Metodologia para validar IPS's de código-fonte aberto

Marco Antônio S Trentin[1], Gustavo S Linden[1], Tomás Damo Zandoná[1]

[1]Instituto de Ciência e Geociência – Universidade de Passo Fundo (UPF)

trentin@upf.br, {40579,43999}@inf.upf.br

Resumo. *O presente trabalho tem por objetivo descrever uma metodologia para realizar testes com ferramentas IPS (Intrusion Prevention Systems). Essas ferramentas são mecanismos que são implementados como* gateways *(*in-line*) em uma rede de computadores para receber, analisar e encaminhar o tráfego para o seu destino. A análise é feita através da procura por pacotes que contenham assinaturas de ataques aos computadores da rede. Como se trata de uma nova tecnologia é necessário determinar métricas para avaliar os IPS que estão surgindo no mercado. Da mesma forma como acontece com os IDS's (Intrusion Detection Systems), não é uma tarefa fácil determinar métricas concretas para avaliar os IPS.*

Introdução

A demanda por segurança na comunicação de dados através de redes de computadores nasceu junto com a Internet. Apesar da possibilidade de garantir segurança na comunicação de dados não é sempre possível garantir a utilização correta de serviços e protocolos. Mesmo aplicando um processo rígido de gerenciamento de segurança, não é possível garantir uma segurança absoluta. Uma pessoa pode obter acesso a informações da qual ela não possui acesso através da exploração de falhas encontradas em protocolos e aplicativos.

É para garantir que essa necessidade por segurança seja atendida que proponho esse trabalho. Esse trabalho pretende determinar uma metodologia para a realização de testes em ferramentas que tem por objetivo evitar invasões IPS (Intrusion Prevention Systems). No primeiro capítulo serão vistos conceitos para o entendimento de ferramentas IPS's. A seguir (segundo capítulo), foi definida uma metodologia para os testes que foram aplicadas no terceiro capítulo.

1. IPS

IPS (*Intrusion Prevention System*) é uma ferramenta que visa evitar que os computadores sejam invadidos. Os IPS's foram projetados e desenvolvidos ainda na década de 60 quando os computadores eram grandes *mainframes* com vários usuários conectados simultaneamente. A idéia era previnir que os usuários desses *mainframes* pudessem obter acessos indevidos, para isso eram feitos controles de acesso. Esses controles eram feitos dentro do próprio computador, por isso são chamados de IPS's de *host*[1] (que serão vistos mais adiante). Com o surgimento da Internet a idéia de proteger o acesso indevido a dados permaneceu, porém os computadores mudaram de *mainframes* para servidores. O número de computadores dentro de uma organização cresceu de um *mainframe* e vários terminais para dezenas ou até centenas de PC's. A tarefa de implementar controle de acesso

[1] Tipo de IPS com o funcionamento baseado em um computador.

em cada um desses computadores tornou-se muito complicada. Por isso surgiu a idéia de implementar um IPS de rede, para evitar que todos os computadores de uma rede possam ser alvo de invasão sem acrescentar muita complexidade na instalação e manutenção.

Existem várias definições para o uso do termo IPS. Alguns vendedores de produtos de segurança definem seus produtos como IPS, mesmo sem que eles possuam as características necessárias para um sistema de IPS. A definição genérica pode ser descrita como um IPS sendo: "qualquer sistema que evite que um ataque a um computador ou rede seja bem-sucedido". Porém essa frase não está completamente certa, não é apenas isso, porque um *firewall* e outros dispositos também fazem isso. Para um sistema ser considerado um IPS é necessário que ele aplique algoritmos avançados de detecção de ataques e, após detectar, evitar que o ataque se concretize.

1.1. Funcionamento

A estrutura do IPS encontra-se organizada em módulos. O esquema de funcionamento de um IPS é explicado na figura 1. Basicamente o IPS recebe um pacote, analisa, encaminha/bloqueia o pacote.

