Frank Ned Santa Cruz de Oliveira
Responsável pelo Website Verdade
@Absolutahttp://www.absoluta.org
frank@absoluta.org

ARTIGO

Ferramentas IDS

Resumo
Este documento descreve um modelo de ferramenta de IDS baseado no sistema de defesa dos seres vivos, além disso verificamos a anatomia dos sensores que compõem esta ferramenta e as implicações legais decorrentes dos "logs" coletados.

1 Introdução

As ferramentas para segurança de computadores e redes são necessárias para proporcionar transações seguras. Geralmente as instituições concentram suas defesas em ferramentas preventivas como firewalls mas acabam ignorando as ferramentas de detecção de intrusão (IDS – Intrusion Detection System).

Na primeira parte deste texto faremos uma analogia entre o sistema de defesa dos seres vivos e as futuras (ou atuais) ferramentas de IDS, na segunda parte trataremos de alguns aspectos relacionados a "anatomia" das ferramentas de IDS e finalmente faremos algumas considerações sobre os aspectos legais a respeito dos dados coletados por tais sistemas.

2 Sistema de Defesa dos seres Vivos e as ferramentas de IDS

2.1 A Analogia

Os anticorpos constituem o mais específico mecanismo de defesa que nosso organismo possui. Os anticorpos desempenham importantíssimo papel na proteção de nosso organismo contra substâncias estranhas.

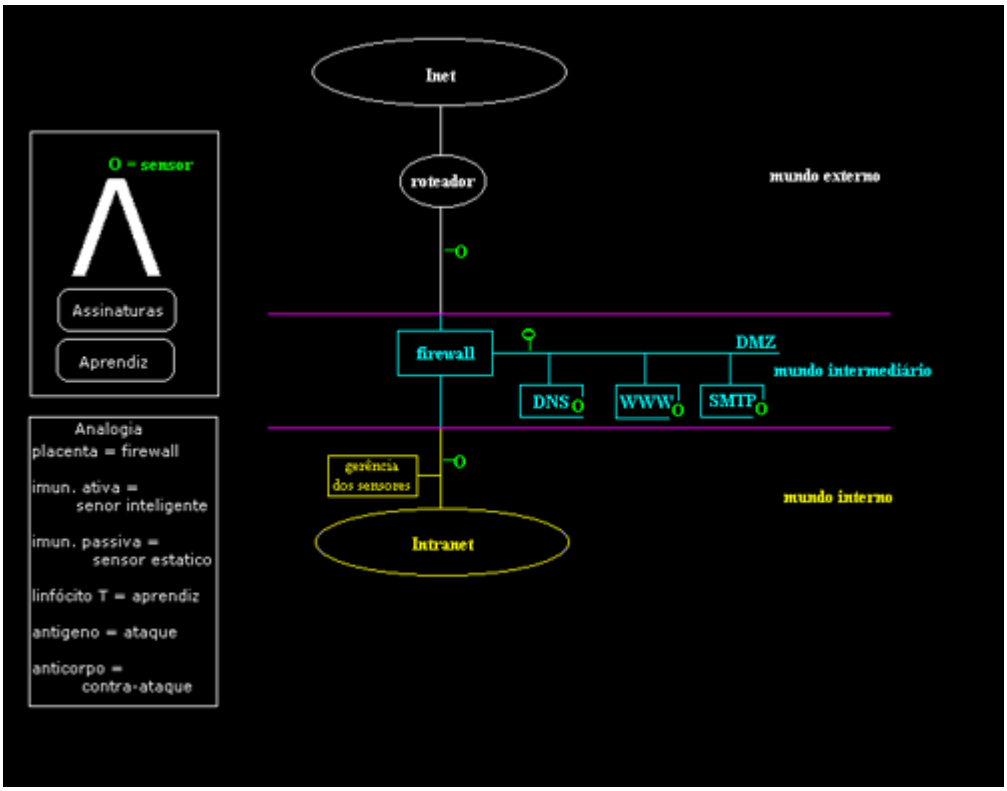
Quando injetamos em um animal uma substância estranha, certos glóbulos brancos do sangue, os linfócitos T, produzem e lançam na corrente sangüínea um tipo especial de proteína capaz de se unir especificamente à molécula estranha, inativando-a. A proteína que o indivíduo sintetiza em resposta ao material estranho, denomina-se anticorpo, e as substâncias estranhas, que induzem a síntese dos anticorpos, são denominadas antígenos.

