Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Exame Teórico de Técnicas de Perceção de Redes
7 de Julho de 2021

Duração: 1h45m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Uma rede empresarial de grandes dimensões foi comprometida e múltiplas máquinas estão infetadas (terminais e servidores) com software ilícito que criou uma BotNet interna. Os elementos da BotNet podem a qualquer momento efetuar uma das seguintes atividades: (i) comunicar diretamente entre si para sincronismos de ações, (ii) receber comandos do exterior da rede via ligações HTTPS e (iii) participar no envio de e-mail em quantidades elevadas (Spam) usando o servidor da empresa.

   a) Proponha um conjunto de metodologias de aquisição de dados ao nível da rede passíveis de ser usados para a identificação das máquinas comprometidas durante as três possíveis atividades das mesmas. (4.0 valores)

   b) Proponha um conjunto de métricas e *features* (calculadas a partir das métricas) que poderão permitir distinguir a comunicação lícita da ilícita entre máquinas na rede. (4.0 valores)

   c) Assumindo que os elementos da BotNet recebem comandos do exterior de forma periódica (de 30 em 30 segundos), proponha uma metodologia de tratamento de dados que permita obter dados relevantes para a sua deteção. (4.0 valores)

   d) Proponha um método para a criação de um perfil de envio de e-mails lícitos por parte dos terminais/servidores da empresa que permita detetar anomalias no envio de Spam. Nota: assuma que servidores comprometidos podem no passado ter enviado grandes quantidades de e-mails lícitos. (4.0 valores)

2. No contexto da criação de perfis comportamentais de entidades de rede, explique a diferença entre um problema de classificação de comportamentos e um problema de deteção de comportamentos anómalos. Apresente alguns exemplos. (4.0 valores)