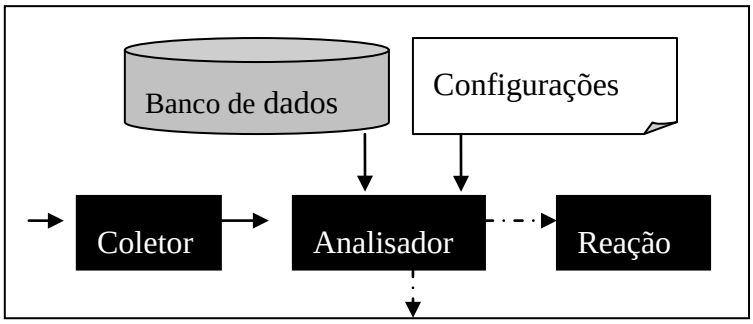

Figura 1. Esquema do funcionamento de um IPS

O IPS recebe o pacote através de um módulo designado coletor. O módulo coletor se encarrega de enviar o pacote para outro módulo, o analisador. O analisador, de posse do pacote, determina, quais as informações do banco de dados deverão ser consultadas. Isso ocorre através da análise do arquivo de configuração. Com base nas informações do banco de dados e características encontradas no pacote, o analisador faz uma comparação para determinar se o pacote é um ataque ou não. Se for constatado que o pacote constitui um ataque então uma reação é tomada, caso contrário o pacote é encaminhado ao seu destino. A reação pode ser baseado nas informações contidas no banco de dados ou pré-definidas no arquivo de configuração.

1.2. Falsos Alarmes

Em IDS de rede é comum encontrar informações sobre falsos positivos ou falsos negativos. Com um IPS de rede (visto adiante) não é diferente. A maneira como são implementadas essas ferramentas abrem brechas para a análise errônea dos pacotes da rede. Existem algumas situações que podem ser encontradas na detecção de um ataque:

Tabela 1. Definições das detecções de um IPS

Ocorrência de detecção	SO vulnerável	Existência de ataque	Definição
Sim	Sim	Sim	Detecção correta
Sim	Não	Sim	Ataque sem sucesso
Sim	Não/Sim	Não	Falso positivo
Não	Sim	Sim	Falso negativo
Não	Não	Sim	Falso negativo
Não	Não/Sim	Não	Tráfego normal

Um IPS possui o problema da situação descrita no quadro acima como falso positivo, ou seja, quando não ocorreu nenhum ataque. Isso ocorre quando não há um ataque, porém o sistema afirma que um pacote recebido por ele é um ataque. A situação ocorre quando pacotes são forjados para caracterizar um ataque quando na verdade não há nenhum. Um artigo de PATTON, et al (2001, p. 3-5) descreve como podem ser forjados pacotes para o IDS *Snort*, e consequentemente qualquer IPS que for baseado no seu código-fonte. Como alguns IPS's são implementados nesse algoritmo essa situação termina no bloqueio de um tráfego normal da rede. Se isso ocorrer o IPS irá detectar ataques que não existem. Como os pacotes são forjados o endereço de origem também será forjado, essa situação poderá acarretar um DoS do tráfego normal da rede. Esse problema deve ser resolvido com 100% de eficiência para não implicar na eficiência de IPS.

Os ataques sem sucesso onde o sistema não é vulnerável só serão um problema se o IPS enviar alertas sobre ataques, sobrecarregando o administrador de redes de informações. O sistema em si ou os IPS's não serão afetados de forma alguma. Se o sistema bloquear o ataque a situação não será um problema. Porém o registro das informações desses eventos são necessárias, uma vez que o atacante pode obter sucesso após algumas tentativas. Conhecer quem está atacando a rede é um fator determinante para tomar medidas de precaução ou reação.

