Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2010/2011

Época Normal – 10/Fev/2011 - Exame Prático – 1ª Parte

Esta prova apenas pode ser realizada por alunos que faltaram às provas de avaliação realizadas durante a frequência.

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 protocolo OSPF ("Open Shortest Path First") …
   - ☐ utiliza o algoritmo de Dijkstra para calcular o caminho mais curto para cada destino.
   - ☐ o algoritmo de Dijkstra garante que o caminho encontrado é sempre o que atravessa menos links.
   - ☐ normaliza a topologia da rede entre todos os routers envolvidos.
   - ☐ o custo de um canal é directamente proporcional à sua largura de banda.
   - ☐ distingue os routers envolvidos sob três designações.
2. O protocolo EIGRP ("Enhanced Interior Gateway Routing Protocol") …
   - ☐ é um protocolo híbrido.
   - ☐ divide a topologia em duas zonas distintas, AS e área.
   - ☐ por omissão, é "classless".
   - ☐ é eficiente na ocupação da largura de banda.
   - ☐ em cada router guarda apenas a sua própria tabela de encaminhamento.
   - ☐ propaga as rotas para zonas distintas daquela em que está configurado.
3. Se uma ACL contiver apenas a regra "**deny tcp any host 194.65.3.5**" …
   - ☐ é redundante aplicá-la pois nenhum tráfego será permitido nesse interface e sentido.
   - ☐ permite que o tráfego ip atravesse esse interface.
   - ☐ só nega o tráfego tcp destinado ao equipamento com endereço 194.65.3.5.
   - ☐ só nega o tráfego tcp com origem no equipamento com o endereço 194.65.3.5.
   - ☐ o tráfego icmp pode atravessar esse interface nesse sentido.
4. Uma ACL definida num router …
   - ☐ é automaticamente aplicada em ambos os sentidos de todos os interfaces activos.
   - ☐ para o mesmo interface, só pode ser aplicada num sentido, não nos dois.
   - ☐ pode ser aplicada apenas a um interface, não a mais do que um.
   - ☐ só será utilizada se aplicada a um interface.
   - ☐ é obrigatoriamente para filtragem de tráfego.

5. O NAT ("Network Address Translation") …

☐ pode ser utilizado para fazer balanceamento de carga para uma server farm.

☐ serve para funcionalidades inbound e outbound.

☐ "Bidireccional NAT" e "Twice NAT" implicam um servidor DNS com extensões ALG.

☐ "Twice-NAT" serve para permitir a interligação entre dois sistemas com endereços privados.

6. A criptografia …

☐ pode ser em bloco ou contínua.

☐ em bloco é menos eficiente na aplicação.

☐ em bloco pode ser periódica.

7. O algoritmo de encriptação …

☐ DES utiliza uma chave de 56 bits.

☐ 3DES obriga à existência de 3 chaves diferentes.

☐ AES é irreversível.

8. O método de autenticação Kerberos …

☐ tem uma arquitectura constituída por três elementos.

☐ possui um servidor (servidor Kerberos) que verifica a identidade dos actores e fornece os bilhetes para acesso.

☐ o servidor de aplicações partilha uma chave secreta com o servidor Kerberos.

9. O par endereço IP/WILDCARD "190.10.0.0 1.0.8.128" …

☐ permite-nos concluir que se trata obrigatoriamente de uma rede IP "classless".

☐ abrange 16 endereços.

☐ inclui o endereço 191.10.8.0.

☐ não é válido por conter um wildcard inválido.

10. A regra de ACL "**permit 140.20.0.0 0.20.255.255**" …

☐ bloqueia o tráfego com origem na rede 140.0.0.0/16.

☐ não bloqueia o tráfego com origem na rede 140.20.0.0/16.

☐ só é aplicável no contexto de uma ACL "extended".

11. Uma ACL constituída apenas pela regra: "**permit tcp any host 200.10.0.1 eq www**" …

☐ não permite nenhum tipo de tráfego IP.

☐ permite apenas tráfego www com destino ao endereço 200.10.0.1.

