

# Universidade de Aveiro

## Exame Teórico (Recurso) – Segurança em Redes de Comunicações 5 de julho de 2024

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

Considerando a rede empresarial em anexo:

1. No contexto das fases de um ataque a uma rede empresarial, explique o que entende por fase de aquisição de conhecimento e indique possíveis meios de recolha de dados por parte dos atacantes. (3.0 valores)
2. Assumindo que a empresa deseja implementar um conjunto de servidores/serviços para suporte à operação, nomeadamente (i) vários servidores Web HTTPS na DMZ com vários sites/domínios (portas TCP 443) públicos que deverão estar disponíveis para o exterior, (ii) um servidor Web HTTPS com a Intranet da empresa (porta TCP 443) no Datacenter B que deverá estar disponível apenas para os terminais internos, (iii) um servidor Web HTTPS com os serviços críticos da empresa (porta TCP 443) no Datacenter C que deverá estar disponível apenas para os terminais da VLAN 5, (iv) os terminais do Edifício A só podem comunicar com os terminais do edifício B usando o serviço Samba (porto TCP 445), e (v) um servidor de backup de dados (porta TCP 5555) no Datacenter B que recolhe dados dos servidores Web HTTPS (DMZ e Datacenter C) e envia-os para um servidor externo.
  - a) Proponha as alterações de arquitetura de rede necessárias de modo a poder implementar o controlo de fluxos e proteção contra ataques DDoS, e defina as diferentes zonas da rede que permitam a implementação dos requisitos de controlo de fluxos. (3.0 valores)
  - b) Apresente as regras de *firewall*/controle de fluxo de tráfego (de alto nível) para o requisito (v). Indique as respetivas zonas e firewalls onde as regras devem ser implementadas. (3.0 valores)
3. Proponha uma solução integrada de comunicação IPv4 ao nível da rede e respetivas alterações nas regras das Firewalls que garanta que o tráfego das máquinas virtuais existentes no Datacenter B para um conjunto de múltiplas máquinas virtuais em diversos servidores (em diferentes localizações geográficas) na Cloud da Microsoft seja transmitido de forma segura que garanta confidencialidade. Considere que as redes virtuais e servidores remotos são extremamente dinâmicos (são criados e destruídos frequentemente) e são geridos pela empresa. (3.0 valores)
4. Proponha um sistema SIEM, incluindo a fonte de dados e o processo de coleta desses dados, e a definição de regras de alerta, capaz de alertar para:
  - a) Terminais dos utilizadores comprometidos por Worms/Trojans, que irão efetuar comunicações ilícitas com o exterior da rede usando o Google drive (HTTPS). Apresente pelo menos duas regras. (2.0 valores)
  - b) Identificação de clientes externos a participar num ataque DDoS aos servidores da empresa. Apresente pelo menos duas regras. (2.0 valores)
  - c) Possível comunicação IPv4 de C&C (poucos dados) de uma botnet sobre DNS. (2.0 valores)
  - d) Tentativas de propagação de Worms/Trojans entre máquinas da empresa. (2.0 valores)

- Nos switches Layer 2 do edifício A estão configuradas portas de acesso para as VLANs 1, 2 e 3.
- Nos switches Layer 2 do edifício B estão configuradas portas de acesso para as VLANs 4, 5 e 6.
- As ligações entre os switches Layer2 e os switches Layer3 F1 a F4 são feitas usando ligações trunk/inter-switch com permissão de transporte para todas as VLANS;
- Os interfaces entre os switches Layer 3 são portas Layer 3 (IP routing) e os interfaces entre os switches Layer 3 e os routers são portas Layer 3 (IP routing);
- A empresa possui dois Datacenters para serviços internos (Datacenter A e Datacenter B);
- Os switches Layer3, routers e firewalls têm os processos dos protocolos OSPFv2 e OSPFv3 ativos em todas as redes IP;
- Os routers de acesso à Internet (Routers 1 e 2), estão a anunciar (por OSPF) rotas por omissão;
- Todos os interfaces tem um custo OSPF de 1.

