Sistemas de Detecção de Intrusão (IDS)

Motivação

Motivação para IDS

- Ataques irão, eventualmente, ocorrer!
- Ataques permitirão a atacantes ganhar acesso não-autorizado a recursos
- Boa estratégia "prevenir" alguns ataques e "detectar" outros
- Sistemas de Detecção de Intrusão (IDS - Intrusion Detection Systems) buscam detectar ataques
- Monitorar e analizar sistemas para avisar sobre intrusões
- Resposta a um ataque detectado pode ser técnica ou legal

Tipos de Intruso (classificação do livro)

- Masquerader / Impostor (outsider)
  - Alguém não-autorizado a usar um sistema penetra o sistema decontrole de acesso fazendo-se passar por usuário legítimo
- Misfeasor / Malfeitor (insider)
  - Usuário legítimo que acesso recursos aos quais nãodeveria ter acesso
- Clandestine / Usuário Clandestino (outside/insider)
  - Usuário toma controle dos sistemas de asministração de controle de acesso e evade mecanismos de detecção

Exemplos de Intrusão

- Root/admin remoto – comprometimento de servidor
- Deface de servidor web
- Advinhação de senhas
- Cópia/extrusão de bases de dados com informações confidenciais
- Visualização de dados sensíveis
- Captura de pacotes de redes para obter usernames e senhas
- Uso de sistemas para distribuir conteúdo ilegal/inapropriado
- Fazer-se passar por outrem (e.g., help-desk) para obter informações sensíveis (como senhas)
- Uso de contas logadas sem conhecimento/permissão

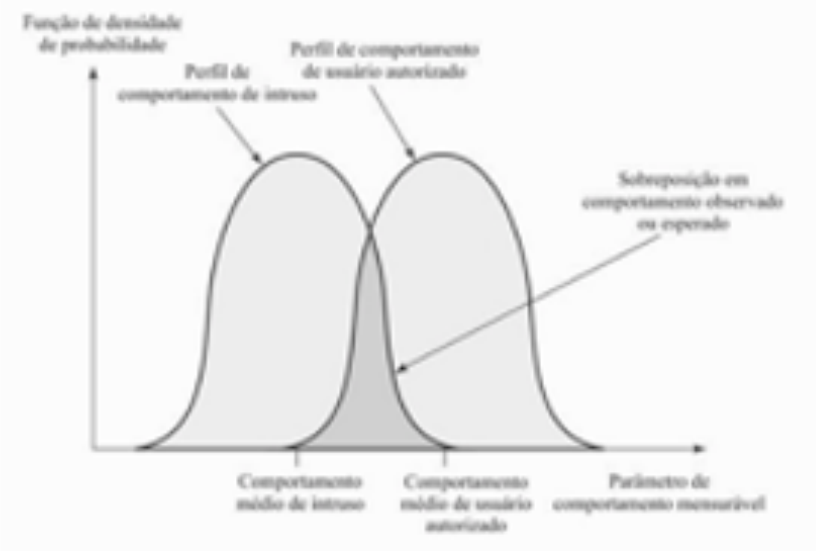
Sistema de Detecção de Intrusão

Sistema de Detecção de Intrusão

- dispositivo ou aplicativo de software que monitora uma rede ou sistemas quanto a atividades mal-intencionadas ou violações de políticas
- Qualquer atividade ou violação maliciosa é normalmente relatada a um administrador ou coletada centralmente
- Tipos de IDS variam de escopo de computadores individuais a grandes redes

Hipótese da diferença de comportamento

› Assume intruder behaviour is dierent from that of legitimate users

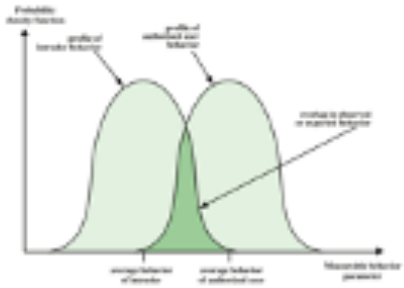


› False positives: legitimate user identied as intruc

› False negative: intruder not identied

IDS Principles

Assume intruder behaviour is different from that of legitimate users



Credit: Figure 8.1 in Stallings and Brown, Computer Security, 2nd Ed., Pearson 2012

False positives: legitimate user identified as intruder
False negative: intruder not identified

Recursos e aplicações de IDS

- Monitoramento e análise da atividade do usuário e do sistema
- Auditoria de configurações e vulnerabilidades do sistema
- Avaliando a integridade de arquivos críticos de sistema e dados
- Análise estatística de padrões de atividade com base na correspondência com ataques conhecidos
- Análise de atividade anormal
- Auditoria do sistema operacional

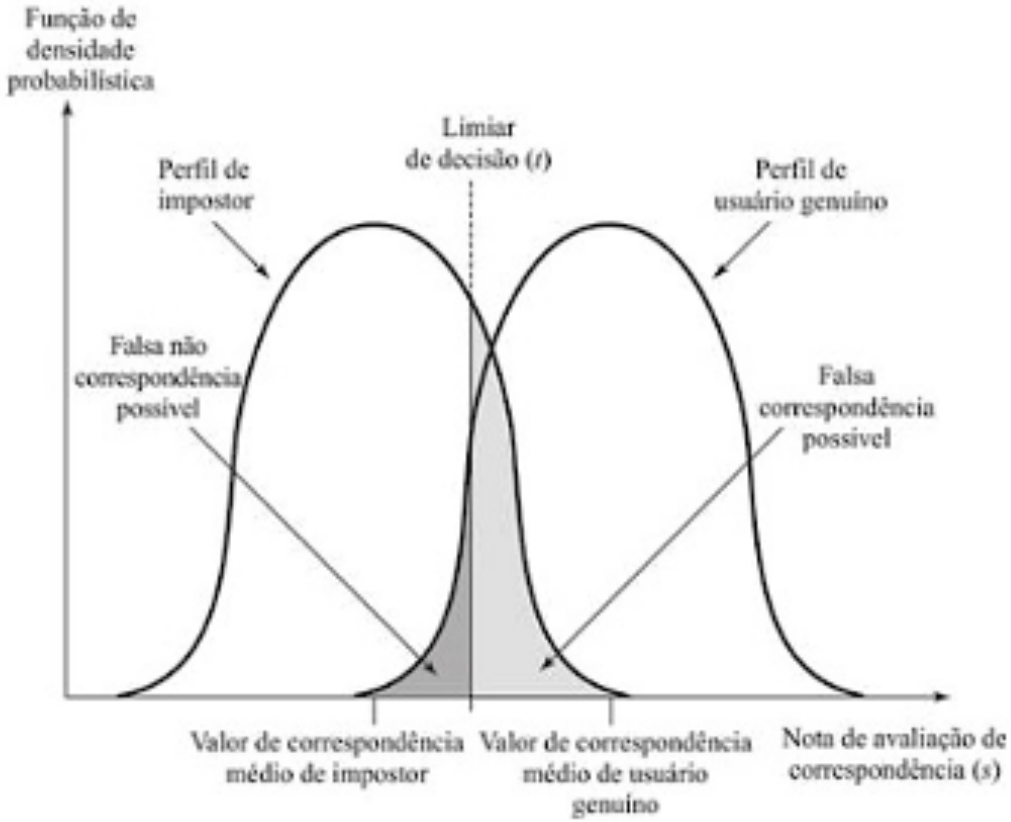
Classificação de IDS

- Posicionamento: HIDS versus DIDS versus NIDS
  - HIDS: baseado em host – analisa dados e sistema local
  - DIDS: host distribuído – analisa dados de vários hosts
  - NIDS: baseado em rede – analisa tráfego de rede
- Abordagem de detecção: assinatura versus anomalia
  - Baseado em assinatura: reconhece padrões de intrusão, exemplo, presença de malware, por meio de assinaturas
  - Baseado em anomalia: modela o "bom comportamento" e detecta desvios a esse modelo de comportamento
- Capacidade de resposta: o conceito de IPS

