Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Exame Teórico de Recurso de Técnicas de Perceção de Redes
6 de fevereiro de 2024

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

1. A rede de uma organização de grandes dimensões foi comprometida e múltiplos terminais estão potencialmente infetados com software ilícito que permite o seu controlo remoto. Não é possível efetuar qualquer tipo de monitorização ao nível de cada terminal.

   a) Suspeita-se que o software ilícito colocou alguns terminais a participar num ataque DDoS a servidores HTTPS externos, no entanto gerando poucos pedidos por segundo. Proponha um conjunto de metodologias de aquisição e processamento de dados que permita a identificação dos terminais comprometidos. (5.0 valores)

   b) Assumindo que o software ilícito é controlado remotamente (C&C) usando túneis IP sobre DNS (UDP). Note que a política de segurança da empresa bloqueia o tráfego DNS para o exterior. Proponha uma metodologia de aquisição e processamento de dados que permita a identificação de terminais comprometidos. (5.0 valores)

2. Perante um ataque de DDoS aos servidores da organização, proponha uma possível metodologia de diferenciação dos clientes (lícitos e ilícitos) quando o ataque é dirigido aos servidores HTTPS. Considere que não existe qualquer processo de autenticação no acesso ao serviço, a origem dos ataques é muito diversificada e alguns ataques tem origem em redes de parceiros comerciais. (5.0 valores)

3. Suponha que possui cinco modelos comportamentais já treinados (A, B, C, D e E) para a classificação de tráfego aplicacional ao nível da rede (considere a existência de quatro classes de aplicações).

   a) Proponha uma metodologia de avaliação do desempenho dos modelos levando em conta apenas a identificação correta de uma aplicação específica (uma das quatro classes). (1.5 valores)

   b) Proponha uma metodologia para melhorar o desempenho na classificação do tráfego aplicacional ao fim de um período de observação. (3.5 valores)