DEI-ISEP	**Administração de Sistemas Informáticos – Época Normal**	Data: 2009/01/22 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

Algumas considerações importantes a ter em conta na definição de uma politica de Segurança Informática numa organização são...

☐ Uma correcta definição dos ataques possíveis, tendo em conta os factores humanos

☐ Implementação de uma linha de defesa contra intrusão com múltiplos firewalls..

☐ Assegurar que todos os elementos do departamento de informática são envolvidos na definição dessa politica, independentemente dos elementos dos outros sectores da organização.

☐ Nenhuma das anteriores está correcta

Nos sistemas informáticos, as falhas ...

☐ Nunca podem ser provocadas pelos utilizadores.

☐ De confidencialidade podem ser combatidas com cópias de segurança.

☐ Podem ter menores consequências se existirem cópias de segurança actualizadas.

☐ De energia podem ser totalmente resolvidas por uma UPS com bateria.

☐ Devem ser imperceptiveis quando existe tolerância a falhas.

☐ Incluem situações de tempo de resposta elevado para um serviço de rede.

A criptografia simétrica ...

☐ utiliza a mesma chave para cifrar e decifrar

☐ facilita a distribuição de chaves públicas.

☐ consegue ser mais rápida do que a de chave pública.

☐ usada actualmente emprega chaves com 64 bits.

☐ não pode usar chaves com mais do que 128 bits.

☐ não é suficientemente segura para as aplicações actuais.

O algoritmo ...

☐ RC4 é um algoritmo de cifragem de chave pública.

☐ de cifragem RC5 suporta vários comprimentos de chave.

☐ DES suporta chaves de 128 bits.

☐ MD5 é um algoritmo de cifragem simétrica.

☐ 3DES usa 3 chaves DES distintas.

As chaves públicas RSA podem ser usadas para ...

☐ produzir uma assinatura digital.
☐ verificar a origem de uma mensagem.
☐ produzir um "hash code".
☐ produzir um "checksum" criptográfico.
☐ cifrar usando criptografia simétrica.
☐ cifrar mensagens para garantir a confidencialidade.

A distribuição de chaves ...

☐ é muito mais simples para as chaves públicas.
☐ por "puzzles" é muito usada na actualidade.
☐ secretas pode ser feita usando certificados de chave pública.
☐ públicas tem de garantir a confidencialidade das mesmas.
☐ secretas pode ser feita por correio electrónico.
☐ secretas pode ser realizada durante a autenticação do utilizador.

As assinaturas digitais ...

☐ não garantem a integridade/origem de um documento.
☐ apenas podem ser verificadas pelo emissor.
☐ servem propositos diferentes das assinaturas manuais.
☐ devem impossibilitar a negação de autoria.
☐ devem garantir a confidencialidade.
☐ mais usadas actualmente aplicam criptografia de chave pública.

Pode-se definir "precedencia IP" como ...

☐ Protocolo usado os tipos de filas numa interface de output para a definição do QoS
☐ Utilização dos 3 bits mais significativos do campo TOS num header IP, para marcar um pacote IP
☐ Metodologia de sinalização entre um host e uma aplicação num servidor, para garantir um determinado nível de largura de banda para o acesso a essa aplicação.
☐ Metodologia para evitar a congestão de uma interface sob o TCP
☐ 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 PrivA e decifrada com a PubA

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

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

☐ Nenhuma das anteriores está correcta

O WRED (Weight Random Early Detection) usa a seguinte estratégia de gestão de tráfego, para evitar a congestão da rede...

☐ Cria processos de sinalização entre aplicações e a rede para garantir níveis de largura de banda através da rede

☐ Implementa funcionalidades de controlo de fluxo do TCP

☐ A precedência IP para definir critérios para descartar os pacotes de mais baixa prioridade antes de descartar os de alta prioridade.

☐ O mecanismo de filas do WFQ para controlar o fluxo de pacotes de uma conversação, de acordo com o QoS acordado.