Falsos positivos e falsos negativos

- Como todo sistema destinado à detecção de ameaças, erros podem ser cometidos
  - Falso positivo: evento identificado como intrusão é, na verdade, um evento legítimo
  - Falso negativo: evento de intrusão não é identificado pelo sistema
- Métodos baseado em assinatura tendem a ter poucos falsos positivos
  - mas deixam escapar novos ataques (falsos negativos)
- Métodos baseado em anomalia tem maior capacidade de identificar novos ataques (menos falsos negativos)
  - mas pagam o preço de identificar ataques erroneamente (falsos positivos)
  - ainda assim, podemos ajustar o threshold

Falsos positivos, falsos negativos e o limiar de decisão



Requisitos de IDSs

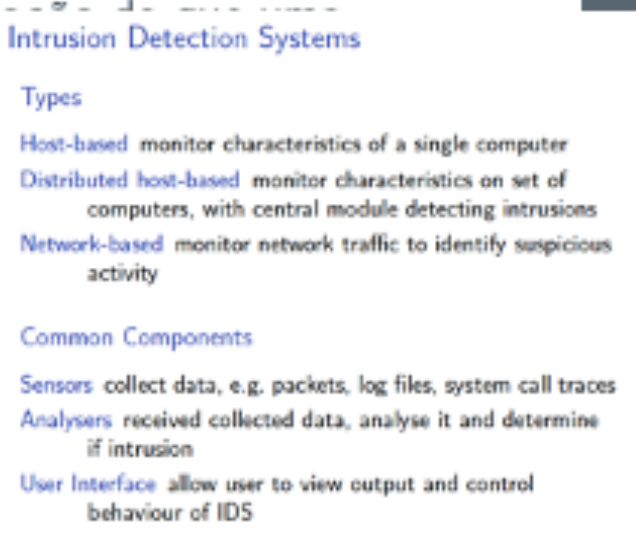
- Executar continuamente com mínima supervisão humana.
- Ser tolerante a falhas no sentido de ser capaz de se recuperar de quedas e reinicializações de sistema
- Resistir à subversão. O IDS deve ser capaz de monitorar a si mesmo e detectar se foi modificado por um atacante.
- Impor um sobrecusto computacional mínimo ao sistema no qual está executando.
- Poder ser configurado de acordo com as políticas de segurança do sistema que está sendo monitorado
- 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 pararem de funcionar por qualquer razão, o resto deles deve ser afetado o mínimo possível.
- Permitir
é, a cap
sem ter

IDS Requirements

- Run continually with minimal human supervision
- Recover from system restart/crashes
- Monitor itself and detect attacks on itself
- Impose minimal overhead on system
- Configurable according to system security policies
- Adapt to system and user behaviour changes over time
- Scale to monitor large number of hosts
- Still (partially) work if some components stop working

Componentes Lógicos do IDS

- 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. Tipos de entrada para um sensor incluem pacotes de rede, arquivos de registro e conjuntos de eventos de chamadas do sistema. Os sensores coletam e transmitem essas informações ao analisador.
- Analisadores
  - Os analisadores recebem entradas de um ou mais sensores ou de outros analisadores. O analisador é responsável por determinar se ocorreu uma intrusão. A saída produzida por esse componente é indic
    intrusão ocorreu e pode incluir evidências que suportam
    uma intrusão ocorreu. O analisador pode dar orientaçãc
    a tomar como resultado da intrusão.
- Interface de usuário
  - A interface de usuário com um IDS habilita um usuário a
    ou controlar o comportamento do sistema. Em alguns si
    usuário pode corresponder a um componente de gerenci
    console.



Evasão

- Intruso busca ”parecer” com usuário legítimo
  - Aumenta taxa de falsos negativos
  - Ajustar o threshold leva a aumento de falsos positivos
- Exemplos de técnicas
  - Fragmentação de pacotes
  - Mudança de valores default
  - Ataques coordenados de baixa vazão
  - Spoofing de enredeço
  - Uso de proxies
  - Modificação de payloads ”padrão”

Sistemas de Detecção de Intrusão

Conteúdo do Capítulo 8 do livro

Objetivos

- Distinguir entre vários tipos de padrões de comportamento de intrusos.
- Entender os princípios básicos de detecção de intrusão e seus requisitos.
- Discutir os aspectos fundamentais de detecção de intrusão baseada em estação.
- Explicar o conceito de detecção de intrusão distribuída baseada em estação.
- Discutir os aspectos fundamentais da detecção de intrusão baseada em rede.
- Definir o formato de troca de dados de detecção de intrusão.
- Explicar a finalidade de honeypots (potes de mel).
- Apresentar uma visão geral do Snort

Tipos de Intrusos

- Impostor (atacante externo)
  - "Um indivíduo que não está autorizado a usar o computador e que penetra no sistema burlando seu controle de acesso para explorar a conta de um usuário legítimo."
- Malfeitor (atacante interno)
  - "Um usuário legítimo que acessa dados, programas ou recursos aos quais não tem acesso autorizado ou aos quais tem acesso autorizado, mas usa de forma maliciosa seus privilégios."
- Usuário clandestino (?)
  - "Um indivíduo que se apodera do controle de supervisão do sistema e usa esse controle para escapar de auditorias e controles de acesso ou para suprimir a coleta de dados de auditoria."

Tipos (impactos) de Ataques

- ”Benignos” (como o tumor...)
  - Acesso a sistemas sem ações que comprometam a segurança dos dados e integridade dos sistemas
- Graves
  - Comprometimento grave da segurança dos dados e integridade dos sistemas
- E cinquenta tons de cinza entre esses dois extremos...

