SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS)

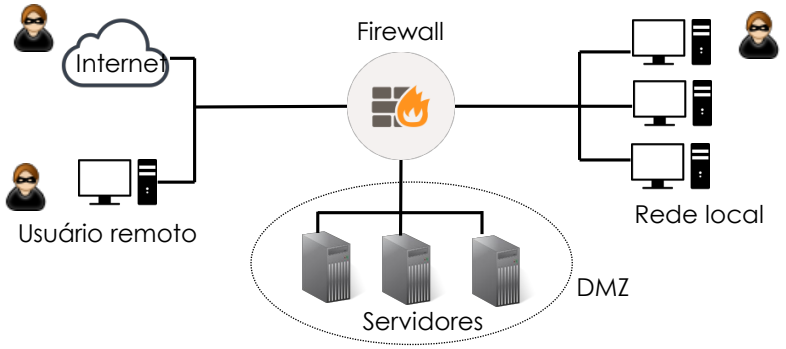
Roberto Sadao Yokoyama

UTFPR-CP

Outubro, 2016

PRINCIPAIS AMEAÇAS

- **IDS** -*Intrusion Detections System*



CLASSES DE INTRUSOS

- **Impostor**: Individuo não autorizado e que penetra no sistema para explorar uma conta de um usuário legítimo
- **Malfeitor**: usuário legítimo que acessa dados, programas ou recursos aos quais não tem acesso autorizado
- **Usuário clandestino**: indivíduo que se apodera do controle de supervisão e usa esse controle para escapar de auditorias e controle de acesso

EXEMPLOS DE INTRUSÃO

- Desfigurar um servidor Web
- Adivinhar senhas
- Copiar banco de dados que contém números de cartões de crédito
- Executar um software que captura pacotes em uma estação de trabalho para capturar login e senhas
- Usar um erro de permissão em um servidor Web para distribuir softwares e músicas piratas

DEFINIÇÕES

- **RFC 2828 define:**
  - **Intrusão de segurança:** Um evento de segurança ou uma combinação de vários eventos de segurança, que constitui um incidente de segurança no qual um intruso obtém acesso a um sistema (ou recurso de sistema) sem ter a devida autorização.
  - **Detecção de intrusão:** Um serviço de segurança que monitora e analisa eventos de sistemas com a finalidade de descobrir e avisar em tempo real ou quase em tempo real que estão ocorrendo tentativas de acesso a recursos de sistema de modo não autorizado.

EXEMPLOS DE PADRÕES DE COMPORTAMENTOS DE INTRUSOS

- **Hacker**:
  1. Seleciona o alvo usando ferramentas de consulta de endereço IP, como NSLookup
  2. Mapeia a rede em busca de serviços acessíveis, usando ferramentas como NMAP
  3. Identifica serviços potencialmente vulneráveis (nesse caso pcAnywhere)
  4. Adivinha (por força bruta) a senha do pcAnywhere
  5. Instala ferramenta de administração remota
  6. Espera que o administrador entre no sistema e captura a sua senha
  7. Usa essa senha para acessar o restante da rede

EXEMPLOS DE PADRÕES DE COMPORTAMENTOS DE INTRUSOS

- **Empresa criminosa**
  1. Age com rapidez e precisão para dificultar ainda mais a detecção de suas atividades
  2. Explora o perímetro por meio de portas vulneráveis
  3. Usa cavalos de troia para deixar portas abertas e retornar ao sistema
  4. Usa *sniffers* para capturar senhas
  5. Não fica atacando por muito tempo esperando para ser notado
  6. Comete poucos erros

EXEMPLOS DE PADRÕES DE COMPORTAMENTOS DE INTRUSOS

- **Ameaça Interna**
  - Cria contas na rede para si e para seus amigos
  - Acessa contas e aplicações que normalmente não usaria para seu trabalho diário
  - Envia e-mails a empregados antigos e possíveis empregadores
  - Conduz conversas clandestinas usando serviço de mensagens instantânea
  - Visita sites da Web que atendem empregados insatisfeitos
  - Executa grandes operações de download e de cópia de arquivos
  - Acessa a rede em horários fora do expediente normal

