Intrusion Detection Systems' Performance for Distributed Denial-of-Service Attack

Tiago Emílio de Sousa Araújo
Centro de Informática – Programa de Pós-Graduação em Informática
Universidade Federal da Paraíba - UFPB - João Pessoa, Brasil
tiagoaraujo@ppgi.ci.ufpb.br

Fernando Menezes Matos
Centro de Informática – Programa de Pós-Graduação em Informática
Universidade Federal da Paraíba - UFPB - João Pessoa, Brasil
fernando@ci.ufpb.br

Josilene Aires Moreira
Centro de Informática – Programa de Pós-Graduação em Informática
Universidade Federal da Paraíba - UFPB - João Pessoa, Brasil
josilene@ci.ufpb.br

***Abstract*— Intrusion Detection Systems (IDSs) are signature-based software tools that provide mechanisms for detection and analysis of network intrusions. Using an experimental scenario and real traffic collected at a higher education institution in Brazil, we evaluate the performance of Snort and Suricata IDSs for detection of current Distributed Denial-of-Services attack (Slowloris). Our study has found the IDS Suricata is not a suitable number for alerts to catch the attention of the network manager about the Slowloris attack, while Snort IDS does. Evaluation of CPU consumption and memory of target server. In addition, an analysis of offline traffic reveals that the higher education institution is under DDoS attacks during the analyzed period.**

Keywords—DDoS attack; Intrusion detection systems; IDS performance; network security.

I. INTRODUÇÃO

ATAQUES de negação de serviço (Denial of Service - DoS) não visam adquirir informações confidenciais, alterar informações ou disseminar softwares maliciosos pela rede; seu principal objetivo é tornar indisponíveis aos usuários legítimos os serviços acessados pela Web [1]. De acordo com a CISCO, o número de ataques DoS detectados globalmente em 2015 foi de 6,6 milhões, devendo aumentar para 17,4 milhões em 2020, o que representa uma taxa anual de crescimento de 21% [2]. A Verisign, empresa que atua na área de segurança na Internet, destaca em sua análise lançada no final do segundo trimestre de 2016 que a quantidade de ataques DoS aumentou em 75% em um ano, e que 64% das ocorrências detectadas neste trimestre foram coordenadas para usar mais de uma variante de ataques DoS simultaneamente, dificultando a sua identificação. O tamanho médio do pico destes ataques detectados pelos serviços da companhia foi de 17,37 Gbps, um crescimento de 214% quando comparado ao mesmo período de 2015 [3].

Em 21 de outubro de 2016 aconteceu um dos maiores ataques distribuídos de negação de serviço (*Distributed Deny of Service* - DDoS) que se tem notícia na história. O alvo do ataque foi um grande provedor de acesso[1] localizado nos Estados Unidos e a consequência foi a retirada do ar de diversos sites que figuram entre os mais populares da Internet. Foram afetados o *Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest* e *Fox News* assim como os jornais The Guardian, The New York Times e The Wall Street Journal, entre outros. Embora os usuários dos Estados Unidos e da Europa tenham sido os mais afetados, também foram sentidos reflexos na América do Sul, incluindo o Brasil, Uruguai e Argentina, assim como na Índia e na Austrália [4][5].

Entre as formas de detecção de intrusão mais atuais encontram-se os Sistemas de Detecção de Intrusão (Intrusion Detection Systems - IDS), que é um conjunto de ferramentas de software que permitem a detecção e a análise de intrusões em redes [6]. Os IDS são capazes de detectar diversos tipos de ataques e intrusões e, em geral emitem alertas para o administrador que, ao ser avisado do ataque, pode iniciar ações para mitigá-lo e diminuir ou evitar as suas consequências [7]. Os IDSs Snort e o Suricata são sistemas de detecção de intrusão muito utilizados globalmente. O primeiro foi desenvolvido por Martin Roesch e adquirido pela CISCO em 07 de outubro de 2013 e hoje é utilizado por várias empresas [8]. O segundo é um IDS desenvolvido e mantido pela Open Information Security Foundation (OISF), este sistema foi criado para implementar algumas novas ideias e tecnologias no campo de detecção de intrusões, sendo a principal vantagem seu mecanismo multithread [9].

