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 (SRC) - 2017/06/29
Repetição do 1º teste

Nome:_____; Número_____
Docente: Vítor Almeida Curso: LEIM ☐ MEIC ☐ MEET ☐ MERCM ☐

Nas questões de resposta múltipla assinale com um V (verdadeira), um F (falsa) ou não ponha nada (neste caso nem conta nem desconta na cotação).

O exame/teste global é composto por todas as perguntas pares dos dois testes parciais.

V F

1) **Se o One-Time Pad (OTP) é referido como a forma mais segura do mundo de cifrar porque é que não é mais utilizado?**
Devido ao facto de ser necessário gerar uma sequência aleatória da mesma dimensão do texto em claro a cifrar e de ser necessário enviar essa sequência aleatória para o destino onde vai ser decifrado o texto cifrado.
2) **Numa rede como a do ISEL, em que não existem *hubs*/repetidores, realizando *switch table poisoning* tornaria, em teoria, menos difícil fazer:**

☐ ☐ *Sniffing*
☐ ☐ *Phishing*
☐ ☐ *Smurfing*
☐ ☐ *Port scanning* #
☐ ☐ Nenhum dos anteriores

3) **O princípio de Kerckhoffs sobre "segurança através da obscuridade" é utilizado atualmente nos sistemas criptográficos?**
Sim, hoje em dia segue-se cada vez mais o princípio de Kerckhoffs divulgando os algoritmos mantendo secretas as chaves usadas. A força de uma cifra deve estar no algoritmo usado, o qual pode e deve ser público, e nas chaves usadas as quais se devem manter secretas e não no secretismo do algoritmo usado.
4) **Quais as razões pelas quais um ataque do tipo *port scan* consegue identificar o sistema operativo, os serviços ativos e as potenciais vulnerabilidades de um sistema?**
Existem portos UDP e TCP associados oficialmente a determinados protocolos. Assim sendo se o porto estiver ativo o protocolo está presente.
5) **Qual o requisito para que a cifra de Vernam pudesse ser considerada *one-time pad*?**
Chave aleatória usada uma única vez
6) **Que vantagem poderia ter um atacante que tivesse acesso e conseguisse modificar registos em servidores de DNS referentes ao domínio que pretende atacar?** Poderia colocar um domínio a apontar para um endereço IP de um servidor que controlasse e assim obter vantagem em ataques de, por exemplo, *phishing*.
7) **Tendo em consideração as cifras clássicas indique quais das seguintes afirmações estão corretas:**

☐ ☐Numa cifra de substituição mona alfabética a permutação aplicada aos diferentes símbolos do bloco é sempre a mesma #
☐ ☐Numa cifra de polialfabética a permutação difere de símbolo para símbolo dentro do mesmo bloco #
☐ ☐A cifra de Vigenère não mantém a frequência dos caracteres e por isso é uma cifra de substituição monoalfabética
☐ ☐A difusão através de transposição é um método usado para dissipar a estrutura estatística do texto em claro no texto cifrado #

8) Porquê utilizar um protocolo de autenticação baseado em HMAC (e.g. HMAC-SHA1) em vez de em MAC e cifra simétrica (e.g. DES)?

☐ ☐ Maior velocidade #
☐ ☐ Maior dimensão da chave
☐ ☐ O SHA-1 é mais seguro que o DES
☐ ☐ HMAC-SHA1 K(M)<MAC/DES K(M)
☐ ☐ Licença de exportação dos EUA mais fácil de obter #

9) Em qual dos seguintes modos um bloco de saída com texto cifrado não depende do texto cifrado no bloco anterior ou de um vetor de inicialização?