☐ Nenhuma das anteriores está correcta

Numa SAN:

☐ Com o protocolo iSCSI é possivel a utilização da infra-estrutura de rede IP existente, incluindo switches, routers, adaptadores de rede,....

☐ As interfaces do tipo TOE (TCP Offload Engine") permitem, sobre o iSCSI, obter melhores taxas de transferencia de dados relativamente ás interfaces de rede classicas.

☐ O protocolo "FCIP" é especialmente desenhado para interligar duas redes iSCSI sobre uma estrutura "Fibre Channel".

☐ Nenhuma das anteriores está correcta.

Quais as afirmações correctas

☐ Num planeamento de um processo de continuidade de negócio o Recovery Time Objective (RTO) para os diferentes processos de negócio de uma empresa é estabelecido durante a fase de análise de impacto de uma ruptura de continuidade no negócio e depois apresentado á gestão da empresa para aceitação .

☐ O Recovery Time Objective (RTO) consiste na definição do tempo necessário para restaurar um backup total depois da ocorrência de um desastre, de forma a evitar consequências inaceitáveis associadas á quebra de continuidade do negócio.

☐ O Recovery Point Objective (RPO) define o intervalo de tempo necessário para restaurar os dados de um backup.

☐ 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. RSVP é uma camada de transporte capaz de fornecer níveis diferenciados de serviço para os diferentes fluxos de dados ..... ___

2. A definição de um QoS permite proporcionar um tratamento preferencial a um determinado fluxo de dados. Deve também proporcionar um serviço suficiente para o trafego dos restantes fluxos ..... ___

3. Algumas considerações importantes para a definição de uma correcta politica de segurança são:

   3.1 Ter em conta os factores humanos ..... ___
   3.2 Limitar o ambito de acessos ..... ___
   3.3 Ter apenas em conta os acessos via rede informática ..... ___
   3.4 Não esquecer a segurança fisica ..... ___
   3.5 Conhecer os pontos fracos ..... ___
   3.6 Cifrar toda a informação que passa sobre a rede ..... ___
   3.6 Conhecer bem o ambiente onde está inserido ..... ___

4. Um objectivo importante da monitorização de recursos de rede consiste em proporcionar ao Administrador de Sistema informação exaustiva e permanente sobre todos os problemas da rede ..... _

5. Uma gestão de configurações sobre uma rede informática deve monitorizar as informações de configuração da rede de forma a que os efeitos sobre a operação das diferentes versões de HW e SW possa ser controlado ..... ___

6. Uma correcta gestão de falhas sobre uma rede informática deve detectar e registar as falhas ocorridas e notificar os operadoresde forma a que as falhas possam ser rápidamente resolvidas e que a rede continue em operação ..... ___

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2008/2009 – Exame prático 1º parte

22/01/2009

Efectue as correcções na tabela de routing (se aplicável) e 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*, interface (LAN ou WAN) e sentido em que a aplicaria.

Número: _____ **Nome:** _____

Prova a realizar sem recurso a consulta. Duração: 30 minutos.
Nas questões de escolha múltipla, seleccione todas as opções correctas.
Duas respostas incorrectas descontam uma resposta correcta. **Bom trabalho.**

