

Universidade Fernando Pessoa

Mecanismos de Detecção de Intrusão – OSSEC HIDS

Análise e implementação numa organização



Sheilla Raquel Leite Nascimento

Porto, Setembro de 2017

Universidade Fernando Pessoa

Praça 9 de Abril, 349

P-4249-004 Porto

Tel. +351-22550.82.70

Fax. +351-22550.82.69

geral@ufp.pt

# Mecanismos de Detecção de Intrusão – OSSEC HIDS

## Análise e implementação numa organização

Sheilla Raquel Leite Nascimento

Dissertação apresentada à Universidade Fernando Pessoa como parte dos requisitos para obtenção do grau de Mestre em Engenharia Informática, ramo Sistemas de Informação e Multimédia (SIM), orientada pelo Professor Doutor Feliz Ribeiro Gouveia.

# Mecanismos de Detecção de Intrusão – OSSEC HIDS

## Análise e implementação numa organização

Por:

Sheilla Raquel Leite Nascimento

---

Orientador

Professor Doutor Feliz Ribeiro Gouveia

Universidade Fernando Pessoa

Faculdade de Ciência e Tecnologia

Praça 9 de Abril, 349, 4249-004 Porto, Portugal

Setembro de 2017

III

# Resumo

Nesta dissertação, realizou-se um estudo comparativo analítico, com o objetivo de testar a inclusão do *Open Source Security* (OSSEC), um *Host Intrusion Detection System* (HIDS), na infraestrutura de segurança de uma organização de grande porte. Inseriu-se a infraestrutura de Segurança Digital já implementada uma nova ferramenta para auxiliar o monitoramento, testar a utilização em conjunto com ferramentas de rede, cito: *Firewall*, *Intrusion Prevention System* (IPS) e *Web Application Firewall* (Waf). Para a execução do estudo, propõe-se a utilização de um mecanismo de detecção de intrusão em servidor como complemento à política de segurança da instituição.

Foram definidos os principais elementos componentes da infraestrutura. Os alertas gerados foram analisados e comparados aos alertas produzidos por mecanismos de prevenção de intrusão como de um *Intrusion Prevention System* (IPS), identificando falhas. Com estes resultados analisados, se demonstra que a complementação da infraestrutura de rede com a inclusão da ferramenta para monitoramento, trouxe resultados favoráveis e comprovou sua eficácia.

O estudo de caso foi realizado em um ambiente real, numa organização de grande porte no Brasil. Por questões de confidencialidade, o nome e quaisquer outros dados que possam identificar a instituição foram preservados, a fim de garantir o anonimato e a segurança da instituição que possibilitou o estudo.

# Abstract

In this dissertation, an analytical comparative study was carried out to test the inclusion of Open Source Security (OSSEC), a Host Intrusion Detection System (HIDS), in the security infrastructure of a large organization. The Digital Security infrastructure was implemented a new tool to help the monitoring, test the use in conjunction with network tools, I cite: Firewall, Intrusion Prevention System (IPS) and Web Application Firewall (Waf). For the execution of the study, it is proposed to use a server intrusion detection mechanism as a complement to the institution's security policy.

The main components of the infrastructure were defined. The generated alerts were analyzed and compared to alerts produced by intrusion prevention mechanisms such as an Intrusion Prevention System (IPS), identifying faults. With these results, it is demonstrated that the complementation of the network infrastructure with the inclusion of the tool for monitoring, has brought favorable results and proved its effectiveness.

The case study was carried out in a real environment, in a large organization in Brazil. For reasons of confidentiality, the name and any other data that may identify the institution were preserved in order to guarantee the anonymity and security of the institution that made the study possible.

# Dedicatória

A Deus, pois sem sua permissão nada é possível. Aos meus mentores espirituais que sempre me guiam, protegem, auxiliam e suportam.

A cada ser de luz que fez parte da minha jornada, contribuindo para minha formação e evolução.

Nascer, morrer, renascer ainda e progredir sempre, tal é a lei. Allan Kardec

# Agradecimentos

A elaboração desta dissertação foi um desafio pessoal, necessitando de determinação, dedicação e desprendimento.

Quero registrar meu agradecimento e amor incondicional a minha filha, minha amada Amanda Letícia Nascimento Cardoso, por entender minha ausência em virtude do afastamento nos períodos de aulas presenciais e o apoio nas longas horas de estudo individual. A minha mãe Maria das Graças por me auxiliar e compreender e a minha família por me apoiar e encorajar sempre.

Ao meu orientador, Professor Doutor Feliz Ribeiro Gouveia, por toda a disponibilidade, incentivo e dedicação, pelo exemplo de profissional focado e capacitado e pela ajuda em todos os momentos.

Agradeço a equipa parceira que me facilitou os acessos, conversou e explicou as dificuldades da instituição, bem como suas fragilidades.

# Índice

Lista de Figuras.....	X
Lista de Tabelas .....	XI
Lista de Acrónimos .....	XII
1 Introdução .....	13
1.1 Motivação .....	13
1.2 Objetivo.....	16
1.3 Metodologia utilizada .....	17
1.4 Estrutura da Dissertação .....	19
2 Segurança de redes.....	20
2.1 Conceitos essenciais.....	20
2.2 Intrusion Detection System – IDS .....	25
2.2.1 Arquitetura do IDS .....	26
2.2.2 Detecção de ameaças.....	28
2.3 HIDS (Host-Based Intrusion Detection System) .....	29
2.4 NIDS (Network-Based Intrusion Detection System).....	30
2.5 Intrusão, definição de perfil e possível deteção .....	31
2.6 OSSEC – Open Source Security .....	32
2.6.1 Regras de Classificação do OSSEC .....	33
2.6.2 Exemplos de Alerta do OSSEC .....	35
2.6.3 Recursos e funcionalidades do OSSEC .....	37
3 Especificação da infraestrutura do caso de estudo.....	40
3.1 Infraestrutura atual .....	40
3.2 Problemas na segurança atual .....	43
3.3 Inclusão do OSSEC.....	44



4 Implementação e Testes .....	46
4.1 Instalando o OSSEC .....	46
4.1.1 Instalar o OSSEC no servidor .....	47
4.1.2 Instalar o OSSEC no Agente .....	49
4.1.3 Configuração dos agentes: .....	51
4.1.4 Configurar a Interface Web .....	52
4.1.5 Portsentry e configuração do OSSEC.....	54
4.1.6 Configuração para leitura de portas com o Nmap .....	54
4.2 Detecção do IPS.....	55
4.3 Detecção do HIDS OSSEC.....	60
4.3.1 Alertas obtidos .....	60
4.3.2 Exemplo de Detecção .....	63
4.4 Exemplos de ações tomadas.....	65
4.5 Análise dos dados .....	67
5 Conclusão.....	69
Bibliografia .....	70
Anexo A .....	72
Anexo B .....	75

# Lista de Figuras

Figura 1: Estatísticas dos Incidentes repostados ao CERT.br.....	14
Figura 2: Estatísticas de Incidentes de Rede - CTIR e IPS.....	15
Figura 3: Sistema de Prevenção de Intrusão (IPS).....	22
Figura 4: Funcionamento de um IDS.....	27
Figura 5: Tipos de IDS.....	27
Figura 6: Plataformas que o OSSEC suporta .....	33
Figura 7: Demonstração do console do OSSEC .....	38
Figura 8: Demonstração da Infraestrutura de Rede .....	42
Figura 9: Categorias de aplicativos por contagem de ataque .....	44
Figura 10: Infraestrutura com o OSSEC.....	45
Figura 11: Tela de instalação do OSSEC.....	47
Figura 12: Tela de inicialização do OSSEC .....	49
Figura 13: Tela inserir Agente no OSSEC.....	50
Figura 14: Tela inserir chave no Agente OSSEC .....	51
Figura 15: Server OSSEC modo Web .....	55
Figura 16: Alertas .....	57
Figura 17: Quantidade de ataques. Portal 1 dia 2 .....	57
Figura 18: Ataques total.....	58
Figura 19: Ataques bloqueados Portal 1 .....	59
Figura 20: Endereços que geraram alertas. ....	62
Figura 21: Detecção por porta. ....	63
Figura 22: Exemplo de tabela detecções. ....	64
Figura 23: Quantidade de alertas gerados em um dia de conturbação social .....	66

# Lista de Tabelas

Tabela 1: Instalação do <i>Portsentry</i> .....	53
Tabela 2: Alertas aos portais monitorados pelo IPS .....	56
Tabela 3: Ataques aos Portais monitorado pelo IDS .....	58
Tabela 4: Alertas OSSEC acima de nível 3 .....	60
Tabela 5: Alertas OSSEC acima de nível 5. ....	61

# **Lista de Acrónimos**

OSSEC - Open Source Security

IDS - Intrusion Detection System

HIDS - Host Intrusion Detection System

NIDS - Network Intrusion Detection System

IPS - Intrusion Prevention System

HIPS - Host Based Intrusion Prevention System

NIPS - Network Based Intrusion Prevention System

WAF - Web Application Firewall

VPN - Virtual Private Network

CMS - Cryptographic Message Syntax

DES - Data Encryption Standard

AES - Advanced Encryption Standard

IPSec - Internet Protocol Security

OSSIM - Open Source Security Information Management

SSL - Secure Sockets Layer

WPA - Wi-Fi Protected Access

PIN - Personal Identification Number

DMZ - Desmilitarize Zone

# 1. Introdução

O objetivo deste trabalho foi verificar a utilidade da informação fornecida por um *Host Intrusion Detection System* (HIDS) em uma rede com *Intrusion Prevention System* (IPS), *Firewall* e outros aplicativos de segurança. O estudo foi realizado com o objetivo de comprovar a eficácia da arquitetura proposta.

O *Open Source Security (OSSEC)* foi instalado e seus resultados avaliados, com o intuito de verificar se é uma ferramenta útil e agregadora, visando possibilitar uma medida de segurança adicional, auxiliando aos profissionais de segurança e subsidiando com informações na tomada de decisões.

O nosso desafio é propor a instalação de uma ferramenta de código aberto e sem custos de licenciamento, em uma rede com mecanismos proprietários já atuantes. Nesse ínterim, iremos propor a integração e garantir a utilidade do *Open Source Security (OSSEC)*, como uma ferramenta de análise de computador em uma infraestrutura que não possui esta funcionalidade.

O estudo foi realizado em uma Instituição Pública Federal do Brasil e por questões de segurança o nome da instituição e os dados que a possam revelar foram omitidos.

O trabalho conclui que a utilização do OSSEC melhora a qualidade e a quantidade da informação disponível e contribui para o aumento da segurança.

## 1.1. Motivação

A necessidade de proteger uma informação, seja armazenada ou em trânsito tem sido uma preocupação e um campo de estudo desde a Antiguidade. Com o advento dos computadores, o armazenamento e a transmissão da informação passaram a ser feitos, em grande parte, em sistemas informatizados, tornando-se imprescindível protegê-los, a primeira publicação sobre *Intrusion Detection Systems* foi feita em 1980, onde os autores tentaram apresentar a importância dos sistemas de monitoramento para auditar trilhas que levam ao mau uso (Kizza, Joseph 2005).

Mesmo usuários donos de um menor patrimônio líquido podem ser interessantes para os atacantes, especialmente no caso de pessoas que tenham acesso profissional a redes corporativas ou a recursos de alto valor. Os atacantes podem manter tais funcionários como alvos, numa posição de reféns em que seriam obrigados a colaborar, facilitando acesso a um banco de dados corporativo ou permitindo um vazamento de dados.

Ataques a grandes empresas são documentados diariamente, conforme o Centro de Estudos, Resposta e Tratamento de incidentes de segurança no Brasil CERT-BR. Os números do gráfico abaixo demonstram a quantidade de ataques às grandes corporações no Brasil.

#### Total de Incidentes Reportados ao CERT.br por Ano

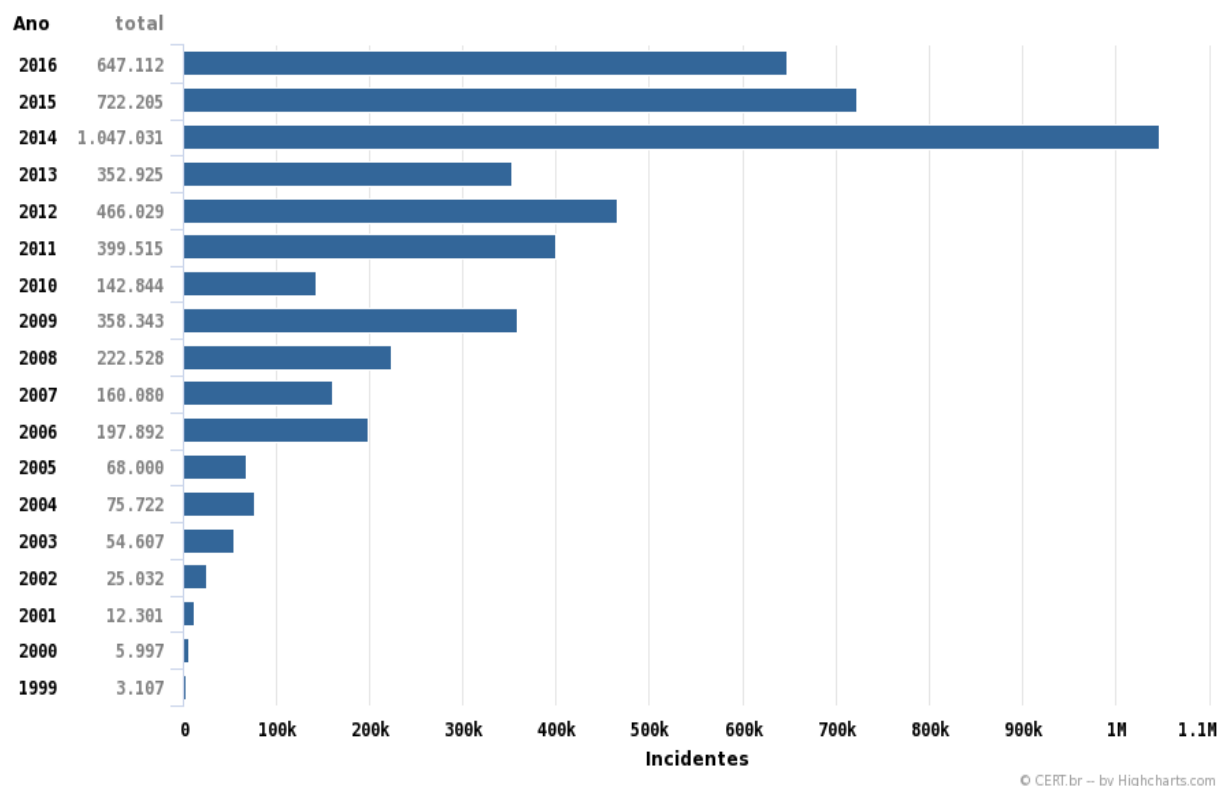


Figura 1: Estatísticas dos Incidentes reportados ao CERT.br

Conforme as corporações utilizam mais sistemas de detecção de violações e melhoram os processos de resposta a incidentes, os atacantes se aprimoram. Essa mudança levou a adaptações no seu modo de ataque e empresas menores e com menos segurança se tornaram alvo. A importância destas empresas é o acesso que podem permitir a redes das grandes empresas.

É necessário analisar quem tem acesso à rede da empresa, realizar testes de segurança para garantir endereços de página seguros, controlar redes virtuais privadas (*VPN*), e implementar autenticação em dois fatores para garantir que o acesso e a comunicação estejam seguros.

O potencial de ameaça que se pode alcançar com um ataque direcionado, seja para descobrir falhas, porta dos fundos nos sistemas, mapeamentos de rede ou tentativas por força bruta para se descobrir senhas tem gerado grandes danos às corporações. Alguns tipos de ataque se aproveitam da fase de manutenção dos servidores, onde os atacantes tentam usar para dissimular seu rastro, ou tentar esconder a intrusão.

Um exemplo da vulnerabilidade que é premente na atualidade pode ser constatado ao avaliarmos o gráfico abaixo, parte integrante do Relatório de Estatísticas de Incidentes de Rede no Governo no 2º Trimestre/2017. O gráfico foi elaborado pelo Centro de Tratamento de Incidentes de Redes (CTIR), subordinado ao Gabinete de Segurança Institucional da Presidência da República do Brasil. São apresentados os percentuais por categoria de incidentes. Destacam-se, como de maior ocorrência, as categorias de “Abuso de Sítio” (30,89%), seguido de “Indisponibilidade de Sítio” (16,05%). A figura seguinte apresenta os principais incidentes.

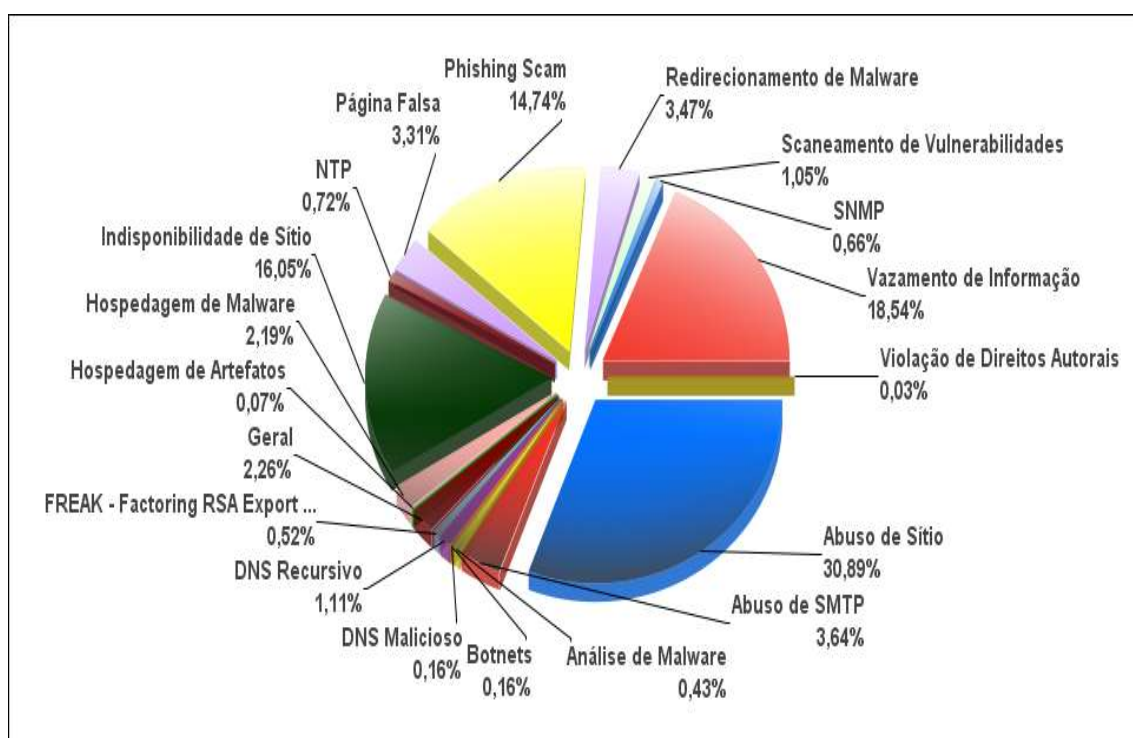


Figura 2: Estatísticas de Incidentes de Rede - CTIR

A segurança em rede é o processo de prevenir e detetar qualquer uso não autorizado de uma rede de computadores. Mesmo sistemas que aparentam despertar pouco interesse aos atacantes, como os de uma universidade ou os domésticos ligados à Internet, são constantemente alvos de ataques. Detetar estas investidas e os métodos utilizados é muito importante para uma política de segurança.

