






**Universidade de Aveiro**  
**Mestrado em Cibersegurança**

Exame Teórico de Ep. Especial de Segurança em Redes de Comunicações  
13 de Setembro de 2021

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

-  1. Explique as diferentes fases e possíveis **vetores de ataque** para o **roubo de dados** numa sistema de base de dados numa empresa. Apresente **possíveis mecanismos de defesa**. (4.0 valores)
  
-  2. Uma empresa pretende colocar na sua infraestrutura de rede um conjunto de **servidores HTTPS** (portos TCP 443 e TCP 8888) acessíveis do **exterior** com vários serviços Web da empresa. Proponha uma solução de proteção da rede que permita (i) **controlar os fluxos de tráfego de acesso aos serviços** e (ii) **proteger a infraestrutura contra ataques de negação de serviço distribuídos (DDoS)**. Assuma que a empresa apenas tem uma infraestrutura de encaminhamento de tráfego IP e que possui utilizadores internos que precisam de aceder à Internet (4.5 valores)
  
-  3. Proponha uma solução de interligação entre **múltiplos polos de uma empresa** que providencie **confidencialidade** para o **tráfego de videoconferência** e **tráfego de sincronismo** de base de dados entre elas (e apenas a esse tráfego). (4.0 valores)
  
-  4. Admitindo que numa rede empresarial existem **múltiplas fichas Ethernet** em espaços públicos ou semi-públicos e terminais Wi-Fi, proponha uma solução integrada de **controle do acesso** de máquinas à rede. (3.0 valores)
  
-  5. Numa rede empresarial pretende-se implementar um **sistema de deteção de intrusões (IDS)** que permita detetar as máquinas comprometidas por uma **BotNet**. 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**. Explique como o sistema pode ser **integrado na arquitetura** de uma rede empresarial e proponha um possível **conjunto de regras** para a deteção de comunicações ilícitas. (4.5 valores)