Examen 1 septiembre 2009- pregun...

Anónimo

Redes

2º Grado en Ingeniería Informática

Facultad de Informática
Universidad de A Coruña

Redes (Parcial 2) – 4 Setembro 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 acerca de PAP non é correcta:

a) O cliente inicia o proceso de autenticación
b) O cliente envía o seu contrasinal ao servidor.
c) O servidor non precisa almacenar o contrasinal do cliente.
d) Todas as anteriores son correctas.

2 Temos unha rede que fai uso dun servidor RADIUS centralizado, que os distintos servidores de acceso á rede (NAS) empregan para verificar que o usuario ten acceso. Supoñendo que se emprega o protocolo CHAP para autenticar aos clientes, cal debe ser a resposta do servidor RADIUS ao recibir unha petición Access-Request desde un NAS?

a) Un Access-Accept ou ben un Access-Reject, dependendo de se a autenticación tivo éxito ou non.
b) Un Access-Challenge, para enviar ao cliente un desafío ao que este deberá responder posteriormente.
c) Un Access-Accept en calquera caso, xa que o NAS se encarga previamente de comprobar se o cliente debe ter ou non acceso á rede.
d) A petición RADIUS Access-Request non se envía desde o NAS, senón desde os clientes.

3 Temos unha rede wireless 802.11i, na que se emprega o protocolo EAP-MD5 para autenticación. Despois varios meses de funcionamento, decídese cambiar o sistema de autenticación, e empregar o sistema EAP-TLS, máis seguro. Que elementos deberán re-configurarse?

a) Únicamente os clientes, nos que haberá que instalar un certificado dixital.
b) Tanto os clientes como os puntos de acceso (AP).
c) Tanto os clientes como o servidor RADIUS.
d) Deberemos modificar a configuración de clientes, AP e servidor RADIUS.

4 4. En kerberos, cando o cliente solicita un ticket para acceder a un servizo (TGS), envía ao "Ticket Granting Server" unha petición TGS_REQUEST que contén o TGT. Pero, como autentica o "Ticket Granting Server" ao usuario?

a) Non o fai, o TGS envíase cifrado coa clave secreta do usuario, polo que se o usuario non é quen di ser, non poderá acceder ao TGS.
b) Non é necesario facelo, xa que o servizo ao que se quere acceder vai a requerir a autenticación do usuario xunto ao TGS.
c) Non necesita facelo, o "Ticket Granting Server" unicamente debe comprobar que o TGT é válido.
d) Ningunha das anteriores é correcta.

5 Temos un firewall de filtrado de paquetes con estado entre a nosa rede interna (LAN) e internet (WAN), configurado coas seguintes regras:

```
1. Permitir calquera paquete saínte (LAN -> WAN) que abra unha nova conexión.
 2. Denegar paquetes entrantes (WAN -> LAN).
 3. Permitir conexións xa establecidas.
 4. Permitir calquera paquete entrante con destino o porto 80/TCP.
 5. Denegar o resto de paquetes.
```

Cal das seguintes afirmacións é correcta.

a) Os equipos da LAN poden visitar páxinas web sen problemas.
b) Se instalamos un servidor Web na LAN e engadimos, despois da primeira regra, unha que permita abrir novas conexións desde a WAN ao porto 80/TCP do servidor web, poderase acceder a este desde internet.
c) Se instalamos un servidor Web na LAN, a configuración actual xa permite acceder a el desde internet.
d) Ningunha das anteriores é correcta.

6 Cal das seguintes afirmación acerca de LDAP non é certa?

a) Nun directorio distribuído, as entradas "referral" empréganse para referenciar ao pai

desde o directorio subordinado.

b) O formato LDIF permite expresar operacións de modificación sobre un directorio.

c) Nun directorio replicado con estratexia de replicación "single-master", as modificacións só se poden efectuar nunha soa das réplicas.

d) Todas as anteriores son correctas.

7 Un firewall de filtrado de paquetes sen estado non permite...

a) filtrar paquetes segundo a IP de orixe.

b) bloquear paquetes que abren novas conexións.

c) deixar pasar paquetes pertencentes a conexións establecidas.

d) b) e c) son correctas.

8 Que ventaxas ten un proxy a nivel de circuíto fronte a un firewall de filtrado de paquetes?

a) Maior rendemento

b) Funciona con calquera protocolo de aplicación.

c) Elimina certos problemas con paquetes mal formados, xa que non enruta paquetes a nivel IP.

d) Permite analizar riscos ou vulnerabilidades dun determinado protocolo de aplicación.

9 Sinala cal das seguintes afirmacións acerca do modelo de información de LDAP non é certa:

a) A entrada de directorio é a unidade básica de información.

b) Unha entrada de directorio ten un DN (Distinguished Name) que a identifica.

c) Unha entrada de directorio pertence a unha única clase de obxecto (ObjectClass)

d) Unha entrada de directorio ten un conxunto de atributos.

