Instituto Superior de Engenharia de Lisboa

Área Departamental de Engenharia da Eletrónica e Telecomunicações e de Computadores

MEIC/MEET/MERCM/LEIM - Segurança em Redes de Computadores - 2017/05/08 - 1º teste

Nome _____ Número _____

Curso: LEIM ☐ MEIC ☐ MEET ☐ MERCM ☐

- As perguntas de escolha múltipla podem ter uma ou mais respostas certas. Assinalar todas as repostas certas marcando no quadro correspondente a letra "V" ou então, nas erradas, colocando a letra "F". As perguntas de desenvolvimento devem ser resolvidas nas costas da folha do enunciado do teste, em folha de teste/exame ou numa folha A4 branca.
- Como elemento de consulta durante o teste apenas pode usar uma folha A4 manuscrita, original (não pode ser fotocópia) e não pode conter perguntes e respostas.
- Todas as folhas em cima da mesa durante a prova escrita devem conter a rubrica e o número do aluno, incluindo a folha de consulta.

V F

1) O TCP utiliza um número de sequência cujo valor inicial é gerado aleatoriamente. Qual o tipo de ataque(s) que este procedimento permite atenuar?

☐☐ 1.1) *DoS* #

☐☐ 1.2) *Teardrop*

☐☐ 1.3) *Man in the middle* #

☐☐ 1.4) *Connection hijacking*

2) A descrição "Recolher informação após uma violação da segurança de forma poder criar uma base para uma resposta" corresponde a uma ação do tipo:

☐☐ 2.1) Deteção

☐☐ 2.2) Forense #

☐☐ 2.3) Resposta

☐☐ 2.4) Prevenção

3) "O segredo é a alma do negócio" contraria o princípio de:

☐☐ 3.1) Euler

☐☐ 3.2) Schneier

☐☐ 3.3) Kerckhoff #

☐☐ 3.4) Diffie-Helman

4) A cifra de César pode ser classificada como cifra:

☐☐ 4.1) Poligrâmica

☐☐ 4.2) Polialfabética

☐☐ 4.3) Monoalfabética #

☐☐ 4.4) De substituição #

☐☐ 4.5) De transposição

5) A não-repudiação é um:

☐☐ 5.1) Ataque à segurança

☐☐ 5.2) Serviço de segurança #

☐☐ 5.3) Algoritmo de segurança

☐☐ 5.4) Mecanismo de Segurança

Instituto Superior de Engenharia de Lisboa

Área Departamental de Engenharia da Eletrónica e Telecomunicações e de Computadores

MEIC/MEET/MERCM/LEIM - Segurança em Redes de Computadores - 2017/05/08 - 1º teste

6) Assuma que tem a capacidade de prever o número de sequência inicial no estabelecimento de uma ligação TCP a um servidor HTTP. Indique que ataques ficarão mais facilitados:

☐☐6.1) Fecho prematuro de uma ligação TCP #

☐☐6.2) Injetar dados sobre uma ligação TCP existente #

☐☐6.3) Causar problemas de sincronismo numa ligação TCP existente #

☐☐6.4) Intercetar uma ligação TCP mesmo sem ter acesso ao canal de comunicação

7) As operações de substituição e transposição ou permutação são utilizadas em:

☐☐7.1) Cifras simétricas #

☐☐7.2) Funções de *hash*

☐☐7.3) Cifras assimétricas

☐☐7.4) Assinaturas digitais

8) Identifique problemas da cifra *One-time pad*:

☐☐8.1) É uma cifra de fluxo e por isso é considerada insegura

☐☐8.2) Problema da geração de chaves com tamanho igual ao comprimento da mensagem #

☐☐8.3) É uma cifra lenta porque o tamanho da chave deve ser maior ou igual ao da mensagem

☐☐8.4) Necessidade de gerar uma nova chave aleatória para cada processo de encriptação de mensagens #

9) Identifique características são necessárias numa função de *hash* (H) segura:

☐☐9.1) H produz uma saída de comprimento fixo. #

☐☐9.2) H tem de ser aplicado a um bloco de dados de um tamanho fixo #

☐☐9.3) É computacionalmente possível para encontrar qualquer par (x, y) de tal modo que H (x) = H (y).

