Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2013/2014 – Exame Teórico

Exame de época de recurso e melhoria – 15 de fevereiro de 2014

Número: _____ Nome: _____

Prova a realizar sem recurso a consulta. LER COM ATENÇÃO
Duração: 55 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 nunca deve acumular a função de administrador de redes, mas é o responsável pela formação dos operadores ____
2. O número de pessoas com possibilidade de acesso físico ao CPD ("Centro de Processamento de Dados") deve ser o mais limitado possível ____
3. No CPD ficam concentrados todos os sistemas de processamento e armazenamento e também todos os equipamentos ativos da infra-estrutura de rede ____
4. É vantajoso que o acesso físico ao CPD seja apenas possível através do local de trabalho dos administradores e operadores ____
5. A virtualização de "hardware" permite reduzir a quantidade de "hardware" físico necessário para implementar as mesmas funções ____
6. Com a virtualização é possível criar um novo servidor virtual e instalar o respetivo sistema operativo sem aceder fisicamente ao CPD ____
7. Numa SAN ("Storage Area Network"), um único sistema de "storage" pode ser usado para fornecer discos lógicos a vários servidores ____
8. Uma vantagem da virtualização de "storage" é que o "backup" e "mirroring" podem ser realizados sem a intervenção do servidor que usa os discos lógicos ____
9. Um "initiator" iSCSI pode usar "targets" do tipo FCoE ("Fibre Channel over Ethernet"), mas não "targets" do tipo FCP ("Fibre Channel Protocol") ____
10. Quando uma SAN é implementada sobre "ethernet", é fundamental assegurar a redundância, por exemplo com recurso ao STP ("Spanning Tree Protocol") ____
11. Um HBA ("Host Bus Adapter") "Fibre Channel" pode ser diretamente ligado por um cabo a outro HBA "Fibre Channel" ____
12. O parâmetro MTTR ("Mean Time To Repair") está fortemente dependente do DRP ("Disaster Recovery Plan") ____
13. Num sistema, aumentar o número de componentes redundantes provoca uma diminuição do valor do MTBF ("Mean Time Between Failures") do conjunto ____
14. Se conseguirmos diminuir o MTTR, conseguimos aumentar a disponibilidade do sistema ____
15. Num sistema "fail safe", em caso de falha os serviços continuam disponíveis como se a falha não tivesse ocorrido ____
16. Uma forma de eliminar um SPOF ("Single Point Of Failure") é tornar o componente que a provoca redundante ____
17. Com cinco discos configurados em RAID 1, se três dos discos falharem simultaneamente, o conjunto ainda se mantém operacional ____
18. Se uma falha A tem uma probabilidade de ocorrer superior a uma falha B, então necessariamente o risco da falha A é superior ao da falha B ____
19. Após a falha de um sistema espera-se que ele seja recuperado num periodo de tempo inferior ao RTO ("Recovery Time Objective") ____
20. O BCP ("Business Continuity Plan") tem como único objetivo definir a forma como a infra-estrutura informática deve manter o seu funcionamento ____
21. O plano de contingência ("Contingency Plan") é ativado apenas em situações nas quais a recuperação do sistema a curto prazo não é possível ____
22. Um plano de "backup/restore" baseado apenas em cópias integrais nunca pode garantir um RPO ("Recovery Point Objective") de 24 horas ____
23. Se a operação de "backup" demora duas horas, nunca será possível garantir um RPO inferior a duas horas ____
24. O "mirroring" síncrono de discos garante um RPO e um RTO nulos, o "mirroring" assíncrono garante apenas o RPO nulo ____
25. A "Politica de segurança" é um documento que deve ser do conhecimento dos administradores, não dos utilizadores "normais" ____
26. Para garantir a autenticação com uma cifra assimétrica (chave pública) o emissor tem de cifrar com a chave privada, mas não garante a confidencialidade ____
27. Se "quebrar" uma chave por força bruta demora 5000 horas, então se a chave tivesse mais um bit demoraria 10000 horas ____
28. Num certificado de chave pública quando o proprietário ("owner") e igual ao emissor ("issuer"), diz-se que o certificado é auto assinado ____
29. Na aplicação de uma função "hash", se for alterado apenas um bit nos dados de entrada então o resultado também terá apenas um bit alterado ____
30. Uma assinatura digital deve garantir duas propriedades: autenticação e "não repúdio". Não garante a confidencialidade ____
31. O protocolo PAP ("Password Authentication Protocol") utilizado isoladamente garante a autenticidade do utilizador, mas não a autenticidade do serviço ____

