Network Security: Open-Source Intrusion Detection Systems

Ana Murta, Ana Henriques and Leonardo Freitas
University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {93284, 93268, 93281}@alunos.uminho.pt

Abstract. Com o crescimento da *Internet* e consequente conexão ao mundo cibernético, as redes encontram-se cada vez mais expostas a ameaças informáticas (*Cyber Threats*). Assim, *Intrusion Detection Systems* (IDS) procuram alertar os administradores quando algo ou alguém está a tentar comprometer a informação do seu sistema. Contudo, o processo de seleção e implantação de IDS é altamente técnico, caro e demorado, pelo que, para superar isto, é necessário tomar conhecimento de ferramentas de IDS (IDS tools), que serão a base deste ensaio escrito.

Keywords. *Intrusion Detection Systems*; *Network Security*; *Open Source Intrusion Detection; Suricata*; *Samhain*; *Snort*; *Security Onion*; IDS; HIDS; NIDS.

1 Introdução

Desde o aparecimento da tecnologia que a segurança da informação se evidencia um problema persistente, agravado pela constante evolução da tecnologia e pelo aumento do contacto com o mundo cibernético. Perante estas adversidades, tiveram de ser desenvolvidos mecanismos para proteger a informação destas ameaças. [4]

Neste ensaio, elaboramos um estudo detalhado acerca das *Open Source IDS Tools*, usando, para tal, alguns exemplos, quer de *Network Based Intrusion Detection System* (NIDS), como o Suricata e o Snort, quer de *Host Based Intrusion Detection System* (HIDS), como o OSSEC e o Samhain. Para além destes, temos, ainda, o Security Onion, que pertence a ambas as categorias anteriormente mencionadas. [4]

O significado de *Network Security* é um termo amplo e abrangente que descreve soluções de *hardware* e *software*, bem como processos e configurações relacionadas ao uso da rede, para proteger a mesma e os seus dados contra intrusões e outras ameaças. [4]

2 Intrusion Detection System (IDS)

Tal como o nome sugere, os IDS detetam e previnem entradas não autorizadas num ambiente informático. Todavia, os IDS não se focam apenas em detetar atividades anormais, estes também verificam se tais atividades são maliciosas. Aliás, em alguns casos, assim que permitida a tomada de ações de prevenção de forma automática, um IDS pode ser referido como um *Intrusion Prevention System* (IPS). [4]

Existem dois tipos de IDS: *Network Based IDS* (NIDS) e *Host Based IDS* (HIDS). Por um lado, o NIDS, implementado em locais estratégicos da rede, foca-se em analisar o fluxo de informação que circula na rede, procurando encontrar comportamentos suspeitos. Por outro lado, o HIDS concentra-se em examinar somente as atividades de um único *host*, monitorizando, por exemplo, os sistemas de arquivos acessados, os aplicativos utilizados ou *log* de dados. [4]

Quanto à sua categorização, os IDS podem ser classificados como ativos ou passivos. Ao recorrer a um ativo, que funciona sobre a base do IPS, os ataques suspeitos são automaticamente bloqueados, cumprindo um conjunto de regras pré-programadas. Já os passivos, que funcionam sobre a base do IDS, só monitorizam a rede e, perante uma situação suspeita, enviam um alerta ao administrador para este tomar medidas.[4]

3 IDS Tools

Existem várias ferramentas HIDS e NIDS disponíveis no mercado, tal como podemos observar na Fig.1. No decorrer deste ensaio, serão dadas a conhecer com mais pormenor as seguintes: a Snort e o Suricata, a título de exemplos de um NIDS, e a OSSEC, como HIDS. Adicionalmente, será, também, abordada a Security Onion dada a particularidade de ser uma ferramenta que oferece os dois tipos possíveis de IDS. [5]

Tool	Free	Open Source	NIDS/HIDS	Custom mod-rules	Mac Support	Analysis on Host
Suricata	✓	✓	**NIDS**	✓	✓	-
Samhain	✓	✓	**HIDS**	✓	✓	✓
Snort	✓	✓	**NIDS**	✓	✓	-
OSSEC	✓	✓	**HIDS**	✓	-	-
Security Onion	✓	✓	**HIDS, NIDS**	✓	-	✓

Fig. 1: Algumas ferramentas IDS.

