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

(Modelo B)

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 kerberos, cal das seguintes afirmación acerca do TGT non é certa:

a) Envíase como resposta a unha petición AS_REQUEST
b) Encapsula unha clave de sesión a empregar entre o cliente e o servizo a que desexa acceder.
c) Está cifrado coa clave secreta do Ticket Granting Server
d) Normalmente só é válido durante un certo período de tempo.

2 Un atributo LDAP...

a) ...sempre ten un único valor por entrada de directorio.
b) ...só está presente nas entradas folla (que non teñen fillos).
c) ...ten asociado un tipo que determina as regras de comparación entre distintos valores (entre outras características).
d) ...ao contrario das clases de obxecto non está definido no esquema de directorio.

3 Temos unha rede cun único firewall con tres interfaces de rede, que corresponden ás redes WAN, LAN e DMZ. O fw, que é do tipo "Stateful Packet Filtering" ten configuradas as seguintes regras, na orde indicada:
1. Permitir paquetes entrantes desde a rede WAN, con destino o servidor web (na DMZ), ao porto 80/TCP e estado "nova conexión"
2. Denegar paquetes procedentes da rede WAN
3. Permitir calquera paquete sainte desde a rede LAN
4. Denegar o resto de paquetes
Que cambios nos permitirían consultar por HTTP, desde a rede WAN, as páxinas web aloxadas no servidor web da DMZ?

a) Situar o servidor web na LAN en lugar de na DMZ.
b) Non é necesario engadir ningunha regra, a configuración actual xa permite o acceso requerido.
c) Unha regra para permitir todo despois da 3ª.
d) Ningunha das anteriores é correcta.

4 Cal das seguintes afirmacións referidas á configuración indicada na pregunta anterior é certa:

a) Os equipos da LAN poden navegar por internet.
b) Os equipos da LAN non poden consultar as páxinas aloxadas no servidor web da DMZ.
c) Os equipos da DMZ teñen acceso HTTP a máquinas na rede WAN.
d) Se a 4ª regra estivese en primeiro lugar, non sería posible a comunicación entre dous equipos da LAN.

5 Cal das seguintes situacións pode ser controlada por un firewall de filtrado de paquetes básico (sen estado).

a) Bloquear paquetes que inicien novas conexións TCP.
b) Bloquear o acceso desde certas IPs.
c) Bloquear o acceso a paquetes TCP que non inicien novas conexións.
d) As tres son correctas.

6 En cal dos seguintes protocolos de autenticación o contrasinal se envía pola rede en claro?

a) CHAP
b) PAP
c) MS-CHAP
d) a) e c) son correctas

7 Por que opción debemos decantarnos se queremos permitir o acceso desde internet a un servidor de correo e outro web, situados nunha DMZ detrás dun firewall, pero só temos unha IP pública.

a) Só é posible, usando NAT, se os servidores están desplegados en máquinas virtuais (como vmware) na mesma máquina física coa rede configurada con bridge.
b) Podemos utilizar PAT (port forwarding) no firewall para mapear ambos servidores, que contarán con IPs privadas.
c) Non é posible, temos que ter IPs públicas para cada un dos servidores.

d) Debemos configurar as tres máquinas co mesmo enderezo IP.

8 Cal das seguintes afirmación acerca do protocolo EAP non é certa:

a) É un protocolo extensible que permite distintos métodos de autenticación.
b) Os tres elementos que interveñen na autenticación (cliente, NAS e servidor de autenticación) deben coñecer o método de autenticación empregado.
c) Os clientes precisan coñecer o método de autenticación empregado.
d) Utilízase no estándar de autenticación 802.1X.

9 Cal das seguintes operacións non está definida no protocolo LDAP:

a) BIND
b) COMMIT
c) SEARCH
d) ADD

10 Cal dos seguintes protocolos non se utiliza nunha arquitectura RSN 802.11i en redes wireless:

a) WEP
b) EAP
c) EAPOL
d) RADIUS

11 Que búsqueda LDAP debemos empregar para listar os fillos directos da entrada "ou=people,dc=udc,dc=es" que teñan o valor "Victor" no atributo "cn".

a) Base "dc=udc,dc=es", search scope "SUB" e filtro "cn=Victor"
b) Base "ou=people,dc=udc,dc=es", search scope "BASE" e filtro "cn=Victor"
c) Base "ou=people,dc=udc,dc=es", search scope "SUB" e filtro "cn=Victor*"
d) Base "ou=people,dc=udc,dc=es", search scope "ONELEVEL" e filtro "cn=Victor"

12 Queremos controlar as descargas que realizan os nosos usuarios desde internet (vía HTTP) para detectar posibles virus, pero non temos a posibilidade de modificar a configuración en cada equipo cliente. Cal sería a mellor opción?

a) Bloquear o acceso HTTP cun firewall de filtrado de paquetes.
b) Instalar un proxy transparente.
c) Instalar un proxy dedicado, para evitar cargar en exceso o firewall principal.
d) Non é posible solucionar o problema sen poder cambiar a configuración nos clientes.

