Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Theoretical Exam of Técnicas de Perceção de Redes
February 14th, 2022

Duration: 2h00m. Carefully justify all your answers.

1. A large enterprise network has been compromised and multiple servers are infected with illicit software that allows remote control with administration permissions and is assumed to be used for cryptocurrency mining.
   a) Propose a set of data acquisition methodologies at the network or server level that can be used to identify compromised servers. (5.0 points)
   b) Propose a set of metrics and features (calculated from the metrics) that may allow to distinguish between legal and illegal communication with these servers. Assume the services are still active and serving licit customers. (5.0 values)
   c) Assuming that the illicit server controllers receive commands, from the exterior of the network, periodically (every 10 seconds) and the mining software downloads and uploads data is also done periodically (every 2 minutes). Propose a methodology of data processing that allows obtaining relevant data for its detection. (5.0 points)
2. Explain the difference between a disruption attack and a data exfiltration attack, and propose solutions that can be incorporated into the architecture of an enterprise network to detect both types of attacks. (5.0 points)