SNORTIK - UMA INTEGRAÇÃO DO IDS SNORT E O SISTEMA DE FIREWALL DO MIKROTIK ROUTEROS

Brunno Fagundes[1], Charles V. Neu[14], Alex M. S. Orozco[24], Regio A. Michelin[34], Avelino F. Zorzo[4]

[1]Universidade de Santa Cruz do Sul(UNISC)

[2]Instituto Federal Sul-rio-grandense (IFSUL)

[3]Instituto Federal do Rio Grande do Sul (IFRS)

[4]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

mail.br.net@gmail.com,charles1@unisc.br,orozco@sapucaia.ifsul.edu.br

regio.michelin@restinga.ifrs.edu.br,avelino.zorzo@pucrs.br

Abstract. *This work proposes the use of SNORT Intrusion Detection System as an attack detection tool and the development of an intermediate system that uses the logs generated by SNORT to create protection rules for the Mikrotik RouterOS firewall. The achieved results show that this system can be used to automate the reaction process to attacks identified by SNORT without the system administrator intervention, blocking suspect hosts identified.*

Resumo. *Este trabalho propõe a utilização do Sistema de Detecção de Intrusão SNORT como ferramenta de detecção de ataques e o desenvolvimento de um sistema intermediário para transformar os registros de detecção em regras de proteção junto ao firewall do sistema Mikrotik RouterOS. Os resultados mostram que este sistema pode ser utilizado para automatizar o processo de reação aos ataques identificados pelo IDS SNORT, sem a necessidade de intervenção direta do administrador do sistema, impedindo o acesso de hosts identificados como suspeitos.*

1. Introdução

A Internet possibilitou uma mudança de paradigma no estilo de vida da sociedade. Normalmente essa rede é utilizada de forma adequada, mas existem sistemas ou pessoas que visam prejudicar o seu funcionamento, utilizar os recursos disponíveis de forma prejudicial ou ilegal, ou ainda, adquirir informações sem a devida autorização[Chaudhari et al. 2010] [Anand 2014].

Os Sistemas de Detecção de Intrusão (IDS - *Intrusion Detection System*) são desenvolvidos com o objetivo de monitorar, identificar, registrar e informar os administradores destes sistemas e/ou redes de computadores quando algum tipo de atividade maliciosa ou suspeita ocorre [Comer 1988] [Zaman and Karray 2009] [Njogu et al. 2013]. Estes sistemas operam realizando a leitura de informações contidas nos pacotes transmitidos pela rede e comparam os dados coletados com uma coleção de regras que permitem identificar ataques conhecidos [Junqi and Zhengbing 2008] [Hoque et al. 2014]. Estas regras podem conter assinaturas de ataques ou a descrição de um comportamento fora

das características normais de operação da rede/sistema, caracterizando uma anomalia [Chaudhari et al. 2010] [Anand 2014].

Apesar de realizar a identificação, o registro e o envio de alertas de ataques em uma rede/sistema, originalmente, um IDS não é capaz de reagir de forma a bloqueá-lo ou impedir novas tentativas. Da mesma forma, IDS não são capazes de reparar os danos causados por um ataque, ficando esta função sob responsabilidade exclusiva do administrador do sistema/rede [Njogu et al. 2013]. Por outro lado, sistemas de *firewall* são responsáveis por garantir o controle do acesso à rede ou dispositivo, impedindo ou restringindo o acesso de dispositivos, de acordo com as regras de controle e políticas de segurança estabelecidas pelo administrador da rede/sistema [Junqi and Zhengbing 2008].

Dentre as diversas soluções de IDS existentes, destaca-se o SNORT [SNORT 2015]. Este IDS é capaz de identificar diversos tipos de ataques, baseado tanto em assinaturas quanto em anomalias. Também possibilita a integração com algumas soluções de *firewall*, como por exemplo, com o sistema IPTABLES, através do uso de complementos. Contudo, sistemas como IPTABLES não são otimizados para esta tarefa e não possuem um *hardware* otimizado para tal finalidade, isto é, com um desenvolvimento voltado para a tarefa que se destina, diferente de soluções como Mikrotik RouterOS.

O sistema Mikrotik RouterOS é especializado no controle e gerenciamento de redes de dispositivos desenvolvido pela Mikrotik. Esta solução é executada de forma embarcada, utilizando para isso um *hardware*, também desenvolvido pela Mikrotik. Este sistema conta com um *firewall* que permite controlar todo o fluxo de dados transmitido pela rede. Contudo, não existe uma integração ou um complemento para integrar o IDS SNORT e o sistema de *firewall* do Mikrotik RouterOS. Com isso, este trabalho apresenta uma forma de integração entre as duas soluções, convertendo as detecções realizadas pelo IDS SNORT em regras de proteção no sistema de *firewall* do Mikrotik RouterOS para ampliar a capacidade de reação aos ataques.

O restante deste trabalho está organizado da seguinte maneira. Na Seção 2 é feita uma análise e comparação de diferentes IDS encontrados na literatura. O sistema desenvolvido é descrito na Seção 3 e os testes realizados e os resultados obtidos na Seção 4. A conclusão e as considerações finais são apresentadas na Seção 5.

2. TRABALHOS RELACIONADOS

Zaman *et* al. [Zaman and Karray 2009] destacam que o IDS utiliza diferentes critérios para restringir o tráfego, de acordo com a camada e tipos de ataques monitorados não é proposta nenhuma forma de integração destes sistemas aos *firewalls*. No trabalho de Chaudhari *et* al. [Chaudhari et al. 2010] é proposta uma classificação dos ataques de forma semi-supervisionada. Apesar de propor uma melhoria para os IDS e destacar seus principais objetivos, Chaudhari *et* al. não apresenta nenhum tipo de integração com algum tipo de sistema de proteção.

Já o trabalho de Valgenti *et* al. [Valgenti et al. 2014] propõe um filtro de tempo real para o tráfego da rede. Raghunath *et* al. [Raghunath and Mahadeo 2008] sugerem um modelo de mineração de dados para detectar comportamentos anormais em uma rede. Sherry *et* al. [Sherry et al. 2015], abordam o problema de detecção de intrusão baseado em assinaturas para pacotes criptografados. Mesmo com estas melhorias na identificação

de ataques, ainda existe a ausência de uma integração com um sistema para proteger a rede de novos incidentes, o que não é abordado por nenhum destes trabalhos.

O trabalho descrito em [Huang et al. 2010] apresenta uma integração entre um IDS e um sistema de *firewall*. Apesar de apresentar uma abordagem para a integração entre os IDS (SNORT) e um sistema de *firewall* não especificado, não contempla a integração com o sistema de *firewall* do Mikrotik RouterOS. O trabalho de Lei-Jun *et* al. [Lei-jun and Hong 2010] apresenta uma proposta de integração, de fato, entre estas duas soluções de segurança (*firewall* e IDS), apontando suas vantagens, desvantagens e desafios. Contudo, não menciona nenhum sistema em específico e conclui afirmando que este é ainda um modelo teórico e não apresenta sua implementação.

Considerando os trabalhos estudados na literatura, observou-se que o foco principal de estudo da maioria destes está relacionado a melhoria na detecção dos ataques. Apesar de alguns mencionarem que o IDS e o sistema de *firewall* se complementam, poucos tratam sobre esta integração, conforme mostra a Figura 1.

Trabalho	Integração	Automatização	SNORT	Mikrotik	Implementado
Zaman *et* al.	X	X	X	X	X
Chaudhari *et* al.	X	X	X	X	X
Valgenti *et* al.	X	X	X	X	X
Raghunath et *al.*	X	X	X	X	X
Lee *et* al.	X	X	X	X	X
Sherry *et* al.	X	X	X	X	X
Huang *et* al.	✔	✔	X	X	X
Lei-Jun *et* al.	✔	✔	X	X	X
Este Trabalho	✔	✔	✔	✔	✔

Figura 1. Comparativo entre trabalhos estudados e trabalho proposto

A Figura 1 mostra que mesmo os trabalhos que apresentam uma proposta de integração entre as duas ferramentas, não contemplam o sistema Mikrotik RouterOS. Desta forma, este trabalho propõe um sistema intermediário que utiliza os registros de detecção do IDS SNORT como fonte de informação para gerar regras de proteção no *firewall* do sistema Mikrotik RouterOS.

3. Trabalho Desenvolvido

A operação do sistema foi dividida em três etapas. A primeira delas refere-se a detecção dos ataques. Esta tarefa é de responsabilidade do IDS SNORT, operando como NIDS, o qual tem como principal funcionalidade identificar, registrar e notificar o administrador do sistema. A segunda refere-se ao sistema intermediário, foco deste trabalho, o qual tem a finalidade de capturar os registros do IDS SNORT, extrair as informações e utilizá-las na formatação das regras de proteção. A terceira trata da aplicação das regras criadas pelo sistema intermediário no sistema de *firewall* do sistema Mikrotik RouterOS.

3.1. Arquitetura

A arquitetura desenvolvida para este sistema está distribuída em três fases: (i) Detecção, (ii) Extração e Conversão e (iii) Aplicação, conforme apresenta a Figura 2.

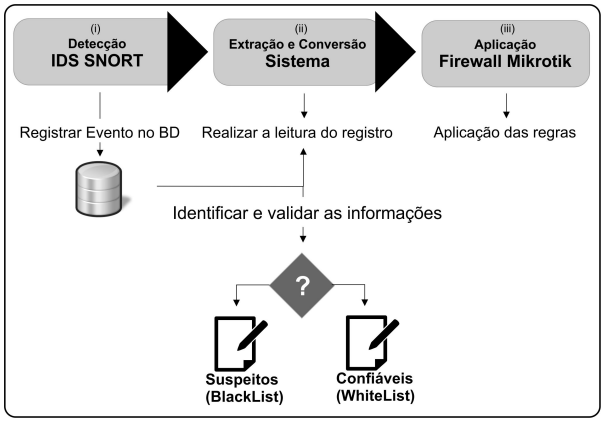

Figura 2. Fluxo dos processos do sistema desenvolvido

A fase de detecção é responsável por identificar os ataques. Para isso, utiliza-se o IDS SNORT. Sempre que identificado um incidente, é realizado o registro desta ocorrência. Para o desenvolvimento deste trabalho, foram utilizados complementos para armazenar estas informações em uma base de dados. Esta base é utilizada na próxima etapa, para extrair todo o conteúdo necessário para operação das próximas fases do processo.

Para identificar ataques ou acessos não permitidos, primeiramente foi necessário estabelecer uma política de utilização da rede. Para isso foram elaboradas regras de detecção que identificam situações que ”desrespeitassem”algumas restrições estabelecidas pelo administrador. Dentre as regras desenvolvidas, por exemplo, identificar conexões na porta TCP 80. Outra regra refere-se ao serviço de DNS, via porta UDP 53 e ao serviços de FTP. Também foram descritas regras para identificar tentativas de conexões à base de dados através da porta 3306. Além disso, foi elaborada uma regra que permite identificar ataques externos de PING *Flood*, onde um atacante envia inúmeras requisições de PING sem aguardar resposta, com o intuito de sobrecarregar o sistema e causar a indisponibilidade de recursos e serviços.

Na segunda etapa ocorre a leitura dos registros realizados pelo IDS SNORT, a extração das informações e formatação das regras de proteção. Estas regras serão aplicadas ao módulo de *firewall* do sistema Mikrotik RouterOS, afim de identificar o endereço que originou o ataque e qual o *host* de destino do ataque. Da mesma forma, pode-se identificar a regra que gerou o alerta e quando o ataque ocorreu, além de visualizar o protocolo e as portas utilizadas. Com estas informações já é possível criar as regras que impeçam o acesso deste *host* de origem à rede, prevenindo novos ataques descritos nas regras utilizadas. Nesta etapa o sistema intermediário captura estas informações do registro das ocorrências e realiza a identificação dos atributos necessários para elaborar as regras de proteção, como por exemplo, endereço IP de origem utilizado para realizar o ataque.

As informações extraídas do registro de ocorrências do IDS SNORT são aplicadas na criação das regras de proteção do sistema de *firewall* de Mikrotik RouterOS e servem para popular uma lista de *hosts* classificados como suspeitos junto ao sistema Mikrotik

RouterOS. Os endereços de IP identificados como origem do ataque são inseridos nesta lista e terão o seu acesso à rede negado pelo *firewall* permanentemente até que o administrador remova-os desta lista de controle. Com esta abordagem, busca-se minimizar problemas de detecção do tipo falso negativo, isto é, permitir acesso à rede aos *hosts* identificados como suspeitos.

Contudo, é necessário realizar uma validação destes endereços de origem. Os endereços não são registrados na lista de suspeitos caso estejam registrados na lista de *hosts* confiáveis. Esta lista é mantida pelo administrador da rede e identifica os *hosts* que não devem ter o acesso à rede bloqueada, mesmo que identificados como origem de um possível ataque pelo IDS SNORT. Esta abordagem busca evitar o bloqueio de ocorrências de falsos positivos, isto é, quando acessos legítimos à rede são identificados como ataques.

O sistema permite ao administrador do sistema registrar manualmente, via um painel de administração, *host* conhecidos e identificados como maliciosos, bem como *host* definidos como "Confiáveis". Isso permite ao sistema impedir o acesso destes host mesmo que o IDS não identifique seus endereços como maliciosos e garante que os endereços contidos na lista de "confiáveis"não devem ser bloqueados pelo sistema por se tratarem de *hosts* definidos como seguros, devendo ser ignorada a criação de regras de bloqueio junto ao sistema de firewall do Mikrotitik RouterOS. É importante ressaltar que, neste caso, outros mecanismos de controle e de segurança para estes endereços definidos como "confiáveis"devem ser adotados, a fim de garantir a segurança da rede.

O painel de administração do sistema, permite além da manutenção das configuração de *host* confiáveis e suspeitos, alterar e ajustar o tempo de ciclo de leitura das informações de registro do IDS. Ciclos de tempo muito altos podem resultar em reações retardadas à ataques, ao passo que ciclos de leitura muito curtos, podem gerar sobrecarga de leitura do sistema, dependendo do volume de dados contidos nos registros do IDS.

Após identificar e gerar as regras de proteção, é necessário aplicá-las ao *firewall*. Para isso, o sistema desenvolvido estabelece uma conexão através da API da Mikrotik, e realiza a execução do conjunto de comandos necessários para efetuar os registros. Após a conexão com o sistema Mikrotik, é realizada a criação de bloqueio total de acesso para todos os *hosts* que estão na lista de suspeitos. Assim, o acesso à rede é totalmente negado a estes *hosts*, impedindo novos ataques através da regra de *firewall*. Com isso, reduz-se também o volume de dados maliciosos, permitindo ao IDS SNORT dedicar recursos computacionais à identificação de outros ataques com origens diferentes dos *hosts* já identificados.

4. Resultados

Para validar este trabalho foi elaborado um ambiente, bem como um conjunto de regras que permitissem ao IDS SNORT identificar atividades que desrespeitassem a política de utilização definida para a rede e/ou ataques à rede. A Figura 3 apresenta o ambiente utilizado para realização dos testes e validação da aplicação desenvolvida. Foi utilizada uma RouterBOARD modelo 1100, com sistema Mikrotik embarcado operando na versão 6.28, como dispositivo Servidor IDS, foi utilizado um processador Intel Core 2 Duo de 2.0 GHz, 3Gb de RAM e Ubuntu Server 14, com PHP e MySQL. Para simular estações de trabalho foram utilizados 3 computadores. Estes dispositivos foram conectados à Rou-

terBOARD e o conteúdo transmitidos pelas suas respectivas interfaces de conexão, foram espelhados para a porta de conexão do IDS SNORT v.2.9.7. Para simular os acessos na rede de teste foram realizados diferentes tipos de acessos aos serviços que infringissem à política de utilização da rede.

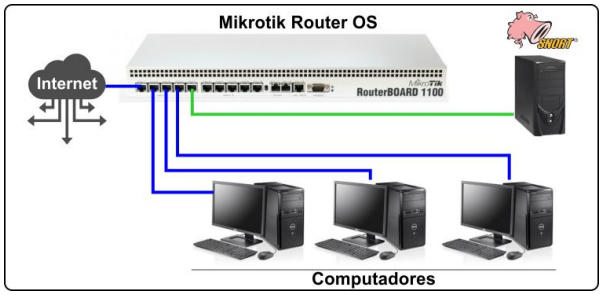

Figura 3. Ambiente de teste

Para validar a regra de detecção de acessos aos serviços que utilizam a porta 80, foram realizados acessos a websites e realizados acessos ao servidor configurado junto ao IDS SNORT, o que também não é permitido de acordo com política estabelecida. Ao acessar estas páginas, também foi validada a detecção para o serviço de DNS. Para verificar a regra que trata da porta TCP 3306, padrão para conexões com base de dados Mysql, foram realizados acessos de uma rede externa à base de dados instalada junto ao servidor IDS SNORT. Da mesma forma, foram realizados acessos, internamente à rede, à mesma base, o que também contraria as regras de detecção. Ainda sobre os testes de detecção, foi simulada uma tentativa de PING *Flood*, utilizando a ferramenta disponível pelo sistema Mikrotik RouterOS. Neste teste foram enviadas 1000 requisições de PING por milissegundo ao IDS SNORT (IP 10.1.1.254).

Para avaliar as funcionalidades do sistema, o intervalo de verificações foi alterado de 10s para 30s, sendo observada a operação do sistema enquanto esta funcionalidade estava ativada e os resultados comparados com a funcionalidade desativada. Após, foram realizados testes para validar os recursos de controle de listas de endereços IP, onde foram adicionados endereços à lista de confiáveis e verificado o tratamento do sistema à estes endereços. Da mesma forma, foi realizada a remoção destes endereços da lista de confiáveis e observado se o sistema tornava a considerar estes endereços para criação das regras de proteção.

Os resultados obtidos através da análise da utilização da rede mostram que o IDS SNORT conseguiu identificar as violações geradas e registrar as informações referentes à estas ocorrências com sucesso. No caso do acesso à websites, o IDS SNORT identificou e registrou as ocorrências, as quais foram utilizadas pelo sistema para a geração das regras de proteção. Da mesma forma, o sistema desenvolvido foi capaz de ler as informações do registro do IDS SNORT e realizar a inserção destas informações à tabela auxiliar, responsável por armazenar os endereços de IP que terão seu aceso bloqueado (midle_db.ip_blaclist). No que diz respeito à simulação de ataque de PING *Flood*, utilizando a ferramenta disponível pelo sistema Mikrotik, o sistema IDS SNORT foi capaz de identificar e registrar este ataque.

Apesar de ter simulado o ataque de PING *Flood* através da RouterBOARD Mikrotik, a qual estava utilizando o endereço IP 10.1.1.1, este foi apenas detectado, sem a inserção do mesmo na lista de bloqueio. Isto por que este endereço IP está presente na lista de confiáveis. Esse resultado valida com sucesso à operação do sistema, respeitando a lista de confiáveis, evitando o bloqueio do acesso aos *hosts* e reduzindo a ocorrência de falsos positivos. Sobre os testes de acesso à base de dados Mysql, o IDS SNORT foi capaz de identificá-los com sucesso. Também identificou as tentativas de comunicação com servidores DNS utilizando a porta UDP 53.

Através dos alertas gerados pelo IDS SNORT, o sistema desenvolvido também conseguiu identificar os endereços de IP de origem dos ataques e bloqueá-los, através da inserção deste endereços IP na lista do *firewall* do Mikrotik RouterOS, respeitando a lista de *hosts* confiáveis. Foi verificado se os endereços de IP registrados como suspeitos (que devem ter regras de bloqueio junto ao *firewall* do Mikrotik RouterOS) de fato estavam inseridos na lista de bloqueio SNORT_DETECTION do *firewall*. A Figura 4.a apresenta os endereços inseridos na tabela midle_db.ip_blacklist. Já a Figura 4.b mostra a lista gerada no *firewall*, com todos os endereços devidamente inseridos.

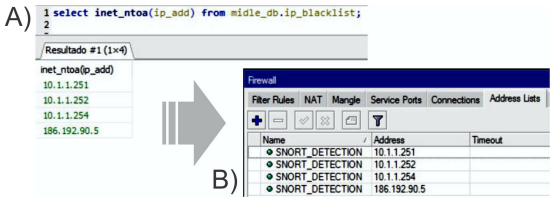

Figura 4. Comparativo: Informações de registro X Regras *firewall*

O sistema também foi capaz de realizar a remoção dos endereços de IP da lista de bloqueio do Mikrotik RouterOS, quando estes endereços de IP foram adicionados à lista de *hosts* confiáveis. Desta forma garantiu-se as configurações estabelecidas pelo administrador. Essa funcionalidade validou o controle das tabelas do sistema e a aplicação da *trigger*, responsável por manter a integridade destas regras.

