Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto
Administração de Sistemas – 2013/2014 – Exame Teórico
Exame de época normal – 06 de fevereiro de 2014

Número: _____ Nome: _____

Prova a realizar sem recurso a consulta. LER COM ATENÇÃO
Duração: 55 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 pelo funcionamento do CPD ("Centro de Processamento de Dados"), mas não pela sua instalação inicial..... _____
2. O acesso físico ao CPD apenas deve ser usado para operações de administração que não podem ser realizadas remotamente..... _____
3. Uma das vantagens da virtualização de "hardware" é que permite reduzir a taxa de utilização dos recursos físicos ..... _____
4. A virtualização de servidores aumenta o número de operações de administração que podem ser realizadas remotamente ..... _____
5. Se um servidor virtual consumir uma quantidade exagerada de recursos, não há forma de impedir que isso interfira com os restantes servidores virtuais..... _____
6. Na virtualização de "storage" os servidores disponibilizam aos clientes o acesso ao sistema de ficheiros através de diretórios partilhados (pastas partilhadas).. _____
7. As SAN ("Storage Area Network") do tipo iSCSI são dispendiosas porque obrigam à utilização de "hardware" especificamente desenvolvido para o efeito ..... _____
8. Uma vez que ambos usam TCP/IP, é possível ligar diretamente dispositivos iFCP com dispositivos iSCSI..... _____
9. O TOE ("TCP/IP Offload Engine") é um componente de "hardware" que contém uma implementação do protocolo iSCSI..... _____
10. Duas SAN do tipo FCoE ("Fibre Channel over Ethernet") podem ser diretamente ligadas através da INTERNET ..... _____
11. Na terminologia iSCSI designa-se por "initiator" o servidor que fornece discos lógicos a outras máquinas..... _____
12. O parâmetro MTBF ("Mean Time Between Failures") aumenta quando a probabilidade de falha diminui ..... _____
13. O MTBF de um sistema redundante é igual ao menor dos MTBF dos seus componentes ..... _____
14. Um sistema que em média está inoperante durante um dia por ano tem uma disponibilidade do tipo "três noves" (364/365 = 0,997260...)..... _____
15. Um sistema com uma UPS que ordena o encerramento dos servidores após 10 minutos de falha de energia pode ser classificado como "fail safe" ..... _____
16. Se vários servidores partilham uma ligação de rede, essa ligação de rede constitui um SPOF ("Single Point Of Failure") ..... _____
17. A diferença entre um sistema de discos redundante RAID 1 e RAID 2 é que o primeiro usa apenas um disco e o segundo necessita de dois discos iguais..... _____
18. A quantificação do risco associado a uma dada falha depende exclusivamente da probabilidade dessa falha ocorrer..... _____
19. O RPO ("Recovery Point Objective") especifica uma quantidade de tempo medida após o instante em que ocorre o desastre ..... _____
20. O DRP ("Disaster Recovery Plan") é constituído por BCP ("Business Continuity Plan") e "Política de segurança" ..... _____
21. Um plano de "backup/restore" com uma cópia integral semanal e cópias incrementais diárias é suficiente quando se pretende um RPO de 12 horas..... _____
22. A grande vantagem da utilização de cópias incrementais relativamente a cópias integrais é que reduz o tempo necessário à realização da cópia..... _____
23. Para implementar uma continuidade de negócio de categoria 3 ("Tier 3") é necessário recorrer a "mirroring" síncrono de discos ..... _____
24. Entre muitos outros aspetos, a "Política de segurança" deve estabelecer regras para a definição e manuseamento das "passwords" dos utilizadores..... _____
25. A utilização de uma chave pública para cifrar dados (cifra assimétrica) não dá garantias ao recetor da identidade do emissor ..... _____
26. O "não repúdio" deve ser garantido pelas assinaturas digitais, consiste em impedir que uma entidade possa negar que recebeu uma dada mensagem..... _____
27. Um certificado de chave pública identifica duas entidades: proprietário ("owner") e emissor ("issuer"), e transporta a chave pública do proprietário..... _____
28. É pouco provável encontrar duas mensagens pouco diferentes que produzam o mesmo resultado com a aplicação de uma dada função "hash"..... _____
29. O algoritmo AES ("Advanced Encryption Standard"") é do tipo assimétrico e é normalmente utilizado com chaves de 1024 ou 2048 bits..... _____
30. O CHAP ("Challenge Handshake Authentication Protocol") garante a autenticidade de ambos os intervenientes, mas necessita de um segredo pré partilhado _____
31. Num sistema AAA, o NAS ("Network Access Service") permite ou não o acesso de acordo com a resposta do PDP ("Policy Decision Point")..... _____

32. Uma limitação dos servidores RADIUS é que o PIP ("Policy Information Point") tem de estar localizado na mesma máquina física do servidor ____

33. Ao contrário do que acontece com o protocolo RADIUS, no protocolo TACACS+ a autenticação e a autorização são verificadas separadamente ____

