Segurança
1º Semestre, 2013/14

2º Teste / 1º Exame
10 de Janeiro de 2014

- Todas as perguntas têm a mesma cotação.
- A duração total do **teste** é de 1 hora e 30 minutos (**últimas 10 perguntas**).
- A duração total do **exame** é de 3 horas (**20 perguntas**).

1. Considere o problema de ataques por envenenamento de *caches* ARP. Explique:
    a. Como é realizado?
    b. Indique duas formas de defesa que considere viáveis para determinados ambientes de trabalho.

2. Considere os ataques de XSS (*Cross-Site Scripting*).
    a. Explique por que razão os utentes de serviços Web têm dificuldade em detetar este tipo de ataques.
    b. Que princípio básico, presente no modelo de integridade de Clark-Wilson, deveria ser aplicado (nos servidores) para evitar este tipo de ataques?

3. Considere o problema do alinhamento (*padding*) de mensagens para efeitos de cifra. Explique:
    a. Por que razão o mesmo pode ser necessário quando se usam modos de cifra por blocos?
    b. Indique uma forma eficaz de o realizar (descreva o que acontece na decifra).

4. Inúmeras cifras por blocos foram criadas tendo como elemento estrutural base várias redes de Feistel. Explique:
    a. Como funciona uma rede de Feistel?
    b. Por que razão se usam não apenas uma mas várias em cada operação de cifra (ou decifra)?

5. As cifras contínuas são particularmente vulneráveis a ataques à integridade do criptograma. Explique:
    a. Qual a razão estrutural deste tipo de cifras que cria essa vulnerabilidade?
    b. Considera que uma simples síntese da mensagem, cifrada juntamente com esta última, poderia resolver esse problema? Justifique.

6. Indique, justificando, o que distingue uma função de síntese (*digest*) de uma função de dispersão (*hashing*) vulgar?

7. As assinaturas digitais só se tornaram possíveis após a descoberta de cifras assimétricas. Explique porquê.

8. Para efeitos de assinatura digital é fundamental a existência de certificados de chave pública e de cadeias de certificação aceites de forma generalizada. Explique porquê.

9. Um certificado de chave pública pode ser validado, para uma determinada data, através de um serviço de OCSP (*Online Certificate Status Protocol*).Indique.
    a. Dado um certificado, como se sabe qual é o serviço OCSP apropriado?
    b. Qual a relação entre a informação prestada por um serviço OCSP e listas de certificados revogados (listas base e delta)?

10. Um *smartcard*, como o Cartão de Cidadão, é uma ferramenta imprescindível para implantar um serviço de assinatura digital que seja aceitável. Explique porquê, de forma tão completa quanto possível.

11. Considere o conceito de autenticação multimétodo (*multi-factor).*
    a. Explique em que consiste.
    b. Explique como e porque é usado no caso do Cartão de Cidadão.

12. Considere a arquitetura PAM (*Pluggable Authentication Modules*). Explique:
    a. Indique de que forma é usada no âmbito de processos de autenticação.
    b. Indique duas vantagens que advêm do seu uso.

13. Considere o protocolo cliente-servidor SSL/TLS (*Secure Sockets Layer / Transport Layer Security*). Explique
    a. Como é realizada a autenticação dos clientes e servidores?
    b. Tendo em conta as credenciais apresentadas por clientes e servidores, que diferença existe na escolha dessas credenciais pelos próprios?

14. Considere o conceito de matriz de controlo de acesso.
    a. Em que consiste?
    b. Normalmente é concretizada de forma desmembrada, em listas de controlo de acesso (*access control lists*, ACL) ou capacidades (*capabilities*). Explique o que são estes dois conceitos.

15. Explique os princípios base dos modelos de controlo de fluxos de informação.

16. Considere o mecanismo de Set-UID do Unix/Linux. Explique:
    a. Explique como é que o mesmo funciona.
    b. Explique como é usado no caso do comando **`sudo`**.

17. Nos sistemas operativos os processos estão associados a identificadores de utilizadores e de grupos.
    a. Explique porquê.
    b. Explique como é que num sistema Unix/Linux se sabe quais são esses identificadores.

18. Considere a cifra de conteúdos de sistemas de ficheiros. Explique que vantagens e desvantagens advêm da cifra realizada ao nível dos controladores de dispositivo face a cifras realizadas ao nível aplicacional.

19. Explique o objetivo e o princípio da técnica do K-anonimato.

20. Uma JVM (*Java Virtual Machine*) carrega classes dinamicamente quando necessita (ou quando é instruída nesse sentido) e as classes são segregadas por domínios de proteção (*protection domains*). Explique:
    a. Como são estabelecidos (ou definidos) esses domínios de proteção?
    b. Que vantagens em termos de segurança advêm dessa segregação?