☐ não permite nenhum tipo de tráfego UDP.

☐ permite todo o tráfego TCP com destino ao endereço 200.10.0.1.

12. Uma ACL "extended" permite utilizar como critério …

☐ a data/hora.

☐ o número de porto de destino das ligações TCP.

☐ o endereço IP de origem.

13. Para permitir apenas o tráfego com origem na rede 197.120.0.0/23, pode ser usada a ACL …

☐ "access-list 102 permit ip 197.120.0.0 0.0.1.255 any".

☐ "access-list 50 permit host 197.120.0.0".

☐ "access-list 12 permit 197.120.0.0 0.0.1.255".

☐ "access-list 14 permit network 197.120.0.0".

14. Uma ACL constituída apenas pela regra "**permit icmp any 170.1.1.1 0.2.0.0**" …

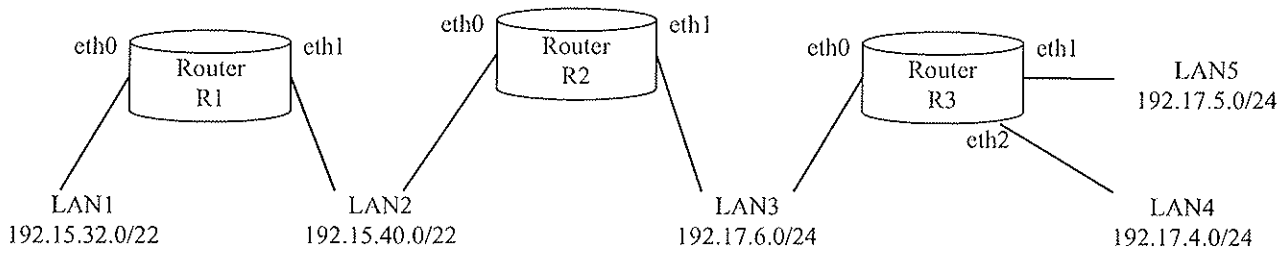
☐ permite tráfego ICMP destinado ao endereço 170.3.1.1.

☐ é uma access list do tipo extended.

☐ não permite tráfego TCP nem UDP.

Grupo 2 (12 valores)

Observe o seguinte conjunto de redes:



Pretende-se atingir os seguintes objectivos:

LAN1: apenas pode aceder à rede LAN5.

LAN2: apenas pode aceder às redes LAN1 e LAN3, mas os primeiros 8 endereços da rede (.1 a .8) podem aceder a tudo.

LAN3: apenas pode aceder à LAN1 e LAN2, também pode aceder aos endereços 192.17.5.16 e 192.17.5.18 da LAN5, exclusivamente para tráfego TCP destinado ao serviço HTTP.

LAN4: pode aceder a tudo, mas apenas para tráfego UDP.

LAN5: os endereços impares podem aceder a tudo, os endereços pares não podem aceder a nada.

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

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 – 2010/2011

Exame Teórico de Época Normal – 10/Fev/2011

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. As funções do administrador de sistemas informáticos não incluem o planeamento e projecto da infra-estrutura ..... _____

2. Na actualidade, os custos operacionais dos servidores superam claramente os custos de aquisição..... _____

3. A virtualização de servidores reduz os custos operacionais de consumo energético..... _____

4. A virtualização de servidores aumenta os custos operacionais de gestão e administração..... _____

5. Duas máquinas virtuais residentes numa mesma plataforma, não podem usar sistemas operativos de tipos diferentes..... _____

6. Numa plataforma de virtualização um mesmo CPU pode ser usado por várias máquinas virtuais ..... _____

7. A virtualização de "storage" permite que as unidades de disco sejam usadas simultaneamente por vários servidores ..... _____

8. Numa SAN ("Storage Area Network") os sistemas operativos usam os dispositivos remotos como se fossem discos locais ..... _____

9. Uma desvantagem das SAN é que não permitem a transferência de dados para localizações remotas não locais..... _____

10. Os protocolos usados nas SAN são os protocolos normais de partilha de ficheiros como por exemplo o SMB/CIFS ..... _____

