Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2011/2012

Exame Recurso – Prática – 1ª Parte - 18/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 tabela de partições de um disco identifica a posição e o tipo de cada partição existente no disco .....
2. Aumentando o tamanho da partição SWAP podemos reduzir a quantidade de memória central (RAM) necessária no servidor .....
3. O comando "fdisk" permite visualizar a tabela de partições de um disco.....
4. O "Name Service Switch" (NSS) permite que utilizadores definidos em repositórios remotos sejam reconhecidos no servidor.....
5. Para cada utilizador definido no ficheiro "/etc/passwd" o UID tem de ser sempre igual ao GID .....
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, a falha num módulo "required", vai provocar a falhas da cadeia.....
9. O módulo "pam_deny.so" pode ser usado em qualquer uma das 4 cadeias do sistema PAM.....
10. Em Linux cada interface de rede apenas pode ter um único endereço IPv4 atribuído .....
11. O "Name Service Switch" (NSS) é usado apenas para a resolução de nomes de máquinas e serviços .....
12. O comando "chown" permite alterar o proprietário de um ficheiro ou directório.....
13. A "umask" 0077 permite criar objectos sem qualquer permissão para "others".....
14. O módulo "pam_winbind.so" pode ser usado na cadeia "auth" do sistema PAM.....
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 ou o IPv6 de uma interface de rede.....
17. O comando "vconfig" serve para configurar servidores virtuais no "Apache".....
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" permite todo o trafego 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. O comando "usermod" permite alterar os grupos locais a que um utilizador pertence ..._____

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

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

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 "10 5 5 * * root /etc/teste" define a execução do comando uma vez em cada mês ..._____

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 20 * * * root /root/teste" provoca a execução do comando dez vezes por dia ..._____

39. O comando "openssl" permite criar chaves privadas, as correspondentes chaves públicas e certificados..._____

40. A interface "eth1.193" é uma interface de VLAN, com VLANID=193..._____

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. Nos servidores Windows deve ser usado o sistema de ficheiros FAT32, em detrimento do NTFS.....

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

5. As configurações de discos RAID0 e RAID1 são ambas tolerantes a falhas num dos discos envolvidos .....

6. No WS2008 o protocolo RDP ("Remote Desktop Protocol") garante a autenticação e a confidencialidade dos dados.....

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

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. Os Serviços de Terminal no WS2008 não suportam encriptação e por isso exigem uma ligação segura.. .....

21. Entre os vários domínios de uma árvore ("TREE") existe automaticamente uma relação de confiança. .....

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

23. Um servidor WS2008 na qualidade de "domain member" implementa o serviço Active Directory localmente.....

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2011/2012

Exame Teórico de Época de Recurso e Melhoria – 18/Fev/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. A gestão da base de dados de utilizadores do sistema não é da responsabilidade do administrador de sistemas ..... _____

2. Num CPD ("Centro de Processamento de Dados") o número de servidores não afecta o consumo energético..... _____

3. O custo operacional que mais importante de um CPD é o custo com o pessoal para a sua administração..... _____

4. O custo com o consumo energético de um CPD aumenta significativamente com o aumento de servidores virtuais ..... _____

5. Para cada servidor virtual é necessário existir um CPU físico (real) na plataforma de virtualização..... _____

6. A virtualização de servidores reduz os custos operacionais ..... _____

7. Uma SAN ("Storage Area Network") é uma rede de elevado desempenho que permite a virtualização de "storage"..... _____

8. A virtualização sem recurso a uma SAN não permite que um mesmo disco seja usado por vários servidores virtuais..... _____

9. Uma desvantagem das SAN é que dificultam a implementação de alta disponibilidade e redundância..... _____

10. Não é possível implementar uma SAN com recurso a hardware de rede corrente como por exemplo "Gigabit Ethernet"..... _____

11. As SAN "Fibre Channel" utilizam todas a taxa de transmissão de 10 Gbps ..... _____

12. Duas SAN do tipo "Fibre Channel" nunca podem ser interligadas através da Internet de nenhuma forma..... _____

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

14. As SAN iSCSI constituem uma alternativa mais económica às SAN "Fibre Channel"..... _____

15. Um iSCSI HBA ("Host Bus Adapter") garante uma performance superior às restantes alternativas ..... _____

16. Um "target" iSCSI pode ser implementado com recurso a "hardware" corrente e um sistema operativo corrente ..... _____

17. Numa implementação de continuidade de negócio de categoria 7 ("Tier 7") existe redundância de servidores ..... _____

18. O "disk mirroring" é obrigatório nas implementações de continuidade de negócio de categoria 6 ("Tier 6") e superiores ..... _____

19. O RTO ("Recovery Time Objective") de "hardware" e dados é o ponto final do processo de recuperação ..... _____

20. A política de segurança deve definir as consequências da violação das regras nele definidas ..... _____

21. A política de segurança deve definir os protocolos de autenticação que são usados ..... _____

22. Se um serviço fica indisponível durante algum tempo, não pode ser considerado tolerante a falhas ..... _____

23. A detecção de intrusos é um meio de reduzir as consequências das falhas ..... _____

24. A manutenção de cópias de segurança actualizadas permite minimizar a possibilidade de ocorrência de falhas ..... _____