PRINCÍPIOS BÁSICOS

- Assume que o **comportamento dos intrusos são diferentes dos usuários legítimos** em modos que podem quantificados
- Sobreposições no comportamento pode causar problemas
  - Falso positivos
  - Falso negativos

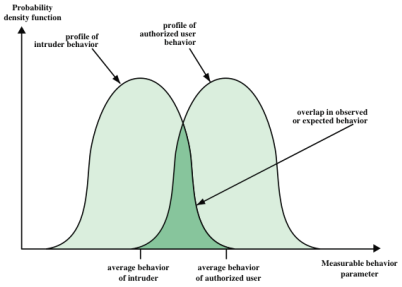


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

SISTEMA DE DETECÇÃO DE INTRUSÃO (IDS)

- Um IDS compreende três componentes lógicos:
  - **Sensores:** Os sensores são responsáveis pela coleta de dados. A entrada para um sensor pode ser qualquer parte de um sistema que pode conter evidência de intrusão.
  - **Analisadores:** Os analisadores recebem entradas de uma ou mais sensores de outros analisadores. O analisador é responsável por determinar se ocorreu uma intrusão.
  - **Interface de usuário:** A interface de usuário com um IDS habilita um usuário a ver a saída do sistema ou controlar o comportamento do sistema.

REQUISITOS DE IDS

- **Executar continuamente** com mínima supervisão humana
- Ser **tolerante a falhas** no sentido de ser capaz de se recuperar de quedas e reinicializações de sistema
- **Resistir à subversão**. O IDS deve ser capaz de monitorar a si mesmo e detectar se foi modificado por um atacante
- Impor um sobre **custo computacional mínimo** ao sistema no qual está executando
- Pode ser **configurado** de acordo com **as políticas de segurança** dos sistema que está sendo monitorado

REQUISITOS DE IDS

- Ser capaz de se **adaptar a mudanças no comportamento** do sistema e do usuário ao longo do tempo
- **Ser escalável**, de modo a poder monitorar grande número de estações
- Prover degradação elegante de serviço no sentido de que, se alguns **componentes do IDS parem** de funcionar por qualquer razão, o resto deles ser **afetado o mínimo possível**
- Permitir **reconfiguração dinâmica**, isto é, a capacidade de reconfigurar o IDS sem ter que reiniciá-lo

TIPOS DE IDS

- **HIDS** baseado em estação (host-based IDS)
  - Monitora os eventos de uma única estação em busca de atividade suspeita
- **NIDS** baseado em rede (network-based IDS)
  - Monitora tráfego de rede para segmentos ou dispositivos de rede específico e analisa protocolos de rede, transporte e aplicação para identificar atividade suspeita

ABORDAGENS DE ANÁLISE

- **Detecção de anomalia**
  - Envolve a coleta de dados relacionada ao comportamento de usuários legítimos durante um período de tempo.
  - Testes estatísticos são aplicados ao comportamento observado para determinar se esse comportamento não é o comportamento de um usuário legítimo
    - **Detecção limiar**: definir um limiar para a frequência de ocorrência de vários eventos
    - **Baseada em perfil**: um perfil da atividade de cada usuário é desenvolvido e usado para detectar mudanças no comportamento de conta individuais

ABORDAGENS DE ANÁLISE

- Sistemas baseados em perfil (métricas)
  - **Contador**: Conta certos eventos em um período
    - número de *logins*, número execução de comandos, senhas erradas
  - **Gabarito**: usado para medir o valor corrente de alguma entidade
    - Número de conexões lógicas de uma aplicação, número de mensagens de saída enfileiradas
  - **Cronômetro de intervalo**: duração do tempo entre dois eventos relacionados
    - Tempo transcorridos entre *logins* sucessivos
  - **Utilização de recursos**: recursos consumidos durante um período especificado
    - Tempo total consumido pela execução de um programa

ABORDAGENS DE ANÁLISE

- **Detecção de assinatura**
  - Envolve a tentativa de definir um conjunto de regras ou padrões de ataque que podem ser usados para decidir se dado comportamento é o de um intruso.
  - Identifica somente ataques que padrões e regras são conhecidos.
- Na prática, um sistema pode empregar uma combinação de ambas as abordagens para ser efetivo contra grande gama de ataques.