☐☐9.4) H (x) é relativamente fácil de calcular para um dado x, permitindo implementações práticas tanto em *hardware* como em *software*. #

10) Em Junho de 2012, o *linkedin* confirmou a divulgação não autorizada de uma lista com 6.5 milhões de *usernames* e *hashes* de *passwords* cifradas com SHA-1, dos seus clientes. Indique:

☐☐10.1) Na lista é muitíssimo provável que haja *hashes* iguais

☐☐10.2) O problema são as colisões que a função SHA-1 exibe

☐☐10.3) Devia ter sido usado um MAC com uma chave pública

☐☐10.4) Um *nonce* (ou *salt*) torna mais difícil os ataques de dicionário #

11) Considere o uso do HMAC-SHA1 com a chave K:

☐☐11.1) O HMAC-SHA1 permite a verificação de integridade e autenticação #

☐☐11.2) O HMAC-SHA1 é tão seguro como calcular o SHA-1 (chave | mensagem)

☐☐11.3) O número de bits à saída do HMAC depende do tamanho da chave K usada

☐☐11.4) Se possuir a chave é possível obter o texto em claro a partir do valor do HMAC

Instituto Superior de Engenharia de Lisboa

Área Departamental de Engenharia da Eletrónica e Telecomunicações e de Computadores

MEIC/MEET/MERCM/LEIM - Segurança em Redes de Computadores - 2017/05/08 - 1º teste

12) O algoritmo de *Diffie-Hellman* serve para:

☐☐ 12.1) Transmitir uma chave de sessão sem nada passar pela rede

☐☐ 12.2) Distribuir a chave de protocolos de cifras simétricas sem esta passar pela rede #

☐☐ 12.3) Distribuir a chave privada de protocolos de cifra assimétricos sem esta passar pela rede

☐☐ 12.4) Distribuir a chave pública de protocolos de cifra assimétricos sem esta passar pela rede

13) [x2] Tendo em conta o algoritmo RSA e *p*=13 e *q*=11, determine:

a) Uma chave pública {*e, n*} e uma privada {*d, n*}

- p = 13 e q = 11, logo n= p * q = 13 * 11 = 143
- ϕ(n) = (p - 1) * (q - 1) = 12 * 10 = 120
- *e* e *n* devem ser coprimos: gcd(e,n)=1; 1 < e < ϕ(n). Um valor para *e* não divisor de 120 é e = 7
- Inverso multiplicativo de d: d * e = 1mod ϕ(n).Uma solução é d=103 pq 103*7=721≡1mod(120)
- Public key is (e, n) => (7, 33)
- Private key is (d, n) => (103, 33)

- gcd(120,7)=1
  120=7*17+1
  7=1*7+0
- Euclides estendido para determinar o d:
  1=7*d+120*x
  1=120+7(-17)
  Como o valor de d tem de ser positivo: d=-17+120=103

b) Podia ser escolhido outro valor para a chave privada (d) mantendo o valor da chave pública que escolheu anteriormente? Com o ***p*** e o ***q*** escolhidos e com o ***e*** escolhido o ***d*** pode ser igual a: **d=-17+n*120** em que n é um número natural. Por exemplo, tendo em consideração a alínea c) vem:
Desencriptação c = 128; d= 103+120=203; m = $128^{103+120} \bmod 143 = 2$

c) Descreva, executando, o processo de encriptação e desencriptação para o seguinte texto em claro: m = 2

Encriptação m = 2, c = $2^7 \bmod 143 = 128 \bmod 143 = 128$

Desencriptação c = 128, m = $128^{103} \bmod 143 = 2$

14) Quais das seguintes são vantagens da criptografia de chave pública em comparação com a criptografia de chave simétrica:

☐☐ 14.1) Baixa complexidade

☐☐ 14.2) Permite autenticação #

☐☐ 14.3) Maior velocidade de cifra

☐☐ 14.4) Permite a não repudiação #

☐☐ 14.5) Fácil distribuição de chaves privadas

15) Considere que Alice pretende enviar uma foto pelo *Facebook*, para que seja vista apenas por um grupo de amigos (N) e não por todos. Tanto Alice como cada um dos seus amigos possuem as respetivas chaves privadas e públicas. Indique quais são verdadeiras:

- ☐☐ 15.1) Alice deve cifrar com a sua chave privada
- ☐☐ 15.2) Alice deve cifrar com a sua chave pública
- ☐☐ 15.3) Alice deve cifrar N cópias com a chave privada de cada um dos seus amigos
- ☐☐ 15.4) Alice deve cifrar N cópias com a chave pública de cada um dos seus amigos #

16) Considere o uso de certificados de chave pública:

- ☐☐ 16.1) É possível revogar um certificado através de CRL #
- ☐☐ 16.2) A assinatura do certificado corresponde ao cálculo de um *hash* sobre alguns campos do certificado
- ☐☐ 16.3) Uma *certification authority* precisa de possuir a chave privada do sujeito (nome) do certificado a emitir
- ☐☐ 16.4) Pode existir confiança numa chave pública mesmo que esta não tenha sido obtida a partir de uma *certification authority* #

17) Um certificado digital x.509v3 inclui, entre outros parâmetros, os seguintes:

- ☐☐ 17.1) Chave pública do dono do certificado #
- ☐☐ 17.2) Chave privada do dono do certificado
- ☐☐ 17.3) *Distinguished Name* do dono do certificado #
- ☐☐ 17.4) Chave privada da autoridade de certificação que o emitiu
- ☐☐ 17.5) Assinatura digital do certificado usando a chave privada do proprietário #

18) O IEEE 802.1x:

- ☐☐ 18.1) Transporta mensagens EAP V
- ☐☐ 18.2) Define o método de autenticação a utilizar
- ☐☐ 18.3) Realiza a cifra de todas as mensagens trocadas entre o suplicante e o autenticador
- ☐☐ 18.4) O suplicante não tem acesso à rede protegida pelo autenticador até ser validada a identidade do suplicante V
- ☐☐ 18.5) Quando o porto controlado pelo 802.1X está no estado não autorizado bloqueia todo o tráfego 802.1X

19) Considere a autenticação de mensagens RADIUS:

- ☐☐ 19.1) O RADIUS suporta o uso de PAP para autenticação #
- ☐☐ 19.2) O RADIUS não suporta o uso de mecanismos de autenticação usando EAP
- ☐☐ 19.3) As mensagens RADIUS são transportadas sempre em cima do protocolo de rede de nível 2 do OSI
- ☐☐ 19.4) A comunicação entre os clientes e o servidor de autenticação é encriptada usando uma chave secreta do conhecimento de ambos, chave essa que nunca é enviada pela rede

20) Descreva a forma como o RADIUS protege o atributo *user-password*?

Designe-se o segredo partilhado por S e os 128 bits pseudo-aleatórios por *Request Authenticator* (RA). Parta-se a *password* em bocados de 128 bits p1, p2, etc. Com o último bloco preenchido com nulos até ao limite de 128 bits . Chame-se aos blocos cifrados c(1), c(2), etc. Utilizando os valores intermédios b1, b2, etc. teremos:

b1 = MD5(S + RA); c(1) = p1 xor b1;

b2 = MD5(S + c(1)); c(2) = p2 xor b2;

... .

bi = MD5(S + c(i-1)); c(i) = pi xor bi

O valor a colocar na *user-password* será c(1)+c(2)+...+c(i), onde + denota concatenação.