Redes (Parcial 2) – 15 Xuño 2009

Departamento de Tecnoloxías da Información e as Comunicacións
Facultade de Informática da Coruña

D.N.I.: _____ **Titulación:** Enxeñería Informática

Apelidos: _____ **Nome:** _____

- ***SÓ SE EVALUARÁN AS RESPOSTAS SINALADAS NA TÁBOA DE RESPOSTAS***.
- *En cada pregunta existe* ***unha soa*** *resposta válida que puntúa* ***+0.66***.
- *As respostas incorrectas* ***-0,2*** *e as non contestadas non puntúan.*
- *A duración máxima do examen será de* ***30 minutos***

Pregunta	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		16	17
Resposta																		

1 Cal das seguintes afirmacións non é correcta.
a) En CHAP o usuario/cliente non precisa ningún tipo de contrasinal ou clave secreta.
b) A autenticación mediante PAP non é adecuada cando a liña de comunicacións non é segura.
c) CHAP require do intercambio de tres mensaxes entre cliente e autenticador.
d) En CHAP é o autenticador (servidor) quen envía o desafío.

2 En Kerberos o Ticket Granting Server (TGS) non precisa almacenar a clave pública do usuario, por que?
a) A afirmación é incorrecta, o TGS si precisa almacenar a clave pública do usuario.
b) Porque o TGT previamente solicitado polo usuario xa garda a clave pública nun formato que o TGS pode interpretar.
c) Porque o usuario nunca interactúa co TGS.
d) Ningunha das anteriores é correcta.

3 A rede wifi da UdC emprega WPA-Empresarial e autenticación baseada en EAP-TTLS (emprega PAP para a autenticación do cliente). Cal das seguintes afirmacións acerca do funcionamento desta rede non é correcta:
a) No cliente debemos configurar o contrasinal que se enviará ao servidor mediante o protocolo PAP.
b) Os puntos de acceso precisan coñecer o funcionamento do protocolo PAP.
c) O cliente deberá coñecer o funcionamento do protocolo EAP.
d) Os puntos de acceso non precisan coñecer os contrasinais dos usuarios autorizados.

4 Na autenticación en redes non soe ser necesario que o cliente coñeza o protocolo...
a) PAP
b) CHAP
c) RADIUS
d) 802.1X

5 Nun directorio LDAP realizamos unha búsqueda con parámetros base "ou=people,dc=udc,dc=es", search scope BASE e filtro "ou=*". Cal sería a resposta?
a) As entradas para as cales o pai sexa a entrada "dc=udc,dc=es", en calquera caso.
b) As entradas para as cales o pai sexa a entrada "dc=udc,dc=es", pero só se teñen definido o atributo "ou"
c) A propia entrada "ou=people,dc=udc,dc=es", en caso de existir.
d) Todas entradas que colgan de "dc=udc,dc=es", aínda sen ser fillos directos, que teñan definido o atributo "ou".

6 Cal é o obxectivo da operación BIND en LDAP
a) A operación BIND non existe en LDAP.
b) A autenticación do usuario
c) A monitorización de cambios nunha entrada de directorio
d) Ningunha das anteriores

7 Temos pensado instalar un proxy transparente para controlar o acceso web (HTTP) desde os equipos dunha rede. Cal das seguintes afirmacións non é correcta.
a) O proxy pode empregarse para a análise de contido malicioso nas páxinas web.
b) Poderemos controlar que usuarios teñen acceso á web.
c) Poderemos rexistrar as peticións ou páxinas que visitan os usuarios.
d) Deberemos configurar os equipos cliente para facer uso do proxy.

8 Un firewall de filtrado de paquetes sen estado...

a) non permite bloquear o acceso segundo a IP de orixe.
b) permite bloquear paquetes TCP que non inicien unha nova conexión.
c) non permiten bloquear paquetes pertencentes a protocolos diferentes de UDP ou TCP.
d) soe consumir máis recursos (memoria, etc) que un que si manteña o estado das conexións.

9 Temos un firewall de filtrado de paquetes con estado, que protexe dúas subredes internas (LAN e DMZ) do acceso desde internet (WAN). Supoñendo que o firewall ten 3 interfaces de rede (1 por subreds) e está configurado coas seguintes regras, na orde indicada:
1. Bloquear todo o tráfico entrante desde a WAN.
2. Permitir todo o tráfico procedente da LAN.
3. Permitir paquetes entrantes desde a WAN con destino o servidor Web na DMZ.
4. Permitir paquetes procedentes da DMZ sempre que correspondan a conexións xa establecidas.
5. Permitir paquetes entrantes desde a WAN pertencentes a conexións xa establecidas e destino na rede LAN.
6. Bloquear todos os paquetes.
Cal das seguintes afirmacións é correcta?

a) Os equipos da LAN teñen acceso ao servidor Web da DMZ
b) Os equipos da LAN poden navegar por internet.
c) É posible acceder ao servidor Web desde internet.
d) O servidor Web da DMZ pode acceder a internet, por exemplo para descargar paquetes, sempre que se elimine a regra 1.

