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

2º Teste 96
10 de fevereiro de 2022

Número mecanográfico: _____
Nome: _____

O teste é único 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 $0, 0, 0.12, 0.19, 0.24, 0.28, 0.31, 0.34, 0.36, 0.38, 0.4, ...0.4$ face ao valor da questão, para $n >= 0$
As perguntas de desenvolvimento valem 0.5 pontos cada.
O teste tem a duração de 75 minutos.

1. Relativamente à autenticação com desafio e resposta:
   (a) Não permite uma fácil implantação de protocolos de autenticação mútua
   (b) Não pode ser utilizada em combinação com smartcards
   (c) Pode ser utilizado em comunicações unidirecionais
   (d) É fundamental que os desafios apresentados a uma mesma credencial nunca se repitam

2. Relativamente à autenticação por apresentação de senha direta memorizável:
   (a) O sal serve para aumentar a dimensão das senhas
   (b) É vulnerável a ataques por dicionário
   (c) Os utentes memorizam senhas complexas com facilidade
   (d) Se o administrador definir a necessidade de senhas de 256 bits aleatórios, o processo torna-se seguro

3. Considerando a autenticação de utentes em Smartphones:
   (a) O *Trusted Execution Environment* é um ambiente seguro implementado pelo cartão SIM
   (b) As chaves são fornecidas às aplicações pelos componentes do TEE para validação
   (c) O reconhecimento facial é considerado robusto
   (d) A exploração de canais paralelos pode ser problema para autenticação com PIN

4. Relativamente à autenticação de utentes com S/Key:
   (a) Permite que, para o mesmo utente, a mesma senha produza senhas descartáveis diferentes para sistemas diferentes
   (b) As senhas descartáveis são geradas mentalmente a partir de uma senha
   (c) Usa pares de chaves assimétricas como credenciais
   (d) É um protocolo de autenticação mútua

5. Relativamente à autenticação biométrica de utentes:
   (a) Facilita a transferência de credenciais entre utentes
   (b) É o método de autenticação ideal quando se tem muitos utentes
   (c) É um método de autenticação universal (não exclui pessoas)
   (d) Pode dar origem a falsos negativos, mas estes não são perigosos para o sistema

6. A segunda fase do 802.1X destina-se a
   (a) Autenticar mutuamente o Suplicante e o Servidor de Autenticação
   (b) Autenticar apenas o Servidor de Autenticação
   (c) Autenticar mutuamente o Autenticador e o Servidor de Autenticação
   (d) Autenticar apenas o Suplicante

7. A proteção do tráfego Wi-Fi no meio sem fios com WEP permite qual das seguintes funcionalidades
   (a) Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES
   (b) Controlo de integridade do cabeçalho e da carga útil com Michael
   (c) Cifra da carga útil com o algoritmo RC4
   (d) Cifra da carga útil com o algoritmo AES

8. A autenticação do WPA no acesso de um terminal móvel à rede
   (a) Depende sempre de um serviço central de autenticação
   (b) Mantém a autenticação SKA do WEP mas evita a sua insegurança
   (c) Segue os princípios do padrão 802.1X
   (d) Elimina apenas o modo OSA do WEP

9. No UNIX/Linux, caso um ficheiro tenha a proteção `-w-rwx--x`, qual dos seguintes acessos é **negado**?
   (a) Leitura por um processo com um GID igual ao do ficheiro
   (b) Escrita/alteração por um processo com um GID igual ao do ficheiro
   (c) Escrita/alteração pelo dono
   (d) Leitura pelo dono

10. Considerando que um ficheiro pertence ao utilizador `root` (`uid=0`) e grupo root (`gid=0`), tendo as permissões `rwsrwsr-x`, se este for executado pelo utilizador com `uid=1000` e `gid=1000`, qual é a informação **correta** do processo?
    (a) O *real* UID terá o valor 0 e o *effective* UID terá o valor 0
    (b) O *real* UID terá o valor 0 e o *real* GID terá o valor 0
    (c) O *real* UID terá o valor 1000 e o *real* GID terá o valor 0
    (d) O *effective* UID terá o valor 0 e o *effective* GID terá o valor 0

11. No UNIX/Linux, relativamente à chamada ao sistema `chroot`, qual das seguintes afirmações é **verdadeira**?
    (a) A noção de raiz do sistema de ficheiros é global para todo o sistema
    (b) Um processo pode reverter em qualquer momento uma alteração que tenha realizado na sua raiz do sistema de ficheiros