Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Exame Teórico de Técnicas de Perceção de Redes
14 de Fevereiro de 2022

Duração: 2h00m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Uma rede empresarial de grandes dimensões foi comprometida e múltiplos servidores estão infetados com software ilícito que permite o seu controlo remoto com permissões de administração e assume-se que serão usados para a mineração de cripto-moedas.
   a) Proponha um conjunto de metodologias de aquisição de dados ao nível da rede ou dos servidores passíveis de ser usados para a identificação dos servidores comprometidos. (5.0 valores)
   b) Proponha um conjunto de métricas e *features* (calculadas a partir das métricas) que poderão permitir distinguir a comunicação lícita da ilícita com estes servidores. Assuma que os serviços continuam ativos e a servir clientes lícitos. (5.0 valores)
   c) Assumindo que os controladores ilícitos dos servidores recebem comandos do exterior de forma periódica (de 10 em 10 segundos) e o software de mineração faz o download e upload de dados também de forma periódica (de 2 em 2 minutos), proponha uma metodologia de tratamento de dados que permita obter dados relevantes para a sua deteção. (5.0 valores)
2. Explique a diferença entre um ataque de disrupção e um ataque com exfiltração de dados, e proponha soluções passíveis de serem incorporadas na arquitetura de uma rede empresarial para detetar os dois tipos de ataques. (5.0 valores)