# SISTEMAS DE DETEÇÃO DE INTRUSÃO GRATUITOS E DE CÓDIGO ABERTO: UM ESTUDO

**Eduardo Cunha a98980; Fábio Ribeiro a100058; Gonçalo Magalhães a100084**

**Universidade do Minho, Portugal**

**ABSTRACT** - A importância da cibersegurança não pode ser negada no atual ambiente cibernético. Com o crescimento contínuo da internet, a cibersegurança tornou-se uma necessidade tanto para grandes organizações, como para pequenas empresas e indivíduos. Os sistemas de deteção de intrusões (IDS) são considerados uma forma eficiente de detetar e prevenir ameaças à segurança cibernética. No entanto, não há atenção e sensibilização suficiente sobre os IDS, especialmente em pequenas empresas e indivíduos. Para superar isto, é necessário criar uma consciência das ferramentas IDS que formam a base deste trabalho. Nesta fase, apresentamos um estudo detalhado de três ferramentas IDS de código aberto que são as mais populares nas respetivas categorias. Os softwares IDS utilizados para este estudo são: Samhain, um IDS Baseado em Host (HIDS), Suricata um IDS baseado na rede (NIDS) e o Ironbee, um sistema universal de firewall de aplicação web. Este estudo de ferramentas IDS num só local servirá como fonte de conhecimento para todos. Além disso, isto também ajudará na identificação do software IDS adequado para cada caso.

**Keywords:** Cibersegurança, IDS, Samhain, Suricata, Ironbee.

## 1. Introdução

O presente trabalho abordará o tema da segurança na internet mais concretamente, o papel dos IDS's. Terá como principal objetivo informar as pessoas dos vários tipos de IDS's que existem e como funcionam.

A segurança da informação tem sido um problema contínuo desde o aparecimento da Tecnologia de informação (TI). O rápido desenvolvimento da Internet e dos sistemas de informação teve um impacto direto nas crescentes preocupações com a segurança. Com a dinâmica de ameaças em constante mudança de estratégias, os defensores devem acompanhar o ritmo dos "atacantes" e para isso as pessoas/organizações têm de estar cientes dos métodos de segurança cibernética e das suas várias aplicações.

## 2. Desenvolvimento

O papel da segurança cibernética é implementar um ambiente TI seguro e a melhor forma para isso é protegê-lo, pois, como diz o ditado: é melhor prevenir do que remediar.

A segurança cibernética envolve uma estratégia com a compreensão dos riscos cibernéticos devido às vulnerabilidades e propõe soluções para mitigá-los. As vulnerabilidades de segurança cibernética são aberturas no sistema que expõem o ambiente de TI aos invasores. Há vários tipos de ameaças à segurança, mas neste trabalho iremos abordá-las de forma generalizada.

## 3. Intrusion Detection System (IDS)

Tem a tarefa de detetar e prevenir invasões num ambiente de TI. Normalmente, inspeciona todas as atividades de entrada e saída e envia alertas apropriados aos administradores para ação posterior.

Vantagens:

- Monitorização, análise e classificação de eventos;
- Identificação de anomalias nas atividades dos utilizadores;
- Definição de limites na segurança;

Desvantagens:

- Escalabilidade difícil e complexa;
- Limitações ao nível dos recursos solicitados, na análise de grande volume de dados;
- Taxas altas de falsos positivos em IDS baseado em assinaturas;
- Perda de efetividade contra técnicas de evasão ou ataques sofisticados;

[4]

O IDS pode ser ativo ou passivo. No ativo, os ataques suspeitos são bloqueados automaticamente, com base em regras pré-programadas. Já o passivo apenas monitoriza as atividades, regista as suspeitas e relata-as ao administrador para ação.

Outro tipo de classificação é relativamente ao seu modo de deteção e de fonte de informação: o que deteta intrusões ao nível da máquina, é chamado de Host Intrusion Detection System (HIDS) já o que deteta intrusões na rede, é conhecido como Network-Based Intrusion Detection System (NIDS).

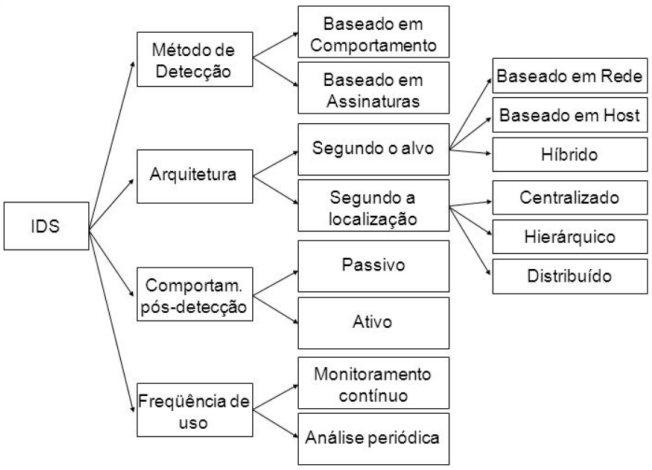


**Fig. 1.** Classificação de IDS

### 3.1. HIDS (Host-Based Intrusion Detection System)

Têm como principal função analisar toda a informação relevante, como logs do tráfego e da máquina onde está instalado, violações de integridade nos ficheiros do sistema, tentativas falhadas de login, entre outras possíveis anomalias.