REGISTROS DE AUDITORIA

- **Registros de auditoria nativos:** Sistemas operacionais multiusuário incluem software de contabilidade que coleta informações sobre a atividade de usuários.

- **Registros de auditoria específicos de detecção:** pode-se implementar um recurso de coleta que gera registros de auditoria que contêm somente as informações exigidas pelo IDS.

EXEMPLO DE REGISTRO DE AUDITORIA

- **Sujeito**: tipicamente um usuário final
- **Ação**: ação executada pelo sujeito sobre um objeto (acessar, ler, etc)
- **Objetos**: receptores da ação (arquivos, programas, mensagens, registros, etc)
- **Condição de exceção**: denota qual condição de exceção, se houver alguma, é lançada com resultado da ação
- **Utilização de recurso**: lista de elementos quantitativos (tempo de processamento, tempo decorrido de cada sessão)
- **Carimbo de tempo**: tempo e data que identificam quando a ação ocorreu

TESTES

- **Média e desvio padrão:** retrata o comportamento médio e de sua variabilidade
- **Multivariado**: é a correlação entre duas métricas
  - Tempo de processamento e frequência de login
- **Processo de Markov**: probabilidade de transição entre estados
  - Examinar transições entre certos comandos
- **Série temporal:** se concentra em intervalos de tempo, procurando sequências de eventos
- **Modelo operacional:** é baseado no julgamento do que é considerado anormal
  - Grande número de tentativas de *login* durante curto período de tempo

TIPOS DE IDS

- IDS baseado em estação (host-based IDS)
  - Monitora os eventos de uma única estação em busca de atividade suspeita

- **IDS baseado em rede (network-based IDS)**
  - Monitora tráfego de rede para segmentos ou dispositivos de rede específico e analisa protocolos de rede, transporte e aplicação para identificar atividade suspeita

IDS BASEADO EM REDE

- *Network-based IDS* (NIDS) monitora o tráfego em ponto selecionados da rede ou em um conjunto de redes interconectada
  - Examina pacote por pacote
  - Tempo real
  - Protocolos nível da rede, transporte e/ou aplicação
- Sensores para monitorar pacotes
  - Inline
  - Passivos
- Análise de padrões de tráfego para detectar intrusão

NIDS

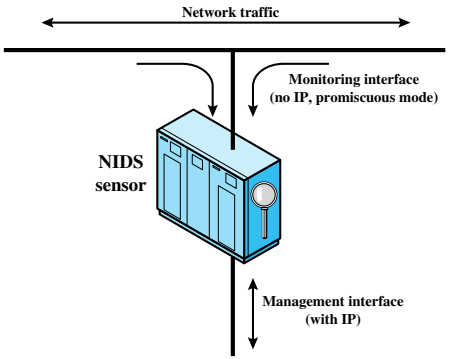


Figure 8.4 Passive NIDS Sensor

DISPONIBILIZAÇÃO DE SENSOR NIDS

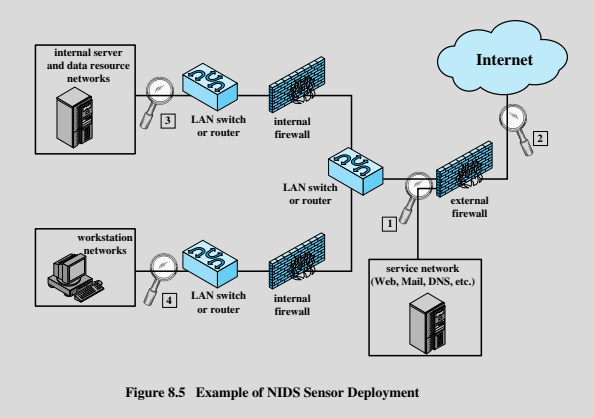


Figure 8.5 Example of NIDS Sensor Deployment

Localização (1):
- Enxerga ataques externos que penetram no firewall
- Enxerga ataques que visam servidores web e FTP
- Reconhece tráfego de saída de algum host comprometido