Possuímos dois tipos de sistemas de imunização, são eles:

- **Imunização ativa**: é a que se consegue pela formação de anticorpos elaborados pelo próprio indivíduo. Nos seres humanos inicia-se a partir do 3º mês de vida do feto, entre o 4º e 6º mês de vida do feto outros órgãos completam o sistema imunitário. Como o sistema imunitário se estabelece só a partir do 3º mês, durante os três primeiros meses de vida, o feto é incapaz de se defender por seus próprios meios contra eventuais infecções que atravessem a barreira placentária. Nesta fase, o feto conta só com a imunização passiva (anticorpos que existem na mãe), transferida da mãe

ao filho através da placenta.

- **Imunização passiva**: um animal é imunizado contra um determinado antígeno. Esta imunização é feita através de injeção cada vez mais concentradas do antígeno, no animal. O animal reage a este antígeno produzindo quantidades cada vez maiores de anticorpos específicos, que vão se acumulando no sangue. Após a imunização, é extraido sangue do animal imunizado e a fração sangüínea que contem as moléculas de anticorpo, são separadas. Esta fração rica em anticorpos é chamada soro e é injetado na corrente sangüínea do indivíduo que se deseja imunizar.



O sistema de detecção de intrusão ou IDS, tem como um dos objetivos principais detectar se alguém está tentando entrar no seu sistema ou se algum usuário legitimo está fazendo mau uso do mesmo. Esta ferramenta roda constantemente (24 x 7) em background e somente gera uma notificação quando detecta alguma coisa que seja suspeita ou ilegal; assim sendo podemos dizer que a placenta corresponde aos sistemas de firewalls, a imunidade passiva está dentro dos sensores e são os padrões de ataques / assinaturas, ou seja, os ataques conhecidos previamente, a imunidade ativa também estão dentro dos sensores e são caracterizadas por possuírem inteligência para aprender com o comportamento da rede e com isso identificar novos padrões ou mutação dos padrões existentes, a identificação dos novos padrões é realizada pelos aprendizes (linfócitos T), o antigeno é a doença, a ameaça o ataque e os anticorpos são os contra-ataques.

Um sensor é composto por um conjunto de componentes, entre eles: sub-sensor estático, sub-sensor inteligente e aprendiz. O sub-sensor estático deve inicialmente ser configurado de arcordo com a política de segurança além de possuir as assinaturas dos ataques conhecidos, isso caracteriza a imunização passiva, já o sub-sensor inteligente inicialmente passa por um período de adaptação e aprendizado fase em que o sensor aprende e reconhece o padrão

de funcionamento da rede, este período pode ser variável dependendo do volume de tráfego, após esta fase estes sub-sensores inteligentes estariam em condições de reconhecer padrões que fogem da normalidade da rede (linfócitos T) e tomarem ações.

Os sensores podem ser de dois tipos:

- Os sensores de rede devem localizar-se em segmentos estratégicos observando o tráfego da rede e os formatos de pacotes entre outros;

- Os sensores de hosts, ficam dentro dos servidores críticos observando as ações realizadas no sistema operacional, as ações dos serviços e o comportamento da pilha TCP/IP.

Os sensores devem interagir entre si a fim de construirem uma matriz de eventos que tem por objetivo a qualificação do padrão de ataque, minimizando desta forma a ocorrência de alertas falsos (falso positivo). Outras características fundamentais são: o gerenciamento centralizado, a possibilidade do sensor interagir com outros elementos de rede como firewall, roteadores e consoles de gerência; e a possibilidade de construir uma base de conhecimento centralizada de forma a permitir uma visão ampla do nível de segurança da rede.

Desta forma quando algum ataque (antigeno) for detectado pelos sensores torna-se possível ações de conta-ataque (anticorpos) que podem ser: envio de email para o administrador, envio de mensagem via pager, ativação de alertas nas estações de gerência via SNMP, reconfiguração de elementos de rede como firewall e roteadores, e até mesmo o encerramento da conexão através do envio de pacotes de reset (flag RST do TCP) para a máquina atacante e para a máquina atacada, com o objetivo de descarregar a pilha TCP.