Exemplos de intrusão

- Executar um comprometimento remoto da conta raiz de um servidor de e-mail.
- Desfigurar um servidor Web.
- Adivinhar e quebrar senhas.
- Copiar um banco de dados que contém números de cartões de crédito.
- Visualizar dados sensíveis, incluindo registros de folhas de pagamento e informações médicas, sem autorização.
- Usar uma estação de trabalho ligada não supervisionada, sem permissão
- Executar um software de captura de pacotes em uma estação de trabalho para capturar nomes de usuários e senhas.
- Usar um erro de permissão em servidor FTP anônimo para distribuir software e arquivos de música pirateados.
- Discar para um modem não seguro e obter acesso à rede interna.
- Fazer-se passar por um executivo, chamar o serviço de suporte, mudar a senha de e-mail do executivo e descobrir a nova senha.

Padrões de comportamento de intrusos

- Intrusos tentem a seguir ”padrões de comportamento”
  - De acordo com técnicas e objetivos do ataque
  - Variam também conforme tipo de atacante
- Atacante externo
  - Reconhecimento em redes abertas, dentificação de alvos vivos, mapeamento de topologia,...
- Atacante interno
  - Realização de scan em redes internas, criação de contas, acesso a rede corporativa fora do expediente

Detecção de intrusão

- *Um evento de segurança ou uma combinação de vários eventos de segurança, que constitui um incidente de segurança no qual um intruso obtém ou tenta obter acesso a um sistema (ou recurso de sistema) sem ter a devida autorização.*

RFC2828

Classificação de IDS

- Host-based IDS (baseado em estação)
  - Monitora as características de uma única estação e os eventos que ocorrem dentro dessa estação em busca de atividade suspeita.
- Network-based IDS (baseado em rede)
  - Monitora tráfego de rede para segmentos ou dispositivos de rede específicos e analisa protocolos de rede, transporte e aplicação para identificar atividades suspeitas

Componentes Lógicos do IDS

- 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. Tipos de entrada para um sensor incluem pacotes de rede, arquivos de registro e conjuntos de eventos de chamadas do sistema. Os sensores coletam e transmitem essas informações ao analisador.
- Analisadores
  - Os analisadores recebem entradas de um ou mais sensores ou de outros analisadores. O analisador é responsável por determinar se ocorreu uma intrusão. A saída produzida por esse componente é indicação de que uma intrusão ocorreu e pode incluir evidências que suportam a conclusão de que uma intrusão ocorreu. O analisador pode dar orientação quanto às providências a tomar como resultado da 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. Em alguns sistemas, a interface de usuário pode corresponder a um componente de gerenciamento, direção ou console.

Motivação para IDS

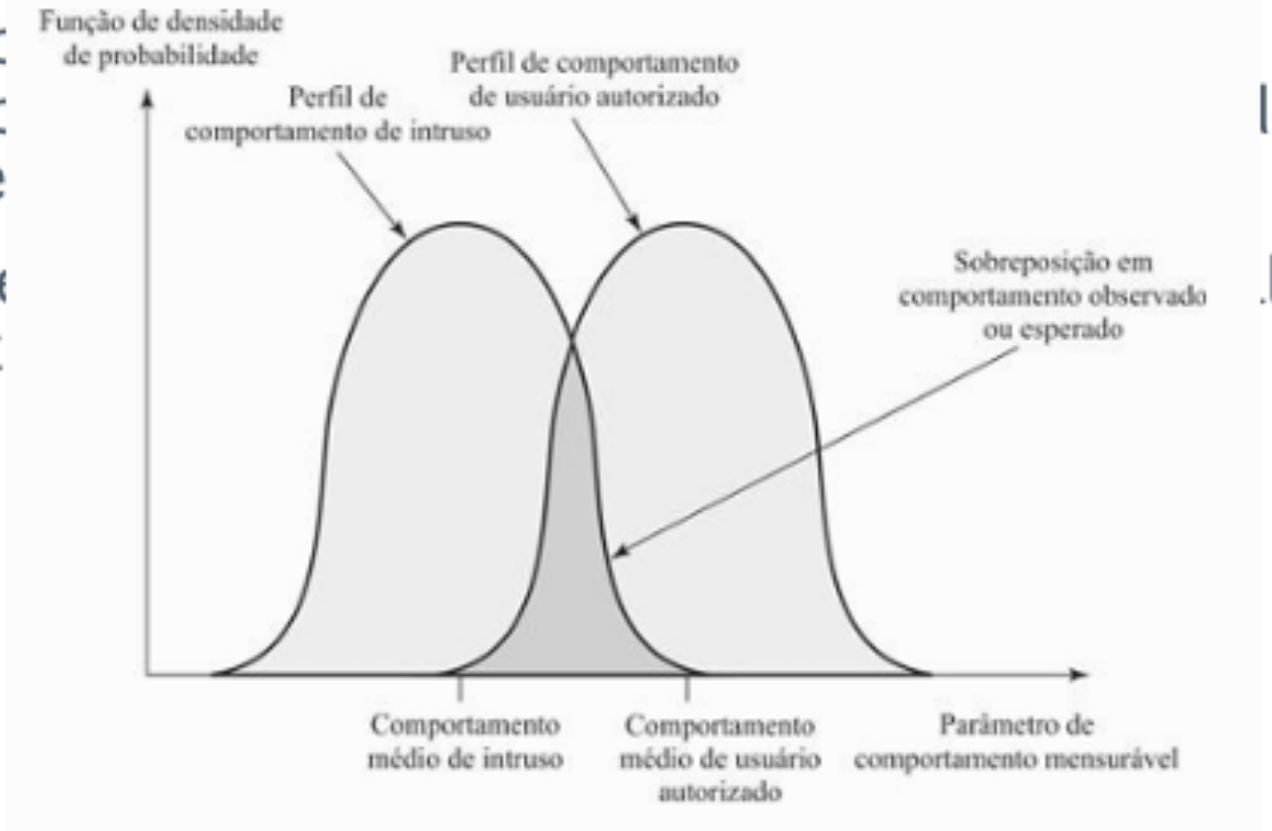
- Redução de dano: quanto mais cedo for detectada, menor o dano e maior a rapidez da recuperação.
- Inibição de atacante: um IDS efetivo pode servir como inibidor e, assim, agir para prevenir intrusões.
- Realimentação de defesas: a detecção de intrusão habilita a coleta de informações sobre técnicas de intrusão que podem ser usadas para fortalecer medidas de prevenção de intrusão

Premissa da diferença de comportamento

- A detecção de intrusão é baseada na premissa de que o comportamento do intruso é diferente do comportamento de um usuário legítimo em modos que podem ser quantificados.
- Sobreposição de comportamentos resulta em falsos positivos e falsos negativos

Premissa da diferença de comportamento

› A detecção de intrusão é baseada na premissa de que o comp
comp los que pode
› Sobre .lsos posit



Requisitos de IDSs

- 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 sobrecusto computacional mínimo ao sistema no qual está executando.
- Poder ser configurado de acordo com as políticas de segurança do sistema que está sendo monitorado
- 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 pararem de funcionar por qualquer razão, o resto deles deve ser afetado o mínimo possível.
- Permitir reconfiguração dinâmica, isto é, a capacidade de reconfigurar o IDS sem ter de reiniciá-lo

