==========
---------- 2do Parcial de Seguridad - 2012 ----------
==========
(traducción del pdf, pasa que me costaba entender la letra manuscrita :P)

Ejercicio 1 - Enuncie que tipos de firewall describen c/u de las sig definiciones:
a) Controla el intercambio de paquetes verificando direcciones, puertos o protocolos en los mismos utilizando condiciones.
b) Controla los accessos inspeccionando y manteniendo información de estado de c/conexión, permitiendo llevar un control de secuencia de los paquetes que se inspeccionan y verifica condiciones sobre los mismos.
c) Controla las comunicaciones a nivel de la capa de aplicación del modelo OSI, adaptandoes a cada protocolo de la misma.

Ejercicio 2 - Marque cuales de las siguientes técnicas previenen que un virus sea detectado por un antivirus?
. Polimorfismo
. Compresión
. Metamorfosis
. Encriptación

Ejercicio 3 - A qué hace referencia backdoor y cual es la diferencia con respecto a los troyanos.

Ejercicio 4 - 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 utilizado para lograr el objetivo.

Ejercicio 5 - Explique
a) Reflexión
b) Amplificación

Ejercicio 6 - Los sistemas de autenticación usualmente verifican las contraseñas con la ayuda de firmas digitales almacenadas en archivos protegidos.
a) Próposito de almacenar las firmas de las contraseñas en vez de las contraseñas en si mismas?
b) Por qué hay que proteger los archivos que contienen dichas firmas?
c) Próposito de incorporar valores (salts) en el cómputo de una firma para una contraseña?

Ejercicio 7 - A partir de que tipos de redes se pueden efectuar los siquientes ataques? Qué característica principal poseen estas redes?
. Ataque distriubuido de denegación de servicio.
. Envío masivo de correo electronico.
. Fraude.
. Computación paralela y distribuida.

Ejercicio 8 - Un administrador de infraestrucura instala un IDS que genera alarmas cada vez que se produce una intrusión.
a) Mencionar un ataque típico que puede ser detenido por un IDS.
b) Los siquientes son dos métodos que permiten decidir si una acción pede ser clasificada como una intrusión, explique en 2 renglones en que consiste c/u de ellos.
I. detección de una anomalia.
II. Detección por firmas.

Ejercicio 9 - Describa 3 métodos que puedan ser utilizados para la autenticación de usuarios.

Ejercicio 10 - Verdadero o falso:

. 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 sensibles a partir de datos sensibles. <¿sensibles X 2?>

. La implementación de seguridad multinivle en BD es una tarea fácil por la baja granularidad de los items que se deben controlar.