Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2011/2012 – Exame prático – 2ª Parte

09/02/2012 – 18:30

Prova a realizar sem recurso a consulta. Duração: 50 minutos. Bom trabalho.

Número: _____ **Nome:** _____

Grupo 1 (8 valores)

Questões de escolha múltipla. Seleccione todas as opções correctas, o número TOTAL de opções correctas é cerca de 50%. **Duas respostas incorrectas descontam uma resposta correcta.**

1. O OSPF (*Open Shortest Path First*)...
   - ☐ envia sempre periodicamente LSA's.
   - ☐ não propaga rotas entre áreas diferentes.
   - ☐ tem um limite de 2^{32} saltos.
   - ☐ encapsula directamente as mensagens sobre IP.
   - ☐ tem em conta a largura de banda das rotas disponíveis para um mesmo destino.
   - ☐ classifica logicamente os encaminhadores sob três classes.
2. O EIGRP ...
   - ☐ é um protocolo *standard*.
   - ☐ por omissão, utiliza o conceito de *classless*.
   - ☐ utiliza quatro tecnologias para obter uma melhor capacidade de encaminhamento.
   - ☐ obriga a que as redes trabalhem em IP.
   - ☐ provoca pouco *overhead* na tarefa de detectar a disponibilidade de vizinhos.
   - ☐ só permite a redistribuição de rotas sobre protocolos *distance-vector*.
3. A utilização do NAT em balanceamento de carga ...
   - ☐ distribui aleatoriamente cada novo pedido por um dos servidores disponíveis.
   - ☐ não obriga à paragem de todo o *server farm* se um dos servidores tiver de ser desligado.
   - ☐ permite o balanceamento dos pedidos de acordo com a capacidade de cada servidor.
   - ☐ não obriga a cuidados especiais de implementação em termos de segurança, acessos, etc.
   - ☐ só pode ser efectuado se o dispositivo de NAT for um encaminhador.
4. O *Twice NAT* ...
   - ☐ permite que redes independentes mas com o mesmo endereço de rede comuniquem entre si.
   - ☐ obriga à existência de servidores DNS com extensões específicas.
   - ☐ só pode ser utilizado se os endereços das redes forem privados.
   - ☐ mantém os mapeamentos criados por um tempo definido (*bind-holdout time*).
   - ☐ pode ser substituído por NAT estático.
   - ☐ faz a translação dos endereços internos mas não dos externos.

5. O CBAC ...
   - ☐ é um protocolo *standard.*
   - ☐ coloca as regras dinâmicas criadas após as regras estáticas existentes.
   - ☐ só permite validar protocolos do nível 7 do modelo OSI.
   - ☐ tem métodos diferentes de aplicação consoante o interface ser interno ou externo.
   - ☐ permite abrir acessos numa *firewall* para os tipos de tráfego pretendidos.
6. A criptografia ...
   - ☐ pode ter o método bloco ou contínuo.
   - ☐ em bloco pode ser periódica.
   - ☐ em contínuo cifra cada parte da mensagem original com a mesma chave.
   - ☐ em bloco permite obter cifras diferentes para blocos iguais da mensagem original.
7. O sistema Kerberos ...
   - ☐ só trabalha sobre TCP.
   - ☐ tem um ponto de falha crítico que é o próprio servidor Kerberos.
   - ☐ tem um custo significativo na ocupação da largura de banda.
8. Uma DMZ (*Delimitarized Zone*) ...
   - ☐ consiste na prática numa rede interna mas acessível do exterior.
   - ☐ pode ser criada por um *bastian host.*
   - ☐ pode ser criada na mesma rede de endereços IP da rede interna da organização.
9. O par endereço IP / WILDCARD: 194.28.32.64 / 0.32.2.63 ...
   - ☐ define parte dos endereços de um total de duas redes de classe C.
   - ☐ define 256 endereços.
   - ☐ inclui o endereço 194.60.33.0.
   - ☐ inclui o endereço 194.28.34.70.
10. A regra de ACL "**deny icmp 223.20.5.1 0.0.32.0 any**" ...
    - ☐ não tem qualquer efeito sobre tráfego UDP nem TCP.
    - ☐ bloqueia o tráfego ICMP destinado ao endereço 223.20.5.1.
    - ☐ não é válida no contexto de uma ACL *standard.*
    - ☐ bloqueia o tráfego ICMP com origem no endereço 223.20.37.1.
11. Uma ACL constituída apenas pela regra: "**permit ip any 195.100.1.20 0.0.18.0**" ...
    - ☐ permite tráfego ICMP.
    - ☐ permite tráfego TCP destinado ao porto 70 do nó 195.100.3.20.
    - ☐ permite tráfego TCP destinado ao porto 60 do nó 195.100.2.20.
    - ☐ permite tráfego UDP com destino ao nó 20 da rede 195.100.21.0/24.
    - ☐ permite tráfego UDP com destino ao porto 40 do nó 195.100.17.20.
    - ☐ permite tráfego TCP com destino ao nó 195.100.20.20.