Há muitas ferramentas disponíveis para a segurança de uma rede de computadores e também para o ataque. Elas podem ser de dois tipos: aplicativos (*software*) e equipamentos (*hardware*). As ferramentas evoluíram nas últimas décadas, da mesma que forma que as técnicas de ataque se aprimoraram. Assim, pode-se definir que um ataque à segurança é qualquer ação que comprometa a segurança da informação de uma organização.

O *Open Source Security* (OSSEC) é uma ferramenta considerada o canivete suíço de sistemas de detecção de intrusão. Com essa ferramenta é possível fazer análise de *Logs*, verificar a integridade de arquivos, monitorar ações de administradores e obter alertas em tempo real. As ferramentas de detecção de intrusão são conjuntos de técnicas que são feitas para identificar qualquer tipo de atividades maliciosas, Vokorokos (2006).

Ante as funcionalidades supracitadas, será proposto a utilização conjunta com outros mecanismos de segurança, buscando aumentar a segurança da instituição parceira onde os testes serão validados. Trabalhando na área de segurança digital há algum tempo, principalmente com os contratos de aquisição e manutenção dos serviços de segurança, nota-se que os valores das ferramentas são consideravelmente altos. Valores elevados inviabilizam que empresas de menor expressividade tenham acesso a estes serviços, portanto, encontrar uma alternativa sem custos para garantir a segurança digital destas organizações é uma possibilidade interessante.

## 1.2. Objetivo

O objetivo deste trabalho é fornecer segurança, a baixo custo, com a utilização de ferramenta livre, que possa ser utilizada em conjunto a outras tecnologias, ou separadamente para prover segurança.

A questão principal é validar o funcionamento do OSSEC e verificar a fiabilidade de utilização desta ferramenta, sem custos para a instituição. Foi verificada a viabilidade e utilidade de uma estrutura onde o OSSEC fez a verificação em alguns servidores específicos.



A proposta deste estudo é a utilização do OSSEC em uma infraestrutura de rede robusta, onde foi avaliado a sua capacidade e o grau de efetividade, trabalhando em conjunto a outros mecanismos de segurança já implantados, demonstrando que uma ferramenta de software livre pode complementar e mesmo aprimorar a estrutura existente. A hipótese inicial, é que um sistema com vários níveis de detecção de intrusão, seja melhor com o OSSEC utilizado como complemento.

Os servidores monitorados receberam um tráfego já tratado por um mecanismo de prevenção de intrusão, *Host Based Intrusion Prevention System (HIPS)* e um *Firewall*, tentando assim, aprimorar a segurança. O IDS OSSEC não interferirá na rede ou no servidor monitorado.

O objectivo foi verificar a necessidade e utilidade da estrutura em paralelo com a existente, constatar o emprego da ferramenta na emissão de alertas, baseada na análise de log, servidores, portas e alertas específicos, que conseguiram passar pelas ferramentas que fazem análise de rede

Adicionalmente foi decidido utilizar o OSSEC para detetar ataques internos. Esta possibilidade está diretamente associada ao fato da rede analisada não possuir nenhum tipo de monitoramento interno, ou seja, os sistemas de detecção de intrusão já existentes não conseguem detetar ataques internos ou a servidores específicos.

### **1.3. Metodologia utilizada**

Este comparativo será elaborado com o intuito de validar as funcionalidades do OSSEC em complementação com ferramentas proprietárias, que geram um grande custo para as instituições que necessitam dos serviços de proteção. Sendo o OSSEC uma ferramenta sem custos de licenciamento não será fonte de custo adicional, o que torna a proposta viável e interessante para a instituição parceira, bem como para outras instituições.

E necessário esclarecer que este estudo foi feito com intervalo de cinco dias coletando dados, com uma massa de dados considerável, respeitando o tempo disponível para o mesmo, bem como deixarmos ressaltada a possibilidade de um estudo mais avançado, a posteriori. O tema é vasto, ressalta-se que apenas alguns tipos de comparativos serão feitos neste trabalho. A proposição de correções na infraestrutura da instituição estudada é um norteador do trabalho, sendo que o estudo não se encerra com os resultados que serão tratados neste, as possibilidades de implementação e aprimoramento são muitas e serão definidas em um momento oportuno.

O OSSEC não realizará nenhum tipo de intervenção na rede, sendo apenas um mecanismo de alertas. Produzirá as estatísticas e emitirá alertas de monitoramento dos servidores para os endereços eletrônicos cadastrados.

Na fase de testes da ferramenta, nenhuma regra adicional será criada no OSSEC, ele funcionará com a instalação básica e sem nenhum tipo de adaptação. As adaptações e possíveis interferências nos servidores monitorados bem como a elaboração de regras e a análise comportamental da rede da instituição serão alvo de estudo futuro.

Inicialmente foi permitido apenas o monitoramento dos servidores em modo promíscuo, onde a ferramenta apenas coletará dados sem intervir neles, visando a confirmação da utilidade do *software* em uma rede que não possui nenhum mecanismo de monitoramento específico para computador: o sistema de detecção de intrusão em computador (*Nakamura and Geus 2007*), faz o monitoramento com base em informações de arquivos de *Logs* ou de agentes de auditoria.

As restrições consideradas neste trabalho são a estrutura organizacional e a necessidade de preservar o nome da instituição onde foram feitos os testes, uma vez que qualquer tipo de informação pode colocar a segurança da referida instituição em risco. Os nomes de servidores, equipamentos e as parametrizações da rede tem que ser avaliadas minuciosamente, a fim de revelar o estritamente necessário, respeitados os termos de confidencialidade e o grau de acesso do autor na referida instituição.

O tempo para coleta e análise dos dados foi restrito de forma que, um período mais substancial de dados e outras análises ficarão para trabalhos futuros. A coleta será feita com a instalação do agente OSSEC nos servidores a serem analisados. Os dados serão analisados e comparados com as saídas dos mecanismos de segurança já existentes, buscando testar a eficácia de um controle de segurança com a utilização conjunta das ferramentas.

Como restrição a este estudo, ficou clara a dificuldade em conseguir uma instituição parceira que permitisse que os testes fossem realizados. Um desafio foi elaborar o estudo sem criticar a política de segurança da instituição e não expor o nome da instituição, bem como qualquer tipo de falha. Conseguir os acessos que permitissem a instalação dos softwares e deixar o ambiente pronto para os testes foi um processo demorado e de difícil aceitação pela instituição parceira.

Foi necessário, para a configuração complementar da ferramenta, a instalação de programas adicionais como o *Portsentry*, o *Nmap* e para a confecção das análises o *QlikView*.

Como premissa foi dada a garantia constante que a instituição não seria de forma alguma prejudicada, bem como não teria nenhum tipo de constrangimento. A instituição não permitiu nenhum tipo de

intromissão no ambiente e aceitou receber recomendações sobre ações de prevenção, tendo a ferramenta que ser utilizada sempre em modo promíscuo, isto é sem atuar nos dados ou servidores, e nenhuma regra nova pode ser criada ou implementada.

Como proposição para outros trabalhos, fica a implantação em todos os servidores do OSSEC HIDS, bem como a configuração de todos os servidores, a criação de regras personalizadas e um possível desenho de uma infraestrutura mais robusta, com a utilização da OSSEC para agregar valor e segurança a instituição parceira.

## 1.4 Estrutura da Dissertação

Este trabalho está disposto em cinco capítulos, sendo que o primeiro expõe a motivação para o tema escolhido, os objetivos pretendidos com o estudo que busca validar a questão “Qual é a utilidade do OSSEC em uma infraestrutura com ferramentas de Segurança Digital em nível de rede?”, e o método de investigação, que será comparativo analítico entre um *Intrusion Prevention System (IPS)* e um *Host Intrusion Detection System (HIDS)*.

No segundo capítulo serão definidos conceitos fundamentais referentes a segurança da informação, mecanismos de detecção de intrusão, e mais especificamente, aos mecanismos de detecção de intrusão em computador e por sua vez uma explicação sobre o funcionamento do OSSEC. Neste capítulo, estão elencadas algumas formas de intrusão, definição de perfis de intrusão e possíveis métodos de detecção. Nele apresenta-se as regras de classificação dos alertas e esclarece-se alguns recursos e funcionalidades do OSSEC.

O terceiro capítulo, apresenta a infraestrutura da instituição parceira, trazendo informações de tipos de equipamentos, modelo da rede e descrições sobre a infraestrutura de segurança digital da instituição parceira. No quarto capítulo, temos a implementação do estudo, como a instalação do OSSEC, dicas de comandos e outros. Segue com as detecções feitas pelo *Intrusion Prevention System (IPS)* que está como primeira barreira e o OSSEC que está instalado nos servidores e serve como último mecanismo de detecção e emissão de alertas para a infraestrutura estudada.

São feitas algumas explicações sobre os resultados do OSSEC e as melhorias que os resultados possibilitaram que fossem implementadas na instituição. No quinto e último capítulo, temos as conclusões sobre o estudo realizado, os conhecimentos aprendidos e algumas propostas para futuro.

## 2. Segurança de redes

Um sistema seguro é aquele que faz tudo o que foi projetado para fazer e nada que não tenha sido determinado para fazer, mesmo que alguém tente forçá-lo a se comportar de maneira diferente, conforme *Stalling* (2008). Isto se aplica a uma rede de computadores, um software, um esquema físico de proteção de uma informação, enfim, a uma variedade de sistemas. Sendo assim, segurança de sistemas de informação é um meio termo entre segurança e funcionalidade. Para que um sistema funcione, devemos correr riscos que não podem ser anulados. Como disse Bruce *Schneier* (2000), em seu livro “*Secrets and Lies*”, segurança da informação é, no fundo, um gerenciamento de risco.

O modelo de um sistema seguro consiste em uma mensagem que é transmitida entre duas partes, através de algum canal de comunicação, que pode ser, por exemplo, a internet ou outra ligação por meio eletrônico conforme Terada, Routo (2008). As duas partes que se comunicam serão chamadas de principais na transação. Só é possível conseguir um canal seguro se as duas partes concordam com a adoção de mecanismos de segurança. Assim, propor um modelo geral confiável, prospectar uma configuração de rede que possa aprimorar a segurança, o modelo deverá ser tal que um oponente não possa violar a sua segurança

As ferramentas de segurança das redes de computadores são projetadas de acordo com três princípios básicos: o primeiro princípio é a prevenção de possíveis ataques; o segundo é a detecção de qualquer atividade maliciosa, a última, mas não menos importante, a resposta a qualquer tipo de ataque, *Kizza, Joseph* (2005). É importante destacar que a instituição possui uma política de segurança implementada, com uma infraestrutura de *Firewall* e um *Web Application Firewall* (WAF). Alguns conceitos essenciais necessários para o estudo serão apresentados abaixo.

### 2.1 Conceitos essenciais

Os conceitos aqui descritos são utilizados como o suporte para o entendimento do estudo, e são fundamentados nas definições de Santos, Osvaldo (2011), Goodrich e Tamissa (2013) e Nakamura (2007).

**Ataque à segurança do sistema**, derivado de uma ameaça inteligente, ou seja, um ato inteligente que é uma tentativa deliberada (especialmente no sentido de um método ou técnica) de burlar os serviços de segurança e violar a política de segurança.

**Backdoor ou Porta dos Fundos**, programa que permite ao invasor manipular um computador comprometido. Normalmente este programa é colocado de forma a não ser notado.

**Bot** é um programa que, além de incluir funcionalidades de replicação, sendo capaz de se propagar automaticamente através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados e enviar spam.

**Cavalo de Troia** é um programa, normalmente recebido dentro de outro programa, por exemplo um cartão virtual, álbum de fotos, protetor de tela ou jogos. Este programa além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

**Checkpoint** é um equipamento que combina tecnologias rápidas de rede com recursos de processamento de alto desempenho, fornecendo o mais alto nível de segurança e agrega ferramentas de segurança, Firewall, VPN e resposta a solicitações de acesso HTTP. Funciona como um ponto de controle para os acessos a rede.

**Código malicioso** é um termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, vermes, *bots*, cavalos de tróia e *rootkits* que são tentativas de se descobrir senhas de administrador.

**Controle de roteamento** é a seleção de rotas fisicamente seguras para certos dados e permite mudanças de roteamento, especialmente quando existe suspeita.

**Distributed Denial of Service (Ddos)** é um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

**Demilitarized Zone (DMZ) ou rede de perímetro**, é uma sub-rede física ou lógica que suporta os serviços de fronteira externa de uma organização a uma rede maior e não confiável, normalmente a Internet. Quaisquer dispositivos situados nesta área, isto é, entre a rede confiável, ou seja, a rede

privada local e a rede não confiável ou a Internet, está na zona desmilitarizada.

**Firewall** em sua definição é um conjunto de componentes que restringe o acesso entre uma rede protegida e a internet, ou entre um conjunto de redes. As funcionalidades do *Firewall* decorrem da filtragem seletiva de pacotes baseada nas informações contidas nos cabeçalhos. A filtragem obedece a regras que analisam o cabeçalho dos pacotes e não aprofundam no conteúdo das informações transitadas. Há filtros de pacotes dinâmicos, ou baseados em estado, que mantêm também o estado das conexões, o que aperfeiçoa a função de filtragem. No entanto, ainda possuem vulnerabilidades.

Entre as desvantagens, destaca-se a impossibilidade de identificar as aplicações dos computadores que estão a enviar ou receber dados das redes inseguras. *Firewalls* de perímetro não são capazes de bloquear aplicações maliciosas presentes nos computadores das redes internas que usem métodos de comunicação aparentemente benignos, como, por exemplo, o protocolo HTTP.

**Intrusion Prevention System (IPS)** ou Sistema de Prevenção de Intrusão, pode trabalhar na detecção de computador ou de rede e se dividem em dois tipos HIPS (computador) ou NIPS (rede). Um NIPS ou *Network Intrusion Prevention System* tem o foco no monitoramento e atuação na rede em que está acoplado, baseando-se no histórico de comportamento e tráfego de dados desta rede. Um HIPS ou *Host Intrusion Prevention System* tem o foco no monitoramento e atuação no computador em que está acoplado. Na figura que segue temos a representação dos tipos de IPS.

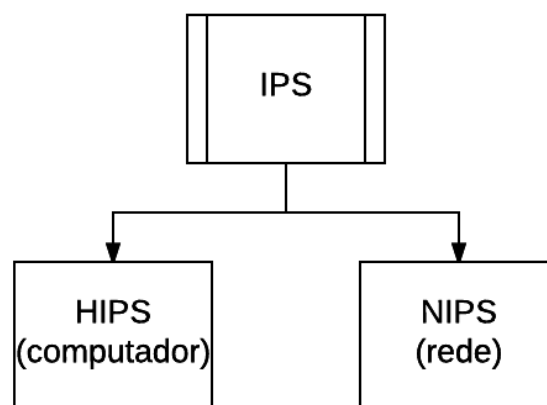


Figura 3: Sistema de Prevenção de Intrusão (IPS)

**Invasão** é um ataque bem-sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

**Log** é o registro de atividades gerado por programas de computador. No caso de *Logs* relativos a

incidentes de segurança, eles normalmente são gerados por *Firewalls* ou por IDS.

**Mecanismos de Segurança** são ferramentas utilizadas para garantir a segurança da instituição são divididos em duas categorias:

- Funções de “porteiro” são mecanismos destinados a controlar o acesso ao sistema, impedindo a entrada de visitante indesejado. Fazem parte desta categoria os sistemas de senha e login, e os sistemas de proteção contra vírus e vermes, que examinam automaticamente arquivos acessados na internet e em componentes de armazenamento, detetando e limpando pragas diversas. Ex.: *Firewall*.
- A segunda linha de defesa são os mecanismos de controle interno, programas que monitoram a atividade de uma rede, buscando detetar a presença de intrusos. Ex.: *Intrusion Detection System*.

**Nmap** é uma das ferramentas mais utilizadas para exploração de rede e auditoria de segurança.

**Relatório de segurança** é um documento (ou um dispositivo incorporando vários relatórios) que é elaborado com procedimentos para detetar, informar ou permitir a recuperação de um ataque à segurança.

**Portsentry** é um tipo de IDS capaz de monitorar as portas do computador, detetando tentativas de *scanner* de portas.

**Rootkit** são programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido.

**Scanner** é utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados.

**Segurança da Informação** possui alguns princípios básicos que são confidencialidade, integridade e disponibilidade. A política de segurança se define como um conjunto de regras e procedimentos que regulam a forma como se protege os recursos informáticos de ameaças, seguindo os princípios abaixo:

- Confidencialidade é a proteção dos dados contra divulgação não autorizada, a proteção da informação em trânsito ou armazenada e a defesa para os ataques passivos. Os sistemas criptográficos podem torná-la ininteligível a quem não tenha autorização para conhecê-la e proteção contra uma análise de tráfego. Neste caso, o atacante não tem acesso à informação

diretamente (quando se encontra cifrada, por exemplo), mas consegue saber sua origem e seu destino, o tamanho da mensagem, a frequência com que é transmitida, e outras informações que podem ser úteis.

- Integridade de dados é a garantia que o dado recebido não tenha sido corrompido. A integridade pode ser comprometida de duas maneiras: a alteração maliciosa e a alteração acidental. A alteração maliciosa funciona quando um atacante altera a mensagem armazenada ou em trânsito, a alteração acidental acontece por exemplo, por erros de transmissão ou corrupção de dados armazenados.
- Disponibilidade é a garantia que a informação esteja sempre disponível para uso quando usuários autorizados necessitarem.

**SIEMI** é um sistema de gerenciamento de eventos de informações de segurança. Esta definição de segurança da informação e gestão de eventos é utilizada para cobrir os requisitos do PCI-DSS (*Payment Card Industry – Data Security Standard*), um fórum aberto global que trata da segurança para proteção de dados de pagamento.

**Sniffer** é um programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

**Spyware** é um programa que monitora atividades de um sistema e envia as informações coletadas para terceiros.

**Vírus** é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

**Virtual Private Network (VPN)** é um termo usado para se referir à construção de uma rede privada, utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Estes sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados, possam ter acesso a rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.



