O EMPREGO DO SISTEMA DE DETECÇÃO DE INTRUSÃO SNORT EM AMBIENTES COOPERATIVOS

RODRIGO ADÃO DA SILVA

Pós-graduado, lato sensu, em Guerra Eletrônica e em Sistemas de Comunicações e Defesa

RESUMO: Este artigo consiste em abordar o emprego do sistema de detecção de intrusão Snort em ambientes cooperativos. A detecção de intrusão é uma das áreas de maior expansão, pesquisa e investimento em segurança de rede de computadores. Com o crescimento da interligação de computadores em todo o mundo, houve um aumento nos tipos e números de ataques contra sistemas de computadores, produzindo uma complexidade muito alta para a capacidade dos mecanismos preventivos tradicionais. Para a maioria das aplicações atuais, a partir de redes corporativas simples para sistemas de *e-commerce* ou aplicações de banco, é praticamente impossível o simples uso de mecanismos para reduzir a probabilidade de ataques. Um ataque pode provocar a interrupção total de serviços, forçando a ocorrência de um lento e dispendioso processo de auditoria, e a restauração manual do sistema. Esse contexto justifica todo o investimento feito, a fim de criar dispositivos que superem a barreira de prevenção simples, garantindo aos sistemas uma operação contínua e correta, mesmo na presença de falhas de segurança. Assim, aparece o Sistema de Detecção de Intrusão ou *Intrusion Detection System* (IDS). Basicamente, o IDS é uma ferramenta inteligente (um sistema de configuração e regras) capaz de detectar intrusões em tempo real e capaz de verificar se um usuário está usando a rede corretamente, produzindo alertas quando detecta pacotes que podem ser parte de um possível ataque. Nesse contexto, aparece o *software* Snort, amplamente utilizado em ambientes cooperativos, como uma solução de aviso sobre a possibilidade de ataques e anomalias em redes de computadores.

Palavras-chave: snort, segurança, detecção de intrusão.

1 INTRODUÇÃO

Com o advento da globalização, cotidianamente, grandes uniões ocorrem nos setores econômico, social, político e cultural, atinentes à sociedade pós-moderna. Como consequência, surgem numerosos problemas relacionados à segurança no campo do tráfego de dados entre os diferentes agentes envolvidos neste processo.

Assim, o espaço permeado pela diversidade de conexões entre parceiros comerciais, clientes - fornecedores, matrizes - filiais, e indivíduos, no qual a rápida troca de informações é um fator determinante de sucesso, é denominado de ambiente cooperativo (NAKAMURA e GEUS, 2004, p. 22).

Ademais,

> o ambiente cooperativo é caracterizado pela integração dos mais diversos sistemas de diferentes organizações, nos quais as partes envolvidas cooperam entre si, na busca de um objetivo comum: velocidade e eficiência nos processos e nas realizações dos negócios (NAKAMURA e GEUS, 2004, p. 22).

Nesse contexto, a segurança é uma condição indelével para o êxito do objetivo acima colocado, o que provoca uma perene busca pela proteção dos ativos informacionais. E há de ressaltar que a aquisição de conhecimento, oportunamente, pode ser um fator de vantagem competitiva no mercado atual.

As informações, do ponto de vista do negócio, configuram-se como ativos de uma empresa, juntamente, com todo o ambiente por onde trafegam e em decorrência devem ser protegidas, conforme visão de Caruso e Steffen (1999, p. 23).

Logo, cresce de importância no âmbito das redes de computadores a adoção de *firewall,* associado com um IDS.

Nesse aspecto, Marçula e Filho fornecem a seguinte conceituação:

> Um *Firewall* é uma combinação de *hardware* e *software* usados para implementar uma política de segurança comandando o tráfego da rede entre duas ou mas redes, algumas das quais podem estar sob seu controle administrativo (por exemplo, redes da sua empresa) e algumas das quais podem estar fora de seu controle (por exemplo, a *Internet*). Um *firewall* normalmente serve como uma primeira linha de defesa contra ameaças externas ao sistema de computadores, redes e informações críticas de sua empresa. *Firewalls* podem também ser utilizados para particionar as redes internas de sua empresa, reduzindo o risco de ataques internos (FITHEN *et al*., 1999 *apud* MARÇULA e FILHO, 2009).

O IDS "é um serviço que monitora e analisa eventos de uma rede com o propósito de encontrar e providenciar alertas em tempo real e acessos não autorizados aos recursos de uma rede" (SANTOS, 2010, p. 801).

Ratificando o exposto acima, Nakamura e Geus afirmam que:

> um sistema de detecção de intrusão trabalha como uma câmera ou um alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas de ataques, ou em desvios de comportamento […]. Ao reconhecer os primeiros sinais de um ataque, e por meio de uma resposta coerente, os perigos de um ataque real podem ser minimizados. Além disso, quando um dispositivo do ambiente computacional falha, devido a um erro de configuração ou um erro do usuário, o IDS pode reconhecer os problemas e notificar o responsável (NAKAMURA e GEUS, 2004, p. 253).

Com vistas a elucidar os próximos tópicos do presente artigo, Murini cita que:

> devemos ter uma diferenciação entre "Ataque" e "Intrusão", pois parecem ser a mesma coisa, mas tem algumas particularidades: ataque refere-se à tentativa de perturbação, já intrusão é um ataque realizado que obteve sucesso (foi bem sucedido), pois invadiu a rede (MURINI, 2014, p. 20).

E a intrusão trata-se de um conjunto de ações realizadas por um intruso, visando comprometer os elementos: integridade, confidencialidade e

disponibilidade, que constituem a estrutura básica de segurança da informação de um sistema (SILVA e SAMPAIO, 2006, *apud* MURINI, 2014, p. 19-20).

Por fim, existem vários tipos de ferramentas de IDS para diferentes plataformas, mas o IDS opera basicamente da mesma forma, analisando os pacotes que viajam numa rede e comparando-os com as assinaturas de ataques, com vistas a alertar sobre vicissitudes indesejáveis.

2 DESENVOLVIMENTO

2.1 CARACTERÍSTICAS DE UM IDS

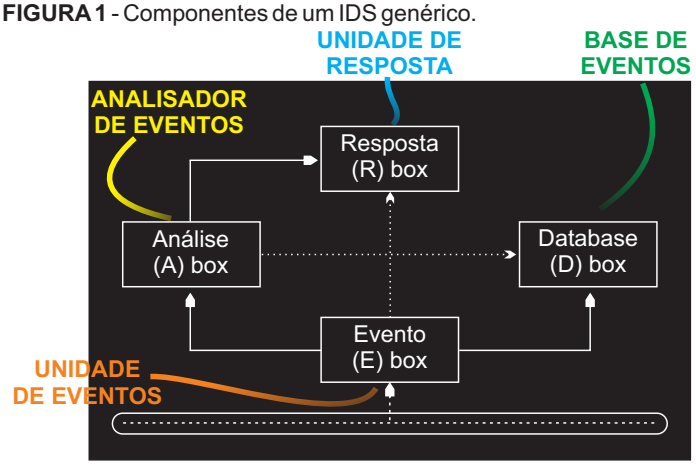
De acordo com Santos (2010, p. 801), um IDS deve possuir algumas características, como:

a) funcionar continuamente, operando normalmente em segundo plano;
b) ser tolerante a falhas;
c) ter a capacidade de monitorar a si próprio;
d) detectar mudanças no funcionamento normal da rede;
e) detectar o menor número de falsos positivos – que é a classificação de uma ação legal como uma possível invasão;
f) não deve permitir falso negativo – que ocorre quando uma intrusão real acontece, mas o sistema a classifica como legítima;
g) não deve permitir a subversão – que ocorre quando o intruso modifica a operação de ferramenta IDS para forçar a ocorrência de falso negativo;
h) deve avisar o administrador de rede ou de sistema, em tempo real, sobre uma possível invasão e, quando configurado, ativar automaticamente alarmes e mecanismos de segurança;
i) colher informações de intrusos para a sua captura; e
j) diagnosticar e corrigir eventuais falhas de segurança.

2.2 ARQUITETURA GENÉRICA DE UM IDS

Devido a ampla variedade de sistemas IDS, inicialmente foi proposto um modelo genérico denominado de *Common Intrusion Detection Framework* (CIDF), o qual reúne um conjunto de ferramentas que definem a configuração de um IDS, conforme figura a seguir:

FIGURA 1 - Componentes de um IDS genérico.



Fonte: Confeccionada pelo autor.

O objetivo do CIDF era promover a intercomunicação entre dispositivos de comunicação de intrusos e sistemas de respostas, como os *firewalls,* por intermédio de uma linguagem chamada de *Common Intrusion Specification Language* (CISL), na visão de Militelli (2006, p. 12).

Balizando-se pela figura 1, percebe-se que o modelo CIDF é composto pelos seguintes blocos: Unidade de Eventos (*E-box*), Analisador de Eventos (*A-box*), Unidade de Resposta (*R-box*) e Base de Eventos (*D-box*). Nesse contexto, Militelli (2006, p.12-13) afirma que estas unidades são responsáveis, respectivamente, pelas funções de:

a) gerar eventos e segurança que poderão se tornar alertas, a partir da informação proveniente de uma fonte de dados. Em se tratando de um meio físico, o *E-box* é o responsável por reconstruir o pacote de dados e repassar para análise;
b) realizar toda a análise e correlacionamento dos eventos, além da interação direta com o módulo e resposta;
c) promover as respostas no sistema IDS; e
d) armazenar o histórico de eventos conforme a ocorrência.

Posteriormente, em 1998 foi criado o *Intrusion Detection Exchange Format Working Group* (IDWG), grupo que se balizou nos conceitos contidos no CIDF e padronizou requisitos e novos protocolos de comunicação entre dispositivos envolvidos no sistema de detecção de intrusos, como o IAP e o IDXP.

E como aperfeiçoamento do IDXP, foi idealizado o *Secure Components Exchange Protocol* (SCXP), com o objetivo de promover um protocolo único de comunicação no escopo do IDS (YANG; CHANG; CHU, 2003 *apud* MILITELLI, 2006, p. 17).

2.3 CLASSIFICAÇÃO E TIPOS DE IDS

O IDS pode ser classificado em sistema de detecção por: assinatura (ou conhecimento) e por anomalias (ou comportamento). E segundo Nakamura e Geus (2004, p. 256) pode ser tipificado em três categorias: IDS baseado em máquina – *Host Based Intrusion Detection System* (HIDS), em rede – *Network Basead Intrusion Detection System* (NIDS) e híbrido – *Hybrid*. Vale ressaltar que este último aproveita as melhores características do HIDS e do NIDS.

2.4 SNORT

2.4.1 Características Técnicas

O Snort é um *software* livre desenvolvido por Martin Roesch, bastante popular por sua flexibilidade nas configurações de regras e constante atualização frente as novas ferramentas de invasão. Ele se baseia em assinaturas, ao monitorar tentativas de ataques contra uma rede e gera arquivos com as ocorrências diagnosticadas. Por isso, é classificado como um IDS baseado em rede.

Também é capaz de realizar análises em tempo real com suporte a diversos protocolos em nível de rede e aplicação, sobre o conteúdo hexadecimal e ASCII (GONÇALVES, 2015, p. 199). Pode ser usado para detectar uma variedade de ataques, como: *buffer overflows*, *stealth port scans*, ataques CGI, SMB *probes,* OS *fingerprinting*, dentre outros.

Essa ferramenta é compatível com arquiteturas RISC e CISC, e com distintas plataformas, como: distribuições *Linux* (*Red Hat, Debian, Slackware, Ubuntu*, etc.), sistemas operacionais (SO) da *Microsoft* – *Windows* e *Apple* – MAC OS.

O código fonte está calcado em linguagem de programação C e as documentações afetas ao seu emprego e funcionamento são de domínio público.

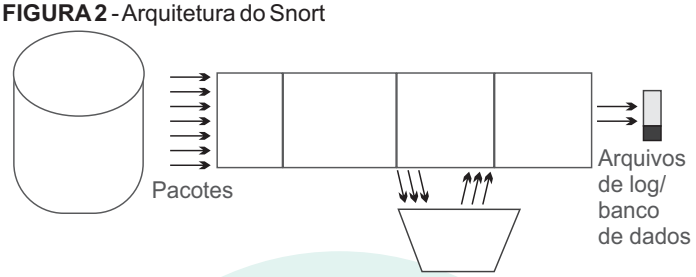
No Brasil, existe o projeto Snort-BR, um esforço para a criação de uma comunidade de usuários que podem usar um IDS de código aberto no país.

2.4.2 Arquitetura do Snort

Caswell e outros (2003) afirmam que a arquitetura do Snort é composta por quatro blocos, a saber:

a) o farejador de pacotes;
b) o pré-processador;
c) o mecanismo de detecção; e
d) o mecanismo de alerta/registro.

FIGURA 2 - Arquitetura do Snort



Fonte: Caswell et al., 2003, p.26.

2.4.2.1 Farejador de Pacotes

Os farejadores de pacotes são dispositivos de *hardware* ou de *software* utilizados na escuta das redes, capturando todos os dados trafegados.

Segundo Caswell *et al.* (2003), farejadores de pacotes podem ser utilizados para:

- análise de diagnóstico e solução de problemas na rede;
- análise e comparativo de desempenho; e
- intromissão para obter senhas em texto puro e outros dados interessantes.

A criptografia de tráfego da rede pode impedir que os dados sejam analisados por um farejador, o que se configura como uma desvantagem para o Snort.

2.4.2.2 Pré-Processador

De acordo com Caswell *et al*. (2003), este componente pega os pacotes brutos e verifica em relação a certos *plug-ins*, determinando assim o comportamento do pacote analisado. Uma vez detectado o comportamento particular do pacote, o mesmo é encaminhado para o mecanismo de detecção. A grande vantagem de trabalhar com *plug-ins*, é a possibilidade de ativar e desativar alguns deles de acordo com a necessidade e o perfil da rede onde o IDS está sendo configurado. Em suma, o pré-processador classifica os pacotes oriundos do farejador.

2.4.2.3 Mecanismo de Detecção

Na visão de Caswell *et al.* (2003), este é o bloco mais importante do IDS Snort. Os dados vindos do mecanismo de pré-processamento são recebidos pelo mecanismo de detecção e comparados com um conjunto de regras de assinatura de ataques conhecidos. Uma vez que os dados dos pacotes correspondam com as informações de alguma regra, estes são enviados para o processador de alerta.

Em se tratando do Snort, as regras são conjuntos de requisitos que geram um alerta. E para a criação de regras, é de vital importância ter conhecimento sobre os arquivos *snort.conf*, *threshold.conf* e *community.rules*,

que podem ser editados por intermédio de um editor de texto, como o *wordpad* (para o SO *Windows*).
O *download* das regras é feito do sítio eletrônico www.snort.org. Depois estas são descomprimidas e inseridas na pasta *rules* (*c:\snort\rules*), no caso do emprego do SO *Windows,* possibilitando que o mecanismo de detecção funcione de forma adequada.

2.4.2.4 Sistema de Alerta

Quando os dados que passam pelo mecanismo de detecção correspondem com alguma regra, então um alerta é disparado pelos *plug-ins* de saída. Sobre este evento, destaca-se a opinião de Caswell *et al.*(2003), ao afirmar que os *plug-ins* de saída fornecem aos administradores a capacidade de configurar *logs* e alertas de fácil compreensão. Ressalta-se que a análise de fluxo seria inútil sem eles para processar e formatar os dados analisados.

Os alertas podem ser enviados para um arquivo de *log* através de uma conexão de rede, por meio de soquetes UNIX ou *Windows Popup* e também podem ser armazenados num banco de dados. Existem muitas ferramentas adicionais que podem ser utilizadas para tratar os dados de saída do Snort como *plug-ins Perl* e PHP, além de servidores *Web* para exibir os dados processados.

2.4.3 Exemplificação da utilização do Snort

A representação do Serviço Federal de Processamento de Dados (SERPRO) em Recife tem adotado o Snort em suas redes internas, o que tem proporcionado uma economia da ordem de milhões de reais, caso fosse adquirida uma solução proprietária (BRASIL, [201-]).

3 CONCLUSÃO

O presente artigo busca dar uma visão panorâmica sobre o contexto de um Sistema de Detecção de Intrusão, abordando em particular o *software* Snort, um dos mais empregados no âmbito de sistemas cooperativos.

O emprego de um IDS, como o Snort, é de grande valia, tendo em vista que a solução já está consolidada no mercado de tecnologia da informação e possui atualizações constantes de regras, o que promove uma maior segurança numa rede de computadores.

Na visão de Gonçalves (2015, p. 199), seus módulos são capazes de analisar o conteúdo dos cabeçalhos tão quanto dos pacotes em redes *Internet Protocol* (IP), gerando elevada quantidade de informação sobre os ataques detectados. Ademais, uma das mais notórias características do seu funcionamento é a ampla possibilidade de tratamento dos alertas gerados, através de ações que vão desde mensagens ao administrador de rede a bloqueios de tráfego.

Outro detalhe que favorece a adoção do Snort é a característica do sistema ser baseado em assinaturas, trabalhando somente em comparação com seu banco de regras, ao contrário dos sistemas de detecção por anomalias.

Gonçalves (2015, p. 199) afirma que estes IDS possuem alguns inconvenientes, como: falsos positivos equivocadamente sinalizados como intrusão em relação a atividades anômalas, porém não intrusivas e falsos negativos, por não produzirem alguma anomalia perceptível, possibilitando que intrusões não sejam detectadas.

Assim, espera-se que o trabalho possa contribuir na difusão do emprego do Snort, visando elevar os níveis de segurança no universo das redes de computadores e *gadgets* que circundam o cotidiano da sociedade pós-moderna.

EL EMPLEO DEL SISTEMA DE DETECCIÓN DE INTRUSOS SNORT EN AMBIENTES COOPERATIVOS

RESUMEN

El presente trabajo científico consiste en abordar el “empleo del sistema de detección de intrusos en ambientes cooperativos”. La detección de intrusión es una de las áreas de mayor expansión, investigación e inversión en seguridad de redes de ordenadores. Con el crecimiento de la interconexión de ordenadores alrededor del mundo, por intermedio de internet, ocurrió un aumento en los tipos y números de ataques a los sistemas informáticos, produciendo una complejidad muy elevada para la capacidad de los tradicionales mecanismos de prevención. Para la mayoría de las aplicaciones actuales, a partir de redes corporativas simples hasta los sistemas de comercio electrónico o aplicaciones de banco, es prácticamente imposible el simple uso de mecanismos para reducir la probabilidad de ataques. Un ataque puede, en casos extremos, causar una interrupción total de los servicios, forzando la ocurrencia de un lento y costoso proceso de auditoría, y una restauración manual del sistema. Este contexto justifica toda la inversión realizada con el fin de crear dispositivos que superen la barrera de la simple prevención, asegurando a los sistemas una operación continua y correcta, mismo en la presencia de fallos de seguridad. Así, aparecen lo Sistema de Detección de Intrusos o Intrusion Detection System (IDS). Básicamente, el IDS es una herramienta inteligente (un sistema de configuración y reglas) capaz de detectar los intentos de intrusión en tiempo real y capaz de verificar si un usuario está usando la red correctamente, produciendo alertas cuando detecta paquetes que pueden ser parte de un posible ataque. En este contexto, se presenta el software Snort, ampliamente utilizado en

ambientes cooperativos, como una solución de aviso sobre la posibilidad de ataques y anomalías en redes de ordenadores.

Palabras-clave: snort, seguridad, detección de intrusos.

REFERÊNCIAS

BRASIL. **Snort**: ferramenta livre garante segurança na rede Serpro, [201-]. Disponível em: < http://www.softwarelivre.gov.br/noticias/snort-ferramenta-livre-garante-seguranca-na-rede-serpro/>. Acesso em: 06 jun. 2017.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2. ed. São Paulo: SENAC, 1999.

CARVALHO, João Antônio. **Informática para concursos**: teoria e questões. Rio de Janeiro: Elsevier, 2013.

CASWELL, Brian et al. **Snort 2**: sistema de detecção de intrusão. Rio de Janeiro: Alta Books, 2003.

GONCALVES, Denis Pohlmann. **Utilização de sistema de detecção e prevenção de intrusos modo NIDS**. In: ENCONTRO ANUAL DE TECNOLOGIA DA INFORMAÇÃO. 2015, Frederico Westphalen. Anais... Frederico Westphalen: IFF FARROUPILHA, ano 5, n. 1, nov. 2015. Disponível em: < http://eati.info/eati/2015/assets/anais/Longos/L24.pdf>. Acesso em: 06 jun. 2017.

KAHN, C.; PORRAS, P. A.; STANIFORD-CHEN, S.; B., A **Common Intrusion Detection Framework**. Journal of Computer Security, Julho, 1998.

LEMKE, Alexandre; SANTOS, Vagner. **Ferramenta Snort**. Disponível em: <http://olaria.ucpel.tche.br/rii/lib/exe/fetch.php?media=texto-trabalhosnortfinal.pdf>. Acesso em: 06 jun. 2017.

MARÇULA, Marcelo; FILHO, Pio Armando Benini Filho. **Informática**: conceitos e aplicações. 3. ed. São Paulo: Érica, 2009.

MILITELLI, Leonardo Cavallari. **Proposta de um agente de aplicação para detecção, prevenção e contenção de ataques em ambientes computacionais.** 2006. Dissertação (Mestrado em Engenharia Elétrica) – Escola Politécnica da Universidade de São Paulo, 2006. Disponível em: < http://www.lsi.usp.br/~volnys/academic/trabalhos-orientados/Agente-de-aplicacao-para-IDS.pdf>. Acesso em: 06 jun. 2017.

MURINI, Cléber Taschetto. **Análise dos sistemas de detecção de intrusão em redes: snort e suricata comparando com dados da DARPA.** 2014. Trabalho de Conclusão de Curso (Tecnólogo em Redes de Computadores) – Universidade Federal de Santa Maria, 2014. Disponível em: <http://www.redes.ufsm.br/docs/tccs/CleberMurini.pdf>. Acesso em: 06 jun. 2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. 2. ed. São Paulo: Futura, 2004.

SANTOS, André Alencar dos. **Informática descomplicada:** teoria e exercícios para concursos públicos. 5. ed. Brasília: Gran Cursos, 2010.

SILVA, Edelberto Franco; JULIO, Eduardo Pagani. **Sistema de detecção de intrusão** – artigo Revista Infra Magazine 1. Disponível em: <http://www.devmedia.com.br/sistema- de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819>. Acesso em: 05 jun. 2017.

SNORT. Site of Snort Community. Disponível em: <https://www.snort.org/>. Acesso em: 05 jun. 2017.

_____. Snort Uses Manual 2.9.9. [S. l.]. 2016. Disponível em: < http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>. Acesso em: 05 jun. 2017.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). Capitão da Arma de Comunicações do Exército Brasileiro, possui especialização nas áreas de Manutenção de Comunicações e Guerra Eletrônica. Concluiu com aproveitamento o curso de Manutenção de Comunicações da Escola de Comunicações, o curso Básico de Guerra Eletrônica, no Centro de Instrução de Guerra Eletrônica (CIGE) e o curso Expedito de Guerra Eletrônica para Oficiais, no Centro de Adestramento Almirante Marques Leão da Marinha do Brasil. É pós-graduado em Guerra Eletrônica pelo CIGE e em Sistemas de Comunicações e Defesa, pela Universidade Politécnica de Madri. Atualmente, exerce a função de Instrutor na Escola de Comunicações e pode ser contactado pelo email adao.silva@eb.mil.br.