Redes (Temas 4, 5 Part II e Práctica 2) - Marzo 2009

(Modelo A)

Departamento de Tecnoloxías da Información e as Comunicacións

Facultade de Informática da Coruña

D.N.I.: _____ **Titulación:**_____

Apelidos: _____ **Nome:** _____

- ***SÓ SE EVALUARÁN AS RESPOSTAS SINALADAS NA TÁBOA DE RESPOSTAS.***
- *En cada pregunta existe **unha soa** resposta válida que puntúa **+0.5**.*
- *As respostas incorrectas **-0,2** e as non contestadas non puntúan.*
- *A duración máxima do examen será de **50 minutos***

Pregunta	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20		21	22
Resposta																							

1 En cal dos seguintes protocolos de autenticación o contrasinal do usuario se envía cifrado pola rede ?

a) CHAP
b) MS-CHAP
c) PAP
d) Ningunha das anteriores é correcta.

2 Durante o proceso de autenticación nunha rede wireless con 802.11i, o Punto de Acceso recibe unha mensaxe Access-Challenge desde o servidor RADIUS. Que debe realizar o AP?

a) Enviar ao cliente a mensaxe EAP que contén o paquete Access-Challenge.
b) Encapsular a mensaxe RADIUS nun paquete EAPOL e enviarlla ao cliente, xa que este sabe como interpretar as mensaxes do servidor RADIUS
c) Interpretar o contido da mensaxe e denegar ou permitir o acceso segundo corresponda
d) Descartar a mensaxe.

3 Para cal das seguintes situacións nunca usarías un arquivo LDIF?

a) Insertar datos nun directorio LDAP
b) Modificar entradas dun directorio LDAP
c) Especificar filtros de búsquedas sobre un directorio LDAP
d) Exportar información dun directorio LDAP

4 Cal das seguintes non é unha ventaxa dos proxies dedicados respecto aos firewalls de filtrado de paquetes básicos:

a) Posibilidade de detectar virus.
b) Posibilidade de bloquear certos comandos de aplicación.
c) Maior rendemento.
d) Autenticación avanzada de usuarios.

5 Nun directorio LDAP temos unha entrada de nome "cn=Vreixo + uid=vfor,ou=people,dc=udc,dc=es". Cal é o DN da entrada pai:

a) uid=vfor,ou=people,dc=udc,dc=es
b) ou=people,dc=udc,dc=es
c) ou=people
d) Nengunha das anteriores é correcta

6 Temos unha rede con dous firewalls de filtrado de paquetes con estado, configurados coas seguintes regras:
Firewall 1 (externo):
1.1. Permitir paquetes entrantes destinados ao porto 80 de TCP
1.2. Denegar todos os paquetes
Firewall 2 (interno):
1.1 Permitir conexións xa establecidas.
1.2 Denegar paquetes entrantes.
1.3 Permitir o resto de paquetes.
Cal das seguintes afirmacións non é certa?

a) É posible que desde internet se consulte calquera servidor web situado na DMZ.
b) Os equipos situados na DMZ poden comunicarse entre si.
c) Os usuarios da rede interna teñen acceso ao servidor web da DMZ.
d) Non é posible comunicarse desde a DMZ con servidores da rede interna.

7 Que cambios serían necesarios, na configuración do exemplo anterior, para permitir aos usuarios da rede interna conectarse a internet.

a) Debemos cambiar a configuración do segundo firewall.
b) É necesario tocar a configuración do primeiro firewall.
c) É necesario tocar a configuración de ambos firewalls.
d) Necesitaríamos un proxy web, non é posible usando unicamente filtrado de paquetes.

8 Que mecanismo emprega kerberos para protexer a clave secreta do Ticket Granting Server cando esta se envía sobre unha rede insegura.

a) Criptografía de clave simétrica, porque se envía cifrada cunha clave de sesión xerada automaticamente.
b) Unha combinación de criptografía simétrica e asimétrica, xa que a clave de sesión,

secreta, se intercambia primeiro utilizando a clave pública do usuario.
c) Criptografía de clave simétrica, xa que se cifra coa clave secreta do usuario, compartida por el e o Key Distribution Center.
d) Nengunha das anteriores é correcta

9 Que tipo de firewall permitiría bloquear páxinas web segundo o seu contido?
a) Un firewall de filtrado de paquetes.
b) Un application-level proxy.
c) Un circuit-level proxy.
d) Un firewall de filtrado de paquetes con estado.

10 Cal das seguintes afirmacións acerca do modelo de información de LDAP é certa:
a) Unha entrada de directorio nunca pode ter varios valores para un mesmo atributo.
b) As entradas de directorio pertencen unicamente a unha clase de obxectos.
c) O esquema de directorio especifica entre outras cousas os tipos de atributos permitidos.
d) Todas as clases de obxectos deben ter un atributo "cn".

11 Temos unha rede protexida de internet mediante un firewall de filtrado de paquetes. Se queremos permitir aos clientes da rede interna o acceso web, pero por medio dun proxy dedicado situado nesa rede interna, que tráfico debemos permitir no firewall.
a) Ningún, os clientes saen a internet a través do proxy.
b) O acceso HTTP desde calquera equipo da rede interna.
c) Únicamente o tráfico HTTP desde o proxy.
d) Ningunha das anteriores soluciona o problema, o proxy ten que estar na rede externa.