**Vulnerabilidade** é uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

**Web Application Firewall (WAF)** é um software que trabalha entre o servidor HTTP/S e o cliente, filtra entradas do cliente e saídas do servidor *WEB*. Ele monitora o tráfego, analisa a lógica de aplicação *web* na camada 7 do modelo OSI, e trabalha com os aplicativos / servidores *web*. Seguindo sempre regras de segurança e graças a esse conjunto de regras é possível registrar ataques e bloquear.

Possui funcionalidades como *blacklist*, lista de endereços IP a serem bloqueados, funções para controle de banda e até mesmo bloqueio de ataques *Denial of Service* (DoS). É importante notar que o WAF possui a mesma estrutura de uma *firewall*.

Nakamura (2007), explica que a necessidade da mudança no enfoque dado à segurança, que passa de uma abordagem única baseada na segurança ‘de borda’ (controle das conexões com outras redes), para a necessidade de maior acompanhamento e monitoramento das atividades internas, o que representa novas camadas de segurança. O ambiente cooperativo e o grande nível de interconetividade intensificam a necessidade de diferentes mecanismos de segurança.

## 2.2 *Intrusion Detection System – IDS*

Os sistemas de detecção de intrusão ou *Intrusion Detection System* (IDS) possuem a capacidade de detectar e alertar os administradores quanto a possíveis ataques com base em comportamentos anormais na rede ou nos servidores. Há dois tipos de IDS, o que detecta intrusão em computador *Host Intrusion Detection System* (HIDS) e o que detecta intrusão em redes *Network-Based Intrusion Detection System* (NIDS).

O IDS oferece algumas funcionalidades, que podem ser obtidas com a análise de *Logs* e arquivos, como:

- Monitorar e analisar atividades de usuário e sistema;
- Analisar a integridade de arquivos importantes do sistema;
- Analisar estatisticamente padrões de comportamento desconhecidos;
- Analisar comportamento baseado em padrões conhecidos (assinaturas);
- Analisar atividades anormais; e

- Identificar origem e destino de ataques.

O OSSEC é um HIDS e realiza operações de análise de *Logs* e de integridade de sistemas, detecção de *rootkits*, alertas e resposta ativa, algumas características:

- Análise de *Log* e correlação;
- Regras flexíveis baseadas em XML;
- Alertas baseados em horários;
- Grande biblioteca de regras existentes;
- Verificação de integridade;
- Detecção de *rootkits*; e
- Resposta ativa com emissão de alertas.

Os próximos tópicos explicam a arquitetura do IDS, definições de HIDS e NIDS, conceitos de intrusão e especificação do HIDS OSSEC.

### 2.2.1 Arquitetura do IDS

O IDS possui uma arquitetura de constituição funcional com quatro componentes: *E boxes*, *A boxes*, *D boxes* e *C boxes*. A sua definição é a seguinte:

*E box (Event)* – sensor que captura os eventos do ambiente monitorado, os elementos de baixo nível são enviados para *A box*, é feita a busca por padrões, que podem revelar ataques ou intrusões.

*A box (Analysis)* - produz eventos de alto nível, indicadores de atividades de mais alto nível, estes elementos retroalimentam a *A box* e são enviados para as *D box* e *C box*.

*D box (Storage)* – sistema de armazenamento de informação (sistema de ficheiros ou base de dados).

*C box (Countermeasure)* recebe as deteções efetuadas (eventos reveladores de intrusões, ou tentativas) de baixo ou alto nível, as *C box* são componentes responsáveis pela reação a ataques, por exemplo enviando e-mail, relatórios ou alertas.

As setas representam o fluxo de dados transmitidos entre as caixas.

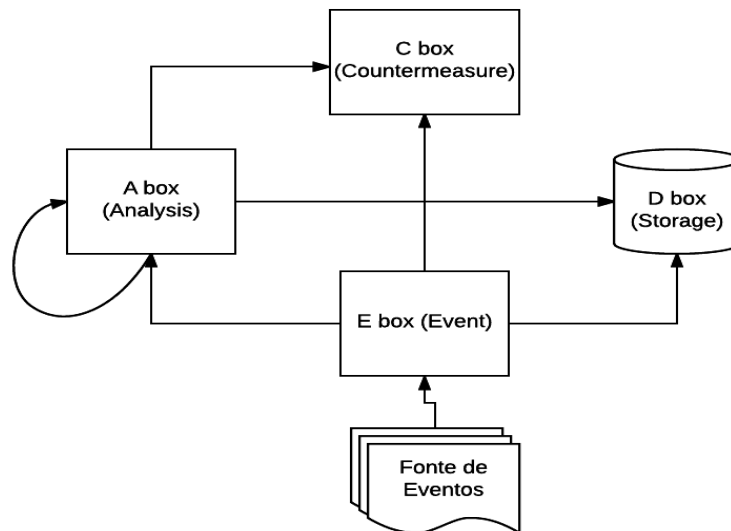


Figura 4: Funcionamento de um IDS

A classificação do IDS é feita por suas características operacionais. No Método de detecção pode-se basear em conhecimento ou em comportamento. No tipo de fonte de eventos monitorados que podem ser computadores (*host based*), redes (*network based*) e híbridos. No instante de detecção que pode ser tempo real, tempo real virtual ou à posteriori e com relação a reatividade pode ser ativo ou passivo e o tipo de análise que realiza singular ou cooperativa. Abaixo segue uma figura com os tipos de IDS, que podem ser HIDS, NIDS ou IDS Híbrido.

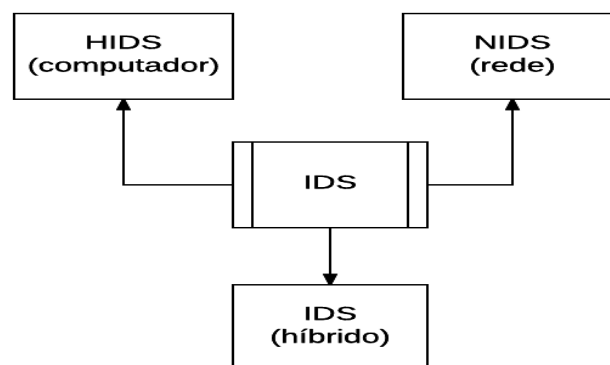


Figura 5: Tipos de IDS

O IDS trabalha como um alarme que pode realizar o controle com base em um tipo de conhecimento como as assinaturas de ataques ou em desvios de comportamento, ele funciona de acordo com uma

série de funções que trabalham de modo integrado, sendo possível detectar, analisar e responder a atividades suspeitas. Conforme postula *Kizza* (2005) as principais vantagens dos IDS são:

- Detecção e resposta em tempo real, se estiver em pontos estratégicos da rede, consegue detectar intrusões e emitir alertas;
- Capacidade de detectar ataques, porque monitora no nível de transporte da arquitetura da rede. Nesse nível analisa pacotes não apenas por endereços, mas também em números de porta; e
- Baixo custo, são necessários apenas alguns agentes em alguns pontos estratégicos da rede. O monitoramento passivo é outro ponto positivo, pois não há tráfego de rede normal resistente a intrusão. A combinação de diferentes tipos de *Intrusion Detection System* pode ser útil para a organização, buscando proteger a rede de diferentes tipos de ameaças, principalmente de ataques internos com um *Network-Based Intrusion Detection System* (NIDS) e os ataques externos podem ser detectados por um *Host Intrusion Detection System* (HIDS).

### 2.2.2 Detecção de ameaças

Um dos problemas do IDS, considerando a eficiência (precisão da detecção), que se contabiliza através do número de erros de detecção que ocorrem, conforme esclarece Nascimento, Gustavo (2010) é a quantidade de Falso Positivo. Para avaliar a qualidade dos sistemas IDS, primeiro precisamos definir alguns termos.

Quando um IDS está monitorando o tráfego ou os eventos de rede, ele tenta decidir se o tráfego ou evento é mal-intencionado ou não. Quando o IDS indica uma intrusão, isso é chamado de positivo. Se o alerta correspondente se refere a uma tentativa de intrusão real, então temos um Verdadeiro Positivo (VP), ou seja, a afirmação positiva do IDS deve ser confiável, pois é uma asserção correta. No entanto, o IDS também pode indicar uma intrusão mesmo que não tenha ocorrido nenhum ataque. Neste caso, temos o que chamamos de Falso Positivo (FP).

Verdadeiro positivo: um verdadeiro positivo é um alerta real, levantado em resposta a uma tentativa de intrusão. Isso indica que o sistema de detecção de intrusão detecta precisamente um ataque particular ocorrido.

Falso Positivo: um falso positivo é um alerta falso, levantado em resposta a um comportamento não-malicioso, ou seja, um evento incorretamente identificado pelo IDS como sendo uma intrusão quando nenhum ocorreu. Isso indica que o sistema de detecção de intrusão detecta um ataque apesar de nenhum ataque real ter ocorrido.

Por outro lado, se o IDS indicar que o tráfego ou o evento é inofensivo, isso é chamado de negativo. Quando o IDS indica que não há intrusão e esta é uma asserção correta, é chamado de Verdadeiro Negativo (VN). Pelo contrário, quando o IDS não indica uma intrusão, mas uma tentativa de intrusão realmente existe, temos um Falso Negativo (FN).

Negativo Verdadeiro: é o evento quando nenhum alerta é aumentado e nenhuma tentativa de intrusão ocorre. Isso indica que o sistema de detecção de intrusão não cometeu um erro na detecção de uma condição normal.

Falso Negativo: é o evento quando nenhum alerta é gerado, mas ocorre uma tentativa de intrusão real, ou seja, um evento que o IDS não consegue identificar como uma intrusão quando de fato ocorreu.

O OSSEC possui uma deficiência na detecção e bloqueio de *portscans*, por isto precisa ser integrado a outras ferramentas para garantir esta funcionalidade.

### **2.3 HIDS (Host-Based Intrusion Detection System)**

Um sistema de detecção de intrusão em computador, segundo Nakamura e Geus, (2007) faz o monitoramento do sistema com base em informações de arquivos de *Logs* ou de agentes de auditoria. O *Host Intrusion Detection System* pode ser capaz de monitorar os acessos e alterações em arquivos importantes do sistema, modificações nos privilégios dos usuários, processos do sistema e programas que estão sendo executados, uso da CPU e detecção de *port scanning*. Essas ferramentas são usadas para detetar atividades maliciosas em um único computador Kizza (2005).

A detecção de intrusão em computador conforme Kizza (2005) apresenta algumas vantagens:

- Capacidade de verificar sucesso ou falha de um ataque rápido analisando os *Logs* do evento, apresentando informações mais precisas e menos falsos positivos;
- Detecção em tempo quase real, sendo os alertas enviados ao administrador rapidamente;
- Não necessita de hardware adicional para sua instalação assim tendo um custo reduzido;
- Pode acessar informações antes e após a encriptação de dados;
- É capaz de analisar atividades em baixo nível, como acesso as permissões dos arquivos e tentativas de mudanças de privilégios;

Ele utiliza a soma de verificação (*checksum*), para a validação da integridade dos arquivos do sistema, porque em arquivos alterados ou corrompidos, pode ter sido instalado algum tipo de programa espião que busque de alguma forma, comprometer o sistema.

Um *Host Intrusion Detection System* tem funções específicas como controle de conexões, uso da central de processamento da unidade, tipos de programas executados, processamento do sistema, controle de privilégio de usuários, validação de integridade de arquivos por meio de soma de verificação (*checksum*), e os arquivos que sofreram algum tipo de acesso. Com isto é possível controlar o computador e detetar qualquer tipo de ação ou anomalia, enviando mensagens para o responsável que tomará as decisões sobre o tipo de alteração a ser feita e classificá-la em uma ameaça ou uso normal do sistema.

## 2.4 NIDS (Network-Based Intrusion Detection System)

Um sistema de detecção de intrusão em rede segundo Nakamura e Geus (2007), faz o monitoramento do tráfego do segmento de rede, agindo de modo promíscuo, ou seja, apenas lê a informação que o servidor recebe e não interfere diretamente no fluxo. É realizada a captura e posterior análise dos cabeçalhos dos pacotes, efetuando uma comparação com os padrões anômalos ou assinaturas de ataques. As possíveis ameaças detetadas gerarão alarmes.

Conforme Kizza (2005) as principais vantagens dos NIDS são:

- Detecção e resposta em tempo real: estando em pontos estratégicos da rede, consegue detetar intrusões rapidamente e notificar ao administrador;
- Capacidade de detetar ataques que os HIDS não pegam, porque monitora no nível de transporte da arquitetura da rede. Nesse nível analisa pacotes não apenas por endereços, mas também em números de porta;
- Dificuldade de remover evidências: os NIDS ficam em uma máquina dedicada e protegida, o que dificulta bastante a remoção de evidências pelo atacante;
- Baixo custo: segundo Wang (2009), é necessário apenas sondas em alguns pontos estratégicos da rede. A monitoração passiva é outro ponto positivo, pois não há tráfego de rede normal resistente a intrusão.

O sistema de detecção de intrusão em rede se divide em duas partes:

- os sensores espalhados pela rede e que fazem a captura, formatação e análise dos dados e do tráfego; e
- o gerenciador que administra os sensores e permite que trabalhem de forma integrada, com a definição do tipo de resposta para cada ameaça detetada.

Com a capacidade de detetar ameaças em tempo real, o sensor atuando em modo promíscuo em um segmento de rede que tenha um servidor atacado, poderá capturar os pacotes referentes ao ataque. As técnicas de ataque mais comuns são a fragmentação, ataques por meio de portas, tentativas programadas para mapeamento da rede, ataques coordenados, identificação negativa e mudança de padrão de ataques. Caberá ao NIDS emitir os alertas e as atividades de defesa serão tomadas de acordo com os alertas emitidos e as melhores práticas escolhidas pelo profissional de segurança, que receberá os alertas.

## 2.5 Intrusão, definição de perfil e possível detecção

A definição de intrusão pode ser dada como qualquer ação ou conjunto delas, que tenham por intuito comprometer a integridade, a confidencialidade ou a disponibilidade de um recurso, sistema ou rede. Assim, o resultado de um ataque que pode ou não provocar alterações permanentes nas informações ou serviços será uma intrusão. Um ataque é um conjunto básico de iniciativas tomadas pelos atacantes, buscando falhas para invadir a segurança e concretizar a intrusão, conforme Stallings (2008).

Inicialmente, a tentativa de intrusão consiste em fazer um reconhecimento externo, com o intuito de identificar a topologia do sistema e a existência de sistemas de proteção. O atacante analisa o envio e recepção de mensagens com formatos específicos (opção *Record Packet Route* em cabeçalhos IP, diversas mensagens ICMP e verificação de outros protocolos). Na próxima fase, o atacante tenta um reconhecimento interno. Os servidores da rede são testados em busca de vulnerabilidades, como detetar o tipo de sistema operativo, o hardware do computador, os serviços prestados, e nomes de usuários. Este contato com os servidores analisados, causa um tráfego anormal na rede.

Com as informações da rede e dos sistemas, o atacante escolhe o sistema a ser atacado, onde foram encontradas as vulnerabilidades que podem ser exploradas. Como objeto final, o atacante aproveita a intrusão para transformar a máquina numa base de operações para outros ataques, tenta capturar as informações contidas para obter vantagem, a partir deste ponto, o atacante tem o controle do computador.

Como o IDS coleciona dados, se torna fundamental na defesa contra intrusões, de forma dinâmica. As boas práticas recomendam que um sistema seja implantado com mecanismos de segurança, que seja testado, e que se implementem políticas e mecanismos de segurança, Santos (2001). Com o sistema em produção, o IDS começa a fazer análise de comportamento e pode detetar ataques desconhecidos ou políticas de segurança mal implementadas. É necessário reforçar a segurança de infraestrutura de rede, atualizar os softwares, diagnosticar a rede para recuperação e correção de falhas, documentar os ataques conhecidos, os sofridos e as ações de contingência e resposta.

Uma ressalva sobre o IDS, possui uma alta taxa de falsos positivos, o que pode levar os profissionais de segurança a desconsiderar os avisos.

O IDS tem uma utilização personalizada e precisa ser adaptado ao sistema ou rede que esteja monitorando, quanto mais adaptado a rede e personalizado, maior sua possibilidade de sucesso. As taxas de erros são difíceis de controlar e são críticas para o funcionamento útil do IDS; os falsos positivos em demasia, atrapalham a avaliação do profissional de segurança, e os falsos negativos em grande quantidade, tornam inútil a utilização da ferramenta.

A saída padrão do IDS após uma análise do sistema, poderá ser:

- Comportamento normal, tráfego legítimo considerado legítimo, não emite alerta.
- Falso negativo, tráfego suspeito não detetado, não emite alerta.
- Falso positivo, tráfego legítimo identificado como suspeito pelo IDS, emite alerta.
- Positivo, tráfego ilegítimo identificado como suspeito pelo IDS, emite alerta.

Estas saídas geram os alertas que são emitidos pelo IDS. O analista de segurança utiliza estas informações para embasar suas ações.

## **2.6 OSSEC – Open Source Security**

O OSSEC foi desenvolvido por Daniel Cid em 2004, tendo sido adquirido pela empresa *Third Brigade, Inc*, e mais tarde em 2009, a empresa foi adquirida pela *Trend Micro*. O sistema é um *software* livre, sem custos de licenciamento e de fonte aberta, e trabalha com a detecção de intrusão em computador. Ele possui versões para vários sistemas operativos e seu funcionamento pode ser Local ou Agente e Servidor.



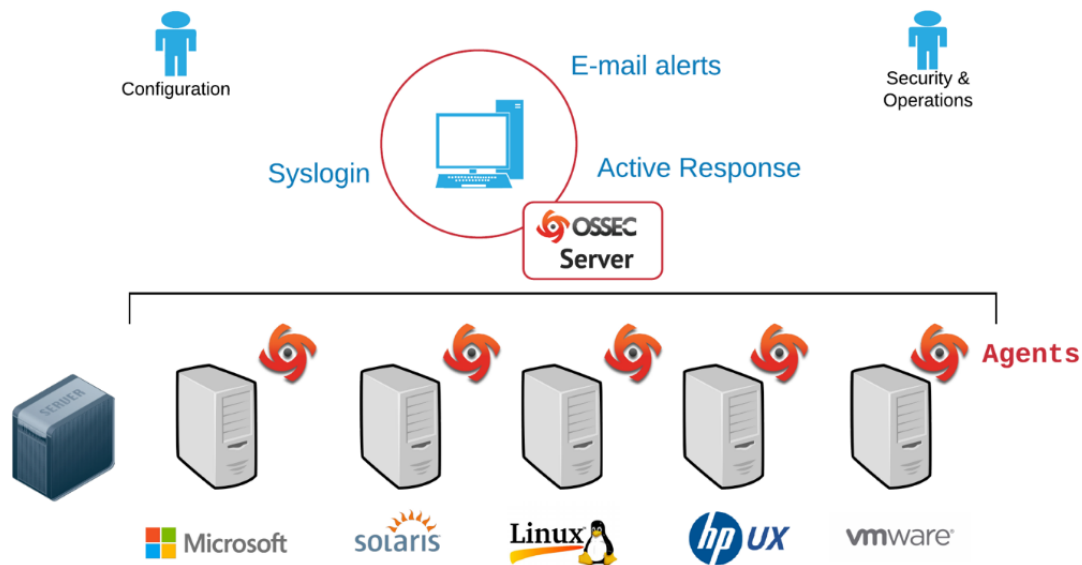


Figura 6: Plataformas que o OSSEC suporta

Sendo o OSSEC um OSSIM (*Open Source Security Information Management*) é uma solução de código fonte aberto para gerenciamento de eventos de segurança, ou seja, é um SIEMI.

