Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2012/2013

Exame de Recurso/Melhoria – Prática – Parte 2 – 19/Fevereiro/2013

Número: _____ Nome: _____

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

Bom trabalho.

Grupo I

(12 valores)

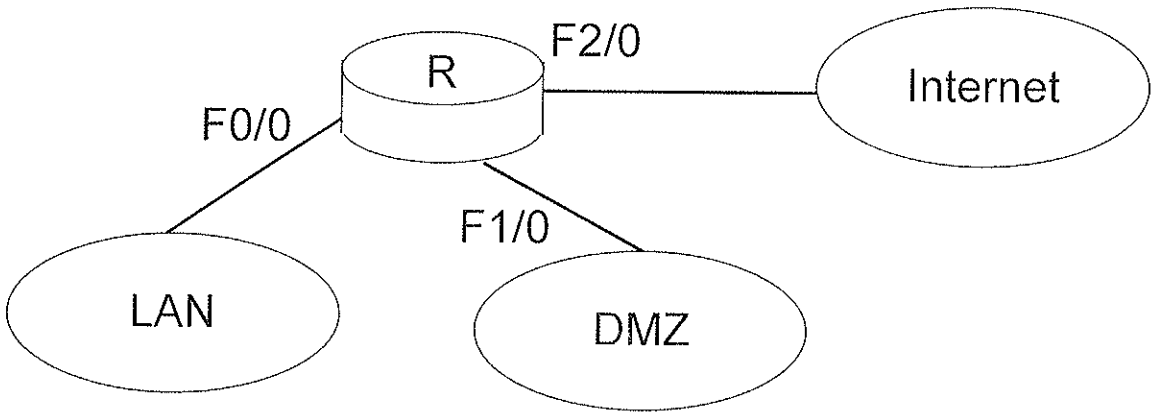
Em cada afirmação assinale V ou F (Verdadeiro ou Falso) conforme considere aplicável.
Se não tiver a certeza, não responda. Cada resposta errada desconta meia resposta certa.

1. As ACL *standard* permitem usar como critério o porto de destino _____
2. Se o protocolo for omisso numa ACL *extended* assume-se o IP _____
3. Uma ACL é *standard* se tiver um identificador entre 1 e 99 _____
4. O comando **access-list 5 permit 192.168.0.0 0.0.5.255** nega todos os IP's privados da classe C com excepção de 4 redes. _____
5. O comando **no access-list 105** elimina toda a ACL 105 _____
6. O endereço 197.22.15.2 com o *wildcard* 0.0.13.0 representa o 2º endereço de nó de cada uma de 8 redes da classe C _____
7. O endereço 12.0.0.1 com o *wildcard* 0.0.0.254 representa 128 endereços da rede 12.0.0.0/8 _____
8. É possível ter um *wildcard* que abrange apenas e só 6 endereços _____
9. Um *wildcard* é exactamente o inverso de uma máscara de rede _____
10. Uma ACL constituida apenas pela regra **access-list permit 12.0.0.0 0.255.255.255** bloqueia todo o tráfego com origem na rede 13.0.0.0/8 _____
11. Os O comando **access-list 5 permit 12.0.0.0 0.0.0.255** não é válido _____
12. O endereço 7.5.2.0 associado ao *wildcard* 0.4.15.7 inclui o endereço 7.5.17.1 _____
13. O *wildcard* 0.0.0.153 corresponde a um conjunto de 16 endereços _____
14. O bloqueio de *spoofing* IP deve ser efectuado no sentido OUT da interface que liga a rede ao exterior _____
15. O comando **access-list 10 permit any established** é válido _____
16. Num router só pode existir uma interface **ip nat outside** _____
17. O comando **ip nat inside source list 5 pool A** nega os pacotes cujo endereço de origem não exista na ACL 5 _____
18. Nas configurações NAT não pode ser usada a opção **overload**, só nas configurações NAPT _____
19. O bidirectional NAT exige o DNS_ALG _____

Grupo II

(8 valores)

Considere o seguinte conjunto de redes interligadas pelo router R:



Router R
interface F0/0
ip address 15.0.0.190 255.255.255.192
interface F1/0
ip address 15.0.0.30 255.255.255.224
interface F2/0
ip address 17.0.0.9 255.255.255.252

Escreva os comandos necessários para implementar as seguintes políticas de acesso:

- Bloquear o "spoofing IP" qualquer que seja a sua origem.