Localização (2):
- Documenta ataques originários da internet
- Documenta tipos de ataques originários da internet

Localização (3):
- Monitora grande quantidade de tráfego
- Detecta atividade não autorizada dentro do perímetro de segurança

Localização (4):
- Detectam ataques que visam sistemas e recursos críticos
- Pode ser sintonizado para protocolos específicos

ABORDAGENS DE ANÁLISE

- **Detecção de anomalia**:
  - **Ataques de negação de serviço** (DoS): Esses ataques envolvem aumento significativo de tráfego de pacotes ou aumento significativo de tentativa de conexão
  - **Escaneamento**: O atacante sonda a rede ou sistema enviando diferentes tipos de pacotes. Usando as respostas recebidas do alvo, o atacante pode aprender muitas características e vulnerabilidades do sistema
  - **Vermes**: Vermes que se espalham entre as estações podem ser detectados de mais de um modo.
    - Para se propagar rapidamente usam grande quantidade de largura de banda
    - Comunicam com outras máquinas com as quais normalmente não se comunicam
    - Estações usam portas que normalmente não usam

ABORDAGENS DE ANÁLISE

- **Detecção de assinatura**:
  - Camada de aplicação
    - DHCP, DNS, FTP, HTTP, IMAP, NFS, POP, RPC, SIP, SMB etc.
    - Protocolos de banco de dados, mensagens instantâneas e peer-to-peer
    - Ataques: estouro de capacidade de buffer, adivinhação de senha e transmissão de *malware*
  - Camada de transporte
    - TCP e UDP
    - Ataques: escaneamento de portas vulneráveis e ataques específicos aso TCP, como inundação de SYN
  - Camada de rede
    - IPv4, ICMP e IGMP
    - Ataques: Endereços IP falsificados e valores de cabeçalhos IP ilegais

REGISTROS DE ALERTAS

- Carimbo do tempo;
- ID de conexão ou sessão (tipicamente um número designado a cada conexão TCP)
- Tipo de evento ou alerta
- Classificação (p. ex. prioridade, gravidade, impacto)
- Protocolos de camada de rede, transporte e aplicação

REGISTROS DE ALERTAS

- Endereços IP de origem e destino
- Portas TCP ou UDP de origem e destino
- Número de bytes transmitidos pela conexão
- Dados de carga útil decodificados, como requisições e respostas de aplicações
- Informações relacionadas a estado (p. ex. nome do usuário)

HOST-BASED IDS (HIDS)

- Vantagens
  - Pode verificar o sucesso ou falha de um ataque utilizando *logs* do sistema;
  - Monitora atividades específicas;
  - Ataques que ocorrem fisicamente no servidor;
  - Independente da topologia da rede;
  - Não necessita de *hardware* adicional.

HOST-BASED IDS (HIDS)

- Desvantagens
  - Problema de escalabilidade;
  - Depende do SO;
  - Não é capaz de detectar ataques na rede, somente local;
  - Se HIDS for invadido, as informações podem ser perdidas;
  - Precisa de espaço adicional de armazenamento;
  - Reduz o desempenho do *host* monitorado.

NETWORK-BASED IDS (NIDS)

- Vantagens
  - Monitoramento de múltiplas plataformas;
  - Detecta ataques a rede, como: *port scanning*, IP *spoofing;*
  - Monitora portas conhecidas ou permitidas;
  - Detecta e identifica ataques em tempo real;
  - Detecta tentativas de ataques;
  - É difícil o atacante saber se existe IDS na rede;
  - É difícil para atacante apagar seus rastros;
  - Não causa impacto no desempenho;

NETWORK-BASED IDS (NIDS)

- Desvantagens
  - Não funciona bem em redes alta taxa de perdas de pacotes elevada;
  - Dificuldade de análise protocolos específicos;
  - Não monitora tráfego cifrado;
  - Dificuldade de utilização em redes segmentadas;
  - Armazena e processa uma grande quantidade de dados.

