Utilização da Ferramenta *Snort 3* para Detecção de Intrusão em Redes de Pequeno Porte

Adan Campos Diniz[1], Douglas Henrique Oliveira Costa[1], Victor de Oliveira Vieira[1], Fábio Castro Araújo[1]

[1]Departamento de Computação

Universidade Luterana do Brasil – Palmas – TO

Resumo: *À medida que as redes pequenas se tornam mais complexas e têm um número maior de dispositivos conectados, a segurança dessas redes se torna cada vez mais relevante. Este estudo investigou o uso do Snort3, uma ferramenta de detecção de intrusões baseada em rede de código aberto, para identificar atividades suspeitas e anomalias nesses tipos de ambientes. Ao configurar e implementar o Snort3, foi possível monitorar o tráfego de rede em tempo real e receber alertas sobre possíveis ameaças. Como resultado, foi observado a eficácia da ferramenta no que tange ao tempo de resposta de aviso no seu log em relação a uma possível intrusão estando três dispositivos conectados à mesma rede, sendo o dispositivo A quem faz o ataque, o dispositivo B que sofre o ataque e o dispositivo C quem monitora a segurança da rede.*

Introdução

A segurança de redes é um dos principais desafios enfrentados pelas organizações em todo o mundo. De acordo com Lima, Ferreira e Peixoto (2022), as organizações estão cada vez mais vulneráveis a ataques cibernéticos, que podem resultar em perda de dados, interrupção de serviços e danos à reputação. Nesse contexto, é fundamental proteger as redes contra essas ameaças, pois a integridade, confidencialidade e disponibilidade das informações e serviços dependem disso.

Segundo a Check Point (2023), o ambiente de cibersegurança no Brasil demonstra preocupação. O país apresenta um volume de ataques cibernéticos, em uma base semanal, que ultrapassa os padrões globais. Tal panorama, conforme sugerido pela organização, pode ser atribuído, em grande parte, à postura adotada pelas empresas brasileiras. "Há uma predominância no foco em detectar ataques já efetivados ao invés de investir proativamente em medidas de prevenção, resultando em custos de remediação frequentemente mais elevados" (CHECK POINT RESEARCH, 2023).

Elucidando tal temática, a *Check Point Research (CPR)* divulgou um levantamento referente ao período de abril a junho de 2023, evidenciando uma tendência alarmante na cibersegurança global. Enquanto os ataques cibernéticos semanais no cenário global aumentaram 8%, atingindo o maior número em dois anos, a américa latina apresentou um crescimento de 9%, contabilizando uma média de 1.745 ataques semanais por organização (CHECK POINT RESEARCH, 2023).

Neste contexto, a salvaguarda das redes torna-se crucial no panorama tecnológico contemporâneo. De acordo com a Revista Militar de Ciência e Tecnologia (2022), mais do que implementar medidas de segurança robustas, é essencial contar com ferramentas e algoritmos capazes de identificar e responder rapidamente a anomalias e intrusões. O *Snort* 3, emerge como uma solução de destaque para essa finalidade. Especializado na detecção de irregularidades e potenciais invasões, o software se apresenta como um recurso necessário para as organizações que buscam fortalecer a segurança das redes e responder eficazmente a

ameaças em tempo real (UTIMURA,2020).

2 Referencial Teórico

2.1 Conceitos de Detecção de Intrusões (IDS - *Intrusion Detection System*)

A detecção de intrusões (IDS) desempenha um papel fundamental na segurança cibernética, ela é "Um sistema ou dispositivo que monitora redes ou sistemas de computadores para identificar atividades suspeitas ou maliciosas" (SCARFONE; MELL, 2007). Em essência, um IDS é um dispositivo ou aplicativo que rastreia o tráfego da rede e/ou do sistema, procurando por atividades que se desviem de um padrão estabelecido (REHMAN 2003). Ao contrário dos *firewalls*, que se concentram na prevenção de acessos não autorizados, os sistemas de detecção de intrusão estão mais voltados para a identificação e notificação de possíveis invasões em andamento (FARES 2021).

