Grupo 10	EJEMPTO Examen parcial Seguridad Informática	2016-QP
Nombre:	Apellidos:	DNI:

Tiempo de respuesta estimado: **30** minutos. Las preguntas son multi-respuesta.
Cada respuesta **cierta** marcada con **C o falsa marcada con F** vale **0,125 puntos**.
Cada respuesta marcada incorrectamente descuenta **0,1 puntos**

OS Sec

1. Cada línea del archivo etc/passwd de linux contiene:
   a. Una contraseña cifrada
   b. La fecha de caducidad de la contraseña
   c. El identificador de usuario
   d. El identificador de grupo
2. La implantación del sistema de control de acceso lock-key:
   a. Combina las listas de control de acceso con las listas de capacidades
   b. Cada objeto tiene una única identidad (patrón de bits: lock)
   c. Cada dominio tiene una única identidad (patrón de bits: key)
   d. Toda la información lock-key se almacena en una table global
3. El principio del mínimo privilegio tiene los siguientes objetivos:
   a. Impedir la conmutación (switching) de dominios
   b. Limitar el riesgo de daños causados por un programa malicioso o erróneo
   c. Minimizar los derechos requeridos por un usuario para realizar sus tareas
   d. Simplificar la implantación del Sistema de control de acceso.
4. Para acreditar la identidad de un usuario y darle acceso a un Servicio podemos usar:
   a. Una contraseña desechable
   b. Un identificador de usuario
   c. Un identificador biométrico
   d. Un token emitido por un servidor de identidad (tipo SSO, OpenID)

Malware

5. Cuáles de las siguientes afirmaciones sobre código malicioso son ciertas:
   a. En general los gusanos tienen un período de incubación o latencia más corto que los troyanos
   b. Tanto los virus como los gusanos se ocultan dentro de otros programas, para pasar inadvertidos
   c. Los troyanos siempre se propagan (replican) de forma automática
   d. Los programas espía siempre se propagan de forma automática
6. Los antivirus utilizan las firmas de malware para:
   a. Detectar mutaciones en virus
   b. Identificar virus conocidos
   c. Detectar nuevos virus
   d. Crear de reglas para el analizador basado en firmas
   e. Analizar el sistema periódicamente
7. Cuál de las siguientes afirmaciones es cierta:
   a. Los sanbox no penalizan el rendimiento del Sistema
   b. Los sandbox no se usan en combinación con sistemas AV basados en firmas
   c. AV basados en ponderaciones y AV basados en firmas son incompatibles
   d. Las variables de entorno no son importantes para detectar un virus

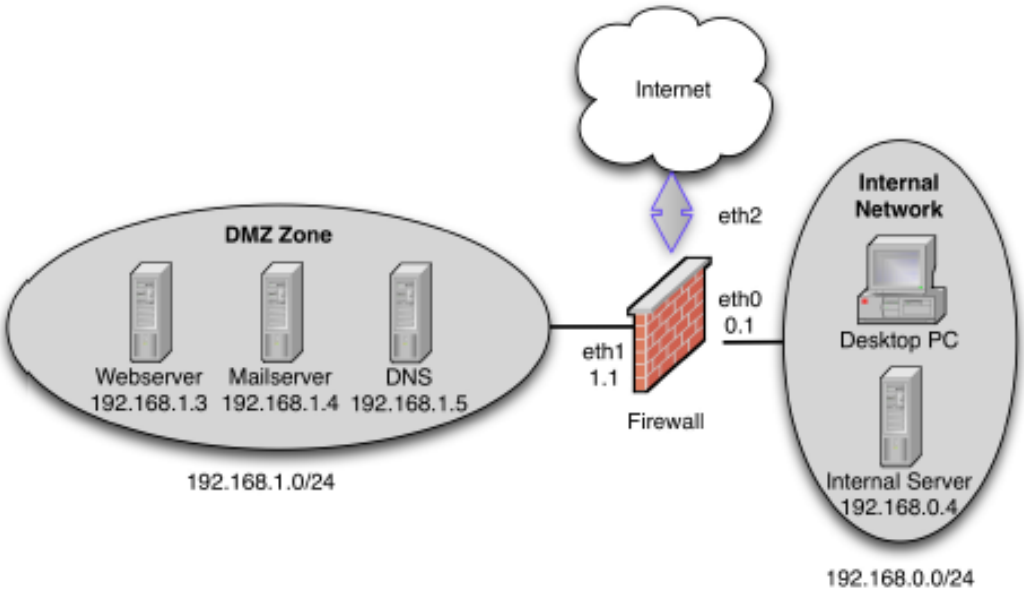
8. Cuáles de las siguientes afirmaciones son ciertas:
   a. Un worm necesita un programa host para ejecutarse
   b. Un virus necesita un programa host para replicarse
   c. Los worms no tienen capacidad para reproducirse
   d. Cada vez que se ejecuta un virus, éste ejecuta su código malicioso

Grupo 10	**1er Examen parcial Seguridad Informática**	**2015-QT**
Nombre:	Apellidos:	DNI:

IP Sec

9. IPSec usa criptografía de clave pública para ...
   a. Cifrar la carga útil de los paquetes transmitidos a través de la VPN
   b. Compartir una clave secreta durante el establecimiento de un canal seguro, cuando IKE S.A. es negociado
   c. Autenticar los paquetes si AH está activado
   d. Ninguna de las anteriores
10. ¿Cuál de los siguientes usos de VPN son correctos?
   a. Arquitectura Gateway-to-Gateway para usuarios remotos
   b. Arquitectura Host-to-Host para tareas de administración de sistemas
   c. Arquitectura Host-to-Gateway para establecer conexiones seguras entre las redes de un campus
   d. Arquitectura Gateway-to-Gateway para establecer conexiones seguras entre las redes de un campus

11. La empresa de lampisteria “YahPoo, Inc.” Dispone de la ssiguiente arquitectura de red, y os han contratado para mejorar las políticas de seguridad dentro de su Firewall iptables.



iptables –t filter –A FORWARD –i eth0 -o eth1 –p TCP –dport ssh –j ACCEPT
iptables –t filter –A FORWARD –o eth0 -i eth1 –m state -sport ssh --state established –j ACCEPT
Que hacen estas reglas? Asumir política por defecto DROP

- Permitir el acceso desde la red interna a los servidores de la DMZ usando el protocolo ssh
- Permitir el acceso desde la DMZ al servidor de la red interna usando el protocolo ssh
- Permitir el acceso desde la DMZ todos los ordenadores de la red interna usando el protocolo ssh
- Permitir el acceso desde la red Internet a los servidores de la DMZ usando el protocolo ssh