

<div>P.PORTO</div> <div>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</div>	Tipo de Prova Exame Época Normal	Ano letivo 1º	Data 20-06-2022
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora 10h00	
	Unidade Curricular Segurança Informática	Duração 01h50	

Observações

- Com consulta de documentação própria.
- A cotação atribuída a cada pergunta é apresentada entre parêntesis retos.
- O tempo previsto para responder a cada questão é apresentado entre parêntesis retos.

PARTE I

1) [5 min]

(2,5 valores)

Classifique cada um dos seguintes mecanismos, em termos de medidas para garantir Confidencialidade (C), Integridade (I), Disponibilidade (D), ou combinação de várias.

Nota: à seleção de uma resposta incorreta é descontado 50% do valor atribuído à questão

- Mecanismo de controlo de acesso discrecionário DAC (0,5 valores)
- Mecanismo HMAC (0,5 valores)
- Mecanismo de cifra AES-CBC (0,5 valores)
- Mecanismo de sistema de ficheiros distribuído (0,5 valores)
- Mecanismo SELinux (0,5 valores)

2) [15 min]

(3,5 valores)

A Alice pretende comunicar com o Bob. Para isso, admitamos que (E_A, D_A) e (E_B, D_B) são os pares de chaves pública-privada de Alice e Bob, respetivamente. Enc e Dec são os processos de cifra e decifra, respetivamente. Se necessário, Alice e Bob têm acesso a uma função de hash H (e.g., SHA-512).

A título de exemplo, ficam algumas expressões:

- cifrar uma mensagem M com a chave E_A : $Enc(E_A, M)$
- criar um resumo da mensagem M: $H(M)$

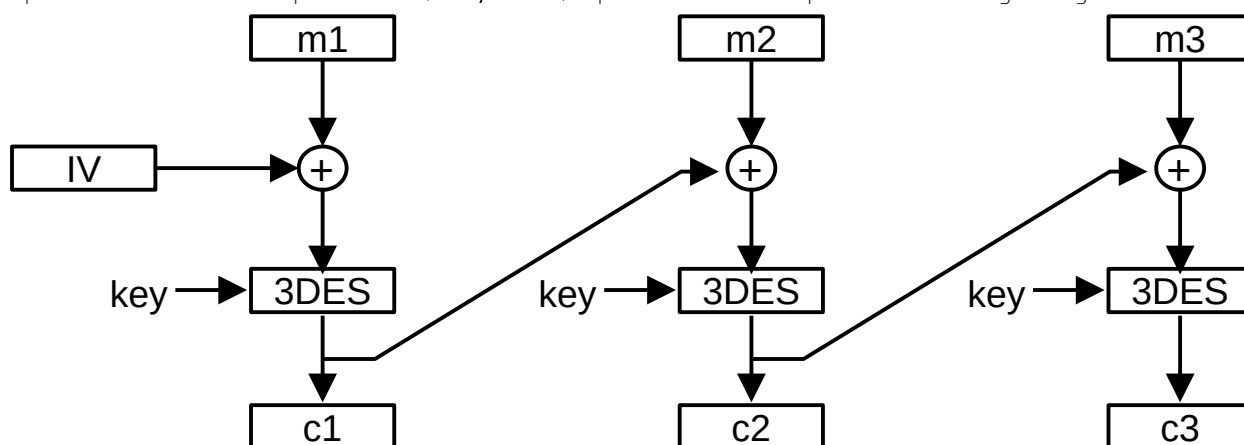
A Alice pretende enviar uma mensagem M ao Bob. Indique a expressão de cifra que permita:

- O envio da mensagem M, garantindo apenas confidencialidade (1,0 valores)
- O envio da mensagem M, assinada digitalmente (1,0 valores)
- Admita que o Bob pretende responder à Alice com a mensagem M', garantindo a confidencialidade e integridade da mensagem. (1,5 valores)

3) [20 min]

(3,5 valores)

Considere uma mensagem m, divisível em blocos de mensagens m1, m2 e m3. A cifra 3DES, usando o modo CBC, é aplicada de forma a obter o par cifrado c (i.e. c1, c2 e c3). O processo de cifra é apresentado na imagem seguinte.



P.PORTO <small>ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO</small>	Tipo de Prova Exame Época Normal	Ano letivo 1 ^a	Data 20-06-2022
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora 10h00	
	Unidade Curricular Segurança Informática	Duração 01h50	

Na imagem, ivector representa o vetor inicial e \oplus é a operação XOR. Assuma ainda que os processos de cifração e decifração são representados pelas expressões ENC_{3DES} e DEC_{3DES} , respetivamente.