34. Em certos casos, o servidor LDAP ("Lightweight Directory Access Protocol") pode assumir a função PDP, mas normalmente assegura a função PIP ____

35. As bases de dados LDAP são especialmente eficientes para operações de escrita. Devido à sua estrutura em árvore, as operações de consulta são lentas ____

36. Implementar redundância com servidores LDAP é complexo devido à dificuldade em manter a sincronização ____

37. Numa base de dados LDAP não pode haver dois objectos diferentes a pertencer à mesma classe estrutural ____

38. Numa base de dados LDAP o DN ("Distinguished Name") de um objeto define a localização do mesmo na DIT ("Directory Information Tree") ____

39. No sistema KERBEROS os nomes "exemplo.com" e "EXEMPLO.COM" identificam um mesmo "realm" ____

40. A pré-autenticação no sistema KERBEROS impede que intrusos consigam obter um TGT ("Ticket Granting Ticket") ____

41. No sistema KERBEROS é impossível um "principal" de um "realm" estabelecer sessões com "principals" de outros "realms" ____

42. O "Active Directory" da Microsoft, além de serviços LDAP, usa também o sistema KERBEROS ____

43. A mensagem "ServerHello", usada no TLS ("Transport Layer Security"), é enviada pelo cliente ao servidor indicando qual o "cipher suite" a utilizar ____

44. Em TLS o "cipher suite" "TSL_RSA_WITH_AES_256_CBC_SH256" significa que a autenticação é realizada através de certificados de chave pública ____

45. O "firewall" que separa a DMZ ("DeMilitarized Zone") da "Internet" nunca pode ser o mesmo que separa a DMZ da "Intranet" ____

46. A funcionalidade "stateful packet inspection" (SPI) leva a que o "firewall" tenha um comportamento que depende apenas do pacote individual que analisa ____

47. Os ataques de "sniffing" (inspeção furtiva) podem ser combatidos com um "firewall", desde que seja um "firewall" dinâmico ____

48. A maioria dos ataques do tipo DoS ("Denial of Service"), podem ser combatidos de forma eficaz com recurso a "firewalls" estáticos ____

49. As implementações ARP ("Address Resolution Protocol") estão expostas a ataques do tipo "SYN flood" ____

50. Os ataques MITM ("Man-in-the-middle") podem ser evitados se forem utilizados mecanismos de autenticação em todas as comunicações ____

51. Os ataques com "spoofing" de endereços IP são mais complexos de realizar sobre serviços TCP do que sobre serviços UDP ____

52. O ataque DDOS ("Distributed DOS") refletido só é possível se a origem do ataque não estiver protegida contra "spoofing" ____

53. No IPsec, o "Encapsulating Security Payload" (ESP) nunca pode ser usado em "Transport mode" ____

54. Qualquer um dos dois mecanismos do IPsec, ESP ou AH ("Authentication Header"), permitem garantir a autenticação ____

55. A utilização do IPsec em "Transport mode" implica que a confidencialidade dos dados transportados nos pacotes nunca pode ser assegurada ____

56. O protocolo IKE ("Internet Key Exchange Protocol") versão 2 utiliza o algoritmo "Diffie-Hellman" apenas na "Phase 1" ____

57. O IPsec nunca pode ser usado quando existem dispositivos NAT ("Network Address Translation") interpostos ____

58. Numa VPN do tipo LAN-LAN, cada utilizador estabelece uma ligação VPN independente com o servidor, tendo para o efeito de se autenticar ____

59. O "Layer 2 Tunneling Protocol" (L2TP) isoladamente não permite implementar uma VPN, para esse efeito, tem de ser aliado por exemplo ao IPsec ____

60. O protocolo PPTP ("Point to Point Tunneling Protocol") inclui mecanismos de segurança que garantem a autenticação e a confidencialidade ____

61. Nas transmissões de dados em tempo real, geralmente a utilização de mecanismos de correção de erros com retransmissão não faz sentido ____

62. A compressão de cabeçalhos ("header compression") é normalmente aplicada entre "routers" diretamente interligados, não entre nós finais ____

63. O LFI ("Link Fragmentation and Interleaving") tem impacto negativo nos pacotes não prioritários de grande dimensão ____

64. Sob o ponto de vista do TCP o RTO ("Retransmission TimeOut") e o RTT ("Round-Trip Time") são a mesma coisa e têm sempre valores iguais ____

65. Quando um nó emissor entra em modo "Slow Start", esse facto não afeta a emissão de "datagramas" UDP ____

66. Através do RED ("Random Early Detection") os nós intermédios levam alguns emissores a entrar em modo "Slow Start" ____

67. O CAR ("Committed Access Rate") é uma técnica HARD QoS, por isso cada tipo de tráfego está limitado a uma fração da capacidade disponível ____

