SEGURIDADES DE SOFTWARE

"Como estudiante de ESPOL me comprometo a combatir la mediocridad y a actuar con honestidad; por eso no copio ni dejo copiar" **----------** **Firma de compromiso del estudiante**	**_ _ _** **20**

Estudiante: _ **MARZO 9 del 2015**

EXAMEN FINAL

TEMA 1

Escoger la(s) opción(es) correcta(s): (5 puntos)

1. El tipo de virus que se oculta en memoria RAM permanentemente. Así, puede controlar todas las operaciones llevadas a cabo por el sistema operativo, infectando los programas que se ejecute, es :
    a) Virus mutante
    b) Virus sobre escritura
    c) Virus residente
    d) Virus macros

2. Cuál o cuáles de las siguientes son políticas de seguridad del DMZ:
    a) Tráfico de la red externa hacia la red interna prohibida
    b) Tráfico de la DMZ hacia la red interna prohibida
    c) Tráfico de la DMZ desde la red interna prohibida
    d) Ninguna de las anteriores

3. Comandos de IPTABLES:
    a) -A, append
    b) I, insert
    c) N, net

d) F, flat

4. Cifrado Asimétrico:
   a) 1 sola clave
   b) 2 claves diferentes
   c) 2 claves diferentes y una firma electrónica
   d) 1 clave y una firma electrónica

5. DNS spoofing:
   a) Altera las direcciones IP del servidor WEB
   b) Altera las direcciones MAC del servidor WEB
   c) Altera las direcciones IP del servidor DNS
   d) Altera las direcciones MAC del servidor WEB

TEMA 2 (5 puntos)

Coloque el numeral correspondiente de acuerdo a los niveles de certificados:

Niveles de certificados
Nivel 1
Nivel 2
Nivel 3
Nivel 4
Nivel 5

Niveles	Certificados de Seguridad
	Cifrado-autenticado (SSL)
	Autenticar (Certificado Digital)
	Autenticar (Usuario y Password)
	Firma Digital (doc., pdf., gif., jpg., tiff.)
	Autenticar (Llave privada almacenada en un Token)

SEGURIDADES DE SOFTWARE

TEMA 2 (10 PUNTOS)

Realizar la siguiente configuración en IPTABLES:

1. Borrar las reglas previas.
2. Definimos que la política por defecto sea aceptar.
3. Bloquear una IP atacante (192.168.1.34) - Servidor
4. Bloquear el trafico saliente al dominio de Twiter - Cliente
5. Bloquear el puerto 80 - servidor
6. Aceptamos enviar y recibir correos - Cliente
7. Aceptamos paquetes entrantes de cualquier dirección IP de origen que pertenezca a la red 172.90.0.0/24, a través de la interfaz eth0
8. Bloquear ping - cliente
9. Denegar acceso a kerberos - Servidor
10. Bloqueamos los servicios FTP para el servidor