Seguridad en Sistemas - 2do parcial 2013

Ejercicio 1
Cual de las siguientes técnicas previenen que un virus sea detectado por antivirus
. Polimorfismo
. Compresión
. Metamorfismo
. Cifrado

Ejercicio 2
Marcar respuesta correcta

a) Fortalezas que presenta un firewall ubicado en el perimetro de una red.
- Permite controlar tráfico entrante desde equipos externos y puede proteger frente a diversos ataques provenientes del exterior.
- Establecer y actualizar politicas debido a su ubicación central.
- Proteger de algunos tipos de ataque de negación de servicio provenientes del exterior.

b) Debilidades que presenta un firewall ubicado en el perimetro de una red.
- Ausencia de protección contra programs o usuarios maliciosos internos.
- No provee protección para equipos móviles mientras se conectan a otras redes.
- Sin protección si se infecta los equipos portatiles durante un viaje y luego se propaga infección cuando se vuelven a conectar a la red interna.

Ejercicio 3
Dada la siguiente definición: Acción destinada a impedir que un sistema de información (o red de computadoras) brinde los servicios para los cuales fue diseñado e implementado.
a) Tipo de ataque que caracteriza?
b) Describa en que consiste y que mecanismos son utilizado para lograr el objetivo.

Ejercicio 4
Marcar respuesta correcta
a) Capa OSI en la cual aplicar seguridad para evitar ataque man in the middle.
. Aplicación
. Session
. Red

b) Tecnología para atraer atacantes.
. Intrussión Attraction System
. IDS
. Honeypot

c) capa Osi que maneja cifrado.
. Aplicación.
. Session.
. Presentación.
. Red.

Ejercicio 5
. Politica por defecto aplicada.
. A que tabla pertenecen.
. Describir brevemente objetivo de c/regla.
. Existe alguna regla redundante?
<secuencia de instrucciones de configuración de host con enlace eth1 (externo) eth2(interno) iptables>

Ejercicio 6
. Politica por defecto aplicada.
. A que tabla pertenecen.

. Describir brevemente objetivo de c/regla.
<secuencia de instrucciones de configuración de iptables para nat>

Ejercicio 7
a) Tipo de protocolo que es Kerberos.
b) Describirlo brevemente.

Ejercicio 8
a) Qué es tunel SSH?
b) Dar ejemplo concreto de su utilización para alcanzar servidor interno desde el exterior. Graficar.
c) Mencionar otra tecnología que use el mismo concepto. Ejemplificar. [VPN]

Ejercicio 9
a) Sería necesario incorporar cifrado para alcanzar privacidad en la transmisión hasta el servicio que se ejecuta en el servidor interno propieamente dicho? Por qué? Cite servicio.
b) En qué capa de red se ubica el protocolo adecuado para llevar a cabo la solución al inciso anterior ¿De qué protocolo hablamos?

Ejercicio 10
Como mantener integridad en una base de datos:
. Trabajar con transacciones las cuales deban cumplir 2 requisitos: operaciones atomicas y correctas. Además de producirse algún incidente mientras se realiza una transacción debería tener métodos para recuperar el estado anterior. A su vez controlar transacciones concurrentes.
. Debemos controlar que los usuarios no autorizados no puedan conseguir el archivo en el que se encuentra la bd mediante firewall.
. Hay que controlar los accesos indebidos con fin de modificar la bd. Limitar los privilegios en usuarios. Utilizar <..no me entiendo la letra.> limitando privilegios a grupos de usuarios.

Ejercicio 11
V o F
. El término "seguridad a través de oscurecimiento" hace referencia a una práctica para ocultar la contraseña del usuario cuando este la recibe, así nadie más puede verlo por pantalla.
. Al utilizar matrices para el control de acceso se puede representar cualquier cosa que se representa a través de listas de control de acceso (ACL).
. Los firewalls pueden ser utilizados para bloquear todo ataque de denegació de servicio mientras permiten al mismo tiempo que se establezcan todas las comunicaciones autorizadas.
. Juan quiere protegerser de los rootkits, así que ejecuta una máquina virtual con windows XP en un linux ¿Juan es vulnerable a los ataques existente para windows XP?
. La inferencia es una forma de deducir o derivar datos relevantes a partir de datos sensibles.
. La implementación de seguridad multinivle en BD es una tarea fácil por la baja granularidad de los items que se deben controlar.
. Inyección de código se puede producir al utilizar consultas SQL y lenguaje script.
. El contenido de una página no puede modificarse mediante ataque a server DNS.