2023 16 janeiro

1. uma rede empresarial ... maquinas infetados DNS.

a) proponha um conjunto de metodologias de aquisição de dados ao nível da rede e dos servidores possiveis de ser usados para identificação.

b) proponha um conjunto de metricas e features (calculados a partir das metricas) que poderão permitir distinguir de comunicaçt DNS licita da ilicita destes terminais comprometidas.

c) Assumindo que os controladores ilicitos dos terminais recebem comandos do exterior de forma periodica (de 30 em 30 segundos) e o sw ilicito faz o dw e up de dados também de forma periodica (de 5 em 5 seg), proponha uma metodologia de tratamento de dados que permita obter dados relevantes para sua deteção.

2. Durante um ataque de (igual exame de recurso 2022) DDoS a um servidor explique qual a importancia de identificar os clientes licitos dos ilicitos, proponha um conjto de os diferenciar.