Falsos negativos são ataques que ocorreram e que o IPS não detectou. Os falsos negativos não são tão frequentes, isso porque os IPS são implementados de forma que todo o tráfego será analisado, apenas se ocorrer um DoS no IPS ele irá deixar de analisar os pacotes. Quando o algoritmo é baseado em assinaturas essa situação não ocorre tão facilmente, apenas quando descrita acima ou então quando não são ataques conhecidos. Como os IPS's baseados em anomalias e comportamento ainda estão amadurecendo essa situação pode ocorrer em maiores proporções.

Falso negativo constitui um problema para o IPS quando o ataque ocorreu em um SO vulnerável e não houve detecção. Essa situação é inaceitável, uma vez que um ataque com essa consequência irá resultar em uma falha na segurança que pode comprometer toda a rede onde o IPS funciona.

2. Definição da metodologia para a avaliação de IPS's

A seguir estão descritas algumas métricas para obter subsídios para a definição da metodologia deste trabalho. Essas métricas são utilizadas para determinar as características presentes nos testes realizados. As métricas utilizadas para os testes são descritas abaixo.

2.1. Cobertura

Esta medida serve para determinar quais ataques o IPS é capaz de detectar e evitar o sucesso (isso em uma situação ideal) de um ataque. Para sistemas baseados, na maior parte, em assinaturas essa

medida é o número total de assinaturas que o IPS contém dentro do seu banco de assinaturas. Para sistemas que não são baseados em assinaturas a tarefa não é tão simples. Uma forma seria diante de todos os ataques conhecidos quais o IPS é capaz de detectar. Esta tarefa pode ser exaustiva, além de não comprovar a eficiência em uma situação real, apenas em uma situação ideal.

2.2. Probabilidade de ocorrência de falsos alarmes

Essa medida determina a taxa de falsos positivos ou negativos produzidos em um determinado período de tempo.

Um falso positivo pode ser medido através da subtração do número de ataques que o IPS evitou com o número de ataques que foram enviados para o ataque. Essa taxa cresce à medida que assinaturas deixam de ser específicas para abranger um número maior de variações de um determinado ataque.

O falso negativo pode ser obtido através da subtração do número de ataques enviados ao IPS com o número de ataques detectados. Essa medida testa ataques enviados ao IPS inseridos em conjunto com tráfego normal que não deverão caracterizar ataques.

2.3. Probabilidade de detecção

Essa medida é a taxa de ataques detectados corretamente em um determinado ambiente em um período de tempo. Essa medida é dependente dos ataques utilizados no teste. Uma forma de testar é utilizar os ataques que possuam maior ocorrência na Internet. Essa medida é relacionada com a taxa de falsos positivos, uma vez que o IPS pode ser configurado para evitar falsos positivos diminuindo a taxa de detecção ou vice-versa.

2.4. Resistência a ataques dirigidos ao IPS

Essa medida consiste na resistência que um IPS possui quando os ataques são dirigidos a ele a fim de evitar seu correto funcionamento. Os tipos de ataques dirigidos ao IPS podem ser:

- o envio de uma grande quantidade de pacotes que não caracterizem ataques pode exceder a capacidade de processamento do IPS. Com muito tráfego para ser processado o IPS pode deixar de encaminhar os pacotes para o seu destino e causar um DoS;

- pacotes desenvolvidos especialmente para enquadrar em diversas assinaturas do IPS entopem o administrador de registros de ataques;

- envio de pacotes ao IPS, contendo dados que exploram uma vulnerabilidade do mecanismo de processamento. Esse ataque só é bem sucedido se for encontrado em algum IPS um erro de programação.

2.5. Capacidade de gerenciar altas bandas de rede

Essa medida visa demonstrar como um IPS irá funcionar dada uma crescente largura de banda de rede. Esse teste permite determinar a quantidade máxima de pacotes que o IPS irá analisar. Levando em consideração alguns quesitos como tamanho do pacote e tipo de tráfego. O ideal é utilizar tráfego real ao invés de um gerador de pacotes. Porém se for o caso o teste em questão não poderá ser reproduzido.