10 Partindo da configuración da pregunta anterior, queremos situar un servidor tomcat na DMZ, correndo no porto 8080. Que cambios serían necesarios para permitir o acceso desde internet a este servidor.

a) Ningún, xa funcionaría coa configuración actual.
b) Engadir na posición 4 unha regra igual á 3, pero que permita o acceso desde á WAN cara o novo servidor tomcat.
c) Substituír a regra 6 por unha que permita calquera tipo de tráfico.
d) Ningunha das anteriores é correcta.

11 Temos dous servidores Web, correndo no porto 80 de distintas máquinas, cada unha delas con IP privada. Queremos empregar PAT (Port Address Translation) para permitir o acceso desde internet a ambos servidores. Supoñendo que contamos cun firewall con IP pública e soporte a PAT, é isto posible?

a) Non, xa que PAT so permite traducir enderezos públicos a unha única máquina interna.
b) Non, xa que ambos servidores corren no mesmo porto e PAT traduce cada par dirección-porto a unha IP interna.
c) Si, é posible sempre e cando empreguemos dous portos distintos na IP pública (p.ex 80 e 81) cada un deles mapeado a un servidor diferente.
d) Si, é posible xa que PAT distingue entre distintas peticións ao porto 80 (na IP pública), e sabe a que servidor interno deben ser mapeadas.

12 Temos unha rede con dous firewalls, interno e externo, con dúas subredes: unha DMZ entre ambos firewalls, e outra interna (LAN). Onde situarías unha Base de Datos que debe ser accesible desde internet.

a) Na rede interna, para protexer mellor os datos almacenados, que poderían ser confidenciais.
b) Fora incluso do firewall exterior, xa que podería ter unha carga elevada de tráfico.
c) Na DMZ, xa que en caso de ser atacado con éxito polo menos o atacante non terá acceso á LAN.
d) Ningunha das anteriores é correcta, habería que engadir unha segunda DMZ, interna, para situar alí a BD.

13 A partir del siguiente script iptables, ¿qué afirmación es FALSA?:

```
#!/bin/sh
iptables -F
iptables -X
iptables -Z
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

iptables -A OUTPUT -o eth0 -j ACCEPT

iptables -A INPUT -i eth0 -p icmp -m state --state
ESTABLISHED -j ACCEPT

#SSH
iptables -A INPUT -i eth0 -p tcp --sport 22 -m state --state
NEW,ESTABLISHED -j ACCEPT

#FTP
iptables -A INPUT -i eth0 -p tcp --sport 21 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

a) Todo paquete que no active ninguna de las reglas será rechazado (política por defecto DROP).
b) Podríamos conectarnos a un servidor ssh remoto; en caso de no estar levantado recibiríamos un paquete icmp como respuesta.
c) No se pueden descargar y subir ficheros de un servidor FTP activo remoto ya que es necesario permitir no sólo la conexión de control, sino también la de datos.
d) Estamos rechazando cualquier conexión a nuestro puerto 22 (ssh).

14 ¿Cuál de las siguientes afirmaciones sobre el comando apt-get es FALSA?:

a) Se ha de ejecutar un "apt-get update" antes de un apt-get upgrade. De este modo apt-get conocerá qué versiones están disponibles de los paquetes ya instalados.
b) "apt-get install" permite descargar e instalar un único paquete. Para descargar e instalar más de un paquete es necesario ejecutar el comando en varias ocasiones.
c) "apt-get upgrade" permite instalar las versiones más recientes de los paquetes existentes en el sistema. Dichos paquetes se descargarán de las fuentes descritas en /etc/apt/sources.list
d) "apt-get update" obtiene los repositorios de los paquetes del fichero /etc/apt/sources.list.

15 A la hora de configurar las interfaces de red de las máquinas virtuales de las prácticas un alumno de Redes realizó los siguientes pasos:

Primero en el fichero /etc/network/interfaces introdujo lo siguiente:
...
auto eth0
iface eth0 inet static
address 192.168.1.5
netmask 255.255.255.0
gateway 192.168.1.1
...
- A continuación, levantó la interfaz puesto que no estaba levantada...
 # ifup eth0

- En este momento se dio cuenta de que la IP no era correcta:
 # ifdown eth0
 # ifconfig eth0 192.168.1.101 netmask 255.255.255.0 gateway 192.168.1.1
 # ifup eth0

¿Qué resultado ha obtenido el alumno?:

a) La interfaz eth0 se ha levantado con la IP 192.168.1.5
b) La interfaz eth0 se ha levantado con la IP 192.168.1.101
c) La interfaz eth0 no ha sido levantada (el comando ifup no existe en Ubuntu 8.10).
d) La interfaz eth0 no ha sido levantada (error después de aplicar un ifup tras un ifconfig)

RESERVA:

16 O uso dun proxy dedicado...
a) é a mellor opción para filtrar a nivel IP.
b) permite eliminar carga no firewall principal.
c) é a mellor opción para realizar todo tipo de filtrado de paquetes.
d) só ten sentido en redes wireless.

17 Un arquivo LDIF non...
a) permite o intercambio de datos entre directorios LDAP.
b) é un arquivo de texto.
c) permite operacións de actualización sobre un directorio.
d) permite realizar búsquedas nun directorio LDAP.