Universidade de Aveiro

Exame Teórico (Recurso) – Segurança em Redes de Comunicações
20 de julho de 2022

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 propagação do ataque e proponha metodologias de deteção destas atividades ilícitas. (3.0 valores)

2. Proponha um conjunto de alterações arquiteturais à rede empresarial de modo a protegê-la de ataques DDoS e permitir a implementação de controles de fluxo de tráfego entre as diferentes zonas da empresa e o exterior. Desenhe um novo diagrama de rede com as alterações/adições, indicando o tipo, funcionalidade e/ou modo de operação de cada equipamento. (4.0 valores)

3. Assumindo que a empresa deseja implementar um conjunto de servidores para prestação de serviços, nomeadamente (i) um servidor Web HTTPS com vários sites/domínios (porta TCP 443) públicos que deverão estar disponíveis para o exterior, (ii) um servidor Web HTTPS com a Intranet da empresa (porta TCP 443) que deverão estar disponíveis apenas para os terminais internos, e (iii) três servidores de base de dados MySQL (porta TCP 3306) que apenas deverão estar acessíveis pelos servidores HTTPS e por um servidor MySQL pré-definido externo para sincronização/replicação. Proponha as alterações de arquitetura de rede necessárias e apresente uma lista das regras de *firewall*/controle de fluxo de tráfego (de alto nível) nos vários locais. (4.0 valores)

4. Proponha uma solução de interligação, entre um conjunto de servidores de base de dados no Datacenter A e um Datacenter na Internet, capaz de fornecer confidencialidade ao nível de rede para o tráfego de sincronização dos dados dos servidores HTTPS (e somente esse tráfego). Apresente também as alterações necessárias às políticas de controlo de fluxo de tráfego nas firewalls para permitir o estabelecimento da ligação segura e transmissão de dados. (2.5 valores)

5. Assumindo que empresa deseja implementar tele-trabalho onde os utilizadores remotos terão acesso privilegiado a dois servidores com SSH (porta TCP 2222) no Datacenter A. Proponha uma solução integrada que permita o acesso dos utilizadores remotos e controlar o acesso aos serviços. Deverá incluir na sua proposta as alterações necessárias às políticas de controlo de fluxo de tráfego nas firewalls. (2.5 valores)

6. Proponha um sistema SIEM, incluindo o processo de coleta de dados e a definição de regras de alerta, capaz de alertar para:
   a) Tentativas de acesso ilegítimo (com logins falhados) aos servidores com SSH no Datacenter A. (1.0 valores)
   b) Possível comunicação sobre HTTPS de tráfego P2P (por exemplo: BitTorrent). (1.5 valores)
   c) Possível exfiltração de dados de servidores MySQL acessíveis do exterior, para os quais não tem permissões de administração. (1.5 valores)

- Nos switches Layer 2 dos edifícios 1 e 2 estão configuradas portas de acesso para as VLANs 1,2,3,4,5 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 internos para serviços internos (Datacenters A e B);
- Os switches Layer3 e routers 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.