3.1 Ferramenta Snort

Como supramencionado, o Snort é um NIDS que se destaca pela sua capacidade de analisar, em tempo real, o tráfego de rede e de registar pacotes em redes IP.[2] Este é capaz de detetar ameaças através de assinaturas[2] e, consequentemente, alertar os seus respetivos usuários. As respostas aos ataques são limitadas, centrando-se na filtragem e no bloqueio do tráfego e, ainda, no desligamento. O mecanismo mais usado é o *backtrace*: conhecer o ataque e ensinar o sistema a proteger-se numa próxima vez.

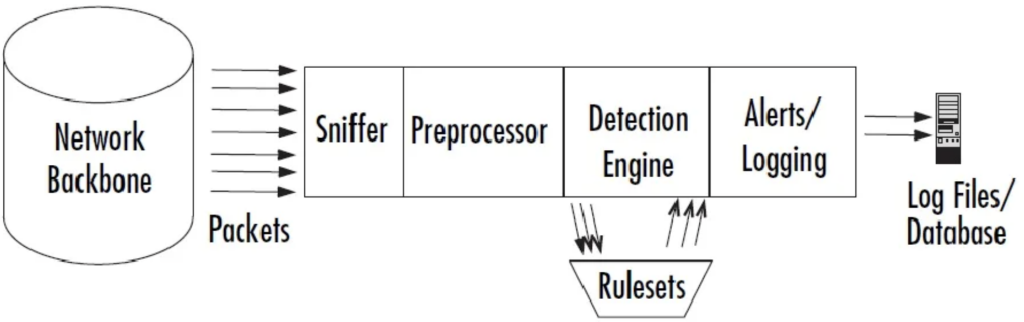

Fig. 2: Arquitetura e funcionamento do Snort.

A arquitetura do Snort consiste, maioritariamente, em 7 módulos:

1. Módulo de Captura de Pacotes;
2. Descodificador de Pacotes;
3. Pré-processadores;
4. Engenharia de Deteção;
5. Arquivos de regras;
6. *Plugins* de Deteção;
7. *Output Plugins*.

Grande parte das funcionalidades do descodificador consiste na colocação de ponteiros nos pacotes de dados para, mais tarde, serem analisados pela arquitetura de deteção. A engenharia de deteção é responsável por garantir que os cabeçalhos dos pacotes estão bem estruturados, verificando, por exemplo, se o *checksum* do cabeçalho IP está correto.[5] O uso de pré-processadores é fundamental visto que garante, por exemplo, a remontagem de pacotes fragmentados, a avaliação de desempenho e performance, o reconhecimento de dados sigilosos, entre outros.[2]

Atualmente, é o NIDS mais usado devido aos inúmeros benefícios que oferece:

- é gratuita e portátil;
- oferece rápidas respostas às ameaças;
- para redes que vão até 10Mbps, o seu desempenho não ultrapassa os 30mbps;
- é fácil de configurar e de implementar em qualquer nodo de uma rede;
- disponibiliza um conjunto bem documentado e testado de assinaturas; [5]

Contudo, esta ferramenta também evidencia algumas desvantagens:

- possui uma capacidade analítica limitada;
- apresenta uma implementação lenta e cansativa;
- é dispendioso ao monitorar pacotes em grandes redes;
- falha ao detetar pacotes fragmentados a altas velocidades de redes (>5Gbps) [5].