Perante as várias funções e métodos que fazem uso para a deteção de intrusões, destacam-se:

- Verificação da integridade de ficheiros: Através de uma função de hash criptográfica é guardado o estado dos ficheiros do sistema, procedendo-se à comparação das hashes mais atuais.
- Análise de logs: Os HIDS utilizam os logs do sistema onde estão instalados para análise e comparação de padrões que, indiquem possíveis atividades "Exemplo: Um utilizador autenticou-se como root 8 fora das horas de trabalho";
- Deteção de rootkits: Busca por rootkits (softwares maliciosos).

### 3.2. NIDS (Network-Based Intrusion Detection System)

Identificam eventos de segurança, através da captura e análise de todo o tráfego na rede, podendo gerar alertas em tempo real ou posteriormente. Um NIDS procede à análise de duas principais componentes: a verificação da pilha protocolar e à verificação da aplicação protocolar. A primeira rastreia pacotes que não se encontram de acordo com as regras dos protocolos de rede, enquanto a outra certifica a aplicação protocolar rastreando violações de utilização de protocolos.

Os sistemas de deteção de intrusões na rede possuem algumas vantagens, nomeadamente na transparência de atuação uma vez que, a sua finalidade não exige obrigatoriamente uma instalação em cada máquina, isto porque, face à sua configuração e funcionamento, consegue resistir e passar despercebida a intrusos. Por outro lado, existem também algumas desvantagens neste tipo de IDS, salientando-se a impossibilidade de analisar tráfego encriptado, assim como a necessidade de configurações especiais e auxiliares, na sua recolha.

Existem muitos IDS disponíveis no mercado, porém para este estudo escolhemos os mais conhecidos de cada categoria, para além de serem todos gratuitos e open source.

## 3.3. Samhain – HIDS (Sistema de detenção baseado em host)

O Samhain é um IDS baseado em Host que pode ser implantado centralizado ou em cada computador como implementação individual.

Algumas das funções do Samhain são:

- Verificação de Integridade de Arquivos
- Monitoramento de Arquivos e Análise
- Deteção de root-kit
- Monitoramento da porta
- Deteção de Rogue SUID
- Monitoramento e Análise de processos ocultos.

### 3.3.1. Características

É um aplicativo multiplataforma de código aberto para sistemas como Linux, Mac OS, Solaris, AIX e Windows com emulador POSIX.

A implementação Cliente/Servidor do Samhain é composta por componentes como: Verificador de Integridade, agente do servidor, software do cliente, servidor Yule, entre outros.

O software cliente funciona como daemon (programa de computador que executa como um processo em plano de fundo) [6], mantendo uma memória das alterações de arquivo logo, o banco de dados de assinatura de arquivo só precisa estar atualizado quando o daemon reiniciar e baixar o banco de dados do servidor central.

O agente do servidor atua como um agente de controle considerando que o agente cliente atua como escravo e está comprometido com o servidor. O servidor Yule é responsável por recolher relatórios e logs dos clientes (processo de registo de eventos) e é através dele que os clientes recebem configurações e atualizações. A integridade do host no Samhain é monitorada usando vários módulos extensíveis tornando-o assim, uma escolha perfeita.

## 3.4. Suricata – NIDS (Sistema de detenção baseado em rede)

Este sistema possui deteção de intrusões em tempo real (IDS), prevenção de intrusão em linha (IPS), monitorização de segurança de rede (NSM) e processamento offline de ficheiros. O método de deteção usado é baseado em assinaturas ou regras, podendo usufruir de conjuntos mais abrangentes das mesmas. Este NIDS foi produzido de forma a trazer novos conceitos e mecanismos ao contexto da deteção de intrusões estabelecendo, o emprego de um mecanismo multi-threaded. Este motor de análise de tráfego, possibilita a utilização mais eficiente dos processadores modernos com múltiplos núcleos, o que ajuda na tentativa de desempenhar as funções de forma mais eficiente.

### 3.4.1. Escalabilidade

Está configurado para executar cada instância do processo IDS em vários threads através de diferentes processadores tendo em conta o "balanceamento da carga" e o desempenho, tornando-o um sistema altamente escalável (um sistema diz-se escalável se ele alinhar o uso dos seus recursos de modo a obter melhor desempenho independentemente do seu sistema). [8]

### 3.4.2. Identificação e suporte de protocolo

É uma prática comum filtrar o tráfego com base no nível da porta. No entanto, os invasores ignoram essa filtragem facilmente. Depois de reconhecer os protocolos comuns em execução na rede, as regras são escritas para o protocolo e não para a porta esperada, dando ao Suricata uma capacidade excecional de análise e controle de malware.