No sistema de segurança proposto por [Carlson e Cláudio, 1999] uma caracteristicas importantes é o aprendizado constante com a utilização de estratégias múltiplas.

2.2 O Intruso

De forma simples podemos dizer que um intruso é alguém que tenta invadir seu sistema ou fazer mau uso do mesmo. Mas como você pode definir um intruso?, O que é tentar invadir o sistema? ou ainda o que é fazer mau uso do mesmo?, Um usuário que tenta acessar seu sistema três vezes consecutivas e erra todas, pode ser classificado como um intruso ou como uma tentativa de intrusão?.

Para você poder diferenciar as ações legitimas das ações nocivas, faz-se necessário a definição de uma política de segurança.

Podemos classificar os intrusos em dois tipos:

- **Intrusos Externos** – Muitas pessoas podem pensar que sua instituição esta sujeita na maior parte do tempo a este tipo de tentativa, ou seja, ataques originados de fora da instituição geralmente da Internet.

- **Intrusos Internos** – Mas os estudos geralmente revelam que a maior porcentagem de ataques tem origem dentro da própria instituição, pois

afinal quem conhece melhor a topologia da sua rede?, Alguém que esta dentro ou fora?, Quem sabe onde os dados sensíveis estão armazenados e quais são os recursos de segurança disponíveis?.

Levando-se em consideração o fato de que a maioria dos mecanismos de segurança são implementados com o objetivo de proteger a instituição dos ataques externos muitos ataques ocorrem e muitas vezes não são notados ou quando o são já é tarde demais. Então faz-se necessário um mecanismo que detecte os dois tipos de ataque – uma tentativa externa ou interna. Um sistema de IDS eficiente deve detectar os dois tipos de ataques.

2.3 A Política de segurança

Uma política de segurança define o que é permitido e o que é proibido em um sistema. Temos basicamente duas filosofias por traz de qualquer política de segurança:

- **Proibitiva** – tudo que não é expressamente permitido é proibido;
- **Permissiva** – tudo que não é expressamente proibido é permitido;

Geralmente as instituições mais preocupadas com a segurança adotam a primeira abordagem. Uma política deve descrever exatamente quais operações são permitidas em um sistema. Qualquer operação que não esteja descrita de forma detalhada na política de segurança deve ser considerada ilegal ao sistema.

Infelizmente hoje em dia muitos usuários não tem respeitado a privacidade de outros usuários. O espirito de competitividade tende a passar por cima da ética, isso quando não se trata de um caso patológico de algum doente mental que não se satisfaz sem que invada a privacidade das outras pessoas. Casos de sabotagem podem ser comuns em ambientes com níveis de competitividade elevado.

Muitos usuários respeitam o conjunto de regras sociais. Estas regras encorajam que uns respeitem aos outros tanto a privacidade quanto o ambiente de trabalho. Então torna-se muito fácil subverter a confiança em um ambiente onde existe um acordo de confiança, ou seja, é relativamente fácil invadir um sistema onde os usuários confiam uns nos outros.

Diante disso torna-se necessário a documentação e divulgação das regras que primam pela manutenção da privacidade e integridade.

A justiça deve ser feita e deve ser mostrado que foi feita!

Elementos de uma política de segurança.

Um sistema de computadores pode ser considerado como um conjunto de recursos que é disponibilizado para ser utilizado pelos usuários autorizados.

Existe um documento escrito por Donn Park [Park, 1994] que descreve seis elementos que devem ser contemplados em uma política de segurança

- **Disponibilidade** - o sistema deve estar disponível para uso quando o usuário precisar. Dados críticos devem estar disponíveis de forma

ininterrupta;

- **Utilização** - o sistema e os dados devem ser utilizados para as devidas finalidades;

- **Integridade** - o sistema e os dados devem estar completamente íntegros e em condições de serem utilizados;

- **Autenticidade** - o sistema dever ter condições de verificar a identidade do usuário e o usuário deve ter condições de verificar a identidade do sistema;

- **Confidencialidade** - dados privados devem ser apresentados somente para os donos dos dados ou para o grupo de usuários para o a qual o dono dos dados permitir;

- **Posse** - o dono do sistema deve ter condições de controlá-lo;

3 Anatomia de uma Ferramenta de IDS

3.1 Classificação das Intrusões

Antes de falarmos sobre o sistema de IDS, temos que definir o que significa uma intrusão. Todas as intrusões estão definidas na política de segurança. Enquanto não definirmos o que é permitido e o que não é permitido em nosso sistema é inútil tentar entender uma intrusão.

