1.Intrusion Prevention System

Um **Sistema de Prevenção de Intrusão (IPS - Intrusion Prevention System)** monitora o tráfego da rede em tempo real e bloqueia ameaças automaticamente ao detectar atividades suspeitas. Ele é capaz de impedir ataques conhecidos, como exploração de vulnerabilidades em sistemas operacionais e aplicações, além de proteger contra técnicas genéricas como **buffer overflow** e **injeção de SQL**.

Diferente do IPS, um **Sistema de Detecção de Intrusão (IDS - Intrusion Detection System)** **apenas alerta sobre ameaças, mas não pode bloqueá-las**. Essa diferença é crucial, pois um IDS sozinho não impede que ataques aconteçam, apenas informa que atividades suspeitas foram identificadas.

A implementação de um IPS pode trazer desafios, especialmente em relação à disponibilidade da rede. Como ele atua monitorando pacotes em tempo real, falhas no hardware, falta de energia ou bugs no software podem fazer com que o dispositivo pare de funcionar. Dependendo da configuração, um IPS pode operar em dois modos:

1. **Fail-open**: Se o IPS falhar, o tráfego continua fluindo normalmente, mas sem segurança.
2. **Fail-closed**: Em caso de falha, a rede fica indisponível, impedindo qualquer comunicação.

A arquitetura de um IPS pode ser configurada de duas formas:

- **Monitoramento Ativo (Inline Monitoring)**: O IPS é inserido diretamente no caminho do tráfego de rede, analisando e bloqueando pacotes suspeitos antes que cheguem ao destino. Essa abordagem oferece máxima proteção, mas pode gerar impactos caso o IPS tenha um erro ou bloqueie tráfego legítimo.
- **Monitoramento Passivo (Passive Monitoring)**: O IPS recebe cópias do tráfego de rede sem interferir diretamente na comunicação. Isso é feito através de técnicas como **port mirroring (SPAN) ou network taps, que duplicam os pacotes e enviam uma cópia ao IPS para análise**. Esse método permite a identificação de ataques sem risco de impacto na rede, mas não bloqueia tráfego malicioso em tempo real.

A escolha entre IPS ativo ou passivo depende das necessidades da organização. O monitoramento ativo é ideal para redes que precisam de proteção imediata contra ameaças, enquanto o monitoramento passivo é mais indicado para ambientes onde a estabilidade da rede é prioritária e o foco está na **identificação e resposta rápida a incidentes**.

2.IPS de host (HIPS)

O IPS baseado em host é um software instalado em um host para monitorar e analisar atividades suspeitas. **Uma vantagem significativa do HIPS é de que ele pode monitorar e proteger o sistema operacional e os processos críticos do sistema que são específicos para esse host**. Com conhecimento detalhado do sistema operacional, o HIPS pode monitorar atividades anormais e impedir que o host execute comandos que não correspondem ao comportamento típico.

Esse comportamento suspeito ou mal-intencionado pode incluir atualizações de registro não autorizadas, alterações no diretório do sistema, execução de programas de instalação e atividades que causam estouros de buffer. O tráfego de rede também pode ser monitorado para impedir que o host participe de um ataque de negação de serviço (DoS) ou faça parte de uma sessão de FTP ilícita.

HIPS também podem ser pensados como uma combinação de software antivírus, antimalware e um firewall. **Porém, uma desvantagem do HIPS** é que ele opera apenas a nível local. Ele não tem uma visão completa da rede ou eventos coordenados que possam estar acontecendo em toda a rede. Para ser eficaz em uma rede, o HIPS deve ser instalado em cada host e ter suporte para cada sistema operacional.

3.IPS baseado em rede (NIPS)

Pode ser implementado usando um dispositivo IPS dedicado ou não dedicado. As implementações de IPS baseadas em rede são um componente crítico da prevenção de intrusões. As soluções IDS/IPS baseadas em host são integradas a uma implementação IPS baseada em rede para garantir uma arquitetura de segurança robusta

Os sensores detectam atividades maliciosas e não autorizadas em tempo real e podem agir quando necessário.

Os sensores IPS baseados em rede podem ser implementados de várias maneiras como, dispositivos Cisco Firepower, dispositivo de firewall ASA e roteador ISR. O hardware de todos os sensores baseados em rede inclui três componentes.

- **NIC:** O IPS baseado em rede deve poder conectar-se a toda rede, tal como Ethernet, Fast Ethernet e Gigabit Ethernet.
- **Processador:** A prevenção de intrusões requer poder de processamento para realizar análise de detecção de intrusão e correspondência de padrões
- **Memória:** A análise de detecção de intrusão é intensiva em memória. Essa memória afeta diretamente a capacidade de um IPS baseado em rede para detectar um ataque com eficiência e precisão.

Os sensores IDS/IPS **podem operar em modo in-line ou modo promíscuo**. **Os pacotes não fluem através do sensor no modo promíscuo.** O sensor analisa uma

cópia do tráfego monitorado, não do pacote real enviado. **A vantagem de operar no modo promíscuo** é que o sensor não afeta o fluxo do pacote com o tráfego encaminhado. A desvantagem de operar neste modo é que o sensor não pode impedir que o tráfego malicioso atinja seu alvo pretendido para certos tipos de ataques, como ataques atômicos.