12 Cal dos seguintes protocolos permite que o cliente se autentique mediante certificado.
a) PAP
b) CHAP
c) EAP-TLS
d) WEP

13 Queremos empregar un firewall de filtrado de paquetes básico (sen estado) para restrinxir o acceso a un servidor web interno. Entre os seguintes campos presentes nos paquetes recibidos, cal non se pode especificar nas regras do firewall:
a) A IP de orixe.
b) O tipo de operación solicitado (GET, POST...).
c) Que o flag SYN esté presente e o ACK non, o que indica que é unha conexión nova.
d) O porto de orixe, que non ten sentido comprobar xa que soe ser aleatorio.

14 Se nun servidor LDAP realizamos unha búsqueda con base "dc=udc,dc=es", search scope "BASE" e filtro de búsqueda "(dc=people)", cal será a resposta
a) Unha lista coas entradas de directorio baixo a rama "dc=people,dc=udc,dc=es"
b) A entrada de directorio con DN="dc=people,dc=udc,dc=es"
c) Non devolvería nengunha entrada
d) A entrada de directorio con DN="dc=udc,dc=es"

15 Nunha rede configurada con dous firewalls Stateful Packet Filter, en onde situarías un servidor DNS público.
a) Na DMZ, entre os dos fw, para manter protexida a rede interna en caso de que o servidor sexa atacado con éxito.
b) Fora do firewall exterior, xa que ao ser un servidor público non ten sentido situalo nunha rede interna protexida.
c) Na LAN interna, xa que ao ser un servidor público debemos protexelo especialmente, e a rede interna é a que mellor protexida está.
d) Fora do firewall exterior, xa que como UDP é un protocolo non orientado a conexión non aporta nada protexer o servidor cun firewall con estado.

16 Nun esquema de autenticación basado en 802.11i que compoñentes precisan coñecer a IP do servidor RADIUS
a) O punto de acceso (autenticador)
b) O cliente (suplicante)
c) Cliente e punto de acceso
d) Nengún, é obligatorio usar kerberos

17 Montando LVM no Ubuntu Server con 5 particións (/boot, swap, /, /usr e /var) e con /boot fora de LVM:
a) A mellor opción é crear as particións sen LVM primeiro (/boot, swap, /, /usr y /var) e logo montar os sistemas de ficheiros desexados con LVM.
b) É preferible crear /boot e os volumes físicos directamente antes de crear as outras particións.
c) As dúas opcións anteriores son equivalentes en caso de ter só un disco físico.
d) Todas as opcións anteriores son erróneas.

18 A conexión entre o host (Windows XP) e o guest (Ubuntu) nos equipos do laboratorio usando NAT:
a) É posible porque VMWare mantén unha táboa NAT mediante a cal traduce as IP's públicas que recibe do host.
b) É imposible usando NAT e VMWare.
c) É posible xa que VMWare crea unha interfaz virtual no host que pertence á mesma red na que están as máquinas virtuais instaladas.
d) É imprescindible montar un bridge para logralo.

19 A partir do seguinte script iptables e considerando

que está pensado para unha máquina virtual como as montadas nas prácticas da asignatura:

```
#!/bin/sh
iptables -F
iptables -X
iptables -Z
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -i eth0 -m state --state
ESTABLISHED -j ACCEPT
iptables -A OUTPUT -i eth0 -m state --state NEW,
ESTABLISHED -j ACCEPT
```

Sinalar cal das seguintes opcións é a correcta:

a) Pódese subir e baixar ficheiros dun servidor ftp activo remoto.
b) Se se establece unha conexión UDP cun servidor de "echo" remoto, en caso de estar caído, recibiríase o paquete ICMP correspondente.
c) Pode conectarse desde unha máquina remota empregando un cliente ssh ao porto 22 da máquina, xa que se están permitindo conexións establecidas desde o exterior.
d) Ningunha das anteriores é correcta.

20 Un sistema de ficheiros con journaling como ReiserFS, por exemplo:

a) Crea logs cos cambios nos datos e nas estruturas de datos antes de facelos efectivos.
b) Permite recuperar unicamente datos en caso de haber un fallo de corrente ou unha caída do sistema.
c) Permite recuperar unicamente estruturas de datos en caso de que un atacante teña borrado os logs.
d) Ningunha das anteriores.

PREGUNTAS DE RESERVA:

21 Cal das seguintes situacións non podería ser controlada por un firewall de filtrado de paquetes stateful situado entre duas redes.

a) Evitar que unha máquina na rede externa se faga pasar por unha interna usando técnicas de IP spoofing.
b) Filtrar correo electrónico entrante según cal sexa a IP de orixe.
c) Permitir só o tráfico ICMP relacionado con erros pertencentes a conexións iniciadas desde a rede interna.
d) Todas elas poden ser controladas

22 Cal das seguintes afirmacións acerca do protocolo 802.1X é certa.

a) O switch bloquea calquera tráfico procedente do cliente ate que este se autentique.
b) Cada switch da rede debe ter configurada a lista de usuarios con acceso, xunto as correspondentes claves.
c) Emprega mensaxes EAP para solicitar as credenciais do cliente.
d) É un compoñente clave da arquitectura de seguridade de redes wireless basada en WEP.