Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2010/2011

Época de Recurso/Melhoria – 19/Fev/2011 - Exame Prático – 2ª Parte

ATENÇÃO: Para os alunos que ainda não obtiveram aprovação (recurso) esta prova anula a anterior.

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. As distribuições Linux que não são gratuitas possuem um núcleo ("kernel") diferente das distribuições gratuitas ..... _____

2. "/dev/sda1" identifica uma partição de um disco IDE ..... _____

3. /dev/hdd nunca pode representar um leitor de CD/DVD ..... _____

4. Um disco nunca pode ter mais do que três partições ..... _____

5. A tabela de partições indica onde começa e acaba cada partição ..... _____

6. O formato mais corrente do sistema de ficheiros dos sistemas Windows é diferente do dos sistemas Linux ..... _____

7. O sistema de ficheiros Linux EXT3 e o sistema de ficheiros Windows NTFS suportam ambos ACLs ..... _____

8. Um mesmo utilizador nunca pode ter cotas diferentes em duas partições diferentes ..... _____

9. Uma partição SWAP nunca pode coexistir com outras partições no mesmo disco ..... _____

10. No ficheiro "/etc/group", o primeiro campo de cada linha é o nome do utilizador para quem esse grupo foi criado ..... _____

11. O grupo primário de cada utilizador é identificado no ficheiro "/etc/passwd" ..... _____

12. A utilização dos comandos "useradd" e "usermod" é menos segura do que a edição manual do ficheiros "/etc/passwd" ..... _____

13. O NSS ("Name Service Switch") trata do processo de autenticação de utilizadores usando repositórios remotos ..... _____

14. No caso do módulo "libnss_ldap.so", a identificação do servidor LDAP é guardada no ficheiro "/etc/nsswitch.conf" ..... _____

15. Usando o PAM ("Pluggable Authentication Modules") todas as "passwords" ficam guardadas no ficheiro "/etc/shadow" ..... _____

16. No PAM, na cadeia de autenticação ("auth"), a falha de um módulo provoca sempre a falha de toda a cadeia ..... _____

17. A pasta HOME de cada utilizador deve ter o mesmo proprietário que a pasta "/etc/skel" ..... _____

18. As permissões 700 são adequadas para uma pasta HOME ..... _____

19. A UMASK 0027 compromete gravemente a integridade dos ficheiros criados pelo respectivo utilizador .....

20. As variáveis de ambiente podem ser definidas nos "scritps" de arranque, mas também no PAM .....

21. Para activar cotas numa nova partição (recém formatada) basta usar o comando "quotaon".....

22. Na definição de cotas, o valor do parâmetro HARD LIMIT deve ser superior ao valor do parâmetro SOFT LIMIT.....

23. No comando "ifconfig", a omissão do argumento "<AF>" ("Address Family") leva a assumir o valor "inet".....

24. O único comando disponível para gerir a tabela de encaminhamento IPv4 é o comando "route".....

25. "eth1.5" identifica uma interface VLAN com VLANID=5 .....

26. O comando "vconfig" tem uma sintaxe de argumentos idêntica à do comando "ifconfig".....

27. Os servidores DHCP funcionam sempre em modo dinâmico, não permitindo configurar endereços MAC estáticos.....

28. Para ter sucesso, o cliente DHCP tem de conhecer o endereço IP do servidor DHCP .....

29. O "Internet Daemon" (INETD/XINETD) suporta serviços TCP e também serviços UDP .....

30. O ficheiro "/etc/resolv.conf"apenas pode conter declarações "nameserver".....

31. No IPTABLES, mesmo que um pacote corresponda a uma regra, a cadeia é sempre verificada até ao fim .....

32. Em LINUX o tipo de conteúdo dos ficheiros é identificado através do respectivo nome.....

33. A primeira linha de um "shell script" deve sempre começar pela sequência #!.....

34. A linha de configuração do CRON começada por "5 5 * * * " é executada uma vez por dia, todos os dias .....

35. Num certificado de chave pública SUBJECT identifica o proprietário da chave pública a que o certificado se refere .....

