# Um estudo de caso sobre a implantação de um ambiente de prevenção de intrusões com a ferramenta Suricata

**Gabriel Marvel Vaz**[1], **Tiago Antonio Rizzetti**[1], **Walter Priesnitz Filho**[1]

[1]Universidade Federal de Santa Maria (UFSM)
Caixa Postal 5082 -– CEP: 97.105-900 – Santa Maria – RS – Brazil

{gabrielmarvelvaz, walter, rizzetti}

@redes.ufsm.br

***Abstract.*** *This article presents a case study on the implementation of an intrusion prevention environment in a computer network of an educational institution. The adopted architecture was based on using a Network Intrusion Prevention System (NIPS) together with Host Intrusion Prevention System (HIPS), to detect and block attacks aimed at the network. The Suricata software was configured inline, filtering the network traffic. To visualize the logs, the Elasticsearch, Logstash, and Kibana (ELK) stack was configured together with the Synesis tool, allowing the visualization of the data through a Web interface. With this, it was possible to detect and block threats, including scans, communications originated by malicious hosts, among others. From this, actions were taken such as the addition of new firewall rules, creation of a blacklist, among other measures that contributed to raising the network's security level.*

***Resumo.*** *Neste artigo é apresentado um estudo de caso sobre a implantação de um ambiente de prevenção de intrusões em uma rede de computadores de uma instituição de ensino. A arquitetura adotada baseou-se em utilizar um Network Intrusion Prevention System (NIPS) em conjunto com Host Intrusion Prevention System (HIPS), a fim de detectar e bloquear ataques destinados à rede. O software Suricata foi configurado inline, filtrando o tráfego da rede. Para visualização dos logs, a pilha Elasticsearch, Logstash e Kibana (ELK) foi configurada em conjunto com a ferramenta Synesis, permitindo a visualização dos dados através de uma interface Web. Com isso, foi possível detectar e bloquear ameaças, dentre elas varreduras, comunicações originadas por hosts maliciosos entre outras. A partir disso, foram tomadas ações como a adição de novas regras de firewall, criação de uma blacklist, dentre outras medidas que contribuíram para elevar o nível de segurança da rede.*

## 1. Introdução

Dentro do escopo de segurança da informação, existem diferentes tipos de ameaças e ataques, e as intrusões podem ser consideradas um destes tipos de ameaças. Um exemplo de intrusão é um adversário obter acesso não autorizado a dados sensíveis, burlando proteções de controle de acesso do sistema [Stallings and Brown 2014]. Neste contexto, os IDSs são responsáveis pelo monitoramento e detecção de anomalias em redes de computadores [Utimura and Costa 2018]. Segundo [Mota Filho 2018] o IPS tem um mecanismo interno similar a um IDS. A principal diferença é que o IPS faz o bloqueio de tráfego malicioso.

O presente trabalho tem por objetivo apresentar um estudo de caso acerca da implantação de um ambiente de prevenção de intrusões na rede de computadores de uma instituição de ensino, elencando os principais aspectos de sua implementação e resultados alcançados, contribuindo para com outros administradores que eventualmente venham a realizar implantações semelhantes.

## 2. Trabalhos Relacionados

Em [Xing et al. 2014] os autores propõem uma solução de IPS baseada em SDN para nuvem, chamada de SDNIPS. No trabalho é utilizado o Snort para geração dos alertas, e a partir disso são geradas regras a serem injetadas no dispositivo OpenFlow para reconfigurar a rede. A reconfiguração consiste em redirecionamento de tráfego, ajustes de QoS, isolamento de tráfego através de VLANs, entre outras medidas. Através de simulações, os autores concluíram que o sistema foi capaz de atuar ativamente na detecção e prevenção de ataques através da reconfiguração de um ambiente baseado em nuvem utilizando SDN. Em ambientes deste tipo, tal implementação pode auxiliar no processo de proteção da rede, porém, em redes tradicionais a viabilidade desta solução deve ser verificada, já que as alterações constantes podem eventualmente causar problemas de disponibilidade, exigindo um monitoramento contínuo de suas ações.

No trabalho realizado por [Farhaoui 2016], o autor apresenta aspectos acerca da implantação de um ambiente IPS e como isto pode aumentar a segurança de servidores *Web*. Nesta abordagem, assim como no presente trabalho, é utilizada uma arquitetura composta por NIPS + HIPS. Porém, o autor não aborda de forma clara aspectos práticos, tornando a contribuição do trabalho apenas teórica, e além disso, a questão inicial levantada sobre a proteção de servidores *Web* não é objetivamente respondida.

