Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Técnicas de Defesa
(Sistema de Detecção de Intrusão e HoneyNet)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

O IDS (Sistemas de Detecção de Intrusão) é uma ferramenta que analisa o comportamento da rede ou do sistema, em busca de tentativa de invasão.

De fato não há detecção de intrusão garantida, há apenas a identificação de evidências de intrusão, em andamento ou após o fato ter ocorrido. Para isso, ele monitora uma rede em busca de eventos que possam violar, ou violaram, as regras de segurança dessa rede.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Funcionamento

O IDS funciona **coletando** evidências dos sistemas, **analisando** padrões comportamentais, logs de auditoria, fluxo de dados, horários, dentre outros. **Armazenam** essas informações. Aliado ao conhecimento prévio de padrões de ataque, é possível discernir se o evento em questão é um evento malicioso ou não e **responder** às atividades suspeitas, por exemplo incluindo regras no firewall.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Funcionamento

Ele é baseado na hipótese de que o comportamento de um intruso não é o mesmo de um usuário legítimo. Por isso, o sistema tenta criar um padrão de comportamento de usuários em relação a programas, arquivos e dispositivos. Para isso, esses sistemas utilizam uma combinação de estatística e sistemas especialistas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Dificuldades

- Que informações coletar?
- Por quanto tempo?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Coleta de Dados

A coleta dos dados dos usuários é feita de variadas formas, desde mecanismos de entrada e saída, como mouse e teclado, a arquivos salvos em seus computadores; tabelas de regras, etc. Também é possível analisar a camadas dos protocolos TCP/IP e analisar o tipo de fluxo, pacotes que entram e saem, conexões estabelecidas, dentre outros.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ação

Uma vez detectada, o IDS executa então a ação que melhor corresponde àquela atividade maliciosa. Podendo apenas alertar ao administrador de rede, no caso de um IDS passivo, ou bloquear o fluxo de dados, no caso de um IDS ativo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Tipos de IDS

- IDS baseado em *Host*.
- IDS baseado em Rede.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IDS baseados em *Host* (HIDS)

Monitora e analisa informações coletadas de um único *Host* (Máquina). São instalados para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, sendo mais empregados nos casos em que a segurança está focada em informações contidas em um *host*.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IDS baseados em Host (HIDS)

Informações monitoradas

- Acesso a arquivos.
- Integridade de arquivos.
- Varredura de portas
- Modificação e privilégios de usuários.
- Processos do sistema.
- Execução de programas.
- Uso de CPU.
- Conexões.

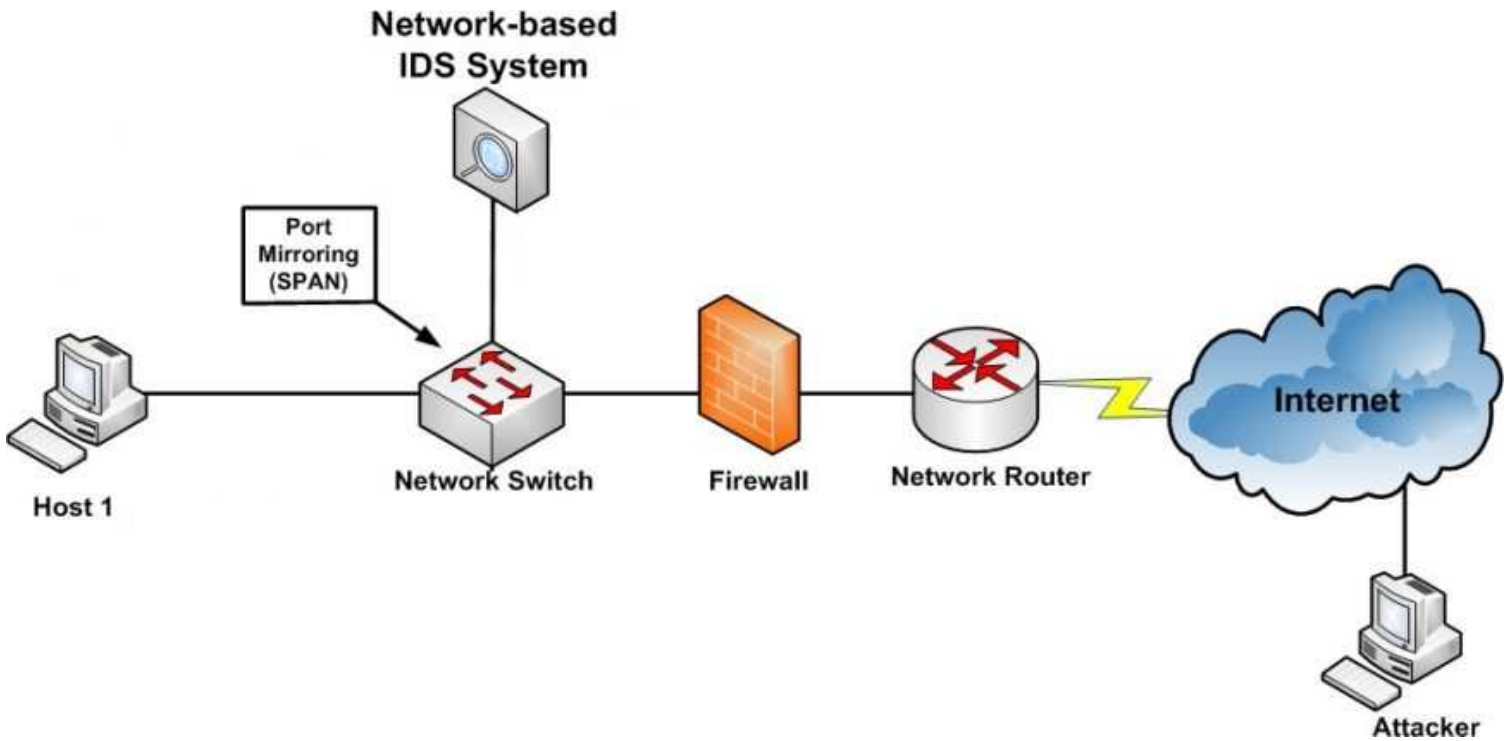
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IDS baseados em Rede (NIDS)