No modo Local, não existe troca de mensagem entre o agente e o servidor, uma vez que o OSSEC atuará diretamente no computador onde foi instalado, todas as outras funcionalidades estão presentes. No modo Agente e Servidor, o agente pode ler os arquivos locais como *Syslog*, *Snort*, *Apache*, *QlikView*, entre outros, e enviar as ameaças detetadas para o servidor analisar.

No modo Agente e Servidor, o servidor realiza a análise de *Logs*, onde são geradas as notificações por e-mail, e o servidor recebe os *Logs* de outros computadores e controlaras regras, analisadores ou interpretadores de códigos e opções de configuração.

### 2.6.1 Regras de Classificação do OSSEC

As regras trabalham em níveis, do nível mais baixo (00), ao máximo (15). Alguns níveis não são utilizados, como o nível 01 que por definição da ferramenta não apresenta alertas. Outros níveis podem ser adicionados, entre eles ou após eles.

O profissional de segurança pode criar novas regras de classificação adaptadas a sua infraestrutura e necessidade, respeitando o comportamento da rede. As regras serão lidas pelo profissional de segurança, do nível mais alto para o mais baixo. Os níveis são os seguintes:

00 - *Ignored* - Nenhuma ação tomada. Usado para evitar falsos positivos. Essas regras são verificadas antes de todas as outras. Elas incluem eventos sem relevância de segurança.

01 - *None* - nenhum alerta emitido.

02 - *System low priority notification* - Notificação do sistema ou mensagens de status. Elas não têm relevância de segurança.

03 - *Successful/Authorized events* - Incluem tentativas de login bem-sucedidas, relatam eventos permitidos.

04 - *System low priority error* - Erros relacionados com configurações incorretas ou dispositivos / aplicativos não utilizados. Eles não têm relevância de segurança e geralmente são causados por instalações padrão ou testes de software.

05 - *User generated error* - Incluem senhas erradas, e ações negadas por falta de autorização. Por si só, elas não têm relevância de segurança, mas podem indicar tentativas de intrusão.

06 - *Low relevance attack* - Eles indicam um erro ou um vírus que não afeta o sistema. Eles também incluem frequentemente eventos IDS e frequentemente erros.

07 - *"Bad word" matching* - Eles incluem palavras como "ruim", ou "erro". Esses eventos são na maioria das vezes, não classificados e podem ter alguma relevância de segurança.

08 - *First time seen* - Inclui eventos pela primeira vez vistos. Primeira vez que um evento IDS é disparado ou a primeira vez que um usuário efetuou o login. Quando se começa a usar o OSSEC, essas mensagens são normais.

09 - *Error from invalid source* - Inclui tentativas de login como um usuário desconhecido ou de uma fonte inválida. Pode ter relevância de segurança (especialmente se for repetida). Eles também incluem erros relacionados à conta "administrador".

10 - *Multiple user generated errors* - Eles incluem várias senhas incorretas, ou vários logins com falha. Eles podem indicar um ataque ou pode ser apenas que um usuário simplesmente esqueceu suas credenciais.

11 - *Integrity checking warning* - Eles incluem mensagens sobre a modificação de binários ou a presença de *rootkits* (por *rootcheck*). Se uma alteração normal foi efetuada na configuração do

sistema, receberá uma mensagem "*syscheck*". Pode indicar um ataque que obteve êxito, caso nenhuma alteração tenha sido realizada, mas a mensagem for emitida. Também incluíam eventos IDS que serão ignorados (alto número de repetições).

12 - *High importancy event* - Eles incluem mensagens de erro ou aviso do sistema e *kernel*. Eles podem indicar um ataque contra um aplicativo específico.

13 - Erro incomum (grande importância) - A maioria das vezes corresponde a um padrão de ataque comum.

14 - Evento de segurança de alta importância - A maioria das vezes é feita com correlação e indica um ataque.

15 - Ataque grave - Sem chances de falsos positivos - É necessária uma atenção imediata.

Os alertas podem ser direcionados, para informar quando uma ação específica acontecer, para necessidades específicas, gerando reações de resposta ativa e para correlação. Uma vez que os *Logs* foram analisados e os dados relevantes identificados, as regras dentro do OSSEC devem ser sintonizadas para evitar a inundação dos administradores com alertas irrelevantes. É necessário aprimorar e adaptar o conjunto de regras, criar substituições de regras locais para assinaturas existentes (Cid D. B., 2010).

OSSEC utiliza uma arquitetura cliente / servidor. A comunicação ocorre na porta UDP 1514 e é criptografada usando o algoritmo da chave simétrica *Blowfish*. O intervalo numérico de regras incluídas é de 00000 a 99.999. As regras personalizadas devem variar entre 100.000 e 119.999. Se escolheu outra ID para uma regra personalizada, a regra pode entrar em conflito com as regras padrão (Cid D. B., 2010).

### 2.6.2 Exemplos de Alerta do OSSEC

Seguem abaixo, alguns exemplos de alertas enviados para o endereço eletrônico cadastrado, uma mensagem de alerta segue a estrutura abaixo comentada:

Número do alerta, tipo de alerta, data, endereço do servidor, regra que gerou o alerta, resposta do servidor, endereço do solicitante, solicitação que gerou o alerta.

Seguem abaixo alguns exemplos.

#### Alerta 1

```
** Alert 1500646993.12188990: mail - web, accesslog,  
  
2017 Jul 21 11:23:13 (portalbr1) 10.100.0.241-  
>/var/log/apache2/access_www_brasil.log  
  
Rule: 31123 (level 4) -> 'Web server 503 error code (Service unavailable).'  
Src IP: 66.249.75.158  
  
66.249.75.158 10.100.0.250 - [21/Jul/2017:11:20:51 -0300] "GET /economia-e-  
emprego/2016/06/analistas-projetam-dolar-menor-ao-fim-de-2016/ HTTP/1.1" 503 -  
"- "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) "
```

O alerta 1, é um alerta nível 4, informando que o serviço está indisponível (Service unavailable). Este alerta indica que a página solicitada não está disponível. A solicitação foi o acesso a uma página em 21/Jul/2017:11:20:51 -0300, a solicitação foi realizada por 66.249.75.158.

#### Alerta 2

```
** Alert 1500646995.12189461: mail - web,accesslog,  
  
2017 Jul 21 11:23:15 (portalbr2) 10.100.0.242-  
>/var/log/apache2/access_www_brasil.log  
  
Rule: 31123 (level 4) -> 'Web server 503 error code (Service unavailable).'  
Src IP: 157.55.39.74  
  
157.55.39.74 10.100.0.250 - [21/Jul/2017:11:20:52 -0300] "GET /economia-e-  
emprego/2016/01/guias-do-simples-domestico-de-1-1-milhao-de-trabalhadores-ja-  
foram-emitidas HTTP/1.1" 503 - "- "Mozilla/5.0 (compatible; bingbot/2.0;  
+http://www.bing.com/bingbot.htm) "
```

O alerta 2, é um alerta nível 4, informando que o serviço está indisponível (Service unavailable). Este alerta indica que a página solicitada não está disponível. A solicitação foi o acesso a uma página em 21/Jul/2017:11:20:52 -0300, a solicitação foi realizada por 157.55.39.74.

#### Alerta 3

```
** Alert 1500646996.12189958: mail - web,accesslog,  
  
2017 Jul 21 11:23:16 (planalto) 10.100.0.230-  
>/var/log/apache2/access_www2_planalto.230.log  
  
Rule: 31101 (level 5) -> 'Web server 400 error code.'  
  
Src IP: 213.180.203.32  
  
213.180.203.32 10.100.0.250 - [21/Jul/2017:11:22:32 -0300] "GET  
/Ccivil_03/decreto/1950-1969/D57618.htm HTTP/1.1" 404 7319 "-" "Mozilla/5.0  
(compatible; YandexBot/3.0; +http://yandex.com/bots)"
```

O Alerta 3 do exemplo acima, é um alerta nível 5, informando um erro de solicitação de banco de dados (*Web server 400 error code*). Este alerta pode indicar uma tentativa de acesso não permitido. A solicitação foi o acesso a uma página de um portal em 21/Jul/2017:11:22:32 -0300, a solicitação foi realizada por 213.180.203.32.

### 2.6.3 Recursos e funcionalidades do OSSEC

Entre as funcionalidades está o serviço centralizado de *Logs* para análise, sistema de alerta, mecanismo de resposta que pode ser acionado, sistema de monitoramento de arquivos, motor *rootkit*.

Zin, Nicolas(2009) especifica algumas funcionalidades que o OSSEC, traz:

- serviço de centralização de log (um pouco como "rsyslog"), mas não armazena logs, analisa;
- um analisador e um sistema de alerta (um pouco como "logstash");
- um mecanismo de "resposta ativa" (como "fail2ban");
- um sistema de monitoramento (como "tripwire");
- um pequeno mecanismo de rootkit (como "rkhunter");

- em um produto leve: não está escrito em ruby / python ou java, mas em um bem antigo C;
- regras já escritas.

Na figura abaixo temos a demonstração de uma tela do modo de administração com interface web, nesta tela é possível fazer a busca de alerta por datas.

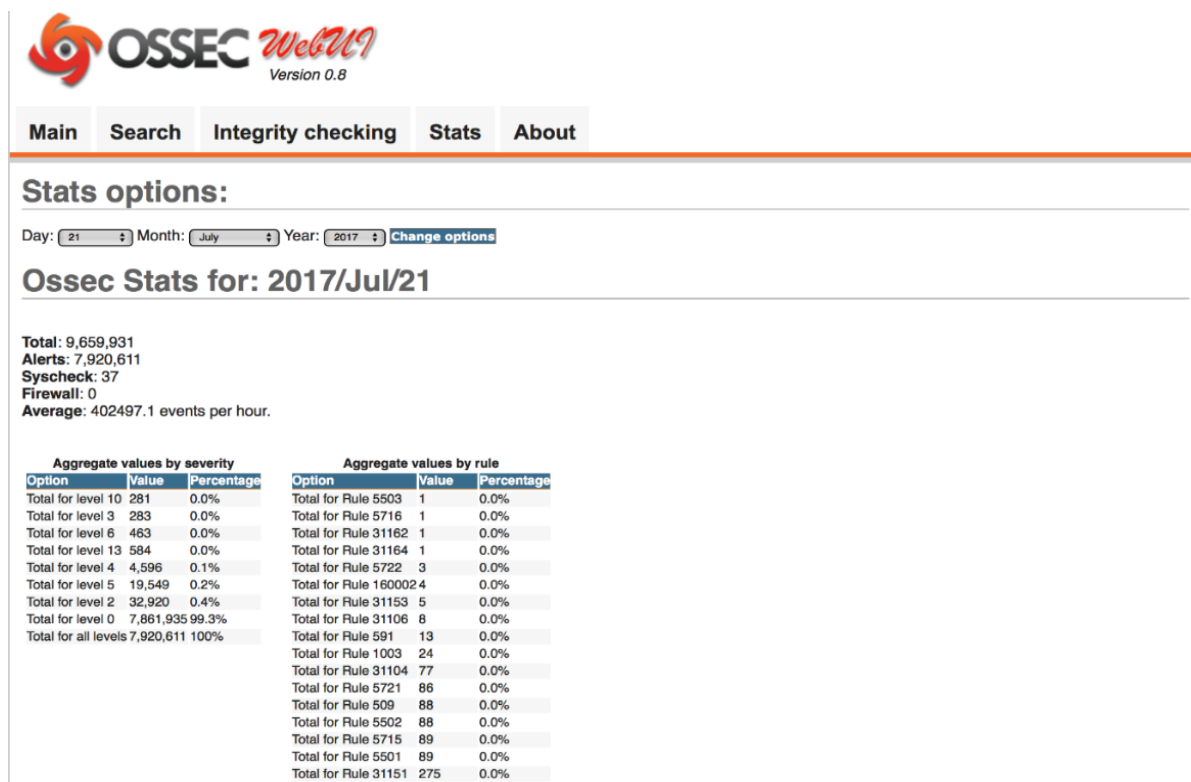


Figura 7: Demonstração do console do OSSEC

Na interface web do OSSEC é possível fazer buscas por data, verificar a quantidade de alertas por regra, por nível, fazer buscas, verificar a integridade do computador e o status do computador, em suma permite a verificação dos *Logs* e os incidentes reportados.

A base de registros coletados fica em um arquivo próprio de *Logs*, no qual é possível a integração com banco de dados *MySQL*, *PostgreSQL*, *Oracle*, *QlikVIEW* e *MSSQL*. O OSSEC com sua interface web, facilita a administração, consultas e visualização de eventos em tempo real. Oferece relatórios e permite consulta por datas.

Os tipos de alerta que a ferramenta emite ao comparar as assinaturas de possíveis atividades suspeitas, dependem da lista de assinaturas que vem com a ferramenta e que são constantemente atualizadas.

Os dados coletados servem para uma análise da rede da instituição pelos profissionais de Segurança, as portas mais acessadas e as assinaturas consideradas na emissão dos alertas, geram mensagens de correio eletrônico que informam a atividades ocorridas no servidor.

A quantidade de alertas é proporcional ao servidor monitorado e a infraestrutura da rede. A análise e as ações de contingência ficam na dependência do profissional que analisa os alertas. A utilização do arquivo de *Logs* em conjunto com outras ferramentas pode produzir relatórios sobre as atividades que ocorreram no computador, identificar os serviços mais solicitados, as solicitações de acesso mais constantes, endereços de solicitação, identificação de padrões de ataque que podem gerar a criação de novas regras.

### 3. Especificação da infraestrutura do caso de estudo

Com foi referido, o nome da instituição estudada será preservado por questão de segurança. Os testes propostos neste estudo que integram o HIDS OSSEC, a uma estrutura de rede já implantada e em funcionamento, serão descritos no próximo capítulo.

#### 3.1. Infraestrutura atual

O ambiente onde o estudo foi feito está abaixo discriminado, buscando possibilitar que se dimensione a proporção de ataques e ameaças a que uma infraestrutura deste porte está exposta.

- 150 Sistemas Hospedados (incluindo em homologação e desenvolvimento).
- 90 Sites e Portais (Incluindo sites em homologação e desenvolvimento).
- 320 servidores virtuais, hospedados em 94 servidores físicos (Dell, HP e IBM).
- 2 Servidores Oracle *Database Appliance*.
- 2 *Gateways* de correio eletrônico.
- 2 *Firewalls* de Aplicação/WAF.
- 2 *Firewalls* de Rede.
- 2 Sistemas de prevenção de Intrusão (IPS).
- 2 *Proxy - Web Gateways*, em obsolescência.
- 1 Sistema de alimentação de emergência com 96KVA (6 módulos de 16KVA) e 144 baterias.
- 4.000 caixas postais.
- 4.000 usuários em rede.
- 15.000 pontos de rede.
- 400 bancos de dados (*Oracle, Postgres e MySQL* – Produção, Homologação e Desenvolvimento).
- 5 sistemas de armazenamento num total de 500 TB.
- 3 sistemas para *backup*.



- Sistema de endereçamento autônomo (ANS) de internet com 801 Mbps.
- 500 pontos de IPTV.
- 16 Equipamentos de videoconferência.
- 5000 Computadores.
- 850 Impressoras do serviço de impressão.

Abaixo, segue um desenho da infraestrutura de redes e dados da instituição, a quantidade de equipamentos, a sequência de segurança utilizada pela instituição tem um esquema simples, que recebe o tráfego com equipamentos que fazem o balanceamento da carga, passando para um IPS, seguido do Firewall. O tráfego que vai para a DMZ passa pelo WAF e o tráfego interno circula dentro da rede local segura.

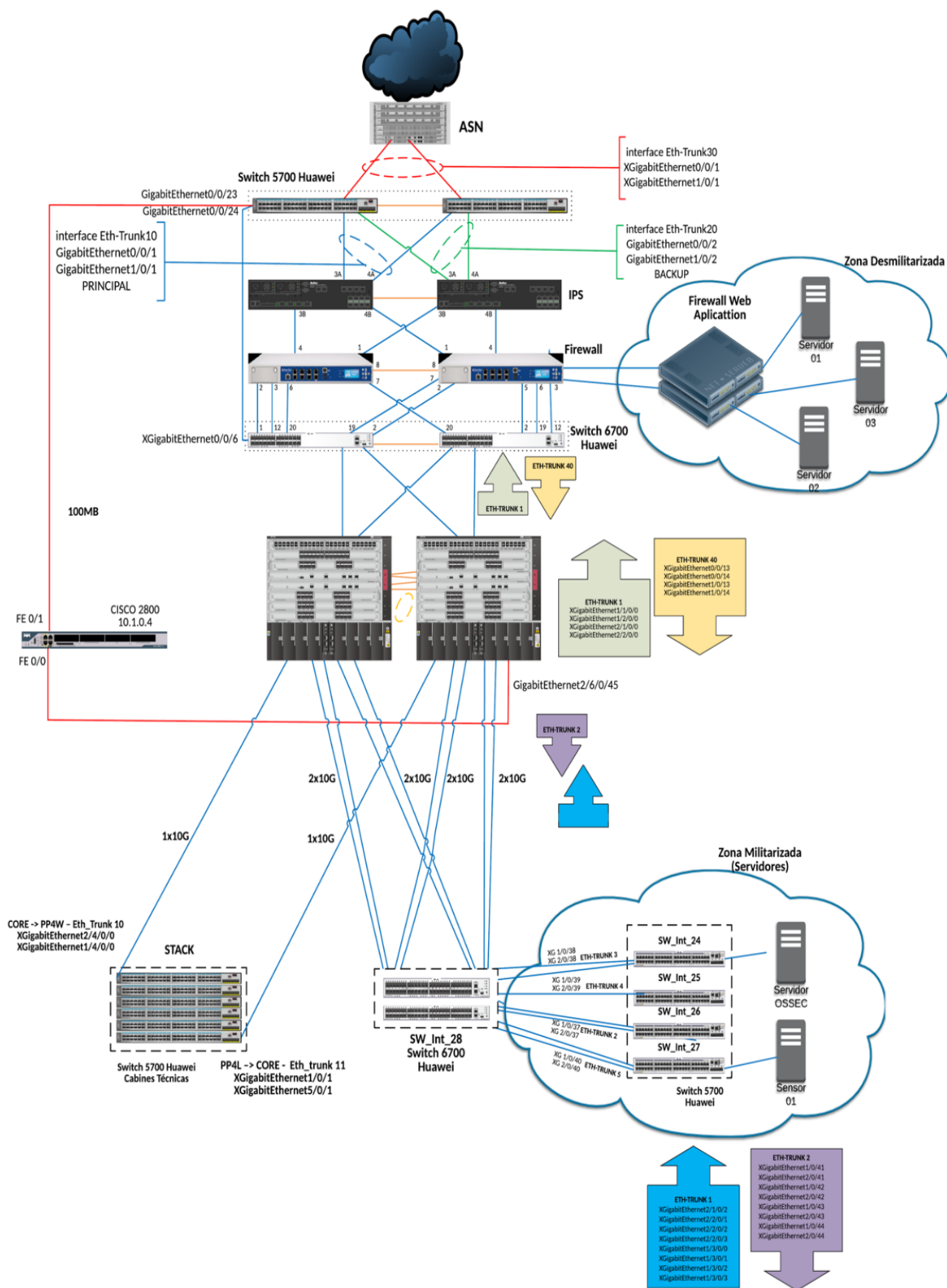


Figura 8: Demonstração da Infraestrutura de Rede

Nesta infraestrutura, inicialmente existe a conexão com o mundo exterior – Internet, feita com o tráfego dividido, entrando por um dos dois equipamentos que trabalham como Mecanismo de prevenção de intrusão.