3.2 Ferramenta OSSEC

O OSSEC é um *open-source* HIDS, que realiza a análise de logs, o monitoramento de registos, a verificação da integridade de um ficheiro, a deteção de *rootkit* baseada em Unix e o alerta e resposta ativa, em tempo real.[5]

Este HIDS possui versões para os vários sistemas operativos e o seu funcionamento pode ser local ou agente e servidor. No modo local, como o OSSEC atua diretamente no computador onde foi instalado, embora todas as suas funcionalidades estejam disponíveis, não existem trocas de mensagens entre o agente e o servidor. No modo agente e servidor, o agente pode enviar as ameaças detetadas para o servidor analisar e ler os arquivos locais. Já o servidor realiza, então, a análise de logs, onde são geradas as notificações por e-mail, recebendo-os de outros computadores, e controla as regras, interpretadores de códigos e opções de configuração.[5]

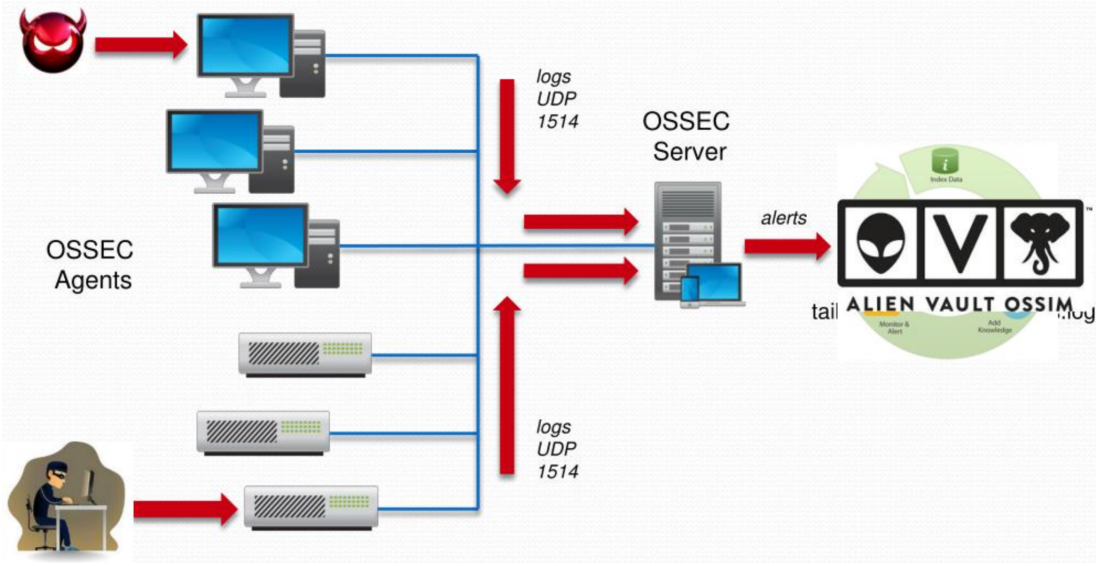

Fig. 3: Arquitetura do OSSEC.

O OSSEC pode ser instalado como uma ferramenta para monitorizar um *host* ou pode ser implantado num cenário *multi-host*, atuando como o servidor e os outros como agentes. Estas entidades comunicam com segurança recorrendo a criptografia. Adicionalmente, o OSSEC possui recursos de prevenção de intrusão, podendo reagir a eventos específicos, em tempo real, através de comandos e respostas ativas.[5]

Relativamente à sua arquitetura, este IDS *tool* é composto por um gerente central, que inspeciona e recebe informações de agentes, *syslog*, bases de dados e dispositivos sem agente. O OSSEC Agent é um pequeno programa, em que o agente recolhe informações e direciona-as para o gerente para análise e correlação.[5]

Assim como o Snort, este HIDS apresenta, no entanto, algumas desvantagens:

- a dificuldade em efetuar *upgrades* entre versões por causa das regras padrão que são *overwritten* em cada atualização;
- a coordenação de chaves pré-compartilhadas pode ser problemática porque, na arquitetura OSSEC, o cliente e servidor comunicam entre si através de um canal criptografado, usando o algoritmo *blowfish*. [5]

