ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

REDES DE COMPUTADORES

SEGUNDA EVALUACIÓN - II TÉRMINO 2014

Nombre: _____ ***Matrícula:*** _____

Sección A

1. Explique en qué consiste el mecanismo *network address translation* (NAT). Describa la estructura de la tabla de traducción para cada una de las estrategias de traducción. Señale las limitaciones en cada caso. ***[12%]***
2. Describa el proceso de mapeo de direcciones por medio de DHCP ***[8%]***
3. Compare y contraste los protocolos IMAP 4 y POP 3. ***[5%]***
4. Con respecto al servicio que proveen los protocolos *Transmission Control Protocol* (TCP) y *User Datagram Protocol* (UDP):
    a. ¿Cuál es la diferencia en el servicio ofrecido a aplicaciones por los protocolos TCP y UDP? ***[4%]***
    b. Para cada una de las siguientes aplicaciones determine si usted usaría TCP o UDP y explique las razones para su selección. ***[8%]***
        i. Transferencia de archivos
        ii. Ver un video transmitido en tiempo real
        iii. Navegar por la Web
        iv. Una conversación telefónica de voz sobre IP (VoIP)
    c. Tanto TCP como UDP proveen números de puerto. ¿Para qué se usan estos números de puerto? ***[4%]***
    d. Un usuario desea establecer una conexión desde su laptop hacia un servidor por medio del Internet usando el protocolo TCP. Considerando los mensajes que TCP genera, explique ¿cómo se establece un circuito virtual entre la laptop y el servidor usando TCP? ***[4%]***

Sección B

5. Confidencialidad, integridad y autenticación son tres características de comunicaciones seguras. Un sistema de red podría estar sujeto a amenazas a estas características por atacantes que explotan vulnerabilidades en el sistema de red. A fin de prevenir estos ataques nosotros implementamos controles sobre los servicios de seguridad.

    Asuma que dos comunicadores, Alice y Bob, nunca se han conocido antes, ellos no confían entre sí y que Alice y Bob pueden usar cualquier sistema criptográfico y funciones de hash criptográficas. Ahora, Alice quiere enviar un mensaje largo a Bob. Conteste las siguientes preguntas (en su protocolo de diseño, usted debe indicar claramente cualquier asunción que realice y las operaciones desarrolladas por cada uno de los comunicadores).

    a. Diseñe un protocolo en el cual Alice pueda enviar este mensaje a Bob y solo Bob pueda desencriptar el mensaje y los procesos de encriptación/desencriptación sean los más eficientes. ***[6%]***
    b. Diseñe un protocolo mediante el cual Alice pueda enviar un mensaje a cualquiera, y cualquiera que reciba el mensaje pueda estar seguro que el mensaje no es un *replay* de un mensaje previamente enviado y si es en verdad de Alice. ***[6%]***
    c. Diseñe un protocolo en el que Alice pueda enviar un mensaje a Bob. El diseño del protocolo debe satisfacer los siguientes requerimientos: confidencialidad del mensaje, autenticación del origen, integridad y frescura estén protegidos durante la transmisión, el protocolo es el más eficiente en términos de costos de comunicación y Bob es menos vulnerable a ataques DoS (Denial of Service). En

MSc. Carlos Mera Gómez

su diseño, usted debe justificar claramente cómo satisface cada requerimiento de diseño especificado. ***[8%]***

6. Considere dos IDSs (*Intrusion Detection Systems*) A y B para aplicaciones Web que analizan como eventos a requerimientos entrantes tales como URLs, parámetros de consulta y sus valores. El IDS A es un *misuse-based* con las siguiente configuración: ***[15%]***
   a. Si el valor del parámetro es igual a "../../" entonces alertar
   b. Si el valor del parámetro es igual a "OR 1=1" entonces alertar

   El IDS B es un *anomaly-based* con la siguiente configuración:

   a. Normalmente, el nombre del parámetro es uno de los siguientes: "page", "lang", "action"
   b. Normalmente, la longitud del valor del parámetro es < 1000
   c. Normalmente, la frecuencia de '.' en el valor del parámetro es 0
   d. Si los requerimientos entrantes son significativamente diferentes, entonces alertar.

   En base a esta información complete la siguiente tabla:

Requerimiento	**Tipo**	**Alerta**	
		Misuse-based IDS	**Anomaly-based IDS**
/view?page=balance			
/view?page=../../etc/passwd			
/view?lang=aa[10K bytes]a			
/view?id=1			
/view?lang=OR 1=1			

   Tipo: Benigno o Maligno
   Misuse-based IDS/Anomaly IDS: Sí o No

7. Suponga que un algoritmo de *distance vector* correrá y convergerá hasta obtener una solución estable en red de la figura. Describa paso a paso, la forma en que la información de ruteo es propagada entre los diferentes nodos. Prepara las tablas de ruteo de todos los cinco nodos. ***[20%]***