HIDS

- Monitora atividades em um sistema/host para detectar comportamento suspeito
- Detecta intrusões externas e internas
- Abordagens gerais
  - Detecção de anomalia: Envolve a coleta de "dados relacionados ao comportamento de usuários legítimos durante um período de tempo
    - Detecção de limiar: Essa abordagem envolve definir limiares independentes de usuário 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 contas individuais.
  - 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

Breve histórico dos Sistemas de Detecção de Intrusão

Origens na década de 1980

- 1980: James Anderson's paper, Computer Security Threat Monitoring and Surveillance
  - Noção formal de ”detecção de intrusão”
- 1983: SRI International (Dr. Doroty Denning) inicia projeto para desenvolver sistema de detecção de intr.
  - Em 1984, a SRI completa contrato com a US Navy e entrega o primeiro IDS funcional (IDES)
  - Em 1985, Denning & Neumann publicam relatório técnico ”Requirements and model for IDES - A real-time intrusion detection system”
  - Em 1987, Dennin publica An Intrusion-Detection Model; o artigo é a base para os IDS que seriam desenvolvidos
- 1984: SRI Int. desenvolve ferramenta de coleta e análise de pacotes da ARPANET

Grupo UCDavis/LLNL e Projeto Haystack

- 1988: UCDavis/LLNL: Haystack Project para a US Air Force
  - Comparava dados com padrões de referência pré-definidos
- Conceito de DIDS
  - Monitorava máquinas-cliente assim como servidores
- 1989: formação da empresa "Haystack Labs" e lançamento da tecnologia "Stalker"
- 1990: publicação do paper "A Network Security Model", Heberlein et al. (aluno UCDavis)
  - Considerado o primeiro NIDS
  - Foi instalado em várias redes do governo
  - Atraiu interesse para o setor de IDS

Década de 1990 -”mercado” de IDS

- Atuação do Haystack com seu ”Stalker”
- A Science Applications International Corporation (SAIC) desenvolve seu Computer Misuse Detection System (CMDS)
- Air Force's Cryptologic Support Center desenvolve seu ” Automated Security Measurement System” (ASIM)
  - Melhorias na portabilidade e escalabilidade
  - Solução integrada de software e hardware
  - Desenvolvedores formaram empresa em 1994 (Wheel group) – lançam NetRanger, primeiro dispositivo IDS comercial
- 1997: ISS desenvolve RealSecure (NIDS)
- 1998: Centrax Corp. desenvolve HIDS para WinNT
- 1998 (março): Cisco compra Wheel Group por US$124mi

Década de 1990 -”mercado” de IDS

- Atuação do Haystack com seu ”Stalker”
- A Science Applications International Corporation (SAIC) desenvolve seu Computer Misuse Detection System (CMDS)
- Air Force's Cryptologic Support Center desenvolve seu ” Automated Security Measurement System” (ASIM)
  - Melhorias na portabilidade e escalabilidade
  - Solução integrada de software e hardware
  - Desenvolvedores formaram empresa em 1994 (Wheel group) – lançam NetRanger, primeiro dispositivo IDS comercial
- 1997: ISS desenvolve RealSecure (NIDS)
- 1998: Centrax Corp. desenvolve HIDS para WinNT
- 1998 (março): Cisco compra Wheel Group por US$124mi

Década de 1990 -”mercado” de IDS

- Atuação do Haystack com seu ”Stalker”
- A Science Applications International Corporation (SAIC) desenvolve seu Computer Misuse Detection System (CMDS)
- Air Force's Cryptologic Support Center desenvolve seu ” Automated Security Measurement System” (ASIM)
  - Melhorias na portabilidade e escalabilidade
  - Solução integrada de software e hardware
  - Desenvolvedores formaram empresa em 1994 (Wheel group) – lançam NetRanger, primeiro dispositivo IDS comercial
- 1997: ISS desenvolve RealSecure (NIDS)
- 1998: Centrax Corp. desenvolve HIDS para WinNT
- 1998 (março): Cisco compra Wheel Group por US$124mi

Década de 1990 -”mercado” de IDS

- Atuação do Haystack com seu ”Stalker”
- A Science Applications International Corporation (SAIC) desenvolve seu Computer Misuse Detection System (CMDS)
- Air Force's Cryptologic Support Center desenvolve seu ” Automated Security Measurement System” (ASIM)
  - Melhorias na portabilidade e escalabilidade
  - Solução integrada de software e hardware
  - Desenvolvedores formaram empresa em 1994 (Wheel group) – lançam NetRanger, primeiro dispositivo IDS comercial
- 1997: ISS desenvolve RealSecure (NIDS)
- 1998: Centrax Corp. desenvolve HIDS para WinNT
- 1998 (março): Cisco compra Wheel Group por US$124mi
- 1999: Snort, o IDS ”open-source”

Década de 2000: padronização

- Setembro de 2000: Intrusion Detection System Requirements, do MITRE
- Novembro de 2001: NIST SP 800-31 - Special Publication on Intrusion Detection Systems
- Fevereiro de 2002: Intrusion Detection Interoperability and Standardization, da SANS
- Fevereiro de 2007: NIST SP 800-94 – Guide to Intrusion Detection and Prevention Systems (IDPS)
- Março de 2007: RFCs 46765, 4766 e 4767 sobre Intrusion Detection Message Exchange

Década de 2010 – mercado consolidado

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

Resumo (visão histórica)

- Sistemas de Detecção de Instrusão passam a se desenvolver no meio acadêmico com financiamento governamental na década de 1980
- Ao final da década de 1980, tecnologia estava estabelecida e ferramentas estavam disponíveis
- Na primeira metade da década de 1990 observou-se o surgimento de empresas (spin-offs dos grupos de pesquisa)
- A segunda metade da década de 1990 foi de consolidação do mercado
- Década de 2000 observa esforços de padronização

O Modelo HIDS de Denning

An Intrusion-Detection Model (1987)
(host-based, anomaly-based)

Fatores/motivação

- most existing systems have security flaws that render them susceptible to intrusions, penetrations, and other forms of abuse; finding and fixing all these deficiencies is not feasible for technical and economic reasons;
- existing systems with known flaws are not easily replaced by systems that are more secure-mainly because the systems have attractive features that are missing in the moresecure systems, or else they cannot be replaced for economic reasons;
- developing systems that are absolutely secure is extremely difficult, if not generally impossible; and
- even the most secure systems are vulnerable to abuses by insiders who misuse their privileges.