3. Ambiente dos testes

Uma vez visto as métricas que foram definidas anteriormente (capítulo 2), é possível, agora, determinar o ambiente e as condições que irão ser aplicadas aos testes.

O ambiente consite em um computador (X) que envia pacotes para um terceiro computador (Y) através de um *gateway,* que é o IPS. Assim, todo o tráfego passa pelo IPS. O esquema de infraestrutura da rede usada para testes pode ser visto na figura 2.

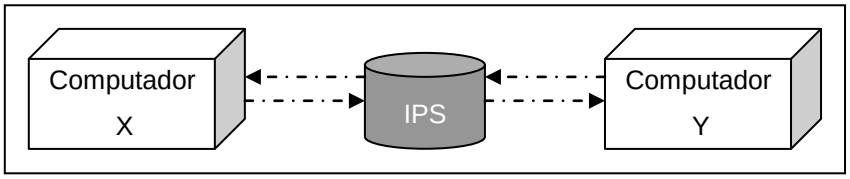

Figura 2. Esquema da infraestrutura da rede usada para testes

Como o processamento é um fator relevante para a análise dos pacotes, o computador mais rápido foi utilizado como IPS. Os computadores são interligados com placas de rede Ethernet a 10/100Mbps. O IPS utiliza duas placas de redes para efetuar a interligação de duas redes de computadores. O computador onde o IPS está rodando é, na medida do possível, dedicado apenas para a ferramenta. Quando os testes foram realizados todos os serviços não necessários foram desativados. Os outros computadores estão rodando aplicativos para gerar, gerenciar e analisar o fluxo dos pacotes. O computador X é responsável pelo envio de pacotes, enquanto que o computador Y recebe esses pacotes e analisa-os.

A segunda etapa é a escolha dos IPS's analisados conforme a metodologia descrita anteriormente. Nesse estudo foram avaliados o IPS *Snort_inline* e o *Hogwash.*

3.1. Snort_inline

A ferramenta *Snort_inline* exige que um *firewall* seja instalado, assim, foi configurado no mesmo computador, para que os pacotes possam ser encaminhados para o *Snort_inline*. O *firewall* utilizado é o *Iptables*, que é o mais utilizado pelo Linux, devido ao fato de acompanhar o SO. Ele encaminha os pacotes da placa de rede para o módulo *ip_queue*, que posteriormente o repassa para o *Snort_inline*. O *ip_queue* permite que os pacotes de rede sejam enviados da placa de rede para um software, que no caso é o *Snort_inline*. O módulo *ip_queue* pode ser encontrado em conjunto com o *Iptables* e deve ser inserido no *kernel* do sistema para que o IPS possa funcionar.

Em relação ao item da seção 2.1. o *Snort_inline* em sua versão atual, 2.1.0, é capaz de detectar 1.986 ataques diferentes, sendo que desses 1.622 estão já habilidados para serem detectados. O restante são ataques que precisam ser selecionados para que possam ser analisados.

Para realizar os testes da seção 2.2 foi necessário coletar tráfego de rede. O tráfego utilizado para a realização dos testes foi conseguido utilizando a ferramenta tcpdump[2] para coletar todos os pacotes da rede para serem posteriormente utilizados através da ferramenta tcpreplay[3]. Os pacotes coletados foram gravados em um arquivo chamado de "*logs"* através da utilização do parâmetro "-

[2] Essa ferramenta funciona como um sniffer e é comumente utilizada para detectar problemas encontrados na comunicação entre os computadores. Todos os pacotes enviados pelo computador X para o Y foram gravados no arquivo logs para o reenvio posterior utilizando a ferramenta Tcpreplay

[3] Essa ferramenta permite o reenvio de pacotes previamente gravados em um arquivo. Dessa forma, o tráfego é igual ao tráfego que foi enviado do computador X para o Y e vice-versa. Os pacotes podem ser enviados a qualquer velocidade e podem ter o seu destino alterado.

w". Eles são pacotes coletados da comunicação do servidor ftp (computador Y) com o cliente (computador X). Eles não representam ataques. Se um desses pacotes for caracterizado pelo *Snort_inline* como um ataque, estaria aconetecendo um falso positivo (seção 1.2) e seria bloqueado. Esse situação representa a interrupção errônea do tráfego normal e por isso não deve ocorrer.