- Todos os nós da LAN devem poder aceder livremente à "Internet" via TCP. Os nós 15.0.0.129 até 15.0.0.131 e 15.0.0.144 até 15.0.0.147 devem poder aceder livremente à DMZ, os restantes apenas podem aceder via HTTP (www) aos nós 15.0.0.7 e 15.0.0.15 e por FTP aos nós 15.0.0.8 e 15.0.0.24.

- A Internet deve poder aceder via HTTP (www) aos nós 15.0.0.7 e 15.0.0.15 da DMZ, deve também poder enviar-lhes pedidos de "echo icmp". Da "Internet" também deve ser possível enviar pedidos de "echo icmp" para a interface externa de R. Os restantes acessos da "Internet" devem ser bloqueados, com a exceção do tráfego TCP estabelecido por iniciativa dos postos de trabalho da LAN.

As ACLs devem ser otimizadas, contendo o número mínimo de regras e, sempre que possível, usando ACLs standard.

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

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2012/2013 – Exame Teórico
Recurso/Melhoria – 19/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 gestão das contas de utilizador ..... _____

2. O CPD ("Centro de Processamento de Dados") é um local de acesso livre a todos os utilizadores ..... _____

3. O custo operacional mais significativo de um CPD é o custo de funcionamento das unidades de refrigeração ..... _____

4. Os custos energéticos de um CPD não estão relacionados com a idade do "hardware" utilizado ..... _____

5. A virtualização de servidores reduz os custos operacionais de um CPD ..... _____

6. A taxa média de utilização dos recursos físicos ("hardware") melhora com a virtualização ..... _____

7. A virtualização de "storage" é implementada através de uma SAN ("Storage Area Network") ..... _____

8. As SAN do tipo iSCSI apenas podem ser implementadas sobre tecnologia "ethernet" ..... _____

9. Duas SAN do tipo "Fibre-Channel" nunca podem ser interligadas através da "Internet" ..... _____

10. O tipo de "target iSCSI" que garante a melhor performance é o "software target" ..... _____

11. Um disco de uma SAN "Fibre Channel" pode ser directamente usado por um iSCSI "initiator" ..... _____

12. O objetivo de criar um sistema redundante é aumentar o MTBF ("Mean Time Between Failures") ..... _____

13. O MTBF nunca pode ser inferior ao MTTF ("mean time to fail") ..... _____

14. Um bom controlo de permissões é uma medida que se enquadra na "prevenção de falhas" ("fault avoidance") ..... _____

15. Num sistema verdadeiramente tolerante a falhas, a falha de um componente não tem qualquer impacto no desempenho ..... _____

16. Uma "common-mode fault" é uma falha que afeta simultaneamente vários componentes de um sistema redundante ..... _____

17. A deteção de falhas (monitorização) permite reduzir o RTO ("Recovery Time Objective") ..... _____

18. Num sistema com cópias de segurança diárias, o RPO ("Recovery Point Objective") é de 24 horas ..... _____

19. O objetivo do DRP ("Disaster Recovery Plan") é reduzir o RTO e aumentar o RPO ..... _____

20. As cópias de segurança devem ser realizadas no horário correspondente ao maior grau de utilização dos sistemas..... _____

21. Uma matriz de risco de falha de um componente relaciona o impacto da falha com a probabilidade de ela ocorrer..... _____

22. O plano de contingência ("contingency plan") destina-se a garantir que o sistema continua a operar com toda a normalidade _____

23. A continuidade de negócio de categoria 7 ("Tier 7") pressupõe valores de RTO inferiores aos da categoria 5 ("Tier 5") ..... _____

24. A politica de segurança deve definir regras na definição, armazenamento e manuseamento das "passwords" ..... _____

25. O "não repúdio" serve para garantir que os dados não são alterados por intrusos ("integridade")..... _____

26. Os certificados de chave pública transportam uma chave que apenas pode ser extraída pelo respetivo proprietário ..... _____

