es un RAS?
5. ¿Qué servicios de seguridad provee una VPN?

Sobre IPSec

1. ¿En qué capa del modelo OSI opera IPSec?
2. ¿Qué diferencia hay entre el protocolo AH y ESP en IPSec?
3. ¿Cuáles son los dos modos en los que es posible utilizar IPSec?
4. ¿Se puede utilizar IPSec para configurar una VPN?
5. ¿Qué es una Base de datos de Asociaciones de Seguridad?

Sobre Certificados X.509

32. ¿En qué consiste un certificado X.509?

33. ¿Por qué son necesarias las Autoridades de Certificación (CA)? ¿Cómo distribuyen sus claves públicas a todos los usuarios?
34. ¿Existe alguna diferencia tecnológica entre un certificado autofirmado y un certificado firmado por una CA?
35. Nombre al menos cuatro causas por las que un certificado puede ser inválido en el contexto de HTTPS.
36. ¿Cómo establece SSL la conexión segura entre un navegador en el equipo de un cliente y un servidor web que implementa HTTPS?
37. Los certificados X.509, ¿se utilizan en otro contexto más allá de SSL?

Sobre TLS

1. ¿Qué es una sesión en el contexto de TLS y SSL?
2. ¿Qué (sub)protocolos engloba el estándar TLS? ¿qué objetivo tiene cada uno de ellos?
3. ¿Cuál es la mínima cantidad de claves que se utilizan en una conexión SSL? ¿De qué tipo (sim/asim) es cada una de ellas?
4. ¿Por qué motivo se utilizan claves simétricas en una conexión SSL?
5. ¿Cuál es la secuencia de mensajes que se intercambian al establecer una sesión TLS entre dos entidades?
6. Dado el escenario en el que el host A y el host B se están comunicando a través de TLS y existen varias sesiones en simultaneo entre ambos hosts. ¿Por qué si una de estas sesiones se ve comprometidas el resto de las sesiones entre A y B pueden considerarse seguras?
7. ¿Qué es un MAC? ¿Y un HMAC? ¿Qué los diferencia?
8. ¿Por qué es necesario negociar los algoritmos de cifrado?
9. ¿Por qué se utilizan claves simétricas en una conexión TLS?

Sobre SSH

1. Nombre al menos dos usos habituales de SSH.
2. ¿Cuáles protocolos se encuentran definidos por SSH?
3. ¿Qué métodos de autenticación soporta SSH?

Sobre virtualización

1. ¿Cuáles son las ventajas y desventajas que provee la virtualización?
2. ¿Qué tipos de virtualización existen?
3. ¿Qué es una instrucción privilegida?
4. ¿Cuáles son las propiedades de las máquinas virtuales definidas por Popek y Goldberg?
5. ¿Qué técnicas pueden utilizarse para implementar virtualización a nivel de plataforma o sistema?
6. ¿Qué es un Hipervisor? ¿Qué funciones tiene?
7. ¿Que diferencias existen entre una máquina virtual y un container (contenedor)?

Sobre Infraestructura de datacenters

1. ¿Qué aspectos deben contemplarse para diseñar un datacenter?
2. ¿Qué es significa que un datacenter sea “Tier II”?
3. ¿De qué manera se puede aumentar la disponibilidad de un datacenter?

Sobre SDN

1. ¿En qué planos se pueden dividir los procesos que tienen lugar en un dispositivo de red?
2. ¿A qué se hace referencia cuando se habla de Software-Defined Networks?
3. ¿Qué ventajas y desventajas tiene SDN?
4. ¿Cuál es la arquitectura básica de SDN según la recomendación de la ITU Y.3300?
5. ¿Qué es OpenFlow? ¿Sobre qué protocolos se apoya OpenFlow para brindar servicios de seguridad?