Hipótese do ”padrão anormal”

- exploitation of a system's vulnerabilities involves abnormal use, of the system; therefore, security violations could be detected from abnormal patterns of system usage.
- Exemplos de violações/intrusões
  - Attempted break-in
  - Masquerading or successful break-in
  - Penetration by legitimate user
  - Leakage by legitimate user
  - Inference by legitimate user
  - Trojan horse
  - Virus
  - Denial-of-Service

Exemplos de violações/intrusões

- · Attempted break-in
  - Someone attempting to break into a system might generate an abnormally high rate of password failures with respect to a single account or the system as a whole.
- Masquerading or successful break-in
  - Someone logging into a system through an unauthorized account and password might have a different login time, location, or connection type from that of the account's legitimate user.
- Penetration by legitimate user
  - A user attempting to penetrate the security mechanisms in the operating system might execute different programs or trigger more protection violations from attempts to access unauthorized files or programs. If his attempt succeeds, he will have access to commands and files not normally permitted to him. ·
- Leakage by legitimate user
  - A user trying to leak sensitive documents might log into the system at unusual times or route data to remote printers not normally used.
- Inference by legitimate user
  - A user attempting to obtain unauthorized data from a database through aggregation and inference might retrieve more records than usual.
- Trojan horse
  - The behavior of a Trojan horse planted in or substituted for a program may differ from the legitimate program in terms of its CPU time or I/O activity.
- Virus
  - A virus planted in a system might cause an increase in the frequency of executable files rewritten, storage used by executable files, or a particular program being executed as the virus spreads.
- Denial-of-Service
  - An intruder able to monopolize a resource (e.g., network) might have abnormally high activity with respect to the resource, while activity for all other users is abnormally low.

Visão geral do modelo - componentes

- Subjects
  - Initiators of activity on a target system- normally users
- Objects
  - Resources managed by the system-files, commands, devices, etc.
- Audit records
  - Generated by the target system in response to actions performed or attempted by subjects on objects-user login, command execution, file access, etc.
- Profiles
  - Structures that characterize the behavior of subjects with respect to objects in terms of statistical metrics and models of observed activity. Profiles are automatically generated and initialized from templates.
- Anomaly records
  - Generated when abnormal behavior is detected.
- Activity rules
  - Actions taken when some condition is satisfied, which update profiles, detect abnormal behavior, relate anomalies to suspected intrusions, and produce reports.

Registros de auditoria (audit records)

- Audit Records are 6-tuples representing actions performed by subjects on objects:
  - <Subject, Action, Object, Exception-Condition, Resource-Usage, Time-stamp>
    - Action: Operation performed by the subject on or with the object, e.g., login, logout, read, execute.
    - Exception-Condition: Denotes which, if any, exception condition is raised on the return. This should be the actual exception condition raised by the system, not just the apparent exception condition returned to the subject.
    - Resource-Usage: List of quantitative elements, where each element gives the amount used of some resource, e.g., number of lines or pages printed, number of records read or written, CPU time or 1/0 units used, session elapsed time.
    - Time-stamp: Unique time/date stamp identifying when the action took place.

Exemplo

- COPY GAME.EXE TO <Library>GAME.EXE
  - issued by user Smith- to copy an executable GAME file into the <Library> directory; the copy is aborted because Smith does not have write permission to < Library >
- <Subject, Action, Object, Exception-Condition, Resource-Usage, Time-stamp>
- (Smith, execute, <Library>COPY.EXE, 0, CPU=00002, 11058521678)
- (Smith, read, <Smith>GAME.EXE, 0, RECORDS=O, 11058521679)
- (Smith, write, <Library> GAME.EXE, write-viol, RECORDS=O, 11058521680)

Vantagens da decomposição

- First, since objects are the protectable entities of a system, the decomposition is consistent with the protection mechanisms of systems. Thus, IDES can potentially discover both attempted subversions of the access controls (by noting an abnormality in the number of exception conditions returned) and successful subversions by noting an abnormality in the set of objects accessible to the subject).
- Second, single-object audit records greatly simplify the model and its application.
- Third, the audit records produced by existing systems generally contain a single object, although some systems provide a way of linking together the audit records associated with a "job step" (e.g., copy or compile) so that all files accessed during execution of a program can be identified.

Perfis de atividade

- An activity profile characterizes the behavior of a given subject (or set of subjects) with respect to a given object (or set thereof), thereby serving as a signature or description of normal activity for its respective subject(s) and object(s).
- Aspectos
  - estrutura
  - geração
  - Aplicações
  - métricas
  - modelos

Métricas

- Event Counter: x is the number of audit records satisfying some property occurring during a period (each audit record corresponds to an event). Examples are number of logins during an hour, number of times some command is executed during a login session, and number of password failures during a minute.
- Interval Timer: x is the length of time between two related events; i.e., the difference between the time- stamps in the respective audit records. An example is the length of time between successive logins into an account.
- Resource Measure: x is the quantity of resources consumed by some action during a period asspecified in the Resource-Usage field of the audit records. Examples are the total number of pages printed by a user per day and total amount of CPU time consumed by some program during a single execution.

Modelos Estatísticos

- Given a metric for a random variable x and n observations x1, … , xn the purpose of a statistical model of x is to determine whether a new observation xn+1 is abnormal with respect to the previous observations. The following models may be included
  - Operational Model: This model is based on the operational assumption that abnormality can be decided by comparing a new observation of x against fixed limits.
  - Mean and Standard Deviation Model: This model is based on the assumption that all we know about x1, … xn, are mean and standard deviation as determined from its first two moments
  - Multivariate Model: This model is similar to the mean and standard deviation model except that it is based on correlations among two or more metrics.
  - Markov Process Model: This model, which applies only to event counters, regards each distinct type of event (audit record) as a state variable, and uses a state transition matrix to characterize the transition frequencies between states
  - Time Series Model: This model, which uses an interval timer together with an event counter or resource measure, takes into account the order and interarrival times of the observations x1, … , xn, as well as their values.

Exemplos

Medição	Modelo	Tipo de intrusão detectada
Atividade de acesso e de sessão		
Freqüência de acesso por dia e por intervalo de tempo	Média e desvio padrão	É provável que os intrusos acessem o sistema em horários incomuns.
Freqüência de acesso em diferentes localizações	Média e desvio padrão	Os intrusos podem acessar o sistema a partir de um local que determinado usuário raramente ou nunca usa.
Tempo desde o último acesso	Operacional	Invasão de uma conta "morta".
Tempo transcorrido por sessão	Média e desvio padrão	Desvios significativos podem indicar um impostor.
Quantidade de tráfego de saída para a localização	Média e desvio padrão	Quantidade excessiva de dados transmitidos para locais remotos podem significar vazamento de dados sensíveis.
Utilização de recursos de sessão	Média e desvio padrão	Níveis não usuais de processador ou de operações de entrada/saída podem sinalizar um intruso.
Falhas de senha no acesso	Operacional	Tentativa de invasão por adivinhação de senha.
Falhas em acessar o sistema a partir de terminais especificados	Operacional	Tentativa de invasão.
Atividade de comando ou execução de programa		
Freqüência de execução	Média e desvio padrão	Pode detectar intrusos, que provavelmente usam comandos diferentes, ou uma penetração bem-sucedida por um usuário legítimo que conseguiu acesso a comandos privilegiados.
Utilização de recursos de programa	Média e desvio padrão	Um valor anormal pode sugerir injeção de um vírus ou cavalo de Troia, que provoca efeitos colaterais que aumentam a utilização de entrada/saída ou de processador.
Recusas de execução	Modelo operacional	Pode detectar tentativa de intrusão por usuário individual que busca privilégios mais altos.
Atividade de acesso a arquivo		
Freqüência de leitura, escrita, criação, remoção	Média e desvio padrão	Anormalidades em acesso de leitura e escrita para usuários individuais podem significar atividades de impostores ou de navegação no sistema.
Registros lidos, escritos	Média e desvio padrão	Anormalidade pode significar uma tentativa de obter dados sensíveis por inferência e agregação.
Falha na contagem de leitura, escrita, criação, remoção	Operacional	Pode detectar usuários que tentam persistentemente acessar arquivos não autorizados.