32. As OTP ("One Time Password") podem ser geradas pelos serviços e transmitidas aos utilizadores para maior segurança em determinadas operações ____

33. Nos sistemas AAA, em alguns casos o PEP ("Policy Enforcement Point") tem a designação NAS ("Network Access Service") ____

34. O PDP ("Policy Decision Point") recorre ao PIP ("Policy Information Point") para verificar as credenciais de autenticação ____

35. Existindo vários PEP ligados ao mesmo PDP, para um dado conjunto de credenciais de acesso, a resposta do PDP pode depender no PEP utilizado ____

36. Os servidores RADIUS utilizam o protocolo LDAP ("Lightweight Directory Access Protocol") para comunicarem diretamente com o PEP ____

37. Uma vez que o protocolo LDAP não garante a confidencialidade dos dados, apenas deve ser usado através de uma VPN ("Virtual Private Network") ____

38. A classe de objeto LDAP do tipo "inetOrgPerson" é do tipo estrutural, por isso um objecto desta classe não pode pertencer a outras classes estruturais ____

39. Em LDAP podem ser criados objectos que pertençam apenas a classes auxiliares, sem pertencerem a nenhuma classe estrutural ____

40. No sistema KERBEROS o TGT ("Ticket Granting Ticket") pode ser usado para obter um "ticket" de acesso a um serviço num "realm" diferente do seu ____

41. Um problema dos sistemas KERBEROS atuais é que apenas suportam cifras baseadas em DES ("Data Encryption Standard"), com chaves de 128 bits ____

42. Uma desvantagem do SASL ("Simple Authentication and Security Layer") é que para ser usado é necessidade de modificar o protocolo de aplicação ____

43. O sistema KERBEROS foi criado pela Microsoft para dar suporte ao "Active Directory" que utiliza o protocolo LDAP ____

44. No diálogo cliente/servidor do TLS ("Transport Layer Security"), o servidor informa qual o "cipher suite" a utilizar através da mensagem "ServerHello" ____

45. O TLS suporta autenticação com chave pré-partilhada, por exemplo através do "cipher suite" "TSL_PSK_WITH_AES_256_CBC_SHA" ____

46. A DMZ ("DeMilitarized Zone") está normalmente localizada no CPD, deve estar separada por "firewalls" das restantes redes ____

47. Um "firewall" que implementa a funcionalidade "stateful packet inspection" (SPI) é habitualmente designado "firewall" dinâmico ____

48. A utilização do protocolo HTTPS com certificados fidedignos está imune a ataques de "sniffing" (inspeção furtiva) e MiTM ("Man-in-the-middle") ____

49. Todos os ataques do tipo DoS ("Denial of Service"), podem ser evitados através da utilização de regras que evitem o "spoofing" IP ____

50. Os ataques ao protocolo ARP ("Address Resolution Protocol") não podem ser evitados com recurso a "firewalls" ____

51. O nó de rede habitualmente designado "honeypot" deve estar particularmente bem protegido contra todo o tipo de ataques ____

52. O ataque do tipo "SYN flood" a serviços UDP só pode ser realizado com recurso a "spoofing" IP ____

53. O objetivo do IPsec ("Internet Protocol Security") é proporcionar mecanismos de autenticação e confidencialidade na camada de rede (nível 3) ____