27. As funções "hash" são usadas na implementação de assinaturas digitais simples ..... _____

28. O algoritmo AES ("Advanced Encryption Standard") é uma cifra de chave simétrica..... _____

29. O algoritmo DES ("Data Encryption Standard") é equivalente em termos de segurança ao AES ..... _____

30. O algoritmo RSA ("Ron Rivest, Adi Shamir e Leonard Adleman") utiliza normalmente chaves com menos de 128 bits..... _____

31. Num sistema AAA, a validade da autenticação ("authentication") garante imediatamente o acesso ao recurso..... _____

32. NAS ("Network Access Service") é uma designação que se dá ao PEP ("Policy Enforcement Point") em certas situações..... _____

33. O protocolo RADIUS verifica em mensagens separadas a autenticação ("authentication") e a autorização ("authorization") .... _____

34. O EAP ("Extensible Authentication Protocol") pode ser usado nas comunicações entre os clientes e o PEP ..... _____

35. Os servidores LDAP ("Lightweight Directory Access Protocol") podem funcionar como PDP ("Policy Decision Point")..... _____

36. Numa base de dados LDAP um objecto pode ser criado apenas com classes auxiliares ..... _____

37. A classe de objecto "inetOrgPerson" contém todos os atributos necessários para contas de utilizador de sistemas UNIX ..... _____

38. Numa base de dados LDAP não podem existir dois objetos com o mesmo DN ("Distinguished Name")..... _____

39. No sistema KERBEROS o TGT ("Ticket Granting Ticket") não pode ser desencriptado pelo "principal" que o recebe..... _____

40. Para o KERBEROS funcionar é necessário que todos os sistemas intervenientes tenham os relógios sincronizados ..... _____

41. O KERBEROS versão 5 exige que todos os intervenientes suportem a cifra AES com chaves de 256 bits..... _____

42. O GSS-API ("Generic Security Services Application Program Interface") usa apenas cifras de chaves simétricas..... _____

43. O SASL ("Simple Authentication and Security Layer") permite usar mecanismos de segurança, sem alterar os protocolos..... _____

44. O "cipher suite" "TLS_RSA_WITH_AES_256_CBC_SHA256" usa autenticação através de certificados de chave pública ..... _____

45. Os "firewalls" dinâmicos possuem a funcionalidade "stateful packet inspection" (SPI) ..... _____

46. A arquitetura "three legged firewall" permite a separação da "Intranet", "DMZ" e "Internet" com apenas um "firewall" ..... _____

47. Os ataques do tipo DoS ("Denial of Service"), podem ser contrariados de forma eficaz com um "firewall" estático ..... _____

48. Os ataques MITM ("Man-in-the-middle") apenas são possíveis sobre protocolos que não implementam autenticação ..... _____

49. Os serviços locais DHCP e ARP estão particularmente expostos a ataques MITM ..... _____

50. O "Spoofing IP" contra serviços TCP é mais complexo do que contra serviços UDP ..... _____

51. No protocolo RTP ("Real-time Transport Protocol") cada pacote transporta uma etiqueta data/hora ..... _____

52. A redução do tamanho dos pacotes só é eficaz se for aliada à compressão de cabeçalhos ("header compression") ..... _____

53. O LFI ("Link Fragmentation and Interleaving") é aplicado entre nós intermédios, sendo transparente para os nós finais ..... _____

54. O valor do RTT ("Round-Trip Time") fornece ao TCP indicações sobre o estado de congestionamento da rede ..... _____

55. O efeito "TCP global synchronization" ocorre quando muitos nós TCP entram no modo "Slow Start" ..... _____

56. O RED ("Random Early Detection") leva os nós intermédios a descartar pacotes, mesmo sem a fila de saída estar cheia ..... _____

57. Os bits de precedência IP podem ser usados com os protocolos TCP e RDP, mas não com o protocolo UDP ..... _____

58. Com SOFT QoS ("Quality Of Service"), alguns pacotes podem ficar em espera mesmo que a interface de saída esteja livre .. _____