O presente trabalho analisa os mecanismos de ação e a eficácia dos IDS Snort e Suricata para a detecção de ataque DDoS. O IDS Snort é o único software na categoria de sistema de detecção de intrusão (IDS) que aparece na lista das soluções de segurança mais usadas globalmente, ocupando o 8º lugar no ranking mundial [8][10]. Por ser mundialmente respeitado, gratuito e de ampla utilização, foi escolhido para o nosso estudo, juntamente com o IDS Suricata com objetivo de fazer uma análise comparativa já que ele também é um NIDS e é baseado na detecção por assinaturas, projetado para ser compatível com componentes de segurança de rede existente e apresenta uma ferramenta unificada de funcionalidade de saída e opções de bibliotecas conectáveis para aceitar chamadas de outros aplicativos. É mais recente e menos difundido do que o Snort.

Nosso estudo utiliza (i) um cenário experimental onde o ataque DDoS é disparado contra uma máquina alvo e (ii)

[1] Dyn. https://www.dynstatus.com/

análise de dados de tráfego real. Em ambos, a eficácia de Snort e Suricata IDS é analisada considerando as detecções do ataque Slowloris.

II. ATAQUES DDOS E IDSS

Os ataques DDoS consistem na geração de enorme tráfego, através do recrutamento de máquinas zumbis para atacar uma ou mais máquinas-alvo. Esse recrutamento é usualmente realizado por uma busca de máquinas com falhas de segurança e/ou vulnerabilidades que possibilitem a injeção de código malicioso para posterior ataque à(s) máquina(s) alvo. Essas máquinas infectadas são chamadas de *botnets* ou agentes, e além de serem usadas para a geração do ataque também podem ser utilizadas para o recrutamento de outras novas máquinas zumbis [11]. O ataque DDoS distingue-se de outros ataques pela sua capacidade de implantar suas armas de forma distribuída através da Internet e de agregar estas forças para criar um grande volume de tráfego letal para a máquina vítima. É um ataque que consome todos os recursos da rede, tendo como objetivo torná-la indisponível [12].

Segundo [13], ataques de negação de serviço distribuídos, na sua maioria, são executados para atingir a camada de transporte de redes de computadores. Porém, atualmente esses ataques já podem ser evitados e mitigados por algumas defesas na literatura. Devido à existência de ferramentas que combatem ataques DDoS na camada de transporte, os atacantes vêm utilizando estratégias mais aprimoradas visando atingir a camada de aplicação, por exemplo, o serviço Web [14]. Ataques de negação de serviço na camada de aplicação (ADoS) são mais poderosos e traiçoeiros por quatro principais motivos: tráfego similar à de usuários honestos, fácil disponibilidade de ferramentas de ataque, baixa quantidade de recursos necessários e indisponibilidade de serviços específicos.

A maioria das ferramentas de ataque ADoS trabalham usando o protocolo HTTP/HTTPS e podem ser subdivididos em ataque de inundação (*Flooding*) e ataques de *LowRate.* Os ataques de inundação consistem na geração e envio de um grande volume de tráfego a fim de sobrecarregar e tornar indisponível o servidor alvo. Ataques desse tipo primeiramente surgiram no cenário das camadas de rede e de transporte, onde podemos exemplificar os ataques ICMP *Flooding*, UDP *Flooding* e TCP *Flooding* [15]. Os ataques *LowRate* consiste em abrir conexões TCP com o servidor Web alvo e enviar a quantidade mínima possível de dados ou enviar requisições incompletas, mantendo o servidor sempre ocupado, aguardando por novos dados referentes àquela conexão anteriormente aberta. Após a quantidade máxima de processos simultâneos, que atendem as conexões dos clientes, configurada no servidor Web for atingida, o servidor irá começar a recusar todas as novas requisições enviadas para ele, pois seus recursos a serem alocados não estará mais disponível. Trazendo prejuízos para futuros e atuais clientes legítimos que estejam enviando requisições para o servidor, como também, o ataque pode afetar completamente o servidor Web, ficando indisponível durante o decorrer do ataque [13].

O Snort é um IDS (Sistema de Detecção de Intrusão), é uma ferramenta open source, tendo passado por diversas atualizações tornando-se a mesma adaptável a vários ambientes (multi-plataforma). Seu desenvolvimento e atualização são constantes, tanto as regras de detecção quanto o código como um todo são atualizados diariamente. Os módulos que o compõem são poderosas ferramentas, com capacidade de produzir uma quantidade enorme de informações sobre os ataques monitorados. Permite o monitoramento de tráfego de pacotes em rede TCP/IP, realizando análises em tempo real sobre diversos protocolos [10].

