colloquium exactarum

SEGURANÇA EM REDES DE COMPUTADORES USANDO SISTEMAS DE DETECÇÃO DE INTRUSÃO BASEADOS EM FLUXOS

COMPUTER NETWORK SECURITY USING INTRUSION DETECTION SYSTEMS BASED FLOWS

Eduardo Massato Kakihata, Helton Molina Sapia, Ronaldo Toshiaki Oikawa, Danillo Roberto Pereira, Francisco Assis da Silva

Universidade do Oeste Paulista, Bacharel em Ciência da Computação, Presidente Prudente, SP.
E-mail: eduardomassato@hotmail.com

RESUMO - O uso constante de internet por diferentes tipos de dispositivos ocasiona um grande fluxo de informações confidencias e pessoais. Essas informações em posse de criminosos ou estelionatários podem causar grandes danos às instituições ou a seus colaboradores. Devido a tal situação, julga-se necessário utilizar ferramentas de segurança computacional, como por exemplo, Sistemas de Detecção de Intrusão (do inglês, *Intrusion Detection System* – *IDS*). Este trabalho apresenta um *IDS* capaz de realizar a análise baseada em fluxos de rede (*netflow*). A metodologia proposta realizou uma análise de comportamentos maliciosos em fluxos previamente coletados e detectou corretamente três diferentes tipos de comportamentos maliciosos. A análise baseada em fluxos mostrou-se eficiente na tarefa de detectar atos maliciosos, além disso o número de itens a serem verificados por meio desta abordagem é consideravelmente menor do que a baseada em pacotes de rede.
Palavras-chave: Sistema de Detecção de Intrusão; Segurança da Informação; Segurança em Redes; Fluxo de Rede.

ABSTRACT - The use of internet by different types of devices causes a large flow of confidential and/or personal informations. This informations in the possession of criminals can cause extensive damage to persons, institution and government. Due to this situation, it is necessary to use computer security tools, such as Intrusion Detection Systems (IDS). This work presents an IDS that can perform the flow-based analysis (*netflow*). The proposed approach realizes an analysis of malicious behaviors in flows that were previously collected, and detected correctly three different types of malicious behavior. The flow-based analysis was efficient to detecting malicious acts, moreover the data number to be scanned of the proposed approach is considerably smaller than the packet-based analysis.
Keywords: Intrusion Detection System; Information Security; Security In Networks; Netflow.

Recebido em: 19/08/2015
Revisado em: 26/08/2015
Aprovado em: 01/09/2015

1. INTRODUÇÃO

À medida que a tecnologia vem evoluindo, aumenta a probabilidade de um sistema informatizado conter falhas e brechas de segurança (BATISTA, 2012). Analisando essa situação, se faz necessário utilizar mecanismos operacionais de segurança, conhecidos como sistemas de detecção de intrusão (*IDS*) e sistemas de prevenção de intrusão (*firewall*). Esses mecanismos têm como objetivo de fornecer um ambiente seguro à rede, garantindo a prevenção e detecção de ataques cibernéticos ou intrusões (KUROSE, 2010). Intrusões ou ataques são ações que visam comprometer a integridade, confidencialidade ou disponibilidade de um recurso computacional, independente de obter sucesso ou não (STALLINGS, 2008).

Os métodos de detecção podem ser classificados segundo uma das abordagens: por mau uso (assinatura) ou anomalia (LIMA, 2005). O *IDS* baseado em assinaturas analisa padrões pré-definidos de ataques, ou seja, para cada ataque se tem uma assinatura. Já o *IDS* baseado em anomalia analisa ações diferentes do padrão normal do sistema, sendo que para cada ação normal do sistema é criado um perfil, e quando uma ação realizada não corresponde a um dos perfis criados o *IDS* alerta que o sistema possivelmente está sofrendo ataque (STALLINGS, 2008).

Atualmente, a maioria dos *IDS* realiza a análise baseada em pacotes de rede, foi proposta a iniciativa de implementar um *IDS* que faz a análise baseada em fluxo de rede. Um fluxo de rede é uma sequência unidirecional entre dois *host*s na rede, e é representada por um tráfego com características similares (CORRÊA, 2009).