Como segunda barreira, existem dois equipamentos que trabalham na função de Firewall com balanceamento de carga que envia o tráfego para os *switchs*. Na rede interna, temos a sub-rede onde ficam os usuários internos em uma zona segura; em um ambiente isolado temos uma sub-rede, a zona desmilitarizada, onde estão hospedados os dois Portais / Sítios que utilizaremos para nossos testes.

A especificação técnica dos equipamentos de segurança não é considerada relevante, como se percebe na figura acima, a primeira barreira é feita por um IPS – *McAfee® Network Security Platform M-3050* e *M-4050*, seguida por um *Firewall Check Point 4200 Appliance* e complementada com um *WAF Web Application Firewall: “F5 BIG-IP® Application Security Manager* para controle do tráfego direcionado para a DMZ.

### **3.2. Problemas na segurança atual**

A equipe de segurança detetou a necessidade de aumentar a segurança, uma vez que os relatórios demonstravam o aumento dos ataques e tentativas de intrusão. Conforme Robertson (2011), existem muitos sinais possíveis de incidentes que podem passar despercebidos a cada dia. Os eventos devem ser estudados principalmente pela análise do comportamento da rede ou pela revisão dos Logs de eventos de segurança do computador. Para evitar ou minimizar as perdas decorrentes de um resultado do incidente, os eventos precisam ser analisados o mais próximo possível do tempo real.

Com a necessidade de aumentar a segurança, surgiu a necessidade de um estudo aprofundado e a instalação de ferramenta que auxiliasse nisto. Os sistemas de registro e detecção de intrusão têm potencial para produzir uma quantidade muito grande de dados e todos esses dados devem ser gerenciados, filtrados e analisados. Ter uma abordagem única e uma plataforma unificada ajuda com esta tarefa muito difícil que é monitorar e relatar em tempo quase real.

No exemplo abaixo, nota-se um relatório dos ataques sofridos, a quantidade e variedade. A contagem de ataques por aplicativos em um período de 12 horas é significativa.

Default - Top 10 Application Categories by Attack Count				
#	Category Name	Bandwidth Usage (Bytes)	Connection Count	Attack Count
1.	Tunnels	331.31G	25754752	752876
2.	Infrastructure Services	146.63G	15046030	211442
3.	Social Networking	19.54G	559487	6918
4.	Web Browsing	1.65G	106304	1589
5.	Streaming Media	38.37G	374480	790
6.	Storage	316.72M	87141	762
7.	Voice over IP (VoIP)	22.83M	5580	167
8.	Web Mail	448.84M	48464	154
9.	File Sharing	477.28M	20410	146
10.	Photo/Video Sharing	1.31G	529997	126

Figura 9: Categorias de aplicativos por contagem de ataque

A instalação do HIDS OSSEC surgiu como alternativa, para auxiliar no controle e fornecer dados que servirão para análises e melhorias na estrutura. OSSEC é um Sistema de Detecção de Intrusão em computador Open Source. Ele realiza análises de log, verificação de integridade de arquivos, monitoramento de políticas, detecção de rootkit, alerta em tempo real e resposta ativa, Trend Micro (2010).

### 3.3. Inclusão do OSSEC

Seguindo esta infraestrutura que não possui nenhum tipo de monitoramento para servidor, será adicionado mais um elemento de segurança, para atender a necessidade de monitorar somente um computador, como um servidor de internet ou um banco de dados, pode-se a instalar o HIDS. A opção foi instalar o OSSEC em dois servidores como agentes OSSEC e um servidor OSSEC que fará o controle dos agentes. Neste caso, os agentes verificam a integridade de seus arquivos localmente e enviam os resultados ao computador servidor.

Com está infraestrutura de grande porte, o constante monitoramento da rede é necessário. Os servidores que prestam serviços a internet ficam na DMZ, temos ainda uma rede local segura. Note que na estrutura abaixo, temos como primeira defesa o IPS e como segunda barreira o Firewall, o WAF na DMZ. Nesta figura já aparece o OSSEC na MZ e nos servidores da DMZ.

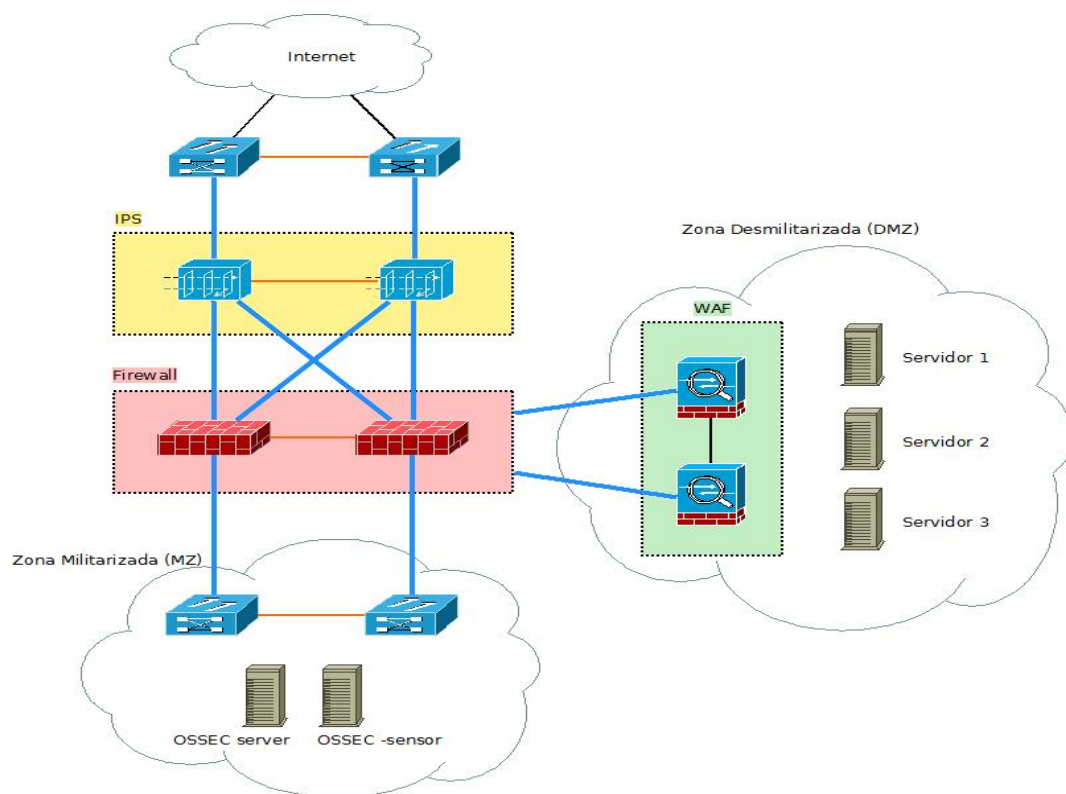


Figura 10: Infraestrutura com o OSSEC

A figura mostra a infraestrutura utilizada para o estudo. O detalhamento da implementação da estrutura, veremos no próximo capítulo.

## 4. Implementação e Testes

O objetivo desta implementação é gerar uma modelagem baseada em hierarquização de aplicações que monitorem a rede ou o computador, em seus vários estados. A necessidade de garantir um grau de segurança e maturidade em caso de incidentes é premente. Objetivasse um resultado confiável e que possa ser reproduzido em um ambiente semelhante, em maior ou menor grau, respeitadas as devidas proporções das organizações.

A proposta do modelo é criar uma arquitetura viável que permite a junção dos mecanismos de controle, de forma adaptativa, buscando ampliar a segurança da instituição. Neste contexto, a junção de um IPS, um Firewall com um HIDS pode ser válida. O IPS funciona como primeira barreira, o Firewall funciona como segunda linha de defesa, realizando o controle de acesso no nível de rede é um fator importante para a segurança e a autenticação dos serviços, buscando controlar o acesso aos recursos, assim o IPS é essencial para o monitoramento do ambiente, tanto de rede quanto de computadores.

Para instalação, o modelo com agentes e um servidor para controle, foi considerado o mais indicado. A escolha foi instalar o servidor na rede interna e os clientes foram instalados na DMZ em três servidores web que suportam dois portais de grande conectividade.

### 4.1. Instalando o OSSEC

O OSSEC foi instalado na estrutura com cliente-servidor, onde os agentes sensores (sensor) foram instalados em três servidores que respondem a requisições Web, no caso três servidores *Apache* e um servidor como controlador. O monitoramento foi feito em dois sítios de grande acesso na instituição parceira; um dos sítios esta hospedado em dois computadores, por isto foram três agentes instalados para dois sítios. Abaixo, segue a instalação padrão do OSSEC e em complemento a integração ao *Portsentry* e *Nmap*.

A versão do utilizada no Servidor é a seguinte: Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86\_64 GNU/Linux

A versão utilizada no Agente é a seguinte: Linux 3.16.0-4-amd64 #1 SMP Debian 3.16.36-1+deb8u2 (2016-10-19) x86\_64

Detalha-se a seguir a instalação do OSSEC.

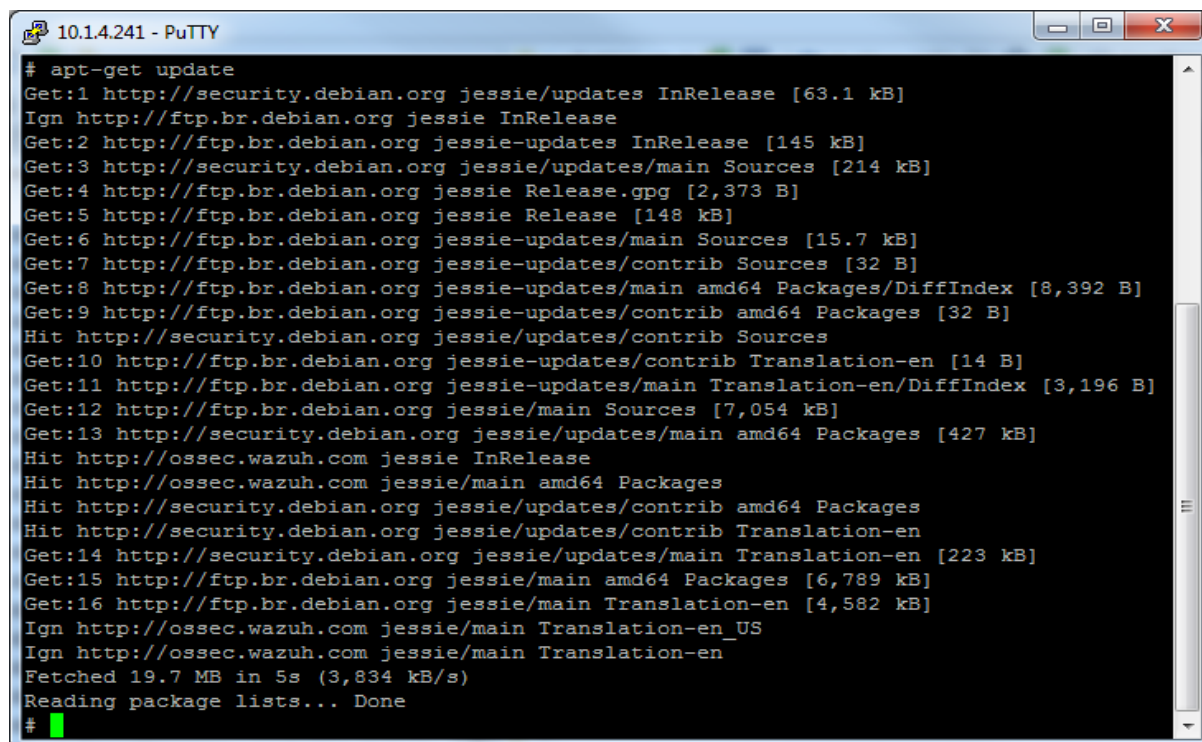
#### 4.1.1 Instalar o OSSEC no servidor

Para instalar o OSSEC em um sistema operacional *Debian*, por intermédio do *apt-get*, é necessário acrescentar o repositório *Wazuh* à lista de repositórios “*sources.list*”. Para o *Debian*, o “*Wazuh*” está disponível em algumas distribuições (*Sid*, *Jessie* and *Wheezy*). Nesta instalação no ambiente de teste foi utilizada a distribuição “*jessie*”.

Para fazer isto foram realizados os seguintes comandos:

```
# apt-key adv --fetch-keys http://ossec.wazuh.com/repos/apt/conf/ossec-key.gpg.key  
  
# echo 'deb http://ossec.wazuh.com/repos/apt/debian wheezy main' >>  
/etc/apt/sources.list  
  
# apt-get update
```

Aparecerá a tela:



```
# apt-get update  
Get:1 http://security.debian.org jessie/updates InRelease [63.1 kB]  
Ign http://ftp.br.debian.org jessie InRelease  
Get:2 http://ftp.br.debian.org jessie-updates InRelease [145 kB]  
Get:3 http://security.debian.org jessie/updates/main Sources [214 kB]  
Get:4 http://ftp.br.debian.org jessie Release.gpg [2,373 B]  
Get:5 http://ftp.br.debian.org jessie Release [148 kB]  
Get:6 http://ftp.br.debian.org jessie-updates/main Sources [15.7 kB]  
Get:7 http://ftp.br.debian.org jessie-updates/contrib Sources [32 B]  
Get:8 http://ftp.br.debian.org jessie-updates/main amd64 Packages/DiffIndex [8,392 B]  
Get:9 http://ftp.br.debian.org jessie-updates/contrib amd64 Packages [32 B]  
Hit http://security.debian.org jessie/updates/contrib Sources  
Get:10 http://ftp.br.debian.org jessie-updates/contrib Translation-en [14 B]  
Get:11 http://ftp.br.debian.org jessie-updates/main Translation-en/DiffIndex [3,196 B]  
Get:12 http://ftp.br.debian.org jessie/main Sources [7,054 kB]  
Get:13 http://security.debian.org jessie/updates/main amd64 Packages [427 kB]  
Hit http://ossec.wazuh.com jessie InRelease  
Hit http://ossec.wazuh.com jessie/main amd64 Packages  
Hit http://security.debian.org jessie/updates/contrib amd64 Packages  
Hit http://security.debian.org jessie/updates/contrib Translation-en  
Get:14 http://security.debian.org jessie/updates/main Translation-en [223 kB]  
Get:15 http://ftp.br.debian.org jessie/main amd64 Packages [6,789 kB]  
Get:16 http://ftp.br.debian.org jessie/main Translation-en [4,582 kB]  
Ign http://ossec.wazuh.com jessie/main Translation-en_US  
Ign http://ossec.wazuh.com jessie/main Translation-en  
Fetched 19.7 MB in 5s (3,834 kB/s)  
Reading package lists... Done  
#
```

Figura 11: Tela de instalação do OSSEC

Depois, basta instalar o pacote OSSEC HIDS no servidor pelo comando:

```
# apt-get install ossec-hids
```

O OSSEC, por padrão, será instalado na pasta */var/ossec/* e suas configurações estarão no arquivo */var/ossec/ossec.conf*.

Durante a instalação, podem ser inseridos e-mails para onde deseja-se que sejam encaminhadas as notificações. Caso não seja configurado inicialmente, pode ser alterado diretamente no arquivo */var/ossec/ossec.conf*:

```
<global>

  <email_notification>yes</email_notification>

  <email_to>sammy@example.com</email_to>

  <smtp_server>mail.example.com.</smtp_server>

  <email_from>name@example.com</email_from>

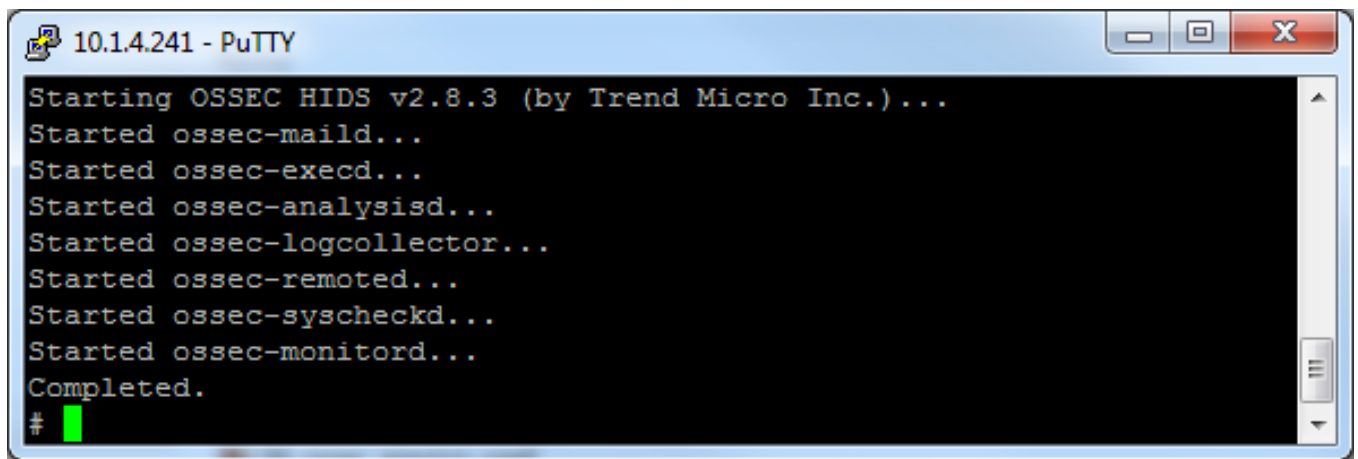
</global>
```

Nesse ponto, já é possível iniciar o OSSEC pelo comando:

```
/var/ossec/bin/ossec-control start
```

O que resultará na tela abaixo:





```
10.1.4.241 - PuTTY
Starting OSSEC HIDS v2.8.3 (by Trend Micro Inc.)...
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
#
```

Figura 12: Tela de inicialização do OSSEC

O OSSEC poderá ser parado pelo comando:

```
/var/ossec/bin/ossec-control stop
```

O OSSEC poderá ser reiniciado pelo comando:

```
/var/ossec/bin/ossec-control restart
```

As configurações mais detalhadas podem ser feitas diretamente no arquivo `/var/ossec/ossec.conf`.