Uma intrusão pode ser definida como [HeadyLugerEtAl, 1990]:

Qualquer conjunto de ações que tentem comprometer a integridade, confidencialidade ou disponibilidade dos dados e/ou sistema.

Podemos classificar as intrusões em duas classes principais:

- **Intrusão devido ao mau uso do sistema** – são os ataques realizados a pontos fracos do sistema, pontos este conhecidos. Eles podem ser detectados a partir da monitoração de certas ações realizadas em determinados objetos.;

- **Intrusão devido a mudança de padrão** – são detectadas com a observação de mudanças de uso em relação ao padrão normal do sistema. Primeiro monta-se um perfil do sistema, em seguida através de monitoração procura-se por divergências significantes em relação ao perfil construído.

Como a intrusão de mau uso segue padrões bem definidos elas podem ser descobertas através da comparação de padrões em relação a auditoria do sistema. Por exemplo, uma tentativa de criar um arquivo com setuis pode ser detectada através da analise dos logs realizados pela chamadas ao sistema, call system. [KumarSpafford, 1994]

Uma intrusão devido a mudança de padrões é detectada observando-se divergências significantes em relação a utilização normal do sistema. Pode-se construir um modelo a partir de valores derivados da operação do sistema. [Denning, 1987]:

Uma variável randomica X valores apurados durante um determinado período de tempo.

Estes valores são apurados a partir de parâmetros do sistema, como utilização da CPU, número de conexões por minuto, número de processos por usuário entre outros.

Uma variação significativa nestes padrões pode ser um indício de intrusão. Devido ao grupo de valores que podem definir a utilização normal do sistema, vamos assumir o seguinte [Denning, 1987]:

Exploração das vulnerabilidades de um sistema envolve a utilização indevida/anormal do sistema; então, podem ser descobertas violações de segurança a partir de padrões anormais de uso de sistema.

Intrusões devido a mudança de padrões são difíceis de serem detectadas. Não existe um padrão fixo que possa ser monitorado, desta forma devemos trabalhar com aproximação.

O ideal seria a combinação de padrões humanos com programas, desta forma o sistema seria monitorado constantemente a procura de intrusão ao mesmo tempo que teria a capacidade de ignorar as ações de usuários legítimos.

3.2 Detecção de uma Intrusão

Muitas ferramentas, de IDS realizam suas operações a partir da analise de padrões do sistema operacional e da rede tais como: utilização de CPU, I/O de disco, uso de memória, atividades dos usuários, número de tentativas de login, número de conexões, volume de dados trafegando no segmento de rede entre outros. Estes dados formam uma base de informação sobre a utilização do sistema em vários momentos do tempo, outras já possuem bases com padrões de ataque previamente montadas permitindo também a configuração dos valores das bases bem como inclusão de novos parâmetros.

Com estas informações a ferramenta de IDS pode identificar as tentativas de intrusão e até mesmo registrar a técnica utilizada.

Uma ferramenta de IDS deve possuir algumas características, entre elas:

- Deve rodar continuamente sem interação humana e deve ser segura o suficiente de forma a permitir sua operação em background, mas não deve ser uma caixa preta;

- Deve ter tolerância a falhas, de forma a não ser afetada por uma falha do sistema, ou seja, sua base de conhecimento não deve ser perdida quando o sistema for reinicializado;

- Deve resistir a tentativas de mudança (subversão) de sua base, ou seja, deve monitorar a si próprio de forma a garantir sua segurança;