Já em [Morais 2011], o autor realiza a implantação de um IDS utilizando uma solução híbrida para detectar intrusões, por meio das ferramentas OSSEC e Snort. Anteriormente à implantação, é realizado um estudo sobre o ambiente. O autor apresenta testes realizados em servidores de teste, verificando a eficácia do IDS em gerar alertas. Esta abordagem destaca-se por utilizar uma solução híbrida e pela organização da implantação realizada, porém o trabalho não traz em seu conteúdo questões reais relacionadas a análises de tentativas de intrusão em um ambiente em produção.

Dadas estas considerações, o presente estudo de caso visa apresentar aspectos práticos da implantação de um IPS em um ambiente real, analisando seus resultados e impacto na segurança do ambiente de rede.

## 3. Desenvolvimento

Nesta seção será apresentado o processo empregado para implantação do IPS, abordando pontos como a arquitetura do mesmo, seus componentes e características.

### 3.1. Localização

A rede de computadores em que foi realizado o estudo de caso possui alguns serviços disponíveis para acesso externo, como por exemplo VPNs, servidores *Web*, além de outros servidores que possuem endereços públicos, logo, é essencial protegê-los. Além de cada um desses *hosts* possuir um *firewall* individual, optou-se por configurar um *Host Based Intrusion Prevention System* (HIPS) em cada um deles. De acordo com [Kaspersky 2016],

o HIPS trata-se de um sistema que pode evitar ataques no nível do computador, sendo uma solução mais prática, visto que pode monitorar aplicativos funcionando em um *host* específico e bloquear atividades indesejadas.

Em conjunto aos HIPS, visando obter um ambiente de prevenção de intrusões capaz de detectar tanto ataques externos quanto ataques originados internamente, foi decidido adotar uma arquitetura composta por NIPS+HIPS. Na ilustração da Figura 1 pode-se visualizar a arquitetura definida para implantação do IPS. Devido a esta estrutura, é possível detectar ameaças destinadas à endereços da própria LAN ou então tendo como alvo a WAN.

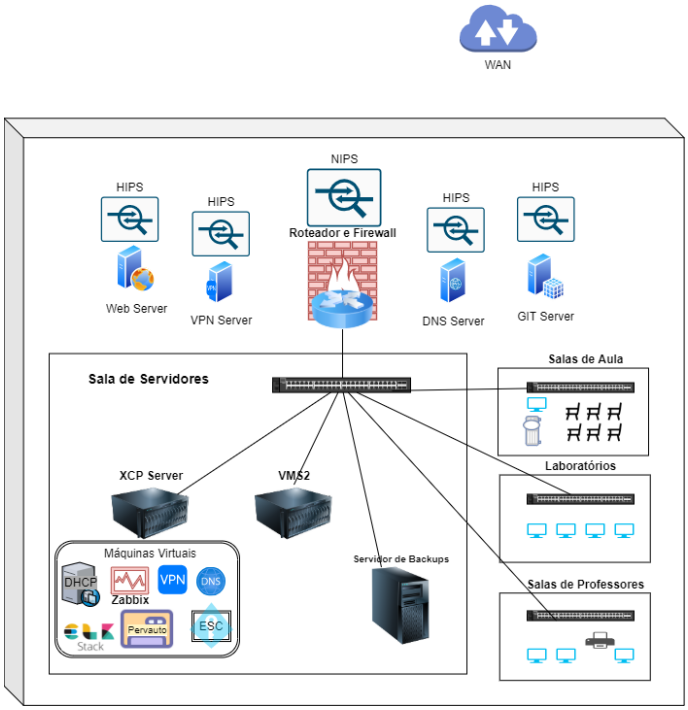


**Figura 1. Arquitetura do IPS.**

## 3.2. Configuração

O *software* utilizado para implantação do IPS foi o Suricata, escolhido devido à sua capacidade de atuar utilizando *multithreads*, o que contribui para seu desempenho, fornecendo maior velocidade na análise do tráfego, usando um poder maior de processamento fornecido pelos processadores multi-núcleo [Wong et al. 2017]. Todas as máquinas que receberam a instalação do Suricata têm como Sistema Operacional o Linux, sendo a distribuição o Ubuntu *Server* 20.04.

