Administração de Sistemas – 2008/2009 – Recurso prático 1° parte

12/02/2009

Número: _____ **Nome:** _____

Prova a realizar sem recurso a consulta. Duração: 30 minutos.
Em cada afirmação assinale Verdadeiro (**V**) ou Falso (**F**).
Duas respostas incorrectas descontam uma resposta correcta. **Bom trabalho.**

1.O EIGRP é um protocolo standard..... _____

2.O RIPV1 envia a tabela de encaminhamento para o endereço 255.255.255.255 enquanto que o RIPV2 a envia para o endereço 224.0.0.9..... _____

3.O OSPF é um protocolo de encaminhamento tipo híbrido..... _____

4.O OSPF usa o algoritmo DUAL para ser mais rápido na convergência..... _____

5.A instrução **route-map** é utilizada para interligar dois dispositivos de encaminhamento com o mesmo protocolo dinâmico..... _____

6.Num **route-map** só podemos indicar um endereço IP de cada vez para efeitos de *match*..... _____

7.Se for definida uma ACL num router, é de imediato aplicada nos dois sentidos de todas as interfaces activas..... _____

8.Uma ACL aplicada no sentido **IN** verifica os pacotes que entram nessa interface..... _____

9.A ACL **access-list 1 permit 15.3.1.4 0.0.0.3** permite os pacotes com endereço de origem **15.3.1.4**, **15.3.1.5**, **15.3.1.6** e **15.3.1.7**..... _____

10.Uma ACL standard filtra os pacotes baseado no endereço IP de destino..... _____

11.Uma ACL standard permite filtrar com base no protocolo..... _____

12.Numa solução *multihomed NAT*, uma só tabela de NAT é partilhada entre todos os dispositivos de NAT..... _____

13.O CBAC é uma funcionalidade que permite aligeirar uma firewall verificando apenas os endereços de origem e de destino..... _____

14.No modo **transporte**, o IPsec mascara os endereços IP de origem e de destino..... _____

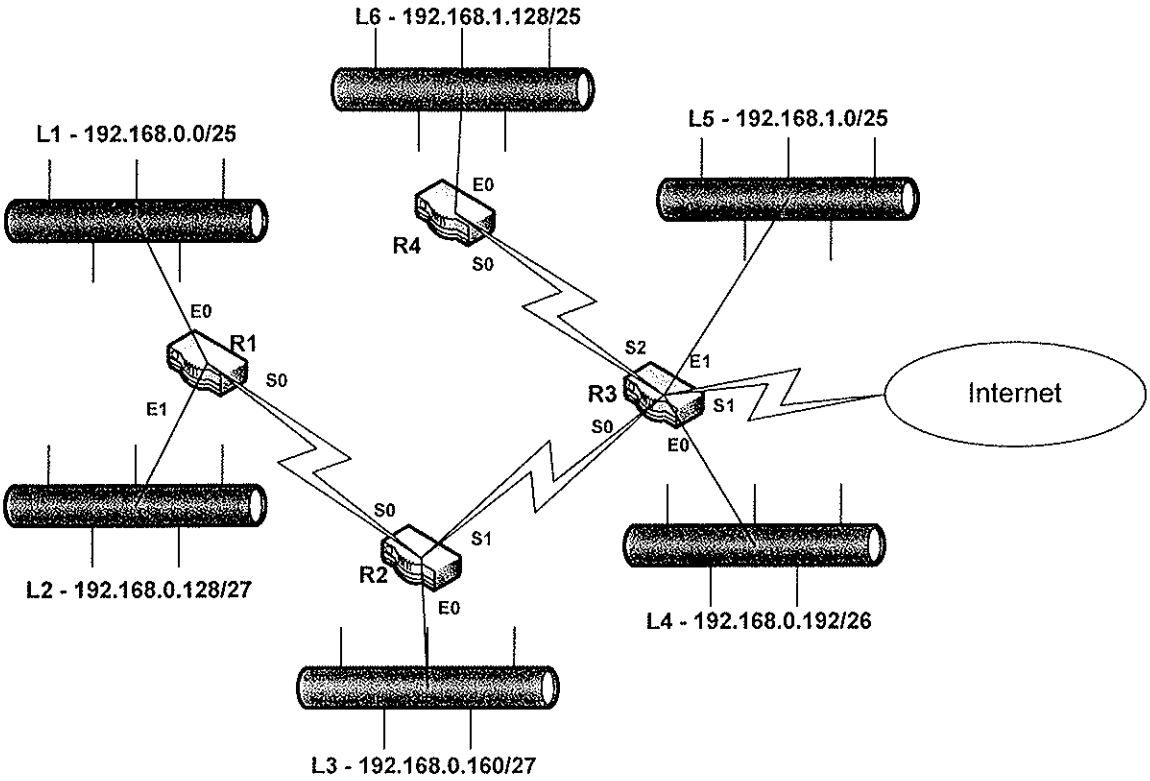
15.A crypto access list **access-list 100 permit tcp host 12.0.0.1 host 11.0.0.1 eq ftp** implica que apenas o *host* 12.0.0.1 possa comunicar com o *host* 11.0.0.1 em FTP..... _____