Existem dois tipos principais de sistemas de detecção de intrusão: os baseados em rede (NIDS) e os baseados em host (HIDS). Os NIDS monitoram todo o tráfego em uma rede, enquanto os HIDS se concentram em atividades suspeitas em um único sistema hospedeiro (KONG, 2022). De acordo com Khraisat (2019), o Sistema de Detecção de Intrusão por Assinatura (SIDS) tem a capacidade de identificar ataques direcionados a um protocolo específico de um dispositivo IoT. Complementando, o Sistema Híbrido de Detecção de Intrusão (HIDS) abraça as características do SIDS e do Sistema de Detecção de Intrusão Baseado em Anomalias (AIDS) com o propósito de detectar não apenas a atividade maliciosa inicial, mas também subsequentes alterações no dispositivo decorrentes deste ataque.

É essencial para as organizações compreenderem os conceitos e funcionalidades dos sistemas IDS, especialmente no contexto da IoT (*Internet of Things*), para garantir a segurança de seus dispositivos e redes. A constante evolução das ameaças cibernéticas torna fundamental que esses sistemas se mantenham atualizados e passem por revisões regulares, com o objetivo de se ajustarem às novas formas de ataques e assegurar a eficiência na detecção (Khraisat et al., 2019).

2.2. Histórico e evolução das ferramentas de IDS

No surgimento das primeiras ciberameaças na década de 1980, identificou-se a necessidade de monitorar sistemas e redes contra atividades suspeitas. Contudo, até a década de 1990, a ênfase em segurança de redes era menos intensa, uma vez que o acesso estava limitado, em sua maioria, a universidades e grandes corporações. Entretanto, com o avanço tecnológico e a democratização do acesso à rede, esta realidade transformou-se, ampliando a interconexão de dados e facilitando a rotina dos usuários. Essa expansão, embora benéfica, suscitou desafios significativos para a segurança das redes, tornando imperativo o desenvolvimento de processos automáticos de detecção e prevenção de intrusões, a fim de mitigar ataques e preservar a integridade dos sistemas (COSER, 2012).

Na ilustração abaixo apresentada, observa-se a evolução das ferramentas e contribuidores principais no domínio dos Sistemas de Detecção de Intrusão (IDS) ao longo das últimas décadas.