### 3.4.3. Identificação de arquivos, somas de verificação MD5 e extração de arquivos

Vários tipos de arquivos transmitidos pela rede podem ser identificados pelo Suricata, podendo até ser encontrados e marcados para extração usando hashes MD5. Estas hashes são calculadas em tempo real durante a extração e gravação dos arquivos para o disco. Além disso, este sistema IDS pode tomar a decisão de manter, ou não esses arquivos.

### 3.4.4. Motor de deteção

O conjunto de regras Suricata permite a deteção para captura, descodificação e classificação de pacotes e até mesmo partes deles. Os algoritmos são baseados em vários padrões de correspondência que podem ser selecionados com uma grande variedade de opções de configuração.

## 3.5. Ironbee (Sistema Universal de Firewall de Aplicação Web)

O Ironbee é um IDS projetado com a intenção de ser uma estrutura padrão de forma a permitir a sua utilização em diferentes locais. É uma estrutura de aplicativos da Web de código aberto que pode atuar como um esqueleto para firewalls de aplicativos da web. A sua especialidade é a sua flexibilidade para construir a firewalls de acordo com as necessidades (firewall é um programa ou equipamento físico, que tem por objetivo proteger um determinado ponto da rede). [9]

### 3.5.1. Regras de Gerenciamento Ironbee

Existem três tipos de abordagens de correspondência de regras:

A Correspondência Básica irá percorrer cada entrada de dados e procurar por correspondências com operadores específicos, executando apenas uma vez no ciclo; o Stream Matching, refere-se ao fluxo de dados que é analisado em pedaços em vez de, analisar um grande volume de dados, esta metodologia garante que não é necessário um buffer grande para realizar a tarefa; as regras externas, que são escritas e implementadas para criar uma comparação personalizada. Estas regras são definidas e configuradas externamente e podem ser mais expressivas e flexíveis.

### 3.5.2. Recursos Funcionais

- Interface baseada no usuário com vários modos de implantação;
- Acompanhamento de atividades de curto e longo prazo com dados históricos;
- Modelo de dados baseado em entidades em tempo real;
- Capacidade de correspondência de padrões múltiplos e mistos;
- Decisões baseadas em políticas;
- Interoperabilidade com outros aplicativos e sistemas de segurança com capacidade de troca de dados.

O Ironbee pode ser configurado para qualquer um dos modelos de segurança disponíveis: deteção de ataque DOS e DDOS; monitoramento de análise segura e validação de XM; segurança política de conteúdo; reconhecimento de ataques de força bruta; verificação de vulnerabilidade; criptografia de cookies; assinatura digital. Possuindo um monitoramento e análise de tráfego integrados para tráfego de entrada e saída para explorações e vulnerabilidades.

## Conclusão

Neste artigo, tentamos enfatizar a importância de sistemas de deteção de intrusão (IDS) fornecendo uma análise de três importantes ferramentas de código aberto: Samhain, Suricata e Ironbee. Este documento fornece ainda uma análise técnica e funcional das ferramentas de IDS para dar uma melhor compreensão para os indivíduos e pequenas empresas que não estão bem a par destas tecnologias. Este estudo servirá como referência na seleção de ferramentas IDS adequadas, com base na finalidade, risco e recursos.

## Referências:


1. Sreenivas Tirumala, Hira Sathu, Abdolhossein Sarrafzadeh, F.: FREE AND OPEN-SOURCE INTRUSION DETECTION SYSTEMS: A STUDY aberto pela última vez 2022/10/6
2. Autor desconhecido, F.: Malware, https://pt.malwarebytes.com/malware/ aberto pela última vez 2022/10/2
3. Autor desconhecido, F.: Open-source, https://en.wikipedia.org/wiki/Open_source aberto pela última vez 2022/10/2
4. Autor desconhecido, F.: IDS, https://pt.wikipedia.org/wiki/IDS 1 aberto pela última vez 2022/10/2
5. Autor desconhecido, F.: Intrusion Detection System (IDS) vs Intrusion Prevention System (IPS), https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs-ips/ aberto pela última vez 2022/10/3
6. Autor desconhecido, F.: Daemon(computação), https://pt.wikipedia.org/wiki/Daemon_(computação) aberto pela última vez 2022/10/5
7. Autor desconhecido, F.: Log de dados, https://pt.wikipedia.org/wiki/Log_de_dados aberto pela última vez 2022/10/5
8. Autor desconhecido, F.: Escalabilidade, https://pt.wikipedia.org/wiki/Escalabilidade aberto pela última vez 2022/10/5
9. Autor desconhecido, F.: Firewall, https://pt.wikipedia.org/wiki/Firewall aberto pela última vez 2022/10/2
10. João Ricardo Claro, F.: Sistemas ids e ips – estudo e aplicação de ferramenta open source em ambiente Linux, https://painel.passofundo.ifsul.edu.br/uploads/arq/20160331191141344853464.pdf aberto pela última vez 2022/10/5
11. Figura.1-“Classificação dos IDS” https://slideplayer.com.br/slide/370233/2/images/9/IDS%3A+classificação+Baseado+em+Comportamento+Baseado+em+Assinaturas.jpg