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: _ **FEBRERO 17 del 2014**

EXAMEN FINAL

TEMA 1

Escoger la(s) opción(es) correcta(s): (10 puntos)

1. El momento en el que el usuario se da a conocer en el sistema :
   a) Identificación.
   b) Autenticación.
   c) Control de acceso físico
   d) Escaneo

2. Verificación que realiza el sistema para validar quien está ingresando:
   a) Identificación
   b) Autenticación
   c) Control de acceso físico
   d) Escaneo

3. Red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida:
   a) Adware
   b) Backdoors
   c) Botnet
   d) Hoax

SEGURIDADES DE SOFTWARE

4. 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

5. Los tipos de filtrados que existen a niveles de capas del modelo OSI son:
    a) Listas de accesos
    b) Software
    c) Pasarela
    d) Anti virus

6. Cuál o cuales 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

7. Los tipos de NAT que existen son:
    a) Iterativa
    b) Dinámica
    c) Estático
    d) Ninguna de las anteriores

8. Alguno de los comandos de IPTABLES son:
    a) -A, append
    b) I, insert
    c) N, net
    d) F, flat

9. El Sniffer puede examinar información importante tales como:
    a) Headers
    b) Username and Password
    c) Firma electrónica
    d) Ninguna de las anteriores

10. Cual es el estándar que contemplan los certificados digitales:
    a) MD5
    b) X.509
    c) PKCS
    d) OCS**P**

TEMA 2 (10 PUNTOS)

Realizar la siguiente configuración en IPTABLES:

1. Mostrar el estado del Firewall y reglas de configuraciones que actualmente tiene el firewall
2. Bloquear el trafico entrante.
3. Bloquear una IP atacante (192.168.1.34)
4. Bloquear el trafico saliente al dominio de facebook
5. Anadir log
6. Denegar el tráfico para la mac 00:0F:EA:91:04:07
7. Bloquear peticiones de PING
8. Permitir acceso al servidor de archivo de SAMBA
9. Permitir acceso al servidor Proxy
10. Permitir DNS SERVER