12. O comando "**ip access-group 150 in**" ...

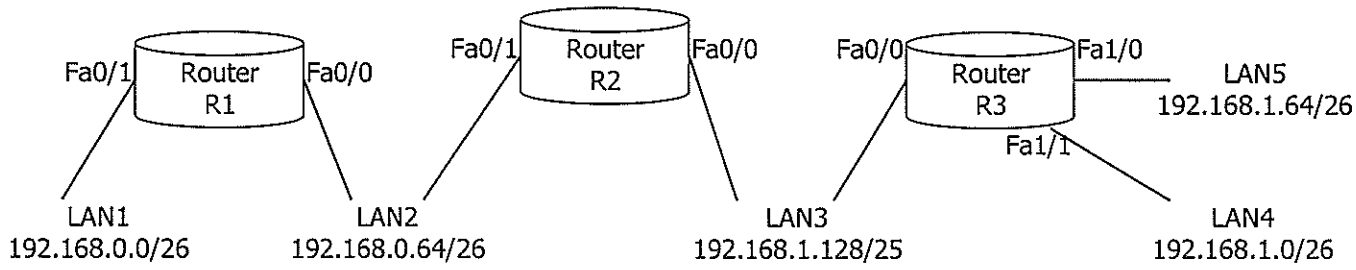
- ☐ aplica uma ACL *extended* a uma interface de rede.
- ☐ aplica uma ACL a uma interface de rede que possui o nome "in".
- ☐ não tem qualquer efeito directo sobre o tráfego que sai pela interface onde é aplicado.
- ☐ é válido no contexto de configuração de uma interface de rede.

13. Para representar apenas os endereços de nó 2, 6, 10, 14, 66, 70, 74 e 78 da rede 192.168.5.0/24 pode-se usar: ...

- ☐ 192.168.5.0 0.0.0.255.
- ☐ 192.168.5.0 0.0.0.78.
- ☐ 192.168.5.2 0.0.0.76.
- ☐ 192.168.5.0 0.0.0.76.

Grupo 2 (12 valores)

Observe o seguinte conjunto de redes:



Pretende-se atingir os seguintes objectivos:

LAN1: só pode enviar tráfego HTTP para as redes LAN4 e LAN5, e responder a pedidos TCP.
LAN2: pode enviar para todas as redes, com excepção dos nós 80 até 90 que não podem enviar nada.
LAN3: apenas pode enviar tráfego ICMP para a rede LAN2.
LAN4: os nós 1 até 60 não podem enviar para lado nenhum, os restantes podem enviar para todo o lado.
LAN5: pode enviar para as redes LAN 2 e LAN3, todo o tipo de tráfego, nada mais.

Escrever os comandos para criar as ACL necessárias indicando sempre o nome do encaminhador onde vai ser aplicada, qual a interface (Fa?/?) e qual o sentido de aplicação (IN/OUT).

Optimize as ACL: minimize o número de regras/linhas e, quando possível, opte por ACLs "standard".