Redes de médio ou grande porte geram um número significativo de pacotes, consequentemente requer um custo computacional considerável para que seja realizada a sua análise. Visto que um fluxo é uma versão resumida dos pacotes trafegados, a análise dos fluxos exige a *priori* o armazenamento para posteriormente serem analisados. Foi utilizada uma ferramenta capaz de coletar e armazenar os fluxos da rede em um banco de dados MySQL.

Após o armazenamento, o *IDS* proposto neste trabalho tem como intuito realizar verificações do comportamento da rede por meio de consultas no banco de dados. Posteriormente o comportamento é procurado de acordo com as assinaturas maliciosas de modo a alertar se algum *host* da rede sofreu ataque. O objetivo deste estudo foi desenvolver um *IDS* que realiza análise baseada em fluxo e verificar sua

viabilidade na detecção de três comportamentos maliciosos.

O restante do trabalho está organizado da seguinte maneira. Na Seção 2 se encontra a fundamentação teórica explicando conceitos da área. A Seção 3 apresenta a metodologia utilizada. Os resultados obtidos são descritos na Seção 4. A Seção 5 discute os resultados previamente apresentados. Por fim, a Seção 6 apresenta as conclusões e propostas futuras.

2. FUNDAMENTAÇÃO TEÓRICA

O *port scanning* (escaneador de portas) consiste em enviar um pacote a cada porta e esperar a resposta, possibilitando determinar no alvo se uma porta está respondendo requisições ou não (GIAVAROTO, 2013). Para realizar o *port scanning*, foi utilizada a ferramenta *NMAP* que tem como funções: descobrir alvos online, detecção de serviços e sistemas operacionais junto com suas respectivas versões, além de outras funcionalidades (MORENO, 2015).

O ataque de força bruta é executado em *hosts* que possuem o serviço *SSH (Secure Shell Protocol)*, que normalmente utilizam a porta 22. Esse ataque visa descobrir *login* e senha por meio de combinações de caracteres e números até que o mesmo seja decifrado (CORRÊA, 2009). Para gerar os fluxos do ataque força bruta foi utilizada a ferramenta *HYDRA*, que realiza a quebra de senhas (GIAVAROTO, 2013).

O ataque de *Denial of Service (DoS)* possui diferentes meios de ser realizado, seja por meio de inundação pacotes ICMP, inundação SYN, entre outros. Neste trabalho foi utilizada a inundação de pacotes ICMP, que consiste em enviar uma grande quantidade de pacotes ICMP ao alvo no menor tempo possível, resultando na lentidão do alvo em atender novas conexões ou até mesmo tornando-o inoperante na rede (MCCLURE, 2003). Para esse tipo de ataque, foi utilizada a ferramenta *HPING3*, um gerador de pacotes que tem como uma de suas funções, testar o desempenho da rede (MORENO, 2015).

3. METODOLOGIA

Foi realizado um estudo detalhado sobre fluxos de redes, principalmente os campos que o integram. Por meio de uma análise, foi possível combinar características de *IDS* e ferramental teórico de modo a obter uma detecção eficiente por meio de assinaturas.

Depois de compreender os campos que compõem um fluxo de rede, algumas informações foram selecionadas para realizar a criação de assinaturas dos comportamentos maliciosos. Posteriormente estas assinaturas foram usadas na identificação de padrões maliciosos. Os campos utilizados foram

escolhidos segundo sua importância no processo de identificação da ação (normal/maliciosa); são eles: *srcaddr* (endereço IP origem), *dstaddr* (endereço IP destino), *srcport* (porta origem), *dstport* (porta destino), *dPkts* (quantidade de pacotes no fluxo), *dOctets* (quantidade de bytes no fluxo), *first* (tempo em milissegundos da entrada do primeiro pacote no fluxo), *last* (tempo em milissegundos da entrada do ultimo pacote no fluxo) e *prot* (tipo de protocolo). A partir dos campos selecionados, foi possível aferir outras informações importantes como duração do fluxo (*last* – *first*) e media de bytes por pacote (*dOctets* / *dPkts*).