1. Relativamente ao NAT tal como definido nas RFC's:
   - ☐ No NAT bidireccional, uma entrada dinâmica criada permanece válida até que seja reiniciada a tabela de NAT, por exemplo, pela reinicialização do dispositivo
   - ☐ No NAT bidireccional é possível definir um número máximo de associações dinâmicas
   - ☐ No NAT bidireccional não podem existir entradas estáticas de NAT
   - ☐ O Twice NAT permite o suporte de ligações entre redes distintas que partilham o mesmo espaço de endereçamento público
   - ☐ Uma das suas desvantagens é uma completa dependência de um só dispositivo
   - ☐ Nenhuma das afirmações anteriores é verdadeira
2. A interligação entre dispositivos com protocolos de encaminhamento dinâmicos diferentes:
   - ☐ Não é possível de efectuar
   - ☐ Pode ser efectuada
   - ☐ Não é conveniente, devendo ser evitada
   - ☐ Nenhuma das afirmações anteriores está correcta
3. Relativamente ao IPsec:
   - ☐ Inclui peers e associações de segurança
   - ☐ Pode ser configurado em modo transporte ou em modo túnel
   - ☐ Permite autenticação ou encriptação, nunca os dois em simultâneo
   - ☐ Qualquer que seja o modo, o header IP inclui sempre o IP original
   - ☐ O AH proporciona autenticação
   - ☐ O AH proporciona autenticação e encriptação
   - ☐ Uma *crypto Access list* filtra os pacotes que podem ou não atravessar o interface
4. Observando apenas a ACL **access-list 1 permit 193.136.62.0 0.0.0.129** podemos afirmar que:
   - ☐ É uma access list standard
   - ☐ Permite o tráfego dos hosts da rede 193.136.62.0 desde o 193.136.62.1 até ao 193.136.62.129
   - ☐ Impede o tráfego dos hosts da rede 193.136.62.0 desde o 193.136.62.130 até ao 193.136.62.254
   - ☐ Nenhuma das opções anteriores é verdadeira
5. O encaminhamento dinâmico:
   - ☐ Não pode coexistir com o encaminhamento estático
   - ☐ Deve ser configurado indicando os caminhos possíveis para os destinos pretendidos

☐ Não impede que não haja um *match* com um destino pretendido, assumindo que todos os dispositivos estão bem configurados

☐ Nenhuma das opções anteriores é verdadeira

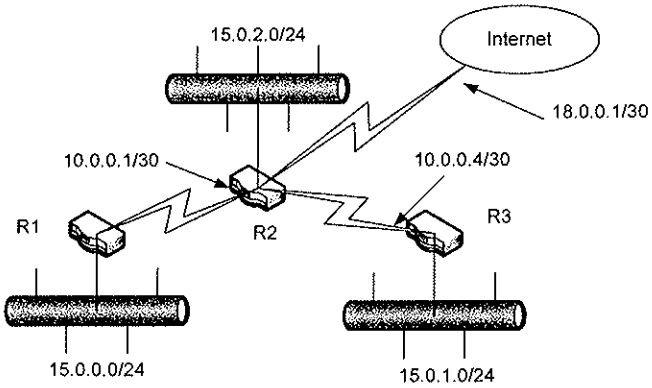
6. O encaminhamento estático:
   ☐ Tem um limite de 256 entradas máximas
   ☐ Quanto mais detalhado for, melhor a performance global da rede
   ☐ Se nada for indicado em contrário, envia todos os pacotes recebidos para a *default route*
   ☐ Se não tiver definida uma *default route* e estiver a tratar de um pacote que não faz *match* com nenhuma linha, envia-o para o primeiro dispositivo da lista para que o encaminhe
   ☐ Nenhuma das opções anteriores é verdadeira
7. Se um *router* com encaminhamento dinâmico bem configurado mas sem *default route* receber um pacote com um destino que desconhece:
   ☐ Guarda-o em memória até que a tabela de encaminhamento seja corrigida
   ☐ Descarta-o como destino inantingível
   ☐ Propaga-o para todos os destinos que conhece para que o encaminhem
   ☐ Nenhuma das opções anteriores é verdadeira
8. Relativamente ao protocolo EIGRP:
   ☐ É um protocolo standard
   ☐ Por omissão, faz a agregação das redes baseado na classe
   ☐ Propaga as redes e as máscaras
   ☐ Envia sempre toda a tabela de encaminhamento
9. A ACL
   access-list 198 deny tcp host 197.23.2.1 194.65.13.64 0.0.1.63 eq http
   access-list 198 deny ip host 197.23.2.1 194.65.13.64 0.0.1.63
   access-list 198 permit ip any any
   ☐ É uma ACL extended
   ☐ Permite que o *host* com endereço 197.23.2.1 comunique em qualquer protocolo com qualquer *host* das redes 194.65.13.64/28 e 194.65.12.64/28
   ☐ Só permite ao *host* 197.23.2.1 comunicar com os *hosts* das redes 194.65.13.64/28 e 194.65.12.64/28 em http
   ☐ Nega o acesso em http do *host* 197.23.2.1 a qualquer sistema
10. A *Crypto Access List* **access-list 100 permit ip 192.0.0.0 0.0.0.63 195.0.0.0 0.0.0.63**:
    ☐ Nega o tráfego proveniente dos *hosts* 192.0.0.64 até 192.0.0.255 destinado aos *hosts* 195.0.0.1 até 195.0.0.63
    ☐ Permite o tráfego proveniente dos *hosts* 192.0.0.1 até 192.0.0.63 destinado aos *hosts* 195.0.0.1 até 195.0.0.63
    ☐ Nada nos diz sobre o tráfego permitido ou negado, apenas nos indica o que é protegido
    ☐ Nenhuma das respostas anteriores é verdadeira
11. O RIPv2:
    ☐ É um protocolo de encaminhamento estático standard
    ☐ Propaga as actualizações de 30 em 30 segundos
    ☐ Propaga toda a tabela de 30 em 30 segundos

