Fundamentos de Segurança Informática 2021/2021 — Exemplos de Perguntas

O teste intercalar e o exame final serão concebidos para 1:30 horas max (1 hora deverá ser suficiente). Terão 4/5 grupos, cada um com 4/5 perguntas, das quais são exemplo as perguntas que se seguem. A cotação de cada grupo será indicada no enunciado; cada pergunta dentro do grupo terá igual peso.

Grupo 1 - Conceitos e Terminologia de Segurança Informática *(20%)*

1.1. Indique duas motivações discutidas em aula para um atacante comprometer a máquina de um utilizador comum.

1.

2.

1.2. Identifique três tipos de atores que usualmente se consideram em análise de segurança

1.

2.

3.

1.3. Atribua um número ①: Ameaça, ②: Vulnerabilidade ou ③: Exploit a cada um dos seguintes exemplos.

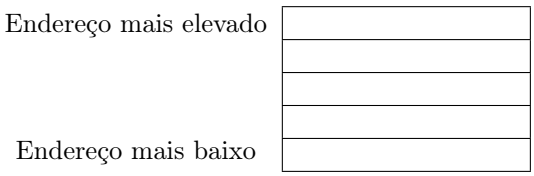
	update de segurança feito anualmente
	terramoto
	string de formatação que causa *crash*
	antigo colaborador em conflito
	utilização de `strcpy` sem teste de tamanho
	duplo `free`
	ficheiro `bitmap` que causa reescrita de endereço na *heap*
	data breach

1.4. Recorde o conceito de *confiabilidade* e preencha as células do lado direito da tabela, explicando como se relacionam os conceitos listados na célula correspondente do lado esquerdo.

ator ativo objetivo de segurança	
modelo de confiança modelo de ameaças política de segurança	

Grupo 2 - Controlo *(20%)*

2.1. Recorde o que estudou sobre a disposição clássica da stack gerida por uma função f chamada por uma função g e preencha o diagrama com os seguintes termos: ① **variáveis locais de** f, ② **frame pointer de** g, ③ **parâmetros passados por** g, ④ **endereço de retorno para** g.



2.2. A seguinte informação é verdadeira ou falsa? Justifique a sua resposta.

Um buffer overflow na stack de apenas um byte não permite a um atacante executar código arbitrário, uma vez que não permite alterar o endereço de retorno da função.