- Escreva as **expressões** para os processos de cifração 3DES, que permitem obter cada um dos blocos de mensagens c_1 , c_2 e c_3 (1,0 valores)
- Considere o cenário em que o bloco de texto c_1 chega corrompido ao recetor. Será possível obter os blocos de mensagens m_1 , m_2 , e m_3 ? **Justifique de forma clara e sucinta** (1,5 valores)
- Escreva a **expressão** de decifra para o bloco c_1 , usado a simbologia presente na imagem (c_1 , m_1 , key, \oplus , etc.). (1,0 valores)

4) [15 min] (2,0 valores)

Assuma um cenário de um KDC, onde clientes utilizam os serviços que executam em servidores na rede. Em sua opinião, há alguma utilidade em cifrar o conteúdo dos bilhetes? Justifique devidamente a sua questão.

5) [15 min] (2,0 valores)

É possível implementar não-repudição recorrendo ao algoritmo AES? Justifique devidamente a sua resposta, indicando de que forma. No caso de considerar impossível, indique uma alternativa

PARTE II

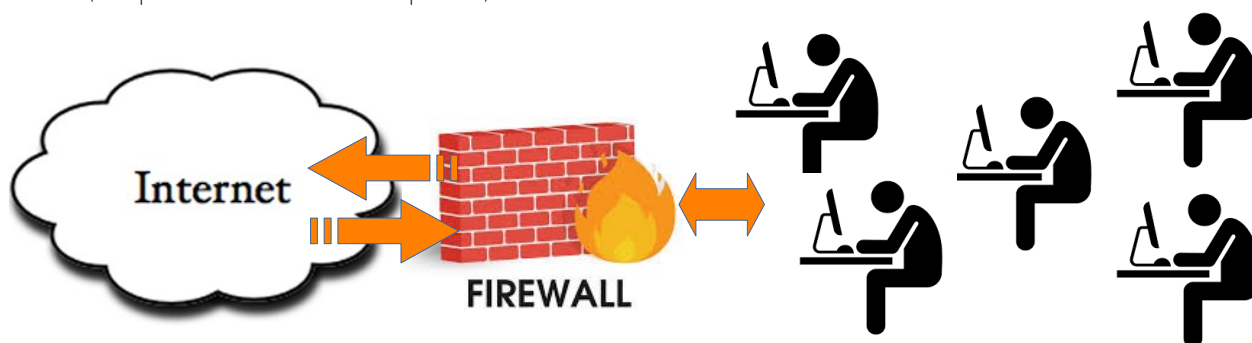
6) [10 min] (2,5 valores)

Usando os mecanismos de controlo de acesso mandatório (MAC), apparmor, e discricionário (DAC), ACLs, implemente as seguintes políticas:

- DAC: sobre o ficheiro "segredos.pdf", o utilizador Antonio tem permissão para ler (apenas e só), e o Augusto tem permissões para ler e escrever (apenas e só) (1,0 valores)
- MAC: o binário "/usr/bin/apache" tem permissões para abrir localmente a porta TCP 443, e para aceder em modo leitura (apenas e só) à diretoria "/var/www/*". Como verificaria que o perfil estaria em "enforce mode"? Apresente os comandos necessários e o conteúdo do perfil (1,5 valores)


7) [20 min] (4,0 valores)

Considere o cenário de uma rede de uma empresa de pequena dimensão, com acesso à Internet protegido por uma firewall (computador Linux + netfilter + iptables):



Defina regras iptables que permitam responder às seguintes políticas:

- Um datagrama é descartado quando não se enquadra nas regras já definidas nas chains INPUT, OUTPUT e FORWARD (1,0 valores)
- O endereço IP de destino para qualquer datagrama, com proveniência num qualquer dispositivo da rede interna da empresa e com destino a porta 53, deve ser alterado para 192.168.10.254:53 (1,0 valores)

 ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO	Tipo de Prova Exame Época Normal	Ano letivo 1º	Data 20-06-2022
	Curso Licenciatura em Segurança Informática em Redes de Computadores	Hora 10h00	
	Unidade Curricular Segurança Informática	Duração 01h50	

- c) É permitido às máquinas na rede interna da empresa acederem às portas 80 (HTTP) e 443 (HTTPS) de qualquer máquina na internet. Qualquer acesso feito neste contexto deve ficar registado (nos logs). A firewall deve permitir que datagramas com origem na Internet, e proveniência nas portas 80 e 443, só possam entrar na rede interna se ocorrerem num contexto de reposta a um pedido feito previamente por qualquer máquina na rede interna. (2,0 valores)