Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

*Administração de Sistemas – 2012/2013*

*Exame de Época Especial – 1ª parte prática – 10/Setembro/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. A principal vantagem das cópias incrementais é a economia de espaço nos dispositivos de arquivo _____
2. Os ficheiros "utmp" e "wtmp" não são criados pelo "System Logger" (syslogd) _____
3. A linha de configuração do "System Logger" "*.alert @teste" envia através da rede todos os eventos do nível "alert" _____
4. O "System Logger" (syslogd) aplica o evento apenas à primeira regra concordante que exista no ficheiro de configuração _____
5. Um certificado de chave pública contém a chave privada da entidade certificadora _____
6. A linha do ficheiro /etc/crontab "10 5 * * 1 root /etc/check" define a execução do comando uma vez em cada semana _____
7. Os ficheiros crontab dos utilizadores têm exactamente o mesmo formato que o /etc/crontab _____
8. O comando "iptables –A INPUT –i eth0 -p icmp –j DROP" aplica-se ao tráfego UDP e também TCP, destinado ao servidor _____
9. Um "shell script" é um ficheiro de texto com a permissão de execução activa que contém comandos de "shell" _____
10. O "Internet Daemon" (INETD) tem como principal vantagem a redução do número de processos em escuta num servidor _____
11. O diálogo directo entre cliente e servidor DHCP apenas é possível se ambos se encontrarem na mesma rede IP _____
12. O comando "quotacheck" permite definir o valor de cota "soft" e "hard" para cada utilizador _____
13. Em Linux cada interface de rede apenas pode ter um único endereço IPv4 atribuído _____
14. As alterações produzidas nos ficheiros de arranque da shell definidos pelo utilizador prevalecem sobre as do administrador. _____
15. O grupo primário de um utilizador é determinado pelo /etc/passwd e não pelo /etc/group _____
16. O comando "chmod" permite alterar o proprietário e grupo de um ficheiro ou directório _____
17. O "Name Service Switch" (NSS) permite que utilizadores definidos em repositórios remotos sejam reconhecidos no servidor _____
18. O ficheiro "/etc/passwd" define todos os grupos a que cada utilizador pertence _____

19. Independentemente do conteúdo do ficheiro /etc/nsswitch.conf, o ficheiro /etc/passwd é sempre consultado .....

20. "/dev/hda1" representa uma partição de um disco do tipo SCSI ou SATA .....

21. A partição SWAP pode ser formatada com o sistema de ficheiros ext3 ou ext4 .....

22. Um certificado de chave pública diz-se auto assinado quando "Subject" = "Issuer" .....

23. Para uma ligação segura usando criptografia de chave pública são necessárias 4 chaves .....

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

25. O comando "iptables –A FORWARD –i eth0 -p udp –dport 500 –j DROP" não se aplica ao tráfego destinado ao servidor .....

26. A interface "eth1:2" é uma interface de VLAN .....

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

28. A pasta HOME dos utilizadores nunca deve ter as permissões 022 .....

29. A definição das partições durante a instalação não é muito importante porque pode ser facilmente alterada mais tarde .....

30. O "System Logger" (syslogd) pode receber eventos via rede, mas apenas de servidores Linux remotos .....

31. Um certificado de chave pública de uma ROOT CA é normalmente auto assinado e tem de ser instalado manualmente .....

32. Para desenvolver um "shell script" é fundamental a utilização de um IDE apropriado .....

33. Um "shell script" é um ficheiro binário executável produzido por um compilador a partir de um ficheiro de texto .....

34. O comando "ip" pode ser usado para gerir a tabela de encaminhamento IPv4 de um "router" Linux .....

35. As permissões 705 num ficheiro permitem a todos os utilizadores lerem o seu conteúdo .....

36. O comando "chown" serve para o proprietário de ficheiros, mas não é válido para directórios .....

37. O comando "chmod o+x lista.txt" dá a todos os utilizadores permissão para ver o conteúdo do ficheiro "lista.txt" .....