O Modelo NIDS de UCDavis

DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype

Abordagem

- Foco na segurança da ”rede”
- Alvo do sistema é um conjunto de computadores e uma LAN
  - Assume-se comunicação broadcast na LAN
- Assume-se que a LAN é fisicamente segura
  - Nenhum atacante tem acesso físico a cabos, interfaces ou equipamentos
- Ataques originam-se do mundo exterior
  - Mas podem fazer uso de hosts internos inseguros

Conceito do NSM

- Matriz 4-dimensional, com dimensões representando:
  - Source (a host which generates traffic),
  - Destination (a host to which traffic is destined),
  - Service (mail, login, etc.), and Connection
  - ID (a unique identifier for a specific connection).
- Each cell in the matrix represents a unique connection on the network from a source host to a destination host by a specific service.
- Each cell holds two values: the number of packets passed on the connection for a certain time interval, and the sum of the data carried by those packets.

Métodos de detecção

- An analyzer must examine the data patterns in the matrix representing the current traffic to determine if an attack is occuring on the system
- One method to examine the traffic matrix is to compare it against a matrix holding a certain pattern. For example, a comparison may be made against a matrix holding the representation of a specific attack.
- To compare the two matrices, the pattern being checked can be treated as a mask through which the current traffic will be passed

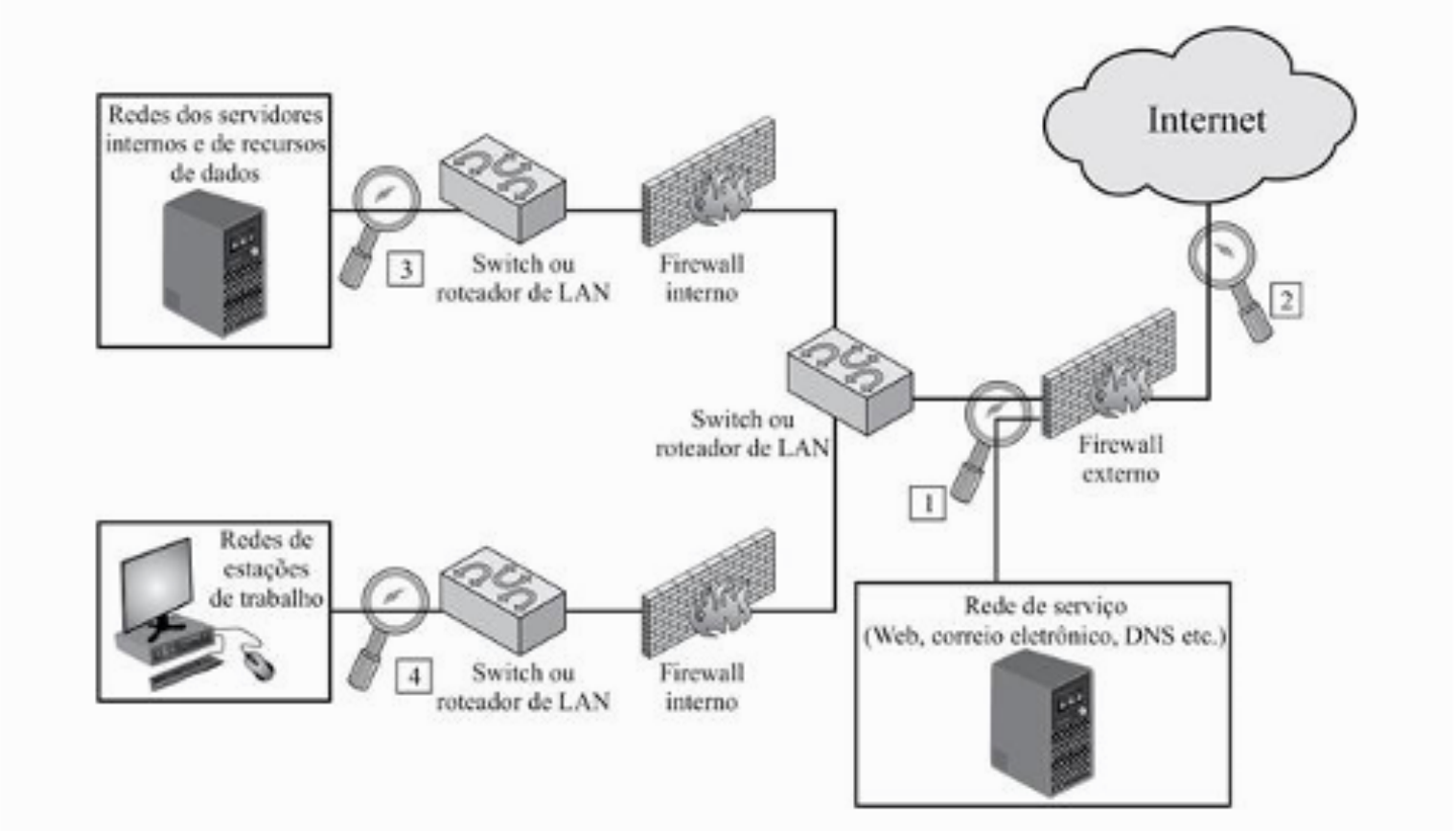
Uso de ”máscara” – anomalous-based

- A mask is a representation of the values for traffic measurements which are observed for some known traffic pattern.
- similar to IDES: to generate a mask of the normal traffic and detect anything outside this pattern
  - This is based on the Denning model [2] which assumes that an attack would generate anomalous patterns
- Mask only allows measurements which do not match this “normal” mask to pass through

Detecção de Intrusão baseada em rede

- Monitora pontos (segmentos) selecionados em uma rede
- Examina o tráfego, pacote por pacote, em tempo real ou próximo ao tempo real, para tentar detectar padrões de intrusão
- Pode examinar atividades de protocolos no nível de rede, transporte e/ou aplicação
- Tipos de sensores
  - Inline: todo o tráfego monitorado passa por ele
  - Passivo: recebe tráfego replicado (modelo mais comum)

Localização do sensor NIDS



O Modelo DIDS de UCDavis

DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and An Early Prototype

Motivação e Oportunidade

- Proliferação de redes de computadores heterogêneas
  - increased opportunity for unauthorized access that is provided by the network's connectivity
  - The problem is exacerbated when dial-up or internetwork access is allowed
  - The use of distributed rather than centralized computing resources also implies reduced control over those resources
  - multiple independent computers are likely to generate more audit data than a single computer, and this audit data is dispersed among the various systems.
    - not all of the audit data can be forwarded to a single IDS for analysis; some analysis must be accomplished locally.