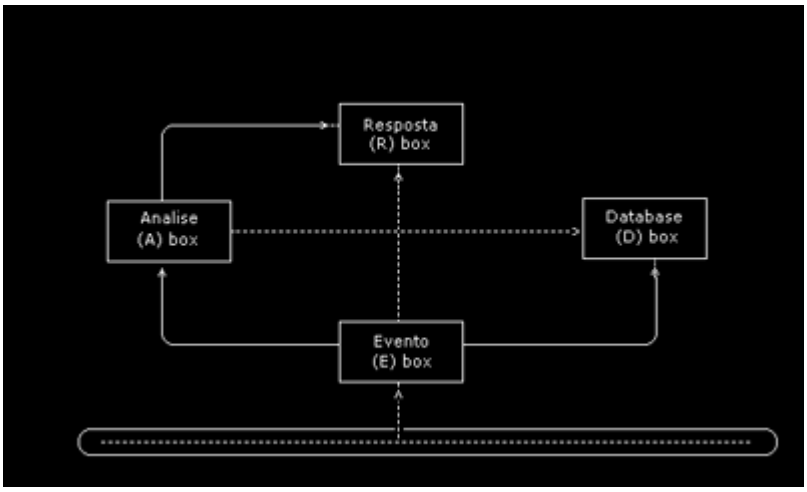
- Dever ter o mínimo de impacto no funcionamento do sistema;

- Deve detectar mudanças no funcionamento normal;

- Deve ser de fácil configuração, cada sistema possui padrões diferentes e a ferramenta de IDS deve ser adaptada de forma fácil aos diversões padrões;

- Deve cobrir as mudanças do sistema durante o tempo, como no caso de uma nova aplicação que comece a fazer parte do sistema;

- E deve ser difícil de ser enganada.



O último ponto faz referências aos prováveis erros que podem acontecer ao sistema. Estes podem ser classificados em: falso positivo, falso negativo e erros de subversão.

- **Falso positivo** ocorre quando a ferramenta classifica uma ação como uma possível intrusão, quando na verdade trata-se de uma ação legítima;

- **Falso negativo** ocorre quando uma intrusão real acontece mas a ferramenta permite que ela passe como se fosse uma ação legítima;

- **Subversão** ocorre quando o intruso modifica a operação da ferramenta de IDS para forçar a ocorrência de falso negativo.

3.3 Modelo Conceitual de uma Ferramenta de IDS

Devido a grande variedade de sistemas de IDS foi proposto um modelo, CIDF – Common Intrusion Detection Framework [CIDF site], este modelo agrupa um conjunto de componentes que define uma ferramenta de IDS:

- Gerador de Eventos (E-boxes)

- Analizador de Eventos (A-boxes)

- Database de Eventos (D-boxes)

- Unidade de Resposta (R-boxes)

Algumas características desejáveis dos componentes são:

- Devem ser reutilizados em um contexto diferente do qual foram

originalmente desenvolvidos, ou seja, devem ser configuráveis de forma a adaptarem-se a ambientes distintos;

- Os sistemas de IDS podem ser elaborados em módulos com funções distintas;

- Estes componentes podem compartilhar/trocar informações entre si, via API ou através da rede, para uma melhor precisão na identificação de ataques;

- Componentes novos devem automaticamente identificar os demais componentes;

- O grupo de componentes poder atuar mutuamente de forma a dar a impressão de ser um único elemento.

Segundo a padronização do CIDF, existe um modelo de linguagem para troca de informações entre os componentes, o CISL – Common Intrusion Specification Language, este formato é referenciado como GIDO – generalized intrusion detection objects.

3.3.1 Gerador de Eventos - (E-box)

A função deste componente é obter os eventos a partir do meio externo ao CIDF, ou seja, ele "produz" os eventos mas não os processa, isso fica a cargo do componente especializado na função de processamento, que por sua vez após analisar os eventos (violação de política, anomalias, intrusão) envia os resultados para outros componentes.

3.3.2 Analisador de Eventos – (A-box)

Este componente basicamente recebe as informações de outros componentes, analisa estas informações e as envia de forma resumida para outros componentes, ou seja, recebe os dados de forma bruta, faz um refinamento e envia para outros.

3.3.3 Database de Eventos – (D-box)

A função deste componente é armazenar os eventos e/ou resultados para uma necessidade futura.

3.3.4 Unidade de Resposta – (R-box)

Este componente é responsável pelas ações, ou seja, matar o processo, resetar a conexão, alterar a permissão de arquivos, notificar as estações de gerência, etc.

3.3.5 Comunicação entre Componentes

A comunicação entre os componentes é definida por uma arquitetura de camadas:

- Gido layer

- Message layer
- Negotiated Transport layer

Esta arquitetura garante a comunicação entre os elementos, bem como sistemas de criptografia e autenticação, estes mecanismos estão definidos no Comm – Communication in the Common Intrusion Detection Framework.