☐ ☐ Cipher Feedback (CFB)
☐ ☐ Output Feedback (OFB)
☐ ☐ Electronic Code Book (ECB) #
☐ ☐ Cipher Block Chaining (CBC)

10) Qual a razão pela qual o AES é considerado mais seguro do que o DES? Protocolo bem mais moderno com um espaço de chaves maiores: DES 56bit, AES 128-bit, 192-bit ou 256-bit

11) O Diffie-Hellman:

☐ ☐ Permite gerar uma chave simétrica #
☐ ☐ Permite gerar a chave privada para um certificado digital
☐ ☐ Utiliza certificados digitais para passar o valor da chave pública
☐ ☐ Usa IPSec quando se pretende fazer passar uma chave de modo criptograficamente seguro

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

12) Responda às seguintes questões assumindo o algoritmo de criptografia assimétrica RSA. Considere que se escolhem como nº primos 31 e 19 e use a tabela anterior de conversão de letras para números (Nota: O *padding* usado no RSA evitaria algumas fragilidades no uso da tabela acima mas neste exercício ignore-se).

a) Determine o totiente de n.

Φ(n) = (p-1)(q-1) = (31-1)(19-1) = 30 x 18 = **540**

b) Dos valores 3, 5 e 7 qual escolheria para chave assimétrica pública (RSA) assumindo que os números primos escolhidos foram p=31 e q =19?

n=pq=31x19=**589**

Φ(n) = 540

'3' e '5' não são primos relativos de Φ(n), isto é gcd(540,3)<>1 (=3) e gcd(540,5)<>1 (=5) 540 é divisível por 1,2,3,4,5,6,…. O único divisor entre primos relativos deve ser o 1, o que é verdade no caso de e=7 pois 7 é divisível por 1 e 7 apenas.

c) Determine qual a informação a publicar para que terceiros possam enviar mensagens cifradas usando este algoritmo. Assuma e=11.

Corresponde ao **n**=pxq=31x19**=589** e ao **e=11**; publique-se: **e=11, n=589**

d) Verifique se, sendo e=11, a chave privada pode ser d=299.

Ou seja $d = e^{-1} \bmod \Phi(n)$

299 e 540 são primos relativos dado que gcd(540, 299)=1; de = 1 mod Φ(n) => 299xe=1 mod (540) ou seja para e=11 a igualdade é falsa: (299x11=)3289=1 mod (540) é falso; **d=299 não é a chave privada.**

e) Qual a informação a publicar para que um destinatário possa verificar a autenticidade de um texto que receba autenticado usando um *hash* bem definido e a cifra assimétrica do exemplo anterior?

e=11 e **n=589**, o destinatário necessita conhecer a chave pública do emissor e o valor n resultante da multiplicação dos dois números primos.

f) Tendo em conta a mensagem do texto em claro "RI", usando o facto de o texto corresponder aos nºs 17 e 8, sendo os valores do emissor para os cálculos p=31; q=19; e e=11, determine o valor da chave privada d. d=491

p=31, q=19; n=589; Φ(n)=540; e=11; 11.d+540.y=1 => **d=491** dado que:
gcd(540,11)=**1**

540=11.x+y
540=11.49+1
11=1.11+0

[Euclides estendido]
1=11.(-49)+540 => d=-49, como 0<=d<=Φ(n) => 0<=d<=540 => **d**=-49+540=**491**

g) Indique quais os cálculos efetuados para calcular o texto cifrado (c) a enviar no caso de o texto em claro ser "R" e tendo em consideração os valores da alínea anterior. c=1711mod 589=270.

13) 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 a Alice como cada um dos seus amigos possuem chaves privadas e públicas. Indique quais as respostas que são verdadeiras:

☐ ☐ Alice deve cifrar com a sua chave pública
☐ ☐ Alice deve cifrar N cópias com a chave privada de cada um dos seus amigos
☐ ☐ Alice deve cifrar N cópias com a chave pública de cada um dos seus amigos #
☐ ☐ Alice deve cifrar apenas uma cópia com uma chave pública de um dos seus amigos

14) O algoritmo/função para cálculo do CRC (deteção de erros numa mensagem) pode ser utilizado com o mesmo objetivo de uma função de *hash*?