Este trabalho utiliza três assinaturas, duas foram baseadas em assinaturas apresentadas no trabalho de Corrêa (2009), portanto foram adaptadas para o ambiente de pesquisa e a outra foi criada no decorrer do desenvolvimento deste trabalho.

A assinatura do comportamento de um *port scanning* consiste em duas etapas: (i) seleção de endereços IP que acessaram diversas portas distintas em um mesmo IP destino; (ii) análise da quantidade de fluxos de acordo com a assinatura para cada *host* origem e destino apresentado da etapa anterior. Caso os fluxos apresentem o campo *prot* igual a 6 (referente ao protocolo TCP), e quantidade de bytes no fluxo entre 150 a 154, e bytes por pacote entre 48 a 52, e duração menor que 15 segundos, e ultrapasse a quantidade de 100 fluxos neste padrão, é disparado um alarme que avisa que o *host* destino sofreu um ataque de *port scanning*.

A assinatura do ataque de força bruta também consiste de duas etapas, são elas: (i) verificação de *hosts* que realizaram um número considerável de tentativas de acesso a um mesmo *host* destino na porta 22; (ii) analisar se todo *host* origem e destino (apresentado da etapa anterior) apresenta fluxos com o campo prot igual a 6, e bytes por pacote entre 85 a 105, e duração menor que 15 segundos e ultrapasse a quantidade de 15 fluxos, então o *host* destino é alertado que sofreu um ataque de força bruta.

A assinatura do ataque de *DoS* consiste em somente uma etapa onde se verifica qual *host* enviou uma quantidade de pacotes ICMP (que é representado pelo campo *prot* com valor igual a 1) maior que 40.000 em um único fluxo e média de bytes por pacote igual a 28. Também foi observado que os fluxos do ataque tinham porta destino igual a 8.

Com as três assinaturas geradas, o *IDS* desenvolvido realiza a verificação dos fluxos que estão armazenados em um banco de dados, e caso o comportamento da rede consultado esteja de acordo com alguma das assinaturas geradas, o *IDS* alerta que algum *host* sofreu um dos atos maliciosos previstos.

4. RESULTADOS

O estudo foi realizado no ambiente de teste da Faculdade de Informática de Presidente Prudente (FIPP). Conforme pode ser observado na Tabela 1, a base de dados contém 317.838 fluxos, e dentro desses fluxos existe cerca de 4.610.545 pacotes.

Tabela 1. Resultado do total de fluxos x total de pacotes da base de dados.

	Qtde_Fluxos	Qtde_Pacotes
▶	317838	4610545

Fonte: Autoria própria.

Nas Tabelas e Figuras abaixo são exibidos alguns resultado dos passos das assinaturas que compõem o *IDS* desenvolvido.

Tabela 2. Resultado da primeira etapa da assinatura de *port scanning*.

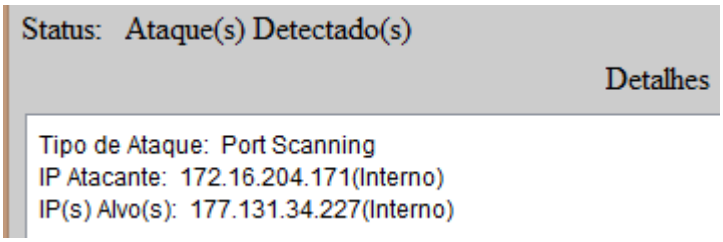
	origem	destino	n_portasverificadas
▶	172.16.204.171	177.131.34.227	563
	177.131.34.227	172.16.204.171	938
	177.131.34.227	177.131.33.3	216
	177.131.34.227	200.27.2.2	198

Fonte: Autoria própria.

Como pode ser visto na Tabela 2, foram detectado 4 situações em que um determinado endereço origem acessa diversas portas em um determinado endereço destino. O próximo passo consistiu em verificar se para cada IP origem e destino apresentado na consulta anterior de fato está ocorrendo ou não um *port scanning*.

De quatro situações apresentadas na Tabela 2, três não foram consideradas ataque de *port scanning* devido a quantidade de fluxos correspondente ao padrão da assinatura não ultrapassar 100, ou seja, os fluxos não apresentaram todas as características estabelecidas como: protocolo TCP, bytes no fluxo entre 150 a 154, bytes por pacote entre 48 a 52 e duração menor que 15 segundos.