Os pacotes TCP/IP (do servidor ftp) que foram enviados ao computador Y pelo computador X foram retransmitidos através da ferramenta Tcpreplay 2.1.0, com uma velocidade máxima real de 10 Mbps, mesmo com as duas placas de rede nas extremidades funcionando em modo de 100 Mbps full-duplex. Essa foi a capacidade máxima de gerenciamento de tráfego encontrada nos testes da seção 2.5.

Como todas as placas de rede estavam configuradas em 100Mbps e o cabo de rede ethernet suportava esse valor, alguns testes foram feitos para determinar o porque da velocidade de transmissão a 10Mbps ao invés de 100Mbps.

Um versão anterior do tcpreplay foi utilizada no computador Y para transmitir os pacotes ao computador X para verificar a velocidade máxima da transmissão. Essa versão da ferramenta enviou os pacotes através da rede ethernet a uma velocidade média de 65Mbps. Quando foi utilizada a ferramenta ethereal no computador X foi possível verificar que um número inferior a 10% dos pacotes estavam realmente chegando ao seu destino. Quando foi reduzida a velocidade da transimssão dos pacotes, os mesmos começaram a chegar ao seu destino em um maior número, porém não atingiu um taxa superior a 70% do número total de pacotes enviados.

A velocidade máxima atingida na comunicação foi de 10 Mbps, uma razão possível poderia ser devido ao protocolo TCP da pilha TCP/IP exige uma garantia de que os pacotes foram recebidos (ACK), o que pode ser responável pela redução da velocidade final da comunicação.

Para simular os ataques aos computadores da rede, pacotes foram forjados com o auxílio da ferramenta hping2. Essa ferramenta envia qualquer tipo de pacote TCP/IP previamente configurado para qualquer computador na rede. Os pacotes podem ser forjados com qualquer conteúdo e enviados para qualquer endereço, protocolo e porta. A ferramenta permite o envio de dados através da placa de rede de um computador para outro.

Para que os pacotes criados através da ferramenta hping2 sejam considerados como um ataque, é necessário conhecer e compreender uma assinatura de um ataque definido nos IPS's e criar um pacote que se enquadre completamente nessa assinatura.

Para realizar os testes descritos na seção 2.2, os pacotes contendo ataques foram manipulados. Algumas mudanças foram realizadas na estrutura do pacote e outras na forma de envio (a divisão do ataque em diversos pacotes menores). Para verificar a correta "montagem" (*reassembly*) dos pacotes, a ferramenta *ethereal* foi executada no computador de destino (Y). Isto possibilitou verificar quantos pacotes chegaram, a sua ordem e o seu conteúdo. Essa ferramenta possibilitou verificar ainda quais pacotes o IPS efetivamente bloqueou e quais o IPS permitiu a passagem. Os falsos alarmes detectados são descritos a seguir.

Os falsos negativos, encontrados durante a realização dos testes da seção 2.2, ocorrem quando os pacotes que constituem o ataque são divididos em pacotes menores do que 16 bytes (campo de dados). Essa situação pode ser evitada se o valor do tamanho mínimo dos pacotes for alterado.

Pacotes com o tamanho maior do que 65.000 também não são analisados pelo IPS o que permite a inserção de ataques em pacotes com o tamanho excedente a esse valor (outra situação de falso negativo). Essa situação pode ser melhorada (aumentando o tamanho máximo para um

pacote), mas acredito que não seja possível evitá-la completamente porque não é possível aumentar o *buffer* para o tamanho dos pacotes infinitamente. O valor do tamanho máximo do pacote é um deficiência do módulo *ip_queue* e não do *Snort_inline*.

