Universidade de Aveiro

Exame Teórico – Segurança em Redes de Comunicações
6 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 como propósito de roubo de dados a uma rede empresarial, explique porque a deteção e mitigação do ataque é muito mais difícil durante a fase de infiltração do que durante as fases de propagação e exfiltração. (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 múltiplos controles de fluxo de tráfego. 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 permitir que os terminais (não servidores) internos apenas acedam a serviços HTTPS na Internet (porta TCP 443). E em paralelo implementar um conjunto de servidores para prestação de serviços ao público (Internet), os novos serviços incluem (i) um servidor Web HTTPS com vários sites/domínios (porta TCP 443) e (ii) um servidor de e-mail (porta TCP 465 para comunicação SMTP segura entre servidores e porta TCP 993 para acesso de cliente via IMAPS) . 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 utilizando a ligação WAN da empresa, entre um conjunto de servidores de base de dados no Datacenter A e Datacenter B, capaz de fornecer confidencialidade ao nível de rede para o tráfego de sincronização dos dados dos servidores (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. (3.0 valores)

5. Assumindo que empresa deseja implementar tele-trabalho onde os utilizadores remotos terão acesso privilegiado a dois servidores HTTPS (porta TCP 443) 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. (3.0 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) a servidores no Datacenter B com origem em terminais internos. (1.5 valores)
   b) Possível comunicação de C&C (*command and control*) via HTTPS entre um atacante externo e máquinas internas comprometidas por agentes de uma Botnet. (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);
- Existe uma ligação WAN via satélite que suporta ligações IPv4 entre a rede da empresa e um datacenter remoto (Datacenter 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.