36. Um certificado auto-assinado de uma entidade desconhecida não tem qualquer valor sob o ponto de vista de autenticação....

37. O SYSTEM LOGGER ("syslog") classifica as mensagens com base no conjunto: "{facility}.{severity}".....

38. O "syslog" pode ser configurado de forma a não guardar localmente nenhuma mensagem.....

39. O registo de entradas e saídas usa três ficheiros de registo separados.....

40. O comando "who" apresenta dados de registos que foram criados pelo SYSTEM LOGGER.....

41. O ficheiro "wtmp" é consultado pelo comando "wtmp" e o ficheiro "utmp" é consultado pelo comando "utmp".....

42. Os comandos "dump" e "restore" usam-se para fazer cópias integrais de partições de qualquer tipo ou discos.....

43. Quando se usam cópias incrementais, estas nunca devem ser intercaladas com cópias integrais .....

2ª Parte – Administração de servidores Windows

1. O Sistema de ficheiros Fat32 suporta file system journaling _____

2. No servidor de DNS do WS2008 existem sempre registos do tipo AAAA _____

3. O RAID0 utiliza um mecanismo conhecido como striping _____

4. ISEP é um exemplo de um Fully Qualified Domain Name _____

5. No Active Directory existem Árvores que implementam relações de confiança bidireccional entre si _____

6. Com os "default password requirements" activos, as passwords tem no mínimo 4 caracteres de 3 conjuntos diferentes _____

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

8. A segurança é parte do Active Directory sendo definida ao nível ao nível das Trees _____

9. O RAID permite conjugar as versões 0 e 1, ou seja existem implementações com as funcionalidades de ambas as versões _____

10. Os servidores de DHCP no WS2008 só suportam IPv6 em modo stateless _____

11. No WS2008 o Servidor de DHCP é uma feature _____

12. Os Serviços de terminal obrigam a que se use uma VPN para proteger as comunicações. _____

13. O RAID5 utiliza pelo menos 2 discos com bits de paridade e 3 com dados _____

14. As homes dos Utilizadores são armazenadas numa zona chamada SYSVOL _____

15. No Active Directory uma Floresta cria automaticamente uma relação de confiança entre as várias árvores que a compõem _____

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

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

18. O Active Directory suporta Kerberos, SSL e certificados X509 _____

19. O BitLocker permite que qualquer sistema aceda aos dados desde que o sistema operativo original esteja em execução _____

20. O Hyper V no WS2008 apenas suporta virtualização de máquinas Windows _____

21. O WS 2008 em modo Server Core permite que seja configurado como servidor DNS, DHCP e domínio _____

22. No servidor de DNS do WS2008 ao activarmos o "Automatic Scavening", eliminamos os registos com mais de 24h _____

23. O "Active Directory" permite criar OU's (Organizational Unit) multi-nivel _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2010/2011

Época de Recurso/Melhoria – 19/Fev/2011 - Exame Prático – 1ª Parte

ATENÇÃO: Para os alunos que ainda não obtiveram aprovação (recurso) esta prova anula a anterior

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") …
   - ☐ é do tipo híbrido.
   - ☐ pode ser redistribuído em EIGRP mas não em RIP.
   - ☐ envia um LSA ("Link State Advertisement") para todos os routers vizinhos.
   - ☐ usa um valor de métrica directamente proporcional à largura de banda.
   - ☐ designa de router de fronteira um router que interliga duas áreas OSPF.
2. O protocolo EIGRP ("Enhanced Interior Gateway Routing Protocol") …
   - ☐ é um protocolo standard.
   - ☐ permite a divisão da infra-estrutura em sistemas autónomos (AS).
   - ☐ suporta, por omissão, redes com endereçamento "classless" (CIDR).
   - ☐ é, tal como o RIP, um protocolo proprietário CISCO.
   - ☐ é eficiente na ocupação da largura de banda.
   - ☐ suporta o envio de pacotes com confirmação de recepção.
3. Em Cisco IOS, o comando "redistribute" …
   - ☐ é usado nos routers que interligam sistemas protocolos diferentes.
   - ☐ só permite a redistribuição de redes ompletas, não de parte delas.
   - ☐ permite definir acções (*set*) baseadas em critérios (*match*).
   - ☐ não permite a redefinição das métricas durante a redistribuição.
   - ☐ pode ser usado para interligar duas zonas RIP desde que apenas uma delas seja RIPv2.
4. A regra de ACL "**permit ip 194.65.12.8 0.0.0.8 200.128.1.0 0.2.0.255**" …
   - ☐ permite tráfego TCP e UDP.
   - ☐ é válida no contexto de uma ACL standard.
   - ☐ pode ser aplicada (a ACL) no sentido OUT, mas nunca no sentido IN.
   - ☐ é omissa em relação ao tráfego ICMP.
   - ☐ permite tráfego do endereço de origem 194.65.12.16.
   - ☐ permite tráfego de um conjunto de 2 endereços de origem.

