SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS: INTRUSION DETECTION SYSTEMS)

Temas abordados no texto

⚫Definição de IDS.
⚫diferenças entre IDS e firewall.
⚫tipos de IDS, em especial aqueles embasados em rede e em host.
⚫Principais técnicas de detecção de intrusos e suas limitações.

Os sistemas de detecção de intrusão (IDS) são de extrema relevância no quesito de segurança de rede ou de sistema. Eles monitoram a rede ou o sistema contra atividades mal-intencionadas e, caso sejam detectadas, o IDS dispara um alarme para o administrador da rede ou do host, para que o mesmo tome as devidas providências.

Em primeiro lugar, vale destacar que IDS e FIREWALL são distintos, ou seja, possuem funcionalidades distintas. Cabe ao IDS monitorar a rede ou o sistema contra atividades mal-intencionadas, agindo como um alarme que dispara caso alguma atividade mal-intencionada seja detectada, podendo ser uma violação de política, que posteriormente é relatada ao administrador. Diferentemente do IDS, o FIREWALL é um recurso voltado para impedir invasões no sistema ou na rede, ou seja, é um filtro de pacotes que gerencia origens e destinos aceitos e não aceitos.Contudo, a principal diferença entre o FIREWALL e o IDS é que o FIREWALL é para impedir invasões, enquanto o IDS é para sinalizar a invasão caso o FIREWALL não a impeça.

Ademais, existem IDS do tipo rede e de host, que são, respectivamente, sistemas de detecção de intrusão em redes (NIDS) e sistemas de detecção de intrusão em dispositivos conectados na rede (HIDS). Nesse contexto, o NIDS é um tipo de IDS que gerencia o monitoramento no quesito de redes, ou seja, oferece segurança dentro de uma rede. Por outro lado, o HIDS é um tipo de IDS específico para hosts, ou seja, oferece segurança para dispositivos conectados na rede.

Portanto, nesse contexto, vale ressaltar as principais técnicas de detecção de intrusão, como a detecção por assinatura, que se fundamenta em invasões anteriores que deixam sua assinatura. Porém, ela possui limitações, como a mudança para outros tipos não convencionais de invasão, que acabam comprometendo essa técnica de detecção. Existe também a técnica de detecção por anomalias, que se baseia em anomalias, ou seja, algo que foge do contexto. Porém, ela possui limitações, como o uso de máscaras convencionais na invasão para disfarçar anomalias, gerando assim uma grande limitação na detecção da invasão. Nesse sentido, geralmente é necessário usar uma combinação de abordagens para fornecer uma proteção abrangente.