4 Aspectos Jurídicos

4.1 Noções fundamentais

Antes de falar-mos sobre o levantamento e preservação das evidências, é fundamental termos algum entendimento a respeito dos termos e definições utilizadas, bem como dos elementos necessários para dar início a um processo.

4.1.1 Indício

Sm (lat indiciu) 1 Vestígio, sinal. 2 Indicação. 3 Sinal ou fato que deixa entrever alguma coisa, sem a descobrir completamente, mas constitui princípio de prova. [MICHAELIS, 1998].

4.1.2 Evidência

Sf (lat evidentia) "Qualidade daquilo que é evidente, que é incontestável, que todos vêem ou podem ver e verificar. E. de fato: a que se adquire pela observação...". [MICHAELIS, 1998].

4.1.3 Prova

"Do latim probare, tornar crível, estabelecer uma verdade, com/provar. Em sentido amplo, todo meio suscetível de demostrar a verdade de um argumento. ... No direito, em sentido objetivo, todo meio lícito empregado pela parte ou interessado na demonstração daquilo que alega. Não se pode, todavia, desconsiderar o aspecto subjetivo da definição, qual seja, o da convicção do próprio juiz. Daí definirmos a prova processual como todo meio lícito e suscetível de convencer o juiz da verdade de uma alegação da parte. ... para que a prova frutifique é imperioso que seja suficiente (plena); seja clara e não incerta, obscura ou duvidosa; concludente e não impertinente ou irrelevante; ... Quanto às provas moralmente ilegítimas, não são apenas como parecem à primeira vista, aquelas que afrontam a decência, os bons costumes, enfim; vêm a ser, também, as obtidas por meios ilícitos, agredindo a privacidade da parte. A nova CF veda, em seu art. 5º, LVI, a prova ilícita: "São inadmissíveis, no processo, as provas obtidas por meio ilícitos". ... a própria Carta Magna faz uma ressalva a tal orientação, ao dispor, no citado art. 5º, XII: "É inviolável o sigilo da correspondência e das comunicações telegráficas de dados e das comunicações telefônicas, salvo, no ultimo caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"...".[Dicionário Jurídico].

4.1.4 Dano

"Do latim damnu, prejuízo, perda.

Prejuízo sofrido pelo patrimônio econômico ou moral de alguém. O dano

pode ser material, também chamado real, quando atinge um bem economicamente apurável;...". [Dicionário Jurídico].

4.1.5 Dano Emergente

"Efeito danoso, direto e imediato, de um ato ilícito. Trata-se de uma conseqüência primaria de tal ato, ensejando reparação, nos termos do art. 159 do CC. ... O CC trata, nos arts. 1.059 a 1.061, das perdas e danos, assim dispondo o art. 1.059: "Salvo as exceções previstas neste código, de modo expresso, as perdas e danos ... abrangem, além do que efetivamente perdeu, o que razoavelmente deixou de lucrar...". [Dicionário Jurídico].

4.1.6 Inquérito policial

"Do latim quaerere, inquiere, inquirir, indagar.

Procedimento destinado à reunião de elementos acerca de uma infração penal. É o conjunto de diligência realizadas pela Polícia Judiciária, para apuração de uma infração penal e sua autoria, para que o titular possa ingressar em Juízo, pedindo a aplicação de lei ao caso concreto...". [Dicionário Jurídico].

4.1.7 Ação Civil

Art. 63. Transitada em julgado a sentença condenatória, poderão promover-lhe a execução, no juízo cível, para o efeito da reparação do dano, o ofendido, seu representante legal ou seus herdeiros.

Art. 64. Sem prejuízo do disposto no artigo anterior, a ação para ressarcimento do dano poderá ser proposta no juízo cível, contra o autor do crime e, se for caso, contra o responsável civil. [Código de Processo Penal].

4.2 Abordagem Adotada

Neste texto assumimos que os logs constituem evidências e a mesmas serão utilizadas para estabelecer a verdade de um fato, ou seja, constituir a prova.

