Nº _____ ALUNO: _____

DI/FCT/UNL - Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 2º Sem., 2017/2018
Teste de frequência #2, 17/Junho/2018 `(Ref. 20180707A)`

PARTE I – (Parte Sem Consulta / 4 Páginas). Duração: 1h15

Questão 1. Responda **Verdadeiro (V) ou Falso (F).** As respostas erradas implicam numa penalização semelhante à valorização das respostas corretas. Se achar necessidade de argumentar sobre a sua resposta em alguma das alíneas pode usar uma folha em branco identificada para anexar às respostas.

a)	No sistema e protocolo Kerberos (ref. V5), utilizado num contexto de autenticação interdomínio (*Kerberos REALMS*), o *Ticket Granting Server* (TGS) de um domínio precisa de partilhar uma chave criptográfica simétrica com o *TGS* de outro domínio.	
b)	No sistema e protocolo Kerberos, um *ticket* emitido pelo AS – *Authentication Server* para um cliente, deve ter um tempo de validade superior ao ticket que esse cliente obterá posteriormente de um *TGS* – *Ticket Granting Server* e que lhe permitirá obter uma chave criptográfica para comunicar seguramente com um servidor final.	
c)	Numa assinatura digital de uma mensagem M em que se utiliza RSA com chaves de um determinado tamanho e *padding* PKCS#1, o tamanho do resultado da assinatura será sempre o mesmo, quer se utilize ou não esse *padding.*	
d)	Um certificado de chave pública, de acordo com a normalização X509v3, para além de certificar a chave pública de um dado principal, ainda permite determinar restrições ao propósito de utilização dessa chave pública, com base em políticas de restrição da utilização da chave pública que está certificada para os fins definidos	
e)	O sistema de controlo de permissões de acesso num sistema de ficheiros como o dos sistemas UNIX (LINUX) ou WINDOWS , segue um modelo DAC – *Discretionary Access Control*	
f)	Considere a noção de "domínio de proteção" no controlo de permissões de execução de processos UNIX (ou LINUX). Um processo que executa em modo utilizador (*user mode*) e cujo dono de execução é um dado utilizador, quando executa chamadas ao sistema (*system calls*), o contexto de execução dessas chamadas é feita sem privilégios em modo supervisor (ou *kernel mode*) pois assim evita-se poder ter acesso a áreas protegidas de memória por parte do *kernel.*	
g)	No protocolo TLS que vai ser usado em modo de autenticação mútua, e onde o servidor imporá ao cliente a *ciphersuite* TLS_DHE_DSS_WITH_AES_ 256_CBC_SHA156, o cliente tem que ter um certificado de chave pública aceite como válido e confiável por parte do servidor, obtido a partir de um par de chaves DSA no qual as chaves em causa podem ter qualquer tamanho admissível de acordo com o processo de geração do par de chaves.	
h)	Se no *trace* de mensagens trocadas na fase de *handshake* TLS entre um cliente e um servidor se detectar que foi enviada uma mensagem do tipo CERTIFICATE_REQUEST do servidor para o cliente, então é porque esse *handshake* está a ser usado necessariamente em modo de autenticação mútua.	
i)	Num *handshake* TLS que utiliza modo de autenticação e distribuição de chaves do tipo EDH – *Ephemeral Diffie-Hellman* e no qual se está a utilizar autenticação unilateral do servidor, o número público *Diffie-Hellman* gerado e enviado pelo cliente durante esse *handshake* não pode ser enviado autenticado pelo cliente.	
j)	Na pilha de protocolos IPSec o protocolo ESP pode pode ser usado em modo transporte	
k)	Em IPSec, o envio de pacotes ESP na adopção do modo túnel obriga a uma forma de encapsulamento do tipo ESP/IP em que o pacote ESP com endereçamento privado pode ser enviado como carga (*payload*) de um pacote IP que também usa endereçamento privado	

Nº _____ ALUNO: _____

Questão 2. Qual a diferença entre os modos EDH e FDH se usados como modo de autenticação e *handshake* no estabelecimento de uma sessão TLS ?

EDH –

FDH –

Questão 3.

a) Qual a diferença entre um modelo de control de acessos do tipo MAC e DAC ?