Para que o Suricata atue em modo *inline* é necessária a utilização do *iptables* através da biblioteca *nfqueue* [Suricata 2021]. Visto isso, no NIPS todas as *chains* do *iptables* foram configuradas para utilizar o *nfqueue*. Já nos HIPS, as *chains* configuradas para utilizar o *nfqueue* foram apenas a *INPUT* e *OUTPUT*. Em relação às regras do IPS, optou-se por utilizar o conjunto disponibilizado pela comunidade do Suricata, o qual abrange uma gama considerável de assinaturas e recebe atualizações constantes.

Durante uma semana, anteriormente ao início da execução dos NIPS+HIPS em modo *inline*, foram realizados testes e análises da solução atuando apenas como IDS, a

fim de identificar falsos positivos e tratá-los. Ao analisar os *logs* gerados ao fim do período deste período, foi possível contabilizar um total de 42.463 alertas. Foi possível observar, que, durante este período destacou-se a realização de varreduras referentes ao protocolo SSH e também a grande quantidade de alertas com cunho apenas informativo. Dentre os alertas de assinaturas referentes a informações apenas, que não necessariamente representam tentativas de intrusão, foram identificadas algumas assinaturas que poderiam vir a gerar falsos positivos após o início da execução do IPS. De acordo [Kirstens et al. 2021], falsos positivos se constituem quando o IDS/IPS identifica uma atividade como um ataque, mas a atividade é um comportamento aceitável.

Realizada a análise, foram desativadas as seguintes categorias de assinaturas:

- ET INFO: Não representa ameaças reais, apenas informações sobre o tráfego analisado que eventualmente se assemelha a comportamentos existentes em *malwares* e outras ameaças [Proofpoint 2020].
- STREAM ALERTS: Identifica que determinados pacotes analisados não seguem todos os padrões de rede adequados, isso acontece com os dados trafegados por diversas aplicações, o que na grande maioria dos casos não representa uma ameaça [Meeks 2017].
- ET *POLICY*: Refere-se à assinaturas que podem indicar violações à política da organização [Proofpoint 2020]. Ao analisar os alertas gerados para esta categoria, foi detectado que os mesmos referiam-se à comunicações legítimas, logo, optou-se por desativá-la.
- ICMP_INFO: Conforme [Proofpoint 2020], esta categoria é para assinaturas relacionadas a eventos específicos do protocolo ICMP, normalmente associados a eventos normais e operações para fins de registro.

### 3.3. Integração com a pilha ELK

A pilha ELK oferece a capacidade de agregar *logs*, analisá-los e criar visualizações para monitoramento de aplicativos e infraestrutura, auxiliando na velocidade de resolução de problemas, análises de segurança e muito mais [Amazon 2021].

A escolha por integrar o ELK com o Suricata se deu para tornar mais automatizada a visualização dos alertas e bloqueios gerados. A ferramenta Filebeat[1], que é responsável por coletar os *logs* do Suricata por meio de arquivos JSON, envia esses dados ao servidor onde está sendo executada a pilha ELK, para que as informações sejam processadas e disponibilizadas em uma interface *Web*. Na Figura 2 é representado o fluxo de tratamento dos dados realizado pela pilha. Na imagem, o primeiro componente trata-se de um *Beats*, que é o agente responsável pela coleta inicial dos dados. Vale ressaltar, que o servidor ELK foi configurado em uma máquina virtual individual, separadamente do Suricata. No NIPS e nos HIPS, foi configurado apenas o Filebeat para realizar a coleta dos *logs* e enviar ao servidor ELK, permitindo assim uma visualização centralizada dos alertas.

Outra ferramenta utilizada para auxiliar no gerenciamento dos *logs* gerados, foi o Synesis Lite, desenvolvido por [COWART 2020]. Essa ferramenta fornece análise de *logs* para o Suricata utilizando a pilha ELK. O projeto *open source* trata-se de uma solução para a coleta e análise de *logs* JSON do Suricata [COWART 2020] por meio da interface *Web* do Kibana. O Synesis, ao ser integrado com o ELK, permite uma visualização gráfica

[1]https://www.elastic.co/pt/beats/filebeat


**Figura 2. Fluxo de processamento dos dados pela pilha ELK.**

de informações como alertas, fluxos de tráfego, estatísticas, gráficos, dentre outros dados que auxiliam no gerenciamento de ameaças. Na Figura 3 é apresentado o *dashboard* principal, que contém dados como o número de alertas gerados em determinado período, gráficos referentes às categorias, assinaturas, serviços e outras informações.