Através de regras que são as assinaturas conhecidas dos ataques, é possível descobrir uma variedade de ataques e sondagens, como *buffer overflow, port scans*, ataques CGI (*Common Gateway Interface*), verificação de SMB (*Server Message Block*). A engenharia de detecção é programada usando um idioma simples que descreve a programação de testes de pacote e ações. A facilidade de uso simplifica e agiliza o desenvolvimento de regras de descoberta de novos ataques. A arquitetura da ferramenta Snort enfoca o desempenho, simplicidade e flexibilidade, trazendo com ela três subsistemas primários que o compõem: decodificador de pacote, engenharia de detecção e subsistema de *login* e alerta [10]. As versões mais atuais do Snort fazem análise na camada de aplicação além da camada de rede e de transporte, onde as regras são aplicadas em todos os pacotes independente do seu tipo e/ou tamanho. O IDS trabalha com regras escritas em formato texto e especificadas definidas no arquivo "*snort.conf"* [16][17].

O IDS Suricata é um IDS desenvolvido pela *Open Information Security Foundation* (OISF), a sua primeira versão beta foi lançada em dezembro de 2009 e a primeira versão estável em julho de 2010. É mais recente e menos difundido do que o Snort. Também é baseado na detecção por assinaturas, projetado para ser compatível com componentes de segurança de rede existente e apresenta uma ferramenta unificada de funcionalidade de saída e opções de bibliotecas conectáveis para aceitar chamadas de outros aplicativos [18]. Como utiliza o mecanismo de *multithread*, o IDS Suricata argumenta que oferece maior velocidade e eficiência na análise de tráfego de rede. Além de aceleração de hardware, o motor é construído para utilizar o poder de processamento oferecido pelos mais recentes processadores multi-core [18].

III. FERRAMENTA DE GERAÇÃO DE ATAQUE (SLOWLORIS)

É uma ferramenta para gerar ataques, utilizada nas simulações a fim de criar cenários que possibilitem analisar a efetividade das ferramentas de detecção de intrusão. Através de um membro chamado "Rsnake" do grupo hacker ativista chamado Anonymous [Anonymous 2016], foi criada e desenvolvida a ferramenta Slowloris, escrita em Perl. O Slowloris cria um grande número de conexões a um servidor Web de destino "alvo", enviando pedidos parciais, e tenta mantê-los abertos por um longo período. Em sequência o servidor alvo mantém essas conexões como abertas, sobrecarregando seu processo de conexão, o que necessariamente, obriga-o a negar as tentativas de conexão legítimas adicionais de clientes [19]. O ataque Slowloris é de difícil detecção por partes dos sistemas anti-DoS, pois consegue gerar tráfego a uma taxa baixa e de pequeno volume. O Slowloris tenta manter muitas conexões com o servidor web alvo pelo maior tempo possível. O mesmo inicia solicitando

várias conexões TCP ao servidor, onde, em cada uma delas, o atacante envia uma requisição GET incompleta. Na etapa seguinte, em algum instante próximo do *timeout*, um novo cabeçalho incompleto é enviado para manter a conexão ativa [20].

IV. Trabalhos Relacionados

O estudo proposto por [21] tem por objetivo comparar os IDS SNORT e Suricata para decidir qual das duas ferramentas é mais eficaz ao utilizar single threading e multithreading para detectar diversos ataques. Em relação ao single core, o Snort foi menos eficaz, pois ao se utilizar apenas um núcleo, torna-se mais difícil processar os pacotes. Porém em relação ao uso de CPU, o Snort mostra uma utilização menor que o Suricata. Caso o usuário opte por utilizar um IDS em uma CPU de baixa performance, o Snort será a melhor escolha. Contudo, o Suricata tem suas vantagens: por ser um IDS desenvolvido mais recentemente, usufrui dos benefícios multithreading dos processadores, obtendo um melhor resultado nas detecções para os ataques estudados. Entretanto este trabalho não especifica os ataques estudados, nem quais as regras utilizadas.