Como foi dito anteriormente, a manipulação dos pacotes permitiu determinar a existência de falsos positivos. Quando um pacote é forjado já existe uma situação de falso positivo. A existência de falsos postivos não é uma falha grave em um IPS, uma vez que, se o ataque não for registrado, ele apenas irá gerar mais tráfego sem conseguir atingir o seu alvo ou o próprio IPS. Os pacotes forjados não foram detectados, pelo *Snort_inline,* como ataques. Isso, porque os pacotes não estão estabelecidos como uma conexão ativa e por esse motivo serão descartados pelo computador alvo.

O *Snort_inline*, em suas últimas versões, não apresentou nenhuma vulnerabilidade que possa ser explorada por um possível atacante (remoto). A única ocorrência de vulnerabilidade está em um ataque de DoS, porém a ferramenta não foi projetada para evitar esse tipo de situação.

3.2. Hogwash

O segundo IPS avaliado nessa pesquisa foi o *Hogwash*[4]*.* Esse IPS também é baseado em assinaturas que são as mesmas utilizadas pelo IPS *Snort_inline*.

O IPS Hogwash está configurado com um padrão de detecção de 106 diferentes assinaturas de ataques. Este número é muito menor se comparado com o IPS *Snort_inline*, porém essas assinaturas são apenas aquelas que garantem o acesso ilegal a um computador. No caso do *Snort_inline* as assinaturas são as mesmas dos IDS *snort*, apenas com a modificação para que os pacotes sejam descartados e não para apenas alertar, como é o caso do IDS. Muitas dessas assinaturas são úteis para um IDS, uma vez que não se tratam de invasões e sim de mal uso ou ações suspeitas, e não de ataques com invasão ou maiores prejuízos.

O tráfego de rede para a realização dos testes é o mesmo utilizado para testar a ferramenta *Snort_inline.*

O IPS deve estar localizado em *gateways* que separam duas redes. É necessário determinar qual a placa de rede possui acesso a rede interna e qual a placa de rede possui acesso a rede externa (a rede de onde são originados os ataques). O Hogwash também trabalha com o conceito de roteamento de pacotes. Existem duas maneiras de se trabalhar com esse IPS: uma delas é utilizando *ip_forwarding*[5], o que em sua configuração padrão não possibilitou o bloqueio dos pacotes contendo ataques em tempo hábil (antes que o pacote seja encaminhado para o seu destino). Outra forma é sem a opção de *ip_forwarding* habilitada, o que torna o próprio IPS o responsável pela transmissão dos pacotes entre as redes que ele intermedia. Através de testes foi possível determinar que o roteamento de pacotes, utilizando o IPS *hogwash*, não está operante na versão 0.4, nem na versão 0.5 (útlima versão). No cronograma[6] de desenvolvimento encontrado na página do hogwash é indicado que essa função e outras ainda estão sendo implementadas. Desta forma, ele atua apenas como um IDS e não como um IPS.

Os ataques utilizados foram os mesmos definidos para o *Snort_inline* (do computador X para o computador Y). O IPS não foi capaz de evitar que o pacote contendo um ataque chegasse ao seu destino, uma vez que o IPS não é capaz de realizar o roteamento dos pacotes independentemente. É necessário utilizar a função de *ip_forwarding* do *kernel* do Linux para realizar o roteamento dos

[4] O IPS *Hogwash* é um software livre de código-fonte aberto, disponível em: http://hogwash.sourceforge.net/
[5] Este é um módulo do kernel responsável por transmitir os pacotes de rede de uma rede onde uma das placas de rede do sistema possua acesso para outra rede onde outra placa de rede possua acesso.
[6] http://hogwash.sourceforge.net/oldindex.html

pacotes, o que resulta na transmissão dos pacotes para o seu destino antes que o IPS tenha chance de analisá-los e definitivamente bloqueá-los. Porém o IPS detectou positivamente os pacotes contendo ataques, apesar que não poder efetivamente bloqueá-los.