11. Uma SAN "Fibre Channel" pode ser implementada sobre equipamento de rede "corrente", como por exemplo "Ethernet"..... _____

12. Uma SAN "Fibre Channel" de topologia ponto a ponto (FC-P2P) suporta um máximo de três nós em "full-duplex"..... _____

13. O protocolo iSCSI permite ao servidor a utilização de unidades de disco da SAN como se fossem discos SCSI locais..... _____

14.O iSCSI é o único protocolo de SAN que usa como transporte a pilha de protocolos TCP/IP ..... _____

15. Numa implementação de continuidade de negócio de categoria 5 ("Tier 5") ou superior as cópias devem ser feitas em disco . _____

16. O RTO ("Recovery Time Objective") de "hardware" e dados é superior ao RTO de integridade de transacções ..... _____

17. A autenticação serve para determinar se um dado utilizador tem permissão para usar um dado recurso..... _____

18. Num sistema AAA é o PDP ("Policy Decision Point") que toma a decisão de permitir ou não um dado acesso..... _____

19. Quando o PDP obtém as credenciais dos utilizadores de um directório LDAP, este é o PIP ("Policy Information Point") ..... _____

20. O protocolo de autenticação CHAP tem como grande vantagem nunca transmitir a "password" ..... _____

21. A autenticação por certificado digital é uma técnica de chave partilhada ..... _____

22. A autorização é normalmente verificada depois da autenticação bem sucedida ..... _____

23. Numa base de dados LDAP, um objecto não pode pertencer a mais do que uma classe "structural" ..... _____

24. A nomeação da base LDAP deve seguir obrigatoriamente a recomendação X.500: regiões geográficas e países ..... _____

25. O protocolo RADIUS ("Remote Authentication Dial In User Service") garante a comunicação entre o PDP e o PIP ..... _____

26. A comunicação entre o NAS ("Network Access Server") e o servidor RADIUS é cifrada com uma chave pré-partilhada ..... _____

27. O protocolo RADIUS não suporta contabilização ("accounting") ..... _____

28. O sistema KERBEROS assegura não apenas a autenticação, mas também a privacidade das comunicações ..... _____

29. As chaves de sessão ("session-key") do sistema KERBEROS são transmitidas simultaneamente ao serviço e ao cliente ..... _____

30. A autenticação via KERBEROS exige que esteja instalado na rede um KDC ("Key Distribution Center") ..... _____

31. O nível de risco de ataque a uma empresa com utilizadores especialistas em informática é mais elevado ..... _____

32. A política de segurança de uma organização deve especificar as consequências do seu incumprimento ..... _____

33. A política de segurança aborda a confidencialidade, integridade e controlo de acesso, mas não a disponibilidade ..... _____

34. Os detalhes técnicos da implementação dos mecanismos de segurança não devem ser incluídos na política de segurança ... _____

35. A manutenção de cópias de segurança actualizadas é um meio de proporcionar tolerância a falhas ..... _____

36. A monitorização / detecção de falhas não tem qualquer relevância para o caso de falhas de confidencialidade ..... _____

37. A utilização de redes locais comutadas (com "switches") resolve o problema da confidencialidade das comunicações ..... _____

38. Os ataques "Packet Sniffing" são ataques do tipo DoS ("Denial of Service") ..... _____

39. O ataque "DNS Spoofing" pode ser implementado com a técnica MITM ("man-in-the-middle") ..... _____

40. Os ataques de "IP Spoofing" externos podem ser evitados através de ACLs estáticas no "router" de ligação ao exterior ..... _____

41. Os ataques do tipo "SYN Flood" são ataques DoS que afectam de igual modo os serviços TCP e UDP ..... _____

42. Os ataque DoS podem ser impedidos através de um "firewall" estático ..... _____

43. Na criptografia de chaves simétricas o algoritmo de encriptação tem de ser mantido secreto ..... _____

44. Em criptografia de chaves públicas o emissor de uma mensagem cifrada não tem a capacidade de a decifrar ..... _____

45. A criptografia de chaves públicas nunca pode ser usada para implementar autenticação, apenas confidencialidade ..... _____