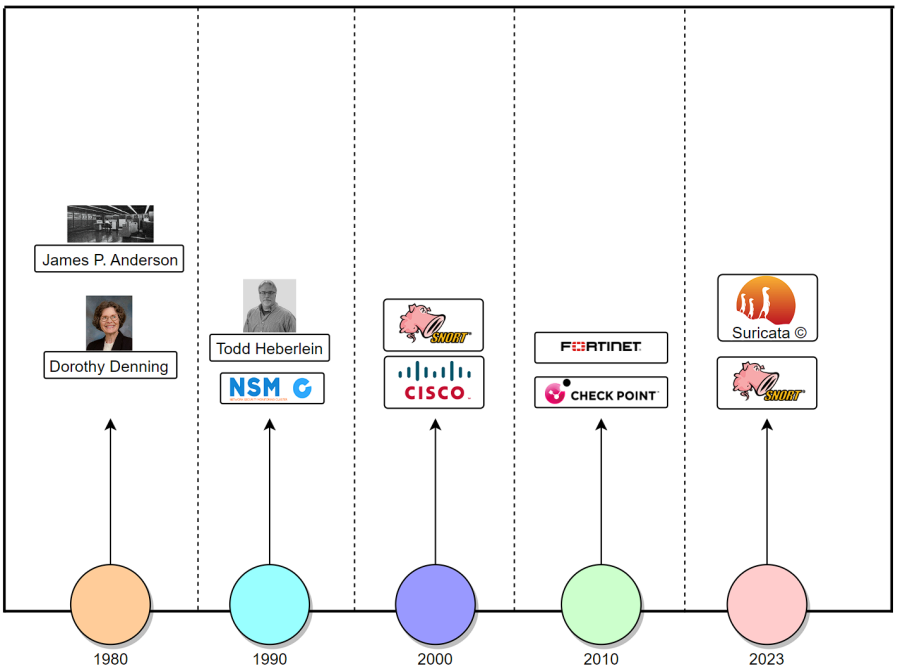

Figura 1. Histórico de evolução das IDS

Na década de 1980, James P. Anderson desempenhou um papel fundamental no estabelecimento de conceitos para sistemas de detecção de intrusão. Anderson, conforme evidenciado por (SPAFFORD 2008), focou na ideia de monitorar trilhas de auditoria em sistemas computacionais. Paralelamente, segundo a *Indiana University Bloomington*, a Dr. Dorothy Denning foi responsável pelo desenvolvimento do *Intrusion Detection Expert System* (IDES) na *SRI International*.

Na década de 1990, Todd Heberlein, da Universidade da Califórnia, *Davis*, desenvolveu o *Network Security Monitor* (NSM), focando na monitorização do tráfego de rede. Nos anos 2000, surgiu o *Snort* como uma solução de código aberto, e, no mesmo período, a *Cisco Systems* adquiriu a *Sourcefire*, empresa responsável pelo desenvolvimento do *Snort*. A década de 2010 evidenciou o crescimento de empresas como *Check Point Software Technologies* e *Fortinet*, ambas introduzindo soluções integradas que combinavam *firewalls* com capacidades de IDS/IPS.

Em 2023, *Snort* e Suricata são ferramentas reconhecidas no campo de IDS, demonstrando a contínua adaptação e desenvolvimento de soluções em resposta às demandas de segurança cibernética.

2.3. Visão geral do *Snort* conhecendo o sistema

O *Snort* representa uma das ferramentas de detecção de intrusão baseadas em rede (NIDS) mais consolidadas no âmbito da segurança da informação. Desenvolvido inicialmente como um projeto de código aberto, sua versatilidade e eficácia propiciaram que ele se tornasse referência na área, sendo amplamente adotado tanto por empresas quanto por especialistas (REHMAN, 2003). O sistema não apenas detecta possíveis invasões, mas também oferece recursos para prevenir ações maliciosas, combinando características de sistemas de detecção e prevenção de intrusões (IDS/IPS).

Além de sua funcionalidade básica, o *Snort* possui um conjunto estruturado de características que inclui a detecção baseada em assinatura, monitoramento de protocolo e uma linguagem flexível de regras. Este último permite aos administradores adaptar o sistema às necessidades específicas de seu ambiente, garantindo uma proteção mais direcionada e efetiva (DAVIS; BARNETT, 2023). A combinação desses recursos posiciona o *Snort* como uma ferramenta abrangente, apta a responder a uma variedade de ameaças cibernéticas.

Com a aquisição da *Sourcefire* pela *Cisco Systems,* empresa por trás do desenvolvimento do *Snort*, houve uma reafirmação da importância dessa ferramenta no cenário global de segurança cibernética. Esta aquisição demonstra o reconhecimento da indústria da relevância e capacidade do *Snort* em fornecer soluções de segurança bem arquitetadas e confiáveis para redes de diferentes tamanhos e complexidades (STALLINGS, 2019).

3 Materiais e métodos

3.1. Materiais

Este artigo empregou uma seleção de materiais e *softwares* para conduzir análises aprofundadas no que tange a segurança de uma rede de pequeno porte. O *Oracle VM VirtualBox* foi utilizado para estabelecer um ambiente de testes através da criação de máquinas virtuais, nas quais o sistema operacional Ubuntu 22.04.3 LTS foi instalado. Esse ambiente possibilitou um espaço controlado para a execução de testes e análises. O *software Snort* 3 desempenhou um papel na detecção de intrusões, enquanto o software de mapeamento de redes *Nmap* auxiliou na identificação de vulnerabilidades e na avaliação do desempenho do *Snort* 3 em relação à detecção de ameaças cibernéticas. A combinação de softwares e recursos contribuiu para as análises aprofundadas e as conclusões apresentadas neste estudo.