16.Para que o CBAC seja utilizado, deve estar sempre permitido o tráfego em análise, por exemplo, no sentido IN da interface externa..... _____

17.O CBAC verifica por omissão todas as comunicações que passam pelo dispositivo..... _____

18.Num contexto de segurança, a integridade é obtida pela encriptação da informação..... _____

19. Tendo em atenção a figura onde os routers estão configurados com um encaminhamento dinâmico:



Pretende-se que:

a) A rede L1 não acede à Internet acedendo a tudo o resto.

b) Na rede L2 apenas o 9°, 10° e 11° endereço IP disponível acedem à Internet mas todos os sistemas acedem a L1, L3, L4, L5 e L6.

c) A rede L3 não acede à rede L5

d) A rede L4 só acede ao 1° e 9° endereço IP disponível da rede L1, não acedendo a mais nada.

e) Na rede L5 apenas o 4° e o 12° endereço IP disponível acedem a L6, e todos os sistemas acedem a L1, L2, L3, L4, L6 e à Internet.

Escreva as regras de filtragem necessárias para que o objectivo seja atingido. Para cada regra que escreva indique imediatamente a seguir a cada uma o *router* (R1, R2, R3 ou R4), a interface (E0, E1, S0, etc.) e sentido em que será aplicada.

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Exame de Recurso/Melhoria de Administração de Sistemas – 2008/2009

Prática – 2ª Parte (2º Teste) – 12 de Fevereiro de 2009

Número: _____ **Nome:** _____

Prova a realizar sem recurso a consulta. **Duração: 30 minutos.**
Em cada afirmação assinale Verdadeiro (**V**) ou Falso (**F**).
Todas as questões/afirmações têm a mesma cotação. A prova é composta por 2 páginas.
Uma opção mal assinalada sofre um desconto adicional de um quarto de uma opção correcta.
Bom trabalho.

I

As figuras seguintes apresentam partes do conteúdo de ficheiros de configuração de um servidor LINUX:

```
root:x:0:0:root:/root:/bin/bash
a4:x:102:200:a4:/home/a4:/bin/sh
u5:x:105:201:User 5:/home/u5:/bin/bash
u9:x:120:201:User 9:/home/u9:/bin/bash
asousa:x:200:210:AntSou:/home/ert:/bin/csh
```

Figura A

```
root:x:0:
users:x:200:u5,asousa
oper:x:201:
adm:x:210:u5,a4
man:x:300:asousa,u9
```

Figura B

```
/dev/hda1 / ext3 defaults 1 1
/dev/hdb /mnt/cdrom auto defaults 0 0
/dev/hda2 /home ext3 defaults,usrquota,grpquota 1 2
/dev/sda1 /usr/local ext3 defaults 1 3
/dev/sda2 swap swap defaults 0 0
```

Figura C

```
passwd:     files nis
group:      files
hosts:      files dns
```

Figura D

Com base nas figuras apresentadas, classifique de verdadeiro (V) ou falso (F) as seguintes afirmações:

1. O utilizador "asousa" pertence ao grupo "adm" ..... _____
2. O GID do grupo primário do utilizador "a4" é 102 ..... _____
3. Os únicos grupos válidos neste sistema são os que estão definidos no ficheiro representado em B . _____
4. O utilizador "asousa" tem uma "home directory" inválida ..... _____
5. Se não existirem em /etc/group, os nomes de grupos são pesquisados no serviço "nis" ..... _____
6. O grupo "root" não tem nenhum utilizador ..... _____
7. Neste servidor os utilizadores só são válidos se estiverem definidos no ficheiro "/etc/passwd" ..... _____
8. A partição de SWAP encontra-se no mesmo disco que a partição RAIZ ..... _____
9. O utilizador "asousa" tem um UID inválido ..... _____
10. O comando "quotaon –a" vai activar o controlo de cotas na partição RAIZ ..... _____
11. A figura D pode representar parte do ficheiro "/etc/ldap.conf" ..... _____

II

Classifique de verdadeiro (V) ou falso (F) as seguintes afirmações

1. Num servidor LINUX as partições SWAP devem ser o maior possível..... _____

2. O comando "umask" serve para alterar as permissões sobre objectos existentes..... _____

3. As permissões 641 sobre um ficheiro, permitem a leitura a todos os utilizadores do sistema..... _____

4. As cotas de utilizador permitem limitar o tamanho máximo que cada ficheiro pode ter..... _____

5. A cadeia "password" do sistema PAM é usada durante o processo de autenticação dos utilizadores _____

6. O administrador pode controlar o acesso dos utilizadores ao serviço "CRON"..... _____

7. O comando "ifconfig" e o comando "ip" têm funcionalidades equivalentes..... _____

8. A partição ROOT de um servidor LINUX nunca deve ter capacidade inferior a 8 Gb..... _____

9. O INETD/XINETD é adequado para serviços de rede que são pouco utilizados..... _____

10. Um utilizador pode ter cotas diferentes em duas partições de um mesmo disco..... _____

11. O serviço CRON permite definir o dia do mês, mas não o dia da semana..... _____

12. A utilização de criptografia simétrica (chave pré-partilhada) garante a autenticação mútua..... _____

13. Os certificados de chave pública de raiz (ROOT CA) são sempre auto-assinados..... _____

14. O comando "ipconfig" não permite gerir as tabelas de encaminhamento..... _____

15. O módulo "pam_env.so" é a única forma de definir as variáveis de ambiente no início da sessão. _____

16. Para o restauro de um sistema é necessária a cópia integral e todas as cópias incrementais..... _____

17. O "System Logger" (syslogd) pode receber notificações através da rede..... _____

18. O ficheiro "/etc/resolv.conf" determina a forma como são resolvidos os nomes dos utilizadores _____

19. O comando "quotacheck" deve ser executado sobre partições em "montadas"..... _____

20. O comando "`iptables -A INPUT ...`" adiciona uma regra à cadeia INPUT..... _____

21. O "ifplugd" é um cliente DHCP..... _____

22. As cópias incrementais são suportadas tanto pelo comando "tar" como pelo comando "dump"... _____

23. O comando "`last`" recorre a dados existentes no ficheiro "lastlog"..... _____

24. A interface de rede "**eth1.30**" representa uma VLAN (VLANID=30) sobre a interface "**eth1**"..... _____

25. O "System Logger" (syslogd) é responsável pela gestão do ficheiro de registo wtmp..... _____

DEI-ISEP	**Administração de Sistemas Informáticos – Época de Recurso**	Data: 2009/02/12 Pág. 1/4

Número: _____ Nome: _____

A duração máxima do teste é de 45 minutos.

I

Indique neste grupo as afirmações verdadeiras. Cada afirmação pode ter mais do que uma resposta correcta. Duas opções erradas anulam uma opção correcta

Uma Politica de segurança:

☐ Não necessita de ter em conta uma avaliação do nível de risco da empresa

☐ Deve ser usada como um enquadramento para a implementação dos mecanismos de segurança,

☐ Deve ser técnica e organizacionalmente exequível,

☐ Não inclui uma definição clara das áreas de responsabilidade dos diferentes intervenientes (utilizadores, gestão de sistemas, direcção da empresa.

