Segurança
1º Semestre, 2016/17

Exame de Recurso (1ª parte) [5]
30 de janeiro de 2017

Número mecanográfico: _____

Nome: _____

Para melhorar a nota do 1º Teste responda apenas à 1ª parte e para melhorar a nota do 2º Teste responda apenas à 2ª parte. Se responder a perguntas de ambas as partes descarta automaticamente as notas dos testes.

O exame tem 40 perguntas, mas **apenas** precisa de responder a 20. Caso esteja a melhorar um teste só precisa de responder a 10 da respetiva parte.

Cada pergunta tem apenas uma resposta, dada no enunciado (que tem de ser entregue). Todas as perguntas têm a mesma cotação, que depende do número de respostas dadas (se > 20, no caso de exame, ou > 10, no caso de teste). Quanto mais respostas, menor será a cotação de cada. Respostas erradas **descontam** (cotação/(hipótese-1)).

A pergunta adicional, no final, servirá **apenas** para lidar com situações próximas da nota mínima.

A duração total do exame é de 2h; a dos testes é 1h.

1. As políticas de segurança:
   (a) São as tecnologias que permitem implementar um determinado objetivo de segurança
   (b) São regras que definem os mecanismos a utilizar de forma a obter segurança
   (c) São constituídas pelas leis que definem o âmbito do crime informático
   (d) São normas, regulamentos e orientações que definem o modelo de proteção num determinado domínio de segurança

2. Um ataque do dia zero é:
   (a) Um ataque lançado no início do ano
   (b) Um ataque inovador usando uma combinação de vulnerabilidades conhecidas
   (c) Um ataque novo para uma vulnerabilidade conhecida
   (d) Um ataque que explora uma vulnerabilidade até aí desconhecida

3. Qual das seguintes afirmações é falsa tendo em conta o que é um registo CVE (*Common Vulnerabilities and Exposures*)?
   (a) Um registo CVE refere a potencial gravidade de uma ataque face a uma vulnerabilidade
   (b) Um registo CVE pode dar indicações acerca do erro que originou uma vulnerabilidade
   (c) Um registo CVE nunca descreve um problema de configuração
   (d) Um registo CVE descreve como pode ser realizado um ataque a um software vulnerável

4. Num ataque XSS (*Cross-Site Scripting*) de armazenamento, onde é executado o código malicioso?
   (a) No computador da vítima
   (b) No servidor
   (c) Num equipamento de rede (e.g. roteador)
   (d) No computador do atacante

5. O processo de manipular o endereço MAC de uma interface local é denominado de:
   (a) ARP Resolution
   (b) ARP Spoofing
   (c) ARP Corruption
   (d) ARP Poisoning

6. Quando se explora um *buffer overflow*, qual é o resultado expectável quando se reescreve o valor do registo EBP guardado na *stack frame* da função atual?
   (a) Alteração imediata dos valores das variáveis locais da função
   (b) Terminar abrupta e imediatamente a aplicação
   (c) Um funcionamento imprevisível quando terminar a função corrente
   (d) Terminar abrupta e imediatamente a aplicação quando terminar a função corrente

7. Qual é o objetivo dos *Stack Canaries*?
   (a) Detectar quando algum código escreve dados para além das suas variáveis locais
   (b) Detectar quando algum código altera o registo EBP
   (c) Detectar quando algum código escreve dados para outras aplicações
   (d) Detectar quando algum código altera o registo ESP

8. Tendo em conta as recomendações relativas ao uso de cifras contínuas, qual não é necessariamente crítica?
   (a) Não usar o mesmo estado inicial no gerador da cifra para mensagens diferentes
   (b) O criptograma deverá incluir um mecanismo de controlo de integridade
   (c) O valor da chave contínua, numa determinada posição, não deverá permitir calcular outros valores da mesma, tanto antes como depois
   (d) Não se devem cifrar mensagens com um comprimento elevado

9. Quando se usa cifra tripla é normal usar o modo EDE (Encrypt, Decrypt and Encrypt). Porquê?
   (a) Porque caso se usasse 3 cifras seria mais simples descobrir as 3 chaves
   (b) Porque se se usasse 3 cifras ficaria menos eficiente
   (c) Porque se pode anular uma cifra com a decifra ou vice-versa
   (d) Porque usar uma decifra entre cifras aumenta a confusão do processo de cifra