O trabalho de [16] apresenta um procedimento para melhorar regras no Snort para detecção de ataques na rede através de mineração de dados. O método proposto consiste em três etapas: classificação, clusterização e associação das regras. Verificou-se que o uso da abordagem proposta melhora a eficiência do Snort, adicionando, porém, maior complexidade e consumo de recursos na sua execução. [22] examinam e sistematizam práticas comuns na área de avaliação de sistemas de detecção de intrusão, definindo uma estrutura de trabalho em três etapas: carga de trabalho, métricas e metodologia de medição. São discutidos os desafios com foco em metodologias de avaliação para novos sistemas de detecção de intrusão, mostrando a importância do uso dessas ferramentas e a dificuldade de se implementá-las. O trabalho realizado por [23], aborda o problema de IDS baseado em assinaturas quando os dados estão criptografados. Para identificar os ataques, apresenta um sistema que permite identificar esses conteúdos criptografados por meio de comparação de pacotes com assinaturas também criptografadas, não perdendo o sigilo das informações armazenadas.

Uma das lacunas encontradas nos artigos relacionados foi a ausência da análise da eficácia das ferramentas na detecção dos diversos tipos de ataques importantes e muito usados atualmente. Deste modo, o presente artigo tem por objetivo avaliar a eficácia das ferramentas IDSs Snort e Suricata na detecção do ataque Slowloris, conhecido como um dos ataques DDoS mais populares na atualidade.

V. Metodologia

A metodologia de análise baseou-se em (i) execução de experimentos de geração de ataque DDoS a uma máquina-alvo, e (ii) análise de dados reais coletados em uma rede de uma instituição de ensino superior (IES) localizada no Nordeste do Brasil. Em ambos foi avaliada a eficácia dos IDSs Snort e Suricata em detectá-lo, assim como foram aferidos o consumo de recursos de CPU e memória do servidor alvo.

Os experimentos foram baseados no ataque DDoS de uma máquina atacante usando a ferramenta Slowloris para alcançar o servidor web de destino (Apache 2), que é configurada com Snort ou Suricata, alternadamente, e uma máquina executando a ferramenta de simulação de clientes honestos *Siege* (Fig.1). As métricas coletadas são: o tempo de detecção inicial (tempo em que o IDS envia o primeiro alerta), o número de alertas gerados pelo IDS e CPU e o consumo de memória do servidor alvo.

Adicionalmente, mais duas métricas foram coletadas do servidor durante os experimentos: taxa de clientes honestos disparados que consegue efetivamente acessar o site (disponibilidade média do domínio) e o TTS (time-to-service) médio de tais requisições, ou seja, o intervalo até que elas sejam atendidas pelo servidor. Assim, é possível analisar o impacto na qualidade de serviço dos clientes [14].

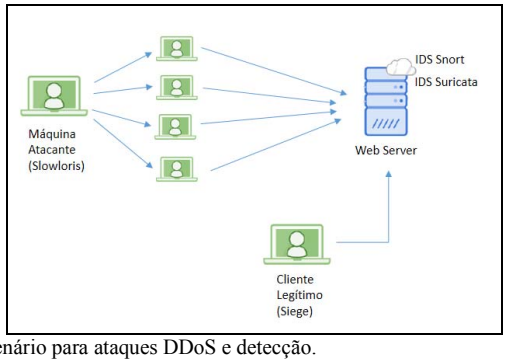

Fig. 1. Cenário para ataques DDoS e detecção.

A escolha do servidor Web usado justifica-se através de dados apresentados pela Netcraft, que mostram que aproximadamente 46% dos sites da Internet são hospedados em servidores Apache 2, representando uma parcela muito superior àquela ocupada por seus concorrentes Nginx e IIS (*Internet Information Services*). Assim, utiliza-se o servidor Web Apache 2, utilizando o *mpm_prefork* para processar requisições, com o parâmetro *MaxRequestWorkers* configurado com o valor 750. Ou seja, um servidor de médio porte, capaz de atender a 750 clientes simultaneamente [20]. Em todos os experimentos, 250 clientes honestos foram simulados pelo *Siege* como usuários constantes do servidor web, enviando requisições do tipo HTTP GET, mantendo uma taxa de ocupação legítima de aproximadamente 33% do *buffer* de atendimento do servidor, que afirmam que esta é a taxa de ocupação em casos de uso normais [20].

Os dados reais coletados foram capturados durante um período de uma semana em maio/2016, usando tcpdump. Para o cenário experimental foi realizado cinco experimentos de 60 segundos e cinco experimentos de 120 segundos. Os resultados têm um nível de confiança de 95%. A validação estatística dos dados é realizada usando análise de variância (ANOVA) e (teste de Tukey). O software usado para as análises estatísticas foi o Assistat. O software Assistat faz análise de variância (ANOVA) e classifica médias pelos testes de Tukey, de Duncan, SNK, t, de Dunnett e de Scott-Knott. Foi desenvolvido pelo Professor Francisco de A. S. e Silva da Universidade Federal de Campina Grande (UFCG). É um

software de apoio a tomada de decisão que transformam os dados em informações importantes e validadas.