Em um segundo momento o pacote contendo o ataque foi enviado ao mesmo tempo em que um tráfego de rede intenso, 9 Mbps, estava sendo enviado para a interface de rede externa do IPS. O IPS foi incapaz de detectar e bloquear os pacotes contendo os ataques. Após foi verificado se o pacote havia realmente chegado ao seu destino. Como dito anteriormente, o IPS não pode bloquear os pacotes contendo os ataques. Para isso foi utilizado novamente a ferramenta *tcpdump*, que confirmou a chegada dos pacotes contendo os ataques ao seu destino.

Os pacotes contendo os ataques em alguns casos chegaram ao seu destino (ocorrência de uma falha no IPS, falso negativo) e em outros o pacotes não chegou ao seu destino, mas não devido a detecção e bloqueio do IPS e sim porque o tráfego intenso destinado ao IPS não permitiu que os pacotes fossem analisados e então ocorreu um DoS quando o IPS não foi capaz de enviar alguns pacotes de rede ao seu destino. Em ambos os casos, o IPS não foi capaz de detectar a existência ou ocorrência de um ataque em andamento.

Então pode-se determinar que o IPS Hogwash é suceptível a ataques na rede de computador que ele está defendendo quando o IPS está sob o alvo de intenso tráfego de rede. Isso não garante a possibilidade de um ataque bem sucedido mas também não garante que o IPS irá agir corretamente, evitando os ataques. Essa situação enquadra-se nos ataques dirigidos ao IPS e também na quantidade de tráfego que o IPS é capaz de suportar, nesse caso inferior a 9 Mbps. Quando o IPS deixa o tráfego passar, ele falha em sua função que é o bloqueio da situação. A segunda medida nesse caso é determinar porque o IPS funciona corretamente com o seu bloqueio em algumas situações? A resposta pode ser determinada através da subtração do número de pacotes enviados com o número de pacotes recebidos, se o valor for superior a 0 o IPS deixou de atender os seus requisitos e entrou em uma situação de DoS.

Conclusão

Este trabalho revelou alguns aspectos pertinentes ao avanço da tecnologia. A proposta de IPS é uma evolução no campo de ferramentas de segurança, pois pretende pôr um fim na insegurança de computadores. Porém não deixa de ser uma afirmação pretenciosa. Conforme o estudo, percebeu-se que IPS bem como IDS ainda não são ferramentas definitivas para resolver o problema de ataques a computadores.

Como o objetivo não era avaliar comparativamente e sim quantitativamente, não é possível definir qual dos dois IPS's avaliados é o melhor e sim destacar pontos positivos e negativos sobre cada um deles. O que é possível descrever nesse momento é o estado de vulnerabilidade em que se encontram esses dois IPS, porém não há dúvidas quanto a utilidade que uma ferramenta dessas pode possuir em um futuro próximo. A metodologia mostrou-se capaz de validar ou não a eficiência dos IPS's em questão e também novas ferramentas que irão surgir.

O primeiro aspecto quanto aos ataques que essas ferramentas são capazes de detectar, ambas são capazes de detectar qualquer ataque que possua características únicas como é o caso da grande maioria dos ataques conhecidos. O problema encontrado são ataques que ainda não são conhecidos, esses os IPS's não são capazes de detectar. Durante testes realizados nesta pesquisa, houve um único caso em que o IDS *Snort* conseguiu detectar um ataque nunca antes visto, mas a situação só foi possível porque a assinatura do ataque em questão era a mesma assinatura de um ataque previamente conhecido.

O único IPS que obteve sucesso quanto a evitar ataques foi o *Snort_inline* visto que o hogwash não possui ainda um mecanismo para que os pacotes da rede sejam retransmitidos por ele.

