UNIVERSIDADE DE AVEIRO

DEPARTAMENTO DE ELECTRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA

Aprendizagem Aplicada à Segurança (2020/2021)

Exame Teórico - Recurso (1/Mar/2021)

Nome: Nº Mec:

Parte I

1. (3.0 valores) Identifique possíveis metodologias/vetores de ataque para efetivar durante um ataque a fase de infiltração numa de rede empresarial. Explique porque nesta fase do ataque é difícil a sua deteção deteção e em muitos casos impossível.

2. (3.5 valores) Explique o que intende por exfiltração de dados durante um ataque a uma rede empresarial, e proponha três metodologias de monitorização de rede que permitam obter dados para identificar potenciais comportamentos de exfiltração de dados.

3. (3.5 valores) Numa rede suspeita-se da existência de atividades ilícitas com comportamento pseudo-periódico entre 30 e 120 segundos. Assumindo que apenas se tem como dados o número de pacotes de upload/download de cada máquina, proponha: (i) uma metodologia de tratamento dos dados e (ii) uma lista de possíveis *features* a extrair, que permitam identificar comportamentos suspeitos em cada máquina.

Parte II