#### 4.1.2. Instalar o OSSEC no Agente

Após a instalação do OSSEC no servidor, procedeu-se a instalação dos agentes. Para isso foram realizados os seguintes comandos:

```
# apt-key adv --fetch-keys http://ossec.wazuh.com/repos/apt/conf/ossec-
key.gpg.key
# echo 'deb http://ossec.wazuh.com/repos/apt/debian wheezy main' >>
/etc/apt/sources.list
# apt-get update
# apt-get install ossec-hids-agent
```

Após o término da instalação, foi necessário iniciar o agente:

```
/var/ossec/bin/ossec-control start
```

A partir de agora, será necessário inserir cada um dos agentes no servidor. Para isso, será necessário executar no servidor:

```
/var/ossec/bin/manage_agents
```

Aparecerá:

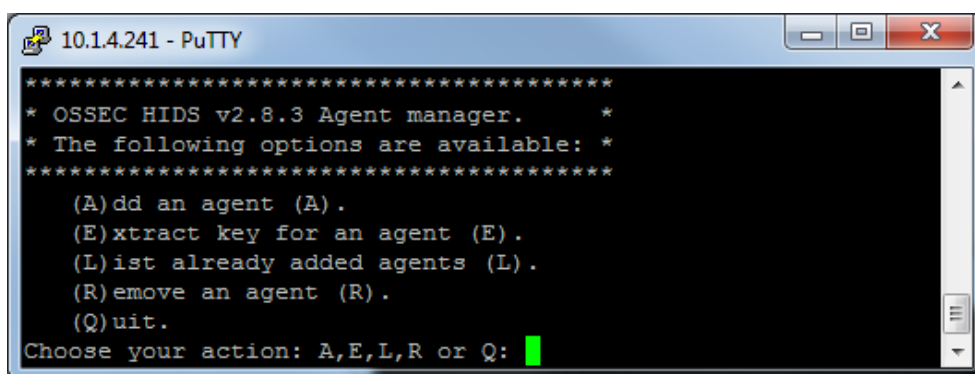


Figura 13: Tela inserir Agente no OSSEC

Então basta executar a opção “A”.

```
Agent information:
ID:001
Name:teste
IP Address:xxx.xxx.xxx.xxx

Confirm adding it?(y/n): y [ Digite 'y' ]

Agent added.
```

Após isso, é necessário gerar uma chave para o agente específico, executando a opção “E”, que gerará a seguinte saída:

```
Available agents:
```

```
ID: 001, Name: teste, IP: xxx.xxx.xxx.xxx

Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent      key      information      for      '001'      is:
MDAxIHRlc3RlIDE3Mi4xNi4wLjYgZmRkMDRiM2EyNTBlYW0
ZWQ5ODU1NWZmNGY0NmM3YTVjMDI2MzA5NTg1Y2M5NjgyO
DczNjIxMTdiMzhlZWFlYWw==
```

Com a chave gerada, é necessário retornar ao agente e inseri-la usando *manage\_agents*.

```
/var/ossec/bin/manage_agents
```

Que gerará a tela:

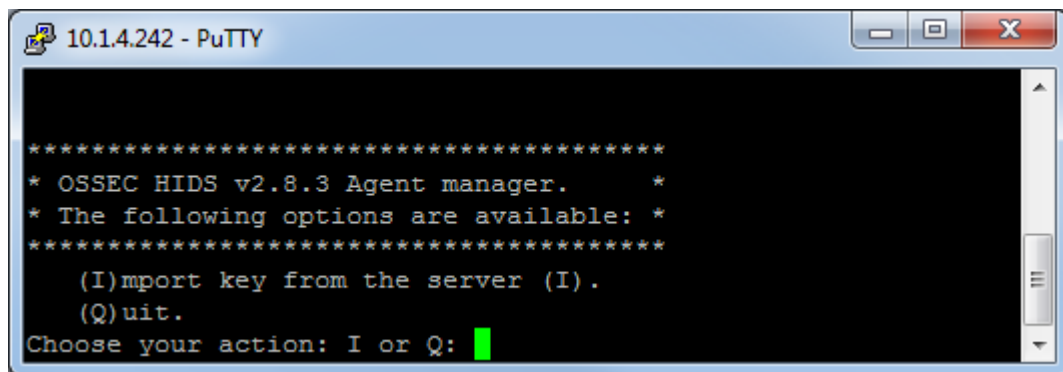


Figura 14: Tela inserir chave no Agente OSSEC

Nesse ponto, basta selecionar a opção “I” e colar a chave gerada no passo anterior.

Após isso, basta reiniciar o serviço no agente e no servidor com o comando:

```
/var/ossec/bin/ossec-control restart
```

#### 4.1.3. Configuração dos agentes:

Na instalação dos agentes, alguns passos devem ser seguidos.

- O agente instalado deverá gerar uma chave de forma, que permite a identificação pelo servidor.

- O servidor gera as chaves, que devem ser configuradas no agente, para que o servidor identifique o agente.
- A chave serve também para a cifragem da informação que vai ser compartilhada entre os agentes e o servidor, garantindo a segurança no processamento das mensagens.
- Utilizou-se a ferramenta “*manage\_agents*”, que gera as chaves, além de controlar a identificação dos agentes, monitorar se estão ativos e permitir a inclusão ou retirada.

#### 4.1.4 Configurar a Interface Web

O OSSEC possui uma interface gráfica, que deve ser configurada no mesmo computador em que foi instalado o servidor.

Para isso, é necessário baixar no servidor:

```
http://www.ossec.net/files/ui/ossec-wui-0.8.tar.gz
```

Após isso, foi descompactado no diretório `/var/www/html`

```
tar -xvf ossec-wui-0.8.tar.gz -C /var/www/html
```

O diretório `/var/www/html/ossec-wui-0.8` e para `/var/www/html/ossec`

```
cd /var/www/html
mv ossec-wui-0.8 ossec
```

Acesse o diretório `/var/www/html/ossec` e execute o arquivo `/gsetup.sh`. Será necessário informar o nome do *admin*, a *senha*.

```
# ./setup.sh

Setting up ossec ui...

Username: admin [ Informe o nome do usuário ]
New password: [ Digite uma senha ]
```

```
Re-type new password: [ Repita a senha digitada anteriormente ]  
Adding password for user admin  
  
Setup completed successfully.
```

Para adicionar o usuário do Apache ( *www-data* ) ao grupo OSSEC

```
adduser p www-data ossec
```

Dentro do diretório */var/www/html/ossec/*, altere as permissões e o grupo do diretório */tmp*

```
chmod 770 tmp/  
  
chgrp www-data tmp/
```

É necessário editar o ficheiro */etc/php5/apache2/php.ini* e alterar as seguintes linhas para os valores abaixo:

```
max_execution_time = 180  
  
max_input_time = 180  
  
memory_limit = 30M
```

Após isso, é necessário reiniciar o Apache

```
apache2ctl restart
```

Após seguir a sequência de instalação acima, o ambiente já estará pronto, pode-se acessar a interface Web pelo navegador de internet, verificar se os agentes que estão funcionando, os alertas já estão sendo emitidos para o endereço de correio eletrónico cadastrado e as informações de Log já estarão sendo registradas. Para aprimorar as funcionalidades do OSSEC faremos a integração com o *Portsentry*, para garantir a detecção de tentativas scanner de portas, e integraremos também o *Nmap* para verificação de redes e auditorias de segurança.

#### 4.1.5 *Portsentry* e configuração do *OSSEC*

Após a configuração do servidor e dos agentes foi realizada a instalação do *Portsentry* para evitar o mapeamento de portas e a adição dos alertas abaixo listados:

Identificação	Grupo ou Alerta	Descrição
160000	Grupo	Grouping for the PortSentry rules
160002	Alerta	Connection from a host.
160003	Alerta	Repeated connections from the same host.
160004	Alerta	Host is still scanning

Tabela 1: Instalação do *Portsentry*

Mais instruções sobre a integração do *Portsentry* com o *OSSEC* podem ser encontradas no Anexo A.

#### 4.1.6 Configuração para leitura de portas com o *Nmap*

A integração do *Nmap*, com o *OSSEC* possibilita que sejam gerados alertas nível 8 sobre o scanner de portas. O *Nmap* é utilizado como ferramenta de correlação e também para alertar com base nas informações do computador, caso as informações sejam alteradas. A integração poder ser realizada conforme as instruções do Anexo B.

A figura seguinte mostra o *OSSEC* funcionando com as integrações *Portsentry* e *Nmap*:

The screenshot displays the OSSEC WebUI interface. At the top, the logo 'OSSEC WebUI Version 0.8' is visible. Below the logo is a navigation bar with tabs: 'Main', 'Search', 'Integrity checking', 'Stats', and 'About'. The 'Search' tab is active. The main content area shows the date 'July 21st 2017 08:08:03 PM' and the section 'Alert search options:'. This section includes search criteria: 'From: 2017-07-21 16:08' and 'To: 2017-07-21 20:08', with a 'Real time monitoring' option. There are also fields for 'Minimum level: 7', 'Category: All categories', 'Pattern:', 'Log formats: All log formats', 'Srcip:', 'User:', 'Location:', 'Rule id:', and 'Max Alerts: 1000'. A 'Search' button is present. Below the search options, the 'Results:' section shows 'Total alerts found: 278'. It includes expandable sections for '+Severity breakdown', '+Rules breakdown', and '+Src IP breakdown'. The first event is at '2017 Jul 21 16:08:08' and the last event is at '2017 Jul 21 20:05:02'. The 'Alert list' section shows a single alert with the following details:
 

- Level: 13 - Possible buffer overflow attempt.
- Rule Id: 40104
- Location: (planalto) 10.100.0.230->/var/log/apache2/error\_www2\_planalto.log
- Message: [Fri Jul 21 20:04:20.490749 2017] [proxy:debug] [pid 19205:tid 139768209786624] proxy\_util.c(2385): [client 10.100.0.250:18420] AH00947: connected /portal\_planalto\_ssl/spinner.gif to 10.100.0.66:80, referer: https://www2.planalto.gov.br/acompanhe-planalto/noticias/

Figura 15: Server OSSEC modo Web

Na figura acima é possível notar a busca por nível de alerta, as buscas são mais precisas, facilitando assim, o trabalho do analista de segurança. A integração do *Nmap* ao OSSEC permite que tentativas de scanner gerem alertas no OSSEC.

## 4.2 Detecção do IPS

Após alguns dias de monitoração, constatou-se que o IPS que controla o tráfego da instituição em estudo, tem uma taxa média de acessos aos Sítios / Portais monitorados de 200.000 acessos diários. Na tabela abaixo, temos o exemplo de quantidade de alertas gerados em cada portal em um período de cinco dias, temos a definição de acesso por dia e o total dos dias somados.

Alertas IPS				
Dia	Portal 1	Portal 2	Outros	Total
1	44 086	13 005	85 483	142 574
2	37 136	12 333	78 249	127 718
3	31 518	12 281	87 026	130 825
4	23 881	8 026	37 240	69 147
5	18 208	7 547	69 466	95 221
Total	154 829	53 192	357 464	565 485

Tabela 2: Alertas dos portais monitorados pelo IPS

A Tabela 2, apresenta a quantidade de Alertas emitidos por dia, com um intervalo de cinco dias, iniciando a contagem a 00:00 horas do dia 1.

O Portal 1 é o mais solicitado, possui notícias e seu conteúdo é constantemente atualizado.

O Portal 2 é o segundo mais solicitado, o seu conteúdo é documental, e são grandes arquivos descarregados e solicitados. Sua atualização é diária.

Os Outros, são cerca de 50 portais que estão disponíveis para acesso e suas atualizações são variadas.

Considerando uma média de 200.000 acessos por dia, a quantidade de alertas é grande, isto se explica pela linguagem utilizada para a criação dos Sítios / Portais o *Zope* e *Plone*.

Um dado relevante é que os portais são em *Zope* e *Plone* e o ambiente possui algumas vulnerabilidades específicas que estão sempre a apresentar problemas de acesso ou hiperligações quebradas, que podem parar o serviço por um ataque de *Ddos*.

Note pelo gráfico abaixo, que a maioria dos alertas é informação.



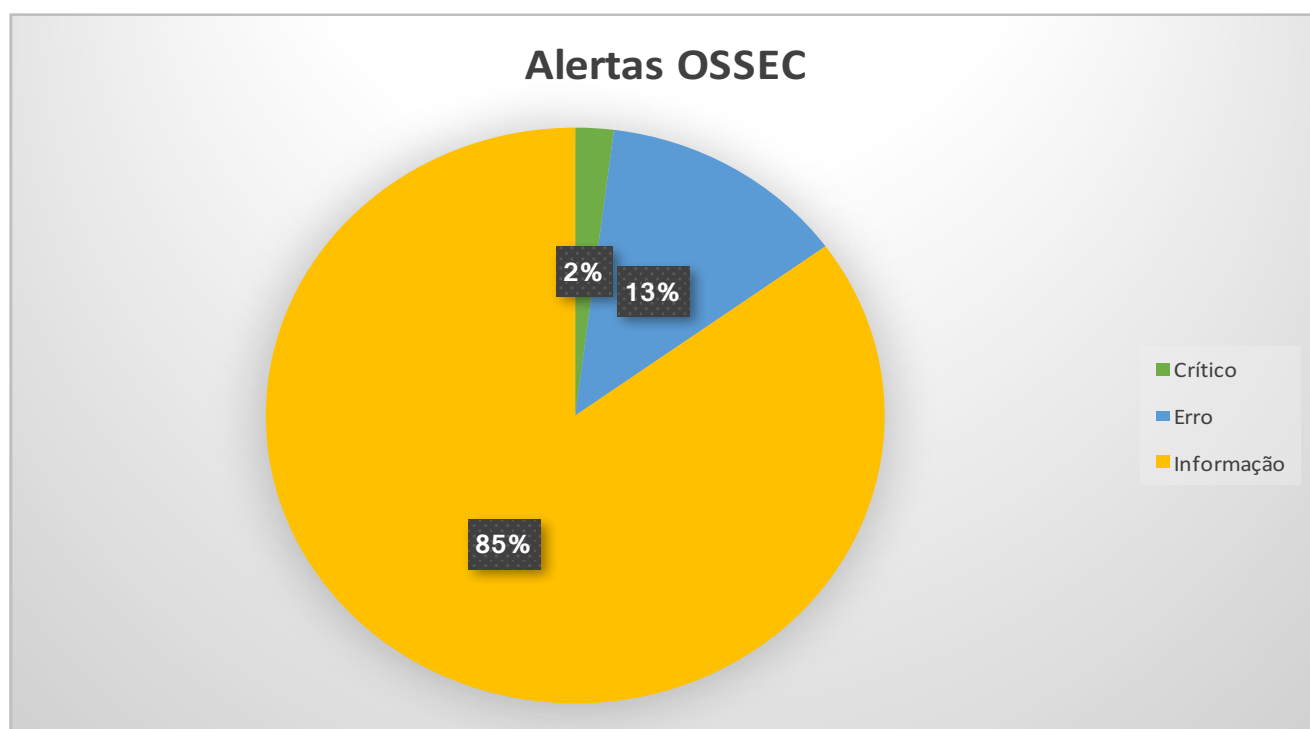


Figura 16: Alertas

Como exemplo, um gráfico de Ataque detetado com alto risco, no Portal 1 dia 2, em que tivemos 37163 alertas, verificamos 204 ataques e deste total 8 eram de alto risco.

Threat Explorer

Top: 25 Attacks Any Direction

Filter: Target IP Address [redacted] X Add Filter View Attacks

Target IP Address - 170.246.252.243

	Attack Name	Attack Category	Attack Subcategory	Attack Severity	Attack Count
1	<a href="#">HTTP: KeepAlive Request Detected</a>	Policy Violation	audit	Medium	170
2	<a href="#">HTTP: Detect PHP-CGI Remote c...</a>	Exploit	code-execution	Medium	6
3	<a href="#">IPv4: TCP Session Hijacking Atte...</a>	Exploit	write-exposure	Medium	5
4	<a href="#">HTTP: Thttpd Stack Overflow</a>	Exploit	buffer-overflow	Medium	4
5	<a href="#">HTTP: PHP Wordpress Plugin Rev...</a>	Exploit	code-execution	High	4
6	<a href="#">HTTP: Apache Struts 2 Remote C...</a>	Exploit	code-execution	High	4
7	<a href="#">UDP: Port Scan</a>	Reconnaissance	port-scan	Medium	3
8	<a href="#">DNS: Linux Kernel Netfilter IP Fr...</a>	Exploit	dos	Medium	2
9	<a href="#">P2P: BitTorrent Meta-Info Retrie...</a>	Policy Violation	restricted-application	Medium	2
10	<a href="#">TCP: SYN Port Scan</a>	Reconnaissance	port-scan	Medium	1
11	<a href="#">HTTP: php.cgi Buffer Overflow</a>	Exploit	buffer-overflow	Medium	1
12	<a href="#">P2P: BitTorrent File Transfer Han...</a>	Policy Violation	restricted-application	Medium	1
13	<a href="#">HTTP: Apache HTTP Server mod</a>	Exploit	dos	Medium	1

Figura 17: Quantidade de ataques. Portal 1 dia 2

Na tabela abaixo, temos os principais ataques aos Sítios / Portais, agrupados no período dos 5 dias. Comparando com o total de alertas emitidos para os 5 dias que é 565.485 a quantidade de ataques é de 2.182.

Upward Movers				
#	Attack Name	Recent Attack Count Value	Previous Attack Count Value	Percentage Change in Attack count
1.	ICMP: Timestamp Probe	64	4	1500.0
2.	P2P: BitTorrent Meta-Info Retrieving	1182	101	1070.3
3.	HTTP: Microsoft Word Out-of-Bounds-Read Vulnerability (CVE-2016-7268)	50	7	614.29
4.	HTTP: Mozilla Products IDN Spoofing Vulnerability aka Homograph Attacks	26	5	420.0
5.	HTTP: CGI Escape Character Directory Traversal	257	72	256.94
6.	HTTP: Microsoft ISA Server Radius OTP Bypass Vulnerability	3	1	200.0
7.	HTTP: Content Length Too Large	3	1	200.0
8.	RPC: Portmap Dump Request	345	115	200.0
9.	HTTP: Oracle BEA WebLogic Server Apache Connector DoS Vulnerability	87	33	163.64
10.	HTTP: Apache 2.0 Path Disclosure	165	65	153.85

Figura 18: Ataques Total

Abaixo segue uma tabela com os ataques efetuados contra o Portal 1 e o Portal 2, durante os 5 dias de monitoramento, a tabela apresenta os totais por dia, por portal e geral.