3.3 Ferramenta Security Onion

A Security Onion é uma distribuição Linux, mais concretamente Ubuntu, grátis e *open-source*, que funciona como um IDS, permitindo a detecção de intrusão, o gerenciamento de registros e monitorizações de segurança. Esta distribuição Linux dispõe de diversas ferramentas de análise, feitas para capturar pacotes que circulam pela rede ou pelos sistemas, que funcionam com base em regras para reconhecer anomalias e tráfego malicioso. Desta forma, podemos ter acesso a, por exemplo, Elasticsearch, Snort, Zeek, Wazuh, Cyberchef e NetworkMiner, entre outras.[1]

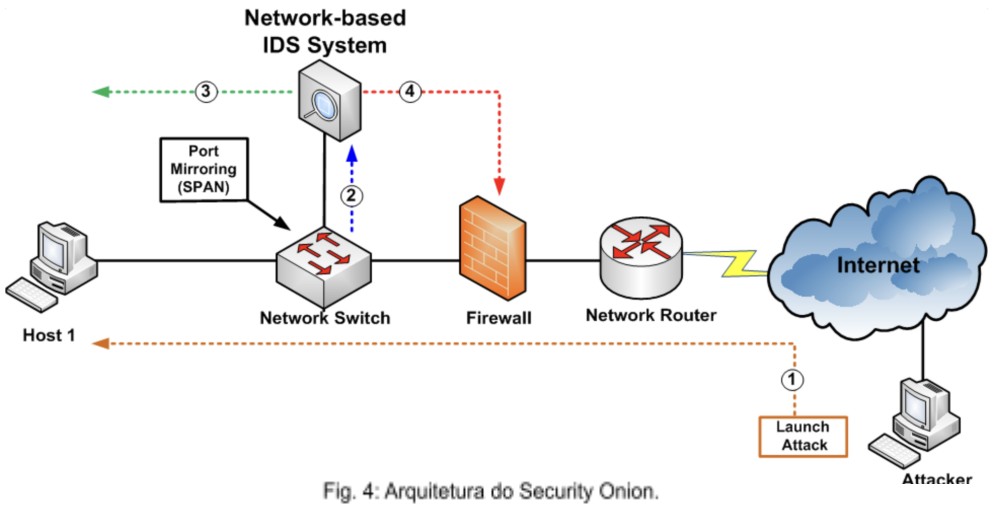

Fig. 4: Arquitetura do Security Onion.

Complementarmente, a Security Onion oferece uma visão interior do que está a acontecer por toda a rede, o que ajuda o usuário a agir perante algum perigo e, inclusive, pode reparar alguma suscetibilidade que possa ameaçar os dados ou o próprio sistema. [1]

Embora seja muito fácil de implementar, devido a um assistente de instalação que leva a que esteja operacional em poucos minutos, para conseguir o melhor funcionamento possível desta ferramenta, é imprescindível cumprir os seguintes requisitos mínimos na hora da instalação :

- usar um dispositivo físico e não visual;
- ter um sistema por cada rede a monitorizar;
- possuir 6TB de espaço em disco para logs e pacotes de rede;
- ter conexão ao *switch* mais próximo da *trunk port* para a *firewall*;
- configurar a porta do SW em modo SPAN. [1]

A Security Onion destaca-se, por isso, por inúmeras vantagens, nomeadamente: fácil instalação e configuração; simples interface de utilização; software gratuito e sem custo de licenças; boa base de apoio, quer em documentação, quer na comunidade que utiliza esta ferramenta. Contudo, também, evidencia algumas desvantagens, como ser preciso conhecimento intermédio/avançado de GNU/Linux e, para uma grande rede, serem necessários ainda mais recursos.[1]