10. Para enviar uma mensagem confidencial a um destinatário, usando criptografia assimétrica, deve:
    (a) Cifrar a mensagem usando a sua (remetente/originador) chave pública
    (b) Cifrar a mensagem usando a sua (remetente/originador) chave privada
    (c) Cifrar a mensagem usando uma síntese da sua (remetente/originador) chave pública
    (d) Cifrar a mensagem usando cifra híbrida com uma chave simétrica aleatória e a chave pública do destinatário

11. Qual dos seguintes modos de cifra não permite um acesso aleatório constante na decifra?
    (a) ECB (*Electronic Code Book*)
    (b) OFB (*Output FeedBack*)
    (c) GCM (*Galois/Counter Mode*)
    (d) CBC (*Cipher Block Chaining*)

12. Qual dos seguintes modos de cifra realiza uma cifra monoalfabética?
    (a) GCM (*Galois/Counter Mode*)
    (b) CFB (*Cipher FeedBack*)
    (c) OFB (*Output FeedBack*)
    (d) ECB (*Electronic Code Book*)

13. Tendo em conta apenas a resistência à descoberta de colisões em funções de síntese, qual destas expressões é **falsa**?
    (a) Se for reduzida, representa um risco caso a função seja usada num MAC (*Message Authentication Code*)
    (b) Se for reduzida, o autor de uma assinatura poderá produzir vários documentos para a mesma assinatura
    (c) Se for reduzida, uma entidade terceira poderá produzir um texto alternativo compatível com a assinatura de outro texto
    (d) É definida apenas pela dimensão do resultado da função, de acordo com o paradoxo do aniversário

14. *Um MAC (Message Authentication Code) é calculado com uma chave secreta*
    (a) Porque a mensagem autenticada com o MAC precisa de ser confidencial
    (b) Porque é necessário garantir o seu secretismo
    (c) Porque usa uma função de cifra
    (d) Para impedir que terceiros possam gerar um MAC válido para outra mensagem

15. *Um dos objectivos das assinaturas digitais é o não-repúdio, que consiste em:*
    (a) forçar o uso de smartcards na geração de assinaturas
    (b) Impedir o acesso não autorizado ao conteúdo das mensagens/documentos
    (c) Garantir que uma mensagem, ou documento, não sofreu qualquer alteração, isto é, está tal como quando foi gerada
    (d) Impedir que uma entidade que produziu uma mensagem/documento assinada(o) o possa negar

16. A assinatura digital de um documento:
    (a) Garante que é possível detetar qualquer adulteração do mesmo após a sua assinatura
    (b) Deixa de ser válida quando o par de chaves do assinante expira
    (c) Impede que o documento possa ser compreendido por quem não estiver autorizado
    (d) Pode, em certos casos, ser realizada com uma chave simétrica

17. Um Entidade Certificadora raiz é confiável porque:
    (a) Certifica muitas outras Entidades Certificadoras
    (b) Está no topo de uma cadeia de certificação
    (c) Tem um certificado autoassinado
    (d) Confiamos na correção da sua chave pública

18. Em qual dos seguintes casos é possível um utente realiza uma verificação incompleta, mas válida, de uma cadei de certificação?
    (a) A data do certificado é válida
    (b) O certificado não está listado na CRL (*Certifica Revocation List*)
    (c) Não é de todo possível
    (d) Existe uma Entidade Certificadora (CA) intermé confiável no caminho de certificação

19. Tendo em conta o uso de CRL (*Certificate Revocati List*), qual destas afirmações é **falsa**?
    (a) As listas delta complementam as listas base
    (b) Quando uma lista base é emitida, importa obrigat riamente a lista delta imediatamente anterior
    (c) As CRL indicam a data de revogação dos certificad revogados
    (d) As CRL delta incluem certificados expirados, mas CRL base não

20. Tendo em conta o período de validade de um certifica qual destas afirmações é **verdadeira**?
    (a) Impede que a chave privada possa ser usada f desse período
    (b) Não permite que o certificado seja usado fora de período
    (c) Pode ser encurtado caso seja revogado
    (d) É uma informação base de qualquer certificado

21. Considere o conceito de cifra contínua (*stream ciph* Explique:
    (a) Por que razão estas cifras não carecem de meca mos de alinhamento (*padding*)?
    (b) Que vantagem operacional advém desse facto?