5. O NAT ("Network Address Translation") ...
   - ☐ pode servir para mascarar endereços reais.
   - ☐ o "Weighted Round Robin" é utilizado no "Twice-NAT".
   - ☐ quando usado para balanceamento de carga pode ser configurado segundo dois protocolos distintos.
   - ☐ tem sempre como ponto adverso ser o único dispositivo de encaminhamento para o exterior.
6. Em segurança ...
   - ☐ a autenticação por utilizador e password garante que o utilizador é quem diz ser.
   - ☐ integridade significa que o utilizador é quem diz ser.
   - ☐ a criptografia simétrica permite a implementação de assinaturas digitais.
7. A criptografia ...
   - ☐ pode ser periódica e em bloco simultaneamente.
   - ☐ bidireccional pode ser irreversível.
   - ☐ pode garantir a confidencialidade.
8. As transformações criptográficas ...
   - ☐ só podem utilizar uma técnica.
   - ☐ por substituição pode servir-se da troca de posição de elementos.
   - ☐ podem utilizar mais do que uma técnica em cascata.
   - ☐ em bloco são mais eficientes mas blocos iguais geram sempre cifras iguais.
9. O par endereço IP/WILDCARD "**190.10.0.0 0.1.8.192**" ...
   - ☐ define uma só rede IP "classful".
   - ☐ define duas redes IP "classfull".
   - ☐ inclui o endereço 190.11.0.64.
   - ☐ não é válido.
10. Uma ACL constituída apenas pela regra "**permit ip 140.20.1.0 0.0.0.255**" ...
    - ☐ bloqueia o tráfego com origem na rede 140.20.0.0/16.
    - ☐ não bloqueia o tráfego com origem na rede 140.20.1.0/16.
    - ☐ 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 ftp**" ...
    - ☐ não permite nenhum tipo de tráfego IP.
    - ☐ permite apenas tráfego FTP com origem no endereço 200.10.0.1.
    - ☐ permite apenas tráfego FTP com destino ao endereço 200.10.0.1.
    - ☐ permite todo o tráfego TCP com destino ao endereço 200.10.0.1.

12. Para permitir num interface todo o tráfego excepto o com origem na rede 197.120.0.0/23, pode ser usada a ACL com a(s) regra(s) ...

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

☐ "access-list 50 deny network 197.120.0.0" e "access-list 50 permit any".

☐ "access-list 12 deny 197.120.0.0 0.0.1.255" e "access-list 12 permit any".

☐ "access-list 14 deny network 197.120.0.0".

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

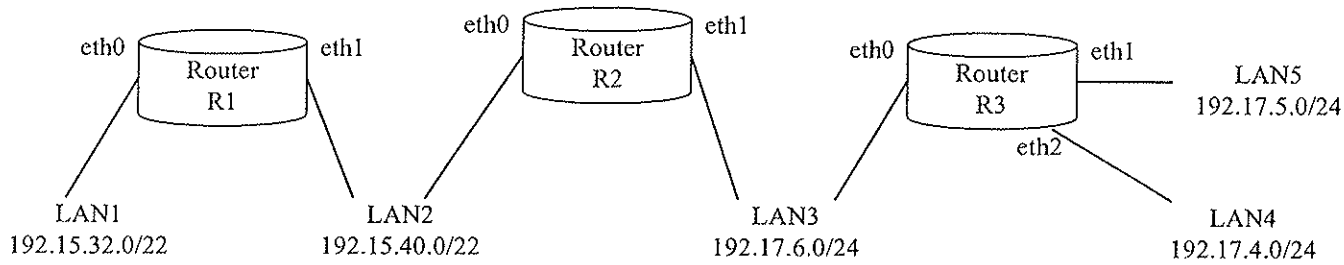
☐ permite tráfego ICMP destinado ao endereço 170.3.1.1.

