1 Considerações gerais

O trabalho prático consiste na pesquisa sobre um tema, e resposta com soluções baseadas em plataformas Linux. O trabalho deverá ser desenvolvido individualmente ou em grupo de dois estudantes (classificações atribuídas a estudantes do mesmo grupo poderão diferir).

A deteção de trabalhos fraudulentos invalida a nota de todos os trabalhos envolvidos. Serão considerados trabalhos fraudulentos, aqueles onde se verifique trabalho desenvolvidos por pessoas que não sejam os estudantes em processo de avaliação, na totalidade do trabalho ou apenas em parte deste.

1.1 Defesa

Todos os trabalhos práticos estão sujeitos a apresentação / defesa por parte dos estudantes que o elaboraram. A apresentação / defesa decorrerá na data indicada no planeamento da Unidade Curricular (aula de 02 de junho). A não comparência de um estudante à apresentação / defesa (exceto se devidamente justificado) implica a não consideração do trabalho para a nota do estudante em questão.

Uma apresentação / defesa considerada como não satisfatória por parte do docente da disciplina implica a não consideração do trabalho para a nota do estudante em questão.

1.2 Datas

A data de entrega é 29 de maio de 2022, pelas 23h59. Os trabalhos entregues fora de prazo não serão considerados. A entrega deverá ser efetuada por envio pelo moodle. Deverá ser entregue um ficheiro zip, designado X_Y.zip (sendo X e Y os números mecanográficos dos estudantes que compõem o grupo), contendo os seguintes itens:

1) Ficheiro com a apresentação, sendo que o primeiro slide deverá conter a identificação (nome, apelido, e número) dos estudantes;
2) Relatório, com máximo de 15 páginas, com resposta aos objetivos de cada tema de trabalho.

Quando solicitado, os estudantes deverão ainda disponibilizar os ficheiros de configuração da solução que implementaram.

1.3 Parâmetros da Avaliação

A avaliação baseia-se na: 1) Qualidade e Segurança na Apresentação (25%); e 2) Resposta aos Objetivos (75%).

2 Descrição do trabalho a desenvolver

O trabalho a desenvolver divide-se em duas fases. Cada uma dessas fases é descrita a seguir.

2.1 Fase I – pesquisa e análise de informação, de forma a responder aos "Objetivos"

2.1.1 Temas

Os temas do trabalho são:

Id	Tema	Objetivos	Área
1	Soluções IDS/IPS (Intrusion Detection/Prevention System)	- Arquitetura comum e serviços disponibilizados; - Princípios de funcionamento/deteção e limitações; - Software existente e abordagens; - Aplicação prática (exemplificar IPS, com criação de regras);	Confidencialidade / Integridade / Disponibilidade
2	Arquitectura IPSec	- Estudo do(s) protocolo(s); - Princípios e modos de funcionamento; - Estrutura dos datagramas; - Limitações; - Aplicação prática (exemplificar);	Confidencialidade / Integridade
3	Protocolos WEP vs WPA2	- Por que o WEP é considerado inseguro; - Exemplo prático da vulnerabilidade do WEP; - Melhoramentos introduzidos pelo protocolo WPA2; - Estudo do(s) protocolo(s); - Exemplificação prática de ataque ao WPA2;	Confidencialidade / Integridade
4	VPN para conexões seguras	- Estudo do(s) protocolo(s); - Princípios e modos de funcionamento; - Limitações; - Software existente; - Aplicação prática (exemplificar), com iptables (tráfego apenas possível sobre a VPN);	Confidencialidade / Integridade
5	Sistemas de armazenamento de ficheiros redundante	- Propriedades e cenários de interesse; - Software existente (usar DRBD + RAID) e alternativas possíveis;	Disponibilidade

		– Redundância no nó, e redundância entre nós; – Alternativas/opções adicionais? – Aplicação prática (exemplificar) com testes de carga;	
6	Facebook phishing com DNS poisoning	– Propriedades do ataque (em que consiste, protocolos envolvidos, técnicas aplicadas, etc.); – Aplicação prática (exemplificar); – Proteções existentes, e aplicação prática;	Confidencialidade / Integridade / Disponibilidade
7	Sistemas para balanceamento de carga	– Propriedades, funcionamento, e cenários de interesse; – Software existente (Nginx) e alternativas possíveis; – Articulação com outros sistemas (SGBD, servidores Web, etc.); – Aplicação prática (exemplificar) com testes de carga;	Disponibilidade/ Integridade
8	HTTP Seguro em CMS	– Estudo do(s) protocolo(s); – Propriedades, funcionamento, e cenários de interesse; – Estrutura dos certificados digitais; – Suporte da comunicação pelo browser; – Aplicação prática (exemplificar);	Confidencialidade / Integridade
9	Criptografia vs. Esteganografia vs. Ofuscação	– Em que consiste e qual o seu propósito; – Limitações e alternativas; – Ferramentas existentes para aplicação das técnicas; – Aplicação prática (exemplificar) de cada técnica, combinação de várias (recorrendo a imagens e som);	Confidencialidade (e integridade)
10	Conceito de sandbox	– Interesse/utilidade prática e funcionalidades; – Java Virtual Machine, chroot e containers; – Executar, ou não executar, aplicações como root dentro de containers, e explicar porquê; – Aplicação prática (exemplificar), utilizando Docker;	Confidencialidade / Integridade / Disponibilidade
11	SIEM – Security information and event management	– Interesse/utilidade prática e funcionalidades; – Integração com outras ferramentas; – Modo de funcionamento e limitações; – Aplicação prática (exemplificar), utilizando o Splunk (análise de logs) com ligação a outros sistemas presentes na rede;	Confidencialidade / Integridade / Disponibilidade
12	Honeypots	– Arquitetura e princípio de funcionamento; – Serviços disponibilizados; – Limitações; – Soluções já existentes e demonstração de funcionalidades; – Aplicação prática (exemplificar) pela construção de um honeypot (com vários serviços);	Confidencialidade / Integridade / Disponibilidade

13	Funcionamento do GPG e OpenPGP	– Porquê GPG, PGP e OpenPGP; – Comparação com PKI; – Como é feita a gestão de chaves; – Arquitetura, modo de operação deste sistema, e o que permite proteger; – Onde pode ser aplicado; – Aplicação prática (exemplificar);	Confidencialidade / Integridade
14	Captura de tráfego em ligações telefónicas	– Sistemas existentes para telefonia voz e vídeo; – Protocolos envolvidos na comunicação; – Limitações dos protocolos relativamente à segurança informática; – Importância dos certificados digitais em comunicações seguras; – Aplicação prática (exemplificar), demonstrando com o Wireshark a possível captura de uma conversa e uso de certificados para impedir o ataque;	Confidencialidade / Integridade

2.1.2 Objetivo

O objetivo do trabalho consiste em responder aos tópicos identificados na coluna "Objetivos", da tabela anterior. A cada grupo será atribuído um tema (ver no moodle).

2.2 Fase II – apresentação

Cada grupo faz a defesa do seu trabalho com base numa apresentação, que terá a duração mínima de 10 minutos, e máxima de 12 minutos Segue-se depois uma sessão de perguntas e respostas, com a duração entre 3 a 5 minutos.