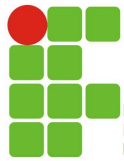
Segurança de Redes

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

Aula 09
Detecção e Prevenção de Intrusos



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

"Não é tanto o que fazemos, mas o motivo pelo qual fazemos que determina a bondade ou a malícia."
(Santo Agostinho)

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

O que Aprenderemos?

- Entender o que é um sistema de detecção de intruso (IDS);
- Compreender o seu funcionamento;
- Diferenciar os tipos de IDS;
- Conhecer alguns exemplos de IDS.

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

Sistemas de Detecção de Intrusos (IDS)

Exitem dois principais tipos de intrusos:

- Mascarado: indivíduo que não está autorizado a usar o computador e que penetra no sistema para explorar a conta de um usuário legítimo;
- Infrator: usuário legítimo que acessa dados, programas ou recursos para os quais não tem autorização;

Os intrusos visam, normalmente, ler dados privilegiados, realizar modificações não autorizada de dados ou interromper o sistema.

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

Sistemas de Detecção de Intrusos (IDS)

É uma ferramenta capaz de detectar diferenças no comportamento de usuários. Padrões de usuários legítimos podem ser estabelecidos observando-se o histórico, e um desvio significativo desses padrões poderá ser detectado. O IDS funciona coletando evidências, analisando padrões comportamentais, logs de auditoria, cabeçalhos de protocolos, fluxo de dados, horários, dentre outros. Estas informações são armazenadas. Aliado ao conhecimento prévio de padrões de ataque, é possível discernir se o evento em questão é de um intruso e, caso afirmativo, responder a invasão, por exemplo, deslogando o usuário.

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

Sistemas de Detecção de Intrusos (IDS)– Classificação

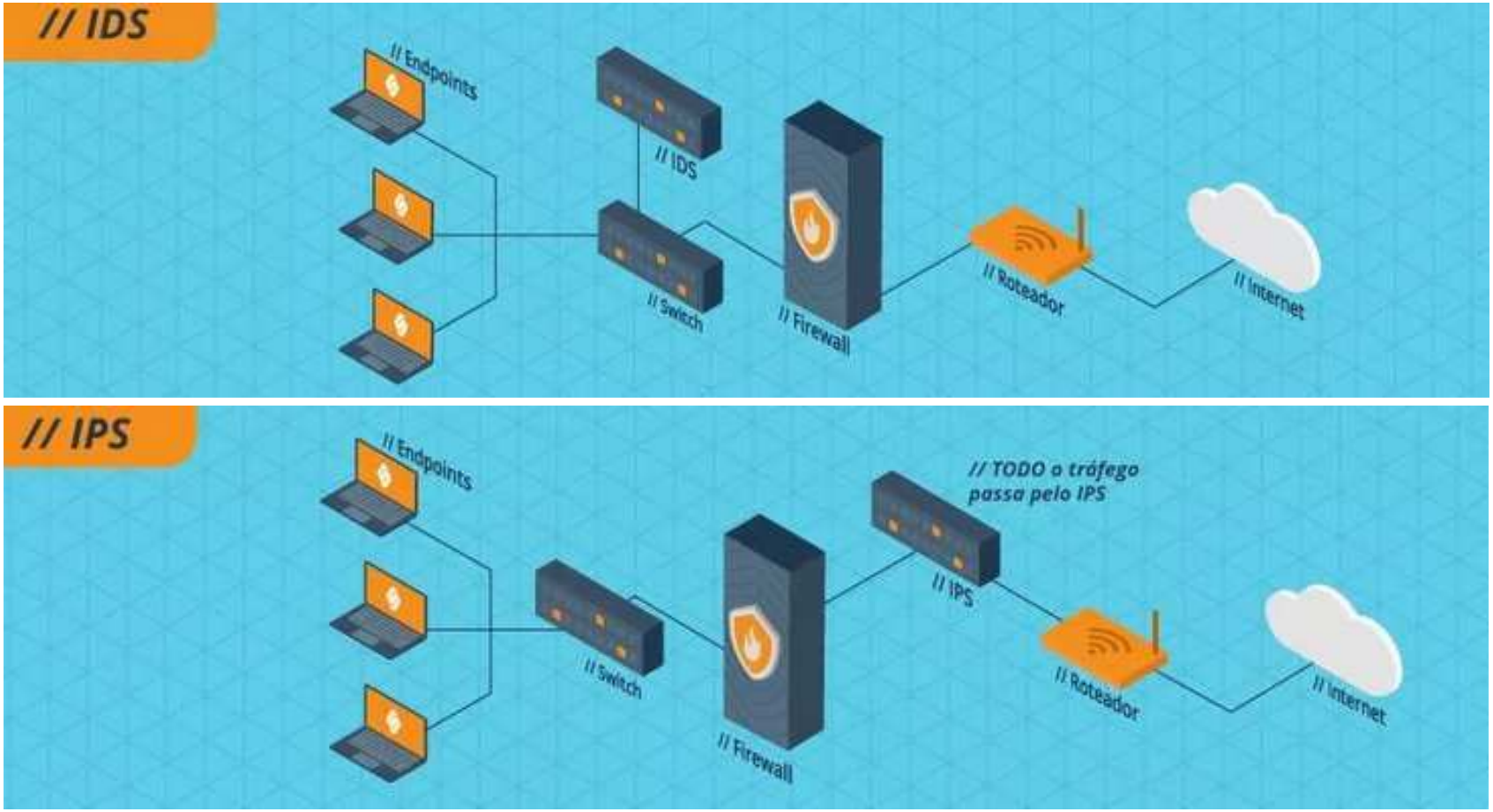
- Detecção estatísticas de anomalia: envolve a coleta de dados relacionado ao comportamento do usuário legítimo por um período de tempo. Depois, de construir o perfil do usuário, testes estatísticos são realizados para monitorar o comportamento do mesmo e detectar possível intruso;
- Detecção baseada em regras: define um conjunto de regras que podem ser usadas para decidir se determinado comportamento é o de um intruso. Por exemplo, apagar arquivos de auditoria, instalação de programas suspeitos, acesso a URLs e envio de endereços de correio eletrônico suspeitos, acessar em horário não comercial.