3.2. Métodos

Na metodologia adotada neste trabalho, diversas etapas foram executadas visando a obtenção dos resultados. Essas etapas podem ser visualizadas a seguir na Figura 2:

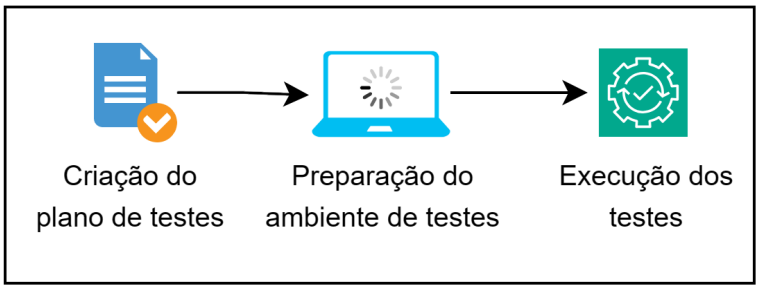

Figura 2. Fluxo de Trabalho

Inicialmente, estabeleceu-se o plano de testes, que contemplou o planejamento dos cenários, a definição dos passos, o ambiente de execução e os resultados almejados em cada fase.

Após o planejamento, procedeu-se com a preparação do ambiente de testes, ajustando os cenários e ambientes preestabelecidos e configurando os arquivos necessários para garantir a correta execução do ambiente.

Na fase subsequente, executaram-se os testes conforme planejado. Após esta etapa, os dados colhidos foram compilados e apresentados como resultados.

4 Resultados

4.1 Aplicação do *snort 3* em uma rede de pequeno porte

Neste estudo, utilizou-se uma configuração de rede composta por três máquinas virtuais hospedadas no ambiente de virtualização *VirtualBox* da *Oracle*, todas com o sistema operacional *Ubuntu 22.04.3 LTS*. Essa abordagem foi escolhida para criar um ambiente controlado e replicável que permitisse a análise e teste da ferramenta *Snort 3* em um cenário de rede realista. Conforme ilustrado na Figura 3, observam-se três máquinas virtuais, cada qual com uma funcionalidade específica voltada ao plano de teste em um ambiente controlado. A máquina virtual 1 (VM1) integra a ferramenta de detecção Snort; a máquina virtual 2 (VM2) atua como a entidade atacante na rede, utilizando o Nmap; e a máquina virtual 3 (VM3) representa o alvo na rede, destinatário do ataque.

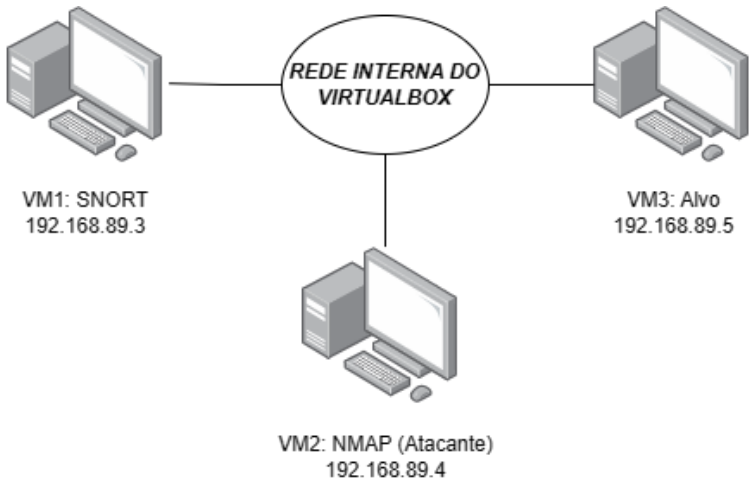

Figura 3. Organização da rede. Fonte: Elaborada pelos autores

4.2. Configuração e parametrização do Snort 3

Na máquina virtual onde é implementado o NIDS (Sistema de Detecção de Intrusões em Rede), foi instalado o *Snort* por meio do seguinte comando:

- ***sudo apt-get install snort***

Após a instalação, teve prosseguimento à criação de uma conta no site oficial do *Snort* para obter as permissões necessárias para o *download* das Regras Registradas. Após a conclusão do cadastro, foi realizado o *download* do arquivo de regras com o nome

- ***snortrules-snapshot-2983.tar.gz***

Com o arquivo de regras baixado, foi descompactado no diretório apropriado, utilizando o seguinte comando:

- ***sudo tar -xvzf snortrules-snapshot-2983.tar.gz -C /etc/snort/rules***

Esses passos garantiram a instalação e configuração necessária do *Snort*, habilitando-o para a detecção de intrusões na rede utilizada como ambiente para tal estudo.

Em seguida, realizou-se a configuração da interface de rede no *VirtualBox* para o modo promíscuo, conforme ilustrado na figura abaixo:

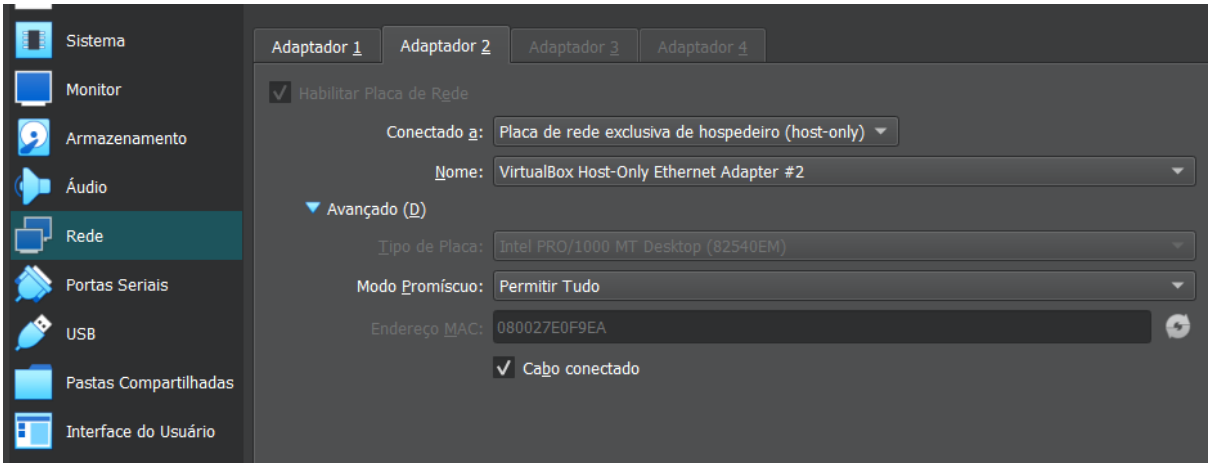

Figura 4. Configuração de Interface de Rede e Modo Promíscuo.

Adicionalmente, foi essencial inserir o seguinte comando no terminal para ativar o modo promíscuo na interface de rede:

- ***sudo ip link set enp0s8 promisc on***

A ativação desse modo é necessária, pois permite que a interface de rede receba e capture todos os pacotes de dados que trafegam por ela, independentemente do destino. Isso implica que a placa de rede no modo promíscuo é capaz de monitorar o tráfego de rede que não se destina especificamente àquela placa.
Após a série de passos é possível iniciar o *snort 3* com o seguinte comando:

- ***sudo snort -d -l /var/log/snort/ -A console -c /etc/snort/snort.conf***

Após iniciar o comando especificado acima, o *snort* estará monitorando os pacotes e pronto para emitir um alerta, conforme imagem abaixo:

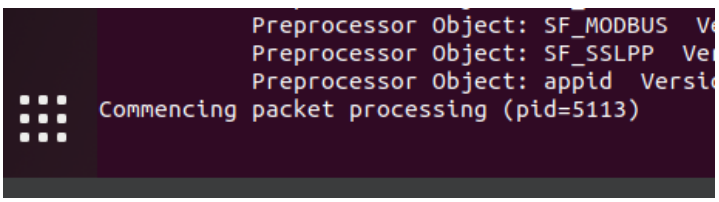

Figura 5. *Snort* processando pacotes.

