Universidade de Aveiro

Mestrado Integrado em Engenharia de Computadores e Telemática

Exame Teórico de Técnicas de Perceção de Redes

18 de Janeiro 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) Assumindo que o software ilícito começou a enviar e-mails de SPAM usando credenciais legítimas (do utilizador do terminal) e os servidores de e-mail da organização, 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 vai tentar fazer a exfiltração de dados pelo serviço de WebOffice da organização (ex. Office365 ou Google Docs), proponha um conjunto de metodologias de aquisição e processamento de dados que permita a identificação de terminais comprometidos. (5.0 valores)

2. Perante um ataque de DDoS a servidores da organização;

   a) Explique qual a importância de diferenciar os pedidos lícitos dos ilícitos. (1.0 valores)

   b) Proponha possíveis metodologias de diferenciação dos clientes quando o ataque é dirigido (i) a um servidor HTTPS com os serviços web da organização (assumindo a existência de um processo de autenticação) e (ii) ao serviço DNS (UDP) da organização. (5.0 valores)

3. Suponha que possui três modelos comportamentais já treinados (A, B e C) para a deteção de comportamentos anómalos. Todos os modelos tem um F1-*score* de aproximadamente 0.75.

   a) Proponha uma metodologia para melhorar o desempenho na deteção de anomalias ao fim de um período de observação. (2.0 valores)

   b) Proponha uma metodologia para melhorar o desempenho da deteção de anomalias num cenário onde a decisão pode ser mais lenta. (2.0 valores)

forest

SVM

LOF