VI. Resultados

A. Cenário Experimental

Este experimento visa determinar a eficácia dos IDSs Snort e Suricata durante o ataque do tipo Slowloris. Foram inicialmente pesquisadas e testadas quatro diferentes regras para detecção deste ataque pela comunidade que trabalha com segurança de redes utilizando IDS. A única regra que foi capaz de detectar este tipo de ataque foi: *Alert tcp any any -> any any (msg: "DOS by Slowloris Tool"; threshold: type threshold, track by_src, count 100, seconds 5; classtype: attempted-dos; sid: 2016001; rev: 1;)* (Tabela 1).

TABELA 1. Descrição da regra para detecção do Slowloris

alert tcp any any	Analisa o tráfego TCP de entrada vindo de qualquer interface (interna ou externa)
msg:"DOS by Slowloris Tool"	A cada detecção, será gerada a mensagem
threshold: type threshold, track by_src, count 100, seconds 5	Quando o limite de 100 conexões da mesma origem for alcançado em 5 segundos, será emitido o alerta
classtype:attempted-dos	Classificação do tipo do ataque
sid:2016001	Identificação da regra
rev:1	Nível do tipo do ataque

O comando utilizado para realizar o ataque envia requisições ao servidor, na porta 80, sendo 600 conexões a cada 5 segundos: *Perl slowloris.pl -dns 192.168.xxx.xxx -port 80 -timeout 5 -num 600 -tcpto 5*. No servidor alvo estavam instalados o IDS Snort e o IDS Suricata, que foram ativados alternadamente. Dessa forma os dados de desempenho puderam ser obtidos de forma independente.

1) Tempo da 1ª Detecção: A Tabela 2 mostra o tempo médio em que foi detectado o primeiro alerta por cada um dos IDSs, em centésimos de segundos. Observa-se que o IDS Suricata é mais rápido para detectar o ataque Slowloris, sendo 40% mais rápido para o experimento com duração de 120s.

TABELA 2. Tempo Médio da primeira detecção (Slowloris)

Tempo (s)	**Slowloris**	
	Snort	***Suricata***
60	0.3048	0.2320
120	0.3179	0.2237

A análise de variância (ANOVA) para o tempo médio da primeira detecção realizados pelos IDS para o ataque Slowloris foi estatisticamente significativa ao nível de 1%, pois o valor de "p" para os de 60 s foi igual a 0,0081 e para os de 120 s foi igual a 0,0024, ambos menores que α=0,01. Os outros resultados são estatisticamente semelhantes. Então, podemos concluir que o IDS Suricata é mais rápido do que o IDS Snort para detectar o ataque de Slowloris.

2) Número de Alertas Detectados: Este conjunto de experimentos visa aferir a capacidade dos IDSs em detectar os ataques, a partir da quantidade de alertas gerados. Como pode ser observado na Tabela 3 mostra número de alertas esperados e detectados. Observamos que o número de alertas detectados pelo IDS Suricata é muito baixo, apaenas 5% (60s) e 3% (120s) dos alertas esperados, enquanto o IDS Snort gera um maior número de alertas, 89,4% (60s) e 94% (120s). Embora o IDS Snort não detecte o número total de alertas, a quantidade detectada pode ser considerada alta o suficiente para chamar a atenção. Se um administrador de rede receber um número elevado de alertas em um período de tempo muito curto, ele provavelmente tomará alguma ação para evitar o ataque. No entanto, com apenas alguns alertas, ele não terá certeza se o ataque está ocorrendo. Assim, o desempenho de IDS Snort é melhor do que o IDS Suricata. O IDS Snort é capaz de detectar o ataque, gerando uma série de alertas suficientes para chamar a atenção do gerente de rede.