IDS HÍBRIDO

- O NIDS e o HIDS monitoram o tráfego de rede e o host, respectivamente.
- No entanto, eles podem se complementar. Os IDS híbridos utilizam e dados da rede e dos host monitorados. Monitorando atividades de diversas fontes.
- São difíceis de gerenciar e implantar

DETECÇÃO DE INTRUSÃO ADAPTATIVA DISTRIBUÍDA

- Até aqui: HIDS e NIDS
- Problemas:
  - Novas ameaças
  - Atualização do esquema para ataques que se disseminam velozmente ou muito lentamente
  - Defesa do perímetro (como firewall) , estações sem fio entram e saem da rede
- Sistemas cooperativos podem reconhecer ataques com base em sinais mais sutis e adaptar-se mais rapidamente

DETECÇÃO DE INTRUSÃO ADAPTATIVA DISTRIBUÍDA

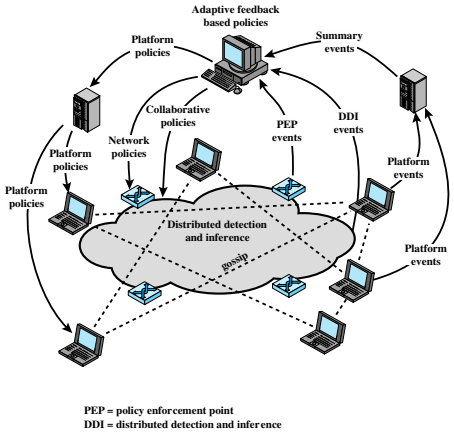


Figure 8.6 Overall Architecture of an Autonomic Enterprise Security System

- Utilização de vários IDS que compartilha informações é capaz de prover maior cobertura
- Análise de tráfego nas estações, onde há menos tráfego, os ataques se destacam mais
- DDI: são alertas gerados quando um ataque está em curso
- PEP: correlacionam informações para detectar intrusões que não estão evidentes no nível da estação

SISTEMA DE PREVENÇÃO DE INTRUSÃO (IPS)

- IPS é um IDS baseado em rede (NIDS) inline que tem a capacidade de bloquear tráfego por meio do descarte de pacotes.
  - Envia comandos ao firewall ou roteador para bloquear o tráfego
- Um IPS é uma adição funcional a um firewall que acrescentou tipos de algoritmos de IDS ao reportório do firewall
- IPS: HIPS (host based) e NIPS (network based)

HONEYPOTS

- "**Potes de mel**": são sistemas chamarizes projetados para atrair um atacante potencial e afastá-lo de sistemas críticos.
- Objetivos:
  - Desviar um atacante do acesso a sistema crítico
  - Coletar informações sobre a atividade do atacante
  - Incentivar o atacante a ficar no sistema por tempo suficiente para que os administradores respondam
- Honeypots estão repletos de informações falsas projetadas para parecerem valiosas, mas que um usuário legítimo do sistema não acessaria.

HONEYPOTS

- O sistema é instrumentado com **monitores** e **registradores** de eventos que coletam informações sobre a atividade do atacante
- Todos os **ataques ao honeypot são bem-sucedidos** para que os administradores possam rastrear os atacantes
- Não há uma razão legítima para alguém de fora interagir com o honeypot, portanto **qualquer tentativa de comunicação é provavelmente um ataque**
- Qualquer **comunicação do honeypot com o ambiente externo** é porque o sistema foi provavelmente comprometido

HONEYPOTS

- **Honeynets**: é uma rede inteira de honeypots que emulam uma rede empresarial. Assim, administradores podem observar o comportamento do hacker e projetar defesas
- Honeypots podem ser disponibilizados em uma variedade de localizações
  - Informação que a organização está interessada em coletar
  - Nível de risco que as organizações podem tolerar para se obter a máxima quantidade de dados