Sintaxe de comandos

```
no access-list NUMERO
access-list NUMERO permit|deny ENDEREÇO-IP WILDCARD
access-list NUMERO permit|deny PROTOCOLO ENDEREÇO-IP WILDCARD ENDEREÇO-IP WILDCARD [ COMPARAÇÃO SERVIÇO ]
```

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2011/2012

Exame Normal – 09/Fevereiro/2012

Número: _____ **Nome:** _____

Prova a realizar sem recurso a consulta. Duração: 50 minutos.
Em cada afirmação assinale V ou F (Verdadeiro ou Falso) conforme considere aplicável.
Se não tiver a certeza, não responda. Cada resposta errada desconta meia resposta certa. Bom trabalho.

1ª Parte – Administração de servidores Linux

1. A partição SWAP é adequada para armazenar as HOMES dos utilizadores ..... _____

2. Independentemente do conteúdo do ficheiro /etc/nsswitch.conf, o ficheiro /etc/passwd é sempre consultado..... _____

3. As permissões 603 são adequadas para o ficheiro /etc/passwd ..... _____

4. O "Name Service Switch" (NSS) permite que utilizadores definidos em repositórios remotos sejam reconhecidos no servidor... _____

5. No ficheiro "/etc/passwd", o último campo de cada linha é o UID do utilizador ..... _____

6. "eth1:1" e "eth1.1" são duas designações alternativas para a mesma interface de rede ..... _____

7. Para configurar a tabela de encaminhamento IP pode ser usado o comando "ip" ou o comando "route" ..... _____

8. Numa cadeia PAM, o sucesso num módulo "sufficient", sem falhas anteriores vai terminar a cadeia e devolver sucesso ..... _____

9. O módulo "pam_deny.so" pode ser usado em qualquer uma das 4 cadeias do sistema PAM ..... _____

10. A pasta HOME dos utilizadores nunca deve ter as permissões 022..... _____

11. As permissões 704 são adequadas para o ficheiro "/etc/nsswitch.conf" ..... _____

12. O comando "chmod" permite alterar o proprietário e grupo de um ficheiro ou directório ..... _____

13. O comando "umask" não tem qualquer efeito sobre objectos já existentes ..... _____

14. As alterações produzidas nos ficheiros de arranque da shell definidos pelo utilizador prevalecem sobre as do administrador . _____

15. A principal vantagem das cópias incrementais é que a operação de restauro é mais rápida ..... _____

16. O comando "ifconfig" pode ser usado para definir o endereço IPv4 de uma interface de rede, mas não funciona para IPv6..... _____

17. O comando "vconfig" tem a mesma sintaxe (parâmetros) que o comando "ifconfig" ..... _____

18. A interface "eth1:2" é uma interface de VLAN ..... _____

19. O ficheiro inetd.conf indica ao inetd quais os portos que devem estar à escuta e qual o servidor a arrancar para cada porto... _____

20. A regra "# iptables -A FORWARD -s 192.168.0.45 -p icmp -j DROP" barra todos os pacotes icmp da origem 192.168.0.45..... _____

21. O comando "# iptables -A INPUT -p tcp -i eth0 --dport ssh -j ACCEPT" permite todo o tráfego SSH que entra por eth0 ..... _____

22. O "System Logger" (syslogd) aplica o evento apenas à primeira regra concordante que exista no ficheiro de configuração ..... _____

23. As permissões 705 num ficheiro permitem a todos os utilizadores escrever no ficheiro ..... _____

24. O comando "quotacheck" serve para indicar que utilizadores ultrapassaram as respectivas cotas ..... _____

25. O ficheiro "/etc/resolv.conf" é o principal ficheiro de configuração do servidor DHCP ..... _____

26. O comando "# iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT" barra todo o trafego Web que entra por "eth0" ..... _____

27. O comando #openssl req" tem como finalidade principal gerar uma chave e emitir um pedido de certificação da mesma ..... _____

28. A linha de configuração do CRON começada por "*/15 3 * * *" é executada 24 vezes por dia ..... _____

29. O comando "last" apresenta um registo sequencial de todas as entradas e saídas de utilizadores no sistema..... _____

30. Uma cópia de um disco, realizada com o comando "dd", só pode ser restaurada para um disco igual ao original..... _____