☐ Não deve ser suficientemente flexível para se adaptar a alterações na organização.

☐ Nenhuma das respostas antreriores está correcta

A estratégia de filas WFQ,...

☐ Usa taxas iguais de extracção de bytes para todas as filas criadas para as diferentes conversações

☐ Evita a congestão da rede, descratando aleatoriamente, aumentando a utilização global do "link".

☐ Suporta "precedência IP" e pode usar a informação de precedência para atribuir o QoS a uma aplicação

☐ Obriga a uma definição do numero de filas e das taxas de extracção de bytes para cada fila .

☐ Nenhuma das anteriores está correcta

Considere-se que num Plano de Continuidade de Negócion, uma análise de impacto, para garantia de um determinado nivel de serviço de uma empresa definiu os seguintes indices: RTO:24 horas; RPO: 5 horas. A empresa tem um horário de funcionamento de 2ª a 6ª, entre as 8 e as 18 horas.

☐ Ums salvaguarda total dos dados efectuada todos os dias ente as 0 e as 5 horas garante que o RTO pode ser cumprido.

☐ É necessária uma replicação "on-line" das transacções para cumprir os dois indices.

☐ Com uma replicação de dados efectuada todos os dias de trabalho ás 13 horas e admitindo que seja possivel repor manualmente, em 5 horas, sobre um sistema de recuperação, os dados perdidos em caso de desastre, o RPO é cumprido.

☐ Nenhuma das anteriores está correcta

O IKE (Internet Key Exchange):

☐ É um protocolo de gestão baseado em três protocolos de gestão de chaves, ISAKMP, Oakley e SKEMI que pode ser usado em conjunto com o IPSec

☐ Implementa SAs IPSec unidireccionais

☐ Sobre o IPSec implementa protecção contra ataques por "imitação".

☐ Define os cabeçalhos AH e ESP que podem ser adicionados ao cabeçalho IP, independentemente ou combinados de forma a proporcionar o desejado conjunto de serviços de segurança.

☐ Nenhuma das anteriores está correcta

A tolerância a falhas...

- ☐ Torna as falhas imperceptíveis para os utilizadores.
- ☐ Usa cópias de segurança para garantir que os dados não se perdem.
- ☐ Permite que após algumas horas os sistemas fiquem operacionais.
- ☐ Serve para garantir que as falhas não ocorrem.
- ☐ De "hardware" não é possível de implementar.

As cópias de segurança...

- ☐ Nunca podem usar como suporte discos IDE.
- ☐ Reduzem as consequências da ocorrência de falhas.
- ☐ Devem ser de acesso de leitura livre a todos os utilizadores.
- ☐ Devem ser armazenadas em local distante do original.
- ☐ Devem usar sempre meios amoviveis como suporte.
- ☐ Servem para tornar os sistemas tolerantes a falhas.

A criptografia...

- ☐ Só pode ser usada sobre dados em forma de texto legivel.
- ☐ De chave pública usa a mesma chave para cifrar e decifrar.
- ☐ Com o algoritmo DES é actualmente considerada segura.
- ☐ Com técnicas de blocos não é usada na actualidade.
- ☐ Apenas garante a confidencialidade durante algum tempo.
- ☐ Simétrica necessita de uma distribuição de chaves prévia.

Os algoritmo MD5

- ☐ É um algoritmo de cifragem do tipo simétrico.
- ☐ Gera um código "hash".
- ☐ É usado para verificação de integridade de ficheiros transferidos.
- ☐ Nenhuma das anteriores está correcta

Os certificados de chave pública...

- ☐ Servem para garantir a confidencialidade das chaves públicas.
- ☐ Devem ser transmitidos de forma confidencial.
- ☐ São assinados pela entidade certificadora.
- ☐ Servem para distribuir chaves públicas de um modo seguro.
- ☐ Contêm uma chave que serve para decifrar.

A autenticação com "password protegida" ...

☐ Exige que a "password" circule num canal seguro (cifrado).