Questões importantes

- IDS baseado em host "tradicional" baseava-se em um único sistema isolado
  - Pode-se conseguir uma defesa mais efetiva realizando-se uma coordenação de diversos IDS numa rede
- Questões importantes num IDS distribuído
  - Existência de diferentes formatos de registro de auditoria
  - Necessidade de transmissão de dados de detecção pela rede – e consequente garantia de segurança desses dados
  - Arquitetura centralizada versus descentralizada
    - Centralizada: único ponto de coleta de dados facilita análise e correlação – mas cria ponto isolado de falha
    - Descentralizada: demanda coordenação das atividades das várias centrais de análise

Modelo de IDS distribuído (UCDavis/ Purdue)

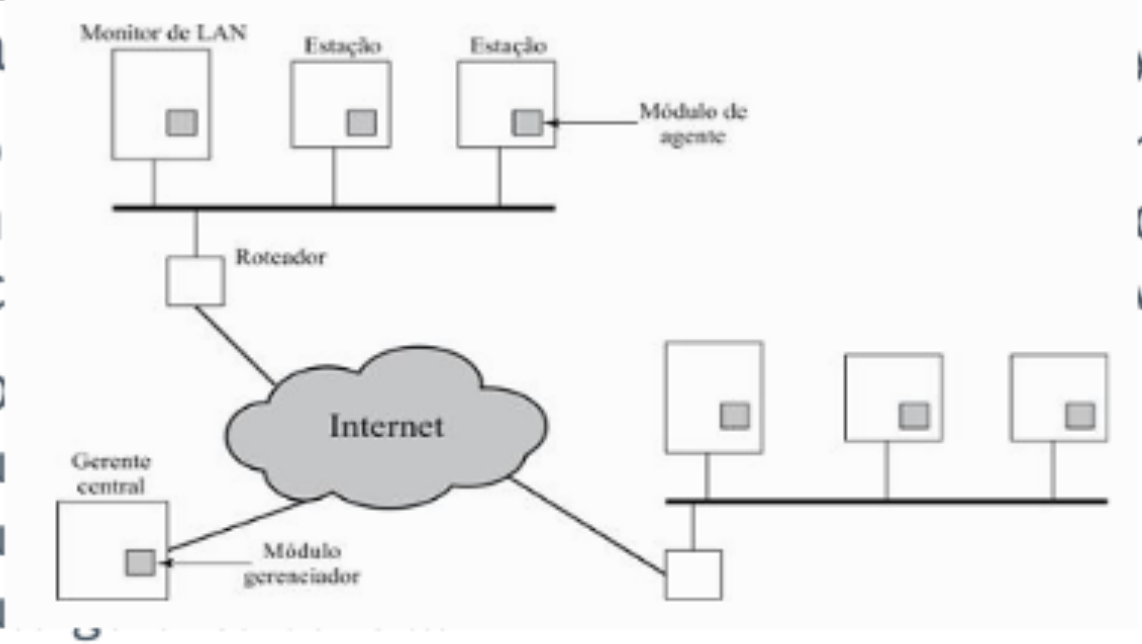
- The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis.
- The components of DIDS are the DIDS director, a single host monitor per host and a single LAN monitor for each broadcast LAN segment in the monitored network.
- Componentes principais
  - Módulo de agente de estação
  - Módulo de agente de monitor de LAN
  - Módulo gerente central

Modelo de IDS distribuído (UCDavis/ Purdue)

› The DIDS architecture combines distributed monitoring and da ysis.

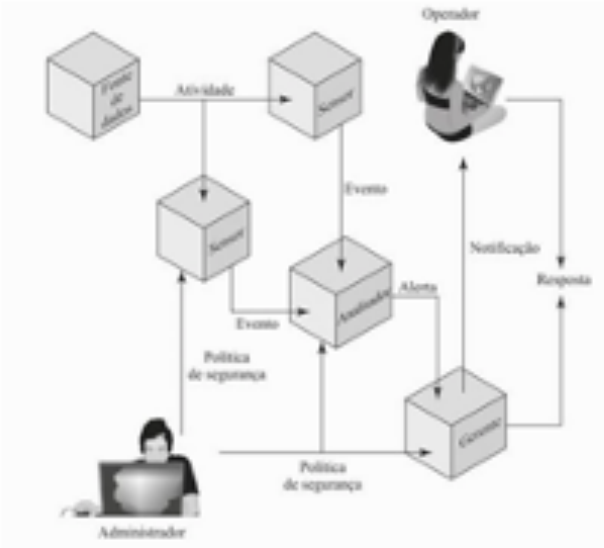
› The co , a single host m or for each broadc work.

