Segurança
1º Semestre, 2014/15

Exame de época de recurso
3 de fevereiro de 2016

- Todas as perguntas têm a mesma cotação.
- A duração total do exame é de 3 horas.

1. Descreva 4 barreiras informáticas de segurança tipicamente utilizadas como medidas de desencorajamento.

2. Em 2014 o *MS Windows* teve 247 entradas de CVE de segurança, enquanto o *Apple OS X* teve 147. O que se conclui da qualidade dos dois sistemas?

3. No âmbito do desenvolvimento de uma aplicação ainda não publicada e sem dependências de outras bibliotecas ou aplicações, os programadores devem estar particularmente cientes dos conteúdos das listas de CWE ou de CVE? Explique a razão.

4. A segurança da utilização de uma cifra contínua beneficia da adição de mecanismos de controlo de integridade. Explique porquê.

5. Explique, ilustrando a sua resposta com um diagrama e com outras provas que considere relevante, por que razão uma cifra por blocos em modo CBC (*Cipher Block Chaining*) é comparável, em termos de resultado final, a uma cifra polialfabética.

6. Considere uma função H(x) que divide um texto em blocos, aplicando sucessivas operações XOR dos blocos da mensagem e um sequência de valores obtidos de um PRNG iniciado com uma constante, invertendo depois a ordem dos bits dos blocos entre cada iteração e tendo como resultado um valor de tamanho fixo (e.x., 20 bytes). Analise qual a adequação desta função para ser utilizada como uma síntese.

7. Por que razão uma assinatura digital não pode ser copiada entre documentos tal como uma assinatura caligrafada?

8. Os certificados X.509 possuem uma extensão crítica (*Key Usage*) que permite definir o âmbito de utilização das chaves públicas que certificam. Explique:
    a. O que é uma extensão crítica?
    b. Que benefícios advêm desta extensão em concreto?

9. As senhas descartáveis foram idealizadas para resolver um problema concreto. Explique:
    a. Qual é esse problema?
    b. De que maneira o mesmo é resolvido por tais senhas?

10. A autenticação de máquinas no SSH (*Secure SHell*) é feita recorrendo a chaves públicas não certificadas. Explique por que razão esta é uma aproximação razoável e funcional, por contraponto ao recurso a chaves públicas certificadas.

11. O Cartão de Cidadão não é, nem poderia ser, um simples dispositivo de armazenamento (i.e., uma memória), concretizada, por exemplo, com um simples cartão com banda magnética ou uma memoria flash. Explique porquê.

12. Considerando um *Smartcard* como o Cartão de Cidadão, que tipos de sessões podemos estabelecer com o cartão e que funções e dados estão genericamente disponíveis em cada tipo?

13. No modelo RBAC, qual o propósito das Funções (Roles) e o que as distingue do conceito geral de Grupos na execução de uma transação?

14. No contexto de controlo de acesso, em que consiste o modelo da Muralha Chinesa e qual o seu propósito? Exemplifique.

15. Descreva o conceito e objetivo dos diversos anéis de execução existentes num processador.

16. Sendo que a autenticação em sistemas Linux é frequentemente realizada através de passwords, que mecanismos dificultam ataques de dicionário, no contexto:
    a. Do armazenamento de segredos no sistema
    b. Das políticas de escolha de senhas implementadas pelos administradores do sistema

17. Descreva o processo de *boot* de um sistema que utilize *Self Encrypting Disks*.

18. Explique como a solução *encFS* pode ser utilizada para segurar dados partilhados na rede num ambiente multi-utilizador, comparando-a com a solução de imagens de volumes cifradas (ex, usando *luks*)

19. Considere um sistema de ficheiros de um computador em que o conteúdo de praticamente todos os ficheiros (incluindo sistema operativo) se encontra cifrado com uma cifra contínua. Esta solução encontra-se protegida por uma chave complexa introduzida pelo utilizador e um IV armazenado. Descreva um ataque que permita revelar quantidades relevantes do conteúdo dos ficheiros.

20. No âmbito de um ficheiro de configuração PAM, descreva os controlos possíveis de definir para um módulo numa ação.