3.4 Ferramenta Suricata

Similarmente às ferramentas previamente apresentadas, o Suricata é um NIDS *open-source* de alta performance, desenvolvido pela OISF (*Open Information Security Foundation*), que deteta anomalias no tráfego da rede. Este implementa uma linguagem de assinatura completa, estabelecendo correspondências a ameaças conhecidas, violações de políticas e a comportamentos maliciosos. [3]

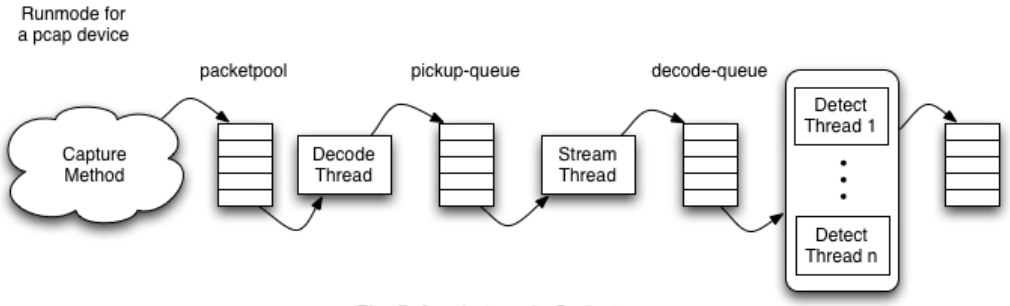

Fig. 5: Arquitetura do Suricata.

Uma das suas funcionalidades é a inspeção de tráfego de multi-gigabits, tendo sido construído num ambiente *multi-thread*, moderno e *clean*. Como revela estas características, o Suricata diferencia-se como uma ferramenta de alta performance. Este NIDS reconhece automaticamente protocolos como HTTP e aplica devidamente o mecanismo de deteção para detetar possível *malware* presente na rede.[3]

4 Conclusão

Com base no que foi apresentado, é indiscutível a importância da segurança da rede, que se revela a maior preocupação de qualquer organização. Com o IDS, é viável detetar o uso indevido de recursos da rede e, aliado ao IPS, proteger a nossa informação e os nossos dados contra potenciais ataques.

Ao longo deste estudo, averiguou-se que cada ferramenta do IDS tem as suas próprias vantagens e desvantagens e que, por isso, a escolha da melhor dependerá dos vários requisitos e necessidades da organização em questão. Ou seja, o OSSEC é uma ótima ferramenta para qualquer organização que procure realizar a detecção de *rootkits* e monitorizar a integridade dos ficheiros enquanto envia alertas em tempo real. O Snort, por outro lado, favorece quem procura um IDS *tool* com uma interface amigável, que seja útil para analisar profundamente os dados que recebe. Já o Suricata é uma ótima alternativa ao Snort que depende de assinaturas e que pode ser executada numa rede corporativa. Finalmente, o Security Onion é ideal para uma organização que ambicione uma ferramenta que construa vários sensores distribuídos para outras empresas em poucos minutos.[6] Ao combinar NIDS e HIDS, podemos descobrir quaisquer ataques que ignoram o NIDS e se um invasor de rede foi bem-sucedido ou não no *host* de destino.[5]

5 Referências

[1] Documentação da Empresa Security Onion (2022), em https://docs.securityonion.net/en/2.3.

[2] Snort: A Solução Completa Para Monitorar Tráfego em Redes, em: https://e-tinet.com/linux/snort-monitor-redes/

[3] Documentação da Empresa Suricata (2022), https://suricata.readthedocs.io/en/suricata-6.0.4.

[4] Tirumala, S., S., Sathu, H., Sarrafzadeh, A.: FREE AND OPEN SOURCE INTRUSION DETECTION SYSTEMS: A STUDY. (2015)

[5] Ambati, B., S., Vidyarthi D.: A BRIEF STUDY AND COMPARISON OF, OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS. (2013).

[6] Top 10 BEST Intrusion Detection Systems (IDS) (2022) https://www.softwaretestinghelp.com/intrusion-detection-systems/#Conclusion