4.3 Levantamento de Evidências

Uma questão que a cada dia torna-se mais importante e preocupante diz respeito aos procedimentos para reunião de provas com a finalidade de instaurar inquérito penal ou ação civil, ou seja, mecanismos que permitam preservar às evidências com o objetivo de assegurar a integridade e autenticidade dos dados coletados de forma a garantir seu valor probante para que futuramente as devidas ações legais sejam instauradas. Estas ações podem ser intentadas na esfera penal, precedidas ao inquérito, nos casos de crimes de ação publica (CPP art. 5º), ou no âmbito civil.

As ações penais caracterizam-se pela violação da legislação penal em vigor, já a ação civil decore dos danos causados.

Segundo [sommer, 1998], a questão é: Quais são os requisitos para tornar os dados coletados pelas ferramentas de IDS em evidências legais?

Devemos ter em mente que a **demonstração** de que uma intrusão ocorreu é apenas um dos pontos para legitimidade de um processo civil/criminal.

Esta dificuldade existe principalmente devido a uma questão filosófica no tocante à interpretação da caracterização de provas para a comunidade de especialistas em computadores e o que o sistema legal considera prova.

Como pudemos ver a principal função de uma ferramenta de IDS é detectar o intruso e acionar processos de contra ataque. No mundo real, nos edifícios, industrias, em nossas casas dispomos de vários dispositivos que permitem a detecção de intrusos, tais como: infravermelho, analisadores de variação de temperatura e pressão, sensores de movimento; todos este equipamentos são úteis para disparar um alarme quando detecta um intruso, mas eles não possuem formas que permita uma coleta imediata de evidências com o objetivo de identificar o intruso, como analogia podemos citar o cachorro latindo durante a noite, provavelmente trata-se de um intruso, mas quem é o intruso? Um gato ou alguém querendo invadir seu espaço? (até os cães possuem falso positivo), para ajudar na identificação do intruso um circuito fechado de TV pode ser útil, este circuito necessariamente não estará sendo monitorado constantemente mas sim coletando evidências visuais de alguns ponto, que serão úteis para identificação do intruso, mas este circuito fechado de TV possui pouco valor para ativar um alarme, desta forma podemos concluir que um sistema de segurança depende da combinação de vários métodos.

Mas sobre o ponto de vista das evidências procuramos elementos para que possamos demonstrar a ocorrência de uma intrusão e a identificação do intruso, para isso devemos incluir vários tipos de logs:

- Log dos sistemas
- Log de auditoria
- Log de aplicações
- Log da rede

Devemos agrupar todos este dados de forma a permitir uma análise fácil e entendimento claro, estes são os dados derivados.

5.4 Preservando as Evidências

A primeira atitude a ser tomada no tocante a preservação das evidências é a realização de uma cópia do disco rígido e dos discos flexíveis, deve ser realizada uma copia de espelhamento de bits, ou seja, um bit stream backup.

Outra questões fundamental em relação as evidências é sua autenticidade. Os advogados de defesa certamente vão questionar a veracidade de qualquer prova da acusação. Isso significa que apenas o fato de ter todos os logs impressos e apresenta-los perante a corte onde alguém esta sendo acusado de invadir uma rede pode ser inútil.

Assim, é recomendável que ao dar início a investigação de incidentes de segurança providenciar um caderno para cada um dos membros da equipe e orienta-los a anotar todos os passo importantes realizados durante o processo

de investigação, ou seja, estes cadernos servirão como livro de registro.

Algumas das provas mais valiosas para a acusação será as anotações da equipe de investigação. Devera ser eleita uma pessoa para ser responsável pelo tratamento das evidências. Todos os membros deverão diariamente entregar os livros de registro a esta pessoa que terá como função tirar cópias das páginas assinar e datar cada página e em seguida guarda-las em um cofre até que chegue o momento de utiliza-las, este procedimento pode ser utilizado para outros processos como as listagens impressas.

Deve-se também realizar uma autenticação (CRC, MD5) dos arquivos e até mesmo do disco se possível de forma a garantir/provar que as evidências originais não foram alteradas.

No processo de documentação deve-se registrar todos os programas utilizados durante a investigação e é de fundamental importância que todos os programas utilizados sejam registrados, pois pirataria é crime.

Este são alguns dos procedimentos da metodologia forense para levantamento e preservação das evidências.