Figura 1. Resultado da segunda etapa da assinatura de *port scanning* (tela da *IDS* desenvolvido).



Fonte: Autoria própria.

Na Figura 1 pode ser observado que das quatro situações apresentadas no primeiro passo, somente uma foi considerado ataque de *port scanning*.

Tabela 3. Resultado da primeira etapa da assinatura de força bruta.

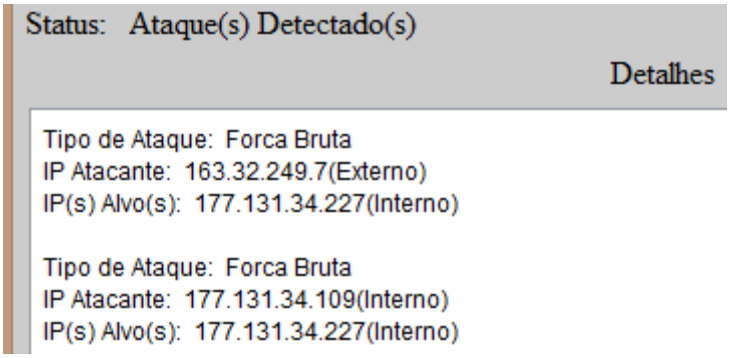
	origem	destino	tentativas
▶	163.32.249.7	177.131.34.224	35
	177.131.34.109	177.131.34.227	99
	59.45.79.117	177.131.34.227	253

Fonte: Autoria própria.

Conforme pode ser observado na Tabela 3, o primeiro passo da detecção da assinatura do ataque de força bruta, foram identificados 3 endereços IP que realizaram uma quantidade de tentativas ao serviço *SSH* por meio da porta 22 no IP destino. Posteriormente foi verificado se realmente para cada situação apresentada é de fato um ataque de força bruta ou não.

Entre as situações apresentadas na Tabela 3, uma não foi considerada ataque de força bruta devido à quantidade de fluxos correspondentes ao padrão da assinatura não ultrapassar 15, ou seja, os fluxos não apresentaram todas as características estabelecidas como: protocolo TCP, bytes por pacote entre 85 a 105 e duração menor que 15 segundos.

Figura 2. Resultado da segunda etapa da assinatura de força bruta (tela do *IDS* desenvolvido)



Fonte: Autoria própria.

O resultado, conforme pode ser observado na Figura 2, mostra que das 3 situações apresentadas no primeiro passo, somente 2 são de ataques de força bruta.

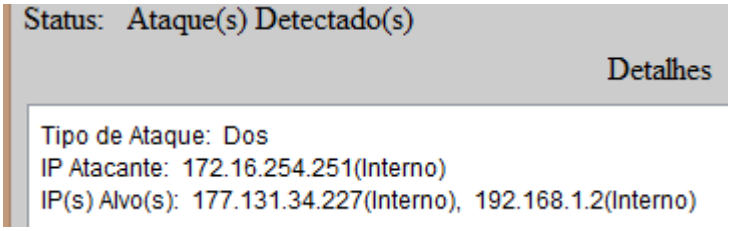
Tabela 4. Resultado da consulta para assinatura de *DoS*.

origem	destino	Qtde_pacotes	protocolo
172.16.254.251	177.131.34.227	64922	1
172.16.254.251	177.131.34.227	63030	1
172.16.254.251	177.131.34.227	55835	1
172.16.254.251	192.168.1.2	55835	1
172.16.254.251	177.131.34.227	53191	1
172.16.254.251	192.168.1.2	53191	1

Fonte: Autoria própria.

A assinatura do ataque de *DoS,* conforme apresenta a Tabela 4, detectou alguns fluxos que contém uma quantidade de pacotes ICMP maior que 40.000 (no mesmo fluxo).

Figura 3. Resultado da assinatura de *DoS* (tela do *IDS* desenvolvido)



Fonte: Autoria própria.

