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

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

[1]Bacharel em Ciência da Computação, [2]Prof. Esp. Ciência da Computação

Centro Universitário FEEVALE
RS 239, 2755 - Cep 93352-000 - Novo Hamburgo - RS – Brasil

steffen@tca.com.br, elbastos@acm.org

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.*

Resumo. *A necessidade de proteger a estrutura de rede contra ataques gerou um conjunto de ferramentas que visam proporcionar esta proteção. Uma ferramenta que faz parte deste conjunto é conhecida como Sistemas de Detecção de Intrusão (Intrusion Detection Systems - IDS), o IDS é uma ferramenta que auxilia na detecção de ataques alertando e realizando ações que possam impedir que um ataque seja concretizado. Este trabalho teve como objetivo apresentar um estudo da ferramenta de IDS e realizar um teste prático com duas ferramentas de IDS diferentes visando verificar o comportamento destas ferramentas frente a ataques realizados com ferramentas disponíveis em sites na Internet.*

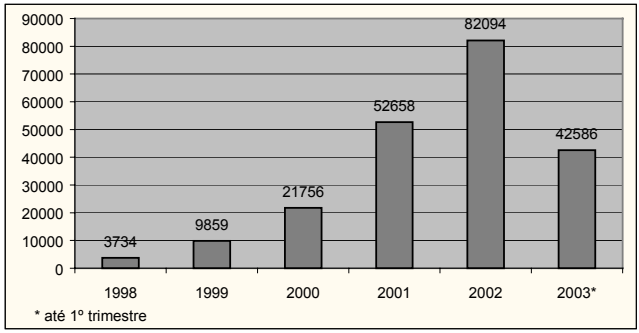
1. Introdução

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 da CERT (Computer Emergency Response Team) os ataques a redes crescem a cada ano como mostra a Tabela 2.1. Como um dos fatores para este crescimento é possível citar a sofisticação das ferramentas de ataques existentes nos dias de hoje e como conseqüência desta sofisticação, houve um aumento no número de pessoas que podem vir a cometer um ataque. [ALLEN, 2000].

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 2.1–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 2 aborda, de maneira clara e objetiva, como o IDS funciona, bem como os tipos, métodos e problemas encontrados em uma ferramenta de IDS. A seção 3 apresenta as duas ferramentas utilizadas nos testes. A seção 4 comenta os testes realizados e aborda os resultados obtidos.

2. 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, p. 156].

Um IDS é composto basicamente por dois dispositivos principais, o Console de Comando e o Sensor. 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 sensor é o dispositivo responsável pela coleta de informação para análise de descoberta de uma invasão" [CROTHERS, 2003. p. 275].

O IDS pode trabalhar basicamente de duas maneiras, uma é analisando o tráfego da rede (Baseado em Rede), onde o sensor analisa todos os pacotes que circulam pelo segmento de rede independente de qual era o destino do pacote. A outra forma é analisando uma determinada máquina (Baseado em *Host*) a procura de códigos maliciosos para identificar sinais de que um ataque está sendo iniciado.

Quanto ao método que o IDS detecta os ataques, ele pode ser classificado como Baseado em Assinatura ou 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, é gerado um alerta ou evento que permita uma ação defensiva [NORTHCUT, 2002]. Já o IDS baseado em anomalia, possui uma base de dados do comportamento da rede, a partir desta base é que o sistema verifica o que é ou não permitido e quando encontra algo fora do padrão gera o alerta.

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

Outro problema que merece uma 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, e a necessidade de formas de evita-las tornou-se uma constante entre os desenvolvedores das ferramentas de IDS, porque o poder de detecção da ferramenta fica comprometido se ela não for capaz de reconhecer essas técnicas.

3. 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 sistema de detecção de intrusão baseado em rede amplamente utilizado, possui uma arquitetura simples baseada em *plugins*, onde executa 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, sendo o seu sistema de detecção baseado em assinaturas [CAMPELLO, 2002].

O Prelude é uma ferramenta de IDS híbrida, pode 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.

4. 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 que foram realizados.

Com o intuito de realizar um estudo comparativo fiel entre as duas ferramentas, ambas foram submetidas aos mesmos ataques sob uma configuração *default* da ferramenta. 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. Porém, este comparativo não tem o intuito de definir qual ferramenta é melhor, pois seria necessário 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. Uma metodologia foi utilizada com o objetivo de padronizar os testes e definir quais os testes que seriam realizados, os tipos de ataques, as ferramentas usadas no teste e como seriam realizados os testes.

Os testes foram divididos em três categorias [NSS GROUP, 2002]:

- Reconhecimento de ataques: foi verificado 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*);
- Performance: foi analisado a capacidade da ferramenta de IDS em detectar os ataques com diferentes taxas de utilização da rede;
- Técnicas de evasão: foi verificado a capacidade da ferramenta em detectar as técnicas de evasão.