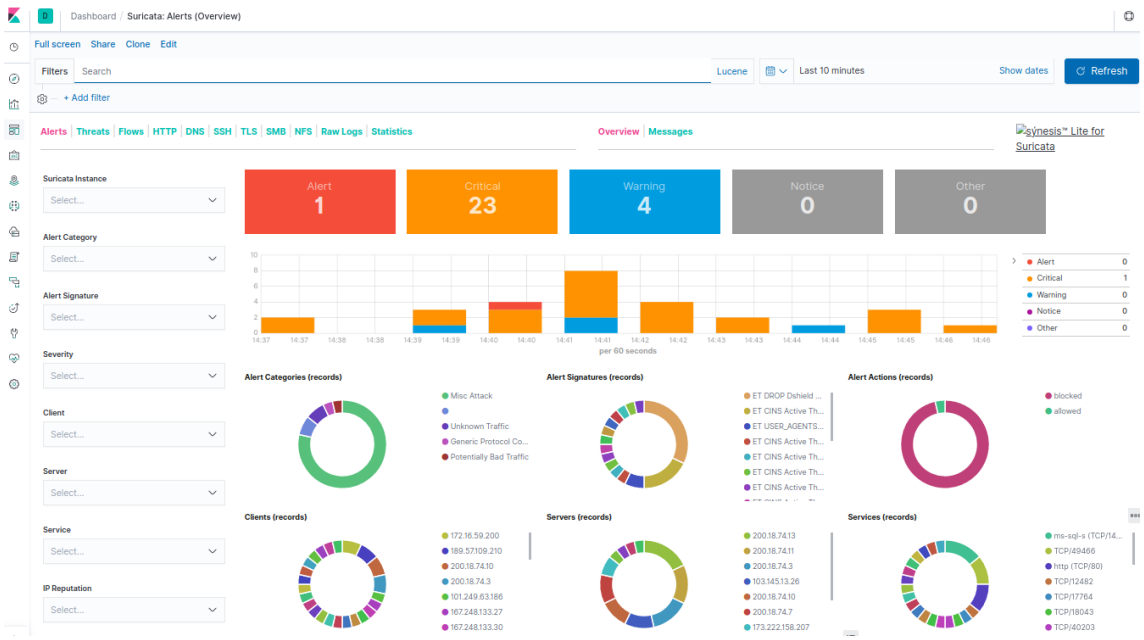


**Figura 3. *Dashboard* disponibilizado pelo Synesis com informações sobre os alertas gerados pelo Suricata.**

## 4. Resultados

Nesta seção será apresentada uma visão geral sobre as detecções e bloqueios realizados pelo IPS desde o início de sua execução até o momento atual, com o objetivo de elencar as principais ameaças identificadas e quais ações foram tomadas para mitigá-las.

Uma característica bastante importante na atuação do IPS, é sua capacidade de gerar bloqueios imediatos, por meio do *iptables* e *nfqueue*. Na Figura 4 podemos ver uma regra que foi criada em um dos HIPS, que têm como função bloquear comunicações originadas da Internet com destino à porta 80 do servidor em questão. Conforme mostrado na Figura 5, por meio da ferramenta *tcpdump* foram identificados pacotes com destino à porta 80 no dia 09/09/21 no horário de 10:47:30 e no segundo seguinte. Na Figura 6, ao analisar o arquivo de *logs* do Suricata, podemos também visualizar que a ferramenta realizou o bloqueio instantaneamente, visto que os pacotes coincidiram com a regra de nome “TESTE DROP 80”, criada para teste.

```
drop tcp $EXTERNAL_NET any -> $HOME_NET 80 (msg: "TESTE DROP 80"; sid:28042102; rev: 1; priority:1;)
```

**Figura 4. Regra criada para teste.**

```
[redacted]:~$ sudo tcpdump -i eth0.1000 host [redacted]
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0.1000, link-type EN10MB (Ethernet), capture size 262144 bytes
10:47:30.273838 IP [redacted].65279 > [redacted].http: Flags [S], seq 3103940794, win 65535, options [mss 1452,nop,wscale 2,nop,nop,sackOK], length 0
10:47:31.283773 IP [redacted].65279 > [redacted].http: Flags [S], seq 3103940794, win 65535, options [mss 1452,nop,wscale 2,nop,nop,sackOK], length 0
```