25. As falhas de confidencialidade em linhas de comunicação podem ser eliminadas através da segmentação da rede ..... _____

26. Para cada utilizador, o "username" deve ser igual em todos os servidores, mas a "password" pode ser diferente ..... _____

27. Só é possível o processo de autorização ("authorization") após sucesso no processo de autenticação ("authentication") ..... _____

28. Num sistema AAA, o PDP ("Policy Decision Point") comunica directamente com o PIP ("Policy Information Point") ..... _____

29. O protocolo de autenticação PAP ("Password Authentication Protocol") não é seguro em nenhum tipo de aplicação ..... _____

30. O protocolo RADIUS ("Remote Authentication Dial In User Service") utiliza pacotes UDP para todas as transacções ..... _____

31. O protocolo RADIUS é normalmente usado na comunicação entre o PEP/NAS (cliente) e o PDP (servidor) ..... _____

32. As bases de dados "Active Directory" são acessíveis através do protocolo LDAP ("Lightweight Directory Access Protocol") .... _____

33. O servidor LDAP nunca pode ser usado directamente para validar credenciais, é necessário usar o servidor RADIUS ..... _____

34. No acesso ao servidor LDAP a autenticação simples com "password" em claro só deve ser usada com TLS/SSL ..... _____

35. Numa base de dados LDAP, um objecto pode pertencer a várias classes auxiliares ("auxiliary") ..... _____

36. Um objecto de uma base de dados LDAP tem de usar todos os atributos definidos nas classes a que pertence ..... _____

37. O KERBEROS garante a confidencialidade dos dados transaccionados entre os PRINCIPAL ..... _____

38. O sistema KERBEROS usa exclusivamente criptografia simétrica ..... _____

39. O KERBEROS pode funcionar mesmo que o serviço KDC ("Key Distribution Center") não esteja disponível ..... _____

40. A autenticação dos PRINCIPAL do sistema KERBEROS usa certificados de chave pública ..... _____

41. Os ataques do tipo "Packet Sniffing" só podem ser adequadamente contrariados com encriptação da informação ..... _____

42. O ataque do tipo "IP Spoofing" consiste em falsear os endereços de origem dos pacotes IP ..... _____

43. Os ataques de tipo MITM ("man-in-the-middle") são ataques de interposição que alteram a integridade das mensagens ..... _____

44. Muitos ataques de "IP Spoofing" podem ser evitados com recurso a ACLs estáticas ..... _____

45. A utilização de HTTPS permite evitar os ataques DoS ("Denial of Service") ..... _____

46. O protocolo ARP está exposto a ataques porque não possui nenhum mecanismo de autenticação ..... _____

47. A criptografia de chave pública necessita de 4 chaves para assegurar uma comunicação segura entre duas entidades ..... _____

48. A utilização de uma chave pré partilhada (criptografia simétrica) assegura a autenticação ..... _____

49. Para um mesmo algoritmo de criptográfico, quanto maior for a chave usada, maior é a segurança ..... _____

50. Para blocos de dados de entrada iguais, uma função de "hash" produz sempre o mesmo resultado ("digest") ..... _____

51. As funções "hash" são algoritmos de criptografia de chave pública ..... _____

52. Na posse de uma mensagem cifrada e o respectivo original torna-se possível "quebrar" a chave por "força bruta" ..... _____

53. A aplicação dupla do algoritmo DES simples corresponde em termos de segurança a aumentar apenas um bit à chave ..... _____

54. O HTTPS difere do HTTP pelo facto de usar uma ligação SSL/TLS em lugar de uma simples ligação TCP ..... _____

55. Os algoritmos RC2, RC4 e RC5 são algoritmos de chave pública ..... _____

56. Os servidores do centro de dados (CPD) devem estar colocados numa DMZ ("DeMilitarized Zone") ..... _____

57. O ataque através da numeração de sequência do TCP tem geralmente como objectivo desencadear um ataque DoS ..... _____

58. O QoS ("Quality of Service") evita que o tráfego menos importante afecte a performance da rede no tráfego prioritário ..... _____

59. Num "router" uma gestão de filas com implementação QoS usa a estratégia FIFO ..... _____

60. Para que o tráfego de baixa prioridade tenha sempre oportunidade de passar o método adequado é "Priority Queuing" ..... _____

61. A marcação de pacotes é necessária se o local onde é feita a classificação de pacotes não é o mesmo onde ela é aplicada.. _____

62. A fragmentação e "Interleaving" de tráfego IP é uma técnica de gestão das filas nos "routers" ..... _____

63. No algoritmo "Custom Queuing" um pacote prioritário pode ficar mais tempo retido do que um de baixa prioridade ..... _____

64. A técnica "Weight Fair Queuing" é uma implementação "Hard QoS" ..... _____

65. O CAR ("Committed Access Rate") pode levar à retenção de pacotes mesmo que a interface de saída esteja livre ..... _____

66. A técnica RED ("Random Early Detection") descarta ("drop") pacotes mesmo que a fila não esteja completamente cheia ..... _____

67. A técnica WRED ("Weighted RED") pode ser usada pelo CAR para implementar "Hard QoS" ..... _____

68. O WRED nunca pode em nenhuma circunstância descartar ("drop") pacotes de elevada prioridade ..... _____