31. Os comandos "dump" e "restore" suportam cópias incrementais..... _____

32. O SAMBA permite criar um servidor Windows em Linux e os clientes Windows podem usar esse servidor ..... _____

33. O Samba permite integrar um servidor Linux num domínio Windows AD ..... _____

34. O comando "chmod 712 lista.txt" dá a todos os utilizadores permissão para ver o conteúdo do ficheiro "lista.txt" ..... _____

35. O comando "passwd" permite ao administrador ("root") alterar a "password" de qualquer utilizador local ..... _____

36. O comando "quotaon" pode ser usado pelo administrador ("root") para definir as cotas máximas de cada utilizador..... _____

37. O comando "iptables –A INPUT –i eth1 –p tcp –j ACCEPT" actua sobre a tabela "filter" ..... _____

38. A linha de configuração do CRON "10 5 * * * root /root/teste" provoca a execução do comando dez vezes por dia..... _____

39. Para configurar o protocolo HTTPS no servidor Apache é necessário fornecer-lhe o certificado e a respectiva chave privada. _____

40. A interface "eth1.17" é uma interface de VLAN, com VLANID=117 ..... _____

41. O "Internet Daemon" (INETD) é particularmente adequado para serviços com reduzidas taxas de utilização..... _____

42. O comando "who" consulta informação criada pelo System Logger" (syslogd)..... _____

43. O comando "tar" suporta cópias incrementais..... _____

2ª Parte – Administração de servidores Windows

1. As configurações de discos RAID1 e RAID5 são ambas tolerantes a falhas num dos discos envolvidos ..... _____

2. O Hyper V no WS2008 suporta virtualização de vários tipos de sistemas operativos, não apenas Microsoft ..... _____

3. A password "X$aB345" é válida com as "default password requirements policies" activas ..... _____

4.Os objectos do Active Directory obedecem a determinadas regras, sendo estas denominadas de Schema ..... _____

5. Entre outros mecanismos de segurança os PDC "Active Directory" utilizam o sistema KERBEROS ..... _____

6. No Servidor de DNS um registo do tipo CNAME contém um endereço IPv4 ..... _____

7. No Windows Server 2008 um conjunto de domínios pode ser agrupado numa OU ("Organizational Unit") ..... _____

8. No WS2008 se o servidor DHCP funcionar em modo stateless não vai gerir os endereços IPv6 através do DHCP ..... _____

9. Entre os domínios pertencentes a uma mesma floresta ("FOREST") existe automaticamente uma relação de confiança ..... _____

10. O Active Directory usa SSL e certificados X509 de forma a garantir a autenticação e a confidencialidade ..... _____

11. No WS 2008 a entidade SITE é uma dos principais responsáveis pela replicação entre domínios ..... _____

12. O programa "dcpromo.exe" serve para configurar o serviço DHCP ..... _____

13. Um servidor WS2008 na qualidade de "domain member" não utiliza o Active Directory local ..... _____

14. Um "Read Only Domain Controller" (RODC) permite efectuar a validação das credenciais dos utilizadores ..... _____

15.O scope de um servidor de DHCP é composto por um nome, endereço inicial, endereço final, máscara e "default gateway" .... _____

16. No Servidor de DNS um registo do tipo CNAME contém registos de hosts do domínio ..... _____

17. O servidor de DNS tem normalmente um registo do tipo MX onde é indicado o servidor de correio electrónico para o domínio _____

18. No WS2008 podemos adicionar Roles como por exemplo encriptação de dados Bitlocker ..... _____

19. No WS2008 a gestão de uma Organizational Unit pode ser delegada ..... _____

20 O sistema de ficheiros FAT32 usa clusters mínimos de 16Kb. ..... _____

21. Uma Tree no Active Directory é um conjunto de controladores de domínio ..... _____

22. O RAID permite conjugar as versões 0 e 5, ou seja existem implementações com as funcionalidades de ambas as versões .. _____

23. No Active Directory a OU é uma subdivisão abaixo do nível de domínio ..... _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2011/2012 – Exame Teórico

Época Normal – 9/Fevereiro/2012

Número: _____ Nome: _____

Prova a realizar sem recurso a consulta. **LER COM ATENÇÃO**
Duração: 50 minutos.
Para cada uma das afirmações assinale com:
V - caso a considere totalmente verdadeira
F - caso a considere total ou parcialmente falsa
Se não tiver a certeza não responda, uma resposta errada anula meia resposta certa.
Bom trabalho.

