Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2012/2013 – Exame Teórico

Época Normal – 7/Fevereiro/2013

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 salvaguarda de sistemas e dados ("backup") _____
2. O CPD ("Centro de Processamento de Dados") é o local de trabalho permanente do administrador de sistemas e operadores. _____
3. A virtualização de "hardware" permite criar novos servidores sem aumentar a quantidade de equipamento _____
4. A virtualização de servidores reduz os custos, mas aumenta a complexidade das tarefas de administração _____
5. A virtualização de servidores facilita a recuperação em caso de desastre ("Disaster Recovery") _____
6. "SMB/CIFS" e "NFS" são exemplos de protocolos usados para implementar a virtualização de "storage" _____
7. O único tipo de SAN ("Storage Area Network") que permite a utilização da pilha TCP/IP é o iSCSI _____
8. A topologia atualmente mais usada nas SAN "Fibre-Channel" é o "Switched fabric" _____
9. Nas implementações iSCSI, a opção de ligação que garante a melhor performance é o TOE ("TCP/IP Offload Engine") _____
10. O FCoE ("Fibre Channel over Ethernet") não utiliza a pilha de protocolos TCP/IP _____
11. Para interligar duas SAN "Fibre Channel" através da "internet" pode ser usado o FCIP ("Fibre Channel over IP") _____
12. O parâmetro MTBF ("Mean Time Between Failures") e o parâmetro FIT ("Failures In Time") não têm qualquer relação entre si _____
13. O MTBF de um sistema redundante é aproximadamente igual ao somatório dos MTBF dos seus componentes _____
14. Um sistema de alta disponibilidade do tipo "três noves" tem uma disponibilidade superior a 99% _____
15. Um sistema designa-se "fail safe" se a falha de um componente não provoca qualquer degradação do desempenho _____
16. Uma "common-mode fault" é uma falha que afeta apenas um dos componentes de um sistema redundante _____
17. O sistema RAID 1 assegura a disponibilidade desde que pelo menos um dos discos se mantenha operacional _____
18. Um dos objetivos do DRP ("Disaster Recovery Plan") é reduzir o RTO ("Recovery Time Objective") _____

19. Num sistema de "storage" com "mirroring" síncrono o RPO ("Recovery Point Objective") é nulo ..... _____

20. O DRP é um dos elementos importantes que constituem o BCP ("Business Continuity Plan") ..... _____

21. O plano de "backup/restore" afeta o RTO, mas não RPO ..... _____

22. A utilização de cópias incrementais não favorece o valor do RTO ..... _____

23. A continuidade de negócio de categoria 6 ("Tier 6") pressupõe valores de RTO entre 24 e 48 horas ..... _____

24. Nas cifras de chave simétrica para desencriptar é necessário usar a mesma chave que foi usada na encriptação ..... _____

25. O "não repúdio" pode ser facilmente garantido através de uma cifra de chave simétrica ..... _____

26. Os certificados de chave pública são usados para distribuir chaves secretas de cifras de chave simétrica ..... _____

27. As funções "hash" são úteis para garantir a confidencialidade de dados ..... _____

28. O algoritmo RSA ("Ron Rivest, Adi Shamir e Leonard Adleman") é uma cifra de chave simétrica ..... _____

29. Uma aplicação do PAP ("Password Authentication Protocol") garante a autenticidade de apenas um dos intervenientes ..... _____

30. Num sistema AAA, só depois de validada a autenticação ("authentication") é que é verificada a autorização ("authorization"). _____

31. Num sistema AAA, é o PEP ("Policy Enforcement Point") que toma a decisão de permitir ou não o acesso ..... _____

32. O protocolo RADIUS é usado nas comunicações entre o PEP e o PIP ("Policy Information Point") ..... _____

33. Com o EAP ("Extensible Authentication Protocol"), o PEP pode funcionar em modo "pass-through" ..... _____

34. Uma implementação PIP muito usada é um servidor LDAP ("Lightweight Directory Access Protocol") ..... _____

35. O "Active Directory" da "MicroSoft" é uma implementação LDAP ..... _____

36. Numa base de dados LDAP um objecto nunca pode pertencer a mais do que uma classe estrutural ..... _____

37. Numa base de dados LDAP vários objetos podem ter o mesmo RDN ("Relative Distinguished Name") ..... _____

38. O sistema KERBEROS só pode ser usado por quem tiver uma chave pré-partilhada com o AS ("Authentication Server") ..... _____