46. As funções de "hashing" obrigam a que os dados de entrada sejam divididos em blocos de dimensão adequada à função..... _____

47. As funções de "hashing" devem produzir resultados iguais para dados de entrada iguais ..... _____

48. O protocolo HTTPS opera sobre o protocolo SSL/TLS ..... _____

49. A dificuldade em "quebrar" uma chave criptográfica por "força bruta" não depende do tempo de execução do algoritmo ..... _____

50. Os algoritmos criptográficos com maior longevidade são aqueles que suportam um aumento do tamanho da chave ..... _____

51. A DZM ("DeMilitarized Zone") pode ser ligada à rede dos utilizadores locais por um comutador Ethernet ..... _____

52. O ataque através da numeração de sequência TCP tem como objectivo estabelecer ligações TCP com "IP Spoofing"..... _____

53. Os registos de actividades ("audit records") são criados manualmente pelo administrador ..... _____

54. As filas de espera dos "routers" são o local onde a QoS ("Quality of Service") é posta em prática..... _____

55. Os bits de precedência do cabeçalho IPv4 ("TOS") são úteis para marcar os pacotes à entrada da rede..... _____

56. A QoS só tem efeito prático quando a fila de espera do "router" fica cheia ..... _____

57. A fragmentação e "Interleaving" de tráfego IP é particularmente útil em "links" de débito muito elevado..... _____

58. Na gestão de fila "Priority Queuing" um pacote só é retransmitido se não existe tráfego de prioridade mais elevada..... _____

59. No algoritmo "Custom Queuing" nunca é processado mais do que um pacote da mesma fila sem passar à fila seguinte ..... _____

60. A precedência IP nunca pode ser usada como critério de classificação numa implementação "Weight Fair Queuing" ..... _____

61. No algoritmo "Weight Fair Queuing" o número de filas existentes deve ser sempre dezasseis ..... _____

62. O CAR ("Committed Access Rate") é uma técnica HARD QoS ..... _____

63. A técnica RED ("Random Early Detection") entra em acção quando a fila de espera do "router" fica cheia ..... _____

64. O "TCP Slow Start" é uma funcionalidade de controlo de fluxo do protocolo TCP ..... _____

65. O RED afecta indirectamente os tempos de retransmissão dos segmentos (pacotes) TCP ..... _____

66. O CAR permite associar a cada tipo de tráfego uma taxa máxima que não será nunca ultrapassada..... _____

67. O WRED ("Weighted RED") pode ser usado pelo CAR através da marcação dos pacotes ..... _____

68. O RSVP ("Resource Reservation Protocol") permite a um nó solicitar à rede determinadas condições QoS ..... _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2010/2011

Época Normal – 10/Fev/2011 - Exame Prático – 2ª Parte

Esta prova apenas pode ser realizada por alunos que faltaram às provas de avaliação realizadas durante a frequência.

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. Todas as distribuições Linux são gratuitas ..... _____

2. "/dev/hdd1", "/dev/hdd2" e "/dev/hdd3" são várias partições de um mesmo disco ..... _____

3. A partição SWAP nunca pode ser mais pequena do que a partição ROOT (raiz) ..... _____

4. As partições num disco têm de estar ordenadas da mais pequena para a maior ..... _____

5. As tabelas de partições dos discos encontram-se armazenadas no BIOS do computador ..... _____

6. A tabela de partições de um disco SATA tem uma estrutura totalmente diferente da de um disco SCSI ..... _____

7. Num sistema Unix (ex.: Linux), as várias partições de um disco são acessíveis através de diferentes "letras de drive" ..... _____

8. As áreas de utilizador ("homes") nunca podem ficar localizadas na partição RAIZ ..... _____

9. Na formatação de uma partição pode ajustar-se o tamanho de bloco para atingir os objectivos pretendidos ..... _____

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

11. Para cada utilizador definido no ficheiro "/etc/passwd" o UID tem de ser sempre igual ao GID ..... _____

12. Os comandos "useradd" e "usermod" apenas funcionam para utilizadores que estão definidos no ficheiro "/etc/passwd" ..... _____