38. A pasta HOME dos utilizadores deve pertencer sempre ao utilizador "root" .....

39. O módulo "Name Service Switch" (NSS) "libnss_dns.so" é usado na pesquisa de utilizadores .....

40. Um servidor Linux pode usar simultaneamente várias partições SWAP .....

41. O "System Logger" (syslogd) classifica os eventos de acordo com a análise que faz do seu conteúdo .....

42. As permissões 703 num ficheiro permitem a todos os utilizadores escrever no ficheiro .....

43. A partição SWAP nunca pode estar no mesmo disco da partição ROOT (raiz) .....

## 2ª Parte – Administração de servidores Windows

1. O Hyper V no WS2008 suporta virtualização de múltiplos sistemas operativos, mas apenas se forem Microsoft _____
2. O "Network Load Balancing" permite adicionar novos servidores sempre que necessário _____
3. Um scope DHCP é composto obrigatoriamente por um nome, endereço inicial, endereço final, máscara e "default gateway". _____
4. Uma Tree no Active Directory é um conjunto de controladores de domínio _____
5. Os Serviços de Terminal no WS2008 não suportam encriptação e por isso exigem uma ligação segura _____
6. Um domain controller é responsável pela segurança de um domínio _____
7. O servidor de DNS pode ter um registo do tipo MX onde é indicado o servidor de correio electrónico para o domínio. _____
8. No Ws2008 a instalação em modo Server Core não permite que o servidor seja controlador de domínio _____
9. O Active Directory suporta Kerberos, SSL e certificados X509 de forma a garantir a encriptação dos dados _____
10. No WS2008 a gestão de uma Organizational Unit pode ser delegada _____
11. O Controlador de Domínio não tem obrigatoriamente instalado localmente um servidor de DNS. _____
12. O Sistema de ficheiros NTFS não suporta file system journaling. _____
13. O Servidor Controlador de Domínio é conhecido na rede pelo nome Fully Qualified Domain Name do domínio _____
14. Com o Hyper-V podemos emular várias máquinas virtuais com vários sistemas operativos _____
15. Nos servidores DNS baseados em 2008 server nunca podem existir registos estáticos, apenas dinâmicos _____
16. Entre outros mecanismos de segurança os PDC "Actve Directory" utilizam o sistema KERBEROS _____
17. No Active Directory a OU é uma subdivisão abaixo do nível de domínio _____
18. A tabela FAT ("File Allocation Table") do sistema de ficheiros FAT32 é uma tabela de partições _____
19. Um componente de um cluster deve ser apelidado de nó _____
20. No WS2008 o servidor de impressão é uma feature _____
21. No Servidor de DNS um registo do tipo CNAME contém registos de hosts do domínio _____
22. No WS2008 podemos adicionar Roles como por exemplo encriptação de dados Bitlocker _____
23. Uma vantagem de uma rede "Server-based" é podermos definir políticas comuns mandatórias _____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

*Administração de Sistemas – 2012/2013*

*Exame de Época Especial – 2ª parte prática – 10/Setembro/2013*

Número: _____ Nome: _____

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

Bom trabalho.

## Grupo I

(12 valores)