☐ 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 às redes LAN2 e LAN6.

LAN2: apenas pode aceder às redes LAN1 e LAN5, mas os 63 endereços de .64 a .127 podem aceder a tudo.

LAN3: apenas pode aceder à LAN2 e LAN5, também pode aceder aos endereços 192.15.32.64, 192.15.32.192, 195.15.33.64 e 192.15.64.192 da LAN1, exclusivamente para tráfego TCP destinado ao serviço HTTP.

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

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

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 de Recurso – 19/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 operações de rotina, como por exemplo "backups", não são da responsabilidade do administrador de sistemas..... _____

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

3. A virtualização de servidores tem como principal vantagem a redução dos custos de aquisição de equipamento..... _____

4. A virtualização de servidores dificulta a implementação de metodologias de alta disponibilidade ..... _____

5. O sistema operativo da plataforma de virtualização tem de ser do mesmo tipo do usado nas respectivas máquinas virtuais ..... _____

6. A virtualização de servidores aumenta a taxa de utilização do "hardware" físico, em especial os CPU ..... _____

7. A virtualização de "storage" utiliza redes de elevado desempenho, designadas SAN ("Storage Area Network")..... _____

8. Todas as SAN são baseadas em IPv4 ou IPv6..... _____

9. Uma desvantagem das SAN é que dificultam a replicação de "storage" ("disk mirroring") ..... _____

10. Todas as SAN são infra-estruturas dedicadas que nunca podem ter outro tipo de utilização ..... _____

11. Todas as SAN "Fibre Channel" utilizam uma topologia em anel de elevado desempenho..... _____

12. Duas SAN do tipo "Fibre Channel" podem ser directamente interligadas através da Internet..... _____

13. Os nós de rede "Fibre Channel" são identificados através de um endereço de físico de 6 bytes..... _____

14.O iniciador iSCSI é o nó de rede que utiliza discos residentes na SAN..... _____

15. Numa implementação de continuidade de negócio de categoria 7 ("Tier 7") exige "disk mirroring" ..... _____

16. O RTO ("Recovery Time Objective") de integridade de transacções é o ponto final do processo de recuperação..... _____

17. As credenciais de autenticação de um utilizador devem ser diferentes nos vários serviços da organização..... _____

18. Um sistema AAA começa por exigir a autenticação do cliente/utilizador..... _____

19. Num sistema AAA, o PDP ("Policy Decision Point") é o responsável pela contabilização ("Accounting") ..... _____

20. O protocolo de autenticação PAP ("Password Authentication Protocol") pode ser usado em ligações sem cifragem..... _____

21. O protocolo de EAP ("Extensible Authentication Protocol") permite a comunicação directa entre o cliente e o PDP..... _____

22. Uma base de dados LDAP pode assumir o papel de PIP ("Policy Information Point") no contexto de um sistema AAA ..... _____

23. A autorização e autenticação são duas designações alternativas para o mesmo tipo de verificação ..... _____

24. Numa base de dados LDAP, todos os registos (objectos) possuem os mesmos campos (atributos)..... _____

25. O acesso a uma base de dados LDAP exige sempre credenciais de autenticação ..... _____

26. O protocolo LDAP é especialmente adequado a alterações frequentes de registos, suportando transacções ..... _____

27. O protocolo LDAP pode ser usado para acesso a bases de dados "Microsoft Active Directory"..... _____

28. O servidor RADIUS ("Remote Authentication Dial In User Service") assume normalmente o papel de PDP ..... _____

29. O sistema de autenticação KERBEROS usa exclusivamente criptografia de chave pública..... _____

30. No sistema KERBEROS cada PRINCIPAL possui uma chave que nunca é dada a conhecer a outros PRINCIPAL ..... _____

31. As comunicações entre elementos do sistema KERBEROS devem ser sempre realizadas sobre SSL/TLS..... _____

32. Entre outros elementos, a política de segurança deve definir o nível de privacidade que é garantido aos utilizadores..... _____