4.3. Simulação de atividade suspeita com *Nmap.*

No contexto deste estudo, foram realizadas simulações controladas de atividades suspeitas utilizando a ferramenta *Nmap* (*Network Mapper*) como parte do método de pesquisa. O *Nmap* é uma ferramenta de código aberto que é usada para explorar redes e auditar a segurança. O *Nmap* é capaz de realizar uma variedade de tarefas, incluindo varredura de portas, detecção de serviços, detecção de sistemas operacionais e detecção de *firewalls* (Nmap, 2023).
Seguindo o exemplo de configuração de rede apresentado na **Figura 2** deverá ser notado se o seguinte modelo de interface de rede esteja previamente configurado, abaixo é possível exemplificar através da figura 6.

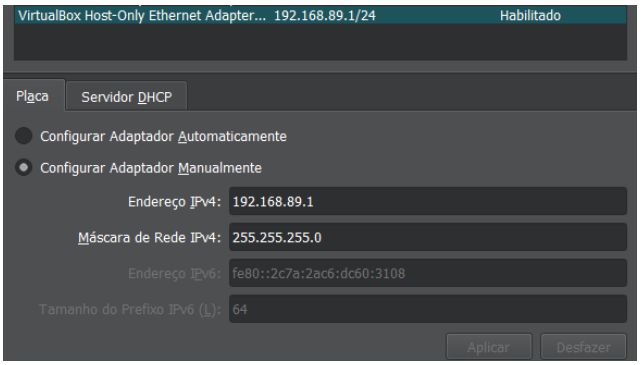

Figura 6. Interface de rede configurada.

Após a preparação do ambiente de teste, há o segmento no que tange à execução do ataque fazendo uso da ferramenta ***Nmap***. Segue o comando executado:

- ***sudo nmap -O 192.168.89.5***

(onde 192.168.89.5 representa o endereço IP do alvo). Esse comando tem a finalidade de mapear redes e conduzir varreduras de portas em dispositivos e *hosts* na rede, com foco na identificação do dispositivo alvo. O resultado dessa ação está disponível na figura a seguir:

```
root@vm2:~# sudo nmap -O 192.168.89.5
Starting Nmap 7.80 ( https://nmap.org ) at 2023-09-30 18:12 -03
Nmap scan report for 192.168.89.5
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.89.5 are closed
MAC Address: 08:00:27:04:8E:D6 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.07 seconds
```

Figura 7. *Nmap* a partir da máquina atacante.

No desfecho dessa etapa, ao realizar a varredura do dispositivo alvo com o *Nmap*, o *Snort* prontamente emitiu alertas de "*Potential Bad Traffic*" (Tráfego Potencialmente Suspeito), sinalizando a detecção de atividades de rede que levantaram suspeitas, independentemente de sua natureza maliciosa ou autorizada. Esse processo está documentado na figura a seguir:

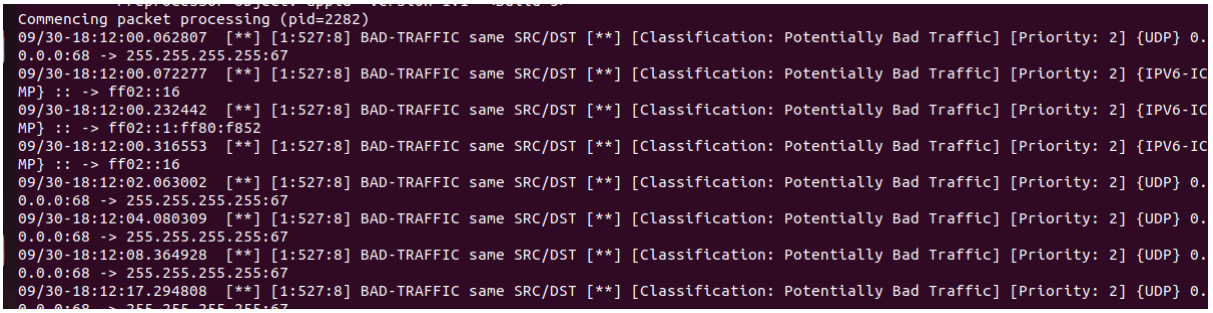

Figura 8. Detecção de anomalias com o *Snort*.