TABELA 3. Número médio de alertas (Slowloris)

Duração do ataque (s)	**IDS Snort**			
	Número total de requisições	**Alertas esperados**	**Alertas detectados**	**%**
60	7200	72	64	89.4
120	14400	144	135	94.0
	IDS Suricata			
60	7200	72	4	5.0
120	14400	144	4	3.0

3) Consumo de CPU: As Fig. 2, 3 e 4 mostram o consumo médio de CPU do servidor alvo em operação normal (clientes legítimos – Siege) e durante os ataques de 60s e 120s com o Siege sendo executado no mesmo momento. Embora o ataque Slowloris não seja praticamente detectado pelo IDS Suricata, percebe-se que o consumo de CPU é bem mais alto do que o do IDS Snort em ambos experimentos. Nota-se que na operação normal o consumo de CPU do servidor funciona sem nenhuma anormalidade, porem no momento do ataque já ocorre um declinio. Lembrando que o consumo de CPU do servidor alvo não fica alto a ponto de se indisponibilizar, é por motivo da configuração do Apache citado anteriormente no capítulo V, servidor de médio porte, pois a intenção não era indisponibilizar o serviço e sim ilustrar que os IDSs detectem o referido ataque.

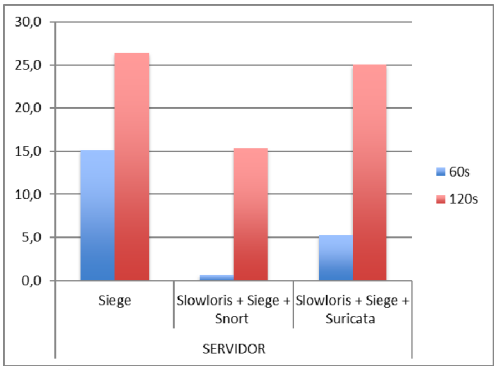

Fig. 2. Consumo de CPU

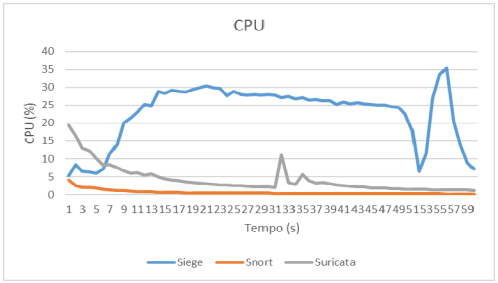

Fig. 3. Consumo de CPU (60s)

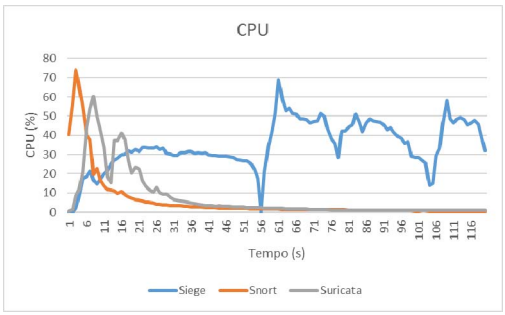

Fig. 4. Consumo de CPU (120s)

4) Consumo de Memória: As Fig. 5, 6 e 7 mostram o consumo médio de memória pelo servidor alvo durante o ataque. Podemos observar que o Slowloris causa um consumo de cerca de 50% da memória no servidor alvo, quando o IDS Snort é usado para detecção. Embora o Snort seja capaz de detectar o ataque ao gerar cerca de 94% de alertas, os recursos de memória da máquina ficam esgotados dependendo do nível do ataque. Por outro lado, embora o IDS Suricata não seja capaz de detectar o ataque, gerando apenas 5% dos alertas, a memória do servidor também fica alta bem próximo ao nível do IDS Snort. Assim, em um contexto geral o desempenho de Suricata é menor que o desempenho de Snort nesse sentido.

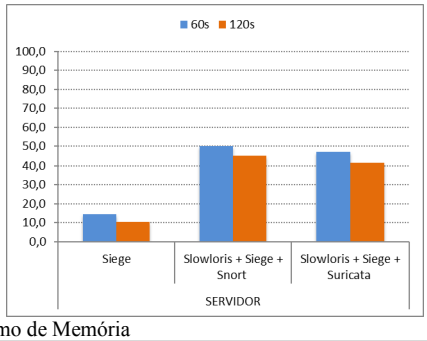

Fig. 5. Consumo de Memória

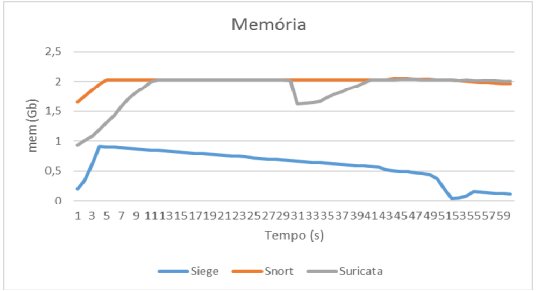

Fig. 6. Consumo de Memória (60s)