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

Sistemas de Detecção de Intrusos (IDS) – Classificação

- Reativos: agem após a ocorrencia de uma intrusão. Podem, por exemplo, inserir regras em um firewall visando encerrar uma conexão, realizar o logoff do usuário, desisnstalar os programas que o intruso instalalou e recuperar os arquivos apagados.
- Passivos: fazem apenas os registros dos eventos e realizam notificações para os administradores;
- Ativos: agem ativamente em caso de uma tentativa de intrução. Os sistemas ativos são chamados de **Sistemas de Prevenção de Intrusos** ou IPS. Eles tentam detectar e impedir que ocorra a intrusão. Podem, por exemplo, desabilitar um usuário e alterar as regras do firewall.

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



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

Sistemas de Detecção de Intrusos em Hosts (HIDS)

São exemplos de HIDS:

- OSSEC: provê análise de logs, verificação de integridade de arquivos, monitoramento de políticas, detecção de rootkits e alertas em tempo real, entre outros.
- SAMHAIN: provê verificação de integridade de arquivos, análise e monitoramento de arquivos de log.
- Osíris: realiza monitoramento de mudanças no sistema de arquivos, lista de usuários e grupos e módulos de kernel.

Muitos antivírus modernos incorporaram as funcionalidade de HIDS.

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

Sistemas de Detecção de Intrusos em Rede (NIDS) – Snort

O Snort é a principal ferramenta de NIDS no mercado. Ela é gratuita de código aberto, baseado em assinaturas. Ele faz análise de tráfego em tempo real, analiza protocolos, 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). Ele pode ser utilizado em Windows, Linux, Solaris, MacOS, entre outros Sistemas Operacionais. Com ele é possível a geração de alertas em arquivos de texto, alteração no firewall, executar comenandos, entre outros.

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

Dúvidas

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