Monitora e analisa todo o tráfego no segmento da rede. Monitorando o conteúdo dos pacotes ou do tráfego e seus detalhes como informações de cabeçalhos e protocolos. Os NIDS tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legítimo está fazendo mau uso do mesmo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

IDS baseados em Rede (NIDS)



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

IDS baseados em Rede (NIDS)

Snort

O Snort é uma ferramenta gratuita de código aberto que atua como IDS via rede, combinando inspeções em protocolos e assinaturas e, ainda, podendo identificar o ataque através do comportamento anormal do tráfego da rede. Ele faz ainda a análise de tráfego em tempo real e registro dos pacotes. Ele pode ser utilizado em Windows, Linux, Solaris, MacOS, entre outros Sistemas Operacionais.

Ele executa análise de protocolo, busca e associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques, tais como buffer overflows, port scans, ataques CGI, SMB probes, OS fingerprinting, entre outras.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Formas de Detecção

Detecção por Assinatura

Analisa as atividades do sistema procurando por eventos que correspondam a padrões pré-definidos de ataques e outras atividades maliciosas. Estes padrões são conhecidos como assinaturas. Uma desvantagem desta técnica de detecção é que ela pode detectar somente ataques conhecidos, ou seja, que estão incluídos no conjunto de assinaturas que o IDS possui, necessitando-se assim de constante atualização diante da rapidez que novos ataques surgem.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Formas de Detecção

Detecção por Anomalias

IDS baseado em anomalias monta um perfil que representa o comportamento rotineiro de um usuário, Host e/ou conexão de rede. Estes IDS's monitoram a rede e usam várias métricas para determinar quando os dados monitorados estão fora do normal, ou seja, desviando do perfil.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Modelo de Ação

- Passivo: gera um alerta e envia para o administrador.
- Reativo: não só detecta o tráfego suspeito ou malicioso e alerta o administrador, como também possui ações pré-definidas para responder as ameaça. Normalmente, isso significa bloquear todo o tráfego do IP suspeito ou do usuário mal-intencionado.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

IDS e IPS

Existe o IDS e o IPS (Intrusion Prevention System). Enquanto o primeiro é um software que automatiza o processo de detecção de intrusão, o segundo faz a detecção e prevenção de intrusão, que tem por objetivo impedir possíveis ataques.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Honeypots

São recursos computacionais dedicados (rede) projetados para serem sondados, atacados ou comprometidos, num ambiente que permita o registro e controle dessas atividades. Análisando detalhes das ferramentas utilizadas, de suas motivações e das vulnerabilidades exploradas.

