Universidade de Aveiro

Exame Teórico (recurso) – Segurança em Redes de Comunicações
28 de junho de 2023

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 exfiltração do ataque e como os atacantes podem aumentar a dificuldade da sua deteção. (2.0 valores)
2. Proponha um conjunto de alterações arquiteturais à rede empresarial de modo a protegê-la de ataques DDoS de forma eficiente e com o menor impacto possível no desempenho da rede e serviços. Desenhe um diagrama de rede com as alterações propostas. (3.0 valores)
3. Assumindo que a empresa deseja implementar um conjunto de servidores para prestação de serviços, nomeadamente (i) os terminais dos edifícios apenas podem comunicar entre si usando comunicações TCP entre os portos 3343 (origem e destino), e comunicar com o exterior usando apenas o porto TCP 443 (destino), (ii) vários servidores Web HTTPS na DMZ com vários sites/domínios (portas TCP 443) públicos que deverão estar disponíveis para o exterior, (iii) um servidor Web HTTPS com a Intranet da empresa (porta TCP 443) no Datacenter A que deverá estar disponível apenas para os terminais internos do edifício A, e (iv) três servidores de armazenamento de dados (portas TCP 6800 a 6900) no Datacenter A que apenas deverão estar acessíveis pelos servidores Web HTTPS e por um servidor AWS externo para sincronização/replicação dos dados.
   a) Proponha as alterações de arquitetura de rede necessárias de modo a poder implementar o controlo de fluxos. Defina as diferentes zonas da rede e desenhe um diagrama de rede com as alterações propostas. (2.5 valores)
   b) Apresente uma lista das regras de *firewall*/controle de fluxo de tráfego (de alto nível) nos vários locais. Indicando a firewall e as zonas entre as quais as regras se aplicam. (3.0 valores)
4. Proponha uma solução de comunicação IPv4 ao nível da rede, respetivas alterações nas regras das Firewalls e soluções de autenticação dos equipamentos envolvidos:
   a) Garanta que o tráfego UDP das máquinas virtuais existentes no Datacenter A para um conjunto conhecido de servidores AWS da Amazon (a lista de redes IP são conhecidas) seja encaminhado de forma que garanta confidencialidade. (2.0 valores)
   b) Garanta que o tráfego UDP das máquinas virtuais existentes no Datacenter A 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). (2.0 valores)
5. 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 uso ilegítimo dos servidores DNS da empresa, para exfiltração ou C&C. (2.0 valores)
   b) Possível comunicação IPv4 de C&C usando um serviço legitimo e autorizado (por exemplo o Twitter). (2.0 valores)
   c) Possível exfiltração de dados por HTTPS de terminais da administração da empresa. (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 um Datacenter interno para serviços internos (Datacenter A);
- 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.