Cada ferramenta de IDS foi testada separadamente para que uma não influenciasse no resultado da outra. O primeiro teste realizado teve a taxa de utilização da rede em 0%, neste teste foi criada a *baseline* dos ataques realizados versos os ataques detectados. Os testes seguintes realizados foram os com taxa de utilização de 25% e 75%, o teste de evasão e o teste de falso positivo. Os testes de falso negativo ocorreram junto com os testes de reconhecimento de ataque e performance, porque sempre que um ataque é gerado e não é detectado pelo IDS ocorre um falso negativo.

Os ataques foram realizados individualmente, um após o outro, para que se tivesse certeza de que o ataque detectado, quando detectado, correspondia ao ataque gerado. Após o alerta de ataque ser gerado no console de gerenciamento ele foi devidamente documentado para análise posterior e comparações entre os resultados obtidos pela mesma ferramenta, bem como comparações entre os resultados das duas ferramentas de IDS e para que ao final dos testes pudesse ser montada uma planilha demonstrativa com os resultados obtidos. Antes de um novo ataque ser iniciado o alerta anterior era apagado.

Na tabela 4.1, 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 números de detecção entre as duas ferramentas se alteraram sensivelmente quando o uso da taxa de rede se tornou presente nos testes.

Tabela 4.1 – Reconhecimento de ataque e Performance

Ferramenta SNORT										Ferramenta PRELUDE									
Tráfego	0%			25%			75%			Tráfego	0%			25%			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	1	10	10	2	20	HTTP	10	10	100	10	10	100	10	8	80
SMTP	10	10	100	10	0	0	10	1	10	SMTP	10	10	100	10	10	100	10	10	100
FTP	10	5	50	10	2	20	10	0	0	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 existiram quatro, de tipos de ataques diferentes, que não foram detectadas por nenhuma das duas ferramentas de IDS. Este fato demonstra que existem centenas de ferramentas de ataques disponíveis e que a constante atualização e criação de novas regras é necessária e que é difícil estar 100% protegido e fica evidente a ocorrência dos falsos negativos. Outro ponto a ser observado 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. Seria necessário um estudo mais aprofundado para determinar qual o real motivo que influenciou a queda tão significativa do poder de detecção da ferramenta Snort, se foi o tipo de tráfego, o método usado pela ferramenta para analisar o tráfego ou a necessidade de otimização em suas configurações após a instalação.

Na tabela 4.2 é possível observar os resultados dos testes de evasão usando a ferramenta *Fragroute* (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 4.2 – Teste de evasão usando *Fragroute*

Tráfego	Ferramenta SNORT									Ferramenta PRELUDE								
	0%			25%			75%			0%			25%			75%		
Ataque	G	D	%	G	D	%	G	D	%	G	D	%	G	D	%	G	D	%
Slice (DoS)	3	3	100	3	3	100	3	3	100	3	3	100	3	3	100	3	3	100
WUFTP (Exploit)	3	3	100	3	3	100	3	3	100	3	0	0	3	0	0	3	0	0
Simplestealth (Portscan)	3	3	100	3	1	33	3	3	100	3	0	0	3	0	0	3	0	0

G= Ataques Gerados D= Ataques detectados

Na tabela 4.3 é encontrado os resultados dos testes de evasão usando a ferramenta *Nikto* (*scanner* que procura por vulnerabilidades em servidores *WWW*). Como é possível verificar, o número de técnicas existente é bem numeroso e ambas 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 taxa de utilização da rede, o que originou 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 são bem elevados.

Tabela 4.3 – Teste de evasão usando *Nikto*

Ferramenta SNORT - Teste de Evasão usando Nikto									
Tráfego	**0%**			**25%**			**75%**		
Técnicas	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%
URL encoding	907	195	21,5	907	13	1,43	907	20	2,21
./ directory insertion	1420	572	40,3	1420	15	1,06	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%**			**25%**			**75%**		
Técnicas	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%	Checadas	Alertas Gerados	%
URL encoding	907	552	60,9	907	326	35,9	907	462	50,9
./ directory insertion	1420	726	51,1	1420	424	29,9	1420	523	36,8
Long URL	1420	1854	131	1420	643	45,3	1420	650	45,8
Fake parameter	1420	2266	160	1420	795	56	1420	1445	102

Como já comentado no início do artigo, a segurança de uma estrutura de rede depende de um conjunto de ferramentas e como pode ser observado nos resultados contidos nas tabelas, o IDS sozinho não pode garantir a total segurança de uma rede, pois apresenta alguns problemas que o impede de ser 100% confiável. Mas, é claro que mesmo com os problemas de falsos positivos, falsos negativos e evasão, sua presença na estrutura de segurança de uma rede é importante, pois fornece informações e ações que sem o IDS seriam difíceis de serem detectadas e tomadas. O que é necessário, é que sejam realizadas mais pesquisas com o intuito de procurar solucionar os problemas existentes em uma ferramenta de IDS, afim 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.