Funcionam como armadilhas para os crackers. Não contém dados ou informações importantes para a organização.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Aplicações

- Honeypots de Pesquisa: são ferramentas de pesquisa que podem ser utilizadas para observar o comportamento de invasores , permitindo análises detalhadas de suas motivações , das ferramentas utilizadas e vulnerabilidades exploradas;
- Honeypots de Produção: podem ser utilizados nas redes ativas como complemento de sistemas de detecção de intrusão.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Tipos

Em um honeypot pode ser instalados ferramentas para emular sistemas operacionais e serviços com os quais os atacantes irão interagir. Desta forma, o sistema operacional real deste tipo de honeypot deve ser instalado e configurado de modo seguro, para minimizar o risco de comprometimento. O honeyd é um exemplo de ferramenta utilizada para implementar honeypots com sistemas e serviços emulados.

Entretanto, podemos utilizar ainda sistemas operacionais, aplicações e serviços reais.

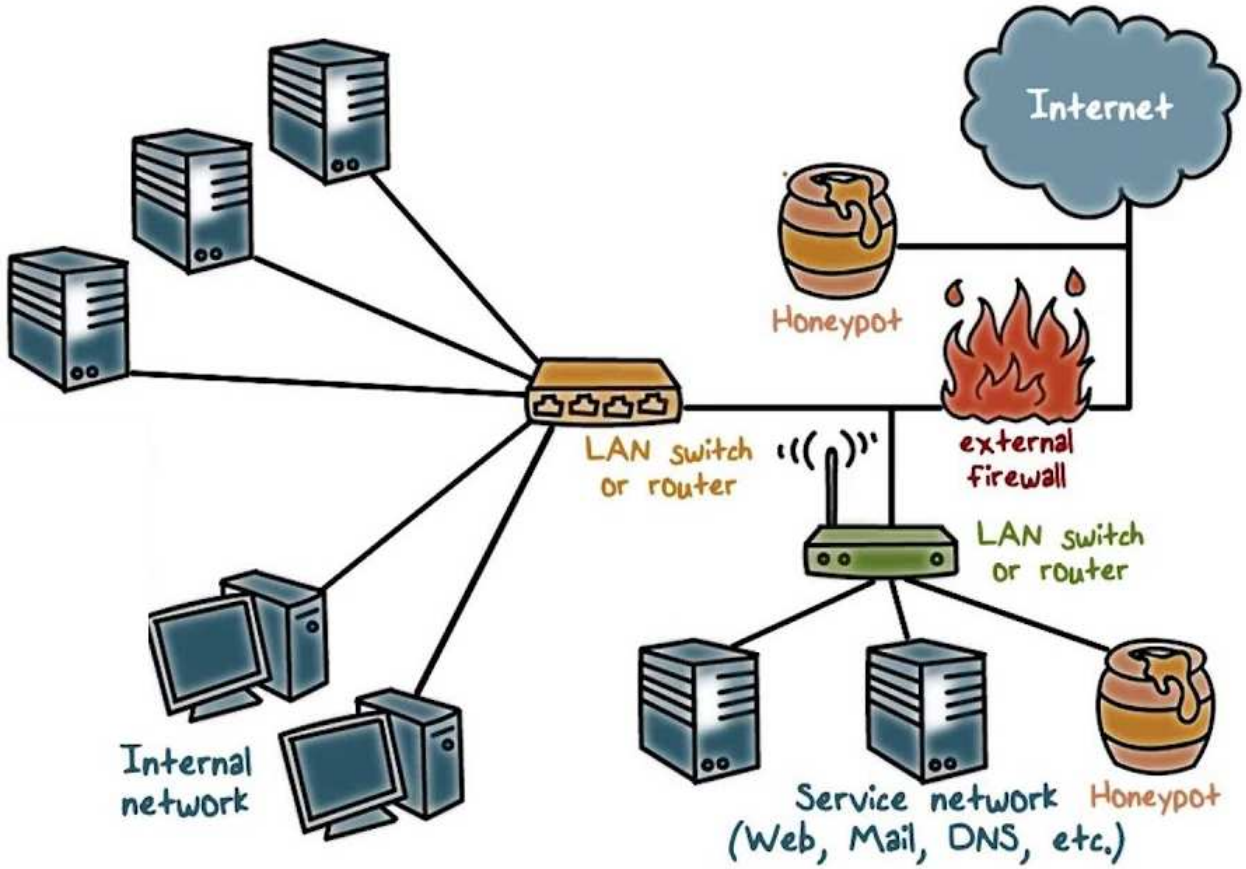
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

HoneyNet

Uma honeynet contém honeypots de diversos sistemas operacionais e que fornecem diversas aplicações e serviços. Também contém mecanismos de controle, além de sistemas para captura e coleta de dados, e para geração de alertas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

HoneyNet



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE