Análise das ferramentas de IDS SNORT e PRELUDE quanto à eficácia na detecção de ataque e na proteção quanto à evasões

Julio Steffen Junior[1], Eduardo Leivas Bastos[2]

[1]Bacharel em Ciência da Computação, e-mail: steffen@tca.com.br; [2]Prof. Esp. Ciências da Computação, ICET/Feevale, e-mail: elbastos@feevale.br.

Resumo

A necessidade de proteger as redes de computadores contra ataques cada vez mais complexos e dinâmicos deu origem a um conjunto de ferramentas denominadas de Sistemas de Detecção de Intrusão (Intrusion Detection Systems - IDS). Tais ferramentas auxiliam na detecção de ataques, alertando e realizando ações que podem impedir que um ataque seja concretizado. Este trabalho tem como objetivo apresentar duas destas ferramentas e avaliá-las quanto ao comportamento apresentado em face a diferentes ataques de domínio público.

Palavras-chave

Segurança de redes; IDS; detecção de intrusão; técnicas de evasão; Snort; Prelude.

Abstract

In order to protect computer networks from attacks, many security tools have been developed. One class of these tools is usually called Intrusion Detection Systems (IDS), which are tools able to detect possible attacks, to produce specific alerts and to take corrective actions in order to prevent that the attack really takes place. This work has as main goal to present a study about IDSs and to perform some experiments with two different IDS tools. The experiments are oriented to evaluate the behavior of these IDSs tools when they are exposed to different attacks generated by means of some tools available in the Internet.

Key words

Network security; IDS; intrusion detection; evasion techniques; Snort; Prelude.

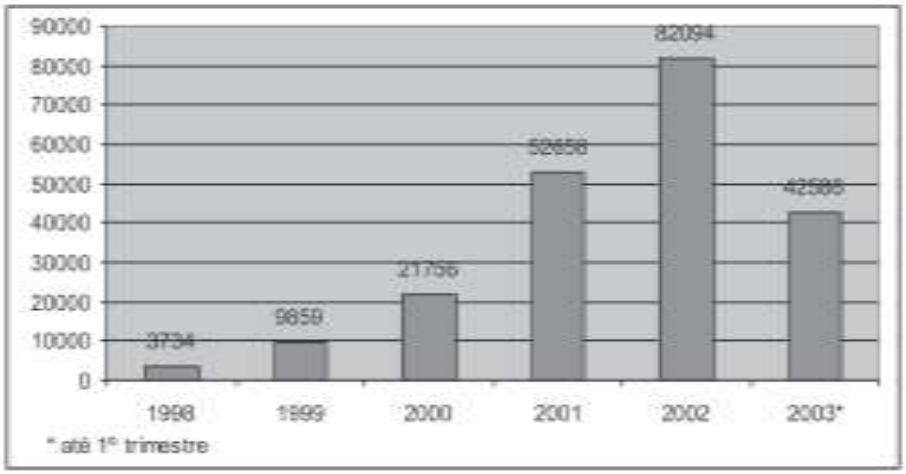
Introdução

A segurança é uma das maiores preocupações enfrentadas atualmente pelos administradores de redes. Manter a empresa longe de ataques é um desafio cada vez maior para evitar o roubo de informações e a paralisação de sistemas. Somente um *firewall* já não garante que a rede esteja 100% segura. A monitoração contra ataques e intrusões, deste modo, tornou-se ponto chave na estrutura de segurança de uma rede de computadores, auxiliando o administrador da rede a prevenir ataques e a agir quando um ataque é iniciado ou detectado.

Segundo estatísticas do *Computer Emergency Response Team* (CERT), os ataques às redes têm crescido substancialmente a cada ano, conforme mostra a tabela 1. Um dos fatores principais para este crescimento é a sofisticação das ferramentas de ataques disponíveis gratuitamente na Internet. Como conseqüência deste fato, houve um significativo aumento no número de pessoas que se tornaram capazes de iniciar um ataque. [ALLEN, 2000].

Os Sistemas de Detecção de Intrusão (*Intrusion Detection Systems* - IDS) são ferramentas cuja finalidade é executar uma monitoração da rede e tentar impedir que o ataque cumpra com seus objetivos.

Tabela 1 – Aumento do número de ataques



Fonte:CERT/CC Statistics 1988-2003

O IDS pode ser visto como mais uma ferramenta para reforçar a política de segurança da informação de uma empresa. A escolha de qual ferramenta utilizar é uma decisão difícil de ser tomada. Basear-se apenas no custo é minimizar outros aspectos relevantes da questão, tais como: funcionalidades oferecidas, facilidade de configuração e gerenciamento, eficácia na detecção, entre outros.

Esse artigo aborda as principais características de um sistema de intrusão e tem como objetivo descrever uma comparação realizada entre duas ferramentas de IDS de código-aberto (*open source*), no que diz respeito à eficácia na detecção de diversos tipos de ataques.

A Seção 1 aborda, de maneira clara e objetiva, como um IDS funciona, bem como os tipos, métodos e problemas encontrados em uma ferramenta deste tipo. A Seção 2 apresenta as duas ferramentas utilizadas nos testes. A Seção 3 comenta os testes realizados e aborda os resultados obtidos.

1. Sistemas de Detecção de Intrusão – IDS

Detecção de intrusão é um processo de coleta de informações que procura identificar sinais de que um ataque está iniciando ou ocorrendo. "(...) a detecção de intrusão da rede permite identificar e reagir a ameaças contra o seu ambiente (...)" [NORTHCUTT, 2002].

Um IDS é composto basicamente por dois dispositivos principais: o console de comando e o sensor. "O sensor é o dispositivo responsável pela coleta de informação para análise de descoberta de uma invasão" [CROTHERS, 2003]. O console de comando tem como função permitir o controle do IDS, monitorar o estado do sensor e processar os alertas enviados pelo sensor [PROCTOR, 2001].

O IDS pode trabalhar basicamente de duas formas: uma delas é analisando o tráfego da rede (*IDS baseado em rede*). Nesta configuração, o sensor analisa todos os pacotes que circulam pelo segmento de rede independente de qual o destino do pacote. A outra forma é analisando uma determinada máquina à procura de códigos maliciosos para identificar sinais de que um ataque está sendo iniciado (*IDS baseado em host*).

Quanto ao método de detecção dos ataques, o IDS pode ser classificado como *IDS baseado em assinatura* ou *IDS baseado em anomalia*. O IDS baseado em assinatura trabalha procurando regras pré-estabelecidas no tráfego da rede. Quando é encontrado algum código na rede que esteja descrito em alguma regra, um alerta ou evento é gerado permitindo uma ação defensiva [NORTHCUT, 2002]. Já o IDS baseado em anomalia possui uma base de dados representativa do comportamento normal da rede. A partir desta base é que o sistema verifica o que é ou não permitido. Quando algum evento estiver fora deste padrão normal, um alerta é gerado.

É bastante comum a incidência de falsos positivos e falsos negativos em um IDS. O falso positivo ocorre quando um sensor classifica uma atividade normal na rede como sendo um ataque [NORTHCUTT, 2002]. O falso negativo ocorre quando um sensor não gera nenhum alerta em uma condição real de ataque [PROCTOR, 2001]. A ocorrência de falsos negativos é mais perigosa do que a de falsos positivos.

Outro problema que merece atenção especial são as técnicas de evasão. Essas técnicas consistem basicamente em métodos que procuram enganar o IDS de forma a fazer com que um ataque real passe desapercebido. Existem inúmeras técnicas de evasão disponíveis, e as formas de evitá-las têm recebido especial atenção por parte dos desenvolvedores de IDS. Um IDS vulnerável a este tipo de ataque torna-se ineficaz e pode comprometer toda a política de segurança da empresa.

2. Ferramentas utilizadas

Para a realização dos testes foram selecionadas duas ferramentas de IDS. A seleção foi baseada em critérios pré-estabelecidos (é importante definir requisitos e critérios condizentes com a estrutura da empresa onde o IDS será instalado). Um dos critérios definidos era que a ferramenta deveria possuir seu modelo de licença de *software* baseada na *GNU General Public License (GPL)*. As duas ferramentas selecionadas foram o Snort e o Prelude.

O Snort é um IDS baseado em rede amplamente utilizado pela comunidade Unix/Linux. Possui uma arquitetura simples, baseada em *plugins* que implementam basicamente as funções de captura de pacotes na rede, análise dos pacotes e geração de alertas. É um sistema leve, capaz de trabalhar em grandes redes e detectar uma grande variedade de ataques em tempo real. Seu sistema de detecção é baseado em assinaturas [CAMPELLO, 2002].

O Prelude é uma ferramenta de IDS híbrida, podendo trabalhar como um IDS baseado em rede ou como um IDS baseado em *host* ou ainda das duas formas ao mesmo tempo. Como o Prelude é composto por módulos, é possível instalar somente o módulo desejado e condizente com a necessidade [TRICAUD, 2002]. O Prelude, assim como o Snort, também possui seu sistema de detecção baseado em assinatura.

3. Análise prática

O objetivo desta análise foi verificar o funcionamento e o comportamento do IDS em um ambiente de rede simulado. Com esta análise, foi possível estudar melhor o funcionamento do IDS frente a diferentes tipos de ataques realizados.

As duas ferramentas foram submetidas aos mesmos ataques sob uma configuração *default*. Esta premissa foi levada em consideração para que se pudesse ter um estudo comparativo fiel entre as duas ferramentas. Após os testes, uma base de dados com uma análise comparativa entre as ferramentas foi gerada com a finalidade de demonstrar a eficiência na detecção dos vários ataques. Esta comparação não tem o intuito de definir qual das duas ferramentas é a melhor. Seriam necessários uma estrutura de testes com recursos mais sofisticados, maiores investimentos e um período de testes superior ao executado para a obtenção de resultados mais precisos.

Durante os testes, alguns itens foram observados em relação às ferramentas: qual o comportamento da ferramenta utilizando-se a configuração *default*, a quantidade de falsos positivos e falsos negativos gerados, a capacidade de detecção de técnicas de evasão e a capacidade de detecção sob diferentes níveis de utilização da rede.

Os testes foram executados em um laboratório exclusivamente montado para a ocasião. Todas as máquinas envolvidas nos testes foram preparadas e configuradas exclusivamente para os testes, de modo que não influenciassem nos resultados. A metodologia empregada definiu os seguintes parâmetros de teste: 1) tipos de ataques, 2) ferramentas utilizadas, 3) quantidade de ataques por ferramenta e 4) nível de tráfego injetado na rede.

Seguindo a metodologia, os testes foram divididos em três categorias [NSS GROUP, 2002]:

1. Reconhecimento de ataques: verifica a capacidade da ferramenta em detectar determinados tipos de ataques (*buffer overflows e exploits, denial of service,* ataques de HTTP, SMTP e FTP e ferramentas de *scanner*);

2. Desempenho: analisa a capacidade da ferramenta em detectar os ataques com diferentes taxas de utilização da rede;

3. Técnicas de evasão: verifica a capacidade da ferramenta em detectar as técnicas de evasão.

Cada ferramenta de IDS foi testada separadamente (somente uma ferramenta estava instalada na máquina em cada teste) para evitar possíveis influências mútuas nos resultados. Nas categorias 1 e 2 foram escolhidos sete ataques que foram executados sob três níveis de utilização da rede (0%, 25% e 75%). Cada ataque foi repetido dez vezes para cada ferramenta. Esta primeira avaliação procurou medir o grau de eficácia na detecção dos ataques sob vários níveis de utilização da rede. Nesta avaliação, também foi medido o índice de falsos negativos (ataques não detectados pela ferramenta). Na categoria 3 foram escolhidos dois aplicativos para a geração dos ataques de evasão: *Flagroute e Nikto*. O *Flagroute* utiliza três técnicas de evasão que foram executadas sob três níveis de utilização da rede (0%, 25% e 75%). Cada ataque foi repetido três vezes para cada ferramenta IDS. O *Nikto* utiliza quatro técnicas de evasão, que foram executadas para cada ferramenta IDS, sob três níveis de utilização da rede (0%, 25% e 75%).

Os ataques foram realizados individualmente, um após o outro, para garantir que o ataque detectado correspondesse ao respectivo ataque gerado. Todos os alertas de ataques apresentados na console de gerenciamento eram devidamente registrados e documentados para análise posterior. Antes de um novo ataque ser iniciado, o alerta anteriormente recebido era apagado.

A tabela 2 apresenta os resultados obtidos nos testes das categorias 1 e 2. É possível verificar que nenhuma das duas ferramentas obteve 100% de aproveitamento com taxa de utilização da rede em 0%. O esperado era que, com taxa de 0%, todos os ataques fossem detectados, pois não havia nenhum fator que pudesse contribuir para que as ferramentas falhassem ao detectar qualquer um dos ataques. Outro ponto importante é que os índices de detecção entre as duas ferramentas se alteraram sensivelmente quando os níveis de utilização de rede foram sendo modificados.

Tabela 2 – Reconhecimento de ataque e Performance

Ferramenta SNORT										Ferramenta PRELUDE									
Tráfego	0%			35%			75%			Tráfego	0%			35%			75%		
Ataque	G	D	%	G	D	%	G	D	%	Ataque	G	D	%	G	D	%	G	D	%
DOS	10	8	80	10	8	80	10	8	80	DOS	10	8	80	10	8	80	10	8	80
http	10	6	60	10	7	10	10	2	20	http	10	10	100	10	10	100	10	8	80
SMTP	10	10	100	10	8	8	10	1	10	SMTP	10	10	100	10	10	100	10	10	100
FTP	10	5	50	10	2	20	10	8	8	FTP	10	5	50	10	5	50	10	5	50
BO(Exploit	10	8	80	10	2	20	10	2	20	BO(Exploit	10	6	60	10	6	60	10	6	60
Portscan	10	8	80	10	4	40	10	8	80	Portscan	10	6	60	10	6	60	10	6	60
Scan Vuln	10	10	100	10	9	90	10	10	100	Scan Vuln	10	10	100	10	10	100	10	10	100

G= Ataques Gerados D= Ataques detectados BO= Buffer Overflow

De todas as ferramentas de ataques utilizadas, quatro delas não foram detectadas por nenhuma das duas ferramentas de IDS. Este fato demonstra a importância da atualização constante destas ferramentas, com novas regras para evitar e/ou minimizar a ocorrência destes falsos negativos. Existem centenas de ataques disponíveis gratuitamente na Internet e de fácil utilização. Um IDS será tanto mais seguro quanto maior for seu nível de atualização.

Outro ponto a ser observado nesta avaliação é que a ferramenta Snort mostrou uma deficiência maior na detecção dos ataques quando submetida a taxas de utilização da rede mais elevadas quando comparada com os resultados da ferramenta Prelude. É necessário um estudo mais aprofundado para determinar qual o real motivo que influenciou a queda tão significativa da capacidade de detecção da ferramenta Snort.

A tabela 3 apresenta os resultados obtidos nos testes da categoria 3 com a utilização do aplicativo *Fragroute*, que permite criar regras para modificar os pacotes enviados. Neste teste, a ferramenta Prelude mostrou uma maior deficiência em relação à ferramenta Snort, conseguindo detectar apenas o ataque de DoS (*Denial of Service*).

Tabela 3 – Teste de evasão usando Fragroute

Tráfego	Ferramenta SNORT									Ferramenta PRELUDE								
	0%			35%			75%			0%			35%			75%		
Ataque	G	D	%	G	D	%	G	D	%	G	D	%	G	D	%	G	D	%
Slice (DoS)	3	3	300	5	3	100	3	3	100	3	3	100	3	3	100	5	3	300
WUFTP (Exploit)	3	3	300	5	3	100	3	3	100	3	0	0	3	0	0	5	0	0
Simplestealth (Portscan)	3	3	300	5	1	33	3	3	100	3	0	0	3	0	0	5	0	0

G= Ataques Gerados D= Ataques detectados BO= Buffer Overflow

A tabela 4 apresenta os resultados obtidos nos testes da categoria 3 com a utilização do aplicativo *Nikto*, *scanner* que procura por vulnerabilidades em servidores *WWW*. Como é possível verificar, as ferramentas não foram capazes de detectar 100% das técnicas de evasão, apresentando, novamente, variações em sua capacidade de detecção quando submetidas ao teste com diferentes taxas de utilização da rede. Pelos dados apresentados, pode-se constatar um alto índice de falsos negativos. Por esse motivo é que as técnicas de evasão são consideradas perigosas, pois os números de ataques não detectados apresentam-se elevados.

Tabela 4 – Teste de evasão usando Nikto

Ferramenta SNORT - Teste de Evasão usando Nikto									
Tráfego	0%			35%			75%		
Técnicas	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%
URL encoding	987	305	31,5	987	13	1,42	987	29	2,21
./ directory insertion	1420	372	48,3	1420	13	0,96	1420	77	5,42
Long URL	1420	1185	83,5	1420	13	0,92	1420	169	11,9
Fake parameter	1420	1262	88,9	1420	28	1,97	1420	166	11,7
Ferramenta PRELUDE - Teste de Evasão usando Nikto									
Tráfego	0%			35%			75%		
Técnicas	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%
URL encoding	987	332	60,5	987	526	35,8	987	462	58,9
./ directory insertion	1420	726	51,1	1420	424	29,9	1420	323	56,9
Long URL	1420	1854	131	1420	643	45,2	1420	658	46,4
Fake parameter	1420	2506	160	1420	795	56	1420	1440	102

4. Resultados e trabalhos futuros

Conforme citado no início deste artigo, a segurança das redes de computadores depende de um conjunto integrado de ferramentas de controle e monitoramento. A simples utilização de um IDS, conforme pode ser visto nos resultados dos testes, não garante que uma rede esteja completamente protegida contra ataques. Ainda existem vários problemas a serem resolvidos nas ferramentas de detecção intrusão, como a perda da capacidade de detecção dos ataques com o aumento de tráfego (visto neste artigo), complexidade de configuração e desempenho apresentado em redes de alta velocidade (como, por exemplo, em redes Gigabit Ethernet). No entanto, mesmo com tais dificuldades, a implantação de um IDS na estrutura de segurança de uma empresa é altamente recomendável. Além de oferecer uma barreira complementar ao *firewall*, o IDS é capaz de coletar uma ampla gama de informações sobre o padrão de ataques sofridos por uma rede que pode ser de grande valia no entendimento de futuros ataques. É necessário que sejam realizadas mais pesquisas com o intuito de procurar solucionar os problemas existentes nas ferramentas atuais, a fim de torná-las mais representativas no escopo de proteção das redes de computadores.

Referências Bibliográficas

ALLEN, Julia et al. **State of the Practice of Intrusion Detection Technologies, 2000.** Disponível em: <http://www.cert.org/archive/pdf/99tr028.pdf>. Acesso em: 18 set. 2002.

Campello, Rafael Saldanha; WEBER, Raul Fernando. **Sistemas de detecção de intrusão.** Disponível em: <http://www.inf.ufrgs.br/~gseg/producao/minicurso-ids-sbrc-2001.pdf>. Acesso em: 10 nov. 2002.

CERT - Computer Emergency Response Team. **CERT/CC Statistics 1988-2003, 2003.** Disponível em: < http://www.cert.org/stats/>. Acesso em: 25 mai. 2003.

Crothers, Tim. **Implementing Intrusion Detection Systems:** A Hands-on Guide for Securing the Network. Indianapolis: Wiley Publishing, 2003. 297p.

Northcutt, Stephen; ZELTSER, Lenny et al. **Desvendando segurança em redes.** Rio de Janeiro: Editora Campus, 2002. 650p.

NSS GROUP. **Intrusion detection systems, Group test (edition 3)** 2002. Disponível em: <http://www.nss.co.uk/ids/edition3/index.htm>. Acesso em 11 nov 2002.

Proctor, Paul E. **The practical intrusion detection handbook.** New Jersey: Prentice-Hall PTR, 2001. 359p.

Tricaud, Sebastien. **Prelude's FAQ, v0.5.** Disponível em: http://www.prelude-ids.org/article.php3?id_article=8. Acesso em: 25 abr 2003.