Os IPS's aqui analizados não são capazes de gerenciar com eficiência todo o tráfego de todos os serviços de uma rede de computadores, porém não existe obstáculos para a sua utilização em redes de computadores com pouco tráfego ou então para o gerenciamento de tráfego de poucos serviços o que iria diminuir sua carga.

A tecnologia, atual, ainda não é uma opção aceitável para a maioria das empresas, uma vez que possuem diversas situações que não são adequadamente tratadas. Essa tecnologia não deve, no entanto, ser completamente descartada. Algumas funções e até mesmo um evolução pode proporcionar a utilização dessa tecnologia nas empresas. No entanto os IPS atuais são eficientes para evitar-se a propagação de *worms* e proteger vulnerabilidades conhecidas em serviços indispensáveis para uma rede de computadores.

No início da realização deste trabalho, a eficiência do IPS *Snort_inline* deixava a desejar. Porém a situação atual da ferramenta está se encaminhando para estabelecer a tecnologia como uma forma de garantir a segurança de redes de computadores. O próximo passo é possibilitar que essas ferramentas sejam capazes de detectar apenas por si só, sem a intervenção de um ser humano para determinar o que é e o que não é um ataque.

Referência Bibliográfica

DENISH, Sequeira. **Intrusion Prevention Systems –** Security's silver bullet? Disponível em: <http://www.sans.org/rr/papers/30/366.pdf>. Acesso em: 10 de ago. 2003.

DESAI, Neil. **Intrusion Prevention Systems:** the next step in the evolution of IDS. Disponível em: <http://www.securityfocus.com/infocus/1670>. Acesso em: 15 de set. De 2003.

FRATTO, Mike. **Network-Based Intrusion-Prevention System (NIPS).** Disponível em: <http://www.nwc.com/1417/1417p1.html>. Acesso em 07 de out. de 2003.

LISSBERGER, David A. **NETWORK CLOAKING ™ AS A DEFENSIVE STRATEGY FOR INTRUSION PREVENTION SYSTEMS.** Disponível em: <http://sentinel.econet.com/NETWORK_CLOAKING.pdf>. Acesso em: 25 de set. de 2003.

PATTON, Samuel. YURCIK, William. DOSS, David. **An Achilles' Heel in Signature-Based IDS:** Squealing False Positives in SNORT. Disponível em: <http://www.raid-symposium.org/Raid2001/papers/patton_yurcik_doss_raid2001.pdf>. Acesso em: 01 de out. de 2003.

PESCATORE, John. **Enterprise Security Moves Toward Intrusion Prevention.** Dinsponível em: <http://www.csoonline.com/analyst/report1771.html>. Acesso em: 15 de out. de 2003.

PTACEK, Thomas H. NEWSHAM, Thimothy N. **Insertion, Evasion, and Denial of Service: Eluding Network Intrudion Detection.** Disponível em: <http://www.insecure.org/stf/secnet_ids/secnet_ids.html>. Acesso em 03 de jul. de 2003.

PUKETZA, Nicholas J. et al. **A Methodology for Testing Intrusion Detection Systems.** Disponível em: <http://seclab.cs.ucdavis.edu/papers/tse96.pdf>. Acesso em: 05 de nov. de 2003.

RANUM, Marcos J. **Coverage in Intrusion Detection Systems.** Disponível em: <http://philby.ucsd.edu/~cse291_IDVA/papers/orig_names/Coverage-in-IDS-White-Paper-final.pdf>. Acesso em: 03 de nov. de 2003a.

STREBE, Matthew. **Firewalls.** São Paulo: Makron Books, p. 411, 2002.

WILKISON, Michael. **How to evaluate Network Intrusion Detection Systems?** Disponível em: <http://www.sans.org/resources/idfaq/eval_ids.php>. Acesso em: 01 de nov. de 2003.

MELL, Peter. et al. **An Overview of Issues in Testing Intrusion Detection Systems**. Disponível em: <http://csrc.nist.gov/publications/nistir/nistir-7007.pdf>. Acesso em: 15 de ago. de 2003.