68. Na gestão de filas "Priority Queuing" (PQ), após processar um pacote, o pacote seguinte será o da fila de prioridade imediatamente abaixo ____

69. Com um conjunto de 10 filas do tipo "Fair Queuing" (FQ), para uma ligação com 1 Gbps, cada fila dispõe de uma capacidade de cerca de 100 Mbps ____

70. O "Weighted RED" (WRED) diferencia-se do RED porque no primeiro os pacotes que estão mais tempo em espera são descartados em primeiro lugar ____

Departamento de Engenharia Informática – Instituto Superior de Engenharia do Porto
Administração de Sistemas – 2013/2014 – Prova prática
Exame de época normal – 06 de fevereiro de 2014

Número: _____ **Nome:** _____

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

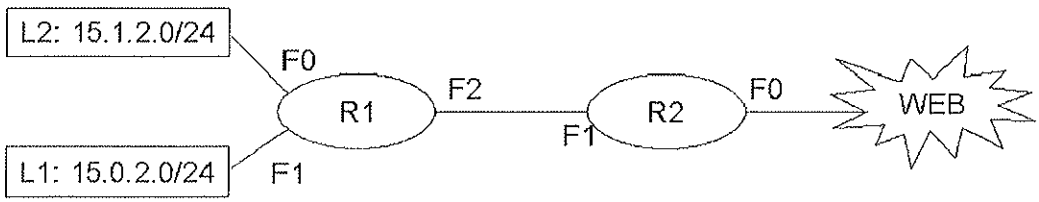
Grupo I (50%)

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.

1. A SHELL (sh/bash) e a CSHELL (csh/tcsh) usam exactamente os mesmos ficheiros de arranque ..... _____
2. O serviço CRON pode ser usado pelos utilizadores normais apenas se o administrador o permitir ..... _____
3. Um certificado de chave pública contém a chave privada da entidade certificadora ..... _____
4. A linha de configuração do "System Logger" "*.alert @teste" envia através da rede todos os eventos do nível "alert" ..... _____
5. No ficheiro "/etc/passwd", o último campo de cada linha é o UID do utilizador ..... _____
6. Os comandos "useradd" e "usermod" apenas funcionam para utilizadores que estão definidos no ficheiro "/etc/passwd" ..... _____
7. Toda a configuração dos vários módulos NSS está guardada no ficheiro "/etc/nsswitch.conf" ..... _____
8. Uma interface de rede nunca pode ter mais do que um endereço IPv4 associado a ela ..... _____
9. O ficheiro "/etc/resolv.conf" é o principal ficheiro de configuração do servidor DHCP ..... _____
10. A linha de configuração do CRON começada por "*/15 3 * * *" é executada 24 vezes por dia ..... _____
11. Uma "feature" disponível no Windows 2008 Server é o Active Directory Domain Services ..... _____
12. As regras que definem os objectos que são armazenados no Active Directory são denominadas "schemas" ..... _____
13. Apesar da replicação "multimaster" se um Domain Controller falhar numa rede Windows 2008 Server, a rede pára ..... _____
14. Um "site" representa a estrutura lógica de uma rede e um "domínio" a estrutura física ..... _____
15. O par endereço IP e "wildcard" 21.13.1.0 0.0.0.254 representa todos os endereços da rede 21.13.1.0 excepto o 21.13.1.0 .... _____
16. O par endereço IP e "wildcard" 170.12.0.64 0.2.0.31 inclui o endereço IP 170.13.0.95 ..... _____
17. A regra de ACL "access-list 10 deny ip 190.0.1.0 0.0.0.255" é válida ..... _____
18. O "bidirectional NAT" exige sempre um servidor DNS com as extensões ALG instaladas ..... _____
19. Uma interface de um "router" pode ter no máximo duas regras de ACL aplicadas ..... _____
20. Uma ACL extended só pode conter um tipo de serviço se o protocolo não for do nível 3 do modelo OSI ..... _____

Grupo II (50%)

Observe o seguinte diagrama de rede



Os endereços IPv4 dos "routers" são os seguintes:

R1	F0: 15.1.2.254/24 F1: 15.0.2.254/24 F2: 15.0.0.2/30
R2	F0: 9.0.0.2/30 F1: 15.0.0.1/30

Escreva os comandos (CISCOIOS) que permitem implementar as seguintes políticas de acesso. Tendo em vista a eficiência, as ACLs devem conter o menor número de regras possível.

- Bloquear o "spoofing" IP com origem nas redes locais e na "Internet"
- L2 pode enviar pedidos de "echo" ICMP para qualquer interface de R1 e R2
- L2 pode aceder à Internet
- L2 pode aceder a L1 em TCP
- A Internet pode enviar pedidos de "echo" ICMP para L2 mas não para L1, R1 e R2
- A Internet pode aceder a L1 em http
- A Internet pode aceder a L2
- **Todo o restante tráfego deve ser bloqueado**

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
interface nome-interface