☐ ☐ Não, dado não garantir a não-repudiação
☐ ☐ Pode se o polinómio utilizado for de grau 128 ou superior
☐ ☐ Pode se o polinómio utilizado apenas utilizar expoentes primos
☐ ☐ Não, dado que é computacionalmente realizável achar um par de mensagens (x, y) tal que CRC(x)=CRC(y) #

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

☐ ☐ O HMAC-SHA1 permite a verificação de integridade e autenticação #
☐ ☐ O HMAC-SHA1 é tão seguro como calcular o SHA-1 (chave | mensagem)
☐ ☐ O tamanho da saída do HMAC não depende do tamanho da chave K usada #
☐ ☐ Se possuir a chave é possível obter o texto em claro a partir do valor do HMAC

16) O objetivo da utilização de certificados digitais X.509 é a divulgação segura da:

☐ ☐ Chave privada do dono do certificado
☐ ☐ Chave pública do dono do certificado #
☐ ☐ Chave privada da entidade de certificação
☐ ☐ Chave simétrica da entidade de certificação

17) IEEE 802.1x:

☐ ☐ As mensagens IEEE802.1x "correm" sobre IP
☐ ☐ Utiliza como protocolo de autenticação o EAP
☐ ☐ As mensagens EAP enviadas pelo servidor de autenticação terminam no Suplicante #
☐ ☐ As mensagens EAP enviadas pelo servidor de autenticação terminam no Autenticador
☐ ☐ Todos os pacotes IP que chegam a uma porta de um *switch* que use IEEE802.1x têm de estar devidamente autenticados para que a porta os deixe passar

18) Uma porta dum *switch* Ethernet controlada através de 802.1x:

☐ ☐ Só recebe tramas com endereço destino *multicast* 802.1x até o suplicante ser autenticado pelo servidor de autenticação, altura em que passa a deixar passar tudo #
☐ ☐ Só deixa passar qualquer tráfego Ethernet após negociação através de EAPoL #
☐ ☐ Deixa passar tudo durante um tempo pré-configurado no equipamento com a finalidade de permitir a negociação ente o suplicante e o servidor de autenticação RADIUS, se após este tempo o suplicante não for autenticado o porto fecha durante outro tempo pré-definido. No limite se este tempo for zero o *switch* pode deixar passar todo o tráfego sem autenticação do suplicante
☐ ☐ Se a porta suportar Gigabit Ethernet só deixa passar as mensagens que fizerem parte dum *burst*

19) RADIUS:

☐ ☐ A *user-password* P é cifrada através de P XOR MD5(Request Authenticator)
☐ ☐ As mensagens access-request são autenticadas através do campo Request-Authenticator
☐ ☐ O Request-Authenticator deve ser temporalmente e globalmente único (sem haver repetições)
☐ ☐ As mensagens access-accept e access-reject enviadas pelo servidor de autenticação vão autenticadas
☐ ☐ É possível lançar um ataque ao segredo partilhado S se o atacante conseguir efetuar uma tentativa de autenticação com uma *user-password* conhecida #

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 (SRC) - 2017/06/29
Repetição do 2º teste

Nas questões de resposta múltipla assinale com um V (verdadeira), um F (falsa) ou não ponha nada (nem conta nem desconta na cotação).

O exame/teste global é composto por todas as perguntas pares dos dois testes parciais.