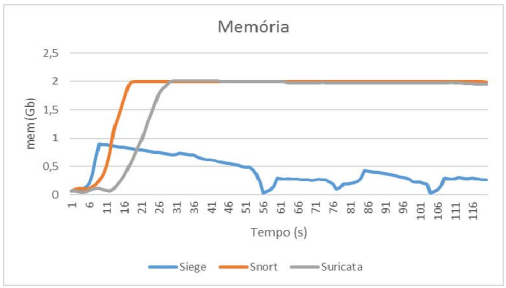

Fig. 7. Consumo de Memória (120s)

5) Disponibilidade e TTS

A Tabela 4 apresenta os resultados de disponibilidade média do domínio e TTS (time-to-service) médio de tais requisições.

TABELA 4. MÉDIA DE DISPONIBILIDADE E TTS

SERVIDOR	**60s**		**120s**	
	Disponibilidade (%)	***TTS (s)***	***Disponibilidade (%)***	***TTS (s)***
Siege	100,00	0,06	100,00	0,08
Slowloris + Siege + Snort	97,74	0,37	99,48	0,17
Slowloris + Siege + Suricata	98,34	0,26	98,56	0,30

Observa-se que, o servidor em nem um momento dos experimentos tornou-se indisponível, só se torna indisponível a partir de ataques cuja intensidade definida é superior ao porte do servidor, já que o número de atacantes não é superior ao número máximo de clientes que podem ser atendidos simultaneamente pelo servidor. Outro fato importante é o impacto no tempo de serviço (TTS) gerado pelo ataque a partir do momento em que todas as posições do servidor encontram-se ocupadas. Isso mostra que em nenhum momento dos nossos experimentos ocorreu.

B. Análise de dados coletados

Os dados coletados foram processados por IDSs no modo off-line. A Tabela 5 mostra o volume de tráfego, o número de alertas eo consumo de CPU para cada IDS. Em todos os traces e dias, o IDS Snort detectou mais ataques. O consumo de CPU do IDS-Snort foi significativamente menor do que o Suricata, com até 51% menos.

TABELA 5. VOLUME DE TRÁFEGO (GB) E NÚMERO DE ALERTAS

	Manhã					**Tarde**		
Dia	**Volume de Tráfego**	**Snort Alertas**	**Suricata Alertas**	**CPU. Snort**	**CPU. Suricata**	**Volume (GB)**	**Snort Alertas**	**Suricata Alertas**
1	0.5	3499	163	52%	100%	140.0	880	94
2	10.8	92357	1730	65%	100%	46.4	369764	220
3	33.8	248859	2909	58%	100%	19.4	161205	1805
4	34.9	255815	1460	62%	100%	40.1	330370	79
5	26.5	354482	2075	77%	100%	28.5	352628	2441
6	14.9	79298	142	49%	100%	7.7	40597	82
7	17.1	125551	29	70%	94%	3.6	2474	46

Também isolamos os ataques encontrados nos traces. O ataque do tipo Slowloris foi detectados atráves dos IDSs estudados, como também alguns outros tipos de ataques. A quantidade de notificações geradas para o ataque de Slowloris é considerada surpreendentemente alta. Deve-se notar que o IDS Snort é mais eficaz na detecção de Slowloris, conforme concluído no cenário experimental. Então, podemos afirmar que o site está sob ataque de Slowloris durante os períodos estudados. Para os outros tipos de ataques, ambos geraram o mesmo número de alertas, mostrando desempenho semelhante.

VII. Considerações Finais

A detecção de ataque é um aspecto importante da segurança da rede. Os ataques DDoS estão se tornando ainda mais simples, com ferramentas capazes de tornar um serviço web indisponível em minutos. Sistemas IDS como Snort e Suricata são capazes de detectar tais ataques. Neste trabalho, esses IDSs são analisados em termos de eficácia e consumo de recursos para a identificação de ataque DDoS Slowloris.

