

PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO
CARGO 20: TÉCNICO JUDICIÁRIO
ÁREA: APOIO ESPECIALIZADO
ESPECIALIDADE: TECNOLOGIA DA INFORMAÇÃO

Prova Discursiva

Aplicação: 6/11/2022

PADRÃO DE RESPOSTA DEFINITIVO

Em seu texto, o(a) candidato(a) deve mencionar os aspectos apresentados a seguir.

Definição e objetivo da solução sistema de detecção de intrusão (IDS)

- A tecnologia de segurança de rede, originalmente, foi criada para detectar explorações de vulnerabilidade em um aplicativo ou um computador de destino.
- Um IDS é um dispositivo de monitoramento passivo que detecta ameaças potenciais e gera alertas, permitindo que analistas do centro de operações de segurança (SOC) ou respondentes de incidentes investiguem e respondam ao incidente em potencial.
- Um IDS não oferece proteção real para o *endpoint* ou a rede.
- É um sistema passivo que verifica o tráfego e relata as ameaças.

Definição e objetivo solução sistema de prevenção de intrusão (IPS)

- Estendem as soluções de IDS, adicionando a capacidade de bloquear ameaças, além de detectá-las. Tornaram-se a opção de implantação dominante para as tecnologias IDS/IPS.
- *Software* que procura atividades suspeitas e alerta os administradores.
- Analisa ativamente e realiza ações automatizadas em todos os fluxos de tráfego que entram na rede. Essas ações podem incluir o envio de um alarme para o administrador; o descarte de pacotes maliciosos; o bloqueio do tráfego do endereço de origem; a redefinição da conexão; e a configuração de *firewalls* para evitar ataques.
- Sistema que pode detectar uma atividade intrusiva e também pode tentar interromper a atividade, idealmente antes que ela atinja seus alvos.

Definição e objetivo da solução *firewall*

- Dispositivo de conexão entre redes que restringe o tráfego de comunicação de dados entre duas redes conectadas.
- Encaminha ou rejeita/descarta pacotes em uma rede.
- *Firewalls* geralmente têm regras que restringem quais portas estão abertas.
- Em essência, um *firewall* é projetado para proteger uma rede ou um conjunto de redes conectadas dentro do *firewall* contra tráfego da Internet e outros tráfegos que vêm do lado de fora do *firewall*.
- Um *firewall* pode agir como um filtro de pacotes. Ele pode funcionar como um filtro positivo, permitindo somente a passagem de pacotes que estejam de acordo com critérios específicos, ou como um filtro negativo, rejeitando qualquer pacote que satisfaça certos critérios.
- Um *firewall* é um dispositivo de segurança de rede que monitora o tráfego de rede de entrada e saída e decide se permite ou bloqueia tráfego específico com base em um conjunto definido de regras de segurança.

QUESITOS / CONCEITOS

0 – Respondeu erroneamente ou não respondeu.

1 – Respondeu corretamente, contudo de forma muito parcial (25% do esperado de acordo com o padrão de resposta).

2 – Respondeu corretamente, contudo de forma parcial (50% do esperado de acordo com o padrão de resposta).

3 – Respondeu corretamente, mas não de forma completa (75% do esperado de acordo com o padrão de resposta).

4 – Respondeu corretamente de forma completa (100% do esperado de acordo com o padrão de resposta).