UNIVERSIDADE DE AVEIRO

DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA

Aprendizagem Aplicada à Segurança (2020/2021)

Exame Teórico (15/Fev/2021)

Nome: Nº Mec:

Parte I

1. (3.5 valores) Explique a diferença entre um ataque de disrupção e um ataque de interceção, e dê um exemplo onde ambos os tipos de ataques podem ser usados em sequência de modo a potenciar o resultado final dos ataques.

2. (3.5 valores) Numa rede empresarial pretende-se implementar um sistema de monitorização da utilização do serviço DNS de modo a detetar ataques de phishing e comunicações ilícitas de BotNets. Proponha duas metodologias de aquisição de dados, incluindo, identificação do local de aquisição de dados e eventuais alterações à infraestrutura de rede.

3. (3.0 valores) Explique o que entende por dados qualitativos e dados quantitativos, e apresente uma solução de monitorização do estado geral dos equipamentos de uma rede (routers, switches, pontos de acesso, etc) usando o protocolo SNMP que permita obter os dois tipos de dados.

Parte II