Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

# *Administração de Sistemas – 2010/2011 – Exame Teórico*

## *Época Especial de Setembro – 05/Setembro/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. A gestão da infra-estrutura de rede é normalmente da responsabilidade do administrador de sistemas ..... _____

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

3. Uma das vantagens da virtualização de servidores é a redução do custo de administração ..... _____

4. A virtualização de servidores permite um melhor aproveitamento da capacidade de processamento dos CPUs ..... _____

5. Cada tipo de plataforma de virtualização apenas permite um tipo de sistema operativo nas respectivas máquinas virtuais ..... _____

6. A virtualização de servidores apenas é possível em conjunto com a virtualização de "storage" ..... _____

7. As SAN ("Storage Area Network") exigem que o "hardware" de rede use fibra óptica ..... _____

8. As SAN suportam discos "Fibre Channel" e também podem suportar discos SATA ..... _____

9. Uma desvantagem das SAN é que um disco físico nunca pode ser utilizado por mais do que um único servidor ..... _____

10. Uma mesma SAN nunca pode ser partilhada por vários servidores ..... _____

11. Uma SAN "Fibre Channel" pode ser constituída apenas por um cabo, num topologia ponto-a-ponto ..... _____

12. As SAN "Fibre Channel" baseadas em comutadores ("switches") devem possuir ligações redundantes ..... _____

13. As SAN "Fibre Channel" utilizam como protocolo de transporte o TCP ..... _____

14. O iniciador iSCSI é o servidor que vai utilizar os discos residentes na SAN ..... _____

15. Os protocolos iSCSI e o iFCP permitem a ligação directa de SANs através da "Internet" ..... _____

16. Numa implementação de continuidade de negócio de categoria 0 ("Tier 0") são realizadas cópias de segurança ..... _____

17. O RTO ("Recovery Time Objective") é menor numa implementação "Tier 5" do que numa implementação "Tier 3" ..... _____

18. O RTO de integridade das transacções é sempre maior do que o RTO de "hardware" ..... _____

19. As credenciais de autenticação de um utilizador devem ser iguais nos vários serviços da organização ..... _____

20. Um sistema AAA começa por verificar a autorização e de seguida verifica a autenticação do cliente/utilizador ..... _____

21. O PDP ("Policy Decision Point") é o responsável pelo armazenamento das credenciais dos utilizadores ..... _____

22. O protocolo de autenticação PAP ("Password Authentication Protocol") só deve ser usado em canais seguros ..... _____

23. O PIP ("Policy Information Point") é o responsável pela tomada de decisão de autorização ..... _____

24. Numa base de dados LDAP todos os registos (objectos) têm a mesma estrutura (campos/atributos) ..... _____

25. O protocolo LDAP foi optimizado para operações de leitura ..... _____

26. O RDN de um objecto numa base de dados LDAP tem de ser um nome único em toda a base de dados ..... _____

27. O acesso de leitura a uma base de dados LDAP pode ser realizado sem qualquer credencial de acesso ..... _____

28. O protocolo RADIUS ("Remote Authentication Dial In User Service") é usado na comunicação entre o PEP e o PDP ..... _____

29. O protocolo RADIUS ("Remote Authentication Dial In User Service") usa como transporte o protocolo UDP ..... _____

30. O servidor RADIUS é uma implementação de centro de distribuição de chaves KDC para o sistema KERBEROS ..... _____

31. No sistema KERBEROS apenas o KDC conhece as chaves dos PRINCIPAL participantes ..... _____

32. As comunicações entre elementos do sistema KERBEROS são cifradas com chaves simétricas ..... _____

33. A política de segurança é um documento que deve estar acessível a todos os utilizadores do sistema informático ..... _____

34. O tipo de actividade e características da organização condicionam o potencial de ataque ao respectivo sistema informático .. _____

35. Entre outros elementos, a política de segurança deve indicar as consequências da sua violação ..... _____

36. A manutenção de cópias de segurança actualizadas é um mecanismo de tolerância a falhas ..... _____

37. Para reduzir as consequências das falhas é fundamental ter uma detecção de falhas eficiente ..... _____

38. É possível implementar mecanismos de tolerância a falhas de confidencialidade ..... _____

39. Os ataques do tipo "Packet Sniffing" são evitados se forem usados comutadores ("switches") ethernet ..... _____

40. Os ataques tipo "Spoofing" são passivos, ou seja, não produzem qualquer alteração na informação que circula na rede ..... _____

41. A melhor defesa contra os ataques de "Sniffing" é o recurso à criptografia ..... _____

42. Os ataques do tipo DoS ("Denial of Service") são um caso particular de ataque MiTM ("man-in-the-middle") ..... _____

43. A protecção contra ataques do tipo DoS ("Denial of Service") exige um firewall dinâmico ("stateful packet filter") ..... _____

44. A criptografia de chave pública tem como principal vantagem a facilidade no processo de distribuição de chaves ..... _____

45. Quando é usada criptografia de chave pública, o emissor de uma mensagem cifrada não tem a capacidade de a decifrar..... _____

46. O algoritmo DES utiliza chaves secretas de 128 bits ..... _____

47. Os algoritmos MD5 e SHA-1 são exemplos de funções de "hashing" usadas actualmente ..... _____

48. O IPsec é uma implementação de segurança que funciona na camada de transporte (nível 4) ..... _____

49. O resultado de uma função de "hashing" ("hash code") pode ser usado para obter a mensagem original ..... _____

50. O algoritmo de cifragem RC4 é um dos mais usados na actualidade..... _____

51. O protocolo HTTPS usa o IPsec..... _____

52. A DZM ("DeMilitarized Zone") deve estar separada por um "firewall" da rede interna onde se encontram os utilizadores ..... _____

53. O número de sequência inicial numa ligação TCP é completamente aleatório ..... _____

54. Os registos de actividades ("audit records") permitem a implementação de tolerância a falhas ..... _____

55. A implementação de QoS obriga sempre à marcação de pacotes através dos bits de precedência (TOS)..... _____

56. A fragmentação e "Interleaving" de tráfego IP é uma técnica HARD QoS ..... _____

57. Num "router" os primeiros pacotes a entrar são sempre os primeiros a sair ..... _____

58. Na gestão de fila "Priority Queuing" um pacote de prioridade mais elevada é retransmitido antes dos restantes ..... _____

59. No algoritmo "Weight Fair Queuing" existem apenas duas filas de espera..... _____

60. Um pacote pode ser marcado para mais tarde ter um tratamento diferenciado de acordo com a marcação..... _____

61. A implementação "Weight Fair Queuing" dá prioridade absoluta ao tráfego mais importante, ignorando o restante ..... _____

62. O RED ("Random Early Detection") aproveita as funcionalidades de controlo de fluxo do protocolo TCP..... _____

63. O CAR ("Committed Access Rate") define limites para a ocupação de largura de banda através de uma "rate policy" ..... _____

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

65. O RSVP ("Resource Reservation Protocol") permite a um nó negociar as características QoS pretendidas..... _____

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

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

68. Com "Soft QoS" nunca se pode ter garantias de largura de banda absoluta disponível para uma aplicação ..... _____