Ataques por Portal			
Dia	Portal 1	Portal 2	Total
1	330	6	336
2	204	2	206
3	149	3	152
4	619	2	621
5	30	3	33
Total	1332	16	1348

Tabela 3: Ataques aos Portais monitorado pelo IDS

Na figura abaixo temos um total de ataques bloqueados por tipo, os 20 mais representativos. Este gráfico foi elaborado com dados do dia 3, quando foram emitidos 130.825 alertas do IPS, foram bloqueados 1021 ataques.

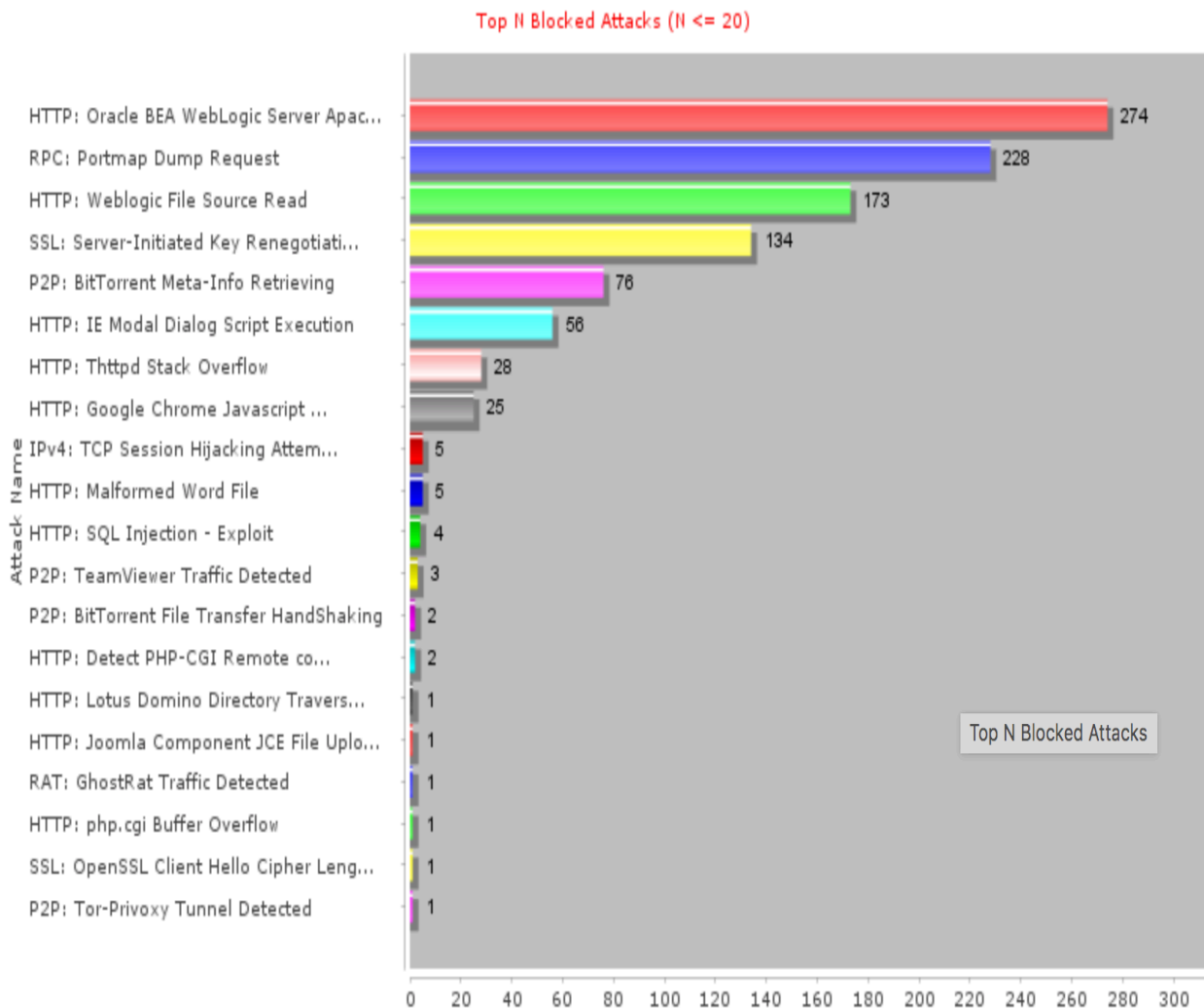


Figura 19: Ataques bloqueados Portal 1

Os dados acima expostos, demonstram que os Sítios / Portais monitorados recebem um grande número de acessos. Alguns acessos geram alertas do IPS e solicitam monitoramento e atenção ao analista de segurança. Como o IPS é uma ferramenta de prevenção de intrusão, os acessos identificados como ataques são bloqueados e relatados ao analista de segurança.

### 4.3 Detecção do HIDS OSSEC

O HIDS OSSEC monitora os computadores onde estão os Portais 1 e 2, já exemplificados acima, o Portal principal 1 tem dois servidores com balanceamento de carga e o Portal 2 tem apenas um servidor. Foram instalados os agentes OSSEC em cada uma das máquinas e o tráfego começou a ser monitorado. Note-se que o intuito é demonstrar que mesmo em uma DMZ, com várias camadas de segurança antecedentes, o OSSEC conseguiu gerar muitos alertas, o que deixa claro que a estrutura complementar é uma forma mais robusta de segurança.

#### 4.3.1 Alertas obtidos

A tabela abaixo demonstra o total de alertas acima de nível 3, emitidos no período dos 5 dias em que o estudo foi realizado. Os alertas estão agrupados por Portal e por dia. A terceira coluna apresenta os alertas de nível 3 ou superiores. Os alertas abaixo do nível 3 são bem numerosos, e são desconsiderados por serem alertas de mensagens de sistema, conforme explicado anteriormente.

A quantidade de alertas emitidas pelo OSSEC durante o período do estudo foi 39.798.242, um total bem superior aos alertas do IPS.

Alertas OSSEC acima nível 3				
Dia	Portal 1	Portal 2	Acima nível 3	OSSEC Geral
1	17774	43204	60978	11212857
2	19115	50902	70017	10396387
3	17277	49683	66960	9260402
4	1902	28415	30317	4775438
5	9199	21071	30270	4153158
Total	65267	193275	258542	39798242

Tabela 4: Alertas OSSEC acima de nível 3

Um detalhe na tabela acima, demonstrou uma anomalia, o Portal 2 que é menos solicitado gerou mais alertas que o Portal 1, depois de confirmados os dados buscou-se a detecção do motivo para tantos alertas. Constatou-se que o Sítio estava com programas desatualizados, houve a recomendação para a atualização do sítio e a criação de uma política que garanta sistemas atualizados e seguros.

A tabela abaixo, demonstra o total de alertas acima de nível 5, emitidos no período dos 5 dias em que o estudo foi realizado. Os alertas estão agrupados por Portal e por dia, a tabela apresenta os totais por dia e por portal. O total geral de alertas acima do nível 5, onde já se considera uma possibilidade de ataque ficou em 113.416.

Alertas OSSEC acima nível 5			
Dia	Portal 1	Portal 2	Total
1	23704	7574	31278
2	19902	7112	27014
3	16716	7188	23904
4	12409	4703	17112
5	9782	4326	14108
Total	82513	30903	113416

Tabela 5: Alertas OSSEC acima de nível 5.

Comparando as duas tabelas, fica nítido que a quantidade de alertas emitida pelo OSSEC é gigantesca, a maioria dos alertas é de nível 2, podendo ser desconsiderada. Acima de nível 3 ainda temos um número representativo, mas aceitável considerando a quantidade de acessos. Os alertas de acima do nível 5, devem ser considerados para buscar as melhorias na segurança da instituição.

O OSSEC permite a extração de dados para outras ferramentas, podendo assim, trabalhar com bancos de dados, gerar estatísticas e padrões. Estas informações aumentam o conhecimento do profissional de segurança sobre o comportamento, o tipo de ataques mais comuns e a estrutura da rede. A criação de regras específicas é embasada por estes conhecimentos.

Neste estudo não foi possível fazer o experimento de configuração de regras, pois não foi permitido pela instituição. Todavia com o experimento e os dados coletados algumas características da rede já foram percebidas e os profissionais de segurança já tiraram proveito dos alertas enviados pela ferramenta; os gráficos foram elaborados com a ferramenta *Qlikview*.

O gráfico abaixo, identifica o endereço de rede que gerou o alerta, isto possibilita verificar o endereço e caso necessário, incluir o endereço na lista de endereços negados (*blacklist*).

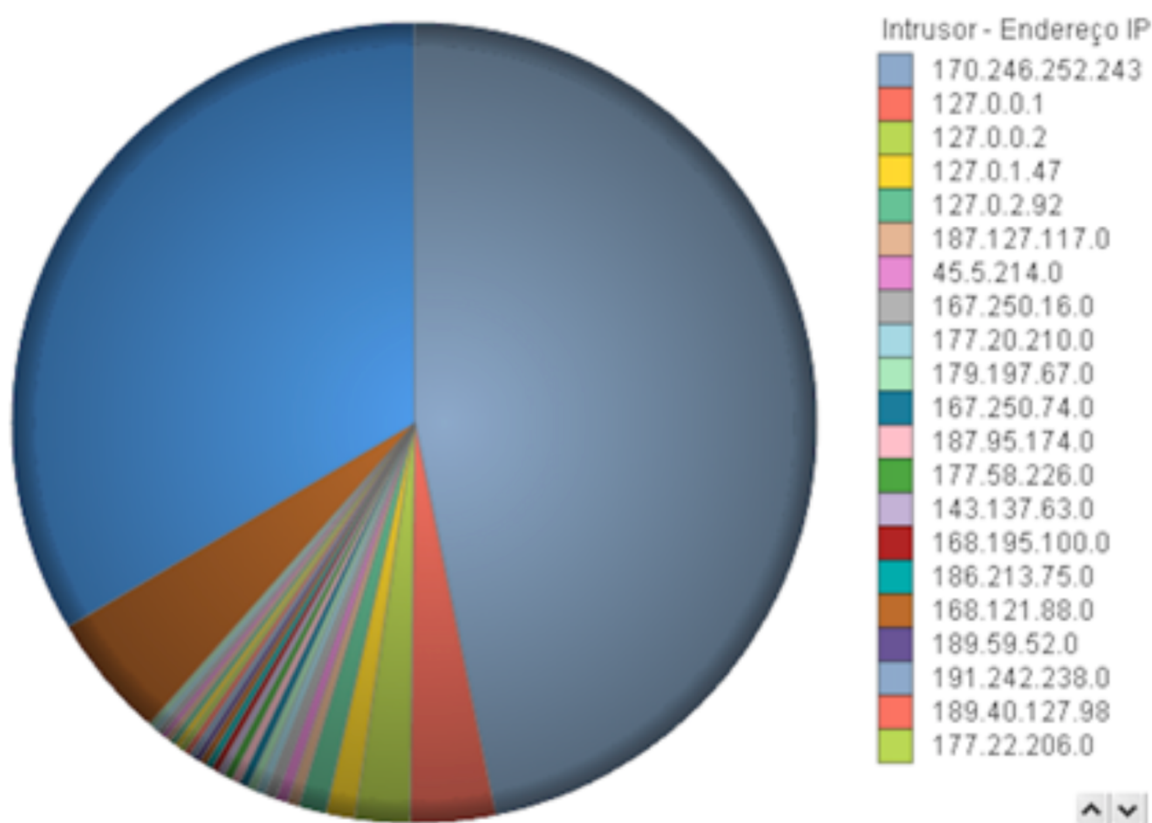


Figura 20: Endereços que geraram alertas.

No exemplo acima, temos os endereços de IP que mais efetuaram solicitações aos Portais e geraram a maior quantidade de alertas. O endereço 170.246.252.243 é o endereço de uma instituição brasileira e a quantidade de alertas foi considerada aceitável pois a origem das solicitações é conhecida.

O endereço 167.250.74.0 é de uma cidade do interior do Brasil, o endereço foi considerado suspeito pela equipa de segurança e o endereço passou a ser monitorado, uma possível solução caso o endereço persista com as solicitações é incluir o endereço na *blacklist*. O endereço 168.195.100.0 é de uma empresa prestadora de serviços de acesso a internet, foi considerado endereço seguro.

Na figura abaixo, vemos a quantidade de alertas emitidos por porta nos computadores monitorados, neste exemplo pode-se notar as portas mais solicitadas e a critério do administrador a porta que não deva estar acessível deve ser bloqueada, como neste caso notou-se que a necessidade de portas que não prestam o serviço de acesso as páginas do portal podem ser bloqueadas, buscando assim, mitigar os riscos.

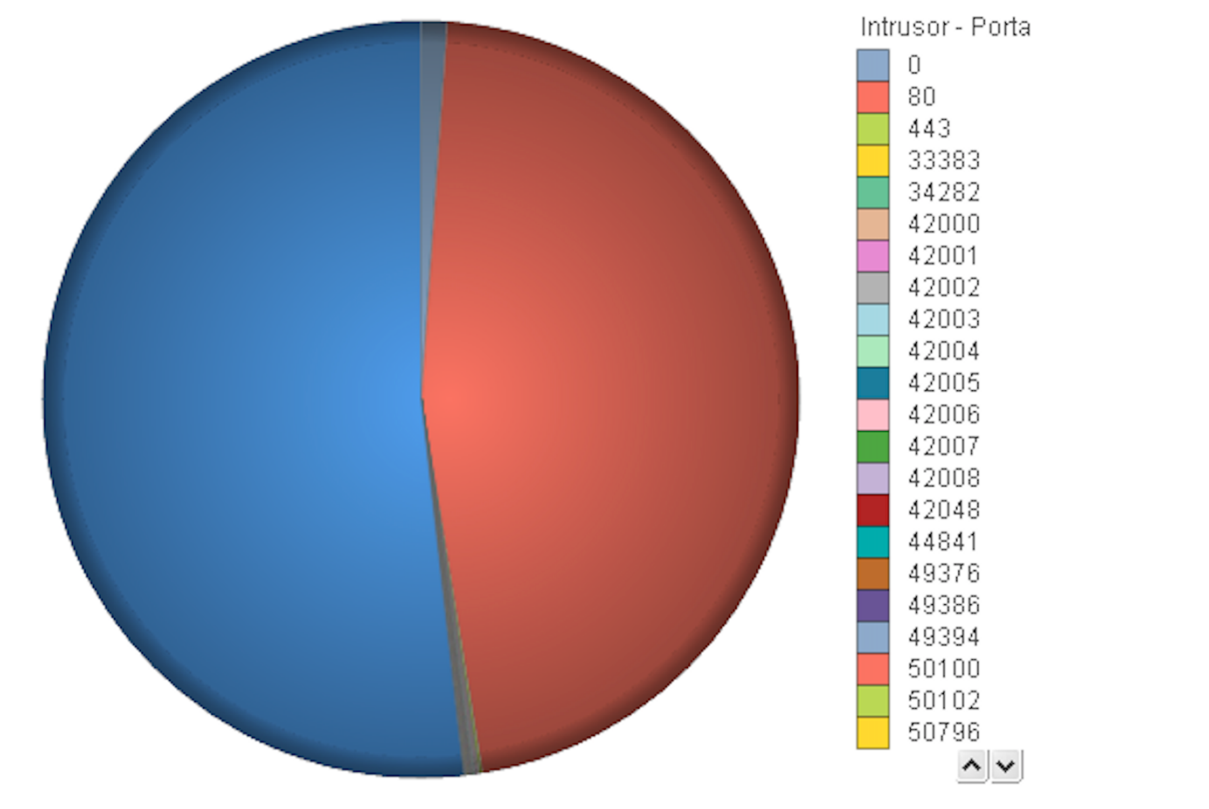


Figura 21: Detecção por porta.

Observando a figura, fica nítida a quantidade de alertas para a porta 80, que recebe as solicitações HTTP, como o monitoramento foi feito em dois portais, esta quantidade de alertas é comum. A porta 42048 responde pelas solicitações TCP – UDP, foi considerado normal a quantidade de alertas. Este relatório serve para auxiliar o analista a verificar solicitações anormais ou se alguma porta que não deveria estar recebendo solicitações está em uso, caso isto esteja ocorrendo procedimentos de segurança devem ser adotados.

#### 4.3.2 Exemplo de Detecção

A tabela abaixo é um exemplo de tabela gerada com os arquivos do OSSEC, nesta tabela temos a regra, o nível do alerta, o tipo, a descrição e a soma.

Regra	Level	Arquivo	Tipo	Descrição	SOMA
31104	6	web_rule s.xml	Web access	Common web attack.	264
31106	6	web_rule s.xml	Web access	A web attack returned code 200 (success).	23
31108	0	web_rule s.xml	Web access	Ignored URLs (simple queries).	34.219.594
31120	5	web_rule s.xml	Web access	Web server 500 error code (server error).	1.945
31122	5	web_rule s.xml	Web access	Web server 500 error code (Internal Error).	5.485
31123	4	web_rule s.xml	Web access	Web server 503 error code (Service unavailable).	21.566
31140	0	web_rule s.xml	Web access	Ignoring google/msn/yahoo bots.	20.290
31151	10	web_rule s.xml	Web access	Multiple web server 400 error codes from same source ip.	759
31153	12	web_rule s.xml	Web access	Multiple common web attacks from same source ip.	17
31162	10	web_rule s.xml	Web access	Multiple web server 500 error code (Internal Error).	37
31163	10	web_rule s.xml	Web access	Multiple web server 503 error code (Service unavailable).	85
31164	6	web_rule s.xml	Web access	SQL injection attempt.	1.035
31508	6	web_app sec_rule s.xml	BAD/Annoying user agents	Blacklisted user agent (known malicious user agent).	2.315
31515	6	web_app sec_rule s.xml	PHPMyAdmin scans	PHPMyAdmin scans (looking for setup.php).	4
31530	3	web_app sec_rule s.xml	Checking POST requests - Too many in a small type = likely a bot	POST request received.	7
40104	13	attack_ru les.xml	Attack signatures	Possible buffer overflow attempt.	1.471
160002	3	local_rul es.xml	SYSLOG,LOCAL	Connection from a host.	19
160003	8	local_rul es.xml	SYSLOG,LOCAL	Repeated connections from the same host.	1
Total					69.967.607

Figura 22: Exemplo de tabela detecções.



Tabelas assim, servem para embasar a tomada de decisão do analista de segurança, quanto mais documentação e detalhes tiver sobre o comportamento da infraestrutura, mais preparado estará para mitigar os riscos de ataques e solucionar com brevidade os que acontecerem.

No período monitorado com o OSSEC, observou-se um grande número de alertas, e o OSSEC apresentou um bom desempenho com pouca necessidade de processamento ou memória. Os níveis do alerta auxiliaram a escolha do que se deveria priorizar. Os alertas mais utilizados no OSSEC foram os seguintes.