Nº _____ ALUNO: _____

b) No controlo de permissões no sistema de ficheiros UNIX (ou LINUX) que diferença tem estabelecer as seguintes permissões numa diretoria ?

B1) rwxr-xr-x ou B2) rwxrw----

c) Nos casos de b) podem os elementos do grupo do utilizador dono da diretoria em causa listar a diretoria nos dois casos ? Porquê ?

Questão 4. Indique (coluna 1 da tabela abaixo)os subprotocolos da pilha IPSec - identificando-os e associando-os às propriedades de segurança indicadas. Note que cada linha a preencher pode ter obviamente mais do que um subprotocolo, consoante as garantias de segurança associadas. Respostas erradas são penalizadas com valorização igual à de uma resposta correta.

Subprotocolos (suite IPSEC)	**Propriedade de segurança**
	Autenticação dos endereços IP da origem e destino do pacote IPSec
	Confidencialidade das cargas (*payload*) que viajam nos pacote IPSec entre um emissor e o receptor
	Autenticação dos dados (*payloads*) do pacote IPSec que foi enviado pelo emissor
	Gestão e estabelecimento seguros de associações de segurança (SAs) subjacentes à gestão das bases de dados de associações de segurança e políticas de segurança IPSec nos *endpoints*
	Integridade dos pacotes IPSec enviados pelo emissor ao receptor
	Garantias contra *Non-Replaying* de envio deepacotes IPSec
	Proteção (ainda que limitada) para garantias de confidencialidade do fluxo de tráfego (ou *traffic-flow-confidentiality*)

Nº _____ ALUNO: _____

Questão 5. Na segurança de uma assinatura digital RSA de uma menagem M, estão envolvidos vários componentes configuráveis: uma função de *padding*, uma função de síntese segura e a função de cifra que utiliza a chave privada. No processamento da assinatura obtida, o tamanho (em número de bytes) da assinatura (*ciphertext*) é igual ao tamanho das chaves utilizadas e não do tamanho do output da função de síntese usada. Verdadeiro ou falso ? JUSTIFIQUE DE MODO A ARGUMENTAR A SUA RESPOSTA.

Questão 6.

a) Na pilha TLS, os diferentes subprotocolos, de acordo com os seus objetivos, estão associados do ponto de vista do nível de abstração que representam a uma de duas noções: "**transporte seguro**" ou "**sessão segura**". Indique na tabela (coluna 2) os que estão associados a uma ou outra noção. Cada resposta incorreta é penalizada de modo semelhante à valorização de uma resposta correta)

SUB PROTOCOLO (TLS Stack)	Transporte Seguro **ou** Sessão Segura ?
HP (Handshake Protocol)	
CCSP (Change CipherSuite Protocol)	
AP (Alert Protocol)	
RLP (RecordLayer Protocol)	
HBP (Heartbit Protocol)	

b) O protocolo TLS, por concepção, pode ser implementado sobre transporte UDP ou TCP. Havendo o perigo de desordenação de pacotes IP no encaminhamento dos mesmos na INTERNET, com consequente desordenação de datagramas UDP enviados como cargas (*payload*) desses pacotes, de acordo com o seu estudo sobre o protocolo TLS justifique se esta situação ser detectada e se é corrigida pelo processamento do TLS - *Record Layer Protocol*.

Nº _____ ALUNO: _____

DI/FCT/UNL - Mestrado Integrado em Engenharia Informática
Segurança de Redes e Sistemas de Computadores - 2º Sem., 2017/2018
Teste de frequência #2, 16/Junho/2017(Ref. 20180707)

PARTE II – (Parte Com Consulta / 4 Páginas). Duração: 1h15

Questão 1. Considere o seu estudo sobre modelos de controlo de acesso e o modelo de controlo de acesso no sistema de ficheiros UNIX, responda.

a) O princípio dos mínimos privilégios indica que um programa, um utilizador e até o código do sistema não devem ter mais privilégios do que aqueles, que num dado instante, são necessários à execução das funções que lhe são confiadas. Diga, justificando, se considera que no controlo de acessos a ficheiros no UNIX com base num modelo DAC este princípio é seguido.

b) Um ficheiro executável pode ter uma permissão envolvendo um chamado *setuid bit*. Diga como funciona este mecanismo, dizendo para que é o mesmo utilizado e referindo as repercussões do mesmo em relação aos privilégios de execução por parte do *owner* de um ficheiro executável ou de outros utilizadores que também o passam executar.