Finalizando, é possível afirmar que, dentro do ambiente testado, o IDS SNORT foi capaz de identificar ataques baseado nas regras desenvolvidas. Da mesma forma, o sistema proposto cumpriu com seu objetivo e realizou o bloqueio do acesso dos *hosts* identificados como suspeitos. Para realizar esse bloqueio, o sistema utilizou-se dos registros de detecção para gerar regras e inserí-las automaticamente no *firewall* do Mikrotik RouterOS, formando uma ferramenta reagente aos ataques.

5. Considerações finais

Os resultados demonstraram que o sistema intermediário implementado foi capaz de aplicar, de forma automatizada, regras de controle de acesso ao sistema de *firewall* e impedir o acesso de *hosts* identificados pelo IDS como suspeitos. É importante ressaltar que o sistema proposto ainda não é totalmente automatizado, sendo dependente da intervenção do administrador para configurações de inicialização, tempo de ciclo do processo e de inserção de *hosts* definidos como confiáveis.

Como melhorias possíveis, pode-se mencionar a possibilidade de integração do presente trabalho com outros sistemas de IDS e outros sistemas de *firewall*. Contudo, estas novas integrações demandam estudos sobre métodos possíveis de comunicação entre estes sistemas e padrões de registro das informações dos IDSs. Pode-se ainda replicar as regras de proteção para outros dispositivos de forma pró-ativa.

Referências

Anand, V. (2014). Intrusion detection: Tools, techniques and strategies. In *Proceedings of the 42Nd Annual ACM SIGUCCS Conf. on User Services*, SIGUCCS '14, pages 69–73, New York, NY, USA. ACM.

Chaudhari, N., Tiwari, A., Thakar, U., and Thomas, J. (2010). Semi-supervised classification for intrusion detection system in networks. In *Cybernetics and Intelligent Systems (CIS), 2010 IEEE Conf. on*, pages 120–125.

Comer, D. (1988). *Internetworking with TCP/IP: Principles, Protocols, and Architecture*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA.

Hoque, N., Bhuyan, M. H., Baishya, R., Bhattacharyya, D., and Kalita, J. (2014). Network attacks. *J. Netw. Comput. Appl.*, 40(C):307–324.

Huang, X., Wang, X., and Zhu, S. (2010). Study on intelligent firewall system combining intrusion detection and egress access control. In *Intelligent System Design and Engineering Application (ISDEA), 2010 International Conf. on*, volume 2, pages 456–459.

Junqi, W. and Zhengbing, H. (2008). Study of intrusion detection systems (idss) in network security. In *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conf. on*, pages 1–4.

Lei-jun, L. and Hong, P. (2010). A defense model study based on ids and firewall linkage. In *Information Science and Management Engineering (ISME), 2010 International Conf. of*, volume 2, pages 91–94.

Njogu, H. W., Jiawei, L., Kiere, J. N., and Hanyurwimfura, D. (2013). A comprehensive vulnerability based alert management approach for large networks. *Future Gener. Comput. Syst.*, 29(1):27–45.

Raghunath, B. R. and Mahadeo, S. N. (2008). Network intrusion detection system (nids). *Emerging Trends in Engineering & Technology, International Conf. on*, 0:1272–1277.

Sherry, J., Lan, C., Popa, R. A., and Ratnasamy, S. (2015). Blindbox: Deep packet inspection over encrypted traffic. *SIGCOMM Comput. Commun. Rev.*, 45(5):213–226.

SNORT (2015). The snort project. Disponível em: <http://www.snort.org/>. Acesso em: Dezembro de 2015.

Valgenti, V., Sun, H., and Kim, M. S. (2014). Protecting run-time filters for network intrusion detection systems. In *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conf. on*, pages 116–122.

Zaman, S. and Karray, F. (2009). Tcp/ip model and intrusion detection systems. In *Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conf. on*, pages 90–96.