☐ É simples de implementar em sistemas Unix que usam o /etc/passwd.

☐ Exige que ambos os intervenientes conheçam a "password".

☐ Permite a distribuição de uma chave de criptografia simétrica.

☐ Usa-se principalmente para autenticar máquinas.

☐ Cifra a "password" antes desta ser enviada.

Numa infra-estrutura de uma SAN...

☐ Pode ser usada uma topologia Fibre Channel "fabric" que é especialmente apaptada para manipular comunicaçõies entre dispositivos de "storage".

☐ iSCSI que obriga á implementação de uma infra-estrutura fisica em fibra optica e a dispositivos de "switching" com sinalização e protolos de rede diferentes dos usados na rede IP.

☐ A utilização de fibra optica e de switchs de fibra obriga obriga á implementação de "Fibre Channel".

☐ O protocolo "FCIP" é especialmente desenhado para interligar multiplas SANs FC locais sobre uma infra-estrutura IP.

☐ Nenhuma das anteriores está correcta

Configuração IKE:

☐ Sobre o Cisco IOS implementa mecanismos para criar automática e dinamicamente chaves expiradas.

☐ Requer a utilização de chaves públicas emitidas por uma autoridade pública de certificação

☐ Usa as SAs estabelecidas pelo IPSec para autenticar entre si os dois peers IPSec que necessitam de estabelecer uma comunicação segura.

☐ Nenhuma das anteriores está correcta

O par chave publica/privada em criptografia assimétrica entre duas entidades A e B ....

☐ Garante a confidencialidade de uma mensagem enviada de A para B se essa mensagem for cifrada com a PubB e decifrada com a PrivB

☐ Garante a autenticação de uma mensagem enviada de A para B se essa mensagem for cifrada com a PubB e decifrada com a PrivB.

☐ Garante a autenticação e confidencialidade de uma mensagem enviada de A para B se essa mensagem for cifrada com a PrivB + PrivA e decifrada com a PubB+PubA

☐ Nenhuma das anteriores está correcta

Sobre o IPSec ....

☐ Para garantir confidencialidade deve implmentar uma associação de segurança AH

☐ Para garantir autenticação forte e integridade deve implementar uma associação de segurança AH

☐ Para garantir autenticação forte, integridade e confidencialidade deve implementar duas associações de segurança: uma AH e outra ESP

☐ Nenhuma das anteriores está correcta

II

Classifique de verdadeiras (V) ou falsas (F) as seguintes afirmações. Uma opção mal assinalada sofre um desconto adicional de um quarto de uma opção correcta

1. O iSCSI não é compativel com as infra-estruturas IP LAN e WAN existentes..... ____

2. Uma SAN (Storage Area Network) é um tipo de rede local especialmente pensada para manipular grandes volumes de dados..... ____

3. Num processo de continuidade de negócio devem ser avaliados logo de início:

   3.1 Se a informação que passa na rede está ou não cifrada..... ____

   3.2 Se existem de processos de cifragem assimétrica..... ____

   3.3 O impacto potencial de cada tipo de desastre ou evento e a magnitude dos riscos resultantes..... ____

   3.4 Se existe um plano de continuidade de negócio e um plano de testes que garanta que ele está actualizado e que é exequivel..... ____

   3.5 Se os switches de backbone são redundantes..... ____

4. A virtualização de storage refere-se ao processo de agregação de recursos de storage em pools..... ____

5. A precedencia IP consiste na utilização dos 3 bits mais significativos do byte ToS do header IP para marcar um pacote..... ____

6. O RED é uma ferramenta de QoS usada para limitar o fluxo ou a largura de banda máxima..... ____

7. O CAR tenta evitar a congestão da rede garantindo que uma fila não fica cheia, para que haja sempre espaço para os pacotes de mais alta prioridade..... ____

8. Fibre Channel over IP (FCIP) traduz dados e códigos de controlo FC para pacotes IP para que eles possam ser transmitidos entre redes IP geograficamente distantes..... ____

9. Fibre Channel é um protocolo que permite a clientes (iniciadores) enviar comandos SCSI para dispositivos de storage SCSI (targets) em servidores remotos..... ____