c) A parametrização de controlo de acesso com o *setuid bit* na máscara de permissões de ficheiros executáveis põe em causa o princípio dos mínimos privilégios ? Justifique.

d) No contexto do sistema de autenticação usado no UNIX, suponha que o dono (*owner*) do ficheiro */etc/passwd* é o utilizador *root* e o grupo do dono é um grupo de que só o utilizador *root* faz parte; Considere que o ficheiro tem os direitos de acesso 0*644*. Diga porque é que a configuração de bits deve ou não ser esta e quais os inconvenientes desta solução.

e) Suponha agora que o ficheiro */etc/passwd* tem os direitos *0600* e que tem o *setuid bit* a 1. Quais as vantagens em relação à solução da alínea e) ?

Questão 2.

a) Em TLS, num acordo de Diffie-Hellman que usa o modo EPHEMERAL DIFFIE-HELLMAN e autenticação mútua, quantas operações do tipo exponencial módulo (X^Y modN) terão que ser realizadas pelo cliente, desde que inicia e até poder ser concluído o *handshake* e estabelecimento dos parâmetros de segurança da sessão TLS ? Justifique

Resposta:

_____ Exponenciais Módulo, para cada uma das seguintes operações:

Nº _____ ALUNO: _____

b) Em TLS, num acordo de Diffie-Hellman que usa o modo EPHEMERAL DIFFIE-HELLMAN e autenticação unilateral do servidor, quantas operações do tipo exponencial módulo (X^Y modN) terão que ser realizadas pelo cliente até poder ser concluído o *handshake* e estabelecimento dos parâmetros de segurança da sessão TLS ? Justifique.

Resposta:

_____ Exponenciais Módulo, para cada uma das seguintes operações:

Questão 3.

Como sabe o protocolo TLS pode ser usado com diferentes configurações, que dão origem a propriedades de segurança muito diferentes. Entre essas diferenças uma das configurações corresponde ao modo de autenticação (anónima, unilateral ou mútua). Outra repercute-se no tipo de autenticação subjacente à *CIPHERSUITE* usada. Como é sabido do estudo teórico do protocolo e seu impacto na prática, as configurações possuem impacto na operação do sub-protocolo *HANDSHAKE*, nomeadamente no fluxo de mensagens e máquina de estado de processamento por parte dos *endpoint*s.

No caso de uso de *CIPHERSUITES* que envolvem o algoritmo *Diffie-Hellman* (em diversas versões do protocolo) é possível estabelecer chaves de sessão nos modos "*EDH - Ephemeral Diffie-Hellman*", "*FDH - Fixed Diffie-Hellman*" ou "*ADH - Anonymus DIffie-Hellmen*".

a) Qual a diferença entre esses modos ? Justifique, discutindo os níveis de segurança de cada um desses modos.

b) No caso de *CIPHERSUITES* usando o modo EDH com autenticação unilateral do servidor, o que permite proteger um ataque contra a autenticação dos *endpoints* por interposição de um adversário do tipo "homem-no-meio" ? Justifique.

Nº _____ ALUNO: _____

c) Se a *ciphersuite* escolhida usar EDH e o modo de autenticação for mútua, então o cliente e o servidor não podem usar certificados de chaves públicas DSA. Verdadeiro ou Falso ? Justifique.

d) Suponha que lhe fornecem um *trace* do protocolo Handshake-TLS (por exemplo obtido com uma ferramenta do tipo *wireshark*).

D1) Como reconhece que se verificou autenticação unilateral só do cliente ?

D2) Como reconhece que o fluxo TLS (*endpoint* cliente e servidor) não está invertido, comparando com o cliente que pediu a conexão TCP e o servidor que aceitou essa conexão ?

Questão 4.

Suponha que dois *routers* estão a usar IPSec com uma combinação de *bundling* de SAs em túnel iterado, sendo as duas SAs as seguintes: uma SA usando AH e outra SA usando ESP com autenticação e confidencialidade. Que proteção de segurança adicional esse *bundling* permite, comparativamente a usarem uma única SA usando autenticação e confidencialidade ? Justifique.