59. A gestão de filas "Custom Queueing" (CQ) oferece menos garantias ao tráfego prioritário do que a "Priority Queueing" (PQ) . _____

60. A gestão de filas do tipo "Weighted Fair Queueing" (WFQ) é uma técnica SOFT QoS ..... _____

61. O "Weighted RED" (WRED) pode usar os bits de precedência para escolher os pacotes que devem ser descartados ..... _____

62. O CAR ("Committed Access Rate") é uma técnica HARD QoS ..... _____

63. O RSVP ("Resource Reservation Protocol") permite aos nós recetores configurar o QoS nos nós intermédios ..... _____

64. O IPsec em "Tunnel mode" nunca pode garantir a confidencialidade do cabeçalho IP original ..... _____

65. O "IP Authentication Header" (AH) permite garantir a autenticidade/integridade, mas não a confidencialidade ..... _____

66. A "Security Policy Database" (SPD) é uma ACL com 3 resultados possíveis (DISCART; BYPASS e PROTECT) ..... _____

67. O protocolo IKE usa o algoritmo "Diffie-Hellman" para criar a primeira SA ("Security Association") entre dois nós (IKE SA) ..... _____

68. No "Layer 2 Tunneling Protocol" (L2TP) um LAC ("L2TP Access Concentrator") opera como um comutador de rede (nível 2). _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2012/2013

Exame de Recurso/Melhoria – Prática – Parte 1 – 19/Fevereiro/2013

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. Na instalação do Linux Ubuntu a definição das partições é importante pois não pode ser facilmente alterada mais tarde .....

2. A configuração da resolução de nomes DNS pode ser feita no ficheiro "/etc/resolv.conf".....

3. Aumentando o tamanho da partição SWAP podemos reduzir a quantidade de memória central (RAM) necessária.....

4. A tabela de partições de um disco identifica a posição de cada partição existente no disco .....

5. Na formatação de um sistema de ficheiros a utilização de blocos grandes conduz a um melhor aproveitamento do espaço.....

6. Num servidor Linux Ubuntu o ficheiro "/etc/network/interfaces contém informações sobre endereço e nome DNS .....

7. O "Name Service Switch" (NSS) afecta apenas a resolução de nomes de máquinas.....

8. Numa cadeia PAM, a falha num módulo "required", vai provocar a falhas da cadeia .....

9. O comando "quota" se usado pelo administrador permite visualizar as cotas de qualquer utilizador.....

10. O comando "passwd" permite ao administrador ("root") alterar a "password" de qualquer utilizador local.....

11. O serviço NSS permite configurar a ordem pela qual os vários repositórios de informação disponíveis vão ser usados .....

12. O módulo "pam_winbind.so" pode ser usado na cadeia "auth" do sistema PAM.....

13. As permissões 603 são adequadas para o ficheiro /etc/passwd.....

14. O NSS e o PAM ("Pluggable Authentication Modules") são dois sistemas alternativos que fazem exactamente o mesmo .....

15. Quando se utiliza a gestão de quotas, o comando "quotacheck" deve ser utilizado regularmente .....

16. O comando "chmod 705 lista.txt" dá a todos os utilizadores permissão para ver o conteúdo do ficheiro "lista.txt".....

17. O comando "vconfig" serve para configurar servidores virtuais no "Apache".....

18. O "PUTTY" pode ser usado para o acesso a um servidor Ubuntu, mesmo ele não tenha instalado um servidor SSH.....

19. O comando "ip" pode ser usado para gerir as interfaces de rede e a tabela de encaminhamento de um "router" Linux .....

20. As interfaces de VLAN dos servidores Linux podem ser geridas com o comando "ip" ou com o comando "ifconfig".....

21. Em Linux cada interface de rede apenas pode ter um único endereço IPv4 atribuido .....

22. A interface "eth1.22" é uma interface de VLAN, com VLANID=122.....

23. O "Internet Daemon" (INETD) tem como principal vantagem uma melhoria no tempo de resposta aos clientes.....

24. O cliente DHCP usa o protocolo UDP para enviar pedidos em "broadcast" ao servidor DHCP .....

25. No ficheiro de configuração "/etc/resolv.conf" nunca pode existir mais do que uma declaração "nameserver".....

26. O comando "iptables –P FORWARD DROP" afecta a tabela "filter" .....

27. O comando "iptables –A FORWARD –p tcp –j DROP" não afecta o tráfego TCP que tem como destino o próprio servidor .....