O resultado da detecção do ataque *DoS* pode ser visto na Figura 3, e nele foi possível observar que todos os fluxos listados eram tentativas de ataque válidas, sendo quatro contra o *host* cujo IP é 177.131.34.227 e os outros dois contra o *host* cujo IP é 192.168.1.2.

Tabela 5. Comportamentos maliciosos que contém na base de dados

Comportamento Malicioso	**Quantidade**
Port Scanning	4
Força Bruta	20
DoS	3
Total	**27**

Fonte: Autoria própria

A base de dados de fluxos contém 27 ataques, conforme descriminado na Tabela 5. A ferramenta acadêmica criada conseguiu detectar todos os ataques descritos acima.

5. DISCUSSÃO

Ao realizar consultas em um banco de dados MySQL onde os fluxos estão armazenados, nos casos em que as informações consultadas se encaixem com as características das assinaturas, é avisado que algum *host* da rede sofreu determinado ato malicioso. A ferramenta foi capaz de identificar todas as tentativas de comportamentos maliciosos gerados propositalmente, e também conseguiu identificar ataques com origem externa, ou seja, alguém de fora realizando ataque de força bruta tentando descobrir o usuário e senha para obter acesso a um dos servidores do nosso ambiente por meio da internet.

Ainda com relação ao fato de não terem sido detectados ataques de *DoS* de origem externa, foi observado posteriormente que o ambiente de pesquisa estava protegido por *firewall* externo que impedia a entrada de pacotes ICMP.

6. CONCLUSÃO

A ferramenta acadêmica criada realiza a detecção de comportamentos maliciosos por meio da análise baseada em fluxos de rede. Ela detectou todos os atos maliciosos gerados propositalmente, e também foi possível detectar ataques de força bruta sem

ser de autoria própria. Os outros dois comportamentos maliciosos não foram detectados devido às configurações do *firewall* que bloqueia alguns pacotes.

O trabalho apresentou algumas limitações, o coletor dos fluxos não armazenou alguns campos importantes, como por exemplo, o *tcp_flags*. Essa limitação impediu a realização de verificações mais precisas em relação ao comportamento da rede. Também houve a dificuldade em encontrar base de dados de pesquisas similares na internet, impossibilitando assim a comparação das assinaturas aqui apresentadas com outros métodos de detecção de intrusão.

A base de dados utilizada neste trabalho foi gerado pelos pesquisadores usando o ambiente de pesquisa da FIPP *NetBuilder*.

Como trabalhos futuros sugere-se organizar e normalizar os dados armazenados dos fluxos para que possa ser usado em algoritmos de aprendizado de máquina, que terá o objetivo de classificar cada fluxo verificado como comportamento malicioso ou não, podendo posteriormente analisar qual algoritmo de aprendizado de máquina obteve melhor resultado em relação ao número de erros e acertos.

REFERÊNCIAS

BATISTA, M.L. **Análise de eventos de segurança em redes de computadores utilizando detecção de novidade**. 2012. Dissertação (Mestrado) - Universidade Estadual Paulista “Júlio de Mesquita Filho”, São José do Rio Preto, São José do Rio Preto – SP.

CORRÊA, J.L. **Um modelo de detecção de eventos em redes baseado no rastreamento de fluxos**. 2009. Dissertação (Mestrado) - Universidade Estadual Paulista “Júlio de Mesquita Filho”, São José do Rio Preto – SP.

GIAVAROTO, S. C. R.; SANTOS, G. R., **Backtrack Linux auditoria e teste de invasão em redes de computadores.** Rio de Janeiro: Ciência Moderna, 2013.

KUROSE, J.F. **Redes de computadores e a internet: uma abordagem top-down.** 5. ed. São Paulo: Pearson, 2010.

LIMA, I. **Uma abordagem simplificada de detecção de intrusão baseada dm redes neurais artificiais**. 2005. Dissertação (Mestrado) - Universidade Federal de Santa Catarina, Florianópolis – SC.

MCCLURE, S. et al. **Hackers expostos.** 4. ed. Rio de Janeiro: Campus, 2003.

MORENO, D. **Introdução ao Pentest.** São Paulo: Novatec, 2015.

STALLINGS, W. **Criptografia e segurança em redes.** 4. ed. São Paulo: Pearson, 2008.