› Compo
  – Módu
  – Módu
  – Módu

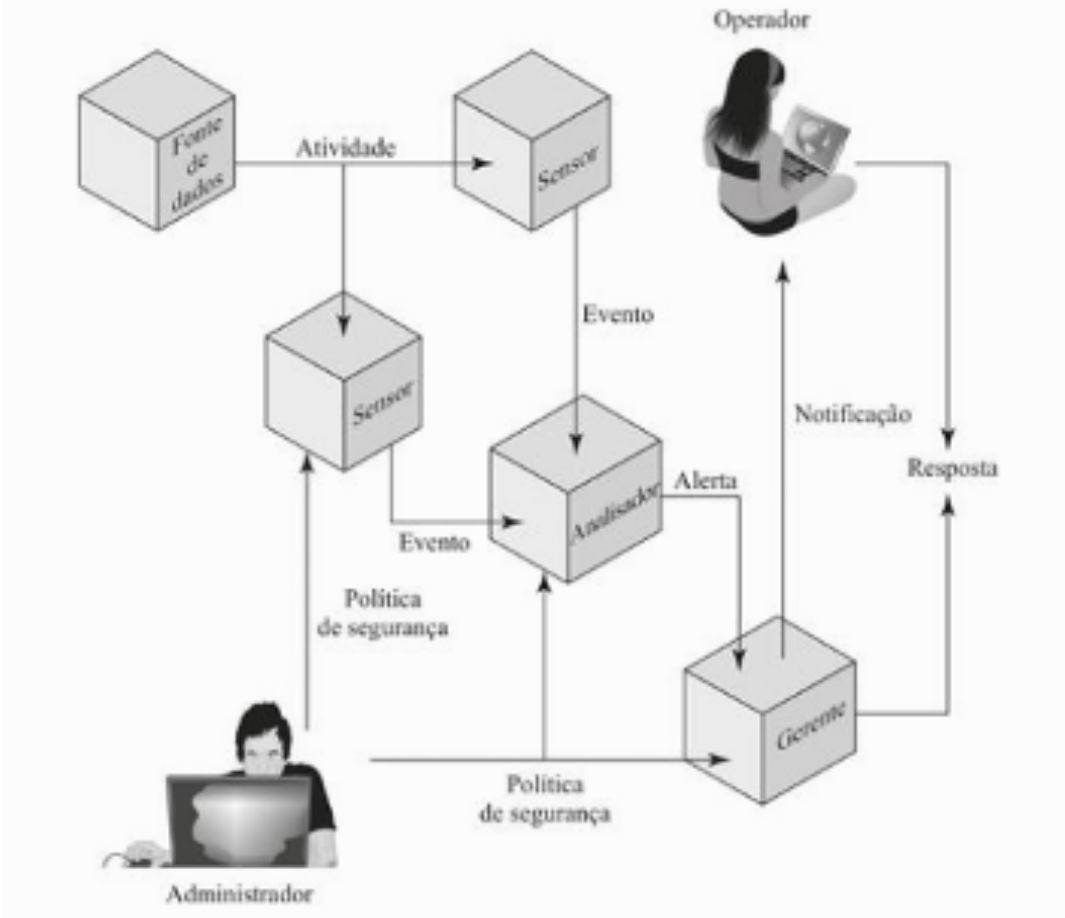


Troca de Mensagens em IDS distribuídos

- Foco na interoperabilidade
  - Atuação do IETF Intrusion Detection Working Group
    - Requisitos para troca de mensagens de detecção de intrusão (RFC 4766)
    - Formato de troca de mensagens de detecção de intrusão (RFC 4765)
    - Protocolo de troca de detecção de intrusão (RFC 4767)
- Modelo para troca de mensagens no IDS
  - Fonte de dados
  - Sensor
  - Analisador
  - Administrador
  - Gerente
  - Operador



Troca de Mensagens em IDS distribuídos



Técnicas de IDS

Baseado no NIST SP 800-94

Signature-based versus Anomaly-based

- Detecção baseada em assinatura
  - Constrói modelos baseados em "padrões de intrusão"
    - Dados (tráfego, logs de eventos etc.) que estejam compatíveis com os padrões de intrusão indicam a existência de uma intrusão
  - Boa taxa de acerto (true positive) sobre ataques conhecidos
  - Dificuldade de identificar novos ataques
- Detecção baseada em anomalia
  - Constrói modelos baseados em "padrões de normalidade"
    - Dados (tráfego, logs de eventos etc.) que não estejam compatíveis com os padrões de normalidade indicam intrusão
  - Boa capacidade de identificar novos ataques
  - Possibilidade de muitos falsos-positivos
    - "Anormalidade legítima"

Detecção Signature-based

- A *signature* is a pattern that corresponds to a known threat.
  - *Signature-based detection* is the process of comparing signatures against observed events to identify possible incidents
- Examples of signatures are as follows:
  - A telnet attempt with a username of "root", which is a violation of an organization's security policy
  - An e-mail with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware
  - An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled.

Detecção Anomaly-based

- *Anomaly-based detection* is the process of comparing definitions of what activity is considered normal against observed events to identify significant deviations.
  - An IDPS using anomaly-based detection has *profiles* that represent the normal behavior of such things as users, hosts, network connections, or applications.
  - The profiles are developed by monitoring the characteristics of typical activity over a period of time.
    - For example, a profile for a network might show that Web activity comprises an average of 13% of network bandwidth at the Internet border during typical workday hours.
    - Profiles can be developed for many behavioral attributes, such as the number of e-mails sent by a user, the number of failed login attempts for a host, and the level of processor usage for a host in a given period of time.

Construção de ”padrão” na abordagem ”anomaly-based”

- An initial profile is generated over a period of time (typically days, sometimes weeks) sometimes called a *training period*.
- Padrões ”estáticos” e ”dinâmicos”
  - Once generated, a static profile is unchanged unless the IDPS is specifically directed to generate a new profile
  - A dynamic profile is adjusted constantly as additional events are observed.
- Inadvertently including malicious activity as part of a profile is a common problem with anomaly-based IDPS products.

Técnicas de Detecção por tipo de ataque

- Detecção de Assinatura
  - Ataques à camada de aplicação – exemplos: estouros de buffers, adivinhação de senha e transmissão de malware
  - Ataques à camada de transporte – exemplos: fragmentação não usual de pacotes, escaneamento de portas, e ataques específicos ao TCP, como inundação de SYN
  - Ataques à camada de rede – exemplos: endereços IP falsificados e valores de cabeçalhos IP ilegais
  - Serviços de aplicação inesperados – exemplos: estação que executa um serviço de aplicação não autorizado
  - Violações de política – exemplos: uso de sites Web inadequados e de protocolos de aplicação proibidos
- Detecção de Anomalia
  - Ataques DDoS
  - Scanning
  - Worms

Stateful Protocol Analysis

- comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.
  - Some vendors use the term "deep packet inspection" to refer to performing some type of stateful protocol analysis, often combined with a firewall capability that can block communications determined to be malicious
- The "stateful" in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state.
  - Exemplo do FTP autenticado versus não-autenticado
- Desvantagens
  - Intensivo em uso de recursos
  - Não detecta ataques que não violem características dos protocolos

Componentes e arquiteturas de IDS

- Componentes típicos de IDS
  - Sensor ou Agente
  - Servidor de Gerenciamento
  - Servidor de banco de dados
  - Console
- Arquitetura de Redes
  - Rede da Organização
  - Rede de Gerenciamento

Capacidades de Segurança

- Coleta de informações
- Registro de eventos (logs)
- Detecção
  - Threshholds
  - Black-list e white-list
  - Alertas
  - Visualização/Edição de algoritmos de detecção
- *Prevenção

Honeypots

Honeypots

- sistemas chamarizes projetados para atrair um atacante potencial e afastá-lo de sistemas críticos.
- são projetados para
  - Desviar um atacante do acesso a sistemas críticos
  - Coletar informações sobre a atividade do atacante (attack datasets)
  - Incentivar o atacante a ficar no sistema por tempo suficiente para que os administradores respondam
- repletos de informações falsas projetadas para parecerem valiosas, mas que um usuário legítimo do sistema não acessaria
  - Assim, qualquer acesso ao pote de mel é suspeito
- instrumentado com monitores e registradores de eventos sensíveis que detectam esses acessos e coletam informações sobre as atividades do atacante

Posicionamento dos honeypots

- Além do firewall externo
  - Não aumenta o risco para a rede interna
  - atrai ataques – reduzindo alertas por FW e IDS
  - Pouca capacidade de capturar atacantes internos
- Honeypot na DMZ
  - Classe restrita de atacantes (focados nos sistemas da DMZ)
  - Administrador deve garantir a segurança dos outros sistemas na DMZ (webserver, e-mail, etc.)
  - Efetividade limitada caso esteja atrás de um FW
- Honeypot Interno
  - Captura atacantes internos
  - Desvantagens análogas ao caso anterior

Posicionamento dos honeypots