Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

Exame Teórico de Recurso de Técnicas de Perceção de Redes
28 de Fevereiro de 2022

Duração: 2h00m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Uma rede empresarial de grandes dimensões possui um sistema de acesso remoto para gestão da infraestrutura, serviços e dos sistemas de armazenamento de dados.
   a) Proponha um conjunto de metodologias de aquisição e de tratamento de dados passíveis de serem usadas para a identificação de acessos externos ilegais ao sistema de gestão, justificando o propósito das mesmas. Deve assumir que os acessos ilegais são feitos usando credenciais válidas que de alguma forma foram comprometidas. (5.0 valores)
   b) Assumindo que a rede foi comprometida e múltiplas máquinas estão infetadas (terminais e servidores) com software ilícito que criou uma BotNet interna. Os elementos da Botnet interna vão comunicar entre si para coordenar ataques. Proponha um conjunto de metodologias de aquisição de dados ao nível da rede passíveis de ser usados para a identificação das máquinas comprometidas, justificando o propósito das mesmas. (5.0 valores)
   c) Após a coordenação dos elementos da Botnet estes vão exfiltrar dados para apenas um servidor externo usando HTTPS. Num determinado momento, apenas um elemento da BotNet transmite dados e os outros estão silenciosos. O elemento transmissor irá mudar aleatoriamente. Proponha uma metodologias de identificação das máquinas comprometidas. (5.0 valores)
2. Durante um ataque de DDoS a um servidor HTTP/HTTPS explique qual a importância de identificar os cliente lícitos e os ilícitos. Proponha possíveis metodologias de os diferenciar. (5.0 valores)