10 Na operación SEARCH de LDAP:

a) Cando o "search scope" é BASE, só se devolven as entradas de directorio que son fillas directas do "base object".

b) É posible establecer un límite máximo de elementos a devolver.

c) Devólvense sempre todos os atributos das entradas que cumplan os criterios de búsqueda.

d) Só se poden especificar filtros de búsqueda de igualdade, aproximación ou combinacións booleanas (AND, OR) deles.

11 Unha empresa desexa por en marcha un conxunto de aplicacións web, polo que se decide instalar un servidor tomcat, un apache (frontend) e un servidor de base de datos. Supoñendo que a empresa conta cunha rede similar á presentada nos exemplos de clase, con dúas DMZ, interna e externa, separadas entre elas e da LAN por firewalls de filtrado de paquetes, cal das seguintes afirmacións é correcta:

a) O servidor apache debería situarse na WAN, fora incluso do firewall exterior, para minimizar problemas derivados de posibles vulnerabilidades do servidor.

b) Os tres equipos deberán situarse na mesma rede (DMZ interna ou externa), xa que o tráfico entre eles é elevado e así evitamos saturar o firewall.

c) Sería preferible que o apache se situase na DMZ externa, deixando a Base de Datos na DMZ interna, máis protexida.

d) Non é posible instalar os tres servidores (tomcat, apache e BBDD), xa que unicamente dispoñemos de 2 DMZs.

12 Cales das seguintes non é unha característica do uso de NAT:

a) Axuda a ocultar os enderezos usados nas máquinas internas.

b) Impide que se sitúen servidores accesibles desde internet na rede interna.

c) Permite que distintas máquinas accedan a internet pese a contarse cunha única IP pública.

d) As tres anteriores son características de NAT.

13 Según el siguiente script iptables

```
#!/bin/sh

iptables -F
iptables -X
iptables -Z

iptables -A INPUT -j DROP
iptables -A OUTPUT -j DROP
iptables -A FORWARD -j DROP

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

iptables -A OUTPUT -o eth0 -m state
--state ESTABLISHED,RELATED -j
ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport
22 --sport 1024:65535 -m state
--state NEW -j ACCEPT

iptables -A INPUT -p tcp -i eth0 --dport
80 --sport 1024:65535 -m state
--state NEW -j ACCEPT

iptables -A INPUT -i eth0 -p tcp -m state
--state ESTABLISHED,RELATED -j
ACCEPT

Suponiendo que tenemos un servidor web
corriendo en el puerto 80 y un
servidor ssh en el 22
```

a) No podemos hacer una petición a www.fic.udc.es desde nuestro navegador, puesto que no recibiríamos la respuesta ya

que la política por defecto para INPUT es DROP.

b) Podemos navegar por www.fic.udc.es.

c) No nos pueden hacer una petición a una aplicación web en nuestro servidor, puesto que la petición se haría desde el puerto 80 y sólo se están permitiendo peticiones desde puertos entre 1024 y 65535.

d) Las 3 respuestas anteriores son incorrectas.

14 Los archivos que cuelgan bajo directorio /etc/rc0.d en un sistema

a) Tienen como propósito parar todos los servicios y preparar al sistema para poder ser reiniciado.

b) Generalmente son enlaces simbólicos que apuntan a ficheros situados en /etc/init.d y su propósito es parar todos los servicios y permitir que el sistema se apague correctamente.

c) No son enlaces (son ficheros regulares) y su propósito es parar todos los servicios y permitir que el sistema se apague correctamente.

d) Tienen como propósito parar todos los servicios y poner al sistema en modo mono-usuario (single-user mode).

15 El uso de LVM es útil...

a) ...cuando no sabemos como evolucionarán las necesidades de almacenamiento en más de un disco duro (no aporta nada usarlo con un único disco, por motivos evidentes).

b) ...cuando no sabemos cómo evalucionarán las necesidades de almacenamiento en cada una de las particiones que queremos crear.

c) ...cuando en un sistema se desea realizar stripping entre dos volúmenes lógicos exactamente del mismo tamaño y con el mismo sistema de ficheros, siendo, de este modo, el sistema más eficiente computacionalmente.

d) ...cuando usamos Ubuntu, puesto que este administrador de volúmenes lógicos es exclusivo de este sistema operativo.

RESERVA:

16 Cal das seguintes afirmacións acerca do protocolo 802.1X non é correcta:

a) Fai uso do protocolo EAP.

b) Require soporte por parte do cliente.

c) O porto controlado só permite tráfico cando o cliente está autenticado.

d) O porto non controlado só permite tráfico cando o cliente está autenticado.

17 Temos unha rede no que o acceso a internet está controlado por un firewall de filtrado de paquetes con estado. Actualmente, todos os equipos da LAN poden acceder a internet, pero queremos filtrar o tráfico HTTP a nivel de aplicación, polo que instalamos un proxy na LAN. Para asegurarnos de que o acceso a internet só se fai a través do proxy deberemos realizar certos cambios. Pero, cal dos seguintes cambios podería non ser necesario?

a) Configurar os clientes para que fagan uso do proxy.

b) Bloquear o acceso a internet desde os equipos da LAN, a excepción do proxy.

c) Permitir ao proxy acceder a internet.

d) As opcións a) e c) poderían ser innecesarias, segundo as condicións do enunciado.