HONEYPOTS

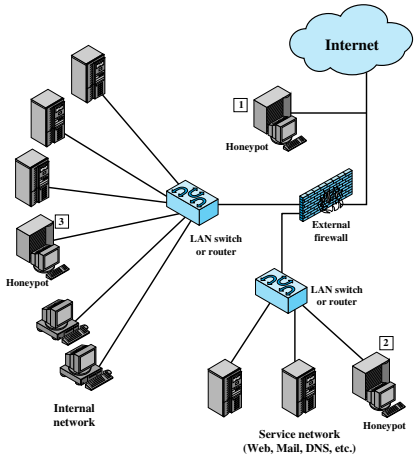


Figure 8.8 Example of Honeypot Deployment

Localização (1):

- Rastrear tentativas de conexão a endereços IP não utilizados dentro do escopo da rede
- Atrai muitos ataques, reduzindo alertas de firewall e IDS internos
- Não captura ataques internos

Localização (2):

- Rastreia tentativas a serviços disponíveis externamente (web e correios)
- Administrador deve garantir que outros sistemas estejam seguros contra qualquer atividade gerada pelo honeypot

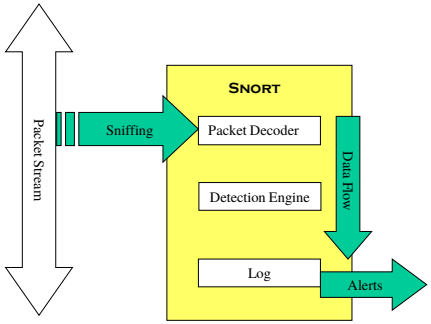
Localização (3):

- Captura ataques internos e detecta problemas no firewall
- Se o honeypot for comprometido, pode ser usado para atacar outros sistemas internos, porque qualquer tráfego até o honeypot não será bloqueado pelo firewall.

SNORT

- Snort é um IDS baseado em **estação ou em rede**.
  - É fácil disponibilizar na maioria dos nós (estação, servidor, roteador) de uma rede
  - Operação eficiente que usa **pouca memória e tempo de processador**
  - É fácil de configurar por administradores de sistema
- Snort pode executar **captura de pacotes, análise de protocolos e busca e verificação de conteúdo** em tempo real
- Pode **detectar uma variedade de ataques** usando regras configuradas por um administrador do sistema

SNORT



- Arquitetura Snort
  - **Decodificador**: isola os protocolos da camada de enlace, rede, transporte e aplicação
  - **Detecção**: analisa cada pacote tendo como base um conjunto de regras
  - **Registrador**: para cada pacote que corresponder à regra, é armazenado uma informação que pode ser lido por seres humanos
  - **Alerta**: Para cada pacote detectado, um alerta pode ser enviado.

REGRAS SNORT

- Snort usa uma linguagem de definição de regras. Cada regra consiste em um cabeçalho fixo e zero ou mais opções.

Action	Protocol	Source IP address	Source Port	Direction	Dest IP address	Dest Port

(a) Rule Header

Option Keyword	Option Arguments	• • •

(b) Options

REGRAS SNORT

- **Ação**: o que fazer quando encontrar o pacote que está de acordo com a regra
- **Protocolo**: continua a analise se o protocolo do pacote corresponder a esse campo
- **IP de origem**: designa a origem do pacote
- **Porta de origem**: porta de origem para o protocolo designado
- **Direção**: unidirecional (->) ou bidirecional (<->)
- **IP destino**: designa o destino do pacote
- **Porta destino**: designa a porta de destino

REGRAS SNORT

- Opções:
  - **Metadados**: fornece informações sobre a regra
  - **Carga útil**: procura dados dentro da carga útil do pacote
  - **Não carga útil**: Procura dados em locais diferentes da carga útil
  - **Pós-detecção**: acionadores específicos de regras que ocorrem depois de detectada a correspondência entre um pacote e uma regra.