- A verificação do tamanho das pastas dos servidores monitorados, se mostrou muito útil em uma instituição onde muitos tem senhas de administrador e podem fazer alterações nas pastas, o *checksum* ou controle de integridade é muito útil.
- O alerta de autenticação ou tentativa, foi útil para validar tentativas de acesso, possibilitando assim, a auditoria de acesso e mitigação de risco de ataques *rootkits*, ou tentativas furtivas de autenticação com senha errada.
- A informação de “palavras grandes no Log”, foi útil porque os portais são em Zope e Plone, e muitos endereços que não existem ainda estão nas páginas, possibilitando que aconteça a sua solicitação. Esses são caminhos para páginas que já não existem e isto gerava um grande tráfego de solicitações. As solicitações percorriam toda a tabela de endereços, antes de retorna o erro. Esta ação gerava transtornos na gestão de tráfego, além de ser um canal para um possível ataque Ddos, com as informações do OSSEC a equipa tomou atitudes.

#### **4.4 Exemplos de ações tomadas**

A equipa de segurança agora trabalha para tratar os alertas gerados e utilizar o conhecimento oferecido pela ferramenta, algumas ações são detalhadas abaixo.

- Corrigir os links quebrados, evitando novas solicitações e como alternativa enquanto a correção dele é feita, foi criada uma regra na memória do processador que responde a solicitação, caso ela traga como resultado um erro. Com isto se evita novas pesquisas na tabela e mitiga a possibilidade de um possível ataque.
- A deteção de ações que caracterizam a atividade de robô, realizando solicitações em um curto período ou no mesmo horário todos os dias. Um determinado endereço de internet efetuava requisições aos servidores todos os dias em um mesmo horário. Após análise se identificou que era um endereço de outro país e a quantidade de solicitações por minuto era demasiado rápida para ser

uma solicitação humana manual. Após verificado que se tratava de robô efetuando requisições, houve a inclusão do endereço na *blacklist*.

- Utilização dos dados para gerar relatórios que embasam as ações da equipa de segurança, um dos relatórios mostra a quantidade de ataques por hora. Este estudo específico por hora foi muito importante, pois comprovou o que a equipa esperava, que durante momentos de grande comoção social ou de incertezas e insatisfações da população com a instituição em estudo, os alertas do Portal 1 que produz notícias, aumentam e a possibilidade de ataques também.

Os registros de alertas utilizados para este gráfico são de um dia em que denúncias de corrupção saíram na imprensa e geraram uma grande revolta na população. Logo após a divulgação dos factos a quantidade de alertas se elevou e a tentativas de ataque também, segue o gráfico de alertas por hora.

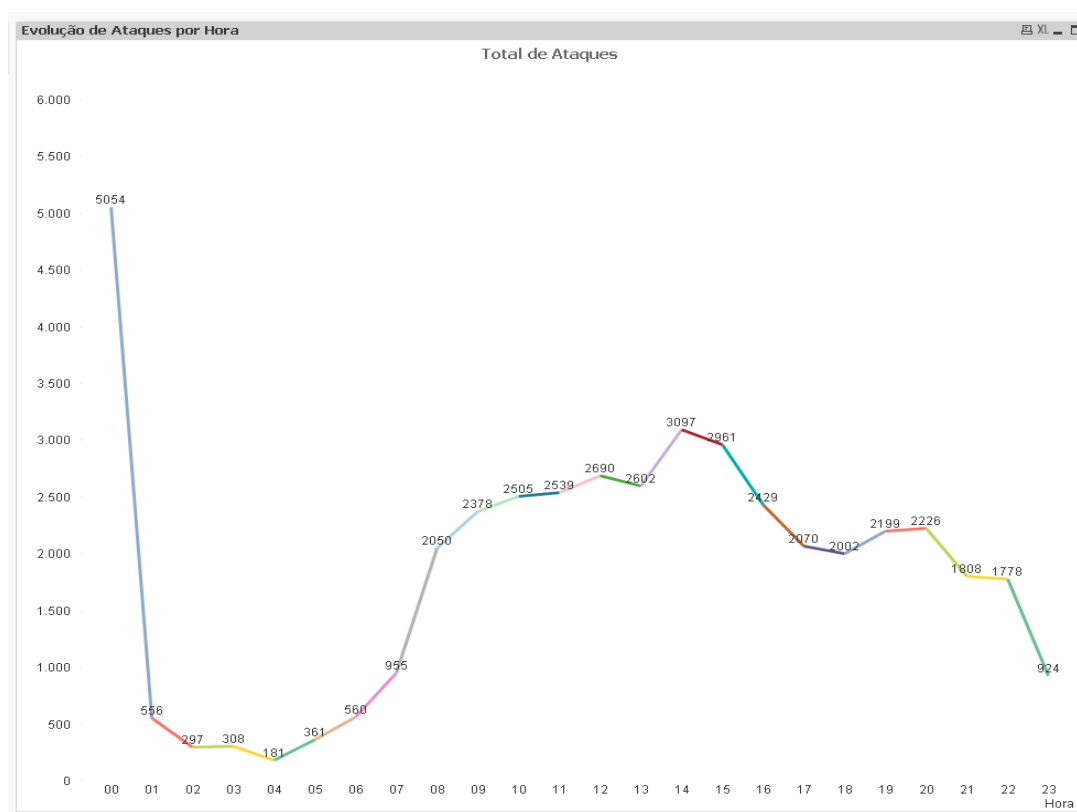


Figura 23: Quantidade de alertas gerados em um dia de conturbação social

O acontecimento nacional que suscitou o comportamento anormal da rede não será revelado para garantir a segurança da instituição.

## 4.5 Análise dos dados

A análise dos dados foi feita após os cinco dias da experiência da estrutura proposta e testada, o OSSEC foi capaz de identificar comportamentos não detetados pela *firewall*:

- “*Multiple web server 400 error codes from same source ip*”;
- “*Multiple common web attacks from same source ip*”;
- “*Multiple web server 500 error code (Internal Error)*”; e
- “*Multiple web server 503 error code (Service unavailable)*”.

Foram utilizados os registros de *Log* do OSSEC para a confecção de relatórios que servem para embasar as decisões e ações da equipa de segurança.

Dessa forma, a estrutura de *firewall* + *WAF* (*Web Firewall Application*) + OSSEC é mais robusta que uma estrutura de monitoramento apenas em rede, pois acrescenta a análise de comportamento em computador. O administrador da rede pode identificar os sintomas de um possível ataque no computador de destino, além de oferecer um registro em *Logs* dos comportamentos que permitem uma auditoria e o aprendizado de novos ataques.

A opção foi escolhida em razão do ambiente corporativo com vários computadores e a necessidade de centralização dos resultados para análise. A estrutura de agentes espalhados nos servidores e um controlador único que facilita o monitoramento e a expansão dos agentes, conforme o crescimento da infraestrutura ou da necessidade é um fator de destaque. Alguns resultados práticos obtidos com este estudo:

- Verificação de solicitações de robôs, e inclusão dos endereços na *blacklist*.
- Validação de tamanho de palavras identificando endereços inexistentes, correção do Sítio e implementação de regras de acesso.
- Grande quantidade de alertas demonstrou sítio desatualizado e inseguro, recomendação de atualização dos programas e criação de uma política.
- Verificação de *scanner* de portas, identificou vários computadores infetados na rede interna, recomendação da atualização do programa de segurança e implementação de política de segurança específica.
- Descoberta de caminho errado na rede interna que estava gerando alertas. A rede estava configurada de forma errada, correção da configuração e recomendação de documentação da infraestrutura da rede.

- Grande quantidade de alertas enviados fora do horário de expediente, caracterizou um ataque *Ddos*, foram realizadas de medidas de mitigação e contingência ao ataque.

A estrutura proposta de incluir o HIDS OSSEC em uma infraestrutura de grande porte, foi atendida e se mostrou válida pela resposta da ferramenta, que comprovou que os computadores sofriam ataques dentro da DMZ.

Se demonstrou que a infraestrutura existente não era segura, pois a DMZ estava garantida e avaliada como segura e os computadores dentro dela receberam ataques, como a rede não possuía implementado nenhum tipo de análise de computador estes ataques não eram detetados.

Como último esclarecimento, note-se que o alerta de nível de severidade 6 para cima é relevante e foram gerados em média 476 alertas/dia, acima do nível 6, sendo que estes alertas podem ser fruto de análise em tempo real, pois podem representar sintomas de ataques, auxiliando o profissional de segurança.

Ficou como recomendação para a instituição parceira, a realização de um projeto para reestruturar a infraestrutura de segurança, foi proposto que o *Firewall* deve ser a primeira linha de contenção, seguida do IPS e IDS nos computadores mais importantes. O *Waf* fica na DMZ para garantir a segurança em camada 7 e a instalação do agente OSSEC em todas os computadores da DMZ e um servidor OSSEC.

Em todos os testes, o OSSEC apresentou resultados complementares ao IPS e demonstrou que sua inserção na infraestrutura existente foi salutar. A instituição parceira começou a utilizar efetivamente o OSSEC em seu conjunto de ferramentas de segurança digital.

## 5. Conclusão

Como conclusão deste trabalho, entende-se que a ferramenta é eficaz, demonstrando através de uma quantidade de alertas significativa, a sua capacidade de monitoramento a computadores com grande quantidade de acessos, sem gerar atraso nas requisições ou dificuldades de processamento e armazenamento dos dados.

Um diferencial constatado com a utilização do OSSEC, foi a capacidade de identificar ataques internos. As tentativas de acesso não autorizado, o controle de *scanner* de rede, o controle de solicitações de robôs e o controle de tamanho de pacote são primordiais para a garantia da segurança. As funcionalidades do OSSEC auxiliam na garantia da integridade dos serviços, em ambientes corporativos de alto desempenho, e que precisam garantir a integridade, autenticidade, confidencialidade e disponibilidade.

Um dispositivo de segurança mau configurado, ou apenas com a configuração padrão, pode ser extremamente inseguro de forma que, o OSSEC oferece uma perspectiva complementar que pode servir tanto para reações diretas aos ataques, quanto à auditoria devido ao número e formato de log que produz, possibilita a geração de relatórios, integração com outras ferramentas e análises comportamentais do computador.

Nesse ínterim, conclui-se que para se garantir uma infraestrutura com Segurança Digital, o OSSEC é item necessário. A emissão de alertas e a classificação em nível, permitiram priorizar alertas que eram na verdade ataques, viabilizando a mitigação dos riscos e um aumento da segurança digital da instituição.

O modelo proposto de incluir o HIDS OSSEC em uma infraestrutura já implantada, configurou-se válido, tendo em vista que a ferramenta atendeu a todos os objetivos da investigação, sem desrespeitar as políticas de segurança da instituição pesquisada, sem gerar custos e possibilitando o sucesso nos resultados apresentados na análise.

O OSSEC é uma ferramenta sem custos, que pode atender a infraestruturas grandes ou pequenas, instituições menores que necessitam de segurança podem utilizar a ferramenta. A implantação do OSSEC é simples, com regras já configuradas e dois tipos de instalação o modo Local, que pode atender a um computador ou modo Agente e Servidor que atende estruturas maiores. Com a eficácia do OSSEC comprovada, fica a recomendação pela utilização da ferramenta.

# Bibliografia

OSSEC. Conf (2017). [Em linha]. Disponível em:

<[https://ossec.github.io/docs/syntax/head\\_agent\\_config.html](https://ossec.github.io/docs/syntax/head_agent_config.html)>. [Consultado em: 15/07/2017].

OSSEC (2012). [www.ossec.net](http://www.ossec.net). Retrieved from <http://www.ossec.net>

Cid, Daniel B. (2007). Log Analysis using OSSEC. Retrieved from <http://www.ossec.net/ossec-docs/auscert-2007-dcid.pdf>

Presidência da República, Brasil (2000). Decreto no 3.505, de 13 de junho de 2000 - institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília: Senado. [Em linha]. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto/d3505.htm](http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm)>. [Consultado em: 20/02/2017].

Presidência da República, Brasil (2015). Guia de Orientações ao Gestor em Segurança da Informação e Comunicações, Gabinete de Segurança Institucional, Secretaria Executiva, Departamento de Segurança da Informação e Comunicações. Brasília: DF. [Em linha]. Disponível em: < <http://dsic.planalto.gov.br/legislacao/guiagestor.pdf>>. [ Consultado em: 20/06/2017].

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. (2016). [Em linha]. Disponível em <https://www.cert.br/stats/incidentes>: [Consultado em: 28/07/2017].

Arora, Himanshu (2013), Introduction to intrusion prevention systems Detect and block attacks in real time, IBM

Check Point (2017). [Em linha]. Disponível em: <https://www.checkpoint.com/downloads/product-related/datasheets/4200-appliance-datasheet.pdf>. [Consultado em: 15/07/2017].

Estatísticas De Incidentes De Rede No Governo – 2º Trimestre (2017). [Em linha]. Disponível em: [http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas\\_CTIR\\_Gov\\_2Trimestre\\_2017.pdf](http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_2Trimestre_2017.pdf). [Consultado em: 23/07/2017].

Trend Micro (2010). [Em linha]. Disponível em: <https://www.trendmicro.com> [Consultado em: 15/07/2017].

Goodrich, M. T.; Tamassia R. (2013). *Introdução à Segurança de Computadores* 1ª ed. Porto Alegre: Bookman. p. 282.

- Moreno, E. D. (2005). *Criptografia em Software e Hardware*. São Paulo: Novatec Editora.
- Nakamura, E.T. (2007). *Segurança de Redes em Ambientes Cooperativos*. São Paulo: Novatec Editora.
- Nmap (2017). [Em linha]. Disponível em: <<https://nmap.org/>>[Consultado em 15/07/2017].
- Ossec. (2017). [Em linha]. Disponível em: <http://www.3way.com.br/2017/02/14/monitore-sua-rede-contra-intrusos-com-hids-ossec/> [Consultado em: 23/06/2017].
- Stallings, William (2008). *Criptografia e Segurança de Redes*. 4.ed. tradução Daniel Vieira; revisão técnica Graça Bressan, Ákio Barbosa e Marcelo Succi. - São Paulo: Pearson Prentice Hall.
- Santos, Osvaldo (2011) Fiewalls Soluções Práticas. Lisboa: FCA Editora de Informática
- Terada, Ruto - Segurança de dados: Criptografia em redes de computador - 2ª edição revisada e ampliada – São Paulo: Blusher, 2008.
- Santos, Leonardo Thomas (2001) Criptografia, Universidade Católica de Salvador
- Kizza, Joseph (2005) System Intrusion Detection and Prevention. Computer Network Security
- Zin, Nicolas (2009) OSSEC How-To – The Quick and Dirty Way
- Wang, Yang, Li (2010) Study of Network-based Intrusion Detection System for Virtualization. 2010 2nd International Conference on Computer Engineering and Technology.
- Nascimento, Gustavo Miguel Barroso Assis do (2010), Anomaly detection of web-based attacks, Universidade de Lisboa
- Robertson, CHAD (2011) Practical OSSEC, SANS Institute InfoSec Reading Room
- Rossi, Jeremy (2015), OSSEC Documentation, Release 2.8.1
- Vokorokos, Kleinova, Latka (2006) Network Security on the Intrusion Detection System Level. INES 2006- 10th International Conference on Intelligent Engineering Systems.

# Anexo A

1 - Detalhes para integração do Portsentry ao OSSEC.

No arquivo `/var/ossec/etc/decoder.xml`, retirar o trecho a seguir:

```
<!-- Portsentry -->
  <decoder name="portsentry">
    <program_name>^portsentry</program_name>
  </decoder>
  <decoder name="portsentry-attackalert">
    <parent>portsentry</parent>
    <prematch>attackalert: Connect from host: </prematch>
    <regex offset="after_prematch">(\S+)/\S+ to (\S+) port:
    (\d+)\$</regex>
    <order>srcip,protocol,dstport</order>
  </decoder>
  <decoder name="portsentry-blocked">
    <parent>portsentry</parent>
    <prematch>is already blocked. Ignoring$</prematch>
    <regex>Host: (\S+) is</regex>
    <order>srcip</order>
  </decoder>
```

No arquivo com as informações do decodificador é necessário uma alteração, editar a pasta `/var/ossec/etc/decoder.xml`, antes do EOF, inserir o trecho a seguir:

```
<decoder name="portsentry">
  <program_name>^portsentry</program_name>
</decoder>

<decoder name="portsentry-attackalert">
  <parent>portsentry</parent>
  <prematch>attackalert: TCP SYN/Normal scan from host: </prematch>
  <regex offset="after_prematch">(\S+)/\S+ to (\S+) port:
  (\d+)\$</regex>
  <order>srcip,protocol,dstport</order>
</decoder>

<decoder name="portsentry-blocked">
```



```

    <parent>portsentry</parent>
    <prematch>is already blocked Ignoring$</prematch>
    <regex>Host: (\S+)/\S+ is</regex>
    <order>srcip</order>
</decoder>

```

```

<decoder name="portsentry-scan">
    <parent>portsentry</parent>
    <prematch>^attackalert: </prematch>
    <regex offset="after_prematch">scan from host: (\S+)/\S+ to \S+ port:
(\d+)$</regex>
    <order>srcip, dstport</order>
</decoder>

```

```

<decoder name="portsentry-host">
    <parent>portsentry</parent>
    <prematch offset="after_parent">^attackalert: Host: </prematch>
    <regex offset="after_prematch">^(\S+)/\S+ </regex>
    <order>srcip</order>

```

No arquivo com as informações das regras, é necessário editar a pasta /var/ossec/rules/local\_rules.xml, antes do EOF, inserir o trecho a seguir:

```

<group name="syslog,portsentry,">
    <rule id="160000" level="0" noalert="1">
        <decoded_as>portsentry</decoded_as>
        <description>Grouping for the PortSentry rules</description>
    </rule>

    <rule id="160002" level="3">
        <if_sid>160000</if_sid>
        <match>attackalert:</match>
        <description>Connection from a host.</description>
    </rule>

    <rule id="160003" level="8" frequency="4" timeframe="180" ignore="60">
        <if_matched_sid>160002</if_matched_sid>
        <description>Repeated connections from the same host.</description>
        <same_source_ip/>

```

```
    <group>recon,</group>
  </rule>

  <rule id="160004" level="10" frequency="8" timeframe="180"
ignore="60">
    <if_matched_sid>160002</if_matched_sid>
    <description>Host is still scanning</description>
    <same_source_ip />
    <group>recon,</group>
  </rule>
</group>
```

## Anexo B

Detalhes para integração do Nmap ao OSSEC.

Acesso o arquivo `/var/ossec/etc/ossec.conf`, e adicione a saída nmap:

```
<ossec_config>
  <localfile>
    <log_format>nmapg</log_format>
    <location>/var/log/nmap-out.log</location>
  </localfile>
</ossec_config>
```

Se o arquivo não existir, criar o arquivo na linha de comando:

```
# touch /var/log/nmap-out.log
```

Reiniciar o OSSEC:

```
#!/var/ossec/bin/ossec-control restart
```

Rodar o scan do nmap (exemplo: 192.168.2.0/24 network):

```
# nmap --append_output -sU -sT -oG /var/log/nmap-out.log 192.168.2.0/24
```