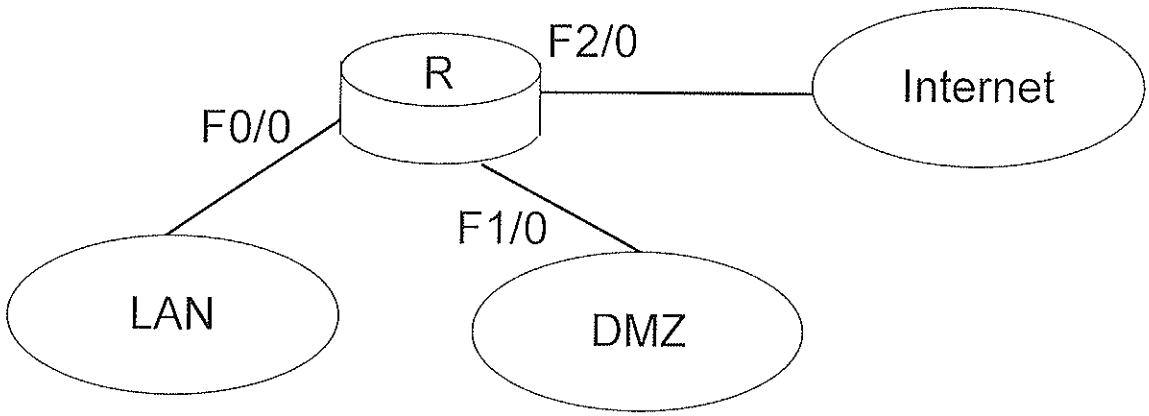
Em cada afirmação assinale V ou F (Verdadeiro ou Falso) conforme considere aplicável.
**Se não tiver a certeza, não responda. Cada resposta errada desconta meia resposta certa.**

1. As ACL *extended* permitem usar como critério o porto de origem _____
2. Pode-se omitir o protocolo numa ACL *extended* mas não numa *standard* _____
3. Uma ACL *standard* pode filtrar o tráfego com base no endereço destino _____
4. Uma ACL permite a aplicação da regra a apenas, por exemplo, 2, 4 ou 8 endereços, mas não a 10 endereços _____
5. O comando **no access-list 105** elimina toda a ACL 105, mas dará erro se ela não existir previamente _____
6. O endereço 12.5.29.32 com o *wildcard* 0.2.0.24 abrange exactamente um conjunto de 8 endereços _____
7. Não se pode configurar um *wildcard* para abranger apenas 128 endereços _____
8. É possível ter um *wildcard* que abrange apenas e só 16 endereços _____
9. O endereço 192.168.0.0 com o *wildcard* 0.0.0.255 nunca deve ser aplicado no sentido *IN* da interface externa _____
10. Uma ACL constituída apenas pela regra **access-list 1 permit 12.0.0.0 5.255.255.255** bloqueia todo o tráfego com origem na rede 14.0.0.0/8 _____
11. A ACL **access-list 5 permit ip 12.0.0.0 0.0.0.255** não é válido _____
12. O endereço 7.5.2.0 associado ao *wildcard* 0.6.1.5 inclui o endereço 7.5.2.2 _____
13. O *wildcard* 0.0.0.45 corresponde a um conjunto de 16 endereços _____
14. O bloqueio de *spoofing* IP deve ser efectuado no sentido *IN* da interface que liga a rede ao interior _____
15. O comando **access-list 109 permit ip any any established** é válido _____
16. Num router só pode existir uma interface **ip nat inside** _____
17. O comando **ip nat inside source list 5 pool A** nega os pacotes cujos endereços de origem existam na ACL 5 _____
18. O NAT só pode ser dinâmico, nunca estático _____
19. O twice 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 12.0.0.190 255.255.255.224 |
| interface F1/0 |
| ip address 12.0.0.30 255.255.255.248 |
| interface F2/0 |
| ip address 13.0.0.126 255.255.255.252 |

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 12.0.0.161 até 12.0.0.163 e 12.0.0.168 até 12.0.0.171 devem poder aceder livremente à DMZ, os restantes apenas podem aceder via HTTP (www) aos nós 12.0.0.17, 12.0.0.24 e 12.0.0.25 e por FTP aos nós 12.0.0.17 e 12.0.0.25.

- A Internet deve poder aceder via HTTP (www) aos nós 12.0.0.17, 12.0.0.24 e 12.0.0.25 da DMZ, deve também poder enviar-lhes pedidos de "echo icmp". Da "Internet" também deve ser possível enviar pedidos de "echo icmp" para todas as interfaces de R. Os restantes acessos da "Internet" devem ser bloqueados, com a excepção 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
```