54. O "Encapsulating Security Payload" (ESP) permite garantir a autenticação e a confidencialidade, todas as implementações IPsec o devem suportar ____

55. O IPsec em "Transport mode" não pode garantir a integridade de todos os campos do cabeçalho IP, quer use ESP quer use AH ("Authentication Header") ____

56. Quando um pacote IPsec com a confidencialidade garantida circula na rede, todos os nós intermédios por onde passa podem obter os dados transportados ____

57. As implementações IPsec nunca podem funcionar sem o auxilio do protocolo IKE ("Internet Key Exchange Protocol") ____

58. Para criar a IKE SA ("Security Association") é usado o algoritmo "Diffie-Hellman", as restantes SA são criadas usando a IKE SA ____

59. Numa VPN do tipo HOST-LAN, após a ligação o posto de trabalho fica numa situação equivalente a estar fisicamente ligado à rede remota ____

60. O "Layer 2 Tunneling Protocol" (L2TP) e o PPTP ("Point to Point Tunneling Protocol") são dois protocolos muito utilizados na implementação de VPN ____

61. O RTP ("Real Time Protocol") é bastante mais eficiente do que o TCP sob o ponto de vista do seu mecanismo de correção automática de erros ____

62. A compressão de cabeçalhos ("header compression") deve ser seletiva, apenas sendo aplicada aos pacotes prioritários de reduzida dimensão ____

63. A técnica LFI ("Link Fragmentation and Interleaving") leva a que os pacotes sejam fragmentados no nó de origem e reconstruídos no nó de destino ____

64. O RTT ("Round-Trip Time") é calculado pelos emissores TCP, em função do seu valor, ajustam o valor do RTO ("Retransmission TimeOut") ____

65. Uma razão possível para um segmento TCP (pacote) se perder é por atuação do RED ("Random Early Detection") num nó intermédio ____

66. Na gestão de filas "Custom Queuing" (CQ), o tráfego prioritário passa primeiro, um exemplo desta implementação é o CAR ("Committed Access Rate") ____

67. As técnicas de gestão de filas "Custom Queuing" (CQ) e "Fair Queuing" (FQ) são do tipo HARD QoS, com limite de capacidade por tipo de tráfego ____

68. Ao contrário do RED, o "Weighted RED" (WRED) pode usar os bits de precedência IP para tomar a decisão de descartar ou não um pacote ____

69. A técnica "Fair Queuing" (FQ) permite garantir que o tráfego mais importante é retransmitido antes do tráfego menos importante ____

70. O RSVP ("Resource Reservation Protocol") só pode ser usado se ao longo do caminho esse protocolo for suportado por todos os nós intermédios ____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto
Administração de Sistemas – 2013/2014 – Prova prática
Exame de época de recurso e melhoria – 15 de fevereiro de 2014

Número: _____ Nome: _____

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

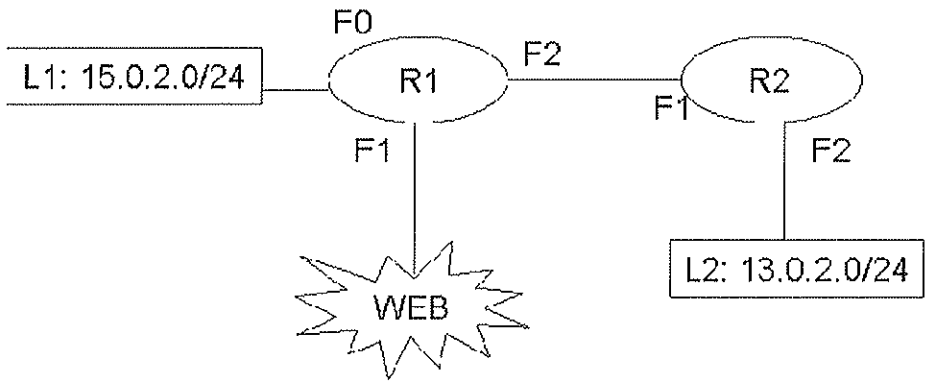
Grupo I (50%)

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.