Esses alertas identificam e registram atividades que demandam maior análise e avaliação, contribuindo significativamente para a eficácia do *Snort* 3 na detecção de intrusões no contexto deste estudo.

4.4 Eficiência na detecção de intrusões simuladas

No ambiente controlado, conforme delineado nas seções anteriores, três máquinas virtuais desempenharam papéis distintos: VM1 com a ferramenta *Snort*, VM2 como a entidade atacante e VM3 como o alvo. Ao longo da simulação, diversas tentativas de intrusão foram realizadas por meio da VM2, utilizando o *software Nmap*, visando explorar possíveis vulnerabilidades na VM3.

Os resultados obtidos demonstraram que o *Snort* 3, instalado na VM1, foi capaz de identificar e registrar diversas tentativas de intrusão. Cada tentativa detectada foi categorizada de acordo com sua natureza e grau de risco, permitindo uma análise mais aprofundada sobre os tipos de ameaças enfrentadas por redes de pequeno porte.

É relevante destacar que, além da detecção, o *Snort* 3 ofereceu informações detalhadas sobre os métodos de intrusão, contribuindo para a tomada de decisão sobre medidas de mitigação e proteção.

5 Considerações finais

Nesta pesquisa, foi explorada a aplicação do *Snort* 3 em uma configuração de rede composta por três máquinas virtuais, operando sob o ambiente de virtualização *VirtualBox* da *Oracle*. O estabelecimento deste cenário visou a criação de um ambiente controlado que permitisse análise e teste da ferramenta.

A configuração e parametrização do *Snort* 3 envolveram etapas desde a instalação até o ajuste das regras necessárias para sua operação adequada. Complementarmente, a utilização do *Nmap* permitiu simulações controladas que avaliaram a capacidade de resposta do *Snort* 3 frente a atividades de rede específicas.

Ao longo dos testes, o *Snort* 3 demonstrou sua capacidade de emitir alertas ao identificar atividades suspeitas, validando sua função como ferramenta de monitoramento. Os procedimentos adotados e os resultados obtidos fornecem um guia para a implementação e utilização do *Snort* 3 em contextos similares.

Para futuras abordagens, recomenda-se a investigação de funcionalidades avançadas do *Snort* e a avaliação de sua integração com outras soluções de segurança. Adicionalmente, estudos em ambientes de rede com diferentes características podem enriquecer o entendimento sobre a adaptabilidade e aplicabilidade do *Snort* 3.

6 Referências Bibliográficas

CHECK POINT. Average weekly global cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research. Disponível em: https://blog.checkpoint.com/security/. Acesso em: 08 out. 2023.

CHECK POINT. Sobre a empresa: visão geral. 2022. Disponível em: https://www.checkpoint.com/pt/about-us/company-overview/. Acesso em: 11 out. 2023.

COSER, Ezequiel. Automatização do processo de contenção de ameaças baseada em ferramenta de IDS/IPS (Sistema de Detecção e Prevenção de Intrusão). 2012. Monografia (Graduação em Engenharia de Controle e Automação) – Universidade do Vale do Taquari - Univates, Lajeado, 07 mar. 2012. Disponível em: http://hdl.handle.net/10737/257. Acesso em: 05 out. 2023.

DAVIS, Michael J.; BARNETT, Ryan. Snort 3: The Definitive Guide. O'Reilly Media, 2023.

E-TINET. Snort: o monitor de redes. Disponível em: https://e-tinet.com/snort-monitor-redes/. Acesso em: 09 out. 2023.