33. Um sistema é tolerante a falhas, quando a ocorrência de falhas se torna imperceptível para os utilizadores ..... _____

34. Um mecanismo eficiente de detecção de falhas é um meio de reduzir as consequências das falhas ..... _____

35. A manutenção de cópias de segurança actualizadas é um meio de reduzir as consequências das falhas ..... _____

36. As falhas de confidencialidade podem ser evitadas, mas as suas consequências não podem ser minimizadas..... _____

37. As redes sem fios são particularmente expostas a ataques do tipo "Packet Sniffing" ..... _____

38. Os ataques "Packet Sniffing" são ataques em que os endereços de origem dos pacotes são manipulados ..... _____

39. Os ataques do tipo MITM ("man-in-the-middle") alteram a integridade das mensagens ..... _____

40. Os ataques de "IP Spoofing" têm muitas vezes como objectivo a realização de ataques DoS ("Denial of Service") ..... _____

41. A utilização de HTTPS torna muito difícil um ataque do tipo "DNS Spoofing"..... _____

42. As ACLs estáticas não são suficientes para evitar ataques DoS ..... _____

43. A criptografia de chave pública assegura a confidencialidade e a autenticação com uma única aplicação ..... _____

44. Em criptografia de chave secreta é necessária apenas uma chave para uma comunicação segura entre duas entidades ..... _____

45. As chaves envolvidas na criptografia de chaves públicas podem ser todas divulgadas livremente ..... _____

46. O resultado de uma função de "hashing" pode ser usado para obter a mensagem original..... _____

47. As funções de "hashing" destinam-se a implementar a confidencialidade das transacções de dados ..... _____

48. A "Criptoanálise diferencial" é uma técnica vulgarmente conhecida por "força bruta" ..... _____

49. O algoritmo DES simples é considerado inseguro na actualidade..... _____

50. O SSL/TLS e o IPsec são duas implementações de segurança, alternativas para a camada de rede (nível 3) ..... _____

51. O algoritmo RC4 com chave de 256 bits é bastante seguro ..... _____

52. O local de trabalho dos utilizadores de uma organização deve ser a DZM ("DeMilitarized Zone")..... _____

53. O ataque através da numeração de sequência afecta de igual modo as comunicações UDP e TCP..... _____

54. A detecção de intrusos pode ser vista como um mecanismo para minimizar as consequências de falhas..... _____

55. O QoS ("Quality of Service") tem como objectivo garantir que todas as aplicações têm as mesmas oportunidades..... _____

56. Num "router", quando o tráfego de entrada supera a capacidade da ligação de saída, o excesso é descartado ..... _____

57. O QoS só pode ser implementado com recurso é marcação de pacotes através dos bits de precedência (TOS)..... _____

58. A fragmentação e "Interleaving" de tráfego IP é uma técnica "hard" QoS..... _____

59. Na gestão de filas "Priority Queuing" todas as filas são tratadas do mesmo modo ..... _____

60. No algoritmo "Custom Queuing" tem como objectivo evitar que as filas de espera fiquem "cheias" ..... _____

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

62. O "Hard QoS" implica que os pacotes podem ser descartados ou retidos, mesmo que a ligação de saída esteja livre ..... _____

63. O "Soft QoS" permite a reserva de determinada largura de banda para uma aplicação em particular..... _____

64. A técnica RED ("Random Early Detection") simples não é um mecanismo QoS..... _____

65. O RED aproveita a funcionalidade "Slow Start" do protocolo TCP..... _____

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

67. O CAR só pode ser implementado em conjunto como o WRED ("Weighted RED") ..... _____

68. O RSVP ("Resource Reservation Protocol") permite definir prioridades de tráfego a pedido do cliente..... _____