1. O administrador de sistemas é o responsável pela elaboração de um plano de recuperação em caso de desastre ..... _____

2. O consumo energético é o custo operacional mais significativo num CPD ("Centro de Processamento de Dados") ..... _____

3. A virtualização implica um aumento da quantidade de "hardware" necessário no CPD ..... _____

4. A virtualização de servidores aumenta a eficácia na utilização da capacidade de processamento disponível ..... _____

5. Uma vantagem da virtualização de servidores é que facilita a implementação de metodologias de alta disponibilidade ..... _____

6. A virtualização de servidores exige necessariamente e virtualização de "storage" ..... _____

7. Um CPU de uma infra-estrutura virtual pode ser usado por vários servidores virtuais ..... _____

8. A virtualização de "storage" dificulta a realização de cópias e "mirroring" para CPDs remotos ..... _____

9. Uma SAN ("Storage Area Network") é uma rede que serve para interligar servidores que partilham os seus discos entre si ..... _____

10. As SAN "Fibre Channel" podem ser implementadas sobre "hardware" corrente como por exemplo comutadores "ethernet" .... _____

11. As SAN "Fibre Channel" de topologia "switched fabric" não garantem a ordem de entrega dos pacotes ..... _____

12. A taxa de transmissão usada nas SAN "Fibre Channel" é sempre inferior à das redes Ethernet Gigabit (1 Gbps) ..... _____

13. Para ligar um servidor a uma SAN "Fibre Channel" é necessário um "Fibre Channel HBA" ("Host Bus Adapter") ..... _____

14.As SAN iSCSI funcionam directamente sobre qualquer tipo de rede IP ..... _____

15.Um "target iSCSI" é normalmente um sistema de "storage" contendo discos ..... _____

16.Um "HBA iSCSI" garante uma performance superior a um "TOE card" ("TCP Offload Engine") ..... _____

17.Usando a tecnologia "Fibre Channel" torna-se impossível qualquer tipo de interligação de SANs via "Internet" ..... _____

18. Numa implementação de continuidade de negócio de categoria 2 ("Tier 2") são realizadas cópias de segurança ..... _____

19. A continuidade de negócio de categoria 7 ("Tier 7") assegura o arranque automático de servidores alternativos ..... _____

20. O RTO ("Recovery Time Objective") numa implementação "Tier 0" pode ser de vários dias ..... _____

21. O RTO de integridade das transacções é superior ao RTO de "hardware" ..... _____

22. A política de segurança deve ser acessível a todos os utilizadores e justificar as opções tomadas ..... _____

23. O controlo da temperatura no CPD é uma medida para minimizar consequências das falhas ..... _____

24. A política de segurança deve conter detalhes técnicos sobre a implementação dos mecanismos de segurança ..... _____

25. A disponibilidade dos sistemas é um parâmetro importante sob o ponto de vista de segurança ..... _____

26. Num "cluster" de servidores tolerante a falhas, a falha de um dos servidores não afecta os serviços prestados ..... _____

27. A forma mais eficaz de garantir a confidencialidade nas linhas de comunicação é controlar o acesso físico ..... _____

28. A implementação de mecanismos de tolerância a falhas obriga muitas vezes à duplicação do "hardware" ..... _____

29. O facto de um utilizador possuir credenciais de autenticação válidas, pode não garantir o acesso a um determinado recurso. _____

30. Num sistema AAA o processo de autorização ("authorization") verifica se o cliente/utilizador é quem diz ser ..... _____

31. O PIP ("Policy Information Point") armazena os dados relativos às credenciais dos utilizadores e permissões de acesso ..... _____

32. O PEP ("Policy Enforcement Point") é muitas vezes implementado através de um NAS ("Network Access Server") ..... _____

33. Na arquitectura AAA o PEP comunica directamente com o cliente e com o PDP ("Policy Decision Point") ..... _____

34. No protocolo CHAP ("Challenge Handshake Authentication Protocol") a "password" nunca é transmitida ..... _____

35. O protocolo LDAP ("Lightweight Directory Access Protocol") pode ser usado para comunicação entre o PDP e o PIP ..... _____