V F

1) **Quais as principais diferenças entre um gerador de números aleatórios e pseudoaleatórios?**
Os geradores aleatórios geram os números a partir de fontes que são conhecidas pela sua aleatoriedade, não usam meios determinísticos para fazer a geração como, por exemplo usando uma função de *hash*.
2) **Descreva qual a função principal do protocolo PPPoE.**
Descobrir o concentrador de serviços numa rede multiponto (Ethernet). Controlar a entrega dos parâmetros necessários para o cliente poder funcionar. Controlar o acesso do cliente à rede do operador.
3) **Quais as vantagens de correr o L2TP em cima do IPSec em vez de correr apenas o IPSec?**
O IPSec fornece serviços de segurança (confidencialidade, integridade e autenticação) que o L2TP não suporta de forma nativa. Por sua vez a utilização do L2TP em cima do IPSec permite fornecer um serviço da camada 2, *data link*, (túnel) e, como tal, suportar outros protocolos de nível 3 para além do IP.
4) **Descreva uma forma de evitar ataques por repetição.**
É possível usar um número de sequência protegido em termos de integridade e uma janela deslizante de dimensão constante (pode ser negociável) na receção. Cada mensagem terá um número de sequência distinto e a janela só aceitará uma mensagem se não tiver chegado outra mensagem antes, cuja integridade seja comprovada, como o mesmo número. A janela avança quando chega uma mensagem válida com um número acima do limite superior da janela.
5) **A primeira mensagem trocada no IKEv2 (IKE_SA_INIT) é autenticada:**
☐☐ Pelo seu campo AUTH
☐☐ Pela mensagem IKE_AUTH no mesmo sentido #
☐☐ Pela mensagem IKE_AUTH em sentido contrário
☐☐ Pela próxima mensagem IKE_SA_INIT em sentido contrário
☐☐ Nunca, dado ainda não terem sido trocado os parâmetros necessários
6) **Para que a criação de um novo SA IKEv2 com PFS (*Perfect Foward Secrecy*) devem obrigatoriamente ser trocados:**
☐☐ Novos *nonces*
☐☐ Novos certificados
☐☐ Novas chaves privadas
☐☐ Novas chaves de sessão
☐☐ Novos valores para o Diffie-Hellman #
7) **No IPsec na escolha das *suites* a serem utilizadas nas SA a regra para a escolha é:**
☐☐ O *initiator* decide indicando a *suite* ao responder
☐☐ O responder decide qual das que lhe são propostas é que vai utilizar
☐☐ Aquela que proponha os algoritmos criptográficos comuns mais avançados #
☐☐ Aquela que proponha os algoritmos criptográficos mais avançados comuns ao *initiator* e ao responder
8) **No IPSec quando se refere a "granularidade do serviço de segurança" está-se a falar de:**
☐☐ Dimensão dos datagramas IPsec
☐☐ Quantidade de SA gerados para suporte de cada VPN
☐☐ Dimensão das chaves utilizadas nos algoritmos de autenticação e cifra
☐☐ Definição de quais as características dos fluxos IP associados a VPN distintas #

9) **Explique como é que no IPSec é possível usar um contador de 64 bit e só enviar os 32 bit de menor peso nas mensagens quando se pretende evitar ataques por repetição.**

O cálculo da integridade da mensagem é realizado usando os 64 bit mas só são enviados os 32 bit de menor peso.

10) **Como é que uma máquina que tem em simultâneo vária ligações IPsec sabe como deve tratar um pacote IP que acabou de chegar?**

Através do SPI que indica qual o SA a usar. Os endereços IP também podem contribuir para resolver ambiguidades.

11) **No WEP a utilização do vetor de inicialização (IV) serve:**

☐ ☐ Como chave de sessão diferente para cada uma das tramas
☐ ☐ Como índice para a chave de sessão que está a ser utilizada
☐ ☐ Para aumentar e variar a chave de cifra de trama para trama #
☐ ☐ Como número de sequência para evitar ataques por repetição

12) **Para fornecer integridade o WEP utiliza:**

☐ ☐ Um CRC protegido pelo RC4 #
☐ ☐ RC4 sobre o campo de dados da trama
☐ ☐ O WEP não dá nenhuma garantia de integridade
☐ ☐ HMAC-MD5 da concatenação da trama com a chave partilhada

13) No SSL/TLS o Master Secret:

☐ ☐ O Master Secret nunca passa na rede #

☐ ☐ É gerado a partir do pre Master Secret #

☐ ☐ É trocado entre cliente e servidor através de Diffie-Hellman

☐ ☐ É trocado entre cliente e servidor cifrado com uma cifra assimétrica e chave pública do servidor

14) Em SSL/TLS como são decididos quais os algoritmos criptográficos a usar numa ligação?

