Segurança Informática e nas Organizações
1º Semestre, 2021/22

1º Exame (2ª parte) [32]
10 de fevereiro de 2022

Número mecanográfico: [redacted]
Nome: [redacted]

Esta parte é única por aluno e tem 18 perguntas, sendo todas de resposta obrigatória.

Todas as perguntas de escolha múltipla valem 0.25 pontos. As perguntas só possuem uma resposta correta, mas os alunos podem assinalar várias respostas. As respostas incorretas **descontam** *de acordo com* $p = -0.25 \times min(0.4, 0.4 \times \log(n))$ *onde* n *representa o número de questões com respostas incorretas.*
Os descontos serão aproximadamente $0.25 \times 0, 0, 0.12, 0.19, 0.24, 0.28, 0.31, 0.34, 0.36, 0.38, 0.4, ...0.4,$ *para* $n >= 0$
As perguntas de desenvolvimento valem 0.5 pontos cada.

O teste possui a duração máxima de 150 minutos.

1. Relativamente à autenticação no SSH (*Secure Shell*):
   (a) Usa sempre segredos partilhados entre utentes e servidor
   (b) Usa sempre pares de chaves assimétricas não certificadas para autenticar o servidor
   (c) Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS)
   (d) É da responsabilidade do servidor SSH forçar a utilização de segredos complexos

2. Relativamente à autenticação usando TLS (*Transport Layer Security*):
   (a) Não protege a integridade da informação
   (b) Serve para garantir a negociação de uma chave de sessão entre os interlocutores corretos
   (c) O cliente pode escolher livremente quais as credenciais que usa na sua autenticação
   (d) A autenticação dos clientes é uma opção dos mesmos

3. Relativamente à autenticação no GSM (*Global System for Mobile Communications*):
   (a) A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis
   (b) Baseia-se no conhecimento mútuo (utente e rede) de um PIN
   (c) A posse do módulo SIM onde está a chave secreta é normalmente suficiente para um terminal móvel se autenticar
   (d) Usa um protocolo de autenticação multimétodo

4. Relativamente à autenticação de utentes com S/Key:
   (a) São usadas senhas descartáveis memorizadas pelos utentes
   (b) Os autenticados precisam de reinstalar as suas credenciais de autenticação após um determinado número de utilizações
   (c) É imune a ataques com dicionários
   (d) É um protocolo de autenticação mútua

5. Relativamente à autenticação de utentes com desafio-resposta e pares de chaves assimétricas:
   (a) Quem se autentica deve cifrar a resposta com a chave pública do autenticador
   (b) Quem se autentica deve apresentar a sua chave privada
   (c) A utilização de certificados de chave pública pode fornecer os mecanismos de identificação de quem se autentica
   (d) A validação das credenciais obriga à pré-partilha da chave pública do autenticador

6. A proteção do tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades
   (a) Controlo de integridade da carga útil com CBC-MAC e AES
   (b) Controlo de integridade do cabeçalho e da carga útil com Michael
   (c) Controlo de integridade da carga útil com Mich
   (d) Controlo de integridade da carga útil com CR

7. A autenticação do WPA no acesso de um terminal à rede
   (a) Usa sempre EAP
   (b) Permite a utilização de SKA para sistemas ma gos
   (c) Elimina apenas o modo OSA do WEP
   (d) Permite o modelo SOHO para redes de pequ mensão

8. A fase *Four-Way Handshake* do 802.1X destina-se
   (a) Autenticar mutuamente o Suplicante e o Serv Autenticação
   (b) Distribuir chaves criptográficas entre o Sup o Servidor de Autenticação
   (c) Distribuir chaves criptográficas entre o Aute e o Servidor de Autenticação
   (d) Autenticar mutuamente o Suplicante e o cador

9. No UNIX/Linux, caso um ficheiro tenha a -w-rwx--x, qual dos seguintes acessos é **negad**
   (a) Escrita/alteração pelo dono
   (b) Execução por um processo com um GID ig ficheiro
   (c) Leitura pelo dono
   (d) Leitura por um processo com um GID ig ficheiro

10. Relativamente ao mecanismo *apparmor*, afirmações é correta?
    (a) Não acrescenta nada face ao mecanismo
    (b) Apenas limita as comunicações na rede
    (c) Aplica regras genéricas, válidas par aplicações com o mesmo comportament
    (d) Não se aplica a processos executados p *root*

11. Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação verdadeira?
(a) A permissão de Set-UID altera o UID associado a um ficheiro
(b) A permissão de Set-GID altera o GID associado a um ficheiro
(c) Um ficheiro com permissão Set-UID irá executar com as permissões de quem o executa
(d) Um ficheiro com permissão Set-UID irá executar com as permissões do UID dono do ficheiro

12. Relativamente ao mecanismo de namespaces, qual das afirmações é correta?
(a) É equivalente ao mecanismo apparmor
(b) Os interfaces de rede não podem pertencer a um namespace pois não são processos
(c) Os processos não podem pertencer a vários namespaces
(d) Os processos podem pertencer a vários namespaces de tipos diferentes

13. Em relação às cópias de segurança ao nível do sistema de ficheiros, que afirmação é correta?
(a) Permitem utilizar mecanismos de deduplicação de blocos
(b) Garantem integridade do estado de cada ficheiro
(c) Não garantem integridade do estado global dos ficheiros
(d) Não garantem integridade do estado de cada ficheiro

14. Relativamente ao método de backups incrementais do sistema de ficheiros, qual das afirmações é verdadeira?
(a) A adição de novos dados é feita considerando o último backup completo
(b) A longo prazo, o caráter incremental deste método irá resultar na utilização de mais espaço do que backups completos
(c) A recuperação de dados é mais complexa que em outros métodos
(d) Permite salvaguardar versões incrementais e globalmente consistentes de bases de dados

15. Num sistema RAID 4 com N discos, qual a situação limite, após o qual existirá perda de informação?
(a) Avaria de todos os N discos
(b) Avaria do disco que contém as somas de controlo e um outro qualquer
(c) Avaria de qualquer disco, exceto o que contém as somas de controlo (paridade)
(d) Avaria de 1 disco (qualquer)

16. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?
(a) RAID 6
(b) RAID 0
(c) RAID 1
(d) RAID 0+1

17. No protocolo TLS, qual o objetivo e conteúdo de uma definição de uma *CipherSuite*?

Num sistema de *backups*, devem existir cópias em vários
íveis, ou deve-se escolher um nível em particular? Jus-
ique.