

**Universidade de Aveiro**  
**Mestrado em Cibersegurança**  
Exame Teórico de Recurso de Segurança em Redes de Comunicações  
12 de Julho 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 sensíveis 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 (porto TCP 443) acessíveis do exterior com vários serviços Web da empresa. Proponha uma solução, assumindo a existência já de firewalls de proteção da rede mas nenhum servidor com acesso do exterior. (2.5 valores)
3. Proponha uma solução integrada de proteção de uma rede empresarial contra ataques de negação de serviço distribuídos (DDoS). (4.0 valores)
4. Proponha uma solução de interligação entre múltiplos polos de uma empresa que providencie confidencialidade para o tráfego VoIP entre elas (e apenas a esse tráfego). (2.5 valores)
5. Admitindo que numa rede empresarial existem múltiplas fichas Ethernet em espaços públicos ou semi-públicos, proponha uma solução integrada de controle do acesso de máquinas à rede. (3.0 valores)
6. Numa rede empresarial pretende-se implementar um sistema de deteção de intrusões (IDS) que permita detetar (i) comunicações de comando e controlo de elementos de uma BotNet por HTTPS e (ii) envio de Spam por máquinas na empresa usando o servidor de e-mail 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. (4.0 valores)