Através de experiências controladas e análise de traces de dados reais, descobrimos que o IDS Snort é mais eficaz na detecção de ataques de Slowloris nos cenários estudados. Embora o Suricata IDS seja capaz de detectar os vários tipos de ataques rapidamente, ele não consegue detectar o ataque de Slowloris na prática, gerando menos de 5% dos alertas esperados nas experiências controladas. Na análise do tráfego em tempo real, a Suricata gera apenas 3% dos alertas gerados pelo Snort para este ataque. Pretendemos realizar estudos de duração mais longa, bem como criar variantes das regras que permitem a melhoria da detecção IDS.

References

[1] Beitollahi, H.; Deconink, G. Analyzing well-known countermeasures against distributed denial of service attacks. Computer Comm., v. 35, n. 11, 2012, p. 1312-1332.

[2] Cisco. Cisco® Visual Networking Index (VNI). 2016.

[3] Verisign. Verisign Distributed Denial of Service Trends Report, volume 3, issue 2 - 2nd Quarter 2016.

[4] Payão, Felipe. Quebrando a internet: estamos sofrendo o maior ataque DDoS da história. 2017. https://www.tecmundo.com.br/ataque-hacker/110842-grande-ataque-ddos-afeta-twitter-psn-spotify-outros-estragos.htm. Acessado em 22/03/2017.

[5] Ackerman, Spencer. The Guardian. Major cyber attack disrupts internet service across Europe and US. 2016. https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service. Acessado em 24/10/2017.

[6] Thongkanchorn, K., Ngamsuriyaroj, S., & Visoottiviseth, V. Evaluation studies of three intrusion detection systems under various attacks and rule sets. *In TENCON 2013-2013 IEEE Region 10 Conference. 2013.*

[7] Nakamura, E. T. Paulo Licio de Geus. *Novatec. Segurança em redes cooperativas. Editora Novatec*. 2007.

[8] Idatalabs. Companies using Snort. 2016. https://idatalabs.com/tech/products/snort. Acessado em 01/12/2016.

[9] Albin, E., & Rowe, N. C. (2012). A realistic experimental comparison of the Suricata and Snort intrusion-detection systems. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th Int. Conference* (pp. 122-127). IEEE.

[10] Snort Brasil. The Open Source Network Intrusion Detection System. 2016. http://www.snort.org.br. Acesso em jun. 2016.

[11] Robinson, R. R., & Thomas, C. Evaluation of mitigation methods for distributed denial of service attacks. *7th IEEE Conf. on Industrial Electronics and Applications, 2012.*

[12] Yan, Q., & Yu, F. R. Distributed denial of service attacks in software-defined networking with cloud computing. *IEEE Communications Magazine*, 2015, *53*(4), 52-59.

[13] Pascoal, T. A. (2016). Implementação e implantação de uma defesa contra-ataques DDoS em um servidor WEB. Monografia. Departamento de Informática. UFPB.

[14] Dantas, Y, G.; Nigam, V.; Fonseca, I. A Selective Defense for Application Layer DDoS Attacks, Intelligence and Security Informatics Conference (JISIC), Hague, 8/12/2014.

[15] Durcekova, V., Schwartz, L., Shahmehri, N. (2012). Sophisticated denial of service attacks aimed at application layer. In: ELEKTRO. IEEE, p. 55-60.

[16] Khamphakdee, N., Benjamas, N., & Saiyod, S. Improving Intrusion Detection System Based on Snort Rules for Network Probe Attacks Detection with Association Rules Technique of Data Mining. *Journal of ICT Research and Applications. 2015*.

[17] Caruso, L. C. M. Proposta de arquitetura para NIDS acelerado por Hardware. Master Thesis PUC-RS, Porto Alegre, 2005, p. 25.

[18] Suricata. Manual Suricata. 2016. https://suricata-ids.org.

[19] Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network Computer Aplications*.

[20] Netcraft. NetCraft WebServer Survey. Disponível em:https://news.netcraft.com/archives/2016/09/19/september-2016-web-server-survey. html. Acesso em 20/06/2017.

[21] Park, W., & Ahn, S. Performance Comparison and Detection Analysis in Snort and Suricata Environment. *Wireless Personal Comm.*, 2016, 1-12.

[22] Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A., & Payne, B. D. Evaluating Computer Intrusion Detection Systems: A Survey of Common Practices. *ACM Computing Surveys (CSUR)*, 2015, *48(1), 12.*

[23] Sherry, J; Lan, C., Popa, R. A., Ratnasamy, S. BlindBox: deep packet inspection over encrypted traffic. SIGCOMM Comp. Comm. Rev., New York, NY, USA. 2015.