1. O comando "last" apresenta um registo sequencial de todas as entradas e saídas de utilizadores no sistema ..... _____
2. Os comandos "dump" e "restore" suportam cópias incrementais ..... _____
3. "/dev/hdd1" representa um disco SATA ou SCSI ..... _____
4. O comando "fdisk" permite visualizar a tabela de partições de um disco ..... _____
5. O "Name Service Switch" (NSS) serve para autenticar utilizadores em repositórios remotos de utilizadores ..... _____
6. O ficheiro "/etc/passwd" contém o nome do grupo primário de cada utilizador local ..... _____
7. O comando "chmod g+r lista.txt" dá a todos os utilizadores permissão para ver o conteúdo do ficheiro "lista.txt" ..... _____
8. O ficheiro "/etc/profile" é sempre o último a ser executado durante o arranque da SHELL ..... _____
9. O INETD é particularmente adequado para serviços com reduzidas taxas de utilização ..... _____
10. A linha de configuração do CRON "10 10 5 * * root /root/teste" define a execução do comando uma vez em cada mês ..... _____
11. O Hyper V no WS2008 suporta virtualização de múltiplos sistemas operativos, mas apenas se forem Microsoft ..... _____
12. Um componente de um cluster deve ser apelidado de nó ..... _____
13. O scope de um servidor de DHCP é composto por um nome, endereço inicial, endereço final, máscara e "default gateway"... _____
14. Uma Tree no Active Directory é um conjunto de controladores de domínio ..... _____
15. O Active Directory suporta Kerberos, SSL e certificados X509 de forma a garantir a encriptação dos dados ..... _____
16. O par endereço IP e "wildcard" 130.2.0.0 0.1.255.255 corresponde a 3 redes classe B completas ..... _____
17. O "wildcard" 2.1.5.0 aplicado a um endereço IP abrange 16 endereços diferentes ..... _____
18. A regra de ACL "access-list 120 permit ip any host 198.15.2.1" permite os pacotes UDP destinados ao endereço 198.15.2.1. _____
19. É possível englobar num só par endereço IP e "wildcard" 8 endereços diferentes, mas não é possível englobar 12 ..... _____
20. Um inconveniente do NAT bidireccional é que não é possível controlar o tempo de mapeamento automático criado ..... _____

Grupo II (50%)

Observe o seguinte diagrama de rede



Os endereços IPv4 dos "routers" são os seguintes:

R1	F0: 15.0.2.254/24 F1: 9.0.0.2/30 F2: 15.0.0.2/30
R2	F1: 15.0.0.1/30 F2: 13.0.2.254/24

Escreva os comandos (CISCOIOS) que permitem implementar as seguintes políticas de acesso. Tendo em vista a eficiência, as ACLs devem conter o menor número de regras possível.

- Bloquear o "spoofing" IP com origem nas redes locais e na "Internet"
- A Internet pode enviar pedidos "echo" ICMP para L2 e interface externa de R1, mas não para L1, R2 e restantes interfaces de R1
- A Internet pode aceder a L2 em HTTP
- A Internet deve responder aos pedidos provenientes de L1
- L1 pode enviar pedidos "echo" ICMP para qualquer interface de R1 e R2
- L1 pode aceder à Internet em HTTP
- L1 pode aceder a L2 em TCP
- **Todo o restante tráfego deve ser bloqueado**

Sintaxe dos comandos necessários

access-list identificador permit|deny endereço_ip wildcard

access-list identificador permit|deny protocolo ip_origem wildcard_origem ip_destino wildcard_destino [comparação porto_destino | tipo | established]

ip access-group identificador in|out

interface nome-interface