As ações de resposta implementadas por dispositivos promíscuos são respostas pós-evento e muitas vezes exigem assistência de outros dispositivos de rede para responder a um ataque. Tais ações de resposta podem impedir algumas classes de ataques. Contudo, em ataques atômicos, o único pacote tem a possibilidade de alcançar o sistema de destino antes que o sensor promíscuo possa aplicar uma modificação ACL de um dispositivo controlado.

Operar em modo in-line coloca o IPS diretamente no fluxo de tráfego e torna as taxas de encaminhamento de pacotes mais lentas adicionando latência. Este modo permite que o sensor pare ataques, derrubando o tráfego malicioso antes de atingir o alvo pretendido, proporcionando assim um serviço de proteção. Além de processar informações nas camadas 3 e 4, ele analisa o conteúdo e a carga útil dos pacotes para ataques incorporados mais sofisticados (3 até 7). Essa análise mais profunda permite que o IPS identifique, pare e bloqueie os ataques que passariam por um dispositivo de firewall tradicional.

Um sensor IPS contém dois componentes:

- **Detecção IPS e mecanismo de aplicação:** Para validar o tráfego, o mecanismo de detecção compara o tráfego de entrada com assinaturas de ataque conhecidas que são incluídas no pacote de assinatura de ataque IPS.
- **Pacote de assinatura de ataque IPS:** Esta é uma lista de assinaturas de ataques conhecidos que estão contidas em um arquivo. O pacote de assinatura é atualizado com frequência à medida que novos ataques são descobertos.

Existem dois tipos de assinaturas baseadas em termos:

- **Conjunto de regras comunitárias:** Este conjunto oferece cobertura limitada contra ameaças, com foco em resposta reativa às ameaças de segurança versus trabalho proativo de pesquisa. Há 30 dias de acesso atrasado, as assinaturas atualizadas no conjunto de regras da comunidade, e esta assinatura não dá direito ao cliente ao suporte Cisco.
- **Conjunto de regras de assinantes:** Este conjunto oferece a melhor proteção contra ameaças. Ele inclui coberturas antes das explorações usando o trabalho de pesquisa dos especialistas em segurança Cisco Talos. O conjunto de regras de assinante também fornece o acesso mais rápido às assinaturas atualizadas em resposta a um incidente de segurança ou à descoberta proativa de uma nova ameaça. Esta assinatura é totalmente suportada pela Cisco.

Uma rede deve ser capaz de identificar o tráfego malicioso de entrada para pará-lo. Conceitualmente semelhante ao arquivo virus.dat usado por antivírus, uma assinatura é um conjunto de regras que um IDS e um PS usam para detectar atividades típicas de intrusão. As assinaturas identificam exclusivamente vírus, worms, anomalias de protocolo e tráfego malicioso específico.

Um fluxo de pacotes malicioso tem um tipo específico de atividade e assinatura. Os sensores IPS devem ser ajustados para procurar assinaturas correspondentes ou padrões de tráfego anormais. À medida que os sensores verificam pacotes de rede, eles usam assinaturas para detectar ataques conhecidos e responder com ações predefinidas. Um sensor IDS ou IPS examina o fluxo de dados usando muitas assinaturas diferentes. As assinaturas também têm três atributos distintos dos quais são os tipos, o gatilho e a ação.

Algumas ameaças podem ser identificadas em um pacote, enquanto outras ameaças podem exigir muitos pacotes e suas informações de estado para identificar uma ameaça. Existem dois tipos de assinaturas:

- **Assinaturas atômicas:** Este é o tipo mais simples de assinatura porque um único pacote, atividade ou evento identifica um ataque. O IPS não precisa manter informações de estado e análise de tráfego, geralmente pode ser realizado de forma muito rápida e eficiente.
- **Assinaturas compostos:** Também chamado de assinatura stateful porque o IPS requer várias partes de dados para corresponder a uma assinatura de ataque. O IPS também deve manter informações estatais, que é referido como o horizonte de eventos. O comprimento de um horizonte de eventos varia de uma assinatura para outra.

O alarme da assinatura para um sensor IPS pode ser qualquer coisa que possa sinalizar confiantemente uma violação da intrusão ou da política de segurança. Um IPS baseado em rede pode desencadear uma ação de assinatura se detectar um pacote com uma carga útil que contenha uma string específica que esteja indo a uma porta TCP específica.

Ele é análogo ao alarme em um sistema de segurança doméstica. O mecanismo de disparo para um alarme de assinatura pode ser um detector de movimento. Quando o alarme do assinante está ativado, o movimento de um indivíduo que entra em uma sala é detectado. Isso aciona o alarme.

Esses mecanismos desencadeadores podem ser aplicados a assinaturas atômicas e compostas. Os mecanismos de desencadeamento podem ser simples ou complexos. Cada IPS incorpora assinaturas que usam um ou mais desses mecanismos de disparo básicos para acionar ações de assinatura.