13 Supoñamos que nun schema LDAP temos definida a clase de obxecto "customPerson" cun atributo obligatorio "cn", e dous atributos opcionais: "telephoneNumber" e "postalAddress". Se temos unha entrada de directorio no cal o atributo "objectclass" ten o valor "customPerson", cal das seguintes afirmacións non é certa:

a) A entrada debe ter polo menos un valor no atributo "cn".
b) A entrada podería ter atributos adicionais aos indicados no enunciado, en caso de que o atributo "objectclass" tivese valores adicionais ao de "customPerson"
c) O RDN da entrada debe ser da forma "cn=XXX", onde XXX sería calquera valor que cumpra as regras sintácticas definidas para o atributo.
d) Poderíanse especificar varios valores para o atributo "postalAddress", sempre a cando no esquema estivese configurado como un atributo multivaluado.

14 Cal das seguintes non é unha mensaxe RADIUS válida:

a) Access-Challenge
b) Access-Request
c) Access-Denied
d) Access-Reject

15 Cal das seguintes é unha limitación dos firewalls de filtrado de paquetes básicos (sen estado)

a) O seu rendemento é moi limitado.
b) Son incapaces de distinguir se un paquete pertence a unha conexión xa establecida.
c) Só poden bloquear tráfico TCP ou UDP, tendo problemas con outro tipo de tráfico (ex: ICMP)
d) Non son capaces de bloquear tráfico procedente da rede interna.

16 Temos unha rede con dous firewalls, un exterior (boundary router, filtrado de paquetes básico) e un principal (stateful packet filtering). Entre ambos sitúase a DMZ externa. Detrás do fw principal temos a rede interna (LAN), e unha DMZ interna de tipo Service Leg. Cal dos seguintes sería o lugar máis apropiado para situar un servidor HTTP público cun nivel de tráfico relativamente elevado?

a) Na DMZ externa, para manter o servidor protexido polo firewall exterior, ao tempo que o firewall interno protexe as outras redes, máis sensibles.
b) Na DMZ interna, xa que as DMZ de tipo Service Leg son as máis apropiadas para manexar altos volúmenes de carga.
c) Na LAN, xa que os servidores públicos requiren de especial protección, e estar tras 2 firewalls é o máis adecuado neste caso.
d) Na rede exterior, xa que os servidores públicos, por definición, non deben estar detrás dun firewall.

17 Creouse un script con nome iptables.sh (con permisos 744) baixo /etc/init.d e executouse o comando "update-rc.d iptables.sh defaults". Tendo en conta que o script non ten erros:

a) A configuración é correcta e non ten ningún problema.

b) No modo monousuario non se levanta o firewall (hai un problema de seguridade na configuración, xa que neste nivel se levantan servizos de rede).
c) É necesario colocar o script no directorio /etc/network/if-pre-up.d e calquera outra solución sería errónea.
d) Ao empregar defaults como opción xa se crean enlaces en todos os niveis nos que se levantan servizos de rede.

18 En Ubuntu, se un usuario quere crear unha tarefa cron que se execute regularmente pode:

a) Crear un script e colgalo baixo /etc/cron.hourly cos permisos 666, en caso de ser root.
b) Editar o arquivo /etc/crontab e programar nel a súa tarefa, independentemente dos permisos do usuario.
c) Usar o comando crontab coa opción -e, co que sempre se executará calquiera tarefa que programe.
d) Crear un script con permisos 711 e colgalo baixo /etc/cron.hourly esté ou non no cron.deny, sempre e cando esté no cron.allow e teña permisos de root.

19 Partindo do seguinte script iptables:

```
#!/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 -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 1:1024 -j DROP # A
iptables -A OUTPUT -p tcp --sport 1:1024 -j DROP # B
```

¿Poderíase acceder a un servidor HTTP correndo na máquina?

a) Non, xa que coas regras A e B estaríamos bloqueando o acceso ao servizo HTTP.
b) Si, xa que as regras A e B non se chegan a aplicar en tráfico HTTP.
c) Si, pero só se cambiamos a política por defecto para ACCEPT.
d) Non, xa a política por defecto (DROP) se aplica en primeiro lugar xa que aparece antes no script.

20 O comando apt-key é útil para:

a) Xestionar a lista de claves usadas por apt para autenticar paquetes.
b) Xestionar a lista de claves usadas por calquera xestor de paquetes instalado no sistema.
c) Comprobar o CRC dos paquetes descargados.
d) Descargar paquetes dunha forma rápida e sinxela.

PREGUNTAS DE RESERVA:

21 En Linux, para que un sistema poida enrutar paquetes debe ter activado o flag "IP forwarding". Que tipo de firewall, implementado sobre un sistema Linux, podería ter este flag desactivado:

a) Un proxy dedicado
b) Un firewall de filtrado de paquetes.
c) Os firewalls nunca enrutan paquetes, polo que dito flag non é necesario en ningún caso.
d) Calquera tipo de firewall precisa enrutar paquetes, polo que dito flag sempre é necesario.

22 Cal das seguintes afirmacións acerca dos certificados dixitais <u>non</u> é correcta:

a) Idealmente están firmados dixitalmente por unha entidade certificadora.
b) Utilízanse para distribuir as claves secretas sobre redes inseguras evitando fraudes de suplantación de identidade.
c) Unha das súas principais aplicacións é a Public Key Infraestructure (PKI)
d) Distribúense no formato regulado polo estándar ITU-T X.509.