FARES, Awatef Ali Yousef Rodrigues. Proposta de integração de um sistema de detecção de intrusão (IDS) entre uma rede SDN e uma honeynet. 2021. xvi, 67 f., il. Dissertação (Mestrado Profissional em Engenharia Elétrica) – Universidade de Brasília, Brasília, 2021.

HARE, Chris; BEAVER, Kevin. Intrusion Detection Systems: A System Approach to Network Security. Pearson Education, 2018.

IEEE COMPUTER SOCIETY. James P. Anderson: um pioneiro em segurança da informação - 2008. Disponível em: https://www.computer.org/csdl/magazine/sp/2008/01/msp2008010009/13rRUwjGoEs. Acesso em: 09 out. 2023.

INDIANA UNIVERSITY. Profiles: Current Trailblazers - Denning. 2022. Disponível em: https://womenandtech.indiana.edu/programs/cybersecurity/profiles-current-trailblazers/denning.html. Acesso em: 09 out. 2023.

KHRAISAT, A.; GONDAL, I.; VAMPLEW, P.; KAMRUZZAMAN, J.; ALAZAB, A. A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. Electronics, 8(9), 1033. 2019. Disponível em: https://doi.org/10.3390/electronics8091033. Acesso em: 05 out. 2023.

KONG, Jiaqi. Análise baseada em HIDS e NIDS. In: 5ª CONFERÊNCIA INTERNACIONAL SOBRE CIÊNCIA DA INFORMAÇÃO INFORMÁTICA E

TECNOLOGIA DE APLICAÇÃO (CISAT 2022). Proc. SPIE, v. 12451, p. 1245112, 20 out. 2022. Disponível em: https://doi.org/10.1117/12.2656478. Acesso em: 04 out. 2023.

LIMA, Paulo Ricardo Silva; FERREIRA, Leonardo Matheus Marques; PEIXOTO, Ana Lydia Vasco de Albuquerque. Gestão da segurança da informação. P2P e Inovação, [S.L.], v. 9, n. 1, p. 206-221, 29 set. 2022. Logeion Filosofia da Informacao. http://dx.doi.org/10.21721/p2p.2022v9n1.p206-221.

LOPES, R. DA S.; DUARTE, J. C.; GOLDSCHMIDT, R. R. Detecção de ataques cibernéticos utilizando aprendizado de máquina: uma revisão. Revista Militar de Ciência e Tecnologia, v. 39, n. 2, 9 nov. 2022.

NMAP. Descrição. Disponível em: https://nmap.org/book/man.html#man-description. Acesso em: 11 out. 2023.

REHMAN, Rafeeq. Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID. 1. ed. New Jersey: Prentice Hall, 2003.

SCARFONE, Karen; MELL, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS). Nist Special Publication 800-94, [S.L.], v. 5, n. 1, p. 1-127, 20 fev. 2007. National Institute of Standards and Technology. http://dx.doi.org/10.6028/nist.sp.800-94. Acesso em: 18 out. 2023.

SPLUNK. NSM: Network Security Monitoring. 2022. Disponível em: https://www.splunk.com/en_us/blog/learn/nsm-network-security-monitoring.html. Acesso em: 09 out. 2023.

SPAFFORD, E. James P. Anderson: Um Pioneiro em Segurança da Informação. IEEE Security & Privacy, v. 6, n. 01, p. 9, 2008. Disponível em: https://doi.ieeecomputersociety.org/10.1109/MSP.2008.15. DOI: 10.1109/MSP.2008.15. Acesso em: 05 out. 2023.

STALLINGS, William. Network Security: A Top-Down Approach. Pearson Education, 2019.

UTIMURA, Luan Nunes. Aplicação em Tempo Real de Técnicas de Aprendizado de Máquina no Snort IDS. 2020. 96 f. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual Paulista (Unesp), Instituto de Biociências Letras e Ciências Exatas, São José do Rio Preto, 2020.