☐ Nunca consegue eliminar rotas inatingíveis

☐ Propaga apenas os endereços

☐ Nenhuma das respostas anteriores é verdadeira

12. Tendo em atenção a figura e as tabelas de routing estático seguinte:



Router R1	
0.0.0.0	10.0.0.1

Router R2	
15.0.0.0/24	10.0.0.2
15.0.1.0/24	10.0.0.4
0.0.0.0	18.0.0.1

Router R3	
0.0.0.0	10.0.0.5

Pretende-se que:

a) A rede 15.0.1.0/24 só consiga aceder aos quatro primeiros *hosts* da rede 15.0.0.0/24 e ao 10° e 11° *host* da rede 15.0.2.0/24, podendo contudo aceder à Internet tal como todos os outros *hosts* dessa rede.

b) Só os primeiros 5 *hosts* da rede 15.0.2.0/24 possam aceder às redes 15.0.0.0/24 e 15.0.1.0/24, podendo contudo aceder à Internet tal como todos os outros *hosts* dessa rede.

Efectue as correcções na tabela de routing (se aplicável) e 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*, interface (LAN ou WAN) e sentido em que a aplicaria.

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto

Administração de Sistemas – 2008/2009 – 2º Teste Escrito Individual

Número: _____ Nome: _____

Prova a realizar sem recurso a consulta. Duração: 60 minutos.
Em cada afirmação assinale Verdadeiro (**V**) ou Falso (**F**).
Todas as questões/afirmações têm a mesma cotação. A prova é composta por 3 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 vários ficheiros de configuração de um servidor LINUX:

```
root:x:0:
bin:x:220:
adm:x:2:u2
sys:x:1001:daemon
usr:x:101:daemon
```

Figura A

```
passwd:      files ldap
shadow:      files
group:       files
hosts:       files dns ldap
```

Figura B

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:2:bin:/bin:/bin/sh
daemon:x:50:2:daemon:/sbin:/bin/sh
u2:x:105:101:User 2:/home/u2:/bin/bash
sysuser:x:110:1001:Sys User:/tmp:/bin/csh
```

Figura C

```
42 4 1 * * root /etc/check-users
22 4 5 * 2 root /etc/make-backups
*/5 * * * * daemon /etc/check-hosts
20 23 * * 4 u2 /home/u2/test-net
```

Figura D

```
/dev/hda1 / ext3 defaults,grpquota 1 1
/dev/hdb /mnt/cdrom auto defaults 0 0
none /proc proc defaults 0 0
/dev/hdc1 /home ext3 defaults,usrquota 1 2
/dev/hda2 swap swap defaults 0 0
```

Figura E

```
auth,authpriv.*   /var/log/auth.log
*.emerg           *
daemon.err        @192.168.100.5
```

Figura F

