Segurança
1º Semestre, 2014/15

2º Teste / 1º Exame
9 de Janeiro de 2015

- 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 mecanismo ASLR (*Address Space Layout Randomization*) que é usado para mitigar ataques por esmagamento da pilha (*stack smashing attack*s). Explique:
    a. Em que consiste?
    b. De que forma permite mitigar os ataques de esmagamento da pilha?

2. Explique em que consiste um Ataque de Dia Zero (*Zero Day Attack*).

3. Considere os ataques por análise estatística para descoberta do período de uma cifra contínua.
    a. Explique como se usa o método de Kasiski para esse fim.
    b. Indique o período provável usado para gerar o seguinte criptograma:
    BHMBTNJTQBBIIDWBTFMGXDDWLBXQDWLSXHPLFHDF

4. Considere o problema da alteração de um 1 bit apenas de um criptograma. Indique, justificando, que consequências daí advêm para o valor obtido após decifra quando se usa:
    a. Uma cifra contínua.
    b. Uma cifra por blocos em modo CBC (*Cipher Block Chaining*).

5. Considera a cifra assimétrica RSA. Explique pormenorizadamente como funciona (i.e., como realiza as transformações criptográficas). NOTA: não descreva o método de geração dos pares de chaves.

6. Considere as funções de síntese (*digest functions*). Explique o algoritmo geral de concretização das mesmas.

7. Considere um autenticador de mensagem (*Message Authentication Code*, MAC). Descreva duas formas possíveis de o calcular usando apenas:
    a. Uma função de síntese.
    b. Uma cifra.

8. Para efeitos de autenticação de servidores Web na Internet é fundamental a existência de certificados de chave pública e de cadeias de certificação aceites de forma generalizada. Explique porquê.

9. Considere as listas base e delta de revogação de certificados (*Certificate Revocation List*, CRL). Explique:
    a. Qual a relação entre os dois tipos de listas?
    b. Que conjunto de listas fornece, em qualquer altura, a totalidade dos certificados revogados por uma Entidade Certificadora?

10. Considere o padrão PKCS #11. Explique:
    a. O que é, ou para que serve?
    b. Por que razão ele é útil para realizar assinaturas digitais recorrendo a diferentes *smartcards*?

11. Considere a arquitetura PAM (*Pluggable Authentication Modules*) e a autenticação multimétodo (*multi-factor)*. Explique de que forma é que a primeira facilita a concretização da segunda.

12. Considere os ataques com dicionários a protocolos de autenticação. Explique:
    a. Em que consistem?
    b. Para realizar estes ataques em modo desligado (i.e., sem contactar o sistema de autenticação alvo), que elementos (dados, conhecimento) é necessário possuir?

13. Explique como funciona o protocolo de autenticação do GSM.

14. Considere o modelo genérico de controlo de acesso.
    a. Descreva o mesmo.
    b. Explique como é que o mesmo atua para concretizar políticas de controlo de acesso obrigatórias *(Mandatory Access Control*, MAC) ou discricionárias (*Discretionary Access Control*, DAC).

15. Considere os modelos de controlo de fluxos de informação. Explique:
    a. Explique como é que os mesmos atuam tendo em conta certificações de segurança (*security clearance*s) e classificações de segurança (*security classifications*).
    b. Como é que os modelos podem ser refinados através da introdução de compartimentos?

16. Considere a distinção feita pelos núcleos dos sistemas UNIX (Linux, MacOS, etc.) entre um super-utilizador (*super user*) e um utente normal para efeitos de controlo de acesso.
    a. Explique como é que a mesma é realizada.
    b. Indique, justificando, se se trata de uma política MAC *(Mandatory Access Control*, MAC) ou DAC (*Discretionary Access Control*).

17. Que elementos são usados pelo núcleo de um sistema operativo UNIX (Linux, MacOS, etc.) para decidir se um processo tem ou não um determinado tipo de acesso (leitura, escrita ou execução) relativamente a um ficheiro?

18. Considere a cifra de ficheiros realizada ao nível dos controladores de dispositivo e ao nível aplicacional. Discuta a possibilidade de uso de modos de cifra com realimentação em cada uma das aproximações.

19. Explique como aplicaria a política de controlo de fluxos de Bell-LaPadula a uma base de dados com proteção multinível concretizada através da cifra de registos (note que esta proteção multinível envolve a existência de políticas de acesso a chaves de cifra/decifra).

20. Uma JVM (*Java Virtual Machine*) permite definir políticas usando ficheiros de configuração e instâncias da classe **`java.security.Policy`**. Explique como é que estas políticas podem ser genericamente exploradas pelas classes do Java.