5.5 Evidências Passíveis de Apreciação pela Corte

As evidências devem satisfazer duas condições:

- **Aceitação** - devem estar em conformidade com certas regras legais;
- **Valor** – devem ser claras e convincentes perante a corte;

As evidências serão descartadas caso sejam coletadas incorretamente ou de forma ilegal.

Existem vários tipos de evidências que podem ser apresentadas à corte:

- **Real** – um objeto que pode ser levado para a corte e examinado no próprio local;
- **Testemunhal** – observações de alguém que estava presente e pode descrever os fatos perante a corte;
- **Documental** – registros que permitam a verificação da autenticidade do mesmo;
- **Parecer de Especialista** – opinião de algum especialista no assunto ou as conclusões deste especialista após realizar uma investigação;
- **Derivada** – desenhos, vidio, etc,. criados a partir das evidências primarias de forma a permitir o entendimento de certas conclusões;

As evidências geradas por uma ferramenta de IDS enquadram-se no tipo documental, mas requerem o testemunho da pessoa responsável pela configuração e coleta dos dados, de forma complementar um especialista pode ser solicitado para atestar o conteúdo, realizar explicações e interpretações. Podemos também apresentar o tipo derivado, através da utilização de gráficos,

desenhos, etc.

Durante um processo de crime eletrônico devemos demostrar as seguintes ações:

- Que um computador esta envolvido;
- Que o mesmo foi acessado;
- Que foi um acesso não autorizado;
- Que a pessoa que realizou o acesso sabia que o acesso não era autorizado;

Desta forma uma ferramenta de IDS é útil no tocante aos dois primeiros itens.

Outra questão interessante é que a maioria dos intrusos, senão todos, utilizam pseudônimos assim torna-se necessário a ligação do "apelido" utilizado na rede à identidade real da pessoa.

5 Conclusão

O assunto possibilita um vasto campo para estudo e pesquisas desta forma com sua modesta abrangência, este trabalho pretende servir como motivação ao leitor para busca de novos conhecimentos no campo da segurança da informação. Não houve aqui a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado reunindo conceitos fundamentais ao entendimento dos termos relacionados.

Agradecimentos

Meus sinceros agradecimentos a:

- Alexandra Droeber Basilio, mestre em direito pela UnB, pela sua ajuda inestimável no entendimento da legislação e dos termos bem como pela correção ortográfica.
- Ari Fazano, ..., pelo incentivo.
- Carlson Batista de Oliveira, mestre em ciências da computação pela UCB, pela leitura e sugestões.
- A todos que de alguma forma ajudam a construir este mundo virtual de uma forma sadia e ética.

Referências Bibliográficas

- Carlson e Cláudio, 1999

  OLIVEIRA, Carlson Batista; NEHME, Claudio Chauke, "Segurança pró-ativa e consciente para redes corporativas: avaliação de alternativas na Inteligência Artificial". Brasília: UCB, 1999. Disertação de mestrado.

- Parker, 1994

  Donn B. Parker. Demonstrating the elements of information security with threats. In Proceedings of the 17th National Computer Security Conference, pages 421-430, 1994.

- HeadyLugerEtAl, 1990

  Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla. The architecture of a network level intrusion detection system. Technical Report CS90-20, Department of Computer Science, University of New Mexico, August 1990.

- KumarSpafford, 1994

  Sandeep Kumar and Eugene H. Spafford. A pattern matching model for misuse intrusion detection. In Proceedings of the 17th National Computer Security Conference, pages 11-21, October 1994.

- Denning, 1987

  Dorothy E. Denning. An intrusion-detection model. IEEE Transactions on Software Engineering, 13(2):222-232, February 1987.

- CIDF site

  http://gost.isi.edu/cidf/

- Ptacek e Newsham, 1998

  Ptacek, Thomas H.; Newshan, Timothy N., "Insertion, Evasion, and Denial os Service: Eluding Network Intrusion Detection", 1998.

- IDS page

  http://www.cs.purdue.edu/coast/intrusion-detection/

- MICHAELIS, 1998

  Moderno dicionário da língua portuguesa.

O que você achou deste Artigo ?

Qualidade: Excelente Medio Fraco

Abordagem do Assunto: Objetiva Extensa Reduzida

Comentário:

Enviar Limpar