**Figura 5. Análise da comunicação via TCPDUMP.**

```
09/09/2021-10:47:30.273838  [Drop] [**] [1:28042102:1] TESTE DROP 80 [**] [Classification: (null)] [Priority: 1] {TCP} [redacted]:65279 -> [redacted]:80
09/09/2021-10:47:31.283773  [Drop] [**] [1:28042102:1] TESTE DROP 80 [**] [Classification: (null)] [Priority: 1] {TCP} [redacted]:65279 -> [redacted]:80
```

**Figura 6. *Logs* gerados pelo Suricata.**

## 4.1. Principais ameaças

Até o momento da escrita deste estudo de caso, o IPS está sendo executado há aproximadamente 2 meses. Durante esse período, destacam-se três tipos de tentativas de intrusão: varreduras, tentativas de conexão remota e tentativas de exploração de vulnerabilidades em servidores *Web*. Ataques a servidores Web e *scans* também estiveram entre os tipos de ataques mais reportados ao [CERT.br 2021] em 2020, os *scans* representando 59.85% e os ataques Web 3.99% do total.

O número de alertas gerados durante o primeiro mês de execução foi de 432.898, somando os alertas do NIPS e também dos HIPS. No gráfico da Figura 7 podemos visualizar os protocolos mais visados. Outro dado que destaca-se é o alto número de alertas com origem de endereços IP que de acordo com as assinaturas do Suricata, já possuem má reputação na Internet.

Além destas ameaças, foram identificados também alguns falsos positivos. Estes falsos positivos tiveram um impacto baixo, gerando apenas alguns bloqueios indevidos de comunicações HTTP específicas envolvendo usuários finais.

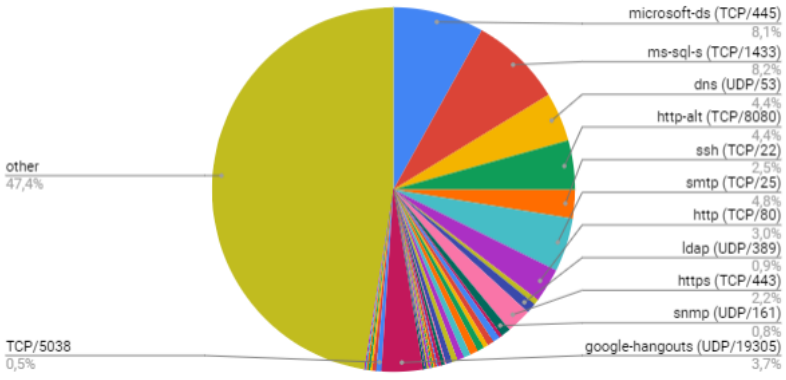


**Figura 7. Gráfico com a porcentagem de alertas relacionados aos protocolos.**

## 4.2. Mitigação das ameaças

Ao analisar os alertas e bloqueios gerados, identificou-se que uma quantidade considerável de alertas sobre escaneamentos estava sendo gerada acerca de protocolos que não são utilizados na rede, como o *mssql* e *microsoft-ds* por exemplo. Essas varreduras,

segundo [Kak 2021], tem como principal objetivo a verificação de portas para descobrir quais delas estão abertas, fechadas e filtradas. Visando otimizar execução do IDS/IPS, foram criadas regras de *firewall* para bloquear este tipo de pacote, evitando assim a geração de alertas desnecessários.

Outra ação tomada com base nos dados coletados, foi a criação de uma *blacklist* incluindo os endereços IP com maior número de registros de tentativas de intrusão. Para que não fossem bloqueados endereços legítimos e teoricamente não maliciosos, foram realizadas buscas na Internet em sites como o AbuseIPDB[2], onde é possível visualizar o histórico de atividades maliciosas de determinado endereço IP. Feito isso, foram criadas regras para bloquear comunicações com estes endereços conhecidamente maliciosos. As regras foram implantadas no *Firewall* principal da rede e também nos *Firewalls* individuais de cada *host* que possui IPv4 público.

As ações citadas foram tomadas após a análise dos alertas do primeiro mês de execução. Feitos os ajustes, ao final do segundo mês de execução do IDS/IPS, foi registrado um total de 204.533 alertas, representando uma diminuição de aproximadamente 47% em relação à quantidade contabilizada anteriormente aos ajustes e ações de mitigação.

## 5. Conclusões

O processo de implantação de um IPS demanda de planejamento, entendimento sobre a estrutura da rede e também sobre os serviços que a mesma provê.Tal compreensão é essencial para que as configurações do IPS sejam as mais otimizadas e eficientes quanto possível, buscando evitar a incidência de falsos positivos e negativos e principalmente bloquear as ameaças direcionadas à rede. É essencial que o ambiente seja monitorado e aprimorado constantemente, realizando as adequações e medidas necessárias para tornar a rede de computadores cada vez mais segura.

Outro aspecto importante neste processo é a visualização e gerenciamento dos alertas gerados pelo IDS/IPS com o auxílio de ferramentas como ELK e Synesis, que permitem a criação de um ambiente *Web* capaz de prover diversas informações sobre as detecções realizadas. Um ponto a se destacar em relação aos registros gerados, foi a dificuldade em gerenciar questões de armazenamento, visto que não há uma rotação automática dos *logs*, por isso foi necessária a criação de *scripts* para deletar registros antigos, mantendo apenas os do mês atual e anterior. Outra dificuldade encontrada foi em relação à pilha ELK, que demanda de uma quantidade de recursos computacionais considerável.

Dentre as principais contribuições do trabalho, destaca-se o processo de integração do Suricata com a pilha ELK e a ferramenta Synesis, visto que tutoriais e documentos sobre esta solução não são encontrados na Internet até o momento. Tal integração permite um maior controle acerca da atuação do IPS, permitindo visualizar detalhes dos dados acerca das detecções e bloqueios realizados, o que contribui para a tomada de ações referentes ao processo de mitigação de ameaças.

Um direcionamento futuro que pode trazer melhorias para a solução implantada é a criação de um conjunto de regras personalizadas, com foco na proteção dos serviços

[2]https://www.abuseipdb.com/

operantes da rede. Outra medida interessante seria a criação de um processo estruturado de testes de intrusão, com o fim de avaliar a segurança da rede existente por meio da simulação de ataques e mitigar as ameaças a partir disso.

## Referências


Amazon (2021). The ELK stack. Acesso em 07 jun. 2021.
Disponível em: https://aws.amazon.com/pt/elasticsearch-service/the-elk-stack/.

CERT.br (2021). Incidentes Reportados ao CERT.br - 2020.

COWART, R. (2020). sýnesis™ Lite for Suricata. Acesso em 07 jun. 2021.
Disponível em: https://github.com/robcowart/synesis_lite_suricata.

Farhaoui, Y. (2016). How to secure web servers by the intrusion prevention system (ips)? *International Journal of Advanced Computer Research*, 6:65–71.

Kak, A. (2021). Lecture Notes on "Computer and Network Security". *Purdue University*.

Kaspersky (2016). Host-based Intrusion Prevention System (HIPS).

Kirstens, Wichers, Jkurucar, and Kingthorin (2021). Intrusion Detection. Acesso em 14 jul. 2021.
Disponível em: https://owasp.org/www-community/controls/Intrusion_Detection.

Meeks, B. (2017). Suricata STREAM Alerts. Acesso em 13 jul. 2021.
Disponível em: https://forum.netgate.com/topic/114340/suricata-stream-alerts/3.

Morais, G. (2011). ANÁLISE E IMPLEMENTAÇÃO DE SISTEMAS IDS E IPS. *UNIVERSIDADE DE LISBOA*, page 71.

Mota Filho, J. E. (2018). IDS / IPS para a segurança em redes. In *15º Congresso Latino-americano de Software Livre e Tecnologias Abertas (15º LATINOWARE).*, Foz do Iguaçu.

Proofpoint (2020). ET Category Descriptions. Acesso em 13 jul. 2021
Disponível em: https://tools.emergingthreats.net/docs/ETPro%20Rule%20Categories.pdf.

Stallings, W. and Brown, L. (2014). *Segurança de Computadores: Princípios e Práticas*. Elsevier, Rio de Janeiro.

Suricata (2021). Setting up IPS/inline for Linux. Acesso em 01 jul. 2021.
Disponível em: https://suricata.readthedocs.io/en/suricata-6.0.2/setting-up-ipsinline-for-linux.html.

Utimura, L. N. and Costa, K. A. (2018). Aplicação e Análise Comparativa do Desempenho de Classificadores de Padrões para o Sistema de Detecção de Intrusão Snort. *Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*.

Wong, K., Dillabaugh, C., Seddigh, N., and Nandy, B. (2017). Enhancing suricata intrusion detection system for cyber security in scada networks. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–5.

Xing, T., Xiong, Z., Huang, D., and Medhi, D. (2014). Sdnips: Enabling software-defined networking based intrusion prevention system in clouds. In *10th International Conference on Network and Service Management (CNSM) and Workshop*, pages 308–311.