13. O NSS ("Name Service Switch") permite a integração entre sistemas, desde que sejam todos do tipo UNIX ..... _____

14. Toda a configuração dos vários módulos NSS está guardada no ficheiro "/etc/nsswitch.conf" ..... _____

15. O NSS e o PAM ("Pluggable Authentication Modules") são dois sistemas alternativos que fazem exactamente o mesmo ..... _____

16. O comando "chown" permite alterar o proprietário de um ficheiro ou directório ..... _____

17. O nome da pasta HOME de cada utilizador é sempre igual ao nome do utilizador ..... _____

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

19. Todos os ficheiros executados durante o arranque da SHELL encontram-se na pasta "/etc" .....

20. O comando "umask" serve para definir as permissões da pasta HOME do utilizador .....

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

22. Para configurar o endereço IP de uma interface de rede pode ser usado o comando "ip" ou o comando "ifconfig" .....

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

24. Uma interface de rede nunca pode ter mais do que um endereço IPv4 associado a ela .....

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

26. A gestão de interfaces VLAN utiliza o comando "vconfig".....

27. Os servidores DHCP utilizam como transporte o protocolo UDP.....

28. O "Internet Daemon" (INETD/XINETD) é um servidor DHCP .....

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

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

31. No IPTABLES, quando um pacote não corresponde a nenhuma regra da cadeia é sempre descartado (DROP) .....

32. Um "script" é um ficheiro de texto que deve ter a permissão de execução activa .....

33. A primeira linha de um "shell script" é sempre "#!/bin/bash" .....

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

35. Um certificado de chave pública diz-se auto-assinado quando SUBJECT=ISSUER.....

36. Para criar um certificado de chave pública com o comando "openssl", basta uma única invocação do comando.....

37. O SYSTEM LOGGER ("syslog") apenas pode registar eventos que ocorram na mesma máquina onde se encontra.....

38. O nível de gravidade de um evento ("severity", "priority" ou "level") é definido pela aplicação que usa o serviço "syslog" .....

39. Os ficheiros utmp e wtmp não são criados pelo SYSTEM LOGGER.....

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

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

42. Os comandos "dump" e "restore" suportam cópias incrementais.....

43. A grande vantagem das unidades de fita é rapidez da operação de restauro .....

2ª Parte – Administração de servidores Windows

1. No "Active Directory" o Schema define apenas os atributos dos objectos a armazenar no sistema _____

2. O WS2008 em modo Server Core não tem suporte a virtualização _____

3. O restauro de um ficheiro a partir de um backup incremental obriga ao restauro de todas as versões existentes _____

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

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

6. O "Network Load Balancing" permite adicionar novos servidores sempre que necessário. _____

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

8. O Controlador de Domínio não tem obrigatoriamente instalado localmente um servidor de DNS _____

9. Com os "default password requirements" activos, as passwords tem no mínimo 6 caracteres _____

10. Os ficheiros públicos do domínio são armazenados numa zona chamada SYSVOL _____

11. No Active Directory, o Global Catalog tem informação acerca dos servidores de domínio _____

12 O Sistema de ficheiros NTFS não suporta file system journaling _____

13 O Active Directory não suporta certificados X509. _____

14. Uma TREE no Active Directory é um conjunto de um ou mais domínios _____

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

16. O Servidor Controlador de Domínio é conhecido na rede pelo nome Fully Qualified Domain Name do domínio _____

17. Os servidores de DHCP no WS2008 não funcionam em modo stateless _____

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

19. No WS2008 o servidor de Terminal Services é uma feature _____

20 O Servidor de DNS do WS 2008 permite adição manual de aliases através da indicação no campo TYPE do valor CNAME _____

21. O WS2008 não permite executar aplicações remotas sem trazer todo ambiente de trabalho _____

22. Com o Hyper-V podemos emular várias máquinas virtuais com vários sistemas operativos _____

23. No WS2008 a instalação em modo Server Core permite que o servidor seja domain controller mas não servidor de DNS _____