```
auth required       pam_env.so
auth sufficient     pam_unix.so nullok
auth sufficient     pam_ldap.so use_first_pass
```

Figura G

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

1. O sistema de ficheiros raiz pertence a um disco do tipo IDE..... _____

2. O utilizador "u2" pertence a 2 grupos..... _____

3. A figura G pode representar parte de um ficheiro de configuração do sistema PAM..... _____

4. O script/programa "/etc/check-users" é executado uma vez por mês..... _____

5. A figura D pode representar parte do ficheiro "/etc/nsswitch.conf"..... _____

6. O serviço "syslog" envia algumas mensagens para "192.168.100.5" ..... _____

7. O utilizador "sysuser" pertence ao grupo "sys" ..... _____

8. O utilizador "daemon" tem como grupo primário o grupo "sys" ..... _____

9. O ficheiro da figura G obriga a que todos os utilizadores se autentiquem no serviço "ldap" ..... _____

10. O utilizador "u2" tem UID=105 ..... _____

11. Os utilizadores só são válidos se estiverem definidos no serviço ldap ..... _____

12. Os nomes de máquinas podem ser procurados no serviço "ldap" ..... _____

13. A partição de SWAP encontra-se no mesmo disco que a partição RAIZ ..... _____

14. O script/programa "`/etc/check-hosts`" é executado de 5 em 5 minutos ..... _____

15. O comando "quotaon –a" vai activar o controlo de cotas na partição `/dev/hdc1` ..... _____

16. Os eventos de nível "`daemon.panic`" são apresentados nos terminais de todos os utilizadores ... _____

17. Os grupos válidos são apenas os que estão definidos no /etc/group ou no serviço "ldap" ..... _____

18. A figura F pode representar parte do ficheiro "`/etc/nsswitch.conf`" ..... _____

19.A partição montada em "/home" pertence ao mesmo disco que a partição "/" ..... _____

20. A figura A pode representar parte do ficheiro "/etc/passwd" ..... _____

21. O grupo "bin" não tem nenhum membro ..... _____

22. Os eventos "`auth.info`" são acrescentados ao ficheiro "/var/log/auth.log" ..... _____

23. Todos os scripts/programas do /etc/crontab são executados com permissão de "root" ..... _____

24. A figura B pode representar parte do ficheiro "/etc/services" ..... _____

25. O script/programa "/etc/make-backups" é executado todas as semanas ..... _____

26. A configuração da figura G refere-se à forma como os utilizadores mudam de "password" ..... _____

27. A unidade de leitura de CD é do tipo SCSI ..... _____

II

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

1. O ficheiro "/etc/resolv.conf" determina quais são os servidores DNS a utilizar ..... _____

2. O comando "quotacheck" deve ser executado com as partições em utilização ..... _____

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

4. O serviço "inetd" é um servidor HTTP ..... _____

5. O serviço "CRON" apenas pode ser usado por quem o administrador desejar ..... _____

6. Os certificados de chave pública auto assinados têm de ser instalados manualmente ..... _____

7. A UMASK 0075 não é normalmente aconselhável ..... _____

8. O serviço "INETD" usa definições de serviços, normalmente residentes em "/etc/services" ..... _____

9. O comando "ifconfig" permite gerir as tabelas de encaminhamento ..... _____

10. O ficheiro "utmp" tem um tamanho proporcional ao número de terminais existentes ..... _____

11. A interface de rede "**eth0:3**" representa uma VLAN sobre a interface "**eth0**" ..... _____

12. A adição e remoção de interfaces VLAN realiza-se com o comando "ifconfig" ..... _____

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

14. O comando "`iptables`" permite administrar a filtragem de tráfego de rede ..... _____

15. O módulo "pam_env.so" permite definir as variáveis de ambiente no início da sessão ..... _____

16. Os certificados de chave pública só são válidos se emitidos por uma "ROOT CA" ..... _____

17. As cópias incrementais têm a grande vantagem de serem mais rápidas ..... _____

18. O comando "`iptables -P FORWARD DROP`" adiciona uma regra à cadeia FORWARD ..... _____