39. A utilização do sistema KERBEROS sem pré-autenticação não garante a autenticidade nas comunicações entre os "principal" _____

40. No "Active Directory" da Microsoft, o KERBEROS usa a transferência de relações de confiança ("transitive trust") ..... _____

41. No TLS ("Transport Layer Security") quem decide a versão que vai ser usada é o servidor ..... _____

42. O TLS exige sempre a utilização de uma cifra de chave assimétrica com troca de certificados de chave pública ..... _____

43. Para um pacote com determinadas caraterísticas, um "firewall" do tipo "packet-filter" tem sempre o mesmo comportamento . _____

44. A funcionalidade "stateful packet inspection" (SPI) não está presente nos "firewalls" estáticos ..... _____

45. Para implementar uma arquitetura de rede com "Intranet", "DMZ" e "Internet" são necessários pelo menos dois "firewalls" ..... _____

46. Os ataques do tipo "sniffing" podem ser combatidos de forma eficaz com recurso a "firewalls" ..... _____

47. O ataque ARP "spoofing" pode ser usado como ponto de partida para um ataque MiTM ("Man-in-the-middle") ..... _____

48. O ataque "SYN flood" é um ataque do tipo DoS ("Denial of Service"), mas apenas pode ser aplicado a serviços TCP ..... _____

49. O ataque aos números de sequência TCP tem como objetivo a utilização de "spoofing" de endereços IP ..... _____

50. Tal como o protocolo TCP, o protocolo RTP ("Real-time Transport Protocol") corrige automaticamente os erros ..... _____

51. A compressão de cabeçalhos ("header compression") é mais vantajosa para pacotes de grande dimensão ..... _____

52. O LFI ("Link Fragmentation and Interleaving") garante que os pacotes maiores são retransmitidos mais rapidamente ..... _____

53. Quando a rede fica congestionada, o TCP aumenta automaticamente o RTO ("Retransmission TimeOut") ..... _____

54. O "Congestion avoidance" e "Slow Start" são mecanismos de controlo de fluxo regulados pelo recetor dos dados ..... _____

55. O RED ("Random Early Detection") permite aos nós intermédios evitaram o "TCP global synchronization" ..... _____

56. O NBAR ("Network Based Application Recognition") serve para classificar o tráfego através dos endereços de origem ..... _____

57. Os bits DSCP ("differentiated services codepoint") são incompatíveis com os bits de precedência TOS ..... _____

58. A utilização de 100% da capacidade das ligações é garantida quer se use HARD QoS, quer se use SOFT QoS ..... _____

59. Na gestão de filas "Custom Queueing" (CQ) uma fila só é atendida quando as de prioridade superior estiverem vazias ..... _____

60. A gestão de filas do tipo "Fair Queueing" (FQ) trata de forma igual as várias filas criadas ..... _____

61. No "Weighted RED" (WRED) o tráfego é sempre tratado de forma diferenciada, seja qual for o estado da fila de saída ..... _____

62. No RSVP ("Resource Reservation Protocol") os pedidos de reserva de recursos são efectuados pelos emissores dos dados. _____

63. O IPsec em "Transport mode" não garante a confidencialidade de todo o pacote IP original ..... _____

64. O "IP Encapsulating Security Payload" (ESP) pode garantir a autenticidade/integridade e a confidencialidade ..... _____

65. O protocolo IKE ("Internet Key Exchange Protocol") estabelece SAs ("Security Associations") entre nós ..... _____

66. O suporte de ESP é obrigatório em todos os nós IPsec ..... _____

67. O protocolo IKE usa o algoritmo "Diffie-Hellman" para criar todas as ("Security Associations") ..... _____

68. O "Layer 2 Tunneling Protocol" (L2TP) possui mecanismo de autenticação e confidencialidade adequados a uma VPN ..... _____