O servidor escolhe do conjunto de *suites* criptográficas que o cliente indica aquela que pretende usar.

15) Num acesso seguro a um banco via um *browser* indique a forma como é que o banco se autentica perante o utilizador e como é que o utilizador se autentica perante o banco.

O banco usa certificados digitais e o cliente usa login e *password* (ou o equivalente na forma de número cliente e senha). Quando o *login* e *password* passam na rede a ligação segura já está estabelecida tendo para isso sido usado o certificado digital do banco

16) Como é que um destinatário de um *email* no formato S/MIME tem acesso à chave de sessão, assumindo que o conteúdo vem cifrado?

☐ ☐ É enviada em claro no corpo do *email*

☐ ☐ É obtida a partir dos certificados ISO/ITU-T X.509v3

☐ ☐ Vem cifrado no corpo do *email* com a chave privada do recetor

☐ ☐ Vem cifrado no corpo do *email* com a chave pública do recetor #

☐ ☐ Vem cifrado no corpo do *email* com a chave privada do emissor

17) Para se poder enviar um *email* com garantia de origem é necessário que:

☐ ☐ O recetor possua um certificado

☐ ☐ O emissor possua um certificado #

☐ ☐ Nenhum certificado dado o SMTP já garantir autenticação da origem

☐ ☐ O emissor possuir uma cópia do certificado do recetor

18) Se utilizar SPF (*Sender Policy Framework*) o servidor de *email*:

☐ ☐ É garantida a confidencialidade das mensagens entre servidores de *email*

☐ ☐ Obriga os clientes a utilizar SMIME para garantir a autenticação das mensagens

☐ ☐ Verifica no DNS qual a chave pública do servidor remetente e verifica a assinatura das mensagens recebidas

☐ ☐ Consulta o DNS para verificar se o servidor que lhe está a enviar a mensagem de *email* está autorizado a fazê-lo em nome do domínio do remetente #

19) Num servidor de DNS existe o seguinte registo: alunos.isel.ipl.pt. 3600 IN TXT "v=spf1 ip4:193.137.220.0/25 ip4:62.48.232.168 a -all"

☐ ☐ Indica que para o domínio alunos.isel.ipl.pt só podem ser enviados *emails* dos servidores com endereços IPv4:193.137.220.0/25 e 62.48.232.168

☐ ☐ Indica que os servidores de *email* que podem enviar emails em nome do domínio alunos.isel.ipl.pt são os com endereços IPv4:193.137.220.0/25 e 62.48.232.168 #

☐ ☐ Indica que quem pode enviar *emails* com origem no domínio alunos.isel.ipl.pt são apenas as máquinas residentes nas redes ip4:193.137.220.0/25 e ip4:62.48.232.168

☐ ☐ Indica que para os servidores residentes em ip4:193.137.220.0/25 e ip4:62.48.232.168 só podem ser enviadas mensagens cujo conteúdo seja apenas texto

20) No Domain Keys como é obtido o certificado que contem a chave pública do emissor?

☐ ☐ Servidor de DNS #

☐ ☐ Servidor DHCP (extensão ao protocolo BOOTP)

☐ ☐ Servidor de Domain Keys residente junto do servidor de email de origem

☐ ☐ Autoridade de certificação (CA) indicada no servidor de DNS referido pelo servidor de origem

☐ ☐ A chave pública é sempre trocada entre os servidores de origem e destino através de certificados X.509v3 enviado na própria mensagem de *email* (SMIME)