36. O protocolo EAP ("Extensible Authentication Protocol") permite o diálogo directo entre o cliente e o PDP ..... _____

37. Numa base de dados acessível por LDAP, um objecto pode pertencer apenas a uma classe do tipo "structural" ..... _____

38. Um RDN ("Relative Distinguished Name") pode ser repetido em ramos diferentes de um mesmo directório LDAP ..... _____

39. O cliente RADIUS ("Remote Authentication Dial In User Service") é normalmente o PEP/NAS ..... _____

40. O protocolo RADIUS exige que o protocolo de autenticação usado seja o CHAP ..... _____

41. As comunicações entre servidor e cliente RADIUS não são cifradas, por isso é obrigatório usar um canal seguro ..... _____

42. O sistema KERBEROS utiliza certificados de chave pública para garantia de autenticidade dos intervenientes ..... _____

43. As comunicações entre "principals" do sistema KERBEROS são cifradas com chaves que variam de sessão para sessão ..... _____

44. MITM ("man-in-the-middle") é um ataque de interposição que começa normalmente com um ataque do tipo "sniffing" _____

45. O DNS "spoofing" falseia as respostas do sistema DNS, fornecendo endereços IP errados para os nomes pedidos _____

46. Os ataques do tipo DoS ("Denial of Service") não podem ser eficazmente contrariados com ACL´s estáticas _____

47. A melhor defesa contra os ataques de "sniffing" é a segmentação com recurso a comutadores de rede _____

48. A maior diferença entre criptografia de chave simétrica e criptografia de chave pública é o tamanho da chave usada _____

49. Uma única aplicação de criptografia de chave pública não pode assegurar confidencialidade e autenticação _____

50. As funções "hash" ou "digest" têm como objectivo garantir a confidencialidade _____

51. O IPsec e o SSL/TSL são duas implementações de segurança alternativas para a camada de transporte (nível 4) _____

52. O DES usa chaves de 64 bits, por isso sob o ponto de vista de segurança, o 3DES é equivalente a usar chaves de 192 bits . _____

53. O tamanho do resultado produzido pelo MD5 ("Message Digest 5") é igual ao tamanho dos dados de entrada _____

54. Os algoritmos RC2, RC4 e RC5, são algoritmos de criptografia simétrica que suportam chaves de 128 bits _____

55. Uma configuração com rede externa, DMZ ("DeMilitarized Zone") e rede interna, exige pelo menos dois "firewalls" _____

56. Numa conexão TCP o tempo aguardado para a retransmissão de segmentos perdidos tem um valor sempre igual _____

57. O ataque do tipo TCP SYN é um ataque DoS que apenas afecta os serviços que usam o protocolo de transporte TCP _____

58. A marcação de pacotes através dos bits de precedência (TOS) é realizada nos cabeçalhos "ethernet" da rede local _____

59. A fragmentação e "Interleaving" de tráfego IP evita que pacotes grandes provoquem atrasos aos pacotes mais pequenos _____

60. Num "router" com filas prioritárias ("Priority Queuing"), os primeiros pacotes a entrar são sempre os primeiros a saírem _____

61. O "Priority Queuing" é mais nefasto para o tráfego de baixa prioridade do que o "Fair Queuing" ou o "Custom Queuing" _____

62. O dispositivo onde um pacote é classificado tem de ser o mesmo onde essa classificação é aplicada _____

63. O CAR ("Committed Access Rate") é uma implementação de WFQ ("Weight Fair Queuing") _____

64. O Hard QoS difere do Soft QoS pelo facto de haver uma reserva estática dos recursos _____

65. O RED ("Random Early Detection") não actua sobre o tráfego transportado pelo protocolo UDP _____

66. O WRED ("Weighted RED") elimina da fila pacotes de baixa prioridade mesmo antes da fila ficar cheia _____

67. O RSVP ("Resource Reservation Protocol") permite a definição negociada de parâmetros Hard QoS _____

68. O CAR pode simplesmente eliminar todos os pacotes que excedem um determinado limite de tráfego _____