Seguridad en Redes

Curso 19/20 :: Cuestionario Topología Seguras

Escuela Superior de Informática

2020/01/13 17:05:03

Este examen consta de 10 preguntas con un total de 40 puntos. Tres preguntas incorrectas restan un punto. Sólo una opción es correcta a menos que se indique algo distinto. No está permitido el uso de calculadora. La duración máxima de este examen será de 15 minutos.

Apellidos: SOLUCIÓN Nombre: _____ Grupo: _____

1 [4p] ¿Cuál de las siguientes sería una definición plausible del concepto «topología segura»?

- ☐ **a)** La que permite acceder a todos los dispositivos conectados mediante protocolos confiables.
- ■ **b)** Aquella que divide la red en distintas zonas y facilita una estrategia de defensa y contramedida ante ataques internos o externos.
- ☐ **c)** La que interpone un *firewall* perimetral que implementa la política de seguridad de toda la organización.
- ☐ **d)** Aquella que utiliza protocolos de cifrado en todas las comunicaciones con el exterior de la organización.

2 [4p] ¿A qué se refiere el concepto *three-legged firewall*?

- ☐ **a)** Es una topología segura que define 3 redes seguras internas: DMZ, MZ, servidores comunes
- ☐ **b)** Se refiere a los tres niveles de seguridad que se implementan en la estrategia *security in depth*: externo, interno y privado.
- ■ **c)** Hace referencia a las tres interfaces del router que conecta la red pública, la DMZ y la MZ.
- ☐ **d)** Es un firewall que detecta paquetes en los nivel enlace, red y transporte.

3 [4p] ¿Qué tipo de direcciones son más adecuadas para los computadores de la DMZ?

- ■ **a)** Estáticas
- ☐ **b)** Dinámicas
- ☐ **c)** Del bloque 10.0.0.0/8
- ☐ **d)** IP versión 4

4 [4p] ¿Cuál NO ES una razón para disponer de un servidor DNS como `dnsmasq` en la red interna de la organización?

- ☐ **a)** Es más seguro.
- ☐ **b)** Es más rápido.
- ☐ **c)** Permite definir nombres privados.
- ■ **d)** Evita que los hosts externos tengan que resolver nombres.

5 [4p] ¿Con cuál de los siguientes tiene más similitud la funcionalidad SNAT?

- ☐ **a)** DNAT
- ☐ **b)** NAPT
- ☐ **c)** NAT transversal
- ■ **d)** IP Masquerade

6 [4p] ¿Qué configuración debe tener necesariamente un router que funcione sobre un computador con GNU/Linux?

- ■ **a)** `echo 1 >/proc/sys/net/ipv4/ip_forward`
- ☐ **b)** `iptables -A INPUT -p ICMP -j ACCEPT`
- ☐ **c)** `iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`
- ☐ **d)** `Cualquier computador con GNU/Linux se comporta como router.`

7 [4p] ¿Por qué para manejar el tráfico externo no deseado se aconseja utilizar DROP, pero para el interno se aconseja REJECT?

- ☐ **a)** Se hace por convenio.
- ■ **b)** Evita ofrecer información al atacante.
- ☐ **c)** Es más eficiente porque no es necesario emitir tráfico adicional.
- ☐ **d)** Es una decisión del administrador de la red, sin relevancia real para la seguridad.

8 [4p] ¿Qué funcionalidad se configura en la cadena PREROUTING de netfilter?

- ☐ **a)** NAT/NAPT
- ☐ **b)** NAT transversal
- ■ **c)** Redirección de puertos
- ☐ **d)** Servidores en el propio router

9 [4p] ¿Por qué es netfilter un sistema cortafuegos de tipo *statefull*?

- ☐ **a**) Puede analizar cabeceras del nivel de red y transporte.
- ☐ **b**) Ofrece un sistema de *logging* configurable.
- ■ **c**) Puede hacer seguimiento de conexiones.
- ☐ **d**) Ofrece compatibilidad con versiones anteriores de `iptables`.

10 [4p] ¿Qué comando permite al tráfico HTTP externo entrar en la red corporativa?

- ☐ **a**) -A INPUT -p tcp –dport 80 -j ACCEPT
- ☐ **b**) -A OUTPUT -p tcp –dport 80 -j ACCEPT
- ■ **c**) -A FORWARD -p tcp –dport 80 -j ACCEPT
- ☐ **d**) -A OUTPUT -p tcp –dport 80 -j DROP