28. O comando "iptables –A INPUT –i eth1 –p icmp –j ACCEPT" actua sobre a tabela "nat" .....

29. Os utilizadores não podem alterar as variáveis de ambiente que foram definidas pelo administrador durante o "login".....

30. Um "script" é um ficheiro executável criado através da compilação de ficheiro com código fonte.....

31. A linha "0 4 * * 6 /sbin/quotacheck –avug" no *cron*, faz com que o comando seja executado às 4h00 todas as quintas-feiras...

32. O serviço CRON permite programar a execução de tarefas com precisão ao segundo.....

33. Não existe nenhuma forma de o administrador ("root") impedir os utilizadores de recorrerem ao serviço CRON .....

34. O nível de gravidade de um evento ("severity", "priority" ou "level") não é usado pelo serviço "syslog".....

35. A principal vantagem das cópias incrementais é a economia de tempo nas cópias de grandes volumes de dados.....

36. A criptografia simétrica, com chave pré-partilhada, assegura não só a confidencialidade como também a autenticação.....

37. Um certificado de chave pública diz-se auto assinado quando não contém nenhuma chave pública.....

38. O envio de uma mensagem cifrada com uma chave pública não garante a autenticação do emissor.....

39. O comando "openssl" permite obter a chave privada contida num certificado de chave pública.....

40. O SYSTEM LOGGER ("syslog") pode registar eventos enviados por servidores Linux remotos .....

41. Os ficheiros "utmp" e "wtmp" são configurados no ficheiro "/etc/syslog.conf" .....

42. O comando "who" consulta informação criada pelo System Logger" (syslogd) .....

43. O comando "umask" não tem qualquer efeito sobre objectos já existentes.....

2ª Parte – Administração de servidores Windows

1.Os servidores Windows 2008 dentro de um mesmo domínio, que não são DC, são classificados como Member Server .....

2. No W2K8 o file system por omissão é o FAT32 .....

3. No Windows Server 2008 a instalação em modo Server Core não permite que o servidor seja controlador de domínio .....

4. A base de dados de utilizadores Active Directory apenas pode ser usada por servidores Windows. .....

5. No W2008 o Hyper-V permite que múltiplos Sistemas Operativos compartilhem uma única plataforma de hardware .....

6. O Active Directory (AD) apenas é instalado nos servidores Windows 2008 que são controladores de domínio (DC) .....

7.Os objectos do Active Directory obedecem a determinadas regras, sendo estas denominadas de Schema.....

8. Os PDC "Actve Directory" implementam um servidor KERBEROS .....

9. Num servidor de DNS um registo do tipo CNAME contém um endereço IPv4 .....

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

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

12. No Windows Server 2008 um conjunto de domínios pode ser agrupado numa OU ("Organizational Unit").....

13. No WS2008 se o servidor DHCP funcionar em modo stateless não vai gerir os endereços IPv6 através do DHCP.....

14. Um domínio Windows 2008 Server Active Directory só pode funcionar em associação com um servidor DNS .....

15. O "dcpromo" é utilizado tanto para promover como para despromover um controlador de domínio .....

16. No Windows 2008 Server a administração de uma OU ("Organizational Unit") pode ser delegada.....

17. No Windows 2008 Server o clustering combinado com o NLB permite soluções de alta disponibilidade .....

18. As relações de confiança entre duas florestas são do tipo "shortcut trust".....

19. Entre os domínios pertencentes a uma mesma floresta ("FOREST") existe automaticamente uma relação de confiança.....

20 Para analisar e detectar inconsistências num controlador de domínio o "dcpromo" analisa o Active Directory .....

21.O programa "dcpromo.exe" serve para configurar o serviço DHCP.....

22. Um servidor WS2008 na qualidade de "domain member" não utiliza o Active Directory local.....

23. Um "Read Only Domain Controller" (RODC) permite efectuar a validação das credenciais dos utilizadores.....