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

2º Teste [redacted]

10 de fevereiro de 2022

Número mecanográfico: [redacted]

Nome: [redacted]

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 usando TLS (*Transport Layer Security*):
   (a) Não protege a integridade da informação
   (b) Está bem adaptada para a autenticação de servidores dos quais nada se conhece (exceto o endereço IP, ou nome DNS)
   (c) O cliente pode escolher livremente quais as credenciais que usa na sua autenticação
   (d) É vulnerável a ataques por dicionário

2. Na autenticação de utentes do sistema Linux:
   (a) O processo de autenticação não suporta múltiplos fatores
   (b) A senha é armazenada no disco, depois de validada pelo TPM
   (c) O administrador pode alterar o método de armazenamento das credenciais
   (d) O ficheiro **`/etc/shadow`** possui um backup do ficheiro **`/etc/passwd`**

3. Qual dos seguintes protocolos de autenticação é vulnerável a ataques com dicionários?
   (a) TTLS
   (b) RSA SecurID
   (c) SSH
   (d) Linux (com pam_unix)

4. Relativamente à autenticação no GSM (*Global System for Mobile Communications*):
   (a) Baseia-se no conhecimento mútuo (utente e rede) de um PIN
   (b) O desafio enviado pela rede é baseado no PIN
   (c) A função de transformação do desafio apresentado pela rede é universal e realizada pelos terminais móveis
   (d) É imune a ataques com dicionários

5. Na autenticação de utentes do sistema MS Windows:
   (a) O TPM fornece credenciais ao sistema após desbloqueio com um PIN
   (b) O TEE executa um sistema seguro para armazenamento de credenciais
   (c) O reconhecimento facial faz uso de um PIN para identificação do utilizador
   (d) O método NTLM Password Hash calcula uma síntese da senha com um SALT

6. O EAP (*Extensible Authentication Protocol*)
   (a) É um protocolo de autenticação baseado em chaves assimétricas
   (b) É usado no 802.1X para autenticar um Suplicante perante um Autenticador
   (c) É um protocolo que permite extender outros protocolos de autenticação
   (d) É usado no 802.1X para autenticar um Suplicante perante um Servidor de Autenticação

7. A proteção do tráfego Wi-Fi no meio sem fios com TKIP permite qual das seguintes funcionalidades
   (a) Controlo de integridade do cabeçalho e da carga útil com Michael
   (b) Controlo de integridade do cabeçalho e da carga útil com CRC-32
   (c) Controlo de integridade do cabeçalho e da carga útil com CBC-MAC e AES
   (d) Controlo de integridade da carga útil com CBC-MAC e 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) Usa sempre EAP
   (d) Realiza sempre uma distribuição de chaves ao Suplicante e ao Autenticador

9. Tendo em conta a existência de diferentes níveis de proteção na execução de um CPU (*protection rings*), indique a resposta certa:
   (a) Sem esses níveis o núcleo de um sistema operativo estaria vulnerável a ataques feitos pelas aplicações
   (b) Os sistemas operativos podem definir as instruções que podem fazer parte de cada nível
   (c) Não é possível transitar de um nível menos privilegiado para outro mais privilegiado
   (d) Existe uma relação direta entre esses níveis e os privilégios de administração de um sistema operativo

10. Relativamente ao mecanismo *apparmor*, qual das afirmações é correta?
    (a) Não é útil para vários programas interpretados, quando chamados através do seu interpretador (e.x, python3 app.py)
    (b) Implementa um mecanismo de armadura que protege as aplicações de atacantes externos
    (c) Uma aplicação pode escolher ignorar as regras do mecanismo

(d) Não se aplica a processos executados pelo utilizador *root*

11. Considerando o mecanismo Set-UID/Set-GID, qual é a afirmação **verdadeira**?
    (a) Um ficheiro com permissão Set-UID irá executar com as permissões de quem o executa
    (b) O mecanismo de Set-UID altera o *effective* UID de um processo mas mantém o seu *real* UID inalterado
    (c) Um processo possui as permissões do utilizador com o *real* UID associado ao processo
    (d) A permissão de Set-GID altera o GID associado a um ficheiro

12. Considerando o UNIX/Linux, qual das seguintes afirmações é **verdadeira**?
    (a) Cabe exclusivamente ao seu núcleo a função de gerir um modelo computacional independente do hardware
    (b) A interação entre processos pode-se realizar sem qualquer pedido expresso ao núcleo
    (c) Os procedimentos de *login* de um utente são geridos pelo seu núcleo
    (d) Um processo com privilégios de administração tem acesso irrestrito a todas as instruções do CPU

13. Qual dos seguintes sistemas tem o menor desperdício de espaço de armazenamento?
    (a) RAID 1
    (b) RAID 0+1
    (c) RAID 6
    (d) RAID 5

14. Num sistema RAID 6 com N discos, qual a situação limite, após o qual existirá perda de informação?
    (a) Avaria de 2 discos (qualquer)
    (b) Avaria de todos os N discos
    (c) Avaria de 5 discos
    (d) Avaria de 4 discos

15. Num sistema RAID 1 com N discos, qual a situação limite, após o qual existirá perda de informação?
    (a) Avaria de $N - 1$ discos
    (b) Avaria de apenas um disco (qualquer)
    (c) Avaria de 3 discos
    (d) Avaria de 2 discos

16. Num sistema RAID 0 com N discos, qual a situação limite, após o qual existirá perda de informação?
    (a) A avaria de qualquer disco implica sempre a perda de dados
    (b) Avaria de todos os N discos
    (c) Avaria de ambos os discos com as somas de controlo (paridade)
    (d) Avaria de $N - 1$ discos

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

18. Num sistema de *backups*, devem existir cópias em vários níveis, ou deve-se escolher um nível em particular? Justifique.